SecureTransport

Version 5.4

2 April 2024

Administrator's Guide

Copyright © 2019 Axway

All rights reserved.

This documentation describes the following Axway software:

Axway SecureTransport 5.4

No part of this publication may be reproduced, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of the copyright owner, Axway.

This document, provided for informational purposes only, may be subject to significant modification. The descriptions and information in this document may not necessarily accurately represent or reflect the current or planned functions of this product. Axway may change this publication, the product described herein, or both. These changes will be incorporated in new versions of this document. Axway does not warrant that this document is error free.

Axway recognizes the rights of the holders of all trademarks used in its publications.

The documentation may provide hyperlinks to third-party web sites or access to third-party content. Links and access to these sites are provided for your convenience only. Axway does not control, endorse or guarantee content found in such sites. Axway is not responsible for any content, associated links, resources or services associated with a third-party site.

Axway shall not be liable for any loss or damage of any sort associated with your use of third-party content.

Revision history

The following changes are added to the SecureTransport 5.4 Administrator's guide:

SecureTransport version	Document revision number	Updated topics
5.4	rev. 01 – initial version	
5.4	rev. 02	Advanced SSL Settings updated in: • *AS2 transfer sites* on page 497 • *SSH transfer sites* on page 579 • *HTTP(S) transfer sites* on page 552 • *PeSIT transfer sites* on page 559 • *FTP(S) transfer sites* on page 515
5.4	rev. 03	• Transfer Sites updated with Alternative endpoints: ◦ *AS2 transfer sites* on page 497 ◦ *HTTP(S) transfer sites* on page 552 ◦ *SSH transfer sites* on page 579 ◦ *PeSIT transfer sites* on page 559 ◦ *FTP(S) transfer sites* on page 515 • Extended server control view topic added: ◦ *Extended Server Control* on page 262 ◦ *Add an FTP server* on page 268 ◦ *Add an SSH server* on page 278 ◦ *Add an HTTP server* on page 271 ◦ *Add an AS2 server* on page 275 ◦ *Add a PeSIT server* on page 282
5.4	rev. 04	A "Redirect hostname" option added to the *Add an HTTP server* on page 271 topic.

SecureTransport version	Document revision number	Updated topics
5.4	rev. 05	MS SQL 2017 support added to the *Axway and third-party software support* on page 39 topic for: • Enterprise Cluster • SecureTransport on AWS
5.4	rev. 06	Maximum parallel transfers configuration added to the following subtopics: • *Transfer site properties* on page 495 • *AS2 transfer sites* on page 497 • *HTTP(S) transfer sites* on page 552 • *SSH transfer sites* on page 579 • *FTP(S) transfer sites* on page 515 • *Generic HTTP transfer sites* on page 525 • *SharePoint transfer sites* on page 572 • Standard cluster setup – *Configuration optimizations in case of increased transfers load* on page 343 • Enterprise cluster setup – *Configuration optimizations in case of increased transfers load* on page 361
5.4	rev. 07	• An "Explicitly uses SiteMinder Attributes" option added to *SiteMinder integration configuration* on page 420 • DSA key support for SSH authentication on transfer sites added
5.4	rev. 08	• Start/Stop controls for Folder Monitor and Scheduler added to *Extended Server Control* on page 262 for SecureTransport Server • *Define attribute mappings for a domain* on page 441 topic updated • Total number of Active users added to *Display the list of user accounts* on page 454 • Total number of search results added to *Track file transfer activity* on page 290
5.4	rev. 09	• *Graceful shutdown of Transaction Manager* on page 266 topic added • *Generate Usage report* on page 162 topic added

SecureTransport version	Document revision number	Updated topics
5.4	rev. 10	• *Define Address Book settings for a domain* on page 443 updated • *Zero downtime in active-passive deployment* on page 356 added • *Graceful shutdown* on page 264 updated with *Graceful shutdown of Transaction Manager* on page 266 and *Graceful shutdown of SecureTransport Server node* on page 267
5.4	rev. 11	• *Track file transfer activity* on page 290 updated
5.4	rev. 12	• *XFB Tracked Object attributes* on page 123 updated • *Configure SecureTransport to send events to Axway Sentinel* on page 148 updated
5.4	rev. 13	• *Using DXAGENT_TRANSFERSAPI variables in transfer sites* on page 497 added • *Extended Server Control* on page 262 updated
5.4	rev. 14	The following topics are updated to reflect the added support for Microsoft Windows Server 2016 and Microsoft Windows Server 2019: • *Axway and third-party software support* on page 39 • *Real users* on page 687
5.4	rev. 15	The following topics are updated with instructions on configuring Pre-connection in PeSIT transfer sites and automatic SSL mode detection for PeSIT transfers: • *Manage the PeSIT server* on page 258 • *Add a PeSIT server* on page 282 • *PeSIT transfer sites* on page 559 • *PeSIT file transfers fail over TLSv1 Legacy for certain ciphers* on page 977 • PeSIT file transfer from SecureTransport to other MFT products fail over TLSv1 Legacy for certain ciphers

SecureTransport version	Document revision number	Updated topics
5.4	rev. 16	• `Substring` added to the EL functions in the *Predefined functions* on page 1022 topic • Oracle 18c added to the list of *Axway and third-party software support* on page 39 • New User class variables added to *Custom expressions* on page 711 • *Configure a secret question* on page 627updated with instructions for setting minimum length for the Secret question answer • Status scripts added to *Utility files* on page 987
5.4	rev. 17	The following topics are updated with information and instructions on using custom JDBC URLs for external Oracle and Microsoft SQL Server databases: • *Change the external Oracle database* on page 100 • *Change the external Microsoft SQL Server database* on page 102
5.4	rev. 18	• *Configure a secret question* on page 627 updated with details on steaming environment configuration • *View file transfer information* on page 293 updated • *Configure SSH server settings* on page 85 updated • *Applications* on page 756 topic updated
5.4	rev. 19	• SSLCypher and SSLAuth attributes in *XFB Tracked Object attributes* on page 123 updated • *Pluggable Transfer Sites* on page 599 topic updated

SecureTransport version	Document revision number	Updated topics
5.4	rev. 20	• *PeSIT transfer sites* on page 559 updated with new settings (Connection timeout, Originator, Store and Forward Mode, and Final destination) • *Send To Partner* on page 881updated with new advanced PeSIT setting (Originator) • `FinalReceiverId` and `OriginalSenderId` in *XFB Tracked Object attributes* on page 123 updated due to behavior changes • *Command line client (FTP, FTPS, HTTPS, and SSH) user authentication* on page 379 updated • *Configure client certificate authentication settings* on page 382 updated • *Utility files* on page 987 updated • *Pluggable authentication* on page 407 updated with instructions for updating plug-ins • *Pluggable authorization* on page 706 updated with instructions for updating plug-ins • *Subscribe to Advanced Routing application* on page 821 updated with details on using flow and subscription attributes • *Mail template commands and variables* on page 173 updated • *Account templates* on page 661 updated • *Session related EL expressions* on page 922 updated • *Change the external Microsoft SQL Server database* on page 102 updated • *FIPS-certified cryptographic libraries* on page 983 and *Advertised ciphers and cipher suites in FIPS mode* on page 984 updated • Instructions for *Configuring asynchronous MDN receipts with AS2 transfers* on page 950 added
5.4	rev. 21	*PeSIT transfer sites* on page 559 updated
5.4	rev. 22	`repconv` in *Utility files* on page 987 updated

SecureTransport version	Document revision number	Updated topics
5.4	rev. 23	• *SSH transfer sites* on page 579 updated with Test connection • *Zero downtime in active-passive deployment* on page 356 updated • *Graceful shutdown of SecureTransport Server node* on page 267 added • *Password policy* on page 185 updated with Minimum password age • *External Script* on page 850 updated with Run scripts as root option • *Enterprise Cluster rules* on page 1017 updated • *View file transfer information* on page 293 updated with `X-Forwarded-For` parameter • *General log files* on page 998 updated to cover the scenario when the user is connecting through an HTTP proxy or a load balancer • *XFB Tracked Object attributes* on page 123 updated • *Event states* on page 110 updated • *Configure SecureTransport to send events to Axway Sentinel* on page 148 updated • *Axway Sentinel tracked objects* on page 112 updated with `EnvironmentID`
5.4	rev. 23	• *Standard browser client* on page 329 updated with instructions on how to control the display of server information and configure response caching policies • *Axway and third-party software support* on page 39 updated • *Axway Sentinel tracked objects* on page 112 updated with `parentCycleID` • *CycleId calculation* on page 146 updated with SFTP transfer tracking • *XFB Tracked Object attributes* on page 123 updated with parent cycle ID

SecureTransport version	Document revision number	Updated topics
5.4	rev. 24	• New settings to avoid filename collision added to the *Decompress* on page 842 step • *Custom Expression Language functions and variables* on page 921 updated
5.4	rev. 25	• Oracle 19c added to *Axway and third-party software support* on page 39 • PeSIT pre-connection settings updated • New metrics added to the SecureTransport usage report • *SecureTransport cipher suites* topic moved to SecureTransport 5.4 Security Guide • `hmac-sha256` and `hmac-sha256@ssh.com` cipher suites added to the FIPS allowed MACs
5.4	rev. 26	• *FIPS transfer mode* on page 983 updated • *Advertised ciphers and cipher suites in FIPS mode* on page 984 updated • The following topics are updated with new settings for protocol servers that allow modifying the list of allowed cipher suites, ciphers, and algorithms in FIPS mode. ◦ *Add an FTP server* on page 268 ◦ *Add an SSH server* on page 278 ◦ *Add an HTTP server* on page 271 ◦ *Add an AS2 server* on page 275 ◦ *Add a PeSIT server* on page 282 • The following topics are updated with new settings in the transfer site configuration that allow modifying the list of allowed cipher suites, ciphers, and algorithms in FIPS mode ◦ *AS2 transfer sites* on page 497 ◦ *FTP(S) transfer sites* on page 515 ◦ *HTTP(S) transfer sites* on page 552 ◦ *PeSIT transfer sites* on page 559 ◦ *SSH transfer sites* on page 579

SecureTransport version	Document revision number	Updated topics
5.4	rev. 27	• `repconv` in *Utility files* on page 987 updated • `ProtocolFileName` and `ProtocolFileLabel` in *XFB Tracked Object attributes* on page 123 updated • *Configure Kerberos as an Identity Provider in SecureTransport* on page 404 topic updated
5.4	rev. 28	• *Manage subscriptions* on page 607 topic updated
5.4	rev. 29	• *Advertised ciphers and cipher suites in FIPS mode* on page 984 updated • *PGP Encryption* on page 829 topic updated • *PGP Decryption* on page 835*PGP Encryption* on page 829 topic updated
5.4	rev. 30	• New topic added: *Command line directory or file listing* on page 990 • *Modify the log4j files* on page 1001 updated • *Manage subscriptions* on page 607 updated • *Bandwidth limits* on page 186 updated
5.4	rev. 31	• *Custom expressions* on page 711 updated with new user attributes
5.4	rev. 32	• *Server log* on page 304 updated • *Track file transfer activity* on page 290 updated
5.4	rev. 33	• *Disable the SecureTransport login* on page 381 updated • *Standard browser client* on page 329 updated • *Command line directory or file listing* on page 990 updated • *Add an SSH server* on page 278 updated • "Configure security policies and HTTP response headers" topic moved to SecureTransport 5.4 Security Guide

SecureTransport version	Document revision number	Updated topics
5.4	rev. 34	The following topics are updated with new configuration options to control the usage of expired certificates: • *SSH transfer sites* on page 579 • *HTTP(S) transfer sites* on page 552 • *PeSIT transfer sites* on page 559 • *FTP(S) transfer sites* on page 515
5.4	rev. 35	*Publish To Account* on page 875 topic updated with a configuration option for better control over Replace of existing file
5.4	rev. 36	*Manage an active/passive cluster* on page 347 updated
5.4	rev. 37	*SSH transfer sites* on page 579 topic added *Update Permissions with Chmod Command* option, to determine whether to use `chmod` or `umask` command to change file permissions
5.4	rev. 38	• Added steps relating to the *Subscription Folder Discovery* option, to better handle multiple subscriptions, in: *Create a user account* on page 456 and *Manage account templates* on page 663 • *External Script* on page 850 topic updated examples of script expressions
5.4	rev. 39	• *Create an Archive Maintenance application* on page 760 updated with options to enable multithreading and set a runtime limit • New troubleshooting topics added: ◦ *Troubleshooting I/O problems* on page 981 ◦ *AR fails while copying the file to sandbox* on page 949
5.4	rev. 40	• *Configure SecureTransport to send events to Axway Sentinel* on page 148 updated

SecureTransport version	Document revision number	Updated topics
5.4	rev. 41	• *Duplicate an account* on page 622 updated • Corrected the example to attach a logger to a non-blocking asynchronous appender in *Modify the log4j files* on page 1001 • *Add a server to a cluster* on page 361 updated • *Remove a server from a cluster* on page 363 updated • New subsection "Proxy states and blacklisting" added to *Manage the communication across Transaction Manager, protocol and proxy servers* on page 218
5.4	rev. 42	• *Filesystem restrictions* on page 723 updated

Contents

Preface **30**
Who should read this document 30
Related documentation 30
Get more help 31

1 SecureTransport overview **33**
SecureTransport Server 34
SecureTransport Edge 36
Deployment models 37
Cluster models 37
Standalone deployment 37
SecureTransport clients 37
Ad hoc file transfers 38
Axway and third-party software support 39
Operating systems 39
Databases for Enterprise Clusters 40
Browsers 41
Software for file exchange 41
Authentication providers and directory services 43
ICAP 44
Business activity monitoring and governance 45
Proxy software 45
PGP 45
File systems 46

2 Setup **48**
Log in to the SecureTransport Administration Tool 49
Certificates 50
Certificate types 51
Certificate Management page 52
Repository encryption certificate 52
Manage local certificates and certificate signing requests 54
Manage trusted CAs 61
Manage the internal CA 63
Change the certificate keystore password 68
Certificates to generate during initial setup 69
Store certificates in a hardware security module 69
PGP key encryption and signing 72
Manage PGP keys 72

PGP transfer settings dependencies ... 74
Configure FTP server messages and modes ... 76
FTP server messages ... 78
Set up FTP active mode ... 79
Set up FTP passive mode ... 80
FTP server limitations ... 82
Improve FTP performance on a multi-homed system ... 83
Increase the timeout for large files using server-initiated transfer ... 83
Configure AS2 server settings ... 84
Configure AS2 transfer settings ... 84
Configure SSH server settings ... 85
Bind SSH and SSHD to the same port number ... 86
Debug SSH issues ... 86
Configure Administration Tool server settings ... 87
Change password settings ... 87
Change session settings ... 88
PeSIT server configuration settings ... 88
Configure adhoc file transfers ... 89
Change the package manager base folder ... 94
Configure your database ... 94
Change the embedded database port or password ... 95
Switch from the embedded database to an external Oracle database ... 96
Direct log data to separate Oracle databases ... 99
Change the external Oracle database ... 100
Improve server resiliency in case of Oracle RAC node failure ... 101
Change the external Microsoft SQL Server database ... 102
Register SecureTransport in Central Governance ... 103
SecureTransport registration in Central Governance prerequisites ... 103
Central Governance configuration ... 105
SecureTransport registration troubleshooting ... 108
Integrate Axway Sentinel ... 109
Event states ... 110
Axway Sentinel tracked objects ... 112
About XFB Transfer tracked objects ... 117
PeSIT protocol ... 117
List of PeSIT states ... 120
XFB Tracked Object attributes ... 123
CycleId calculation ... 146
Axway Sentinel requests ... 148
Configure SecureTransport to send events to Axway Sentinel ... 148
Integrate Decision Insight ... 152
Event states ... 152
Tracked objects ... 153
XFB Transfer tracked objects ... 154

Configure SecureTransport to send events to Decision Insight 155
Server licenses 157
Account session count 158
Ad hoc user licenses 158
Updating SecureTransport licenses 158
Usage reporting for subscription-based licenses 159
What is usage tracking? 159
Must I enable usage tracking? 160
What if I don't enable usage tracking? 160
How do I enable usage tracking? 160
Set up usage reporting 160
Generate Usage report 162
Configure FTP command log 166
Add a command logging entry 167
Enable or disable command logging entries 167
Edit a command logging entry 168
Delete command logging entries 168
FTP SITE META command 168
Configure transfer log 170
Add transfer logging entries 170
Enable or disable transfer logging entries 171
Edit transfer logging entries 171
Delete transfer logging entries 172
Configure holiday schedule 172
Mail templates 173
Mail template commands and variables 173
Add a mail template for AdHoc, Enrollment, or Advanced Routing notifications 176
Download a mail template 177
Upload an updated mail template 177
Delete mail templates 177
Configure miscellaneous settings 178
Miscellaneous options 178
SMTP configuration 183
FTP and HTTP server suspend options 184
Password policy 185
Bandwidth limits 186
ICAP settings 187
The ICAP Server(s) provide 187
Setup of ICAP servers 188
ICAP scan policy expression language 195
Transaction Manager 199
Rules 201
Built-in rules packages 202
Manage rules packages 207

Install agents or functions ... 211
File archiving ... 212
File archiving global configuration ... 213
Communication across Transaction Manager, protocol, and proxy servers ... 215
Streaming deployment ... 216
Manage the communication across Transaction Manager, protocol and proxy servers ... 218
Configure SecureTransport Back End to Edge streaming communication ... 227
Address Book ... 233
Address Book sources ... 233
Address Book configuration settings ... 235
Address Book use cases ... 241
Address Book REST API ... 245

3 Operations ... 249
Operations menu overview ... 250
Server control ... 250
Manage server operations ... 252
Manage the FTP server ... 254
Manage the HTTP server ... 254
Manage the AS2 server ... 255
Manage the SSH server ... 256
Manage the PeSIT server ... 258
Manage the Transaction Manager server ... 259
Manage the Proxy server on SecureTransport Edge ... 260
Manage the Monitor server ... 260
Use the operating system to monitor SecureTransport processes ... 261
Extended Server Control ... 262
Graceful shutdown ... 264
Add an FTP server ... 268
Add an HTTP server ... 271
Add an AS2 server ... 275
Add an SSH server ... 278
Add a PeSIT server ... 282
Server usage monitor ... 287
Server sessions by User Class ... 288
Bandwidth usage by login name ... 288
Server sessions ... 289
Auto refresh Server Usage Monitor info ... 289
Disable automatic snapshot updates ... 290
Track file transfer activity ... 290
Resubmit status ... 291
Transfer status ... 292
View file transfer information ... 293
Manage file transfers ... 303

Transfer Log Maintenance application 304
Server log 304
Search and view server log contents 305
Export the results of a server log search 307
Log Entry Maintenance application 307
Audit log 308
Search and view audit log contents 310
Enable or disable audit logging 311
Export the results of an audit log search 311
Add or edit an audit log entry comment 312
Display audit log entry details 312
Compare audit log entries 312
Link to the audit log 313
Audit Log Maintenance application 314
Server configuration 314
Editable server configuration parameters 315
Local server configuration parameters 315
View and change server configuration parameters 315
Update server configuration files 317
Export and import server configuration 318
Support tool 324
Configure the support tool 325
Add custom information to the support information file 326
Run the support tool 327
Directory browsing 328
Set up the structure for directory browsing 328
Standard browser client 329
Customize a web client 329
Server backup 333

4 Standard Cluster 335
Standard Cluster model 335
Active/active and active/passive clustering 336
Scheduled tasks 340
Consolidated log data representation 340
Services used for cluster management 340
Cluster configuration and setup 341
Set up an active/active cluster 341
Specify the cluster connection timeout 343
Configure servers in a cluster to trust a certificate 344
Set up an active/passive cluster 344
Manage a Standard Cluster 344
Manage an active/active cluster 345
Manage an active/passive cluster 347

Standard Cluster synchronization ... 348

5 Enterprise Cluster ... 351

Enterprise Cluster model ... 351
Enterprise Cluster deployment ... 352
Workload distribution ... 353
Passive disaster recovery ... 354
Zero downtime in active-passive deployment ... 356
Manage an Enterprise Cluster ... 359
Enterprise Cluster prerequisites ... 359
Set up a cluster ... 360
Configuration optimizations in case of increased transfers load ... 361
Add a server to a cluster ... 361
Remove a server from a cluster ... 363
View cluster status ... 363
Notification of cluster status ... 364
Set up a disaster recovery cluster ... 365
Maintain a disaster recovery cluster ... 366
Disaster recovery failover and fallback ... 367
Direct cluster workload ... 368

6 SecureTransport Edge synchronization ... 372

Manual synchronization ... 372
Requirements for synchronization ... 373
What information is synchronized ... 373
Set up SecureTransport Edge servers for synchronization ... 374
Manually synchronize SecureTransport Edge servers ... 375
Maintain synchronized SecureTransport Edge servers ... 375

7 SiteMinder integration ... 377

SiteMinder overview ... 377
User authentication ... 378
Web client (HTTP and HTTPS) user authentication ... 379
Command line client (FTP, FTPS, HTTPS, and SSH) user authentication ... 379
User access control (authorization) ... 379
Configure SiteMinder for SecureTransport integration ... 381
Configure SiteMinder settings in SecureTransport ... 381
Disable the SecureTransport login ... 381
Configure client certificate authentication settings ... 382
Import trusted CA certificates ... 382
Update the Secure Socket Layer settings ... 382
Integration troubleshooting ... 383
SiteMinder troubleshooting tools ... 383
SecureTransport troubleshooting tools ... 383

8 Authentication **385**
Single Sign-On (SSO) and Single Logout (SLO) 386
Single Sign-On (SSO) configuration 387
SecureTransport Single Sign-On (SSO) configuration prerequisites 387
Single Sign-On (SSO) configuration files overview 388
Accessing Single Sign-On (SSO) attributes 391
Access the system attributes 392
Enable Single Sign-On (SSO) for administrators 393
Configure Single Sign-On (SSO) for administrators 393
Single Sign-On (SSO) administrators configuration 394
Enable Single Sign-On (SSO) for end-users 395
Configure Single Sign-On (SSO) for end-users 395
Single Sign-On (SSO) account configuration 397
Multiple Identity Provider configuration 398
Identity Provider resolution 398
Identity Provider resolution for administrators 398
Identity provider resolution for end-users 400
Tenant resolution 401
Configure Single Sign-On (SSO) for streaming 401
Configure Single Sign-On (SSO) for clusters 402
SecureTransport as an Identity Provider 402
Single Sign-On SSO authentication flows 403
Service Provider initiated Single Sign-On (SSO) authentication flow 403
Identity Provider initiated Single Sign-On (SSO) authentication flow 403
Service Provider initiated Single Logout (SLO) authentication flow 403
Identity Provider initiated Single Logout (SLO) authentication flow 404
Configure Kerberos as an Identity Provider in SecureTransport 404
Generate a Kerberos keytab file on Windows 404
Create a Kerberos configuration file 405
Edit the sso-enduser.xml file 405
Configure supported browser authentication 406
Verify SSO authentication 406
Pluggable authentication 407
Plug-in deployment 407
Plug-in registration 408
Plug-in activation 408
Plug-in management 408
Plug-in configuration 409
Pluggable authentication status 409
Plug-in authentication notifications 409
User mapping 410
System attributes 411
Usage in User Class custom expressions 411
Login settings 412

End-user login options ... 412
Administrator login options ... 417
SiteMinder integration configuration ... 420
LDAP integration ... 426
LDAP connections, binds, and searches ... 427
LDAP logins ... 427
LDAP domains ... 429
Create an LDAP domain ... 430
Define LDAP search criteria for a domain ... 433
Define LDAP user settings for a domain ... 440
Define attribute mappings for a domain ... 441
Manage DN filters for a domain ... 442
Manage DN filters ... 442
Define Address Book settings for a domain ... 443
Edit a domain ... 445
Delete domains ... 445
Configure default domains ... 446
LDAP domains example ... 446
Secure LDAP ... 447
LDAP and Active Directory configuration ... 447
LDAP home folders ... 448
Create a home folder entry ... 448
Enable or disable home folder entries ... 449
Edit a home folder entry ... 449
Delete home folder entries ... 449
LDAP user type ranges ... 450
Create a user type range entry ... 450
Enable or disable user type range entries ... 451
Edit a user type range entry ... 451
Delete user type range entries ... 451

9 Manage accounts ... 452

Accounts overview ... 452
User accounts ... 453
Service accounts ... 453
Subscriptions, transfer sites, and certificates ... 453
Applications ... 453
User accounts ... 453
Display the list of user accounts ... 454
Create a user account ... 456
Maker-Checker user creation ... 464
Web password compatibility ... 465
View account settings ... 465
Change how long user account information is cached in memory ... 466

Disable or enable a user account ... 466
Lock or unlock a user account ... 466
Expire a user account password ... 467
Change a user account password ... 467
Edit user account settings ... 468
Delete user accounts ... 470
Delete and purge a user account ... 470
Export a single user account ... 470
Unlicensed users ... 471
Protected folders and accounts ... 475
User certificates ... 476
Manage certificates ... 476
Transfer sites ... 494
Transfer site properties ... 495
Using DXAGENT_TRANSFERSAPI variables in transfer sites ... 497
AS2 transfer sites ... 497
Connect:Direct transfer sites ... 505
File services interface protocol transfer sites ... 508
Folder Monitor transfer sites ... 511
FTP(S) transfer sites ... 515
Supported Active / Passive FTP(S) connections ... 525
Generic HTTP transfer sites ... 525
HTTP(S) transfer sites ... 552
PeSIT transfer sites ... 559
SharePoint transfer sites ... 572
SSH transfer sites ... 579
System to Human transfer sites ... 595
Manage transfer sites ... 597
Pluggable Transfer Sites ... 599
Transfer profiles ... 600
Create a transfer profile ... 600
Edit a transfer profile ... 602
Delete a transfer profile ... 603
Subscriptions ... 603
Encryption options ... 604
Post-transmission actions ... 605
Manage subscriptions ... 607
Manage service accounts ... 621
Export a single service account ... 622
Duplicate an account ... 622
Control login name case sensitivity ... 623
Password Reset ... 624
Configure a secret question ... 627

10 Advanced account administration 631
Account export and import 631
Account XML schema 632
Edit an XML file 632
Export and import accounts 636
Manage administrator accounts 644
Add an administrator account 647
Edit an administrator account 648
Delete an administrator account 649
Lock an administrator account 650
Unlock an administrator account 650
Expire an administrator account password 650
Reset an expired administrator account password 651
Change administrator password 651
Delegated administration 651
Maker and Checker 652
Create a delegated administrator 654
Administrative roles 655
Predefined administrative roles 656
Add an administrative role 659
Edit an administrative role 661
Account templates 661
Account templates and external users 662
Account template required values 663
Manage account templates 663
Site templates 681
Manage site templates 681
Use a site template to define a transfer site 685
System users 687
Real users 687
Manage password files 688
Business units 692
Manage business units 692
Display active users 700
Client-initiated and server-initiated transfers 701
Transfer mode for server-initiated transfers 702
Transfer multiple files 702
Configure retry parameters for server-initiated transfers 703
Outgoing connections 703
Authentication methods 703
Server authentication 704
Limitations for server-initiated transfers 704
Encryption and server-initiated transfers 705

11 Access control **706**
Pluggable authorization 706
Plug-in deployment 707
Plug-in registration 707
Plug-in activation 708
Plug-in management 708
Plug-in configuration 708
Plug-in authorization notifications 709
Plug-in authorization considerations and special cases 709
Plug-in file filtering capabilities 710
User classes 710
Default user classes 711
Custom expressions 711
Manage user classes 714
Secure Socket Layer access 718
SSL and SSH 718
Manage SSL access 719
Virtual groups 721
Manage virtual groups 721
Filesystem restrictions 723
Manage filesystem restrictions 724
Upload restrictions 727
Manage upload restrictions 728
Download restrictions 732
Manage download restrictions 732
FTP command restrictions 736
FTP SITE command 736
Manage FTP command restrictions 736
Protocol server access control 738
Access rule order 739
Enable host names for access control 739
Manage protocol server access 740
User limits 743
Manage user limits 743
User and group access 746
Manage user and group access 746
Login restrictions 747
Manage Login Restriction Policies 748
Create Login Restriction Policy entries 751

12 Applications **756**
Application overview 756
Manage applications 757
Access applications 758

View or edit an application 758
Delete an application 759
Create applications 760
Create an Archive Maintenance application 760
Enable Multithreading 762
Set maximum run time 763
Create an Audit Log Maintenance application 763
Create an Axway Sentinel Link Data Maintenance application 765
Create an Axway Transfer CFT application 766
Create a Basic Application 767
Create a File Transfer via File Services Interface application 768
Create a Human to System application 769
Create a Log Entry Maintenance application 770
Create a Login Threshold Maintenance application 774
Create a Package Retention Maintenance application 776
Create a Shared Folder application 778
Create a Site Mailbox application 779
Create a Standard Router application 780
Create a Transfer Log Maintenance application 786
Create a Unlicensed Accounts Maintenance application 792

13 Advanced Routing 795
Advanced Routing overview 795
What can Advanced Routing do? 795
Advanced Routing glossary of terms 796
Triggering conditions and events 796
Advanced Routing setup overview 797
Advanced Routing features 797
Order of configuration 798
Create Advanced Routing administrator 799
Create user accounts 799
Create Advanced Routing application 799
Create Route Package Template 799
Assign Route Package Template 799
Subscribe to Advanced Routing application 800
Configuration 800
Advanced Routing delegated administrator 800
Create user accounts 804
Create Advanced Routing application 805
Manage Route Package Templates 806
Manage Routes 812
Assign Route Package Template 818
Subscribe to Advanced Routing application 821
Transformations 829

PGP Encryption ... 829
PGP Decryption ... 835
Compress ... 838
Decompress ... 842
Line Ending ... 846
External Script ... 850
Encoding Conversion ... 853
Characters Replace ... 856
Line Padding ... 861
Line Truncating ... 865
Line Folding ... 869
Rename ... 873
Route steps ... 875
Publish To Account ... 875
Send To Partner ... 881
Operation ... 894
Basic use cases ... 894
Advanced use cases ... 908
Advanced Routing best practices ... 917
Chain of route execution ... 917
Inherited settings vs. Specific Settings ... 918
Skipped transformation ... 918
Transformation on multiple files ... 919
Route failure ... 919
Transformed file as the input to the next step ... 920
Routing to multiple transfer sites ... 920
Custom Expression Language functions and variables ... 921
Exceptional case: absolute path to sandbox folder in EL expressions ... 921
Session related EL expressions ... 922
Predefined EL functions ... 926
Account related EL expressions ... 927
LDAP related EL expressions ... 929
PeSIT related EL expressions ... 930
Routing related EL expressions ... 936
Special routing variables ... 937
STFS PeSIT related EL expressions ... 937
Transfer related EL expressions ... 943
Trigger related EL expressions ... 945
User related EL expressions ... 946
HTTP header EL expressions ... 946
Troubleshoot Advanced Routing ... 947
General troubleshooting steps ... 948
Debug logging ... 948
Log into a file ... 948

AR fails while copying the file to sandbox ... 949
Configuring asynchronous MDN receipts with AS2 transfers ... 950
AS2 MDN receipts overview ... 950
SecureTransport Applications for AS2 transfers ... 950
AR uses Route setup for outbound transfers ... 950
Scenario 1: Combine AR and Basic application for outbound transfers ... 951
Scenario 2: Combine AR and Basic application for both inbound and outbound transfers ... 952
Scenario 3: Combine AR for outbound and SiteMail for inbound transfers ... 952

14 AS2 transfers ... 954
AS2 implementation ... 954
Synchronous and asynchronous receipts ... 955
AS2 and application framework: Architecture and workflow ... 955
SecureTransport AS2 server: Setup overview ... 956

15 File services interface transfers ... 958
File services interface overview ... 958
Receive files using a file services interface protocol ... 959
Metadata file ... 959
Location of the transferred file ... 962
Send files using a file services interface protocol ... 963

Appendix A: Administration Tool features checklist ... 964

Appendix B: Troubleshoot common problems ... 968
Communication problems ... 968
Clocks out of sync ... 969
Trust establishment issues ... 969
Connectivity ... 970
Servers do not start ... 970
No SSL certificate configured for the server ... 971
Conflicting port numbers ... 971
Incorrect host name and IP address in the host file ... 971
Cannot log in as a client ... 972
License issues ... 973
Connectivity to server failed ... 973
SiteMinder issues ... 973
LDAP issues ... 974
File system commands not functional ... 974
Cannot log in to SecureTransport Edge ... 975
Client certificate authentication fails ... 975
Logged in to client with reduced functionality ... 975
Session terminates due to CSRF protection ... 975
FTP does not work through the firewall ... 976

Firewall rules prevent the port from opening 976
Passive port range is not defined in the firewall 976
Check Point firewall is not configured for bidirectional transfers 977
PeSIT file transfers fail over TLSv1 Legacy for certain ciphers 977
Failed PeSIT file transfers to SecureTransport 977
Failed PeSIT file transfers from SecureTransport 978
Performance issues 978
Evaluate performance issues 979
DNS settings 979
Firewall issues 980
Other services using to much CPU or memory 980
Installation on network drive 981
Debug log output slows computer 981
Troubleshooting I/O problems 981

Appendix C: FIPS transfer mode 983
FIPS-certified cryptographic libraries 983
Advertised ciphers and cipher suites in FIPS mode 984

Appendix D: Command line utilities 987
Control the servers 987
Utility files 987
Command line directory or file listing 990

Appendix E: Server logs 992
Log file list 992
Log output details 995
Log4j files 995
Database log files 997
FTPD log file 997
Admin log file 998
General log files 998
Modify the log4j files 1001
Redirect log4j output from the database 1003
Control log fallback from database to file 1005
Server log rotation scheduling 1006

Appendix F: Firewall settings 1008
Enable bidirectional connections in a firewall 1008
Check Point firewall 1009
Cisco PIX firewall 1009
Raptor firewall 1009
Configure firewall ports 1009
Communication between the outside and SecureTransport Edge 1010

Communication between SecureTransport Server and SecureTransport Edge 1010
Communication between SecureTransport Server and an internal network 1011
Internal SecureTransport communication 1011
Firewall rules 1011
Protocol rules 1012
Authentication rules 1015
Administration rules 1015
TM server communication rules 1016
Server transfer rules 1017
Standard Cluster rules 1017
Enterprise Cluster rules 1017
Protocol rules - outbound from SecureTransport Edge 1018

Appendix G: Expression Language 1020
Expression Language overview 1020
Expression Language operators 1021
Predefined variables 1021
Predefined variable examples 1022
Predefined functions 1022
Predefined function examples 1023
SecureTransport specific named variable sets 1025
SecureTransport-specific named variable set examples 1026
PeSIT variables 1026
Advanced Routing EL functions and variables 1029
Match and replace functions 1029
Regular expression examples 1029
Expression examples 1029
Expression variables and examples 1030

Appendix H: IP addresses and host names 1032
IP address and host name syntax 1032
Exact IPv4 or IPv6 address 1032
Range of address using Classless Inter-Domain Routing notation 1033
Range of address using IPv4 address and subnet mask 1033
Patten matching an IPv4 address 1033
Exact host name 1034
Pattern matching a host name 1034

Appendix I: Regular expressions 1035
Regular expression characters 1036
General character classes 1036
Predefined character classes 1036
Boundary matches 1038
Regular expression closures 1039

Logical and grouping operators 1039
Back references 1040

Appendix J: Velocity email notification package 1041
Email notification overview 1041
Velocity overview 1042
Configure the ServerTransferNotify rules package 1043
Customize the email notification templates 1044
Velocity troubleshooting 1046
Restart SecureTransport 1046

Appendix K: SSO filter mapping 1048
Rename mapping 1048
Filter mapping 1048
Filter syntax 1048
Examples 1049

Appendix L: Sample SSO configuration file for administrators 1050

Appendix M: Sample SSO configuration file for end-users 1057

Preface

This guide provides information about common administration and management tasks performed by Axway SecureTransport administrators.

Who should read this document

This guide is intended for system administrators who configure and maintain SecureTransport. As SecureTransport system administrator, you must be able to work effectively with the operating system platform and network used by SecureTransport. As a system administrator who deploys and configures SecureTransport and maintains its configuration, you must know or learn the file transfer requirements of your organization including the systems, protocols, and other standards used within your corporate network and by your partners. You must also be familiar with the configuration of systems that you integrate with SecureTransport, including LDAP, CA SiteMinder, Axway Sentinel, Axway Transfer CFT, and other file transfer clients and servers. As a system administrator who manages user and service accounts and maintains day-to-day operation of SecureTransport, you must understand the roles of your users and partners so you can assign them correct account properties and access permissions and restrictions. You must also be familiar with application logs and reports so you can interpret those provided by SecureTransport.

Related documentation

SecureTransport provides the following documentation:

- *SecureTransport Administrator's Guide* – (This document) This guide describes how to use the SecureTransport Administration Tool to configure and administer your SecureTransport Server. The content of this guide is also available in the Administration Tool online help.
- *SecureTransport REST API documentation* – The portal published API documentation derived from the API swagger documents. To access the administrator API documentation, go to SecureTransport Administrator API v1.4. To access the end-user API documentation, go to SecureTransport End-User API v1.4.
- *SecureTransport Appliance Guide* - This guide provides the SecureTransport Appliance installation, configuration, and operation instructions. It also provides SecureTransport installation and upgrade instructions for Axway Appliances.
- *SecureTransport Capacity Planning Guide* – This guides provides information useful when planning your production environment for SecureTransport.
- *SecureTransport Developer's Guide* – This guide provides the descriptions and usage of the plug-able information for the SecureTransport Pluggable Transfer Site and how to implement a

Pluggable Transfer Site. It also provides Swagger REST API integration instructions and custom Address Book source implementation instructions and custom plugins/exits source implementation instructions.

- *SecureTransport Getting Started Guide* – This guide explains the initial setup and configuration of SecureTransport using the SecureTransport Administrator setup interface.
- *SecureTransport Installation Guide* – This guide explains how to install and uninstall SecureTransport on UNIX-based platforms and Microsoft Windows.
- *SecureTransport Release Notes* – This document contains information about new features and enhancements, information received after the finalization of the rest of the documentation, and a list of known and fixed issues.
- *SecureTransport Security Guide* – This guide provides security information necessary for the secure operation of the SecureTransport product.
- *SecureTransport Software Development Kit (SDK)* – A set of software development tools and examples that allow extending SecureTransport by consuming and implementing available APIs.
- *SecureTransport Upgrade Guide* - This guide explains how to upgrade SecureTransport on UNIX-based platforms and Microsoft Windows.
- *ST Web Client Configuration Guide* – This guide describes how to configure and customize the ST Web Client user interface.
- *ST Web Client User Guide* – This guide describes how to use the ST Web Client.

Go to Axway Support at support.axway.com to view or download documentation. The website requires login credentials and is for customers with active support contracts.

Get more help

Go to Axway Support at support.axway.com to get technical support, download software, documentation and knowledgbase articles. The website requires login credentials and is for customers with active support contracts.

The following support services are available:

- Official documentation
- Product downloads, service packs, and patches
- Information about supported platforms
- Knowledgebase articles
- Access to your cases

When you contact Axway Support with a problem, be prepared to provide the following information for more efficient service:

- Product version and build number
- Database type and version
- Operating system type and version
- Service packs and patches applied

- Description of the sequence of actions and events that led to the problem
- Symptoms of the problem
- Text of any error or warning messages
- Description of any attempts you have made to fix the problem and the results

SecureTransport overview 1

SecureTransport is part of the Axway family of managed file transfer (MFT) products. SecureTransport allows organizations to adeptly control and manage the transfer of files inside and outside of the corporate firewall in support of mission-critical business processes and ad hoc human transactions, while satisfying policy and regulatory compliance requirements. SecureTransport serves as a hub and router for moving files between humans, systems, and more. SecureTransport also completes tasks related to moving files (push or pull), hosting files in mailboxes or "FTP-like" folders, and provides portal access with configurable workflow for file handling and routing. SecureTransport delivers user-friendly governance and configuration capabilities, including delegated administration and pre-defined and configurable workflows, while providing the highest possible level of security.

Designed to handle everything from high-volume automated file transfers between systems, sites, lines of business, and external partners, to user-driven ad hoc communications, to portal-based file exchange, SecureTransport supports the full range of file transfer scenarios while satisfying stringent security, policy, and regulatory compliance requirements. Serving as an MFT gateway, SecureTransport can perform the following key MFT functions:

- Accelerate and manage movement of files (push or pull) and host files in secure mailboxes or folders
- Push data securely to trading partners in real time
- Support ultra-high-end shared service bureaus to meet the demands of multiple business units and organizations in one scalable infrastructure
- Provide a configurable workflow for flexible and dynamic file handling and routing

Also, user-friendly governance and configuration capabilities, including delegated administration and pre-defined and configurable workflows, make SecureTransport a secure, easy-to-implement, and easy-to-use alternative to high-maintenance proprietary file transfer software, simple MFT gateways, and costly VANs and VPNs.

SecureTransport is compatible with FTP, FTPS, HTTP, HTTPS, SSH, FIPS 140-2 Level 1, AS2, and PeSIT standards. SecureTransport includes features that support business processes that are mission-critical to the enterprise and the documentation, auditing, and accountability required by government regulations such as HIPAA, GLBA, and Sarbanes-Oxley.

SecureTransport has many enterprise-class features, including the following:

- Standard Clustering and Enterprise Clustering
- Comprehensive authentication and access control
- A user-friendly HTML5-based end user client for file transfers, transfer status, and full email-style message compose, inbox, and outbox views for ad hoc transactions
- Comprehensive multiple LDAP system integration and mapping
- Complete representational state transfer (REST) web services APIs for administration, for file transfers management, and for custom end user interactions

- Interactive and automated transfers
- Guaranteed delivery
- Flexible support for deployments using one or more peripheral networks (DMZs) that host SecureTransport Edge servers configured to provide specific protocol and proxy services
- Data integrity
- Comprehensive logging and auditing
- Event-driven agents
- Java APIs and protocol support for application integration
- Scheduled transfers
- Advanced Routing
- PGP encryption and decryption
- Compression and decompression
- Line ending and transcoding
- Embedded Axway File Bus support

The cryptographic libraries used by SecureTransport for the AS2 (SSL), FTPS, HTTPS, PeSIT (SSL and legacy SSL), and SSH (SFTP and SCP) protocols have been certified Federal Information Protection Standard (FIPS) 140-2 Level 1 compliant by the US National Institute of Standards and Technology (NIST), Computer Security Division, and the Communications Security Establishment of the Government of Canada Information Protection Group.

SecureTransport Server

SecureTransport Server provides a centrally managed system for monitoring and managing secure file transfer activity across multiple file transfer sites or applications. Key capabilities of the SecureTransport Server include:

- **Guaranteed delivery** – Guarantees secure, reliable, and scalable file transfer service even over unstable network connections or dial-up lines using integrity checking implemented with a cryptographic hash algorithm and provides powerful automation to integrate with back-end systems
- **Checkpoint restart** – With Axway clients, allows restarting stopped or failed HTTP, PeSIT, and some FTP file transfers from the point of failure
- **Secure connectivity** – Accepts, validates, and secures incoming connections and file transfers
- **Multi-protocol support** – Executes file transfers using widely adopted open standard FTP, secure FTP, HTTP, HTTP(S), AS2, PeSIT, SSH-based (SFTP and SCP), and Folder Monitor protocols
- **Proxy support** – Can use the SOCKS5 proxy provided by SecureTransport Edge or an HTTP proxy

- **Native Axway File Bus support** – Supports PeSIT for connectivity with the Axway File Bus and implements the Axway File Bus using metadata, routing, and automation capabilities aligned with Axway Transfer CFT
- **Ad hoc file transfer support** – Manages human-to-human (H2H) and human-to-system (H2S) file transfers sent using ST Web Client or one of the Axway Email Plug-ins and system-to-human (S2H) file transfers delivered through email notifications
- **Repository encryption** – Encrypts all files on disk at the server transparently
- **PGP encryption** – Handles PGP encryption and decryption, the generation and storing of PGP keys, and the management of the stored keys
- **Application integration** – Includes REST and Java APIs, protocols, a file services interface, and Axway File Bus support
- **Transfer scheduling** – Allows administrators to plan and configure scheduled file transfers and AdHoc tasks
- **Monitoring and reporting** – Monitors and analyzes file transfer activity, providing real-time reports and alerts
- **Signed messaging disposition notification (MDN) receipts** – Can generate receipts for all transfers, regardless of protocol
- **Flexible clustering models** - Includes Standard Clustering for simple deployment with no external dependencies and optional Enterprise Clustering to increase the capacity of a SecureTransport deployment to handle large workloads
- **Database support** – Uses an embedded database or, with optional Enterprise Clustering, an external database to store and retrieve configuration parameters and data pertaining to objects and events
- **Web administration and configuration** – Provides a web-based user interface (the Administration Tool) for centralized administration, configuration, and monitoring of file transfer activity and applications
- **Fully Embeddable** – Includes a REST API with resources for administration, configuration, and file transfer request management and for creating custom end user access

SecureTransport Server is available as software on Windows and UNIX platforms and as a Cloud service. You can deploy it as part of an Enterprise Cluster or as a stand-alone server.

In addition to being offered as a software version, the SecureTransport Server is available as an appliance. The Axway SecureTransport Appliance offers the SecureTransport file transfer solution using the Axway appliance platform, which is an easily deployable hardened Linux server. This self-contained appliance version of SecureTransport greatly simplifies the implementation and management of a secure file transfer infrastructure. SecureTransport appliances provide enterprises with enhanced security, high performance, and lower acquisition, deployment, and ownership costs.

SecureTransport Edge

SecureTransport Edge is the gateway required in the perimeter network (also called demilitarized zone or DMZ) in a typical multilayer security architecture deployment. You can use SecureTransport Edge to implement secure interactions between client systems in a public or other external network and SecureTransport Servers in your internal secure network.

SecureTransport Edge serves as a protocol converter in such a deployment. It treats a wide range of file transfer protocols as presentation layer services and each protocol server translates its protocol onto the streaming protocol used to communicate with the Transaction Manager (TM) server on the SecureTransport Server. The TM Server connects to the protocol servers on the configured SecureTransport Edge servers to establish the connections for the streaming protocol, so no process on a SecureTransport Edge ever makes a connection from the DMZ into the internal secure network. A flexible network zone configuration supports connection to the protocol servers on specific SecureTransport Edge servers for different protocols and file transfers. For more information see *Communication across Transaction Manager, protocol, and proxy servers* on page 215.

SecureTransport Edge serves all the protocols supported by SecureTransport. When an external partner client program or file transfer server initiates a connection to one of the protocol servers hosted on SecureTransport Edge, it terminates the inbound connection from the client, collects the client's credentials, and establishes an authenticated encrypted connection to the TM. SecureTransport Edge sends the credentials to the TM as a service request. The TM attempts to authenticate the account using the configured method and returns the result to SecureTransport Edge. If the account is authenticated, SecureTransport Edge establishes the connection.

For a file transfer, SecureTransport Edge uses the streaming protocol to check the access control rules on SecureTransport Server to authorize the transfer. SecureTransport Edge converts the network messages between the client protocol and the SecureTransport streaming protocol, decrypting and encrypting the data as needed. The data is *streamed* between the external-facing protocol server and the Transaction Manager, the streaming protocol server, running on the SecureTransport Server. No transferred file data is stored in the SecureTransport Edge file system in the perimeter network.

When SecureTransport Server connects to a partner server in the external network to check for files or to transfer a file, it can use the SOCKS5 circuit-level proxy component of SecureTransport Edge to broker the connection through the perimeter network to the external network. Thus, the authentication credentials exist only in the internal secure network and are encrypted until they are presented to the external server. (SecureTransport Server can also use an HTTP proxy.)

SecureTransport Edge is available as software on Windows and UNIX platforms. You can deploy it with stand-alone or clustered SecureTransport Servers. You can deploy two or more SecureTransport Edge systems in support of a SecureTransport Server cluster and synchronize configuration changes dynamically. Each SecureTransport Edge stores its configuration in a local embedded MySQL database. For more information see *SecureTransport Edge synchronization* on page 372.

In addition to being offered as a software version, the SecureTransport Edge is available as an appliance. The Axway SecureTransport Appliance offers the SecureTransport file transfer solution using the Axway appliance platform, which is an easily deployable hardened Linux server. This self-contained appliance version of SecureTransport greatly simplifies the implementation and management of a secure file transfer infrastructure. SecureTransport appliances provide enterprises with enhanced security, high performance, and lower acquisition, deployment, and ownership costs.

Deployment models

SecureTransport cam be deployed as part of a Standard Cluster (SC), Enterprise Cluster (EC), or in standalone mode.

Cluster models

To provide flexibility for both ease in managing clustering and scale to meet the most demanding of loads, SecureTransport Server offers two cluster models. These are the Standard Cluster and Enterprise Cluster.

Standard Clustering uses an embedded MySQL database, which minimizes external dependencies and overhead and reduces the cost of clustering. A Standard Cluster can have from two to three nodes (servers). For more information, see *Standard Cluster* on page 335.

For a situation that exceeds the capacity of a Standard Cluster or requires a shared Microsoft SQL Server or Oracle database, SecureTransport 5.4 offers an Enterprise Cluster option. An Enterprise Cluster using an external database and a high-performance cache-management layer significantly improves efficiency, provides near-linear scaling, and enables very large scale configurations. With the Enterprise Cluster option, an active/active cluster can have up to 20 nodes. The Enterprise Cluster option requires your organization to provide and maintain an Oracle or Microsoft SQL Server database. You must also provide a high-performance shared file system for the user files. For more information, see *Enterprise Cluster* on page 351.

Standalone deployment

When you do not need a cluster for additional capacity or improved availability, you can deploy SecureTransport Server as a single server. A stand-alone SecureTransport Server can use the embedded database or an external database. All stand-alone deployments can use a local file system for user files.

Note Multiple standalone SecureTransport instances sharing the file system where the user home directories are located is not a supported configuration.

SecureTransport clients

Axway Secure Client is a secured FTP, HTTP, and SFTP client designed to operate with Axway SecureTransport, Axway Gateway, or any standard FTP server. Axway Secure Client runs as a stand-alone application, as a service, or as a background task. Moreover, working with Axway SecureTransport, Axway Interchange, and Axway Gateway, Axway Secure Client guarantees data delivery and data integrity while protecting corporate bandwidths. The Auto Restart feature automatically re-establishes broken connections and resumes transfers from the point where the transfer stopped. When a clustered deployment supports automatic failover, the transfer can resume on another server after a server failure.

SecureTransport Server and SecureTransport Edge support a broad set of file transfer clients to enable a wide range of applications and data transfer scenarios, including third-party file transfer clients or browser-based open standard protocols.

SecureTransport supports the following Axway clients:

- Axway Secure Client
- ST Web Client
- SecureTransport Browser Client
- Axway Outlook Add-in

See *Axway and third-party software support* on page 39 for supported browsers and versions.

Ad hoc file transfers

In addition to scheduled and event-driven server-initiated file transfers, SecureTransport supports ad hoc file transfers. Using the ST Web Client or an Axway Email Plug-in, a SecureTransport user with the required rights can compose an email, attach one or more files, and send it to any email address. Because the files are uploaded to the SecureTransport Server instead of sent in the email, SecureTransport ad hoc file transfer provide the following features not available with the standard email protocol:

- Large file size (for ST Web Client in a 32-bit browser, a maximum of 2 GB per message)
- Choice of methods of file delivery to the mail recipient, including limits on allowed recipients and secure delivery options
- Human-to-system (H2S) ad hoc file transfers where the SecureTransport server can process the file and forward it to another system

A message from ST Web Client can transfer at most 2 GB data. There is no limit for messages from an Axway Email Plug-in.

The route the email takes to its recipient depends on the client the sender uses:

- **ST Web Client** – The SecureTransport Server sends the email using its SMTP configuration.
- **Axway Email Plug-ins** – The email client, Microsoft Outlook or Lotus Notes, sends the email.

The recipient has different requirements to access the files, depending on the delivery mode, Delivery modes are:

- **Anonymous** – The recipient clicks a link to access the files.
- **Challenge** – The recipient must answer a question correctly to access the files.
- **Account** – The recipient must log on to SecureTransport using ST Web Client with an existing user account or use an Axway Email Plug-in to access the files.
- **Auto-enroll** – SecureTransport creates a user account for the recipient before the recipient can access the files. The recipient must log in to SecureTransport using a temporary password and set a new password before retrieving the files.

The following features of SecureTransport are useful for ad hoc file transfer recipients:

- **Login by email** – The user can use an email address as the user name in a web client log in page.
- **Unlicensed user accounts** – The user can only log in using ST Web Client to access the files and reply once to an ad hoc file transfer email. The user can use an Axway Email Plug-in to access the files.

For information about configuring ad hoc file transfers, see *Configure adhoc file transfers* on page 89, *Create a user account* on page 456, *Create a site template* on page 682, and *Create or edit a business unit* on page 693. For information about configuring H2S file transfers, see *Human to System type application* on page 615.

SecureTransport also supports system-to-human (S2H) file transfers. S2H file transfers are like other server-initiated file transfers, except the destination is a human, not a system. For example, the SecureTransport server can upload a large file from another server and send it to an email recipient using an S2H transfer site. The recipient of an S2H file transfer uses the same procedures to retrieve the file as the recipient of an ad hoc H2H file transfer. For more information, see *System to Human transfer sites* on page 595.

Axway and third-party software support

This section lists the Axway and third-party software supported for the various protocols and integrations.

- *Operating systems* on page 39
- *Databases for Enterprise Clusters* on page 40
- *Browsers* on page 41
- *Software for file exchange* on page 41
- *Authentication providers and directory services* on page 43
- *ICAP* on page 44
- *Business activity monitoring and governance* on page 45
- *Proxy software* on page 45
- *PGP* on page 45
- *File systems* on page 46

Operating systems

UNIX

- SUSE® Linux Enterprise Server 12 SP5
- SUSE® Linux Enterprise Server 11 SP4 on Appliance platform
- SUSE® Linux Enterprise Server 12 SP4

- SUSE® Linux Enterprise Server 11 any SP
- Red Hat Enterprise Linux 6.x
- Red Hat Enterprise Linux 7.x
- Oracle Linux 6.x
- Oracle Linux 7.x
- CentOS 7.x
- Oracle Solaris 10/Zones/VM for SPARC
- Oracle Solaris 11/Zones/VM for SPARC
- IBM AIX 7.1 WPAR/LPAR
- IBM AIX 7.2 WPAR/LPAR

Microsoft Windows

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

Virtual

- IBM AIX 7.1 or 7.2 LPAR or WPAR
- Oracle Solaris Zone in Oracle Solaris 10 or 11
- Virtual appliance running under VMware ESX(i)
- An Amazon Elastic Compute Cloud (EC2) VM instance
- MS Azure Virtual Machines
- A supported version of RHEL or SLES in any x86 virtual environment
- Microsoft Windows Server 2012 R2 in any x86 virtual environment
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

Appliance

- Appliance Platform 7.1.1

Databases for Enterprise Clusters

- Microsoft SQL Server 2014, 2016 or 2017 – Standard Edition and Enterprise Edition
    - AlwaysOn Failover Cluster Instances

- Oracle 11g, 12c, 18c, 19c – Enterprise Edition
    - Oracle RAC (with SCAN)
- Amazon RDS for Oracle 12c and Microsoft SQL Server 2017

Browsers

- Microsoft Edge - latest version
- Mozilla Firefox - latest version
- Apple Safari - latest version (*not supported for Administration Tool*)
- Google Chrome - latest version (*not supported for Administration Tool*)

Software for file exchange

SecureTransport is expected to work properly with any client or server software which complies with:

- RFC 959, RFC 2228, RFC 2389, RFC 2428, RFC 2640, RFC 4217, **MD5** Command Extensions, **MFxx** Command Extensions for **FTP** transfers
- RFC 4251, RFC 4252, RFC 4253, RFC 4254, Draft RFC - **Secure Shell** File Transfer Protocol, Draft RFC - **SSH** File Transfer Protocol draft-ietf-secsh-filexfer-04.txt for **SFTP and SCP transfers**.
- Any software certified by Drummond Group for **AS2** transfers (list as of Q3 2017)
- **PeSIT** protocol **PSIT_HS_E over TCP/IP**
- **pTCP** protocol v2
- Any of the supported browsers can be used to transfer files over **HTTP** to SecureTransport

List of certified software for file exchange

Software	Versions	Certification details
Axway Gateway	6.16	FTP(S), SSH, PeSIT
Axway Interchange	5.12.0	PeSIT
Axway Secure Client	6.1, 6.2, 6.3	FTP(S), SSH, HTTP(S)
Axway SecureTransport	5.0, 5.2.1, 5.3.0, 5.3.1, 5.3.3, 5.3.5, 5.3.6	FTP(S), SSH, HTTP(S), AS2, PeSIT, Ad-hoc
Axway Transfer CFT	3.0.1 SP10; 3.1.3 SP11; 3.2.4 SP2	PeSIT

Software	Versions	Certification details
cURL	7.58.0	FTP(S), HTTP(S)
CuteFTP Professional	9.2.0.8 (Windows)	FTP(S)
FileZilla Client	3.31.0	FTP(S), SSH
GlobalSCAPE EFT Server	7.4.5	FTP(S), SSH
IBM Mainframe FTP (S)	14 (ZOS version)	FTP
Ipswitch WS_FTP (only latest version)	12.6(Client)/8.0.1 (Server)	FTP(S)
LFTP	4.8.3	FTP(S)
OpenSSH	7.6	SSH - server initiated transfers
Oracle Solaris 10 FTP Server	10	FTP
PSCP (PuTTY)	0.70	SSH
PSFTP (PuTTY SFTP)	0.70	SSH
SmartFTP Client	9.0.2558.0	FTP(S)
Tectia Server	6.4	SSH - server-initiated transfers
Tectia SSH Client	6.4.15	SSH
VanDyke SecureFX	8.3	SSH
VanDyke Vshell	4.3	SSH - server initiated transfers (not certified, missing license)
WGET	1.13	FTP(S), HTTP(S)
WinSCP	5.13	SSH
Microsoft SharePoint 2013	15.0.4420.1017	using "SharePoint Transfer Site" (not certified for "Address" + "Site Name")
Apache HTTP Server	2.4.23	using "Generic HTTP Transfer Site"

Software	Versions	Certification details
MS Windows Server 2012 R2	6.3.9600	SMBv2 (using "SMB Connector", available in the AMPLIFY Repository)
Samba	3.6.6	SMBv2 (using "SMB Connector", available in the AMPLIFY Repository)
Amazon S3 Cloud Service	N/A	using "Amazon S3 Transfer Site"
Ceph	12.2.2	S3 (using "Amazon S3 Connector", available in the AMPLIFY Repository)
Syncplicity Cloud Storage	N/A	Syncplicity (using "Syncplicity Connector", available in the AMPLIFY Repository)
Hadoop	2.7.3	WebHDFS (using "Hadoop Connector", available in the AMPLIFY Repository)

Authentication providers and directory services

SecureTransport is expected to work properly with any LDAP server implementations which have been generated with compliance with:

- RFC 1777 - LDAP v2
- RFC 2251 - LDAP v3

List of certified software

Software	Versions	Comments
CA SiteMinder	12.52	As authentication authority
Microsoft ActiveDirectory	2008, 2012	
Oracle Directory Server	11.1.1.7.2	

Single Sign-On (SSO)

SecureTransport is expected to work properly with any software which complies with:

- SAML 2.0
- Kerberos 5

List of certified software

Software	Versions	Certification details	Limitations
Keycloak	2.5.0	Over SAML 2.0	Not supported for IdP initiated logout (Keycloak limitation)
Shibboleth	3.3.0	Over SAML 2.0	
Microsoft ActiveDirectory	2008	Over Kerberos 5	Not supported for administrators

ICAP

SecureTransport implements the ICAP functionality adhering to the published ICAP standard, therefore it is expected that SecureTransport will work with any server complying to the finalized ICAP standard (RFC 3507).

However, based on the experience from validating of the ICAP servers, connecting to each additional server supporting ICAP to ST Server was associated often with particularities and idiosyncrasies in requests/responses for ICAP scan, which could result in behavior change and/or failures in the processing.

Therefore, in future cases of utilization of other ICAP enabled Servers, Axway will evaluate such incidents (if any) and, whenever possible, will address them in the SecureTransport.

ICAP implementation to ensure file content validation operation continuity.

Incidents requiring major changes will be evaluated individually.

List of certified ICAP software

Software	Versions	Certification details
CA DLP	12.5	DLP
McAfee DLP	9.2.0	DLP
Symantec DLP	12.5	DLP
Symantec Protection Engine for Network Attached Storage	7.5.1.5	AV
McAfee Web Gateway	7.5.2.2.0	AV

Business activity monitoring and governance

SecureTransport is expected to work properly with any software which is in compliance with QLTv1.

List of certified software for Business Activity Monitoring and Governance

Software	Versions	Certification details
Axway Sentinel	4.1.0 SP6; 4.2.0 SP6	
Central Governance	1.1.3	
Decision Insight	2.0.0	

Proxy software

Software	Versions	Certification details
Apache Reverse Proxy	2.2.15	CIT and SIT via HTTP(s)
IBM Webseal	6.1	Plain HTTP only
Oracle iPlanet Web Proxy Server	4.0	CIT and SIT via HTTP(s)

PGP

SecureTransport is expected to work properly with any PGP keys which have been generated with compliance with:

- RFC 4880.

List of certified PGP software

Software	Versions	Certification details
GnuPG	2.2.4	

File systems

SecureTransport is certified against following shared file systems used for Users Home Folders.

List of supported shared file systems

Software	Versions	Certification details
NFS	v3	1. SecureTransport installed on Linux/Unix OS. 2. Directory exported from `ext4` file system over NFS protocol.
NFS	v4	1. SecureTransport installed with non-root user. 2. SecureTransport installed on Linux/Unix OS. 3. Directory exported from `ext4` file system over NFS protocol.
OCFS2	v2	1. SecureTransport installed on Linux (Oracle Linux) 2. SecureTransport installed with root user. 3. Number of nodes in the cluster: 2.
SMB	v1	Local file system of the SMB server is NTFS
SMB	v2.1	Local file system of the SMB server is NTFS
SMB	v3	Local file system of the SMB server is NTFS
GPFS	4.1	Not available for Axway Appliances.
GlusterFS	Any	Certified on GlusterFS 3.11.1 1. SecureTransport and GlusterFS client installed on Linux/Unix OS. 2. GlusterFS server installed on Linux/Unix OS with two or more virtual disks. 3. One of the disks is formatted with XFS FS and exported as a Gluster "brick". 4. "Bricks" form a volume, which is mounted on the GlusterFS client side.
GFS2	v2	1. SecureTransport installed on Linux (CentOS). 2. SecureTransport installed with root user. 3. Number of nodes in the cluster: 2.

Software	Versions	Certification details
Amazon EFS	any	1. EFS Mount targets in two availability zones. 2. Each mount target is mounted on a SecureTransport instance. 3. SecureTransport installed on Linux (RHEL). 4. SecureTransport installed with non-root user. 5. Number of nodes in the cluster: 2. 6. Encryption at rest and in transit.

Setup 2

The following set of topics provides detailed SecureTransport configuration and setup information:

- *Certificates* on page 50 - Describes the different types of certificates used in SecureTransport and how to import, export, and generate certificates and certificate signing requests.
- *PGP key encryption and signing* on page 72 - Describes PGP encryption and signing.
- *Configure FTP server messages and modes* on page 76 - Describes the FTP server configuration and provides how-to instructions for FTP server configuration.
- *Configure AS2 server settings* on page 84 - Describes the AS2 server configuration and provides how-to instructions for configuring AS2 transfers.
- *Configure SSH server settings* on page 85 - Provides how-to instructions for configuring the SSH server.
- *Configure Administration Tool server settings* on page 87 - Describes the Administration Tool server configuration and provides how-to instructions for configuring the Administration Tool server.
- *PeSIT server configuration settings* on page 88 - Provides how-to instructions for configuring the PeSIT server.
- *Configure adhoc file transfers* on page 89 - Provides how-to instructions for configuring the AdHoc file transfers.
- *Configure your database* on page 94 - Describes configuring the selected database.
- *Register SecureTransport in Central Governance* on page 103 - Provides the SecureTransport registration in Central Governance prerequisites, configuration information, and troubleshooting procedures.
- *Integrate Axway Sentinel* on page 109 - Describes Axway Sentinel integration with SecureTransport.
- *Server licenses* on page 157 - Describes installing server licenses using the *Server License* page.
- *Configure FTP command log* on page 166 - Describes the FTP command log configuration.
- *FTP SITE META command*on page 1 - Describes FTP SITE META command structure and functionality.
- *Configure transfer log* on page 170 - Describes the transfer log configuration.
- *Configure holiday schedule* on page 172 - Describes the holiday schedule configuration and provides how-to instructions for configuring the holiday schedule.
- *Mail templates* on page 173 - Describes the managing mail templates using the *Mail Template Repository* page.

- *Configure miscellaneous settings* on page 178 - Describes using the *Miscellaneous Configuration* page to specify the administrator's e-mail address, set usage monitor options, enable or disable reverse DNS lookups, set the session timeout limits, select a default HTML template, limit FTP login failures, set FTP and HTTP server startup password timeout configuration and shutdown options, and define password policy.
- *ICAP settings* on page 187 - Describes the ICAP settings configuration and provides how-to instructions for configuration ICAP.
- *Transaction Manager* on page 199 - Describes how to import, export, enable, disable rules packages. It also describes how to install agents and functions.
- *File archiving* on page 212 - Describes the file archiving feature and provides how-to instructions for the global file archiving configuration.
- *Communication across Transaction Manager, protocol, and proxy servers* on page 215 - Describes the Transaction Manager protocol and proxy server communication.
- *Configure SecureTransport Back End to Edge streaming communication* on page 227 - Provides how-to instructions for configuring streaming communication between SecureTransport Edge to Back End.
- *Address Book* on page 233 - Describes the Address Book feature and sources. Also, provides global, business unit, and account level configuration information and Address Book use cases.

Log in to the SecureTransport Administration Tool

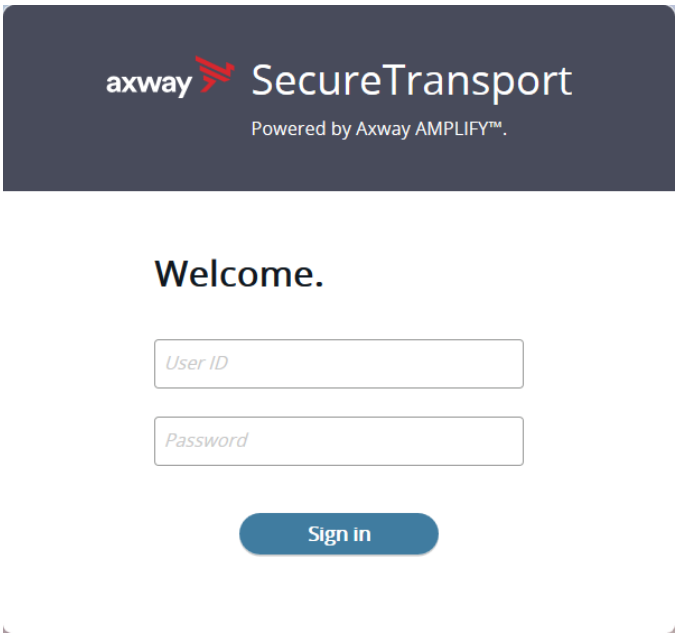
To log in to the SecureTransport Administration Tool through a web browser, take the following steps. For a list of supported web browsers, see *Axway and third-party software support* on page 39.

1. Open the web browser.
2. Type the URL for the Administration Tool as follows:

   `https://<host>:port`

   where `<host>` is the host name, FQDN or IP of the computer running SecureTransport and `port` is the administration port number entered during installation. The default port number is 444 for root installations. When SecureTransport is installed as non-root, the default port is 8444.
3. Following the instructions for your browser, add a certificate exception for the SecureTransport instance if needed.

   The login page is displayed.



4. Type the administrator name and password. The default user name is `admin` and the default password is `admin`.
5. Click **Log In**.

If an error occurs when logging into the Administration Tool, SecureTransport prompts you to type the name and password again.

Note When using the Administration Tool, make sure that your browser does not block pop-up windows for SecureTransport.

For more information about administrator login, see *Administrator login options* on page 417 and *Manage administrator accounts* on page 644.

Certificates

This topic describes the different types of certificates used in SecureTransport and how to import, export, and generate certificates and certificate signing requests.

SecureTransport uses digital certificates for many security functions. These certificates can either be signed by a self-signed Internal Certificate Authority (CA), that is, issued by the SecureTransport Server; signed by an imported internal CA; or signed by a third party, such as an external company like Verisign or a corporate CA. During the installation process, SecureTransport installs a default self-signed CA (valid for one month) that you should replace during the initial setup procedures. For details about initial setup procedures for certificates, refer to the *SecureTransport Getting Started Guide*. You can also import an external CA to serve as the SecureTransport internal CA so that certificates signed by SecureTransport are trusted by clients that trust that CA.

The following topics describe the certificate types and provide how-to instructions for managing certificates.

- *Certificate types* on page 51
- *Certificate Management page* on page 52
- *Repository encryption certificate* on page 52
- *Manage local certificates and certificate signing requests* on page 54
- *Manage trusted CAs* on page 61
- *Manage the internal CA* on page 63
- *Change the certificate keystore password* on page 68
- *Certificates to generate during initial setup* on page 69
- *Store certificates in a hardware security module* on page 69

Certificate types

SecureTransport uses the following types of certificates overall:

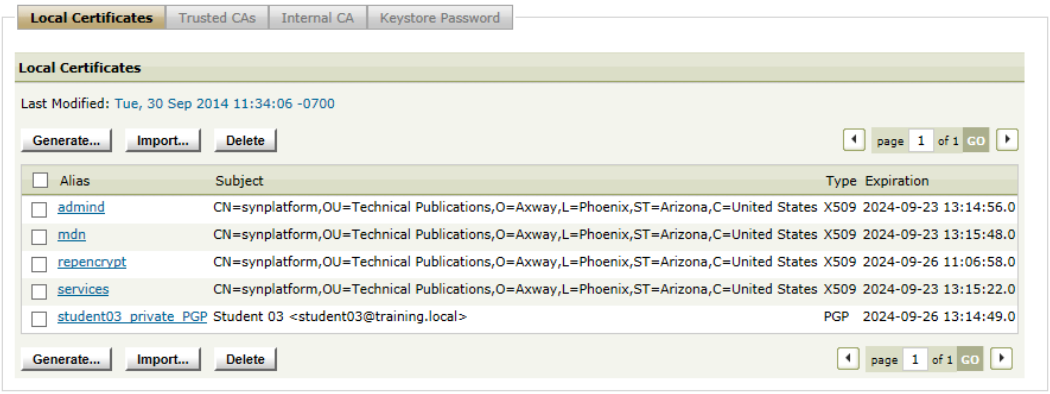
- **Local Certificates** – Local certificates are used for server authentication. They are also used to decrypt incoming documents and sign documents and receipts. The SecureTransport administrator can generate self-issued local certificates, import local certificates signed by a third-party certificate authority, and export certificate public keys and private keys to a file. For example, if you have a certificate signed by a widely-trusted CA such as Verisign, you can import it as a local certificate and use it for the HTTPS SSL key alias so browsers do not require the user to accept a certificate which they cannot validate. You manage server-scoped local certificates from the Setup menu. For more information, see *Manage local certificates and certificate signing requests* on page 54.
- **Trusted Certificate Authority (CA) Certificates** – CA certificates are used for indirect trust of SSL client or server certificates. SecureTransport includes a set of commonly used CA certificates. For SecureTransport to use imported local certificates, the trusted CA certificates must include certificates for all CAs in their certification paths (certificate chains). CA certificates are only server-scoped, and there are no account-specific CA certificates.
- **Internal CA** – A CA is the authority that issues, manages, revokes, and renews certificates, and assists people with performing certificate life cycle tasks such as retrieving, renewing, revoking, and so on. CAs are represented by a certificate that contains the name of the issuer and they are used to sign end-user certificates. An internal CA represents the company that you work for or a company that you pay to issue you a certificate.
- **Login Certificates** – Client authentication certificates are assigned to a specific user and are required for logging in to SecureTransport. You can use SecureTransport to generate X509 login certificates and to import X509 login certificates and SSH keys. You can manage user certificates from the **Accounts** menu. For more information, see *View a login certificate* on page 480.
- **Partner Certificates** – Account-specific public certificates are used for encrypting PGP and AS2 data before sending to the respective account and for verifying the signature of data from the account. Account-specific certificates can be managed using the **Accounts** menu. For details, see *View a partner certificate* on page 485.

- **Private Certificates** – Account-specific certificates used to decrypt incoming documents and sign documents and receipts. The Certificate Manager can generate self-issued private certificates, import private certificates signed by a third-party certificate authority, and export certificate public keys and private keys to a file. You manage account-specific private certificates from the **Accounts** menu. For more information, see *View a private certificate* on page 489.

Certificate Management page

To access the *Certificate Management* page, select **Setup > Certificates**.

Note In SecureTransport 5.3.6, regardless of installation type (either fresh install or upgrade from previous version), trusted certificates come with a `jdk` label in the certificate alias. This indicates that they are imported from JRE and does not affect the SecureTransport operations.



Use the *Certificate Management* page to perform the following certificate management functions:

- Import certificates
- Delete certificates
- Generate self-issued local certificates and certificate signing requests (CSRs)
- View certificates
- Export certificates to a file
- View, delete, or finish pending CSRs

Note Because SecureTransport stores the trusted and local certificates and the protocol server configuration in the database and recreates them in the file system when a server starts, you must import certificates into the database using the Administration Tool. You cannot install a certificate by copying it into a directory as you could in previous releases.

Repository encryption certificate

Repository encryption increases SecureTransport security by avoiding storing unencrypted files. Repository encryption can be enabled on different levels (for example, per account). When you enable repository encryption, SecureTransport encrypts (according to the activated repository

encryption level) each file that it pulls from a partner site or that a client pushes to it. When SecureTransport pushes a file to a partner site or a client pulls a file from it, SecureTransport decrypts the file. SecureTransport encrypts and decrypts each file dynamically in memory as it receives and sends it, so the files never exist unencrypted in the storage of the host system.

1. Generate a self-issued local certificate or import a PKCS#12 file. See *Generate a self-issued server certificate* on page 55 and *Import a local certificate* on page 59.
2. Set the value of the `Stfs.Encryption.CertAlias` server configuration parameter to the alias of the certificate. SecureTransport uses this certificate to encrypt and decrypt files. See *View and change server configuration parameters* on page 315.

   SecureTransport prevents you from deleting the certificate referenced by `Stfs.Encryption.CertAlias`.

   Note If `Stfs.Encryption.CertAlias` is not set, Repository Encryption will not be enabled.
3. To choose the encryption algorithm, set the value of the `Stfs.Encryption.Algorithm` server configuration parameter to one of the following values:
   - `AES128` (default)
   - `AES256`
   - `3DES`

   See *View and change server configuration parameters* on page 315.
4. To configure SecureTransport to compute the MD5 checksum for an uploaded file dynamically as the file is uploaded, set the value of the `Stfs.Hash.HashOnUpload` server configuration parameter to `true`. When the value is `false`, the default value, SecureTransport computes the MD5 checksum after the file transfer is complete.
5. Create a user class named `EncryptClass`. Files transferred by users in this class are encrypted. See *Add a user class* on page 714.

   Note For server-initiated transfers, the user class is defined by the UID and GID only. If you define the `EncryptClass` using user name or other attributes, there are limitation on server-initiated transfers. See *Encryption and server-initiated transfers* on page 705.

   Note Repository encryption can also be enabled on an individual account basis. When the setting is specified in the account, the user class is ignored.
6. Restart the TM Server. See *Start and stop servers* on page 253.

Note If you enable repository encryption, the following SecureTransport functions are not supported: resume PeSIT transfers and pause and resume transfers when SecureTransport is the server.

Note When changing the repository encryption certificate, the Transaction Manager should be restarted in order for the changes to be applied.

Manage local certificates and certificate signing requests

Use the *Certificate Management* page to generate local, self-issued server certificates or to generate certificate signing requests. Generated certificates are assigned RSA or DSA keys.

A certificate signing request is an unsigned copy of a certificate that you submit to a CA when requesting a signed certificate. Based on the information in the CSR, the CA creates a new signed certificate for your use. After receiving the signed certificate from the CA, you must import it into SecureTransport. For details, see *Import a new certificate for a pending certificate signing request* on page 57.

The following topics describe and provide how-to instructions managing local certificates and certificate signing requests:

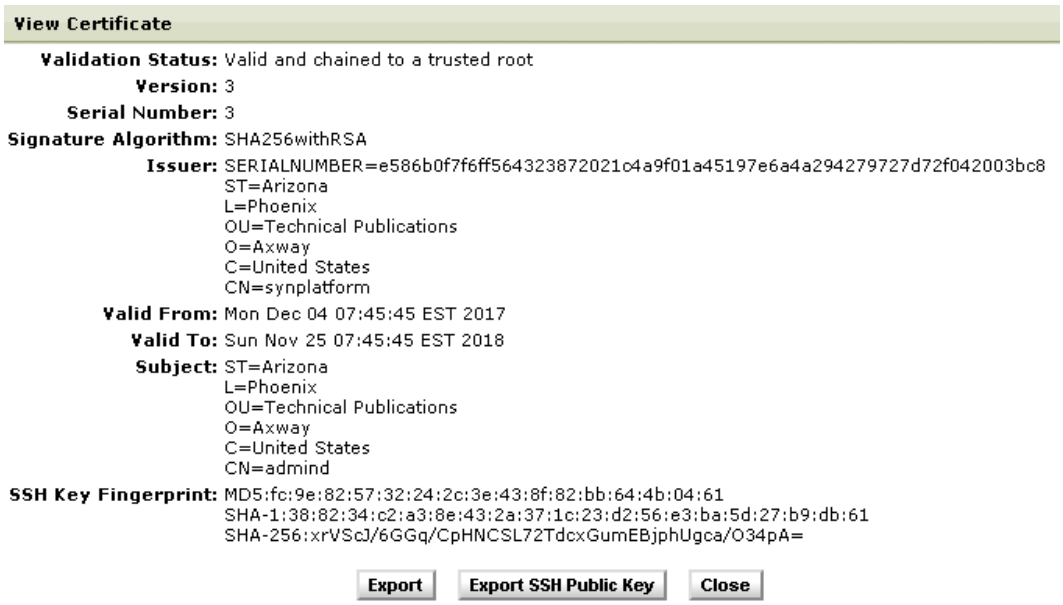
- *View local certificates* on page 54
- *Generate a self-issued server certificate* on page 55
- *Generate a certificate signing request* on page 56
- *Import a new certificate for a pending certificate signing request* on page 57
- *Delete a pending certificate signing request* on page 58
- *Export a local certificate* on page 58
- *Import a local certificate* on page 59
- *Import an SSH key* on page 60
- *Delete a local certificate* on page 61

View local certificates

You can view a list of all the local certificates or view the details of a specific certificate.

1. Select **Setup > Certificates**.
2. Click the **Local Certificates** tab.
3. Select a certificate alias from the list.

The *View Certificate* page displays the detailed information about the certificate.



Generate a self-issued server certificate

Use the following procedure to generate a self-issued server certificate.

1. Select **Setup > Certificates**.
2. Click the **Local Certificates** tab.
3. Click **Generate**.
4. Select **Self-issued Certificate**.

5. Type the required information for the self-issued certificate, including the fields that are displayed below the **Certificate Signing Request** option.

   The alias name should contain only lower case letters, digits, and hyphens (-). It must be at most 80 characters long. If the alias name you type is already assigned to another certificate, you are prompted to overwrite the existing certificate or cancel the operation.

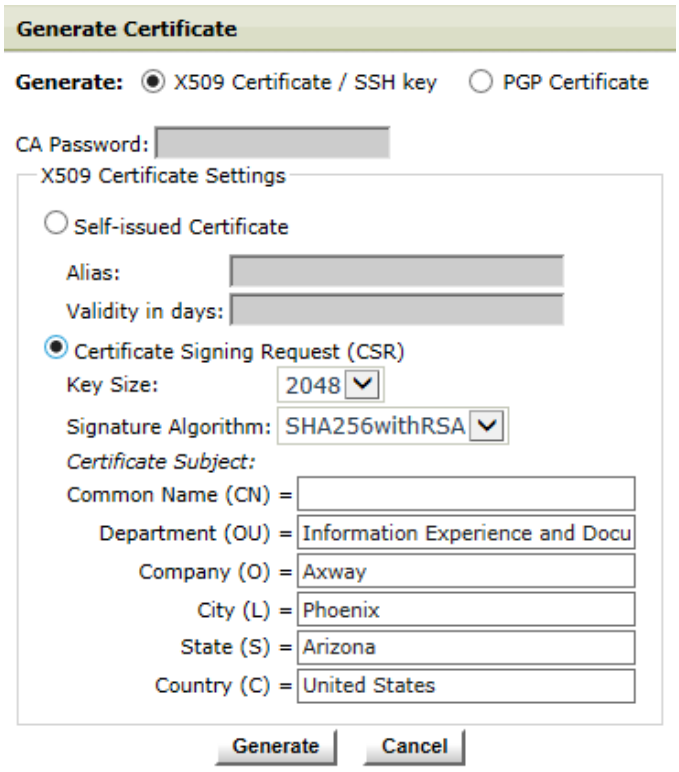
   You can overwrite any existing certificate including the default SecureTransport`admind` server certificate.

6. Click **Generate**.

Generate a certificate signing request

A certificate signing request (CSR) is a request to an external CA to sign a certificate.

1. Select **Setup > Certificates**.
2. Click the **Local Certificates** tab.
3. Click **Generate**.



4. Select **Certificate Signing Request (CSR)**.
5. Type the required information for the certificate signing request.

   The **Common Name (CN)** field must be the FQDN to be secured by the CA-signed certificate.
6. Click **Generate**.

   A message is displayed that explains how to download the CSR and send it to your CA.

The CSR is displayed in the list of Pending Local Certificates where it remains until you delete it or import the signed certificate you receive from the CA. You cannot use the new CA-signed certificate until you import it into SecureTransport.

Import a new certificate for a pending certificate signing request

Use the following procedure to import a new certificate for pending certificate signing request.

1. Select **Setup > Certificates**.
2. Click the **Local Certificates** tab.
3. Click **Finish** beside the appropriate CSR in the Pending Local Certificates list.
4. In the **Certificate Alias** box, type an alias.

5. Identify the certificate to import using one of the following methods:
    - Click **Import CA signed certificate from file** and specify the file name.
    - Click **Paste CA signed certificate in space below** and paste the certificate text in the box.
6. Click **Finish**.

    The certificate is displayed in the list of local certificates.

After you have imported the certificate, to use the certificate for a protocol server, set the Key Alias to the certificate alias and restart the protocol server. You can also use the certificate for other purposes, for example, as a login certificate for a transfer site or as an encryption or signing certificate for an AS2 transfer site.

Delete a pending certificate signing request

Use the following procedure to delete a pending certificate signing request.

1. Select **Setup > Certificates**.
2. Click the **Local Certificates** tab.
3. Click **Delete** beside the appropriate CSR in the Pending Local Certificates list.

Export a local certificate

Use the following procedure to export a local certificate.

1. Select **Setup > Certificates**.
2. Click the **Local Certificates** tab.
3. Click the alias of the certificate to export.

    The *View Certificate* window displays the certificate details.
4. To export a PGP certificate:
    a. Click **Export**.
    b. In the *Export Certificate* window, click **Export** to save the certificate as an ASCII-Armored (`.asc`) file, or select **Export private key**, type and confirm a password, and click **Export** to save the certificate as an `.asc` file with the private key.
5. To export a PGP certificate:
    a. Click **Export**.
    b. In the *Export Certificate* window, click **Export** to save the certificate as an ASCII-Armored (`.asc`) file, or select **Export private key**, type and confirm a password, and click **Export** to save the certificate as an `.asc` file with the private key.

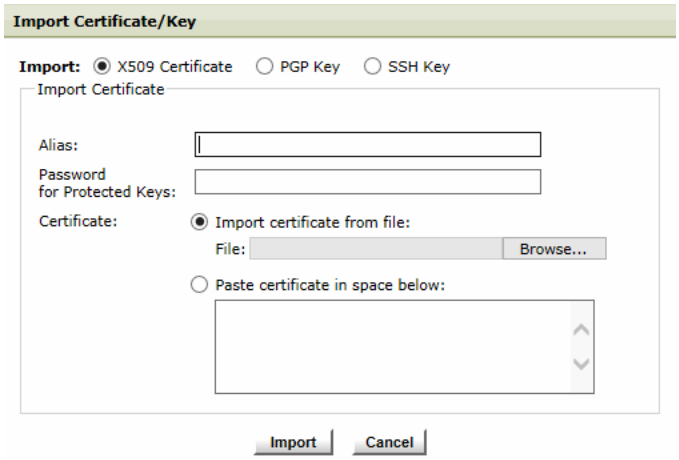
6. To export an X509 certificate:
    a. Click **Export**.
    b. In the *Export Certificate* window, click **Export** to save the certificate as a PEM-encoded certificate (`.crt`) file, or select **Export private key**, type and confirm a password, and click **Export** to save the certificate as a PKCS#12 (`.p12`) file.
7. To export an X509 certificate public key:
    a. Click **Export**.
    b. In the *Export Certificate* window, click **Export SSH Public Key** to save the public key as a `.pub` file.

Import a local certificate

You can import a private key and the corresponding certificate in **Local Certificates** as a PKCS#12 (`.p12`) file. You can then use it where you need a certificate that a remote client or system must trust, for example as the HTTPS SSL key alias.

1. Select **Setup > Certificates**.
2. Click the **Local Certificates** tab.
3. Click **Import**.

    The *Import Certificate/Key* window is displayed.



4. Select **X509 Certificate** or **PGP key**.
5. In the **Alias** field, type an alias name for the certificate.

    If the alias name is already assigned to another certificate, you are prompted to either overwrite the existing certificate or cancel the operation.
6. If the PKCS#12 (`.p12`) file being imported is password protected, type the password. You can also import PGP certificate files (`.asc` files).
7. Select **Import certificate from file** and type or browse to the file name or select **Paste**

certificate in space below and paste the certificate text into the text field.

8. Click **Import**.

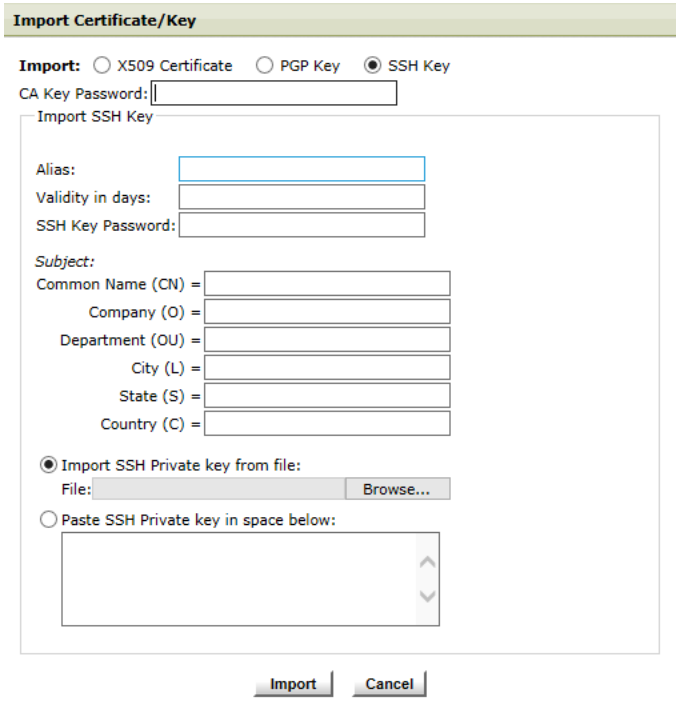
Note For specific requirements for certificates used to secure the SSL communication between the TM Server and the other servers, see *Secure the communication between the TM server and the protocol servers* on page 225.

Import an SSH key

Use the following procedure to import an SSH key. RSA and DSA keys in SSH2 format can be imported.

1. Select **Setup > Certificates**.
2. Click the **Local Certificates** tab.
3. Click **Import**.

   The *Import Certificate/Key* window is displayed.
4. Select **SSH key**.



5. Type the **CA Key Password** specified during the certificate generation.

   Note Imported SSH Keys are stored as X509 certificates.

   Note **CA Key Password** is not a required field. When a SSH key is imported (without providing the internal CA key password), the key will be stored as X.509 certificate and signed with temporarily generated certificate. As a result, the SSH key will be stored as X.509 self-signed certificate.

6. Type the information necessary to import the key. **Alias** and **Validity in days** are required fields.
7. Paste the certificate content directly in the provided space, or import the certificate from a file. To import from file, type the file path or click **Browse** to browse for the file.
8. Click **Import**.

Delete a local certificate

Use the following procedure to delete a local certificate.

1. Select **Setup > Certificates**.
2. Click the **Local Certificates** tab.
3. Select the check boxes for the certificates to delete or select the check box in the table header to select all certificates.
4. Click **Delete**.
5. Confirm the deletion.

Do not delete the certificate with the `admind` alias which is implicitly assigned to the Administration Tool server. SecureTransport prevents you from deleting a certificate that is in use, for example, a server certificate configured as the SSL key alias the AS2, FTP, HTTP, or SSH server or configured as the repository encryption certificate.

Manage trusted CAs

Trusted CAs represent the list of root and intermediate CAs used to build the certificate chain for client and server certificates.

The following topics provide how-to instructions for managing trusted CAs:

- *View a trusted CA certificate* on page 61
- *Export a trusted CA certificate* on page 62
- *Import a trusted CA certificate* on page 62
- *Delete a trusted CA certificate* on page 63

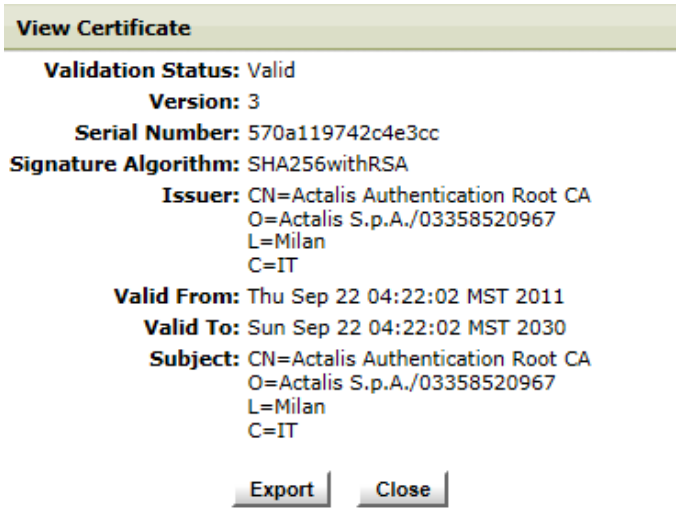
View a trusted CA certificate

Use the following procedure to view a trusted CA certificate.

1. Select **Setup > Certificates**.
2. Click the **Trusted CAs** tab.

   The list of trusted certificates is displayed.
3. Navigate to the page that lists the certificate to view.
4. Click the alias from the list.

The *View Certificate* page displays the detailed information about the certificate.



Export a trusted CA certificate

Use the following procedure to export a trusted CA certificate.

1. Select **Setup > Certificates**.
2. Click the **Trusted CAs** tab.
3. Navigate to the page that lists the certificate to export.
4. Click the alias of the certificate to export.
5. On the *View Certificate* page, click **Export** and save the certificate file in the desired location.

Import a trusted CA certificate

A X509 certificate can be imported as a trusted CA in the form of a X509 DER or PEM encoded file.

Note SecureTransport protocol servers and services does not require restart after importing, overwriting, or deleting a trusted certificate.

1. Select **Setup > Certificates**.
2. Click the **Trusted CAs** tab.
3. Click **Import**.
4. Type an alias for the certificate in the **Alias** box.

   If you use an alias that is already assigned to another certificate, the imported certificate overwrites the original one. Be sure that you are entering the appropriate alias for the new certificate.

5. Identify the certificate to import using one of the following methods:
    - Click **Import certificate from file** and type the file name.
    - Click **Paste certificate in space below** and paste the certificate text in the box.
6. Click **Import**.

Delete a trusted CA certificate

Use the following procedure to delete a trusted CA certificate.

1. Select **Setup > Certificates**.
2. Click the **Trusted CAs** tab.
3. Navigate to the page that lists the certificates to delete.
4. Select the check boxes for the certificates to delete.
5. Click **Delete**.

Note If an end user has a certificate issued by a trusted CA that was deleted, the user can no longer authenticate using that certificate.

Manage the internal CA

Each SecureTransport installation maintains its own copy of the internal CA. During the initial post-installation setup procedure, an internal CA is generated. All SecureTransport Servers in a cluster share the same internal CA. If you have a disaster recovery site, the DR cluster should use the same internal CA, replicated from the primary production site.

Note For security reasons, client certificates should only be stored inside the SecureTransport home folder or within a sub-folder of the home folder.

The internal CA can be used to generate server or client certificates. It provides a convenient alternative to using a third-party CA. It is used implicitly in the following cases:

- Generating a local certificate. For detail, see *Manage local certificates and certificate signing requests* on page 54.
- Generating an account certificate. For detail, see *Manage certificates* on page 476.
- Signing imported SSH Keys. For detail, see *Import an SSH login public key* on page 483.

The internal CA key is protected with a password. Any operation that involves use of the internal CA require that password. This password cannot be retrieved if it is lost. Contact Axway Global Support for more information. For contact information, see *Get more help* on page 31.

In addition to issuing certificates signed by internal CA, SecureTransport supports a few management operations for the internal CA. These operations include:

- Viewing the internal CA certificate
- Generating a new internal CA

- Importing an internal CA
- Exporting the internal CA

Note If you attempt to delete the internal CA, an alert dialog box is displayed.
If the certificate of the internal CA is deleted the Validation Status of all X509 local certificates, as well as imported SSH keys (because they are converted to X509 certificates during the import,) become `Not chained to a trusted root`. This has critical impact on the generated Login Certificates because users are no longer able to log into the SecureTransport Server.

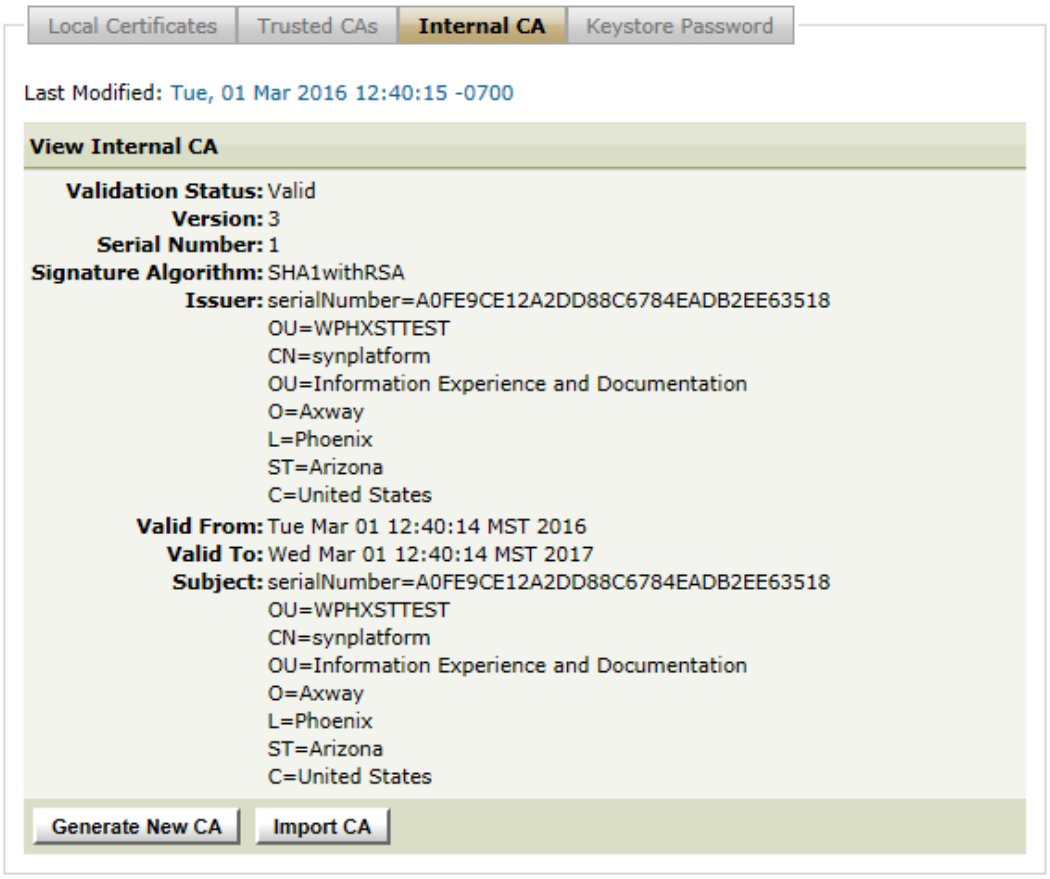
The following topics provide how-to instructions for managing the internal CA:

- *View the internal CA* on page 64
- *Generate an internal CA* on page 65
- *Import an external CA* on page 67
- *Export the internal CA* on page 68

View the internal CA

1. Select **Setup > Certificates**.
2. Click the **Internal CA** tab.

Basic certificate information is displayed including the validation status.

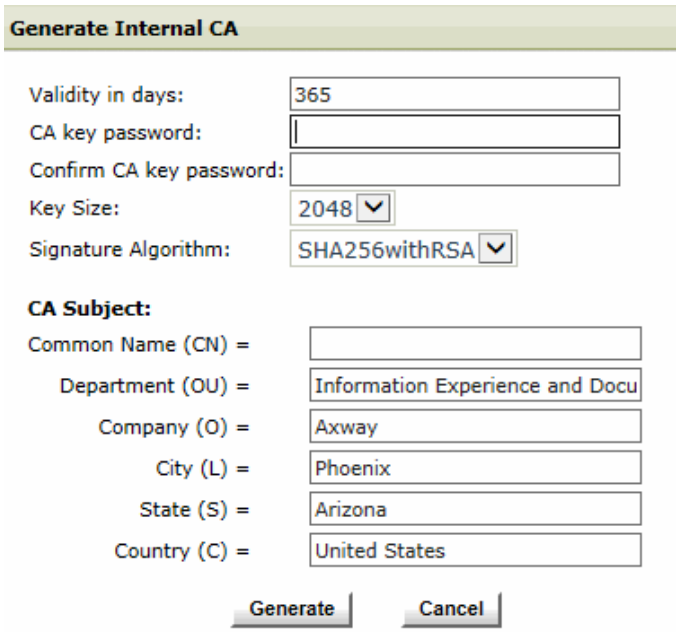


Generate an internal CA

There are a number of reasons why you might want to generate an internal CA. The most common reason is that the current CA is nearing its expiration date.

1. Select **Setup > Certificates**.
2. Click the **Internal CA** tab.
3. Click **Generate New CA**.

   The *Generate Internal CA* dialog box is displayed.



4. Provide the required information for the internal certificate.

   Internal certificates require the Certificate Subject information. For internal certificates, provide following information:

   - **Validity in days** – the number of days the certificate is valid.
   - **CA key password** – the password to protect internal CA. This password is requested when generating certificate signed by the internal CA.
   - **Confirm CA key password** – the key password must be entered again for confirmation.
   - **Key Size** – a number representing the size of the generated key, expressed in bits. Possible values are 1024, 2048 (default), 3072, or 4096 bits.
   - **Signature Algorithm** – the selection of the signature signing hashing algorithm. Possible values are SHA1withRSA, SHA256withRSA (default), SHA384withRSA, and SHA512withRSA.

     Note SHA1withRSA is available for backwards compatibility, but its usage is not recommended.

   - **Common Name** – the name that identifies the certificate.
   - **Department** – the name of department that the certificate is issued.
   - **Company** – the name of the company that the certificate is issued.
   - **City** – the name of the city where the location of the certification is located.
   - **State** – the name of the state where the location of the certification is located.
   - **Country** – the name of the country where the location of the certification is located.

5. Click **Generate**.

Generating a new internal CA does not automatically invalidate the certificate issued by the previous CA. When you generate an internal CA, SecureTransport adds the certificate to the Trusted CAs list under alias `ca`. The previous internal CA certificate is still in the Trusted CAs list under an alias of the form `ca-old-<serialNumber>`. When you do not want to accept certificates issued by the old internal CA, you can delete the `ca-old-<serialNumber>` aliases from the Trusted CAs list. For detail, see *Delete a trusted CA certificate* on page 63.

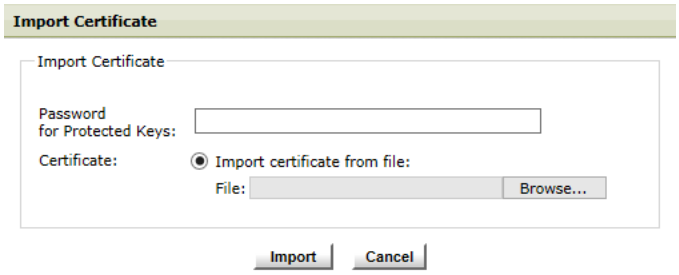
Once the new internal CA is generated, all certificates generated from that point on are signed by the new internal CA. Unless the new internal CA is added to the list of trusted certificates on the remote host, the host might reject the new certificates. An internal CA can be exported into a file that in turn can be used to add the CA to the list of trusted CAs.

Import an external CA

Optionally, you can also import an external certificate. Make sure the certificate is valid and configured to validate certificates before you import it. The CA attribute in the X509v3 extension section of the certificate must be true.

1. On the *Generate CA* page, click **Import CA**.

   SecureTransport displays *Import Certificate* page.



2. Type a password in the field provided. The password is required.

   If the CA certificate requires a pass phrase, SecureTransport uses this password. If the certificate does not require a pass phrase, the password is ignored. SecureTransport also uses this password to encrypt the CA private key in the keystore stored in the database and file system.

3. Specify the certificate by typing the path to the PKCS#12 (`.p12`) file in the field or by browsing to the file.

4. Click **Import**.

   SecureTransport reports if the import was successful.

Now, SecureTransport uses the imported certificate as the internal CA and signs all certificates generated using that CA. To make sure that a remote host accepts those certificates, add the certificate for this CA to the list of trusted certificates on that host. To export the certificate for import on another system, see *Export the internal CA* on page 68.

Generating or importing an internal CA does not automatically invalidate the certificate issued by the previous CA. When you generate or import an internal CA, SecureTransport adds the certificate to the Trusted CAs list under alias `ca`. The previous internal CA certificate is still in the Trusted CAs list under an alias of the form `ca-old-<serialNumber>`, where `<serialNumber>` is the value of the

certificate serialNumber field. When you do not want to accept certificates issued by the old internal CA, you can delete the `ca-old-<serialNumber>` aliases from the Trusted CAs list. For detail, see *Delete a trusted CA certificate* on page 63.

Once the internal CA is imported, all certificates generated from that point on are signed by the new internal CA. Unless the new internal CA is added to the list of trusted certificates on the remote host, the host might reject the new certificates. An internal CA can be exported into a file that in turn can be used to add the CA to the list of trusted CAs.

After you import a certificate authority, you might need to update the `CertificateStores.CertificateAuthority.serialNo` server configuration parameter. SecureTransport uses this parameter as a serial number and then increments it every time it generates a certificate. If the imported CA has been used by another SecureTransport server, set the parameter to the value from that server for consistency. To propagate the change, restart all SecureTransport servers in the cluster.

Export the internal CA

You can export the internal CA public certificate using the Administration Tool. You can also copy the certificate files from the server file system.

1. Select **Setup > Certificates**.
2. Click the **Trusted CAs** tab.
3. In the Alias column, click **ca**.

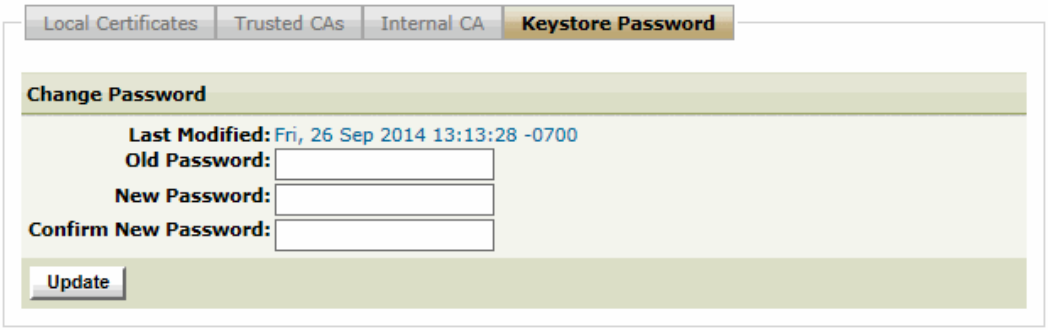
   The *View Certificate* page for the internal CA is displayed.
4. Click Export to export the public certificate for the internal CA as a `.crt` file.

Note The internal CA files are located in the `<FILEDRIVEHOME>/lib/certs/db` directory as `.pem` files. The public certificate is `ca-crt.pem`. The private key is `ca-key.pem`.

Change the certificate keystore password

SecureTransport stores all the available certificates for the system in the Certificate Keystore and the database.

1. Select **Setup > Certificates**.
2. Click the **Keystore Password** tab.



3. Type the old and new passwords, confirming the new one a second time. Leave the **Old Password** field empty if this is the first time you are changing the keystore password and SecureTransport uses the default.
4. Click **Update**.

Note Before you change the password the first time, you do not need to type the old password, because SecureTransport supplies the default value.

Certificates to generate during initial setup

For SecureTransport Edge and SecureTransport Server installations, generate an `admind` SSL server certificate for users connecting to the Administration Tool. This certificate may be signed by the internal SecureTransport CA.

Note If this certificate or any of the CA certificates in its certification paths (certificate chains) are expired or otherwise not valid, the Administration Tool server does not start.

To use repository encryption or MDN receipts, generate a repository encryption certificate or an `mdn` certificate, respectively. For information about the repository encryption certificate, see *Repository encryption certificate* on page 52.

To be able to enable FTPS, HTTPS, AS2 using SSL, SFTP, SCP, or PeSIT over a secured socket, generate the required certificates.

When you set up FTPS, HTTPS, AS2 (SSL), SSH, PeSIT, or SecureTransport Edge communication with the Transaction Manager on the SecureTransport Server, you select a key alias to specify the certificate to use to secure the communications. You created the alias when you generated the certificate. For a list of certificates commonly used with SecureTransport, refer to the *SecureTransport Getting Started Guide*.

Note For more information about the post-installation setup process, refer to the *SecureTransport Getting Started Guide*.

Store certificates in a hardware security module

You can store the certificates for the FTPS and HTTPS protocols in the HSM key storage provider or security world of a Thales nShield hardware security module (HSM). You can use any Thales nShield HSM that supports the nCipherKM JAC/JCE Java API. You must obtain the API and install it on the SecureTransport system.

The following topics provide the how-to instructions for storing certificates in a hardware security module:

- *Install and configure the HSM* on page 70
- *Generate and sign an HSM certificate* on page 70
- *Use an HSM certificate for FTPS or HTTPS* on page 71

Install and configure the HSM

SecureTransport maintains a keystore that stores references to the certificates stored in the HSM. Before you configure the HSM, decide on a location for the SecureTransport keystore file, for example, `<FILEDRIVEHOME>/lib/certs/hsm.keystore`.

1. Install the nShield hardware.
2. Install the nShield software, including the JCA/JCE cryptography service provider (CSP) on the system where the FTP Server and the HTTP Server run. Note the following values:
    - `<NFAST_HOME>`, the path name of the installation directory of the nFast client, `/opt/nfast` by default
    - The keystore passphrase
3. Make sure that `nonpriv_port` is set to `9000` and `priv_port` is set to `9001` in the hard server configuration file, `<NFAST_HOME>/kmdata/config/config`.
4. Copy the `nCipherKM.jar` file from `<NFAST_HOME>/java/classes` to `<FILEDRIVEHOME>/jre/lib/ext`.
5. Run `<FILEDRIVEHOME>/jre/bin/java com.ncipher.provider.InstallationTest`.

    The output include a list of installed providers. Ignore the statement that the nCipher provides is not correctly installed. The provider is installed at run time.

Generate and sign an HSM certificate

This procedure uses the following placeholders:

- `<alias>` – the SSL key alias for FTPS or HTTPS, for example `ftpd` or `httpd`
- `<cert_file>` is the file name of the PEM-format certificate file, for example, `ftpd.pem` or `httpd.pem`
- `<CSR_file>` – the file name of the CSR request file, for example, `ftpd.req` or `httpd.req`
- `<FILEDRIVEHOME>` – SecureTransport installation directory, for example, `/opt/TMWD/SecureTransport`
- `<key_size>` – the key size, for example, `1024`, `2048`, `3072`, or `4096`
- `<keystore_passphrase>` – the passphrase for the HSM keystore
- `<keystore_path>` – the path to the SecureTransport HSM keystore
- `<validity>` – the validity of the certificate in days

1. Make the SecureTransport installation directory the current working directory using the following command.

    ```
    cd <FILEDRIVEHOME>
    ```

2. Generate a key using the following command.

```
jre/bin/keytool -genkey -keyalg RSA -keysize <key_size> \
    -keystore <keystore_path> -storetype nCipher.sworld \
    -providername nCipherKM \
    -providerclass com.ncipher.provider.km.nCipherKM \
    -alias <alias> -storepass <keystore_passphrase>
```

3. Generate a certificate signing request (CSR) using the following command.

```
jre/bin/keytool -certreq -keystore <keystore_path> \
    -storetype nCipher.sworld -providername nCipherKM \
    -providerclass com.ncipher.provider.km.nCipherKM \
    -alias <alias> -file <CSR_file> -storepass <keystore_passphrase>
```

4. Sign certificate and create the PEM-format certificate file using the following command.

```
bin/openssl x509 -req -in <CSR_file> -days <validity> \
    -CA lib/certs/db/ca-crt.pem -CAkey lib/certs/db/ca-key.pem \
    -CAserial lib/certs/db/serial -out <cert_file>
```

5. Append the public part of the internal CA to the certificate file using the following command. This is required so that SecureTransport can build the certificate chain.

```
cat lib/certs/db/ca-crt.pem >> <cert_file>
```

6. Import the signed certificate into the HSM device using the following command.

```
jre/bin/keytool -importcert -keystore <keystore_path> \
    -storetype nCipher.sworld -providername nCipherKM \
    -providerclass com.ncipher.provider.km.nCipherKM
    -storepass <keystore_passphrase> -alias <alias> -file <cert_file>
```

Use an HSM certificate for FTPS or HTTPS

1. Specify the HSM for SecureTransport by setting the following server configuration parameters:
    - Set `Hsm.keystorePath` to the location of the SecureTransport HSM keystore relative to `<FILEDRIVEHOME>`.
    - (Optional) Set `Hsm.keystorePassword` to the keystore passphrase.

      If you do not store the passphrase as a server configuration parameter, you must enter it each time you start a protocol server that uses an HSM certificate. If you do not type the passphrase in the time allotted, the protocol server does not start.
2. Enable HSM for the protocol servers by setting the following server configuration parameters:
    - Set `Ftp.Hsm.enabled` to `true` to enable HSM for the FTP Server
    - Set `Http.Hsm.enabled` to `true` to enable HSM for the HTTP Server

3. Create a local certificate with the same alias as the HSM certificate you created, for example, `ftpd` or `httpd`. See *Generate a self-issued server certificate* on page 55. SecureTransport does not use this certificate, but you must have a certificate with the correct alias to reference the HSM certificate.
4. Set the SSL key aliases for the protocol servers. See *Manage the FTP server* on page 254 and *Manage the HTTP server* on page 254.
5. Restart the protocol servers. See *Start and stop servers* on page 253.

PGP key encryption and signing

SecureTransport supports PGP encryption. The system handles the generation and storing of PGP keys and the management of the stored keys. The PGP keys are managed from the Administration Tool.

PGP signature verification, encryption, and signing do not work properly when the PGP key has expired. However, SecureTransport continues to decrypt files successfully even when the PGP key has expired.

PGP encryption and signing only support ZIP, BZIP2, and ZLIB compression.

PGP verification is performed using the current time on the computer, not the time when signing occurred.

The following topics describe how to manage the PGP keys and provide the PGP key transfer dependencies:

- *Manage PGP keys* on page 72 - Describes managing the PGP keys.
- *PGP transfer settings dependencies* on page 74 - Provides the PGP key transfer settings dependencies.

Manage PGP keys

PGP keys are managed from the Administration Tool according to their scope: *local* or *partner*.

- *Local PGP keys* can be either server-scoped or account-based. To manage server-scoped certificates select **Setup > Certificates** and the *Local Certificates* tab. Account-based certificates are managed from the *Private Certificates* pane of the *Certificates* pane of the *User Account* page. You can use the appropriate page to get detailed information for a particular key, generate a key, delete a key, or export public and private keys.
- *Partner PGP keys* are also managed by account. You can generate, import, delete, and export account-specific PGP keys. For partner PGP keys, the private key can be exported on certificate creation only. For more information on managing account-based PGP keys, see *Import an X509 or PGP partner certificate* on page 488.

The following topics provide how-to instructions for managing PGP keys:

- *Generate PGP keys* on page 73
- *Export PGP keys* on page 73
- *Import PGP keys* on page 73
- *Local (server) PGP keys management* on page 73

Generate PGP keys

The two scenarios for generation of PGP keys are:

- Generate a local key pair and export it into a text file that can be used by the respective partners for encryption of the incoming data. You can export the private key for a local or account private certificate at any time.
- Generate a partner key pair and export the private key in a file that can be used by the partner for decryption and signing. In this case only the public key is saved and used by SecureTransport. You can save the private key immediately after you generate the key pair. SecureTransport deletes the private key after you save it or decline to save it.

Note Partner and local PGP keys are stored in different key rings. Partner keys are account-specific and have a relation to the account, while local keys are not connected to a particular account. To this end, all partner keys are stored in a single key ring and all partner private keys are stored in a corresponding single secret key ring.

Export PGP keys

PGP keys are exported in the format of ASCII-armored key data in compliance with RFC 2440. The data of the exported PGP key is stored directly in a file. The private key of a partner key pair can only be exported when the certificate is first generated by SecureTransport.

Import PGP keys

There are three scenarios for importing PGP keys into SecureTransport:

- Import a partner PGP public key
- Import a PGP key pair, generated by a third party, in the set of local keys that applies to all of the SecureTransport system
- Import a local PGP key pair as a private certificate from the *Private Certificates* pane of the *Certificates* pane of the *User Account* page

Note The supported formats of the imported keys are as specified in the RFC 2440 standard: a binary or armored PGP public/private key message.

Local (server) PGP keys management

Local (server) and partner PGP keys are generated, exported, imported, and deleted for a particular account. See *Manage certificates* on page 476.

PGP transfer settings dependencies

The following PGP transfer settings dependency matrix shows different configurations and scenarios for PGP-encrypted transfers depending on the transfer settings, accessible from the *Subscription* page.

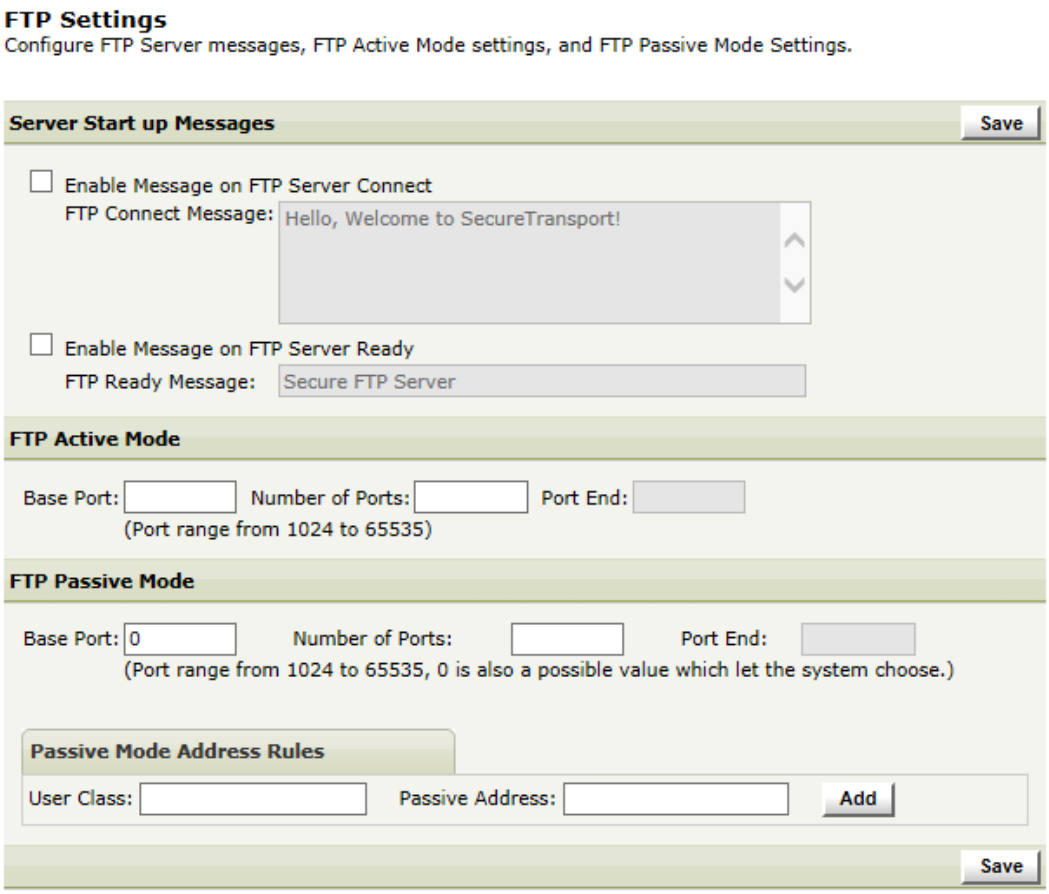
Incoming file	Encryption required	Signature required	Server action	Result	Transfer status
Signed only	ON	ON	SecureTransport attempts decryption and verification.	Decryption fails, because the file is not encrypted, and therefore no verification is performed.	Unsuccessful
Encrypted only	ON	ON	SecureTransport attempts decryption and verification.	Decryption is successful, but verification fails, because the file is not signed.	Unsuccessful
Signed and Encrypted	ON	ON	SecureTransport attempts decryption and verification.	Decryption and verification are successful, and the signature is removed.	Successful
Plain text	ON	ON	SecureTransport attempts decryption and verification.	Decryption fails because the file is not encrypted, and no verification is performed.	Unsuccessful

Incoming file	Encryption required	Signature required	Server action	Result	Transfer status
Signed only	ON	OFF	SecureTransport attempts decryption without verification.	Decryption fails because the file is not encrypted, and no verification is performed.	Unsuccessful
Encrypted only	ON	OFF	SecureTransport attempts decryption without verification.	Decryption is successful, and no verification is performed.	Successful
Signed and Encrypted	ON	OFF	SecureTransport attempts decryption without verification.	Decryption is successful, and no verification is performed, but the signature is removed.	Successful
Plain text	ON	OFF	SecureTransport attempts decryption without verification.	Decryption fails because the file is not encrypted, and no verification is performed.	Unsuccessful
Signed only	OFF	ON	SecureTransport attempts verification without decryption.	No decryption is performed. Verification is successful and the signature is removed.	Successful

Incoming file	Encryption required	Signature required	Server action	Result	Transfer status
Encrypted only	OFF	ON	SecureTransport attempts decryption (to get to the signature) and verification.	Decryption is successful, but verification fails, because the file is not signed.	Unsuccessful
Signed and Encrypted	OFF	ON	SecureTransport attempts decryption (to get to the signature) and verification.	Decryption and verification are successful.	Successful
Plain text	OFF	ON	SecureTransport attempts verification without decryption.	No decryption is performed. Verification fails because the file is not signed.	Unsuccessful

Configure FTP server messages and modes

Use the *FTP Settings* page to enable and disable FTP server messages and to configure active mode and passive mode for the FTP server.



The following topics describe FTP server messages, provide how-to instructions for setting FTP active and passive modes, provide FTP server limitations, and describes how to improve FTP performance and increase the FTP timeout for large files:

- *FTP server messages* on page 78 - Describes the FTP messages and provides how-to instructions for creating and editing server connect and server ready messages.
- *Set up FTP active mode* on page 79 - Provides the how-to instructions for setting up FTP active mode.
- *Set up FTP passive mode* on page 80 - Provides the how-to instructions for setting up FTP passive mode.
- *FTP server limitations* on page 82 - Describes the FTP server limitations.
- *Improve FTP performance on a multi-homed system* on page 83 - Provides the how-to instructions for improving FTP performance on a multi-homed system.
- *Increase the timeout for large files using server-initiated transfer* on page 83 - Provides the how-to instructions to increase the FTP timeout for large files using server-initiated transfers.

FTP server messages

FTP server messages are messages displayed to users at the startup of an FTP session. Two types of startup FTP server messages are available:

- FTP connect messages
- FTP server ready messages

Users might or might not see FTP server messages, depending on the software they use to connect to SecureTransport. Most FTP client applications display these messages, but they are not displayed on browser clients. Users downloading a single file by URL from a browser might not see these messages.

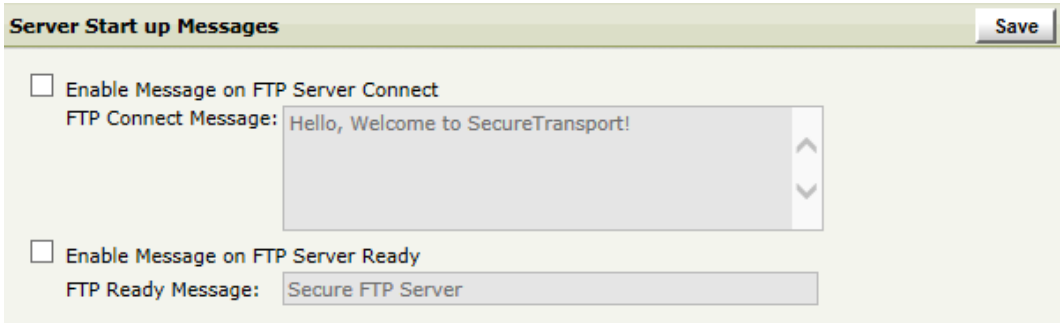
Startup messages are displayed while a connection to the server is being established, prior to any login prompt. A message is displayed to the user when the connection is established. A server ready message also be displayed when SecureTransport is ready to accept a login. The default message displays the host name of the server and the server version, but this can be overridden.

The following topics provide how-to instructions for creating or editing server connect message and server ready message:

- *Create or edit the server connect message* on page 78
- *Create or edit the server ready message* on page 79

Create or edit the server connect message

1. Select **Setup > FTP Settings** to open the *FTP Settings* page.
2. Under *Server Start up Messages:*



   a. Select **Enable Message on FTP Server Connect** to display a message to users logging onto SecureTransport through the FTP Server. By default, this option is not selected.

   b. In the **FTP Connect Message** field, type the message you want to be displayed when a user connects to the SecureTransport Server

3. Click **Save** to apply the changes.

Create or edit the server ready message

1. Select **Setup > FTP Settings** to open the *FTP Settings* page.
2. Under *Server Start up Messages:*
   a. Select **Enable Message on FTP Server ready** to display a message indicating that the server is ready to accept logins. By default, this option is not selected.
   b. In the **FTP Ready Message** field, type the message you want to be displayed when the server is ready.
3. Click **Save** to apply the changes.

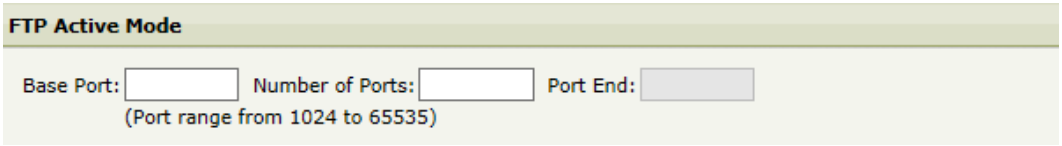
Set up FTP active mode

You can configure SecureTransport to use active mode connections for server-initiated transfers over FTP. Use the active mode options to configure the server-initiated transfer agents to initiate these requests. You can specify an active mode base port and a range of ports that can be used for active mode. Make sure the ports are accessible on the firewall.

The base port represents the first port number you want to assign. The number of ports specifies how many open ports you want to allow. For example, the base port is set to 10000 and the number of ports is set to 1024, active mode connections can use only the ports from 10000 to 11023. The end port should display 11023. Acceptable values are between 1024 and 65535. If the range is not specified, the server randomly selects an unused high port number greater than 1023 for active mode.

Active FTP mode can be used only for internal connections where there is no proxy between SecureTransport and the remote server. You must select **Enable Active Connection Mode** to use Active FTP in an FTP transfer site.

1. Select **Setup > FTP Settings** to open the *FTP Settings* page.
2. Under *FTP Active Mode*:



   a. Type the appropriate port number for the **Base Port**. This is the first port used.
   b. Type the **Number Of Ports**. This value sets the range of ports available for use.

      The **Port End** field should display the appropriate port number for the last port in the range you want to use.
3. Click **Save** to apply the changes.

Note To use Active FTP with an FTP(S) transfer site, by pass the proxy by setting the **Network Zone** field to **none**. See *FTP(S) transfer sites* on page 515.

Set up FTP passive mode

If an FTP client is behind a firewall that does not permit SecureTransport to open a data port as required by active mode FTP, you use the passive mode options to configure the FTP server to accept passive mode FTP connections. You specify a passive mode base port and a number of ports that can be used for passive mode. Make sure the ports are accessible through the firewall. Do not use these ports for any other service.

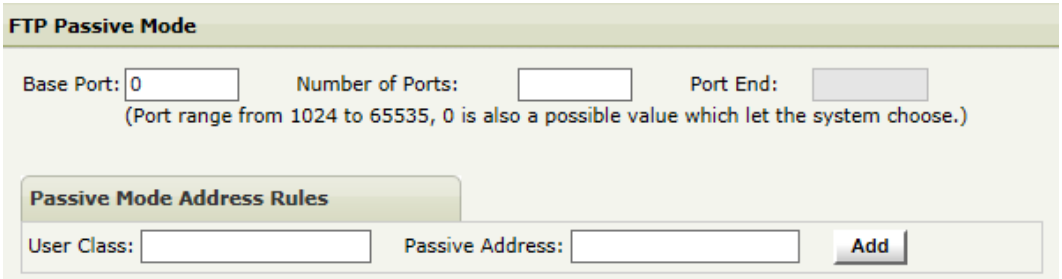
The base port represents the number of the first port available for the FTP server to use for a passive mode data connection. The number of ports specifies how many open ports to allocate. For example, the base port is set to 10000 and the number of ports is set to 1024, the FTP server can use only the ports from 10000 to 11023 for passive mode data connections.

Specify ports for five times the expected number of concurrent connections based on the following considerations:

- If the port range is too small or equal to the number of expected number of connections, a port to connect might not be available when needed. The operating system does not release a port immediately after a user disconnects, so the free port does not become available for another connection immediately. This can result in a failure when a new connection is attempted.
- When most of the ports are used up and a new connection is attempted, the server scans for the next available port. This is resource intensive and can affect the performance of the server. With a large pool of ports, finding next available port is quicker and is less likely to affect the performance.

You can also set up passive address rules, which allow the SecureTransport server to respond with the external address of the firewall instead of the internal address of the server when a FTP client issues the `PASV` (passive mode) command.

1. Select **Setup > FTP Settings** to open the *FTP Settings* page.
2. Under *FTP Passive Mode*:



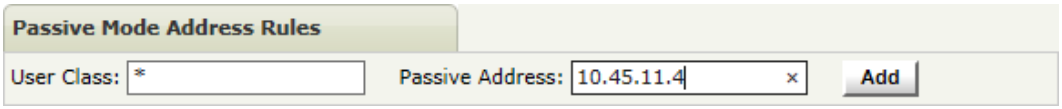
   a. Type the appropriate port number for the **Base Port**. This is the first port used.
   b. Type the **Number Of Ports**. This value sets the range of ports available for use.
3. The **Port End** field displays the number for the last port to use.
4. Click **Save** to apply the changes.

The following topics provide how-to instructions for adding and editing a passive mode address rules and insuring that passive mode sessions are initiated on the correct system:

- *Add passive mode address rules* on page 81
- *Edit a passive mode address rule* on page 81
- *Assure that passive mode sessions are initiated on the correct system* on page 82

Add passive mode address rules

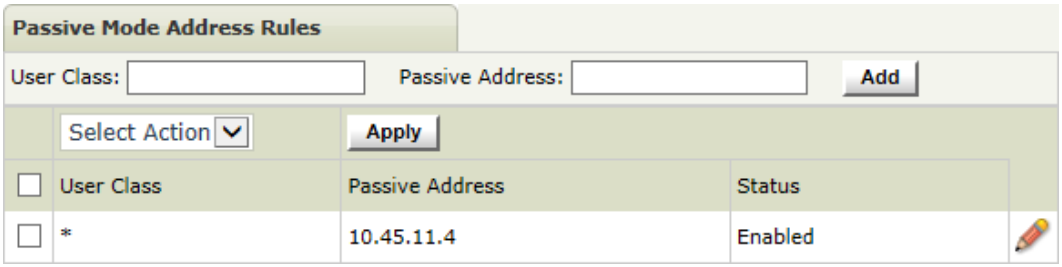
1. Under *Passive Mode Address Rules*, enter in the **User Class** field a pattern that matches the user classes for which this rule will be applied. Use question mark (`?`) to match one character and asterisk (`*`) to match any sequences of characters. For example, enter `*` to apply the rule to all user classes.
2. Type the external address with which the FTP server should respond in the **Passive Address** field.



3. Click **Add** to add the rule. To make the change permanent, click **Save**.

Edit a passive mode address rule

1. To change the **User Class**, **Passive Address** or **Status** of a rule, click the Edit icon ( ) at the end of the rule.



2. Make the required changes in the fields and click the Save icon ( ).
3. To change the status of one or more rules or to remove a rule entirely, select in the left column each rule to modify.
4. From the **Select Action** list, choose **Delete**, **Enable**, or **Disable** and click **Apply** to make the change.
5. To make your updates on this page permanent, click **Save**.

Assure that passive mode sessions are initiated on the correct system

When clients open passive mode sessions though a load balancer, a client communicating on the server assigned port might create a new session which opens a port on a different system than the originally contacted one. You can prevent this issue by configuring the load balancers and servers.

- Set the load balancer to use "session sticky" mode. This ensures that the data-channel connection goes to the same system that serviced the control-channel connection.
- Make sure to set a passive-mode address rule on all the SecureTransport Edge gateways or servers to return the external IP address of the load balancer in the response to the PASV command instead of the internal address of the SecureTransport Edge.

FTP server limitations

The FTP server has the following limitations:

- *FTP APPE command* on page 82
- *FTP COMB command* on page 82
- *FTP client configuration* on page 83

FTP APPE command

SecureTransport handles the FTP `APPE` command differently than it is typically handled. Typically, the `APPE` command appends uploaded content to an existing file of the same name.

FTP COMB command

SecureTransport supports the `COMB` command only for the CuteFTP client. The CuteFTP client separates the file into chunks and uploads them as temporary files on the FTP server. Once CuteFTP uploads all the file chunks on the FTP server, it sends the `COMB` command to combine them. By default, file names are generated by the CuteFTP client to match the pattern: `\d.tmp` where `\d` is a decimal number. However, the first file chunk name is the original file name.

Note The `COMB` command cannot be combined with post-transmission actions, repository encryption, or PGP data transformations.
Because SecureTransport releases the FTP command channel after successfully uploading the multiple file chunks, using the `COMB` command does not provide a guaranteed file transfer. If there is no space left in the upload directory or if errors exist during the process of combining the file chunks, the transfer fails, but no errors are sent to the client.

FTP client configuration

If FTP clients with default settings use SmartFTP and IglooFTP, when users connect to a server, they are unable to view remote files and folders. Some settings for LIST arguments need to be configured manually. The `Resolve Links [-L]` argument must be removed for both clients, but leave the show all file `[-a]` argument.

Improve FTP performance on a multi-homed system

You can improve FTP performance by assigning an IP address to the server if you are using a multi-homed system.

1. Select **Operations > Server Configuration**.
2. In the *Server Configuration* page, search for the `Ftp.Host` parameter.
3. Set the value of the parameter to the IP address for the server.
4. Restart the FTP Server on all servers in your cluster.

Increase the timeout for large files using server-initiated transfer

When sending 1.5 GB or larger files, the default timeout settings might be too low and SecureTransport might throw an exception error. You can increase the timeout settings for the FTP(S) and HTTP(S).

1. Select **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.
2. Search for the `OutboundConnections.connectTimeout` and `OutboundConnections.receiveTimeout` parameters.

   The default value for each parameter is 25 seconds.
3. Set the value of each parameter to the amount of time it takes to upload the file in seconds. For example, if the file takes 20 minutes to upload, then increase the value of each parameter to 1200 seconds or higher.
4. Restart the TM Server on all servers in your cluster.

Configure AS2 server settings

Using the *AS2 Settings* page, you can configure the following AS2 settings that apply to all partnerships:

- Server authentication (enable or disable). By default, server authentication is disabled.
- Sending to and receiving from all partnerships (enable or disable). By default, sending and receiving is enabled for all partnerships.
- Maximum file sizes for sending and receiving. The default maximum file sizes are 50 megabytes.
- Asynchronous Receipt Receiver for HTTP and HTTPS.

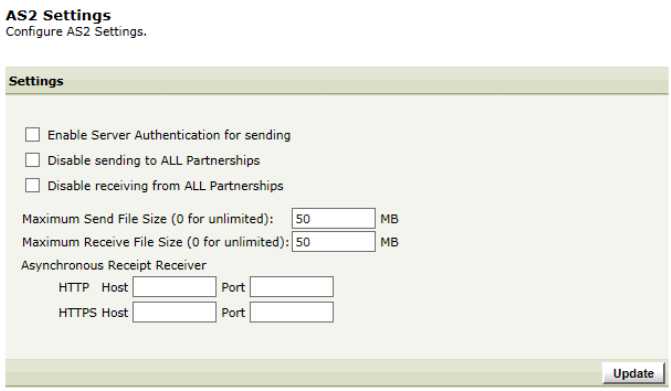
For detailed information about AS2 transfers, see *AS2 transfers* on page 954.

Configure AS2 transfer settings

Use the following procedure to configure AS2 transfer settings.

1. Select **Setup > AS2 Settings**.

   The *AS2 Settings* page is displayed.



2. Select the check box for **Enable Server Authentication for sending** to request server authentication for outbound transfers.

   Note If server authentication is enabled, the local SecureTransport AS2 server authenticates the remote (partner) server during the SSL connection. This is an additional layer of security to that provided by AS2. To be authenticated, the remote server must present a certificate signed by a certificate authority that is trusted by SecureTransport. For information about importing trusted CA certificates for indirect trust of partner server certificates, see *Import a trusted CA certificate* on page 62.

3. Select the check box for **Disable sending to ALL Partnerships** to turn off all outbound transfers to AS2 partner sites.
4. Select the check box for **Disable receiving from ALL Partnerships** to turn off all inbound transfers from AS2 partner sites.

5. Set the **Maximum Send File Size** for outbound traffic. The file size is measured in MB.

   To allow unlimited file sizes, enter 0 (zero). However, to transfer files larger than 2 GB, the remote partner site must support chunking and have it enabled in its Send Options.

6. Set the **Maximum Receive File Size** for inbound traffic. The file size is measured in MB.

   To allow unlimited file sizes, enter 0 (zero).

7. Enter host names and port numbers for the HTTP and HTTPS protocols for the **Asynchronous Receipt Receiver**.

   Outgoing AS2 messages are sent by the SecureTransport Server. If an asynchronous receipt is requested from a partner, the partner server tries to reach the AS2 port on the SecureTransport Server. In a two-layer architecture, asynchronous receipts should be delivered to SecureTransport Edge. In that case, host and port numbers in these fields should be set to AS2 server on SecureTransport Edge.

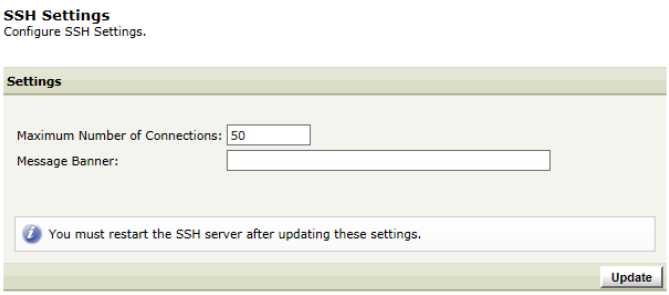
8. When you complete editing the settings, click **Update**.

Configure SSH server settings

Use the *SSH Settings* page to specify the maximum number of SSH connections and to set up an SSH message banner with text that you want users to see when logging onto SecureTransport from an SSH client.

1. Select **Setup > SSH Settings**.

   The *SSH Settings* page is displayed.



2. Provide the following SSH settings:

   - **Maximum Number of Connections** – Type the maximum number of SSH clients that can simultaneously connect to the SSH server. If the maximum number of concurrent connections is reached, SecureTransport prevents any further connections before the user is authenticated.
   - **Message Banner** – Type the message that you want users to see when logging in to the SecureTransport Server from an SSH client. For example, you can enter a legal notice, a disclaimer, or a welcome message.

3. If you increase the value of **Maximum Number of Connections**, you must also increase the value of `JAVA_MEM_MAX` in the `<FILEDRIVEHOME>/bin/start_sshd` script.

The script uses the `JAVA_MEM_MAX` value to set the maximum heap size for the Java Virtual Machine (JVM). The SSH server allocates memory in the heap for each connection (and frees it when the connection is closed). To avoid SSH service interruptions when no memory is available in the Java heap, you must configure `JAVA_MEM_MAX` to the desired **Maximum Number of Connections** (as defined in the previous step) multiplied by 10,000 Kibibytes. However, in the script file, you must convert this result to Megabytes (10,000 Kibibytes is equivalent to 10.24 Megabytes). For example, 500 concurrent connections would require a value of 500 * 10,000 KiB = 5,000,000 KiB. This is equivalent to 5120 Megabytes, so enter this in the script file as:

```
JAVA_MEM_MAX="5120M"
```

Use `M` to specify Megabytes. Do not insert a space between the number and the `M`.

4. Click **Update**.
5. After updating the SSH settings, restart the SSH server. See *Start and stop servers* on page 253.

Related topics:

- *Bind SSH and SSHD to the same port number* on page 86
- *Debug SSH issues* on page 86

Bind SSH and SSHD to the same port number

When you need to use port 22 for an AIX server and for SecureTransport, use the following steps:

1. On the server hosting SecureTransport, edit the SSHD configuration file, for example, `/etc/ssh/sshd_config`. (To find the location on your system, refer to `man 5 sshd_config`.) Set the `ListenAddress` directive, then find the `sshd` process ID and use the command `kill -HUP`. You should perform these steps directly on the server so you must have a keyboard and monitor for the computer.
2. Log on to the Administration Tool and select **Operations > Server Configuration**.
3. On the *Server Configuration* page, search for the `SSH.Host` parameter and sets its value to the actual IP address of the host.
4. Restart the SSH server.

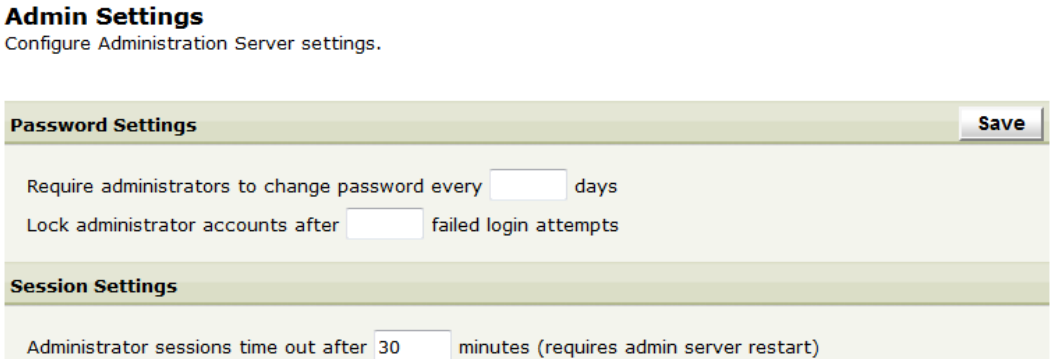
Debug SSH issues

If you are trying to determine an issue with SSH, changing the `mchange` and `ehcache` logger parameters in the `sshd-log4j.xml` file to `Debug` can prevent SSH from receiving connections. To work around this issue, you can reset `sshd-log4j.xml` to send log messages to a file instead of the database. Follow the steps in *Redirect log4j output from the database* on page 1003 to change the log.

Note When log messages are stored in the database, they are displayed in the *Server Log* page. When you store the log messages in a file, they are not displayed in the *Server Log* page.

Configure Administration Tool server settings

Use the *Admin Setting* page to configure administrator login options. You can configure the password expiration, the number of consecutive failed login attempts allowed and the length of a login session.



The following sections provide how-to instructions for changing password settings, session settings, and certificate settings:

- Change password settings
- Change session settings

Change password settings

Use the password settings to control how often an administrator needs to change the login password and to control how many consecutive failed login attempts are allowed before the administrator is prevented from logging in.

1. Select **Setup > Admin Settings**.
2. Type the number of days the administrator password is valid without changing it.

   You can leave this field blank, which is the default setting. When left blank, the password never expires.
3. Type the number of consecutive failed login attempts to allow before preventing an administrator from logging in to the server.

   You can leave this field blank, which is the default setting. When left blank, there is no limit to the number of login attempts permitted.
4. Click **Save** to accept the changes.

Note If the master administrator is locked out (or the wrong password is used too many times), contact Axway Global Support for the procedure to reset the required parameters.

Change session settings

Use the session settings to control how long an administrator can be logged into SecureTransport before the session expires and the administrator must log in again.

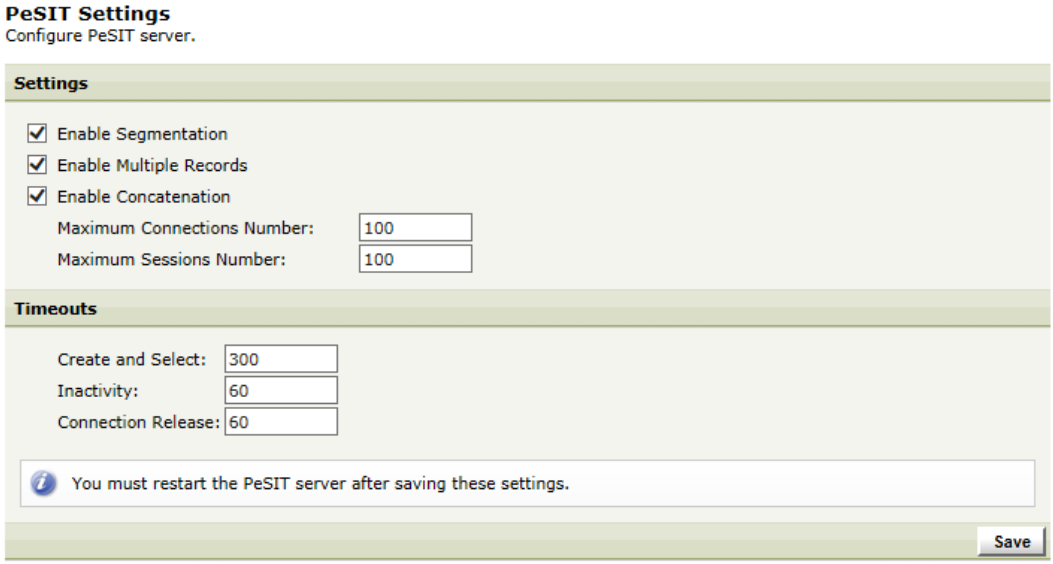
1. Select **Setup > Admin Settings**.
2. Type the number of minutes the session stays active. The default setting is 30 minutes.
3. Click **Save** to accept the changes.
4. Restart the Administration Tool server using the `stop_admin` and `start_admin` commands.

PeSIT server configuration settings

Use the *PeSIT Settings* page to configure the PeSIT protocol server.

1. Select **Setup > PeSIT Settings**.

   The *PeSIT Settings* page is displayed.



2. Provide the information as described in the following table:

Name	Description
Settings	
Enable Segmentation	If a data article (record) is larger than the maximum size, it is sent in multiple FPDUs (messages).

Name	Description
Enable multiple records	If more than one data article fits in a FPDU, they are sent in one FPDU.
Enable Concatenation	Allow several FPDUs to be sent in one TCP message unit.
Maximum Connections Number	The maximum number of concurrent TCP connections remote PeSIT servers can make
Maximum Sessions Number	The maximum number of concurrent sessions remote PeSIT servers can make
Timeouts	
Create and Select	For connections initiated by a remote PeSIT server, the time in seconds that SecureTransport waits for a PeSIT F.CREATE or a F.SELECT command before SecureTransport closes the connection
Inactivity	For connections initiated by a remote PeSIT server, the time in seconds that a connection may be inactive before SecureTransport closes it
Connection Release	For connections initiated by a remote PeSIT server, the time in seconds that SecureTransport waits for a response to a PeSIT F.RELEASE command before SecureTransport closes it

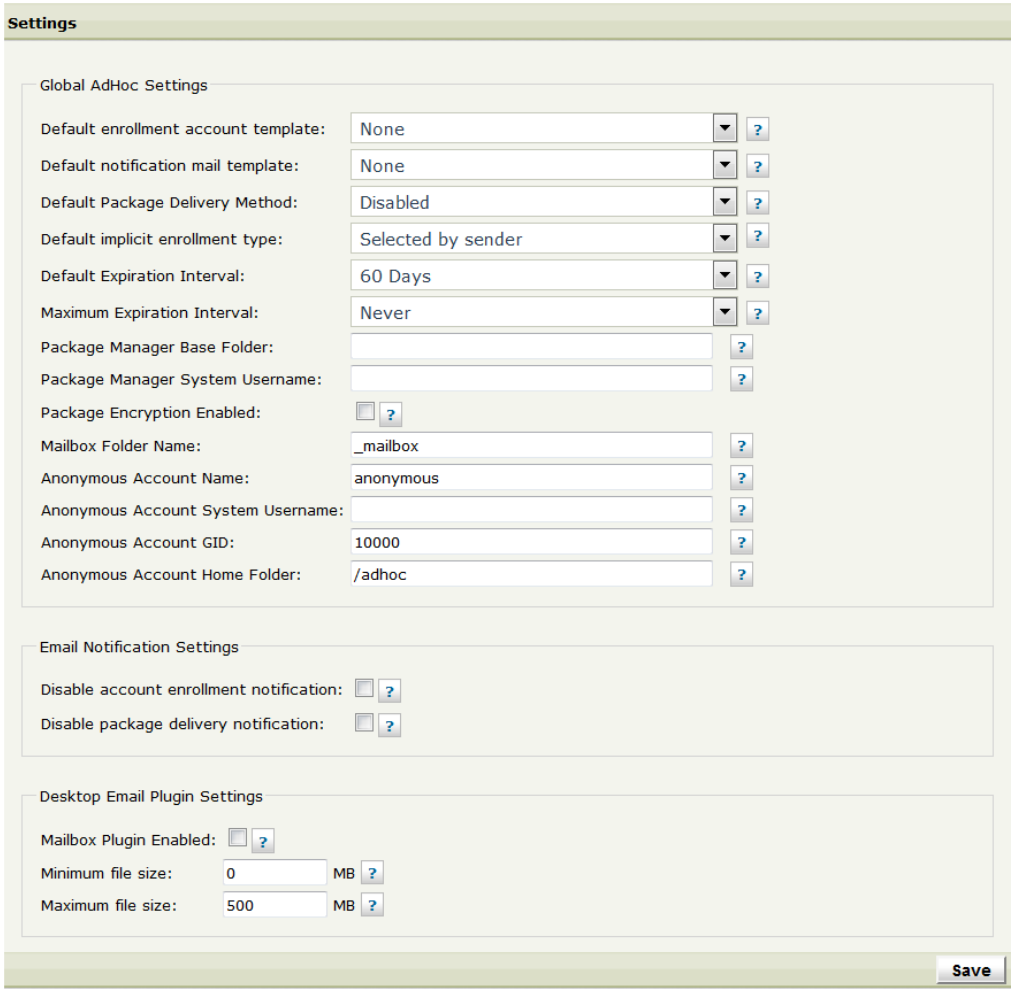
3. Click **Update**.
4. On the *Server Control* page, restart the PeSIT server.

Configure adhoc file transfers

Use the *AdHoc Settings* page to configure parameters and defaults for adhoc file transfers using ST Web Client or the Axway Email Plug-ins.

1. Select **Setup > AdHoc Settings**.

   The *AdHoc Settings* page is displayed.



2. Provide the information as described in the following table:

Name	Description
Global AdHoc Settings	
Default enrollment account template	SecureTransport uses this account template when enrolling an adhoc file transfer recipient. For information about account templates, see *Account templates* on page 661.
Default notification mail template	SecureTransport uses this mail template to create all notification emails to adhoc file transfer recipients and senders. For more information about mail templates, see *Mail templates* on page 173.

Name	Description
Default Package Delivery Method	SecureTransport uses this delivery method when the **Delivery Method** field in *Account Setting* for a user account, in an account template, or in a business unit is set to **Default**. • **Disabled** – Adhoc file transfers are disabled. • **Anonymous** – The adhoc file transfer recipient receives a link to retrieve the files and is not enrolled as a user. • **Account Without Enrollment** – Do not enroll adhoc file recipients. Only existing users can receive files. • **Account With Enrollment** – The adhoc file must enroll as a SecureTransport user before retrieving the files. • **Custom** – Select the allowed enrollment types in the **Default enrollment type** field. Depending on the value of the **Default implicit enrollment type** field, the sender chooses one of the selected enrollment types when composing the mail in ST Web Client.
Default enrollment type	• **Anonymous** – The adhoc file transfer recipient receives a link to retrieve the files and is not enrolled as a user. • **Challenge** – The adhoc file recipient receives a link and must answer a challenge question correctly to retrieve the files. The recipient is not enrolled as a user. • **Existing Account** – Do not enroll adhoc file recipients. Only existing users can receive files. • **Enroll Unlicensed** – The adhoc file recipient must enroll as a SecureTransport unlicensed user before retrieving the files. An unlicensed user can only reply once to the email and retrieve the files. Other user attributes are defined by the enrollment template. • **Enroll Licensed** – The adhoc file recipient must enroll as a SecureTransport user with all the attributes specified in the default enrollment template before retrieving the files.
Default implicit enrollment type	The values displayed depend on the settings of **Default Package Delivery Method** and **Default enrollment type**. ST Web Client sets this value as the initial value selected in the *User Access* window when a user with the **Delivery Method** field set to **Default** composes an email. The Axway Email Plug-ins use this value as the delivery method when a user with the **Delivery Method** field set to **Default** composes an email. **Challenge** is not an option because the Axway Email Plug-in do not include the challenge question and answer function.

Name	Description
Default Expiration Interval	ST Web Client displays this value as the initial value of the **Expiration** drop-down list in the *Compose Mail* tab. The Axway Email Plug-ins use this value as the expiration interval for all messages. The choices are: 1 Day, 7 Days, 30 Days, 60 Days, and Never.
Maximum Expiration Interval	ST Web Client displays this value as the largest value of the **Expiration** drop-down list in the *Compose Mail* tab. The choices are: 1 Day, 7 Days, 30 Days, 60 Days, and Never.
Package Manager Base Folder	SecureTransport uses this working folder to process adhoc file transfers. In a cluster, all servers use the same folder, so specify the same location in shared storage. To enable adhoc file transfers, you must specify this folder. For a list of folder that are not allowed, see *Protected folders and accounts* on page 475.
Package Manager System Username (Windows only)	If the package manager base folder is in shared storage, enter the user name of the Windows system user that SecureTransport uses to access the package manager base folder. The user must be in the SecureTransport password vault. If you change this field, you must not remove the previous user from the password vault.
Mailbox Folder Name	SecureTransport creates a folder with this name in the user's home folder to store the user's mail folders. Because the mail folders are for use for adhoc file transfers only, these folders are not visible to clients. Do not modify any files in these folders or in the mail folders.
Anonymous Account Name Anonymous Account UID Anonymous Account GID Anonymous Account Home Folder	SecureTransport uses this account name, UID, GID, and home folder when an adhoc file transfer recipient logs in anonymously to retrieve a file. You must create this account.
Email Notification Settings	
Disable account enrollment notification	SecureTransport does not send out account enrollment notifications when this option is selected. If you select this option, you must manage any account enrollment notifications externally using REST API from your email system. By default, this option is not selected.

Name	Description
Disable package delivery notification	SecureTransport does not send out package delivery notifications when this option is selected. If you select this option, you must manage any package delivery notifications externally using REST API from your email system. By default, this option is not selected. **Note** Package delivery notifications can also be disabled by the end user. If you do not select this option, the end user can disable package delivery notifications. If you select this option, the end user cannot override your selection and package delivery notifications will be disabled even if they are enabled by the end user.
Desktop Email Plugin Settings	
Mailbox Plugin Enabled	SecureTransport allows adhoc file transfers using the Axway Email Plug-ins when selected.
Minimum file size	SecureTransport does not transfer files smaller than the value specified using the Axway Email Plug-ins.
Maximum file size	SecureTransport does not transfer files larger than the value specified using the Axway Email Plug-ins.

3. Click **Save**.

Two server configuration parameters control handling of human-to-system (H2S) transfers:

- By default, value of the `PackageManager.DualDeliveryDisabled` server configuration parameter is **true** and SecureTransport stores the files attached to an H2S email in the target folder and processes them but does not send the email to the system user. If value of `PackageManager.DualDeliveryDisabled` is **true**, SecureTransport also sends the email to the system account. If the email recipients also include H2H addresses, SecureTransport sends the email to the those recipients regardless of the value of `PackageManager.DualDeliveryDisabled`.
- By default, value of the `PackageManager.BodyRoutingDisabled` server configuration parameter is **true** and SecureTransport ignores the body of an H2S email. If value of `PackageManager.BodyRoutingDisabled` is **false**, SecureTransport puts the body of the email in a text file with a name of the form *`uniqueID`*`_body_wap.txt` and stores it with the files attached to an H2S email in the target folder.

The following topics provide how-to instructions for changing the package manager base folder and describe the Package Retention Maintenance application.

- *Change the package manager base folder* on page 94
- *Create a Package Retention Maintenance application* on page 776

Change the package manager base folder

To change the package manager base folder on a root installation:

1. Log on to the SecureTransport Server as root.
2. Stop all SecureTransport protocol servers and services.
3. If the new folder is on a network share, so that LDAP users can access the package manager base folder, mount the new network share on which the new package manager base folder is located using the default UID and GID specified in LDAP domain page for those users.
4. Copy the package manager base folder to its new location.
5. Delete the old package manager base folder.
6. So that references to the old package manager base folder still work, create a symbolic link that points to the new package manager base folder at the location of the old package manager base folder with the same names as the old package manager base folder.
7. Start the database and the Administration Tool service.
8. In the Administration Tool, change the **Package Manager Base Folder** field to reference the new package manager base folder.
9. Start the remaining SecureTransport services and protocol servers.

Note You can make a package manager base folder stored on a network share accessible for users of only one LDAP domain.

- *Create a Package Retention Maintenance application* on page 776

Configure your database

SecureTransport uses a database to store configuration parameters and data, including log data. With Standard Clustering, SecureTransport Server uses an embedded MySQL database server. With the Enterprise Clustering (EC) option, SecureTransport Server uses a shared external Microsoft SQL Server or Oracle database. With the external Oracle database, you can direct log data to separate databases. SecureTransport Edge always uses an embedded database server.

During installation, you specified the database to use and its parameters. Use the *Database Setting* page to change database parameters, to switch from the embedded database to an external Oracle database, or to direct log data to separate Oracle databases.

The following topics provide how-to instructions managing databases, changing from internal database to external database, and changing external databases.

- *Change the embedded database port or password* on page 95
- *Switch from the embedded database to an external Oracle database* on page 96
- *Direct log data to separate Oracle databases* on page 99
- *Change the external Oracle database* on page 100

- *Improve server resiliency in case of Oracle RAC node failure* on page 101 .
- *Change the external Microsoft SQL Server database* on page 102

Change the embedded database port or password

If your SecureTransport installation uses an embedded database, you can change the database port or password. The MySQL configuration is stored in the `<FILEDRIVEHOME>/conf/mysql.conf` file.

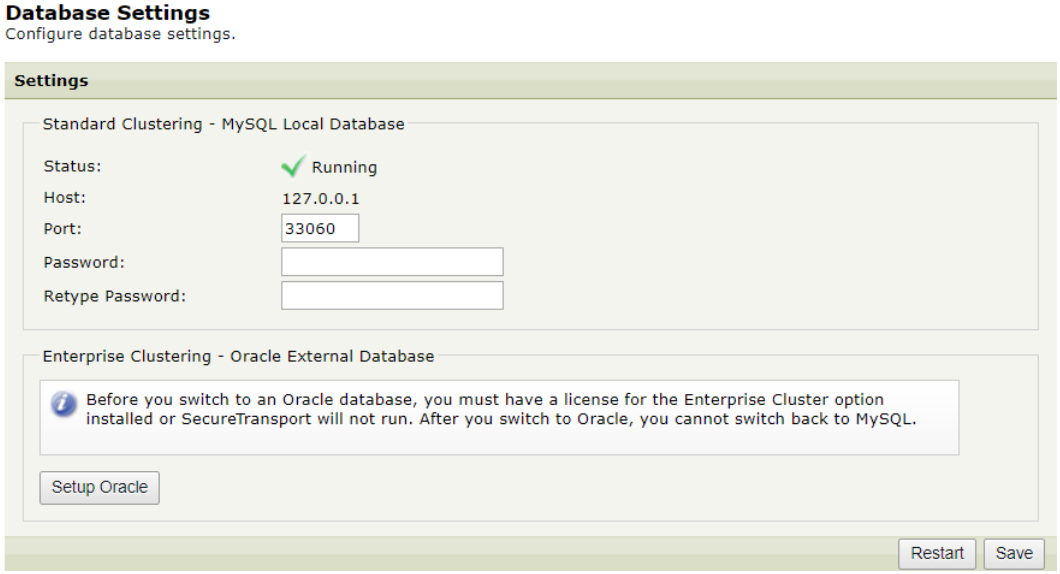
Make sure you perform these changes separately, as described in the following subtopics.

Note A SecureTransport administrator with database reconfiguration permissions can change the MySQL port and password and restart the MySQL database service using the respective Admin REST API resource: `/configurations/database/mysql`.

Change the embedded database port

1. Select **Setup > Database Settings**.

   The *Database Setting* page is displayed.



2. Under *Standard Clustering - MySQL Local Database*, type the new port number in the **Port** field.
3. Click **Save**.
4. Click **Restart Database Now**.
5. After the database restart, restart all SecureTransport services.

Change the embedded database password

Note After installation, the embedded database password is `tumbleweed`. For better security, change it as described in the following procedure.

1. Select **Setup > Database Settings**.

   The *Database Setting* page is displayed.

2. Under *Standard Clustering - MySQL Local Database*, type the new password in both the **Password** and **Retype Password** fields.
3. Click **Save**.
4. Restart all SecureTransport services.

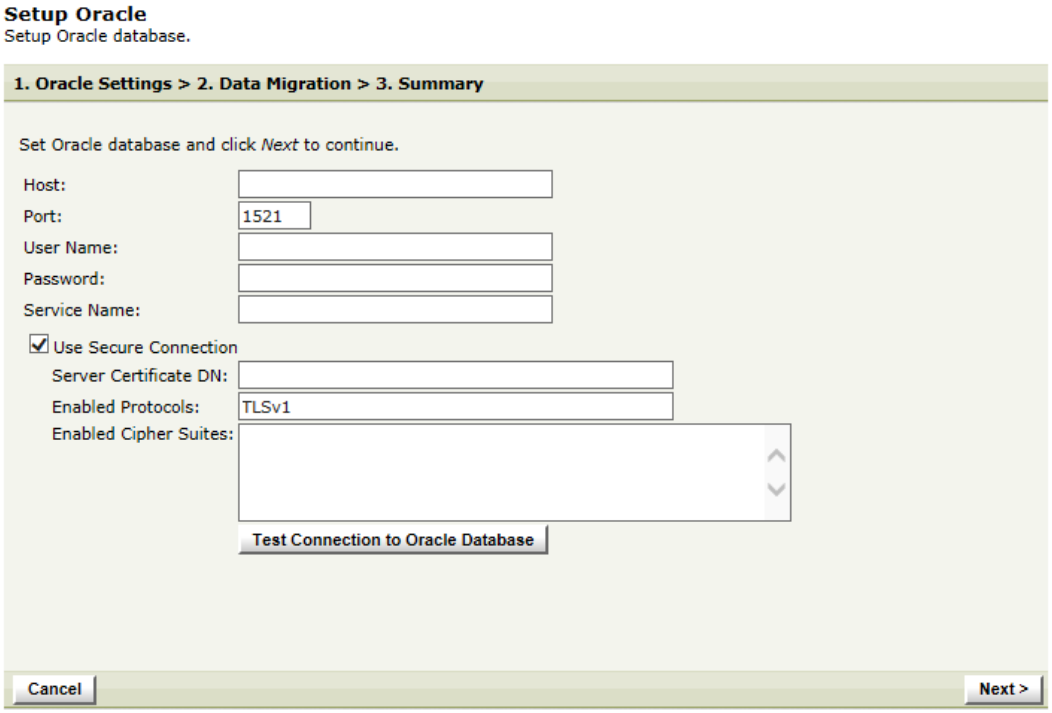
Switch from the embedded database to an external Oracle database

If you upgraded a SecureTransport Server that used the embedded database or selected the embedded database when you installed SecureTransport Server, you can switch to an external Oracle database. In order to switch to an external Oracle database, you must have a license for the EC option installed or SecureTransport will not run. After you switch to the external database, you cannot switch back to the embedded database.

When you switch from the embedded database to an external Oracle database, you must set up the database. In this process, you specify the parameters of the Oracle database and SecureTransport migrate the configuration and data from the existing embedded database to the Oracle database. When the migration completes, you can use the SecureTransport Server as a stand-alone server or as the first server in an Enterprise Cluster (EC).

1. Make sure the Oracle database has the characteristics listed in the *Database installation prerequisites* topic of the *SecureTransport Installation Guide*.
2. Select **Operations > Server Control** and stop all servers.
3. Select **Setup > Database Settings > Setup Oracle**.

   The *Database Setting* page is displayed.



4. On the *Oracle Settings* page of the Oracle wizard, type the values necessary to connect to the external database.

   The information required is:

   - **Host** – The host name or IP address of the Oracle server or cluster
   - **Port** – The port used to access the server or cluster, 1521 is the default
   - **User Name** – The name of the user authorized to create the SecureTransport schema and populate it
   - **Password** – The password for the user, not displayed
   - **Service Name** – Used to connect a server or cluster
   - **Use secure connection** – When **Use secure connection** is checked, the connection between SecureTransport and the database server will be encrypted. If **Use secure connection** is checked, the following options should be configured:
     - **Server Certificate DN** (optional) – If the server is successfully authenticated (meaning its certificate is trusted), its DN can be checked. If a value is entered in this field, it will be compared with the server certificate DN. If they do not match, the connection won't be successful.
     - **Enabled Protocols** - List of enabled protocols. TLSv1 is the default protocol.
     - **Enabled Cipher Suites** - List of the enabled cipher suites.

     Note Before secure connection is enabled, the issuers certificates of the database server certificate, should be imported in the Trusted CA certificates store.

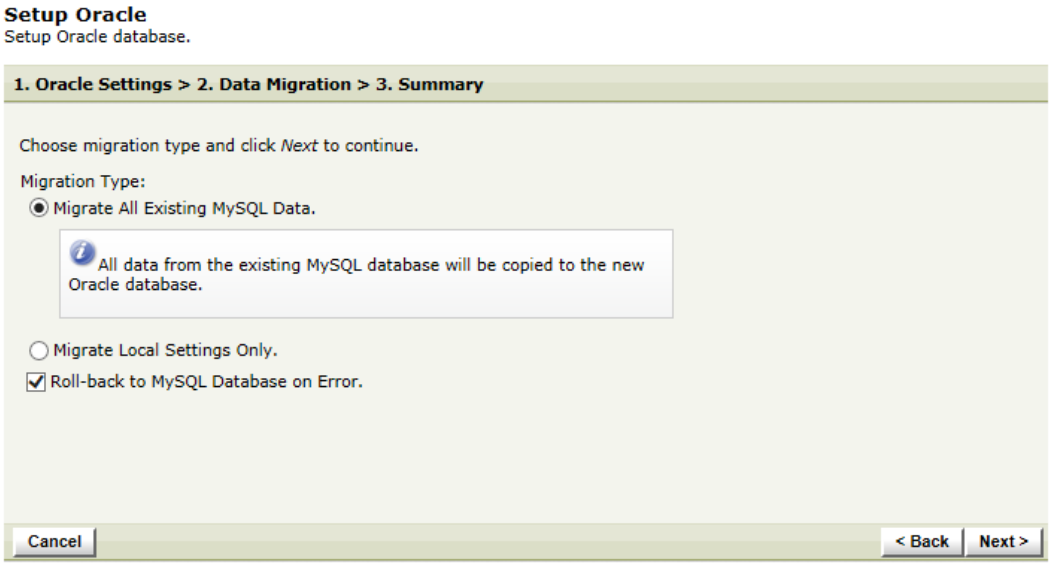
5. To direct log data to separate external databases, see *Direct log data to separate Oracle databases* on page 99.

6. Click **Test Connection to Oracle Database**.

   If SecureTransport displays a failure message, correct the network, Oracle, or other error reported and try again.

7. Type the password again, and click **Next**.

8. On the *Data Migration* page, select the **Migration Type**:



   - If you are upgrading the first server in a cluster, select **Migrate All Existing MySQL Data**. The process creates a new database schema that contains all the data from the existing database and configuration.
   - If you are upgrading the second and subsequent servers in a cluster, select **Migrate Local Setting Only**. The installer adds the local data for this server from the embedded database to the existing database schema it created for the first server.

     Note Set the `Cluster.mode` server configuration parameter to **disabled** prior migrating from a Standard Cluster to an Enterprise Cluster. For more information on changing server configuration parameters, refer to *View and change server configuration parameters* on page 315.

9. Leave **Roll-back to MySQL Database on Error** selected.

10. Click **Next**.

11. On the *Summary* page, review your settings. Click **Back** to return to a previous page and change a setting. Click **Setup Now** to migrate the data from the embedded database to the Oracle database or create the Oracle database.

    SecureTransport reports it progress as it transfers the server configuration and data from the embedded database to the external Oracle database.

    When the data migration is complete, the embedded database is no longer available and the *Database Settings* page includes the external database settings under *Enterprise Clustering - Oracle External Database*.

    The log output for the migration is in `<FILEDRIVEHOME>/var/logs/migration.log`.

12. Once the data migration is completed, shutdown and restart the SecureTransport server instance.

Note You can also migrate configuration data using the `data_migrate` command-line utility in the `<FILEDRIVEHOME>/bin` directory. For usage information, run `data_migrate -h`. Before you migrate the data, stop all servers except the database.

Direct log data to separate Oracle databases

If SecureTransport Server uses an external Oracle database, you can direct transfer log (file tracking) data and server log data to different databases from the one used for the rest of the SecureTransport configuration and data.

You can direct the transfer log data and server log data to the same database or to different databases. When you change the database used to store log data, SecureTransport does not copy the data from its current location to the new location.

SecureTransport continues to operate when the external server log database is unavailable. SecureTransport directs the server log data to `<FILEDRIVEHOME>/var/logs/serverlog-fallback.log`. The *Server Log* page indicates that the log is unavailable and provides a link you can use to download the file.

1. Make sure the Oracle databases have the characteristics listed in the *Database installation prerequisites* topic of the *SecureTransport Installation Guide*. Depending on the log data you direct to a database, you must define the `ST_FILETRACKING` tablespace or the `ST_SERVERLOG` tablespace.
2. Select **Setup > Database Settings**.

   The *Database Setting* page is displayed with the external database settings under *Enterprise Clustering - Oracle External Database*.
3. Select **Show Advanced Settings**.

   The settings for the two additional databases are displayed.
4. Under *Enterprise Clustering - Oracle External Database - Transfer Log* and *Enterprise Clustering - Oracle External Database - Server Log*, type the values necessary to connect to the external databases. To continue to use the primary database, retain the default values.

   For description of the required values, see *Switch from the embedded database to an external Oracle database* on page 96.
5. For each database, click **Test Connection to Oracle Database**.

   If SecureTransport displays a failure message, correct the network, Oracle, or other error reported and try again.
6. Type the passwords again and click **Save**.

   The first time the new database is referenced, SecureTransport creates the tables for the log data. SecureTransport does not copy the log data from the previous database to the new database and does not display the log entries from the previous database in the *File Tracking* and *Server Log* pages.
7. Select **Operations > Server Control**.

8. On the *Server Control* page, stop and restart all the protocol servers and the TM Server.
9. Log out of the Administration Tool.
10. Log on to the SecureTransport server and stop and restart the Administration Tool service using the `stop_admin` and `start_admin` commands in `<FILEDRIVEHOME>/bin`.
11. In an Enterprise Cluster (EC), repeat steps 2 though 10 for all SecureTransport Servers.

Change the external Oracle database

If the SecureTransport Server uses an external Oracle database and any of the database settings change, you must change the corresponding settings in the Administration Tool.

1. Log on to the SecureTransport Administration Tool as user `dbsetup`.
2. Select **Setup > Database Settings**.

   The *Database Setting* page is displayed.
3. Type the values necessary to connect to the new external database.
   - **Host** – The host name or IP address of the Oracle server
   - **Port** – The port used to access the server, 1521 is the default
   - **User Name** – The name of the user authorized to create the SecureTransport schema and populate it
   - **Password** – The password for the user, not displayed
   - **Service Name** – Used to connect a server
   - **Use secure connection** – When **Use secure connection** is checked, the connection between SecureTransport and the database server will be encrypted. If **Use secure connection** is checked, the following options should be configured:
     - **Server Certificate DN** (optional) – If the server is successfully authenticated (meaning its certificate is trusted), its DN can be checked. If a value is entered in this field, it will be compared with the server certificate DN. If they do not match, the connection won't be successful.
     - **Enabled Protocols** – List of enabled protocols. TLSv1 is the default protocol.
     - **Enabled Cipher Suites** – List of the enabled cipher suites.

     Note Before secure connection is enabled, the issuers certificates of the database server certificate, should be imported in the Trusted CA certificates store.

     - **TrustStore File Path** – Browse and select the TrustStore file to import the trusted certificates.
   - **Use Custom JDBC URL** – Unchecked by default. When checked, you can specify a custom JDBC URL string for SecureTransport to use to connect to one or multiple Oracle databases. In the URL, you can specify an address list that lists the protocol, host, port, and service name of each database. In addition to the standard connection parameters, you can include additional properties to define specific behavior, for example, a connection via SSL. If the custom JDBC URL connects to your database using SSL, make

sure the **Use secure connection** checkbox is selected.

```
#Example
JDBC URL with two support databases using both placeholders and data
defined by the admin:

jdbc:oracle:thin:${user}/${password}@(DESCRIPTION=(ADDRESS_LIST=
(LOAD_BALANCE=OFF)(FAILOVER=ON)(ADDRESS=(PROTOCOL=TCP)(HOST=2.2.2.2)
(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=3.3.3.3)(PORT=1521)))
(CONNECT_DATA=(SERVICE_NAME=${databaseName})))
```

Note When specified, the custom JDBC configuration is kept on patch revert.

Note The option to specify a custom JDBC URL is also exposed as a REST API resource.

4. Click **Test Connection to Oracle Database**.

   If SecureTransport displays a failure message, correct the network, database, or other error reported and try again.

5. Click **Save**.

Note You can enable encryption of the communication between the SecureTransport Server and the Oracle database by adding `SQLNET.ENCRYPTION_SERVER=requested` to the `$ORACLE_HOME/network/admin/sqlnet.ora` file for your Oracle server. For more information, refer to the Oracle documentation.

Note You can get the existing Oracle database configuration, update it and test the connection to an Oracle database using the respective Admin REST API resource `/configurations/database/oracle`.

Improve server resiliency in case of Oracle RAC node failure

Note The following procedure will have some SecureTransport Server performance impact.

Adjust the SecureTransport connection pool settings per the following procedure.

1. Set the C3P0 connection pools configured in `<FILEDRIVEHOME>/conf/configuration.xml` (set for each component) as follows:

   `hibernate.c3p0.testConnectionOnCheckout=`**`true`**

   `hibernate.c3p0.preferredTestQuery=`**`select 1 from DUAL`**

2. The DBCP connection pool is used for Quartz scheduling component. Set the DBCP settings configured in `<FILEDRIVEHOME>/conf/scheduler.properties` as follows:

   `org.quartz.dataSource.DS.validationQuery=`**`select 1 from DUAL`**

   `org.quartz.dataSource.DS.testOnBorrow=`**`true`**

Note Please note that the name of dataSource can be different than DS, for example, if SecureTransport database was migrated from embedded MySQL to external Oracle, the name of dataSource will be DS2-migrate, and configuration options will be:
`org.quartz.dataSource.DS2-migration.validationQuery=`**`select 1 from DUAL`**
`org.quartz.dataSource.DS2-migration.testOnBorrow=`**`true`**

Change the external Microsoft SQL Server database

If the SecureTransport Server uses an external Microsoft SQL Server database and any of the database settings change, you must change the corresponding settings in the Administration Tool.

1. Log on to the SecureTransport Administration Tool as user `dbsetup`.
2. Select **Setup > Database Settings**.

   The *Database Setting* page is displayed with the external database settings under *Enterprise Clustering - Microsoft SQL Server External Database*.
3. Type the values necessary to connect to the new external database:
   - **Host** – The FQDN or IP address of the Microsoft SQL Server system
   - **Port** – The number of the port used to access the server, 1433 is the default
   - **User Name** – The name of the user authorized to connect to the database
   - **Password** – The password for the user, not displayed
   - **Database Name** – Used to connect to the Microsoft SQL Server.
   - **Use secure connection** – When **Use secure connection** is checked, the connection between SecureTransport and the database server will be encrypted. If **Use secure connection** is checked, the following option should be configured:
     - **Server Certificate CN** (optional) – If specified, SecureTransport will match the specified value with the database server certificate CN. If it is not specified, SecureTransport will match the host name with the database server certificate CN. If neither of them is matched, the connection will fail.
     - **TrustStore File Path** – Browse and select the TrustStore file to import the trusted certificates.
   - **Use Custom JDBC URL** – Unchecked by default. When checked, you can specify a custom connection string for SecureTransport to use to connect to a Microsoft SQL Server database. In the URL, specify the host, port, database name, user name and password or use the available placeholders. You can include additional connection properties to define specific behavior, for example, a connection via SSL. If the custom JDBC URL connects to your database using SSL, make sure the **Use secure connection** checkbox is selected.

The exact syntax of a JDBC URL is specified by your DBMS.

```
#Example
To specify an encrypted connection to mirror SQL instances by using
a username and password:
jdbc:sqlserver://${host}:${port};databaseName=${databaseName};user=${user};password=${password};encrypt=${encrypt};trustStore=${trustStorePath};trustStorePassword=${trustStorePassword};hostNameInCertificate=${hostNameInCertificate};failoverPartner=${failoverHost};
```

The option to specify a custom JDBC URL is also exposed as a REST API resource.

Note When specified, the custom JDBC configuration is kept on patch revert.

4. Click **Test Connection to SQL Server Database**.

   If SecureTransport displays a failure message, correct the network, database, or other error reported and try again.

5. Click **Save**.

Note You can retrieve and update an existing Microsoft SQL Server database configuration, and test the connection to the database using the respective Admin REST API resource: `/configurations/database/mssql`.

Register SecureTransport in Central Governance

The following topics provide the SecureTransport registration in Central Governance prerequisites, configuration, and troubleshooting:

- *SecureTransport registration in Central Governance prerequisites* on page 103
- *Central Governance configuration* on page 105
- *SecureTransport registration troubleshooting* on page 108

SecureTransport registration in Central Governance prerequisites

The following prerequisites must be completed prior to registering a SecureTransport Server instance in Central Governance:

1. Install the SecureTransport Server instance per the installation instructions in the *SecureTransport Installation Guide*.
2. Perform the initial setup and configuration of the SecureTransport Server instance per the instructions in the *SecureTransport Getting Started Guide*.

3. Create a master or delegated administrator per the instructions in *Add an administrator account* on page 647 or *Create a delegated administrator* on page 654.

   Settings for master administrator

Function	Setting
Administrator Name	stadmin
Password	(user specified)
Confirm Password	(user specified)
Administrative Role	Master Administrator

   Settings for delegated administrator

Function	Setting
Administrator Name	stadmin
Password	(user specified)
Confirm Password	(user specified)
Administrative Role	Delegated Administrator
Parent Administrator	/admin
Assigned Business Units	CentralGovernance (To create the CentralGovernance business unit, refer to *Create or edit a business unit* on page 693.)
Select what the delegated administrator will be allowed to do	For example: Create Users, Manage Administrators, Update Users, Manage Applications, Manager 'External Script' Step, and Manage Business Units

4. Enable certificate authentication for administrators per the instructions in *Administrator login options* on page 417.
   a. Using certificates issued by any trusted issuer:
      i. Select **Enable administrator login using client certificates** (requires admin server restart).
      ii. Select either **optional** or **required** in the *Client certificates* list.
      iii. Choose Accept certificates issued by **any trusted issuer** from the drop-down list.
      iv. Click **Save**.

5. Restart the admin service from **Operations > Server Control** page or using `<FILEDRIVEHOME>/bin/stop_admin` and `<FILEDRIVEHOME>/bin/start_admin` scripts.

Proceed to *Central Governance configuration* on page 105 to configure the SecureTransport Server instance integration with Central Governance.

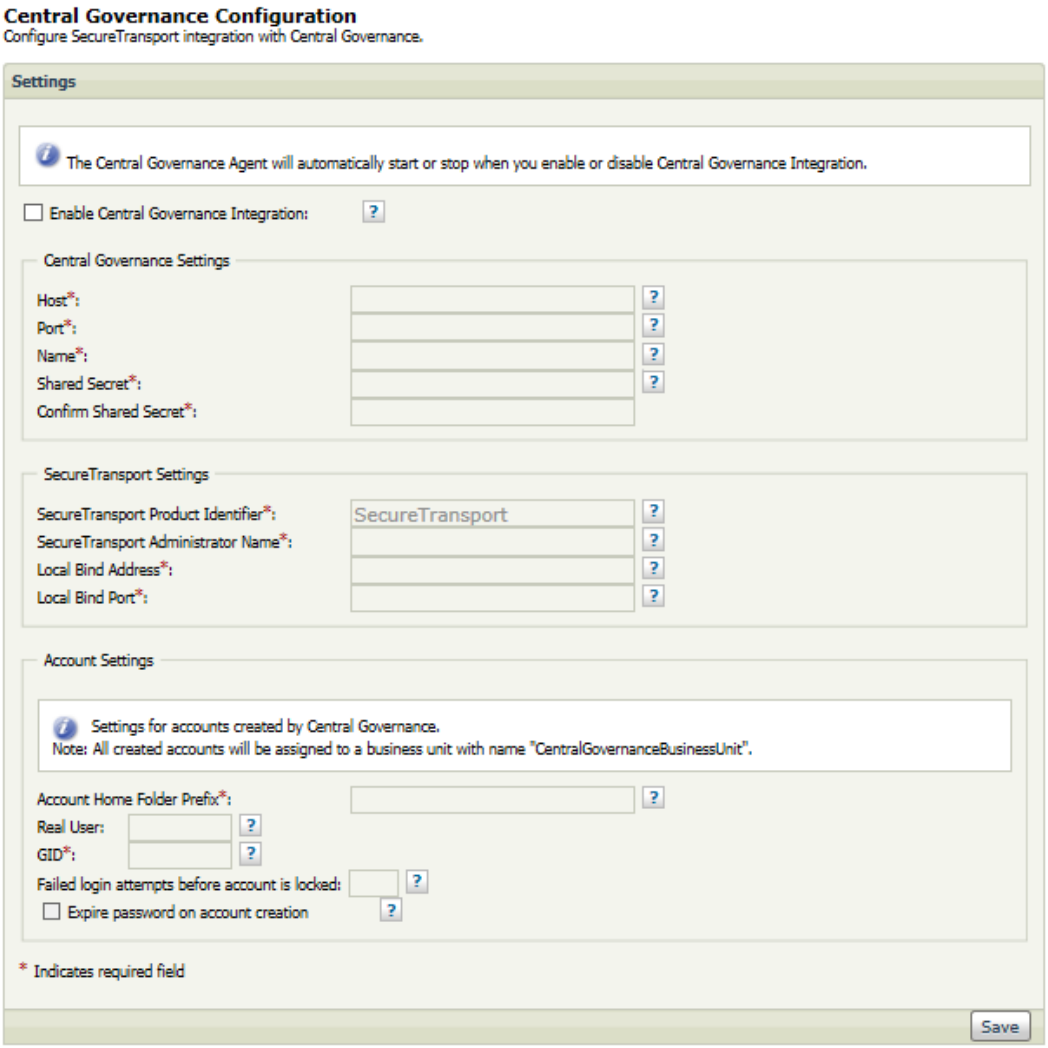
Central Governance configuration

The Central Governance integration can be configured from the SecureTransport Administrative interface. Prior to configuring the Central Governance integration, the SecureTransport administrator must know the Central Governance host, port, name, and the shared secret of the Central Governance instance to be integrated with the SecureTransport instance.

To configure SecureTransport integration with Central Governance:

1. Select **Setup > Central Governance**.

   The Central Governance Configuration page is displayed.



2. Select **Enable Central Governance Integration** check box.

   When performing registration to Central Governance, SecureTransport sends all its available server communication profiles. Each server communication profile represents the necessary information for communicating with SecureTransport over a specific network protocol and can be used by Central Governance when deploying flows.

   For example, an FTP server communication profile can consist the FQDN where the FTP daemon of the SecureTransport is running and the port on which it is listening (and a server certificate if this is a secured port).

   So if you want the SecureTransport to provide this information the protocol daemon must be running including Transaction Manager. The server communication profiles of the SecureTransport Edges are also collected.

   When registering SecureTransport clusters, only one node of the cluster should be registered. It automatically collects the server communication profiles from the other cluster nodes.

   The Central Governance Agent automatically starts or stops when you enable or disable Central Governance Integration by selecting or deselecting the **Enable Central Governance Integration** check box and click **Save**.

3. In the *Central Governance Settings* pane:

   a. Enter the **Host**.

      The fully qualified domain name (FQDN) or IP address of the computer where Central Governance is running. Central Governance and the SecureTransport Host both must use either FQDN or IP. Using IP on one side and FQDN on the other will not work.

   b. Enter the **Port**.

      Port on which Central Governance is running. This is the Central Governance agent port.

   c. Enter the **Name**.

      Agent name set while configuring Central Governance.

   d. Enter the **Shared Secret**.

      Shared secret set while configuring Central Governance.

   e. Confirm the **Shared Secret**.

4. In the *SecureTransport Settings* pane:

   a. Enter the **SecureTransport Product Identifier**.

      Unique and logical identification of the Product. The value of this option is reported to Central Governance during registration and uniquely identifies the SecureTransport instance or cluster in the product list. The value is also reported in the Location attribute of the all XFB Transfer Tracked Object Sentinel events.

   b. Enter the **SecureTransport Administrator Name**.

      Administrator account used by Central Governance to login to the Administrator's Tool. This is the administrator account used by the Central Governance when it deploys flows. It can be used for creation and modifying SecureTransport accounts, subscriptions, applications, and so forth.

   c. Enter the **Local Bind Address**.

The fully qualified domain name (FQDN) or the IP address through which the communication channel to Central Governance will be established (for example, 10.1.1.1). It is the IP address or FQDN of the machine where SecureTransport is installed.

d. Enter the **Local Bind Port**.

The local port through which the communication channel to Central Governance will be established (for example, 5701).

5. In the *Account Settings* pane:

a. Enter the **Account Home Folder Prefix**.

The absolute path to the base home folder for accounts created by Central Governance.

b. (Optional - Windows) Enter the **Real User**.

In case the account home folder prefix is on a shared network; specify a real user that has access to it.

Note The specified real user needs to added in a password vault file. For more information, refer to *Add a user to a password vault* on page 690.

c. (Mandatory - UNIX) Enter the **UID** (user identifies).

UID for accounts crated by Central Governance.

d. Enter the **GID** (group identifier).

GID for accounts created by Central Governance.

e. (Optional) Enter the **Failed login attempts before account is locked**.

Failed login attempts after which the account will be locked.

f. Determine **Expire password on account creation**.

If selected, all accounts created by Central Governance need to change their password on next login.

6. Click **Save**.

After a successful start up, the SecureTransport Server instance should be registered in Central Governance (listed under products) along with its communication profiles and certificates.

In case of an error:

- Check the Central Governance configuration page: host, port, certificate, and so forth.
- On the SecureTransport side, check the `<FDH>/central-governance/logs/uma.log.0` for error and warning messages.
- On the Central Governance side, check `<cg-installation>/runtime/com.axway.nodes.ume_<business_ID>/logs/opnode.log` for error and warning messages.

If the SecureTransport Server instance registers with errors, refer to *SecureTransport registration troubleshooting* on page 108.

SecureTransport registration troubleshooting

The following topics provide procedures to troubleshoot SecureTransport registration errors:

- *SecureTransport is registered with errors* on page 108
- *Product errors* on page 108
- *SecureTransport registration hangs* on page 109
- *SecureTransport registration limitations* on page 109

SecureTransport is registered with errors

Use the following procedure to troubleshoot SecureTransport registration with errors.

1. Check the following logs for warnings and errors:
    a. On the SecureTransport side:

    `<FDH>/central-governance/logs/uma.log.0`

    b. On the Central Governance side:

    `<cg-installation>/runtime/com.axway.nodes.ume_<business_ID>/logs/opnode.log`

    c. From the Central Governance User Interface:

    Administration > Services > Core Services

    Products > Products > Product List > [ProductName]
2. Remove the SecureTransport instance from Central Governance.
3. Disable the Central Governance integration using the SecureTransport Administrator Tool.
4. Restart the registration process.

Product errors

If there are product errors in **Products > Products > Product List > [ProductName]**, check the following:

- If the error is: `Registered in error since [TIME] [DATE] |Explanation: [CONFIGURATION CANNOT BE UPDATED ON THE COM.AXWAY.SECURETRANSPORT.NODE: ERROR SETTING CERTIFICATE DN OF THE ST ADMINISTRATOR USED FOR CG AUTHENTICATION.]`, check if there are duplicate administrator names on the SecureTransport *Accounts > Administrators* page and in the *Administrator Name* field on the *Setup > Central Governance* page .
- If the error is: `Registered in error since [TIME] [DATE] | Explanation: [Unauthorized access to SecureTransport Admin UI.,`

check if administrators are allowed to login to SecureTransport using client certificates. To check if administrators are allowing to login using certificates, navigate to the *Setup > Admin Settings* page and verify that **Enable administrator login using client certificates** is selected.

SecureTransport registration hangs

Sometimes the registration process stops right after the `createSecureTransport.umas`. If you encounter a registration hang, perform the following steps.

1. Stop the agent on the SecureTransport side.
2. Start the agent on the SecureTransport side.

SecureTransport registration limitations

Use one of the following configurations due to a Hazelcast limitation:

1. If Central Governance is configured to use FQDN, you should use the following SecureTransport configuration because of a Hazelcast limitation:

   SecureTransport Central Governance Configuration page:

   Host: <should use **only FQDN**>
2. If Central Governance is configured to use IP, you should use the following SecureTransport configuration because of a Hazelcast limitation:

   SecureTransportCentral Governance Configuration page:

   Host: <should use **only IP**>

Integrate Axway Sentinel

Axway Sentinel is a Business Activity Monitoring (BAM) product that collects, aggregates, correlates, and reports events from SecureTransport and other products, applications, and systems throughout your infrastructure. Sentinel is a separate product that you can buy from Axway or an authorized partner. Once you license and configure SecureTransport to send file transfer and processing events to Sentinel, data is collected and displayed on a dashboard.

For the Sentinel versions that SecureTransport 5.4 can send events to, see *Axway and third-party software support* on page 39.

Note When a SecureTransport Enterprise Cluster (EC) is configured to direct PGP encryption and decryption tasks to one server, Sentinel reporting for a transfer with a PGP task is not accurate because Sentinel cannot combine the processes of the transfer.

The following topics provide additional for the SecureTransport Axway Sentinel integration:

- Axway Sentinel *Event states* on page 110 - Describes the Axway Sentinel event states.
- *Axway Sentinel tracked objects* on page 112 - Lists the attributes of the Tracked Objects used to report Axway SecureTransport events to Axway Sentinel.

- *About XFB Transfer tracked objects* on page 117 - Describes the XFB transfer tracked objects.
- *PeSIT protocol* on page 117 - Describes the XFB tracked object attributes and provides monitoring errors, tracked-event processing, processing cycles, and tracked-event links.
- *List of PeSIT states* on page 120 - List the PeSIT protocol states.
- *XFB Tracked Object attributes* on page 123 - Provides the XFB tracked object roles, sender and receivers, production identification, and transfer attributes.
- *CycleId calculation* on page 146 - Describes the internal CycleId structure for PeSIT protocol transfers.
- *Axway Sentinel requests* on page 148 - Lists the Axway Sentinel requests.
- *Configure SecureTransport to send events to Axway Sentinel* on page 148 - Provides how-to instructions for configuring SecureTransport to send events to Axway Sentinel.

Event states

An *event state* specifies the current state of a file transfer. You choose the information SecureTransport sends to Sentinel by selecting the event states to report. For details, see *Configure SecureTransport to send events to Axway Sentinel* on page 148.

SecureTransport uses three pre-defined Sentinel Tracked Objects to report events:

- **XFBTransfer** – to report states that occur during file transfers.
- **XFB ST Info** – to report general additional info.
- **ST_VAS** (Value-Added Services) – to report states that occur during process other than file transfers.
- **Heartbeat** – to indicate to Sentinel that SecureTransport is running and connected.

Every event in the same group about one file transfer is identified using the same *cycle ID*. Sentinel uses the cycle ID to associate the event information in its display.

The following table describes the available event states:

Event state	Description
ACKED†	SecureTransport has sent an acknowledgment for a transfer.
AVAILABLE (ST_VAS)	SecureTransport application has completed successfully.
AVAILABLE (XFBTransfer)*†	SecureTransport has published a file in a target folder using Publish To Account step.
CANCELED*†	An application, agent, or user has canceled a file transfer.
DECRYPTED	SecureTransport has performed a successful PGP decryption.

Event state	Description
DECRYPTING	SecureTransport is starting to decrypt a file.
DELETED	A client, post-processing action (PPA), or post client download action has deleted a file.
ENCRYPTED	SecureTransport has performed a successful PGP encryption.
ENCRYPTING	SecureTransport is starting to encrypt a file.
ENDED_TO_ACK†	SecureTransport has received an acknowledgment for a transfer.
ERROR	An error has occurred during file deletion, renaming, transformation, or routing.
FAILED*†	An error has occurred during a file transfer, Advanced Routing execution, or while an agent was running.
FORWARDED	A routing application (such as Standard Router) has completed successfully.
FORWARDING	SecureTransport is starting a routing application (such as Standard Router).
INTERRUPTED†	A remote PeSIT server paused a transfer it initiated.
POST_PROC/ICAP_ DENIED	Access to the file is denied.
POST_PROC/ICAP_ SCANNED	The scanning of the file has successfully finished.
POST_PROC/ICAP_ SCANNING	The scanning of the file has started.
POST_ PROC/ROUTED†	An Advanced Routing application has successfully completed.
POST_ PROC/ROUTING†	SecureTransport is starting an Advanced Routing application.
PRESERVED	The original file was not deleted after an decryption or encryption.
RECEIVED*†	SecureTransport has successfully received a file by server-initiated pull or client-initiated push.
RECEIVING†	SecureTransport is starting to receive a file by server-initiated pull or client-initiated push.

Event state	Description
RENAMED	A client action, or a post-transmission action (PTA), or post-processing action has renamed a file.
ROUTED†	As the intermediate partner in a routed PeSIT transfer, SecureTransport has sent a file to the routing destination.
SENDING†	SecureTransport is starting to send a file by server-initiated push or client-initiated pull.
SENT*†	SecureTransport has successfully sent a file by server-initiated push or client-initiated pull.
SUBMITTED†	SecureTransport has sent a wild card pattern for a server-initiated pull.
TO_EXECUTE†	SecureTransport is ready to start a server-initiated transfer.

* Event state that is always monitored by Sentinel.

† Event state reported using the XFBTransfer Tracked Object and selected by default to be sent to Sentinel. The other event states are reported using ST_VAS.

The following event states are *in-process* states: DECRYPTING, ENCRYPTING, FORWARDING, POST_PROC/ICAP_SCANNING, POST_PROC/ROUTING, RECEIVING, SENDING, and TO_EXECUTE. All other event states are *processed* states that report the successful or unsuccessful completion of processing.

Note Added data transformations and other SecureTransport customizations can add additional event states to be sent to Sentinel.

Axway Sentinel tracked objects

The tables in this topic list the attributes of the Tracked Objects used to report Axway SecureTransport events to Axway Sentinel. All the Tracked Objects have the same standard attributes. Each Tracked Object also has attributes specific to it.

The standard attributes are:

Name	Format	Description
CYCLEID	string	For XFBTransfer and ST_VAS: ID used to relate events about the same transfer For Heartbeat: ID used to identify the SecureTransport Server
EVENTDATE	date	Date (generated by Sentinel)
EVENTID	integer	Unique ID for the event (generated by Sentinel, not in Heartbeat)

Name	Format	Description
EVENTTIME	time	Timestamp (generated by Sentinel)
GMTDIFF	integer	Time zone (generated by Sentinel)
ISALERT	bool	1 means permanent error or last entry (not in Heartbeat)
ISEND	integer	1 or 2 means End (not in Heartbeat)
ISEXCEPTION	bool	1 means temporary failure (not in Heartbeat)
OBJECTID	string	Object ID (generated by Sentinel, not in Heartbeat)
PRODUCTIPADDR	string	IP address of the SecureTransport host
PRODUCTNAME	string	SecureTransport
PRODUCTOS	string	Operating system of Axway SecureTransport host (generated by Sentinel)
RETURNCODE	integer	Event exit code (not in Heartbeat)
RETURNMESSAGE	string	Error message (not in Heartbeat)
STATE	string	State reported by event (not in Heartbeat)

The attributes specific to XFBTransfer are:

Name	Format	Description
APPLICATION	string	Name of the application the SecureTransport uses
COREID	string	File identifier reported with every state
CREATIONDATE	date	Date of last file modification
CREATIONTIME	time	Timestamp of last file modification
DIRECTION	string	R for receive, S for send
ENDDATE	date	Date of end of transfer
ENDTIME	time	Timestamp for end of transfer
EVENTTIMESTAMP	time	Timestamp of the current event reported with every state

Name	Format	Description
FILENAME	string	Path and name of transferred file
FILESIZE	integer	Size in bytes of transferred file
FILETYPE	string	File type
FINALRECEIVERID	string	Name of the final receiver of the transfer
GROUPNAME	string	Axway SecureTransport account business unit
IDAPPL	string	The ID of the route template package that is executed
INTERNALCYCLEID	string	Long cycle ID
ISSERVER	string	1 means Server
ISSSL	string	1 means SSL
LOCALID	string	Randomly-generated ID
LOCATION	string	SecureTransport by default. Its value is controlled by the server configuration option: `AxwaySentinel.Attributes.Attribute.value.Location`
MACHINE	string	ST-*OS* where *OS* is the operating system of the SecureTransport Server
MONITOR	string	Name of remote agent or machine monitored
MONITORVERSION	string	Axway SecureTransport version from `<FILEDRIVEHOME>/conf/version.txt`
ORIGINALSENDERID	string	Name of the original sender of the transfer
PROTOCOL	string	Exact protocol
PROTOCOLFILENAME	string	File name only
RECEIVERID	string	Name of the receiving partner
RETRYMAXNUMBER	integer	Maximum retries attempted
RETRYNUMBER	integer	Current retry count
SENDDATE	date	Date of start of transfer

Name	Format	Description
SENDERID	string	Name of the sending partner
SENDTIME	time	Timestamp for start of transfer
STARTDATE	date	Start date of transfer
STARTTIME	time	Start time of transfer
TRANSMITTEDBYTES	integer	Actual number of bytes transferred
USERID	string	Axway SecureTransport Login Name/Account Name or account name of the account the triggered the Advanced Routing feature
USERPARAMETER1	string	Account type: E for Partner, I for Internal, N for Unspecified
USERPARAMETER2	string	Indicates whether the transfer is originated by a user account, a service account, or a site
USERSTATE	string	User state to track pre- or post-transfer processing such as DENIED, SCANNED, SCANNING, and so forth
VIRTUALDIRNAME	string	Name of the virtual directory used in the transfer or name of the sandbox folder used by route template package
ENVIRONMENTID	integer	As defined in the Server Configuration
PARENTCYCLEID	integer	ID of the parent processing cycle. It is reported with the following states: TO_EXECUTE, SENDING, SENT.

The attributes specific to ST_VAS are:

Name	Format	Description
ACTIVITYDURATION	integer	Duration of activity in milliseconds
ACTIVITYNAME	string	Name of activity reporting the event
DIRECTION	string	R for receive, S for send
DIRECTORYNAME	string	Directory name
FILENAME	string	Path and name of the transferred file
FILESIZE	integer	Size in bytes of transferred file

Name	Format	Description
ORIGINALFILENAME	string	File name before the action of the activity
USERID	string	Axway SecureTransport Login Name/Account Name

The attributes specific to XFBSTINFO are:

Name	Format	Description
ACTIVEACCOUNTS	integer	Number of active accounts in SecureTransport: current value is taken from the existing list in *Accounts > Active Users* in SecureTransport
COMPANYNAME	string	Company name as defined in the license
ENVIRONMENTNAME	string	Environment name as defined in the `StatisticsSummaryReport.EnvironmentName` configuration option
ENVIRONMENTID	integer	Environment ID as defined in the `StatisticsSummaryReport.EnvironmentId` configuration option
PRODUCTLINE	string	MFT
PRODUCTNAME	integer	SecureTransport
PRODUCTVERSION	string	Current base product version
CURRENTPATCH	string	Version number of currently installed patch
ISECENABLED	bool	A flag identifying if Enterprise Clustering is enabled
ISFMENABLED	bool	A flag identifying if Flow Management integration is enabled
ISADIENABLED	bool	A flag identifying if Axway Decision Insight (Sentinel) integration is enabled
PLUGINS	string	A list of installed plugins along with their versions

The attribute specific to Heartbeat is:

Name	Format	Description
DELAY	integer	Heartbeat interval set on the *Axway Sentinel Events* page

About XFB Transfer tracked objects

A XFB Transfer Tracked Object (TO) is the Sentinel structure used to store transfer related events coming from the following Axway products: Transfer CFT, Gateway, Gateway Interchange, SecureTransport, and InterPel.

For each step of each SecureTransport file transfer process, SecureTransport generates a Tracked Object (TO) instance and sends this to Sentinel. In each TO instance, the State attribute identifies the relevant step of the transfer process.

Each file transfer has a unique identifier that consists of a set of parameters that are exchanged at the beginning of the transfer, or parameters that make the transfer unique in the product. A computation of these parameters creates a unique Sentinel identifier called a CycleID. Linking these CycleIDs together can provide end-to-end monitoring when using a store and forward, or when the Sentinel Universal Agent (UA) is used in an implementation to integrate application processing.

Each transfer passes through different States during its execution, so Sentinel receives an event each time the State changes. A UserState is also available to track pre or post transfer processing. These UserState values vary depending on the operation performed.

The attributes contained in a tracked object fall into one of two categories:

- System attributes that are common to most tracked objects. System attributes identify application and platform events and errors.
- User attributes that are not common to all tracked objects. User attributes describe the application- or platform-specific properties of monitored events.

PeSIT protocol

This topic describes the XFB tracked object attributes and provides monitoring errors, tracked-event processing, processing cycles, and tracked-event links.

XFB_TO system attributes

The XFB tracked objects are monitored and the errors, tracked-event processing, processing cycles, and tracked-event links are passed to Sentinel.

The following topics list errors, tracked-event processing, processing cycles, and tracked-event links are passed to Sentinel:

- *Monitoring errors* on page 118
- *Monitoring tracked-event messages* on page 119
- *Monitoring processing cycles* on page 120
- *Monitoring tracked-event links* on page 120

Monitoring errors

Sentinel attribute	Data type	Length	Description	Name in SecureTransport
IsException	Integer	1	Indicates a temporary error. Values: • **0**: The relevant Tracked-Event Message does not describe an exception. • **1**: The relevant Tracked-Event Message describes one or more exceptions.	IsException
IsAlert	Integer	1	Indicates a permanent (unrecoverable) error. Values: • **0**: No alert is associated with the relevant Tracked-Event Message. • **1**: The relevant Tracked-Event Message is associated with a processing exception that generated an alert.	IsAlert
ReturnCode	String	20	Processing details that the relevant tracked application generated. When the value of *IsAlert* is 1, this attribute often contains an error code. The error code corresponds to the exit code of the event.	ReturnCode

Sentinel attribute	Data type	Length	Description	Name in SecureTransport
ReturnMessage	String	250	Processing details that the relevant tracked application generated. In case of successful transfers this message is empty.	Stores the details for the transfer error. Corresponds to DXAGENT_ EXECUTION_ERROR_ MESSAGE.

Monitoring tracked-event messages

Sentinel attribute	Data type	Length	Description	Name in SecureTransport
GMTDiff	Integer		Positive or negative difference between the Greenwich Mean Time (GMT) and the local time expressed in minutes.	GMTDiff
ProductName	String	50	The constant SecureTransport.	Reports the name of the product.
ProductIPAddr	String	255	IP address of the product/application that generated the relevant Tracked Event.	Reports the host name assigned to the system.
ProductOS	String	20	Operating system of the application that generated the relevant Tracked Event.	Java os.name system property.
State	String	29	Status of the relevant Tracked Event. The possible values of this attribute depend on the tracked application/product and file transfer protocol used. See List of PeSIT states.	State

Monitoring processing cycles

Sentinel attribute	Data type	Length	Description	Name in SecureTransport
CycleId	String	250	CycleId of the relevant Tracked Event.	CycleId
IsEnd	Integer	1	Values: • **0**: The relevant Processing Cycle is not complete. • **1**: The relevant Processing Cycle is complete.	IsEnd

Monitoring tracked-event links

Sentinel attribute	Data type	Length	Description	Name in SecureTransport
UserParentID	String	250	Unique string that identifies the parent of the relevant Tracked Event	Not used
UserObjectId	String	250	Unique string that identifies the relevant Tracked Event.	Not used
UserChildId	String	250	Unique string that identifies a child of the relevant Tracked Event	Not used

List of PeSIT states

This topic describes the roles and states for PeSIT protocol transfers.

The following topics lists the PeSIT states:

- *Roles of transfer partners* on page 121
- *Server/Sender transfer states* on page 121
- *Server/Receiver transfer states* on page 121
- *Requester/Receiver transfer states* on page 122
- *Requester/Sender transfer states* on page 122

Roles of transfer partners

Although each transfer occurs between only two transfer partners, each transfer partner plays two roles:

- **Sender** or **Receiver** (the file is sent or received)
- **Requester** or **Server** (the transfer request is sent or received)

For a given transfer, only the following combinations of partner roles are possible:

- **Sender/Requester** and **Receiver/Server** (The partner that sent the file requested the transfer).
- **Receiver/Requester** and **Sender/Server** (The partner that received the file requested the transfer).

Server/Sender transfer states

SecureTransport acts as a protocol server.

SecureTransport sends a file.

Server/Sender corresponds to a CIT Download in SecureTransport terminology.

State	Description
SENDING	SecureTransport is sending a file.
SENT	SecureTransport has sent a file.
ENDED_TO_ACK	Indicates that SecureTransport has received an acknowledgment for the file transfer.
CANCELED	File transfer has been canceled by the client.
INTERRUPTED	The file transfer has been locally suspended.
SUSPENDED	The file transfer has been remotely suspended.

Server/Receiver transfer states

SecureTransport acts as a protocol server.

SecureTransport is receiving a file.

Server/Receiver corresponds to a CIT Upload in SecureTransport terminology.

State	Description
RECEIVING	SecureTransport is receiving a file.
RECEIVED	SecureTransport has received a file.
POST_PPROC	Post processing in progress.
ACKED	Indicates that SecureTransport has acknowledged the transfer to the partner.
CANCELED	File transfer has been canceled by the client.
INTERRUPTED	The file transfer has been locally suspended.
SUSPENDED	The file transfer has been remotely suspended.
ROUTED	File transfer has been successfully routed (only on the relay site in store and forward mode).

Requester/Receiver transfer states

SecureTransport acts as a protocol client.

SecureTransport is receiving a file.

This corresponds to SIT Pull in SecureTransport terminology.

State	Description
TO_EXECUTE	SecureTransport is about to execute a scheduled job.
RECEIVING	SecureTransport is receiving a file.
RECEIVED	SecureTransport has received a file.
ACKED	Indicates that SecureTransport has acknowledged the transfer to the partner.
INTERRUPTED	The file transfer has been locally suspended.
SUSPENDED	The file transfer has been remotely suspended.
POST_PROC	Post processing in progress.

Requester/Sender transfer states

SecureTransport acts as a protocol client.

SecureTransport is sending a file.

This corresponds to SIT Push in SecureTransport terminology.

State	Description
TO_EXECUTE	SecureTransport is about to execute a scheduled job.
SENDING	SecureTransport is sending a file.
SENT	SecureTransport has sent a file.
ENDED_TO_ACK	Indicates that SecureTransport has received an acknowledgment for the file transfer.
CANCELED	File transfer has been canceled by the client.
INTERRUPTED	The file transfer has been locally suspended.
SUSPENDED	The file transfer has been remotely suspended.
POST_PROC	Post processing in progress.
ROUTED	File transfer has been successfully routed (only on the relay site in store and forward mode).

XFB Tracked Object attributes

This topic provides the XFB tracked object roles, sender and receivers, production identification, and transfer attributes.

Note Depending on the type of transfer some Sentinel attributes may not be reported in SENDING or RECEIVING state, but are correspondingly available for SENT or RECEIVED.

The following topics list the XFB tracked object roles, sender and receivers, production identification, and transfer attributes:

- *Tracked object roles* on page 124
- *Tracked object sender and receivers* on page 125
- *Tracked object product identification* on page 130
- *Tracked object transfer users* on page 131
- *Tracked object transfer identification* on page 131
- *Tracked object transfer dates and times* on page 135
- *Tracked object transfer protocols* on page 137
- *Tracked object transfer options* on page 139
- *Tracked object transfer size* on page 142

- *Tracked object transfer structure and content* on page 143
- *Tracked object other attributes* on page 145

Tracked object roles

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`Direction` *integer*	1	One of the following: • **S**: The file is sent (Sender). • **R**: The file is received (Receiver).	All	Direction Corresponds to the DXAGENT_TRANSFER_DIRECTION SecureTransport event environment variable.
`IsServer` *integer*	1	One of the following: • **1**: The Sender or the Receiver acts as a Server. • **0**: The Sender or the Receiver is a Requester.	All	Action By

Tracked object sender and receivers

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`ReceiverId` *string*	80	Receiver Login Name	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	For PeSIT transfers, corresponds to PeSIT PI4. • In case of SecureTransport receiving a file from CFT, the PI4 value is the login name of the SecureTransport account that receives the file. • In case of SecureTransport uploading a file to a CFT partner, the PI4 value corresponds to the transfer site name that identifies the partner. For non-PeSIT transfers, the value of this attribute is the `ip:port` of the remote partner, the hostname, or the SecureTransport login name. For ADHOC transfers: • In case of an incoming ADHOC transfer, the value of this attribute is the account email. • In case of an outgoing ADHOC transfer, the value of this attribute is the recipient email.

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`SenderId` *string*	80	Sender Login Name	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	For PeSIT transfers, corresponds to PeSIT PI3. • In case of SecureTransport receiving a file from CFT, the PI3 parameter value is the name of the transfer site that identifies the partner. • In case of SecureTransport uploading a file to a CFT partner, the PI3 parameter value corresponds to the SecureTransport account name that's doing the transfer. For non-PeSIT transfers, reports the SecureTransport login name of the transfer site owner, the hostname, or the `ip:port` of the remote partner where SecureTransport pulled the file from. For ADHOC transfers: • In case of an incoming ADHOC transfer, the value of this attribute is the email of the sender. • In case of an outgoing ADHOC transfer, the value

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
				of this attribute is the account email.
`FinalReceiverId` *string*	80	The Login Name of the final Receiver in case of Store and Forward	All	For PeSIT transfers, corresponds to PeSIT PI62 or PI4. • If PI62 is not present, PI4 is used in both Sentinel and PeSIT. • In case of SecureTransport initiating a new Store and Forward transfer, the PI62 value corresponds either to the Final Destination property of the PeSIT transfer site or to the Final Destination property of the Send To Partner step. If both properties are left blank, PI62 is not populated. • In the PRESERVE store and forward mode, PI preserves the PI62 value. For non-PeSIT transfers, the value of this attribute is the ReceiverId. In case the ReceiverId value is not present, the value of the FinalReceiverId is the `ip:port` of the Remote Partner or the hostname.

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`OriginalSenderId` *string*	80	The Login Name of the original Sender in case of Store and Forward	All	For PeSIT transfers, corresponds to PeSIT PI61. • In case of SecureTransport initiating a new Store and Forward transfer, the PI61 value corresponds either to the Originator property, specified in the PeSIT transfer site settings, or the Originator property in the Send To Partner step settings. If both properties are left blank, PI61 is not populated. • In the PRESERVE store and forward mode, PI preserves the PI61 value. For non-PeSIT transfers, the value of this attribute is the login name of the SecureTransport account which received/sent the file from a Remote Partner. If login name is not present, the value is SenderID or UserID.

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`UserID` *string*	80	Transfer site owner	All	For non-PeSIT transfers, reports the transfer site owner. If no transfer site is used, reports the account name of the user who initiated the transfer. When an account template is used, the login name is reported. If no values are present for the account name and the transfer site, **N3** is reported.
`Site` *string*	80	Transfer site name	All	For non-PeSIT transfers, reports the transfer site name. If no value is present for the transfer site name, **N2** is reported.

Tracked object product identification

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`MonitorVersion` *string*	25	Version of SecureTransport in the X.Y.Z format e.g. 5.3.0 or 5.2.1	All	MonitorVersion
`ProductName` *string*	50	The constant "SecureTransport"	All	ProductName
`ProductIPAddr` *string*	255	IP address assigned to the server hosting the SecureTransport application	All	java.net.InetAddress. getLocalHost()

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`ProductOS` *string*	20	Operating system name as returned by os.name Java system property	All	os.name Java system property.
`EnvironmentID` *integer*		Environment ID as defined in Server Config	All	EnvironmentID

Tracked object transfer users

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`GroupId` *string*	80	The name of the SecureTransport account	All	Account name

Tracked object transfer identification

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`Application` *string*	80	Application name.	All	SecureTransport application name.
`CoreId` *string*	100	File identifier. Preserved during all types of processing.	All	Corresponds to `DXAGENT_CORE_ID` environment variable
`EventTimeStamp` *string*	100	Event time stamp.	All	

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`FileName` *string*	512	If the value of the CommandType attribute is: • File and the value of the Direction attribute is **E** (Sender), this attribute identifies the file from which the Sender retrieved the transfer data (full path). • File and the value of the Direction attribute is **R** (Receiver), this attribute identifies the file in which the Receiver recorded the transfer data (full path).	All	Fullpath of the filename. Corresponds to the DXAGENT_ FULLTARGET SecureTransport event environment variable.
`FlowName` *string*	100	Parameter to define a flow name in Central Governance for monitoring purposes.	All	FlowName
`LocalId` *string*	36	Stores the file tracking transfer ID.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Transfer ID. Corresponds to the TRANSFER_ STATUS_ID SecureTransport event environment variable.

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`ProtocolFile Name` *string*	512	Corresponds to the PeSIT PI12. Reports the new name of a file that has been renamed using the "Send File As" functionality of an internal or pluggable transfer site.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	File. Corresponds to the DXAGENT_ TARGET SecureTransport event environment variable.
`ProtocolFile Label` *string*	80	Corresponds to the PeSIT PI37 – file label. Reports the remote file path and the new name of a file that has been renamed using the "Send File As" functionality.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	When SecureTransport is a sender, this is configured in the Transfer Profile. When SecureTransport is a receiver, this value is configured and supplied by the sender.
`ProtocolId` *string*	80	Corresponds to the PeSIT PI13 – Transfer ID.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Transfer ID

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`Protocol Message` *string*	4000	If the value of the CommandType attribute is: • **A**: the value of this attribute is the content of the message sent as part of the acknowledgment. • **F**: this attribute is empty.	ACKED ENDED_TO_ACK	Corresponds to the DXAGENT_ TRANSFER_ACK_ MESSAGE SecureTransport event environment variable.
`Protocol Parameter` *string*	512	Corresponds to PI99. (ServiceParam or User message); For FTP server-initiated transfers, reports the upload command used in the FTP transfer site.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	User message Upload command in FTP transfer sites
`User Parameter1` *string*	255	Contains information whether the transfer is with an Internal partner, External partner or Unknown. • For transfer with an Internal partner **I** is reported. • For transfer with an External partner **E** is reported. • If the Administrator has not specified Internal or External – **N** is reported.	All	TransferType in account or site name.

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`User Parameter2` *string*	255	Reports the account type: • **User** (meaning that account has been specified in SecureTransport's database). • **Template** (meaning that this is a template). • **Service** (Service account).	All	Account Type
`ParentCycleID` *integer*		ID of the parent processing cycle.	TO_EXECUTE, SENDING, SENT	ParentCycleID

Tracked object transfer dates and times

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`StartDate` *date*		If the value of the State attribute is: • **SENT**, the value of this attribute is the date on which the Sender began sending the transfer. • **RECEIVED**, the value of this attribute is the date on which the Receiver began receiving the transfer. These dates are expressed in dd.mm.yyyy format.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`StartTime` *time*		If the value of the State attribute is: • **SENT**, the value of this attribute is the local time at which the Sender began sending the transfer. • **RECEIVED**, the value of this attribute is the local time at which the Receiver began receiving the transfer. These times are expressed in hh:mn:ss format.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	
`EndDate` *date*		If the value of the State attribute is: • **SENT**, the value of this attribute is the date on which the Sender stopped sending the transfer. • **RECEIVED**, the value of this attribute is the date on which the Receiver stopped receiving the transfer. These dates are expressed in dd.mm.yyyy format.	SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`EndTime` *time*		If the value of the State attribute is: • **SENT**, the value of this attribute is the local time at which the Sender stopped sending the transfer. • **RECEIVED**, the value of this attribute is the local time at which the Receiver stopped receiving the transfer. These times are expressed in hh:mn:ss format.	SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	
`Transmission Duration` *integer*		Transfer duration (expressed in seconds).	SENT RECEIVED INTERRUPTED SUSPENDED ACKED ENDED_TO_ACK ROUTED	Duration

Tracked object transfer protocols

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`Protocol` *string*	25	The following: • **PSIT_HS_E**	All	Protocol. Corresponds to the DXAGENT_PROTOCOL SecureTransport event environment variable.

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`IsSSL` *string*	1	One of the following: • **1**: SSL/TLS used for the transfer. • **0**: SSL/TLS not used for the transfer.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Use TLS/SSL in transfer site.
`SSLAuth` *string*	1	One of the following: • **S**: The Server sent X.509 certificates to the Requester. For SSH sessions, the value of SSLAuth will be always **S** if the Requester does not present a key. • **B**: Both the Server and the Requester sent X.509 certificates to each other. • **N**: Neither the Server nor the Requester sent X.509 certificates.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	DXAGENT_ SSLAUTH
`SSLCypher` *integer*		One of the following: • the **RFC code** of the cipher suite that the Server and the Requester used during the SSL/TLS session. The cipher suite identifies the authentication method, the encryption algorithm, and the hash algorithm for MAC calculation. • **0** for all SSH sessions.	All	DXAGENT_ SESSION_SSL_ CYPHER

Tracked object transfer options

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`Compression` *string*	1	One of the following: • **0**: Undefined • **1**: Horizontal • **2**: Vertical • **3**: Both horizontal and vertical • **4**: Not compressed Corresponds to PI21.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Compression in transfer site.
`RetryMax Number` *integer*		Maximum number of times that the Sender can attempt to send transfers.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	`EventQueue. maxRetry Count` on *Server Configuration* page.
`Retry Number` *integer*		Number of times that the Sender attempted to send the transfer. Each time the Sender established a connection with the Receiver, the Sender counted one attempt.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Corresponds to the DXAGENT_ PERSISTED_ EVENT_RETRY_ COUNT SecureTransport event environment variable.

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`Request Type` *string*	1	One of the following: • **S**: The Sender sent a single transfer to a single Receiver. This corresponds to a normal file transfer. • **F**: The Sender sent a group of transfers to a single Receiver. For each transfer in the group, the product generated one Processing Cycle. This corresponds to multiselect PeSIT option. • **D**: The Sender sent a single transfer to a group of Receivers (diffusion). For each Receiver in the group, the product generated one Processing Cycle. This corresponds to send to multiple transfer sites SecureTransport configuration.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	SecureTransport always reports as value for RequestType.

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`Transfer Type` *string*	1	One of the following: • **S**: The Sender sent a single transfer to a single Receiver. This corresponds to a normal file transfer. • **F**: The transfer belongs to a group of transfers that the Sender sent to a single Receiver. For each transfer in the group, the product generated one Processing Cycle. This corresponds to multiselect PeSIT option. • **D**: The Receiver belongs to a group of Receivers to whom the Sender sent the transfer (diffusion). For each Receiver in the group, the product generated one Processing Cycle. This corresponds to send to multiple transfer sites SecureTransport configuration.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	SecureTransport always reports as value for RequestType

Tracked object transfer size

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`FileSize` *integer*		An estimation of the file size given at the beginning of the transfer and updated upon completion of the transfer with the real value checked by ST using the file system. Corresponds to PI42.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	
`TransmittedBytes` *integer*		Number of bytes transferred, after decompression, to transfer the file. This size is expressed in bytes. Corresponds to PI27. **Note**: For PeSIT, this value sent is crosschecked by both the sender and receiver.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Corresponds to the DXAGENT_ TRANSFERRED_ BYTES SecureTransport event environment variable.

Tracked object transfer structure and content

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`CommandType` *string*	1	One of the following: • **F**: File transfer • **A**: Acknowledgment	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	
`FileType` *string*	60	One of the following: • **B**: the transferred file is a Binary file. • **T**: the transferred file is a Text file.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Transfer Mode in Transfer Profile or Data Encoding in Send To Partner step.
`RecordNumber` *integer*		Number of record in the file. This size is expressed in bytes. **Note**: For PeSIT, this value sent is crosschecked by both the sender and receiver. Corresponds to PeSIT PI28.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`RecordFormat` *string*	64	One of the following: • **F**: **fixed**: The transferred data contains fixed-length records. • **V**: **variable**: The transferred data contains variable-length records. Corresponds to PeSIT PI31.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Record Format in Transfer Profile or in Send To Partner step.
`RecordSize` *integer*		One of the following: • If the value of RecordFormat attribute is **fixed**, the value of this attribute is the size of all records in the transferred file, expressed in bytes. • If the value of RecordFormat is **variable** or **undefined**, the value of this attribute is the size of the largest record in the transferred file, expressed in bytes. Corresponds to PeSIT PI32.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Record Length in Transfer Profile or in Send To Partner step.
`Transcoding` *integer*		Character code of the transferred data: • **A**: ASCII • **B**: Binary • **E**: EBCDIC From PI16.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	Transfer Mode in Transfer Profile or Data Encoding in Send To Partner step.

Tracked object other attributes

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`VirtualDirName` *string*	255	The current folder relative to the home folder.	All	DXAGENT_ TARGET_PATH
`GroupName` *string*	80	Business Unit name	All	DXAGENT_ BUSINESS_UNIT_ NAME
`SessionTag` *string*	50	Represents SecureTransport session ID. The Session ID could be used to query the server log for a particular session.	All	Session ID
`TransferTag` *string*	50	Represents SecureTransport transfer status operationIndex. Transfer ID could be used to query the file tracking log for a particular transfer	All	
`RemoteAddr` *string*	255	Partner remote address (IPv4 and IPv6).	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED ROUTED	

Sentinel attribute	Length	Description	Applicable states	Name in Secure Transport
`RemoteSAP` *integer*		Partner remote port number.	SENDING RECEIVING SENT RECEIVED ACKED ENDED_TO_ACK INTERRUPTED SUSPENDED	Not reported by SecureTransport.

CycleId calculation

This topic describes the internal CycleId structure for PeSIT and SFTP protocol transfers.

Internal CycleId structure with PeSIT

The internal CycleId is an XFB Transfer Tracked Object attribute. This field has the following structure for PeSIT transfers:

Offset	Length	PI/Value	Description
1	4	"SUIV"	Eye catcher
5	24	PI3 CONNECT	For Transmission
		PI4 CONNECT	For Reception
29	24	PI4 CONNECT	For Transmission
		PI3 CONNECT	For Reception
53	5	"0 "	For File Transfer
		"65535"	For Message Transfer
		"REPLY"	For Acknowledgment
58	76	PI12	Logical file name

Offset	Length	PI/Value	Description
134	8	PI13	Transfer ID
142	12	PI51	Only the date is used (YYMMDD), and the time is filled with 6 spaces.
154	1	E	For Transmission
		R	For Reception

Internal CycleId structure with SFTP

The internal CycleId is an XFB Transfer Tracked Object attribute. This field has the following structure for SFTP transfers:

Offset	Length	PI/Value	Comments
1	4	SUIV TEMP	Eye catcher
5	24	Sender identifier	Sender account login na me SEND: System login of the process that runs the SFTP client RECV: SFTP login name sends by the client to connect to the SFTP server
29	24	Receiver identifier	Receiver login name SEND: SFTP login name sends by the client to connect to the SFTP server RECV: System login of the process that runs the SFTP client
53	5	"0"	For File Transfer
58	76	Virtual Filename	Logical file name, NIDF for CFT
134	8	Sequence number	Unique number identifying the transfer sent, NIDT for CFT
142	12	Date YYMMDD /padded to 12 with spaces on the right/	Only the date is used (YYMMDD), and the time is filled with 6 spaces
154	1	E	For Transmission
		R	For Reception

Generating common CycleID for end-to-end tracking of SFTP transfers

With transfers occurring across Axway's MFT solutions SecureTransport and Transfer CFT, the CycleID is used for consistent end-to-end reporting to Sentinel. In order to report the common CycleID, you must set the dedicated configuration option: `Ssh.AxwayVendorExtensions.enabled` to `true`. In order to apply this change, you must restart the SSH services and the Transaction Manager (TM) on all Server and Edge instances.

Note When this option is enabled, in the case when SecureTransport acts as client and transfer CFT acts as server, make sure to name each of your transfer sites to exactly match the corresponding NIDF name in Transfer CFT. Also, for correct SFTP end-to-end reporting with CFT, make sure to use only capital letters for each SecureTransport user's Account name (Login name).

Axway Sentinel requests

SecureTransport provides three requests you can use to display events and cycle links:

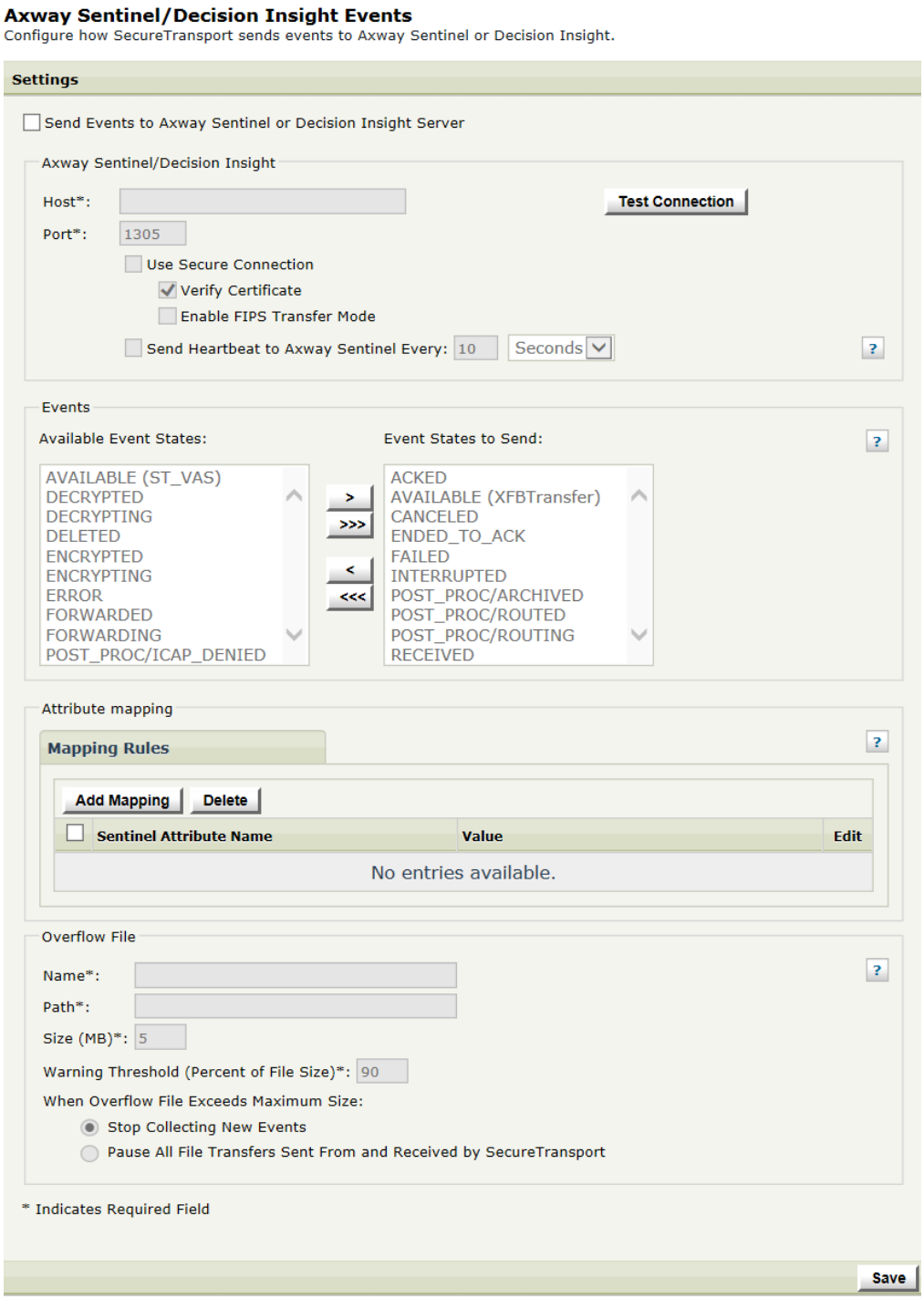
- `CurrentAlerts` displays all `ST_VAS` and `XBFTransfer` alerts (events with `IsAlert=1`).
- `CurrentDayTransfersAndVAS` displays all `ST_VAS` and `XBFTransfer` events for the current day.
- `TransfersAndVAS` displays all `ST_VAS` and `XBFTransfer` events.

Configure SecureTransport to send events to Axway Sentinel

Use the SecureTransport Administration Tool to configure SecureTransport to send events to Sentinel.

The setting applies to all servers in your Enterprise Cluster (EC). Each server must have its own overflow file.

1. Select **Setup > Axway Sentinel/DI** to open the *Axway Sentinel/Decision Insights Events* page.



Note Use the `AxwaySentinel.ConnectionTimeout` server configuration option to set up the connection timeout when Sentinel is unavailable. The default value is 5 seconds. A timeout of zero is interpreted as an infinite timeout and may result in a process hang.

2. Select the check box for **Send Events to Axway Sentinel or Decision Insight Server**.

The rest of the fields on the screen are enabled and SecureTransport sends events to Axway Sentinel as configured.

3. In the *Axway Sentinel/Decision Insight* pane, specify the FQDN or IP address of the Axway Sentinel server in the **Host** field and a valid TCP port on the server to which events will be sent in the **Port** field.
4. (Optional) Select the check box for **Use Secure Connection** to enable sending the selected event to Sentinel over a secured connection.
5. (Optional) Select the check box for **Verify Certificate** to enable the SSL certificate verification. The **Verify Certificate** check box is selected by default.
6. (Optional) Select the check box for **Enable FIPS Transfer Mode** to enable sending events to Sentinel over the secure connection in FIPS transfer mode.

   Note Changes to these settings in Step 3 through Step 6 take effect the next time you restart the Transaction Manager.

7. (Optional) Click the **Test Connection** button. This test indicates whether the port specified on the Axway Sentinel host accepts connections.
8. (Optional) Select **Send Heartbeat to Axway Sentinel Every** and set the heartbeat interval to send periodic messages to Axway Sentinel to tell it that SecureTransport is running and connected. The default interval is 10 seconds.
9. In the *Events* pane, select the event states to send to Sentinel.

   An Event State specifies the current state of a file transfer. If an Event State is not selected to be sent, SecureTransport performs the processing represented by the state, but it does not send the event that reports the state to Axway Sentinel. For the available states, see *Event states* on page 110.
10. In the *Attribute mapping* pane, click the **Add Mapping** button to create a **Sentinel Attribute Name** and **Value** attribute mapping rule. The attributes can also be updated or deleted.

    The Mapping Rules columns refer to:

    - **Sentinel Attribute Name** – The Sentinel column where the attribute is reported.
    - **Value** – The value which is reported in Sentinel under the related column. The value column accepts either real values or SecureTransport expressions.

      Note Subscription attributes can be accessed using the following expression: `${flow.attributes['userVars.ATTRIBUTE_NAME']}`

      Note The value of the DXAGENT_ROUTE_SOURCE_FULL_TARGET variable is the absolute path to the file triggered via Advanced Routing. When performing a push transfer via Advanced Routing over PeSIT, the DXAGENT_ROUTE_SOURCE_FULL_TARGET variable is not populated in ACK or ENDED_TO_ACK state.
11. In the *Overflow file* pane, specify information about the file to be used to store SecureTransport event data when there is no connection between SecureTransport and Axway Sentinel. Changes to these settings take effect the next time the Transaction Manager is restarted. Specify the following information:

Field	Description
Name	The base name of the file to contain buffered SecureTransport event data.
Path	The path of the directory where the overflow file will be located. You can specify either a local absolute or relative path. If you specify a relative path, it is created within the `<FILEDRIVEHOME>` directory. Specify a local path, not one in shared storage, because each server in a cluster must have its own overflow file.
Size (MB)	The maximum overflow file size in MB. A 1 MB file can store events from about 150-200 transfers. With a fast and dependable connection between the SecureTransport Server and a dependable Sentinel server, 1-10 MB should be sufficient. If the connection is slow or the connection or the Sentinel server might be down, 10-50 MB is better. When the overflow file size exceeds this size, it invokes the action you configure under **When Overflow File Exceeds Maximum Size**.
Warning Threshold	Specify a percentage of the maximum file size that, when reached, triggers a warning. The value you enter must be an integer between 1 and 94. When a warning is triggered, an email is sent to the SecureTransport administrator. The email message is formatted using the standard email template, `SentinelOverflowFileWarning.xhtml`, located in `<FILEDRIVEHOME>/conf/mailer-templates/`. The recipient of any warning email is the administrator specified in the *FTP/HTTP Startup Password Timeout Configuration* pane of the **Setup > Miscellaneous** page. For details, see *Set the administrator's email* on page 178.
When Overflow File Exceeds Maximum Size	Select the action to take when the overflow files exceed the maximum size you set. Choose one of the following: • **Stop Collecting New Events** – Stop tracking events for Sentinel, but continue to process transfers, run agents and run SecureTransport applications. Use this option in a clustered configuration so that the Sentinel server is not a potential single point of failure. • **Pause All File Transfers** – Stop tracking events for Sentinel and stop processing transfers, running agents and running SecureTransport applications. Use this option with care because it is operationally equivalent to stopping SecureTransport. To restart transfers, either clear the overflow file or select the other option.

12. Click **Save**.

    Your settings are saved and SecureTransport transmits data about file transfer activities to the Axway Sentinel server you specified.

Note For XFB ST Info events, you must enable the dedicated Server Configuration option: `StatisticsSummary.AutoReportAdditionalInfo`. Periodically generate a Sentinel event with usage information on the SecureTransport instance. This includes count of active accounts, product version, enabled features, installed plugins, etc.

Integrate Decision Insight

Decision Insight is a Business Activity Monitoring (BAM) product that collects, aggregates, correlates, and reports events from SecureTransport and other products, applications, and systems throughout your infrastructure. Decision Insight is a separate product that you can buy from Axway or an authorized partner. Once you license and configure SecureTransport to send file transfer and processing events to Decision Insight, data is collected and displayed on a dashboard.

For a list of the Decision Insight versions that are supported by SecureTransport 5.4, see *Axway and third-party software support* on page 39.

Note Decision Insight does not support Attribute mapping in SecureTransport.

Note Decision Insight will not monitor ad hoc activity.

For addition information please refer to the official confluence page Embedded Analytics for Secure Transport Home

The following topics provide additional for the SecureTransport Decision Insight integration:

- *Event states* on page 152 - Describes the Decision Insight event states.
- *Tracked objects* on page 153 - Lists the attributes of the Tracked Objects used to report Axway SecureTransport events to Decision Insight.
- *XFB Transfer tracked objects* on page 154 - Describes the XFB transfer tracked objects.
- *Configure SecureTransport to send events to Decision Insight* on page 155 - Provides how-to instructions for configuring SecureTransport to send events to Decision Insight.

Event states

An event state specifies the current state of a file transfer. Every event in the same group about one file transfer is identified using the same cycle ID. For Axway Sentinel events information, refer to *Event states* on page 110.

The following event states indicate a transfer start and end.

Direction	Start	Success	Failure	Cancellation
Incoming	`RECEIVING`	`RECEIVED`	`FAILED`	`CANCEL`
Outgoing	`SENDING`	`SENT`	`FAILED`	`CANCEL`

The following event states indicate a post processing action.

Event state	Description
DECRYPTED	SecureTransport has performed a successful PGP decryption.
DECRYPTING	SecureTransport is starting to decrypt a file.
DELETED	A client, post-processing action (PPA), or post client download action has deleted a file.
ENCRYPTED	SecureTransport has performed a successful PGP encryption.
ENCRYPTING	SecureTransport is starting to encrypt a file.
POST_ PROC/ARCHIVED	The file has been archived.
POST_PROC/ICAP_ DENIED	Access to the file is denied.
POST_PROC/ICAP_ SCANNED	The scanning of the file has successfully finished.
POST_PROC/ICAP_ SCANNING	The scanning of the file has started.
POST_ PROC/ROUTED	An Advanced Routing application has successfully completed.
POST_ PROC/ROUTING	SecureTransport is starting an Advanced Routing application.
RENAMED	A client action, or a post-transmission action (PTA), or post-processing action has renamed a file.
ROUTED	As the intermediate partner in a routed PeSIT transfer, SecureTransport has sent a file to the routing destination.

Tracked objects

This topic lists the attributes of the Tracked Objects used to SecureTransport events to Decision Insight. For information on all the of standard attributes, refer to *Axway Sentinel tracked objects* on page 112.

The attributes that Decision Insight uses to build the dashboards are:

Name	Format	Description
COREID	string	File identifier reported with every state
CYCLEID	string	ID used to relate events about the same transfer.
DIRECTION	string	R for receive, S for send
FINALRECEIVERID	string	Name of the final receiver of the transfer
GROUPNAME	string	Axway SecureTransport account business unit
ISALERT	0/1	1 means permanent error on last entry
ISEXCEPTION	0/1	1 means temporary failure
ORIGINALSENDERID	string	Name of the original sender of the transfer
RECEIVERID	string	Name of the receiving partner
REQUESTGROUPID	string	Local identifier of the group to which the requesting user belongs
REQUESTUSERID	string	Local identifier of the user who requested the transfer
SENDERID	string	Name of the sending partner
USERID	string	Axway SecureTransport Login Name/Account Name or account name of the account the triggered the Advanced Routing feature
USERPARAMETER1	string	Account type: E for Partner, I for Internal, N for Unspecified

XFB Transfer tracked objects

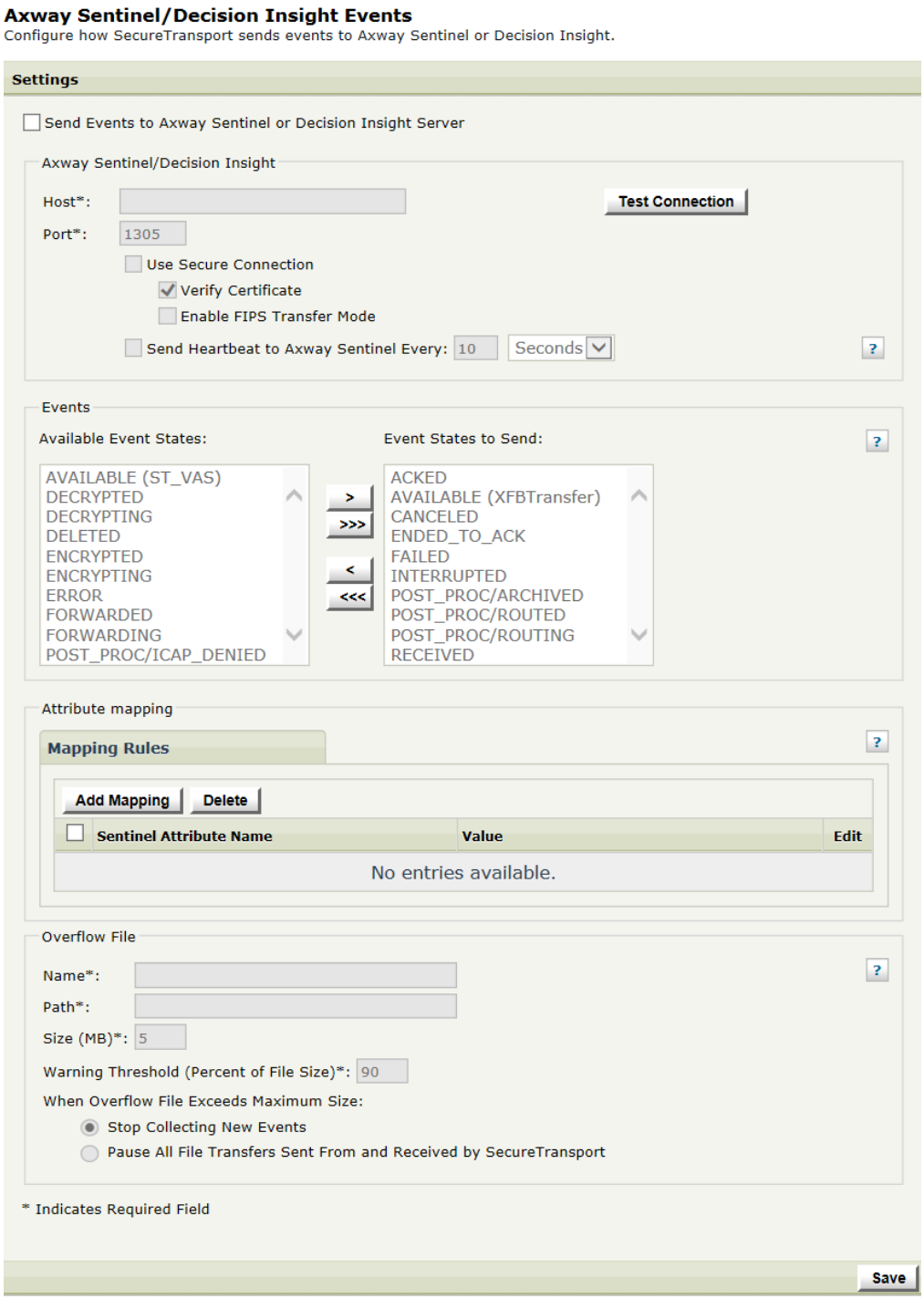
This topic provides the XFB tracked object roles, sender and receivers, production identification, and transfer attributes. For more information, refer to *XFB Tracked Object attributes* on page 123.

Configure SecureTransport to send events to Decision Insight

Use the SecureTransport Administration Tool to configure SecureTransport to send events to Decision Insight.

The setting applies to all servers in your Enterprise Cluster (EC). Each server must have its own overflow file.

1. Select **Setup > Axway Sentinel/DI** to open the *Axway Sentinel/Decision Insights Events* page.



2. Select the check box for **Send Events to Axway Sentinel or Decision Insight Server**.

   The rest of the fields on the screen are enabled and SecureTransport sends events to Decision Insight as configured.

3. In the *Axway Sentinel/Decision Insight* pane, specify the FQDN or IP address of the Decision Insight server in the **Host** field and a valid TCP port on the server to which events will be sent in the **Port** field.

4. (Optional) Select the check box for **Use Secure Connection** to enable sending the selected event to Decision Insight over a secured connection.
5. (Optional) Select the check box for **Verify Certificate** to enable the SSL certificate verification. The **Verify Certificate** check box is selected by default.
6. (Optional) Select the check box for **Enable FIPS Transfer Mode** to enable sending events to Decision Insight over the secure connection in FIPS transfer mode.

   Note Changes to these settings in Step 3 through Step 6 take effect the next time you restart the Transaction Manager.

7. (Optional) Click the **Test Connection** button. This test indicates whether the port specified on the Decision Insight host accepts connections.
8. In the *Events* pane, select the event states to send to Decision Insight.

   An Event State specifies the current state of a file transfer. If an Event State is not selected to be sent, SecureTransport performs the processing represented by the state, but it does not send the event that reports the state to Decision Insight.

   Note The Event states that indicate transfer start and end must be enabled to build Decision Insight dashboards. Refer to *Event states* on page 152.

9. In the *Overflow file* pane, specify information about the file to be used to store SecureTransport event data when there is no connection between SecureTransport and Decision Insight. For more information, refer to *Configure SecureTransport to send events to Axway Sentinel* on page 148.
10. Click **Save**.

Server licenses

Use the *Server License* page to update SecureTransport licenses. You usually install licenses when you perform initial SecureTransport setup and configuration after installation. Update licenses whenever required, for example, when you receive your permanent license for SecureTransport after an evaluation period.

SecureTransport requires two licenses. The core server license specifies the number of accounts allowed and the number of ad hoc users allowed. The core license can limit the license to a specified host and to a specified date range. The features license specifies if the AS2, SSH, and Connect:Direct protocols are allowed, if SiteMinder integration is allowed, if the Enterprise Cluster (EC) option is included, and the number of cluster nodes allowed.

The FTP and HTTP protocols are included in the core license. For other features, contact your local account executive or supplier.

The following topics describe the account session count and ad hoc licenses and provide how-to instructions for updating the SecureTransport licenses:

- *Account session count* on page 158
- *Ad hoc user licenses* on page 158
- *Updating SecureTransport licenses* on page 158
- *Generate Usage report* on page 162

Account session count

The number of accounts in the core server license controls the number of connections allowed to the server. An account license is considered in use when a user logs in. A license is also considered in use when used for a site that is initiating transfers. The license is considered in use for 60 days after the initial login or site transfer. The Folder Monitor, AS2 receiving, and asynchronous AS2 MDN receiving are excluded from license counting.

Account licenses apply to all protocols. To limit the number of concurrent users who can connect to the SecureTransport FTP and HTTP servers, see *User limits* on page 743.

Note SecureTransport does not perform DNS lookups. Therefore a single site referred to in one place by name and another place by IP address is counted as two sites.

Ad hoc user licenses

You must install a core license with ad hoc user licenses included to enable users to compose, send, reply to, or forward messages using ST Web Client or the Axway Email Plug-ins. There are four categories of ad hoc user licenses:

- **Unlimited ad hoc user licenses**: If your company has purchased an unlimited number of ad hoc user licenses, then the display shows "unlimited" for the number of ad hoc Users.
- **One ad hoc user license for each account license**: If your company has purchased one ad hoc user license for each account license, then the display shows the same number of licenses for Accounts and for ad hoc users.
- **Fewer ad hoc user licenses than account licenses**: If your company has purchased fewer ad hoc user licenses than account licenses, then the display shows the maximum number of users that can compose, send, reply to, or forward messages using ST Web Client or one of the Axway Email Plug-ins. One ad hoc user license is consumed the first time a user performs one of these actions.
- **No ad hoc user licenses**: If your company did not purchase any ad hoc user licenses, then end users cannot use ad hoc file transfers. The display does not include the line with ad hoc users.

Updating SecureTransport licenses

To obtain the text files that contains the server licenses, contact Axway Global Support. For contact information, see *Get more help* on page 31.

1. Select **Setup > Server License**.

   The *Server License* page is displayed.

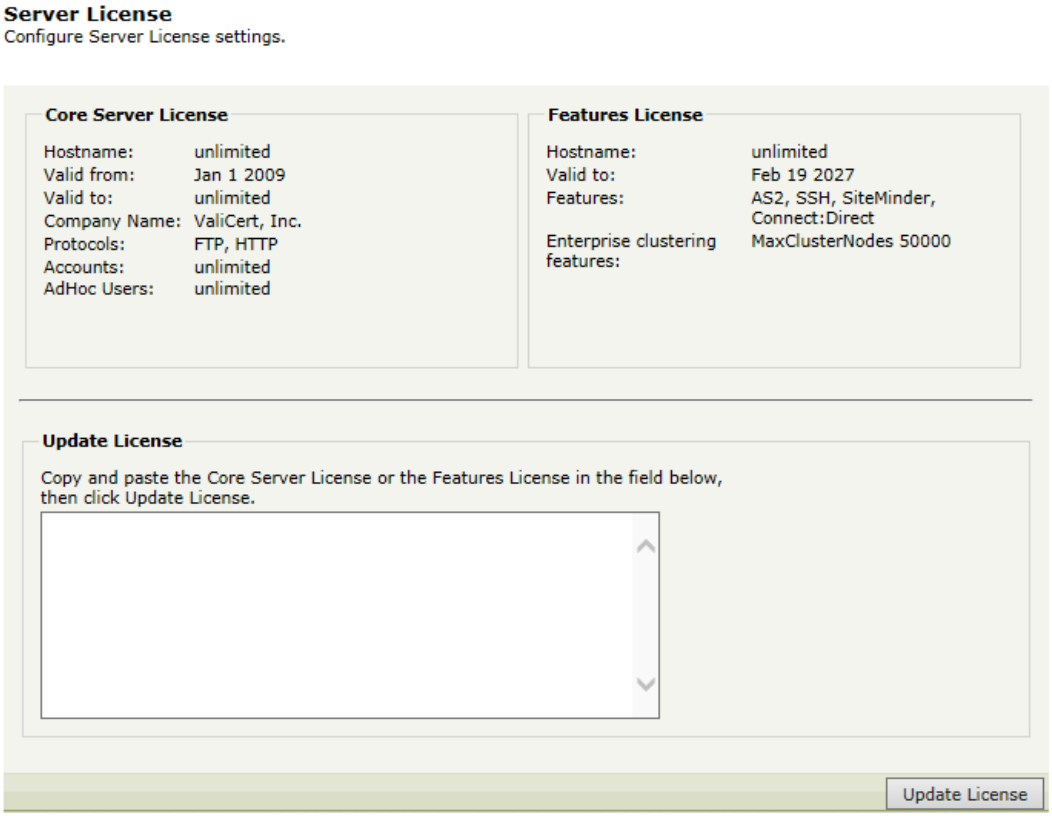
2. Copy and paste the entire contents of the Core Server License into the **Update License** text area.

3. Click **Update License**.

   The updated license information is displayed on the *Server License* page.

4. Copy and paste the entire contents of the Features License into the **Update License** text area.
5. Click **Update License**.

   The updated license information is displayed on the *Server License* page.



   Note The Connect:Direct license is listed only when the Connect:Direct protocol is enabled.

6. Restart all SecureTransport servers that are running.

   The licenses for your SecureTransport Server are updated.

Usage reporting for subscription-based licenses

This topic describes the concepts and logic in usage tracking and why you might need to enable it for your on-premises Axway product.

What is usage tracking?

Usage tracking identifies how Axway measures the subscription services you use on a monthly basis. Axway measures your usage to make sure it is within the prescribed thresholds specified in your subscription and determine whether overages require billing adjustments.

Must I enable usage tracking?

You must enable usage tracking if you use an Axway on-premises product on a subscription basis. You do not need to use usage tracking if you have a perpetual license.

If you have an AMPLIFY account, you can log on to the AMPLIFY Platform and look up information about your subscriptions and service entitlements. If you don't have an AMPLIFY account, most likely you are using products under licenses and do not have any subscriptions. However, if you are unsure whether usage tracking applies to you, contact your Axway representative or Axway support.

What if I don't enable usage tracking?

Your subscription agreement with Axway requires usage tracking. If you don't enable usage tracking for an on-premises product used under a subscription, you might be in violation of your agreement and, as a consequence, be subject to penalties. It's in your best interest to enable usage tracking because it ensures are using the services you are entitled to.

How do I enable usage tracking?

SecureTransport offers two options for usage reporting:

- *Automatic* for MFT environments using the AMPLIFY Edge Agent
  See *Set up usage reporting* on page 160.
- *Manual* for SecureTransport deployments only
  This option is only applicable to environments with SecureTransport only (without Transfer CFT or other MFT products). See *Generate Usage report* on page 162.

Set up usage reporting

This page describes how to configure the Edge Agent for AMPLIFY MFT implementations and configure Axway SecureTransport for the following use cases:

- Usage tracking only
- Usage tracking and Sentinel monitoring

Figure 1. Usage tracking only

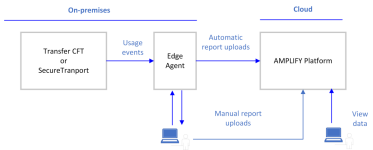
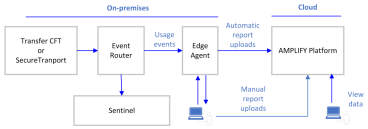


Figure 2. Usage tracking and Sentinel monitoring



Configure the Edge Agent

Prerequisite: You must have your Edge Agent installed and configured to work with SecureTransport.

Perform the following steps on the Edge Agent for MFT implementations that use Transfer CFT or SecureTransport.

1. Download the `AMPLIFY_Edge_Agent_MFT_<version>_configuration_<BNxxx>.zip` package from the Axway Support Site.
2. Extract the zip locally.
3. Edit the `MFT.json` file to change the value of the `envId` parameter to the `Environment ID` from the Platform.
4. Upload the `MFT.json` file from the package to the `<Edge_Agent_install_dir>/conf/agent/report` directory.
5. Upload the `MFT-usage.json` file from the package to the `<Edge_Agent_install_dir>/conf/agent/aggregation` directory.
6. Restart the Edge Agent. .

Note The MFT.json file name is the `configurationName` that you use when querying the Edge Agent.

Configure SecureTransport

There are two methods of configuration depending on the use case you implement.

Usage tracking with the Edge Agent

In this use case, SecureTransport sends the usage events to the Edge Agent. Follow this simple procedure to configure usage tracking:

1. From ***Setup > Axway Sentinel/DI***, configure reporting to Edge Agent by following the steps 1-9 as described in *Configure SecureTransport to send events to Axway Sentinel* on page 148. Note that you must use the connection details for Edge Agent and not for Sentinel.
2. Test and save the configuration.
3. From ***Operations > Server Configuration***:
    i. Set `StatisticsSummary.AutoReportAdditionalInfo` to `true`. This is needed in order to periodically generate a Sentinel event with usage information on the SecureTransport instance.

ii. Set `Ssh.AxwayVendorExtensions.enabled` to `true`. This is needed if SecureTransport communicates with Transfer CFT over the SFTP protocol. Note that in order for this change to take effect, you must restart the SSH service on each Server and Edge instance.

4. Restart the Transaction Manager to apply the configuration.

Usage tracking with the Edge Agent and monitoring with Sentinel

In this use case, SecureTransport uses the Event Router to send notifications to both Sentinel and the Edge Agent.

You need an installed Sentinel and Event Router to implement this method. For more information, refer to the latest Sentinel Event Router User Guide.

Note that in this case you must follow the *Usage tracking with the Edge Agent* on page 161 procedure (described just above), with an important exception: in step 1, you must use the connection details for the Event Router.

On the Event Router

You must configure the Event Router to allow sending *usage tracking messages* to the Edge Agent and *monitoring messages* to Sentinel. In the following configuration steps, `XFBTransfer` and `CycleLink` are sent to both the Edge Agent and Sentinel. However, `XFBSTInfo` and `XFBCFTInfo` are only sent to the Edge Agent.

Note The default target is called `SENTINEL` in the instructions that follow.

Edit the Event Router configuration file to route the usage information to Sentinel (`SENTINEL`) and the Edge Agent (`EDGEAGENT`).

1. Add the Edge Agent as a new target.
2. Define a route to send the `XFBTransfer` Tracked Object to the Edge Agent.
3. Define a route to send the `CYCLELINK` to the Edge Agent.
4. Define a route to send the `XFBSTInfo` only to the Edge Agent.
5. If you are also implementing Transfer CFT, define a route to send the `XFBCFTInfo` only to the Edge Agent.

Generate Usage report

You can manually generate a usage report that provides an overview of the daily usage of SecureTransport. This option is applicable to environments with SecureTransport only (without Transfer CFT or other MFT products).

The report provides daily usage metrics and totals for a selected period or date range:

- number of active users
- number of unique transfers based on coreID

- number of successful inbound and outbound file transfers

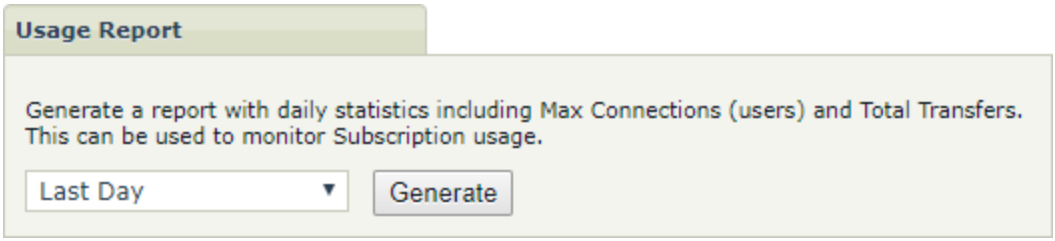
Along with these daily metrics, the report contains information regarding your current SecureTransport setup.

The report is in JSON format and is available as a REST API resource.

The Administration Tool provides a simple interface to generate the report as a JSON file.

1. Select **Setup > Server License**.

   The *Server License* page is displayed.

2. In the *Usage Report* pane, select a reporting period from the drop-down and click **Generate**.
3. A dialog box prompts you to open the report or save it to disk as a `.json` file.
4. Select your preference, and click **OK**.

The generated JSON report contains the following parameters:

Element *(type)*	Description
envId *(string)*	Unique custom identifier useful for specifying each cluster instance. Blank by default, this value can be changed using the `StatisticsSummaryReport.EnvironmentId` server configuration option.
schemaId *(string)*	The JSON schema to validate the file against. Blank by default this value can be changed using the `StatisticsSummaryReport.SchemaId` server configuration option.
timestamp *(string)*	Timestamp when the report is generated. This value is in ISO 8601 format: `{YYYY}-{MM}-{DD}T{hh}:{mm}:{ss}.{SSS}{TZ}`.
granularity *(number)*	Report interval granularity: *86400000* milliseconds (24 hours)
report *(object)*	Collection of *daily reports*, chronologically ordered by date in the specified reporting period.

Element *(type)*	Description
date *(object)*	The date of the daily report. This value is in ISO 8601 format: `{YYYY}-{MM}-{DD}T{hh}:{mm}:{ss}.{SSS}{TZ}`. The number of daily reports depends on your selection of the reporting period.
product *(string)*	Name of the MFT product, e.g. *SecureTransport*
usage *(object)*	Collection of daily metrics related to the product. With SecureTransport it contains the active users and information about the file transfers performed within the day.
ST.ActiveUsers *(number)*	Number of active users for the day
ST.TransfersCore *(number)*	Total number of unique transfers (based on `coreID`) for the day
ST.TransfersIn *(number)*	Number of successful inbound file transfers (with state RECEIVED) for the day. Internal routing (within SecureTransport) via Advanced Router and Standard Router is excluded.
ST.TransfersOut *(number)*	Number of successful outbound file transfers (with state SENT) for the day. Internal routing (within SecureTransport) via Advanced Router and Standard Router is excluded.
ST.TransfersMaxInOut *(number)*	The greater number between `ST.TransfersIn` and `ST.TransfersOut`
meta *(object)*	Additional meta information for the daily report
meta *(object)*	Additional meta information for the summary report.
companyName *(string)*	Company name as specified in the license

Element *(type)*	Description
envName *(string)*	Custom display name of the environment. Blank by default, this value can be changed using the `StatisticsSummaryReport.EnvironmentName` server configuration option.
productLine *(string)*	Name of the product line: e.g. *MFT*
productName *(string)*	Name of the MFT product: e.g *SecureTransport*
productVersion *(string)*	Base product version: e.g. *5.4* (SecureTransport version)
currentPatch *(string)*	Currently installed patch: e.g. *PATCH-23*
isECEnabled *(boolean)*	Specifies if *Enterprise Clustering* is enabled: can be *true* or *false*.
isFMEnabled *(boolean)*	Specifies if *Flow Management (Central Governance)* integration is enabled: can be *true* or *false*
isADIEnabled *(boolean)*	Specifies if *AxwayDecisionInsight (Sentinel)* integration is enabled: can be *true* or *false*
plugins *(object)*	List of installed plug-ins along with their versions
authorization *(object)*	List of installed authorization plug-ins.
authentication *(object)*	List of installed authentication plug-ins
site *(object)*	List of installed transfer site plug-ins
customARStep *(object)*	List of installed Advanced Routing step plug-ins

Element *(type)*	Description
reportTimeframe *(object)*	The report time frame
startDate *(string)*	Timestamp of the start date of the reporting period
endDate *(string)*	Timestamp of the end date of the reporting period. Note that the end date is not included in the report. For example, to generate a report for May, the start date should be 1 May, the end date should be 1 June.
reportSummary *(object)*	Usage aggregations for the selected period based on daily usage information
ST.ActiveUsers *(number)*	Maximum number of active users for the reporting period
ST.TransfersCore *(number)*	Total number of unique transfers (based on `coreID`) for the reporting period
ST.TransfersIn *(number)*	Number of successful inbound file transfers (with state RECEIVED) for the reporting period. Internal routing (within SecureTransport) via Advanced Router and Standard Router is excluded.
ST.TransfersOut *(number)*	Number of successful outbound file transfers (with state SENT) for the reporting period. Internal routing (within SecureTransport) via Advanced Router and Standard Router is excluded.
ST.TransfersMaxInOut *(number)*	Total of the `ST.TransfersMaxInOut` values for the reporting period

Configure FTP command log

The SecureTransport command logging feature works as a tracking system. It maintains a log of the commands entered by the users during an FTP session. Command logging is available for the FTP server only. You can use the `Ftp.CommandLogging.File` server configuration parameter to set the location of the command log. By default, the location is `<FILEDRIVEHOME>/var/logs/cmdlog`.

Use the *Command Logging* page to view and determine which user classes should have their commands logged. You can restrict this feature by user class, so that the FTP sessions of only certain user classes are logged.

The following topics provide how-to instructions for configuring and managing the FTP command log:

- *Add a command logging entry* on page 167
- *Enable or disable command logging entries* on page 167 -
- *Edit a command logging entry* on page 168
- *Delete command logging entries* on page 168

Add a command logging entry

Use the following procedure to add a command logging entry.

1. Select **Setup > Command Logging** to open the *Command Logging* page.

2. Click **Add Logging**.
3. An entry is added to the *Command logging entries* table.
4. Select a **User Class** or * for all classes.

   On SecureTransport Server, the user class is validated. On SecureTransport Edge, the user class is not validated and if it does not exist, nothing is logged.
5. Click the Save icon ( ) in the **Edit** column.

   The status of the new entry is set to disabled.

Note To cancel an add operation, select **Setup > Command Logging** again.

Enable or disable command logging entries

Use the following procedure to enable or disable command logging entries.

1. Select **Setup > Command Logging** to open the *Command Logging* page.
2. Select the entries to enable or disable.
3. Click **Enable** or **Disable**.

   The icon in the **User Class** column changes to show that the entry is enabled or disabled.

If a Command Logging is added, but it is disabled; no Protocol Commands will be logged.

Edit a command logging entry

Use the following procedure to edit a command logging entry.

1. Select **Setup > Command Logging** to open the *Command Logging* page.
2. For the entry to edit, click the Edit icon ( ) in the **Edit** column.
3. Change the value in the **User Class** column as needed.
4. Click **Enable** or **Disable**.
5. Click the Save icon ( ) in the **Edit** column.

Note To cancel an edit operation, select **Setup > Command Logging** again.

Delete command logging entries

Use the following procedure to delete command logging entries.

1. Select **Setup > Command Logging** to open the *Command Logging* page.
2. Select the entries to delete.
3. Click **Delete**.

   The entry is removed from the *Command logging entries* table.

FTP SITE META command

SecureTransport has added support for a new command - SITE META. The command is part of the already existing SITE commands and provides capabilities to store user-specific information as metadata over the FTP protocol. It does not comply with any RFC documents and has a generic syntax.

The command accepts input in the format of key - value pairs. The supplied information is stored in the FTP session and is available until the session finishes or times out. For files uploaded during the same session, the provided information will be stored as file metadata attributes. The information can be evaluated at a later point for each file.

This way, the SITE META input could be used for defining routing rules for server-initiated transfers. For file metadata persistence specifics, see *Subscription flow attributes and FTP related attributes* on page 170.

Note To save the SITE META attributes for a file, the command execution and the file upload must happen within one session. Sharing attributes between different FTP sessions is not supported.

FTP SITE META command syntax

The command accepts arguments in the format of key-value pairs. Everything beyond the META will be considered as a command argument. The format follows the pattern:

```
SITE META <key>=<value>
```

The commands supports multiple arguments as well:

```
SITE META <key1>=<value1>;<key2>=<value2>;<key3>=<value3>
```

Supplying same key names with different values will result in overwriting the previous values with the latest one.

Note The "=" and ';' are considered special symbols:
- the semicolon sign (';') is used to delimit the different pairs,
- the equals sign ("=") splits the key name from its value.
If using them as part of the payload, escaping is required. They must be preceded by "\" or \\, depending on the manner how FTP clients accept command arguments.

When a file is uploaded using a common session, the commands arguments are stored as part of the file meta information. They are written in an existing namespace - the flow attributes user variables (*userVars*). For more information about flow attributes, see *Flow attributes* section in *Mail template commands and variables* on page 173.

The command supports entering keys with empty values:

```
SITE META <key1>=;<key2>=;
```

This will result in deleting existing flow attributes with the same key name (if any) for already existing files. For new files these attributes are discarded and will not be persisted.

Note The supplied key-value pairs are saved on the file system as metadata for each file. The information is stored in a serialized and readable format. We do not recommend storing any sensitive or confidential information.

Evaluate SITE META user metadata

FTP meta information can be evaluated and used to define basic transfer flows for server-initiated transfers. Evaluation of those attributes is possible from the Advanced Routing Steps, Transfer Sites and Subscriptions for fields that support expression evaluation (marked with a yellow stripe).

Within the Routing steps, metadata that comes from the SITE META command, along with any other file flow attributes can be evaluated using:

```
${flow.attributes['userVars.<key>']}
```

When using transfer sites and subscriptions, the file flow attributes (both SITE META and subscription), the expression is:

```
${stenv['DXAGENT_FLOW_USERVARS.<KEY-in-upper-case>']}
```

Subscription flow attributes and FTP related attributes

Key-value pairs from subscription properties and those from FTP SITE META share a common space and are all persisted as file attributes for each file (if any).

Uploading files in the subscription directory within an FTP session with SITE META commands, the subscription flow attribute settings will always take precedence.

For more information about flow attributes settings, see *Configure general settings* section in *Subscribe to Advanced Routing application* on page 821.

Configure transfer log

The transfer log tracks the file uploads and downloads on the system and records a lot of basic and additional information, such as whether the transfer was initiated by the server or by a user, protocol used and other information.

The tracking information is kept in the database and in a log file named `xferlog`, which is located in the `<FILEDRIVEHOME>/var/logs` directory. For information about the `xferlog` log file, see *General log files* on page 998. If you have the Enterprise Cluster (EC) option, you can store the transfer log data in a separate external database from the rest of the SecureTransport data. See *Direct log data to separate Oracle databases* on page 99.

Use the *Transfer Logging* page to add and edit logging entries to determine which transfers will be logged. You can also enable this feature for a specific user class.

The following topics provide how-to instructions for managing the transfer log configuration:

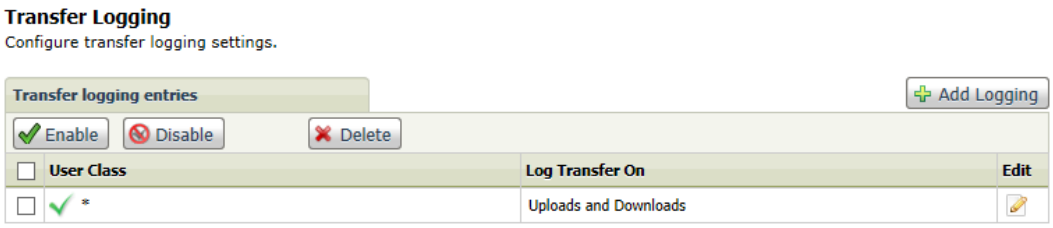
- *Add transfer logging entries* on page 170 - Provides how-to instructions for adding transfer logging entries.
- *Enable or disable transfer logging entries* on page 171 - Provides how-to instructions for enabling or disabling transfer logging entries.
- *Edit transfer logging entries* on page 171 - Provides how-to instructions for editing transfer logging entries.
- *Delete transfer logging entries* on page 172 - Provides how-to instructions for deleting transfer logging entries.

Add transfer logging entries

Use the following procedure to add transfer logging entries.

1. Select **Setup > Transfer Logging**.

   The *Transfer Logging* page is displayed.



2. Click **Add Logging**. A row is added to the *Transfer logging entries* list.
3. Select a **User Class**. The user class must already be defined in the *User Classes* page of the **Access** menu.

   Asterisk (*) means all users.
4. In the **Log Transfers On** list, select `Uploads`, `Downloads`, or `Uploads and Downloads`.
5. Click the Save icon ( ) in the **Edit** column.

   Your entry is added to the *Transfer logging entries*. By default, the status is disabled.

Note To cancel an add operation, select **Setup > Transfer Logging** again.

Enable or disable transfer logging entries

Use the following procedure to enable or disable transfer logging entries.

1. Select **Setup > Transfer Logging**.

   The *Transfer Logging* page is displayed.
2. Select the check box for each entry to modify.
3. Click **Enable** or **Disable**.

   The icons in the **User Class** column change to indicate the status of the entries.

Edit transfer logging entries

Use the following procedure to edit transfer logging entries.

1. Select **Setup > Transfer Logging**.

   The *Transfer Logging* page is displayed.
2. Click the Edit icon ( ) in the **Edit** column for the entry to edit.
3. Make the required changes to the fields in the entry.
4. Click the Save icon ( ) in the **Edit** column.

Note To cancel an edit operation, select **Setup > Transfer Logging** again.

Delete transfer logging entries

Use the following procedure to delete transfer logging entries.

1. Select **Setup > Transfer Logging**.

   The *Transfer Logging* page is displayed.

2. Select the entries to delete.
3. Click **Delete**.

   The entry is removed from the *Transfer logging entries* table.

Configure holiday schedule

You can specify holiday dates for the SecureTransport system and use them later when creating scheduled transfers or tasks. Having set up official holiday dates, you can take one of the following actions when creating a scheduled task or transfer:

- Ignore the holiday schedule – this is the default option
- Take no action if the scheduled date happens to be a holiday specified in the holiday schedule

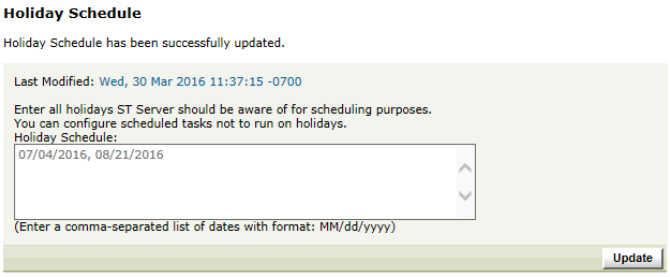
Keep the following items in mind when listing holiday dates:

- The list of holidays applies to all users on the server – it is not dependent on the time zones of users. The dates specified as scheduled are interpreted in local time by the server.
- The Holiday Schedule functionality does not allow for executing a scheduled task on the next working day if the specified date happens to be a holiday – when this occurs, the tasks are not executed.
- Weekend days are treated as holidays by default.

For information about creating scheduled transfers, see *Scheduled downloads and tasks* on page 616 and *Set up a scheduled transfer task for a subscription* on page 617.

1. Click **Setup > Holiday Schedule**.

   The *Holiday Schedule* page is displayed.



2. Enter one or more holiday dates in the **Holiday Schedule** field.

   Use the *MM/dd/yyyy* date format. If you enter more than one date, separate them with commas.

3. Click **Update**.

The configured Holiday Schedule applies to all users of the SecureTransport server and is applicable for all accounts and transfers.

Mail templates

Use the *Mail Template Repository* page to manage the email templates used in Human to Human and System to Human file transfers. SecureTransport uses the mail template selected on the *AdHoc Settings* page to create all notification emails to ad hoc file transfer recipients and senders. To select the mail template, see *Configure adhoc file transfers* on page 89.

SecureTransport sends the following email notifications to ad hoc file transfer recipients and senders:

- Account enrollment notification to the recipient
- Package delivery notification to the recipient and the sender
- Account enrollment failure notification to the sender
- Package delivery failure notification to the sender

The mail template uses variables in `style` attributes to select the information that SecureTransport includes in each notification.

The following topics describe the mail template command and variables and provide how-to instructions for managing mail templates:

- *Mail template commands and variables* on page 173 - Describes the mail template commands and variables.
- *Add a mail template for AdHoc, Enrollment, or Advanced Routing notifications* on page 176 - Provides how-to instructions for adding a mail template.
- *Download a mail template* on page 177 - Provides how-to instructions for downloading a mail template.
- *Upload an updated mail template* on page 177 - Provides how-to instructions for uploading an updates mail template.
- *Delete mail templates* on page 177 - Provides how-to instructions for deleting mail templates.

Mail template commands and variables

When you create a custom mail template, make sure to include the CSS in the `<style>` element in the default file, `AdhocDefault.xhtml`. You can download the default mail template, rename it, customize it and upload your custom mail template.

The following topics lists the notification type and information variables and provide an email template variable example:

- *Notification type variables* on page 174
- *Notification information variables* on page 174
- *Additional attributes* on page 175

- *Flow and subscription attributes* on page 175
- *Email template variable example* on page 176

Notification type variables

Reference the following variables in the `display` property of the `style` attribute of an XHTML element in the mail template to select what information is included:

- `$DISPLAY_ENROLLMENT` – Enrollment notification
- `$DISPLAY_DELIVERY` – Delivery success or failure notification
- `$DISPLAY_PKG_INFO` – Display the message information including the sender, the recipient and the message text
- `$DISPLAY_FAILURE_ENROLLMENT` – Enrollment failed
- `$DISPLAY_FAILURE_FORBIDDEN` – Delivery was forbidden based on the delivery method
- `$DISPLAY_FAILURE_GENERAL` – General delivery failure
- `$DISPLAY_FAILURE_RECIPIENT` – Delivery to the recipient failed
- `$DISPLAY_FAILURE_UNRESOLVED` – The recipient could not be resolved

If the value of a variable is the empty string, the information is displayed. If the value is `none`, the information is not displayed.

Notification information variables

The following variables contain information used in account enrollment notifications:

- `$ENROLL_USERNAME` – User name for enrollment
- `$ENROLL_PASSWORD` – Password for enrollment
- `$ENROLL_LOGINURL` – URL for enrollment using `$ENROLL_USERNAME` and `$ENROLL_PASSWORD`

The following variables contain information used in package delivery failure notifications:

- `$PKG_FAILURE_ENROLLMENT` – Error message for an account enrollment failure
- `$PKG_FAILURE_FORBIDDEN` – Error message for a forbidden delivery failure
- `$PKG_FAILURE_GENERAL` – Error message for a general delivery failure
- `$PKG_FAILURE_RECIPIENT` – Error message when the email cannot be delivered to a recipient
- `$PKG_FAILURE_UNRESOLVED` – Error message when an account cannot be resolved
- `$PKG_TO` – Recipients from the TO list
- `$PKG_CC` – Recipients from the CC list

- `$PKG_BODY` – Text of the message
- `$PKG_ATTACHMENTS` – Names of the files attached to the message

Additional attributes

Additional attribute user variables (`userVars`) are defined per account or account template in the *Additional Attributes* pane. For additional account creation information, refer to *Create a user account* on page 456. For additional account template creation information, refer to *Add an account template* on page 664.

To use `userVars` for email notifications, you must create your own mail template and specify the desired value with following expression:

```
$DXAGENT_ACCOUNT_ATTR_USERVARS_{KEY}
```

Where `KEY` is the additional attribute key.

For example, if you want an user name defined in the Additional Attributes you must type:

```
$DXAGENT_ACCOUNT_ATTR_USERVARS_NAME
```

If the key of an additional attribute contains periods (.) in its name you must replace this all occurrences of periods with underscores (_), when using this attribute in email template.

For example:

To use `userVars.name.first` in an email template you must type:

```
$DXAGENT_ACCOUNT_ATTR_USERVARS_NAME_FIRST
```

If there is collision between Additional Attributes keys after they are used for email template notifications, the value to which they will be evaluated in email template is not determined.

For example:

`userVars.name_first` and `userVars.name.first` are both used as:

```
$DXAGENT_ACCOUNT_ATTR_USERVARS_NAME_FIRST
```

It is not clear to which value this expression is going to be evaluated.

Flow and subscription attributes

Flow and subscription attributes user variables (`userVars`) are defined per subscription in the *Flow/Subscription Attributes* pane. For additional subscription information, refer to *Subscribe an account to an application* on page 607.

To use `userVars` for email notifications, you must create your own mail template and specify the desired value with following expression:

```
$DXAGENT_SUBSCRIPTION_ATTR_USERVARS_{KEY}
```

Where `KEY` is the flow attribute key.

For example, if you want an user name defined in the Flow Attributes you must type:

`$DXAGENT_SUBSCRIPTION_ATTR_USERVARS_NAME`

If the key of a flow attribute contains periods (.) in its name, you must replace all periods with underscores (_) when using this attribute in email template.

For example:

To use `userVars.name.first` in an email template you must type:

`$DXAGENT_SUBSCRIPTION_ATTR_USERVARS_NAME_FIRST`

If there is collision between flow attribute keys after they are used for email template notifications, the value to which they will be evaluated in the email template is not determined.

For example:

`userVars.name_first` and `userVars.name.first` are both used as:

`$DXAGENT_SUBSCRIPTION_ATTR_USERVARS_NAME_FIRST`

It is not clear to which value this expression is going to be evaluated.

Email template variable example

The following example from the default email template uses a variables to select a row of a table that includes information from another variable.

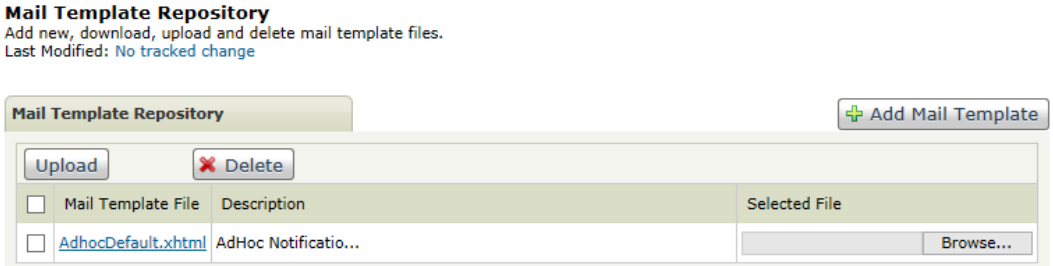
```
<tr style="display: $DISPLAY_DELIVERY">
   <th>To</th>
   <td style="vertical-align: top;">$PKG_DELIVERY_TO</td>
</tr>
```

Add a mail template for AdHoc, Enrollment, or Advanced Routing notifications

Use the following procedure to add a mail template.

1. Click **Setup > Mail Templates**.

   The *Mail Template Repository* page is displayed.



The default mail template is loaded in the repository initially.

2. Click **Add Mail Template**.

   A line is added to the list.

3. On the new line, click **Browse**.

   A file upload window is displayed.

4. Select a file template file to upload.

5. Click the Save icon ( ) in the **Selected File** column.

   SecureTransport uploads the mail template file and adds it to the repository.

Download a mail template

Use the following procedure to download a mail template.

1. Right-click the template name in the Mail Template File column and select **Save Link As** or **Save Target As**.

   The web browser displays a dialog box.

2. Navigate to the folder and change the file name as needed.

3. Click **Save**.

   The file is saved to the location you specify.

Upload an updated mail template

After you download a mail template and update it, you can upload the update to SecureTransport.

1. In the first column, select the mail templates for which you have updated files.

2. On each selected line, click **Browse** and selected the updated file.

   The file name of the updated template must be the same as the file name of the existing template.

3. Click **Upload**.

   SecureTransport uploads the updated files and replaces the existing files. Any references to the file templates are not changed.

Delete mail templates

Use the following procedure to delete mail templates.

1. In the first column, select the mail template files to delete.

2. Click **Delete**.

SecureTransport displays a confirmation dialog.

3. Click **OK** to delete the selected mail template files.

Configure miscellaneous settings

Use the *Miscellaneous Configuration* page to specify the administrator's e-mail address, set usage monitor options, enable or disable reverse DNS lookups, set the session timeout limits, select a default HTML template, limit FTP login failures, set FTP and HTTP server startup password timeout configuration and suspension options, and define password policy.

The following topics describe and provide how-to instructions for managing the miscellaneous configuration setup options:

- *Miscellaneous options* on page 178 - Describes how to configure the miscellaneous setup options and provides how-to instructions for the miscellaneous setup options.
- *SMTP configuration* on page 183 - Provides how-to instructions for configuring SMTP.
- *FTP and HTTP server suspend options* on page 184 - Provides the how-to instructions for configuring FTP and HTTP server suspension options.
- *Password policy* on page 185 - Describes the password policy and provides how-to instructions for configuring the password policy.

Miscellaneous options

This topic describes how to configure the miscellaneous setup options.

Note As of SecureTransport 5.3.3 Java Applet and ActiveX are no longer available or supported.

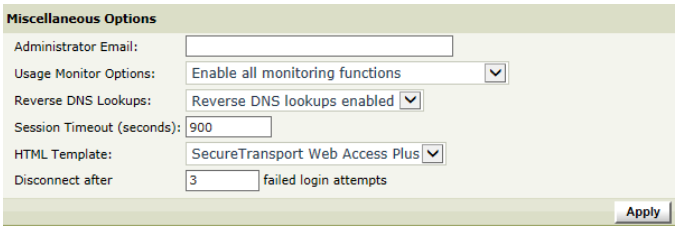
The following topics provide how-to instructions for configuring the miscellaneous options:

- *Set the administrator's email* on page 178
- *Set usage monitor options* on page 179
- *Enable or disable reverse DNS lookups* on page 179
- *Set the session timeout* on page 180
- *Select a default HTML template* on page 180
- *Limit FTP login failures* on page 183

Set the administrator's email

The administrator e-mail is the email address for the system administrator of the FTP server. This address (if specified) is used in several server response messages and is available (%E macro) for run-time messages. Administrator email is available for the FTP server only.

1. Select **Setup > Miscellaneous** and view the *Miscellaneous Options* pane.



2. Enter an e-mail address in the **Administrator Email** field.
3. Click **Apply**.

Set usage monitor options

The Server Usage Monitor can be configured to monitor several different aspects of the server or cluster nodes. You can also turn it off entirely.

Each of the monitoring options requires additional CPU resources per server process to compute and track the enabled measurements. To improve server performance, disable all unnecessary monitoring functions. The usage monitor is available for the FTP, SSH and HTTP(S) servers only.

The possible option settings are as follows:

Option	Description
Enable all monitoring functions	Enables all monitoring functions
Enable monitor - Measure bandwidth	Keeps track of the instantaneous transfer rate of each FTP server process running
Enable monitor - Display user commands	Keeps track of which FTP command a user is currently executing
Enable monitor - No bandwidth/commands	Displays process information per FTP server connection
Disable monitor	Disables all FTP, SSH and HTTP(S) monitoring

1. Select **Setup > Miscellaneous** and view the *Miscellaneous Options* pane.
2. In the **Usage Monitor Options** field, select a monitoring option or disable monitoring.
3. Click **Apply**.

Enable or disable reverse DNS lookups

Note This procedure has been replaced by the `Server.ReverseDNSLookups` server configuration parameter. Edit the `Server.ReverseDNSLookups` server configuration parameter to enable or disable reverse DNS lookups.

Reverse DNS lookups are used to resolve an IP address into a fully qualified domain name. The domain name is used for logging purposes and for applying access rules that specify a host name (instead of an IP address).

In cases where the DNS server is under heavy load, this can significantly affect the startup time of an FTP, HTTP, or SSH session. If the fully qualified domain name is not needed in the log files, it is best to turn off this feature.

Note This feature is available for the FTP, HTTP, and SSH servers.

1. Select **Setup > Miscellaneous** and view the *Miscellaneous Options* pane.
2. In the **Reverse DNS Lookups** field, choose to enable or disable reverse DNS lookups.
3. Click **Apply**.

To disable reverse DNS lookups for the Administration Tool server, see *DNS settings* on page 979.

Set the session timeout

You can set a session timeout for SecureTransport so that users are automatically logged out if they are inactive for the specified duration. SecureTransport uses separate values for the session timeout for the SecureTransport Edge and SecureTransport Server. For example, when logged into the SecureTransport Edge, the Edge session timeout value is applied and when logged into the SecureTransport Server, the Server value is applied.

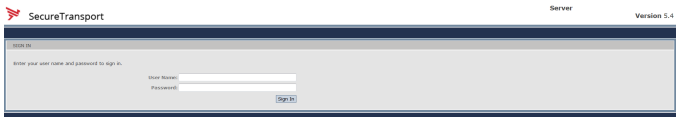
1. Select **Setup > Miscellaneous** and view the *Miscellaneous Options* pane.
2. Enter the number of seconds (60 seconds minimum) in the **Session Timeout** field to specify the session timeout duration.
3. Click **Apply**.

Select a default HTML template

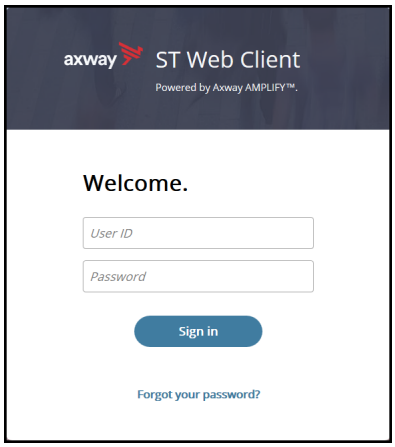
SecureTransport provides several different templates that change the look and feel of the web client user interface. The available options include: SecureTransport Legacy Client, Axway Jelly Ball 9, Axway Box and Stripe in Blue, and ST Web Client. If you configure a user account to use the default HTML template, it uses the one you configure here. For more information about the web clients, refer to the *SecureTransport Web Client User's Guide*.

The following examples show what the login page looks like in the client browser when each template is applied.

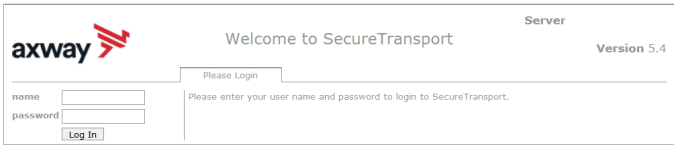
The Axway Box and Stripe in Blue template:



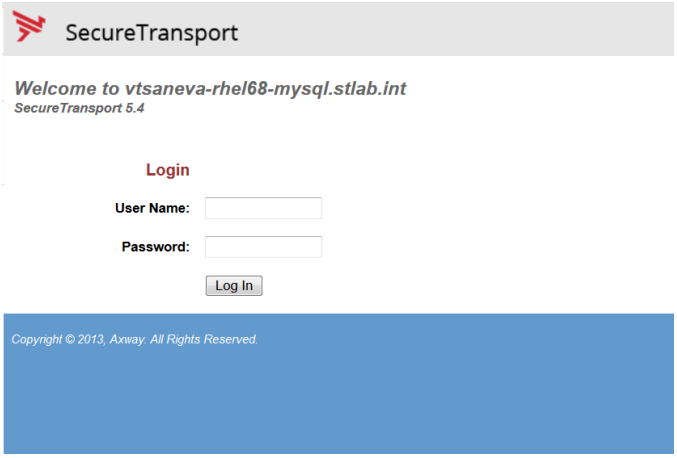
ST Web Client:



The Axway Jelly Ball 9 template:



The SecureTransport Legacy Client template:



Select a default HTML template for web client users

1. Select **Setup > Miscellaneous** and view the *Miscellaneous Options* pane.
2. Select one of the templates from the **HTML Template** field. There are four choices that ship with SecureTransport: SecureTransport Legacy Client, Axway Jelly Ball 9, Axway Box and Stripe in Blue, and ST Web Client.
3. Click **Apply**.

Note The login page of the HTML template you specify here is displayed when the user first accesses this SecureTransport Server. The rest of template is used if the user is configured

to use the default HTML template. To set the HTML template for business unit, see *Create or edit a business unit* on page 693. To set the HTML template for an individual user, see *Create a user account* on page 456.

Use the HTML templates in a new locale

You can adapt an HTML template to a different locale by copying the existing template files and editing them. You also need to create a file for each locale named `skin.conf` that contains the descriptive information for the HTML Template. The SecureTransport Legacy Client template resides in `<FILEDRIVEHOME>/share/ftdocs/html/C`. In SecureTransport, `C` is the default locale.

You need to create a locale folder for the files in the following location: `<FILEDRIVEHOME>/share/ftdocs/html/skin/<SKIN_NAME>/<LOCALE>/` where `<SKIN_NAME>` is the name of the template you want to use and `<LOCALE>` is the name of the new locale.

Create a locale folder

1. Copy the files you want to modify from `<FILEDRIVEHOME>/share/ftdocs/html/C`. The files for the default template are in the locale directory C. To use one of the other template styles, copy the files from `<FILEDRIVEHOME>/share/ftdocs/html/skin/jb9` or `<FILEDRIVEHOME>/share/ftdocs/html/skin/sm6`.
2. create a directory based on the new locale: `<FILEDRIVEHOME>/share/ftdocs/html/skin/<SKIN_NAME>/<LOCALE>/` and paste the copied files into the new directory.

   Note If you only translate the templates, you can use an existing skin name when you create the new directory, just create a locale subdirectory. If you change the file content, use a new skin name. Do not overwrite the original HTML templates.

3. Create the file `skin.conf` using a text editor. The contents of `skin.conf` are:

   ```
   description "<SkinTitle>"
   icons-access "public"
   ```

   where `<SkinTitle>` is the name of the HTML templates you are modifying. You can use any name.
4. Select **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.
5. Search for the `Admin.Locale` parameter and change its value to the new locale.
6. Restart all servers in the cluster.

Modify the HTML files

1. Edit the copied HTML files. You can translate or modify the files.

   For additional information about editing the HTML pages and the default locale, see *Customize a web client* on page 329.

Note If you change the file content, use a new skin name. Do not overwrite the original HTML templates. create a `<SKIN_NAME>` directory and create a `C` subdirectory if you are using the default locale. Store your modified files under the `C` directory.

2. Select **Setup > Miscellaneous** and view the *Miscellaneous Options* pane.
3. Select one of the templates from the **HTML Template** field and click **Apply**.

Limit FTP login failures

You can limit the number of consecutive failed login attempts before the FTP Server terminates a user connection. Limiting the number of consecutive failed login attempts provides added security.

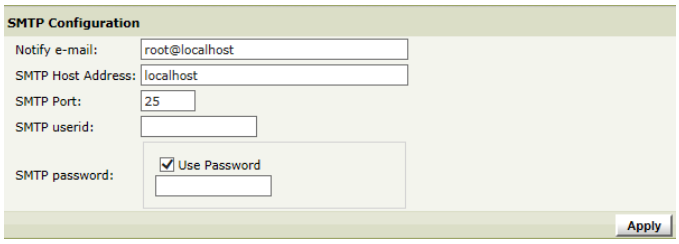
Note This limit is applicable only to FTP login attempts. The HTTP protocol by definition allows only one login attempt per connection.

1. Select **Setup > Miscellaneous** and view the *Miscellaneous Options* pane.
2. In the **Disconnect after _____ failed login attempts field**, type a value greater than zero to identify the number of failed login attempts you want to allow before disconnecting the user.
3. Click **Apply**.

SMTP configuration

Use the *SMTP Configuration* pane to configure SMTP for outgoing email.

1. Select **Setup > Miscellaneous** and view the *SMTP Configuration* pane.



2. In the **Notify e-mail** field, type the email address to which notification emails are sent.
3. In the **SMTP Host Address** field, type the host address of the SMTP e-mail server.
4. In the **SMTP Port** field, type the port number of the SMTP email server.
5. In the **SMTP userid** field, type the user ID required to access the SMTP server.
6. If the SMTP server requires a password, select **Use Password** under *SMTP password* and type the required password in the field provided.
7. Click **Apply**.

Note All fields in this pane are mandatory. Enter valid values for user ID and password fields, if authentication is enabled on the SMTP mail server. If the SMTP mail server does not require authentication, enter a value such as `guest` and `password` in these fields, but do not leave them empty.

FTP and HTTP server suspend options

SecureTransport provides following two options for suspending the FTP and HTTP servers:

- Specify a schedule to suspend the server.
- Suspend the server immediately.

The server suspend option only applies to the HTTP and FTP servers.

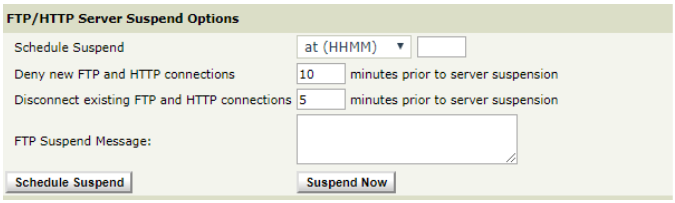
The following topics provide how-to instructions for scheduling server suspensions and immediately suspending the server:

- *Schedule server suspensions* on page 184
- *Suspend now* on page 185

Schedule server suspensions

Use the server suspension options to schedule a specific time of day for the server to suspend and to define a period of time in minutes before the scheduled suspension during which new FTP and HTTP connections are no longer accepted and existing FTP and HTTP connections are disconnected.

1. Select **Setup > Miscellaneous** to and view the *FTP/HTTP Server Suspend Options* pane.



2. Select a format for the time of suspension and type the time for its occurrence. The following time format options are available:
   - **at (HHMM)** – Schedule suspension at exact specified time.

     When defining an exact time, type the time in the HHMM format (a 2-digit hour followed by 2-digit minutes, based on a 24-hour clock) with no spaces or separators.

     If you set a scheduled time to start suspension before the current system time, SecureTransport schedules the suspension for the next day. For example, if the current time is 1400 and a HHMM suspension time of 1330 is specified, the server is scheduled to suspend at 1:30 pm. on the next day.
   - **in (minutes)** – Schedule suspension after the specified number of minutes.
   - **in (hours)** – Schedule suspension after the specified number of hours
3. Type the time, in minutes, when the server must refuse new FTP or HTTP connections before suspension.
4. Type the time, in minutes, when the server must disconnect existing FTP or HTTP connections before suspension.
5. Enter a short text message to be displayed to FTP users before suspension.

Users might or might not see the suspension message based on how the FTP client settings are configured.

6. Click **Schedule Suspend**.

   The page now displays information about the scheduled suspension. To cancel or modify the scheduled suspension, click **Reschedule Suspend**.

Suspend now

This option allows you to suspend the server immediately. When the server suspends in this manner, it automatically disconnects all FTP users and disables any connections. FTP users cannot make any further requests. Users are not issued a warning with this option. The Administration Tool server continues to run.

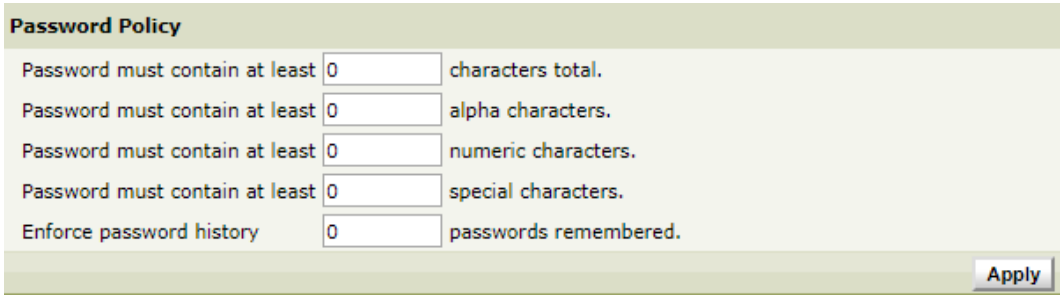
1. Select **Setup > Miscellaneous** to and view the *FTP/HTTP Server Suspend Options* pane.
2. Click **Suspend Now**.

Password policy

Use this to define a set of requirements that users need to comply with when they change their passwords. You can set the minimum number of characters as well as require the minimum number of letters, numbers, and special characters.

Specify password policy

1. Select **Setup > Miscellaneous** and view the *Password Policy* pane.



2. Specify the desired values in the fields of the *Password Policy* pane.
   - **Password must contain at least [*n*] characters total** – the minimum number of characters that the password must contain. Set *n* = 0 for no minimum number of characters.
   - **Password must contain at least [*n*] alpha characters** – the minimum number of letters that must be in the password. Set *n* = 0 for no minimum number of letters in the password.

- **Password must contain at least [*n*] numeric characters** – the minimum number of numeric characters that must be in the password. Set *n* = 0 for no minimum number of numbers in the password.
- **Password must contain at least [*n*] special characters** – the minimum number of special characters (anything other than letters or numeric characters) that must be in the password. Set *n* = 0 for no minimum number of special characters in the password.
- **Enforce password history [*n*] passwords remembered** – the number of the last *n* stored passwords which are restricted for reuse; should be less or equal to 50. Set *n* = 10 to have the last 10 passwords stored and restricted for reuse upon a password change attempt. Set *n* = 0 to bypass this restriction.

  Note SecureTransport stores the last 50 passwords of an user regardless of the value set in the **Enforce password history** field.

- **Minimum password age [*n*] days** – the minimum number of days until next allowed password change. This restriction applies when a user changes their password and ends after expiration of the configured *Minimum password age* period. Enter a positive integer value to define the number of days when a user will not be allowed to change their password. Set *n* = 0 to apply no *Minimum password age* restriction.

  Note The configured *Minimum password age* restriction does not apply when a SecureTransport administrator changes the password of another user or administrator account. Also, the policy does not apply when a user's or administrator's password expires or if they are forced to change their passwords. However, this restriction does apply when a SecureTransport administrator changes their own password.

3. Click **Apply.**
4. Restart the HTTP server on both the SecureTransport Server and the SecureTransport Edge.

If you are using a streaming setup and you change the password policy while a user is logged into SecureTransport, the old password policy is displayed in the Browser Client when a user tries to change the password.

If you are using an Enterprise Cluster and you change the password policy, a TM restart is required on all nodes of the cluster to apply the changes.

Bandwidth limits

Note Bandwidth limits apply to transfers over the following protocols: HTTP, FTP and SSH. These limits do not affect PeSIT and AS2 transfers.

You can set the global Bandwidth Limits on this panel. You set bandwidth limit for inbound and outbound transfers in kilobytes per second per user account. Apart from global bandwidth limits, you can apply a hierarchy of bandwidth limits on business unit, account template and individual account level.

The hierarchy works in the following way: *global > business unit > account*. Account is on the same level as account template but note that limits set on the account level override global and business unit configurations.

When you add a zero for either limit, no bandwidth limits are applied.

ICAP settings

The Internet Content Adaptation Protocol (ICAP) settings allow the administrator to configure ICAP engines to be used as part of the SecureTransport file transfer processes so that data loss prevention (DLP) is achieved and anti-virus (AV) scans are completed. SecureTransport allows the administrator to use the ICAP connector to set up a SecureTransport server to scan (with external DLP engine) files and AdHoc messages when delivering them to the recipient folder or mailbox. ICAP server scan is executed when a file is going to be (therefore before it is) delivered.

Prior to configuring ICAP scanning, verify that ICAPScan is enabled. For information on enabling ICAPScan, refer to *Enable a rules package* on page 208.

Note The SecureTransport administrator can edit the entire DLP/AV ICAP URL in the following format `icap://dlpav-address:port/servicename`. Both the Symantec anti-virus AVSCAN and AVSCANREQ are supported, though AVSCANREQ is preferred.

Note SecureTransport will scan received AdHoc messages and attachments when recipients open a message or download an attachment.
- An AdHoc message, identified as blocked by the DLP policy, will be displayed but the content will be changed to a notification stating that you are not allowed to view this message because it was blocked by the DLP policy. Subjects of messages remain changed.
- When downloading message attachments, identified as blocked by DLP policy, they will be successfully downloaded but the content will be changed to a notification stating that you are not allowed to view the file because it is blocked by the DLP policy. This applies for all file types regardless if they are text files or not. File extensions will not be changed.

The ICAP Server(s) provide

- Multiple ICAP servers
- Incoming and outgoing ICAP scanning for all file and message transfers
- Scanning policy support
- ICAP headers reporting: `X-Authenticated-User`, `X-Client-IP`, `X-Server-IP`

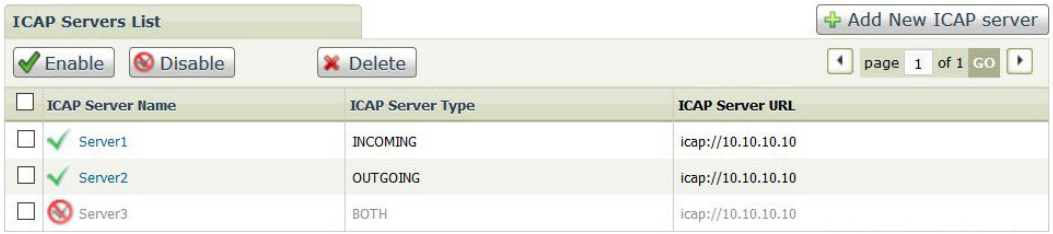
Note X-Server-Icap header reports the SecureTransport local IP address with each scanning request. If multiple network interfaces are available on the machine, the reported IP may not match the actual one.

- Custom HTTP headers reporting
- Certain variables are now exposed to Advanced Routing

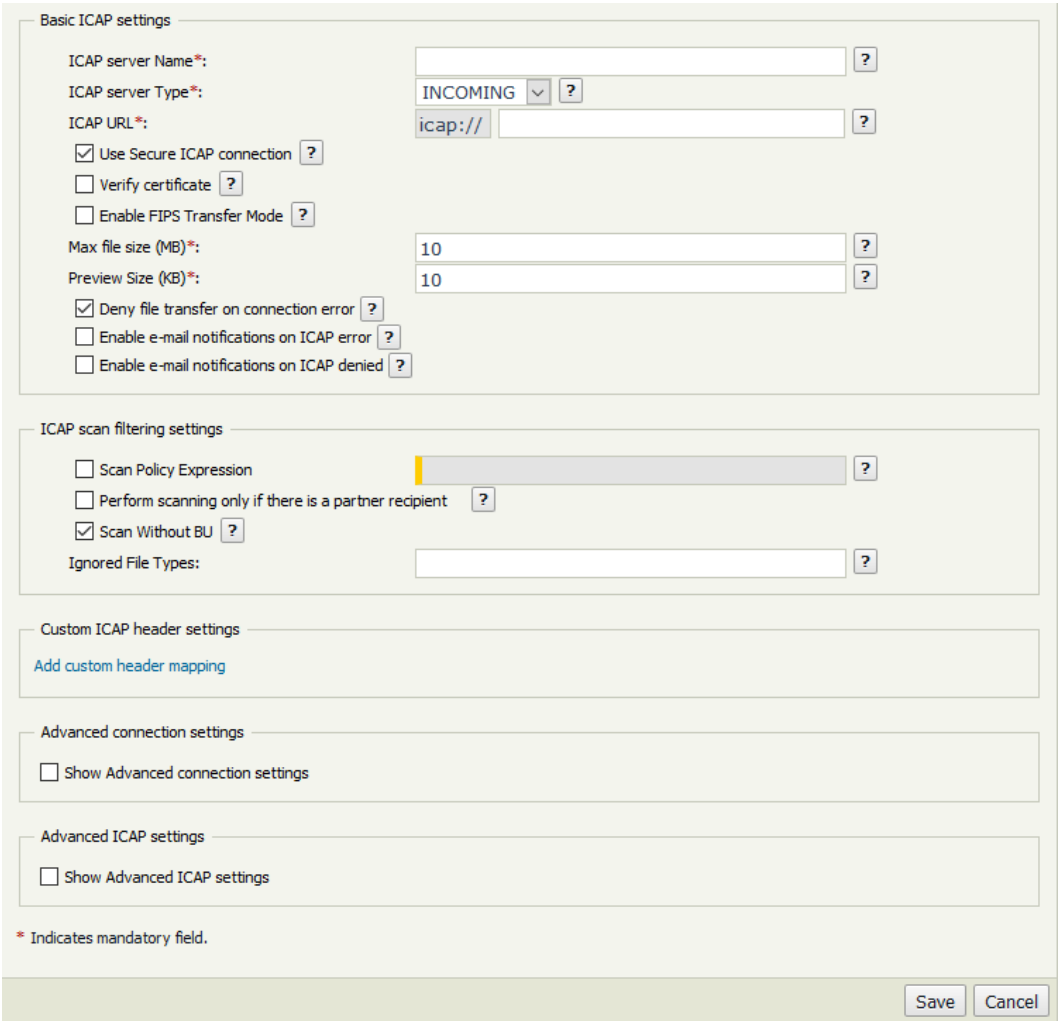
Setup of ICAP servers

Multiple ICAP servers can be configured. There is no limitation about the number of servers. Scanning will be performed only by ICAP servers which are enabled. There will be no prioritization – all the servers will be used for scanning files and messages. If a server along the chain returns a negative result from scanning - the other servers will not be used and the transfer will be denied.

Navigate to **Setup** > **ICAP Settings**. The *ICAP Servers List* page presents a list of ICAP servers with basic management controls plus the option to create (add) a new server.



Click **Add new ICAP server** to open the *ICAP Server Settings* page with multiple sets of options.



Basic ICAP settings

- Enter the **ICAP server name**. It must be unique and there cannot be two ICAP servers with the same name.
- Enter the **ICAP server type**. It can be INCOMING, OUTGOING or BOTH.
    - **INCOMING** means that scanning will be performed by this ICAP server for all Incoming transfers: File upload, AdHoc message creation, Server-initiated pull (for example from a Transfer Site)
    - **OUTGOING** means that scanning will be performed by this ICAP server for all Outgoing transfers: File download, Reading of an AdHoc message, Server-initiated push (for example in the Advanced Router step: Send to Partner or Publish to Account)
    - **BOTH** means that scanning will be performed by this ICAP server for all types of transfers
- Enter the **ICAP URL**. Enter the DLP/AV ICAP URL in the following format:
  `icap://dlpav-address:port/servicename`
  The `servicename` can be the same as the mode of operation - `REQMOD` or `RESPMOD`, or something custom and vendor-specific.
  For the exact `servicename`, refer to the Data Loss Prevention (DLP) or Anti-virus (AV) documentation.
  If the default ICAP port (1344) is used, leave the port blank - it will be auto-populated.
  Examples:
  `icap://dlpav-address:1344/AVSCAN`
  `icap://dlpav-address:1344/REQMOD`
  `icap://dlpav-address:1344/RESPMOD`
    - **Use Secure ICAP connection** for a secure connection to the ICAP server.
    - Select **Verify certificate** to use certificate verification to secure the connection to the ICAP server.
    - Select **Enable FIPS Transfer Mode** to enable transfers to the ICAP server to be in accordance with the Federal Information Processing Standard (FIPS).
      Note: Verify certificate and Enable FIPS Transfer Mode can be selected together or individually depending on the level of security needed for the ICAP server connection.
- Enter **Max file size** (MB).
  The default maximum file size is 10 MB. If the actual file size is larger than the maximum file size, SecureTransport will send up to the maximum configured file size to the ICAP server.
- Enter **Preview Size** (KB).
  The default preview size is 10 KB. If the ICAP server requires more data, SecureTransport will send it up to the maximum configured file size.
    - Select **Deny file transfer on connection error**.
      If the **Deny file transfer on connection error** option is selected, file transfers will be denied on a connection error to the ICAP server
    - Select **Enable e-mail notifications on ICAP error**.
      If the **Enable e-mail notifications on ICAP error** is selected, notification emails will be sent when there is a connection failure to the ICAP server.

- Select **Enable e-mail notifications on ICAP denied**.
  If the **Enable e-mail notifications on ICAP denied** is selected, notification emails will be sent when there is a deny by the ICAP server.

ICAP scan filtering settings

Select **Scan Policy Expression** if you want to perform scanning only under specific circumstances. When you select the **Scan Policy Expression** checkbox, the text box field allows you to use SecureTransport Expression Language. If both settings are disabled, scanning will always be performed. Sample usage - do not scan if the transfer is taking place over SSH protocol:
`${session.protocol ne 'ssh'}`
Refer to the *ICAP scan policy expression language* on page 195 subtopic for the complete list of available expressions.

Select **Perform scanning only if there is a partner recipient**.
This field enables or disables ICAP scanning for AdHoc messages if at least one of the recipients is external. User type - *internal* or *external*- is controlled by the account setting **Account Type**. Possible values are **Internal** - internal accounts - and **Partner** - external accounts.
If the type of a recipient cannot be identified or is set to **Unspecified**, the account will be considered **External**. If both the filtering settings are enabled, this particular setting will be applied over AdHoc messages.

Select **Scan Without BU** to choose whether or not to enable ICAP scanning for accounts with no Business Unit assigned.

Ignored File Types Enter a list of file extensions, separated by comma. Files with these extensions will not be scanned.

Custom ICAP header settings

This allows you to specify any additional custom headers that must be passed to the ICAP server when making requests, along with their values. The **Header value** fields can either have a static value or a ST expression-based one. Expressions allow you to dynamically set a value, based on a specific context, by utilizing the SecureTransport session or environment variables.
By default, there aren't any custom headers configured, but you can add any number of headers by selecting **Add custom headers mapping**.
If a header value is not present or can’t be resolved, the header will be added with an empty or null value, when sending the request.
Example:

- Header Name: `X-Account-Name`
- Header Value: `${account.name}`
- If a user with name - user1 has logged in and the ICAP scan is performed, the `Header:Value` will be evaluated to `X-Account-Name = user1` and it will be reported to the ICAP server (s).

Advanced connection settings

- By selecting **Show advanced connection settings** you can see the additional server configuration options for connection.
- **Connection timeout**. This is the maximum connection timeout in seconds that the server will wait until it stops trying to reconnect.
- **Read timeout**. This is the maximum read timeout in seconds.
- **Enabled Ciphers**. This is a list of ciphers to be used for an SSL connection. The ciphers must be comma-separated. The default ciphers are:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,
  TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,
  TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_EMPTY_RENEGOTIATION_INFO_SCSV
- **Enabled Protocols**. This is a list of SSL protocols to be enabled. The protocols must be comma separated. The default value is: TLSv1.2.

Advanced ICAP settings

- By selecting **Show advanced ICAP settings** you can see the additional server configuration options.
  - Select **Enable WindowsNt format**. With this setting you can choose whether or not to report X-Authenticated-User in WinNT format in case of LDAP authentication.
  - X-Authenticated-User
    X-Authenticated-User is reported with each LDAP request. The header is reported differently depending on user type. Below are the supported X-Authenticated-User formats:
    - User with a local account and a locally stored password: Local://<account name>
    - Real OS user: Local://<login name>
    - Non LDAP user mapped to a template (SiteMinder or SSO): Local://<login name>

- LDAP user options:
  - If WinNT format is not enabled for the server: LDAP://<LDAP domain name>/<user DN>*
  - If WinNT format is enabled for the server: WinNT://<LDAP domain name>/<login name>

    Note For more information about user DN format, see *User DN format* on page 194.

- Select **Stop transfers modify or not handled** to choose whether or not to stop the transfer if ICAP server returns a MODIFY result or an unhandled status.
- Select **Treat modify as Block** to choose whether or not to treat the ICAP MODIFIED action as block.

- To enable or disable an ICAP server, mark the preferred ICAP server and select the **Enable** or **Disable** button.
- To delete an ICAP server, mark the preferred ICAP server and select the **Delete** button.
- To edit an ICAP server, click on the record in the list of ICAP servers displayed on the page.

ICAP legacy system import and upgrade

Mapping between old ICAP options and new ICAP server during legacy system import and upgrade from 5.3.6 GA to 5.4:

ICAP Server	Old Configuration option
`icapServer.connectionTimeout`	`icap.First/SecondServer.ConnectTimeout`
`icapServer.enabledCiphers`	`icap.First/SecondServer.EnabledCipherSuites`
`icapServer.enabledProtocols`	`icap.First/SecondServer.EnabledProtocols`
`icapServer.fipsEnabled`	`icap.First/SecondServer.enableFipsMode`
`icapServer.scanWithoutBu`	`icap.First/SecondServer.enableScanForAccountsWithoutBusinessUnit`
`icapServer.useSecure`	`icap.First/SecondServer.enableSecureConnection`
`icapServer.ignoredFileTypes`	`icap.First/SecondServer.IgnoredFileTypes`

icapServer.mailAddressesOnIcapError	icap.First/SecondServer.mailtoAddressesForMailsIfIcapErrors
icapServer.mailAddressesOnIcapDenied	icap.First/SecondServer.mailtoAddressesForMailsIfTransferDeniedByIcap
icapServer.maxSize	icap.First/SecondServer.MsgMaxSize
icapServer.previewSize	icap.First/SecondServer.PreviewSize
icapServer.readTimeout	icap.First/SecondServer.ReadTimeout
icapServer.enabled	icap.First/SecondServer.ScanEnabled
icapServer.sendEmptyPreview	icap.First/SecondServer.sendEmptyPreview
icapServer.notifyOnIcapErrors	icap.First/SecondServer.sendMailsIfIcapErrors
icapServer.notifyOnIcapDenied	icap.First/SecondServer.sendMailsIfTransferDeniedByIcap
icapServer.denyOnConnectionError	icap.First/SecondServer.stopTransfersIfIcapErrors
icapServer.stopModifyOrNotHandled	icap.First/SecondServer.stopTransfersIfIcapResultModifyOrNotHandled
icapServer.treatModifyAsBlock	icap.First/SecondServer.treatModifyAsBlock
icapServer.url	icap.First/SecondServer.Url
icapServer.certVerify	icap.First/SecondServer.verifyCertificate
icapServer.id	runtime generated value
icapServer.enableWinNtFormat	false (0)

icapServer.headersMapping	NULL
icapServer.name	Name mapping (ex. i_cap.FirstServer.Url_FirstServer)
icapServer.scanOnlyIfPartnerRecipient	false (0)
icapServer.scanPolicyExpression	NULL
icapServer.type	INCOMING
icapServer.customAttributesId	NULL

On legacy system import:

- If the value of configuration option FirstServer.Url_ is not empty, the new ICAP server entity with name FirstServer _ will be created, if an ICAP server with the same name exists - the legacy system import will fail.
- If the value of configuration option SecondServer.Url_ is not empty, the new ICAP server entity with name SecondServer_ will be created, if an ICAP server with same name exist - the legacy system import will fail.

On upgrade from 5.3.6 GA:

- If the value of configuration option icap.FirstServer.Url is not empty, the new ICAP server entity with name FirstServer will be created.
- If the value of configuration option icap.SecondServer.Url is not empty, the new ICAP server entity with name SecondServer will be created.

User DN format

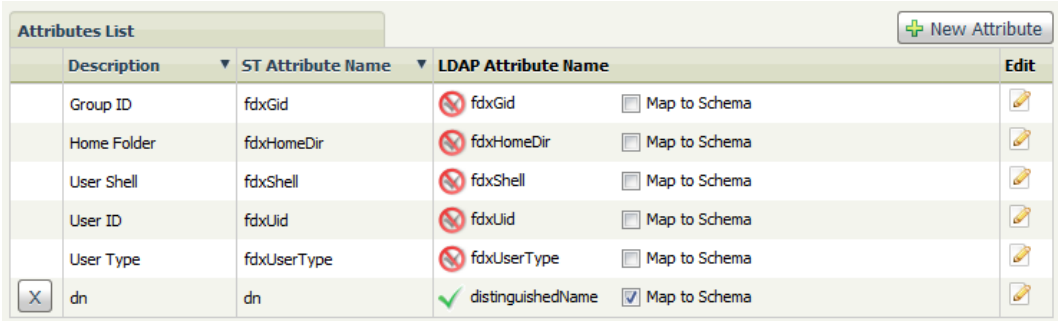
User DN is reported when authenticating over LDAP. There are 2 supported formats for User DN.

If no additional configuration is performed user DN contains the exact attribute containing the user login name, for example: LDAP://elf/CN=test

User DN can be configured to contain the full DN of the logged in user or the value of any existing LDAP attribute. Below are the configuration steps:

1. Navigate to the desired LDAP domain.
2. Go to the **Attributes List** section.
3. Add a new attribute with an **ST Attribute Name** that equals DN.

4. The value of the **LDAP Attribute Name** can be any LDAP attribute. To display the complete DN of the logged in user, type in the attribute that contains the complete DN of the logged-in user. (for example `distinguishedName`).
5. Click **Map to Schema** and save.
   Example:
   `LDAP://userDirectory/CN=exampleuser,CN=Users,DC=example,DC=com`



ICAP scan policy expression language

This topic provides the expression language and variable available with the ICAP **Scan Policy Expression** option part of the **ICAP scan filtering settings**.

The samples are distributed in dedicated subtopics, as follows:

- *Transfer-related expressions* on page 196
- *Session-related expressions* on page 196
- *LDAP-related* on page 197
- *HTTP-related expressions* on page 197
- *Flow attributes expressions* on page 197
- *Account-related expressions* on page 198
- *User-related expressions* on page 199
- *Business Unit-related expressions* on page 199

Note All the environment variables that are styled in *`italics`*, depend on user input and the values shown in the tables are only sample. For more detailed examples about expression language usage, see *Custom Expression Language functions and variables* on page 921.

Transfer-related expressions

Transfer-related	
Expression	**Possible/Sample Values**
transfer.targetDirFull	/stusers/sthome/acc1/ The path to the transferred file current directory
transfer.transferredBytes	10 The amount of bytes transferred
transfer.startTime	1520951365644 The difference, measured in milliseconds, between the time the transfer has started and midnight, January 1,1970 UTC
transfer.endTime	1520951366212 The difference, measured in milliseconds, between the time the transfer has ended and midnight, January 1, 1970 UTC
transfer.xferType	'A' – stands for ASCII 'I' – stands for Binary
transfer.targetDir	/ The root directory of the TARGETPATH

Session-related expressions

Session-related	
Expression	**Possible/Sample Values**
session.protocol	HTTP, FTP, SSH, Routing, AS2, PESIT
session.remoteAddress	10.134.12.224 The IP address of the machine from which the transfer has been initiated
session.remoteHost	10.232.15.109 The IP of the ST server that performed the scanning
session.streamingClient	Server, HTTPD, FTPD, SSHD

Session-related	
session.isSSL	0,1
session.siteProtocol	AS2, FTP, HTTP, SSH, PeSIT, FM, SystemToHuman, SharePoint

LDAP-related

LDAP-related	
Expression	**Possible/Sample Values**
ldap.attributes['ATTRIBUTE_NAME'] or *ldap.attributes.ATTRIBUTE_NAME*	ldap.attributes.mail where ATTRIBUTE_NAME stands for any exported LDAP attribute
ldap.domainName	ldapDomain The name of the domain to which a user has been logged in
ldap.dn	cn=mike.smith The distinguished name for that LDAP server
ldap.authByEmail	0, 1

HTTP-related expressions

HTTP-related	
Expression	**Possible/Sample Values**
http.headers['HEADER_NAME'] or *http.headers.HEADER_NAME*	http.headers.myHeader where 'myHeader' is the name of any available HTTP header

Flow attributes expressions

Flow attributes	
Expression	**Possible/Sample Values**
flow.attributes['userVars.NAME'] or *flow.attributes.userVars.NAME*	Flow.attributes.userVars.name By replacing NAME with a value any additional attribute declared in user account userVars and any flow attribute declared in subscriptions userVars can be retrieved

Account-related expressions

HTTP-related	
Expression	**Possible/Sample Values**
account.disabled	0, 1
account.email	acc1@aa.bb The email of the account
account.name	acc1 The name of the account
account.notes	Notes The notes of the account
account.type	template, service, user, unlicensed
account.home	/stusers/sthome/acc1 The path to the account home directory
account.attributes.transferType	'N' – stands for Unspecified 'I' – stands for Internal 'E' – stands for Partner
account.attributes['ATTRIBUTE_NAME'] or *account.attributes.ATTRIBUTE_NAME*	account.attributes.transferType where ATTRIBUTE_NAME stands for any account custom property

User-related expressions

User-related	
Expression	**Possible/Sample Values**
account.user.loginName	acc1 The user login name
account.user.type	virtual, real, sso, siteminder
account.user.class	VirtClass The user class name
account.user.gid	1000 The user unique group identifier by which its belonging to a group of users is determined
account.user.uid	1000 User account unique identifier

Business Unit-related expressions

Business Unit-related	
Expression	**Possible/Sample Values**
account.businessUnit.name	bu1 The name of the business unit to which the account is related

Transaction Manager

The Transaction Manager is an event-based rules engine that provides Axway SecureTransport Server with extensible server-side functionality used for process automation and real-time delivery of data. This topic describes how to use the Transaction Manager to create and manage rules.

Note SecureTransport does not automatically copy changes made under the **TM Settings** menu to other servers in your Enterprise Cluster (EC), so you must deploy a new or changed rules package and enable or disable a rules package on all servers in the cluster. Typically you modify rules and develop applications on a development server and use export and import to deploy them after you test them.

Note Transaction Manager Administration Tool edit function is deprecated and removed for SecureTransport 5.4.

Select **Setup > TM Settings** to display *TM Settings* page.

The following topics describe managing Transaction Manager rules, rules packages, and agents:

- *Rules* on page 201
- *Built-in rules packages* on page 202
- *Manage rules packages* on page 207
-
- *Export a rules package* on page 209
- *Import a rules package* on page 209
- *Install agents or functions* on page 211

Rules

You can define sets of actions that execute when a set of conditions are met. This set of actions and conditions is called a *rule*. Rules in SecureTransport are bundled into *rules packages*. Rules packages consist of a collection of rules that are applicable to a business process.

The Transaction Manager is an event-based rules engine. You can replace existing rules to modify SecureTransport Server functionality and create new rules to extend SecureTransport Server functionality to implement process automation and real-time delivery of data. Transaction Manager rules implement secure file transfer as an integrated part of a custom or third-party solution.

Rules overview

Rules consist of a name, the precedence setting, conditions, and actions.

- Rule Name – A descriptive identifier to distinguish the rules in a rules package.
- Precedence – A number higher than 0 used to determine which rules are executed when the conditions match more than one rule. The lower the number, the higher the priority. Rules with the highest precedence are executed. For example, a rule with a precedence of 50 is executed instead of a rule with a precedence of 100. If two rules have the same precedence value, the rules execute sequentially in no particular order. You can use NextPrecedence along with precedence values to help organize the order in which rules execute.

  Note If you need to have multiple actions fire in a certain order under the same set of conditions, you should use one rule with multiple actions in sequence.

- Condition – A condition is a logical expression that contains a comparison condition or a condition function. A condition can examine events and event attributes.
- Action – An action is a set of agents that are triggered when certain conditions are met. Actions can be either agents written in Java which allow in-process sharing of information between agent invocations or an external mechanism used to integrate with agents written in scripting languages, such as Perl or Python. Such actions can be performed through a shell mechanism.

When a user accesses SecureTransport Server or SecureTransport Edge, the Transaction Manager receives events from the SecureTransport Server. Depending on the event, the Transaction Manager selects the rules, matches them, and then executes them.

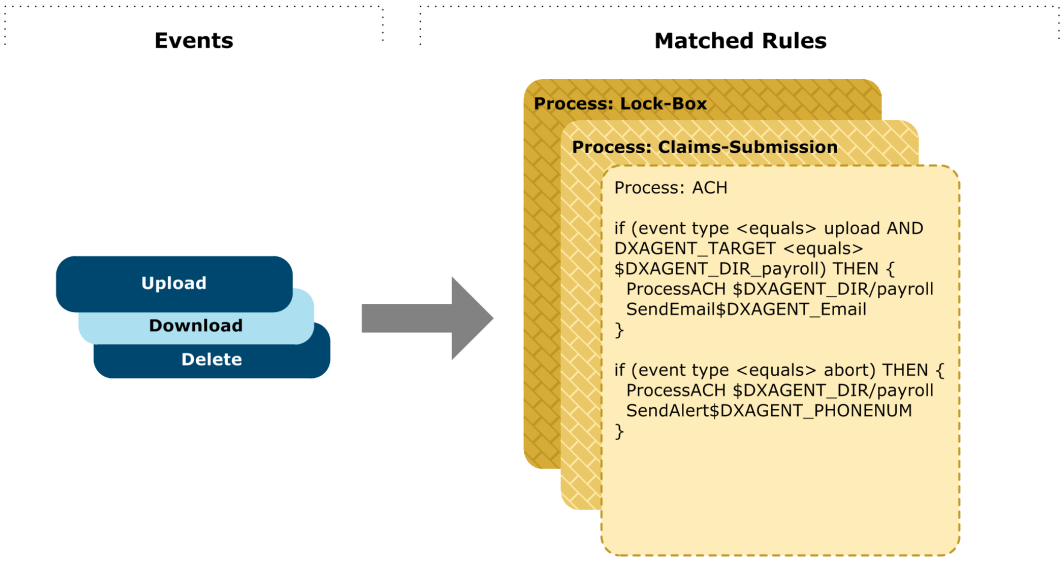


Figure 3. Example events and matched rules

Define a rules package

Use the following procedure to define a rules package.

1. Determine the events that should trigger the rule.
2. Determine the event attributes that are relevant to the rule.
3. Specify conditions associated with event attributes you want to select and combine them with logical expressions such as, AND and OR.
4. Outline the set of actions to be taken if the conditions are matched as specified.

Note Rule packages must be created using an external XML editor and imported onto the SecureTransport Server. For instructions on importing rules packages, refer to *Import a rules package* on page 209.

Built-in rules packages

SecureTransport ships with several predefined rules packages. These packages contain rules used by SecureTransport as part of the standard functionality of the product. Because these rules and packages are part of the product, it is very important that you do not delete or modify the rules or the rules packages. This topic provides a list of the built-in packages and explains their uses.

Streaming

The following packages control much of the functionality involved with authenticating users and executing transfers. Streaming and InStreaming packages contain the default functionality optimized for performance in the current release.

- Streaming
- InStreaming

Server-initiated transfers

The following packages call agents when a server-initiated transfer is executed. Each rules package represents a different protocol.

- FolderTransfer
- FtpTransfer
- HttpTransfer
- Pesit
- PesitTransfer
- SshTransfer
- STAS2

Note The STAS2 package provides AS2 functionality including file transfer and handling of receipts.

Ad hoc transfers

The following packages support ad hoc file transfers:

- AddressBook
- PackageManager

Applications

The following packages calls the agents used in the corresponding built-in application types:

- AdvancedRouting
- ArchiveMaintApp
- AuditLogMaintApp
- AxwaySentinel
- AxwayTransferCFT
- BasicApp
- FileServicesInterface
- HumanSystem
- LogEntryMaintApp
- PackageRetentionMaintApp
- SharedFolder

- SiteMailbox
- StandardRouter
- TransferLogMaintApp
- UnlicensedAccountMaintApp

The rules are required to trigger the application agent.

Permission checking

InPermissionCheck represents an implementations of checking file permissions before allowing SecureTransport operations to continue.

InPermissionCheck contains an in-process Java agent. It's efficient and provides basic check based on UID/GID and the file permission flags. For details, see *Access control* on page 706.

- InPermissionCheck

Other packages

The following packages handle specific SecureTransport functionality.

The following topics describe the other Transaction Manager rules packages:

- *ArchiveAgent* on page 204
- *Axway Sentinel* on page 205
- *ConnectDirectTransfer* on page 205
- *FileServicesInterface* on page 205
- *ICAPScan* on page 205
- *MDNReceipting* on page 205
- *Pesit and PesitTransfer* on page 206
- *PGPTransform* on page 206
- *Resubmit* on page 206
- *SendToSite* on page 206
- *ServerTransferNotify* on page 206
- *SNMPTransferNotify* on page 206
- *WebServicesAPI* on page 207

ArchiveAgent

Use this package to archive transferred files. This package is enabled by default. The package copies each transferred file to the archive directory specified in the global File Archiving configuration page. Copied files are renamed to a unique file name to avoid duplicates. The file name format is:

```
<File_name><unique_file_name_modifier>
```

For example:

```
1223375981000_12233759819160.08926095676257206
```

The location of the files is as follows:

```
<archive_folder>/<account_name>/<login_name>/<relative_path_to_
file>/<archived_file>
```

Where:

- `archive_folder` - The archive folder location configured in the global File Archiving configuration page.
- `account_name` - Name of the account who performed the transfer. When there's no account (for LDAP users for example), account_name has value of NO_ACCOUNT.
- `login_name` - Login name for the user who performed the transfer.
- `relative_path_to_file` - Path to the file relative to the account's home folder.

For more information, see *Create an Archive Maintenance application* on page 760 and *File archiving global configuration* on page 213 .

Axway Sentinel

This package is enabled by default. SecureTransport uses it to send file transfer and processing events to Axway Sentinel and to call the agent used in a Axway Sentinel Link Data Maintenance application. For more information about configuring SecureTransport to send events to Sentinel, see *Integrate Axway Sentinel* on page 109.

ConnectDirectTransfer

Enable this package when you want to create and use a Connect:Direct transfer site. This package is disabled by default. For more information, see *Connect:Direct transfer sites* on page 505.

FileServicesInterface

This package is used to implement transfers initiated by SecureTransport using a file services interface protocol.

ICAPScan

This package is used to implement anti-virus or DLP scans initiated by SecureTransport using external ICAP servers. The package is disabled by default and must be enabled if ICAP servers are configured.

MDNReceipting

This package provides functionality to generate MDN receipts for the transferred files. The package is enabled by default.

Note To generate MDN receipts, create an `mdn` certificate in addition to enabling the MDNReceipting package. For more information about the `mdn` certificate, see *Certificates to generate during initial setup* on page 69.

Pesit and PesitTransfer

These packages provide the functionality for PeSIT protocol operations, including authentication, server-initiated transfers, client-initiated transfers, routed transfers, and acknowledgments. They are enabled by default.

PGPTransform

This package handles PGP encryption and decryption when Advanced Routing is not used. The package is enabled by default.

Resubmit

This package contains rules for canceling events. It is enabled by default.

SendToSite

Use this package when you want to upload files to a specific site without subscribing an account to an application. This package is disabled by default. This package is used with the **Send Files Directly To** option. For details, see *Subscribe an account to an application* on page 607.

In order to use `SendToSite` package, enable it and modify its content. For example, by adding a transfer site name as a value to the Site parameter. For details, refer to *Manage rules packages* on page 207.

ServerTransferNotify

This package implements HTML email notification for file transfers. This package is disabled by default. For more information, see *Velocity email notification package* on page 1041.

SNMPTransferNotify

This package implements SNMP notifications for failed transfers. This package is disabled by default.

SecureTransport includes support for Simple Network Management Protocol (SNMP) v2 and v3 to help you monitor failed transfers. SecureTransport works with SNMP managers such as Hewlett-Packard OpenView Network Node Manager. You can send messages when file transfers fail after retrying the transfer the number of times allotted. SecureTransport provides a trap MIB file located at `<FILEDRIVEHOME>/conf/Transfer.mib`.

1. Select **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.

2. Search for `TransactionManager.SNMP.enabled` and change the value to `true`.

3. Search for `TransactionManager.SNMP.ManagerHost` and change the value to the IP address of the SNMP manager.
4. Search for `TransactionManager.SNMP.ManagerPort` and change the value to the port of the SNMP manager.
5. Set the other `TransactionManager.SNMP.*` server configuration parameters as required by your SNMP manager and configuration
6. Select **Setup > TM Settings**.

   The *Rules Packages* page is displayed.
7. Click **Enable SNMPTransferNotify**.
8. Select **Operations > Server Control**.
9. Restart the **TM Server**.
10. Repeat steps 6 through 9 on each server in your cluster.

WebServicesAPI

This package supports the REST web service file transfer API.

Manage rules packages

Rules packages are a collection of rules applicable to a business process.

Managing rules packages consists of:

- Enabling and disabling rules packages
- Creating Rules Packages
- Editing Rules Packages
- Importing and Exporting Rules Packages

To work with rules, you must login to the SecureTransport Administration Tool as a system administrator with the appropriate privileges and access the **Admin UI > Setup > TM Settings** page.

Note All changes to rules packages are local to the SecureTransport server you are logged in to. For an Enterprise Cluster (EC), you typically develop and modify rules packages on a development server, test them, export them, and import them on the production servers.

Enable a rules package

Use the following procedure to enable a rules package or packages.

1. Select **Setup > TM Settings** to display *TM Settings* page.
2. In the **Select** column, select the Disabled rules package or packages to enable.
3. Click the **Enable** button.

Disable a rules package

Use the following procedure to disable a rules package or packages:

1. Select **Setup > TM Settings** to display *TM Settings* page.
2. In the **Select** column, select the Enabled rules package or packages to disable.
3. Click the **Disable** button.

Export a rules package

Use the following procedure to export a rules package or packages.

1. Select **Setup > TM Settings** to display *TM Settings* page.
2. In the **Select** column, select the rules package or packages to export.

   If only one rules package is selected, the rules package will be exported as a XML file.

   If multiple rules packages are selected, the rules packages will be exported as a ZIP file.
3. Click **Export**.
4. Select the **Save As** option from the **File** menu of the new browser window.

   The *Save As* dialog box is displayed.
5. Select the directory in which you want to save the rules package or packages.
6. Type an appropriate name for the rules package.
7. Click **Save**.

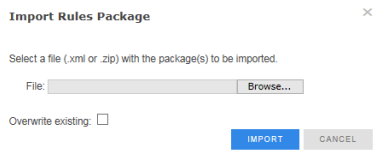
Import a rules package

Use the following procedure to import a rules package.

1. Select **Setup > TM Settings** to display *TM Settings* page.
2. Select **Import** on the *TM Settings* page.

   Note The XML of ZIP file used to import rules packages must be well formatted. Importing an XML file with the XML elements in a single line causes the import to fail. If the import fails, an error message is written to tm.log and the rule are unavailable to execute at runtime.

   The *Import Rules Package* screen opens.



3. **Browse** and select a file (XML or ZIP) with the packages to be imported.
4. (Optional) Verify to overwrite existing rules packages by selecting **Overwrite existing**.
5. Select **Import** on the *Import Rules Package* screen.

The server checks if the file is a valid XML file or if the ZIP file contains valid XML files. If the file is a valid XML file or if the ZIP file contains valid XML files, the Rules Packages are displayed. If the file is not a valid XML file or if the ZIP file does not contain valid XML files., an error message is displayed.

Create a rules package

Rules packages are a collection of rules applicable to a business process. To create rules, you must first define a rules package.

You must create rules packages externally and import them into the SecureTransport Administration Tool. For a detailed explanation of each step in this procedure, refer to the following topics.

1. Create a rules package.
2. Add the arguments that need to be passed to the rule.
3. Specify rule comparisons and conditions for the rule.

   Conditions are event-based clauses that permit you to compare attribute values or functions that return a logical value.
4. Insert clauses to add multiple comparisons and conditions.

   Conditions can be composed of multiple clauses that are combined as logical expressions with the use of AND, OR, or NOT. These clauses can be nested to provide more complex rule processing.
5. Add an action to rule.

   Actions specify agents that are triggered depending on the result of a condition. A condition can trigger in-process agents or external agents.
6. Save the rules package.
7. Import the rules package into the SecureTransport Administration Tool as described in the above subtopic.

Edit a rules package

A rule consists of conditions and actions. You can add conditions or actions to rules package by exporting the rules package, editing the rules package locally, and importing the updated rules package.

Delete a rules package

Removing a rules package from the server is allowed. Agents referred to by a deleted rules package are not removed. These agents maybe used in other rules packages.

Use the following procedure to delete a rules package or packages.

1. Select **Setup > TM Settings** to display *TM Settings* page.
2. In the **Select** column, select the rules package or packages to delete.

3. Click the **Delete** button.
4. Confirm the deletion.

Install agents or functions

After developing an agent, you must install it to use the agent. An agent can be a script file, a Java class file, or JAR file. In a Standard Cluster (SC) and an Enterprise Cluster (EC), each agent must be installed on each node in the cluster individually.

Note During the install process of Agents or Functions, the recommended file size to be used is up to 40 MB. If the processing time of the uploaded file exceeds 20 seconds the 'Read timed out' error will be displayed.

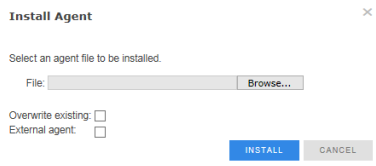
Install an agent

After you have created the external agent file, you must install it in order to use the agent.

Note During the install process a ^M character is appended to each line of the script file. If you are using a Perl or shell script you need to convert the scripts to a UNIX format before installing.

1. Select **Setup > TM Settings** to display *TM Settings* page.
2. Select **Install Agents**.

   The *Install Agents* page is displayed.



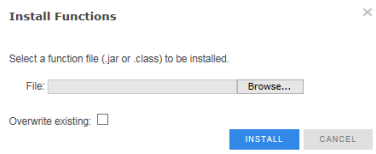
3. Browse your local file system and choose the agent's script file. The agent file formats can be `.jar`, `.class`, `.exe`, `.pl`, and so forth.
4. Select the **External Agent** check box if the external agent you are installing is a `.jar` or `.class` file.
5. Select the **Overwrite existing** check box if existing agents should be overwritten.
6. Click **Install**.

Install a function

After you have created the external function file, you must install it in order to use the function.

1. Select **Setup > TM Settings** to display *TM Settings* page.
2. Select **Install Functions**.

   The *Install Functions* page is displayed.



3. Browse your local file system and choose the function's script file. The function file formats can be `.jar` and `.class`.
4. Select the **Overwrite existing** check box if existing functions should be overwritten.
5. Click **Install**.

File archiving

The file archiving feature enables the archiving and retrieval of files at the global, business unit, and account levels.

The global File Archiving configuration page is found at **Setup > File Archiving**. There you can enable the feature and configure the global archiving policy, the archiving folder, whether or not encryption is required including the encryption certificate, and how long to keep the archived files. To configure the file archiving global configuration, refer to *File archiving global configuration* on page 213.

The file archiving configuration for each business unit can be inherited from the global file archiving configuration or changed for the current business unit. To configure file archiving for a business unit, refer to *Manage business units* on page 692.

For individual accounts the file archiving policy can be inherited or overwritten. To configure the file archiving policy for an account, refer to *Manage accounts* on page 452. File archiving can also be configured for account templates. To configure the file archiving policy for an account template, refer to *Manage account templates* on page 663.

To configure the maintenance schedule for the archive folder, refer to *Create an Archive Maintenance application* on page 760.

Note The file archive folder and user home folders should reside on a separate storage devices. There is a negative performance impact when the archive folder is on the same storage device as user home folders due to writing data twice on the same storage device.

The archived files are stored using a structured archive format so that the following use cases are supported:

- When global archive folder is moved along with its content, the archived files are usable in their new location.
- When account is moved from one business unit to another business unit, the archived files are usable without any additional copying.
- When business unit archive folder is moved along with its content, the archived files are usable in their new location.
- When the business unit archive is moved from the global archive one to a dedicated archive, the archived files are usable without any additional copying.

The files in the structured archive folder are searchable by the following parameters:

- transfer id
- cycle id
- start date
- end date
- account name
- file name
- folder (relative to the account home folder)

The decision whether or not to archive a file is based on the following parameters:

- If an account is configured with archiving on, the file will be archived.
- If an account is configured with archiving off, the file will not be archived.
- If an account is configured with archiving inherited from a business unit and the business is configured with archiving on, the file will be archived.
- If an account is configured with archiving inherited from a business unit and the business is configured with archiving off, the file will not be archived.
- If an account is configured with archiving inherited from a business unit and the business unit is configured with archiving inherited from the global archiving configuration, the global configuration will determine whether of not a file is archived.

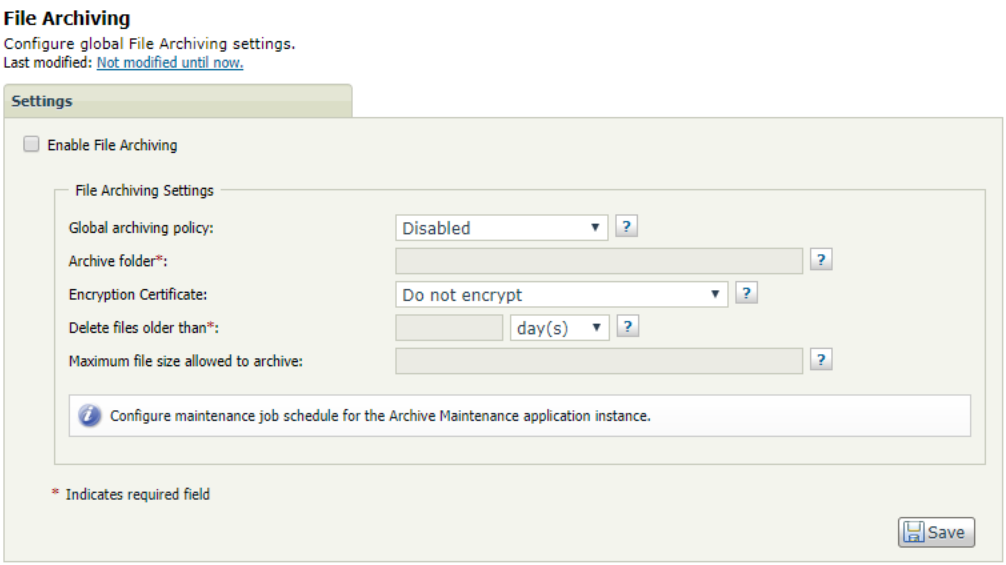
File archiving global configuration

The global file archiving configuration provides the inheritable file archiving configuration for users accounts and business units. For additional information on the inheritance of the file archiving configuration, refer to *File archiving* on page 212

To enable and configure the global file archiving configuration:

1. Navigate to **Setup > File Archiving**.

   The *File Archiving* page is displayed.



2. Select **Enable File Archiving**.

   The additional field and menus on the *File Archiving* page become active.

3. In the *File Archiving Settings* pane:

   a. (Optional) Determine the default *Global archiving policy* to be applied by selecting either **Enabled** or **Disabled**. The default is **Disabled**. The policy configured here can be overridden at Business Unit or Account level.

   b. Complete the **Archive folder** field by entering the absolute path to the global archive folder. The folder location can be overridden at Business Unit level.

   c. (Optional) Determine whether or not to encrypt the global archive folder by selecting **Do not encrypt** or which configured certificate to use for encryption from the *Encryption Certificate* menu. The default is **Do not encrypt**. The chosen certificate can be overridden at Business Unit level. The encryption certificate must be a local x.509 certificate. For information on adding local certificates, refer to *Manage local certificates and certificate signing requests* on page 54.

      Note When you delete or overwrite a certificate which previously was used for encryption, all files encrypted with this certificate will be useless and can't be restored.

      Note When changing the encryption certificate, the Transaction Manager should be restarted in order for the changes to be applied.

   d. Set the options for **Delete files older than** field. You can specify days or hours and any number equal to or greater than 1. Files older than the configured period will be deleted by the maintenance job (if enabled).

   e. Set the **Maximum file size allowed to archive** in Kilobytes. If the file is bigger or equal than the file size limit, it will not be archived. Empty or zero value means that no file size limit applies.

4. Click Save.

Note You must also configure maintenance job schedule for the Archive Maintenance application instance. For information on configuring the Archive Maintenance application instance, refer to *Create an Archive Maintenance application* on page 760.

Note If you disable the File Archiving after being enabled and saved, the fields will stay populated with the old values, so if you enable it again you do not need to enter anything. If a certificate is selected, you cannot delete or overwrite it, even if file archiving is enabled or disabled. If you want to delete or overwrite it, you have to change the certificate option on the *File Archiving* page to another certificate or to **Do not encrypt**.

Communication across Transaction Manager, protocol, and proxy servers

SecureTransport uses a streaming protocol for communication between the protocol servers running on SecureTransport Edge and the Transaction Manager (TM) server running on SecureTransport Server. The streaming protocol abstracts all file transfer protocols and unifies and secures this central communication. When you deploy one or more SecureTransport Edge servers in a peripheral network (DMZ), the deployment is called *streaming* because no file transfer data is stored on the SecureTransport Edge server. The protocol servers translate the protocol they are serving to the streaming protocol but do not read or write files.

With a streaming deployment, the TM Server connects to the protocol servers on the configured SecureTransport Edge servers to establish the connections for the streaming protocol, so no process on a SecureTransport Edge ever makes a connection from the DMZ into the internal secure network. For more information, see *SecureTransport Edge* on page 36. (The TM server and protocol servers running on SecureTransport Server also use the streaming protocol internally.)

Note Unless a number is specified via the corresponding system properties, the number of established streaming connections from Transaction Manager to a single protocol daemon (Admin, FTP, HTTP, and so forth) is calculated with the help of formula: min(20, 2*CPUs)

SecureTransport, when used as a client, can use a proxy server. With AS2 and HTTP/S protocols, any RFC 7231 compliant HTTP proxy is expected to work. With all other protocols, SecureTransport can use the SOCKS5 proxy component of SecureTransport Edge.

You configure the communication between the TM server and protocol servers and access to SOCKS5 and HTTP proxies by defining network zones. Each network zone on a SecureTransport Server can have one or more network zone nodes that define access either within the SecureTransport Server or between the SecureTransport Server and one or more SecureTransport Edge servers. This is also applicable when your implementation uses HTTP proxy servers or the SOCKS5 proxy components of the relevant SecureTransport Edges. The TM Server connects to all protocol servers configured in all network zones. In the configuration of each transfer site, you can select a network zone to specify which proxy (HTTP or SOCKS5 on Edge) will be used for server-initiated transfers through that transfer site. SecureTransport selects a node from the network zone using a load-balancing policy when a server-initiated transfer uses the network zone.

Note Remember that HTTP proxy is only supported with HTTP(S) and AS2 transfer sites. Proxying server-initiated transfers over the other supported protocols (SSH, FTP(S), PeSIT, etc.) requires the use of the SOCKS5 proxy on SecureTransport Edge.

Because you can specify multiple SecureTransport Edge addresses in a node and multiple nodes in a network zone, you can implement any required many-to-many communication between TM servers (on SecureTransport Server nodes) and protocol servers and / or SOCKS5 proxies (on SecureTransport Edge servers).

On a SecureTransport Server, a special network zone named `Private` defines the ports used for internal communication between the TM Server and the protocol servers and the Administration Tool server running on the SecureTransport server.

On a SecureTransport Edge server, there is only one network zone, a special one named `Private` that specifies the ports that the protocol servers listen on for connections from TM servers on SecureTransport Servers. The port number must match the port number configured in the network zone on the SecureTransport Servers that defines the connection to the SecureTransport Edge server. You cannot define more network zones on a SecureTransport Edge server.

Note Do not configure a connection from the SecureTransport TM Server to the SecureTransport Edge ADMIN server.

The following topics describe the streaming deployment and describe managing the Transaction Manager (TM), protocol, and proxy server communication:

- *Streaming deployment* on page 216 - Describes SecureTransport streaming deployment.
- *Manage the communication across Transaction Manager, protocol and proxy servers* on page 218 - Describes managing the Transaction Manager (TM), protocol, and proxy server communication and provides how-to instructions for configuring the Transaction Manager (TM), protocol, and proxy server communication.

Streaming deployment

The following diagram illustrates a streaming deployment with clients and servers in the both the public network and the internal secure network. The arrows show the direction of network connections for all the protocols. Data flows in both directions after the connection made.

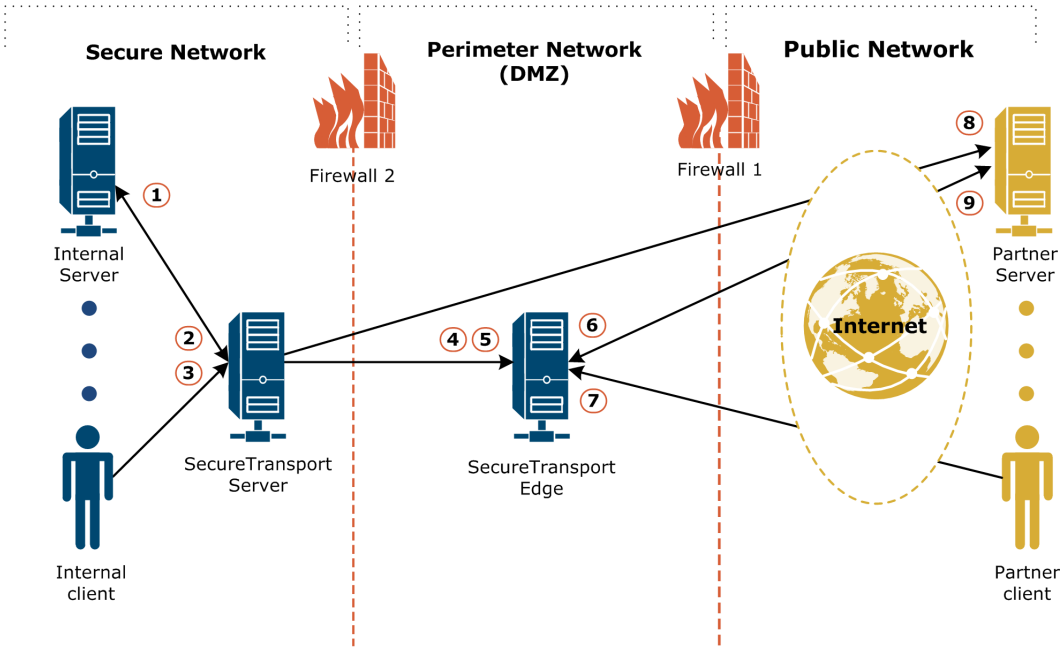


Figure 4. Streaming deployment network connections

Some lines represent two network connections. The connections are labeled as follows:

1. From the SecureTransport Server to an internal server for a server-initiated transfer
2. From an internal server to the protocol servers on the SecureTransport Server for a client-initiated transfers
3. From an internal client to the protocol servers on the SecureTransport Server for a client-initiated transfers
4. From the TM server on the SecureTransport Server to the protocol servers on the SecureTransport Edge so that the protocol servers can stream client-initiated transfers from partners using the streaming protocol
5. From the SecureTransport Server to the SOCKS5 proxy server on SecureTransport Edge for server-initiated transfers
6. From a partner server to a protocol server on the SecureTransport Edge for a client-initiated transfer
7. From a partner client to a protocol server on the SecureTransport Edge for a client-initiated transfer
8. From the SecureTransport Server directly to a partner server for a server-initiated transfer
9. From the SOCKS5 proxy server on SecureTransport Edge to a partner server for server-initiated transfers

The diagram does not illustrate the following network connections that you might need to configure depending on the requirements of your deployment:

- From the TM server to the protocol servers within the SecureTransport Server so that the protocol servers can serve client-initiated transfers from the secure network

- From the SecureTransport Server to a separate HTTP proxy server for server-initiated transfers
- From a separate HTTP proxy server to a partner server for server-initiated transfers
- From the TM server on the SecureTransport Server to the protocol servers and the SOCKS5 proxy server on a SecureTransport Edge in a less restrictive DMZ for internal clients and servers
- From the TM server on the SecureTransport Server to the protocol servers and the SOCKS5 proxy server on a SecureTransport Edge in a DMZ that has a VPN connection to a specific partner

Manage the communication across Transaction Manager, protocol and proxy servers

This topic describes managing the Transaction Manager (TM), protocol, and proxy server communication.

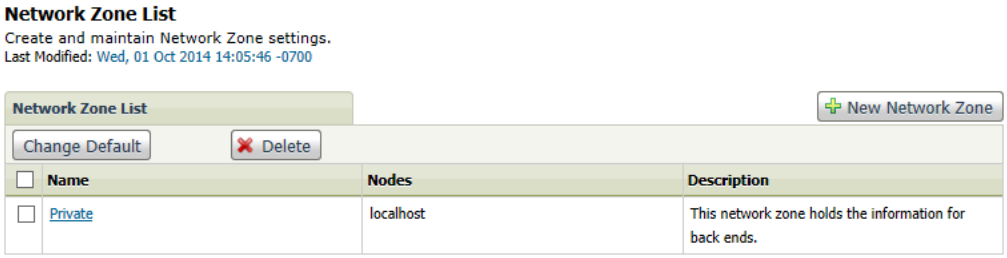
Note If the IP address in a Host of a network zone is changed, the corresponding SecureTransport Server or SecureTransport Edge must be restarted using the `<FILEDRIVEHOME>/stop_all` and `<FILEDRIVEHOME>/start_all` scripts. If the IP address in a Host of a non-private zone in a cluster environment is changed, all nodes in the cluster need to be restarted.

Specify ports for internal TM server communications

Use the `Private` network zone to specify the ports and certificates used for communication between the TM Server and the protocol servers and the Administration Tool server running on the SecureTransport Server. The `Private` network zone defines one node named `Host` with one address, `localhost`. For the `Private` network zone and internal Transaction Manager server communications to work correctly, `localhost` must resolve to the IP address of the system loopback device.

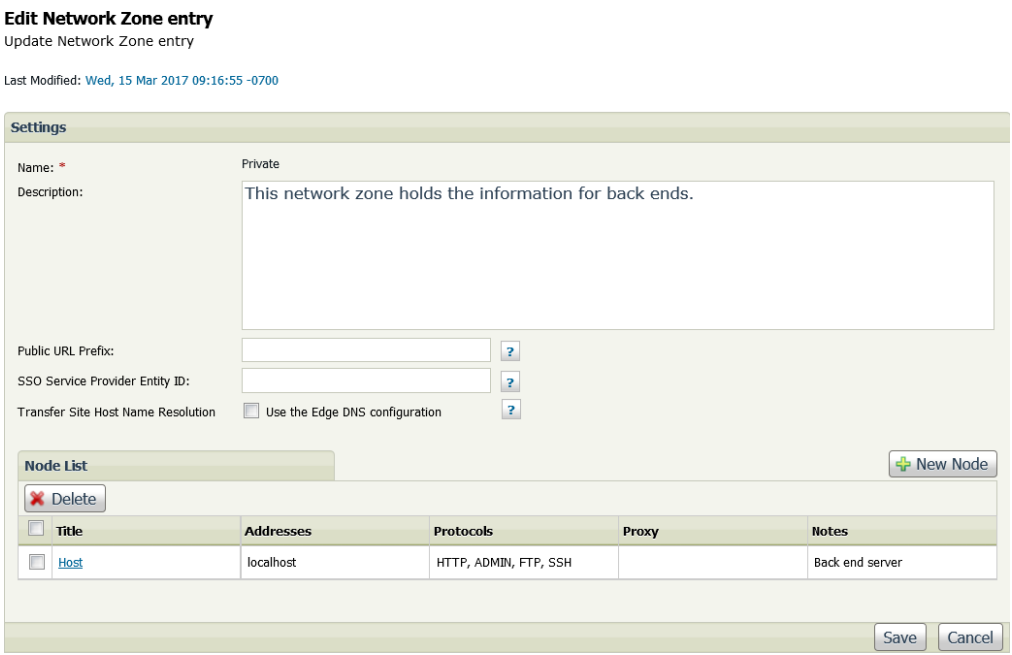
1. Select **Setup > Network Zones**.

   The *Network Zone List* page is displayed.



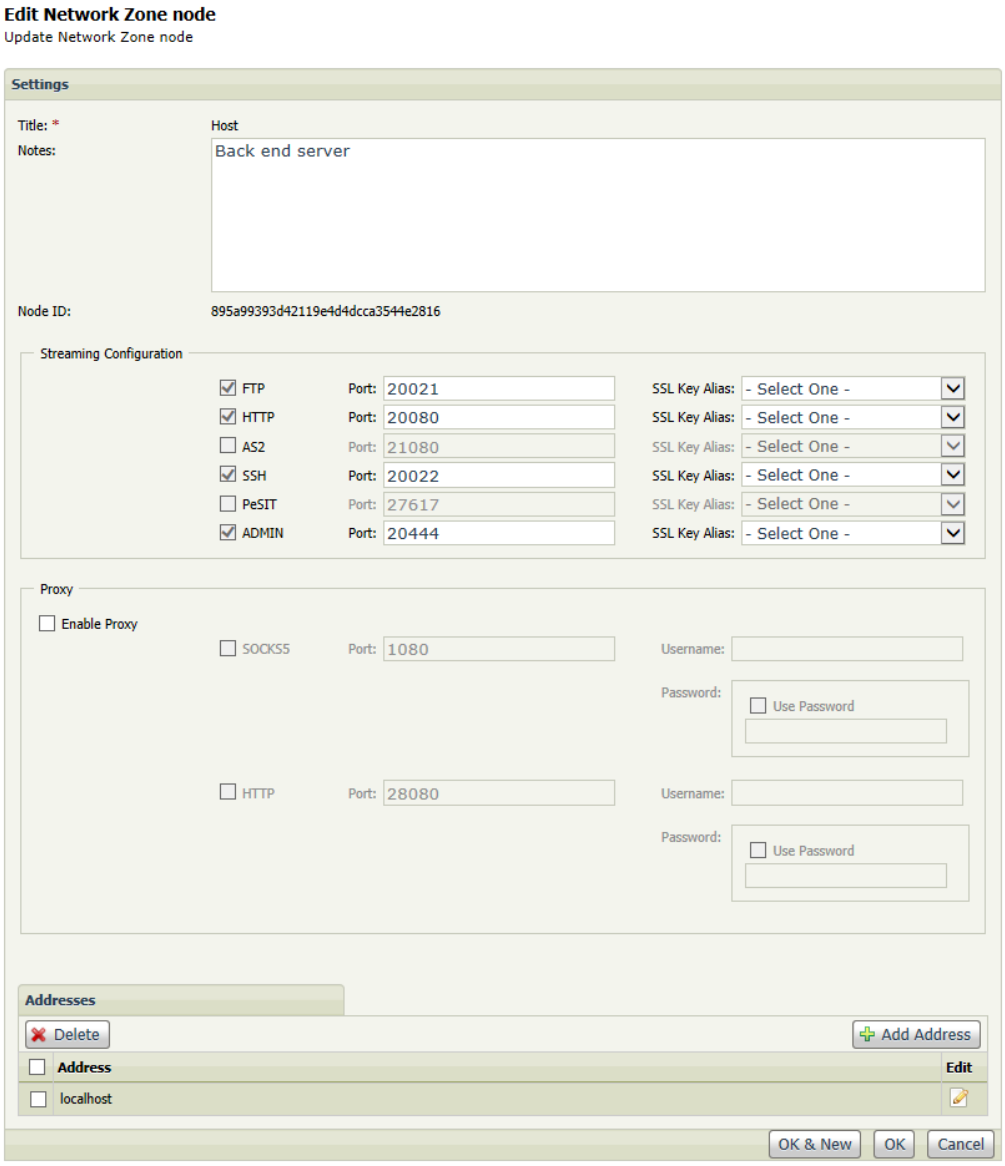
2. In the list, click `Private`.

   The *Edit Network Zone entry* page is displayed.



3. In the *Node List*, click `Host`.

   The *Edit Network Zone node* page is displayed.



4. Under *Streaming Configuration*, enter ports for the TM Server to connect to for each enabled protocol server and for the Administration Tool server.

   In the special `Private` network zone on SecureTransport Server, these settings define both the ports that the TM Server connects to and the ports that the protocol servers and the Administration Tool server listen on for connections from the TM Server.

5. (Optional) Under *Streaming Configuration*, select SSL key aliases to secure the SSL communication between the TM Server and the other servers. Do not select any of the SSL key aliases selected to secure protocol communications on the *Server Control* page. Also, add to the value of the `Streaming.TrustedAliases` server configuration parameter the aliases of the CAs that issued the certificates. For details, see the description of the `Streaming.TrustedAliases` server configuration parameter on the *Server Configuration* page.

6. Click **Save** to save your changes.

Create a network zone to define communications with SecureTransport Edge servers

Each network zone can define the communications between the TM Server on a SecureTransport Server and one or more SecureTransport Edge servers. If different protocol servers run on different SecureTransport Edge servers, you can control which protocol servers on which SecureTransport Edge servers the TM Server connects to by specifying different protocol servers and different SecureTransport Edge servers in different nodes.

1. Select **Setup > Network Zones**.

   The *Network Zone List* page is displayed.

2. Click **New Network Zone**.

   The *New Network Zone entry* page is displayed.

3. In the **Name** field, enter a name for the network zone. This name is only used in the *Network Zone List* page.

4. In the **Description** field, enter a description of the network zone to help you understand it purpose and use.

5. In the **Public URL Prefix** field, enter a prefix for the URLs displayed in notification emails send to ad hoc file transfer recipients.

   If a user is assigned to a business unit that references a network zone, emails to that user use the prefix specified in that network zone. If a user is not assigned to a business unit, emails to that user use the prefix specified in the default network zone. See *Set a default network zone* on page 224.

6. In the **SSO Service Provider Entity ID** field, enter the Single Sign-On (SSO) service provider entity ID. If an entity ID is not provided, SecureTransport uses the entity ID under the `<ServiceProvider>` element from the `sso-enduser.xml` file.

   When Single Sign-On is enabled and a user is successfully signed on to an Identity Provider (IdP), the IdP uses the specified entity ID to identify what network zone to redirect the user to.

   Note After restarting Transaction Manager if you specify a SSO Service Provider Entity ID value, SecureTransport will clone the `sso-enduser.xml` file (if any), and will make a transformation changing the `entityId` attribute in the *<ServiceProvider>* element, which will be used by the corresponding SecureTransport Edges on this Network Zone when the user is trying to authenticate via this Network Zone.

7. If the SOCKS5 proxy is enabled in this network zone and DNS is not available on this SecureTransport Server, select **Use the Edge DNS configuration** to resolve transfer site host names and FQDNs using the DNS on the SecureTransport Edge so that SecureTransport can route transfers correctly.

8. Click **New Node**.

   The *New Network Zone Node* page is displayed.

9. In the **Title** field, enter a title for the node.

10. If this server is part of a DR deployment, select the value for **Deployment Site**. For more information, see *Set up a disaster recovery cluster* on page 365.
11. In the **Notes** field, enter information to help you understand the purpose and use of the node.
12. Under *Streaming Configuration*, select the protocol servers that the TM Server connects to using this node of this network zone.
13. For each enabled protocol server, enter the port for the TM Servers to connect to.

    For each SecureTransport Edge server configured under *Addresses*, for a connection to be successful, the SecureTransport Edge server must allow connection from this SecureTransport Server, the `Private` network zone must specify the same port for the protocol server, and the certificate must be trusted. See *Specify allowed SecureTransport Servers on SecureTransport Edge* on page 226 and *Specify TM Server communication ports and IP address for protocol servers on SecureTransport Edge* on page 224.
14. Under *Addresses*, click **Add Address**.
15. In the **Address** field, enter the IP address of a SecureTransport Edge server that runs the protocol servers configured for this network zone node.
16. Repeat step 10 and 11 for each SecureTransport Edge server in this network zone node.
17. Click **OK** to save this node or **OK & New** to save this node and add another using steps 7 though 12.
18. Click **Save** to save the network zone.

    SecureTransport save the network zone in the database.

Specify proxy settings in a network zone

Use network zones to specify how SecureTransport connects to the SecureTransport Edge SOCKS5 proxy (or a HTTP proxy, where relevant) for server-initiated file transfers. You can use the same network zone node to define streaming and proxy configuration or you can define only streaming or only proxy configuration in a node or network zone.

Note Remember that HTTP proxy is only supported with HTTP(S) and AS2 transfer sites. Proxying server-initiated transfers over the other supported protocols (SSH, FTP(S), PeSIT, etc.) requires the use of the SOCKS5 proxy on SecureTransport Edge.

When you define an AS2, FTP(S), HTTP(S), PeSIT, or SSH transfer site, you can select a network zone to specify the proxy servers for transfer through that transfer site.

1. Select **Setup > Network Zones**.

   The *Network Zone List* page is displayed.
2. Click a name in the list or click **New Network Zone**.

   The *Edit Network Zone entry* page or the *New Network Zone entry* page is displayed.
3. For a new network node, enter values in the **Name**, **Description**, and **Public URL Prefix** fields as needed.
4. Click a title in the *Node List* or click **New Node**.

   The *Edit Network Zone node or the New Network Zone node* page is displayed.

5. For a new node, enter values in the **Title** and **Notes** fields as needed.
6. Under *Proxy*, select **Enable Proxy**.
7. Select the proxies, **SOCKS5** or **HTTP**, to configure in the node.
8. For each selected proxy:
    a. Enter the **Port**. The proxy server must listen for connections on this port. For the SOCKS5 proxy on SecureTransport Edge, configure the port for the proxy server on the *Server Control* page. See *Manage the Proxy server on SecureTransport Edge* on page 260. If you use a third-party proxy server, refer to its documentation to configure the port.
    b. (Optional) If required by the proxy server, enter a **Username** and, if also required, select **User Password** and enter a **Password**. The SOCKS5 proxy on SecureTransport Edge does not use this authentication.
9. For a new node, add the address of the SecureTransport Edge servers that run the SOCKS5 proxies or the addresses of the other proxy servers. If you selected **SOCKS5**, you must use IPv4 addresses. SecureTransport Server selects the servers at these address sequentially (round-robin) when it uses this node for server-initialed transfer.
10. If DNS is not available on this SecureTransport Server, select **Use the Edge DNS configuration** to resolve transfer site host names and FQDNs using the DNS on the SecureTransport Edge so that SecureTransport can route transfers correctly.
11. Click **OK** to save the new node or the changes to the node.
12. Click **Save** to save the network zone.

Proxy states and blacklisting

Secure Transport provides a mechanism for dynamic blacklisting of SecureTransport Edge proxies in case of failure. An Edge proxy can be in one of three states - available, failed, or denied. It is added to a list of "failed" proxies if a connection cannot be established through it. The failed proxy then becomes "denied" when the number of failed connection attempts, defined in `Proxy.Max.Failure.Series` (3 by default), is reached within the time interval specified by the `Failed.Proxy.Timeout` option value (3 minutes by default). At this point, the "denied" proxy is blacklisted, and no connections are routed through it, for the period of time specified by the `Denied.Proxy.Timeout` configuration option value (10 minutes by default). After the blacklisting timeout period elapses, the proxy returns its state to "available".

The failed and denied Edge proxies lists are local to each server node and cleared upon TM restart. As result, a backend node in a multi-node cluster may still make connection attempts to a proxy that is in another node's "denied" proxies list. This may result in errors and even failed server-initiated transfers, as the backend node is yet to detect a failing Edge proxy.

To minimize the likelihood of such an event occurring, set the configuration options `Denied.Proxy.Timeout, Failed.Proxy.Timeout, Proxy.Max.Failure.Series`, and `EventQueue.maxRetryCount` to values that will allow all nodes in the cluster to detect potential unavailability earlier.

By default, proxy blacklisting is enabled. To disable it, set the `Proxy.Blacklisting.Enabled` configuration option to `false`. Changing the value requires a TM restart.

When the blacklisting functionality is disabled, the network zones are always considered alive, the `Denied.Proxy.Timeout`, `Failed.Proxy.Timeout`, and `Proxy.Max.Failure.Series` values are disregarded and backend nodes will not detect potential Edge proxies unavailability.

Set a default network zone

Business units can specify a network zone that defines the public URL for users in that business unit. For details, see *Create or edit a business unit* on page 693. AS2, FTP(S), HTTP(S), PeSIT, and SSH transfer sites can specify a network zone that defines the proxy for that site. For details, see *Transfer sites* on page 494. In all cases, you can select **Default** in the business unit or transfer site.

The default network zone defines the public URL for users in business units where you selected **Default** and for users who are not in a business unit. The default network zone also defines the proxy for transfer sites where you selected **Default**. If a transfer site selects the default network zone and no default is defined, transfers from that site fail.

1. Select **Setup > Network Zones**.

   The *Network Zone List* page is displayed.

2. Select one network zone in the list.
3. Click **Change Default**.

   The selected network zone is marked as the default.

Specify TM Server communication ports and IP address for protocol servers on SecureTransport Edge

The `Private` network zone is the only network zone defined on the SecureTransport Edge server. You cannot delete it or define more network zones.

Use the `Private` network zone to specify the ports and IP address that the protocol servers and the Administration Tool server listen on for connections from TM Servers. The `Private` network zone defines one node named `Host`.

1. Select **Setup > Network Zones**.

   The *Network Zone List* page is displayed.

2. In the list, click `Private`.

   The *Edit Network Zone entry* page is displayed.

3. In the *Node List*, click `Host`.

   The *Edit Network Zone Node* page is displayed.

4. For each enabled protocol server, enter the protocol server listens on for connections from TM Servers.

   For a connection to be successful, the SecureTransport Edge server must allow connection from this SecureTransport Server, there must be a network zone on a SecureTransport Server with these same ports configured for the host name or IP address of this SecureTransport Edge server

and the certificate must be trusted on the SecureTransport Server. See *Specify allowed SecureTransport Servers on SecureTransport Edge* on page 226 and *Create a network zone to define communications with SecureTransport Edge servers* on page 221.

5. Under *Addresses*, Click the Edit icon ( ) for the `localhost` entry.
6. In the **Address** field, enter the IP address of the interface that the servers listen on for connections from TM Servers.
7. Click the Save icon ( ).
8. Click **OK** to save your changes.

Secure the communication between the TM server and the protocol servers

You can use SSL to secure the communication between the TM server running on SecureTransport Server and the protocol servers running on SecureTransport Edge.

In a streaming deployment, the protocol servers on SecureTransport Edge have the role of server because the TM server on SecureTransport Server connects to them and the TM server on SecureTransport Server has the role of client because it connects to the protocol servers on SecureTransport Edge.

1. Generate or obtain the following certificates:
   - The TM server client certificate with `extendedKeyUsage` = `clientAuth` and `keyUsage` = `digitalSignature`
   - The protocol servers server certificate with `extendedKeyUsage` = `serverAuth` and `keyUsage` = `digitalSignature`, `keyEncipherment`
2. On SecureTransport Edge:
   a. Import into the trusted CAs the public part of the certificate for the CA used to generate the TM server client certificate.
   b. Add to the `Streaming.TrustedAliases` server configuration parameter the alias you specified when you imported the certificate in step a.
   c. Import into the local certificates the protocol servers server certificate.
   d. In the `Private` network zone, open the *Edit Network Node* page and, to secure the SSL communication for a protocol, select the **SSL Key Alias** you specified when you imported the certificate in step c.
3. On SecureTransport Server:
   a. Import into the trusted CAs the public part of the certificate for the CA used to generate the protocol servers server certificate.
   b. Add to the `Streaming.TrustedAliases` server configuration parameter the alias you specified when you imported the certificate in step a.
   c. Import into the local certificates the TM server client certificate.

d. In the network zone you created to define communications with SecureTransport Edge servers, open the *Edit Network Node* page and, to secure the SSL communication for a protocol, select the **SSL Key Alias** you specified when you imported the certificate in step c.

Specify the SecureTransport Edge load-balancing policy

When a client establishes a user session to a protocol server running on SecureTransport Edge, the load-balancing policy that SecureTransport Edge uses to allocate a Transaction Manager connection to that session is specified by the `Streaming.LoadBalancingPolicy` server configuration parameter. The valid values are:

- **`Round-Robin`** — SecureTransport Edge directs connections to connected Transaction Managers in a circular sequence and allocates the least-used connection to that Transaction Manager to the session.
- **`Random`** — SecureTransport Edge randomly selects a connection from all the connections to all the connected Transaction Managers and allocates it to the session.
- **`Blacklist-Round-Robin`** — SecureTransport Edge directs connections to connected Transaction Managers in a circular sequence and allocates the least-used connection (but filters bad connections) to that Transaction Manager to the session. `Blacklist-Round-Robin` is the default and recommended value.
- **`Blacklist-Random`** — SecureTransport Edge randomly selects a connection from all the connections (but filters bad connections) to all the connected Transaction Managers and allocates it to the session.

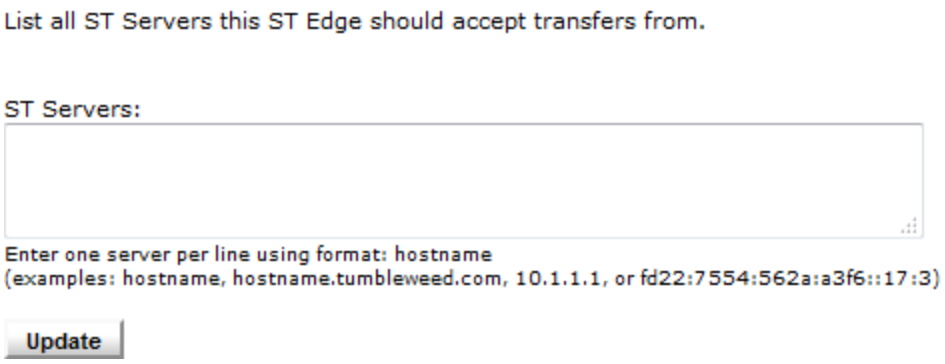
In all cases, the user session uses the allocated connection until it terminates.

Specify allowed SecureTransport Servers on SecureTransport Edge

The SOCKS5 proxy on a SecureTransport Edge server accepts connections for server-initiated transfers only from the SecureTransport Servers listed. There is no HTTP proxy on the SecureTransport Edge server. The Transaction Manager on any SecureTransport Server can connect to a protocol server on any SecureTransport Edge server.

1. Select **Setup > Allowed ST Servers**.

   A page is displayed with the server list.



2. Under *ST Servers*, list the host names or IP address of the SecureTransport Servers that are allowed to connect to this SecureTransport Edge server, either to a protocol server or to a SOCKS5 or HTTP proxy.
3. Click **Update**.
4. Restart the SOCKS proxy on the SecureTransport Edge server.

Configure SecureTransport Back End to Edge streaming communication

The Edge to Back End server communication utilizes Network Zones that allows one or multiple Edge servers to be grouped in a "zone" that all inbound and outbound communications will go through. The existence of several zones provides the opportunity to have multiple peripheral networks (for example, one for intranet and one for internet traffic). Additionally, the communications are entirely outbound from Back End perspective. That means that no inbound ports in the firewall placed in between the Edge and Back End need to be opened for communication between the Edge and Back End.

To configure streaming communications between the Edge and Back End server, take the following steps:

1. Exchange the Internal CA certificates of the Edge(s) and the Back End(s). To exchange CA certificates of a Back End and Edge, the CA certificate of the Back End should be exported and imported on the Edge and the CA certificate of the Edge should be exported and imported on the Back End. For additional information, refer to *Manage trusted CAs* on page 61.
    a. On the Back End, select **Setup > Certificates**.
    b. Click the **Trusted CAs** tab.
    c. Navigate to the page that lists the certificate labeled *ca*.
    d. Click the alias of the CA certificate.
    e. Click **Export** and save the certificate file in the desired location.
    f. On the Edge, select **Setup > Certificates**.
    g. Click the **Trusted CAs** tab.
    h. Click **Import**.

i. Browse and select the CA certificate exported from the Back End.

j. Enter an alias for the CA certificate. For example, enter **ca_be** for the certificate exported from the Back End imported into the Edge and **ca_edge** for certificate exported from the Edge and imported into the Back End.

Note Do not over write the Edge or Back End CA certificate with imported certificate.

k. Click **Import**.

l. Follow the Steps a to k in the opposite direction in order to export the internal CA of the Edge and import it on the Back End.

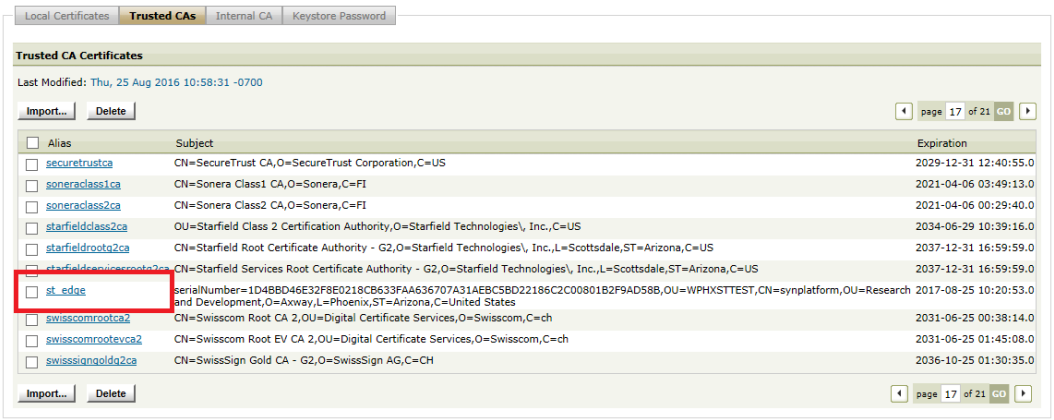
On the Back End:

2. Generate a self-issued local certificate server that will only be used for streaming communications. For additional information, refer to *Generate a self-issued server certificate* on page 55.

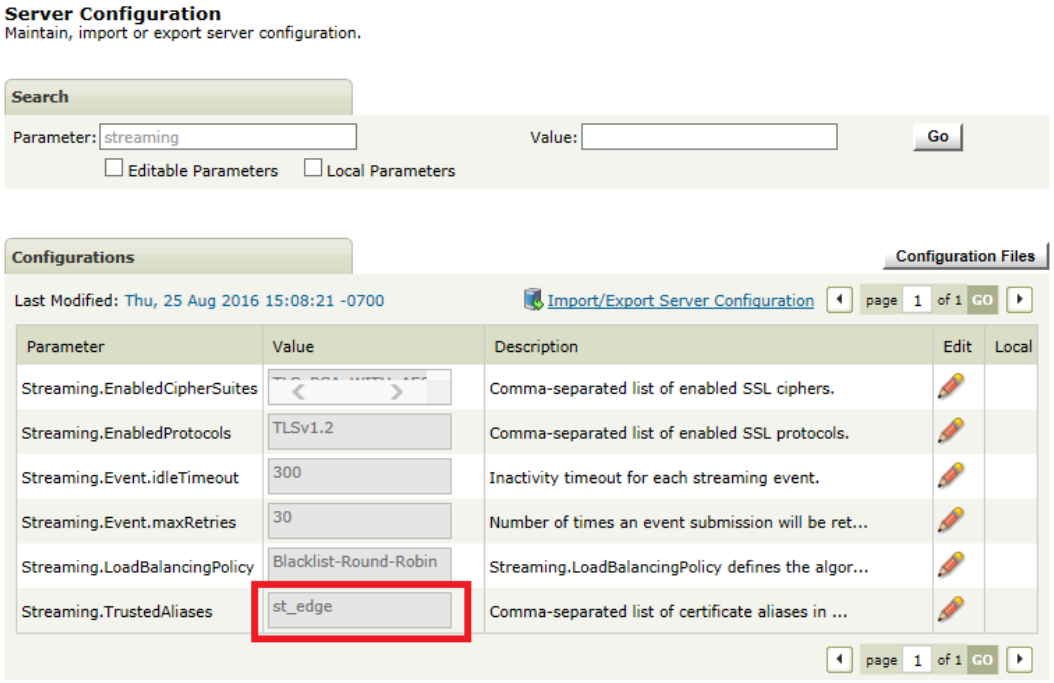
Display of the self-issued local certificate for streaming.

3. Search for and configure the `Streaming.TrustedAliases` parameter with the alias of the CA certificate of the Edge that was imported. For information on searching for configuration parameters, refer to *Search for a parameter* on page 316. For information on changing configuration parameters, refer to *Change a parameter value* on page 317.

Display of the imported CA certificate.



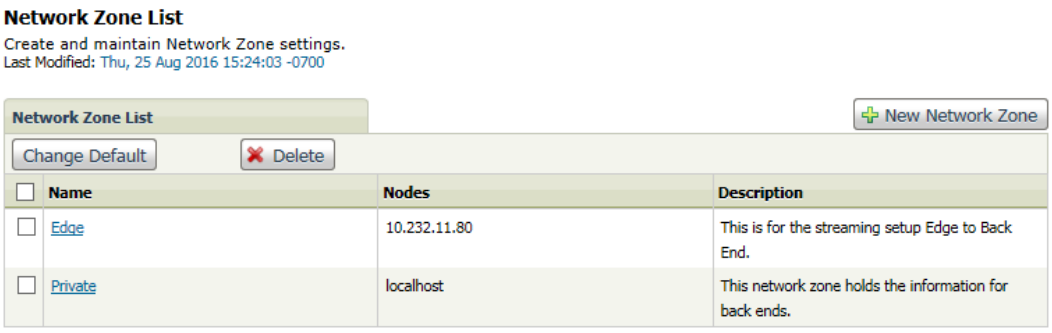
Display of the `Streaming.TrustedAliases` parameter configuration.



4. Add a new zone on the Back End for the Edge. For additional network zone configuration information, refer to *Manage the communication across Transaction Manager, protocol and proxy servers* on page 218

   Note The Private zone on the Back End should not be modified.

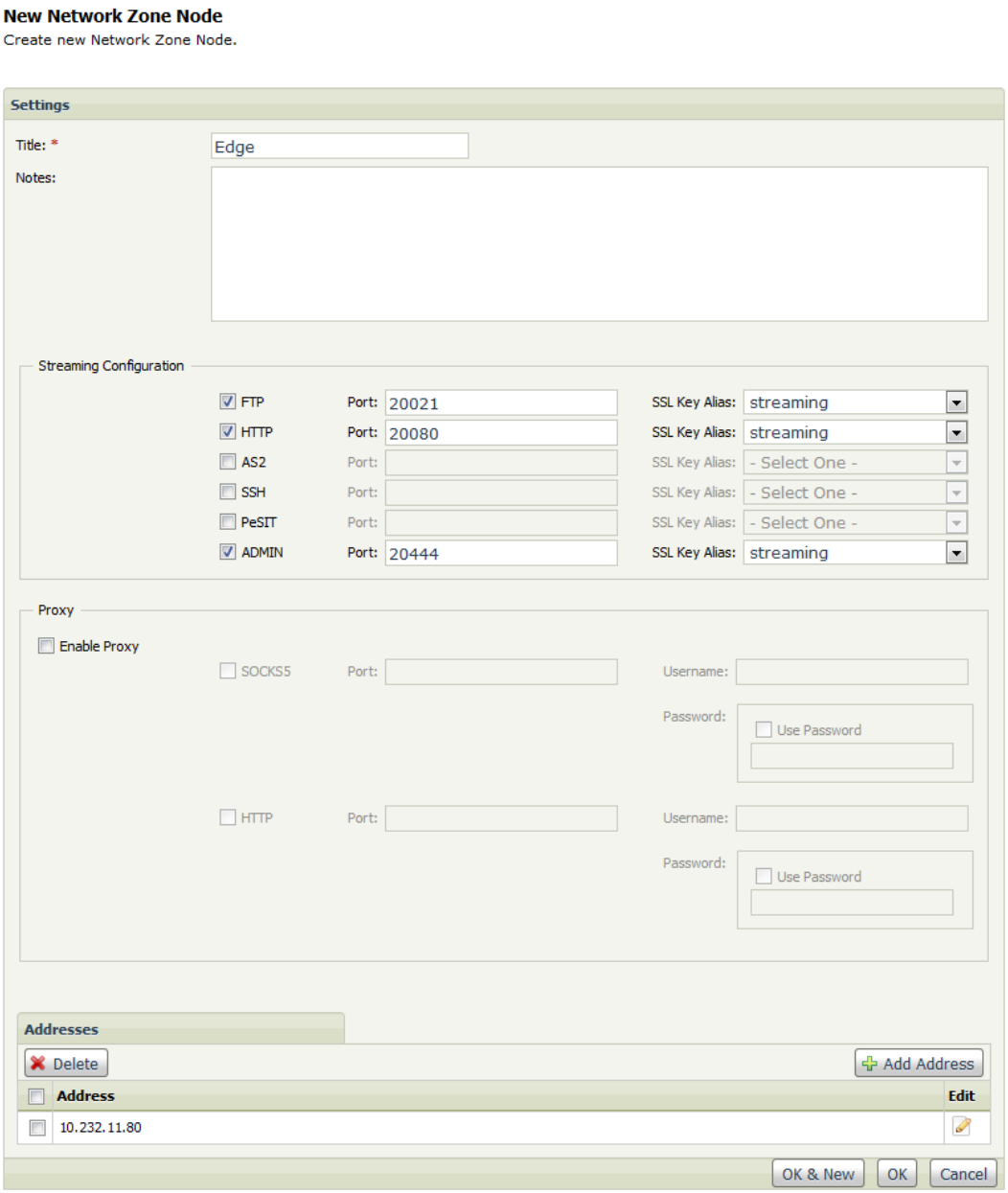
   Display of the new zone on the Back End.



5. Enter a Title, Description, and Notes. In the *Streaming Configuration* pane, select the protocols which should be used for the streaming communications. Enter the port number of each selected protocol. The Back End will connect to the Edge to establish the streaming connections using these ports. The streaming connections are established in outbound direction - from Back End to Edge. The port numbers must match between the Back End and the Edge. For each selected protocol, select the alias of the certificate generated in Step 2 for the **SSL Key Alias**. Additionally, the streaming port numbers and certificate alias must be different from port numbers and certificates used for server control. Add the IP address of the Edge in *Addresses* pane.

   Note **ADMIN** must be selected whenever another streaming protocol is selected. The ADMIN protocol is used for internal functions like DNS resolving and DNS reverse lookups (`Server.ReverseDNSLookups`). For additional information refer, to *Enable or disable reverse DNS lookups* on page 179.

   Display of the Back End streaming configuration.

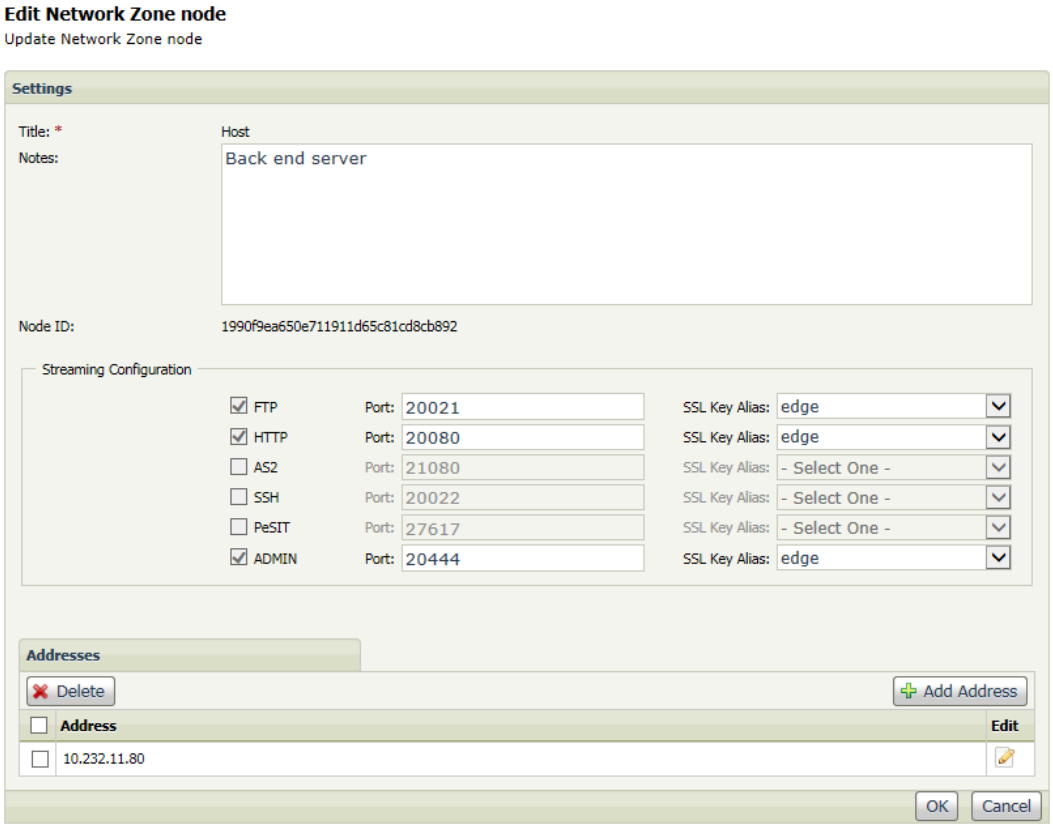


On the Edge:

6. Generate a self-issued local certificate server that will only be used for streaming communications. For additional information, refer to *Generate a self-issued server certificate* on page 55.
7. Edit the Network Zone node and change the default **localhost** to the IP address of the Edge server itself. To edit the Network Zone node, select the alias of the Network Zone from the *Network Zone List* and then select the Node from the *Node List*. For additional configuration information, refer to *Create a network zone to define communications with SecureTransport Edge servers* on page 221.

Note **ADMIN** must be selected whenever another streaming protocol is selected. The ADMIN protocol is used for internal functions like DNS resolving and DNS reverse lookups (`Server.ReverseDNSLookups`). For additional information refer, to *Enable or disable reverse DNS lookups* on page 179.

Display of the Edge streaming configuration.



8. Verify that the ports for the services (FTP, HTTP, etc.) are the same and match the ports, configured for the same zone on the Back End. For each protocol, select the alias of the certificate generated in Step 6 for the **SSL Key Alias**.
9. Search for and configure the `Streaming.TrustedAliases` parameter with the alias of the CA certificate of the Back End that was imported. For information on searching for configuration parameters, refer to *Search for a parameter* on page 316. For information on changing configuration parameters, refer to *Change a parameter value* on page 317.
10. For the streaming communication configuration to take effect, restart all of the services (`stop_all`/`start_all`) on both Back End and the Edge.
11. Wait for at least 2 minutes for Transaction Manager to connect to the Edge. You should have a streaming communications up and running once Transaction is connected to the Edge. Successful streaming communications can be verified with server log messages which contain "Established streaming connection".

To test Client Initiated Transfers, try to login using the address of the Edge.

Address Book

The Address Book feature provides built-in and custom address books data sources to the SecureTransport server. End users are allowed via the ST Web Client to send messages or share folders to a predefined list (address book) of users and groups. End users are able to send or share folders directly by using the display name defined in the address book. Implementing Address Book functionality allows SecureTransport administrators to control the users' collaboration with external (non-address book) users.

The global Address Books configuration page is found at **Setup > Address Books**. There you can configure the global address book sources list, enable or disable global address books, and determine whether or not to allow address book collaboration. To configure the global address book sources list, refer to *Address Book global configuration* on page 236.

Note The *Address Book Sources* page is only displayed if the Address Book feature is enabled (the value of the `AddressBook.Enabled` configuration option is set to **true**).

The Address Book sources list configuration for each business unit can be inherited from the global Address Book sources list configuration or changed for the current business unit. To configure Address Book sources list for a business unit, refer to *Address Book business unit level configuration* on page 239.

For individual accounts the Address Book sources list can be inherited or overwritten. To configure the Address Book sources list for an account, refer to *Address Book account level configuration* on page 240.

Additionally, the LDAP address book settings can be configured. To configure the LDAP address settings, refer to *LDAP domains* on page 429.

Address Book sources

The Address Book feature has two built-in address book sources – Local source and LDAP source. These two sources become available by default when the Address Book functionality is enabled. Multiple custom address book sources can also be registered on the SecureTransport server.

Local source

The local Address Book source includes local SecureTransport accounts with registered e-mails and has two options for specifying the address book entries:

- Own Business Unit – This includes entries which belong to the same business unit as the account to which the local source is assigned (including sub business units).
- All Business Units – This includes all virtual accounts in SecureTransport server which have associated email address.

All entries are populated in a tree structure; for example, there is one parent group for all entries – Parent Display Group. This parent group name is based (evaluated) on the Address book source configuration – either account, business unit, or global level. Each business unit is also considered a

parent group to all accounts that belong to it. So each account produces an address book user entry with the parent group as its business unit (or the parent group defined for the local source if the account does not have a business unit) and each business unit produces an address book group entry. If there are nested business units, the result address book entries structure is nested in the same way.

LDAP source

The LDAP source specific settings are defined in the LDAP configuration page. For configuration information on defining the Address Book Settings for a domain, refer to *Define Address Book settings for a domain* on page 443.

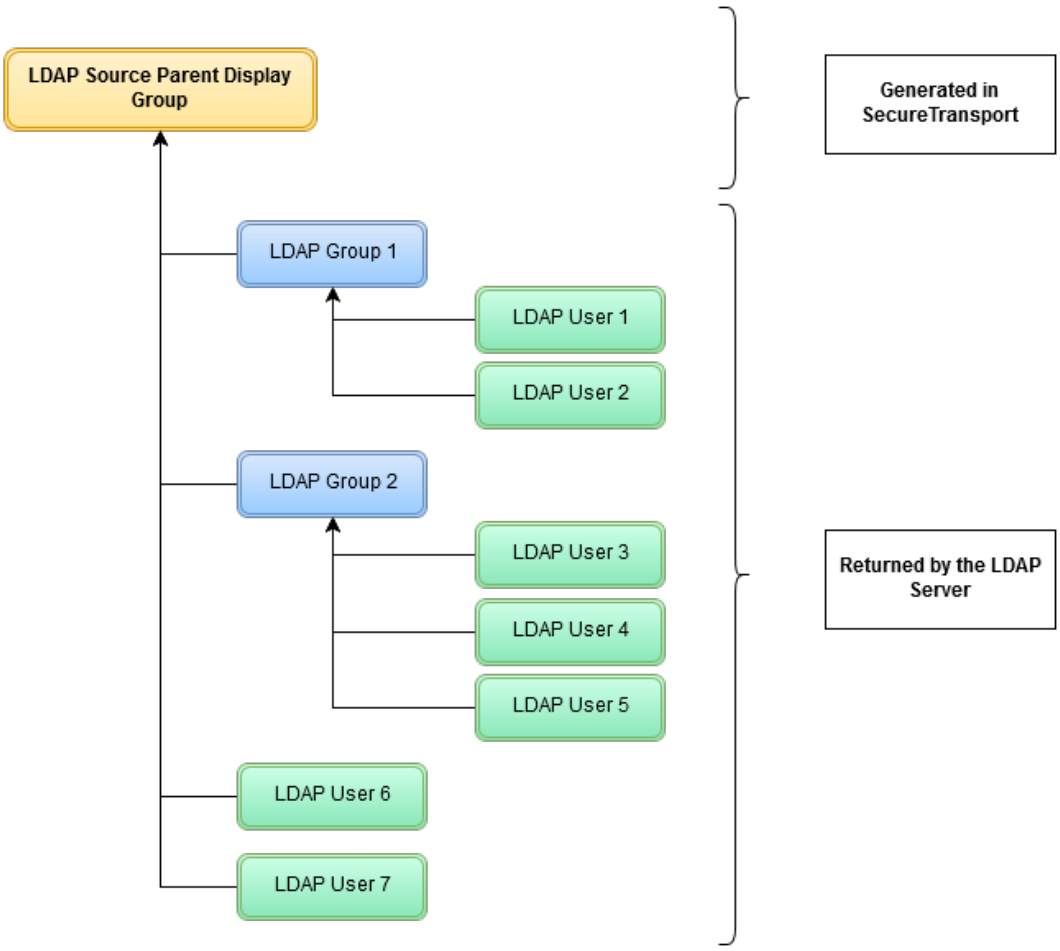
The Address Book entry map settings, as well as search query, are exposed into the LDAP configuration page. There are 3 predefined properties for an entry:

- Display name
- Primary email
- Parent group

The mapping configurations allow defining new properties, which can be extracted from the LDAP object. All additionally added key value pairs are populated as custom properties of the address book entry.

When fetching new entries from the LDAP source, if a `parentGroup` mapping has been specified by the SecureTransport administrator, its value will override the `parentGroup` value defined for the LDAP source. For example, the LDAP source is configured as an Address Book data source, it is enabled, has LDAP Source as its parent group, and the `parentGroup` property has been mapped to the LDAP attribute group. All entries which are fetched from this source will override the LDAP source value and will map the value of the group attribute to the `parentGroup` property instead. In other words, only the direct parent of an entry will be displayed in its `parentGroup` property.

All entries are populated in a tree structure; for example, there will be one parent group (root) for all LDAP entries. The parent group name is based (evaluated) on the Address Book source configuration – either account, business unit, or global level. All nested parent groups will depend on the `parentGroup` attribute mapping. In other words, the tree structure of entries returned by the LDAP server will be attached as child of the evaluated root parent group, defined for the LDAP source. In that case, all LDAP groups and user entries which do not belong to a group will be considered as direct children of the root parent group. This allows all entries coming from a source to be addressed using a single display name – the source Parent Display Group.



Custom source

For instructions on how to implement a custom Address Book source, refer to the *SecureTransport Developer's Guide*.

Address Book configuration settings

The Address Book data source configurations are arranged hierarchically in three levels. The first level of configuration is the global level, the second level is business unit level, and the third level is the account level. Each level deeper is able to either inherit or override the settings of the upper level Address Book configurations.

Example:

A custom source "MSSQL DS" is enabled at the global level and then "MSSQL DS" is assigned to a business unit. For this business unit, the SecureTransport administrator is able to enable or disable the source, specify the group property, and set permissions if these settings can be overridden for underlying accounts by delegated administrators. All these settings are taken with higher precedence than the global settings.

The order of the Address Book data source hierarchy is:

- Account level
  - Business unit level
    - Global level

Address Book global configuration

The Address Book global configuration consists of enabling the Address Book feature and configuring the global level Address Book settings.

Address Book server configuration settings

By default the Address Book feature is not enabled and Address Book sources global configuration page is hidden. Additionally, the business unit and account level address features are hidden by default. To enable the address book feature:

1. Navigate to **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.
2. Search for the `AddressBook.Enabled` configuration parameter.
3. Click the **Edit** ( ) icon in the *Edit* column.
4. Change the `AddressBook.Enabled` configuration parameter to **true**.
5. Click the **Save** ( ) icon in the *Edit* column.

For more information on changing server configuration parameters, refer to *View and change server configuration parameters* on page 315.

All Address Book configuration settings are stored under the `AddressBook` namespace in the server configuration:

- `AddressBook.Enabled` - Enable or disable Address Book functionality. When enabled, the Address Book user interfaces appear in the Administration Tool, allowing configuration on global, business unit, and account levels. New REST API endpoints also become available for configuring and querying the Address Book. When disabled the Address Book related UI is hidden, REST API endpoints return empty result set to the client, and all Address Book related configuration settings (described below) are not taken into consideration.
- `AddressBook.AllowCollaboration` - Default setting for controlling Address Book collaboration with external recipients. This setting can be set from the Address Book global setting **Setup> Address Books> Allow collaboration with non-Address Book recipients** and can be overridden on the business unit and account levels. If Address Book functionality is disabled (`AddressBook.Enabled` is set to **false**) this setting does not affect user collaboration.
- `AddressBook.Limit.AdHoc.Recipients` - The total number of recipients allowed for AdHoc packages and Shared Folders collaboration. If the recipient count exceeds this value, an error will be returned to the client. The default value is **100**.

- `AddressBook.Limit.DefaultDisplayEntries` - Specifies the default limit of Address Book entries displayed to the user if no limit is specified in the request. The default value is **10**.
- `AddressBook.Limit.MaxDisplayEntries` - Specifies the maximum number of Address Book entries returned by the server in a single response. The default value is **100**.
- `AddressBook.Limit.MaxDisplayPages` - Specifies the maximum number of Address Book pages in a single request. The maximum number of entries returned by an Address Book source is the multiplication of this value and `AddressBook.Limit.MaxDisplayEntries`. The default value is **100**.
- `AddressBook.Search.Min.Length` - Specifies the minimum search string length when performing wildcard search for Address Book entries. The default value is **3**.

Address Book global sources list configuration

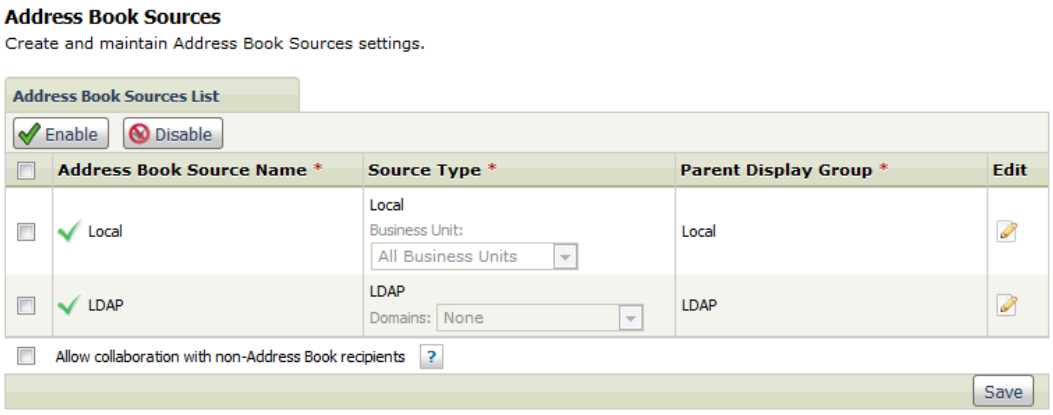
You can configure (enable and disable) Address Book data sources, define a parent group for each resource, and specify if allow collaboration is enabled for the whole system. You cannot add or remove Address Books from the Address Book Sources List on the *Address Book Sources* page because of the Address Book provider auto-discovery registration process. This process works the following way – in order to add a new address book source, the address book provider implementation package must be placed inside the `<FILEDRIVEHOME>/lib/jars` folder. On Transaction Manager startup, the provider is dynamically loaded and any new Address Book sources are registered into the SecureTransport system.

To view and configure the global Address Book sources list:

Navigate to **Setup > Address Books**.

The *Address Book Sources* page is displayed.

Note The *Address Book Sources* page is only displayed if the Address Book feature is enabled (the value of the `AddressBook.Enabled` configuration option is set to **true**).



Enable an Address Book source

1. Select the Address Book source to enable.
2. Click **Enable**.

Disable an Address Book source

1. Select the Address Book source to disable.
2. Click **Disable**.

Edit the Local source

1. Click the **Edit** icon ( ).
2. Select the **Business Unit** source from the *Source Type* menu. Select either **All Business Units** or **User's own business unit**. If the local source type is **All Business Units**, the user can send emails to all SecureTransport accounts that have email addresses configured. If the local source type is **User's own business unit**, the user can send emails only to accounts in the same business unit.
3. Edit the **Parent Display Group**.
4. Click the **Save** icon ( ).

Edit the LDAP source

1. Click the **Edit** icon ( ).
2. Select the **Domain** from the *Source Type* menu.
3. Edit the **Parent Display Group**.
4. Click the **Save** icon ( ).

Edit a Custom source

1. Click the **Edit** icon ( ).
2. Edit the **Parent Display Group**.
3. Click the **Save** icon ( ).

Allow collaboration with non-Address Book recipients

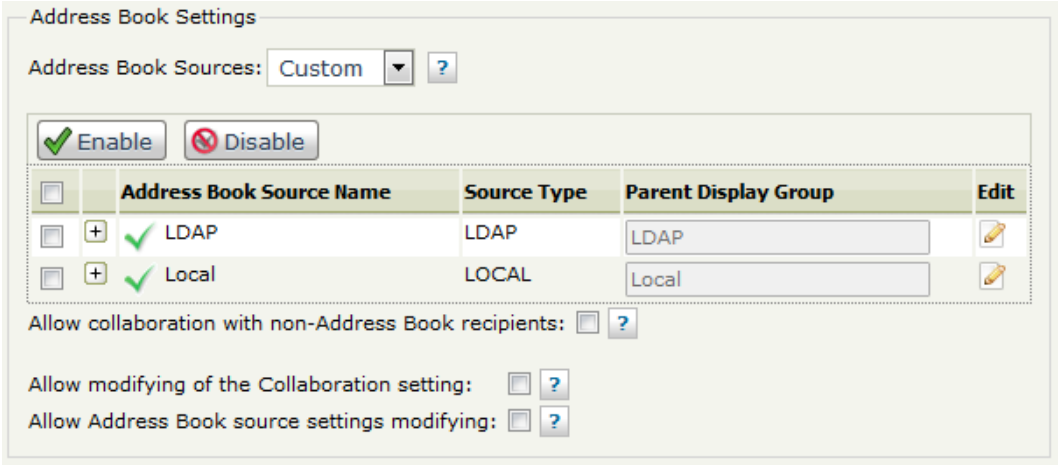
1. Select **Allow collaboration with non-Address Book recipients**.
    - When **checked**, accounts that use the global Address Book policy will be allowed to send email packages and share folders with users that do not exist the defined Address Book.
    - When **unchecked**, accounts that use the global Address Book policy will be allowed to send email packages and share folders only with users that exist in the defined Address Book.

    This global setting can be overridden on business unit and account configuration levels.

Note Users will be able to share folders when **Allow collaboration with non-Address Book recipients** is checked (enabled), only if the `SharedFolders.AllowCollaboration` server configuration parameter is set to **true**. For more information on changing server configuration parameters, refer to *View and change server configuration parameters* on page 315.

Address Book business unit level configuration

At the business level, SecureTransport administrators can configure the following settings:



- Address Book Sources - Address Book Policy that will apply for the current business unit.
  - Default - When **Default** is selected, the business unit inherits either its parent's Address Book policy or the global Address Book policy if it is a top level business unit.
  - Custom - When **Custom** is selected, a custom Address Book policy configuration will be set for this business unit only. A list of all registered Address Books is displayed and for each the administrator is able to:
    - Enable or disable Address Book sources for the business unit.
    - Specify the parent group for a given Address Book source.
    - Specify the domain for LDAP Address Book sources.
    - Specify **All Business Units** or **User's own business unit** for local and custom Address Book sources.
  - Disabled - When **Disabled** is selected, the Address Book policy is set to disabled for this business unit.
- Allow collaboration with non-Address Book recipients - Enable address book collaboration. If Address Book functionality is disabled, this setting does not affect user collaboration.
  - When **checked**, accounts that use the Address Book policy defined on the business unit level will be allowed to send email packages and share folders with users that do not exist the defined Address Book.

- When **unchecked**, accounts that use the Address Book policy defined on the business unit level will be allowed to send email packages and share folders only with users that exist in the defined Address Book.

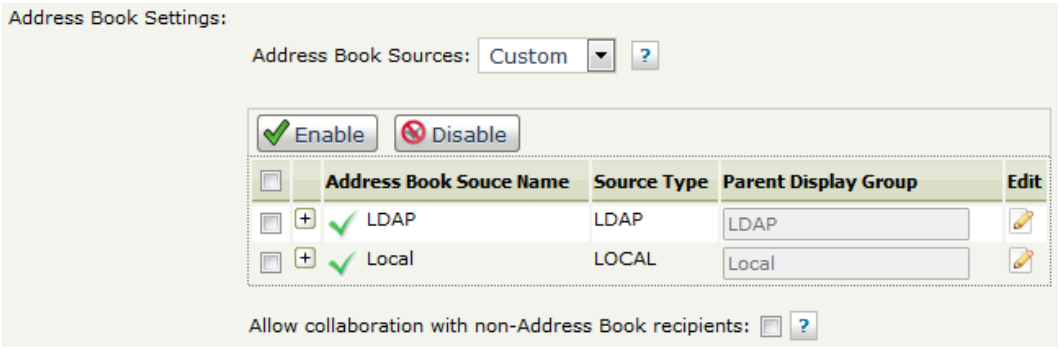
This business unit setting overrides the global Address Book policy setting for collaboration. This setting can be overridden on the account level if **Allow modifying of the Collaboration setting** is checked.

Users will be able to share folders when **Allow collaboration with non-Address Book recipients** is checked (enabled), only if the `SharedFolders.AllowCollaboration` server configuration parameter is set to **true**. For more information on changing server configuration parameters, refer to *View and change server configuration parameters* on page 315.

- Allow modifying of the Collaboration setting - Allow Address Book Collaboration setting modification.
  - When **checked**, accounts that use the Address Book policy defined in this business unit will be allowed to override the **Allow collaboration with non-Address Book recipients** setting specified here.
  - When **unchecked**, accounts that use the Address Book policy defined in this business unit will be not allowed to override the **Allow collaboration with non-Address Book recipients** setting specified here.
- Allow Address Book source settings modifying - Allow Address Book Policy modification.
  - When **checked**, accounts that use the Address Book policy defined in this business unit will be allowed to override the Address Book Sources specified here.
  - When **unchecked**, accounts that use the Address Book policy defined on business unit will be not allowed to override the Address Book Sources specified here.

Address Book account level configuration

At the account level, SecureTransport administrators can configure the following settings:



- Address Book Sources - Address Book policy that will apply for the current account.
    - Default - When **Default** is selected, the account inherits either its business unit Address Book policy or the global Address Book policy.
    - Custom - When **Custom** is selected, a custom Address Book policy configuration will be set for this account only.
        - Enable or disable Address Book sources for the account.
        - Specify the parent group for a given Address Book source.
        - Specify the domain for LDAP Address Book sources.
        - Specify **All Business Units** or **User's own business unit** for local and custom Address Book sources.
    - Disabled - When **Disabled** is selected, the Address Book policy is set to disabled for this account.
- Allow collaboration with non-Address Book recipients - Enables Address Book collaboration with non-Address Book recipients. If Address Book functionality is disabled, this setting does not affect user collaboration.
    - When **checked**, the account will be allowed to send email packages and share folders with users that do not exist in the defined Address Book.
    - When **unchecked**, the account will be allowed to send email packages and share folders only with users that exist in the defined Address Book.

  This account setting overrides the business unit or global Address Book Policy setting for collaboration.

  Users will be able to share folders when **Allow collaboration with non-Address Book recipients** is checked (enabled), only if the `SharedFolders.AllowCollaboration` server configuration parameter is set to **true**. For more information on changing server configuration parameters, refer to *View and change server configuration parameters* on page 315.

Address Book use cases

This topic outlines Address Book use cases. In all of the use cases, only Local and LDAP sources are enabled.

Local user sends an AdHoc package to recipients

Assuming that the global Address Book settings are taken into consideration and the user's Address Book setting is Default. At the global configuration level a LDAP source is enabled and **Allow collaboration with non-Address Book recipients** is selected. A user can send AdHoc packages to all entries available in its address book (the LDAP source) and to external users.

When the user creates a draft message, a list of the available Address Book entries that can be selected as recipients is displayed. In this case, the user can also type in email addresses that do not exist in their configured Address Book.

Note If the total number of recipients (resolved email addresses) exceeds the value of the `AddressBook.Limit.AdHoc.Recipients` configuration option, the send operation will fail and an error message will be displayed to the user stating the reason for the failure.

Note If **Allow collaboration with non-Address Book recipients** is not selected, the user is not allowed to type email addresses in recipient fields - only Address Book contacts can be selected.

For additional information, refer to the *SecureTransport Web Client User Guide*.

Local user in a Business Unit sends AdHoc package to recipients

Assuming that the business unit level Address Book settings are taken into consideration and the account level Address Book settings are Default. At the business unit level, the Address Book settings are **Custom** and a Local source is assigned. **Allow collaboration with non-Address Book recipients** is not selected for the business unit. When the Local source type is **All Business Units**, the user can send mails to all SecureTransport accounts that have email addresses configured. When the Local source type is **User's own business unit**, the user can send mails only to accounts in the same business unit. The list of available contacts will be displayed to the user. The user will not be able to type external emails as this type of collaboration is not allowed for its business unit.

Local user shares a folder

As well as sending mails, an account can share folders to defined recipients. The server configuration option `SharedFolders.AllowCollaboration` should be **true**. This is valid for global and account level. If an account is in a business unit, the business unit option **Allow collaboration with non-Address Book recipients** should be selected. Then Address Book settings can regulate whether a folder will or will not be shared with the list of recipients.

When the user starts to type in shared folder collaborators, a list of Address Book contact names are displayed to the end user. Each of the listed contacts can be selected as collaborators.

If the **Allow collaboration with non-Address Book recipients** option is enabled for the user, the user will be able to type in email addresses and specify them as collaborators.

If the number of specified collaborators exceeds the `AddressBook.Limit.AdHoc.Recipients` option value, the share operation will fail and an error message will be displayed to the user stating the reason for the failure.

Note If the **Allow people to view collaborators** option is enabled, only collaborators' email addresses will be displayed, display names will not be shown even if collaborators are part of the address book.

For additional information, refer to the *SecureTransport Web Client User Guide*.

LDAP user shares a folder

For LDAP sources, the SecureTransport administrator can specify one of the already defined LDAP domains or the **Logged In (current domain)** option. When an LDAP user is logged in to SecureTransport and the **Logged In** domain is set as an Address Book source, all members of the same LDAP server will be displayed as Address Book entries.

Assuming that account settings are taken into consideration - LDAP users are mapped to an account template which has custom Address Book settings. An LDAP source **Logged In (current domain)** is assigned to the account template. The LDAP user which is mapped to the account template can share folders with all other users and groups defined in the same LDAP domain.

Note If the total number of resolved collaborators exceeds the value of the `AddressBook.Limit.AdHoc.Recipients` configuration option, the share operation will fail and an error message will be displayed to the user stating the reason for the failure.

Sending and AdHoc package through REST API

The end-user REST API is able to identify Address Book entries by their IDs. When sending a message through REST API recipients can be: user entry IDs, group entry IDs, and email addresses. Email addresses will be filtered out if they are not part of the Address Book and the user is not allowed collaboration with external users. The list of user's available contacts is displayed by making a REST call to `/addressBook`.

Create message draft:

POST `/api/v1.4/mailbox/messages`

POST DATA:

```
to=petya@sofia-pso.tumbleweed.com&cc=<group_entry_id>&bcc=<user_
entry_
id>&subject=from+api&message=sample+message&security=ANONYMOUS_
LINK&question=+What+is+the+name+of+your+best+friend+from+childhoo
d%3F+&answer=&expiration=86400
```

RESPONSE:

```
http://10.232.3.211:8080/api/v1.4/mailbox/messages

200 OK
Headers
Response body

{
 "info": "Draft was successfully created",
 "messageId": "6a5467d4a084445687b1cdc0cd11f3a3"
}
```

Send draft:

PUT
`/api/v1.4/mailbox/messages/6a5467d4a084445687b1cdc0cd11f3a3/send`

Consider the following use case:

A user creates a draft and specifies an email address in the **To** recipient category, an Address Book entry ID in **CC** and an Address Book group ID in **BCC**. When the user sends the message the following happens:

- If the email address specified in **To** does not belong to any entry of the current user's Address Book, the message will be sent to that email address only if the **Allow collaboration** option is enabled for this user.
- The group ID specified in **CC** will be searched in user's Address Book and if it is found, it will be resolved to all users email addresses that belong to this group.
- The user ID specified in **BCC** will be searched in user's Address Book and if it is found, it will be resolved to corresponding entry email address.
- The message will be sent to all resolved email addresses.

Note If the total number of resolved collaborators exceeds the value of the `AddressBook.Limit.AdHoc.Recipients` configuration option, the share operation will fail and an error message will be displayed to the user stating the reason for the failure.

Note If **Allow Collaboration** is turned off and the user tries to send mail to an external user, the user will be removed from recipients list and a warning message will be displayed in the server log.

Sharing a folder through REST API

When sharing a folder through REST API collaborators can be user entry IDs, group entry IDS, and email addresses. Email addresses will be filtered out if they are not part of the Address Book and the user is not allowed collaboration with external users. The list of user's available contacts is displayed by making a REST call to `/addressBook`.

Example request for sharing folder (`sharedFolder`) with an Address Book user entry:

PUT `/api/v1.4/shares/sharedFolder`

DATA:

```
'{
 "users": [
  "<user_entry_id>"
 ],
 "shareRights": 7,
"notifications": 1,
"ownerNotifications": 1,
"showCollaboratorsToAll": true
}'
```

Note Only collaborators' email addresses will be listed when getting sharing metadata for the specified folder, display names will not be showed even if collaborators are part of the Address Book.

Note If the total number of resolved collaborators exceeds the value of the `AddressBook.Limit.AdHoc.Recipients` configuration option, the share operation will fail and an error message will be displayed to the user stating the reason for the failure.

Address Book REST API

This topic provides Address Book administrator and end user REST API examples and provides REST API support information for Address Book recipients.

Administrator REST API

The Address Book functionality introduces the following REST API endpoints which allow configuring and assigning address book data sources on all configuration levels:

- Address Book Global Registry REST API

  GET `/addressBookSources` - Lists all available Address Book data sources.

  GET `/addressBookSources/<ABSourceId>` - Gets an Address Book data source.

  POST `/addressBookSources/<ABSourceId>` - Modifies properties: enabled, group.

- Business Unit Address Book REST API

  GET `/businessUnit/<name>/addressBookSources` - Gets list of the assigned Address Book sources

  PUT `/businessUnit/<name>/addressBookSources/` - <set of Address Book entries in the body> - replaces all assigned to a business unit.

  GET `/businessUnit/<name>/addressBookSources/<ABSourceId>` - Gets an Address Book source assigned to a business unit.

  POST `/businessUnit/<name>/addressBookSources/<ABSourceId>` - Assigns and updates an Address Book source to a business unit. The body may contain the parent group.

  DELETE `/businessUnit/<name>/addressBookSources/<ABSourceId>` - Removes an Address Book source from those assigned to a business unit.

- Account Address Book REST API

  GET `/accounts/<name>/addressBookSources/` - Gets list of assigned Address Book sources to an account.

  PUT `/accounts/<name>/addressBookSources/` - <set of Address Book entries in the body> - replaces all assigned.

  GET `/accounts/<name>/addressBookSources/<ABSourceId>` - Gets an Address Book source assigned to an account.

POST `/accounts/<name>/addressBookSources/<ABSourceId>` - Assigns or updates an Address Book source to an account. The body may contain the parent group property.

DELETE `/accounts/<name>/addressBookSources/<ABSourceId>` - Removes an Address Book source from the list of assigned sources to an account.

GET `/accounts/<accountName>/addressBook/contacts` - Get address book contacts of a specified account entity.

POST `/accounts/<accountName>/addressBook/contacts` - Create address book contacts to a specified account entity.

DELETE `/accounts/<accountName>/addressBook/contacts/<id>` - Delete an address book contact of an account entity.

PUT `/accounts/<accountName>/addressBook/contacts/<id>` - Update an address book contact of an account entity.

- Address Book global settings

  GET `/addressBookSources/settings/` - Gets `AddressBook.AllowCollaboration` and `AddressBook.Enabled` server configurations.

  POST `/addressBookSources/settings/<name>` - Updates `AddressBook.AllowCollaboration` server configuration.

End User REST API

The following endpoints are exposed for the end user REST API:

- **GET** `/addressBook` - Lists all available contacts for the given account.
- **GET** `/addressBook?displayName=test%K&mail=test@axway.com&group=Axway&type=user&orderBy=email&limit=10&offset=0` - Search for all entries matching all parameters together. The search is case sensitive for all sources except for LDAP sources. The logical operation between the parameters is AND.
- **GET** `/addressBook?searchFor=test&limit=10&offset=0` - Searches all entries which `displayName`, email or group contain the given value. The search is case insensitive. The search phrase is looked up anywhere in the fields `displayName`, email, and group (wildcard search), except for LDAP sources where it is looked up in the beginning of these fields only (wildcard is at the end of the search phrase). The logical operation between the fields is OR.
-

Parameter Name	Description	Type
`displayName`	Optional. Case sensitive exact search by `displayName` field.	String
`mail`	Optional. Case sensitive exact search by `mail` field.	String

Parameter Name	Description	Type
`parentGroup`	Optional. Case sensitive, exact search by `parentGroup` field.	String
`type`	Optional. Case insensitive search by `type`. The `type` can be either a user or a group.	String
`orderBy`	Optional. Specify the sort order of the result. Could be `displayName` or `email`.	String
`limit`	Optional. Page size for pagination. If not specified a default value will be set.	Integer
`offset`	Optional. Starting index of the pagination. If not specified a default value will be set.	Integer
`searchFor`	Optional. Case insensitive, wildcard search between `group`, `displayName`, and `mail` parameters.	String

- **GET** `/addressBook/count` - Returns the count of all Address Book entries from all enabled Address Book sources assigned to the current user.
- **GET** `/addressBook/<id>` - Gets an address book entry by ID.
- **GET** `/addressBook/myself` - Returns map of Address Book settings with their corresponding values. This includes the following:
  - `addressBookEnabled` – A flag indicating if Address Book is enabled.
  - `addressBookCollaborationAllowed` – A flag indicating if collaboration with external recipients is allowed for the given user.
  - `addressBookMinSearchLength` – Specifies the minimum search string length when performing wildcard search for Address Book entries.
  - `addressBookMaxDisplayEntries` – Specifies the maximum limit of Address Book entries displayed in a single page.
  - `addressBookMaxDisplayPages` – Specifies the maximum limit of Address Book pages in a single request.

Address Book entry schema:

```
AddressBookEntry {
    id: addressBookSourceId:addressBookEntryId,
    displayName,
    mail,
    parentGroup,
    type,
```

```
    customAttr1,
    customAttr2,
    customAttr3
}
```

Note:

The following methods are also available for the `/addressBook` end user REST resource. They are not implemented in SecureTransport 5.3.6.

- **POST** `/addressBook/` - Creates a new user specific entry. The Address Book provider to which entry will be created will generate `ABEntry` ID. The Address Book source is defined by `parentGroup` property mapping.
- **PUT** `/addressBook/<id>` - Updates the user specific entry.
- **DELETE** `/addressBook/<id>` - Deletes the user specific entry.

For each one of them the SecureTransport server returns a response status **403 Forbidden**.

Support for Address Book recipients

Whenever an Address Book user inputs a group or display name either as an email recipient or shared folder collaborator, SecureTransport is able to resolve the recipients email addresses. If the given group members count exceed a predefined value, an error message is shown to the end user and the operation is aborted. A server configuration option is exposed for setting that value - `AddressBook.Limit.AdHoc.Recipients`.

Whenever an end user sends a mail or shares a folder with group or display name in its recipients list, the REST call includes the Address Book entry IDs which corresponds to the names. If the list of recipients does not include Address Book entries, the REST call contains the actual email addresses. This allows the SecureTransport back end to handle cases with recipients not in the Address Book as well as recipients defined in the Address Book, or to determine if the Address Book is enabled or not.

When the client sends a request with Address Book entry IDs and email addresses, all package recipients are stored in the `.stfs` attributes and later when a list operation is performed the response contains the stored recipients (for example, IDs as well as email addresses). If sharing a folder, the SecureTransport will always return the email addresses.

Operations 3

Use the Operations menu of the Axway SecureTransport Administration Tool to initiate operator-driven actions, planned daily tasks, statistics, monitors, and responses to events.

The Administration Tool server runs as an HTTPS server using port 444 by default. The Administration Tool server starts automatically each time a UNIX-based system starts. The installer includes a startup item in the system's `rc` directory tree. On a Windows system, the server runs as a service.

You can also manually start the Administration Tool server by executing the following commands:

- For UNIX, go to `<FILEDRIVEHOME>/bin` and run `./start_admin`.
- For Windows, go to `<FILEDRIVEHOME>\bin\` and run `start_admin.com`.

Note The Administration Tool server reserves ports 8004 and 8005 to be used by the Java-based component. These ports are used strictly for internal communication within the Administration Tool and cannot be used for other purposes.

The following topics provide additional operations menu information and describe the operations menu functions and configurable items:

- *Operations menu overview* on page 250 - When you log in to the SecureTransport Administration Tool, the *Operations* tab is displayed.
- *Server control* on page 250 - Use the *Server Control* page to manage the protocol and TM component servers of your SecureTransport system. On the *Server Control* page for a SecureTransport Server you can specify port, SSL key alias, and FIPS transfer mode settings for the FTP, HTTP, AS2, SSH, PeSIT, and Transaction Manager (TM) servers and start and stop them.
- *Server usage monitor* on page 287 - Use the *Server Usage Monitor* page to view the number of users in each user class who are logged in to the FTP and HTTP servers and the FTP bandwidth used at a specific time.
- *Track file transfer activity* on page 290 - Use the *File Tracking* page to view information about both client-initiated and server-initiated file transfers and to cancel or resubmit transfers.
- *Server log* on page 304 - Use the *Server Log* page to view the contents of the SecureTransport log messages from the following SecureTransport components: the Transaction Manager (TM) and the processes that implement the AS2, FTP, HTTP, SSH (SFTP), and SOCKS5 protocols, the Administration Tool interface (ADMIN), and auditing (AUDIT).
- *Audit log* on page 308 - Use the *Audit Log* page to view, compare, and export log entries that SecureTransport records when any change is made to the SecureTransport configuration.
- *Server configuration* on page 314 - SecureTransport server configuration consists of all the information the server and its components require to operate. You establish most of the server configuration by setting fields on the various pages of the Administration Tool.

- *Support tool* on page 324 - The Axway SecureTransport support tool collects information about SecureTransport and its host operating system and saves it in a support information file that you can send to Axway Global Support to help them diagnose an issue.
- *Directory browsing* on page 328 - By setting up a directory structure, you can access system drives and network mounts on Windows.
- *Standard browser client* on page 329 - You can use a standard browser, such as Firefox or Microsoft Internet Explorer (IE) to connect to a SecureTransport Server.
- *Server backup* on page 333 - To minimize the risk of data loss, perform regular backups of the SecureTransport Server and SecureTransport Edge data.

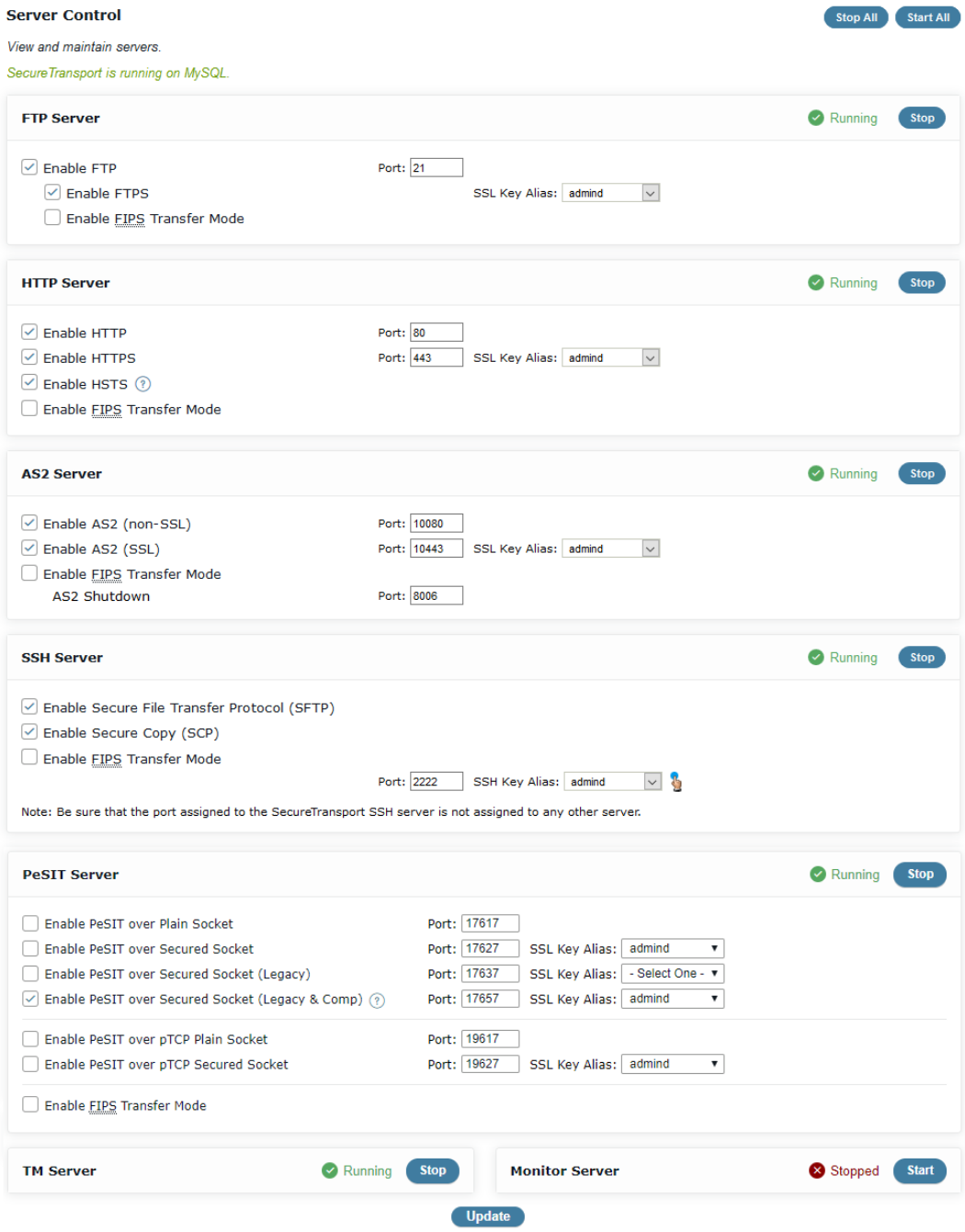
Operations menu overview

When you log in to the SecureTransport Administration Tool, the *Operations* tab is displayed. The *Operations* tab contains the following pages:

- **Server Control** – Used to manage your FTP, HTTP, AS2, SSH, PeSIT, Transaction Manager (TM), and Monitor servers. For details, see *Server control* on page 250.
- **Cluster Management** – Used to view and maintain SecureTransport Servers in cluster. For details, see *Standard Cluster* on page 335 and *Enterprise Cluster* on page 351.
- **Server Usage Monitor** – Used to monitor by user class the FTP, SSH and HTTP, as well as the protocol bandwidth consumed. For details, see *Server usage monitor* on page 287.
- **File Tracking** – Displays a log of the status and attributes of each file transfer. Also, used to display detailed information about a transfer and to cancel or resubmit a transfer. SecureTransport Server only. For details, see *Track file transfer activity* on page 290.
- **Server Log** – Used to view, search, and filter the logs from the SecureTransport Server. For details, see *Server log* on page 304.
- **Audit Log** – Used to view, compare, and export log entries that SecureTransport records when any change is made to the SecureTransport configuration. For details, see *Audit log* on page 308.
- **Server Configuration** – Used to view, change, export, and import server configuration settings. For details, see *Server configuration* on page 314.
- **Support Tool** – Used to collect information about SecureTransport and its host operating system and save it in a support information file that you can send to Axway Global Support. For details, see *Support tool* on page 324.

Server control

Use the *Server Control* page to manage the protocol and TM component servers of your SecureTransport system. On the *Server Control* page for a SecureTransport Server you can specify port, SSL key alias, and FIPS transfer mode settings for the FTP, HTTP, AS2, SSH, PeSIT, and Transaction Manager (TM) servers and start and stop them. These are the component servers of the SecureTransport Server. You can also start and stop the Monitor server.



On the *Server Control* page for a SecureTransport Edge, there is no *TM Server* pane because the Transaction Manager does not run on the SecureTransport Edge, but you can configure the port for the SecureTransport Edge proxy server. For details, see *Manage the Proxy server on SecureTransport Edge* on page 260.

Note By default, SecureTransport Edge uses a cipher strength of `AES 256` for communication between its protocol servers and the TM Server on the SecureTransport Servers. To change the cipher suites enabled, edit the

`TransactionManager.Listeners.Ssl.enabledCipherSuites` server configuration parameter. For valid values, see the cipher suites listed for transfers using AS2, FTPS, HTTPS, and PeSIT over secured socket in the *SecureTransport Cipher suites* topic, part of the *SecureTransport 5.4 Security guide*.

When you disable any of the component servers using the Administration Tool, the scripts used to run the servers from the command line are renamed with the `.disable` extension. To disable a server clear the check box for that server. Once the servers are enabled, the files are restored to the original name. For example, if you disable the FTP server, the script `start_ftpd` is renamed to `start_ftpd.disable`. Once you select the enable check box and start the server using the Administration Tool, the script name returns to `start_ftpd`. All utility scripts are located in the `<FILEDRIVEHOME>/bin` directory.

The following topics provide additional information for managing and monitoring the servers:

- *Manage server operations* on page 252 - Describes monitoring server status indicators, starting and stopping servers, and reloading the server configuration.
- *Manage the FTP server* on page 254
- *Manage the HTTP server* on page 254
- *Manage the AS2 server* on page 255
- *Manage the SSH server* on page 256
- *Manage the PeSIT server* on page 258
- *Manage the Transaction Manager server* on page 259
- *Manage the Proxy server on SecureTransport Edge* on page 260
- *Manage the Monitor server* on page 260
- *Use the operating system to monitor SecureTransport processes* on page 261

Manage server operations

The following topics describe monitoring server status indicators, starting and stopping servers, and reloading the server configuration:

- *Server status indicators* on page 252
- *Start and stop servers* on page 253
- *Reload server configuration* on page 253

Server status indicators

The table below lists the various status options available from the *Server Control* page and when SecureTransport displays that status.

Status	Description	Used during:
Running (displayed in green)	The server is running normally.	Normal operation
Running (displayed in blue)	An HTTP or FTP server suspension is pending, with the server suspension information displayed below.	Scheduled suspensions
Not Running (displayed in red)	The server is stopped.	Disabled or stopped servers
Suspend (displayed in red)	The HTTP or FTP server is scheduled to suspend in the near future. The HTTP or FTP server is running, but does not allow transfers. Users can still connect and get messages.	Temporary suspensions, such as for maintenance

Start and stop servers

Use the button to the right of the status indicator for each server to start or stop that server. Always restart a server when you change a port number or enable FIPS transfer mode.

- When the server is not running, the button label is **Start**. Click it to start the server. You'll be promoted with the following message: "Do you want to start a [name of the server]". If you click **Yes**, the server will start.
- When the server is running, the button label is **Stop**. Click it to stop the server. You'll be promoted with the following message: "Do you want to stop a [name of the server]". If you click **Yes**, the server will stop.

Use the **Stop All** and **Start All** buttons in the top right corner of the *Server Control* page to stop or start all servers. **Stop All** stops all running servers. **Start All** start all protocol servers that are enabled plus the TM server. It also start the Monitor server if it was running and then stopped.

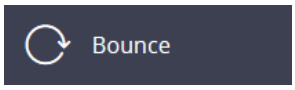
Note When a server is stopped or disabled, its services are unavailable.

Note In case of low disk space do not start servers.

Reload server configuration

The SecureTransport server configuration is stored in the database and loaded into the server component processes when they start or when the configuration changes. You can bounce the server to force a configuration reload. This is the procedure for a stand-alone SecureTransport Server or a SecureTransport Edge. To bounce servers in a cluster, use the *Cluster Management* page.

In the SecureTransport menu bar, click **Bounce**.



The server reloads its configuration. If the bounce is successful, the server displays an "OK" message.

Note A Standard Cluster (SC) must be manually synchronized prior to executing a Bounce on any secondary nodes in the Standard Cluster. For information on Standard Cluster synchronization, refer to *Standard Cluster synchronization* on page 348

Manage the FTP server

To use FTP, specify the FTP settings for both the SecureTransport Edge and SecureTransport Server.

1. Select **Enable FTP**.
2. The default FTP port number is 21 for root installation and 8021 for non-root installation. If the default port is in use, SecureTransport displays a message and you must change the FTP **Port** to use a port number other than the default setting.

Note FTP might already be running on port 21. To avoid a port conflict, you can disable FTP at the OS level or assign it a different port number instead of changing the port number in SecureTransport.

3. To enabled FTPS:
    a. Select **Enable FTPS**.
    b. Select an **SSL Key Alias** from the drop-down list, for example, `ftpd`. For information about storing the FTPS certificate in a hardware security module, see *Store certificates in a hardware security module* on page 69.
    c. To restrict FTPS connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** check box. For more information, see *FIPS transfer mode* on page 983.
4. Click **Start**.

Note To enable FTP without SSL (FTP and not FTPS), you must disable SSL FTP connections and create an SSL encryption entry for a user class with SSL encryption optional. See *Manage SSL access* on page 719.

For information about more FTP settings, see *Configure FTP server messages and modes* on page 76.

Manage the HTTP server

To use HTTP, specify the HTTP settings for both the SecureTransport Edge and SecureTransport Server.

1. Select one or both of **Enable HTTP** and **Enable HTTPS**. If you select Enable HTTPS, by default **Enable HSTS** will also be selected. You can also deselect **Enable HSTS** once **Enable HTTPS** is selected. When HSTS is enabled, a HSTS response will always be sent, redirecting the plain HTTP connection to HTTPS. Enabling HSTS requires a HTTP server restart.

For more information on the HSTS server configuration options, see *Security-related HTTP headers and policies*.

2. The default HTTP port number is 80 for root installations and 8080 for non-root installations. The default HTTPS port number is 443 for root installations and 8443 for non-root installations. If a default port is in use, SecureTransport displays a message and you must change the **Port** to use a port number other than the default setting.
3. If you enabled HTTPS, select an **SSL Key Alias** from the drop-down list, for example, `httpd`. If you enabled HTTPS, HSTS will also be enabled unless you deselect it. For information about storing the HTTPS certificate in a hardware security module, see *Store certificates in a hardware security module* on page 69.
4. If you enabled HTTPS, to restrict HTTPS connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** check box. For more information, see *FIPS transfer mode* on page 983.
5. Click **Start**.

Note To enable HTTP without SSL (HTTP and not HTTPS), you must create an SSL encryption entry for a user class with SSL encryption optional. See *Manage SSL access* on page 719.

Manage the AS2 server

AS2 (Applicability Statement 2) is a specification about how to transport data securely and reliably over the Internet. Security is achieved by using digital certificates and encryption. The AS2 specification describes how to exchange business data securely and reliably using HTTP as an underlying transport. The data is packaged using standard MIME content types so you can use XML, EDI, binary data, and any other data describable in MIME. Message security (authentication, confidentiality) is implemented using S/MIME. Message reliability is enabled through the use of MDNs. Nonrepudiation and Nonrepudiation of Receipt are business and legal concepts that build upon the security and reliability components in AS2.

If an AS2 license is available, enable the AS2 server. Specify the AS2 settings on both SecureTransport Server and SecureTransport Edge.

1. Select one or both of **Enable AS2 (non-SSL)** and **Enable AS2 (SSL)**.
2. Type a port for each protocol you enabled. The default ports are 10080 for AS2 (non-SSL) and 10443 for AS2 (SSL).
3. If you enabled AS2 (SSL), select an **SSL Key Alias** from the drop-down list.
4. If you enabled AS2 (SSL), to restrict AS2 (SSL) connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** check box. For more information, see *FIPS transfer mode* on page 983.
5. In the **AS2 Shutdown Port field,** type a shutdown port for AS2 server. The default port number is 8006.
6. Click **Start**.

Note To enable AS2 without SSL, you must create an SSL encryption entry for a user class with SSL encryption optional. See *Manage SSL access* on page 719.

For information about more AS2 settings, see *Configure AS2 server settings* on page 84.

Manage the SSH server

Secure Shell (SSH) is a command interface and protocol that a user can use to connect to a remote host over an encrypted connection. SecureTransport provides an SSH server that authenticates users of an SSH or SFTP client and enables users to perform file transfers over an SSH channel.

Note The default port number for the SecureTransport SSH server is 22 for a root installation, and 8022 for a non-root installation. This port is typically assigned to the native SSH server. The SecureTransport SSH server and the native SSH server cannot share the same port. Use another available port for the SecureTransport SSH server. If the SSH port number is changed, restart the SSH server to apply the change.

For information about more SSH settings, see *Configure SSH server settings* on page 85.

The following topics provide additional information for managing the SSH server:

- *SCP and SFTP support* on page 256
- *Secure File Transfer Protocol* on page 257
- *SSH settings* on page 257
- *Configure third party clients for SSH* on page 258

SCP and SFTP support

The SecureTransport SSH server supports the protocol version and the following SSH file transfer features:

- Secure Copy (SCP)
- Secure File Transfer Protocol (SFTP)

SecureTransport SSH file transfers can be performed using third-party SSH clients that support SFTP or SCP. (For a complete list of supported SSH clients, see *Axway and third-party software support* on page 39.)

Note SecureTransport SSH does not support guaranteed delivery of file transfers and interactive SSH sessions.

SCP and SFTP commands use the pattern matching rules in the following table. A file name is composed of regular characters and special pattern matching characters that include the following:

Pattern	Description
`?`	Matches zero or one characters.
`*`	Matches zero or more characters.
`[abc]`	Matches a single character from the character listed.

Pattern	Description
[*a*-*b*]	Matches a single character in the range from character *a* to character *b*.
[^*abc*]	Matches a single character that is not listed.
[^*a*-*b*]	Matches a single character not in the range from character *a* to character *b*.
/	Matches one or more directory path separator characters. Slash (/) is sensitive to the underlying operating system and matches the native directory path separator character for the underlying system. For example, it matches / on UNIX-based systems and matches both / and \ on Microsoft Windows systems. This makes it possible to use the same file name pattern on any operating system.
any other character	Matches that character literally.
pq	Matches pattern *p* followed by pattern *q*.
!*p*	Matches any string that pattern *p* does not match.
c	Backslash (\) removes (escapes) any special meaning of character *c*.

Secure File Transfer Protocol

Secure File Transfer Protocol (SFTP) is a protocol for transferring files over an encrypted SSH channel.

While the SFTP protocol provides a wide-range of operations, not all of these operations are relevant to SecureTransport file transfers. The SecureTransport SSH server accepts the following SFTP client file operations only:

- Upload and download (including cancel and resume)
- Create directory
- Remove directory
- Remove file
- Rename file
- Get directory listings
- Change file mode

SSH settings

If you are using SSH, specify the SSH settings for both the SecureTransport Edge and SecureTransport Server.

1. Select one or both of **Enable Secure File Transfer Protocol (SFTP)** and **Enable Secure Copy (SCP)**.
2. Type a port for the SSH server.
3. If the operating system SSH server is using port 22, assign a different port number. To avoid a port conflict, you can disable SSH at the OS level or assign it a different port number instead of changing the port number in SecureTransport. To avoid this conflict, the operating system SSH port for Axway appliances is 10022 by default.
4. Select an **SSH Key Alias** from the drop-down list. The list includes certificates with RSA and DSA keys.
5. To restrict SSH (SFTP and SCP) connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** check box. For more information, see *FIPS transfer mode* on page 983.
6. Click **Start**.

To view the SSH Server Public Key Fingerprint, click **View Fingerprint**.

Note **View Fingerprint** does not work until a key alias is assigned and the page is updated.

Configure third party clients for SSH

Some third-party clients might provide a Resume function that is not compatible with SSH in SecureTransport.

The Resume function fails because of a conflict with post-transmission actions: the file is uploaded using a different extension, such as `.part` and once uploaded the third party client renames it back to the original file name. At this point the post-transmission actions cause the transfer to fail because SecureTransport cannot find the file with the `.part` extension. To avoid this issue, disable the third party client resume feature.

Manage the PeSIT server

PeSIT (Protocole d'Echanges pour un Systeme Interbancaire de Telecompensation, in English, Exchange Protocol for an Interbank Teleclearing System) is a file transfer protocol and framework developed by GSIT, the French interbank teleclearing system. SecureTransport implements the PeSIT version E non-SIT profile and supports the following features also supported by Axway Transfer CFT:

- Mutual authentication by passwords
- Send and receive
- ASCII, EBCDIC and BINARY transfer modes
- Fixed and variable record formats
- Data compression during transfer
- Transfer checkpoint and automatic restart
- Flow control with sliding window
- Integrity checking

- Store and forward routing
- pTCP protocol version 2

When a partner sends a file to SecureTransport using PeSIT, SecureTransport retains the values of many PeSIT PI codes with the file as metadata. The expression in the **User Message Send** field of a PeSIT transfer site can access the protocol identifier (PI) values. For details, see *PeSIT transfer sites* on page 559.

When SecureTransport routes a transferred file to a final PeSIT destination, SecureTransport includes both PI 61 and PI 62.

Because PeSIT transmissions can use SSL, SecureTransport include options to enable SSL.

To use PeSIT, specify the PeSIT settings for both the SecureTransport Edge and SecureTransport Server.

1. Select one or more of the PeSIT transmission options:
    - **Enable PeSIT over Plain Socket** – PeSIT over TCP/IP without SSL
    - **Enable PeSIT over Secured Socket** – PeSIT over TCP/IP using TLS Comp
    - **Enable PeSIT over Secured Socket (Legacy)** – PeSIT over TCP/IP using TLS Legacy Note that PeSIT transfers between SecureTransport and other MFT clients over TLSv1 Legacy fail for certain ciphers. For more information, refer to *Troubleshoot common problems* on page 968.
    - **Enable PeSIT over Secured Socket (Legacy § Comp)** – PeSIT over TCP/IP with SSL/TLS. When SecureTransport is the server, it automatically detects the used SSL/TLS mode - Legacy or Comp, and sets the header length in the FPDU. Information about the detected mode is logged in the server log under **Level > Debug**.
    - **Enable PeSIT over pTCP Plain Socket** – PeSIT over parallel TCP/IP without SSL
    - **Enable PeSIT over pTCP Secured Socket** – PeSIT over parallel TCP/IP using SSL
2. If you are not using the default port, type a port for each option you selected.
3. If you enabled any SSL option, select an **SSL Key Alias** from the drop-down list.
4. If you enabled any SSL option, to restrict PeSIT SSL connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** check box. For more information, see *FIPS transfer mode* on page 983.
5. Click **Start**.

Note To enable PeSIT without SSL (over plain socket), you must create an SSL encryption entry for a user class with SSL encryption optional. See *Manage SSL access* on page 719.

For information about more PeSIT settings, see *PeSIT server configuration settings* on page 88.

Manage the Transaction Manager server

The Transaction Manager (TM) server connects to the ports specified in the network zones. For more information, see *Communication across Transaction Manager, protocol, and proxy servers* on page 215.

- Click **Start**.

Manage the Proxy server on SecureTransport Edge

On the SecureTransport Edge, specify the port for the SecureTransport proxy server. The proxy port is used by SecureTransport Server to handle outgoing connections passed through a SecureTransport Edge. The default is port number 1080.

1. Select **Operations > Server Control**.

   The *Server Control* page is displayed.

2. Under **Proxy Server**, enter a value in the **Proxy Port** field.
3. Click **Start**.

Manage the Monitor server

The Monitor server checks that the SecureTransport servers are running and restarts them if they terminate. However, the Monitor server does not restart a server if a dependent server is not running. The Monitor server can run on SecureTransport Server or SecureTransport Edge.

- Click **Start**.

You can configure the overall behavior of the Monitor server by changing cluster-wide server configuration parameters.

- `Cluster.ServiceStatusChecks.delayBetweenChecks` – the time in seconds that the Monitor server waits between checking the servers. The default is 5 seconds. This parameter is only supported for Standard Cluster (SC).
- `Cluster.ServiceStatusChecks.serviceExpireTime` – the time in seconds that a server is down before the Monitor server stops checking the server and attempting to restart it. The default is 15 seconds. Once the Monitor server stops attempting to restart a service, you must restart it manually. This parameter is only supported for Standard Cluster.

You can configure how the Monitor server attempts to restart each server by changing local configuration parameters. The parameters include one of the server names: `ADMIN`, `AS2D`, `DB` (embedded database only), `FTPD`, `HTTPD`, `SSHD`, and `TM`.

- `Monitor.<server>.retryCount` – how many times the Monitor server tries to restart the server. The default value varies depending on the server.
- `Monitor.<server>.retryDelay` – the time in seconds that the Monitor server waits between attempts to restart the server. The default value varies depending on the server.

Note The Monitor server must use a non-SSL connection to check the PeSIT server, so you must select **Enable PeSIT (no SSL)** on the *Server Control* page for monitoring. To prevent non-SSL PeSIT connections, restrict access to the non-SSL port you configure to the system where the PeSIT server and the Monitor server are running.

Entries in crontab start the monitor server processes. For example,

```
* * * * * "<FILEDRIVEHOME>/bin/monitor_admin" >> /tmp/monitor_
admin.out 2>&1
```

controls monitoring of the Administration Tool server. The entries run the processes every minute and append the log output to files in the `/tmp` directory on UNIX-based systems and the `<FILEDRIVEHOME>\..\cygwin\tmp` directory on Windows.

Note On Windows, it is not possible to modify existing cron jobs or to use cron to run any jobs other than the predefined SecureTransport jobs. Instead, use the Windows Task Scheduler.

Use the operating system to monitor SecureTransport processes

As an alternative to the Monitor server, you can monitor the state of specific processes using operating system tools.

There are two categories of processes, those that implement file transfer and related functions and those that implement the administrative functions. You need to know their process IDs to monitor them.

The following topics describe the file transfer and admin processes:

- *File transfer processes* on page 261
- *Admin processes* on page 262

File transfer processes

For file transfer, there are six parent processes to monitor:

- java – AS2 proxy server
- java – FTP server
- java – HTTP server
- java – PeSIT server
- java – SSH server
- java – Transaction Manager server
- mysqld – Embedded (MySQL) database server, when used

The first five processes all interact with the Transaction Manager server.

The process IDs for each for these processes can be found in `<FILEDRIVEHOME>/var/run`. The files are called:

- `as2d.pid`
- `ftpd.pid`
- `httpd.pid`

- `pesitd.pid`
- `sshd.pid`
- `tm-java.pid`
- `db.pid`

Admin processes

For administration functions, there is one parent processes to monitor:

- java – Tomcat Admin server

It interacts with the file transfer processes by manipulating configuration and performing signaling.

The process ID for this process can be found in `<FILEDRIVEHOME>/var/run/admin/tomcat.pid`.

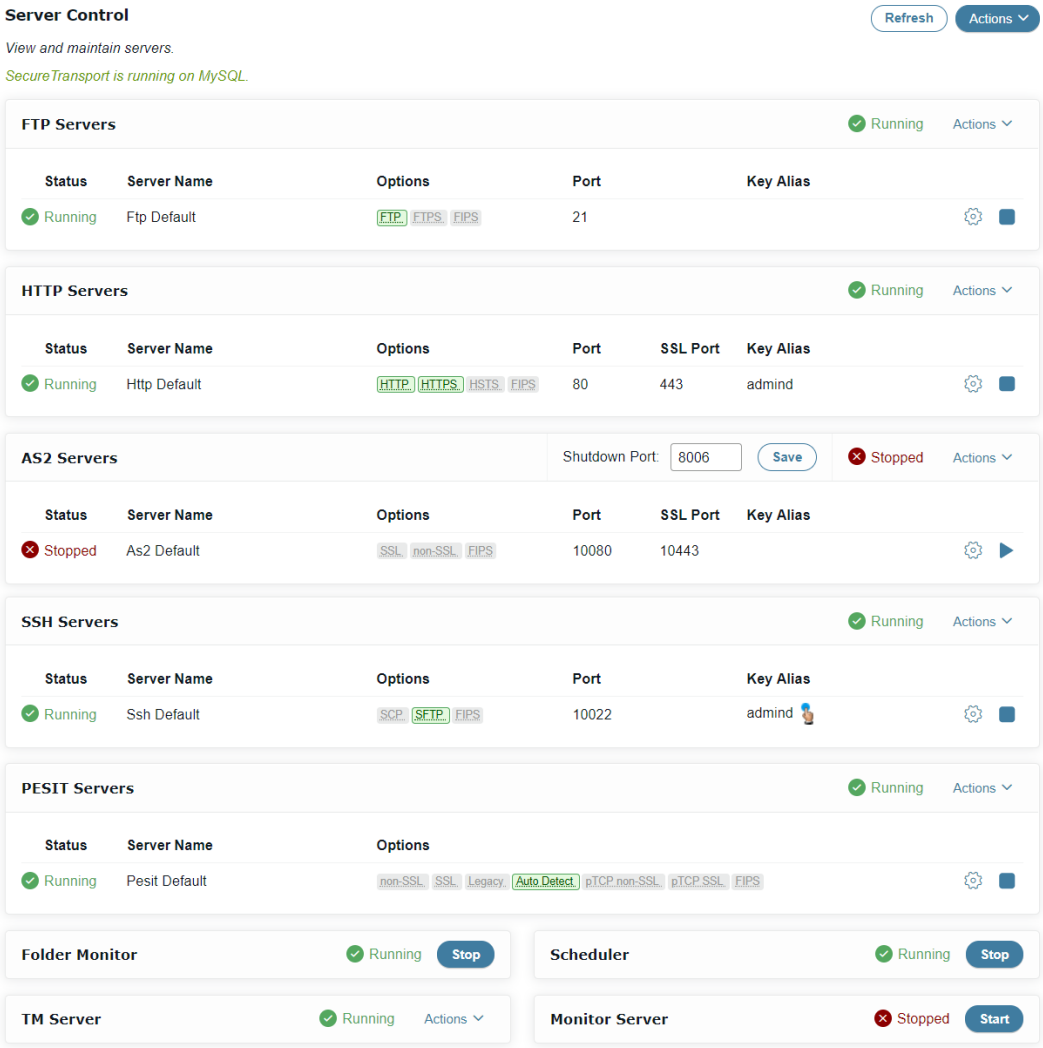
Extended Server Control

Starting with SecureTransport 5.4 Patch 7, a separate management view of the *Server Control* page is introduced. On top of a minor revamp of the regular *Server Control* page layout, the extended view provides controls to add more (listeners to) protocol servers, namely FTP, SSH, HTTP, AS2, and PeSIT.

Extended server control is available for both SecureTransport Server and SecureTransport Edge.

Note Visibility of extended view of the *Server Control* page is controlled by a server configuration option: `ServerControl.ExtendedUI.Enabled`. By default, it is set to *false* and you must set it to *true* in order to enable the server control extended view.

The following image presents the extended view of the *Server Control* page.



The extended view provides the following extended options:

- **Refresh** the page
- perform **Actions** to all servers:
  - **Start All Services**
  - **Stop All Services**
  - **Shutdown Node Gracefully** – this option allows you to perform Graceful shutdown on the SecureTransport Server. For more information, see *Graceful shutdown of SecureTransport Server node* on page 267
- perform **Actions** per daemon: this drop-down list allows you to:
  - start and stop protocol servers
  - add one or more protocol servers
  - gracefully shut down all protocol servers (see *Graceful shutdown* on page 264)
- the "gear" icon allows you to edit the configuration parameters of the corresponding server

- the "play" icon(when server stopped) interchanges with the "stop" icon (when server running); these controls apply the corresponding action to the selected server only

You also have the options to start and stop the following SecureTransport-specific services:

- *Monitor server*
- *Proxy Server* – only available on SecureTransport Edge. For more information see *Manage the Proxy server on SecureTransport Edge* on page 260.
- *Folder Monitor* – only available on SecureTransport Server. Note that the Folder Monitor functionality is dependent on the value of the `FolderMonitor.enable` Server Configuration option.
- *Scheduler* – only available on SecureTransport Server. Note that the Scheduler functionality is dependent on the value of `Scheduler.enable` Server Configuration option.
- *Transaction Manager server* – you can perform the following **Actions**:
  - **Stop Server** instantly
  - Perform **Graceful Shutdown** – for more information, see *Graceful shutdown of Transaction Manager* on page 266.

Note

`Scheduler.enable` and `FolderMonitor.enable` do not start or stop the respective cluster services; these Server Configuration options only enable or disable the service. When Transaction Manager is running and Folder Monitor/Scheduler is disabled from the Server Configuration (the respective configuration parameter is set to `false`), the service runs in the background but does not do any job (schedule events or pull files). Folder Monitor/Scheduler is running and functional only when the Transaction Manager is started and Folder Monitor/Scheduler is started and enabled from the Server Configuration.

The following topics provide more detail on adding and editing protocol servers:

- *Add an FTP server* on page 268
- *Add an SSH server* on page 278
- *Add an HTTP server* on page 271
- *Add an AS2 server* on page 275
- *Add a PeSIT server* on page 282

Graceful shutdown

This topic discusses the concept of performing graceful shutdown of the different SecureTransport components and specifics.

Graceful shutdown of protocol servers

Note The current subtopic contains general information and instructions to perform graceful shutdown on any of the available protocol servers, except where noted otherwise. The option to gracefully shut down protocol servers is available on both SecureTransport Server and Edge.

Graceful shutdown is an option to initiate a shutdown of any or all protocol servers without abrupt cancellation of the currently ongoing client-initiated transfer (CIT) sessions. Once initiated, the graceful shutdown waits for the specified grace period before stopping the selected server. This grace period defines the time allowed for existing transfers to get completed before shutting down. You can set its value to the dedicated configuration option parameter per protocol server:

Protocol	Server option	Default value
FTP	`Ftpd.GracefulShutdownTimeout`	`86400s`
HTTP	`Http.GracefulShutdownTimeout`	`30s` – if not previously modified (see note)
AS2	`As2.GracefulShutdownTimeout`	`86400s`
SSH	`Ssh.GracefulShutdownTimeout`	`86400s`
PeSIT	`Pesit.GracefulShutdownTimeout`	`86400s`

Note With HTTP, the `Http.GracefulShutdownTimeout` server option has been available prior to introducing the graceful shutdown functionality. In case its default value has been modified, the input value is stored.

Note that during the graceful shutdown period:

- Existing CITs are allowed to complete within the specified timeout period.
- Any new attempts for file operations are rejected. This includes not only file uploads and downloads but also: directory listing, deleting or renaming files, as well as deleting or creating directories.

Perform protocol server graceful shutdown

Note Before you proceed with graceful shutdown initiation, the Monitor Server must be stopped.

To initiate this process using the Administration Tool, go to the **Actions** drop-down list of the selected protocol server, click to expand it and select ***Graceful Shutdown***. The process will wait for the countdown period as defined in the corresponding configuration option before it starts.

You can also perform this action using a console command in the following format: `stop_ <protocol_daemon> -g -timeout <interval_in_seconds>`.

- the `-g` parameter can be used to stop the daemon gracefully while using the specific daemon default configuration timeout;
- the `-timeout <interval_in_seconds>` parameter is optional and can be used in conjunction with `-g` to offset graceful shutdown with the defined interval (different than the default one, as defined in the server configuration option for the respective protocol). If you omit this parameter, graceful shutdown will be performed using the respective configuration option value.

For example, if you want to initiate graceful shutdown after 60 seconds using the console command for the respective protocol daemon, enter:

- `stop_ftpd -g -timeout 60` for the FTP daemon
- `stop_httpd -g -timeout 60` for the HTTP daemon
- `stop_as2d -g -timeout 60` for the AS2 daemon
- `stop_sshd -g -timeout 60` for the SSH daemon
- `stop_pesitd -g -timeout 60` for the PeSIT daemon

The option to shut down gracefully a protocol server is also exposed as a REST API resource. For more information, refer to the Admin API Swagger documentation.

Note With HTTP, when you initiate graceful shutdown during active file uploads with the ST Web Client, these uploads will be processed until the current chunk upload is completed. The chunk size is defined as the value of the `uploadChunkSize` parameter in the ST Web Client configuration. By default, its value is `100 MB`, which means that in all cases uploads of files with sizes smaller than 100 MB will be completed during the graceful shutdown. With larger files, uploads might be completed as well; or could be stopped depending on the current chunk upload.

Graceful shutdown logging

The server log displays information about active connections during an initiated graceful shutdown. For better visibility, a dedicated server option is introduced: `GracefulShutdown.Logging.Interval`. By default its value is `60s` which means that active transfer information will be logged once every 60 seconds until all transfers are completed. Note that the graceful shutdown logging interval applies to all protocol servers.

Graceful shutdown of Transaction Manager

Graceful shutdown is a feature that allows you to have a planned Transaction Manager (TM) stop without abrupt cancellation of:

- current SITs
- post routing, post transformation, and post processing actions
- Advanced Routing actions

Once initiated, the graceful shutdown waits for the specified grace period before stopping the selected server. This grace period defines the time allowed for existing transfers to get completed before shutting down. You can set its value (in seconds) to the dedicated configuration option parameter: `TransactionManager.GracefulShutdownTimeout`.

To perform Graceful shutdown of the Transaction Manager server, scroll to the bottom of the extended *Server Control* page, then select **Actions** -> **Graceful Shutdown**. The Transaction Manager will be stopped after timeout expiry.

You can also perform this action using a console command in the following format: `stop_tm -g -timeout <interval_in_seconds>`. For example, `stop_tm -g -timeout 60` will shut down the Transaction Manager after 60 seconds.

It is recommended that you configure the timeout period for no less than 30 seconds: otherwise there is a risk that shutdown would not be "graceful".

The option to shut down the Transaction Manager gracefully is also exposed as a REST API resource. For more information, refer to the Admin API Swagger documentation.

Note: Before performing Graceful Shutdown, make sure all protocol servers plus Monitor server are stopped. Make sure that there is no active streaming connection to an Edge server in order to successfully perform TM graceful shutdown.

Graceful shutdown of SecureTransport Server node

Note Remember that before you proceed with graceful shutdown initiation, the Monitor Server must be stopped.

Expand the **Actions** drop-down list on top of the extended *Server Control* page and select the **Shutdown Node Gracefully** to initiate a Graceful shutdown of the entire SecureTransport Server node.

This process undergoes three consecutive steps:

1. Stop the Folder Monitor server and Scheduler server.
2. Gracefully stop all protocol servers.
3. Gracefully stop the Transaction Manager server.

Note Make sure that there is no active streaming connection to an Edge server in order to successfully perform TM graceful shutdown.

Each step will be executed after successful completion of the previous one. The extended *Server Control* page will have messages displayed, providing status on SecureTransport Server node components shutdown.

After completion of step 3, the current SecureTransport Server will not be processing any transfers until all services are restarted. You must perform these steps manually and no particular order is required.

The option to shut down the SecureTransport Server node gracefully is also exposed as a REST API resource. For more information, refer to the Admin API Swagger documentation.

Note When you initiate Graceful shutdown of SecureTransport Server node using the SecureTransport Administration Tool, you must not close or refresh the extended *Server Control* page until all three steps are completed. If you need to perform actions on other screens in the SecureTransport Administration Tool, it is recommended to open a new tab with the selected SecureTransport screen.

Graceful shutdown of SecureTransport Edge node

Note Remember that before you proceed with graceful shutdown initiation, the Monitor Server must be stopped.

Graceful shutdown on Edge is similar to that on SecureTransport Server. Note that there is no Folder Monitor, Scheduler or Transaction Manager component on Edge; however there is the Proxy server.

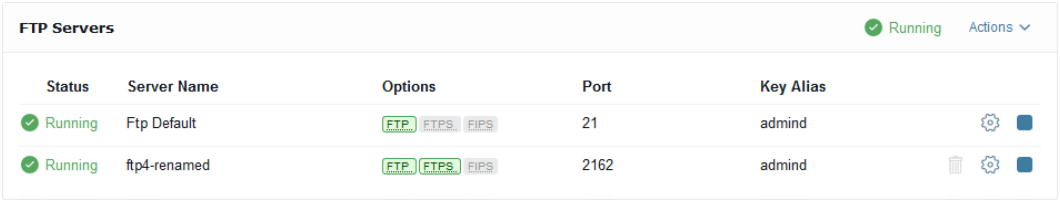
As with Server, expand the **Actions** drop-down list on top of the extended *Server Control* page and select the **Shutdown Node Gracefully**.

This process undergoes two basic consecutive steps:

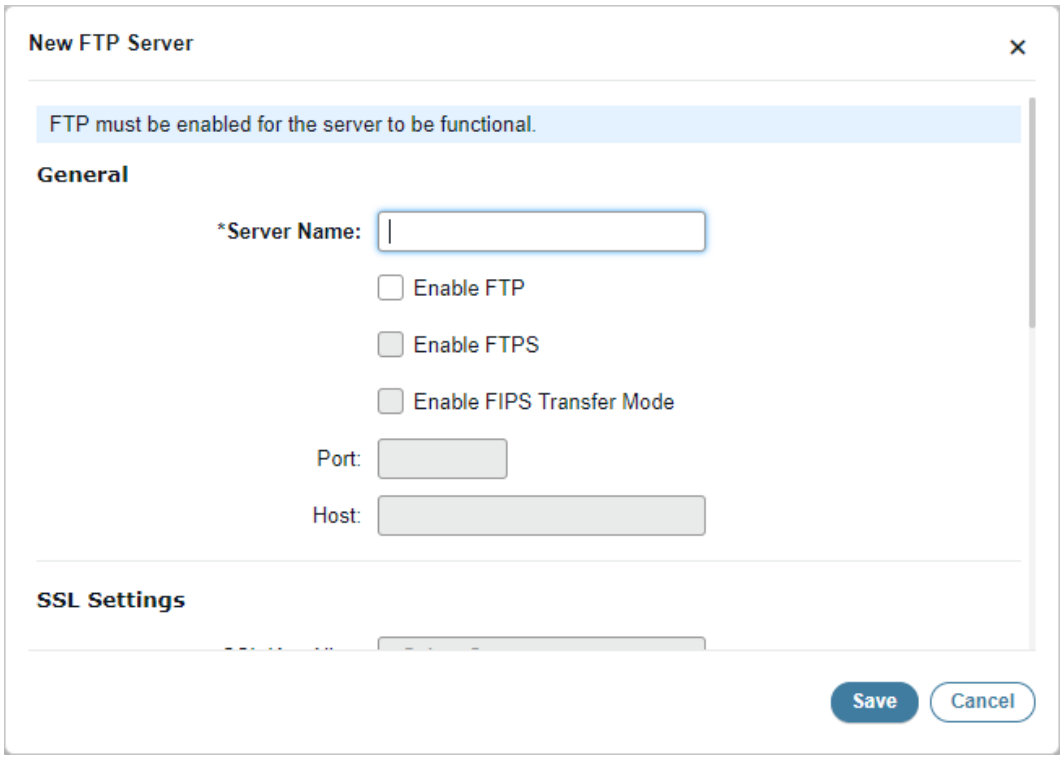
1. Gracefully stop all protocol servers.
2. Stop the Proxy server.

Add an FTP server

To add an FTP server, go to the extended *Server Control* page and on the *FTP Servers* pane, click **Actions > Add Server**.



A new modal box with different FTP server settings pops up.



The following table presents all parameters and expected values associated with your new FTP server.

Field	Description
General	
Server Name	Enter a unique name of your server.
Enable FTP	Select to enable FTP transfers: you must select this option if you want to enable secure FTP (FTPS) transfers.
Enable FTPS	Select to enable FTPS transfers.
Enable FIPS	Select to enable FIPS transfer mode for FTPS connections. By selecting this option, the **Enabled FIPS Ciphers** field becomes editable.
Port	Enter the port number of your FTP or FTPS server.
Host	Enter the IP address of your external FTP (or FTPS) host server. Leave this option blank if you do not need an external host.
SSL Key Alias	Select an SSL Key Alias from the drop-down list, for example, `ftpd`.
Enabled Protocols	Enter a comma-separated list of SSL protocol versions (`TLSv1, TLSv1.1, TLSv1.2` by default).

Field	Description
Key Algorithm	Enter the Key Algorithm (`SunX509` by default). Note that with SecureTransport running on AIX systems, the default value is `IbmX509`.
SSL Protocol	Enter the used SSL protocol group: `SSL` or `TLS` (`TLS` by default). Note that with SecureTransport running on AIX systems, the default value is `SSL_TLS`.
SSL Trust Algorithm	Enter the SSL Trust Algorithm (`SunX509` by default). Note that with SecureTransport running on AIX systems, the default value is `IbmX509`.
Enabled Ciphers	Enter the cipher suites to be used with your FTPS server. For more information on cipher suites, refer to the *SecureTransport Cipher suites* topic, part of the *SecureTransport 5.4 Security guide*.
Enabled FIPS Ciphers	Modify the cipher suite set to be used with your FTP server in FIPS mode. By default, this field is populated with all FIPS compliant TLS cipher suites supported by SecureTransport. For the complete list, see *FIPS-compliant TLS cipher suites* on page 984. Click the "down arrow" icon on the right to access a drop-down menu with options to select and deselect all items and reset value to the previously saved selection. For the default FTP server, the list of allowed cipher suites in FIPS mode is determined by the `Ftp.FIPS.Listeners.Ssl.EnabledCipherSuites` configuration option.
Client Certificate	This drop-down list presents the options to define support for certificate use for FTP authentication. Possible values are: • `Disabled` – no certificate authentication is required • `Required` – the client must authenticate using a certificate • `Optional` – the client can authenticate either using a certificate or a password
FTP Passive Mode	
Base Port	Enter the passive mode base port (`0` by default: this means that SecureTransport will use a random port for FTP passive mode transfers).
Number of Ports	The passive mode port range.

Once you are finished entering the parameters of your FTP server, click **Save** to create it; or **Cancel** to discard all changes and return to the *Server Control* page.

Start and stop a server

You can easily start and stop your FTP server.

- Start your server by clicking the "play" icon:
  A box with a success message pops up on your screen and your server status changes to *Running*.
- To stop your server, click the "stop" icon:
  A box with a success message pops up on your screen and your server status changes to *Stopped*.

You can only start the FTP daemon once the Ftp Default server is operating (enabled). Stopping the daemon will stop all underlying started servers. During daemon start, only the enabled servers will be started. In case of FTP, an "enabled server" means that you have at least selected the **Enable FTP** option.

Edit FTP server settings

You can change any of the FTP server property values. Note that you can change the server name only when the server is stopped. To update an FTP server, click the corresponding "gear" icon:

A new modal box with the FTP settings pops up. Add your changes and click **Save** to apply your changes; or **Cancel** to discard them.

Delete a FTP server

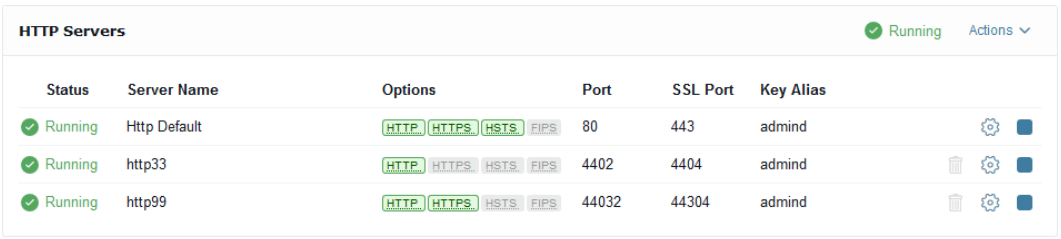
Note You cannot delete or change the name of the "Ftp Default" server from the SecureTransport Administration Tool.

You can only delete a server once it is stopped. You cannot delete a server in *Running* status.

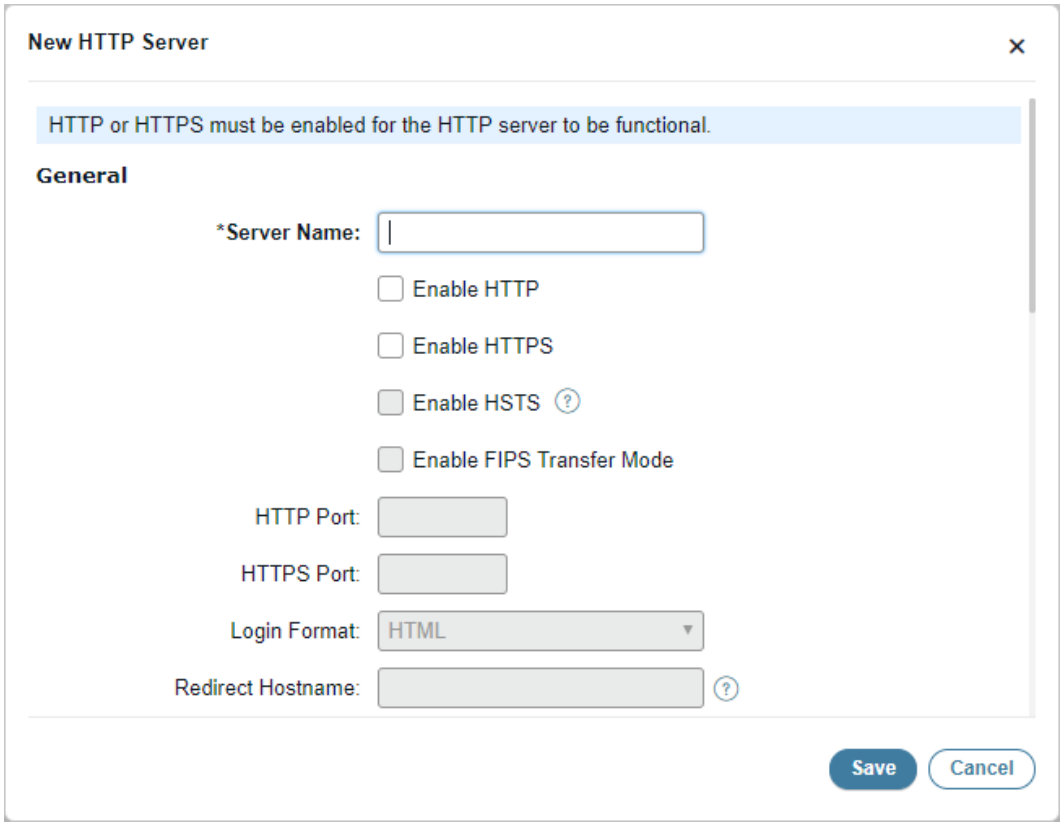
To delete a server, locate it on the *Server Control* page, make sure it is stopped and click the corresponding "trashcan" icon:

Add an HTTP server

To add aн HTTP server, go to the extended *Server Control* page and on the *HTTP Servers* pane, click **Actions > Add Server**.



A new modal box with different HTTP server settings pops up.



The following table presents all parameters and expected values associated with your new HTTP server.

Field	Description
General	
Server Name	Enter a unique name of your server.
Enable HTTP	Select to enable HTTP transfers.
Enable HTTPS	Select to enable HTTPS transfers.
Enable HSTS	Select to enable HSTS if you want to disallow insecure HTTP transfers using this server.
Enable FIPS	Select to enable FIPS transfer mode for HTTPS connections. By selecting this option, the **Enabled FIPS Ciphers** field becomes editable.
HTTP Port	Enter the port number of your HTTP listener.

Field	Description
HTTPS Port	Enter the port number of your HTTPS listener.
Login Format	Select the authentication format for end-user login: • HTML – for user login using the ST Web Client login form • BA – basic authentication • ERR – must use config/auth agents • PREAUTH – config/auth agents + HTML login page in case of failed login
Redirect hostname	Enter a redirect host name or IP address. When you set this value, all requests to the ST Web Client, subsequent to the first one, will be bound to that hostname. Use this option in the case where a DNS switch occurs to avoid requests getting split across different nodes.
SSL Settings	
Client Certificate	This drop-down list presents the options to define support for certificate use for HTTP authentication. Possible values are: • `Disabled` – no certificate authentication is required • `Required` – the client must authenticate using a certificate • `Optional` – the client can authenticate either using a certificate or a password
SSL Key Alias	Select an SSL Key Alias from the drop-down list, for example, `HTTPd`.
SSL Protocol	Enter the used SSL protocol group: `SSL` or `TLS` (`TLS` by default). Note that with SecureTransport running on AIX systems, the default value is `SSL_TLS`.
Enabled SSL Protocols	Enter a comma-separated list of SSL protocol versions (`TLSv1, TLSv1.1, TLSv1.2` by default).
Enabled Ciphers	Enter the cipher suites to be used with your HTTPS server. For more information on cipher suites, refer to the *SecureTransport Cipher suites* topic, part of the *SecureTransport 5.4 Security guide*.

Field	Description
Enabled FIPS Ciphers	Modify the cipher suite set to be used with your HTTP server in FIPS mode. By default, this field is populated with all FIPS compliant TLS cipher suites supported by SecureTransport. For the complete list, see *FIPS-compliant TLS cipher suites* on page 984. Click the "down arrow" icon on the right to access a drop-down menu with options to select and deselect all items and reset value to the previously saved selection. For the default HTTP server, the list of allowed cipher suites in FIPS mode is determined by the `Http.FIPS.Ssl.EnabledCipherSuites` configuration option.
Authentication Parameters	
Allowed Authentication Parameters	Enter the allowed HTTP Authentication parameters, separated by a semi-colon (;).
Allowed Authentication Parameters Max Size	Enter the allowed HTTP Authentication parameters maximum size in bytes.
Content Security Policy	Enter the value of the `Content-Security-Policy` header.
XSS Protection	Enter the value of the `X-XSS-Protection` header.
Content Type Options	Enter the value of the `X-Content-Type-Options` header, for example: `nosniff`.
Referrer Policy	Enter the value of the `Referrer-Policy` header. Accepted values are: `no-referrer, no-referrer-when-downgrade, origin, origin-when-cross-origin, same-origin, strict-origin, strict-origin-when-cross-origin, unsafe-url`
Expect CT	Enter the value of the `Expect-CT` (certificate transparency) header. Accepted values are: `max-age=<age>`; `enforce`; `report-uri=<uri>`. The `enforce` and `report-uri` directives are optional.

Once you are finished entering the parameters of your HTTP server, click **Save** to create it; or **Cancel** to discard all changes and return to the *Server Control* page.

Start and stop a server

You can easily start and stop your HTTP server.

- Start your server by clicking the "play" icon:
  A box with a success message pops up on your screen and your server status changes to Running.
- To stop your server, click the "stop" icon.
  A box with a success message pops up on your screen and your server status changes to Stopped.

You can only start the HTTP daemon once the Http Default server is operating (enabled). Stopping the daemon will stop all underlying started servers. During daemon start, only the enabled servers will be started. In case of HTTP, an "enabled server" means that you have at least selected either option: **Enable HTTP** or **Enable HTTPS**.

Graceful shutdown logging

The server log displays information about active connections during an initiated graceful shutdown. For better visibility, a dedicated server option is introduced: `GracefulShutdown.Logging.Interval`. By default its value is `60s` which means that active transfer information will be logged once every 60 seconds until all transfers are completed. Note that the graceful shutdown logging interval applies to all protocol servers.

Edit HTTP server settings

You can change any of the HTTP server property values. Note that you can change the server name only when the server is stopped. To update an HTTP server, click the corresponding "gear" icon:
A new modal box with the HTTP settings pops up. Add your changes and click **Save** to apply your changes; or **Cancel** to discard them.

Delete a HTTP server

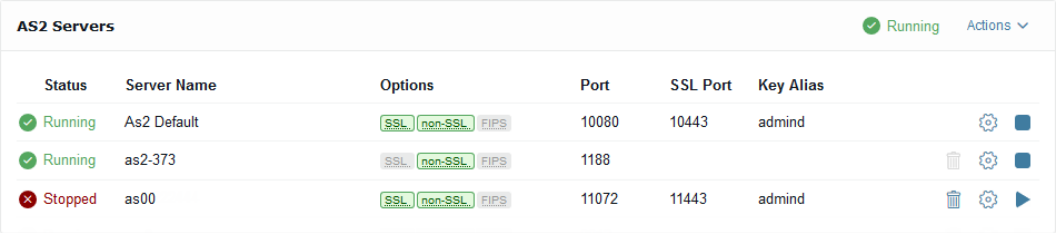
Note You cannot delete or change the name of the "Http Default" server from the SecureTransport Administration Tool.

You can only delete a server once it is stopped. You cannot delete a server in *Running* status.

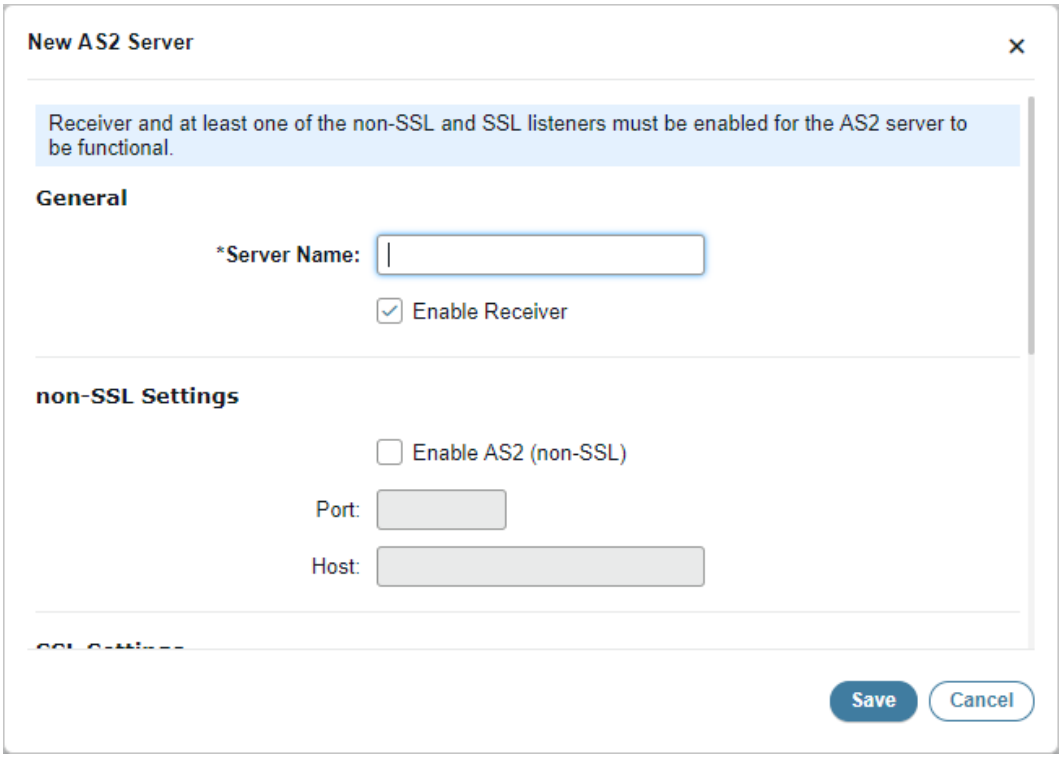
To delete a server, locate it on the *Server Control* page, make sure it is stopped and click the corresponding "trashcan" icon:

Add an AS2 server

To add a AS2 server, go to the extended *Server Control* page and on the *AS2 Servers* pane, click **Actions > Add Server**.



A new modal box with different AS2 server settings pops up.



The following table presents all parameters and expected values associated with your new AS2 server.

Field	Description
General	
Server Name	Enter a unique name of your server.
Enable Receiver	Select to enable receiving of your current AS2 server.
non-SSL Settings	
Enable AS2 (non-SSL)	Select to enable insecure AS2 transfers with your current AS2 server. By selecting this option, the **non-SSL Port** and **non-SSL Host** options become editable.

Field	Description
non-SSL Port	Enter the port number of your non-secure AS2 server.
non-SSL Host	Enter the host address of your non-secure AS2 server.
SSL Settings	
Enable AS2 (SSL)	Select to enable *secure* AS2 transfers with your current AS2 server. By selecting this option, the remaining options become editable.
Enable FIPS	Select to enable FIPS transfer mode for AS2 connections. By selecting this option, the **Enabled FIPS Ciphers** field becomes editable.
SSL Port	Enter the port number of your AS2 server.
SSL Host	Enter the host address of your AS2 server.
SSH Key Alias	Select an SSL Key Alias from the drop-down list, for example, `admind`.
Key Exchange Algorithms	Enter the Key Algorithm (`SunX509` by default). Note that with SecureTransport running on AIX systems, the default value is `IbmX509`.
Enabled SSL Protocols	Enter a comma-separated list of SSL protocol versions (`TLSv1, TLSv1.1, TLSv1.2` by default).
Enabled Ciphers	Enter the cipher suites to be used with your AS2 server. For more information on cipher suites, refer to the *SecureTransport Cipher suites* topic, part of the *SecureTransport 5.4 Security guide*.
Enabled FIPS Ciphers	Modify the cipher suite set to be used with your AS2 server in FIPS mode. By default, this field is populated with all FIPS compliant TLS cipher suites supported by SecureTransport. For the complete list, see *FIPS-compliant TLS cipher suites* on page 984. Click the "down arrow" icon on the right to access a drop-down menu with options to select and deselect all items and reset value to the previously saved selection. For the default AS2 server, the list of allowed cipher suites in FIPS mode is determined by the `As2.FIPS.Listeners.Ssl.EnabledCipherSuites` configuration option.

Once you are finished entering the parameters of your AS2 server, click **Save** to create it; or **Cancel** to discard all changes and return to the *Server Control* page.

Start and stop a server

You can easily start and stop your AS2 server.

- Start your server by clicking the "play" icon:
  A box with a success message pops up on your screen and your server status changes to *Running*.
- To stop your server, click the "stop" icon.
  A box with a success message pops up on your screen and your server status changes to *Stopped*.

You can only start the AS2 daemon once the As2 Default server is operating (enabled). Stopping the daemon will stop all underlying started servers. During daemon start, only the enabled servers will be started. In case of AS2, an "enabled server" means that you have at least selected either option: **Enable AS2 (non-SSL)** or **Enable AS2 (SSL)**.

Edit AS2 server settings

You can change any of the selected AS2 server property values. Note that you can change the server name only when the server is stopped. To update an AS2 server, click the corresponding "gear" icon:

A new modal box with the AS2 settings pops up. Add your changes and click **Save** to apply your changes; or **Cancel** to discard them.

Delete an AS2 server

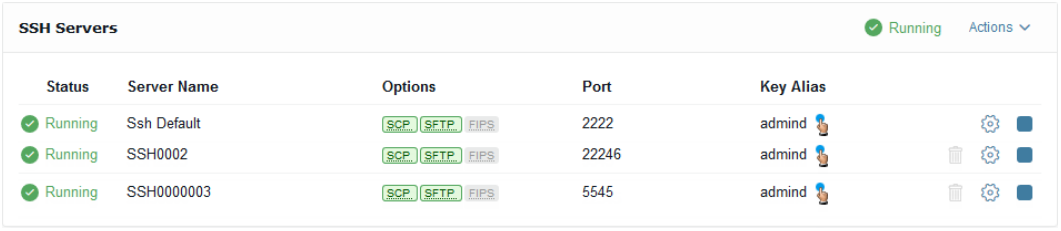
Note You cannot delete or change the name of the "AS2 Default" server from the SecureTransport Administration Tool.

You can only delete a server once it is stopped. You cannot delete a server in *Running* status.

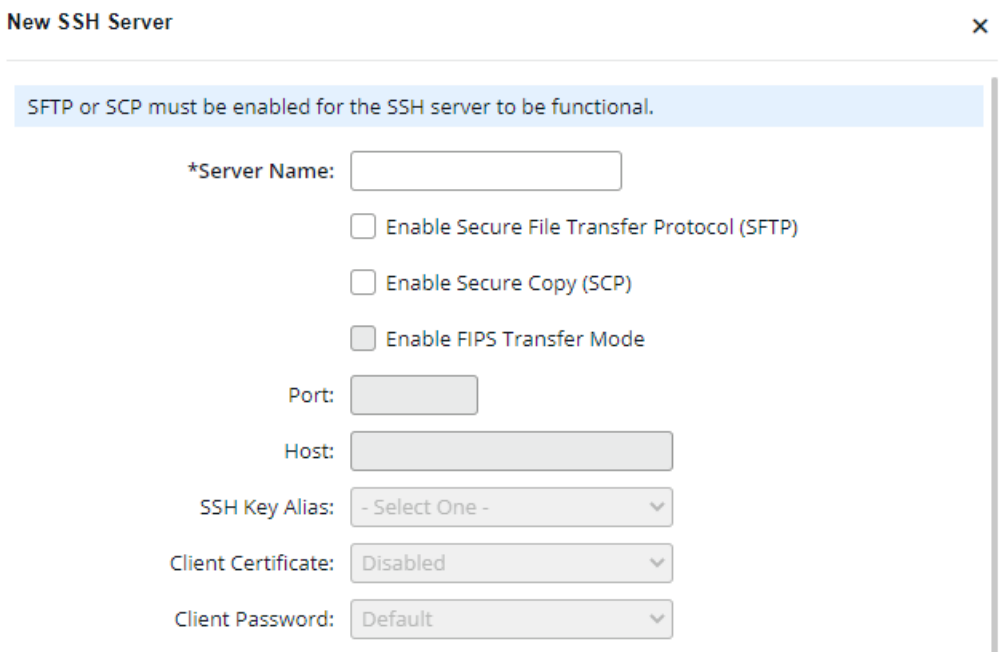
To delete a server, locate it on the *Server Control* page, make sure it is stopped and click the corresponding "trashcan" icon:

Add an SSH server

To add an SSH server, go to the extended *Server Control* page and on the *SSH Servers* pane, click **Actions > Add Server**.



A new modal box with different SSH server settings pops up.



The following table presents all parameters and expected values associated with your new SSH server.

Field	Description
Server Name	Enter a unique name of your server.
Enable SCP	Select to enable SCP (Secure Copy) support with transfers using your current SSH server.
Enable SFTP	Select to enable SFTP transfers with using your current SSH server.
Enable FIPS	Select to enable FIPS transfer mode for SSH connections. By selecting this option, the following fields become editable: • FIPS Exchange Algorithms • FIPS Public Keys • FIPS MAC Algorithms • Enabled FIPS Ciphers
Port	Enter the port number of your SSH server.
Host	Enter the host address of your SSH server.
SSH Key Alias	Select an SSH Key Alias from the drop-down list, for example, `admind`.

Field	Description
Client Certificate	This drop-down list presents the options to define support for certificate use for SSH authentication. Possible values are: • `Disabled` – no certificate authentication is required • `Required` – the client must authenticate using a certificate • `Optional` – the client can authenticate either using a certificate or a password
Client Password	When **Client Certificate** is set to `Required`, you can also specify the authentication methods that the SSH server offers to the SSH client: • `Default` – the server sends the authentication methods set in **Authentication > Login Settings > End-user login options** • `Disabled` – the server sends only "publickey"
Key Exchange Algorithms	Enter the Diffie-Hellman exchange hashing algorithms, for example: `diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha256`.
FIPS Exchange Algorithms	Specify the KEX algorithms to be used with your SSH server in FIPS mode. By default, this field is populated with all FIPS compliant KEX algorithms supported by SecureTransport. For the complete list, see *FIPS-compliant key exchange algorithms* on page 985. Click the "down arrow" icon on the right to access a drop-down menu with options to select and deselect all items and reset value to the previously saved selection. For the default SSH server, the list of allowed KEX algorithms in FIPS mode is determined by the `Ssh.FIPS.KeyExchangeAlgorithms` configuration option.
Minimum key size for Diffie-Hellman exchange algorithms group:	Enter the minimum exchange key size in bits: `128` bit is the minimum (least secure) and `4096` is the maximum (most secure).
Public Keys	Enter the certificate type for your public keys and signature algorithm in the following format: `ssh-rsa,ssh-dss,x509v3-sign-rsa,x509v3-sign-rsa-sha1`

Field	Description
FIPS Public Keys	Specify the public key algorithms to be used with your SSH server in FIPS mode. By default, this field is populated with all FIPS compliant public keys supported by SecureTransport. For the complete list, see *FIPS-compliant public key algorithms* on page 986 Click the "down arrow" icon on the right to access a drop-down menu with options to select and deselect all items and reset value to the previously saved selection. For the default SSH server, the list of allowed public key algorithms in FIPS mode is determined by the `Ssh.FIPS.PublicKeys` configuration option.
MAC Algorithms	Enter the MAC algorithm that warrants the integrity of the transfer using your current SSH server.
FIPS MAC Algorithms	Specify the MAC algorithms to be used with your SSH server in FIPS mode. By default, this field is populated with all FIPS compliant MACs supported by SecureTransport. For the complete list, see *FIPS-compliant MAC algorithms* on page 986 Click the "down arrow" icon on the right to access a drop-down menu with options to select and deselect all items and reset value to the previously saved selection. For the default SSH server, the list of allowed MAC algorithms in FIPS mode is determined by the `Ssh.FIPS.AllowedMacs` configuration option.
Enabled Ciphers	Enter the ciphers to be used with your SSH server. For more information on cipher suites, refer to the *SecureTransport Cipher suites* topic, part of the *SecureTransport 5.4 Security guide*.
Enabled FIPS Ciphers	Specify the ciphers to be used with your SSH server in FIPS mode. By default, this field is populated with all FIPS compliant ciphers supported by SecureTransport. For the complete list, see *FIPS-compliant ciphers* on page 985. Click the "down arrow" icon on the right to access a drop-down menu with options to select and deselect all items and reset value to the previously saved selection. For the default SSH server, the list of allowed public key algorithms in FIPS mode is determined by the `Ssh.FIPS.Ciphers` configuration option.

Once you are finished entering the parameters of your SSH server, click **Save** to create it; or **Cancel** to discard all changes and return to the *Server Control* page.

Start and stop a server

You can easily start and stop your SSH server.

- Start your server by clicking the "play" icon:
  A box with a success message pops up on your screen and your server status changes to *Running*.
- To stop your server, click the "stop" icon.
  A box with a success message pops up on your screen and your server status changes to *Stopped*.

You can only start the SSH daemon once the Ssh Default server is operating (enabled). Stopping the daemon will stop all underlying started servers. During daemon start, only the enabled servers will be started. In case of SSH, an "enabled server" means that you have at least selected either option: **Enable Secure File Transfer Protocol (SFTP)** or **Enable Secure Copy (SCP)**.

Edit SSH server settings

You can change any of the SSH server property values. Note that you can change the server name only when the server is stopped. To update an SSH server, click the corresponding "gear" icon:

A new modal box with the SSH settings pops up. Add your changes and click **Save** to apply your changes; or **Cancel** to discard them.

Delete a SSH server

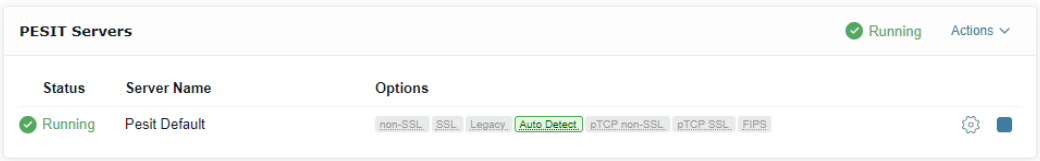
Note You cannot delete or change the name of the "Ssh Default" server from the SecureTransport Administration Tool.

You can only delete a server once it is stopped. You cannot delete a server in *Running* status.

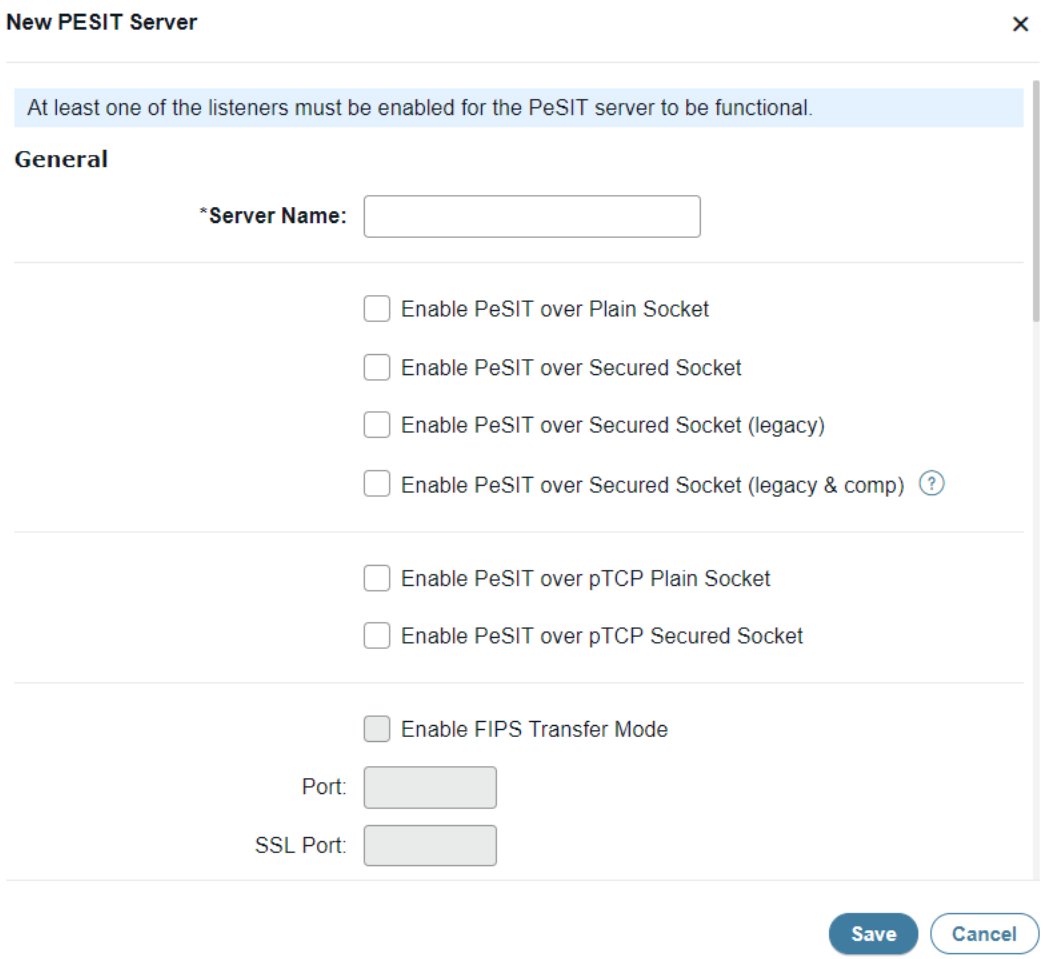
To delete a server, locate it on the *Server Control* page, make sure it is stopped and click the corresponding "trashcan" icon:

Add a PeSIT server

To add a PeSIT server, go to the extended *Server Control* page and on the *PeSIT Servers* pane, click **Actions > Add Server**.



A new modal box with different PeSIT server settings pops up.



The following table presents all parameters and expected values associated with your new PeSIT server.

Field	Description
General	
Server Name	Enter a unique name of your server.
Enable PeSIT over Plain Socket	Select to enable non-secure PeSIT transfers.
Enable PeSIT over Secured Socket	Select to enable secure PeSIT transfers.

Field	Description
Enable PeSIT over Secured Socket (legacy)	Select to enable transfers with remote partners using SSL Legacy.
Enable PeSIT over Secured Socket (legacy § comp)	Select to enable the automatic detection of the used SSL/TLS mode (Legacy or Comp) when SecureTransport acts as a server. Information about the detected mode is logged in the server log under **Level > Debug**. The PeSIT listener used for communication with partners in both TLS Comp and TLS Legacy modes is configured using the following server configuration parameters: • `Pesit.Autodetect.Tls.Mode.Enabled` - enables or disables the listener • `Pesit.Autodetect.Tls.Mode.Port` - specifies the port number of the listener • `Pesit.Listeners.Autodetect.Tls.Mode.keyAlgorithm` - specifies the key algorithm • `Pesit.Listeners.Autodetect.Tls.Mode.keyAlias` - specifies the key alias of the listener • `Pesit.Listeners.Autodetect.Tls.Mode.protocol` - specifies the protocol of the listener • `Pesit.Listeners.Autodetect.Tls.Mode.trustAlgorithm` - specifies the trust algorithm
Enable PeSIT over pTCP plain socket	Select to enable non-secure PeSIT transfers over pTCP.
Enable PeSIT over pTCP secure socket	Select to enable secure PeSIT transfers over pTCP.
Enable FIPS Transfer Mode	Select to enable FIPS transfer mode for PeSIT connections. By selecting this option, the **Enabled FIPS Ciphers** field becomes editable.
Port	Enter the port number of your PeSIT server.
SSL port	Enter the SSL port number for secure connection to your PeSIT server.
Host	Enter the IP address of your external PeSIT (or PeSIT) host server. Leave this option blank if you do not need an external host.

Field	Description
Key Exchange Algorithms	Enter the Key Algorithm (`SunX509` by default). Note that with SecureTransport running on AIX systems, the default value is `IbmX509`.
SSL Key Alias	Select an SSL Key Alias from the drop-down list, for example, `PeSITd`.
PeSIT SSL Protocol	Enter the used SSL protocol group: `SSL` or `TLS` (`TLS` by default). Note that with SecureTransport running on AIX systems, the default value is `SSL_TLS`.
Enabled SSL Protocols	Enter a comma-separated list of SSL protocol versions (`TLSv1, TLSv1.1, TLSv1.2` by default).
Common SSL Settings	
PeSIT Trust algorithms	Enter the key trust algorithm (`SunX509` by default). Note that with SecureTransport running on AIX systems, the default value is `IbmX509`.
Enabled Ciphers	Enter the cipher suites to be used with your PeSIT server. For more information on cipher suites, refer to the *SecureTransport Cipher suites* topic, part of the *SecureTransport 5.4 Security guide*.
Enabled FIPS Ciphers	Modify the cipher suite set to be used with your PeSIT server in FIPS mode. By default, this field is populated with all FIPS compliant TLS cipher suites supported by SecureTransport. For the complete list, see *FIPS-compliant TLS cipher suites* on page 984. Click the "down arrow" icon on the right to access a drop-down menu with options to select and deselect all items and reset value to the previously saved selection. For the default PeSIT server, the list of allowed cipher suites in FIPS mode is determined by the `Pesit.FIPS.Listeners.Ssl.EnabledCipherSuites` configuration option.
Client Certificate	This drop-down list presents the options to define support for certificate use for PeSIT authentication. Possible values are: `Disabled` – no certificate authentication is required `Required` – the client must authenticate using a certificate `Optional` – the client can authenticate either using a certificate or a password
PeSIT over pTCP – to enable editing these options, you must select at least one of the **Enable PeSIT over pTCP** options listed above	
Port	Enter the port number for your PeSIT over pTCP connection.

Field	Description
SSL port	Enter the SSL port number for secure PeSIT over pTCP connection.
Key Exchange Algorithms	Enter the Key Algorithm (`SunX509` by default). Note that with SecureTransport running on AIX systems, the default value is `IbmX509`.
SSL Key Alias	Select an SSL Key Alias from the drop-down list, for example, `PeSITd`.
SSL Protocol	Enter the used SSL protocol group: `SSL` or `TLS` (`TLS` by default). Note that with SecureTransport running on AIX systems, the default value is `SSL_TLS`.
Trust Algorithms	Enter the SSL Trust Algorithm (`SunX509` by default). Note that with SecureTransport running on AIX systems, the default value is `IbmX509`.
PeSIT over Secured Socket (legacy), PeSIT over Secured Socket (legacy & comp) **-** to enable editing these options, you must select the corresponding option listed above	
SSL port	Enter the SSL port number for secure PeSIT connection.
Key Exchange Algorithms	Enter the Key Algorithm (`SunX509` by default). Note that with SecureTransport running on AIX systems, the default value is `IbmX509`.
SSL Key Alias	Select an SSL Key Alias from the drop-down list, for example, `PeSITd`.
SSL Protocol	Enter the used SSL protocol group: `SSL` or `TLS` (`TLS` by default). Note that with SecureTransport running on AIX systems, the default value is `SSL_TLS`.
Trust Algorithms	Enter the SSL Trust Algorithm (`SunX509` by default). Note that with SecureTransport running on AIX systems, the default value is `IbmX509`.

Once you are finished entering the parameters of your PeSIT server, click **Save** to create it; or **Cancel** to discard all changes and return to the *Server Control* page.

Start and stop a server

You can easily start and stop your PeSIT server.

- Start your server by clicking the "play" icon:
  A box with a success message pops up on your screen and your server status changes to *Running*.
- To stop your server, click the "stop" icon.
  A box with a success message pops up on your screen and your server status changes to *Stopped*.

You can only start the PeSIT daemon once the Pesit Default server is operating (enabled). Stopping the daemon will stop all underlying started servers. During daemon start, only the enabled servers will be started. In case of PeSIT, an "enabled server" means that you have at least selected either of the available "Enable PeSIT" options.

Edit PeSIT server settings

You can change any of the PeSIT server property values. Note that you can change the server name only when the server is stopped. To update a PeSIT server, click the corresponding "gear" icon:

A new modal box with the PeSIT settings pops up. Add your changes and click **Save** to apply your changes; or **Cancel** to discard them.

Delete a PeSIT server

Note You cannot delete or change the name of the "Pesit Default" server from the SecureTransport Administration Tool.

You can only delete a server once it is stopped. You cannot delete a server in *Running* status.

To delete a server, locate it on the *Server Control* page, make sure it is stopped and click the corresponding "trashcan" icon:

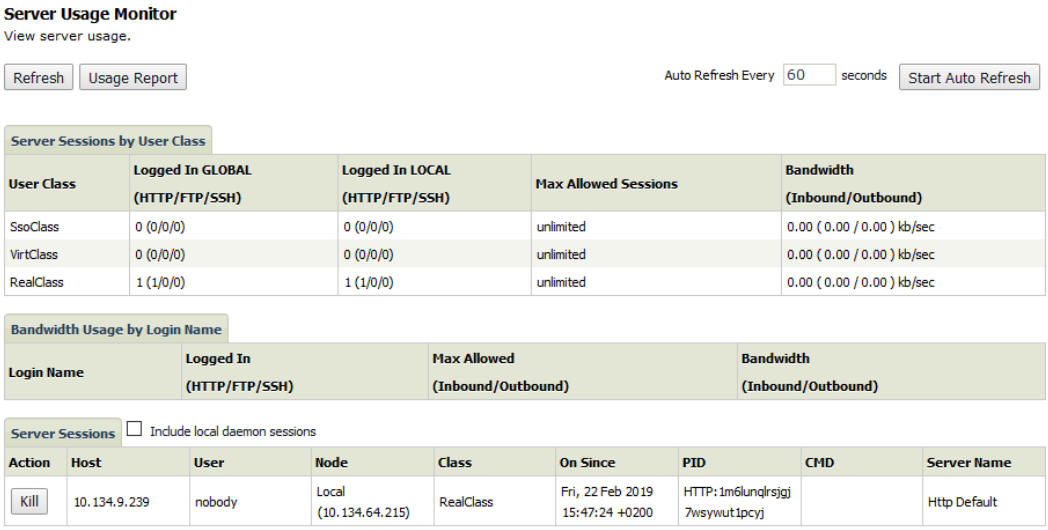
Server usage monitor

The *Server Usage Monitor* page presents info with current session and bandwidth usage, as follows:

- Server sessions by User Class - lists server sessions and bandwidth as consumed by User classes
- Bandwidth usage by login name - lists server bandwidth consumed by individual user accounts
- Server sessions - lists each connection session per user account

You also have the option to *Auto refresh Server Usage Monitor info* on page 289, as well as perform a manual refresh of the page.

Note The *Server Usage Monitor* page shows FTP, HTTP(S) and SSH information only. Also, you can select what info to be monitored. For more information, see *Set usage monitor options* on page 179.



Note When in *cluster setup*, the information presented here includes all current sessions across all nodes.

Server sessions by User Class

This table allows you to monitor server sessions and bandwidth as consumed by User classes. The information is distributed into columns as follows:

- **User class**
- **Logged in GLOBAL (HTTP/FTP/SSH)** – the number of protocol (HTTP(S)/FTP/SSH) sessions that users in the respective user class are currently connected to globally.
- **Logged in LOCAL (HTTP/FTP/SSH)** – the number of protocol (HTTP(S)/FTP/SSH) sessions that users in the respective user class are currently connected to locally.
- **Max allowed sessions** – the upper limitation for open concurrent sessions per user class.
- **Bandwidth (Inbound/Outbound)** – the currently used bandwidth by the respective user class.

Note For more information on the format presented in the different columns of the *Server sessions by User Class* table, see the subtopic that follows: *Bandwidth usage by login name*.

Bandwidth usage by login name

This table allows you to monitor server bandwidth consumed by individual user accounts that are currently logged in. The information is distributed into columns as follows:

- **Login name** – the user account login name.
- **Logged In (HTTP/FTP/SSH)** – the number of protocol (HTTP(S)/FTP/SSH) sessions the user is currently connected to. The format used is [total sessions (HTTP/FTP/SSH)].
  For example, when the respective value for a selected user is (3 (1/1/1), this means that the user currently has 3 open sessions, 1 HTTP(S), 1 FTP and 1 SSH.

- **Max allowed (Inbound/Outbound)** – the maximum allowed traffic speed per the respective user. The format used is [Total allowed bandwidth (Max allowed Inbound bandwidth / Max allowed Outbound bandwidth].
  For example, when the respective value for a selected user is (768.0 (512.0 / 256.0), this means that the user's total traffic (both Inbound and Outbound) is limited to 768 kb/sec, of which 512.0 is the maximum allowed speed for inbound, and 256 is the maximum allowed speed for outbound traffic.
- **Bandwidth (Inbound/Outbound)** – the currently used bandwidth by the respective user. The format used is [Total allowed bandwidth (Max allowed Inbound bandwidth / Max allowed Outbound bandwidth].

Server sessions

This table lists each FTP, SSH and HTTP(S) connection with the option to kill each one. The table presents the following options:

- **Action** – use the **Kill** button for each connection to terminate the respective session.
- **Host** – the IP address of the host location from which the user has connected.
- **User** – the username of the respective user account.
- **Node** – the IP address to which the user is connected.
- **Class** – the user class the respective user belongs to.
- **On Since** – the Date and time the respective connectivity session was established.
- **PID** – the internal process ID of an FTP, SSH or HTTP(S) session within the server process.
- **CMD** – the transfer command.
- **Server Name** – the name of the server.

Select the **Include local daemon sessions** check-box to include the local sessions in the display results.

Auto refresh Server Usage Monitor info

Use the following procedure to enable automatic snapshot updates.

1. On the top right corner of *Server Usage Monitor* page, type the number of seconds between updates in the **Auto refresh every ____ seconds** box.
2. Click **Start Auto Refresh**. The button label changes to **Stop Auto Refresh** so you can later click it again to disable the automatic snapshot update.

Note Wile in Auto refresh mode, do not use **F5** on your keyboard or the **Refresh** button on the screen to refresh the browser window.

Disable automatic snapshot updates

To disable automatic snapshot updates, go to the *Server Usage Monitor* page and click **Stop Auto Refresh**. The button changes back its label to **Start Auto Refresh**.

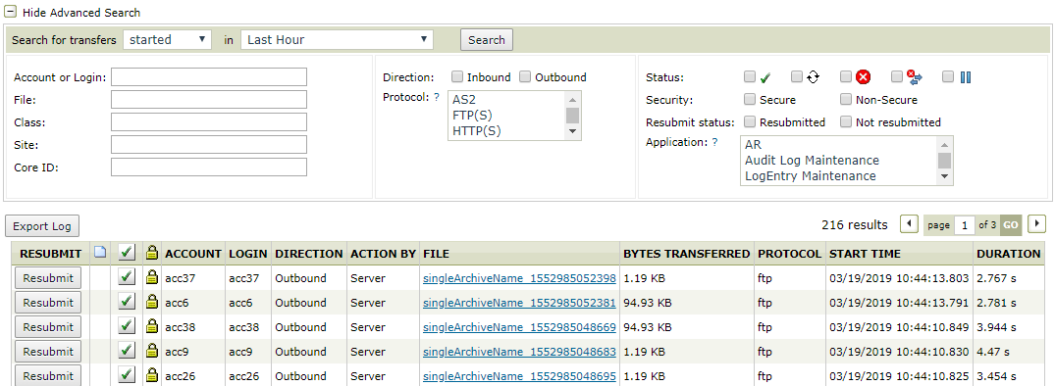
Track file transfer activity

Use the *File Tracking* page to view information about both client-initiated and server-initiated file transfers and to cancel or resubmit transfers. The *File Tracking* page is available only on SecureTransport Server. The log SecureTransport displays on the *File Tracking* page is the transfer log.

When you open the *File Tracking* page, SecureTransport automatically loads the transfer log entries for the past hour. This behavior is determined by the `FileTracking.InitialLoading.Enabled.Admin` server configuration option. It accepts boolean values; the default value is `true`. To disable the initial auto-loading of log entries on the page, set the configuration option to `false`.

By default, SecureTransport stores the transfer log entries in the SecureTransport database. If you have the Enterprise Cluster (EC) option, you can store the transfer log data in a separate Oracle database away from the rest of the SecureTransport data. See *Direct log data to separate Oracle databases* on page 99.

To control which transfers are logged, see *Configure transfer log* on page 170.



For each transfer listed, the *File Tracking* page displays resubmit status, transfer status, account name, login name, direction of transfer, whether action was taken by the user or server, file name, number of bytes transferred, transfer protocol, start time, and duration.

The **Resubmit** button will be displayed in the *Resubmit Status* column except in the following cases:

- AdHoc mail transfer
- AdHoc attachment transfer
- CIT download
- Failed CIT upload

- In-progress transfer
- Re-trying transfer
- PeSIT transfer in Paused state
- Publish To Account Advanced Routing step transfer
- Deleted file transfer log
- Temporary fail transfers

In the listed cases, no **Resubmit** button is displayed. However, resubmit is not guaranteed to succeed. It is coupled with the archiving of the transfers.

Note Due protocol specific operations, when a user pauses or resumes a client initialed transfer (CIT) two entries are observed on the *File Tracking* page for the interrupted transfer. The entries have the following characteristics:

HTTP CIT: The *File Tracking* page entry for the portion of the file uploaded before the transfer is paused is marked as failed and a **Resubmit** button is not displayed. The second entry for the portion of the file uploaded after the transfer is resumed is marked as successful and a **Resubmit** button is displayed.

FTP/SSH CIT: The *File Tracking* page entry for the portion of the file uploaded before the transfer is paused is marked as successful and a **Resubmit** button is displayed. The second entry for the portion of the file uploaded after the transfer is resumed is marked as successful and a **Resubmit** button is displayed.

Note For PeSIT transfers initiated by a partner, the **LOGIN** column displays the name of the PeSIT transfer site that represents the partner. For all PeSIT transfers, the **FILE** column displays the name of the transfer profile used. For the location and name of the file transferred, click the icon in the status column and refer to the detailed status. You will be able to see more comprehensive information about the transfer if you are using Axway Sentinel.

Note When an Oracle RAC database node fails, the transfers being processed by a SecureTransport server connected to the failed Oracle RAC database node, will remain in process indefinitely.

The following topics provide additional information on viewing and managing file transfer activity:

- *Resubmit status* on page 1
- *Transfer status* on page 292
- *View file transfer information* on page 293
- *Manage file transfers* on page 303
- *Transfer Log Maintenance application* on page 304

Resubmit status

The resubmit status displays one of three options:

- A **Resubmit** button for permanently failed transfers and for successful incoming transfers other than AdHoc mail, AdHoc attachment, CIT download, failed CIT upload, in-progress, retried, PeSIT in Paused state, Publish To Account Advanced Routing step, and deleted file log transfers. You can use the **Resubmit** button to try failed transfer again or to resubmit successful incoming transfers other than for those listed.
- A **Cancel** button you can use to stop the transfer retry attempt.
- No button if the transfer is in-progress or if it is an AdHoc mail, AdHoc attachment, CIT download, failed CIT upload, in-progress, retried, PeSIT in Paused state, Publish To Account Advanced Routing step, temporary failed transfers and deleted file log transfer.

When retrying a transfer, SecureTransport uses either an archived copy created when the server first received the file or the original file if it is available. If there is no archive for the transfer and the original file is not available resubmit attempt fails.

Note Archived files are removed from the server periodically. You can control these settings using the Archive Maintenance application and global File Archiving configuration. For more information on the Archive Maintenance application, see *Create an Archive Maintenance application* on page 760. For more information on the global File Archiving configuration, refer to *File archiving global configuration* on page 213.

If the transfer failed, a **Cancel** button is displayed only next to the most recent failure, as indicated by the timestamp associated with the attempt. The **Cancel** button is displayed when the transfer has a temporary failure, while the **Resubmit** button is displayed when the transfer has a permanent failure or when an incoming transfer is successful other than AdHoc mail, AdHoc attachment, CIT download, failed CIT upload, in-progress, retried, PeSIT in Paused state, Publish To Account Advanced Routing step, and deleted file log transfers. Additionally, the **Resubmit** button is not displayed for deleted transfers.

Note SecureTransport always checks if an archive copy of the file is available before checking for the original file. The modification date and time of the original file is kept in the transfer history, so if a file with the same name as the original file exists in the original location. The transfer is not resubmitted if the modification date and time do not match.

Resubmit only restarts the transfer that is resubmitted. If there is not an active subscription for the transfer, at the moment of resubmission, the subscription will be reactivated. If only a post-transmission action fails, the post-transmission action is restarted when you resubmit the transfer.

Note There are limitations on **Cancel**. When using Advanced Routing feature the administrator is not able to control automatic retries using the **Cancel** button.

Transfer status

Transfer status is represented by an icon. The following table shows each icon and its meaning:

Icon	Status	Protocols supported
	MDN Receipt – Click to view or verify the MDN receipt for the transfer or to view the PeSIT acknowledgment for the transfer.	All
	Processed/Successful – The file was transferred successfully.	All
	In progress – The file is currently being transferred.	All
	Paused – The remote server has paused the PeSIT transfer.	PeSIT
	Failed – The file transfer failed for some reason. Transfers intentionally aborted by file transfer clients and end users are included in this category. The *File Tracking* page provides additional information to help distinguish transfers intentionally aborted from those that failed for other reasons.	All
	Failed Subtransmission – The file transfer was successful, but one or more Subtransmission actions requested failed for some reason. Subtransmission actions include post-transmission actions and data transformations such as encryption or decryption.	All

Click each transfer status icon to view detailed status information about the file transfer.

If a padlock icon displays in the Secure Transfer column (fourth from the left), then the transfer was performed over a secure connection such as FTPS, HTTPS, or SSH.

Note If a file is renamed immediately after a file transfer, both the MDN receipt creation and verification may fail.

View file transfer information

Use the *File Tracking* page to search for file tracking information and to view information about a file transfer including:

- Export log statistics
- Resubmitted or non-resubmitted transfers
- MDN receipt information
- Detailed status about a file transfer
- History of a file transfer
- Detailed status about an advanced route execution

The following topics provide how-to instructions for viewing and exporting file transfer information:

- *View and export log statistics about transferred files* on page 294
- *Search file tracking information* on page 294
- *View MDN receipt information about a transfer* on page 295
- *View the detailed status information about a transfer* on page 296
- *View the file history details information about a transfer* on page 299
- *View the detailed status information about an advanced route execution* on page 301
- *Link to the server log* on page 303

View and export log statistics about transferred files

Use the following procedure to view and export file transfer log statistics.

1. Select **Operations > File Tracking**.

   The *File Tracking* page is displayed.

2. Click **Export Log** to export the displayed file tracking data to a `.csv` file. You cannot export all the records from the database at one time.

   A dialog box is displayed asking whether you want to open the file or save it to disk.

3. Specify whether to save the file or open the file, and then click **OK**.

Search file tracking information

Use the following procedure to search file tracking information.

1. Select **Operations > File Tracking**.

   The *File Tracking* page is displayed.

2. Specify the search criteria.
   a. In the *Search for transfers* pane, specify whether you want to search based on time the transfer started or completed and the time frame in which to search.
   b. (Optional) Specify the account or login associated with the transfer for which you are searching.
   c. (Optional) Specify whether to search for inbound or outbound transfers.
   d. (Optional) Specify whether you want to include successful transfers, transfers currently in progress, paused transfers, failed transfers, or failed subtransmissions. You can specify more than one.
3. (Optional) Show the Advanced Search fields and specify additional search criteria.
   a. Specify the file name, class, site associated or Core ID with the transfer for which you are searching.
   b. Specify transfers initiated by the server or the user.

c. Specify the protocols used for the transfers. You can use Control+click and Shift+click to select more than one.

d. Specify whether the transfer was secure or non-secure.

e. Specify whether the transfer was resubmitted or not resubmitted.

f. Specify the application associated with the transfer. YOu can use Control + click and Shift + click to select more than one.

Note

Resubmitted files can be:
- the transfer that is resubmitted with the "Resubmit" button or the REST API resource

Not Resubmitted files can be:
- the transfer that is NOT resubmitted with the "**Resubmit**" button or the **REST API** resource;
- the transfer that is started from the **Resubmit** button or the **REST API**;
- the transfer that is without the **Resubmit** button.

4. When you have finished specifying your search criteria, click **Search**.

Note You can get the transferred file count by using REST API.

View MDN receipt information about a transfer

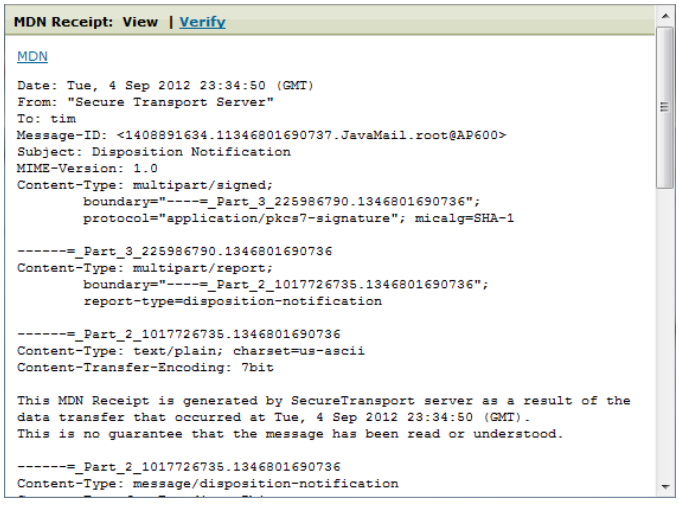
Use the following procedure to view MDN receipt information.

1. Select **Operations > File Tracking**.

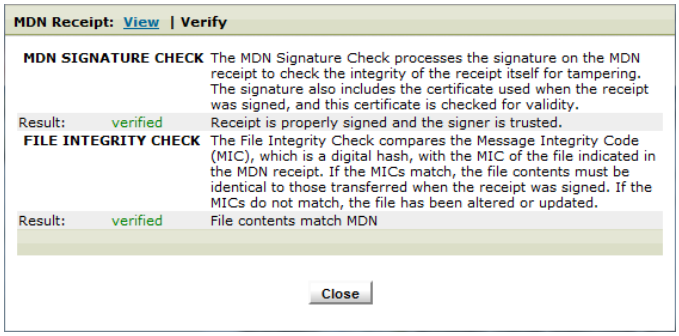
   The *File Tracking* page is displayed.

2. To display MDN receipt information, click the MDN receipt icon for a specific transfer.

   The *MDN Receipt* dialog box is displayed. You can either view the MDN receipt or click **Verify** to view the MDN signature and file integrity check results. Clicking **Close** at the bottom of the MDN receipt closes the dialog box and returns you to the *File Tracking* page.



If you click **Verify** to view the MDN signature and file integrity check results, a new page in the dialog box displays showing the verification status. Click **Close** or **View** to return to the MDN receipt.



Note An MDN receipt icon is displayed only when a receipt for the transfer is available in the system and the transfer was successful. To enable MDN receipts, see *Certificates to generate during initial setup* on page 69.

View the detailed status information about a transfer

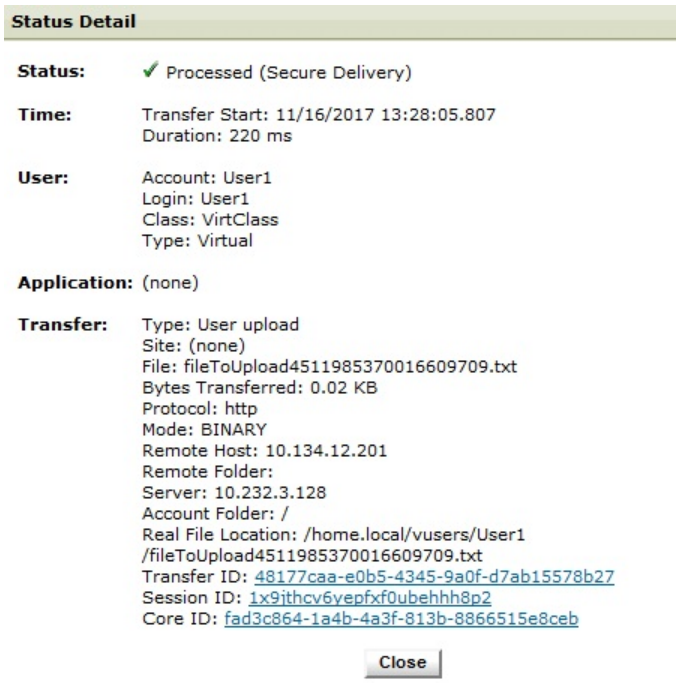
Use the following procedure to view detailed status information.

1. Select **Operations > File Tracking**.

   The *File Tracking* page is displayed.

2. Click the status icon or the file name for a specific transfer.

   The *Status Detail* window is displayed.



3. Click **Close** at the bottom of the details to return to the *File Tracking* page.

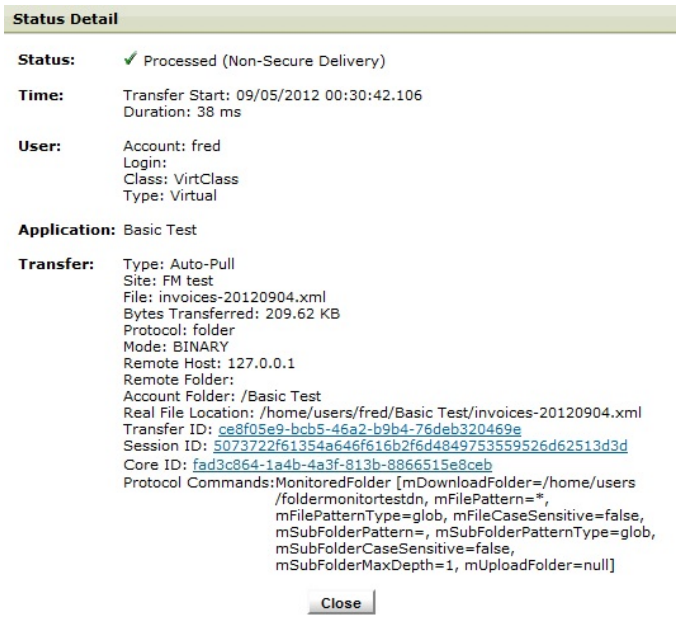
The *Status Detail* dialog box shows the following information:

Name	Description
Status	Displays the transfer status. Values include Processed, In Progress, Failed, Aborted, and Failed Subtransmission.
Time	Displays the Transfer Start date and time and the duration of the transfer in milliseconds.
User	Displays the Account name, login name, class type and user type.
Application	Displays the application instance name.

Name	Description
Transfer	Displays the transfer type, transfer site name, file name, file size, transfer protocol, transfer mode, remote host name, remote folder name, account folder name, real file location, success or failure details, and protocol messages. At the bottom, there are three ID links: • Transfer ID - a unique identifier of a transfer in SecureTransport. It is used to track what happened to a file during a single transfer (e.g upload, download, push, pull). • Session ID - a session identifier in SecureTransport. It is used to track the file(s) during one or multiple transfers that happened in the same session. • Core ID - a unique file identifier in SecureTransport. It is generated the first time the file arrives in SecureTransport, and is stable throughout the lifespan of the file, even if its name changes. Core ID is used to track the file across different transfers and sessions. When you click on the Core ID value, SecureTransport refreshes the *File Tracking* page with the Core ID value pre-filled as a search criterion. **Note** When transfers are performed by users behind a proxy or a load balancer, an additional parameter is listed: X-Forwarded-For. This is a dedicated HTTP header which is commonly used to identify the originating IP address of the user account and is especially useful when the user is behind a proxy or a load balancer. In such case, the Remote Host displays the IP address of the proxy/load balancer, and the X-Forwarded-For parameter displays the user's original IP address. Note that when the user is not behind a proxy/load balancer, the original IP address is displayed with the Remote Host parameter, and X-Forwarded-For is hidden from view.
Post Transmission Status	Displays the operation type, whether the operation whether the operation succeeded or failed, the result of the operation, and comments that can provide additional information, such as if a transformation was performed. Multiple operations might be displayed.

Note When a logged-in account does not have permission to delete files and tries to delete them, the *Status Detail* dialog box is not available.
If the file transfer includes encrypting or decrypting files, this information might be displayed in the success or failure details or the Post Transmission Status. For more information about encryption and decryption, see *Encryption options* on page 604.

The Status Detail for a server-initiated transfer shows the protocol messages as part of the transfer details. For HTTP transfers, the headers are provided since there are no commands sent. For AS2 transfers, messages are also generated from the HTTP headers.



View the file history details information about a transfer

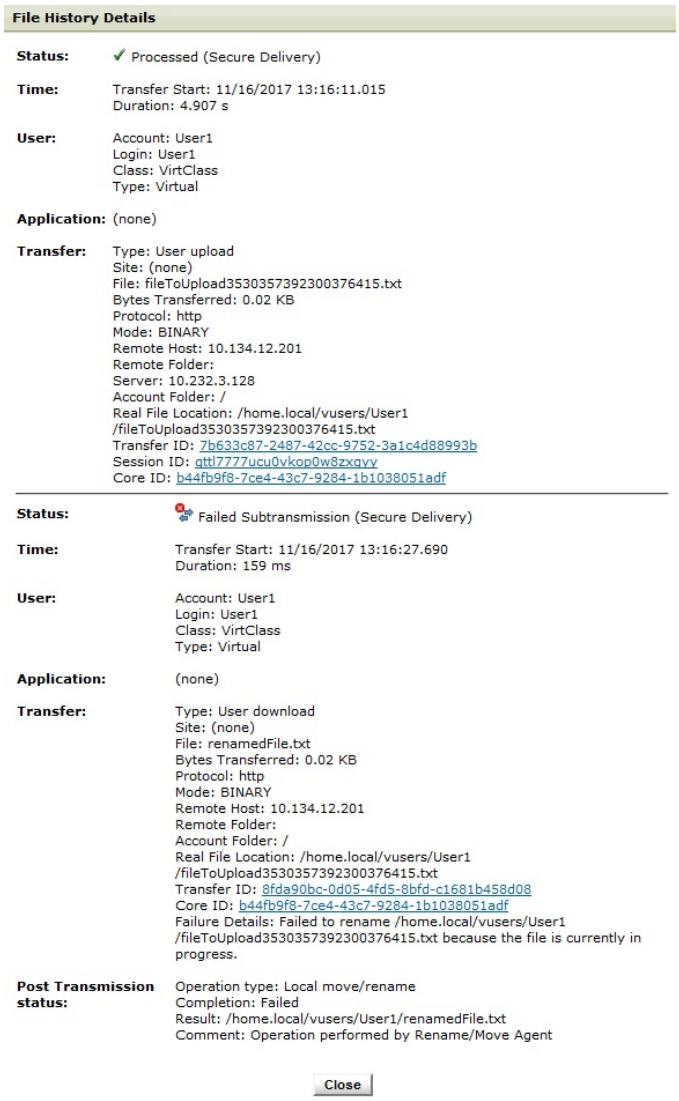
Use the following procedure to view file history details.

1. Select **Operations > File Tracking**.

   The *File Tracking* page is displayed.

2. Click the name of a file to open the *File History Details* dialog box.

   The *File History Details* dialog box is displayed. Click **Close** at the bottom of the details to return to the *File Tracking* page.



The *File History Details* dialog box displays detailed information about tracked events. Tracked events include client-initiated and server-initiated file uploads and downloads, server-initiated transfer protocol messages, PGP encryption, routing a file from one account to another, post-transmission actions, and file deletion or renaming from a client-initiated command. PGP encryption information includes the compression type and level. For more information, see *Encryption options* on page 604.

Note When a logged in account does not have permission to delete files and tries to delete them, the *File History Details* dialog box is not available.

The *File History Details* dialog box displays a chronological list of detailed transfer statuses starting from the last client-initiated upload or server-initiated download and ending with the first renaming or deletion of the file with the same name. If the client-initiated upload or server-initiated download is missing because the file tracking log was rotated, the dialog box shows the first event for that file name.

The *File History Details* dialog box shows the following information:

Name	Description
Status	Displays the transfer status. Values include Processed, In Progress, Failed, Aborted, and Failed Subtransmission
Time	Displays the Transfer Start date and time and the duration of the transfer in milliseconds
User	Displays the Account name, login name, class type and user type
Application	Displays the application instance name
Transfer	Displays the transfer type, transfer site name, file name, file size, transfer protocol, transfer mode, remote host name, remote folder name, account folder name, real file location, Transfer ID link, Session ID link, Core ID link, success or failure details, and protocol messages. Protocol messages are displayed only when a server-initiated transfer is part of the file transfer history. If you are encrypting or decrypting files, this information is included in the success or failure details.
Post Transmission Status	Displays the operation type and if the operation was client-initiated (local) or server-initiated (remote), whether the operation succeeded or failed, the result of the operation, and comments that can provide additional information, such as if a transformation was performed.

View the detailed status information about an advanced route execution

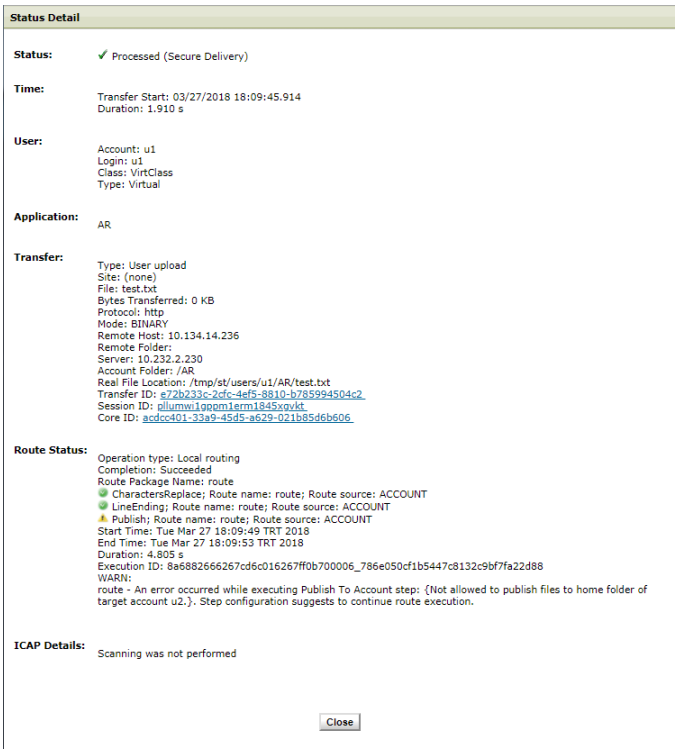
Use the following procedure to view detailed status information about an advanced route execution.

1. Select **Operations > File Tracking**.

   The *File Tracking* page is displayed.

2. Click the status icon or the file name for a specific advanced route execution.

   The *Status Detail* window is displayed.



3. Click **Close** at the bottom of the details to return to the *File Tracking* page.

The *Status Detail* dialog box shows the following information:

Name	Description
Status	Displays the transfer status. Values include Processed, In Progress, Failed, Aborted, and Failed Subtransmission.
Time	Displays the Transfer Start date and time and the duration of the transfer in milliseconds.
User	Displays the Account name, login name, class type and user type.
Application	Displays the application instance name.
Transfer	Displays the transfer type, transfer site name, file name, file size, transfer protocol, transfer mode, remote host name, remote folder name, account folder name, real file location, Transfer ID link, Session ID link, Core ID link, success or failure details, and protocol messages.
Post Transmission Status	Displays the operation type, whether the operation whether the operation succeeded or failed, the result of the operation, and comments that can provide additional information, such as if a transformation was performed. Multiple operations might be displayed.

Name	Description
Route Status	Displays the operation type, whether the route succeeded or failed, the route package name, start and end times, duration, and the execution ID.

Note When a logged-in account does not have permission to delete files and tries to delete them, the *Status Detail* dialog box is not available.
If the file transfer includes encrypting or decrypting files, this information might be displayed in the success or failure details or the Post Transmission Status. For more information about encryption and decryption, see *Encryption options* on page 604.

Link to the server log

The Session ID and Transfer ID listed in the *Status Details* dialog box and the *File History Details* dialog box are links you can use to view the server log entries for that session or transfer.

- From either the *Status Details* dialog box or the *File History Details* dialog box, click the value of either the **Transfer ID** field or the **Session ID** field.

  SecureTransport copies the Session ID or Transfer ID to the search criteria of the *Server Log* page and displays the results of the search.

Manage file transfers

You can restart a file transfer or cancel a file transfer.

The following topics provide how-to instructions for restarting and canceling a file transfer:

- *Restart a transfer* on page 303
- *Cancel a transfer* on page 304

Restart a transfer

If a file transfer fails permanently, SecureTransport displays a **Resubmit** button in the **RESUBMIT** column.

1. Select **Operations > File Tracking**.

   The *File Tracking* page is displayed.

2. Click **Resubmit** to the left of the failed transfer you want to restart.

After you restart a file transfer, the **Resubmit** button no longer displays and a new line is added to the *File Tracking* page showing the progress of the resubmitted transfer.

Cancel a transfer

If a server-initiated file transfer fails temporarily and is scheduled for a retry, SecureTransport displays a **Cancel** button in the **RESUBMIT** column.

- To cancel the file transfer retry, click **Cancel**.

Transfer Log Maintenance application

The built-in SecureTransport application type, Transfer Log Maintenance, maintains the SecureTransport transfer log by exporting and cleaning up transfer log entries on a regular basis, following a schedule you define.

A Transfer Log Maintenance type application has the following features:

- User-definable schedule for transfer log daily backup and export or both. For more information, see *Scheduled downloads and tasks* on page 616.
- Application-specific parameters regarding the processing of transfer log entries include:
  - Expiration period for log entries until export and deletion or both
  - A condition to export the entries before deleting them or not
  - Delete exported files
  - Number of records per file
- Support for a dedicated export folder. By default the exported entries are stored in the following location:

  `<FILEDRIVEHOME>/var/db/hist/transfer-log`

For more information, see *Create a Transfer Log Maintenance application* on page 786.

Server log

Use the *Server Log* page to view the contents of the SecureTransport log messages from the following SecureTransport components: the Transaction Manager (TM) and the processes that implement the AS2, FTP, HTTP, SSH (SFTP), and SOCKS5 protocols, the Administration Tool interface (ADMIN), and auditing (AUDIT).

When you open the *Server Log* page, SecureTransport automatically loads the server log records for the past hour. This behavior is determined by the `ServerLog.InitialLoading.Enabled.Admin` server configuration option. It is available on SecureTransport Edge and SecureTransport Server and accepts boolean values. The option is set to `true` by default. To disable the initial auto-loading of log entries on the page, set the option to `false`. When having a large number of logs, you can filter the entries based on one or more criteria to speed up reporting.

By default, the server log entries are stored in the SecureTransport database. If you have the Enterprise Cluster (EC) option and are using an Oracle database, you can store the server log data in a separate external database from the rest of the SecureTransport data. See *Direct log data to separate Oracle databases* on page 99.

Each line in the log display include the following information:

- **TIME** – The date and time the entry was logged. This is link you can use to display more detailed information.
- **LEVEL** – The severity level of the entry.
- **COMPONENT** – The name of the SecureTransport component that produced the entry.
- **THREAD** – The ID of the SecureTransport execution thread that produced the entry.
- **MESSAGE** – The primary log information.

On SecureTransport Server, but not on SecureTransport Edge, the following information is also included.

- **SESSION ID** – An identifier of the login session associated with the entry. This is a link you can use to copy the session ID into the **Session ID** field in the search criteria.
- **TRANSFER ID** – An identifier of the file transfer associated with this entry. This is a link you can use to copy the transfer ID into the **Transfer ID** field in the search criteria.

Also, you can export the filtered log entries to a `.csv` file.

The following topics describe viewing, searching, exporting, and managing server log content:

- *Search and view server log contents* on page 305
- *Export the results of a server log search* on page 307
- *Log Entry Maintenance application* on page 307

Search and view server log contents

Use the following procedure to search and view server log content.

1. Select **Operations > Server Log**.

   The *Server Log* page is displayed.

2. In the *Search* pane, specify search criteria.

   a. In the **Time Interval** drop-down list, select the time frame of the log entries to display. Choose from the following:

      - Last Hour (default)
      - Last 4 Hours
      - Last 8 Hours
      - Last 12 Hours
      - Last 24 Hours
      - Last 48 Hours

- Last 1 Week
- Last 2 Weeks
- Specific Date/Time Range – Displays field that you use to specify the range

b. (Optional) In the **Account or Login** field, type the name of the account or login associated with the log entries to display.

c. (Optional) In the **Thread** field, type the name of the thread associated with the log entries for to display.

d. (Optional) Under *Level*, select the levels of the log entries to display. Choose from the following:

- TRACE
- DEBUG
- INFO
- NOTICE
- WARN
- ERROR
- FATAL

e. (Optional) Under *Component*, Select the SecureTransport Server component associated with the log entries to display. Choose from the following:

- TM
- AS2D
- SSHD
- Socks
- ADMIN
- AUDIT
- FTPD
- HTTPD
- PESITD

f. (Optional) In a clustered deployment, select the **Cluster Node** associated with the log entries to display. The nodes shown are those listed on the *Cluster Management* page. To select more than one node, click **Select Multiple** and selected the nodes from the list.

3. (Optional) Click **Advanced Search** to display more fields and specify the following:

a. (Optional) Using the **ST Activity** check boxes, specify whether to display inbound or outbound SecureTransport activity.

b. (Optional) In the **Message** field, type a string contained in the messages to display.

c. (Optional) Use a link in the **Session ID** column to copy a session identifier into the **Session ID** field.

d. (Optional) Use a link in the **Transfer ID** column to copy a session identifier into the **Transfer ID** field.

e. (Optional) In the **Client** IP address field, type a string contained in the host name or IP address of the client associated with the transfer when the message to display was generated.

f. (Optional) In the **Edge** IP address field, type a string contained in the host name or IP address of the SecureTransport Edge associated with the transfer when the messages to display was generated.

g. (Optional) In the **Server** IP address field, type a string contained in the host name or IP address of the SecureTransport Server associated with the transfer when the messages to display was generated.

4. Click **GO**.

   The filtered log is displayed.

   Each log entry includes a time stamp, the log level, the names of the component and thread that logged the entry, the node IP address for a node in a cluster, the log message, and session and transfer identifiers.

Note In some cases, the type of a new application reported in the log message is a different form of the type you selected when you created the application.

Export the results of a server log search

Use the following procedure to export the results of a server log search.

1. Search for server log file entries as described in *Search and view server log contents* on page 305.
2. Click **Export Log**.

   A dialog box is displayed asking whether you want to open the file or save it to disk.
3. Specify whether to save the file or open the file, and then click **OK**.

Log Entry Maintenance application

The built-in SecureTransport application type, Log Entry Maintenance, performs the exclusive function of rotating server log files.

The main characteristic features of the Log Entry Maintenance application type are:

- User-definable schedule for transfer log daily backup or export and both. For more information, see *Scheduled downloads and tasks* on page 616.
- Application-specific parameters regarding the processing of server log entries include:
  - Expiration period for log entries until export or deletion and both.
  - Number of records per file.

- Support for a dedicated export folder. By default the exported entries are stored in the following location:

  `<FILEDRIVEHOME>/var/db/hist/log-entry`

For more information, see *Create a Log Entry Maintenance application* on page 770.

Audit log

Use the *Audit Log* page to view, compare, and export log entries that SecureTransport records when any change is made to the SecureTransport configuration. The audit log entries record:

- Changes made using the Administration Tool
- Changes made using the administration REST API
- Changes due to user actions, such as new user enrollment and password change
- Changes that result from a change on another SecureTransport Server in a cluster or on another synchronized SecureTransport Edge
- Changes to configuration objects, such as accounts, business units, and network zones
- Changes to server configuration parameters, whether they are made on the *Server Configuration* page or on other Administration Tool pages

In an active/active Standard Cluster (SC), SecureTransport forwards audit log updates from the secondary servers to the primary server, so the audit log on the secondary servers includes local changes only and the audit log on the primary server includes changes to all servers in the cluster.

Many Administration Tool pages include a **Last Modified** link that you can use to display in the audit log the entry that records the last change for that page. From the audit log, you can compare that entry with the last one to see what changes were made or with any previous entry for that object or parameter.

You can filter the log using one or more of eight criteria to find an entry.

Each line in the log display includes the following information:

- Time - The date and time the entry was logged. This column includes a drop-down menu indicated by an inverted caret that you can use to display more detailed information or compare log entries.
- User Name - The name of the administrator or user who made the change.
- Remote Address - The IP address of the client that made the configuration change – either a browser running the Administration Tool or a program using the administrator resources of the REST API.
- Object Type - The type of the object changed. Possible values are:
  - `Account` – for user account, unlicensed user account, service account and account template
  - `Administrator`
  - `AdministrativeRole`

- `Application`
- `BusinessUnit`
- `Certificate` – for certificate and trusted CA
- `CertificateSigningRequests`
- `ClusterNode`
- `HolidaySchedule`
- `LdapDomain`
- `LdapHomeFolderPrefix`
- `LdapUidRangeMapping`
- `MailTemplate`
- `NetworkZone`
- `PasswordVault`
- `Route`
- `ServerConfigurationParameter` – for changes that are not represented internally as objects by SecureTransport
- `SiteTemplate`
- `UserClass`

- Object ID - A unique identifier for the object changed. For most configuration objects, the object ID is an internal ID.

  For server configuration parameters, the object ID includes the server configuration parameter name, a node ID, and a profile ID. In a cluster, the node ID (`mNode`) identifies the server where a local server configuration parameters is changed. Otherwise, the value is `UNSPECIFIED`. SecureTransport 5.4 does not implement the feature that uses the profile ID (`mProfile`), so the value is always `Default`.
- Object Name - The name of the object changed.
- Operation - The type of operation that changed the object. The value can be `Create`, `Delete`, `Overwrite`, or `Update`.

  When you add a user class, it is added as the first user class as shown on the *User Classes* page. The audit log shows an update for each user classes, because adding a class changes the `Order` attribute for every class.
- Comment - Additional information added by SecureTransport or the administrator who made the change.
- All Audit Log actions are reported into the Server Log as audit information messages and administrators can configure the audit messages to be logged into the SecureTransport database or a flat file using standard `log4j` configurations. The audit information messages in the Server Log can be machine read and analyzed, while the messages on the *Audit Log* page require

interaction to identify what property has changed. The audit messages in the Server Log can also be filtered by the AUDIT component filter. For additional Server Log information, refer to *Server log* on page 304.

The audit information messages are based on the `auditLogEntry` object data. The audit information messages are in the following format:

```
<username> <operation> <objectType> <objectName> <description>
[<list of properties>]
```

Where:

- `<username>` - The name of the user which performed the audit operation.
- `<operation>` - The name of the operation performed. It could be one of the following – create, update, delete, or create_or_update.
- `<objectType>`- The object type being audited.
- `<objectName>` - The name of the object being audited.
- `<description>` (optional) - The description defined for the given `auditLogEntry`. If a description is defined, it will be displayed.
- `[list of properties]` - Contains the mapping between the property name and the old and new value. Only changed properties will be visible in this map. If there is nothing to compare with, all new properties will be visible.

The following topics describe managing the audit logs:

- *Search and view audit log contents* on page 310
- *Enable or disable audit logging* on page 311
- *Export the results of an audit log search* on page 311
- *Add or edit an audit log entry comment* on page 312
- *Display audit log entry details* on page 312
- *Compare audit log entries* on page 312.
- *Link to the audit log* on page 313
- *Audit Log Maintenance application* on page 314

Search and view audit log contents

Use the following procedure to search and view the audit log contents.

1. Select **Operations > Audit Log**.

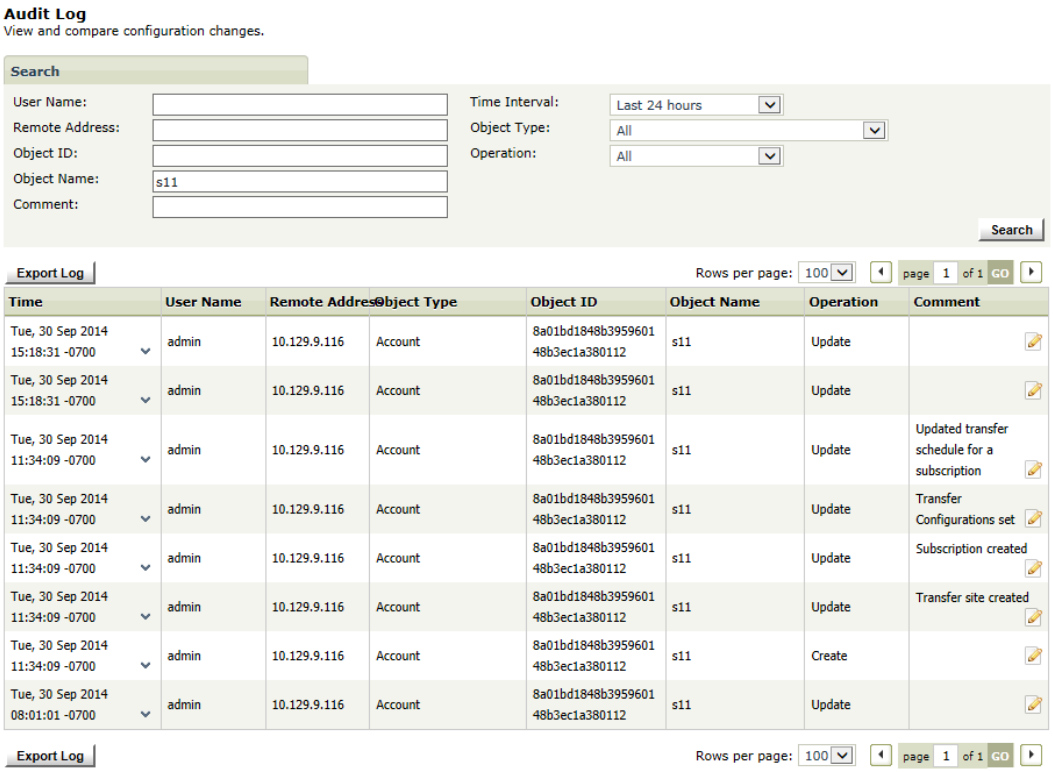
   The *Audit Log* page is displayed.

2. In the *Search* pane, specify the search criteria.

   The search fields include all the information displays in the audit log.

3. Click **Search**.

The filtered log is displayed.



Enable or disable audit logging

Audit logging is enabled by default. You can disable or enable it by setting the following server configuration parameters:

- To disable logging of changes made by the Administration Tool, set the `AuditLog.Enabled.Admin` server configuration parameter to `false`. The default value is `true`.
- To enable logging of changes made by the Transaction Manager, set the `AuditLog.Enabled.TM` server configuration parameter to `true`. The default value is `false`.

To change these parameters, see *View and change server configuration parameters* on page 315.

Export the results of an audit log search

Use the following procedure to export the results of an audit log search.

1. Search the audit log described in *Search and view audit log contents* on page 310.
2. Click **Export Log**.

A dialog box is displayed asking whether you want to open the file or save it to disk.

3. Specify whether to save the file or to open the file, and then click **OK**.

In addition to the fields displayed on the *Audit Log* page, the exported audit log contains the User-Agent string of the client that made the change.

Add or edit an audit log entry comment

Only the administrator that made the change represented by the audit log entry can add or edit a comment.

1. Click the Edit icon ( ) in the **Comment** column.
2. Type or update the comment.
3. Click the Save icon ( ).

Display audit log entry details

Use the following procedure to display the details of an audit log entry.

- From the menu in the **Time** column, select **Details**.

  SecureTransport opens an *Object Detail* window that lists all attributes of the object at the time of the audit log entry with the attribute values.

Compare audit log entries

Use the following procedure to compare audit log entries.

1. From the menu in the **Time** column, select **Compare with** or **Compare with previous**.
2. If you selected **Compare with**, SecureTransport displays a *Compare with Another Entry* window.
3. If previous audit log entries are listed, select one and click **OK**.
4. If you selected **Compare with previous** and there is a previous audit log entry for that object, the result is the same as selecting the previous entry in the *Compare with Another Entry* window.

   If there is no previous audit log entry for the object, SecureTransport displays a message.
5. SecureTransport opens an *Audit Log Entry Comparison* window.

   The *Audit Log Entry Comparison* window lists all attributes and values of the object with one column for each audit log entry. Timestamps in the column headers identify the entries. The older entry is on the left. A colored background indicates attributes with different values.

Link to the audit log

The following Administration Tool pages have a **Last Modified** link that gives the date and time of the last update to any object listed:

- Operations menu:
  - Cluster Management – Enterprise Cluster only, indicates changes to the configuration of the cluster nodes only
  - Server Configuration
- Setup menu:
  - Local Certificates
  - Trusted CAs
  - Internal CA
  - Holiday Schedule
  - Mail Template Repository
  - File Archiving
  - Network Zone List
  - Edit Network Zone entry
- Authentication menu:
  - Login Settings
  - LDAP Domains
  - LDAP Domain
  - User Type Ranges
  - Home Folders
- Accounts menu:
  - User Account
  - Unlicensed User Account
  - Service Account
  - Administrators
  - Edit Administrator
  - Administrative Roles
  - Edit Administrative Role
  - Account Template
  - Passwords Files
  - Edit Password File
  - Business Units
  - Business Units Settings

- Access menu:
    - User Classes
- Application:
    - Applications
    - Application Details

If there has been no change to the object or objects since SecureTransport was installed or upgraded to a version that includes the audit log, the link indicates `No tracked change`.

SecureTransport stores configuration that you change on other pages of the Administration Tool in sever configuration parameters. Some pages save values that are not changed when you make a change, so the audit log might include entries for the corresponding server configuration parameters in addition to the ones for the fields you changed.

When you click a link on a page, SecureTransport opens the *Audit Log* page and displayed the entry for the update that the link represents.

Audit Log Maintenance application

An application of the built-in SecureTransport application type Audit Log Maintenance deletes old audit log entries periodically and can export them to a file. By default, SecureTransport has an Audit Log Maintenance application that runs at midnight on the first day of each month and deletes audit log entries that are six months old after saving them in a file in the `<FILEDRIVEHOME>/var/db/hist/audit-log` directory

For more information, see *Create an Audit Log Maintenance application* on page 763.

Server configuration

SecureTransport server configuration consists of all the information the server and its components require to operate. You establish most of the server configuration by setting fields on the various pages of the Administration Tool. In a SecureTransport cluster, the servers store server configuration parameters in a shared database for an Enterprise Cluster (EC) and in synchronized embedded databases for a Standard Cluster (SC). The server configuration parameters include both shared, cluster-wide parameters and parameters for individual servers. When you change a shared parameter, all the servers in the cluster get the new value.

To support operation of the components that use configuration files, the server copies the configuration from the database into those files when it starts and when you change a parameter on any node of the cluster. It is not necessary to bounce the servers manually to propagate the change.

Use the *Server Configuration* page to view configuration parameters that are stored in the database and change those that are not set elsewhere in the Administration Tool. This page also includes access to pages you can use to view or update server configuration files on your local computer, synchronize configuration files, and export and import server configuration.

The following topics provide additional server configuration information:

- *Editable server configuration parameters* on page 315
- *Local server configuration parameters* on page 315
- *View and change server configuration parameters* on page 315
- *Update server configuration files* on page 317
- *Export and import server configuration* on page 318

Editable server configuration parameters

You set many server configuration parameters in fields elsewhere in the Administration Tool. You can view, but not change those parameters in the *Server Configuration* page.

Server configuration parameters that you can change have an Edit icon ( ) in the **Edit** column of the list.

Note When you hover over the description of an editable server configuration parameter, addition description information is displayed. Before editing a server configuration parameter, refer its description for configuration parameters information.

Local server configuration parameters

Most of the parameters included in the *Server Configuration* page apply to all servers in the cluster. The parameters that apply to the local SecureTransport Server and are not copied to other servers are marked with a check in the **Local** column.

View and change server configuration parameters

Many SecureTransport server configuration parameters are stored in the database. In a cluster, any change you make to any shared parameter is automatically copied to all nodes in the cluster.

The *Server Configuration* page, accessed by selecting **Operations > Server Configuration**, shows all configuration parameters that are stored in the database. You can view the values of all parameters and you can edit the values of some of them. You set the values of parameters you cannot edit on the *Server Configuration* page using fields on other pages of the Administration Tool.

The following topics provide how-to instructions for searching, paging through, and changing parameters:

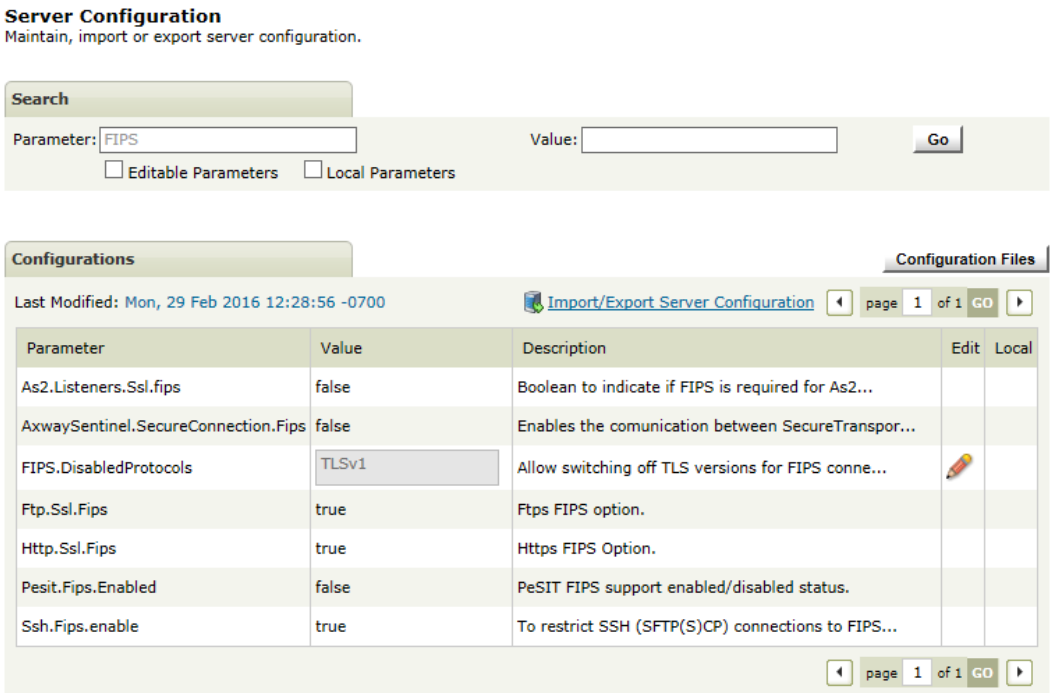
- *Search for a parameter* on page 316
- *Page through the parameter list* on page 316
- *Change a parameter value* on page 317

Search for a parameter

You can filter the list of parameters using fields in the *Search* pane.

1. To display only parameters that contain a string in their name, type that string in the **Parameter** field. The parameter name search is not case sensitive.
2. To display only parameters that contain a string in their value, type that string in the **Value** field. The parameter value search is case sensitive.
3. To display only parameters you can edit, select **Editable Parameters**.
4. To display only local parameters, select **Local Parameters**.
5. Click **Go**.

   The filtered list is displayed.



Note Drag the resize handle of a field in the **Value** column to see or change all the text.

Page through the parameter list

If there are more than 100 parameters in the filtered list, they are displayed on pages.

1. To display to the next or previous page, click the forward or back arrow.
2. To display a page, type the page number in the **page** field and click **GO**.

Change a parameter value

If a parameter is editable, you can change its value. In many case, the valid values are include in the Description column.

1. In the Edit column, click the Edit icon ( ).
2. Type the new value in the **Value** column.
3. In the Edit column, click the Save icon ( ).

   SecureTransport saves the value to the database. If the parameter applies to all nodes in the cluster, SecureTransport copies it to the other nodes.
4. To cancel an edit, click **Go** in the *Search* pane.

Note If you edit the value of a second parameter before saving the value of the first, save each value in turn, waiting for each save operation to complete before saving the next.

Update server configuration files

SecureTransport stores the following server configuration files in the database:

- `brules.xml`
- `FileServicesInterfaceRegistry.xml`
- `mime.types`
- `sentinel-returncode-translation.xml`
- `ssl.csr.conf`
- SSO Configuration Files - The Single Sign-On (SSO) related configuration files. For more information, refer to *Single Sign-On (SSO) and Single Logout (SLO)* on page 386.

You can use the *Server Configuration Files* page to make changes on your local computer to the files listed, save the changes to the database, propagate the changes to all servers in a cluster, and configure SSO for end-users and administrators. For information about how to configure the SSO functionality in SecureTransport, refer to *Single Sign-On (SSO) and Single Logout (SLO)* on page 386.

1. On the *Server Configuration* page, select **Configuration Files**.

   The *Server Configuration Files* page is displayed.
2. Download the file to update. (For example, right-click the file name link in your browser and selected **Save Link As** or **Save Target As**.)
3. Update the file using a editor on your local computer.
4. Click **Browse** and select the file or type the path to the file in the **Selected File** column.
5. Select the checkbox that corresponds to the updated file.
6. Click **Upload**.

   SecureTransport uploads the selected files to the server and copies the files to all the other servers in the cluster. The servers load the updated configuration immediately.

Notes:

- SSO configuration files are replicated on Enterprise Clusters and Standard Clusters after they are uploaded in ZIP format.
- Alternately, you can edit these configuration files on the server and then click **Synchronize** on the *Server Configuration Files* page for that server. The server saves the file in the database and copies the files to all the other servers in the cluster, and the servers load the updated configuration immediately.
- For SSO configuration files, the **Synchronize** button will update the SSO-related configuration files in `<FILEDRIVEHOME/conf/sso>` directory with the database. This will only affect the current node.
- Only ZIP format is accepted for SSO configuration files import.
- Do not put the configuration files in a sub-directory inside the ZIP file.
- You can list all SSO-related configuration files, by clicking on the **Plus** ( ) icon. You can hide the same files, by clicking the **Minus** ( ) icon.
- You can download a single SSO-related configuration file, by clicking on the name of the file. You can also download all SSO files in ZIP format, by clicking on the **SSO Configuration Files** link.
- When importing SSO Configuration Files on a SecureTransport Edge, make sure that the ZIP file contains the `sso-admin.xml`, otherwise the import will not be successful.
- When importing the SSO Configuration Files in a Standard Cluster, make sure that the Transaction Manager service is running on the current node. For more information about Standard Cluster synchronization, *Standard Cluster synchronization* on page 348.

Export and import server configuration

SecureTransport 5.4 supports import from the following releases only, patched to the latest patch or service pack – 5.3.6, 5.3.5, 5.3.3, 5.3.1, 5.3.0, and 5.2.1. The system configuration can be imported from export files produced by the same SecureTransport deployment only.

Note When you import a server configuration, the process overwrites the current configuration. If an improper configuration file is imported (for example, a blank file or potentially an export from another server), no error message is displayed and the configuration files are overwritten. Use system export with caution.

Note System import settings are deployment specific and import and export are to be used for restoration of the environment only, not for the migration or automation of environment deployments.

You can export and import server configuration information in a ZIP file.

Note SecureTransport does not support exporting the server configuration from one Enterprise Cluster (EC) and importing the server configuration into another EC cluster.

Because SecureTransport copies shared server configuration parameters to every node in a cluster upon import, you only import the shared server configuration once for the whole cluster.

The compressed `export_configuration.zip` file includes the files from the <FILEDRIVEHOME> directory plus XML files that record system the configuration parameters stored in the database (including those set on the *Server Configuration* page and elsewhere in the Administration Tool), the holiday schedule, the local certificates, certificate signing requests, and trusted CAs.

Note Database settings like port, password, and so forth are not intended to be exported because database settings are node specific.

You can export the server configuration files using the *Import or Export Server Configuration* page or command line utility. Use the command line utility to customize which folders and files will be exported. For more information, see *Export server configuration files from the command line* on page 321 and *Import server configuration files from the command line* on page 323.

Any administrator with import and export configuration privileges can access the *Import or Export Server Configuration* page to import or export the server configuration information. Any administrator who can access the server can use the command line to import or export server information.

You must supply a password that SecureTransport uses to encrypt sensitive information such as private keys and custom attributes during the export process. When you import the server configuration information, you must type the password to import the server configuration files and decrypt the sensitive information.

The imported files overwrite the existing files, the database is updated with the parameter values from the imported files, the imported files are modified to support changes made to SecureTransport, and the importer adds any new properties needed for the features introduced in the current version of SecureTransport. At the same time, the importer preserves any custom changes you have made to the imported files, applying them to the current version of SecureTransport.

The following topics provide how-to instructions for importing and exporting the server configuration, certificates, and messages:

- *Export user limit messages* on page 319
- *Export and import Internal CA files* on page 320
- *Export server configuration using the Administration Tool* on page 320
- *Export server configuration files from the command line* on page 321
- *Import server configuration files using the Administration Tool* on page 322
- *Import server configuration files from the command line* on page 323

Export user limit messages

To export messages defined on the *Limit User Access* page for successful import, add lines for all files that match `lib/msgs/msg.*Class*.*` pattern to `<FILEDRIVEHOME>/conf/export.conf` before exporting.

Export and import Internal CA files

For SecureTransport 5.0 and later, the Internal CA certificate is exported with system export and with account export. In both cases, the private key for the CA is not exported. You cannot use an imported Internal CA to sign additional certificates without the correct private key. To preserve the Internal CA private key, configure server export and import to include the private key. Perform the following procedures before you export the system configuration files. For more information on exporting and importing accounts, see *Account export and import* on page 631. For more information about exporting and importing the Internal CA, see *Manage the internal CA* on page 63.

Export the Internal CA with the private key

1. Add the following lines to the `<FILEDRIVEHOME>/conf/export.conf` file:

   ```
   lib/certs/db/ca-crt.pem
   lib/certs/db/ca-key.pem
   lib/certs/db/index
   lib/certs/db/serial
   ```

2. Export the system configuration.

   It contains the Internal CA with its private key.

Import the Internal CA with the private key

1. Delete the temporary Internal CA generated during installation, so that the Internal CA is not incorrectly imported as CA-old.
2. Import the system configuration.

Export server configuration using the Administration Tool

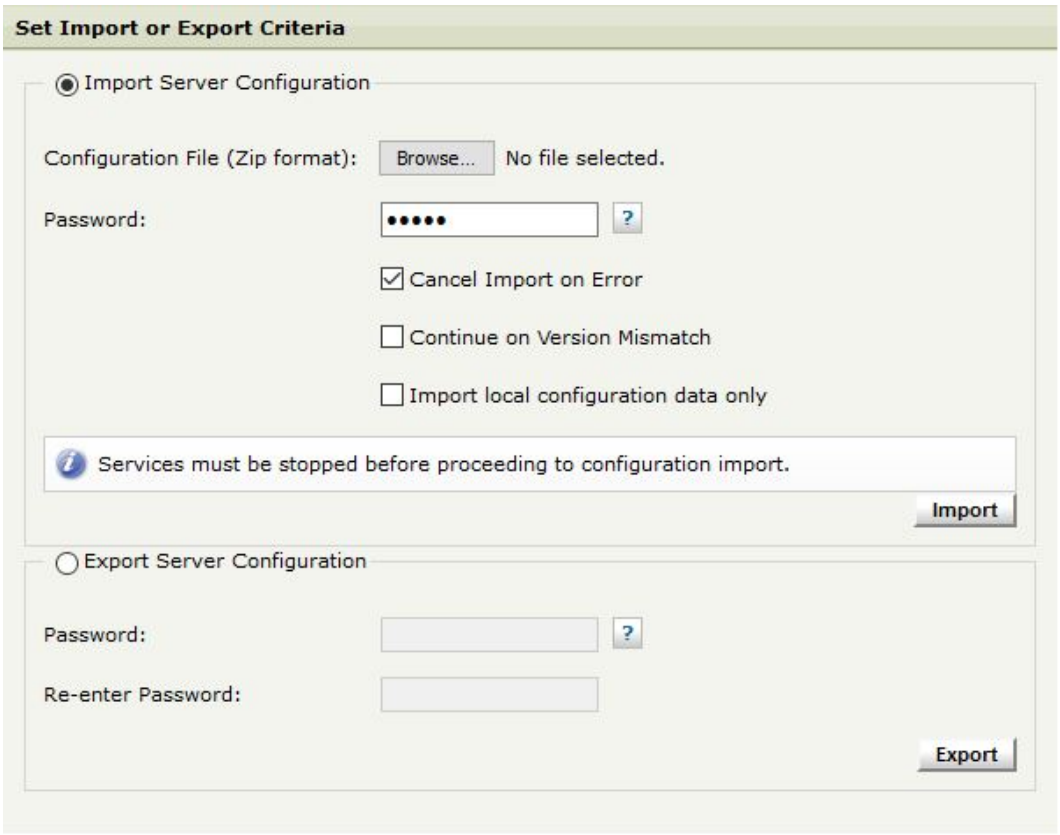
You can export and download server configuration using the SecureTransport Administration Tool. The ZIP file is also automatically backed up on the server as `<FILEDRIVEHOME>/var/tmp/export_configuration.zip`. You cannot specify the file name and location on the server, and the back up file overwrites any existing back up file.

When you export the server configuration from the Administration Tool, SecureTransport uses the file `<FILEDRIVEHOME>/conf/export.conf` to read the list of configuration files to be exported. In addition, the files in the `<FILEDRIVEHOME>/brules/local/wptdocuments` directory are always included.

You can control the file name and location, and the list of files to be exported by using the command line tool to export your server configuration files. For more information, see *Export server configuration files from the command line* on page 321.

1. On the *Server Configuration* page, click **Import/Export Server Configuration**.

   The *Import or Export Server Configuration* page is displayed.



2. Select **Export Server Configuration**.
3. Type the file password in the **Password** and **Re-enter Password** fields.
4. Click **Export**. The *Export Complete* prompt is displayed. The ZIP file is save as `<FILEDRIVEHOME>/var/tmp/export_configuration.zip`.
5. To download the ZIP file to your local computer, click **Download Exported Configuration**. The *File Download* dialog box is displayed.
6. Click **Save** to save the file to a new location or click **Open** to view the contents of the ZIP file.

   To save the file, select the location for the exported server configuration data and click **Save**. You are returned to the Import or Export Server Configuration window.

   If you clicked **Open**, the ZIP file attempts to open and display the contents of the file in a new window.

   If you do not want to download the ZIP file, click **Cancel** to return to the *Import or Export Server Configuration* page.

Export server configuration files from the command line

You can export sever configuration information using a command line tool. When you are using the tool to export a server configuration, you must specify the file name and location that contains the exported configuration.

You can also specify which files you want to export by creating a list file with a `.conf` extension. This file contains the list of configuration files you want to export. This is useful when you have customized SecureTransport and need to export additional files to those listed in the default export list. The default export list is located in `<FILEDRIVEHOME>/conf/export.conf`. Do not modify this file, but create a file with a new name if you need to make a new export list.

SecureTransport provides a script called `system_export` that you can run from the command line to export the server configuration information to a ZIP file. The script has the following options:

- `-exf=<export_file>` where `<export_file>` is the file name and location of the ZIP file. You must specify the file name.
- `-ex1=<export_list>` where `<export_list>` is the file containing a list of all files to be exported. The `<export_list>` file name is relative to `<FILEDRIVEHOME>`. The default is `conf/export.conf`.
- `-help` displays the command format and options.

Note If you run `system_export` without specifying any options, the help message is displayed.

During the export process, you are prompted for an export password. Later, when you import the exported configuration from the command line, you must use the same password for the import process. The following steps illustrate an example sever configuration export:

1. Change to the `<FILEDRIVEHOME>/bin` directory.

   If you installed SecureTransport on Windows, you can run the command without changing to the `/bin` directory.

2. Type one of the following commands:

   - `./system_export -exf=<export_file>` for UNIX-based systems
   - `system_export -exf=<export_file>` for Windows

   where `<export_file>` is the name and location of the ZIP file you are creating.

3. When prompted, type a password for the exported information.
4. Confirm the password by typing it again when prompted.

   The exported file is created in the specified location.

Import server configuration files using the Administration Tool

You can import server configuration information for a cluster or only the local server configuration information for a single server using the Administration Tool. You must know the password entered during the server configuration export process.

1. On the *Server Configuration* page, click **Import/Export Server Configuration**.

   The *Import or Export Server Configuration* page is displayed.

2. Select **Import Server Configuration**.

3. Select the **Configuration File** by clicking **Choose File**. The file must be in the zip format.
4. Type the **Password** to use to encrypt sensitive information in the file. You must use the password specified when the file was exported.
5. Select the options:
    a. Select **Cancel Import on Error** to stop the import process if any error is encountered. This option is selected by default. If the import process is stopped, no changes are made to the server. If you clear this option and the password does not match, the import completes with a warning that information from the zip archive could not be decrypted.
    b. Select **Continue on Version Mismatch** to import server configuration from a different version of SecureTransport.
    c. Select **Import local configuration data only** to exclude cluster configuration data, for example, when you are importing configuration data into a SecureTransport Server that is in an existing cluster. This option is not available if **Continue on Version Mismatch** is selected.
6. Click **Import**.

    The *Import Complete* message is displayed and the server configuration import is successful. If you did not select **Import local configuration data only**, the imported cluster configuration data is propagated to all servers in the cluster.

Note When you import a server configuration, the process overwrites the current configuration. If an improper configuration file is imported (for example, an empty file), no error message is displayed and the configuration files are overwritten.

Import server configuration files from the command line

You can import server configuration information from the command line.

SecureTransport provides a command named `system_import` that can be run from the command line to import information from the ZIP file. The command requires that the Administration Tool service is running on the SecureTransport server where you run the command.

In a Standard Cluster (SC), run the `system_import` command on the primary server. When the import completes, the updates are automatically synchronized to the other servers in the Standard Cluster or Enterprise Cluster. The script comes with the following options:

- `-exf=<export_file>` where `<export_file>` is the file name and location of the ZIP file. You must specify the file name.
- `-coe=<true | false>` where when set to `true`, the import stops if an error occurs and no changes are made to the server ("cancel on error"). If set to `false` the import continues if an error occurs. The default setting is `true`. If set this option to false and the password does not match, the import completes with a warning that information from the zip archive could not be decrypted.
- `-ivm=<true | false>` where when set to `true`, the import continues even if there is a version mismatch. Setting this option to `false` stops the import if there is a version mismatch. The default setting is `false`.

- `-ilo` means import only local configuration parameters. This options requires `-ivm=false`.
- `-help` displays the command format and options.

Note If you run `system_import` without specifying any options, the help message is displayed.

1. Change to the `<FILEDRIVEHOME>/bin` directory.

   If you installed SecureTransport on Windows, you can run the command without changing to the `/bin` directory.

2. Type one of the following commands:

   `./system_import -exf=<export_file>` for UNIX-based systems

   `system_import -exf=<export_file>` for Windows

   where `<export_file>` is the file name and location of the ZIP file. You must specify the file name.

3. When prompted, type the password for the ZIP file. You must type the password created when the file was exported.

   The server configuration information is imported into SecureTransport.

Note When you import a server configuration, the process overwrites the current configuration. If an improper configuration file is imported (for example, a blank file), no error message is displayed and the configuration files are overwritten.

If you import the wrong configuration, and then immediately try to import the correct one, the command displays an error message regarding the database password. You must restart SecureTransport after each system import.

Note Central Governance related options are not imported because they are instance specific.

Support tool

The Axway SecureTransport support tool collects information about SecureTransport and its host operating system and saves it in a support information file that you can send to Axway Global Support to help them diagnose an issue.

You use the *Support Tool Configuration* page to specify the information that the support tool saves and where it saves the file. You run a command line utility to create the support information file. If needed, you can add other information to the file by editing a custom script.

The following topics describe how to configure, customize, and run the support tool:

- *Configure the support tool* on page 325
- *Add custom information to the support information file* on page 326
- *Run the support tool* on page 327

Configure the support tool

Use the *Support Tool Configuration* page to specify the information that the support tool saves in the support information file and where it saves the file.

1. Select **Operations > Support Tool** to display the *Support Tool Configuration* page.
2. Specify the fields listed below.
3. Click **Save**.

   SecureTransport saves the configuration and replicates it to all nodes in a Server cluster or to all synchronized Edge servers.
4. (AIX only) If you selected or deselected the **Collect TM thread dump** or **Collect TM heap dump** option, restart the Transaction Manager on all clustered SecureTransport Servers or all synchronized SecureTransport Edge servers using the `stop_tm` and `start_tm` commands in `<FILEDRIVEHOME>/bin`.
5. Under *Files and Folders to Save*, add, remove, or edit the path names of files and folders to include in the support tool information file. Relative path names are relative to `<FILEDRIVEHOME>`. You can also add absolute path names.

   SecureTransport saves each the change and replicates it to all nodes in a SecureTransport Server cluster or to all synchronized SecureTransport Edge servers.

The following topics describe the support tool fields and how-to instructions for excluding files:

- *Fields* on page 325
- *Exclude files* on page 326

Fields

This topic includes information about the fields you must complete.

- **Support Access Code** - The support tool includes the value of this field in the name of the support information file. Enter the Support Access Code for the support contact that covers this system. Axway Global Support uses the code in the file name to make sure the file is handled correctly.
- **Output Directory** - Enter the path to the directory where the support tool writes the support information file. The default is `${FILEDRIVEHOME}/support` where `${FILEDRIVEHOME}` represents the SecureTransport installation directory.
- **Collect ...** - Select the check box for each category of information that the support tool saves. For the log information, specify the period by selecting a predefined period for the list or specifying the start and end dates and times. The information available for collection is different on SecureTransport Server and SecureTransport Edge.
- **Collect files and folders** - Select this to specify that the support tool save the files listed in the **Files and Folder to Save** table.

- **Files and Folders to Save** - If **Collect files and folders** is selected, the support tool saves the contents of the files listed in this table in the support information file.

  To add a file, click **Add File or Folder**, type the file or folder name in the File/Folder Name column, and click the Save icon ( ) in the right column. To remove files from the list, select the files in left column, and click **Remove**. To change a file or folder name in the list, click the Edit icon ( ) in the right column, type the file or folder name in the File/Folder Name column, and click the Save icon ( ).

Exclude files

The support tool does not save the contents of files or folders whose names are listed in the `SupportTool.ExcludeFilesFoldersList` server configuration parameter. By default, the excluded names are `certs` and `passwd`.

To add or remove names from the excluded files list, see *Change a parameter value* on page 317.

Add custom information to the support information file

The support tool is implemented as an executable script, `<FILEDRIVEHOME>/bin/collect_support_information`, that collects the information that is specified on the *Support Tool Configuration* page and saves it in the support information file.

To add custom information to the support information file, edit the `<FILEDRIVEHOME>/bin/custom_collect_support_information` script. The main script calls this script before it creates the support information file from the collected information.

By default, the custom script does nothing. Your custom script must write the information that you need to include in the support information files to the support directory that the main script writes to. The script can create files and directories in the support directory. The last action that the main script takes is to combine all the files in the support directory into the support information file.

When you write a custom script, you can use the following defined environment variables:

- **`${HOST}`–The host name of the system**
- **`${SUPPORT_DIR}`–The full path name of the directory where the custom script must write its information**

The following example `<FILEDRIVEHOME>/bin/custom_collect_support_information` script illustrates writing a file to the support directory.

```
# Collect user files
#
USER_HOME="/home/users"
USERS="partner2 partner7"

echo "=== Saving user files ==="
```

```
tar -cf "${SUPPORT_DIR}/users_${HOST}.tar" -C "${USER_HOME}" "${USERS}"
```

Run the support tool

The support tool is implemented as an executable script. To create the support information file, run `<FILEDRIVEHOME>/bin/collect_support_information`. The script saves the information configured on the *Support Tool Configuration* page in the configured output directory. The file name is `support_<supportAccessCode>_<hostName>_<timestamp>.tar.gz` where:

- `<supportAccessCode>` is the value of the **Support Access Code** field on the *Support Tool Configuration* page.
- `<hostName>` is the host name of the system that the support tool is run on.
- `<timestamp>` is the UNIX time (the number of seconds that have elapsed since midnight Coordinated Universal Time on January 1, 1970).

To write the support information file to a different directory from the one specified in the **Output Directory** field on the *Support Tool Configuration* page, use the following command:

```
<FILEDRIVEHOME>/bin/collect_support_information -d
<outputDirectory>
```

If the output directory does not exist, the support tool creates it.

The support tool can run when the SecureTransport database in not available, but it cannot collect the following information that is stored in the database:

- Server log
- File tracking
- Audit log
- Server configuration

During execution, the support tool outputs status messages and a final message that path name of the support information file. You can use SecureTransport to push the file to another location.

Note The TM thread dump can slow the operation of the TM and, more significantly, the TM heap dump can prevent the TM from processing events for 30 minutes or more, depending on the configured heap size. It is best to run the support tool when there is no load on SecureTransport.

Run the support tool automatically when the TM runs out of memory

You can configure SecureTransport to run the support tool automatically when the Transaction Manager (TM) fails with an `OutOfMemoryError`. SecureTransport runs the support tool before it restarts the TM.

1. Edit the `<FILEDRIVEHOME>/bin/crash_tm` file and comment out a line so that it is:

   ```
   # collect_crash_info="false"
   ```

2. If **Collect TM heap dump** is selected on the *Support Tool Configuration* page, edit the `<FILEDRIVEHOME>/bin/start_tm_console` file and comment out a line so that it is:

   ```
   # disableHeapDumpOnOutOfMemoryError="true"
   ```

3. Restart the Transaction Manager on all clustered SecureTransport Servers or all synchronized SecureTransport Edge servers using the `stop_tm` and `start_tm` commands in `<FILEDRIVEHOME>/bin`.

SecureTransport runs the support tool using the configuration from the *Support Tool Configuration* page.

Note Due to a technical limitation, when the `crash_tm` script runs the support tool on any system other than IBM AIX, the support information file does not include the TM thread dump.

Directory browsing

By setting up a directory structure, you can access system drives and network mounts on Windows.

Set up the structure for directory browsing

Use the following procedure to set up the structure for directory browsing.

1. Enable browsing for system drives.

   For system drives, create a directory under`<FILEDRIVEHOME>\..\cygwin\drives` with the drive letter as a name, and give permission to everyone. For example, to enable browsing of the `C` drive, create the following folder:

   ```
   <FILEDRIVEHOME>\..\cygwin\drives\c
   ```

2. Enable browsing for network shares.

   For network shares `\\<hostname>\<sharename>`, create a directory structure like the following:

   ```
   <FILEDRIVEHOME>\..\cygwin\net\<hostname>\<sharename>
   ```

   and give permission to everyone for this directory. `<hostname>` and `<sharename>` are both required.

   For example, to enable browsing of network share with path:

   ```
   \\myhost\my-shared-folder
   ```

   create the following folder:

   ```
   <FILEDRIVEHOME>\..\cygwin\net\myhost\my-shared-folder
   ```

Note System drives in the user's home folder are enabled for browsing by default.

Standard browser client

You can use a standard browser, such as Firefox or Microsoft Internet Explorer (IE) to connect to a SecureTransport Server. Using a browser allows easy access to the SecureTransport Server, but it does not offer all the features of Axway Secure Client applications. For example, the browser client does not support the Automatic Restart function. Browsers connecting to SecureTransport must support JavaScript.

No additional configuration is required on the server side for users to connect to the server with a standard browser. You can customize the interface if you prefer.

Note Customization of the interface requires knowledge of HTML and JavaScript.

The client must have JavaScript and cookies enabled.

Customize a web client

To create a custom browser client, copy the files for an existing browser HTML template and modify them. You must make the changes on all servers in a cluster.

Customize the browser client interface

The pages for the SecureTransport default browser client interface are created from HTML template pages. There are template pages for each locale supported by the server. The pages are located in the `<FILEDRIVEHOME>/share/ftdocs/html/<Locale>` directory, where `<Locale>` is the supported locale. The default pages are in the `C` (for English) directory.

Note Additional template pages reside in `<FILEDRIVEHOME>/share/ftdocs/html/skin/jb9` and `<FILEDRIVEHOME>/share/ftdocs/html/skin/sm6`. A `<Locale>` subdirectory contains the HTML files for each additional template. For more information about setting the HTML template used for the browser client, see *Select a default HTML template* on page 180.

The pages include embedded macro strings. A macro string is a special string in HTML which the SecureTransport Server understands and replaces with HTML or JavaScript code. A macro string is enclosed in angle brackets and two dashes and includes an exclamation point. For example:

```
<!--FDX_PARENT_DIR_FUNC-->
```

To customize the browser client interface, edit the HTML template pages. All custom pages must include the appropriate macro strings as listed in the Macro Strings table. Most of the HTML in the templates can be changed. The JavaScript functions can also be changed. Make these changes on each node of the cluster where they are required.

Note Editing or creating a JavaScript function must be defined in the template page.

Do not change the following parameters while editing the templates:

- Name/Value in any of the forms

  These are hardcoded in the server.
- URLs for listing, downloading, and deleting files. Do not define new macro strings or change the definition of existing macro strings.

The browser interface has template pages for the following functions:

- Login and logout
- List
- Download
- Session timeout
- Options
- Account and password management
- Message

Macro strings

The following table provides information on the macro strings that are supported by SecureTransport. Some macro strings are only supported in specific template pages, as indicated in the Description column.

Macro string	Replaced with:	Description
FDX_CHANGE_PASSWORD_MSGS	The policy used in changing passwords. It is replaced by one of four FDX Messages (see *FDX_MESSAGE* on page 331).	Used only on the *Change Passwords* page.
FDX_CLICK_URL	/~	Specifies the relative URL to which the user is redirected after displaying the authentication message, for example if the `AuthMessage` parameter of `AuthAgent` is set to `"Yes"`.
FDX_DIRECTORY_LIST	For every file or directory present in the current directory, SecureTransport adds the following line: `PrintFileURL ("FileURL", "FileName", "isDir", "size", "date", "icon")`	*FileURL* – the name of the file which can be used as the URL *FileName* – the name of file *isDir* – `0` for directory or `1` for a file *size* – size of the file (for a directory, size is N/A), `date` is the modification date of a file *icon* – the URL of an image file to be used as icon Used on the *List* page only.

Macro string	Replaced with:	Description
FDX_FILE_NAME	The current file or directory name.	Used in the *List* and *Options* pages.
FDX_FILE_URL	The escaped file name, which can be used as a URL.	Used in the *List* and *Options* pages.
FDX_HIDDEN_START_URL	<input type="hidden" name="start-url" value="/myfile.txt">	Specifies the original URL that an unauthenticated user attempted to access. Upon successful login, the user is redirected to this URL.
FDX_LIST_PARENT_DIR	The directory hierarchy of the current directory.	This is an alternative to *FDX_PARENT_DIR_FUNC* on page 331, which displays the directory structure as it is displayed in the default template. Used on the *List* page only.
FDX_MESSAGE	`FDX_Msg("message")`	*message* – the message to be displayed Used on the *Login*, *Password Fail*, and *Password Success* pages.
FDX_OPTIONS_PARENT_DIR	The directory structure of the current directory.	An alternative to *FDX_PARENT_DIR_FUNC* on page 331, which displays the directory structure as it is displayed in the default template. Used only on the *Options* page.
FDX_PARENT_DIR_FUNC	`ParentDirFunc ("DirName", "DirURL")`	*DirName* – the name of parent directory. *DirURL* – the name of parent directory which is sent as a URL. This string is an alternative to *FDX_LIST_PARENT_DIR* on page 331, which can be edited. Used in the *List* and *Options* pages.
FDX_PASSWORD_PRINT_FORM	`PrintForm()`	Used on the *Password Success* page only when the server needs to include the login form.
FDX_SERVER_INFO	`PrintServerInfo( "name", "version", "build", "host")`	Server version information: *name* – the name of the server *version* – the version of the server *build* – the build number of server, always `0` *host* – the host name of the server computer. Used only on *Login* page.

Macro string	Replaced with:	Description
FDX_XFER_MODE	`PrintXferMode(`*`mode`*`)`	*mode* – the transfer mode: `1` for binary or `0` for ASCII Used on the *List* page only.

Customize the browser client login

You can customize the type of login page the browser displays for browser client users. Change the values of the parameters described in the following table in the *Server Configuration* page. After you change any of these parameters, bounce the server.

Parameter	Use
Http.FdxAuthReply	Controls what type of login the server displays to browser client users. Valid values are: `BA` – The server displays a basic authentication window for the user to type their name and password. `HTML` – The server displays an HTML page for the user to type their name and password. `ERR` – This is used for special cases, for example where cookies are used for authentication. When ERR is set, an authentication request does not occur. To get an authentication request, enable auth, and config agents. `PREAUTH` – Enable auth and config agents. If authorization fails, the server displays an HTML page for the user to type their name and password. **Note** When `PREAUTH` is set for `Http.FdxAuthReply`, SecureTransport uses `*nobody` as an internal constant value indicating that no user is authenticated with internal agents. If a user with the name **nobody* already exists on the operating system, this may cause a conflict that prevents that user from logging in.
Http.FdxAuthAliases	This parameter controls whether items in the `<FILEDRIVEHOME>/share/ftdocs/icons/` and `<FILEDRIVEHOME>/share/ftdocs/html/` directories are authenticated. Set it to `OFF` to display custom icons on the login page.

Remove the server information displayed on the login screen

To remove the display of server information in the SecureTransport browser client, you must modify the `<FILEDRIVEHOME>/share/ftdocs/html/C/login.html` file.

Modify the function `PrintServerInfo` to return `0` as shown in the following code:

```
function PrintServerInfo(name, ver, build, host) {
    return 0;
}
```

Server backup

To minimize the risk of data loss, perform regular backups of the SecureTransport Server and SecureTransport Edge data.

When performing a server backup, you must back up the following files and directories in `<FILEDRIVEHOME>`:

- `conf/`
- `lib/certs/`
- `brules/conf/brules.xml`
- `brules/local/`
- `bin/agents/`
- `var/db/mysql/` (for servers using the embedded database)

Include the following files if changes have been made after the initial installation of SecureTransport:

- `lib/msgs/`
- `share/ftdocs/`

Include the user account home folders.

Add the following files to keep existing log files, statistics, and MDN receipts:

- `var/logs/`
- `var/db/hist/logs/`
- `var/db/stats/`

For SecureTransport Server with an external database, back up the database using standard Oracle or Microsoft SQL Server procedures.

For SecureTransport Server with an embedded database or SecureTransport Edge, use `<FILEDRIVEHOME>/bin/backup_db` to back up the database tables. The `backup_db` *`Backup_File`* command writes the backup data to the file named. You must enter the database password. You can use the `-skiplog` option to prevent the `TransactionStatus` or `TransactionData` tables from being included. To restore the data, use the following command:

```
<FILEDRIVEHOME>/mysql/bin/mysql -u root -p < Backup_File
```

For additional information about export and importing server configuration parameters and files for backup and restore, see *Server configuration* on page 314.

Standard Cluster 4

This topic describes the concepts and procedures for deploying active-active and active-passive configurations of Axway SecureTransport using Standard Clustering. For information about Enterprise Clustering, see *Enterprise Cluster* on page 351.

The following topics describe the Standard Cluster (SC) model, configuring and setting up a cluster, and managing a Standard Cluster:

- *Standard Cluster model* on page 335
- *Cluster configuration and setup* on page 341
- *Manage a Standard Cluster* on page 344

Standard Cluster model

As described in *Cluster models* on page 37, you can use a Standard Cluster (SC) to provide more capacity than a single SecureTransport Server or to provide a passive standby server to take over processing if an active server fails.

Standard Clustering uses an embedded database in each node. This minimizes external dependencies and overhead and reduces the cost of clustering. SecureTransport synchronizes most configuration changes on all nodes in the cluster.

You can configure a Standard Cluster as an active/active or active/passive (1:1) cluster. You can deploy a maximum of three servers (nodes) in an active/active Standard Cluster. An active/passive Standard Cluster has one active server and one passive standby server.

One node of a Standard Cluster is distinguished as the *primary server*. The passive node of an active/passive cluster and the one to two other nodes of an active/active cluster are *secondary* servers. The Administration Tool login screen and banner indicate **Primary Server** or **Secondary Server**.

The following topics describe the active/active and active/passive clustering and scheduled tasks, the consolidated log data representation, and the services used for cluster management:

- *Active/active and active/passive clustering* on page 336 - Describes active/active and active/passive clustering.
- *Scheduled tasks* on page 340 - Describes active/active and active/passive clustering scheduled tasks.
- *Consolidated log data representation* on page 340 - Describes the consolidated log data representation.
- *Services used for cluster management* on page 340 - Describes the services used for cluster management.

Active/active and active/passive clustering

SecureTransport supports two types of clustering: active/active and active/passive.

The following topics describe the active/active and active/passive clusters and processes:

- *Active/active clusters* on page 336
- *Active/passive clusters* on page 336
- *Active/passive deployment* on page 337
- *Primary server processes* on page 338
- *Failover* on page 339
- *Synchronization* on page 339

Active/active clusters

In an active/active cluster, SecureTransport balances the server-originating load between the primary and the secondary servers. All servers in the cluster are active and provide processing capacity. SecureTransport automatically replicates all event information collected by the primary server to the secondary servers. If the primary server fails, the cluster automatically switches control to the secondary server. An active/active cluster requires a third-party load-balancer. To prevent performance degradation if the primary server fails in an active/active cluster, the servers should have identical hardware.

The main advantages of an active/active cluster are:

- SecureTransport automatically balances the load between the different servers in the cluster.
- The secondary servers are active. This means that they can assume the load from a failed secondary server or take over from a failed primary server almost immediately.

However, to prevent performance problems, you must carefully monitor the load on an active/active cluster. An active/active cluster can suffer performance degradation when one server fails unless the remaining servers can handle the total workload for the cluster.

For more information, see *Set up an active/active cluster* on page 341.

Active/passive clusters

An active/passive cluster consists of one active server and one passive standby server with a third-party load-balancer to determine when failover is required for passive legacy and to send the users to the correct node. For passive, the SecureTransport will failover on its own. To prevent performance degradation if the primary server fails in an active/passive cluster, the servers should have identical hardware.

In an active/passive cluster, the primary server handles the event queue and processes events. While the primary server is active, the standby server remains in a passive state and does not process events. Depending on the server mode (set in the `Cluster.mode` server configuration parameter), an active/passive cluster has different features and advantages.

When the cluster mode is `passive`, the Transaction Manager runs on the secondary standby server and the event data is synchronized from the primary server. The primary server does not dispatch events to the Transaction Manager on the standby server and the standby server does not process events. The Sentinel link data is also synchronized.

The advantages of an active/passive cluster with `passive` cluster mode are:

- The cluster includes a fully redundant secondary standby server to handle the cluster workload if the primary server fails.
- Failover from the primary server to the secondary standby server is automatic.
- On failover, the cluster reports the states of file transfers to Sentinel consistently so that Sentinel can link them, so this mode is required for an active/passive cluster that works with Sentinel.

With `passive_legacy` cluster mode, the Transaction Manager listeners start on the standby server. The event data is not synchronized from the primary server, but the Transaction Manager on the standby server might accept connections and process events. You must stop the Transaction Manager on the standby server or configure your load balancer so that it does not direct traffic to it when the primary server is up and running. The Sentinel link data is not synchronized. You must disable the Folder Monitor and scheduler on the standby server. If the primary server fails, you must perform a manual failover to make the standby server active.

The advantages an active/passive cluster with `passive_legacy` cluster mode are:

- The cluster includes a fully redundant secondary standby server to handle the cluster workload if the primary server fails.
- Because events and Sentinel link data are not sent to a standby server with `passive_legacy` cluster mode, it can be in a different location for a disaster recovery (DR) if the network between the sites has required bandwidth and latency. For information on a more general DR solution using Enterprise Clustering, see *Passive disaster recovery* on page 354.

For more information, see *Set up an active/passive cluster* on page 344.

Active/passive deployment

The following diagram shows a simple active/passive deployment with `passive` cluster mode and one SecureTransport Edge server. On failover, the load balancer in the secure network redirects the connections from the internal clients and servers to SecureTransport Server 2 and the SecureTransport Edge directs the connection from the partner clients and servers to SecureTransport Server 2. For a description of the connections, see *Streaming deployment* on page 216.

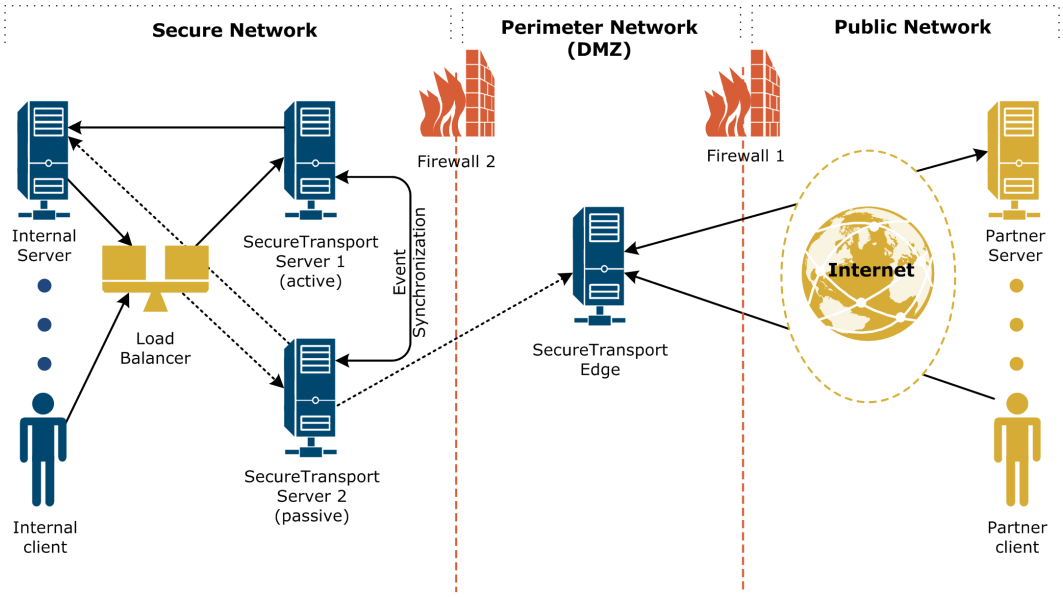


Figure 5. Active/passive deployment

The diagram does not show the shared file system where the user home directories are located.

The diagram does not show any unproxied connections or connections through HTTP proxy servers from the primary active SecureTransport Server or the secondary passive SecureTransport Server to the partner servers. For an illustrations of such a connection and more detail about connections in a streaming deployment, see *Streaming deployment* on page 216.

To handle your file transfer load or to provide redundancy in case of failure, you can deploy more than one SecureTransport Edge servers in the DMZ. Because SecureTransport Edge servers do not create and handle events, they are not clustered, but they can be configured to synchronize configuration changes. For more information, see *SecureTransport Edge synchronization* on page 372. For a deployment diagram showing multiple SecureTransport Edge server, see *Enterprise Cluster deployment* on page 352.

Primary server processes

The primary server hosts the following:

- The Folder Monitor service
- A consolidated transfer log for the cluster, displayed on the Administration Tool *File Tracking* page
- The scheduler that initiates scheduled transfers and maintenance applications

  The scheduler submits items to the internal event queue. The event queue distributes them among servers in the cluster.

Failover

When a server in an active/active cluster fails, two events occur. First, any internal load balancer for the cluster detects the server outage and fails over incoming requests to another server and all protocols servers on SecureTransport Edge servers detect the server outage and begin sending incoming requests to the TM Servers on the other SecureTransport Servers. In this case, the original client sessions are terminated and the clients must reestablish the sessions. Second, items in the event queue are reassigned from the failed server to other servers in the cluster.

When the primary server fails, one of the secondary servers is promoted to primary and the cluster continues processing messages. The secondary server promoted to primary status is determined by the order in which the server names are listed in the `<FILEDRIVEHOME>/lib/admin/config/servers` configuration file. The server listed just below the primary server in the file is considered the new primary server. When the cluster is synchronized, the state of the servers listed in the file are examined. If the first server in the servers list is online, it is reassigned as the new primary.

You can specify a timeout value that controls how long a secondary server waits before becoming the primary. For details, see *Specify the cluster connection timeout* on page 343.

When a secondary server is promoted to primary, it must run the scheduler and the Folder Monitor service. To enable this, the scheduler configuration on the primary server is replicated on all the other computers in the cluster.

When the active (primary) server fails in an active/passive cluster with cluster mode `passive`, the scheduler and the Folder Monitor service are already running on the passive standby server and failover is automatic. As with an active/active cluster, when the original active node recovers and the cluster is synchronized, the servers return to their original roles.

When the active (primary) server fails in an active/passive cluster with cluster mode `passive_legacy`, you must fail over the cluster to the standby server manually. All queued events and Sentinel link data are lost. For details, see *Manual failover* on page 348.

Synchronization

You can configure the cluster on any server. Most configuration changes are dynamically synchronized with the other servers immediately.

You must use the Administration Tool on the primary server to perform manual synchronization after you perform certain actions. Manual synchronization replaces the cluster configuration on the secondary servers with the configuration from the primary server. Data replicated during synchronization includes database tables, cluster configuration data, and cluster management data. The Administration Tool server also performs manual synchronization each time it starts on the primary server. For more details, see *Standard Cluster synchronization* on page 348.

Scheduled tasks

In an active/active cluster, the SecureTransport scheduler manages all scheduled tasks centrally from the primary server in the cluster. When schedules trigger events for scheduled tasks, one consolidated queue for all events is maintained across the cluster. This queue is shared and replicated across all the servers in the cluster so that they share the load by taking events one item at a time from the queue and performing the actual transfers or other tasks. If the primary server fails, the scheduler start on the server that becomes the new primary server.

In an active/passive cluster, the secondary standby server does not process events. If the server mode is `passive`, the standby server starts the scheduler and starts processing events when the primary server fails.

Consolidated log data representation

The transfer log allows file tracking information to be monitored across the entire cluster. To this end, the Administration Tool on the primary server in the cluster provides a consolidated view of the transfer data stored in the server logs.

If the primary server goes down, a secondary server is promoted to primary and starts maintaining the transfer log information. If the old primary server comes back up again and resumes its role as primary server for the cluster, the transfer log information from the temporary primary server is not migrated to the original primary server.

Services used for cluster management

SecureTransport implements the following services to manage and synchronize the cluster and the computers deployed in it.

The following topics describe the services used for cluster management:

- *Persistent Event Queue service* on page 340
- *Account Manager service* on page 341
- *Transfer Status Manager service* on page 341

Persistent Event Queue service

The Persistent Event Queue service is used to:

- Store certain events and replicates them to all cluster servers
- Synchronize the persistent events state to all cluster servers
- Perform recovery operations when a computer from the cluster fails during the processing of an event

- Spread the execution of following operations to all cluster servers:
  - Add a new event to the persistent queue
  - Delete an event from the persistent queue
  - Mark an event as active
  - Repair an event of a failed computer

Note The Event Queue service dispatches all events related to one remote PeSIT server to the same SecureTransport server in the cluster.

Account Manager service

The Account Manager distributes to all cluster servers dynamic information for the following events:

- Change of a user password.
- User login.

Transfer Status Manager service

The Transfer Status Manager service consolidates the transfer log on the primary server. All transfer log entries are stored in the database on the primary server.

Cluster configuration and setup

Much of SecureTransport configuration is stored in the database and synchronized dynamically to all servers in a cluster. Some configuration is stored in files that require manual synchronization. For more information, see the following topics:

- *Requirements for synchronization* on page 349
- *Server configuration* on page 314
- *Synchronize the cluster from the primary server* on page 350

The following topics provide additional configuration and setup information:

- *Set up an active/active cluster* on page 341
- *Specify the cluster connection timeout* on page 343
- *Configure servers in a cluster to trust a certificate* on page 344
- *Set up an active/passive cluster* on page 344

Set up an active/active cluster

You can set up a cluster of SecureTransport Server computers. When you set up a cluster, a shared secret file, called `taeh` file is used by each of the servers in the cluster for authentication purposes across servers and for encryption. The `taeh` file contains a randomly-generated data that secures

the SecureTransport cookies exchanged during server administration. SecureTransport generates the shared `taeh` file as part of the installation process. Refer to the *SecureTransport Installation Guide* for more information.

Note When you install SecureTransport on your secondary computers, you have an opportunity to import the `taeh` file from the primary server. You can only import the `taeh` file on a secondary computer during the installation process.

To set up an active/passive cluster, see *Manage an active/passive cluster* on page 347.

1. Make sure that the hosts file on each SecureTransport Server or SecureTransport Edge host operating system contains the hostnames and IP addresses of all servers with which it communicates: SecureTransport Server, SecureTransport Edge, and internal servers integrated with SecureTransport like LDAP, external database, Sentinel server, SSO server, ICAP server, etc.
2. Select the computer that is to serve as the primary server.
3. Make sure that the `taeh` file of the primary server is installed on all secondary computers.
4. Set up the secondary servers as independent installations. Add licenses for all servers. For instructions, refer to the *SecureTransport Installation Guide* or see *Server licenses* on page 157.
5. Generate an internal CA on each server. For instructions, refer to the *SecureTransport Getting Started Guide* or see *Manage the internal CA* on page 63.
6. Exchange CA certificates between all servers in the cluster. For details, refer to the procedures for exporting and importing SecureTransport Server CA certificates in the *SecureTransport Getting Started Guide* or in *Manage local certificates and certificate signing requests* on page 54.
7. Make sure that Transaction Manager (TM) servers are stopped on all computers.
8. On the primary and all secondary servers, list the servers in the `<FILEDRIVEHOME>/lib/admin/config/servers` configuration file. List the primary server first and continue with the secondary servers in the order you want them promoted to primary server in the event of failover.

   Edit the file and add a line of following form for each server in the cluster:

   ```
   host.example.com https://host.example.com:444
   ```

   where:

   - `host.example.com` is the FQDN or IP address of the computer
   - `https://host.example.com:444` is the URL of the Administration Tool on that computer

   and the two fields are separated by a tab character.

   Note The `<FILEDRIVEHOME>/lib/admin/config/servers` file must be the same on all computer in your cluster. You can create it on one server and copy it to the others.
9. On the primary server, generate a local certificate for encrypting cluster communications. For instructions, see *Generate a self-issued server certificate* on page 55.
10. On the primary server, export the certificate in `.p12` format protected with a password. For instructions, see *Export a local certificate* on page 58.

11. Import the certificate on each secondary server. For instructions, see *Import a local certificate* on page 59.
12. On the primary and all secondary servers, configure encryption for cluster communications. On the *Server Configuration* page, change the value of the `Cluster.Crypto.Alias` server configuration parameter to the alias of the certificate.
13. On the primary server and all secondary servers, activate the cluster. On the *Server Configuration* page, change the value of the `Cluster.mode` parameter to `active`.
14. Start the TM server on the primary server and wait until it promotes itself as a primary server. Start the TM server on all other servers in the cluster. For instructions, see *Start and stop servers* on page 253.
15. Synchronize the secondary servers manually from the Administration Tool of the primary server. For instructions, see *Requirements for synchronization* on page 349.

During cluster operation, most configuration changes are synchronized dynamically. For more information, see *Synchronization* on page 339.

Configuration optimizations in case of increased transfers load

In case of increased transfer payload, you can configure the maximum number of threads for `GeneralMessageProcessing` in the SecureTransport Server Configuration by increasing the value of the following parameter:

`Cluster.ThreadPools.ThreadPool.GeneralMessageProcessing.maxThreads`

By default this value is set to `4`. For optimal performance, you can increase this value up to `100` or even more.

You have to apply this configuration across all nodes.

Specify the cluster connection timeout

You can specify a timeout value that determines how long a secondary server waits before declaring itself the primary server. This is important in cases where the primary server is heavily loaded and takes an extended period of time to respond to a secondary computer.

- On the *Server Configuration* page of the primary server, change the value of the `Cluster.connectionTimeout` parameter to the value required in milliseconds. The default value is 60000.

Configure servers in a cluster to trust a certificate

In a cluster environment, the CA that issued the certificate must be trusted by all servers in the cluster. Refer to the procedure below. The self-signed certificates used to sign the server certificates during the installation of the servers also need to be configured across the servers. If the signing certificates for the SecureTransport servers are issued by different CAs, configure each server with the root CA certificate of that CA.

1. On primary server, export the CA certificate to a local file using the *Trusted CAs* page.
2. Copy the certificate file with the CA certificate from the primary server to the secondary server and import the certificate using the *Trusted CAs* page.
3. On secondary server, export the CA certificate to a local file using the *Trusted CAs* page.
4. Copy the certificate file with the CA certificate from the secondary server to the primary server and import the certificate using the *Trusted CAs* page.
5. Bounce both servers. For instructions, see *Limit FTP login failures* on page 183.

Set up an active/passive cluster

When you change the cluster settings to be active/passive, the secondary standby server stops processing events. For details, see *Active/active clusters* on page 336.

1. Set up a two-server cluster using the instructions in *Set up an active/active cluster* on page 341.
2. Stop the TM server on both servers in the cluster.
3. On the *Server Configuration* page of each server, change the value of the `Cluster.mode` parameter to `passive` or `passive_legacy`.
4. On the primary server, create a file named `<FILEDRIVEHOME>/var/tmp/sentinel_primary`. This file is not used for integration with Axway Sentinel. It is required whether or not Sentinel is used.

   To create the file, you can use the `touch` command in UNIX or create an empty file with no file extension in Windows. The file must have 0 bytes.
5. If you set `Cluster.mode` to `passive_legacy`, on the standby server, set `FolderMonitor.enable` and `Scheduler.enable` to `false`.
6. Start the TM server on both servers in the cluster.

Manage a Standard Cluster

The dynamic functioning of the cluster framework is part of the TM server and therefore any change of the TM server state affects the dynamic state of the respective computer in the cluster.

The following topics describe how to manage active/active and active/passive clusters and describe how to perform Standard Cluster (SC) synchronization.

- *Manage an active/active cluster* on page 345
- *Manage an active/passive cluster* on page 347
- *Standard Cluster synchronization* on page 348

Manage an active/active cluster

The following procedures describe how to perform management tasks for an active/active cluster setup.

The following topic provide the how-to instructions for managing an active/active cluster:

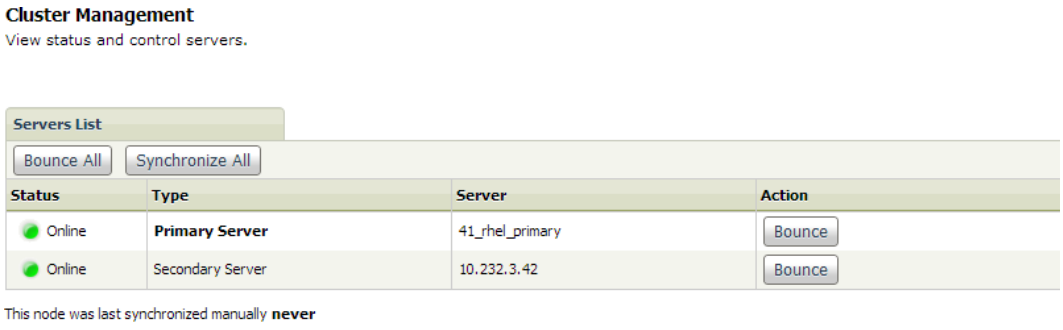
- *Monitor an active/active cluster* on page 345
- *Add a server to an active/active cluster* on page 346
- *Restore a server to an active/active cluster* on page 346
- *Remove a server from an active/active cluster* on page 346

Monitor an active/active cluster

Cluster status is displayed in the Administration Tool.

- Select **Operations > Cluster Management**.

  The *Cluster Management* page is displayed.



For each Server in the cluster, the page lists its status (online or offline), its type (primary or secondary), and its host name or IP address. Online status means the server is running and communicating with the cluster. Offline status means the server has been stopped, has failed, or cannot communicate with the cluster.

The **Bounce**, **Bounce All**, and **Synchronize All** buttons do not appear on secondary servers. To bounce a secondary server locally, see *Reload server configuration* on page 253.

On a secondary server, the time of the last manual synchronization is reported. The timestamp is also reported in the `cluster_last_sync_timestamp` file located in the `<FILEDRIVEHOME>/var/tmp/cluster_last_sync_timestamp` directory.

Cluster status is also stored in the `cluster_state` file. It contains information about which cluster node is the primary server, which are secondary servers, which servers are online, and which are offline. For example:

```
<ClusterGroup name="STCluster">
   <Member hostname="test01.your.cluster" state="online"
      status="primary"/>
   <Member hostname="test02.your.cluster" state="online"
      status="secondary"/>
   <Member hostname="test03.your.cluster" state="offline"
      status="secondary"/>
</ClusterGroup>
```

By default, the `cluster_state` file is located in `<FILEDRIVEHOME>/var/tmp/cluster_state`. You can change the location and file name by editing the following server configuration parameters:

- `Cluster.File.clusterStateFile.relative` – the base location (`fdhome` for `<FILEDRIVEHOME>`)
- `Cluster.File.clusterStateFile.path` – the path and file name relative to `Cluster.File.clusterStateFile.relative`

Add a server to an active/active cluster

1. Stop the TM server on all servers in the cluster.
2. Add the information about the new server into the `<FILEDRIVEHOME>/lib/admin/config/servers` file on the primary server.
3. Copy the `servers` file to the new computer.
4. Follow steps 11 through 15 from *Set up an active/active cluster* on page 341.

Note The new server must use the same secret file as the rest of the nodes in the cluster.

Restore a server to an active/active cluster

1. Start the Administration Tool and TM server on the restored server.
2. Perform a manual synchronization from the Administration Tool of the primary server. For instructions, see *Synchronize the cluster from the primary server* on page 350.

Note Synchronize the restored server as soon as possible. If the restored server becomes primary before it is synchronized, it might process messages based on outdated data it received before it failed.

Remove a server from an active/active cluster

When you remove a server from an active/active cluster, you can configure it as a stand-alone server.

1. On each of the nodes in t he cluster, stop the TM server.
2. On the node you are removing from the cluster:
    a. Open the `<FILEDRIVEHOME>/lib/admin/config/servers` file and remove the lines of information about the servers in the cluster.
    b. On the *Server Configuration* page, set the `Cluster.mode` parameter to `disabled`.
3. On each of the remaining nodes in the cluster, open the `<FILEDRIVEHOME>/lib/admin/config/servers` file and remove the line of information about the server you are removing from the cluster.
4. On each of the remaining nodes in the cluster, start the TM server.
5. On the primary server, perform a manual synchronization from the Administration Tool. For instructions, see *Synchronize the cluster from the primary server* on page 350.

Manage an active/passive cluster

The following procedures describe how to perform management tasks for an active/passive cluster setup.

Note A cluster with cluster mode `passive_legacy` does not monitor the state of each server in the cluster. However, if you attempt to synchronize all the servers in the cluster, and no errors occur, it indicates that both servers in the cluster are up.

Caution In an active/passive cluster, the secondary server cannot be bounced remotely.

The following topics provide how-to instructions for managing an active/passive cluster:

- *Restore a server to an active/passive cluster* on page 347
- *Remove a server from an active/passive cluster* on page 347
- *Manual failover* on page 348

Restore a server to an active/passive cluster

1. Start the Administration Tool server and the TM server on the restored computer.
2. On the primary server, perform a manual synchronization from the Administration Tool. For instructions, see *Synchronize the cluster from the primary server* on page 350.

Note It is recommended that you synchronize the restored computer as soon as possible. If the restored computer becomes primary before it is synchronized, it might process messages based on outdated data it received before it failed.

Remove a server from an active/passive cluster

When you remove a server from an active/passive cluster, the result is two stand-alone servers.

1. Stop the TM server on both servers in the cluster.
2. On each servers, open the `<FILEDRIVEHOME>/lib/admin/config/servers` file and remove the lines of information about the servers in the cluster.
3. On each server, set `Cluster.mode` to `disabled`.
4. If the cluster mode was `passive_legacy`, on the previous standby server, set `FolderMonitor.enable` and `Scheduler.enable` to `true`.
5. Restart the TM server on both servers.

Manual failover

When the primary server fails in an active/passive cluster with cluster mode set to passive_legacy, you must perform a manual failover on the passive standby server:

1. Create a file named `<FILEDRIVEHOME>/var/tmp/sentinel_primary`.

   To create the file, you can use the `touch` command in UNIX or create an empty file with no file extension in Windows. The file must have 0 bytes.
2. On the *Server Configuration* page, set both `FolderMonitor.enable` and `Scheduler.enable` to `true`.
3. On the *Server Control* page, start the TM Server.

Standard Cluster synchronization

You can configure the cluster on any server. Most configuration changes are synchronized with the other servers immediately.

When needed, you must propagate configuration data from the primary server to secondary servers across a cluster through manual synchronization. Use the Administration Tool on the primary server to perform synchronization.

You must perform manual synchronization after you:

- Upgrade SecureTransport
- Restart the whole cluster
- Restore a failed primary server
- Restart the Administration Tool server on a secondary server, if you made changes using the Administration Tool on the primary server while it was down

Manual synchronization replaces the information on the secondary servers with the configuration from the primary server. The Administration Tool server also performs dynamic synchronization each time it starts on the primary server.

You cannot use manual synchronization to data move information from the primary server to selected secondary servers.

A full synchronization may take a long time to complete and during the synchronization process, all dynamic updates are stopped, so make sure that you perform the synchronization when your system is not under heavy load.

When you create an application or account, or change the keystore password on the primary server, like most configuration information, the new application, account settings, or keystore password is copied to the secondary servers using dynamic synchronization when you save the settings. However, the audit log entry for the application, keystore password, or account creation is not copied from the primary to the secondary servers.

The directories for accounts that are synchronized manually use the UID and GID specified within the account settings on the secondary servers when the parent directory of the account exists only on the primary server in the cluster.

Note When synchronizing an application, an error message is returned indicating that the application was not copied if the secondary servers do not already have the application type the application is based on. Clicking the **Synchronize** button copies the application types from the primary server to the secondary servers, along with the application instances created.

Servers that are online, but not fully synchronized, are updated with new account and application information without having to perform a manual synchronization. You must still perform a full synchronization to start the TM server on a server that was previously down, even though the account and application information might be current.

The following topics describe the synchronization requirements and what information is synchronized and provide how-to instructions for synchronization:

- *Requirements for synchronization* on page 349
- *What information is synchronized* on page 350
- *Synchronize the cluster from the primary server* on page 350

Requirements for synchronization

Dynamic and manual cluster synchronization requires the following:

- The SecureTransport administrator account names must be the same on all servers.
- When certificate authentication is enabled for the administrator accounts, Cluster.DynamicSync.adminName and Cluster.DynamicSync.keyAlias configuration options must be set on all nodes manually.
- The SecureTransport installation path must be the same on all servers.
- The `taeh` file must be the same on all servers.
- The certificate for encrypting cluster communications specified in the `Cluster.Crypto.Alias` server configuration parameter must be the same on all servers.
- The internal CAs on all nodes must be trusted by all other nodes. Optionally, you can import the same internal CA on all nodes.
- All the SecureTransport server certificates must be issued by a common CA.

- Each server must be hosted on a different computer or virtual machine.
- All the servers in an active/active cluster must be in the same LAN.
- The two servers in an active/passive cluster with cluster mode `passive_legacy` can be in different locations, but they must be in the same low latency network.
- All servers in a cluster must have their clocks set to the same time.
- The TM Server must be running on all servers.
- All database settings must be *identical* on all the servers.

What information is synchronized

The following types of information are synchronized:

- All configuration files listed in the `<FILEDRIVEHOME>/conf/sync.conf` file
- All database tables listed in the `<FILEDRIVEHOME>/conf/sync_tables.conf` file
- All server configuration parameters that are not local to the server

The files listed in `sync.excl` are not copied from the primary to the secondary server.

Synchronize the cluster from the primary server

Use the Administration Tool on the primary server to synchronize the SecureTransport servers in a Standard Cluster.

Note The upper right corner of the Administration Tool shows whether the server on which it is running is a primary or secondary server.

1. Select **Operations > Cluster Management**.

   The *Cluster Management* page is displayed.

2. Click **Synchronize All**.

   When synchronization completes, the page displays the status of the operation and links to the secondary server Administration Tools.

Enterprise Cluster 5

This topic describes the concepts and procedures for deploying active-active clusters and clusters with passive disaster recover (DR) of Axway SecureTransport using Enterprise Clustering. For information about Standard Clustering, see *Standard Cluster* on page 335.

The following topics describe and provide the how-to instructions for managing an Enterprise Cluster (EC):

- *Enterprise Cluster model* on page 351
- *Manage an Enterprise Cluster* on page 359 -

Enterprise Cluster model

As described in *Cluster models* on page 37, the managed file transfer workload of an enterprise can exceed the capacity of Standard Clustering. Also, an enterprise might prefer to use an external database to allow their DBAs additional tuning of the underlying database. In either of these cases, you can use Axway SecureTransport 5.4 with the Enterprise Cluster (EC) option to implement at a single site a cluster that provides the capacity to handle the file transfer workload required by your organization. With an Enterprise Cluster, an external database and a high-performance cache-management layer significantly improve efficiency and increase potential scale. This allows up to 20 nodes in an active/active cluster. The Enterprise Cluster option requires your organization to provide and maintain a Microsoft SQL Server database or an Oracle database.

An Enterprise Cluster is efficient and flexible. All tasks, including scheduled work, are distributed across the cluster. You can add and remove servers as needed up to the maximum allowed by your SecureTransport features license. You can also control how the workload is directed to the servers in the cluster, for example, based on task type.

In an Enterprise Cluster, all servers are active, so there are no standby servers to replace an active server that fails. However, because the components that direct and schedule tasks are distributed across the clustered servers, the cluster implements failover by continuing to process its workload with reduced capacity when a server fails. For increased availability, you can remove another potential single point of failure by implementing a database cluster for the shared database.

Also, with the Enterprise Cluster option, you can implement an active/active cluster with a passive Disaster Recovery (DR) site. For this, you must provide a properly distributed and replicated database and file storage. To enable your implementation of passive DR, the primary production active/active cluster can notify an external mechanism to trigger failover automatically when the number of active nodes in the cluster falls below a threshold.

The following topics provide additional Enterprise Cluster information:

- *Enterprise Cluster deployment* on page 352
- *Workload distribution* on page 353

- *Passive disaster recovery* on page 354

Enterprise Cluster deployment

An Enterprise Cluster (EC) distributes the workload among a collection of networked SecureTransport Servers, all of which are active. All servers in an Enterprise Cluster must be on the same low latency network.

The following diagram illustrates a possible deployment architecture for an Enterprise Cluster that serves partners who access it using the Internet. The arrows show the direction of network connections for all the protocols. Data flows in both directions after the connection made.

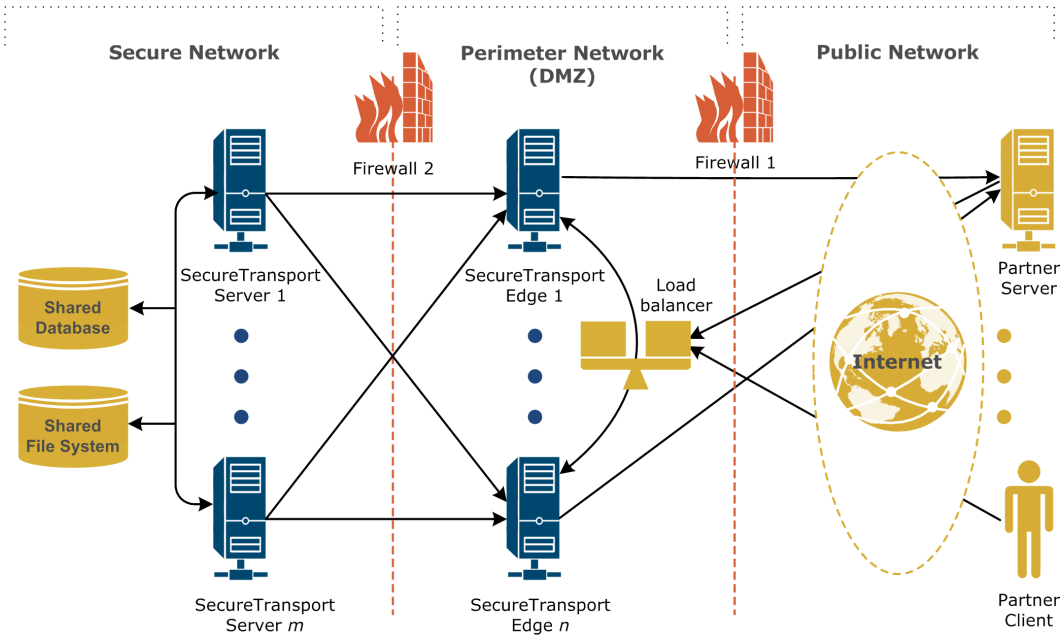


Figure 6. Enterprise Cluster

The diagram does not illustrate the event synchronization among the SecureTransport Servers or any unproxied connections or connections through HTTP proxy servers from the SecureTransport Servers to the partner servers. For an illustration of an unproxied connection and more detail about connections in a streaming deployment and configuration for internal clients and servers, see *Streaming deployment* on page 216.

Deploy the number of SecureTransport Servers and SecureTransport Edge servers required for your file transfer workload. The connections from the TM Servers on the SecureTransport Servers to the protocol and SOCKS5 proxy servers on the SecureTransport Edge servers is many-to-many, so you can design your deployment with consistent or specialized configuration. For more information, see *Communication across Transaction Manager, protocol, and proxy servers* on page 215. Because SecureTransport Edge servers do not create and handle events, they are not clustered, but they can be configured to synchronize configuration changes. For more information, see *SecureTransport Edge synchronization* on page 372.

Components

This example deployment architecture includes the following components:

- **SecureTransport Servers** – An Enterprise Cluster has two or more SecureTransport Servers. Each SecureTransport Server has an installation directory on its local file system. All the installation directories must have the same path. You can also deploy SecureTransport with the EC option as a single Server when you require an external database.
- **Shared external database** – The SecureTransport Servers share an external database that they use to implement the cluster. The shared database stores all the shared (cluster-wide) configuration data and much of the local (individual) configuration data for the servers.
- **Shared file system** – The SecureTransport Servers share a file system on external storage for working directories and files, for example, using a shared disk file system on a storage area network (SAN) or using network-attached storage (NAS). Because all servers in a cluster share many configuration definitions that include references to directories, such as accounts, the shared file system hosts those directories. SecureTransport installation on a private SAN logical unit number (LUN) is also a supported configuration.
- **SecureTransport Edge servers** – If an Enterprise Cluster provides service to systems in a public or external unsecured network, it usually includes SecureTransport Edge servers. A cluster deployment usually includes one SecureTransport Edge for each SecureTransport Server, but this can vary depending on the characteristics of the workload. The SecureTransport Edge servers are not clustered, but their configuration can be synchronized.
- **Firewalls** – The firewalls implement the perimeter network required to serve client systems in a public or external network.
- **Load balancer** – In the Enterprise Cluster deployment diagram, the load balancer implements workload distribution by distributing the incoming requests from the external clients and servers among the SecureTransport Edge gateways. The specific load balancing method depends on the characteristics of your workload and cluster deployment.

Workload distribution

Event distribution in a SecureTransport Enterprise Cluster (EC) is handled by a distributed event processor and a distributed scheduler. As long as one SecureTransport Server is running, incoming and scheduled tasks are assigned.

You can configure the event processor to distribute events based on their attributes, however the event processor assigns all events related to one remote PeSIT server to the same SecureTransport server. Event assignment options are:

- Events can be assigned to a server with required functionality.
- Events associated with an particular account can be assigned to the same server. This can improve the performance of the distributed object cache by caching the object that represents the account and related object where they are used.

Passive disaster recovery

If Axway SecureTransport provides an essential function in your organization, it is likely to require a business continuity plan. To assure business continuity, you can deploy your Axway SecureTransport 5.4 Enterprise Cluster with passive disaster recovery (DR). The following diagram illustrates a recommended deployment architecture for an Enterprise Cluster with passive disaster recovery. The arrows show the direction of network connections for all the protocols. Data flows in both directions after the connection made.

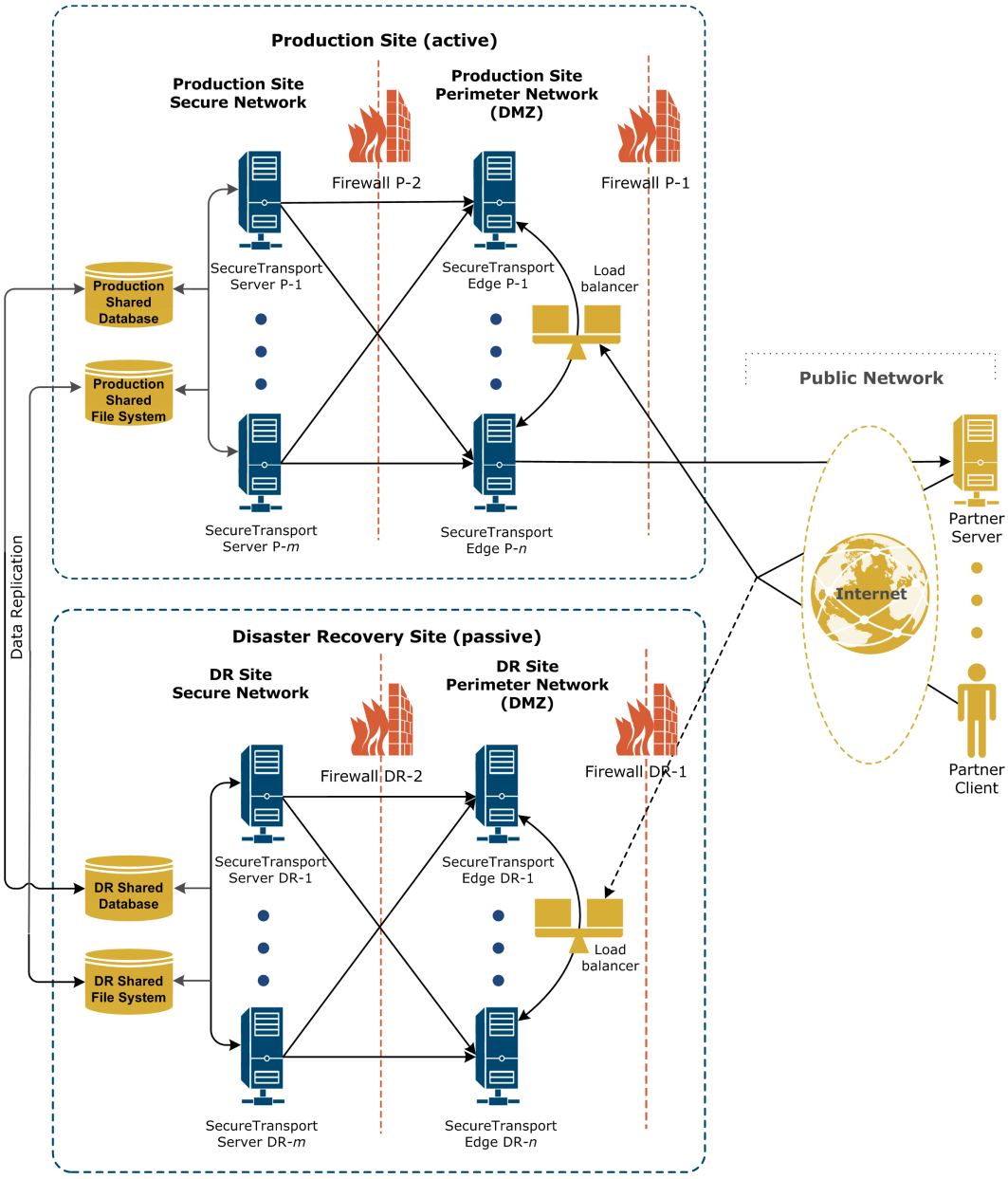


Figure 7. Enterprise Cluster with passive disaster recovery

The diagram does not illustrate the event synchronization among the SecureTransport Servers in one site or any unproxied connections or connections through HTTP proxy servers from the SecureTransport Servers to the partner servers. For simplicity, the diagram shows only one connection from a SOCKS5 proxy on a SecureTransport Edge to a partner server. The SOCKS5 proxies on all the SecureTransport Edge servers can connect to the partner servers through the firewalls as needed. For an illustration of an unproxied connection and more detail about connections in a streaming deployment and configuration for internal clients and servers, see *Streaming deployment* on page 216.

This deployment architecture uses a redundant Enterprise Cluster and SecureTransport Edge servers at a separate site to provide passive DR. The DR cluster must provide the functionality of the production cluster with the same number or fewer servers than the production cluster. The SecureTransport Edge servers must also provide the functionality of the production site with the same number or fewer servers than the production site. All the servers must run on the same type of operating systems with the same installation directory, secret file, and configuration as the production servers. The SecureTransport Servers in the DR cluster must also have the same database type and configuration as the production SecureTransport Servers and the shared file system must be mounted under the same path on all SecureTransport Servers.

Each server in the DR site is associated with a server in the production site. So if there are fewer servers in the DR site, some servers in the production site are not associated with a server in the DR site. If there are fewer servers in the DR cluster, the configuration of the production site servers that are not associated with a server in the DR site must be maintained on the DR site so that the configuration can be replicated to the production site failback. The DR site *Cluster Management* page lists any production site servers that are not associated with a server in the DR site and shows them as offline.

The DR site is a passive standby. The servers in the DR site do not run when the production site is operational, but the configuration of the DR cluster and the DR SecureTransport Edge servers must be consistent with the configuration of the production cluster and SecureTransport Edge servers so that the DR site is ready to replace the production site. However, the IP addresses of the servers in the production site and the servers in the DR site can be different.

Each cluster has its own shared database and shared file system. So that the DR cluster can replace the production cluster when it is needed, you must implement database synchronization between the production cluster database and the DR cluster database so that the configuration and operational data is consistent. You must also implement data synchronization between the production cluster shared file system and the DR cluster shared file system so that the account home folders and other folders are consistent. Do not synchronize the file systems that host the operating systems and the SecureTransport application files. You keep these consistent by applying the same patches, services packs, and configuration file changes to all servers.

The system configuration and account information of the SecureTransport Edge servers in the production site and the SecureTransport Edge servers in the DR site must be consistent. If there is just one SecureTransport Edge server or if the SecureTransport Edge servers in the sites are synchronized, you can export the system configuration and administrator account information from one of the SecureTransport Edge servers in the active site, import it into one of the SecureTransport Edge servers in the inactive site, and synchronize the SecureTransport Edge servers in the inactive site. You need to do this whenever you change the system configuration or accounts on a SecureTransport Edge server in the active site. To import system configuration and account

information into a SecureTransport Edge server or to manually synchronize SecureTransport Edge servers, you must start the database and the Administration Tool server. After the SecureTransport Edge servers are updated, you must stop all services on them.

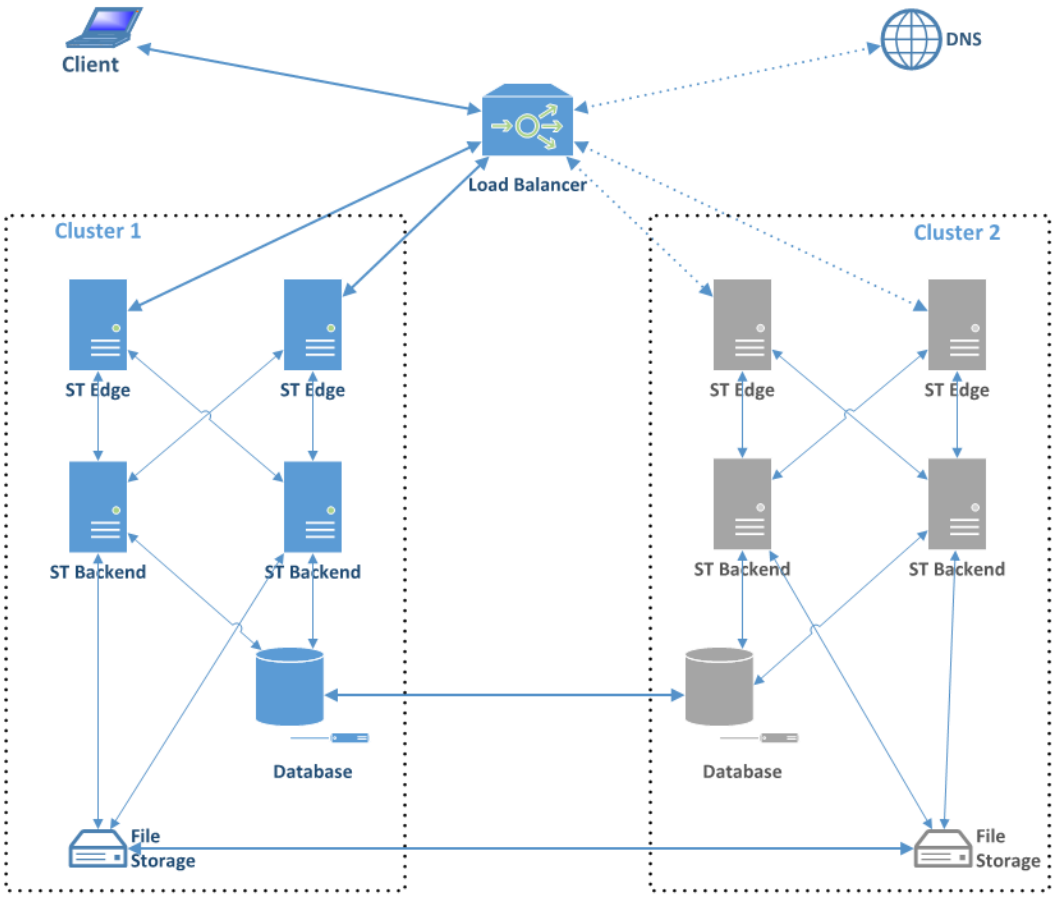
Note If SecureTransport is deployed in a secure perimeter network (DMZ) configuration, the DMZ zones configuration cannot be modified. As a result, streaming is not operational in the DR site (as the nodes have different IP addresses) and all server-initiated transfers set to establish a connection through a DMZ zone will use the IP addresses configured for the production environment.

If you maintain consistency between the production and the DR sites, you can choose to use an external DR solution.

Zero downtime in active-passive deployment

Zero downtime is a concept that allows to smoothly redirect traffic from an active LEC cluster to a passive LEC cluster without experiencing interruptions in file transfers and event logging. This feature allows you to keep current your ongoing transfers running while you prepare your initially active cluster for upgrades or maintenance.

The following diagram shows a simplified model of a setup that includes active Cluster (1) and passive Cluster (2). Initially, Cluster 1 handles all traffic from the load balancer while Cluster 2 is idle: there are no client connections and scheduled transfers are disabled.



The process of zero downtime requires you to follow several steps to ensure best results.

Prerequisites

To ensure zero downtime, the following prerequisites must be met:

- The active and passive cluster must have identical configuration and deployment.
  - both must use the same `taeh` file (used by each of the servers in the cluster for authentication and encryption purposes across servers)
  - both must have the same system configurations and account schemas configured
- The Load balancer balances traffic between the edges (SecureTransport nodes on Cluster 1) by hostname, resolved by internal DNS server (or hosts file on the Load Balancer host)
- File storages on both clusters must be in constant sync and file contents must be identical and present at both clusters
- The database replication requires that databases on both clusters contain a special set of tables. The following list of database tables contains the one that **must not be** synced.
  - AUDITLOG
  - CLUSTERNODE
  - DMZ_EDGE
  - DMZ_EDGE_IP_ADDRESS
  - DMZ_EDGE_PROTOCOL
  - DMZ_EDGE_PROXY
  - DMZ_ZONE
  - EVENT
  - HT_BUSINESSUNIT
  - LOGGING_EVENT
  - LOGGING_EVENT_EXCEPTION
  - LOGGING_EVENT_EXCEPTION_TEMP
  - LOGGING_EVENT_PROPERTY
  - LOGGING_EVENT_PROPERTY_TEMP
  - LOGGING_EVENT_TEMP
  - SUBTRANSMISSIONSTATUS
  - SUBTRANSMISSIONSTATUS_TEMP
  - TRANSFERDATA
  - TRANSFERDATA_TEMP
  - TRANSFERDETAILS

- TRANSFERDETAILS_TEMP
- TRANSFERPROTOCOLCOMMANDS
- TRANSFERPROTOCOLCOMMANDS_TEMP
- TRANSFERRESUBMITDATA
- TRANSFERRESUBMITDATA_TEMP

Zero downtime execution steps

Several steps must be executed on the Cluster 1 and Cluster 2 in order to redirect seamlessly traffic redirection from Cluster 1 to Cluster 2:

1. Stop Monitor Server on all SecureTransport Servers and Edges in Cluster 1 (and Cluster 2, if applicable).
2. Stop all database replications across Clusters 1 and 2. Do not stop file system replications.
3. Redirect the load balancer traffic from Cluster 1 to Cluster 2.
4. On Cluster 1, stop the Scheduler and Folder Monitor on SecureTransport Servers.
5. On Cluster 2, start the Scheduler and Folder Monitor on SecureTransport Servers.
6. On Cluster 1, stop the protocol servers gracefully on all SecureTransport Servers and Edges. For more information, see *Graceful shutdown of protocol servers* on page 265.
7. On Cluster 1, make sure all protocol servers (on all SecureTransport Servers and Edges) are stopped in order to proceed with stopping the Transaction Manager gracefully. For more information, see *Graceful shutdown of Transaction Manager* on page 266.
8. Stop any remaining services on SecureTransport Servers and Edges in Cluster 1 – admin services, proxy services, etc. Use the `stop_all` console command:
   `<FILEDRIVEHOME>/bin/stop_all` (or, on Windows, `<FILEDRIVEHOME>\bin\stop_all.com`).

Note You can execute Steps 4, 6 and 7 on Cluster 1 SecureTransport Server nodes at once by shutting down gracefully each. For more information, see *Graceful shutdown of SecureTransport Server node* on page 267.

This is the list of basic steps your need to go through in order to gracefully shut down Cluster 1 after redirecting the load balancer traffic to Cluster 2. Once in downtime, Cluster 1 is ready for maintenance or upgrade procedures while Cluster 2 will be handling all requests and transfers. At some point Cluster 1 will be in passive mode while Cluster 2 will be the active one.

Once you decide to perform the reverse process: make Cluster 1 active and Cluster 2 passive again, follow the same steps as described above but perform each step on Cluster 2 instead of Cluster 1 and vice versa. This means that, for example, in step 2 you will switch load balancer traffic from Cluster 1 to Cluster 2 and apply steps 3 to 6 on Cluster 2.

Known limitations

- During the zero downtime process, no configuration changes must be performed since replications across clusters are disabled in Step 1.
- After Step 2, the File tracking and Audit log on Cluster 1 will record only data for already initiated connections, events and transfers (on Cluster 1), plus respective post-processing info. events. All "new" traffic will go in Cluster 2, respectively all events will be logged in the File tracking and Audit log on Cluster 2. There is no replication of these logs across Cluster 1 and Cluster 2.

Manage an Enterprise Cluster

As described in *Cluster models* on page 37, an Enterprise Cluster is a SecureTransport deployment that uses a collection of servers at a single site to provide the capacity to handle a very large file transfer workload. All SecureTransport Server systems in the cluster share an external database and a file system. This topic describes how to set up and maintain an Enterprise Cluster (EC). These operations are available only on the SecureTransport Server.

The following topics provide the prerequisites and how-to instructions for managing an Enterprise Cluster:

- *Enterprise Cluster prerequisites* on page 359
- *Set up a cluster* on page 360
- *Add a server to a cluster* on page 361
- *Remove a server from a cluster* on page 363
- *View cluster status* on page 363
- *Notification of cluster status* on page 364
- *Set up a disaster recovery cluster* on page 365
- *Maintain a disaster recovery cluster* on page 366
- *Disaster recovery failover and fallback* on page 367
- *Direct cluster workload* on page 368
- *Configuration optimizations in case of increased transfers load* on page 361 .

Enterprise Cluster prerequisites

Before you deploy an Enterprise Cluster, you must have:

- A features license that permits the number of clustered SecureTransport Servers (nodes) in your cluster.
- A license for all the SecureTransport Edge servers in your cluster.
- An external Oracle or Microsoft SQL Server database server or cluster that satisfies the requirements described in the *SecureTransport Installation Guide*.

- A file system that all servers in the cluster can access (for example, using network-attached storage).
- The working network, including the firewall and load balancer systems required by your cluster deployment.
- The time settings (clocks) on all computers in the network synchronized.
- If a secure connection to the database is used, the cluster server installer will need to have the database certificate or access to the Java key store containing the database certificate.

Set up a cluster

This is an overview of the steps required to create an Enterprise Cluster (EC). For the procedures to perform the server installation and initial configuration, refer to the *SecureTransport Installation Guide*.

1. Implement and test the network and computers for the cluster, including the shared database and shared file system.
2. Install the first SecureTransport Server.

   When you install the first SecureTransport Server, the installer creates the schema for the cluster in the shared database.
3. Perform the initial configuration for the first SecureTransport Server.
4. Install the other SecureTransport Servers. Specify the same installation directory, specify using the existing database schema, and import the `taeh` file from the first server.
5. Perform the **Install Licenses** steps of the initial configuration for the other SecureTransport Servers.

   Do not perform the other steps of the initial configuration because the configuration is copied to the other servers when they are added to the cluster.
6. Stop all the protocol servers and services on all nodes except one. Make sure that the Administration Tool server and the Transaction Manager server are running on only one SecureTransport Server.
7. Log on to the Administration Tool on the running server as the `admin` user, and add to the cluster each of the cluster nodes, including the one you are logged on to. For details, see *Add a server to a cluster* on page 361.

   Note Do not restart any other SecureTransport Server until it is added to the cluster.
8. Restart all SecureTransport Servers.
9. Install all the SecureTransport Edge servers and perform the initial configuration for them.

The Enterprise Cluster is now operational with its basic initial configuration. Because SecureTransport Server automatically copies most configuration to all SecureTransport Servers in the cluster, you perform most configuration tasks once on one SecureTransport Server. For more details, see *Server configuration* on page 314.

Configuration optimizations in case of increased transfers load

The following suggested configuration allows the SecureTransport administrator to specify the number of daemon threads used by the invocation service in the invocation-scheme configuration in `conf/hibernate-cache-config.xml`:

```
<!-- The DefaultInvocationService is used by the
com.tumbleweed.st.server.api.cluster.InvocationManager -->

<invocation-scheme>

        <scheme-name>invocation-service</scheme-name>

        <service-name>DefaultInvocationService</service-name>

        <thread-count>0</thread-count>

        <autostart>true</autostart>

</invocation-scheme>
```

Note `<thread-count>` is an optional parameter which specifies the number of daemon threads used by the invocation service. When set to zero, all relevant tasks are performed on the service thread. Accepted values include '`0`' and positive integers. The default value is the value specified in the `tangosol-coherence.xml` descriptor.

Add a server to a cluster

If a SecureTransport Server uses the cluster shared database schema and shared file system, you can add it to the cluster using the Administration Tool. To connect a SecureTransportServer to an existing database schema, see *Switch from the embedded database to an external Oracle database* on page 96 or *Change the external Oracle database* on page 100.

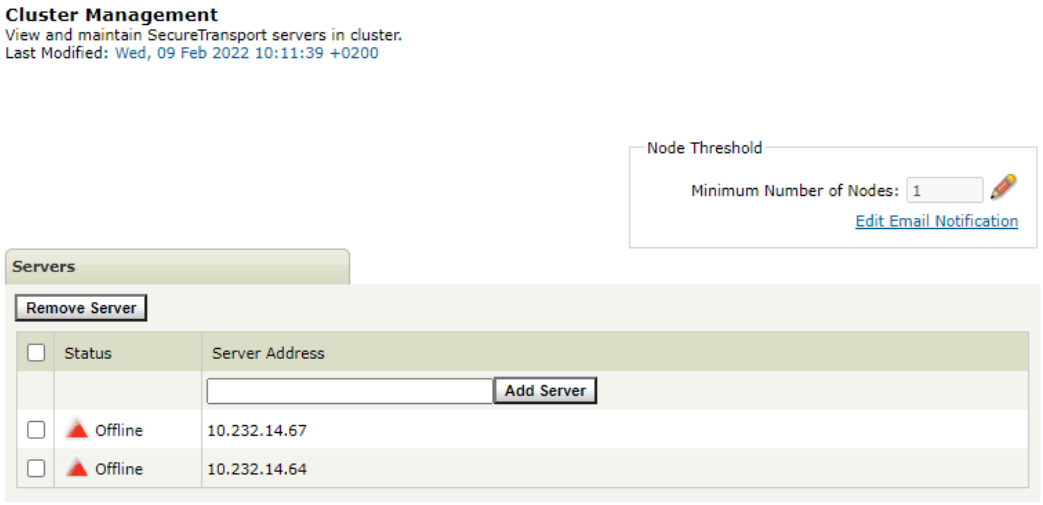
To use IPv6 addresses for communication between servers in an Enterprise Cluster (EC), you must edit the `<FILEDRIVEHOME>/conf/tangosol-coherence-override.xml` file on each server and set the value of the `<address>` element to the IPv6 address of the network interface used for cluster communications. The first lines of the `<cluster-config>` element must be:

```
<cluster-config>
    <unicast-listener>
         <address>IPv6-address</address>
```

Use the following procedure to add a SecureTransport Server to an existing Enterprise Cluster. For instructions on how to set up a cluster, see *Set up a cluster* on page 360.

1. Stop all services on all cluster nodes by running `<filedrivehome>/bin/stop_all` on each one.
2. Stop all services on the server or servers you want to add to the cluster.

3. Start the Administration Tool on the first installed node by running `<filedrivehome>/bin/start_admin`.
4. Log in to the Administration Tool and select **Operations > Cluster Management**.

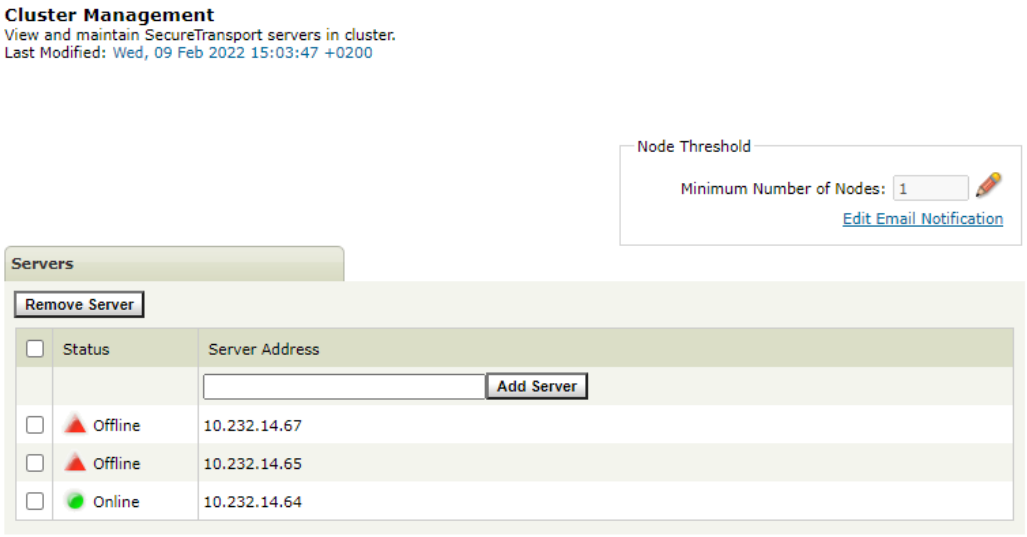


5. In the **Server Address** field in the **Servers** table, enter the IP address of the SecureTransport Server you want to add to the cluster and click **Add Server**. Repeat this step for any other server you want to add.

Note You must use the IP address of the server. Do not use the hostname or the FQDN.

Note The Administration Tool does not prevent you from adding the same IP address to the cluster more than once, but this is not a valid operation and the cluster may not form if an IP address is duplicated.

6. Start all services on the first installed node by running `<filedrivehome>/bin/start_all`.



Only the node you are currently logged on to is displayed with an Online status. The newly added server is displayed in the table with an Offline status, indicating it is not yet connected to the cluster.

7. Start all services on the newly added server or servers by running `<filedrivehome>/bin/start_all`.
8. Validate that all servers have been successfully added to the cluster (displayed with an Online status on the *Cluster Management* page).

Note The Administration Tool service must run on all nodes in the cluster even if you are not accessing them through the Administration Tool.

Note The feature license defines the maximum number of nodes in an Enterprise Cluster. If you attempt to start a Transaction Manager that exceeds the maximum number of nodes, the Transaction Manager will not start or process tasks.

Remove a server from a cluster

Use the following procedure to remove a SecureTransport Server from a cluster.

1. Make sure all services are still running on the node or nodes you are about to remove from the cluster.
2. Log in to the Administration Tool (preferably on the first installed node) and select **Operations > Cluster Management**.
3. In the **Servers** table, select the node or nodes to be removed from the cluster.
4. Click **Remove Server**.

   The selected server is removed from the **Servers** table and is no longer a part of the cluster.
5. Run `<filedrivehome>/bin/stop_all` on the removed server.

Note The local server configuration settings for a removed server remain in the shared database. To avoid problems with the shared database, do not start any removed SecureTransport Server until you add it back to the same cluster.

Note If a server is removed from the cluster and added back after a daemon configuration change, the private zone of the secondary server will not be updated to reflect the change. You will need to apply the changes manually by updating the *Server Control* page of the added server and restarting the changed daemons and the Transaction Manager.

View cluster status

Use the following procedure to view the cluster status.

1. Select **Operations > Cluster Management.**

   The *Cluster Management* page is displayed.

2. In the **Servers** table, check the **Status** column.
    - **Online** – The SecureTransport Server is reachable and both the TM and Administration Tool server are running.
    - **Offline** – Either the SecureTransport Server is not reachable, the Transaction Manager is not running, or the Administration Tool server is not running.

SecureTransport makes an entry in the server log when a server in the cluster goes offline.

To refresh the **Status** column, select **Operations > Cluster Management**.

If the status of a SecureTransport Server is Offline, you can check its status in more detail.

- Log in to the server using the Administration Tool, select **Operations > Server Control**, and make sure that the TM Server is running.
- If you cannot connect to the server using the Administration Tool, log in to the computer that hosts the server and make sure that the SecureTransport Administration Tool and TM server are running.

Note If a SecureTransport Server fails, the distributed event manager assigns pending events to other servers, but user sessions connected to the failed server are closed. However, Axway Secure Client automatically reestablishes the closed session and resumes any transfers.

Notification of cluster status

SecureTransport can send an email notification when the number of online servers in the cluster falls below a limit that you set. If enabled, SecureTransport sends an email each time it detects a server failure. You can use this notification for the following purposes, among others:

- Set the limit to one less than the number of nodes in the cluster and use the notification to inform you to restore the node that is offline.
- Set the limit to one less than the number of nodes required for acceptable performance and use the notification to inform you to evaluate whether to fail over to your standby disaster recovery site.

You configure the email notification in the **Node Threshold** topic of the *Cluster Management* page.

1. Select **Operations > Cluster Management**.

   The *Cluster Management* page is displayed.
2. To change the value of the **Minimum Number of Nodes** field:
    a. Click the Edit icon ( ).
    b. Type the new value in the field.
    c. Click the Save icon ( ).
3. To configure the notification email, click **Edit Email Notification**.

The *Email Notification* page is displayed.

a. To send the emails, select **Send Notification**.

b. Type the email subject in the **Subject** field and the email body in the **Notification** field.

c. Click **Save** to save your changes or **Cancel** to reset the values to the last saved values.

d. Select **Operations > Cluster Management to** return to the *Cluster Management* page.

4. To set the address the email is sent to, select **Setup > Miscellaneous**.
5. Make sure all the fields in the *FTP/HTTP Startup Password Timeout Configuration* pane have valid values.

Note You must change the default value, `root@localhost`, of the **Notify e-mail** field to a complete and valid email address. This address is used for both the sender address and recipient address.

Set up a disaster recovery cluster

Use the following procedure to set up a disaster recovery cluster.

1. For each SecureTransport Server in your production cluster, edit the `<FILEDRIVEHOME>/conf/options-overwrite.conf` file and replace

   `#Cluster.DeploymentSite=Prod`

   with

   `Cluster.DeploymentSite=Prod`

2. On one SecureTransport Server in the production site:

   a. On the *Server Configuration* page:

      - Set `Cluster.EnableDRConfiguration` to `true`.
      - Make sure that `Cluster.DeploymentSite` is set to `Prod`.

   b. For each network zone node, make sure the **Deployment Site** field is set to `Prod` so that this node will be used when `Cluster.DeploymentSite` is set to `Prod` and define another node for the DR site with the **Deployment Site** field set to `DR`.

3. Deploy a separate cluster that duplicates your production cluster. For information you need when you plan your DR cluster and install the servers, see *Passive disaster recovery* on page 354. To initialize the DR site:

   a. Synchronize the database for the DR cluster with database for the production cluster so that configuration is consistent with the production cluster.

   b. Synchronize the data for the DR cluster with data for the production cluster so that the account home folders and other folders are consistent.

4. For each SecureTransport Server in the DR site:
    a. Copy the `<LocalConfigurationsId>` element in `<FILEDRIVEHOME>/conf/configuration.xml` from the corresponding server in the production site.

       The content of the `<LocalConfigurationsId>` element establishes the correspondence between a production server and its corresponding DR server.
    b. Edit the `<FILEDRIVEHOME>/conf/options-overwrite.conf` file.
        - Replace

          `#Cluster.DeploymentSite=Prod`

          with

          `Cluster.DeploymentSite=DR`
        - Replace

          `#node.ip=`

          with

          `node.ip=`*`IP_adderess`*

          where *`IP_adderess`* is the IP address of the system that the SecureTransport Server is running on.

       When SecureTransport Server starts, it updates the database with this IP address.

       Note You can use `options-overwrite.conf` to overwrite any local or shared editable server configuration parameter that you can set on the *Server Configuration* page.
5. For each SecureTransport Edge in the DR site:
    a. Update the network zone node of the `Private` network zone so that it references the SecureTransport Servers in the DR cluster.
    b. Export system configuration from the associated production SecureTransport Edge and import it.
6. If you are using a separate shared databases for each site, log in to the Administration Tool on each SecureTransport Server in the DR cluster and change the database to the DR shared database.
7. Set up email notification on the production cluster and define the procedure by which you decide to switch to the DR site and the method you use to switch.
8. Set up and test the data replication from the production cluster to the DR cluster.

Maintain a disaster recovery cluster

Once your DR site is set up, you must maintain consistency with the production site as described in *Passive disaster recovery* on page 354 so that the data in the DR shared database and the DR shared file system are current.

When you edit a configuration file or a script on an active SecureTransport Server or SecureTransport Edge, consider if you need to make the same changes on the corresponding server in the other site.

After you fail over to the DR cluster, you need to restore your production cluster's functionality. Before you switch back to your production cluster and return your DR cluster to standby status, you must replicate the data in the DR shared database and the DR shared file system to the production site.

Disaster recovery failover and fallback

You can use cluster status notification to decide when you must fail over to the disaster recovery site. See *Notification of cluster status* on page 364.

When the production site is unable to process file transfers, failover to the disaster recovery site:

1. If possible, make sure that the disaster recovery site configuration and data is consistent with the production site.
2. On every SecureTransport Server and SecureTransport Edge in the production site, use the `<FILEDRIVEHOME>/bin/stop_all` (or, on Windows, `<FILEDRIVEHOME>\bin\stop_all.com`) command to stop all SecureTransport processes.
3. On every SecureTransport Server and SecureTransport Edge in the DR site, use the `<FILEDRIVEHOME>/bin/start_all` (or, on Windows, `<FILEDRIVEHOME>\bin\start_all.com`) command to start all SecureTransport processes.
4. Make any changes to your load balancers or other network infrastructure to direct your SecureTransport traffic to the disaster recovery site.

When the production site is able to process file transfers, failback:

1. If possible, make sure that any configuration changes made on the DR site are transferred to the production site and make sure that production data is consistent with the disaster recovery site.
2. On every SecureTransport Server and SecureTransport Edge in the production site, use the `<FILEDRIVEHOME>/bin/start_all` (or, on Windows, `<FILEDRIVEHOME>\bin\start_all.com`) command to start all SecureTransport processes.
3. On every SecureTransport Server and SecureTransport Edge in the DR site, use the `<FILEDRIVEHOME>/bin/stop_all` (or, on Windows, `<FILEDRIVEHOME>\bin\stop_all.com`) command to stop all SecureTransport processes.
4. Make any changes to your load balancers or other network infrastructure to direct your SecureTransport traffic to the production site.

Note The time needed to perform a switch to the DR site can be estimated by assessing the time consumed for each of the following stages: stop and start ST services, perform the manual steps and maintain the data integrity. However, the time needed to keep the data integral is

dependent on multiple factors, such as the chosen solution for database and filesystem synchronization, deployment specifics, connectivity, amount of data to transfer, distance between remote locations, etc.

Direct cluster workload

As described in *Workload distribution* on page 353, an event processor directs events that represent workload tasks to the SecureTransport Servers in the cluster. Using its default policies, the event processor directs all events associated with an account to the same set of servers. This policy improves the performance of the distributed object cache that SecureTransport uses to avoid database fetches for object references. If all tasks associated with an account are performed by the same set of servers, the object that represents that account and related objects are cached at that server. This improves performance because the cache manager does not need to fetch them from another server.

In addition to the default account-based event management, event processor policies can direct events to particular servers based on attributes of each event. By default, the event processor uses a round-robin policy to direct events to servers in the set that is processing events for the account, directing each event to the next server in sequence.

If a server in your cluster has performance characteristics or other resources required for certain tasks, you can direct events that represent those tasks that to those particular servers. By default the following task-type attributes are defined:

- **FM_TRIGGERED** – Caused by an action of a transfer site that uses the Folder Monitor protocol
- **MAINTENANCE** – Log applications: LogEntry Maintenance, Sentinel Link Data Maintenance, and Transfer Log Maintenance
- **PGP** – PGP encryption or decryption
- **PULL** – Server-initiated incoming transfer
- **PUSH** – Server-initiated outgoing transfer

For example, to improve performance of PGP encryption and decryption, you can include in your cluster a server with better computational performance, and direct all PGP task to that server.

The `EventQueue.DispatchPolicy.name` system configuration parameter controls the behavior of the event queue. Valid values are:

- `cacheBasedPolicy` (default) – Directs all events associated with an account to the same server to improve performance
- `attributeMatchPolicy` – Directs events based on specified attributes
- `roundRobinPolicy` – Causes the event queue to direct each event to the next server in sequence without regard to account or attributes

The `attributeMatchPolicy` is not used when a node in the cluster is overloaded. For more information, refer to the description of the `EventQueue.taskProcessor.threshold` parameter on the *Server Configuration* page.

In each case, either the policy identifies a set of servers or, if no servers match, the criteria, a set that includes the whole cluster. The event manager uses the round-robin method and select the next server from the set in sequence. Of course, round-robin distribution does not occur when only one server is selected by the policy.

You can configure a SecureTransport Server to process tasks of one or more types by editing a local configuration parameter.

1. Log on to the SecureTransport Server.
2. Select **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.
3. Search for the local parameter `EventQueue.taskProcessor.attributes`.

   The value is a comma-separated list of task types to direct to this server. The default value is `PGP=false, PUSH=false, PULL=false, FM_TRIGGERED=false, MAINTENANCE=false`.
4. Edit the value and change `false` to `true` for each event type to direct to this server.
5. Save the new value.
6. Search for the parameter `EventQueue.DispatchPolicy.name`, edit it, and change its value to `attributeMatchPolicy`.
7. Select **Operations > Server Control** and restart the TM Server.

The distributed Event Manager now prefers the Server for events of the selected types.

If you configure a SecureTransport Server to process PGP tasks, you must make other changes on every node of your cluster.

1. If your deployment uses NFS to provide the shared file system, you must export the file system with the `sync` and `no_wdelay` options.
2. Log on the SecureTransport Server computer.
3. If your deployment uses NFS to provide the shared file system, change the NFS mount to use the `-o noac,sync` options.
4. Make a backup copy and open the `<FILEDRIVEHOME>/brules/local/wptdocuments/Streaming.xml` file in a text editor.
5. Find the following text:

```
<!-- Uncomment the following if you want to enable the
     PGP Event type distribution -->
<!--
<operator name="or" />
   <expression>
      <item>
         <attribute>EventType</attribute>
```

```
         <comparator name="equal" />
         <value>Transformation</value>
      </item>
      <operator name="and" />
      <item>
         <attribute>DXAGENT_TRANSFORMATION_TYPE</attribute>
         <comparator name="equal" />
         <value>PGP</value>
      </item>
   </expression>
-->
```

6. Delete the following comment lines from that text:

   `<!--`

   and

   `-->`

7. Save the file.
8. Select **Operations > Server Control** and restart the TM Server.

Note When a SecureTransport Server is configured to process PGP tasks, Sentinel reporting for those transfers is not accurate because Sentinel cannot combine the processes of the transfer.

You can add task types (attributes) to `EventQueue.taskProcessor.attributes` by editing the `EventQueue.submissionConfigurator.additionalAttributes` server configuration parameter on any server in the cluster.

The items in this comma-separated list of attributes are the names of environment variables that you need to use to identify events. For example:

- `DXAGENT_APPLICATION_NAME` is used to identify events for all users who are subscribed to the named application.
- `DXAGENT_SITE_NAME` is used to identify events for all users who are subscribed to a transfer site with the given name.

Once you add task types to `EventQueue.submissionConfigurator.additionalAttributes`, you edit `EventQueue.taskProcessor.attributes` in the same way you do for the standard task types. The items you add have the form:

`<environment variable>=<value>`

where the environment variable is listed in `EventQueue.submissionConfigurator.additionalAttributes` and the value selects the events to direct to the server. For example:

- To define a task type for events for all users who are subscribed to an Site Mailbox application named `smbBU1`, the attribute is `DXAGENT_APPLICATION_NAME=smbBU1`.

- To define a task type for events for all users who have a transfer site named `FtpNode3Unit1`, the attribute is `DXAGENT_SITE_NAME=FtpNode3Unit1`.

SecureTransport Edge synchronization 6

You can deploy SecureTransport Edge servers so that configuration changes are dynamically synchronized from a primary SecureTransport Edge to the other (secondary) SecureTransport Edge servers. This synchronization works like configuration synchronization in a Standard Cluster (SC), but because SecureTransport Edge servers do not process events, they are not in a cluster.

You configure the secondary SecureTransport Edge servers on the primary SecureTransport Edge server. Most configuration changes are dynamically synchronized across the SecureTransport Edge servers immediately.

The following topics describe and provide how-to instructions to synchronize SecureTransport Edge servers:

- *Manual synchronization* on page 372
- *Requirements for synchronization* on page 373
- *What information is synchronized* on page 373
- *Set up SecureTransport Edge servers for synchronization* on page 374
- *Manually synchronize SecureTransport Edge servers* on page 375
- *Maintain synchronized SecureTransport Edge servers* on page 375

Manual synchronization

You can also propagate configuration information across a Standard Cluster (SC) by synchronizing the secondary servers from the primary server manually.

A full synchronization can take some time to complete, so perform it when your SecureTransport system is not under heavy load.

Perform manual synchronization after you:

- Upgrade SecureTransport Edge
- Restart all the SecureTransport Edge servers
- Restore a failed primary SecureTransport Edge server
- Add or update administrators or administrative roles, either using the Administration Tool or by importing account configuration
- Add or remove SecureTransport Edge servers
- Change the primary server

- Restart the Administration Tool server on a secondary SecureTransport Edge server, if you made changes using the Administration Tool on the primary server while it was down

Requirements for synchronization

Cluster synchronization requires the following:

- The `<FILEDRIVEHOME>/lib/admin/config/servers` configuration file is correct and identical on all SecureTransport Edge servers.
- The `<FILEDRIVEHOME>/var/tmp/sentinel_primary` file exists on the primary SecureTransport Edge only.
- A shared common secret file (named `taeh` file) is used on all servers.
- Each server is hosted on a different computer or VM.
- All servers use the same installation path.
- All the servers are on the same LAN.
    - The primary administrator user ID is the same on all servers and all have the same password.
- The clocks are set to the same time on all servers.
- The internal CAs on all servers is trusted by all other servers. Optionally, you can import the same internal CA on all servers.
- All database settings are identical on all the computers that will be synchronized.
- Only files used for server configuration are configured for synchronization.
- All the server certificates are issued by a common CA.

What information is synchronized

SecureTransport Edge synchronization moves configuration data from the primary SecureTransport Edge server to all the SecureTransport Edge secondary servers only. SecureTransport does not support moving data from secondary servers to the primary server or from the primary server to selected secondary servers.

The following information is synchronized dynamically from the primary SecureTransport Edge server to the secondary SecureTransport Edge servers when you change it on the primary server:

- All server configuration parameters that are not local to the server

The following information is also synchronized during manual synchronization:

- All configuration files listed in the `<FILEDRIVEHOME>/conf/sync.conf` file
- All database tables listed in the `<FILEDRIVEHOME>/conf/sync_tables.conf` file

The files listed in `<FILEDRIVEHOME>/conf/sync.excl` are not copied from the primary to the secondary server.

Set up SecureTransport Edge servers for synchronization

Use the following procedure to set up SecureTransport Edge servers for synchronization.

1. Install SecureTransport Edge on the system that will be the primary server.
2. Copy the `taeh` file from the `<FILEDRIVEHOME>/bin/` directory to all the other systems.
3. Using the `taeh` file, install SecureTransport Edge on the other systems.
4. Add licenses for all servers. For instructions, refer to the *SecureTransport Getting Started Guide*.
5. Generate an internal CA on each server. For instructions, refer to the *SecureTransport Getting Started Guide*.
6. Exchange CA certificates between all servers in a Standard Cluster (SC) or Enterprise Cluster (EC). For details, refer to the procedures for exporting and importing SecureTransport Server CA certificates in the *SecureTransport Getting Started Guide*.
7. On the primary and all secondary servers, list all the servers in the `<FILEDRIVEHOME>/lib/admin/config/servers` configuration file. List the primary server first and continue with the secondary servers.

   Edit the file and add a line of following form for each server in a cluster:

   `<host> https://<host>:<port>`

   where:

   - `<host>` is the FQDN or IP address of the system
   - `https://<host>:<port>` is the URL of the Administration Tool on that system
   - `<port>` is usually 444

   The two fields are separated by a tab character.

   The `<FILEDRIVEHOME>/lib/admin/config/servers` file must be the same on all computer in your cluster. You can create it on the primary server and copy it to the others.
8. On the primary server, create a file named `<FILEDRIVEHOME>/var/tmp/sentinel_primary`. This file is not used for integration with Axway Sentinel. It is required whether or not Sentinel is used.

   To create the file, you can use the `touch` command in UNIX or create an empty file with no file extension in Windows. The file must have 0 bytes.
9. Log out of the primary SecureTransport Edge server and log in again. Make sure that the server is identified as the primary server and that the **Synchronize All** and **Bounce All** buttons are displayed.
10. Synchronize the secondary servers manually from the Administration Tool of the primary server.
11. On the primary server, either import an external CA or generate a local CA. For instructions, refer to the *SecureTransport Getting Started Guide*. Dynamic synchronization copies the new CA to all servers in a cluster.

12. On the primary server, generate the server certificate required by your configuration and complete other configuration tasks.

Manually synchronize SecureTransport Edge servers

Use the Administration Tool to synchronize the SecureTransport Edge servers. This option is not displayed when the SecureTransport Edge server is not configured for synchronization.

Note The upper right corner of the Administration Tool shows whether the server on which it is running is a primary or secondary server.

1. Select **Operations > Cluster Management**.

   The *Cluster Management* page is displayed.

2. Click **Synchronize All**.

Note The Status column *Cluster Management* page contains N/A entries because the Transaction Manager does not run on the SecureTransport Edge .

Maintain synchronized SecureTransport Edge servers

As long as your synchronized SecureTransport Edge servers meet the requirements for synchronization, you can make changes to the group, such as:

- Change the primary server (manually failing over the primary server to another server or restoring a server to its role as primary server)
- Add a server
- Remove a server

The key requirement is that the `<FILEDRIVEHOME>/lib/admin/config/servers` configuration file is correct and identical on all servers and that only the primary server has a `<FILEDRIVEHOME>/var/tmp/sentinel_primary` file.

1. Stop all the SecureTransport Edge servers.
2. If you are adding or removing a secondary server, update the `<FILEDRIVEHOME>/lib/admin/config/servers` file on the primary server and copy the servers file to all the SecureTransport Edge server systems.
3. If you are changing the primary server, list it as the first line in the `<FILEDRIVEHOME>/lib/admin/config/servers` file on the primary server, copy the `servers` file to all the SecureTransport Edge server systems, delete the `<FILEDRIVEHOME>/var/tmp/sentinel_primary` file on the previous primary server, and create the `<FILEDRIVEHOME>/var/tmp/sentinel_primary` file on the new primary server.
4. Restart all the SecureTransport Edge servers.
5. Log in to the Administration Tool and manually synchronize the servers.

SiteMinder integration 7

SecureTransport can be integrated into a SiteMinder SSO environment and use SiteMinder to SSO authenticate and authorize resource access using only HTTP or HTTPS.

Note You cannot configure both SiteMinder integration and LDAP integration.

The following topics provide a SiteMinder integration overview and how-to instructions for managing the SiteMinder integration:

- *SiteMinder overview* on page 377 .
- *User authentication* on page 378 .
- *Configure SiteMinder for SecureTransport integration* on page 381
- *Configure SiteMinder settings in SecureTransport* on page 381 .
- *Disable the SecureTransport login* on page 381
- *Configure client certificate authentication settings* on page 382
- *Integration troubleshooting* on page 383

SiteMinder overview

Netegrity SiteMinder is a third-party application that controls user access to secured applications and provides a Single Sign-On (SSO) portal. A Single Sign-On portal is a Web gateway or proxy that enables users to access multiple secured Web applications using a single user name and password that are provided once only at the start of the user session.

SecureTransport can be integrated into a SiteMinder SSO environment. When integrated, users can authenticate for HTTP and HTTPS using SiteMinder SSO. They can authenticate for other protocols though SiteMinder using user name and password, but not using SSO.

The following illustration shows how SecureTransport can be integrated into a typical SiteMinder environment.

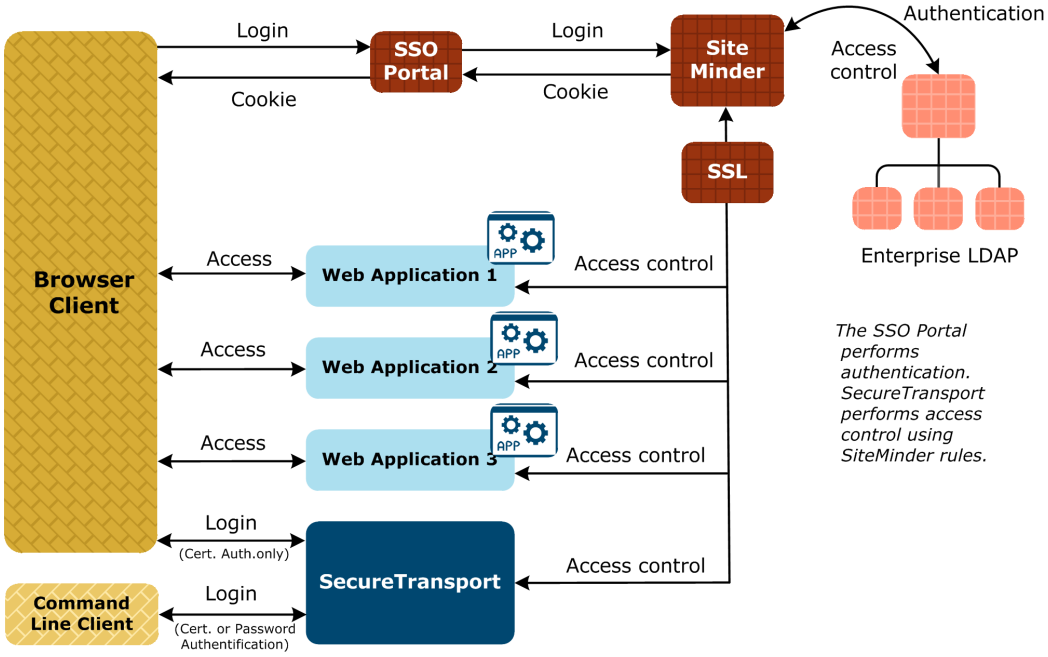


Figure 8. Integration of SecureTransport into a SiteMinder deployment

Typically, in a SiteMinder SSO environment, users log onto the SSO portal using a Browser Client. The SSO portal directly handles all user authentication and access control for the secured Web applications in the SiteMinder network. However, because SecureTransport supports command line clients, it requires more control over authentication and authorization than a typical Web application. The following topic describes how SecureTransport user authentication and authorization is handled in a SiteMinder environment.

User authentication

In a SiteMinder environment, a user can access SecureTransport resources using a web client or a command line client. If the SecureTransport SiteMinder module is enabled, SecureTransport uses different authentication methods depending on the type of client.

Note All SiteMinder users are represented in SecureTransport by default as virtual users, unless no other specific user class is created for them from **Access > User Classes**.

The following topics describe SiteMinder authentication:

- *Web client (HTTP and HTTPS) user authentication* on page 379 - Describes SiteMinder web client user authentication.
- *Command line client (FTP, FTPS, HTTPS, and SSH) user authentication* on page 379 - Describes SiteMinder command line client user authentication.
- *User access control (authorization)* on page 379 - Describes user access control authorization and authentication.

Web client (HTTP and HTTPS) user authentication

Web clients can log in to SecureTransport directly or through the SiteMinder Single Sign-On (SSO) portal. Depending on the SiteMinder configuration, when a web client logs in, SecureTransport can require a client certificate, which it presents to SiteMinder for authentication.

When a web client logs on through the SiteMinder SSO portal, the portal authenticates the user and provides the client with a SiteMinder session cookie. When the client tries to access a SecureTransport resource, SecureTransport presents the user's session cookie to SiteMinder for authentication.

Note Session cookies are by domain, so the SiteMinder SSO portal must be in the same domain as the SecureTransport Server.

Note The SiteMinder SSO portal must be accessed using a fully-qualified domain name (FQDN) because SiteMinder uses domain cookies, and it is possible that different browsers can handle the conversion from partial name to FQDN incorrectly. In the latter case, access to the SSO portal can be denied.

Command line client (FTP, FTPS, HTTPS, and SSH) user authentication

Command line clients log on to SecureTransport directly, not through the SSO portal. If the client presents a user name and password or a certificate, SecureTransport first tries to authenticate the user by comparing it to the user profiles defined in SecureTransport. In case SecureTransport cannot authenticate the user, it passes the user name and password to SiteMinder for authentication. If all authentication attempts fail, the user receives an error message and is disconnected.

Note The SecureTransport command line client does not work through a Web gateway or proxy (even when using HTTPS). So, SecureTransport Server must be made directly accessible to command line clients.

User access control (authorization)

Regardless of the type of client, access control is always performed by SecureTransport, which uses SiteMinder rules to obtain the user's read/write authority to a particular resource. The SSO portal cannot perform access control for SecureTransport resources.

After a user is authenticated, SecureTransport sends an authorization request to SiteMinder to determine whether the user has read/write access to the requested resource. If SiteMinder grants the appropriate access level, SecureTransport proceeds with the file operation.

Note The SiteMinder SSO portal must be accessed using FQDN because SiteMinder uses domain cookies and it is possible that different browsers can handle the conversion from partial name to FQDN in an incorrect manner. In the latter case, access to the SSO portal can be denied.

The following topics describe the SiteMinder authorization rules and provide an authorization request example:

- *SiteMinder authorization rules* on page 380
- *Example authorization request* on page 380

SiteMinder authorization rules

Configure the SiteMinder authorization rules to accommodate SecureTransport authorization requests. A SecureTransport authorization request contains the following elements:

- **Resource Path** – The absolute URI of the resource being accessed by the user. SecureTransport determines the actual file path and uses that file path as the URI. This URI can be modified (section removed or prefix added) based on the **File Storage Root Path** and **SiteMinder Path Prefix** in the SecureTransport SiteMinder settings. (For details, see *Configure SiteMinder settings in SecureTransport* on page 381.) For Windows systems, backslashes (\) in the file path are replaced with forward slashes (/) before the file path is modified as described above.
- **Command** – Either `GET` or `PUT` depending on whether the user is requesting a read or write operation.

Example authorization request

The following example shows how SecureTransport would construct an authorization request to SiteMinder.

Assume a user requests a listing for the following resource:

```
/mnt/data/SecureTransport/MyDirectory
```

If the **File Storage Root Path** (in the SecureTransport SiteMinder settings) is configured as:

```
/mnt/data/SecureTransport
```

and the **SiteMinder Path Prefix** (in the SecureTransport SiteMinder settings) is configured as:

```
/ST
```

the authorization request for this file operation would be:

```
GET /ST/MyDirectory/
```

In this example, SiteMinder authorization rule would be configured to allow or deny the `GET` command to access the `/ST/MyDirectory/` resource. When SiteMinder is enabled, all SecureTransport users must have `GET` access to the path specified in the **SiteMinder Path Prefix** to successfully log in. If the **SiteMinder Path Prefix** setting is left blank, then users must have `GET` access to the / directory. The SiteMinder Policy Server must be set accordingly.

Configure SiteMinder for SecureTransport integration

To successfully integrate SecureTransport with SiteMinder, SiteMinder must be configured appropriately using the SiteMinder administration system. This topic provides general guidelines for configuring SiteMinder 4.X and 5.X. For more information, refer to the SiteMinder documentation.

1. Create a SiteMinder agent that SecureTransport is to use to connect to the SiteMinder Policy Server.

   When creating the agent, either select the **4.X** compatibility option and fill in the **IP address** of the SecureTransport Server (not the SiteMinder Policy server) and **Shared secret** or select the **5.X** compatibility option and fill in the name of the agent only.
2. Create an authentication scheme by selecting one of the following types:
   - **Basic Template** – password authentication
   - **X509 Client Cert Template** – certificate authentication
   - **X509 Client Cert or Basic Template** – certificate *or* password authentication
   - **X509 Client Cert and Basic Template** – certificate *and* password authentication
3. Create a Realm, selecting the agent and authentication scheme that have been created for SecureTransport.
4. Create new rules under the Realm.
5. Create a Response that returns the attributes required by the SecureTransport SiteMinder settings. For details, see *SiteMinder integration configuration* on page 420.
6. Apply the new rules to the necessary SiteMinder Policy.

Configure SiteMinder settings in SecureTransport

Before using SecureTransport with SiteMinder, the you must configure the SiteMinder settings on the SecureTransport Server using the Administration Tool. For details, see *SiteMinder integration configuration* on page 420.

Disable the SecureTransport login

Web clients that have logged on through the SiteMinder SSO portal should not log on again to the SecureTransport login page. Therefore, it is necessary to disable the SecureTransport login page for these clients.

1. Select **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.

2. Search for the `Http.FdxAuthReply` parameter, and change its value to `PREAUTH`.

   Note When `PREAUTH` is set for `Http.FdxAuthReply`, SecureTransport uses `*nobody` as an internal constant value indicating that no user is authenticated with internal agents. If a user with the name **nobody* already exists on the operating system, this may cause a conflict that prevents that user from logging in.

3. Restart the HTTP server and the TM Server.

Configure client certificate authentication settings

Instead of logging on through the SSO portal, web clients and command line clients can log on to SecureTransport directly and request authentication using a client certificate. SecureTransport then presents the client certificate to SiteMinder for authentication. To configure SecureTransport to perform client certificate authentication using SiteMinder, complete these steps:

1. Import into SecureTransport the trusted Certificate Authority (CA) certificates for the client certificates to be authenticated. Client certificates are authenticated using indirect trust.
2. Restart the SSH Server.
3. Bounce the SecureTransport Servers.

The following topics describe importing trusted CA certificates and updating the Secure Socket Layer settings:

- *Import trusted CA certificates* on page 382
- *Update the Secure Socket Layer settings* on page 382

Import trusted CA certificates

Import the trusted CA certificates into SecureTransport that are needed for indirect trust of client certificates. For information about importing trusted CA certificates, see *Import a trusted CA certificate* on page 62.

Update the Secure Socket Layer settings

If SecureTransport Edge is deployed in a peripheral network (DMZ) configuration, change these settings on both the SecureTransport Edge and SecureTransport Server.

1. Select **Authentication > Login Settings (End-user login options) > Certificate**.

   The *Login Settings* page is displayed.

2. Select **Certificate**.

3. In the *Client Certificate Settings* pane, make the following changes:
    - Set **HTTPS** to **Optional** or **Required**.
    - Set **FTPS** to **Optional** or **Required**.
    - Set **SSH** to **Optional** or **Required**.
4. Select **Operations > Server Control**.
5. Restart the TM Server.

The new settings do not take effect until the Transaction Manager server is restarted.

Note After you modify SSH client certificate authentication options, restart the SSH server.

Integration troubleshooting

Use the recommendations in this topic to troubleshoot problems that you might encountered when integrating SecureTransport with SiteMinder.

The following topics describe the SiteMinder and SecureTransport troubleshooting tools:

- *SiteMinder troubleshooting tools* on page 383
- *SecureTransport troubleshooting tools* on page 383

SiteMinder troubleshooting tools

One of the first things to determine is if a problem is in the SiteMinder configuration settings. The following SiteMinder tools are helpful in troubleshooting the SiteMinder configuration:

- **SiteMinder Test Tool** – helpful in testing agent, rule, and policy configurations in SiteMinder.
- **SiteMinder Debug Log files** – helpful in troubleshooting SiteMinder Policy Server configuration issues. These debug log files are configured using the Netegrity Policy Server Management Console.

Refer to the SiteMinder documentation for information about these tools.

SecureTransport troubleshooting tools

If problems still exist after troubleshooting with the SiteMinder tools, use the SecureTransport log files to try to ascertain the problem.

To use the SecureTransport log files effectively to troubleshoot the SiteMinder integration issues, consider the following recommendations:

- Increase the log level of `com.tumbleweed.st.server.siteminder` log generator in `<FILEDRIVEHOME>/conf/tm-log4j.xml` to `debug`. Increase the log levels of other log generators in this file as well.

- Increase all the log levels in <FILEDRIVEHOME>/conf/tm-log4j.xml from warn to debug.
- Check the <FILEDRIVEHOME>/var/logs/tm.log file and the *Server Log* page for any messages when a SiteMinder login fails.

After increasing the logging level settings, restart Transaction Manager to apply the changes.

Restart Transaction Manager

Use the following procedure to restart the Transaction Manager.

1. Select **Operations > Server Control**.

   The *Server Control* page is displayed.
2. Under **TM Server**, click **Stop** and then click **Start**.

Authentication 8

The following set of topics provides detailed SecureTransport login setting configuration and authentication information for end-users and administrators and LDAP and SiteMinder configuration information:

- *Single Sign-On (SSO) and Single Logout (SLO)* on page 386 - Describes the SecureTransport Single Sign-On and Single Logout functionality.
- *Single Sign-On (SSO) configuration* on page 387 - Provides configuration prerequisites, an overview of the main configuration files, and describes configuring SSO.
- *Enable Single Sign-On (SSO) for administrators* on page 393 - Describes how to enable SSO for administrators.
- *Enable Single Sign-On (SSO) for end-users* on page 395 - Describes how to enable SSO for end-users.
- *Multiple Identity Provider configuration* on page 398 - Describes configuring multiple Identity Providers.
- *Configure Single Sign-On (SSO) for streaming* on page 401 - Describes configuring SSO for streaming.
- *Configure Single Sign-On (SSO) for clusters* on page 402 - Describes configuring SSO for clusters.
- *SecureTransport as an Identity Provider* on page 402 - Describes using SecureTransport as an Identity Provider.
- *Single Sign-On SSO authentication flows* on page 403 - Describes the SSO and SLO authentication flows.
- *Configure Kerberos as an Identity Provider in SecureTransport* on page 404 - Describes Kerberos SSO authentication with Active Directory.
- *Login settings* on page 412 - Provides configuration information and instructions for enabling or disabling SSO authentication of end users and administrators, enabling or disabling certificate authentication and client certificate authentication for end users and administrators, enable or disable dual authentication, and set LDAP and SiteMinder authentication levels.
- *SiteMinder integration configuration* on page 420 - Provides how-to instructions for configuring the SiteMinder integration.
- *LDAP integration* on page 426 - Describes the SecureTransport LDAP integration.
- *LDAP connections, binds, and searches* on page 427 - Describes the configuration of LDAP connections, binds, and searches.
- *LDAP logins* on page 427 - Describes how LDAP logins are used and searched when LDAP is enabled.
- *LDAP domains* on page 429 - Describes the management and configuration of LDAP domains.

- *LDAP home folders* on page 448 - Describes LDAP homes folders and provides LDAP home folder configuration instructions.
- *LDAP user type ranges* on page 450 - Describes the configuration of LDAP user type ranges on UNIX systems.

Single Sign-On (SSO) and Single Logout (SLO)

Single Sign-On (SSO) is a user authentication process that authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session. Essentially, it removes the need for your users to log into multiple applications in a particular browser session. Once they log into one system, it exchanges authentication data with another service you have SSO set up with and automatically logs the user in.

SecureTransport supports signed authentication response assertions and this is transparent to SecureTransport as long as correct configuration is supplied. A signed response proves it is sent from an intended Identity Provider. Adding an extra security layer by disabling plain SAML connections is highly recommended, and it ensures confidentiality. SAML profiles are configured by means of SAML bindings.

The Single Logout (SLO) profile enables a user to log out of all participating sites in a created session nearly simultaneously. The user may log out globally from any site, whether Service Provider (SP) or Identity Provider (IdP), as determined by respective Web applications. The associated IdP deployment handles all logout requests and responses for participating sites.

SecureTransport implements:

- Single Sign-On (SSO)
- Single Logout (SLO)

Supported protocols:

- SAML 2.0 for Administrators and End-users
- Kerberos 5 for End-users

Note SSO authentication using SAML 2.0 and Kerberos is only applicable for the HTTP protocol.

Note When SecureTransport is behind a reverse proxy/load balancer, the HOST header needs to be modified to match the hostname of the proxy, not the host where the request is proxied to. For Apache this is achieved by setting the `ProxyPreserveHost` property to **On**. For additional information, refer to https://httpd.apache.org/docs/2.4/mod/mod_proxy.html#proxypreservehost.

It also supports user attribute mapping and authentication decisions on attribute maps.

The SSO authentication process is owned and managed by an Identity Provider (IdP). The IdP provides a token authentication object consisting of a user name and a map of attributes. The SecureTransport filters and re-maps the attributes and prepares them to be consumed by SecureTransport.

Single Sign-On (SSO) configuration

Note SecureTransport supports both Keycloak and Shibboleth for end-users and for administrators.

Prior configuring SecureTransport to use SSO the following steps should be completed:

- Install and configure your selected Identity Provider:
  - For Keycloak - Refer to the Keycloak documentation for getting started and installation and configuration instructions.

    Note SecureTransport 5.4 is certified with Keycloak 2.5.0.
  - For Shibboleth - Refer to the Shibboleth documentation for installation and configuration instructions.

    Note SecureTransport 5.4 is certified with Shibboleth 3.3.0.
- Install and configure Kerberos. Refer to the Kerberos documentation for installation and configuration instructions. Also, refer to the Kerberos protocol tutorial .

Note In a SecureTransport deployment, consisting of both backend and edge nodes, SSO must be configured and enabled on all nodes even if users are only logging in through the edge. On the edge, you must enable SSO for end-users.

SecureTransport Single Sign-On (SSO) configuration prerequisites

1. Navigate to **Operations > Server Configuration**. Click on **Configuration Files**.
2. To download the SSO Configuration Files click on **SSO Configuration Files**. You will be prompted to save the `SSO-configuration-export.zip` file on your file system.
3. Unzip the `SSO-configuration-export.zip` file.

The default SSO configuration files are:

- `sso-admin.xml` – Configure the SSO for administrator component. For a sample of a `sso-admin.xml` file, refer *Sample SSO configuration file for administrators* on page 1050.
- `sso-enduser.xml` – Configure the SSO for end-user component. For a sample of a `sso-enduser.xml` file, refer to *Sample SSO configuration file for end-users* on page 1057.
- `keycloak-idp-metadata.xml` – A Keycloak Identity provider metadata file. This file is generated from Keycloak. For more information regarding how to download this file, refer to the Keycloak documentation.
- `shibboleth-idp-metadata.xml` – A Shibboleth Identity provider metadata file. This file is generated from Shibboleth. For more information regarding how to download this file, refer to the Shibboleth documentation.

- `krb5-login.conf` – A Kerberos configuration file.
- `sample-kerberos.keytab` – A Kerberos `.keytab` file.

Single Sign-On (SSO) configuration files overview

The main SSO configuration files (`sso-admin.xml` for administrators and `sso-enduser.xml` for end-users) are considered mandatory for configuring the SSO functionality in SecureTransport for the respective components.

For the sample SSO configuration files, refer to *Sample SSO configuration file for administrators* on page 1050 and *Sample SSO configuration file for end-users* on page 1057.

The main SSO configuration file contains the following elements:

- `<SSOConfiguration>` element – This is the root element of the configuration descriptor. This section contains one `<CertificateValidation>` element (optional), one `<ServiceProvider>` element (required) and one `<IdentityProviders>` element (required).

  Note You can specify only one `<ServiceProvider>` element.

- `<CertificateValidation>` element – Describes the certificate validation. Configures certificate validation. Validates the Service Provider and Identity Providers certificates specified in its configuration. Validation happens at start-up and at regular intervals. This element is optional. Possible attributes for this element:
  - `trustStoreInitializer` – Set `com.axway.st.server.sso.impl.TrustStoreInitializer` value for `trustStoreInitializer` in order to use SecureTransport trust store.
  - `delayBetweenValidations` – Defines at which interval certificates validation occurs, in hours. Default value is 3 hours.
- `<ServiceProvider>` element – Configures the Service Provider. This element is required. Main attributes for this element:
  - `entityId` – Sets the unique identifier of the Service Provider. This identifier is sent to the Identity Provider so it can know who is requesting an authentication or a logout. This identifier is used by the Identity Provider to differentiate what Service Provider is requesting an authentication or a logout.
  - `filteredUri` – Specifies the URI of the authentication process entry point. The value must be `/*` for both administrators and end-users.
  - `logoutUri` – Specifies the URI which triggers logout process. The value must be `/logout` for both administrators and end-users.

- `logoutRedirectUri` – Specifies the URI to redirect to the initial logout message generated. In turn that message will be redirected to an Identity Provider. The value must be:
  - For end-users the required value is `/logoutRedirect`.
  - For administrators the required value is `/coreadmin`.
- `keystoreInitializer` – Configures key store to use. That key store keeps key-pairs taking part in authentication process. Set `com.axway.st.server.sso.impl.KeyStoreInitializer` as value in order to use the SecureTransport local key store.
- `keyAlias` – Specifies key alias of the private key used to decrypt SAML messages and assertions and to sign SAML messages and assertions.
- `sessionIdCookieName` – Sets the name of the cookie to store the SSO session identifier if sessions are managed by the SSO module.

- `<AssertionConsumerService>` element – Specifies an entry point for receiving SAML Assertions from the Identity Provider.
- `<SingleLogoutService>` element - Specifies the Identity Provider URL where the logout responses are sent.

  Note The recommended values for both `<AssertionConsumerService>` and `<SingleLogoutService>` are listed in *Sample SSO configuration file for administrators* on page 1050 and *Sample SSO configuration file for end-users* on page 1057.

- `<Features>` element - The SSO agent can be fine-tuned by using an extra configuration features. In most cases, the values of these features don't have to be modified. The recommended features are:
  - `<Feature key="secure-cookie" value="true" />` - Configures the session cookie whether to be set with Secure flag. Recommended value is true.
  - `<Feature key="uid-generator" value="com.axway.st.server.sso.impl.UIDGenerator" />` - Type of unique identifier generator to use to assign ids to SAML messages. The value must be `com.axway.st.server.sso.impl.UIDGenerator`.
    - `<IdentityProviderResolution>` - For more information, refer to *Multiple Identity Provider configuration* on page 398.
    - `<TenantResolution>` - For more information, refer to *Multiple Identity Provider configuration* on page 398.
- `<IdentityProviders>` element - Identity provider definitions. Configures various aspects of interaction with Identity Providers. This element is required. The main attributes for this element are:
  - `entityId` – Sets the unique identifier of the Service Provider. This identifier is sent to the Identity Provider so it can know who is requesting an authentication or a logout. For SAML-based Identity provider add here `<EntityDescriptor>` element `entityID`

attribute value, from the Identity provider metadata file.

- `metadataUrl` – Specify the relative location of the Identity provider metadata file. Use only for SAML-based Identity provider.
- `configurationUrl` – Specify the configuration file absolute path. Use only for Kerberos-based Identity provider.
- `verifyAssertionExpiration` - Turn on/off verification of the validity period of assertions. Consider to set to false if Service Provider and Identity Provider times are not synchronized. Default value is true.
- `sign` - If set to true, all SAML messages and their assertions sent by the Service Provider will be signed. There are a couple of features (see below) for fine-grained control of signing. Optional - if not present, default value is false.
- `userNameAttribute` - Sets the name of the Identity Provider attribute that provides the user name.

- `<Mappings>` element:
  - `<FilterMapping>` - This mapping creates output attributes when a filter matches the input attributes from the Identity Provider. For more information about the Filter Mapping syntax, refer to *SSO filter mapping* on page 1048.
  - `<RenameMapping>` - With this mapping, you can rename an attribute from the Identity Provider, keeping its value. For more information, refer to *Accessing Single Sign-On (SSO) attributes* on page 391.
- `<Features>` element - Features control specific behavior of SAML message processing. The recommended features are:
  - `<Feature key="saml-allow-http-connection" value="false"/>` - Allows interaction with the IdP by plain HTTP. Default value is false.
  - `<Feature key="saml-allow-unsigned-assertion" value="false"/>` - Allows unsigned assertions in messages received from the Identity Provider. Default value is false.
  - `<Feature key="saml-verify-metadata-signature" value="false"/>` - Enable or disable the signature verification of the metadata file and the certification path of the certificate used to sign. Set to false if metadata file is not signed. Default value is true.
  - `<Feature key="saml-sign-authnrequest" value="true"/>` - Enable or disable signing of Authentication Request messages. Presence of this feature and its value overrides the meaning of the sign attribute of `IdentityProvider` element.
  - `<Feature key="saml-sign-logoutrequest" value="true"/>` - Enable or disable signing of Logout Request messages. Presence of this feature and its value overrides the meaning of the sign attribute of `IdentityProvider` element.
  - `<Feature key="saml-sign-logoutresponse" value="true"/>` - Enable or disable signing of Logout Response messages. Presence of this feature and its value overrides the meaning of sign attribute of `IdentityProvider` element above.

- `<Feature key="saml-allow-unsigned-assertion" value="false"/>` - Allows unsigned assertions in messages received from the Identity Provider. Default value is false.
- `<Feature key="saml-response-binding" value="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>` - Sets the default response binding value to be `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`.

Note SecureTransport supports signature and decryption of SAML requests. Adding an extra security layer is highly recommended. Enable SSL by setting `<Feature key="saml-allow-http-connection" value="false"/>` in the `sso-admin.xml` and `sso-enduser.xml` SSO configuration files.

Accessing Single Sign-On (SSO) attributes

When your SSO login is successful, your Identity Provider will forward a set of user attributes to the requested Service Provider (SecureTransport). The SSO attributes are used by SecureTransport to configure user account instances, agent sessions, and advanced routing attributes.

Note Accessing Single Sign-On (SSO) attributes is not possible when using SSO with Kerberos authentication protocol. It is possible only with SAML.

There are several system attributes that are considered important for SecureTransport and there are custom mappings for the attributes:

Attribute name (Identity Provider)	Attribute name in SecureTransport*
email	fdxEmail
uid	fdxUid
gid	fdxGid
homeDir	fdxHomeDir

*The expected SecureTransport attribute name in order for the attribute to be mapped correctly.

For more information about the SSO attributes, refer to *SSO filter mapping* on page 1048.

Access the system attributes

1. Access the SSO system attributes in an Advanced Routing environment:

Attribute name	Expression syntax
email	${sso.email}
uid	${sso.uid}
gid	${sso.gid}
homeDir	${sso.homeDir}
tenant	${sso.tenant}
idpId	${sso.idpId}
userName	${sso.userName}

2. Access the SSO system attributes from a Session:

Attribute name	Expression syntax
email	${sess.STSESSION_SSO.email}
uid	${sess.STSESSION_SSO.uid}
gid	${sess.STSESSION_SSO.gid}
homeDir	${sess.STSESSION_SSO.homeDir}
tenant	${sess.STSESSION_SSO.tenant}
idpId	${sess.STSESSION_SSO.idpId}
userName	${sess.STSESSION_SSO.userName}

3. Access the custom SSO attributes. If we have a custom attribute with name `customAttribute`, you can access the first value in the following manner:
   a. From a Session:

      ```
      ${sess.STSESSION_SSO.customAttribute[0]}
      ```

   b. From an Advanced Routing environment:

      ```
      ${sso.attributes['customAttribute'][0]}
      ```

Enable Single Sign-On (SSO) for administrators

The following steps are the general configuration steps to enable SSO functionality for administrators in SecureTransport.

1. Navigate to **Authentication > Login Settings**.
2. In *Administrator login options* pane, select **Required** for *SSO*.
3. Click **Save**.

Configure Single Sign-On (SSO) for administrators

Before configuring SSO for administrators, refer to *SecureTransport Single Sign-On (SSO) configuration prerequisites* on page 387.

In order to configure SSO functionality for administrators, you need to update the `sso-admin.xml` file and remember that SSO authenticated administrators are only mapped to existing SecureTransport administrator accounts. For additional information, refer to *Add an administrator account* on page 647.

Note Do not rename the `sso-admin.xml` configuration file.

SecureTransport is certified with Shibboleth and Keycloak as supported SAML-based Identity providers for administrators.

Note SecureTransport only supports SAML-based Identity providers for SSO for administrators.

Note The following configuration steps describe the setup of a single Identity provider. For multiple Identity Provider configuration, refer to *Multiple Identity Provider configuration* on page 398.

Note Before configuring SSO for Administrators using a SAML-based Identity Provider, make sure that you configured it properly.

Configure SSO for administrators using SAML-based Identity Providers:

1. Download the SAML-based Identity Provider metadata file from your Identity Provider instance.

   Note Do not modify the SAML-based Identity Provider metadata file.

2. Open the `sso-admin.xml` file. The following changes are required:
   - In the `SamlIdentityProvider` element, change the following attribute values:
     - `metadataUrl` to be `./(name of the SAML-based Identity provider metadata file)`
     - `entityId` - add the `<EntityDescriptor>` element `entityID` attribute value, from the SAML-based Identity Provider metadata file.

- `Mappings` element: Both `<FilterMapping>` and `<RenameMapping>` elements are not applicable for administrators.
- `Features` element: The recommended features are listed in *Sample SSO configuration file for administrators* on page 1050.

3. Save the `sso-admin.xml` file.
4. Zip the `sso-admin.xml` file and the SAML-based Identity Provider metadata file from Step 1.

   Note Do not put the configuration files in a sub-directory inside the ZIP file.

5. Navigate to **Operations > Server Configuration**. Click on **Configuration Files**.
6. Select the **Browse** button for SSO Configuration Files. Choose the ZIP file containing the `sso-admin.xml` file and the SAML-based Identity Provider metadata file.
7. Click on the check box for **SSO Configuration Files**.
8. Click **Upload**.
9. Restart the admin service.

Note If, for some reasons after importing SSO configuration files and enabling SSO for administrators, you are still redirected to the default Administrator login page, perhaps there is some misconfiguration. To resolve this situation you can use SecureTransport as an Identity provider to login with the local stored credentials and troubleshoot. For more information, refer to *SecureTransport as an Identity Provider* on page 402.

Note In both Standard Clusters and Enterprise Clusters, after successfully importing the SSO configuration files, they will be automatically redistributed across all nodes in the cluster. Restart of admin service is required on all nodes.

Note In cluster environment SecureTransport will always redirect to the node that is configured in the Service Provider, even if the request came from a different node.

Note Due to the limitation of having only one Service Provider entity ID for the `sso-admin.xml` configuration file and the fact that configuration files are synced between the cluster nodes, all administrators will have the same service provider configuration. Since the IdP cannot differentiate which request is coming from which node, it will always return the user to the assertion consumer service configured on the IdP. This could be worked around by having a separate IdP for each cluster node and the user could select the node they want to login to by choosing the dedicated IdP. For more information about how to configure multiple Identity Provider in SecureTransport, refer to *Multiple Identity Provider configuration* on page 398.

Single Sign-On (SSO) administrators configuration

For more information about how to setup the SecureTransport administrators to use SSO, refer to *Manage administrator accounts* on page 644.

Enable Single Sign-On (SSO) for end-users

The following steps are the general configuration steps to enable SSO functionality for end-users in SecureTransport.

1. Navigate to **Authentication > Login Settings**.
2. In *End-users login options* pane, select **Required** for *SSO*.
3. Click **Save**.

Note When SSO for end-users is enabled, the following configuration options will be updated automatically:

1. `Http.FdxAuthReply` with value **PREAUTH**.
2. `Http.AllowedAuthenticationParameters` with value **SAMLResponse;RelayState**.
3. `AllowedAuthenticationParametersMaxSize` with value **32768**.

Configure Single Sign-On (SSO) for end-users

Before configuring SSO for end-users, refer to *SecureTransport Single Sign-On (SSO) configuration prerequisites* on page 387.

In order to configure SSO functionality for end-users, you need to update the `sso-enduser.xml` file and remember that SSO authenticated users are only mapped to existing SecureTransport user accounts or account templates with user classes. For additional information, refer to *Create a user account* on page 456, *Account templates* on page 661, and *User classes* on page 710.

Note Do not rename the `sso-enduser.xml` configuration file.

SecureTransport certifies Shibboleth, Keycloak as supported SAML-based Identity provider for end-users as well as Kerberos.

Note The following configuration steps describe the setup of the single Identity provider. For multiple Identity Provider configuration, refer to *Multiple Identity Provider configuration* on page 398.

Note Before configuring SSO for end-users using SAML-based Identity Provider or Kerberos, make sure that you configured them properly.

Configure SSO for End-users using SAML-based Identity provider:

1. Download the SAML-based Identity provider metadata file from your Identity Provider instance.

   Note Do not modify the SAML-based Identity Provider metadata file.

2. Open the `sso-enduser.xml` file. The following changes are required:
    - In the `<SamlIdentityProvider>` element, change the following attribute values:
        - `metadataUrl` to be `./(name of the SAML-based Identity provider metadata file)`
        - `entityId` - add the `<EntityDescriptor>` element `entityID` attribute value, from the SAML-based Identity Provider metadata file.
    - `<Mappings>` element:
        - `FilterMapping` - For information on filter mapping, refer to the *SSO filter mapping* on page 1048.
        - `RenameMapping` – For mapping custom attributes from an Identity Provider, refer to *Accessing Single Sign-On (SSO) attributes* on page 391.
    - `<Features>` element: The recommended features are listed in *Sample SSO configuration file for end-users* on page 1057.
3. Save the `sso-enduser.xml` file.
4. Zip the `sso-enduser.xml` and the SAML-based Identity Provider metadata file from Step 1.

    Note Do not put the configuration files in a sub-directory inside the ZIP file.
5. Navigate to **Operations > Server Configuration**. Click on **Configuration Files**.
6. Select the **Browse** button for SSO Configuration Files. Choose the ZIP file containing the `sso-enduser.xml` file and the SAML-based Identity Provider metadata file.
7. Click on the check box for **SSO Configuration Files**.
8. Click **Upload**.
9. Restart the Transaction Manager service and the HTTP service.

Configure SSO for end-users using Kerberos:

1. Configure Kerberos as an Identity provider. For the configuration with Kerberos as an Identity Provider, refer to *Configure Kerberos as an Identity Provider in SecureTransport* on page 404.
2. Open the `sso-enduser.xml` file. The following changes are required:
3. In `KerberosdentityProvider` element change the following attribute values:
    - `configurationUrl` to be the absolute path to the Kerberos `.conf` file.

        Note The Kerberos `.conf` file and `.keytab` file should be added to the SSO configuration ZIP file.
    - `entityId` - add the `entityID` attribute value
    - `<Mappings>` element:
        - `FilterMapping` – For information on filter mapping, refer to the *SSO filter mapping* on page 1048.
        - `RenameMapping` – For mapping custom attributes from an Identity Provider, refer to *Accessing Single Sign-On (SSO) attributes* on page 391.

- `<Features>` element: The recommended features are listed in *Sample SSO configuration file for end-users* on page 1057.

4. Save the `sso-enduser.xml` file.
5. Zip the `sso-enduser.xml` and all additional files (the Kerberos configuration file and the `.keytab` file).

   Note Do not put the configuration files in a sub-directory inside the ZIP file.

6. Navigate to **Operations > Server Configuration**. Click on **Configuration Files**.
7. Select the **Browse** button for SSO Configuration Files. Choose the ZIP file containing the `sso-enduser.xml` and the Keycloak/Shibboleth metadata file.
8. Click on the check box for **SSO Configuration Files**.
9. Click **Upload**.
10. Restart the Transaction Manager service and the HTTP service.

Note If, for some reasons after importing SSO configuration files and enable SSO for end-users you still redirect to default SecureTransport end-users login page, perhaps there is some misconfiguration. To resolve this situation you can use SecureTransport as an Identity provider to login with the local stored credentials and troubleshoot. For more information, refer to *SecureTransport as an Identity Provider* on page 402.

Note In both Standard Cluster and Enterprise Cluster, after successfully importing the SSO Configuration files, they will be automatically redistributed across all nodes in the cluster. Restart operation is required of Transaction Manager service on all nodes.

Note SSO for end-users can be configured using only `sso-enduser.xml` file only for backend instance.

Note Due to the limitation of having only one Service Provider entity ID for the `sso-enduser.xml` configuration file and the fact that configuration files are synced between the cluster nodes, all end-users will have the same service provider configuration. Since the IdP cannot differentiate which request is coming from which node, it will always return the user to the assertion consumer service configured on the IdP. This could be worked around by having a separate IdP for each cluster node and the user could select the node they want to login to by choosing the dedicated IdP. For more information about how to configure multiple Identity Provider in SecureTransport, refer to *Multiple Identity Provider configuration* on page 398.

Single Sign-On (SSO) account configuration

For more information about how to configure SecureTransport accounts with SSO, refer to *Manage accounts* on page 452 and *Advanced account administration* on page 631.

Multiple Identity Provider configuration

SecureTransport supports the multiple Identity Provider configuration. First, you should configure every Identity Provider. Then, for every Identity provider follow the steps described for administrators and end-users. Refer to *Enable Single Sign-On (SSO) for administrators* on page 393 and *Enable Single Sign-On (SSO) for end-users* on page 395.

Note For both administrators and end-users every Identity Provider should be in a different Identity Provider element. For a SAML-based Identity Provider you should use the `<SamlIdentityProvider>` element and for Kerberos you should use the `<KerberosIdentityProvider>` element.

Note For every Identity Provider defined in either the `sso-admin.xml` or `sso-enduser.xml` file, you should have a different Identity Provider metadata file. When uploading the SSO Configuration Files ZIP file, make sure that all required files are in the ZIP.

Note The client name has to be the same on all Identity Providers, SecureTransport only supports one service provider per component (Administrator and End-user).

Identity Provider resolution

Identity Provider resolution provides support for choosing the right Identity Provider based on server configuration and run-time metadata. If such resolution is not present, the first Identity Provider is selected by default, among ones specified under `<IdentityProviders>` element.

For both `sso-enduser.xml` and `sso-admin.xml` configuration files the element to edit is `<IdentityProviderResolution>` element under `<ServiceProvider>` element. The mapping can be done in either one of the following ways:

1. Query parameter – Identity provider mapping using a query parameter. The name of query parameter resolution will be searched for among request parameters during runtime and its value should match to the Identity Provider alias.
2. Header - Header value provided by a user request. The name of header resolution will be searched for among request header during runtime and its value should match to the Identity Provider alias.

Note Only one of these mappings can be done.

Note By default, if no Identity Provider ID is set, the first listed Identity Provider in the configuration file is used.

Identity Provider resolution for administrators

To configure Identity provider resolution for administrators, open the `sso-admin.xml` and edit the `<IdentityProviderResolution>` element under the `<ServiceProvider>` element.

Query parameter resolution example:

```
<QueryParameter name="idp_id">
    <Mapping value="keycloakIdp" entityId="https://st.keycloak.axway.int/" />
    <Mapping value="shibbolethIdp" entityId="https://st.shibboleth.axway.int/" />
</QueryParameter>
```

Note The value of name attribute in the `<QueryParameter>` element should match the Server configuration option `LoginSettings.Admin.SSO.idpResolverKey` value. The default value is `idp_id`.

Note Ensure the name of the query parameter/header is different than SecureTransport configuration option `LoginSettings.Admin.SSO.localIdpId` to be able to configure the selection of SecureTransport as local authentication provider and SSO Identity Provider. For more information on how to use SecureTransport as Identity provider, refer to *SecureTransport as an Identity Provider* on page 402.

In the example above we already have 2 identity providers defined in `sso-admin.xml` file.

Suppose we have the following request:

- `https://<ST>/?idp_id=shibbolethIdp`, where `<ST>` is the IP of the running SecureTransport instance.

SecureTransport will choose the Identity Provider with an `entityId='https://st.shibboleth.axway.int/'`. If no such Identity Provider is found, the login will be effectively rejected.

Header resolution example:

```
<Header name="idp_id">
    <Mapping value="keycloakIdp" entityId="https://st.keycloak.axway.int/" />
    <Mapping value="shibbolethIdp" entityId="https://st.shibboleth.axway.int/" />
</Header>
```

Note The value of name attribute in `<Header>` element should match the SecureTransport configuration option `LoginSettings.Admin.SSO.idpResolverKey` value. The default value is `idp_id`.

Note Ensure that the name of the query parameter/header is different than SecureTransport configuration option `LoginSettings.Admin.SSO.localIdpId` in order to be able to configure selection of SecureTransport as local authentication provider and SSO Identity Provider. For more information on how to use SecureTransport as Identity Provider, refer to *SecureTransport as an Identity Provider* on page 402.

In the example above we already have two Identity Providers defined in the `sso-admin.xml` file.

Suppose we have request to the running SecureTransport instance that contains the following Header:

- `keycloakIdp : https://st.keycloak.axway.int/`

SecureTransport will choose the Identity Provider with an `entityId='https://st.keycloak.axway.int/'`. If no such Identity Provider is found, the login will be effectively rejected.

Identity provider resolution for end-users

To configure Identity provider resolution for end-users, open the `sso-enduser.xml` file and edit the `<IdentityProviderResolution>` element under the `<ServiceProvider>` element.

Query parameter resolution example:

```
<QueryParameter name="idp_id">
    <Mapping value="keycloakIdp" entityId="https://st.keycloak.axway.int/" />
    <Mapping value="shibbolethIdp" entityId="https://st.shibboleth.axway.int/" />
    <Mapping value="kerbIdP" entityId="kerberos" />
</QueryParameter>
```

Note The name attribute in `<QueryParameter>` element should match the SecureTransport configuration option `LoginSettings.EndUser.SSO.idpResolverKey` value. The default value is `idp_id`.

Note Ensure that the name of the query parameter/header is different than SecureTransport configuration option `LoginSettings.EndUser.SSO.localIdpId` to be able to configure selection of SecureTransport as local authentication provider and SSO Identity Provider. For more information on how to use SecureTransport as Identity provider, refer to *SecureTransport as an Identity Provider* on page 402.

In the example above we already have three Identity Providers defined in `sso-enduser.xml` file.

Suppose we have the following request:

- `https://<ST>/?idp_id=shibbolethIdp`, where `<ST>` is the IP of the SecureTransport instance.

SecureTransport will choose the Identity provider with an `entityId='https://st.shibboleth.axway.int/'`. If no such Identity Provider is found, the login will be effectively rejected.

Header resolution example:

```
<Header name="idp_id">
    <Mapping value="keycloakIdp" entityId="https://st.keycloak.axway.int/" />
    <Mapping value="shibbolethIdp" entityId="https://st.shibboleth.axway.int/" />
    <Mapping value="kerbIdP" entityId="kerberos" />
</Header>
```

Note The name attribute in `<Header>` element should match the Server configuration option `LoginSettings.EndUser.SSO.idpResolverKey` value. The default value is `idp_id`.

Note Ensure that the name of the query parameter/header is different than SecureTransport configuration option `LoginSettings.EndUser.SSO.localIdpId` in order to be

able to configure selection of SecureTransport as a local authentication provider and SSO Identity Provider. For more information on how to use SecureTransport as Identity Provider, refer to *SecureTransport as an Identity Provider* on page 402.

In the example above we already have 3 identity providers defined in the `sso-enduser.xml` file.

Suppose we have request to SecureTransport instance that contains the following Header:

- `keycloakIdp : https://st.keycloak.axway.int/`

SecureTransport will choose the Identity Provider with an `entityId= 'https://st.keycloak.axway.int/'`. If no such Identity provider is found, the login will be effectively rejected.

Tenant resolution

Tenant resolution provides a support of multiple identity providers. If not present tenant is null. The supported ways to do that are by:

1. Query parameter
2. Header

Note Only one of the ways can be completed.

The tenant resolution is the same as the Identity Provider resolution in terms of syntax and meaning. However, the precedence is to take the Identity Provider resolution first. Header mapping, if present, will always be the first choice, no matter where it is placed; in the Identity Provider resolution or in tenant resolution.

Configure Single Sign-On (SSO) for streaming

You can configure Single Sign-On (SSO) functionality when using streaming setups.

Here are the basic steps:

1. Setup streaming. Refer to *Configure SecureTransport Back End to Edge streaming communication* on page 227.
2. On backend configure the SSO for end-user. Refer to *Enable Single Sign-On (SSO) for end-users* on page 395.
3. On the SecureTransport Edges navigate to **Authentication > Login Settings** and set **Required** for *SSO* for end-users.

Note The `sso-enduser.xml` file is taken from backend, corresponding to SSO Service Provider Entity ID value in the **Setup > Network zone**.

For the backend network zones:

- Private zone - SSO Service Provider Entity ID should be the Entity ID pointing to the Server.
- Streaming zone - SSO Service Provider Entity ID should be the Entity ID pointing to the Edge.

Note In a SecureTransport deployment, consisting of both backend and edge nodes, SSO must be configured and enabled on all nodes even if users are only logging in through the edge. On the edge, you must enable SSO for end-users. All backend and edge nodes in streaming must have same setting for SSO Authentication (Disabled or Required).

Configure Single Sign-On (SSO) for clusters

To configure SSO in clusters, refer to *Enable Single Sign-On (SSO) for administrators* on page 393 and *Enable Single Sign-On (SSO) for end-users* on page 395.

SecureTransport as an Identity Provider

Using SecureTransport as an Identity Provider allows users to use SecureTransport as an Identity Provider. The users who authenticate using SecureTransport as an Identity Provider, will authenticate using the password stored internally in the SecureTransport, and will be treated as local accounts.

The following configuration options are added in the Server Configuration options:

- For administrators:
  - `LoginSettings.Admin.SSO.idpResolverKey`
  - `LoginSettings.Admin.SSO.localIdpId`
- For end-users:
  - `LoginSettings.EndUser.SSO.idpResolverKey`
  - `LoginSettings.EndUser.SSO.localIdpId`

The `idpResolverKey` corresponds to the Query Parameter name attribute and can be used in both a query parameter as well as a header. This is the key that will be used when requesting local or Identity Provider authentication. The default value is: `idp_id`.

The `localIdpId` corresponds to the value in the mapping that will force SecureTransport to not trigger the SSO flow and continue with local authentication. The default value is: `ST_IDP`.

The value of these options is configurable. For more information about how to edit the Server Configuration options, refer to *Update server configuration files* on page 317.

Example for using SecureTransport as a Identity Provider:

```
https:// <ST IP>/?idp_id=ST_IDP
```

Note Options for using SecureTransport as an Identity Provider can be used either as query parameters or for using requests with header.

Single Sign-On SSO authentication flows

The supported Single Sign-on (SSO) and Single Logout (SLO) authentication flows for SecureTransport are:

- *Service Provider initiated Single Sign-On (SSO) authentication flow* on page 403
- *Identity Provider initiated Single Sign-On (SSO) authentication flow* on page 403
- *Service Provider initiated Single Logout (SLO) authentication flow* on page 403
- *Identity Provider initiated Single Logout (SLO) authentication flow* on page 404

Service Provider initiated Single Sign-On (SSO) authentication flow

The Service Provider initiated Single Sign-On (SSO) authentication flow describes the following behavior, when administrator or end-user access the protected resource directly on a SecureTransport site without being logged on. The user account is not managed on the SecureTransport side, it's managed by a third-party Identity Provider (IdP). The SecureTransport sends an authentication request to the Identity Provider. Practically, the authentication for the admin or user is done by an external agent. After authentication the IdP sends the response to SecureTransport, containing the result of the authentication process and mapped user-specific attributes. SecureTransport uses these attributes in various scenarios.

Identity Provider initiated Single Sign-On (SSO) authentication flow

The Identity Provider initiated flow describes the behavior when administrator or end-user chooses the Identity Provider that will be used for the authentication flow. This is configurable through the browser accessing the URL which is provided from the IdP. For that purpose, the Identity Provider first should be configured with specialized links that refer to the desired Service Provider (SecureTransport in our case).

Service Provider initiated Single Logout (SLO) authentication flow

The Service Provider initiated flow describes the behavior when the administrator or end-user, has already accessed Service Provider (SecureTransport) and the authentication is successful. In this case, SecureTransport initiates logout request that is sent to the IdP. After receiving the logout request from SecureTransport, the Identity Provider sends a logout response to every other Service Provider which was connected, forcing them to effectively logout the current user. After successful logout, the admin or end-user is redirected to the original IdP login page.

Identity Provider initiated Single Logout (SLO) authentication flow

The Identity Provider initiated Single Logout (SLO) flow describes the behavior when the administrator or the end-user, has already accessed the Service Provider (SecureTransport) and the authentication is successful. Then, IdP request for the logout is executed, and sends a logout request to every other Service Provider which was connected. The logout operation is performed and the administrator or end-user is successfully logged out. After successful logout, the admin or end-user is redirected to the original IdP login page.

Configure Kerberos as an Identity Provider in SecureTransport

This topic describes the configuration of Kerberos as an Identity Provider and the configuration of SecureTransport as a Service provider. In order to setup Kerberos to work with SecureTransport you need to have three files; the Kerberos configuration file, the `.keytab` file, and the `sso-enduser.xml` file.

Generate a Kerberos keytab file on Windows

For information about how to configure the Kerberos for UNIX-like systems, refer to the official Kerberos documentation.

A `keytab` file contains pairs of Kerberos principals and encrypted keys that are derived from the Kerberos password. You can use a `keytab` file for resource authentication without entering a password.

1. Open CMD on your Domain Controller.
2. Use the `ktpass` command to set up an identity mapping for the service principal:

```
ktpass -princ HTTP/<FQDN>@<realm> -mapuser <SPN> -pass <password>
-out <PATH_TO_KEYTAB_FILE> -ptype KRB5_NT_PRINCIPAL -crypto
AES256-SHA1
```

Where:

- FQDN - Fully qualified domain name of the Microsoft Windows Server 2012 R2 machine (the command is case-sensitive, therefore make sure you precisely enter the FQDN of your Windows machine)
- Realm - Domain Name (**with UPPERCASE letters**). In case there are multiple domains that have Active Directory replication, use the primary domain name instead of the sub domain.
- SPN - Service Principal Name (the user name of a user created in the Active directory of your Domain Controller)

Path to keytab file – Enter a valid path on your Domain Controller Windows machine for the `keytab` file to be generated to. Example: `C:\key.keytab`

The selected encryption may be different.

After the command is successfully executed, the `keytab` file is generated in the specified location.

Create a Kerberos configuration file

```
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
    principal="<HTTP/FQDN@REALM>"
    keyTab="ABSOLUTE_PATH_TO_KEYTAB_FILE"
    useKeyTab=true
    storeKey=true
    isInitiator=false
    doNotPrompt=true;
};
```

Note In a Standard Cluster or Enterprise Cluster environment, you have to specify the login modules for all Cluster nodes inside the Kerberos configuration file.

Main attributes:

- FQDN - Fully qualified domain name of the Microsoft Windows Server 2012 R2 machine on which SecureTransport is installed (as entered in the `ktpass` command)
- Realm - Domain Name (as entered in the `ktpass` command)
- `keyTab` - The path to which the SSO configuration files are uploaded in SecureTransport. If SecureTransport is installed in C drive of your Windows machine, the path would be: `C:/Axway/SecureTransport/STServer/conf/sso/key.keytab`

Edit the sso-enduser.xml file

In order to use Kerberos as IdP for end-users you need to edit and upload the `sso-enduser.xml` file.

Verify that it contains Kerberos Identity Provider. Example:

```
<KerberosIdentityProvider
entityId="kerberos"
configurationUrl="C:/Axway/SecureTransport/STServer/conf/sso/krb5Login.conf">
</KerberosIdentityProvider>
```

`configurationUrl` - The absolute path to the `krb5Login.conf` file location after the SSO configuration files are uploaded to SecureTransport. If SecureTransport is installed on the C drive of your Windows machine, the path would be the same as the one in the example.

Configure supported browser authentication

For a list of SecureTransport supported browsers, refer to *Browsers* on page 41.

To use Kerberos with SecureTransport the browsers will need some fine tuning.

For example:

For Microsoft Internet Explorer:

1. The SecureTransport instance should be added to the *Trusted sites* list.
2. Navigate to **Internet Options > Security tab > Trusted sites > Custom level**. Scroll all the way to bottom under *User Authentication* and *Logon*, select **Automatic logon with current user name and password**.

   Note This action will prevent the additional authentication pop up.

For Firefox:

Navigate to the **about:config** URL in Firefox and set *http://,https://* to the following properties:

`network.negotiate-auth.trusted-uris`

`network.automatic-ntlm-auth.trusted-uris`

For Chrome:

Google Chrome in Windows will use the Internet Explorer settings, so configure within Internet Explorer's Tools.

For Safari:

Mac OS supports SPNEGO with Kerberos as an authentication mechanism if Mac OS is joined to the Active directory.

Verify SSO authentication

To verify end-user SSO authentication, log onto a Windows machine joined to the same domain used as a realm in the SSO configuration, with a user existing in the Active directory. The Windows machine should be different from the one SecureTransport is installed to. Configure your browser for Kerberos authentication, and enter the URL of the ST Web Client (STWC) using the fully qualified domain name. You should be logged into STWC automatically with the same user account that you logged onto the Windows machine.

Pluggable authentication

A custom authentication plug-in allows you to implement your own authentication logic and override the SecureTransport authentication mechanism. The custom authentication has priority over the rest authentication types except for the Single sign-on (SSO). Only one authentication plug-in can be enabled at a time.

Pluggable Authentication features:

- End-user authentication over the HTTP, FTP, and SSH.
- Administrator authentication over HTTP only.
- Supports multiple authentication methods for administrators and end-users: basic authentication (user name/password), certificates, and dual authentication (both username/password and a certificate)
- The plug-in custom configuration is stored in the Server Configuration and can be exported and imported with it.
- Error and messages from the plug-in are displayed in SecureTransport Server log.

The following conditions apply to Pluggable authentication:

- The deployment of multiple authentication plug-ins is not supported.
- To be authenticated by a plug-in, a SecureTransport account must be created with the "Password is stored locally" option disabled.
- On an Edge server, Pluggable authentication can be configured for administrators only.
- Central Governance registration does not work with administrators with an external password authenticated via a custom plug-in.
- Log-in Restriction Policies work if an IP address is used, and may not work when a username is used for a policy (due to the fact that the plug-in may accept one username and return a completely different one).

Before your custom plug-in can be configured and used, it must be deployed, registered, and then enabled in the Server Configuration.

Plug-in deployment

The custom authentication logic (plug-in) is packaged as .jar file that follows the set of conventions described in the Developer Guide.

To deploy an authentication plug-in, place its JAR file in the `/<st_dir>/plugins/authentication/` directory, and restart the Admin and the TM daemons.

In a cluster environment, the plug-in should be deployed on all nodes, and the Admin service and the TM - restarted on all nodes.

Plug-in registration

SecureTransport identifies the plug-in by the name of its JAR file. Plug-ins are discovered and registered at the Admin daemon start. Each authentication plug-in is added to two configuration registries in the *Server Configuration* page:

- `Plugins.Authentication.Admin.Registry`
- `Plugins.Authentication.EndUser.Registry`

If the plug-in has a custom configuration, its configurable options are added in the Server Configuration page in the following format:

- `Plugins.Authentication.<plugin_name>.<config_option>`

Note The plug-in configuration options are exported upon server configuration export. Before importing a server configuration with custom plug-in configuration options, the relative plug-ins must be deployed. Otherwise, their configuration options will not be imported.

Plug-in activation

After being registered, the authentication plug-ins are added to the admin and the end-user registries in the Server Configuration, but they are disabled (have a hash symbol in front of their names). SecureTransport will not automatically activate a newly registered plug-in. To activate a plug-in, remove the # symbol from its name.

Only one plug-in can be enabled per registry at a time. Otherwise, the authentication fails.

If no plug-in is enabled, users are authenticated by using the SecureTransport internal authentication logic.

Note Plug-in activation does not require service restart.

Plug-in management

To undeploy a plug-in:

1. Delete the JAR file from the `/<st_dir>/plugins/authentication/` directory.

2. Restart the Admin and TM daemons.
The plug-in name is then removed from the registries along with its configuration options.

When you uninstall SecureTransport, the plug-ins JAR files are also removed.

To redeploy or update a plug-in:

1. Undeploy the existing plug-in.

2. After the Admin and TM daemon restart, go to the Server Configuration registries and make sure the plug-in is removed from the registries.

3. Deploy the new plug-in (version).

After the restart, the new plug-in is added to the admin and end-user authentication plug-ins list.

Plug-in configuration

Successful plug-in usage depends on both the authentication methods that are supported by the plug-in and the correct configuration in **Login Settings**.

Example scenarios and troubleshooting

If you have enabled a plug-in that supports Basic authentication, you must configure the users to log in with a username and a password.

If the enabled plug-in supports authentication with a certificate, you must configure certificate authentication.

To configure dual authentication, you must enable a plug-in that supports both authentication methods.

In case the plug-in is enabled but not configured correctly, and you cannot log in to the administration tool to reconfigure, undeploy the plug-in.

In a Standard Cluster, if the jar file is not uploaded to the secondary node, the configuration will not be considered correct, and an error message will be displayed in the Server Log at startup.

Pluggable authentication status

The Login settings page displays the Pluggable authentication status and provides a link to the server configuration option related to the end-user authentication plug-ins list.

Messages and errors:

- "*Plugin <plugin name> enabled.*"- an authentication plug-in with that name is enabled.
- "*No plugins registered.*"- there are no registered plug-ins.
- "*No authentication plugin enabled.*"- there are registered plug-ins, but none of them is enabled.
- "*Invalid configuration. Several authentication plug-ins are enabled.*"- multiple plug-ins are enabled.

Note Plug-in authentication cannot be applied for a specific user class. When enabled, it applies to all user classes.

Plug-in authentication notifications

On each login request, the following messages are displayed in the Server log:

- INFO: "`Authentication call to <plugin_name>.`"- notification of an authentication request sent to an enabled authentication plug-in.
- INFO: "`<plugin_name> successfully authenticated user <username>. Authentication result: SUCCESS, '<plugin_message>'`"- notification of a successful authentication by a plug-in
- INFO: "`<plugin_name> failed to authenticate user. Authentication result: FAILURE, '<plugin_message>'`"- notification of an unsuccessful authentication
- INFO: "`<plugin_name> was unable to authenticate user. Authentication result: CONTINUE, '<plugin_message>'`"- the plug-in does not recognize the user and indicates that an SecureTransport internal authentication must be executed.

Note All data sent/ received to/from a plug-in is available on a DEBUG log level.

User mapping

If the authentication process is successful, user mapping is performed.

End-user only

An end-user can log in to SecureTransport as a virtual account, account template, or an external account. In the first two cases, the user is authenticated based on the user properties pre-defined in SecureTransport; In order for an external user to be successfully authenticated, the plug-in must provide the following attributes: login name, UID, GID, home directory.

1. The user logs in - the user class is determined by the user's properties (login name, GID, UID, Address or the custom expression).

2. SecureTransport searches for an account with the same login name and an externally stored password in its database. If such account is found, the user is mapped.

3. If there is no virtual account with this login name, SecureTransport tries to map the user to an account template (based on the user class).

4. If there is no matching account template, the user logs in as an external user. To determine the user, SecureTransport uses the attributes returned by the plug-in. If the plug-in does not return those attributes, the authentication fails.

Admin only

1. If an admin account with that login name and an externally-stored password is not present, the authentication will fail.
2. For certificate or dual authentication, the respective check boxes on the Admin Settings page must be enabled.

3. If the plug-in successfully authenticates an administrator but their account is locked or it is of a 'dbsetup' type, the authentication will fallback to the internal SecureTransport logic.

System attributes

- Session attributes

Attribute Name	Expression Syntax
email	${sess.STSESSION_PLUGIN.email}
UID	${sess.STSESSION_PLUGIN.UID}
GID	${sess.STSESSION_PLUGIN.GID}
homeDir	${sess.STSESSION_PLUGIN.homeDir}
username	${sess.STSESSION_PLUGIN.username}

  - The first element in a custom attribute `<attribute>`

```
${sess.STSESSION_PLUGIN.additionalAttributes['<attribute>'][0]}
```

- Advanced routing environment attributes

Attribute Name	Expression Syntax
email	${plugin.email}
UID	${plugin.uid}
GID	${plugin.gid}
homeDir	${plugin.homeDir}
userName	${plugin.userName}

  - The first element in the attribute `<attribute>`

```
${plugin.attributes['attribute'][0]}
```

Usage in User Class custom expressions

You can use plug-in attributes in the User Class custom expressions.

For example:

- PLUGIN.UID
- PLUGIN.GID
- PLUGIN.email
- PLUGIN.homeDir
- PLUGIN.pluginName

will return the corresponding attribute value from plug-in data.

For PLUGIN.attributes, you can use the built-in memberOf function (see the **Access Control** -> **User classes** -> **Custom expressions**, also on this page update the possible values for `DXAGENT_USERLOGINTYPE`).

When a custom authentication plug-in is used, the `DXAGENT_USERLOGINTYPE` value is `PLUGIN`; the

`DXAGENT_AUTHN_PLUGIN_NAME` value is the name of the plug-in that performed the authentication for the current user.

Login settings

You can use the *Login Settings* page to disable or require Single Sign-On (SSO), enable or disable certificate authentication and to specify client certificate authentication for end users and administrators, enable or disable dual authentication, and set LDAP and SiteMinder authentication levels.

The following topics describe the end-user and administrator login options:

- *End-user login options* on page 412
- *Administrator login options* on page 417

End-user login options

You can use the end-user login options to disable or require end-user Single Sign-On (SSO), check the current pluggable authentication status, enable or disable end-user certificate requirements, set the certificate requirements level, enable or disable dual authentication, or specify for which classes it will be applied, and set LDAP and SiteMinder authentication levels.

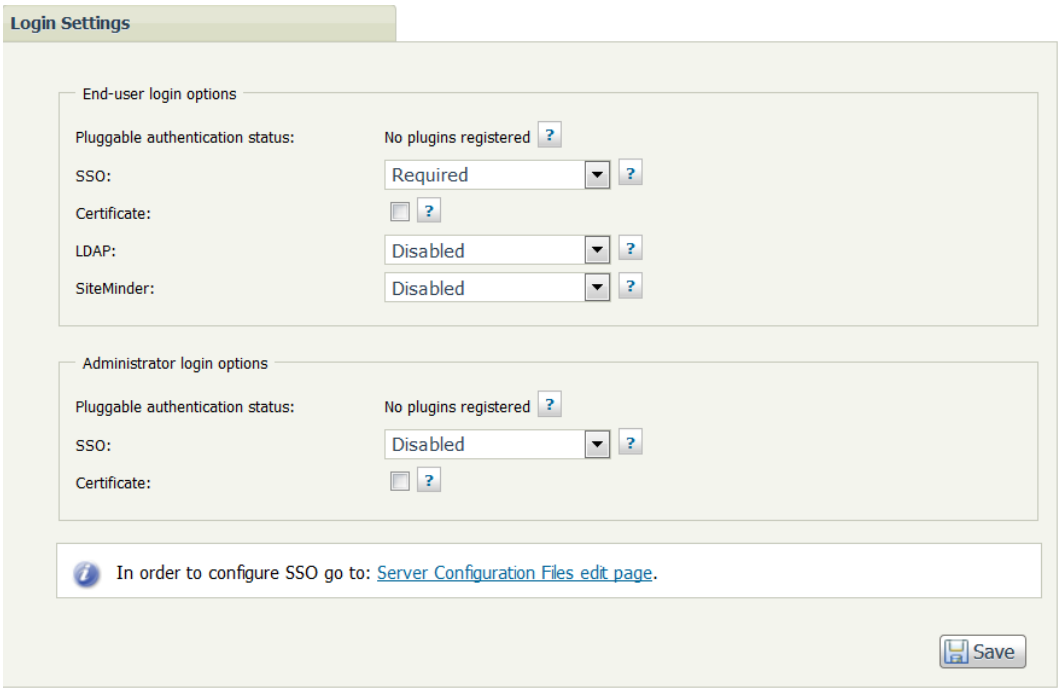
Note The end-user login options Certificate per protocol, LDAP, and SiteMinder are not available on the SecureTransport Edges.

Disable or require end-user Single Sign-On (SSO)

Use the following procedure to disable or require end-user Single Sign-On (SSO).

1. Select **Authentication > Login Settings**.

   The *Login Settings* page is displayed.



2. Under *End-user login options* in the **SSO** drop-down menu, select one of the following values:
   - **Disabled** - SSO will not be used.
   - **Required** - Redirection to Identity provider will always be performed. If the authentication with the Identity Provider (IdP) fails, the login will be rejected. This state will override any of the existing authentication methods via HTTP(s) for end-user - Certificate for HTTPS, LDAP with HTTP(s) and SiteMinder.

     Note Requires Transaction Manager service restart on back-end.

     Note SSO login option is applicable only for HTTP(s).
3. Click **Save**.

Note In order to configure SSO go to: *Server Configuration Files* edit page.

For information on editing and updating the server configuration files, refer to *Single Sign-On (SSO) and Single Logout (SLO)* on page 386.

Pluggable authentication

Shows the Pluggable authentication status and provides a link to the Server Configuration option related with the end-user's available deployed custom plug-ins list.

For information, refer to *Pluggable authentication* on page 407.

Configure end-user certificate requirement and level

The following table describes the settings for Client Certificate Authentication. The settings are the same for the four supported protocols: HTTPS, FTPS, SSH and PeSIT. Each protocol can be configured independently.

Option	Description
Disabled	The server never asks for a client certificate. The server accepts only a password for client authentication.
Required	Client must have a certificate to present to the Server during the SSL handshake. If the certificate is missing, the Server rejects the connection. The SSH server accepts only a key for client authentication.
Optional	Client might have a certificate. The server asks for it during the SSL handshake, but allows the connection to proceed if the client does not present a certificate or when authentication with the presented certificate is not successful. The SSH server accepts either a password or a key for client authentication.

Use the following procedure to enable or disable end-user certificate requirements and to set the certificate requirements level.

1. Select **Authentication > Login Settings**.

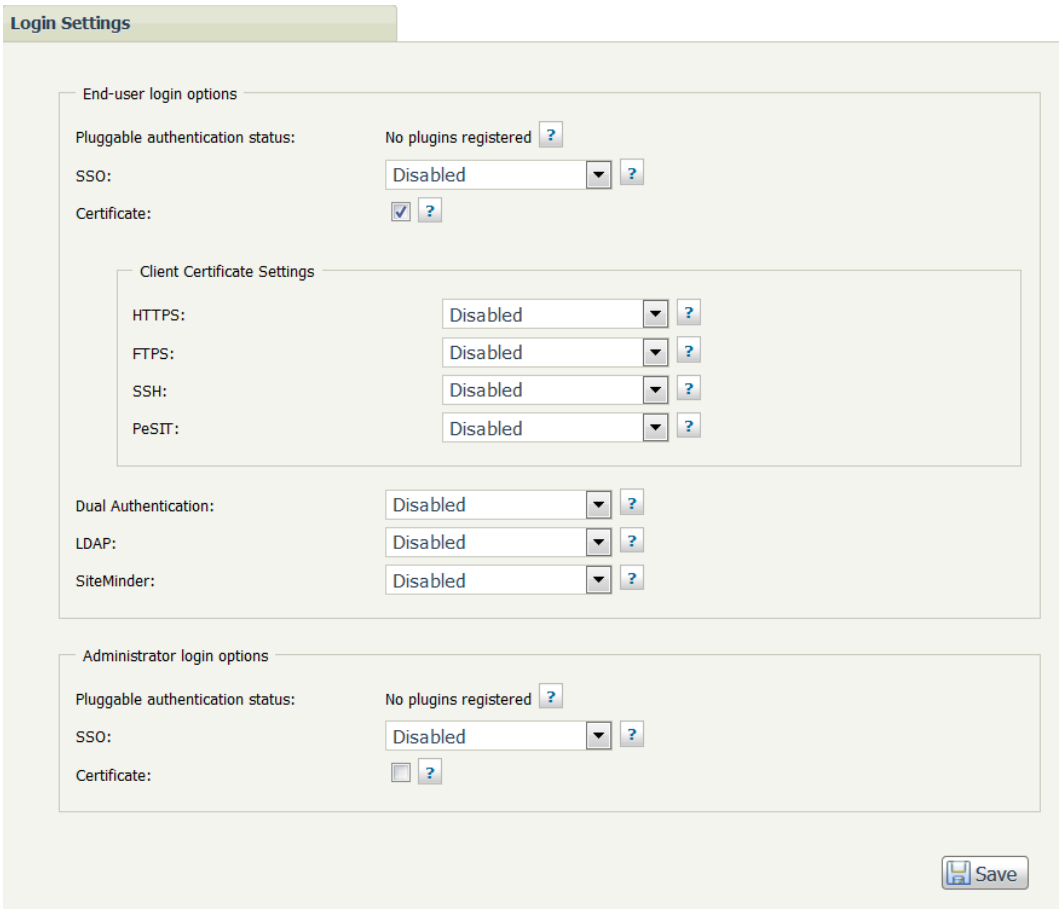
   The *Login Settings* page is displayed.

2. Under *End-user login options*, select or deselect **Certificate** to enable or disable the certificate requirements for end-users.

   Disabled - No certificate required.

   Enabled - A certificate is always required. The login in this case will be rejected in case no certificate is provided or the provided certificate cannot be associated with an account.

   If **Certificate** is selected or enabled, the *Login Settings* page with *Client Certificate Settings* pane visible is displayed.



3. Under *Client Certificate Settings*, select one of the three options to set the client certificate for each of the four protocols:
    - Disabled
    - Required
    - Optional
4. Click **Save**.

Note After you modify client certificate authentication options, restart the SSH server.

Note The HTTPS Certificate option will be set to **Disabled** when the end-user SSO login option is set to **Required**.

End-user dual authentication

Note This option will not be editable when the end-user *Certificate* option is set to **Disabled**.

Use the following procedure to enable, disable or specify user classes in dual authentication for end-users.

1. Select **Authentication > Login Settings**.

   The *Login Settings* page is displayed.

2. Under *End-user login options*, select one of the three options in the **Dual authentication (certificate and password)** drop-down menu to enable, disable or specify user classes in dual authentication for end-users.

   Disabled - No password required in addition to certificate authentication option.

   Enabled - A password is required in addition to certificate authentication option to users from all user classes.

   Specific user classes - A password is required in addition to certificate authentication option only for one or more comma-separated user classes inserted in the text field. User classes are case sensitive.

Note User classes with a comma inside their 'Class Name' should not be used due to the comma being a delimiter.

Note To enable or disable dual authentication for Specific user classes from REST API you must update both configuration options.

```
LoginSettings.Certificate.RequirePassword and
LoginSettings.Certificate.RequirePassword.UserClasses.
```

Example: To enable dual authentication for specific user class "VirtualClass" you must update

```
LoginSettings.Certificate.RequirePassword with value "true" and
LoginSettings.Certificate.RequirePassword.UserClasses with value
"VirtualClass".
```

3. Click **Save**.

For more information about how-to instructions for creating User Classes, see *User classes* on page 710.

Enable or disable LDAP

Use the following procedure to enable or disable LDAP.

1. Select **Authentication > Login Settings**.

   The *Login Settings* page is displayed.

2. Under *End-user login options* in the **LDAP** drop-down menu, select one of the following values:

   Disabled - The LDAP will not be used.

   Optional - SecureTransport searches the SecureTransport database before it searches the LDAP databases in the default domains. If no such user is found in SecureTransport and LDAP databases, then the login will be rejected.

   Required - An LDAP user will be required. If no such user exists, the login will be rejected.

   For details, see *LDAP logins* on page 427.

3. Click **Save**.
4. Restart the TM Server.

You must create one or more domains before SecureTransport can use LDAP to authenticate users. For information on creating LDAP domains, refer to *Create an LDAP domain* on page 430.

Enable or disable SiteMinder

Use the following procedure to enable or disable SiteMinder.

1. Select **Authentication > Login Settings**.

   The *Login Settings* page is displayed.

2. Under *End-user login options* in the **SiteMinder** drop-down menu, select one of the following values:

   Disabled - The SiteMinder configuration will not be used.

   Optional - The SiteMinder configuration may be used.

3. Click **Save**.

You must configure SiteMinder before you can use SiteMinder to authenticate users. For information on configuring SiteMinder, refer to *SiteMinder integration configuration* on page 420.

Administrator login options

You can use the administrator login options to enable or disable administrator Single Sign-On (SSO) and to enable or disable administrator certificate requirements.

Enable or disable administrator Single Sign-On (SSO)

Use the following procedure to enable or disable administrator Single Sign-On (SSO).

1. Select **Authentication > Login Settings**.

   The *Login Settings* page is displayed.

2. Under *Administrator login options* in the **SSO** drop-down menu, select one of the following values:

   - **Disabled** - SSO will not be used.
   - **Required** - Redirection to the Identity Provider (IdP) will always be performed. If the authentication with the IdP fails, the login will be rejected.

3. Click **Save**.

Note When SSO is set to **Required**, it is recommended the Client certificates to be set to **Disabled**. The Client certificates only need to be set to **Optional** when Central Governance will be integrated with SecureTransport.

Note For more information of how to configure SSO for Administrators, refer to *Single Sign-On (SSO) and Single Logout (SLO)* on page 386.

For information on editing and updating the server configuration files, refer to *Update server configuration files* on page 317.

Pluggable authentication

Shows the Pluggable authentication status and provides link to the Server Configuration option related with the end-user's available deployed custom plug-ins list.

For information, refer to *Pluggable authentication* on page 407.

Configure administrator certificate requirement and level

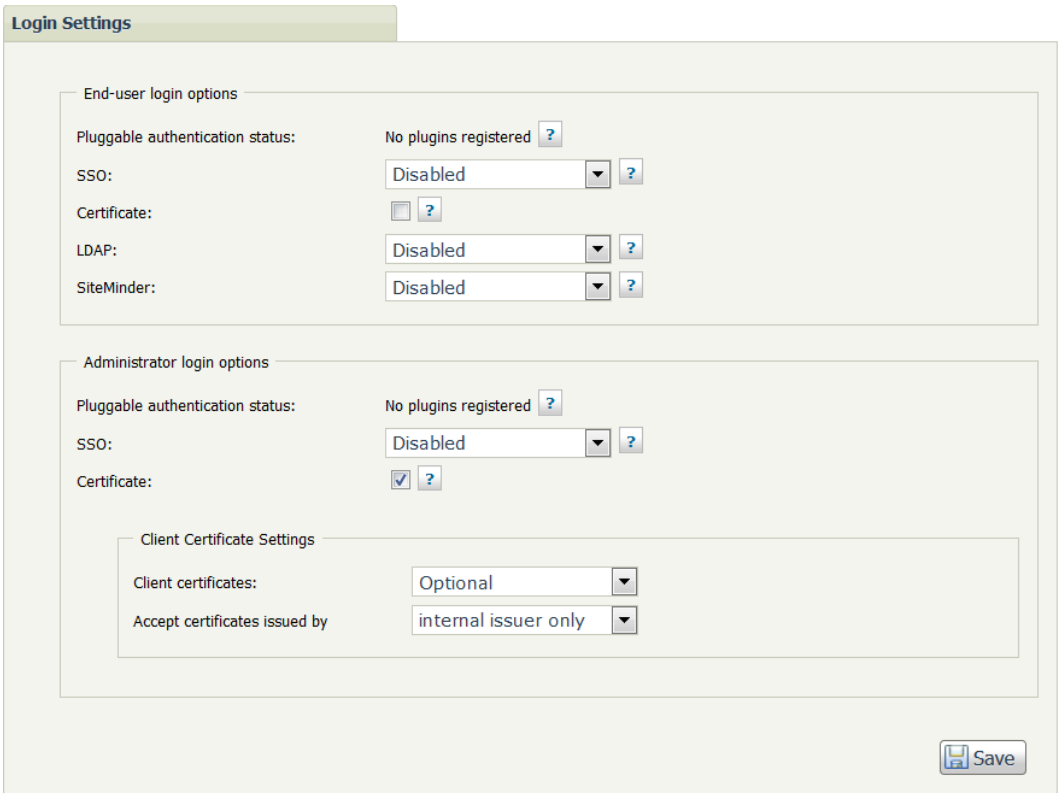
Set the certificate settings to allow administrators to log in by using a client certificate or to use dual authentication with both a certificate and a password. You can enable the ability to login with a client certificate, determine whether the certificate is optional or required, select the certificate issuer, and set the certificate chain limit.

When you want to access the Administration Tool and you have enabled client certificates, you are prompted to select the certificate you are using. Once the certificate is verified, you are logged in unless dual authentication is required. If certificates are optional and you do not select one, the login page is displayed. If SecureTransport cannot verify the certificate, or certificates are required and you did not select one, a connection error displays and you cannot log in.

If you are unable to successfully log in when using a certificate, clear the browser's SSL state, or close the browser and try again with a new browser instance.

1. Select **Authentication > Login Settings**.
2. The *Login Settings* page is displayed.
3. Under *Administrator login options*, select **Certificate** to allow administrators to log in using client certificates.

   The *Client Certificate Settings* pane and the remaining fields are displayed.



4. Select either **Optional** or **Mandatory** in the **Client certificates** drop-down menu. If you select **Optional**, administrators do not need a certificate. If you select **Mandatory**, each administrator must have a client certificate set up. If certificates are required, all administrators must be mapped to a certificate, and all users must present a valid trusted certificate to gain access to the login page.
5. Select one of the following choices from the **Accept certificates issued by** drop-down menu:
   - **internal issuer only** – The certificate must be issued by the internal CA. See *Manage the internal CA* on page 63.
   - **any trusted issuer** – The certificate must be issued by a CA that is trusted by one of the CAs listed as a trusted CA. See *Manage trusted CAs* on page 61.
   - **issuer file or path** – The certificate must be issued by a CA whose certificate is in a file you specify.
6. If you select **issuer file or path**, the following fields are displayed:
   - A field that you use to specify the location of the certificate PEM-encoded (`.pem`) file or a directory that contains the PEM-encoded files.

     You can type either a fully qualified file or path names or a file or path names relative to `<FILEDRIVEHOME>`. Do not put the PEM-encoded files in the keystore directory, `<FILEDRIVEHOME>/lib/certs/issuers`, because the certificates in that directory are regenerated from the database when servers start.

- A **Limit certificate chain depth to** field. Type a number that sets the maximum number of levels for SecureTransport to go through in validating the certificate up to a trusted root. For example, if you set the chain depth to 1, then only a certificate issued directly by a trusted root is allowed and a certificate issued by an intermediate CA is rejected.

7. Click **Save**.
8. Restart the Administration Tool server using the `stop_admin` and `start_admin` commands. If you are running on Windows, you can also use the **Services** console to restart the `admin` service.

If you choose to use certificates for administrator logins, a **Certificate DN** field displays in the *New Administrator* and *Edit Administrator* pages where you must provide the certificate domain name information. For more information, see *Add an administrator account* on page 647.

Note The Client Certificate Settings option will be set to **Disabled** when administrator SSO login option is set to **Required**.

SiteMinder integration configuration

CA SiteMinder is a third-party application that controls user access to secured applications and provides a Single Sign-On (SSO) portal. A SSO portal is a Web gateway or proxy that enables users to access multiple secured Web applications using a single user name and password they provide once at the start of the user session.

SecureTransport can be integrated into a SiteMinder SSO environment and use SiteMinder to SSO authenticate and authorize resource access using only HTTP or HTTPS.

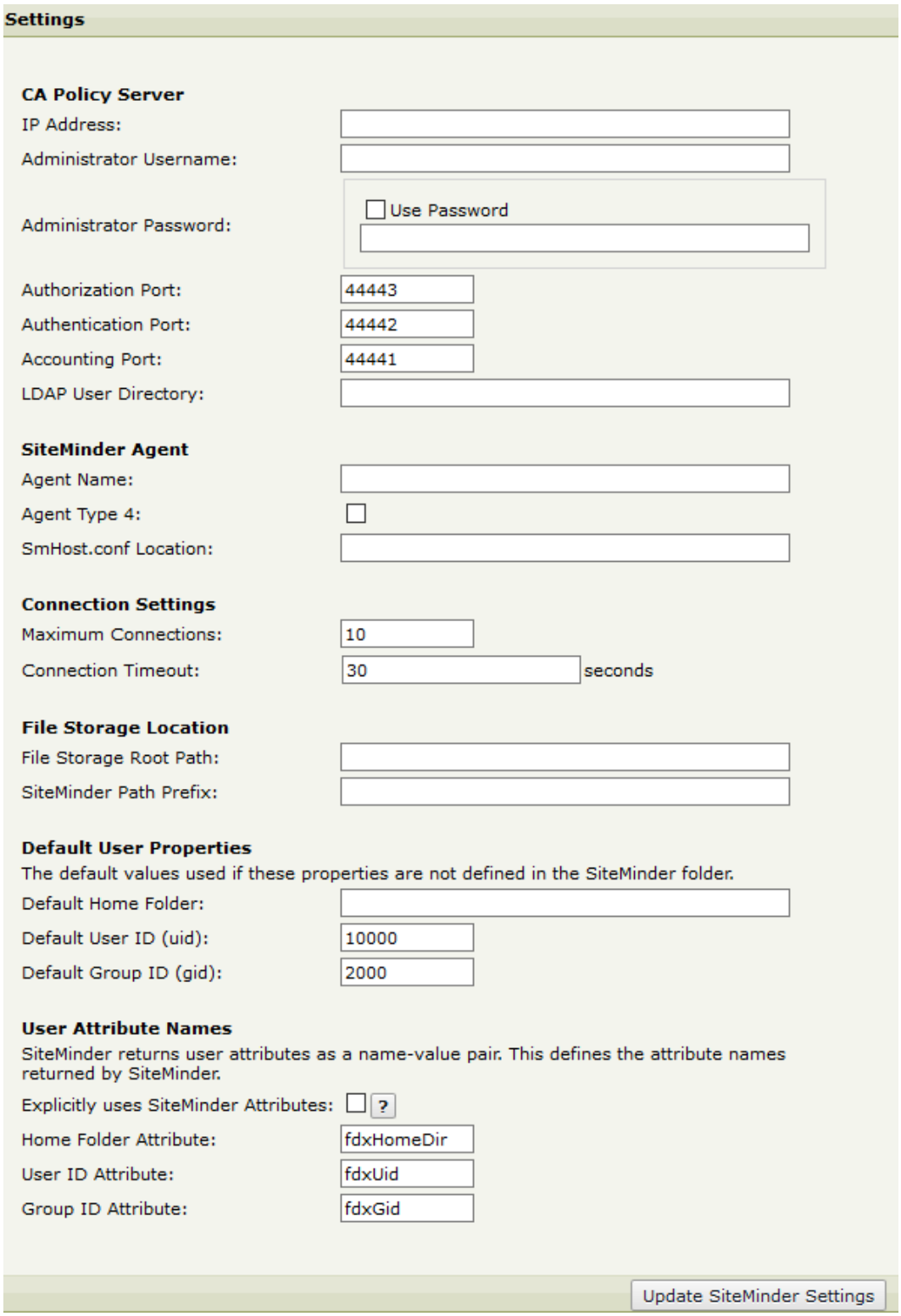
Note Before configuring SiteMinder settings, be sure to read *SiteMinder integration* on page 377.

Before using SecureTransport with SiteMinder, you must configure the SiteMinder settings using the SecureTransport Administration Tool.

Note If SecureTransport is deployed in a secure perimeter network (DMZ) configuration, configure the SiteMinder settings on SecureTransport Server as described in this topic. The *SiteMinder Settings* page is not available on SecureTransport Edge.

1. Select **Authentication > SiteMinder Settings**.

   The *CA SiteMinder Setting* page is displayed.



2. Provide the information as described in the following table:

Name	Description	Required/ optional
IP Address	The network address of the SiteMinder Policy Server.	Required
Administrator Username	The user name used to connect to the SiteMinder database.	Optional
Administrator Password	If a password is required, select Use Password and enter it in the field provided. **Note** Exported configuration from SecureTransport 4.x.y systems does not include the SiteMinder administrator password.	Optional
Authorization Port	The authorization port for the SiteMinder Policy Server.	Required
Authentication Port	The authentication port for the SiteMinder Policy Server.	Required
Accounting Port	The accounting port for the SiteMinder Policy Server.	Required
LDAP User Directory	Name of the SiteMinder user directory used to retrieve the home folder, user ID, and group ID.	Optional
Agent Name	The name for the SiteMinder agent that SecureTransport should use when connecting to the SiteMinder Policy Server.	Required
Agent Type	For SiteMinder protocol version 4 the shared secret used to communicate with the SiteMinder Policy Server. For version 5, the path to `SmHost.conf`.	Required
Shared Secret	The password for the SiteMinder agent that SecureTransport uses to connect to the Policy Server.	Required
Maximum Connections	The maximum number of SiteMinder connections that SecureTransport can have open simultaneously. This does not limit the number of users who can log in to the SecureTransport Server using the Site Minder SSO portal.	Required

Name	Description	Required/ optional
Connection Timeout	The amount of time (in seconds) that a SiteMinder connection can be idle before it is closed. The default is 30 seconds. This is independent of user session timeout.	Required
File Storage Root Path	The segment of the absolute URI that is removed before it is submitted to the SiteMinder Policy Server for authorization. If the entire absolute URI is submitted for authorization, type `/` in this field.	Required
SiteMinder Path Prefix	After the File Storage Root Path is removed, but prior to SiteMinder authorization, this entry is prefixed to the absolute URI. For example, if the absolute URI is `/mnt/ab/user1`, the File Storage Root Path is `/mnt/ab`, and the SiteMinder Path Prefix is `/root`; then `/root/user1` is sent to SiteMinder for authorization. If this box is left blank, no prefix is applied to the URI prior to authorization. **Note** When SiteMinder is enabled, all SecureTransport users must have GET access to the path specified in the SiteMinder Path Prefix to successfully log in. If this setting is left blank, then users must have GET access to /. The SiteMinder administrator must set up the SiteMinder Policy Server accordingly.	Optional
Default Home Folder	The absolute URI of the default home folder of the local user. The default home folder is used when a home folder is not supplied by the SiteMinder Policy Server. **Requirements:** • The folder must be created manually on the machine. • On Windows, the folder should not use shared storage. • On Linux, the permissions of the folder must be set to "777" on all nodes in the cluster.	Required

Name	Description	Required/ optional
Default Local User ID	The numeric user ID (UID) of a user that has full read/write access to the directory specified as the File Storage Root Path and its subdirectories. This default is used only if a UID is not supplied by SiteMinder. **Note** On Windows, type the name of the respective virtual user. Windows does not support UIDs.	Required
Default Local Group ID	The numeric group ID (GID) of a user that has full read/write access to the directory specified in the File Storage Root Path and its subdirectories. If no UID or GID are supplied by SiteMinder, these defaults are used for all file operations (including ownership of new files) performed by SecureTransport for users authenticated by SiteMinder.	Required
Explicitly uses SiteMinder Attributes	When selected, SecureTransport uses the values specified in the *User Attribute Names* section. If not selected, and • if the user is assigned to an account template, the User ID, Group ID, and Home Folder are determined from the template. • if the user is not assigned to an account template, the default home folder, local user ID, and local group ID are used. The state of the checkbox has no effect on SiteMinder users mapped as virtual users.	Optional

Name	Description	Required/ optional
Home Folder Attribute	SiteMinder returns information about the user as name=value pairs. The attributes define the name part of the pair which must be added manually. In `Home Folder Attribute`, you should provide the name of the SiteMinder attribute which value is the absolute URI of the user home folder. **Requirements:** • The folder must be created manually on the machine. • On Windows, the folder should not use shared storage. • On Linux, the permissions of the folder must be set to "777" on all nodes in the cluster. **Note** When changing `Home Folder Attribute`, the Transaction Manager should be restarted in order for the changes to be applied. **Note** If `Home Folder Attribute`, `Group ID Attribute` and `User ID Attribute` are left blank, and the attributes therefore not defined, the default Home Folder, Local User ID, and Local Group ID are used.	Optional
User ID Attribute		Optional
Group ID Attribute		Optional

3. Click **Update SiteMinder Settings**.

   To use one or two more SiteMinder servers for failover, specify server configuration parameters that correspond to the fields described above. The names of the parameters for the second server start with `Siteminder.PolicyServers.Second.PolicyServer`. The names for the third server start with `Siteminder.PolicyServers.Third.PolicyServer`. The final parts of the names are given in the following table:

Field	Sever configuration parameter
Enable SiteMinder Module	`enable`
IP Address	`host`
Administrator Username	`adminUsername`

Field	Sever configuration parameter
Administrator Password	`adminPassword`
Authorization Port	`authorizationPort`
Authentication Port	`authenticationPort`
LDAP User Directory	`ldapUserDirectory`
Maximum Connections	`maxConnections`
Connection Timeout	`timeout`

Note If more than one SiteMinder server is configured in a server that is upgraded from SecureTransport 4.x.y or in configuration that is imported from a SecureTransport 4.x.y server, set the `Siteminder.PolicyServers.Second.PolicyServer.enable` and the `Siteminder.PolicyServers.Third.PolicyServer.enable` system configuration parameters to `true` as required.

There are also parameters for `minConnections` and `connectionsStep` which are not set in the *CA SiteMinder Setting* page.

LDAP integration

You can configure Axway SecureTransport to use Lightweight Directory Access Protocol (LDAP) servers to authenticate users and provide information it uses to set up the user session.

The SecureTransport LDAP integration includes:

- Support for LDAP versions 2 and 3.
- Support for Secure LDAP, also know as LDAP over SSL/TLS or LDAPS.
- Search over multiple LDAP domains that provide authentication information and user attributes for different groups of users.
- Multiple, redundant LDAP servers in a domain for backup when an LDAP server is down or inaccessible.
- One or more default LDAP domains that SecureTransport searches when a user does not specify a domain name on login.

Note You cannot configure both LDAP integration and SiteMinder integration.

The following topics provide LDAP connections, binds, and searches information and logins, agents, domains, home folders, and use type ranges for LDAP:

- *LDAP connections, binds, and searches* on page 427 - Describes LDAP connections, binds, and searches.

- *LDAP logins* on page 427 - Describes LDAP logins and provides how-to instructions for logging into LDAP.
- *LDAP domains* on page 429 - Describes the LDAP domains.
- *LDAP home folders* on page 448 - Describes the LDAP home folders.
- *LDAP user type ranges* on page 450 - Describes the LDAP user type ranges.

LDAP connections, binds, and searches

To configure backup LDAP servers in case a server is not accessible or not responding, you can list two or more LDAP servers for any domain. SecureTransport attempts to connect to the servers and bind to their LDAP databases in the order you specify in the server list. SecureTransport uses the first LDAP database it can bind to. If SecureTransport does not find a record for the user in the first available LDAP database, it does not try to connect to other servers in the sequence. So for each login attempt, SecureTransport searches at most one LDAP database in a domain.

You can configure SecureTransport to bind to an LDAP database anonymously or using a bind DN and password.

To locate a DN in the LDAP database, SecureTransport searches using partial DN information and the user's common name (CN), unique identifier (UID), or Active Directory account name (sAMAccountName). You must define the base DN as required by the server and select the search attribute. You can also define an alias query that is a filter that uses values from an email address used as a login user name.

LDAP logins

If you configure and enable LDAP, SecureTransport uses it as follows when users log in:

- If the user includes a domain name in the login name, *domain_name*/*user_name*, SecureTransport attempts to connect the LDAP servers configured for the named domain. If the first server SecureTransport connect to has record for the user, SecureTransport use it. If not, the login fails.
- If the user does not include a domain name in the login name, SecureTransport can still find the authentication information and user attributes in the LDAP databases of the default domains in the order on the *LDAP Domains* page. Depending on whether or not LDAP authentication is required, SecureTransport also searches other databases:
  1. If LDAP authentication is optional, SecureTransport searches the SecureTransport database before it searched the LDAP databases in the default domains.
  2. If the user specified by the login name is not in the SecureTransport database and login name and password match, SecureTransport searches the databases of the LDAP servers configured for the default domains in the order on the *LDAP Domains* page.
  3. If LDAP authentication is optional and the authentication information is not in any of the databases of the LDAP servers in the default domains, SecureTransport searches the

operating system if real users are enabled.

If SecureTransport does not find the user name in one of these locations, the login fails.

When SecureTransport finds an LDAP entry for the user name, it uses the password from the entry to authenticate the user. If authentication fails, the login fails.

- **User ID** (UID) (UNIX-based systems only) – `fdxUid`. This is the numeric value required by the UNIX system to identify the user. This is not the LDAP attribute `UID`, which represents an LDAP unique identifier.
- **Group ID** (GID) – `fdxGid`
- **Home folder** (HomeDir) – `fdxHomeDir`
- **User type** – `fdxUserType`
- **User shell** (UNIX-based systems only) – `fdxShell`
- **System user** (Windows only) – `fdxSysUser`. This is name of a local or domain user of the Windows server. SecureTransport uses this user's credentials to access the Windows files in the session. If this is a real user, you must add the user to a SecureTransport password vault before you specify the user as the System User in an LDAP record or as the default system user for a domain. See *Add a user to a password vault* on page 690.
- **Login by email** – `fdxAuthByEmail`. If this is enabled, the user can login using an email address as well as a user name if the login by email is enabled in the LDAP domain and the email attribute of the LDAP record has the correct value.

If the LDAP record SecureTransport finds does not include some of the user attributes, SecureTransport uses any enabled attributes maps, any enabled user type ranges, any enabled home folder entries, and the configured defaults for the domain to set the attributes. If any required attribute information is not available or not valid, the login fails.

SecureTransport performs the following actions to set the user attributes and other required session information:

1. Sets all attributes from LDAP record values based on any enabled attribute maps. For configuration, see *Define attribute mappings for a domain* on page 441.
2. On UNIX-based systems, if the `fdxUserType` attribute is not set and there is an applicable entry in the *User Type Ranges* page, sets the user type based on the value of the user ID. For configuration, see *LDAP user type ranges* on page 450.
3. For attributes that are not set, applies the default values for the domain. For configuration, see *Define LDAP user settings for a domain* on page 440.
4. Sets the user class. See *User classes* on page 710.
5. Checks any enabled DN filters configured for the domain. You can use DN filters to permit access to only certain sub-trees of the LDAP directory structure within the domain. If there is an enabled DN filter for the user class set in the previous step or for all users, denoted by asterisk (`*`), the DN from the LDAP record must match one of those filters. If there are enabled DN filters for the user class or for all users and no filter matches, the login fails. See *Manage DN filters for a domain* on page 442.

6. If the `fdxHomeDir` attribute is not set, sets it based on the user class using the entries in the *Home Folder* page. For configuration, see *LDAP home folders* on page 448.
7. Use the alphabetically first applicable account template. If there is an applicable account template, the values from the template replace any value already set. For details, see *Account templates and external users* on page 662.

If, after this process, any required user attributes are not set because there is no enabled attribute map, because the LDAP value for an enabled attribute map is not present in the LDAP record, or because the value was not set by a later step, the login fails.

SecureTransport real users authenticated using LDAP have the following limitations:

- They cannot use certificate authentication.
- They cannot change their passwords using a SecureTransport client.
- You can only subscribe them to an application if you do it in an account template or create a SecureTransport account that stores its password in the LDAP record.

To configure Active Directory in a SecureTransport LDAP domain, see *LDAP and Active Directory configuration* on page 447.

LDAP domains

Note If you setup LDAP in Windows without specifying a `sysuser`, the default configuration is applied.

The following topics describe the management and configuration of LDAP domains:

- *Create an LDAP domain* on page 430 - Provides how-to instructions for creating a domain.
- *Define LDAP search criteria for a domain* on page 433 - Provides how-to instructions for defining the LDAP search criteria for a domain.
- *Define LDAP user settings for a domain* on page 440 - Provides how-to instructions for defining LDAP user settings for a domain.
- *Define attribute mappings for a domain* on page 441 - Provides how-to instructions for defining domain attribute mappings.
- *Manage DN filters for a domain* on page 442 - Describes managing the DN filters for a domain.
- *Manage DN filters* on page 442 - Provides how-to instructions for managing DN filters.
- *Define Address Book settings for a domain* on page 443 - Provides how-to instructions for defining LDAP Address Book searches and Address Book attributes for a domain.
- *Edit a domain* on page 445 - Provides how-to instructions for editing a domain.
- *Delete domains* on page 445 - Provides how-to instructions for deleting domains.
- *Configure default domains* on page 446 - Provides how-to instructions for configuring default domains.
- *LDAP domains example* on page 446 - Provides examples of LDAP domains.
- *Secure LDAP* on page 447 - Describes securing the LDAP connection.

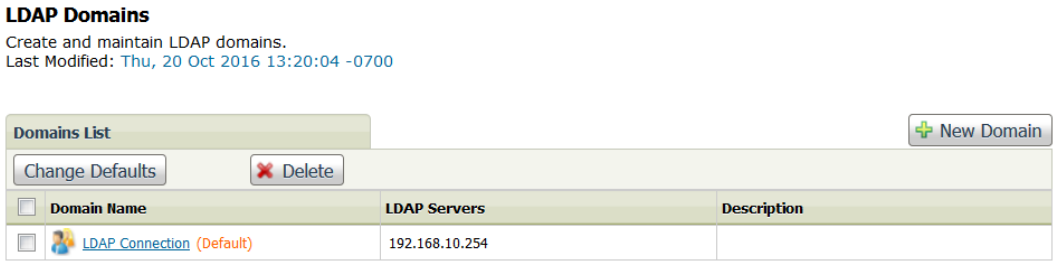
- *LDAP and Active Directory configuration* on page 447 - Describes using LDAP with an Active Directory configuration.

Create an LDAP domain

When you create a domain, you must give it a name and specify at least one LDAP server.

1. Select **Authentication > LDAP Domains**.

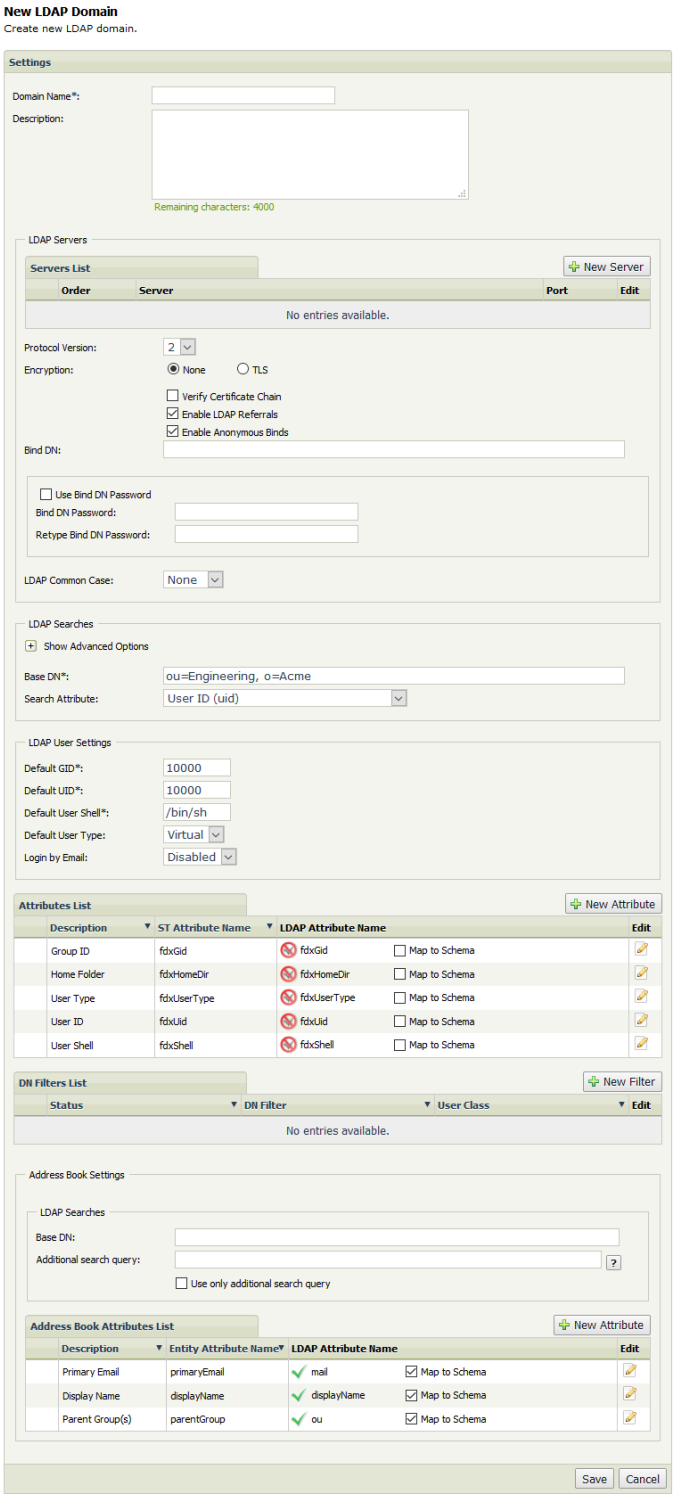
   The *LDAP Domains* page is displayed.



2. Click **New Domain**.

   The *New LDAP Domain* page is displayed.

   Note The *Address Book Settings* pane is only displayed if the Address Book feature is enabled (the value of the `AddressBook.Enabled` configuration option is set to **true**). For information on defining Address Book settings for a domain, refer to *Define Address Book settings for a domain* on page 443. For information on the Address Book LDAP source, refer to *LDAP source* on page 234.



3. Type a **Domain Name**. The user must specify this name in the login name, *domain_name/user_name*, to select this domain if it is not configured as a default domain on *LDAP Domains* page.
4. Type a **Description** for your use.
5. Under *LDAP Servers*, click **New Server**.

A line is added to the *Servers List*.

6. In the **Server** field, type the host name or IP address of the LDAP server.
7. In the **Port** field type the LDAP port number for the server. The default is 389.
8. To test the connection to the LDAP server, click the icon in the column after the **Server** column.
9. Click the Save icon ( ) in the **Edit** column.
10. Add backup LDAP servers, if any, to the *Servers List*.
11. To change the order SecureTransport tries the servers, click **Reorder**, update the numbers in the **Order** column, and click **Save**.
12. Under *LDAP Servers*, complete the following fields:

Field	Description	Valid values and notes
Protocol Version	Select the LDAP protocol version.	2 or 3
Encryption	Enable Secure LDAP, also know as LDAP over SSL or LDAPS.	None, TLS, or StartTLS (for LDAP protocol 3)
Verify Certificate Chain	Configure whether SecureTransport implicitly trusts the LDAP servers in this domain or verifies the LDAP server certificates.	See *Create an LDAP domain* on page 430.
Enable LDAP Referrals	Configure whether SecureTransport allows the LDAP server to refer a request to another LDAP server.	This option is required when the LDAP directory tree is distributed over a group of servers.
Enable Anonymous Binds	Configure whether SecureTransport uses a Bind DN to access to the LDAP server.	You can select this option when LDAP servers supports anonymous binding. If this option is not selected, the **Bind DN** field is required.
Bind DN	Type the distinguished name of a user who is allowed access to the LDAP directory for user lookups.	For authorization purposes, this field is case sensitive. If **Enable Anonymous Binds** is not selected, this field is required.
Use Bind DN Password	If a password is required to bind to the directory service on the LDAP server, select **Use Password** and enter the password in the fields provided.	

Field	Description	Valid values and notes
LDAP Common Case	Configure whether and how SecureTransport changes the case of the user name it receives from the LDAP database.	None, Lower, or Upper. If the value is Lower or Upper, SecureTransport maps the case of all letters in the user name to the case you specify.

13. Click **Save.**

For information on the Address Book LDAP source, refer to *LDAP source* on page 234.

Define LDAP search criteria for a domain

For information about how SecureTransport uses the search criteria, see *LDAP connections, binds, and searches* on page 427.

Note A specific LDAP configuration is required for Active Directory. For details, see *LDAP and Active Directory configuration* on page 447.

1. If you do not have the *New LDAP Domain* page open, select **Authentication > LDAP Domains** and click the domain name in the Domains List to open the *LDAP Domain* page.
2. Under *LDAP Searches*, complete the following fields:

Field	Description	Valid values and notes
Base DN	Define the base DN for the searches	A valid DN, such as, `OU=Sales, DC=ldaps1, DC=Example, DC=com`
Search Attributes	Select the LDAP attribute to use for the searches	User ID (uid), Common Name (cn), or SAM-Account-Name (sAMAccountName)
Alias Query	Define a filter using values from an email address used as a login user name	Click **Show Advanced Options** to display the **Alias Query** field.

3. Click **Save**.

The **Alias Query** field is used to perform real user look-up by email address to filter (limit) the search. If the **Alias Query** filter is selected, the search is performed not only by email but by email OR the specified filter in the **Alias Query** field. The real user look-up also returns only PERSON entities and no other object classes. So, you do not have to add attribute (`objectClass=Person`) in the field because SecureTransport inserts it in the filter. The value of the **Alias Query** field uses the search filter syntax described in *RFC 4515: Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters (June 2006)*, (http://www.rfc-editor.org/rfc/pdfrfc/rfc4515.txt.pdf).

The basic syntax of a search filter is:

`(attribute search_operator value)`

For example:

`(buildingname>=alpha)`

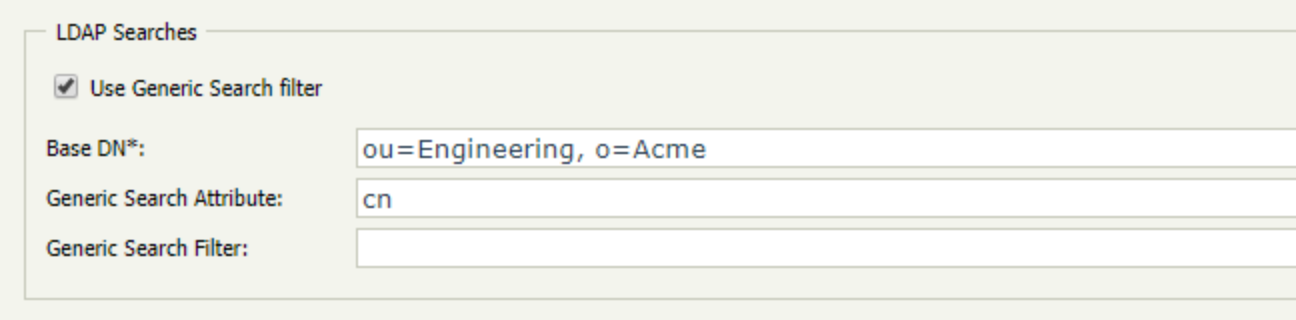
In this example, buildingname is the attribute, >= is the operator, and `alpha` is the value. You can also define filters that use different attributes combined together with logical operators.

Use Generic LDAP search filter

Select the **Use Generic Search filter** check-box and observe the following changes in the *LDAP Searches* options:

- the **Search Attribute** drop-down list is replaced with the **Generic Search Attribute** input text box
- **Alias Query** input text box is replaced by **Generic Search Filter** input text box

You can add any Generic Search attribute to use in the Generic search filter query. Note that the Generic LDAP search is used as it is and no additional attributes are appended.



Fill in the search criteria as described below:

Field	Description	Valid values and notes
Base DN	Define the base DN for the searches	A valid DN, such as, `OU=Sales`, `DC=ldaps1`, `DC=Example`, `DC=com`
Generic Search Attribute	Specify any LDAP property for user configuration mapping	Example values include: Common Name (`cn`), `displayName`, `givenName`, `sAMAccountName`, User ID (`UID`) Use the tooltip for example usage.

Field	Description	Valid values and notes
Generic Search Filter	Specify the query that will be used for performing LDAP search	Basic prefix logical operators (&, |, !) can be used. SecureTransport allows referencing the following values by replacing them: • %s – Complete email address. (SecureTransport replaces %s in the value with the complete email address). • %u – User name. (SecureTransport replaces %u with the user name.). • %keyFromPlugin – (It will be replaced with the value of "keyFromPlugin" coming from the plugin context). Use the tooltip to see the correct query syntax and the accepted values.

Once you are done, click **Save**.

Note The Generic LDAP search filter can access the Plugin Context, part of the `PluginUserData` object.
Values from this plugin context are accessible using the syntax as in the following example: `(mail=%subjectAltNameEmail)`.
As `subjectAltNameEmail` is the key and if its value is "someemail@mail.com" the generic search filter evaluates to `mail=someemail@mail.com`

The following topics provide basic prefix logical operators, attribute names, search filter operators, special characters in search filters, special values, and LDAP configuration example using the Alias Query filter:

- *Basic prefix logical operators* on page 435
- *Attribute names* on page 436
- *Search filter operators* on page 437
- *Special characters in search filters* on page 437
- *Special values* on page 438
- *LDAP configuration using the Alias Query filter* on page 438

Basic prefix logical operators

Operator	Symbol	Description
AND	&	All specified filters must be true for the statement to be true. For example: `(&(filter)(filter)(filter)...)`

Operator	Symbol	Description
OR	|	At least one specified filter must be true for the statement to be true. For example: `(|(filter)(filter)(filter)...)`
NOT	!	The specified statement must not be true for the statement to be true. Only one filter is affected by the NOT operator. For example: `(!(filter))`

Logical expressions are evaluated in the following order: - Innermost to outermost parenthetical expressions first - All expressions from left to right. So, you can use parentheses (and) to specify the order of operations.

For example:

The following example returns users that match attribute `objectClass` value with `Person` and attribute `cn` matches `Babs J*` where `*` means matching of zero or more characters.

```
(&(objectClass=Person)(cn=Babs J*))
```

The following example returns entries containing attribute values that do not match the specified value.

```
(!(cn=Tim Howes))
```

Attribute names

Attribute names depend on the type of LDAP server. For Active Directory servers where the standard alias attribute is `proxyAddresses` an example for the filter is `(proxyAddresses=smtp\3A%s)`. For other LDAP servers an example can be `(|(cn=%u)(mail=%s))`. This will find all users with given primary email address or common name.

Examples for attributes:

uid User ID
cn Common Name
sn Surname
l Location
ou Location
o Organization
dc Domain Component
st State
c Country

Search filter operators

Search type	Operator	Description
Equality	`=`	Returns entries containing attribute values that exactly match the specified value. For example: `cn=Bob Johnson`

Substring	`=string*string`	Returns entries containing attributes containing the specified substring.
		For example:
		`cn=Bob*`
		`cn=*Johnson`
		`cn=*John*`
		`cn=B*John`
		The asterisk (`*`) indicates zero (0) or more characters.

Greater than or equal to	`>=`	Returns entries containing attributes that are greater than or equal to the specified value. For example: `buildingname >= alpha`
Less than or equal to	`<=`	Returns entries containing attributes that are less than or equal to the specified value. For example: `buildingname <= alpha`

Presence	`=*`	Returns entries containing one or more values for the specified attribute.
		For example:
		`cn=*`
		`telephonenumber=*`
		`manager=*`

Special characters in search filters

Use backslash (`\`) followed by two hexadecimal digits to specify any special character or non-ASCII UTF-8 characters.

Special character	Value with special character	Example filter
*	Five*Star	(cn=Five\2aStar)
\	c:\File	(cn=c:\5cFile)
()	John (2nd)	(cn=John \282nd\29)
NUL	0004	(bin=\00\00\00\04)
non-ASCII UTF-8 characters		sn=Lu\c4\8di\c4\87)

Special values

SecureTransport enables to reference the following values by replacing them:

`%s` – Complete email address. (SecureTransport replaces `%s` in the value with the complete email address.)

`%u` – User name. (SecureTransport replaces `%u` with the user name.)

`%d` – Domain name. (SecureTransport replaces `%d` with the domain.)

Examples:

```
(proxyAddresses=smtp\3A%s) - proxyAddresses
```

Active Directory attribute must be smtp: followed by the email address.

```
(proxyAddresses=smtp:testuser@domain.com) (|(cn=%u)(mail=%s))
```

Either the cn attribute is the user name or the mail attribute is the email address.

```
(|(cn=testuser)(mail=testuser@domain.com))
```

LDAP configuration using the Alias Query filter

1. Enable `Login by Email` in the *LDAP User Settings* pane on the *LDAP Domain Settings* page.
2. For two LDAP users a1 and b1, having the same settings, add new LDAP attributes:
   - For user a1 add attribute: `mobile = a1@st1.lab.sofi.axway.int`
   - For user b1 add attribute: `mail = b1@st1.lab.sofi.axway.int`
3. The users exist on same domain in SecureTransport. So, create two new attributes in the *Attributes List* section on the *LDAP Domain Settings* page and map them to the LDAP attributes:

SecureTransport attribute name	LDAP attribute name
fdxAuthByEmail	mail
fdxAuthByOwn	mobile

4. Alias Queries examples:
    - No matter what search criteria the administrator has to set in the **Alias Query** field, the LDAP user can always authenticate using his `uid` (User ID), `cn` (Common Name) and `sAMAccountName` (SAM-Account-Name) search attributes.
    - Using an `&` operation joins all filters together and all conditions should be true.
    - Using and `|` requires at least one true condition.
    - If we filter an e-mail with `%u` (username) only, the user with this attribute will be allowed to login only by providing a username. Try the following queries:
        - `(mail=%u)` - the result filter will be `(&(objectClass=Person)(mail=%u))`. User b1 has mail attribute which represents the full e-mail. So, it is different from the username (`%u`) and e-mail login for user b1 will fail.
        - `(&(mobile=%u)(mail=%u))` - the result filter will be `(&(objectClass=Person)(&(mobile=%u)(mail=%u)))`. User b1 has mail attribute and user a1 has mobile attribute different from the username, so e-mail login for users a1 and b1 will fail.
    - If we filter an e-mail with `%s` (full e-mail address) only, the user with this attribute will be allowed to login by providing both a username or a password. Try the following queries:
        - If **no query** is set, the result filter will be `(&(objectClass=Person)(mail=%s))`. The mail authentication of user a1, with only mobile attribute defined, fails, because we haven't set an e-mail login permissions for the mobile attribute in the search filter. Mail authentication for b1 is successful because by default SecureTransport searches by e-mail with filter `(mail=%s)`.
        - `(mobile=%s)` - We haven't provided additional filtering for mail attribute. The result filter will be `(&(objectClass=Person)(|(mobile=%s)(mail=%s))`. E-mail login for user b1 will be successful. In the filter we have `(mail=%s)` and user b1 have mail attribute references the full e-mail address. For user a1 we have mobile attribute which references the full e-mail address, so e-mail login for a1 will also be successful.
        - `(&(mail=%u)(mobile=%s))` - the result filter will be `(&(objectClass=Person)(&(mail=%u)(mobile=%s)))`. Mail attribute in the filter allows only username login, so e-mail authentication for user b1 which mail attribute references the full e-mail address will fail. Mobile attribute in the filter allows full e-mail authentication, so for user a1 the e-mail authentication will be successful.

- Filter with `%d` (domain name) identifies domain name:
  - `(mobile=%u@%d) equals (mobile=%s)` - the result filter will be `(&(objectClass=Person)(|(mobile=%u@%d)(mail=%s)))`. The search filter allows user a1 with mobile attribute to authenticate using the full e-mail. User b1 will be also authenticated successfully with his mail attribute.
  - `(|(mobile=%u@%d)(mail=%u))` - the result filter will be `(&(objectClass=Person)(|(mobile=%u@%d)(mail=%u)))`. The search filter allows user a1 with attribute mobile to be authenticated by full e-mail address and denies user b1 authentication with the full e-mail.
- If we have two different mail addresses for one account - for example: attribute `mail = x@a.b` and attribute `mobile = y@a.b` the login will be successful by default for `x@a.b`, unless we define the following query `(mobile=%s)`.

Note In Active Directory the `proxyAddress` is the only possible property that we can use for mail attribute (after the primary mail), so we can use filtering with the following query: `(proxyAddresses=smtp\3A%s)`.

Define LDAP user settings for a domain

SecureTransport uses these default values when the LDAP entry does not include the attribute and no mapping to the attribute is enabled in the *Default Attributes List*. For information, see *LDAP logins* on page 427.

1. If you do not have the *New LDAP Domain* page open, select **Authentication > LDAP Domains** and click the domain name in the Domains List to open the *LDAP Domain* page.

2. Under *LDAP User Settings*, complete the following fields:

Field	Description	Valid values and notes
Default GID	The value for the `fdxGid` attribute (group ID) for the LDAP user.	The default value is 10000.
Default UID	The value for the `fdxUid` attribute (user ID) for the LDAP user.	UNIX-based systems only. The default value is 10000.
Default User Shell	The value for the `fdxShell` attribute (user shell) for the LDAP user.	UNIX-based systems only. Valid user shell. The default value is `/bin/sh`.
Default User Type	The value for the `fdxUserType` attribute (user type) for the LDAP user.	`Real` or `Virtual`. The default value is `Virtual`.
Allow login by email	Controls whether the user can log in using an email address stored in the email attribute of the LDAP record.	`Enabled` or `Disabled`. The default value is `Disabled`.

3. Click **Save**.

Define attribute mappings for a domain

For information about how SecureTransport uses the default attribute mappings, see *LDAP logins* on page 427.

The session variables available depend on the attribute mappings:

- The following session variables are always available: `STSESSION_LDAP_AUTH_BY_EMAIL`, `STSESSION_LDAP_DN`, `STSESSION_LDAP_DOMAIN_ID`, and `STSESSION_LDAP_DOMAIN_NAME`.
- To enable `STSESSION_LDAP_fdxGid`, `STSESSION_LDAP_fdxHomeDir`, `STSESSION_LDAP_fdxShell`, `STSESSION_LDAP_fdxUid`, and `STSESSION_LDAP_fdxUserType`, select **Map to Schema** for the corresponding default attribute.
- If you do not select **Map to Schema** for any custom mappings, all LDAP attributes are mapped to session variables named `STSESSION_LDAP_DIR_` followed by the attribute name.
- If you add a custom mapping, only those attributes added with **Map to Schema** selected are mapped to session variables named `STSESSION_LDAP_DIR_` followed by the attribute name.

A multivalued LDAP attribute is mapped to several session variables. To use a multivalued LDAP variable, map it and check the SecureTransport session for the names of the session variables.

1. If you do not have the *New LDAP Domain* page open, select **Authentication > LDAP Domains** and click the domain name in the Domains List to open the *LDAP Domain* page.
2. Under *Attributes List*, for each SecureTransport attribute that will be mapped from an LDAP attribute, select **Map to Schema** to enable an attribute mapping.

You can modify a default attribute mapping.

1. Click the Edit icon ( ) in the **Edit** column.
2. Type the new value in the **LDAP Attribute Name** column.
3. Click the Save icon ( ) in the **Edit** column.

You can define a mapping for a custom LDAP attribute.

1. Click **New Attribute**.

   SecureTransport adds a line to the *Attributes List*.
2. Type the **Description**, **ST Attribute Name**, and **LDAP Attribute Name**.
3. Click the Save icon ( ) in the **Edit** column.
4. Select **Map to Schema** to enable the mapping.

To delete a custom attribute mapping, click **X** in the first column of the table.

Manage DN filters for a domain

SecureTransport uses DN filters to accept users with matching DNs. For details, see *LDAP logins* on page 427.

Manage DN filters

The following topics describe how to manage DN filters:

- *Add a DN filter* on page 442
- *Enable or disable a DN filter* on page 443
- *Edit a DN filter* on page 443
- *Delete a DN filter* on page 443

Add a DN filter

Use the following procedure to add a DN filter.

1. If you do not have the *New LDAP Domain* page open, select **Authentication > LDAP Domains** and click the domain name in the Domains List to open the *LDAP Domain* page.
2. Under *DN Filter List*, click **New Filter**.

   A line is added to the *DN Filters List*.

3. In the **DN Filter** field, type a regular expression to match against the DN retrieved from the LDAP database. To specify only a portion of a DN, use wild cards. For example, to allow access to users from the organization acme, enter `.*O=acme.*` in this field. For more information about regular expressions supported by SecureTransport, see *Regular expressions* on page 1035.
4. In the **User Class** field, select a user class to apply the DN filter only to users in that class or asterisk (`*`) to apply the DN filter to all users.
5. Click the Save icon ( ) in the **Edit** column.

The status of the new DN filter is Disabled.

Enable or disable a DN filter

Use the following procedure to enable or disable a DN filter.

- In the entry in the *DN Filter List*, click **Enable** or **Disable**.

  The Status column is updated.

Edit a DN filter

Use the following procedure to edit a DN filter.

1. In an entry in the *DN Filter List*, click the Edit icon ( ) in the **Edit** column.
2. Make the required changes to the fields in the entry.
3. Click the Save icon ( ) in the **Edit** column.

Delete a DN filter

Use the following procedure to delete a DN filter.

- In the entry in the *DN Filter List*, click **X** in the first column.

  The entry is removed from the list.

Define Address Book settings for a domain

For information on LDAP Address Book sources, refer to *LDAP source* on page 234.

Note The *Address Book Settings* pane is only displayed if the Address Book feature is enabled (the value of the `AddressBook.Enabled` configuration option is set to **true**).

The following topics define Address Book LDAP searches and attribute mappings for a domain:

- *Define Address Book LDAP searches for a domain* on page 444
- *Define Address Book attribute mappings for a domain* on page 444

Define Address Book LDAP searches for a domain

Use the following instructions to configure LDAP search settings for the Address Book feature.

Note All search operations performed via this source will be case insensitive and wild card searches will be supported at the end of the phrase; for example, `(|(displayName=string*)(ou=string*)(mail=string*))`.

1. If you do not have the *New LDAP Domain* page open, select **Authentication > LDAP Domains** and click **New Domain** open the *New LDAP Domain* page.
2. In the *Address Book Settings* pane under *LDAP Searches*, complete the following fields:

Field	Description	Valid values and notes
Base DN	Define the base DN for the searches	A valid DN, such as, `OU=Sales,DC=ldaps1,DC=Example,DC=com`

Additional search query	Enter an LDAP query to specify the selection criteria for Address Book.
	The search behavior depends on the current selection of the **Use only additional search query** checkbox:
	• If selected, SecureTransport executes the exact search query entered in the **Additional search query** field.
	• If not selected, SecureTransport applies pre-defined filters that manage the LDAP server responses to the search query, entered in the **Additional search query** field, and executes the final query.
		Get all user entries with an email attribute and a surname equal to "smith":
		`&(sn=smith)(objectClass=user)(email=*)`
		Get all entries:
		`objectclass=*`

3. Click **Save**.

Define Address Book attribute mappings for a domain

Note Address Book supports only unique group names, so the LDAP server should not have two group entries with exact same value of the attribute which is mapped to `displayName`.

Note Address Book classifies an entry as user or group based on the `objectClass` and `objectCategory` attribute values.

To map an Address Book attribute to a schema:

1. If you do not have the *New LDAP Domain* page open, select **Authentication > LDAP Domains** and click **New Domain** open the *New LDAP Domain* page.
2. Under *Address Book Attributes List*, for each Address Book attribute that will be mapped from an LDAP domain attribute, select **Map to Schema** to enable an attribute mapping.

You can modify a default attribute mapping.

1. Click the Edit icon ( ) in the **Edit** column.
2. Type the new value in the **LDAP Attribute Name** column.
3. Click the Save icon ( ) in the **Edit** column.

You can define a mapping for a custom Address Book attribute.

1. Click **New Attribute**.

   SecureTransport adds a line to the *Attributes List*.
2. Type the **Description**, **Entity Attribute Name**, and **LDAP Attribute Name**.
3. Click the Save icon ( ) in the **Edit** column.
4. Select **Map to Schema** to enable the mapping.

To delete a custom attribute mapping, click **X** in the first column of the table.

Edit a domain

Use the following procedure to edit a LDAP domain.

1. Select **Authentication > LDAP Domains**.

   The *LDAP Domains* page is displayed.
2. Click the domain name in the Domains List.

   The *LDAP Domain* page is displayed.
3. Make the required changes.
4. Click **Save**.

Delete domains

Use the following procedure to delete domains.

1. Select **Authentication > LDAP Domains**.

   The *LDAP Domains* page is displayed.
2. Select the domains to delete in first column of the Domains List.
3. Click **Delete**.

4. Confirm the deletion.

   The selected domains are removed from the Domains List.

Configure default domains

For information about how SecureTransport uses the default domains, see *LDAP logins* on page 427.

1. Select **Authentication > LDAP Domains**.

   The *LDAP Domains* page is displayed.

2. Click **Change Defaults**.

   The Default column is displayed.

3. Click **Toggle** in the Default column to add a domain to or remove a domain from the default domains.

   The default domains are moved to the top of the Domains List and indicated in the Domain Name column.

4. If you specify two ore more default domains, up and down arrows are displayed in a column before the Domain Name column.

5. Using the arrows, you can drag the default domain rows in the Domains List to the order you want SecureTransport to search the domains.

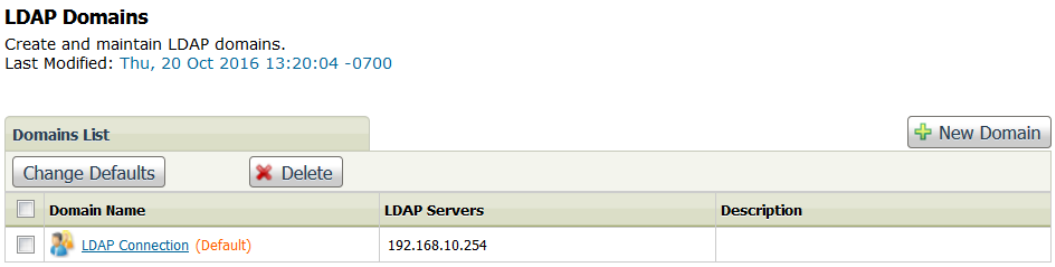
6. When the default domains are correct, click **Save Defaults**.

   The Default column and arrow columns are removed.

LDAP domains example

This example illustrates a scenario with three LDAP domains, one each for Engineering, Operations, and Security. The configuration has the following features:

- Each domain has a primary LDAP server and backup LDAP server.
- The Engineering and Operations domains are default domains. Users with login credentials in those LDAP databases do not need to specify a domain to log in.
- The Engineering domain is searched first. Users who have the same login credentials in both the Engineering and Operations domain will get the attributes stored in the entry in the Engineering domain unless they specify the Operations domain when they log in.
- The Security domain is not a default domain. Users with login credentials in the Security domain LDAP database must specify a domain name to log in.



Secure LDAP

For secure communication between SecureTransport and an LDAP server to work correctly, a trust must be established between the two parties.

When **Verify Certificate Chain** is selected, SecureTransport must trust the CA certificates used to sign the LDAP servers' certificate for encrypted connections. You must add these certificates to the SecureTransport trusted certificate store. For more information, see *Import a local certificate* on page 59.

SSL and TLS support have the following limitations based on the SSL protocol and TLS LDAP server implementation:

- SecureTransport cannot connect to the i-Planet Directory Server, v5.0 using TLS. SecureTransport fails to connect after a few minutes, displays an error message in the client , and makes an entry in its server log.
- The OpenLDAP server might incorrectly report an error when closing a TLS connection. The TLS connection closes properly even though the error is reported.

LDAP and Active Directory configuration

If you use LDAP with Active Directory, you must consider the following requirements for the LDAP server configuration in SecureTransport:

- Under LDAP Searches:
    - Specify a CN value in the **Base DN** field (for example, `cn=users`). The CN value is required for SecureTransport LDAP authentication to work, even though the OpenLDAP `ldapsearch` command generically does not require it when run from a command line interface.
    - Select **Common Name (cn)** or **SAM-Account-Name (sAMAccountName)** for the **Search Attribute**. Use the SAM-Account-Name parameter instead of the CN parameter to log in using the Windows domain login name.
- TLS is only supported in Windows Server 2003 Active Directory or later.
- Disable **Anonymous Binds**.

LDAP home folders

You can define entries in the *Home Folder* page that SecureTransport uses to set the home folder (`fdxHomeDir` attribute) for an LDAP user when the attribute is not set by the other actions listed in *LDAP logins* on page 427. If there is an entry for the user's user class or for all users, SecureTransport uses the configured prefix. For example, if the prefix is `/home/users/partners` and the user name is `suplco`, SecureTransport set the home folder to `/home/users/partners/suplco`.

When SecureTransport is running under Windows, you can use a local file path, such as `D:\home\users\partners` or a UNC path for a share such as `\\NAS2\home\users\partners`. The permissions for the share must permit the SecureTransport Administration Tool service, which runs on Windows with a local system user as its owner, to create the folder. If the permissions granted for the share are not sufficient to create the subfolder for the LDAP user's home folder, SecureTransport refuses the connection.

Note Because operating systems do not accept angle brackets (`< >`) and quotation marks (`"`) in file names, LDAP users with any of those characters in their user name cannot log in to SecureTransport and get a default home directory. You must map such users to a properly configured account template.

You can define a user class based on values from the LDAP entry. See *User classes* on page 710.

If there is no entry for the user class, SecureTransport uses the entry for all users indicated by an asterisk (`*`) in the **User Class** field.

For more information about how SecureTransport uses the entries on the *Home Folder* page during LDAP logins, see *LDAP logins* on page 427 In particular, if there is an applicable account template, the home folder defined in the account template replaces any home folder set from configuration on the *Home Folders* page.

The following topics describe managing LDAP home folders:

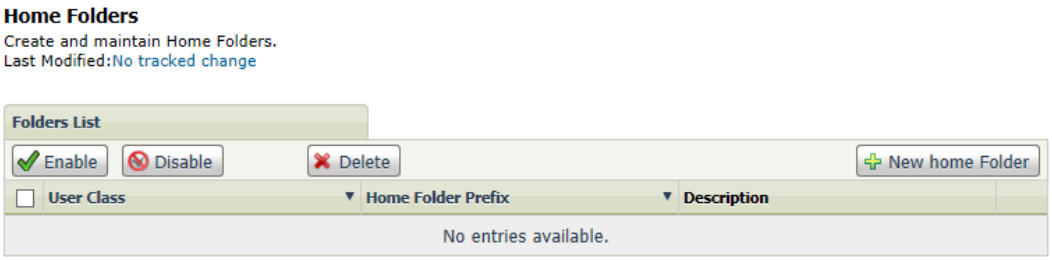
- *Create a home folder entry* on page 448 - Provides how-to instructions for creating a home folder entry.
- *Enable or disable home folder entries* on page 449 - Provides how-to instructions for enabling or disabling home folder entries.
- *Edit a home folder entry* on page 449 - Provides how-to instructions for editing a home folder entry.
- *Delete home folder entries* on page 449 - Provide how-to instructions for deleting home folder entries.

Create a home folder entry

Use the following procedure to create a home folder entry.

1. Select **Authentication > Home Folders**.

   The *Home Folders* page is displayed.



2. Click **New home Folder**.

   A line is added to the *Folders List*.

3. In the **User Class** field, select a user class to apply the home folder prefix only to users in that class or asterisk (*) to apply the home folder prefix to all users.
4. In the **Home Folder Prefix** field, type the path name for the prefix.
5. In the description field, type any notes you want to record about the entry.
6. Click the Save icon ( ) in the **Edit** column.

The status of the new entry is disabled.

Enable or disable home folder entries

Use the following procedure to enable or disable home folder entries.

1. In the first column of the *Folders List*, select the entries to change.
2. Click **Enable** or **Disable**.

   The status icon in the **User Class** column is updated.

Edit a home folder entry

Use the following procedure to edit a home folder entry.

1. In an entry in the *Folders List*, click the Edit icon ( ) in the **Edit** column.
2. Make the required changes to the fields in the entry.
3. Click the Save icon ( ) in the **Edit** column.

Delete home folder entries

Use the following procedure to delete home folder entries.

1. In the first column of the *Folders List*, select the entries to delete.
2. Click **Delete**.
3. Confirm the deletion.

   The entries are removed from the list.

LDAP user type ranges

On UNIX-based systems, you can define entries in the *User Type Ranges* page that SecureTransport uses to set the user type for an LDAP user when the user type is not set by the other actions listed in *LDAP logins* on page 427. You specify a range of values for the user ID (UID) and the user type for SecureTransport to assign to users with values in that range. Every LDAP user on a UNIX-based system has a user ID. See *LDAP logins* on page 427 for the actions that set the user ID.

The following topics provide how-to instructions for managing LDAP user type ranges:

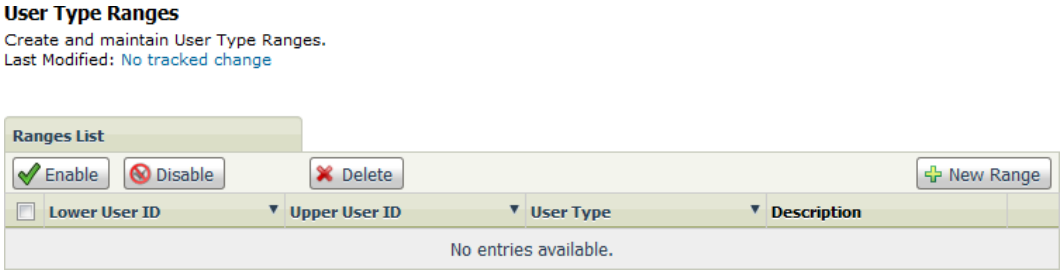
- *Create a user type range entry* on page 450 - Provides how-to instructions for creating a user type range entry.
- *Enable or disable user type range entries* on page 451 - Provides how-to instructions for enabling or disabling user type range entries.
- *Edit a user type range entry* on page 451 - Provides how-to instructions for editing a user type range entry.
- *Delete user type range entries* on page 451 - Provides how-to instructions for deleting user type range entries.

Create a user type range entry

Use the following procedure to create a user type range entry.

1. Select **Authentication > User Type Ranges**.

   The *User Type Ranges* page is displayed.

2. Click **New Range**.

   A line is added to the *Ranges List*.

3. Type the **Lower User ID** and the **Upper User ID**.
4. Select a **User Type**.
5. Click the Save icon ( ) in the **Edit** column.

   The entry is added to the to the *Ranges List*.

The status of the new entry is disabled.

Enable or disable user type range entries

Use the following procedure to enable or disable user type range entries.

1. In the first column of the *Ranges List*, select the entries to change.
2. Click **Enable** or **Disable**.

   The status icon in the **Lower User ID** column is updated.

Edit a user type range entry

Use the following procedure to edit a user type range entry.

1. In an entry in the *Ranges List*, click the Edit icon ( ) in the **Edit** column.
2. Make the required changes to the fields in the entry.
3. Click the Save icon ( ) in the **Edit** column.

Delete user type range entries

Use the following procedure to delete user type range entries.

1. In the first column of the *Ranges List*, select the entries to delete.
2. Click **Delete**.
3. Confirm the deletion.

   The entries are removed from the list.

Manage accounts 9

Use the pages of the **Accounts** menu to create and manage login accounts for users, administrators and partners.

Note Accounts and routes managed by Central Governance should be indicated as such in the User Account Notes. Accounts and routes managed by Central Governance are highlighted with the following message: **Managed by Central Governance.**

Note In order for login by email to function properly, all user accounts must be assigned unique email addresses. Additionally, the client password reset feature will not work if emails assigned to users accounts are not unique.

The following topics provide additional account management information:

- *Accounts overview* on page 452
- *User accounts* on page 453
- *User certificates* on page 476
- *Transfer sites* on page 494
- *Transfer profiles* on page 600
- *Subscriptions* on page 603
- *Manage service accounts* on page 621
- *Duplicate an account* on page 622
- *Control login name case sensitivity* on page 623
- *Configure a secret question* on page 627

Accounts overview

An Axway SecureTransport *account* contains information about a user or an internal system that processes SecureTransport file transfers. SecureTransport supports two kinds of accounts: *user* and *service*.

The following topics describe user and services accounts. They also describe user account subscriptions, transfer sites, certificates, and applications.

- *User accounts* on page 453
- *Service accounts* on page 453
- *Subscriptions, transfer sites, and certificates* on page 453
- *Applications* on page 453

User accounts

A *user account* is typically external to your enterprise. A user account consists of settings such as the account name, contact information, login information, *subscription* information (the *applications* this user account uses to process file transfers), *transfer site* information, and *certificate* information. User accounts connect to SecureTransport through subscriptions to one or more applications. For details, see *User accounts* on page 453.

Service accounts

A *service account* is typically used to represent processes on systems internal to your enterprise. It consists of settings, transfer site information and certificate information. Instead of subscribing to an application, however, a service account uses a *connector* to connect to one or more applications. For details, see *Manage service accounts* on page 621.

Subscriptions, transfer sites, and certificates

A subscription defines how files are submitted to and received from applications. For details, see *Manage subscriptions* on page 607.

A transfer site is a location such as a local folder or protocol server used by SecureTransport to pull data from or send data to during a transfer. For details, see *Transfer sites* on page 494.

A certificate can be one of three types: login, partner, or private. Each certificate type can be used by the account for different purposes. For details, see *Manage certificates* on page 476.

Applications

An application is an instance of an *application type*. An application type is a workflow definition that is triggered by either data arrival or a scheduled event. An application is created when you configure an application type, name it and save it. For more information, see *Applications* on page 756.

User accounts

Use the *User Accounts* page to display, create, modify, and delete user accounts.

The following topics describe managing user accounts:

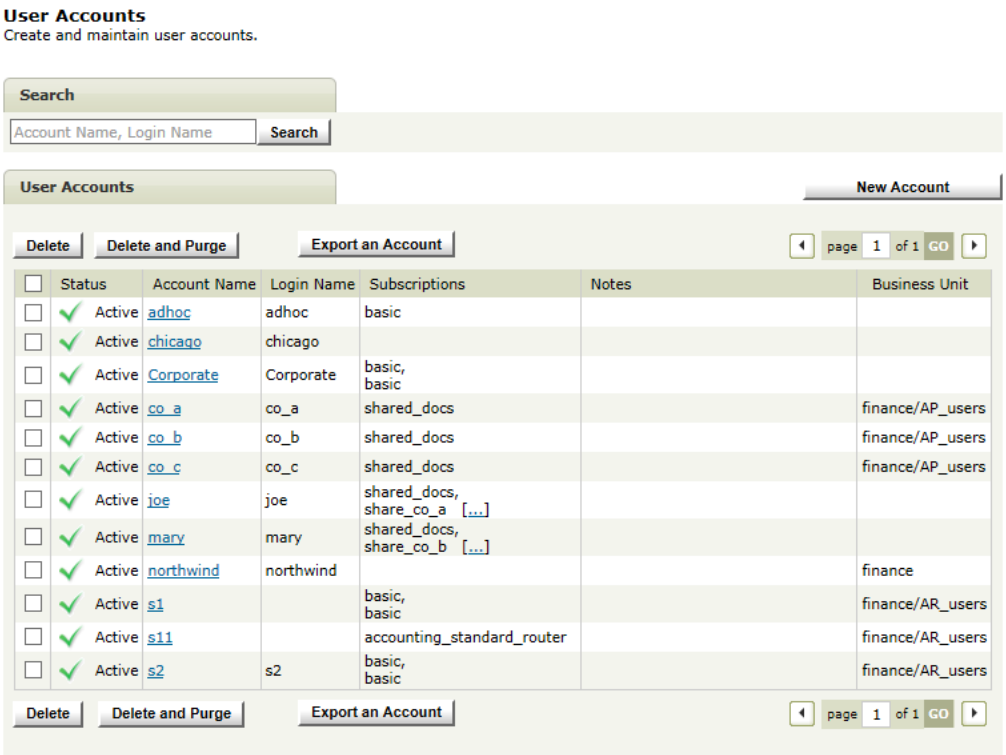
- *Display the list of user accounts* on page 454
- *Create a user account* on page 456
- *Web password compatibility* on page 465
- *View account settings* on page 465
- *Change how long user account information is cached in memory* on page 466

- *Disable or enable a user account* on page 466.
- *Lock or unlock a user account* on page 466
- *Expire a user account password* on page 467
- *Change a user account password* on page 467
- *Edit user account settings* on page 468 .
- *Delete user accounts* on page 470
- *Delete and purge a user account* on page 470
- *Export a single user account* on page 470
- *Unlicensed users* on page 471
- *Protected folders and accounts* on page 475

Display the list of user accounts

The *User Accounts* allows you to view a list of all user accounts or search the list based on account name or login name.

- Select **Accounts > User Accounts**. The *User Accounts* page is displayed.



The *User Accounts* page lists 100 account entries per page by default.

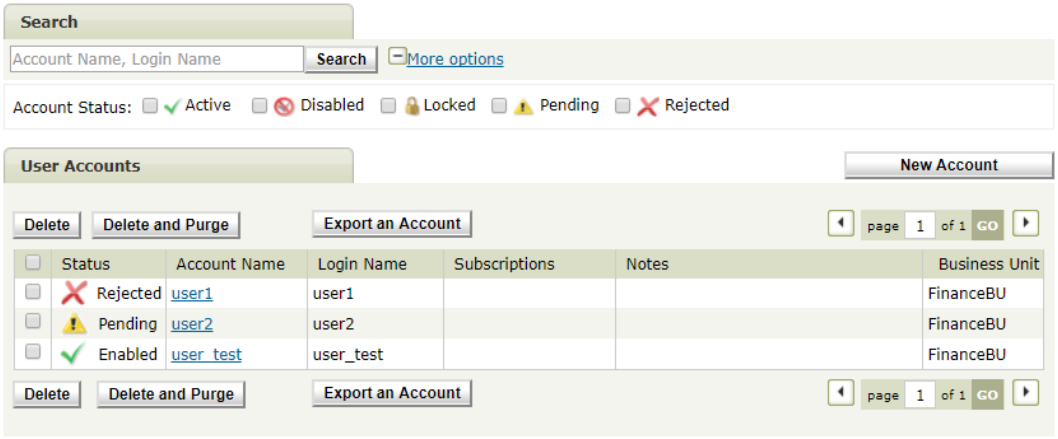
Note You can change the default number of records per page by editing the `LinesPerPage` parameter in the file `<FILEDRIVEHOME>/tomcat/admin/webapps/coreadmin/WEB-INF/web.xml`.

Search for a user account

You can search the user accounts database and display the results on the *User Accounts* page.

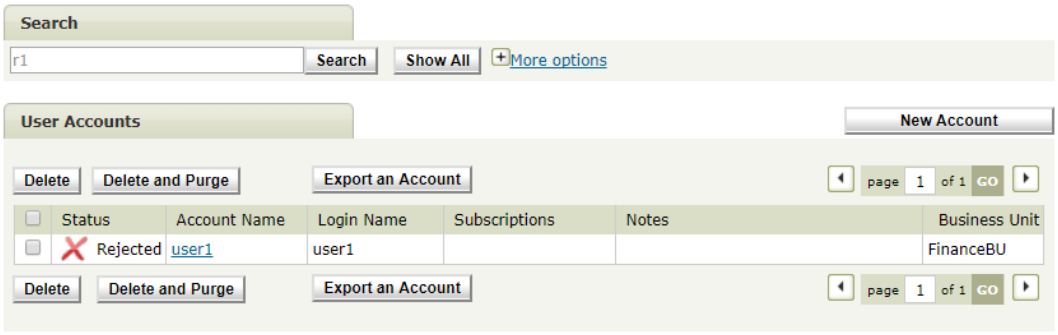
1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. In the *Search* pane, type all or part of a user account name and click **Search**. Wildcards are not accepted.

   The search results are displayed on the *User Accounts* page.



3. (Optional) Click **More Options** to expand the Search panel with Account status checkboxes as additional search filters.
   Note that the **Pending** and **Rejected** account statuses are introduced as part of the Maker-Checker flow.
4. (Optional) Narrow your list of search results. In the *Search* pane, append or prepend your search string.

   For example, adding the string "1" to the end of the search string "s" in the previous example yields the following result.



After you perform a search, the **Show All** button is displayed.

5. To display all accounts, click **Show All**.

Create a user account

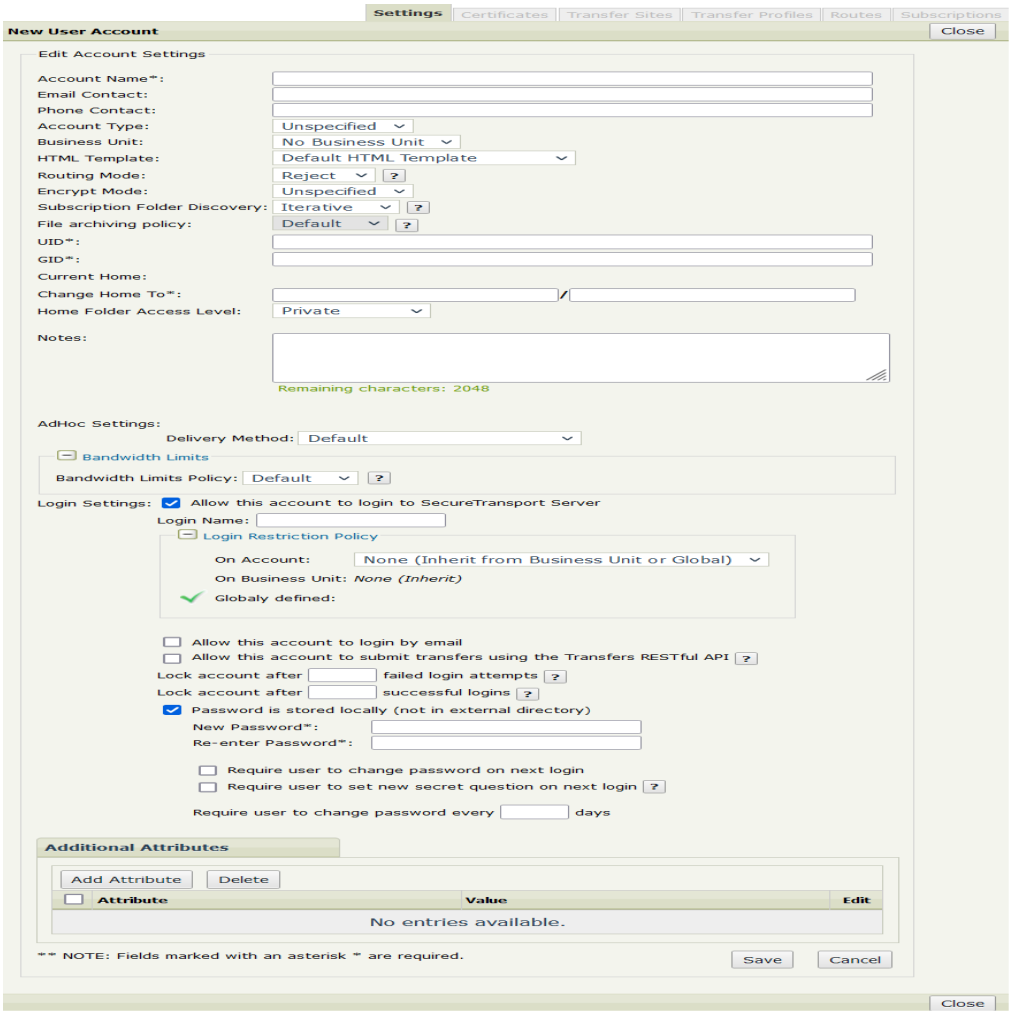
Note In order for login by email to function properly, all user accounts must be assigned unique email addresses. Additionally, the client password reset feature will not work if emails assigned to users accounts are not unique.

You can create new user accounts using the Administration Tool.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click **New Account**.

   The *Settings* pane of the *New User Account* page is displayed.

Note The *Address Book Settings* are only displayed if the Address Book feature is enabled (the value of the `AddressBook.Enabled` configuration option is set to **true**).



Note When you create a user account, all the tabs except **Settings** are disabled.

3. Type the **Account Name**. The name of the account must be unique for the system. If an account already exists with the name you specify, SecureTransport prompts you to enter another name. This field is mandatory. Account Names cannot contain more than 80 characters. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields on page 464*.
4. Enter a valid **Email Contact**.

   When this email address is the recipient of an ad hoc file transfer email sent from ST Web Client or one of the Axway Email Plug-ins, SecureTransport determines that this user is the recipient. If the user is allowed to log in by email, this is the value used in the **User Name** field of the login page.
5. Enter a valid **Phone Contact**.
6. Select an **Account Type**. Use this parameter to differentiate between accounts that transfer files internally and those that transfer files between partners. Choose from the following:
   - **Unspecified** – Default value. All accounts created using versions of SecureTransport that do not have this option have this value.
   - **Internal** – Transfers for this account occur within a single organization.
   - **Partner** – Transfers for this account occur between organizations
7. Select a **Business Unit**. The default setting is No Business Unit.
8. Select the **HTML Template** that SecureTransport displays when the user logs in to the SecureTransport web client.

   Note If you select the default HTML template, the SecureTransport web client uses whatever template is specified on *Miscellaneous Options* page.
9. Select a **Routing Mode**.

   This field controls how SecureTransport behaves when it is the intermediate partner in a PeSIT transfer directed to this account and the transfer cannot be completed because no transfer site matches the routing destination and the account has no PeSIT default site.
   - **Reject** (default) – A PeSIT transfer that cannot be routed is rejected before it starts.
   - **Accept** – A PeSIT transfer that cannot be routed is performed and the file is retained locally.
   - **Ignore** – A PeSIT transfer that cannot be routed is ignored.
10. Select **Encrypt Mode**.

    This field can enable repository encryption for this user.
    - **Unspecified** (default) – Repository encryption is enabled based on the `EncryptClass` user class evaluation.
    - **Enabled** – Repository encryption is enabled for this user account.
11. Select **Subscription Folder Discovery**.

    This field determines the subscription folder discovery mode. For accounts with multiple subscriptions, the number of subscriptions and the target folder depth may impact performance.

- **Iterable** (default): Subscription folder discovery is performed by iteration over all of the account's subscriptions while trying to match the target folder.
  Tip: choose this mode when the number of subscriptions is small and the target folder depth is large.
- **Recursive**: Subscription folder discovery is performed by recursive traversal of the target folder hierarchy - the target folder is checked first and if no match is found, then its parent folder is checked. The process continues until a match is found or there are no more folders to check.
  Tip: choose this mode when the number of subscriptions is large and the target folder depth is shallow.

12. Select **File archiving policy**.

    This field determines the file archiving policy.

    - When **Default** is selected, then the following apply:
      1. If the account is assigned to a business unit, it will inherit its policy.
      2. Otherwise, the global archiving policy applies.
    - When **Enabled** is selected, file archiving will be enabled for this account.
    - When **Disabled** is selected, file archiving will be disabled for this account.

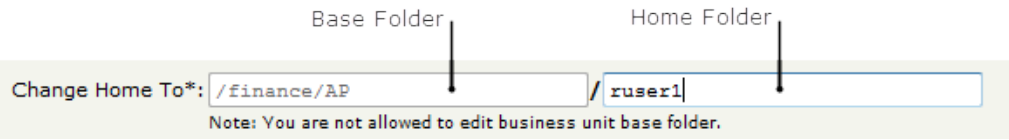
      Note If the global file archiving policy is disabled, or if this account is assigned to a business unit with **Allow File Archiving Policy modifying** unchecked, then this option cannot be modified.

13. Type the numeric user ID of the user in the **UID** field. This field is mandatory on UNIX and Linux platforms. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

    On Windows platforms, this field is named **Real User** and is optional.

14. Type the numeric group ID for the user account in the **GID** field. The account uses the system access rights and privileges valid for this user group on the system. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

15. Enter a valid home folder in the **Change Home To** field for the account as an absolute path. SecureTransport validates the directory path you specify and prompts you for a new path if necessary. This field is mandatory. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.



Add a base folder path in the field to the left of the forward slash (`/`) and add the home folder in the field to the right of it. You can add multiple levels, such as `/home/dev3/test`, but the parent directories must be typed in the field to the left of the slash. Only the final child directory should be in the field to the right of the slash. When you select a business unit, a base folder for

the business unit is automatically added. The base folder must be the business unit base folder. You cannot change the base folder for a user account if a business unit is selected unless the business unit has the option **Allow Base Folder modifying** selected.

Although you can use the / when adding parent directories to a home folder, you cannot use the following characters in the home folder name: * < > ? " / \ | :

Note If you change the home folder when editing a user account, any subscription folders the account has are reinitialized. In other words, the subscription folders are created again under the new home folder of the account. None of the other folders created by the user will be moved and the user will no longer have access to them. This also happens if the user is moved from one Business Unit to another.

Note For SecureTransport on Windows, you can create a home folder for an account in a UNC format, pointing to a local or a remotely shared folder over the network.

Note On Windows, when a network share is used as a home folder for an account, you must manually create a directory with proper access settings. SecureTransport cannot create the home folder because the SecureTransport services run on Windows as service accounts with a local system user as its owner. You must either use SecureTransport impersonation functionality or use permissions sufficient for the network share to be accessed by local system users. For more information, refer to *Real users on Windows* on page 688.

Note Transaction Manager agents must use the Windows impersonation functionality (mapping virtual users to real users) as needed to access directories on a network share (that is, directories in UNC format or on mapped drives. paths.

16. Select **Access Level**. The home folder access level determines whether and which other accounts are able to publish to the home folder of the current account.
    - **Private** – The access level is private. Only the current account is able to publish files to its home folder.
    - **Business Unit** – Account home folder access is limited to the account's business unit. The current account and all accounts in the current account's business unit can publish to this account's home folder.
    - **Public** – Access to the account is public. All accounts are able to publish to this account's home folder.

      Note Access level is applicable only when Advanced Routing feature is used. For more information see *Advanced Routing* on page 795.

17. Enter a text description of the user account in the **Notes** field.

18. The **Delivery Method** value controls the options that ST Web Client displays in the *User Access* window.
    - **Disabled** – The user cannot send files using ad hoc file transfers.
    - **Default** – Use the delivery method specified in the account template, if any, or in the **Default Package Delivery Method** field of the *AdHoc Setting* page.
    - **Anonymous** – The sender can choose **Send attachment link only** or **Protect attachment link with security question**.
    - **Account Without Enrollment** – The sender can choose **Send attachment link only**, **Protect attachment link with security question**, or **Send to existing users only**.
    - **Account With Enrollment** – The sender can choose **Send attachment link only**, **Protect attachment link with security question**, **Send to existing users only**, **Allow recipients to enroll as restricted users (receive and reply to messages only)**, or **Allow recipients to enroll as unrestricted users**. (Elsewhere the Administration Tool refers to restricted users as unlicensed users and unrestricted users as licensed users.)
    - **Custom** – Select the allowed enrollment types in the **Enrollment Types** field. The sender can chose any of the selected enrollment types.
19. For a custom delivery method, select one or more allowed enrollment types in the **Enrollment Types** field:
    - **Anonymous** – The ad hoc file recipient receives a link to retrieve the files and is not enrolled as a user. The ST Web Client option is **Send attachment link only**.
    - **Challenge** – The ad hoc file recipient receives a link and must answer correctly a challenge question specified by the sender to retrieve the files. The recipient is not enrolled as a user. The ST Web Client option is **Protect attachment link with security question**.
    - **Existing Account** – Do not enroll ad hoc file recipients. Only existing users can receive files. The ST Web Client option is **Send to existing users only**.
    - **Enroll Unlicensed** – If the ad hoc file recipient does not have a user account, the recipient must enroll and create an account before retrieving the files. The ad hoc file recipient becomes a restricted user who can only reply once to the email and retrieve the files. Other user attributes are defined by the enrollment template. The ST Web Client option is **Allow recipients to enroll as restricted users (receive and reply to messages only)**.
    - **Enroll Licensed** – If the ad hoc file recipient does not have a user account, the recipient must enroll and create an account before retrieving the files. The ad hoc file recipient becomes a SecureTransport user with all the attributes specified in the default enrollment template. The ST Web Client option is **Allow recipients to enroll as unrestricted users**.
20. In the *Ad-Hoc settings* area: when the value of the **Delivery Method** field is not **Default**, the **Implicit Enrollment Type** value controls which option ST Web Client selects initially in the *User Access* window and which enrollment type is used by the Axway Email Plug-ins. The choices

depend on the enrollment types enabled by the **Delivery Methods** and **Enrollment Types** fields. **Challenge** is not an option because the Axway Email Plug-in do not include the challenge question and answer function.

21. (Optional) When the Address Book feature is enabled, the *Address Book Settings* are displayed. To configure the user account Address Book settings:
    a. Select the Address Book source.
        - **Default** - The account inherits either its business unit Address Book policy or the global Address Book policy.
        - **Custom** - A custom Address Book policy configuration will be set for this account only and the following will be configurable:
            1. Enable or disable Address Book sources for the account.
            2. Specify the parent groups for Address Book sources.
            3. Specify the domain for LDAP Address Book sources.
            4. Specify **All Business Units** or **User's own business unit** for local and custom Address Book sources.
        - **Disabled** - The Address Book policy is set to disabled for this account.
    b. Specify whether or not to allow collaboration with non-Address Book recipients. If Address Book functionality is disabled, this setting does not affect user collaboration.
        - When **checked**, the account will be allowed to send email packages and share folders with users that do not exist in the defined Address Book.
        - When **unchecked**, the account will be allowed to send email packages and share folders only with users that exist in the defined Address Book.

        This account setting overrides the business unit or global Address Book Policy setting for collaboration.

    For additional Address Book account level configuration information, refer to *Address Book account level configuration* on page 240.
22. In the *Bandwidth limits* pane select a **Bandwidth Limits Policy** to apply:

- Default – the current user account inherits their bandwidth limits from the parent business unit or the global bandwidth
- Custom – the panel expands with two additional options for you to configure: **Inbound limit** and **Outbound limit** (both values in kb/s per user)
- Disabled – no bandwidth limits are applied to the users assigned to the current business unit

23. In the *Login Settings* area: select **Allow this account to log in to SecureTransport Server** to allow the new account to log in to SecureTransport. This setting is enabled by default. Disabling the option restricts access of this account to the SecureTransport Server. If you enable this option, the following options are enabled.
    a. Enter a **Login Name** for the account. This is the unique name with which the account is identified by the SecureTransport Server. Login names cannot contain the following characters: +, :, or [. Login Names cannot start with the following character: *.

b. Select the **Login Restriction Policy**. The Login Restriction Policy defines rules for allow or deny login to users based on the client IP or host and other conditions. For additional information, refer to *Login restrictions* on page 747.

   If a Login Restriction Policy is selected as the global default policy, it will be the inherited default selection for the user account.

   If a Login Restriction Policy is not selected as the global default policy and the Business Unit has a Login Restriction Policy selected, it will be the inherited default selection for the user account.

   If neither a global default Login Restriction Policy or a Business Unit Login Restriction Policy is selected, then the policy selected for the users account will be in effect.

   Note The default inherited Login Restriction Policy can be overridden by selecting a Login Restriction Policy from **On Account**.

c. Select **Allow this account to login by email** to allow the user to log in using with the value of the **Email Contact** field as well as the **Login Name**.

   Note A user of one of the Axway Email Plug-ins must either have **Allow this account to login by email** selected or have the identical values in the **Email Contact** field and the **Login Name** field.

d. Select **Allow this account to submit transfers using the Transfers RESTful API** to enable calls from the SecureTransport REST file transfer API authenticated with the credentials from this account. When this option is selected, the account will be allowed to trigger server initiated transfers using the Transfers RESTful API resource and retrieve the tracking information for these transfers.

e. Select **Password is stored locally (not in external directory)** to store the password locally in the system. SecureTransport stores the passwords of real, LDAP, SiteMinder, and SSO users in an external directory, and the passwords of virtual users are stored in the SecureTransport database.

   Note The **Password is stored locally (not in external directory)** option can only be used for a user account that has a virtual user associated with it. If the user associated with the account is a real, LDAP, SiteMinder, or SSO user, then the password cannot be stored locally in the database and this option is unusable.

f. Enter a **New Password** for the account.

g. **Re-enter Password** for the account.

h. Select **Require user to change password on next login** to require the user to change their password on the next login.

i. Select **Require user to set new secret question on next login** to require the user to select and answer a new secret question. When this option is selected, the user must select and answer a new secret question on their next login. For information on configuring the secret question feature, refer to *Configure a secret question* on page 627.

j. Complete the **Require user to change password every X days** field to require the user to change their password every specified number of days. If the number of days is unspecified, the user will not be required to change their password every "X" number of days.

k. Complete the **Lock account after X failed login attempts** field to lock the account after the specified number of failed login attempts. If the number of login attempts is unspecified, the number of possible failed login attempts is infinite.

l. Complete the **Lock account after X successful logins** field to lock the account after the specified number of successful logins. If the number of successful logins is unspecified, the number of successful logins is infinite.

Note The `GlobalLoginThreshold` configuration option is a percentage value that will allow additional successful logins after reaching the threshold specified in the *Account* page (**Lock user after X successful logins**).

24. To add an attribute, click **Add Attribute**. For additional information on Additional Attributes, refer to *Additional attributes* on page 175.

a. Enter the attribute and value in the **Attribute** and **Value** fields.

Add Attribute enables the administrator to add custom properties (Key=Value). Also the administrator will be able to access the custom properties (named Attributes) using any field in Advanced Routing.

Some examples of Attributes are:

Attribute	Value
userVars.1	internalEmail@axway.com
userVars.2	ReportsMonitor

To access attributes, see the following examples:

```
${account.attributes['userVars.1']}
```

```
${account.attributes['userVars.2']}
```

For example, the `account.attributes` is the selector for attributes of the account used to execute the current route - it has to be written exactly as shown.

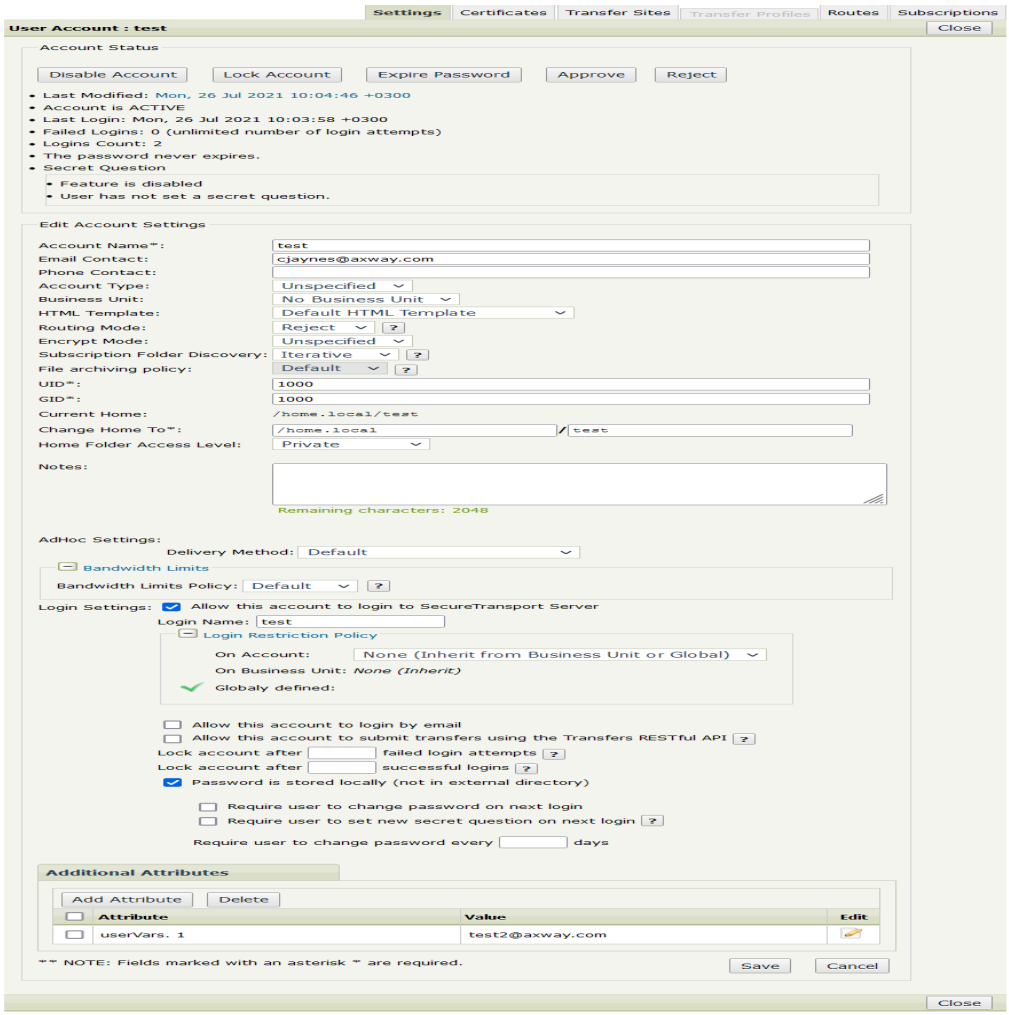
The `userVars.` prefix must be prepended to attribute name.

All this should be written as an EL expression: `${...}`

b. Click the attribute Save ( ) icon.

25. Click **Save**.

The user account information is saved and displayed in the *Settings* pane of the user account.



Once you have saved the account settings, you can select the **Subscriptions**, **Routes**, **Transfer Sites**, or **Certificates** to further define the new account. For more information, see *Manage subscriptions* on page 607, *Manage Routes* on page 812, *Transfer sites* on page 494, and *Manage certificates* on page 476.

Spaces in required fields

Some fields in SecureTransport require that you enter a value. When you enter a value in such a field, SecureTransport trims any leading or trailing spaces and then determines whether the field is empty. This means you cannot enter space-only values in required fields because those fields are treated as empty.

Maker-Checker user creation

Delegated administrators with Maker and Checker rights have two separate complementing roles:

- Maker creates the user account and submits it for approval
- Checker approves or rejects the pending user account

Create and submit user

As a Maker, you can create a user account that will remain in Pending verification status. Your user will not have access until a Checker administrator *approves* their particular account.

In order to submit the account for approval, go to **Accounts > User Accounts** and on the *Settings* tab click **Submit for approval**.

Approve user

As a Checker administrator, you can only view and approve or reject users in pending Account verification status.

If you reject a pending account, you can type in the reason for rejection.

Web password compatibility

If a user created a password that contained the plus symbol (+) while running a web client in a previous version of SecureTransport, you must change the value of the `Http.Password.Compatability.Mode` server configuration parameter to `on` to allow passwords with the + symbol.

When set to `on` this parameter allows users who previously changed their password to a string containing the plus character through a web client to log in and change their password. This option affects only the web clients. Once the password is changed, the user can log in using any client or protocol.

If you have upgraded or performed a system import, and you did not already manually change the parameter, SecureTransport sets the value set to `on` to allow legacy users with a + symbol in the password to log on without an error.

View account settings

Use the *Settings* pane to view and modify account status and settings. When an account is defined for an external authenticated user, such as an LDAP or SiteMinder user, the external UID, GID, and home folder attributes are replaced with the values taken from the account information while the external user is logged into SecureTransport.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account whose settings you want to view.

   The *Settings* pane is displayed with details for the selected account.

Change how long user account information is cached in memory

You can set how long SecureTransport keeps the user account information cached in memory by editing the `TransactionManager.AccountContextAgent.cacheTimeout` parameter on the *Server Configuration* page. The default value is `900` seconds. Change the value to keep the cached information for a longer or shorter period of time. You can also set it to null or a negative value to not cache the account information. Changes you make to an account do not show up until after the cache is refreshed.

Disable or enable a user account

Use the following procedure to disable or enable a user account.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click **Disable Account** or **Enable Account**, depending on the current status of the account.

If an account is disabled:

- Scheduled subscriptions for the account are not triggered.
- The user associated with the account cannot log in the system or perform any transfers.

Lock or unlock a user account

Use the following procedure to lock or unlock a user account.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account that you want to lock or unlock.

   The *Settings* pane is displayed with details for the selected account.
3. Click **Lock Account** or **Unlock Account**, depending on the current status of the account.

   Note An account can be locked or unlocked only if it has a user associated with it. When an account is locked, the user associated with it cannot log in to the SecureTransport Server. However, if an account is locked, server-initiated transfers associated with that account are not affected.

Accounts are locked when:

- When an administrator locks an account using the lock user account procedure.
- When the number failed login attempts exceeds the configured number of allowed attempts.

- When the number successful login attempts exceeds the configured number of successful attempts.
- When the day count exceeds the configured number of days between password changes.

Note Change password failures are counted as failed login attempts.

Expire a user account password

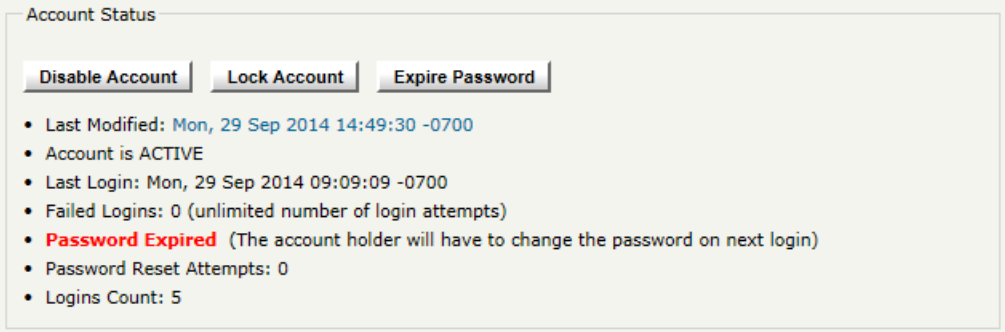
When you expire the password of an account, the user is prompted to change the password on next login. The new password must follow the password policy you configured for SecureTransport. For more information, see *Password policy* on page 185.

Note If you change the password policy of a user while that user is logged in to SecureTransport through a web client, the old password policy is displayed until the user logs out and logs in again.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account whose password you want to expire.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click **Expire Password**.

   The *User Account* page is displayed with the red text in the *Account Status* pane stating that the password is expired.



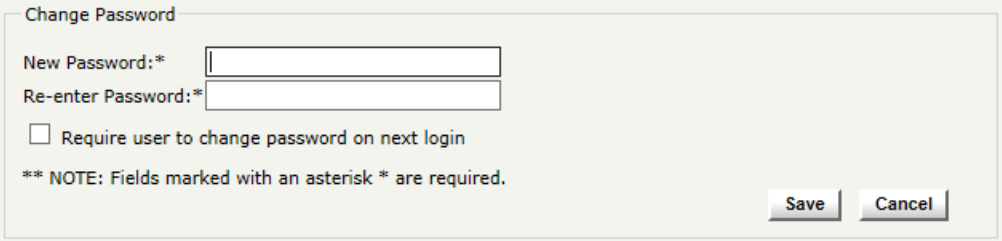
Change a user account password

Use the following procedure to change a user account password.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account whose password you want to change.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click **Change Password**.

   The *Change Password* pane is displayed.



4. Type the new password.
5. Re-type the password to confirm it.
6. (Optional) Select the **Require user to change password on next login** check box.
7. Click **Save**.

   Note Password policy restrictions apply.

Edit user account settings

Note If you are using a FireFox browser, be sure to disable the auto complete function prior to editing user account settings.

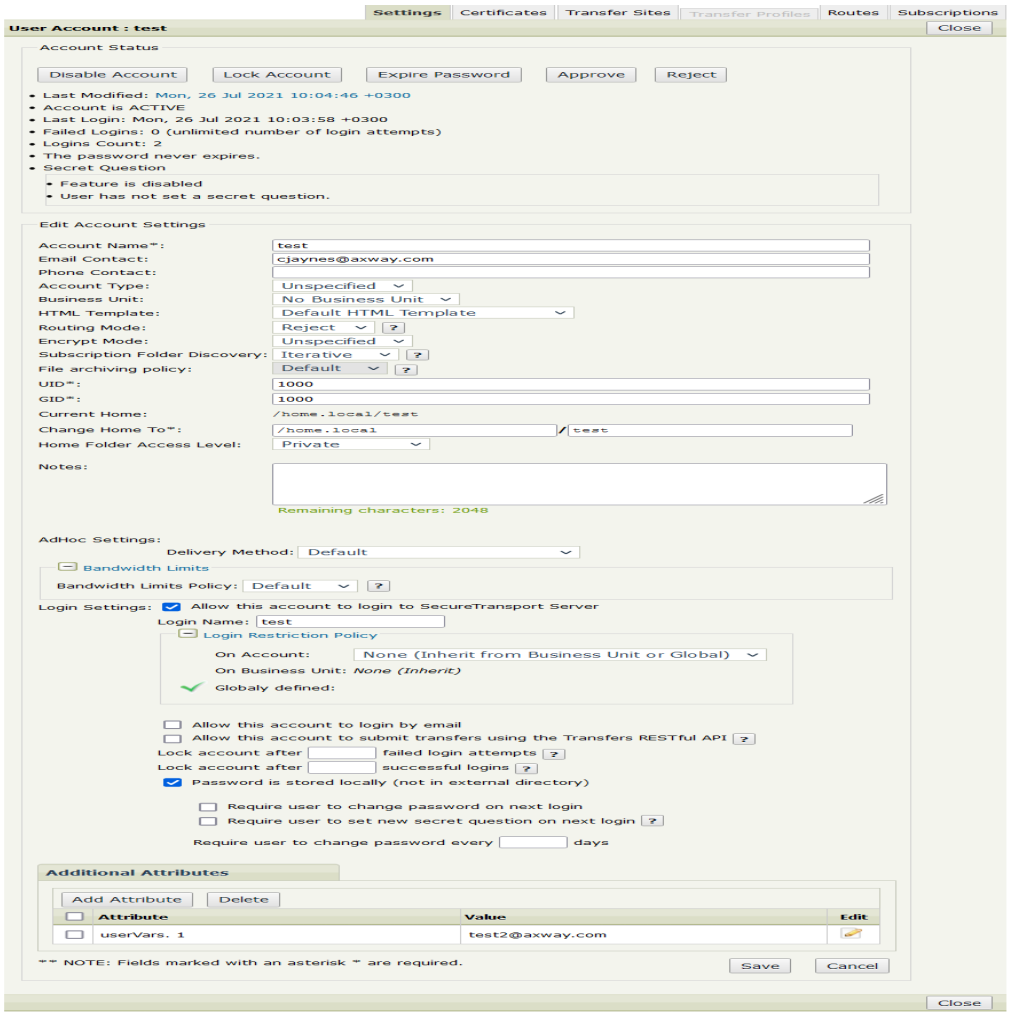
Use the following procedure to edit user account settings.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account whose settings you want to edit.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click **Edit Account Settings**.

   The *Edit Account Settings* page is displayed.

   Note The *Address Book Settings* are only displayed if the Address Book feature is enabled (the value of the `AddressBook.Enabled` configuration option is set to **true**). For Address Book account level configuration instructions, refer to *Address Book account level configuration* on page 240.



4. Edit the account settings. For information about the fields on the *Edit Accounts Settings* page, see *Create a user account* on page 456.

   Note If you change the UID or GID of an account, SecureTransport prompts you to determine whether to change the owner and group of the account's home directory and again to determine whether to change recursively the owner and group of all the subdirectories in the home directory.

5. To add attributes:

   a. Click the **Add Attribute** button.

   b. Complete the **Attribute** and **Value** fields.

   c. Click the attribute Save ( ) icon.

6. To delete an attribute or attributes:

   a. Select the attribute or attributes to delete.

   b. Click the attribute **Delete** button.

7. To edit an attribute:
    a. Select the attribute to edit.
    b. Click the attribute Edit ( ) icon.
    c. Make the desired attribute changes.
    d. Click the attribute Save ( ) icon.

Delete user accounts

When you delete a user account, all its subscriptions to applications are also deleted.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Select the check box for the user account you want to delete. You can select multiple accounts.
3. Click **Delete**. SecureTransport prompts you to confirm that you want to delete the account and informs you that any subscriptions for this account will be deleted.
4. Click **OK** to remove the account.

Delete and purge a user account

When you delete a user account, the home folder for that account is kept on the server. You can both delete the account and remove the home folder and any subdirectories by using the **Delete and Purge** button.

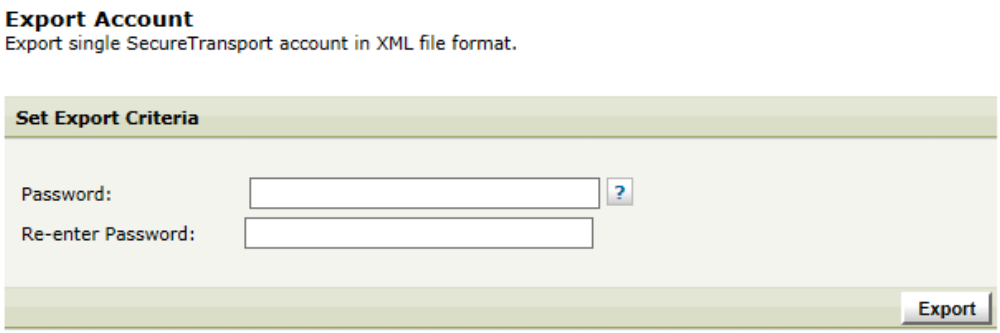
1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Select the check box for the user account you want to delete you can select multiple accounts.
3. Click **Delete and Purge**. SecureTransport prompts you to confirm that you want to delete the account and informs you that any subscriptions for this account will be deleted.
4. Click **OK** to remove the account and the home folder.

Export a single user account

You can export a single user account to an XML file.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Select the account you want to export and click **Export an Account**.

    The *Export User Account* page is displayed.



3. Type a password in the **Password** field. The password is used to confirm that an administrator is importing the correct file.
4. Retype the password in the **Re-enter Password** field.
5. Click **Export**.

   The account is exported to an XML file you can download to your local computer.

For more information, see *Account export and import* on page 631.

Unlicensed users

The recipient of an ad hoc human-to-human file transfer email or a system-to-human file transfer email does not need all SecureTransport user account functionality to retrieve the files. If the recipient does not need other SecureTransport functionality, the recipient can be an unlicensed user. As the name implies, unlicensed users do not require an account license to connect to SecureTransport to retrieve or reply to messages.

Unlicensed users can log in to SecureTransport using ST Web Client or one of the Axway Email Plug-ins to retrieve files. Using ST Web Client, they can reply once to the sender of a file transfer email. Using Microsoft Outlook or Lotus Notes, they can reply to a file transfer email as they would to any email. They cannot create or forward messages with ad hoc file transfers. For an unlicensed user, ST Web Client does not include the file transfer functions.

If the ad hoc human-to-human file transfer specifies enrollment as an unlicensed user or the System to Human transfer site specifies a security level of `Enroll User - Unlicensed`, the recipient becomes an unlicensed user on enrollment.

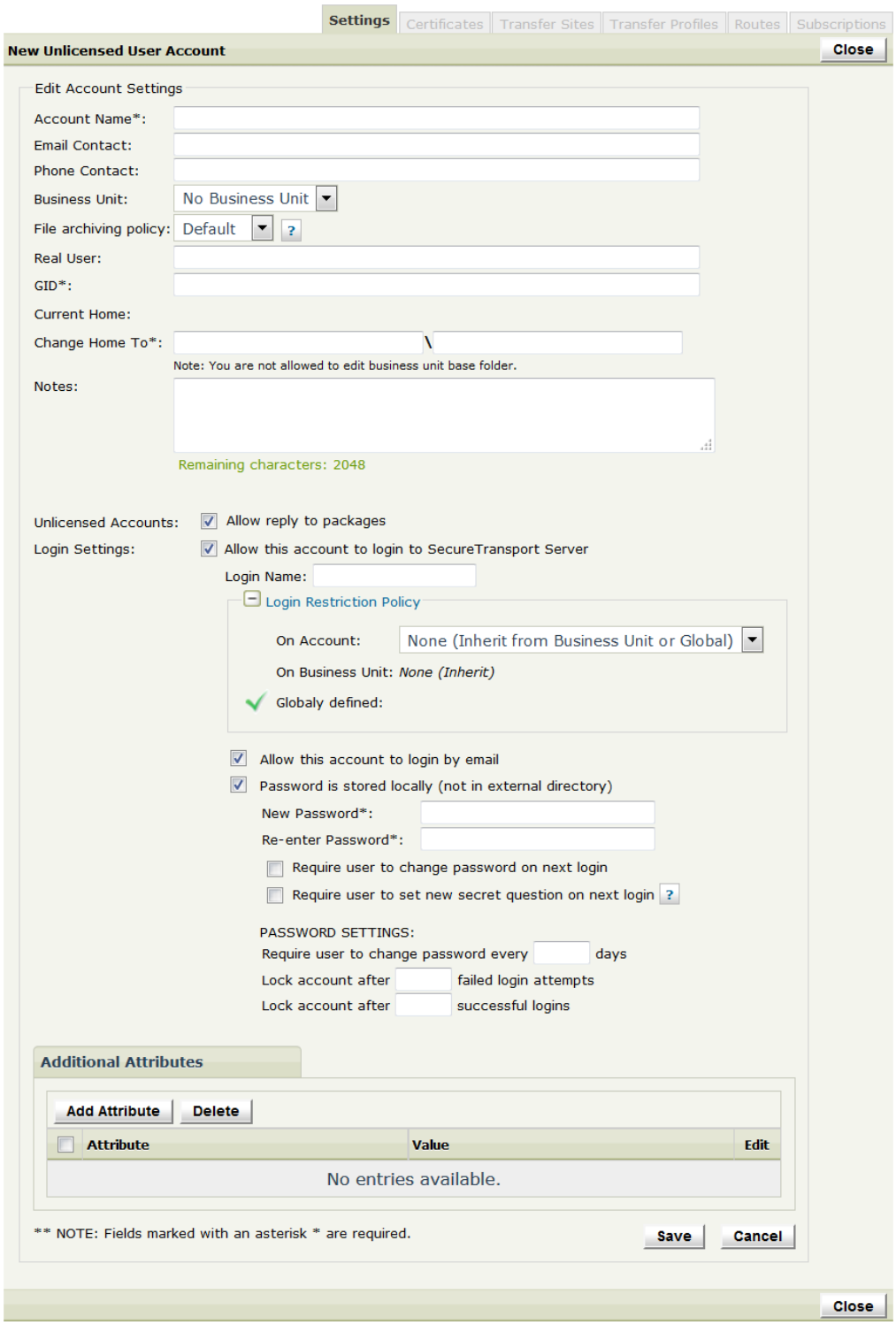
Create account templates for unlicensed users. Configure the account template that applies to unlicensed users in the business unit or in the **Default enrollment account template** field on the *AdHoc Setting* page. See *Manage account templates* on page 663, *Create or edit a business unit* on page 693, and *Configure adhoc file transfers* on page 89.

You can also create an unlicensed user account from the *Unlicensed User Accounts* page.

1. Select **Accounts > Unlicensed Users**. The *Unlicensed User Accounts* page is displayed.
2. Click **New Account**.

   The *Settings* pane of the *New Unlicensed User Account* page is displayed.

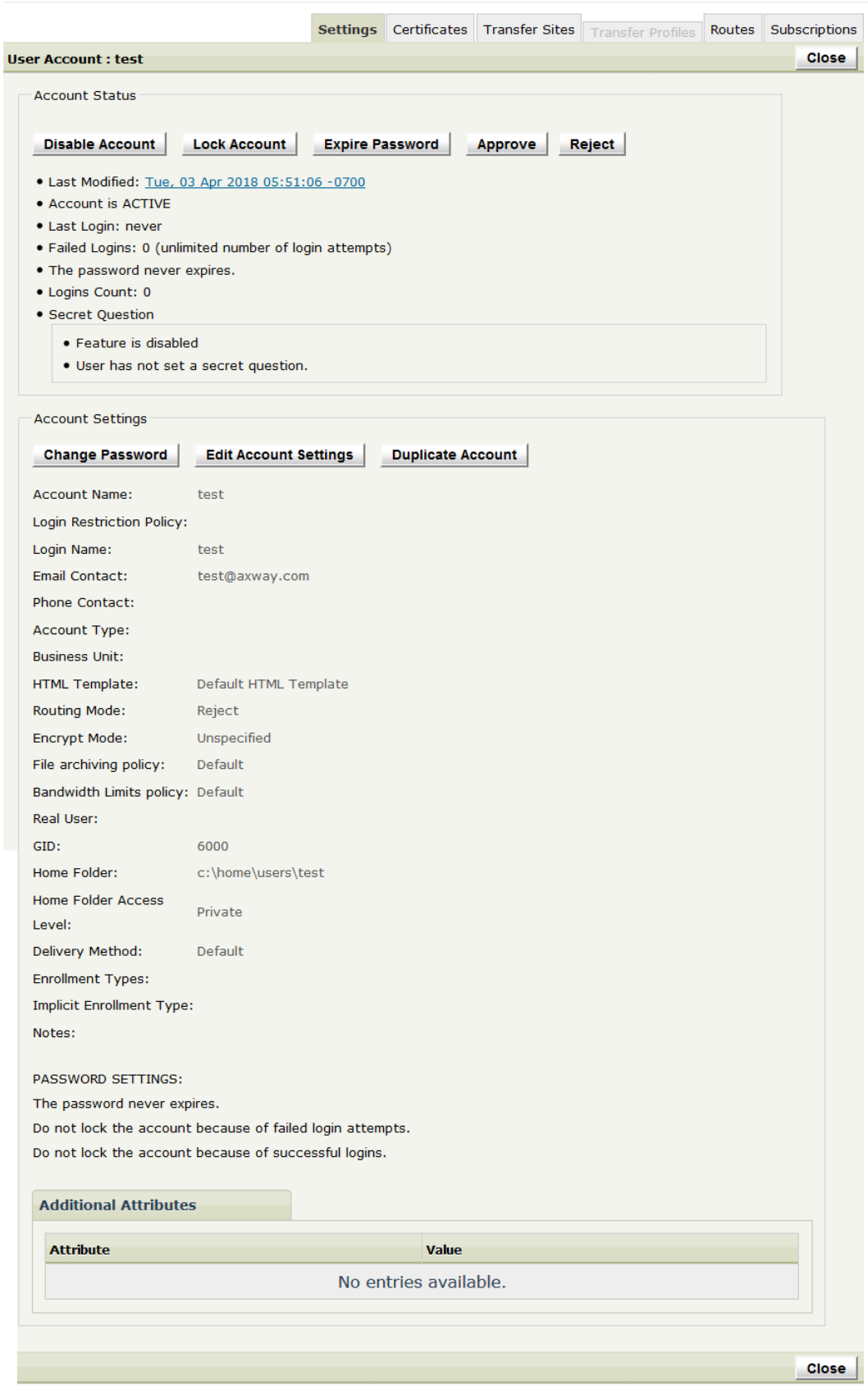
Note The *Address Book Settings* are only displayed if the Address Book feature is enabled (the value of the `AddressBook.Enabled` configuration option is set to **true**). For Address Book account level configuration instructions, refer to *Address Book account level configuration* on page 240.



3. For the common fields, see *Create a user account* on page 456.

4. Select **Allow reply to packages** to permit the unlicensed user to reply once to a received package.
5. If **Allow this account to login to SecureTransport Server** is not selected, the following fields are not displayed.
6. Click **Save**.

   The user account information is saved and displayed in the *Settings* pane of the user account. The other user account tabs are not available for unlicensed users.


Settings
Certificates
Transfer Sites
Transfer Profiles
Routes
Subscriptions
User Account : test
Close
Account Status
Disable Account
Lock Account
Expire Password
Approve
Reject
• Last Modified: Tue, 03 Apr 2018 05:51:06 -0700
• Account is ACTIVE
• Last Login: never
• Failed Logins: 0 (unlimited number of login attempts)
• The password never expires.
• Logins Count: 0
• Secret Question
• Feature is disabled
• User has not set a secret question.
Account Settings
Change Password
Edit Account Settings
Duplicate Account
Account Name: test
Login Restriction Policy:
Login Name: test
Email Contact: test@axway.com
Phone Contact:
Account Type:
Business Unit:
HTML Template: Default HTML Template
Routing Mode: Reject
Encrypt Mode: Unspecified
File archiving policy: Default
Bandwidth Limits policy: Default
Real User:
GID: 6000
Home Folder: c:\home\users\test
Home Folder Access Level: Private
Delivery Method: Default
Enrollment Types:
Implicit Enrollment Type:
Notes:
PASSWORD SETTINGS:
The password never expires.
Do not lock the account because of failed login attempts.
Do not lock the account because of successful logins.
Additional Attributes
Attribute
Value
No entries available.
Close

You can convert an unlicensed user account to a licensed user account.

1. Select **Accounts > Unlicensed Users**. The *Unlicensed User Accounts* page is displayed.
2. Click the name of the account to convert to a licensed user account.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click **Convert to Licensed**.

   The Administration Tool displays the *Settings* pane for the new user account.

The other procedures are the same for licensed and unlicensed user accounts.

Protected folders and accounts

SecureTransport maintains a list of directories which you should not use for home folders for user or service accounts. This type of directory is called a *protected folder*. Protected folders are identified by a specific prefix in the path. The following table lists the prefixes used by default.

Virtual accounts can be purged using SecureTransport, provided these accounts are not in a protected folder.

SecureTransport provides the following precautions that are built-in to prevent accidental or malicious account deletion:

- Paths are converted to equivalent paths without any "." or ".." directories.
- The user home folder cannot directly, or indirectly through a symbolic link, refer to any of the protected directories.
- If the entry for a user home folder is not a directory, it is not purged.
- If the user home folder begins with any of the protected home folder prefixes, the account is not purged.

Platform	Protected home folder prefixes
Oracle Solaris, AIX, Linux, Axway Appliance	`/audit /bin /boot /dev /etc /kernel /lib /lpp /mnt /modules /net /opt /platform /proc /root /sbin /stand /sys /tftp /usr /var /vol`
Windows (in Cygwin Format)	(none)

Note You can add to the list of protected folders by modifying the `UnsafePaths` server configuration option. When adding a folder name that contains spaces, use quotes around the path so the entire path is recognized, for example, "`/user 1/`". Do not remove any of the default protected folder prefix. Make the change on all servers in your Standard Cluster (SC) or Enterprise Cluster (EC).

User certificates

SecureTransport supports the following types of certificates for use across the system:

- PGP and X509 certificates.
- **Partner certificates** – These certificates are managed on a "per account" basis from the **Accounts** menu in the Administration Tool. They are generated, imported, exported, and deleted for the respective account. They fall into the following three types:
    - **Login** – They do not have a private key and are used for logging to SecureTransport Servers. Their private key is exported during the generation of the certificate.
    - **Partner** – They only have a public key and are used for encrypting PGP and AS2 data to an account and verifying the signature of data from the account.
    - **Private** – They have a private key and are used for decryption and signing of PGP and AS2 data.
- Server certificates apply to all of the SecureTransport Server and fall into the following three types:
    - **Local** – Contains a private key and is used by SecureTransport Servers.
    - **Trusted CA** – Used for verification of remote certificates when creating secure connections.
    - **Internal CA** – a Server Certificate Authority.

The following topic describes how to manage user certificates:

- *Manage certificates* on page 476

Manage certificates

Use the *Certificates* pane of the *User Account* page to manage user certificates.

The following topics provide how-to instructions for managing certificates:

- *Generate a partner PGP key* on page 477
- *Import a partner PGP key* on page 479
- *Delete a partner PGP key* on page 480
- *Export a PGP public key* on page 480
- *View a login certificate* on page 480
- *Export a login certificate* on page 481
- *Generate a login certificate* on page 482
- *Import an X509 login certificate* on page 482
- *Import an SSH login public key* on page 483
- *Delete a login certificate* on page 484

- *View a partner certificate* on page 485
- *Export a partner certificate* on page 486
- *Generate an X509 partner certificate* on page 487
- *Generate a PGP partner certificate* on page 487
- *Import an X509 or PGP partner certificate* on page 488
- *Delete one or more partner certificates* on page 489
- *View a private certificate* on page 489
- *Export the SSH public key of an X509 private certificate* on page 490
- *Generate an X509 private certificate* on page 491
- *Generate a PGP private certificate* on page 492
- *Import an X509 or PGP private certificate* on page 492
- *Import an SSH private certificate* on page 493
- *Delete private certificates* on page 494

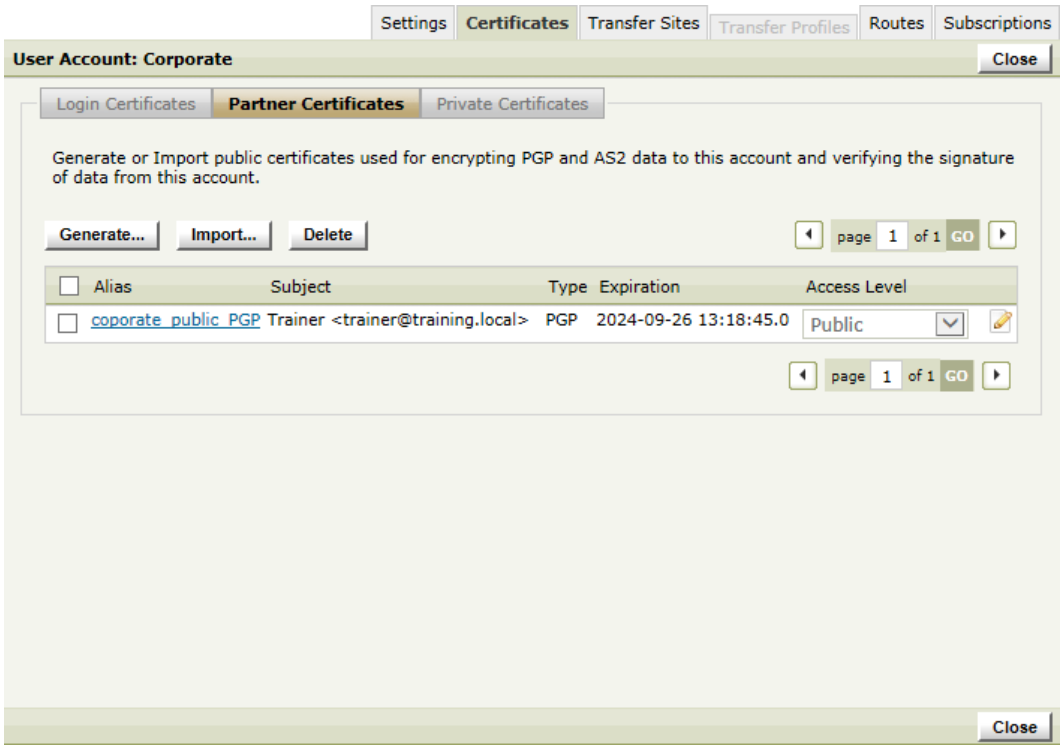
Generate a partner PGP key

Use the following procedure to generate a partner PGP key.

1. Select **Accounts > User Accounts**.
2. Click the name of the account containing the certificate.

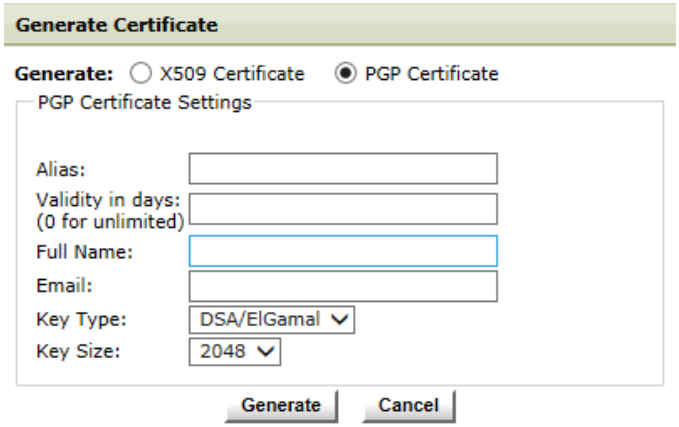
   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab.
4. Click **Partner Certificates** sub-tab.

   The Partner Certificates options are displayed.



5. Click **Generate** to generate a partner PGP key.

   The *Generate Certificate* dialog box is displayed.



6. Fill in the fields in the *Generate Certificate* dialog box and click **Generate**.

   The *Save PGP keypair file* dialog box is displayed.

7. Enter the password in the **Password** field and enter it again in the **Confirm Password** field.
8. Click **Continue**.

   You are prompted to open or save the PGP ASCII-Armored (`.asc`) file. This file contains both the public and private keys.
9. Save a copy of the PGP file and send it to the account user so they can transfer files successfully with PGP encryption.

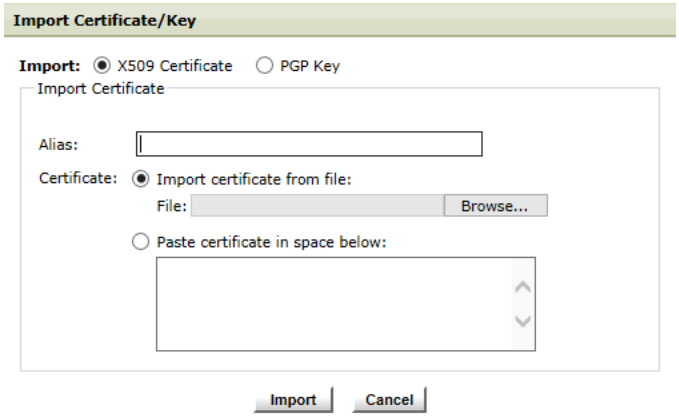
   The certificate is added to the partner certificates for the user. Only the public key is stored.

Import a partner PGP key

Use the following procedure to import a partner PGP key.

1. On the **Partner Certificates** sub-tab, click **Import**.

   The *Import Certificate/Key* dialog box is displayed.



2. Select **PGP key**, fill in the **Alias** field, and select the appropriate radio button to **Import certificate from file** or **Paste certificate in space below**.

   The value you specify in the **Alias** field cannot exceed 50 characters in length.

3. As required, enter the name of the `.asc` file, browse to it, or paste the PGP public key block into the text field.
4. Click **Import**.

   The certificate is added to the partner certificates for the user. Only the public key is stored.

Note The PGP keys imported for use with an account must specify signing algorithms.

Delete a partner PGP key

Use the following procedure to delete a partner PGP key.

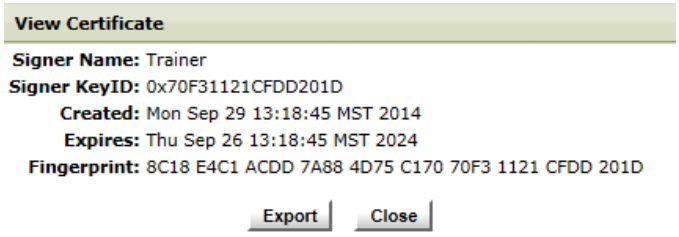
1. On the **Partner Certificates** sub-tab, select the check boxes for the certificates to delete.
2. Click **Delete**.

Export a PGP public key

Use the following procedure to export a PGP public key.

1. On the **Partner Certificates** sub-tab, click the certificate you want to export.

   The *View Certificate* dialog box is displayed.



2. Click **Export**.
3. Save the `.asc` file with the public key.

View a login certificate

SecureTransport uses login certificates when the respective (currently active) account logs in to a SecureTransport Server using a certificate or SSH Key.

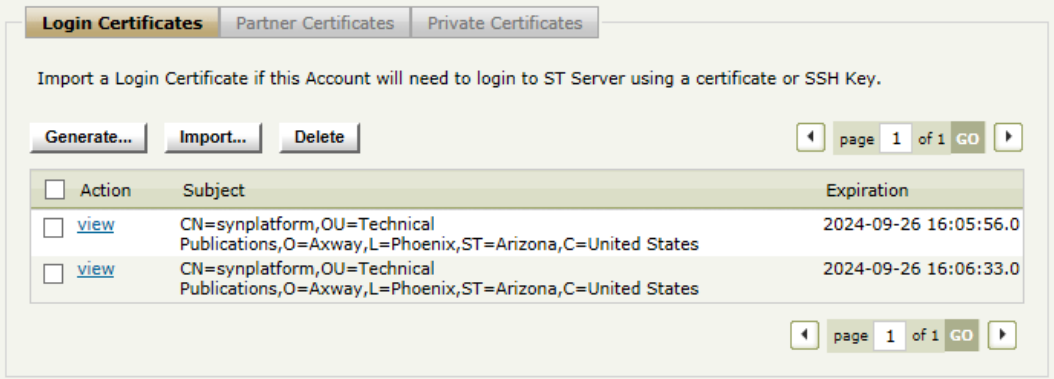
You can view, generate, import and delete login certificates for the active account from the **Login Certificates** tab.

Note SecureTransport generates only X509 login certificates, but you are allowed to import both X509 and SSH Key certificates.

1. Select **Accounts > User Accounts**.
2. Click the name of the account for which you want to view the certificate.

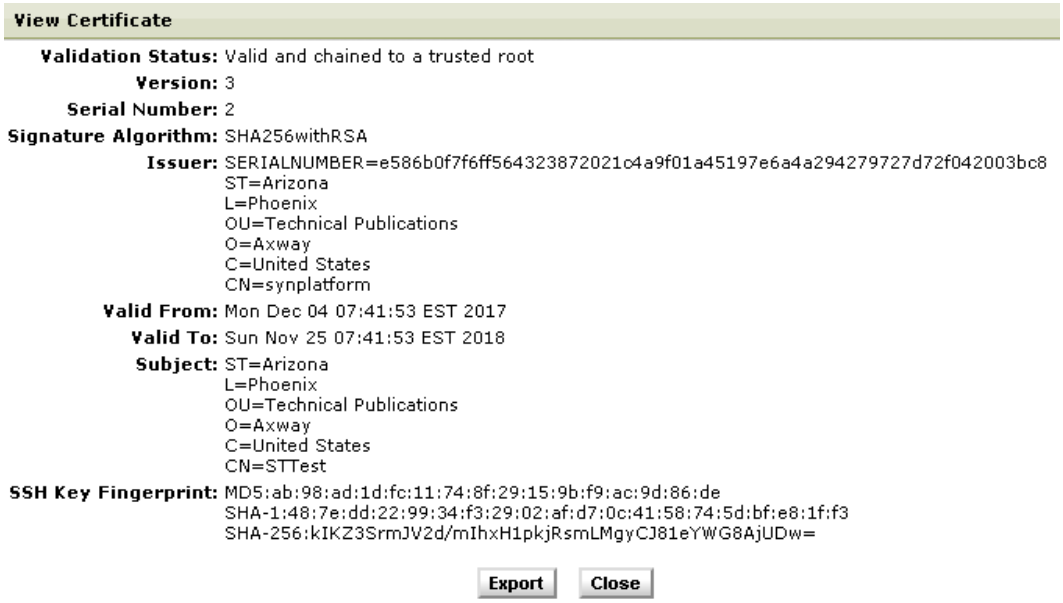
   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab.

The list of login certificates for the selected account is displayed.



4. Click the **View** link for the certificate you want to view.

   Certificate information for the certificate you selected is displayed in a *View Certificate* dialog box.



Export a login certificate

Use the following procedure to export a login certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account containing the certificate.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab.

   The list of login certificates for the selected account is displayed.
4. Click the name of the certificate you want to view.

   Certificate information for the certificate you selected is displayed in a *View Certificate* dialog box.

5. Click **Export** or **Export as SSH Public Key**, as desired.
6. When prompted, save the file containing the key on your file system.

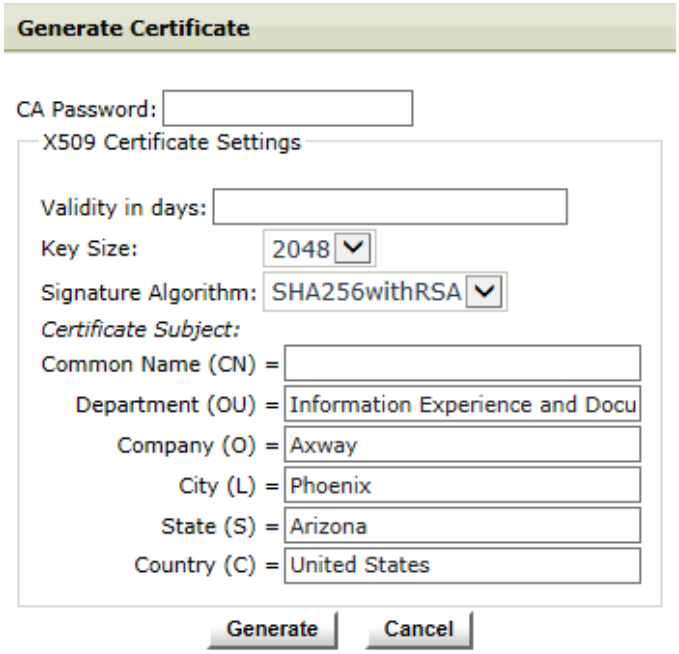
Generate a login certificate

Use the following procedure to generate a login certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account where you want to add the certificate.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab.

   The list of login certificates for the selected account is displayed.
4. Click **Generate**. The *Generate Certificate* dialog box is displayed.



5. Type the necessary information in the *Generate Certificate* dialog box, and then click **Generate**.

   Validity in days and **Common Name (CN)** are required fields.

Import an X509 login certificate

Before the user attempts to log in using an imported certificate, ensure that the CA referenced in the certificate is include in the trusted CAs for the SecureTransport server. For details, see *Manage trusted CAs* on page 61.

1. Select **Accounts > User Accounts**.
2. Click the name of the account where you want to import the certificate.

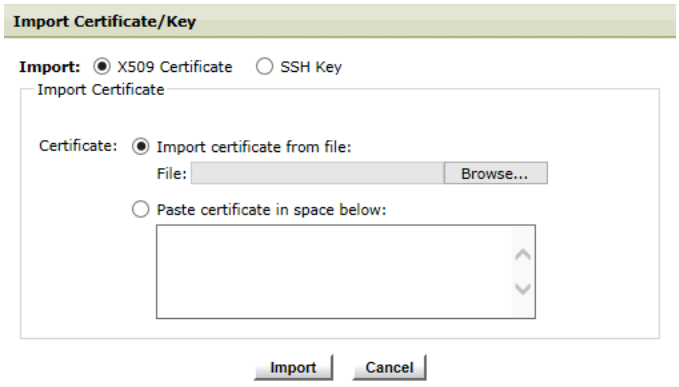
   The *User Account Settings* page is displayed with details for the selected account.

3. Click the **Certificates** tab.

   The list of login certificates for the selected account is displayed.

4. Click **Import**.

   The *Import Certificate/Key* dialog box is displayed.



5. Select **X509 Certificate**.
6. Type the necessary information in the *Import Certificate/Key* dialog box.

   Paste the certificate content directly in the provided space, or import the certificate from a file. To import from file, type the file path or click **Browse** to browse for the file.

7. Click **Import**.

Note Login X509 certificates must be unique.

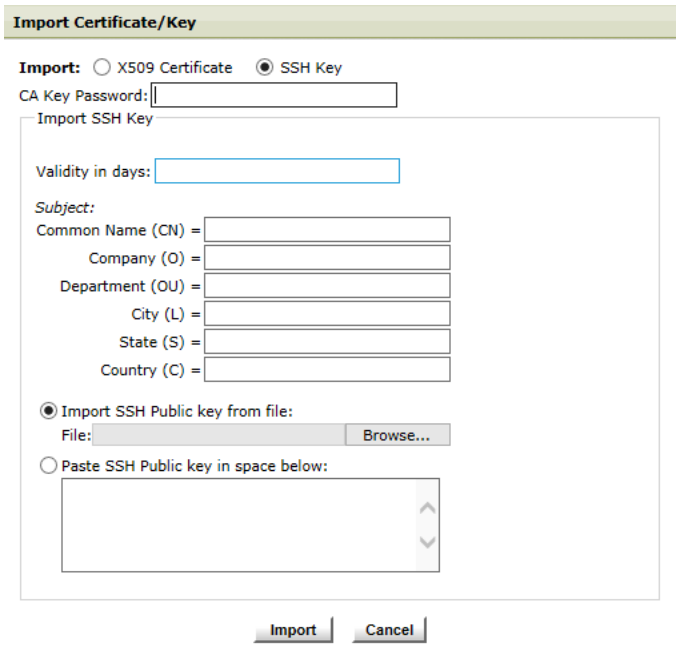
Import an SSH login public key

Note SecureTransport supports the use of both DSA and RSA SSH keys as SSH login public keys.

Use the following procedure to import an SSH login public key.

1. Select **Accounts > User Accounts**.
2. Click the name of the account where you want to import the certificate. The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab. The list of login certificates for the selected account is displayed.
4. Click **Import**.

   The *Import Certificate/Key* dialog box is displayed.



5. Select **SSH Key**.
6. Type the necessary information in the *Import Certificate/Key* dialog box.

   Validity in days is a required fields.

   Note **CA Key Password** and **Common Name (CN)** are not a required fields. When a SSH key is imported (without providing the internal CA key password), the key will be stored as X.509 certificate and signed with temporarily generated certificate. As a result, the SSH key will be stored as X.509 self-signed certificated.
7. Paste the SSH public key directly in the provided space, or import the SSH public key from a file. To import from file, type the file path or click **Browse** to browse for the file containing the key.
8. Click **Import**.

Note The SSH login public key may not be unique.

Delete a login certificate

Use the following procedure to delete a login certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account containing the certificate.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab.

   The list of login certificates for the selected account is displayed.
4. Select the check box next to the certificate you want to delete, and then click **Delete**.

5. Click **OK** to confirm the deletion of the certificate. Otherwise, click **Cancel**. If **OK** is clicked, the selected certificate will be deleted and cannot be recovered.

View a partner certificate

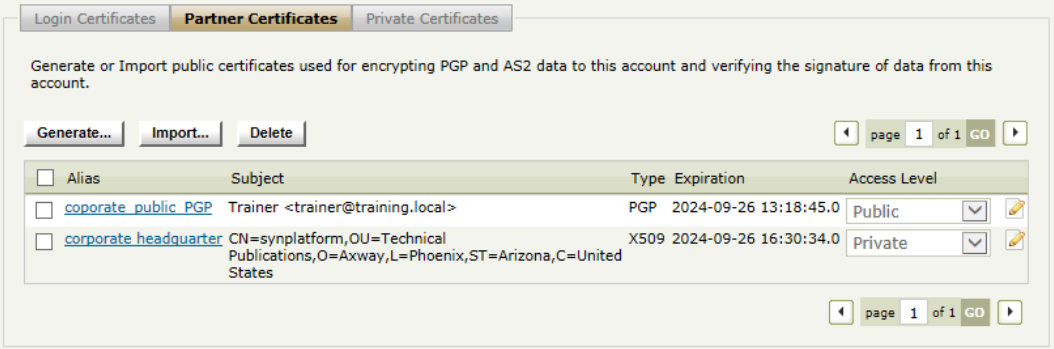
SecureTransport uses partner certificates as public certificates for encrypting PGP and AS2 data to the respective account and for verification of the signature of data from the account.

You can view, generate, import and delete partner certificates for the active account from the *Partner Certificates* tab page.

1. Select **Accounts > User Accounts**.
2. Click the name of the account for which you want to view the certificate.

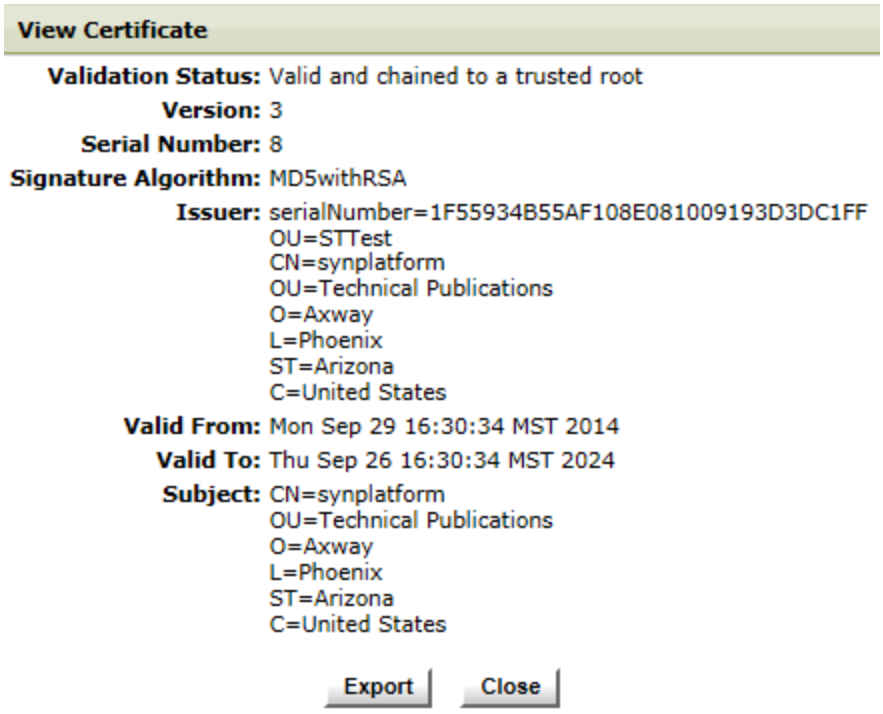
   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab, and then click **Partner Certificates.**

   A list of partner certificates for the selected account is displayed on the *Partner Certificates* page.



4. Click the alias name of the partner certificate you want to view.

Partner certificate information is displayed in the *View Certificate* dialog box.



Note SecureTransport generates and imports X509, PGP, and SSH partner certificates.

Export a partner certificate

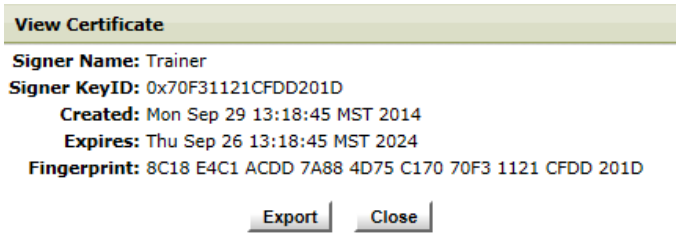
Use the following procedure to export a partner certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account containing the certificate.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab, and then click **Partner Certificates.**

   A list of partner certificates for the selected account is displayed on the *Partner Certificates* page.
4. Click the name of the certificate you want to export.

   Partner certificate information is displayed in the *View Certificate* dialog box.



5. Click **Export**.
6. When prompted, save the file containing the key on your file system.

Generate an X509 partner certificate

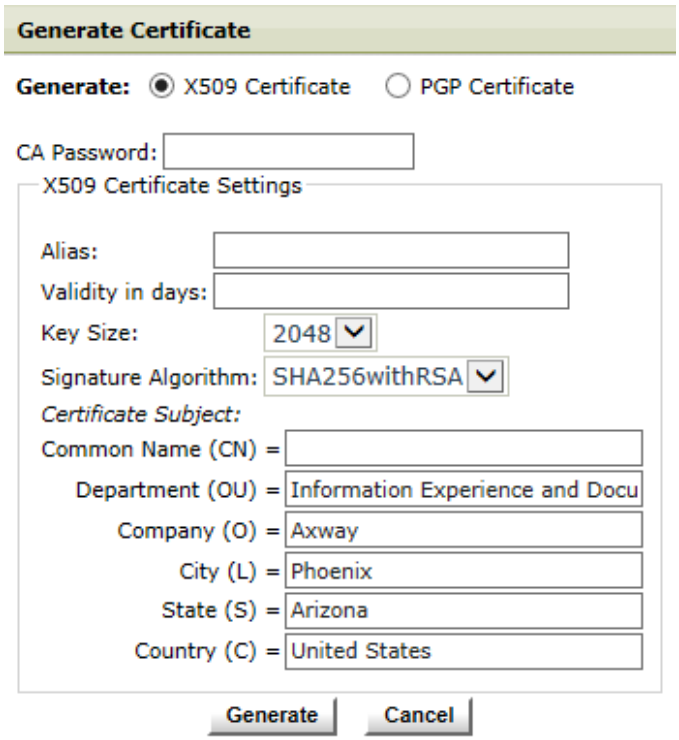
Use the following procedure to generate an X509 partner certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account where you want to add the certificate.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab, and then click **Partner Certificates.**

   A list of partner certificates for the selected account is displayed on the *Partner Certificates* page.
4. Click **Generate**.

   The *Generate Certificate* dialog box is displayed.



5. Select **X509 Certificate**.
6. Type the necessary information in the *Generate Certificate* dialog box.

   Alias, **Validity in days**, and **Common Name (CN)** are required fields. The value you specify in the **Alias** field cannot exceed 50 characters in length.
7. Click **Generate**.

Generate a PGP partner certificate

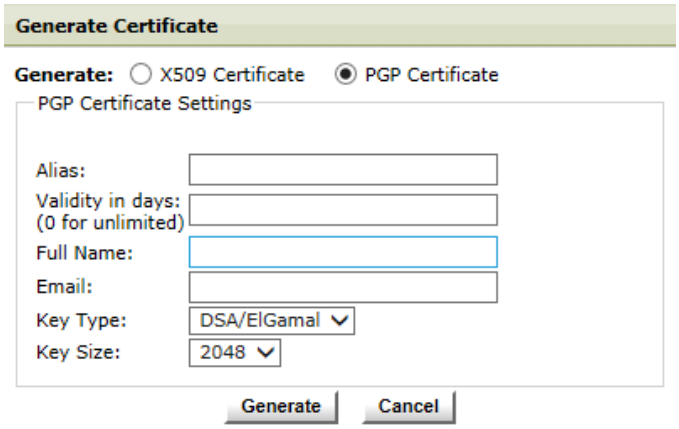
Use the following procedure generate a PGP partner certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account where you want to add the certificate.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab, and then click **Partner Certificates.**

   A list of partner certificates for the selected account is displayed on the *Partner Certificates* page.
4. Click **Generate**.

   The *Generate Certificate* dialog box is displayed.
5. Select **PGP Certificate**.



6. Type the necessary information in the *Generate Certificate* dialog box.

   Alias, **Validity in days**, and **Full Name** are required fields. The value you specify in the **Alias** field cannot exceed 50 characters in length.
7. Click **Generate**.

Import an X509 or PGP partner certificate

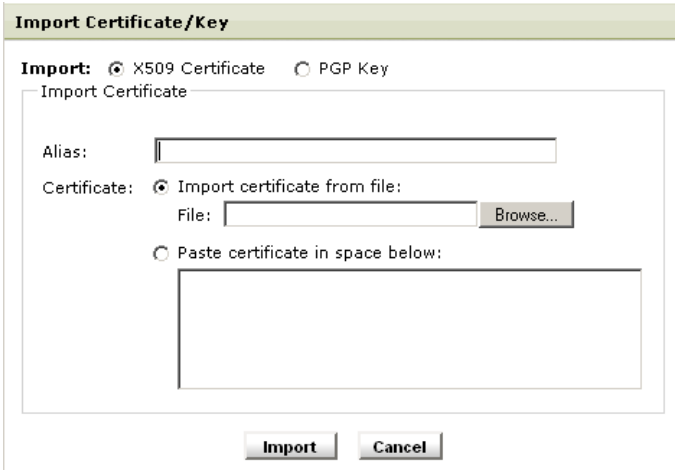
Use the following procedure to import an X509 or PGP partner certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account where you want to import the certificate.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab, and then click **Partner Certificates.**

   A list of partner certificates for the selected account is displayed on the *Partner Certificates* page.
4. Click **Import** button.

   The *Import Certificate/Key* dialog box is displayed.



5. Select the certificate type of the certificate you want to import: **X509** or **PGP**.
6. Type the necessary information in the *Import Certificate/Key* dialog box.

   Paste the certificate content directly in the provided space, or import the certificate from a file. To import from file, type the file path or click **Browse** to browse for the file.
7. Click **Import**.

Note The PGP keys imported for use with an account must specify signing algorithms.

Delete one or more partner certificates

Use the following procedure to delete one or more partner certificates.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account containing the certificate.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Certificates** tab, and then click **Partner Certificates.**

   A list of partner certificates for the selected account is displayed on the *Partner Certificates* page.
4. Select the check box next to the certificate you want to delete, and then click **Delete**.
5. Click **OK** to confirm the deletion of the certificate. Otherwise, click **Cancel**. If **OK** is clicked, the selected certificate will be deleted and cannot be recovered.

View a private certificate

SecureTransport uses private certificates to log in to remote transfer sites for this account, as well as for decrypting and signing PGP and AS2 data.

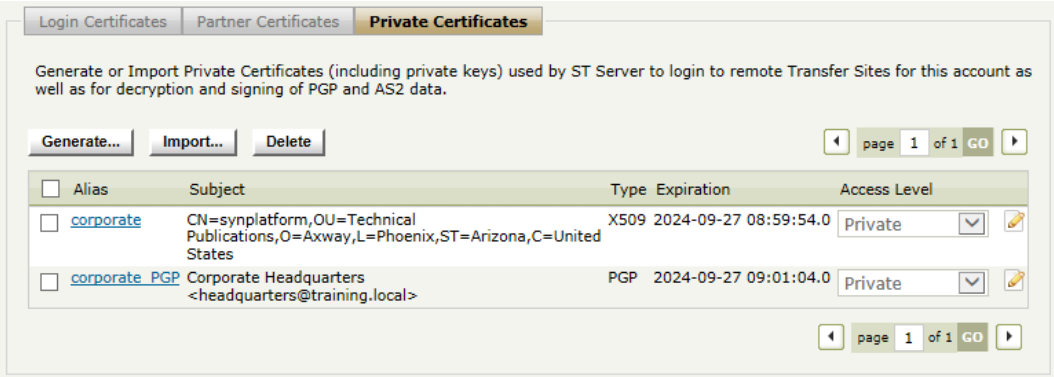
You can view, generate, import and delete private certificates for the active account from the *Private Certificates* page.

1. Select **Accounts > User Accounts**.
2. Click the name of the account for which you want to view the certificate.

The *User Account Settings* page is displayed with details for the selected account.

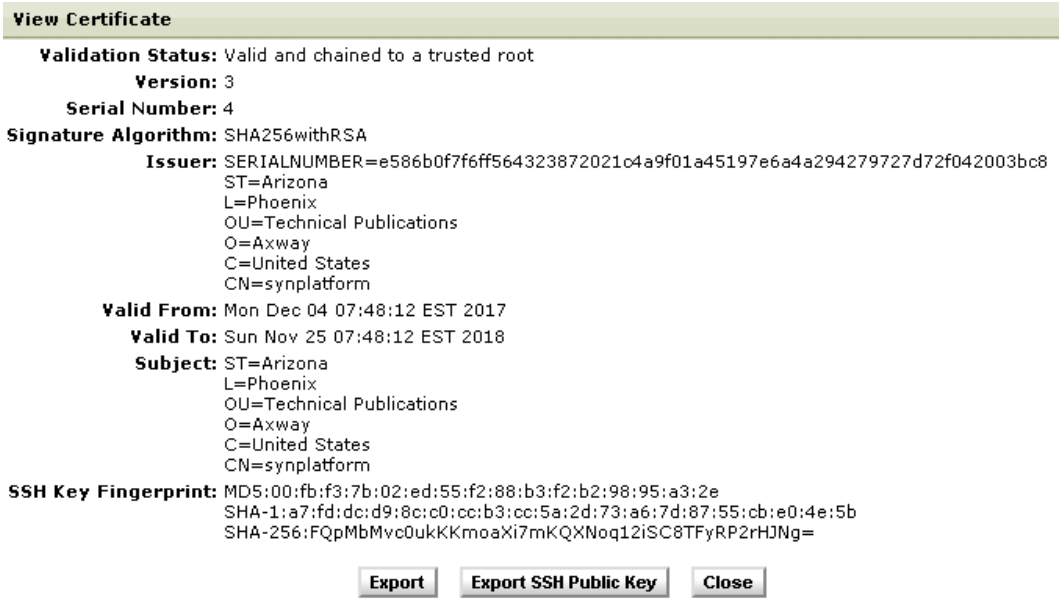
3. Click the **Certificates** tab, and then click **Private Certificates.**

   A list of private certificates for the selected account is displayed on the *Private Certificates* page.



4. Click the name of the certificate you want to view.

   Private certificate information is displayed in the *View Certificate* dialog box.



Export the SSH public key of an X509 private certificate

Use the following procedure to export the SSH public key of an X509 private certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account containing the certificate.

   The *User Account Settings* page is displayed with details for the selected account.

3. Click the **Certificates** tab, and then click **Private Certificates.**

   A list of private certificates for the selected account is displayed on the *Private Certificates* page.

4. Click the name of the certificate you want to export.

   Private certificate information is displayed in the *View Certificate* dialog box.

5. Click **Export SSH Public Key**.

6. When prompted, save the file containing the key on your file system.

Note An SSH Key can be exported for each X509 certificate. In SecureTransport, all certificates are stored as X509 or PGP ones. Imported SSH Keys are also stored as X509 certificates.

Generate an X509 private certificate

Use the following procedure to generate an X509 certificate.

1. Select **Accounts > User Accounts**.

2. Click the name of the account where you want to add the certificate.

   The *User Account Settings* page is displayed with details for the selected account.

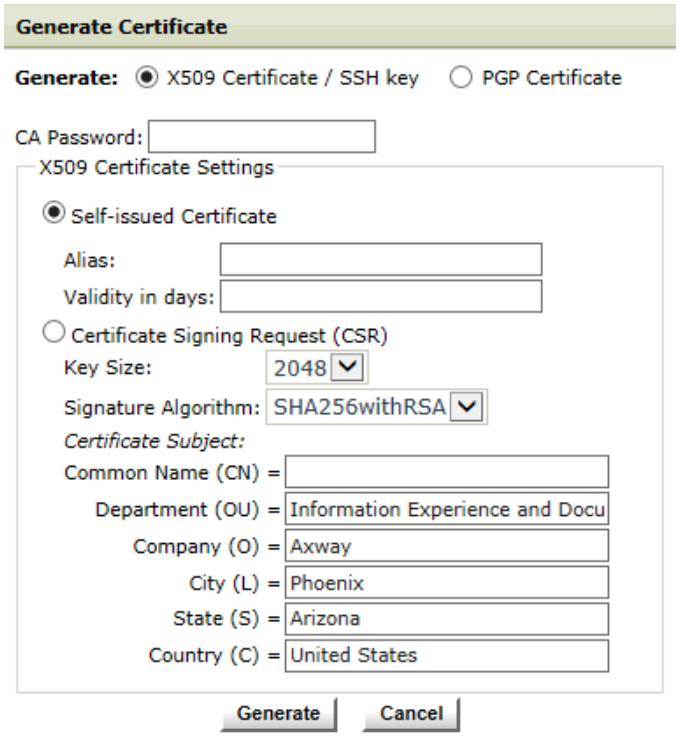
3. Click the **Certificates** tab, and then click **Private Certificates.**

   A list of private certificates for the selected account is displayed on the *Private Certificates* page.

4. Click **Generate**.

   The *Generate Certificate* page is displayed.

5. Select the **X509 Certificate / SSH key** radio button.



6. Select either a **Self-issued Certificate** or a **Certificate Signing Request (CSR)**.

Note If you select **Certificate Signing Request (CSR)**, the field below the**Self-issued Certificate** option are disabled for editing.

7. Depending on your choice, type the necessary information.

   Alias, **Validity in days**, and **Common Name (CN)** are required fields. The value you specify in the **Alias** field cannot exceed 50 characters in length.

8. Click **Generate**.

Generate a PGP private certificate

Use the following procedure to generate a PGP private certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account where you want to add the certificate.

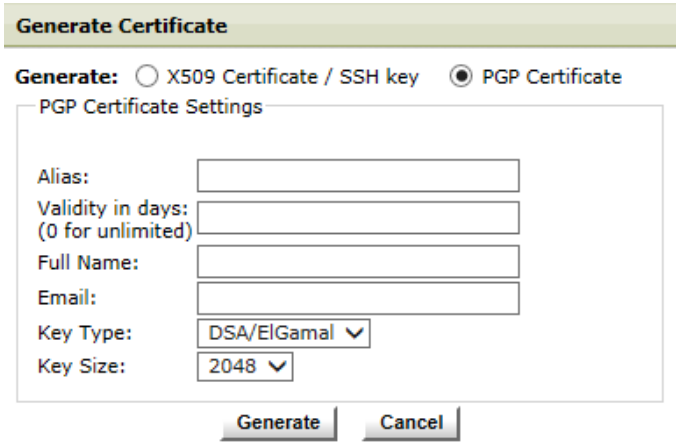
   The *User Account Settings* page is displayed with details for the selected account.

3. Click the **Certificates** tab, and then click **Private Certificates.**

   A list of private certificates for the selected account is displayed on the *Private Certificates* page.

4. Click **Generate**.

   The *Generate Certificate* page is displayed.



5. Select the **PGP Certificate** radio button.
6. Type the necessary information and click **Generate**.

   Alias, **Validity in Days**, and **Full Name** are required fields. The value you specify in the **Alias** field cannot exceed 50 characters in length.

Import an X509 or PGP private certificate

Use the following procedure to import an X509 or PGP private certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account where you want to import the certificate.

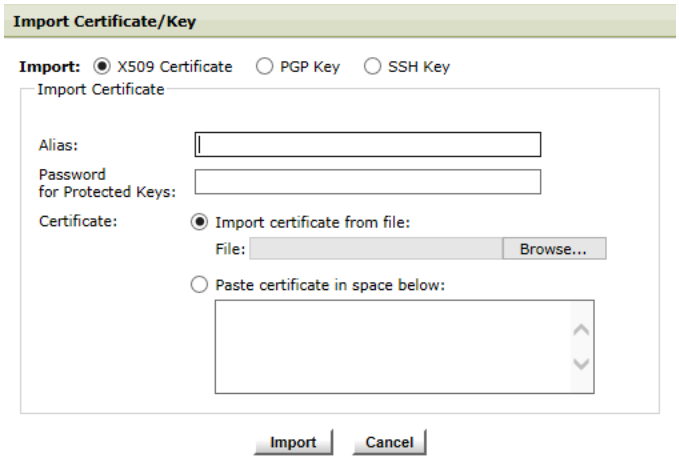
The *User Account Settings* page is displayed with details for the selected account.

3. Click the **Certificates** tab, and then click **Private Certificates.**

   A list of private certificates for the selected account is displayed on the *Private Certificates* page.

4. Click **Import**.

   The *Import Certificate/Key* page is displayed.



   a. Select the type of the certificate you want to import: **X509** or **PGP**.

   b. Type the certificate **Alias**. The value you specify in the **Alias** field cannot exceed 50 characters in length.

   c. Type the certificate **Password**, if one was specified during the certificate generation.

   d. Paste the certificate content directly in the provided space, or import the certificate from a file. To import from file, type the file path or click **Browse** to browse for the file.

5. Click **Import**.

Note The PGP keys imported for use with an account must specify signing algorithms.

Import an SSH private certificate

Use the following procedure to import an SSH private certificate.

1. Select **Accounts > User Accounts**.
2. Click the name of the account where you want to import the certificate.

   The *User Account Settings* page is displayed with details for the selected account.

3. Click the **Certificates** tab, and then click **Private Certificates**.

   A list of private certificates for the selected account is displayed on the *Private Certificates* page.

4. Click **Import**.

   The *Import Certificate/Key* page is displayed.

5. Select the certificate type of the certificate you want to import: **SSH Key**.
6. Type the **CA Key Password** specified during the certificate generation.

Note **CA Key Password** is not a required field. When a SSH key is imported (without providing the internal CA key password), the key will be stored as X.509 certificate and signed with temporarily generated certificate. As a result, the SSH key will be stored as X.509 self-signed certificate.

7. Type the information necessary to import the key.

   Alias and **Validity in days** are required fields. The value you specify in the **Alias** field cannot exceed 50 characters in length.

8. Paste the certificate content directly in the provided space, or import the certificate from a file. To import from file, type the file path or click **Browse** to browse for the file.
9. Click **Import**.

Delete private certificates

Use the following procedure to delete private certificates.

1. Select **Accounts > User Accounts**.
2. Click the name of the account containing the certificate.

   The *User Account Settings* page is displayed with details for the selected account.

3. Click the **Certificates** tab, and then click **Private Certificates.**

   A list of private certificates for the selected account is displayed on the *Private Certificates* page.

4. Select the check boxes next to the certificates you want to delete, and then click **Delete**.
5. Click **OK** to confirm the deletion of the certificate. Otherwise, click **Cancel**. If **OK** is clicked, the selected certificate will be deleted and cannot be recovered.

Transfer sites

A transfer site is a location such as a local folder or protocol server used when sending or receiving files during a server-initiated transfer. Supported protocol servers include AS2, Connect:Direct, Folder Monitor, FTP(S), Generic-HTTP(S), HTTP(S), PeSIT, SharePoint, SSH (SFTP), and System to Human. Transfer sites are specified and managed on a per-account basis.

When defining a transfer site as part of an account, you need to provide the information required for connecting to the site, authenticating the login and sending or receiving files. The transfer protocol you select dictates what information required to define the transfer site.

In general, a site is used for AS2 transfers and server-initiated transfers. In the case of a server-initiated transfer, a file is either uploaded to the site when a subscription processes an uploaded file or downloaded from the site using a schedule in a subscription.

An account can have zero or more transfer sites. An account can subscribe to zero or more applications, and an application can be triggered when a file is transferred using a site.

The following topics describe and provide how-to instructions for managing transfer sites:

- *Transfer site properties* on page 495
- *AS2 transfer sites* on page 497
- *Connect:Direct transfer sites* on page 505
- *File services interface protocol transfer sites* on page 508
- *Folder Monitor transfer sites* on page 511
- *FTP(S) transfer sites* on page 515
- *Generic HTTP transfer sites* on page 525
- *HTTP(S) transfer sites* on page 552
- *PeSIT transfer sites* on page 559
- *SharePoint transfer sites* on page 572
- *SSH transfer sites* on page 579
- *System to Human transfer sites* on page 595
- *Manage transfer sites* on page 597

Transfer site properties

A transfer site in SecureTransport is defined with various properties. To avoid repetition, the current topic describes the properties common for all Transfer Sites. Properties which are custom to each Transfer Site are described in their dedicated topics.

- **Site Name** – the name of the site. This name must be unique for the account.

  You cannot enter spaces-only values in the Site Name field. For more information, see *Spaces in required fields* on page 1.

- **Site Type** – indicates whether transfers are internal (within a single organization) or partner (between organizations). Reported to Axway Sentinel as `USERPARAMETER1` and displayed in the Sentinel event attributes.

- **Access Level** - transfer site access level determines whether and which other accounts could reuse this transfer site in Send To Partner step.

  - **Private** – The access level is private. Only the current account is able to use this transfer site.
  - **Business Unit** – Access to the transfer site is limited to the account's business unit. The current account and all accounts in the current account's business unit can use this transfer site.
  - **Public** – Access to the transfer site is public. All accounts are able use this transfer site.

  Note Access level is applicable only when Advanced Routing feature is used. For more information see *Advanced Routing* on page 795.

- **Maximum parallel transfers** – If you enter a value greater than zero, SecureTransport executes only the specified number of transfers in parallel. If the value is null or zero, the maximum number of parallel transfers is limited by system capacity.

The maximum number of parallel transfers limit is applied cluster wide. The limit for files transferred from the client will not be exceeded. Due to limitations in Standard Cluster communication mode, the parallel pulls limit can be exceeded when there are several connections. If you want to force the limit, then the `force.standard.cluster.sit.transfers.sync=true` system property should be added to the `start_tm_console`. Adding the property to the `start_tm_console` has a performance penalty due to increased cluster communication.
Note that the `force.standard.cluster.sit.transfers.sync` value overrides the value of the `force.standart.cluster.sit.pulls.sync` property, used in previous SecureTransport versions for the same purposes.
You can configure **Maximum parallel transfers** with the following Transfer site protocols: AS2, FTP(S), HTTP(S), SSH, Generic-HTTP(S), SharePoint.

Note When multiple transfers limitations are set, all of them apply but the strictest limitation takes priority over the rest. The following limitations may affect server initiated transfers:

- Maximum Parallel Transfers - the limit per Transfer Site, described here.
- Maximum number of parallel transfers - the limit for "Files Received from this Account or its Partners", specified in Basic Application or Advanced Routing Subscriptions
- Maximum concurrent connections per host for outbound connections

- **Transfer Protocol** – one of the supported protocols: AS2, Connect:Direct, Folder Monitor, FTP (S), HTTP(S), SSH (SFTP), PeSIT, System to Human, or a protocol implemented using the file services interface.
- **Custom properties** – these vary according to the protocol used for the transfer site. For more information about each protocol, see the respective subtopic for each protocol:
  - *AS2 transfer sites* on page 497
  - *Connect:Direct transfer sites* on page 505
  - *Folder Monitor transfer sites* on page 511
  - *File services interface protocol transfer sites* on page 508
  - *FTP(S) transfer sites* on page 515
  - *HTTP(S) transfer sites* on page 552
  - *PeSIT transfer sites* on page 559
  - *System to Human transfer sites* on page 595
  - *SSH transfer sites* on page 579
  - *Generic HTTP transfer sites* on page 525
  - *SharePoint transfer sites* on page 572

Using DXAGENT_TRANSFERSAPI variables in transfer sites

The environment variables with the `DXAGENT_TRANSFERSAPI` prefix can be used in the transfer site definition fields to reference properties submitted via the REST API.

1. On the *Add Transfer Site* page or the *Edit Transfer Site* page, in the desired property field, type: `${DXAGENT_TRANSFERSAPI_*}`, where * is an arbitrary name, for example, "MEMBERNAME".

Note Depending on transfer protocol, you can use environment variables in different transfer site definition fields. If a transfer site is successfully created or edited, all the environment variables and advanced expressions, used in its definition, will be evaluated.

2. To trigger a server-initiated transfer using the Transfers RESTful API resource, you need to set the value of the dynamic property in the request body in the following form: `"YourCustomPropertyName":"value"`, for example, "MEMBERNAME": "Kate".

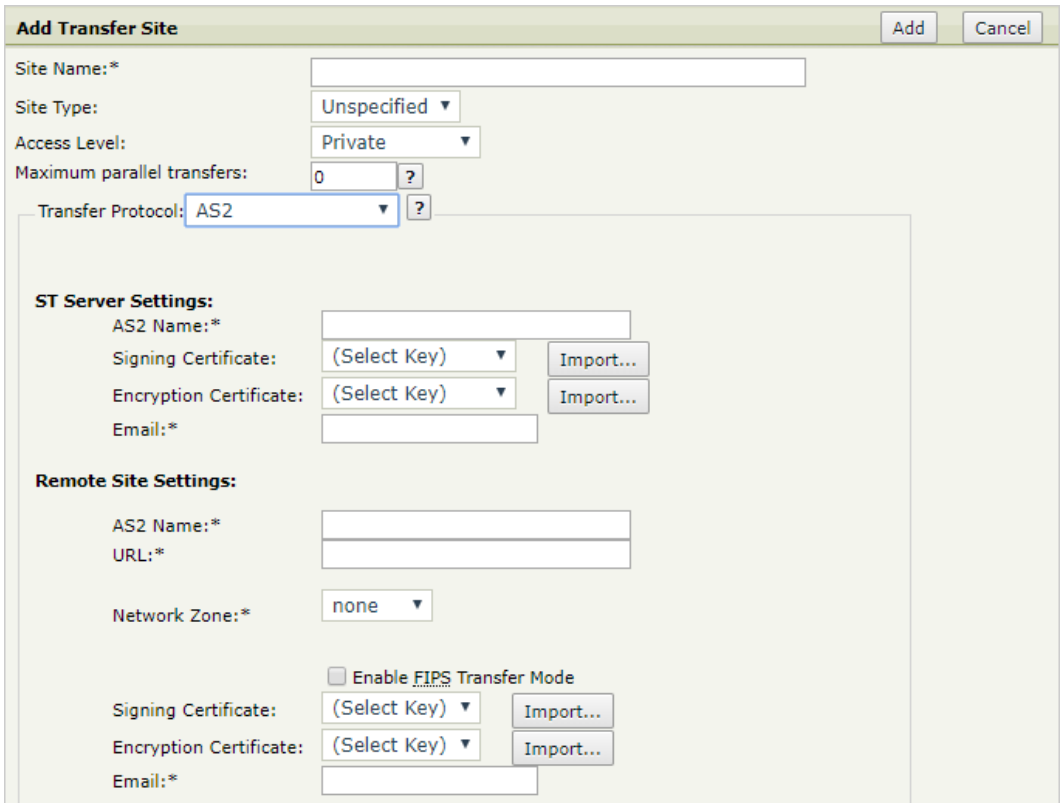
AS2 transfer sites

Although transfers using the AS2 protocol function in a different way than the other supported protocols, you can subscribe accounts with AS2 transfer sites to applications. Among the standard applications, the Site Mailbox and Standard Router applications are appropriate for an AS2 transfer site.

Unlike transfer sites for other transfer protocols, an AS2 transfer site is also used for transfers initiated by the remote AS2 site (considered client-initiated by SecureTransport). Only the fields marked with an asterisk (`*`) as required are needed to define the partnership to enable these transfers.

For detailed information about AS2 transfers, see *AS2 transfers* on page 954.

The following is the *Add Transfer Site* page for a transfer site definition that uses the AS2 transfer protocol.



The following table describes the AS2 protocol options for defining a transfer site.

Field	Description
SecureTransport Server Settings	
AS2 Name*	The local partnership name, which the remote AS2 site uses to identify to this SecureTransport Server. Each AS2 transfer site for a user must have a unique AS2 Name. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Signing Certificate	(Optional) The alias that represents the server or partner certificate used to sign a message.
Encryption Certificate	(Optional) The alias that represents the server or partner certificate used to encrypt a message.
Email	The email address used to receive information from the remote AS2 site. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Remote Site Settings	

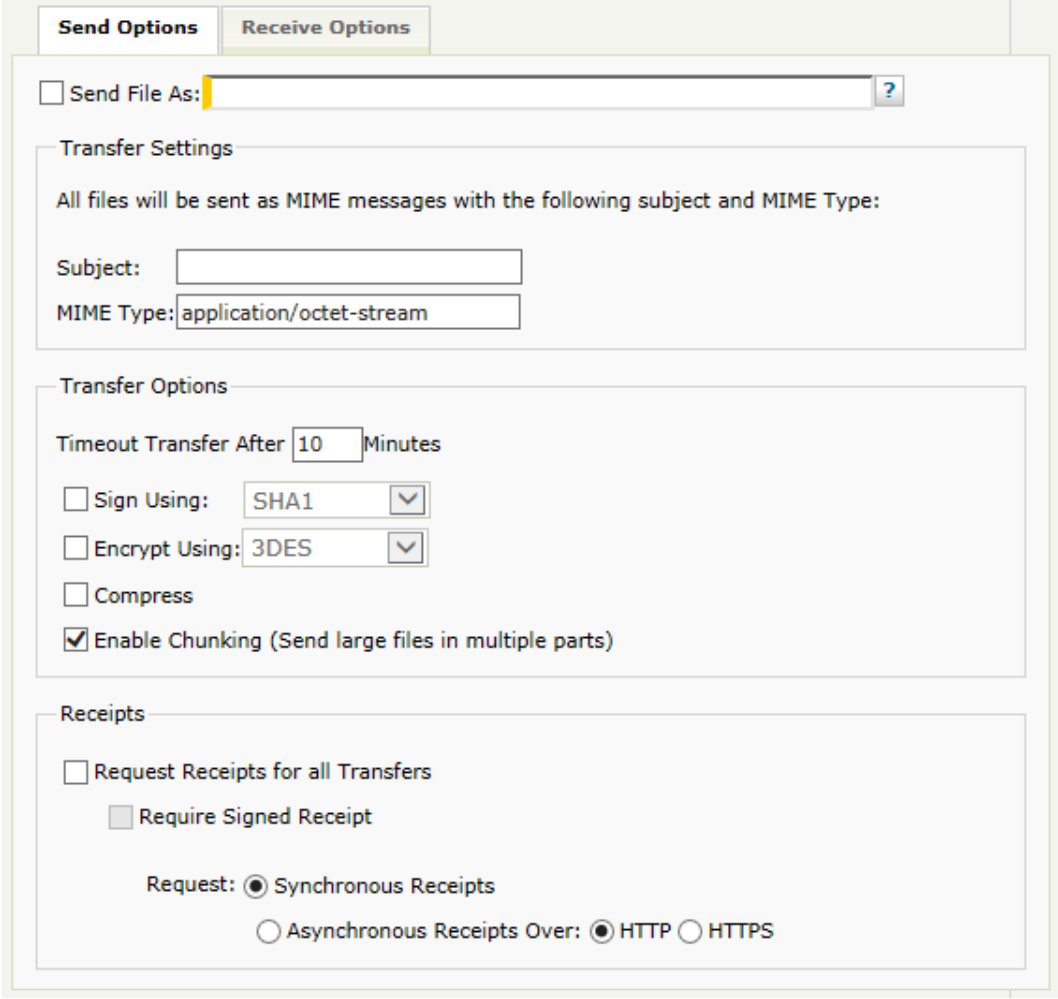
Field	Description
AS2 Name*	The remote partnership name, which the SecureTransport Server uses to identify to the remote AS2 site. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
URL	The URL used to access the remote site. For example, `https://as2.example.com:10443` ,`https://172.23.34.45:10443`, or `https://[FC00:1234:2345:3456::]:10443`. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

Field	Description
Alternative addresses	This set of options allow you to add, delete and set a priority order of alternative endpoints. These endpoints act as backup alternatives to the configured Server-Port Site Settings and are particularly useful in cases of transfer failures. Specifying alternative endpoints as backup servers provides a way to temporarily reroute pending transfers and minimize the risk of transfer failure. With the AS2 transfer sites, the connection to each alternative endpoint is defined by its URL. • To add an alternative server endpoint, click **New Address**. The Alternative Addresses table expands with a new row, that allows you to enter a hostname (or IP address), a port number and save these changes. • To delete an alternative server endpoint, select the corresponding check-box on the same row and click **Delete**. • To reorder the list of alternative endpoints, click **Reorder**. A new option (upward and downward arrow) appears next to each entry. You must hover with the mouse pointer over this newly appeared option and the mouse pointer will assume the "move" shape: a four-directional arrow pointer. This indicates which alternative endpoint is on focus. You can now drag & drop it up and down to the order number you want it at. Perform this action with other alternative endpoints until the list is ordered according to your needs. When you are done, click **Save Order** to keep the newly changed order. Visibility of this option is controlled with the value set for the `TransferSite.AlternativeAddresses.retryPolicy` configuration option. It allows you to set a "retry policy" with a list of alternative endpoints (presented in URLs with AS2 transfer sites) you define on this screen. But before you are able to do so, you must go to **Operations > Server Configuration** and set the policy type using either of the following values: • `AllHostsOnEachRetry` – with this policy SecureTransport iterates through each endpoint, one by one, starting with the first in the list. If connection not successful, SecureTransport will continue trying each endpoint one after another until the maximum number of retries is reached. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `OneHostOnEachRetry` – with this policy SecureTransport tries to connect to the first endpoint in the list. If connection not successful, SecureTransport will continue trying that endpoint until the maximum number of retries is reached; and then will move to the next one in the list. Following that same pattern, SecureTransport will try each endpoint until success; or until end of list. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `Disabled` (default) – this is the default value that keeps the table with endpoints entirely hidden from view.

Field	Description
Network Zone	The network zone that defines the proxies to use for transfers through this site. • Select **none** to connect directly to the partner AS2 server. • Select **any** to allow SecureTransport to select the proxy connection using a network zone that enables an HTTP proxy. • Select **Default** to use the default network zone proxy configuration. If no default is network zone is defined, transfers from this transfer site fail. • Select a specific network zone to use the proxy configuration defined for that zone. For more information, see *Specify TM Server communication ports and IP address for protocol servers on SecureTransport Edge* on page 224.
Enable FIPS Transfer Mode	Restrict AS2 to use only FIPS 140-2 Level 1 certified cryptographic libraries. When you enable FIPS transfer mode, the panel expands with an additional field that lets you specify the desired set of cipher suites to be used in FIPS mode for server-initiated transfers through this site. By default, this set is populated with the cipher suites as defined in the `As2.FIPS.SIT.Ciphers` configuration option. You can add or remove cipher suites. The supported FIPS cipher suites from which you can select when adding a new one are listed in *FIPS transfer mode* on page 983. Note that both the sender and the recipient must use supported FIPS ciphers suites. Otherwise, the transfer will fail.
Signing Certificate	(Optional) The alias that represents the user or partner certificate used to sign a message from this site.
Encryption Certificate	(Optional) The alias that represents the user or partner certificate used to encrypt a message from this site.
Email	The email address used to receive information from SecureTransport Server. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
* Each AS2 transfer site must have a unique combination of SecureTransport Server AS2 Name and Remote Site AS2 Name.	

Transfer Settings: Send Options

This subtopic provides descriptions on the Send Options and Receive Options pages for AS2 transfer sites.



The following table describes the Send Options for an AS2 transfer site.

Field	Description
Send options	
Send File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name. When you enter a new file name in this field, the AS2 message header uses the new name as the value for `original filename`.
Transfer Settings	
Subject	The MIME subject to be used for outgoing messages.
Mimetype	The MIME type to be used for outgoing messages. For example, `application/edi-x12`.

Field	Description
Transfer Options	
Timeout Transfer After x Minutes	The number of minutes after which a transfer is timed out if it is not successful.
Sign Using	The algorithm to be used to sign messages from this site.
Encrypt Using	The algorithm used to encrypt messages from this site. The RC2/40, RC2/64 and RC2/128 algorithms are not FIPS compliant.
Compress	Select this check box to enable compression.
Enable Chunking	Select this check box to enable chunking.
Receipts	
Request receipts for all Transfers	Select this check box to request receipts for all transfers.
Require Signed Receipt	If you select the **Request receipts for all transfers** check box, select the check box to require those receipts to be signed.
Request: Synchronous Asynchronous	Specify whether you want receipts to be synchronous or asynchronous. If you select asynchronous receipts, specify whether you want to receive those receipts via HTTP or HTTPS. If you request receipts via asynchronous HTTP and you specify that an SSL connection in *Receive Options*, you receive receipts via HTTPS instead of HTTP.

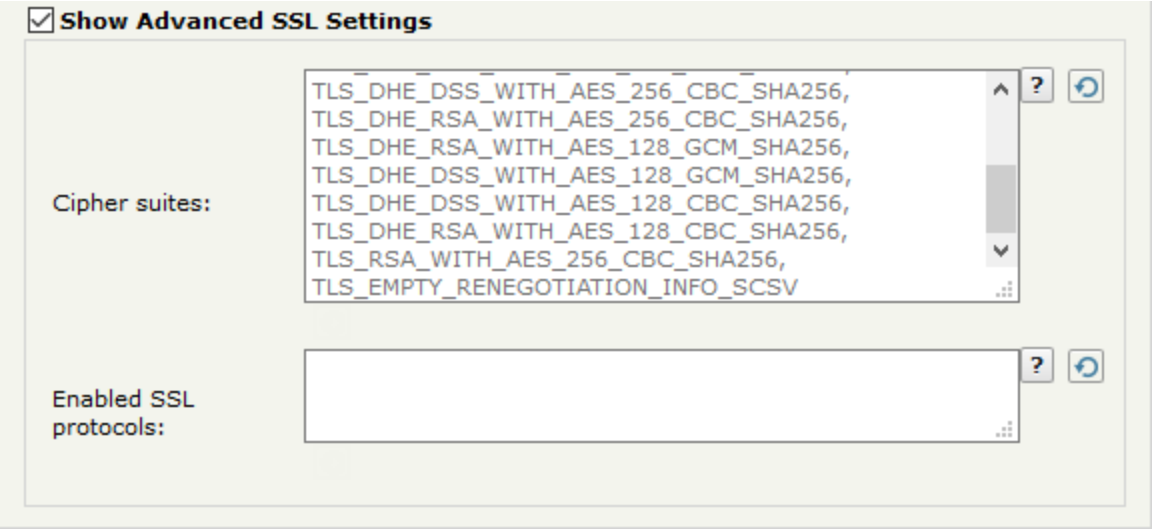
Transfer Settings: Receive Options

The following table describes the Receive Options for an AS2 transfer site.

Field	Description

Field	Description
Receive Options	
Receive File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name when the transfer is received. You can use the SecureTransport-specific variable `${stenv.rawsource}` which takes the value from the `original filename` in the AS2 message header. See *Expression Language* on page 1020 for information on SecureTransport-specific variables.
Require SSL Connection	Select this check box to require an SSL connection for transfers received. If you request receipts via asynchronous HTTP and you specify that an SSL connection, you receive receipts via HTTPS instead of HTTP.
Require Signature	Select this check box to require transfers received to be signed.
Require Encryption	Select this check box to require transfers received to be encrypted.

Advanced SSL Settings



The following table describes the Advanced SSL Settings for an AS2 transfer site.

Field	Description
Show Advanced SSL Settings	

Field	Description
Cipher suites	The set of cipher suites available with the current AS2 transfer site for secure SIT connection. By default this set is populated with the cipher suites as defined in the `As2.SIT.Ciphers` configuration option. To reset to default values, click the button next to the tooltip.
Enabled SSL protocols	The available SSL protocols for secure SIT connection with the current AS2 transfer site. By default this option uses the SSL protocols as defined in the `As2.SIT.EnabledProtocols` configuration option. To reset to default values, click the button next to the tooltip.

Note Use a subscription to a Basic application or a Site Mailbox application to process files received by an AS2 transfer site.
When using asynchronous receipts for outgoing AS2 transfers, post-transmission actions execute, even if the AS2 transfer has failed. This occurs because the transfer initially reports success, triggering the post-transmission action. After the post-transmission action is triggered, an asynchronous failure message is returned, causing the transfer to fail.

Connect:Direct transfer sites

To use the Connect:Direct protocol, you must install the Connect:Direct Java Application Interface (`CDJAI.jar`) in the `<FILEDRIVEHOME>/lib/jars` directory or any subdirectory on the server running SecureTransport. You cannot create or modify a Connect:Direct transfer site without installing the Connect:Direct Java Application Interface. The `CDJAI.jar` file is available as part of the Connect:Direct software.

Note Support for the NDM protocol through a Connect:Direct transfer site does not replace or append your Connect:Direct license.

You also need to manually configure some options in SecureTransport.

1. Stop SecureTransport by running `<FILEDRIVEHOME>/bin/stop_all`.
2. Copy the `CDJAI.jar` file to the `<FILEDRIVEHOME>/lib/jars` directory.
3. If you are using the embedded database, run `<FILEDRIVEHOME>/bin/start_db`.
4. Start the Administration Tool server by running `<FILEDRIVEHOME>/bin/start_admin`.
5. Log in to the Administration Tool and select **Operations > Server Configuration**.

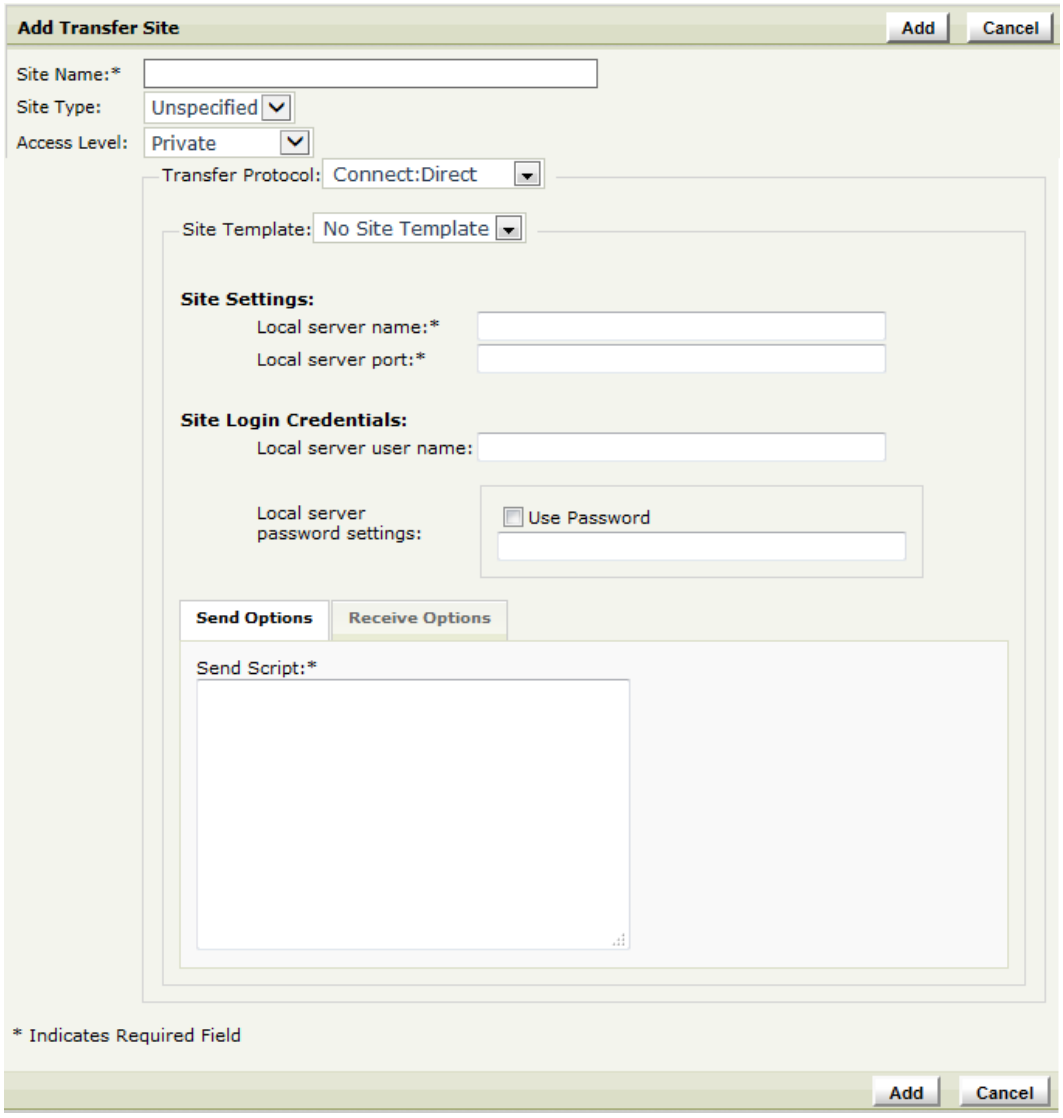
   The *Server Configuration* page is displayed.
6. Search for the `ConnectDirectTransferAgent` parameters.
7. Set `ConnectDirectTransferAgent.transfersFolder` to full path of the directory for the SecureTransport Server to use for the Connect:Direct transfers.

   Note The directory path is not relative to `<FILEDRIVEHOME>`. Specify a full absolute path from `/` (root) in UNIX or `C:\` or another volume on Windows.

Note To manage purging of the Connect:Direct folder, use the `ConnectDirectTransferAgent.transfersFolder.purge` server configuration option. By default, it is set to **true**, which means that the folder used for the Connect:Direct transfers will be purged on Transaction Manager startup. When set to **false**, no purging is performed.

8. Set `ConnectDirectTransferAgent.commandTimeout` to the interval in seconds that SecureTransport waits before the transfer times out.
9. Create the directory for the SecureTransport Server to use for the Connect:Direct transfers on the server. Verify that SecureTransport has full permissions for the directory.
10. Start SecureTransport by running `<FILEDRIVEHOME>/bin/start_all`.
11. Enable the `ConnectDirectTransfer` rules package in the *Rules Packages* page of the Administration Tool.

The following is the *Add Transfer Site* page for a transfer site definition that uses the Connect:Direct transfer protocol.



The following table describes the Connect:Direct protocol options for a transfer site:

Field	Description
Site Settings	
Local server name	Specifies the domain name or IP address of the local server. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Local server port	Specifies the port assigned to the local server. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Site Login Credentials	
Local server user name	Username used to log in to the local server.
Local server password	If the local server uses a password, select **Use Password** and enter the password in the field provided.
Send Options	
Send Script	Specifies the Connect:Direct process to execute when uploading a file to a remote site. You must provide a script in for either the Send Options or the Receive Options. This field must contain a valid Connect:Direct process language script. You can use expression language variables such as `${stenv.target}` in the script. For example, you can use the script field to execute a copy command. The remote server you are calling must be identified by its alias in the script. To correctly identify the file name in a script you must use the variable `${cd_transfer_file}`. The variable is required because the file names might not be known at the time you write the script. When creating an upload script you must use `${cd_transfer_file}` instead of the file name of the file being uploaded. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Receive Options	

Field	Description
Receive Script	Specifies the Connect:Direct process to execute when downloading a file from a remote site. You must provide a script for either the Send Options or the Receive Options. This field must contain a valid Connect:Direct process language script. You can use expression language variables such as `${stenv.target}` in the script. For example, you can use the script field to execute a copy command. The remote server you are calling must be identified by its alias in the script. To correctly identify the file name in a script you must use the variable `${cd_transfer_file}`. The variable is required because the file names might not be known at the time you write the script. When creating a download script you must use `${cd_transfer_file}` to specify the directory where downloaded files are saved. When downloading a single file, use `${cd_transfer_file}<path_separator><file_name>`. For example, `${cd_transfer_file}/xls_sheet.xls`. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

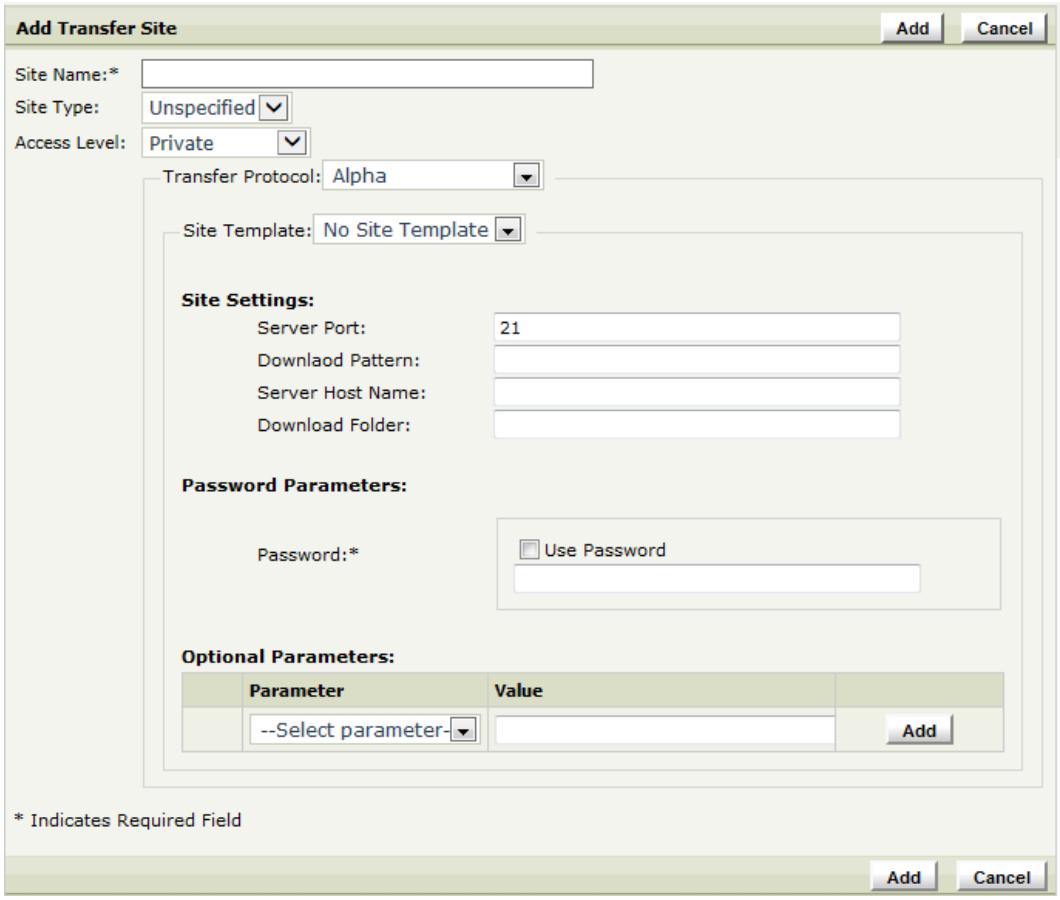
Note The **Send Script** and **Receive Script** accept regular expressions. For more information on writing Connect:Direct scripts, refer to the Connect:Direct documentation.

You can use a site template to define a Connect:Direct transfer site. For more information, see *Site templates* on page 681.

File services interface protocol transfer sites

Each file services interface protocol can have different required and optional parameters as configured by the developer in the file services interface protocol registry file. The developer who created the transfer site protocol can provide you with a list of required and optional parameters with descriptions and valid values.

The following is the *Add Transfer Site* page for a transfer site definition that uses the file services interface transfer.



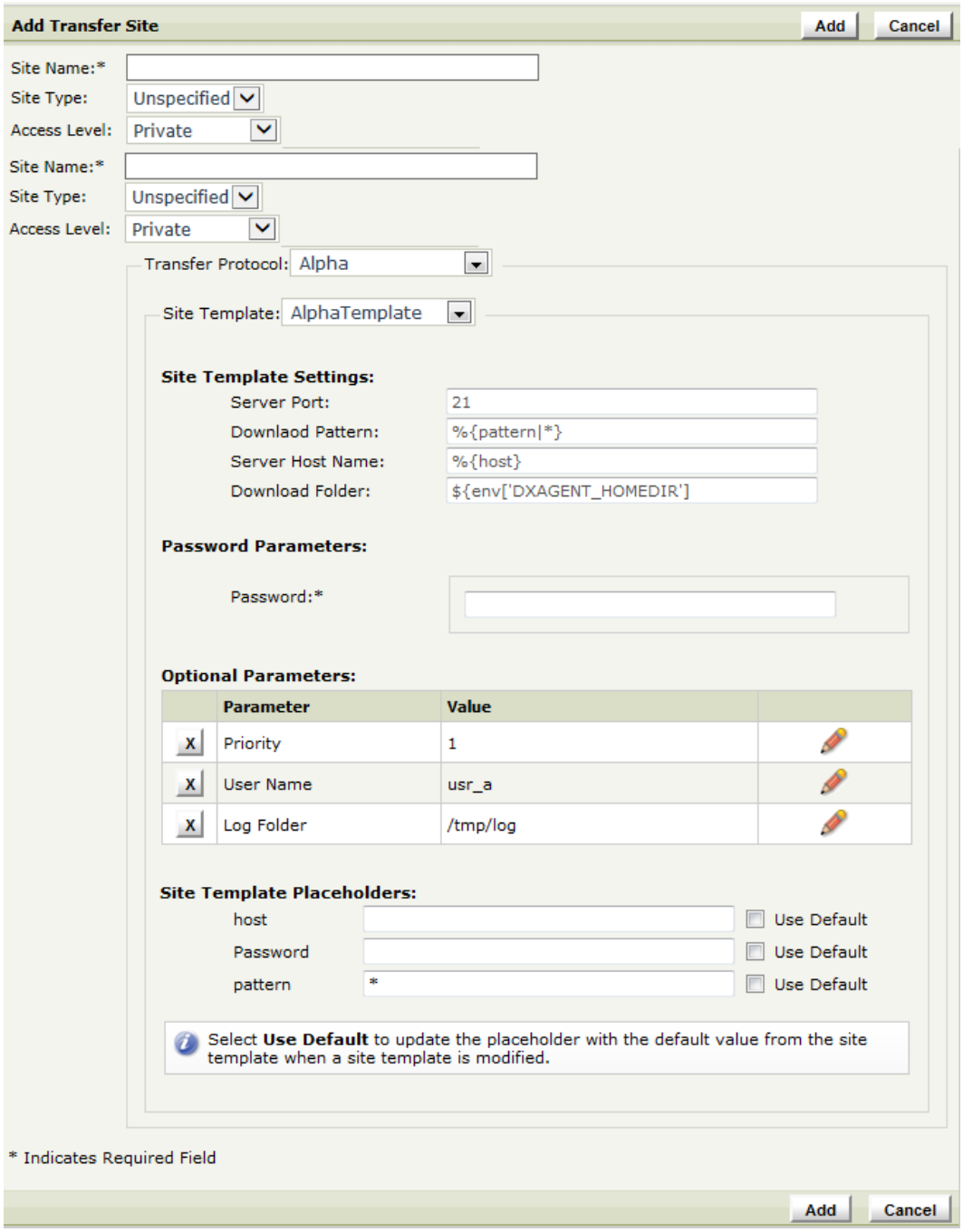
The fields under **Site Settings** are required. If they have default values in the file services interface registry file, the Administration Tool displays those values when the transfer protocol is selected.

To specify a password, select **Use Password** and type the password.

The fields in the **Optional Parameters** table are not required.

- To add an optional parameter, select its name from the **Parameter** list, type a value in the **Value** column, click Add.
- To edit a parameter value, click the Edit icon ( ) type a new value in the **Value** column, and click the Save icon ( ).
- To delete a parameter, click the Delete icon ( ).

You can create a file services interface protocol transfer site using a site template. If you select a template from the **Site Template** list, the transfer site page displays the values from the site template and the list of placeholders you can specify.



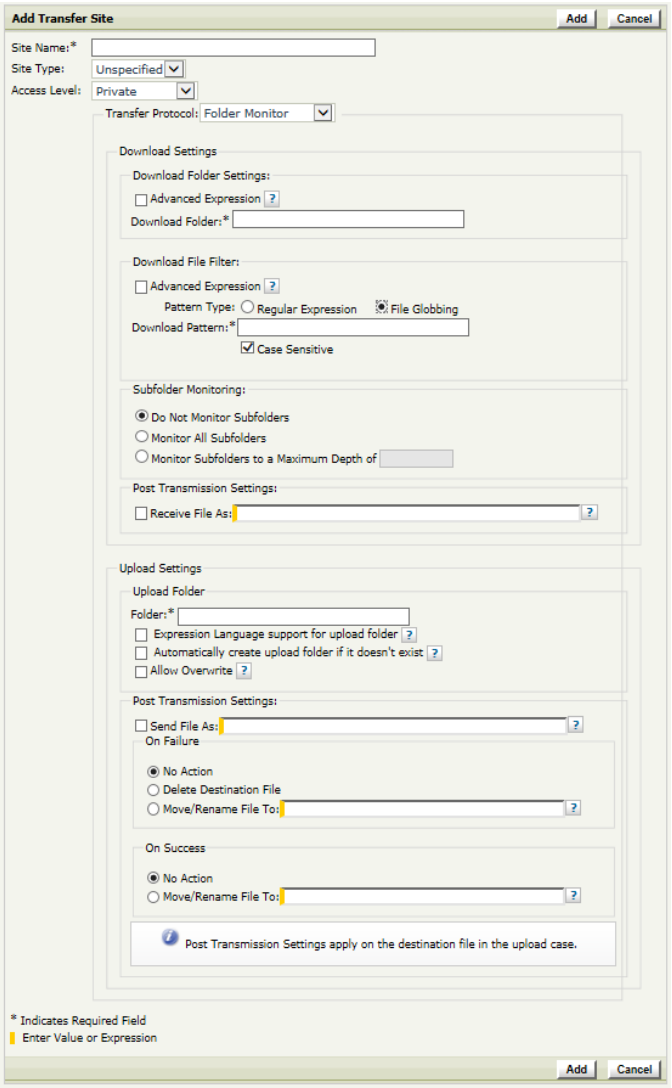
You cannot edit the values in the **Site Template Setting** or the **Optional Parameters**. When you select a site template, the **Site Template Placeholders** fields get the default values from the template. You can type values for these placeholders referenced in the other fields. Select **Use Default** to always use the current default value from the template if it is updated.

You can use a site template to define a file services interface protocol transfer site. For more information, see *Site templates* on page 681.

For more information about file services interface protocols for receiving files from other systems, see *File services interface transfers* on page 958.

Folder Monitor transfer sites

The following is the *Add Transfer Site* page for a transfer site definition that uses the Folder Monitor transfer protocol.



The following table describes the Folder Monitor protocol options for a transfer site.

Field	Description
Download Settings	
Download Folder Settings:	

Field	Description
Advanced Expression	Select **Advanced Expression** to use expression language to evaluate the download folder. To use the expression language to append dates: The download folder will be evaluated using the current date when the transfer site is being executed. For example `folder_20150130`. Example: `folder_${date("yyyyMMdd")}`
Download Folder	The full path to the folder to which incoming file transfers are saved. You cannot enter spaces-only values in this field. **Note** The download folder should not be set to the root (`/`) folder of the operating system, because that can lead to the corruption of the whole Operating System.
Download File Filter:	
Advanced Expression	Select **Advanced Expression** to use expression language to evaluate the download pattern. Using it together with **File Globbing** Pattern Type selected: The download pattern will be evaluated using the current date when the transfer site is being executed. For example `*_20150130.txt`. This will match all files ending with `_20150130.txt`. Example: `*_${date("yyyyMMdd")}.txt` Using it together with **Regular Expression** Pattern Type selected: The download pattern will be evaluated using the current date when the transfer site is being executed. For example `*[a-z]_20150130.txt`. This will match all files starting with any combination of letters from `a` to `z` and ending with `_20150130.txt`. Example: *[a-z]_${date("yyyyMMdd")}.txt
Pattern Type	Select one of two types: **Regular Expression** or **File Globbing**. For regular expression syntax, see *Regular expressions* on page 1035. File globbing uses simple wildcards to specify a pattern. A question mark (`?`) matches any one character. An asterisk (`*`) matches any number of characters.
Download Pattern	The file name pattern or regular expression used to match file names to determine whether a file is processed.
Case Sensitive	Select this check box to enable case-sensitive file name matching.
Subfolder Monitoring	

Field	Description
Do Not Monitor Subfolders	Apply the download pattern to the download folder only.
Monitor All Subfolders	Apply the download pattern to the download folder and all subfolders.
Monitor Subfolders to a Maximum Depth of ___	Apply the download pattern to the download folder and subfolders to the depth specified. For example, if the maximum depth is `2`, apply the download pattern to the download folder and its immediate subfolders.
Download Subfolder Pattern Type	(Displayed only when monitoring subfolders) Select one of two types: **Regular Expression** or **File Globbing**. For regular expression syntax, see *Regular expressions* on page 1035. File globbing uses simple wildcards to specify a pattern. A question mark (`?`) matches any one character. An asterisk (`*`) matches any number of characters.
Download Subfolder Pattern	(Displayed only when monitoring subfolders) The pattern used to match folder names to determine whether to apply the download pattern to the folder. You cannot enter spaces-only values in this field.
Case Sensitive	(Displayed only when monitoring subfolders) Select this check box to enable case-sensitive folder name matching.
Post Transformation Settings	
Receive File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name when the transfer is received. You can use the SecureTransport-specific variable `${stenv.site_target}` which takes the value from the remote file path. See *Expression Language* on page 1020 for information on SecureTransport-specific variables.
Upload Settings	
Upload Folder	The folder from which files to be transferred to the remote host are taken. You cannot enter spaces-only values in this field. **Note** Making the Upload Folder the same as the Download folder may lead to an infinite loop condition when the Transfer Site is used.

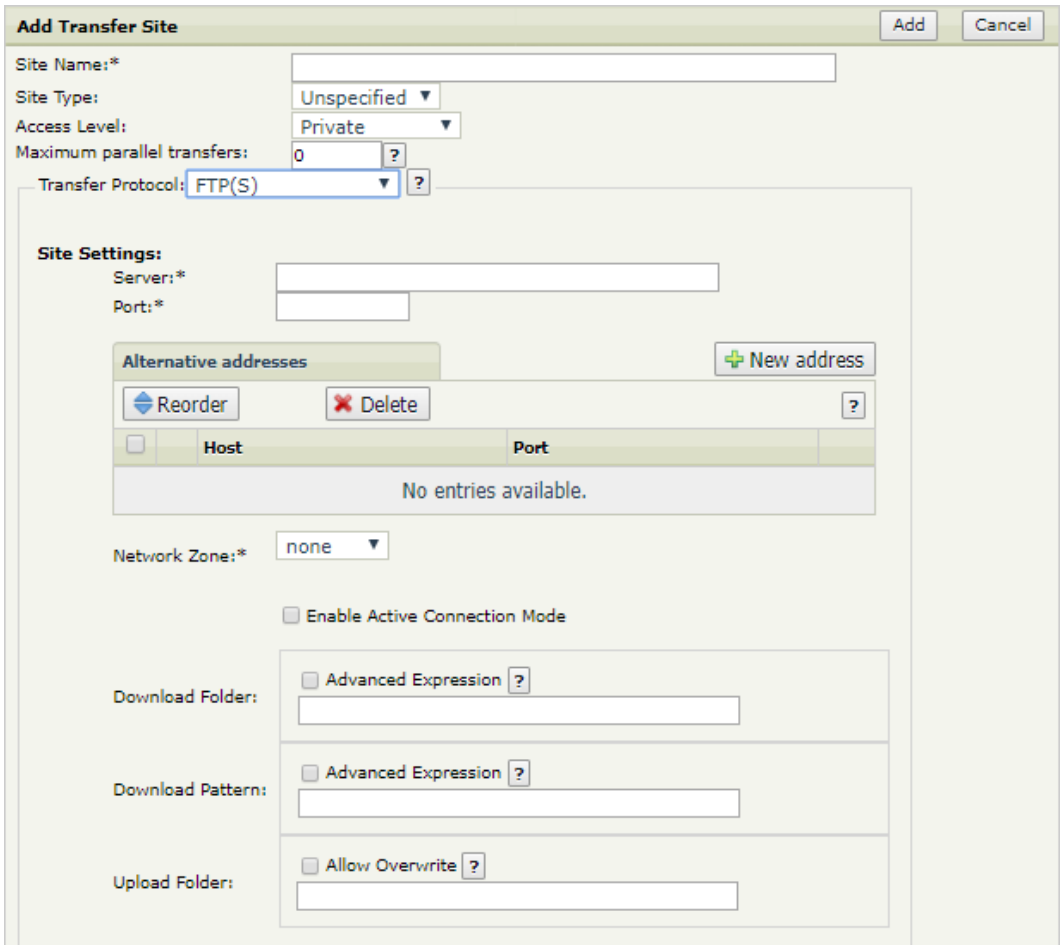
Field	Description
Expression Language support for upload folder	When checked upload folder can contain Expressions.
Automatically create upload folder if it doesn't exist	Upload Folder will be automatically created if it doesn't exist. The automatically created folder will be owned by the user running the SecureTransport TM Server process.
Allow Overwrite	Taken into account when the site is used by Send To Partner step. If checked the value of "Upload folder" will be overwritten with the value of "Overwrite upload folder". For more details see *Advanced Routing* on page 795
Post Transmission Settings	
Send File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name.
On Failure	A failure occurs when the transfer is incomplete and all retry attempts were unsuccessful. Select one of the three choices: **No Action**, **Delete Destination File**, or **Move/Rename File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete Destination File** removes the file from the new location. Selecting **Move/Rename File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.
On Success	Select one of the choices: **No Action**, or **Move/Rename File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Move/Rename File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.

- The Folder Monitor protocol differs from the other supported protocols in the following aspects:
- The folders listed in `<FILEDRIVEHOME>/conf/unsafe.paths.conf` file (and their sub-folders) cannot be specified in the **Upload Folder** and **Download Folder** fields.
- The paths, specified in the **Upload Folder** and **Download Folder** fields, must be full system paths (not relative paths), such as:
  `/tmp/folder_name/opt/TMWD/folder_name/`

- The files uploaded/moved into the specified upload folder are owned by the root user of the system.
- If SecureTransport is installed as a non-root deployment, the files in upload folder are owned by the user running the SecureTransport Server.
- If you configure the account to impersonate a user, the impersonated user must have full rights to the directories specified in the Folder Monitor.
- If you upload or move a file in the specified upload folder and such a file already exists there, it is overwritten without a prompt.
- If SecureTransport is installed as a non-root deployment, the user running the SecureTransport Server must have the necessary permissions to overwrite the file.
- When the Folder Monitor starts to monitor the download folder, the download pattern is applied to all the files in the folder, even if they existed in the download folder before the Folder Monitor began monitoring.
- If SecureTransport is installed as a non-root deployment, the user running the SecureTransport Server must have the necessary permissions to write to the upload folder.
- SecureTransport does not support placing the download folder and the upload folder under a repository encryption user home folder.
- If you create a service account and a Standard Router application that uses a Folder Monitor transfer site, and you specify the same directory for sending and receiving messages, file transfers fail.
- A Folder Monitor transfer site can be used to receive messages for only one subscription.
- The names of the download folder and the upload folder of a Folder Monitor transfer site cannot contain two or more of the following characters in a sequence: `( ) _ - + = { } ~ ! @ # $ % ^ & ; " ” ' ’`. For example, `folder_name` is supported, but `folder_+name` is not supported.
- The name of a file processed by a Folder Monitor transfer site cannot contain two more of the following characters in sequence: `< > | : ? " * / \ % [ ] ~` (at the beginning of the file only).
- Two Folder Monitor transfer sites cannot have the same download folder and download pattern.
- The Folder Monitor service runs on the primary server in a Standard Cluster (SC). If that server fails, the Folder Monitor service automatically fails over to the new primary server.
- The Folder Monitor service runs on one server in an Enterprise Cluster (EC). If that server fails, the Folder Monitor service automatically fails over to the server in the cluster with the Transaction Manager that has been running the longest.

FTP(S) transfer sites

The following screen presents the *Add Transfer Site* page for a transfer site definition that uses the FTP(S) transfer protocol.



The following table describes the FTP(S) protocol options for a transfer site.

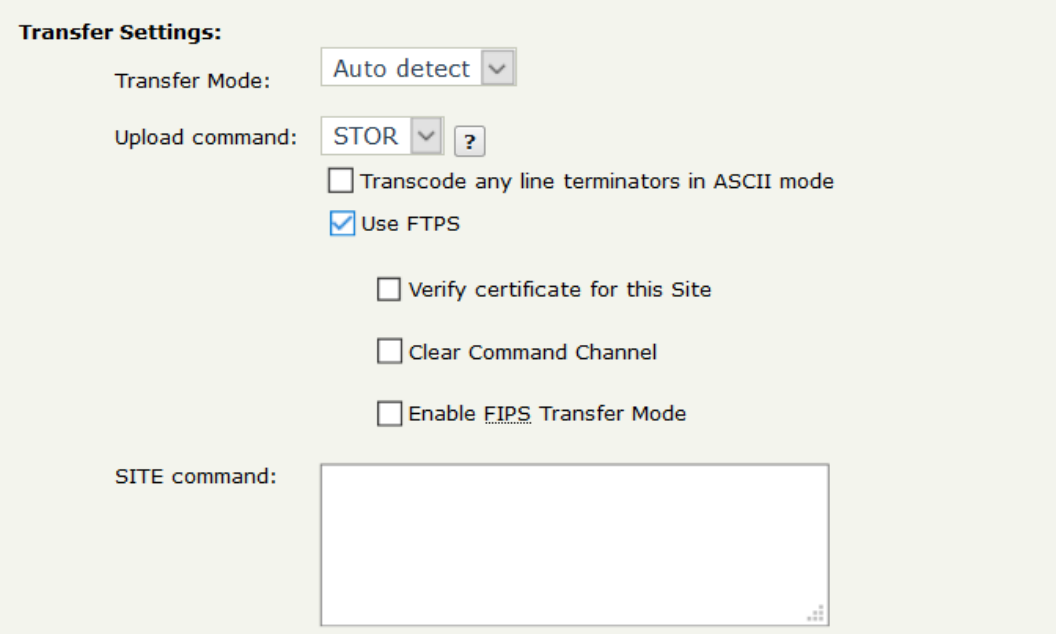
Field	Description
Site Settings	
Server	The host name or IP address of the remote server to connect to for file transfers. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Port	The port on the remote server to be used for file transfers. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

Field	Description
Alternative addresses	Visibility of this option is controlled via a Server configuration option. This set of options allow you to add, delete and set a priority order of alternative endpoints. These endpoints act as backup alternatives to the configured Server-Port Site Settings and are particularly useful in cases of transfer failures. Specifying alternative endpoints as backup servers provides a way to temporarily reroute pending transfers and minimize the risk of transfer failure. As with the Server-Port site settings, the connection to each alternative endpoint is defined by its host name (or IP address) and port number. • To add an alternative server endpoint, click **New Address**. The Alternative Addresses table expands with a new row, that allows you to enter a hostname (or IP address), a port number and save these changes. • To delete an alternative server endpoint, select the corresponding check-box on the same row and click **Delete**. • To reorder the list of alternative endpoints, click **Reorder**. A new option (upward and downward arrow) appears next to each entry. You must hover with the mouse pointer over this newly appeared option and the mouse pointer will assume the "move" shape: a four-directional arrow pointer. This indicates which alternative endpoint is on focus. You can now drag & drop it up and down to the order number you want it at. Perform this action with other alternative endpoints until the list is ordered according to your needs. When you are done, click **Save Order** to keep the newly changed order. **Note** Visibility of this option is controlled with the value set for the `TransferSite.AlternativeAddresses.retryPolicy` configuration option. It allows you to set a "retry policy" with a list of alternative endpoints (presented in IP address: Port number pairs or hostname) you define on this screen. But before you are able to do so, you must go to **Operations > Server Configuration** and set the policy type using either of the following values: • `AllHostsOnEachRetry` – with this policy SecureTransport iterates through each endpoint, one by one, starting with the first in the list. If connection not successful, SecureTransport will continue trying each endpoint one after another until the maximum number of retries is reached. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `OneHostOnEachRetry` – with this policy SecureTransport tries to connect to the first endpoint in the list. If connection not successful, SecureTransport will continue trying that endpoint until the maximum number of retries is reached; and then will move to the next one in the list. Following that same pattern, SecureTransport will try each endpoint until success; or until end of list. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `Disabled` (default) – this is the default value that keeps the table with

Field	Description
	endpoints entirely hidden from view.
Network Zone	The network zone that defines the proxies to use for transfers through this site. • Select **none** to connect directly to the remote FTP server. • Select **any** to allow SecureTransport to select the proxy connection using a network zone that enables an SOCKS5 proxy. • Select **Default** to use the default network zone proxy configuration. If no default is network zone is defined, transfers from this transfer site fail. • Select a specific network zone to use the proxy configuration defined for that zone. For more information, see *Specify TM Server communication ports and IP address for protocol servers on SecureTransport Edge* on page 224.
Enable Active Connection Mode	Determines whether passive or active connection mode is used by SecureTransport for server-initiated transfers over FTP. When selected, Active FTP is used.
Download Folder	The folder on the remote server from which the file are transferred. If **Advanced Expression** is selected for Download Folder, the download folder is evaluated using expression language. To use the expression language to append dates: The download folder will be evaluated using the current date when the transfer site is being executed. For example `folder_20150130`. Example: `folder_${date("yyyyMMdd")}`
Download Pattern	The pattern used to match file names to determine whether a file is downloaded. Asterisk (`*`) matches zero or more characters and question mark (`?`) matches one character. If **Advanced Expression** is selected for Download Pattern, the download pattern is evaluated using expression language. To evaluate the download pattern using dates: The download pattern will be evaluated using the current date when the transfer site is being executed. For example `*_20150130.txt`. This will match all files ending with `_20150130.txt`. Example: `*_${date("yyyyMMdd")}.txt`
Allow Overwrite	Taken into account when the site is used by Send To Partner step. If checked the value of "Upload folder" will be overwritten with the value of "Overwrite upload folder". For more details see *Advanced Routing* on page 795.
Upload Folder	The folder on the remote server to which files are transferred.

Transfer Settings

The Transfer Settings options allow you to define various transfer settings with your current transfer site.

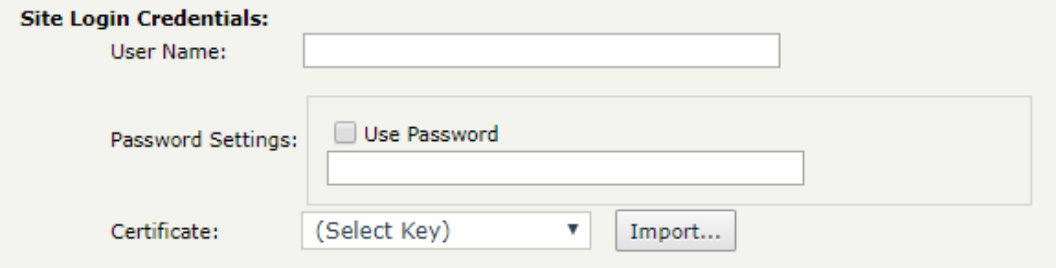


Field	Description
Transfer Settings	
Transfer Mode	Specify whether data is transferred as ASCII or binary. You can also choose to have SecureTransport automatically determine the correct transfer mode. For more information about automatically determining transfer mode, see *Transfer mode for server-initiated transfers* on page 702.
Upload command	Define the FTP command to be used in requests when server-initiated transfers are executed: **STOR** - select to use the *STOR* command for server-initiated transfers. **APPE** - select to use the *APPE* command for server-initiated transfers. **Note** **STOR** is the default command for FTP server-initiated transfers. Upload command is reported to Axway Sentinel and displayed in the Protocol Parameter attribute.
Transcode any line terminators in ASCII mode	When checked it forces SecureTransport to transcode any sequence of line terminators when ASCII mode is used.

Field	Description
Use FTPS	Deselect to use FTP instead of FTPS.
Verify certificate for the Site	Select to verify that the remote system is trusted. This option is displayed when **Use FTPS** is selected.
Clear Command Channel	Select to accept and process a Clear Command Channel subcommand. If the user is authorized to perform the command, send a confirmation message, and change the control connection transmission mode to clear text. This option is displayed when **Use FTPS** is selected.
TLS Shutdown on CCC	Perform a TLS shutdown upon receiving a Clear Command Channel subcommand. This option is displayed when **Clear Command Channel** is selected. **Note** When closing a TLS connection, such as when issuing a CCC command, each party is required to send a `close_notify` before closing the connection. This is mandated by RFC 2246. If both the client and server do not acknowledge that the TLS connection is ending they may be susceptible to a TLS truncation attack. From a security standpoint, Axway recommends that both TLS shutdowns be checked when configuring the transfer site CCC option. When performing FTP transfers to a remote SecureTransport Server, you must configure `Ftp.CCC.TlsShutdownInitiator` for the server. As a result the client sends *Close notify* and the server responds with *Close notify*, the server-initiated transfer is successful, and the partners are not susceptible to a TLS truncation attack.
Enable FIPS Transfer Mode	Restrict FTPS to use only FIPS 140-2 Level 1 certified cryptographic libraries. This option is displayed when **Use FTPS** is selected. When you enable FIPS transfer mode, the panel expands with an additional field that lets you specify the desired set of cipher suites to be used in FIPS mode for server-initiated transfers through this site. By default, this set is populated with the cipher suites as defined in the `Ftps.FIPS.SIT.Ciphers` configuration option. You can add or remove cipher suites. The supported FIPS cipher suites from which you can select when adding a new one are listed in *FIPS transfer mode* on page 983. Note that both the sender and the recipient must use supported FIPS ciphers suites. Otherwise, the transfer will fail.
SITE command	Enter a SITE command. You use this command to provide services specific to your system that are not available as FTP commands.

Site Login Credentials

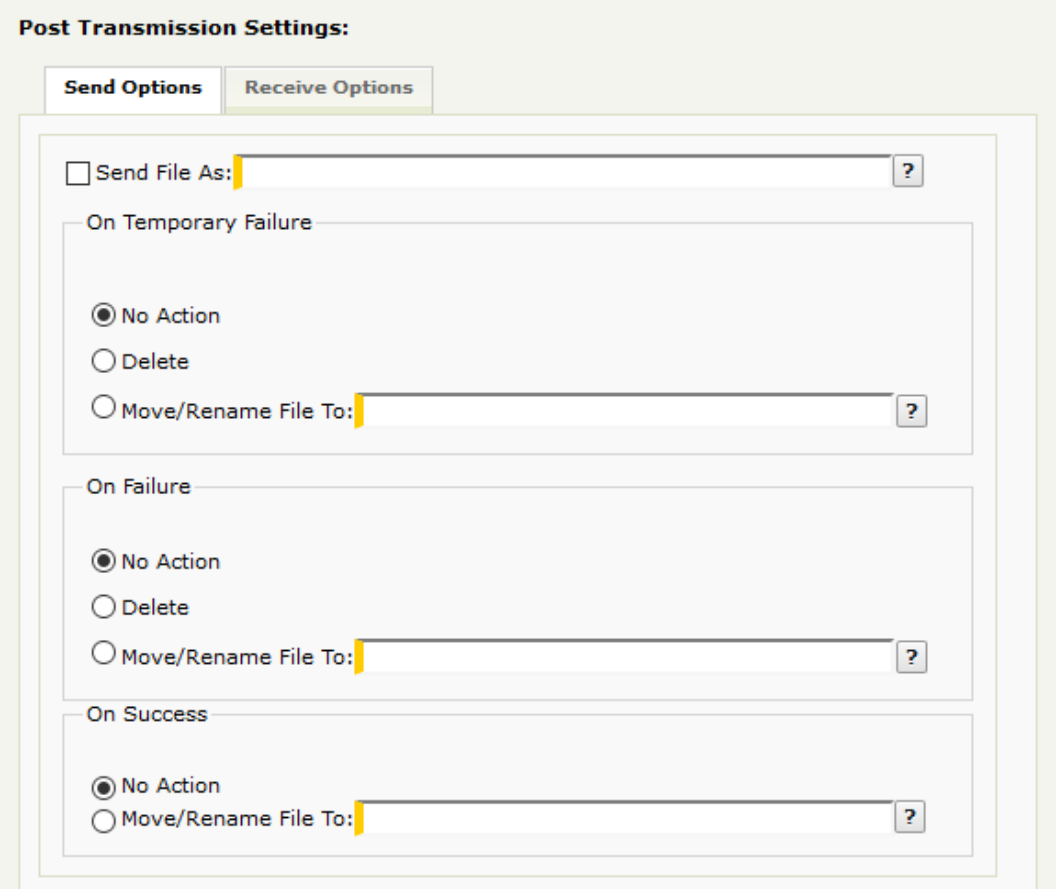
The Site Login Credentials options allow you to define credentials and / or add a certificate for login to the FTP(S) server.



Field	Description
Site Login Credentials	
User Name	The user name to log in to the FTP server. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Use Password	Select to use a password to log in to the FTP server.
Password	Password used to log in to the FTP server.
Certificate	A private certificate for SecureTransport to use to log in to the FTP server. You can select a certificate or import a certificate. This field is displayed when **Use FTPS** is selected. By default, the usage of expired X509 certificates is allowed for SIT transfers. To forbid it, set the `SIT.allowExpiredCertificates` to `false`.

Post Transmission Settings: Send Options

The Send Options allow you to define post transmission actions on success and failure.



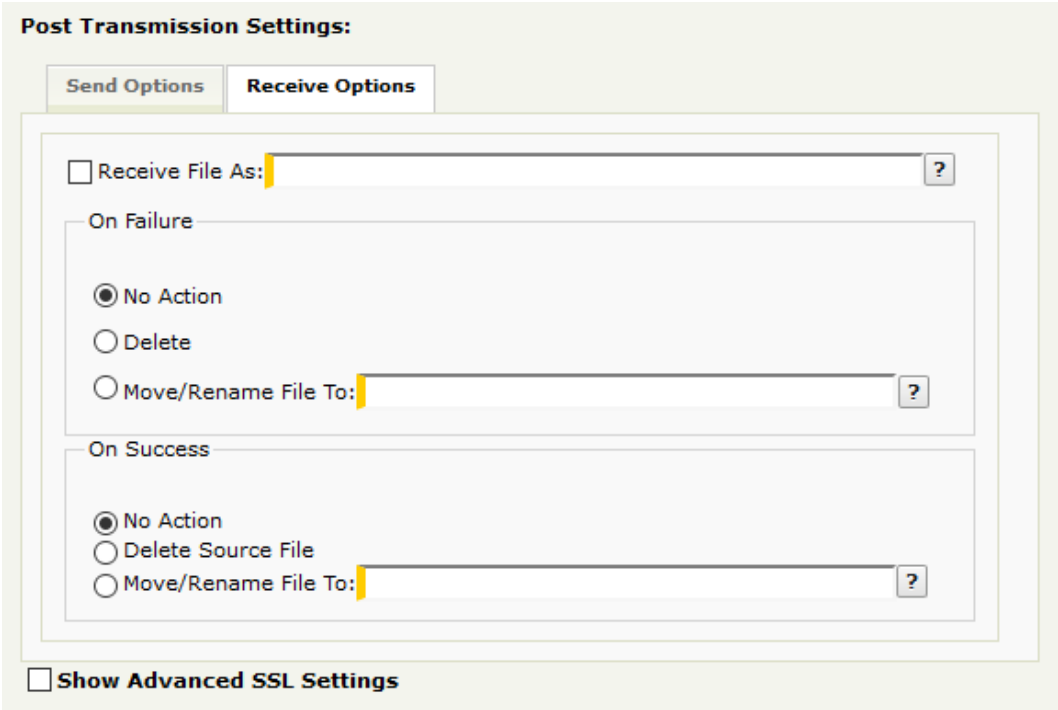
Field	Description
Send Options	
Send File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name.
On Temporary Failure	A temporary failure can occur when the transfer is incomplete and a retry occurs. Select one of the three choices: **No Action**, **Delete Destination File**, or **Move File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete Destination File** removes the file from the new location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.

Field	Description
On Failure	A failure occurs when the transfer is incomplete and all retry attempts were unsuccessful. Select one of the three choices: **No Action**, **Delete Destination File**, or **Move File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete Destination File** removes the file from the new location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.
On Success	Select one of the choices: **No Action**, or **Move File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.

Note To preserve the original file name when using the **Move File To** option, use the `${stenv.target}` or `${stenv['target']}` expressions.

Post Transmission Settings: Receive Options

The Receive options allow you to define post transmission actions on success and failure.

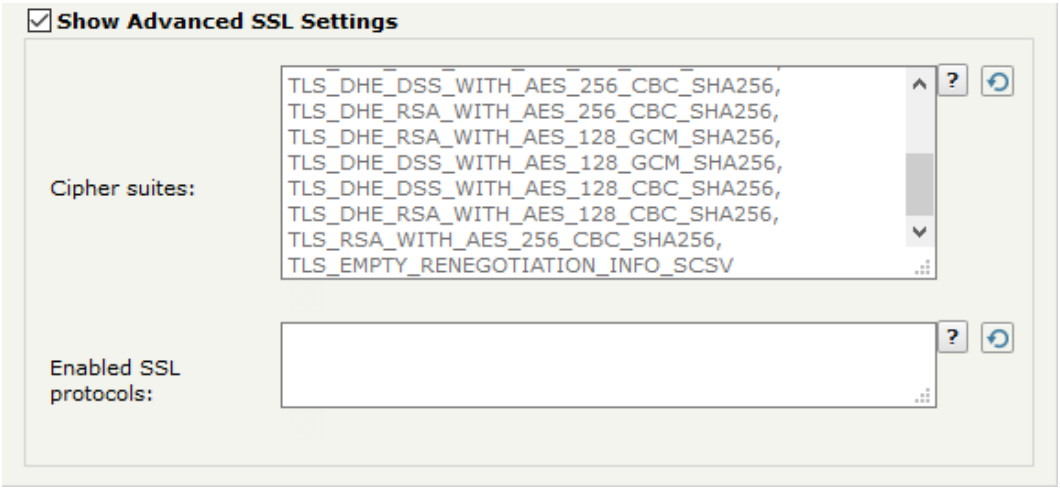


Field	Description
Receive Options	
Receive File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name when the transfer is received. You can use the SecureTransport-specific variable `${stenv.site_target}` which takes the value from the remote file path. see *Expression Language* on page 1020 for information on SecureTransport-specific variables.
On Failure	A failure occurs when the transfer is incomplete and all retry attempts were unsuccessful. Select one of the three choices: **No Action**, Delete Source File, or **Move File To**. Selecting **No Action** causes the file to stay in the original location. If another file with the same name is transferred to this location, the original file is overwritten. Selecting Delete Source File removes the file from the original location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files from and to provide an expression used to rename the file.
On Success	Select one of the three choices: **No Action**, Delete Source File, or **Move File To**. Selecting **No Action** causes the file to stay in the original location. If another file with the same name is transferred to this location, the original file is overwritten. Selecting Delete Source File removes the file from the original location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files from and to provide an expression used to rename the file.

Note To preserve the original file name when using the **Move File To** option, use the `${stenv.target}` or `${stenv['target']}` expressions.

Advanced SSL Settings

Advanced SSL settings allow you to define Cipher suites and SSL protocols with your current FTP(S) Transfer Site.



Field	Description
Show Advanced SSL Settings	
Cipher suites	The set of cipher suites available with the current FTP(S) transfer site for secure SIT connection. By default this set is populated with the cipher suites as defined in the `Ftps.SIT.Ciphers` configuration option. To reset to default values, click the button next to the tooltip.
Enabled SSL protocols	The available SSL protocols for secure SIT connection with the current FTP(S) transfer site. By default this option uses the SSL protocols as defined in the `Ftps.SIT.EnabledProtocols` configuration option. To reset to default values, click the button next to the tooltip.

Supported Active / Passive FTP(S) connections

This table describes the supported Active/Passive FTP(S) connection modes for client/server-initiated transfers over FTP(S).

FTP Exchange type	Active FTP mode supported	Passive FTP mode supported
Client initiated via Edges	Yes	Yes
Server initiated via Edges	No	Yes
Server initiated - no Edges/direct connection	Yes	Yes

Generic HTTP transfer sites

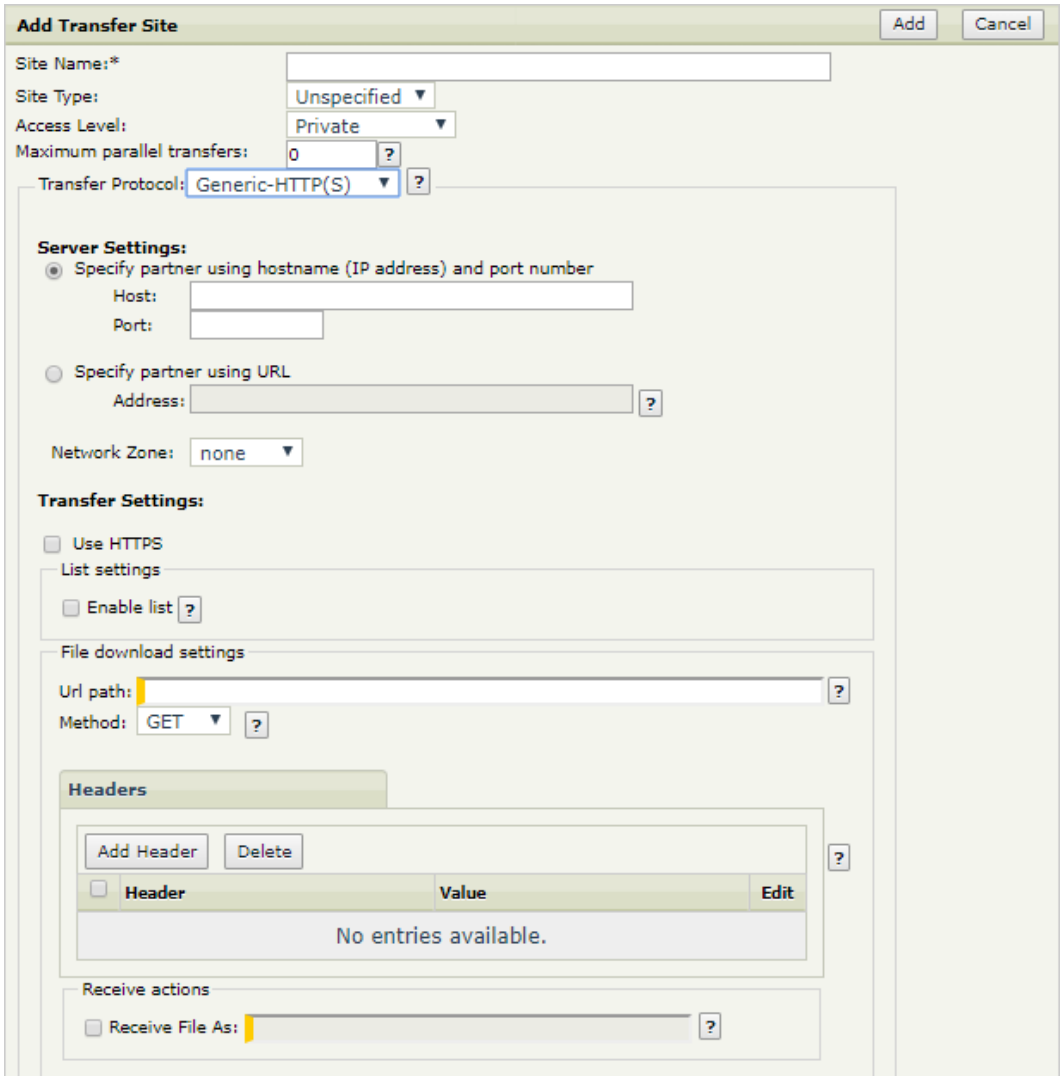
The Generic HTTP transfer site enables file exchange via HTTP protocol with third-party partners over an authenticated connection.

The supported authentication methods are:

- Basic – The client provides a user ID or user ID and password when exchanging files.
- Form-Based – The client will send a request to a remote HTTP server to obtain an authentication cookie.
- Certificate – A HTTPS client certificate is used for mutual authentication. The client certificate can be used in combination with basic or form-based authentications.

The Generic HTTP transfer site can be used with the Basic and Advanced Routing applications for push and pull server-initiated transfers.

The following is the *Add Transfer Site* page for a transfer site definition that uses the Generic HTTP transfer protocol.



The following sections describe the Generic HTTP transfer site configuration options, provide basic sample push and pull flow configurations for Generic HTTP transfer sites, and information on the limited expression language supported by Generic HTTP transfer sites:

- *Configuration options* on page 527
- *Sample configuration — List files and download* on page 542
- *Sample configuration — Download file* on page 544
- *Sample configuration — Upload file* on page 546
- *Sample configuration — Push file to SecureTransport user using Form Authentication* on page 549
- *Supported expression language* on page 551

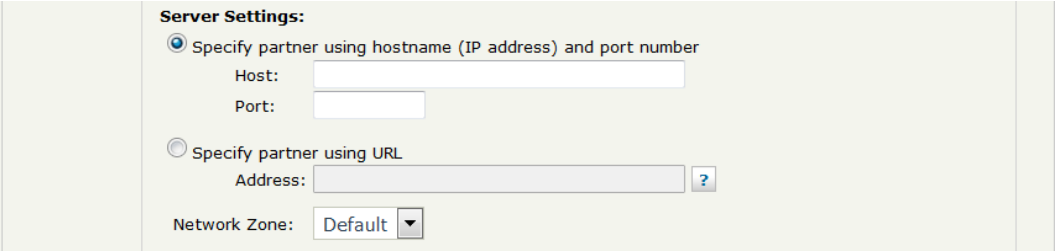
Configuration options

Configuring a Generic HTTP transfer site consists of making selections and completing fields for the following:

- *Server settings* on page 527
- *Transfer settings* on page 528
- *List settings* on page 529
- *File download settings* on page 531
- *Receive actions* on page 534
- *Upload settings* on page 535
- *Send actions* on page 537
- *Login settings* on page 538
- *Advanced settings* on page 540

Server settings

The following example shows the server settings for a Generic HTTP transfer site.



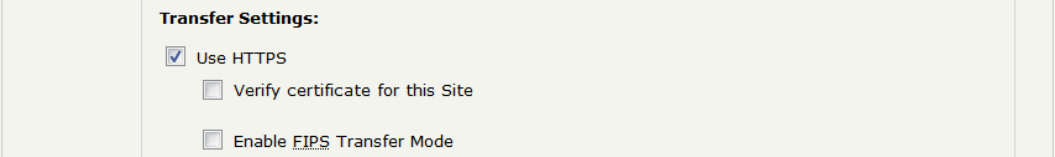
The following table describes the server settings for defining a Generic HTTP transfer site.

Field	Description
Server Settings	
Specify partner using hostname (IP address) and port number	When selected, the partner will be specified using the partner hostname and port number.
Host	The host name or IP address of the remote host to connect to for file transfers.
Port	The port on the remote host to be used for file transfers.
Specify partner using URL	When selected, the partner will be specified using an URL.

Field	Description
Address	A URL that specifies the partner host. It can also include the port and a directory. Examples: • `http://example.com` • `https://example.com:443` • `https://example.com:443/websealjun/`
Zone	The network zone that defines the proxies to use for transfers through this site. • Select **none** to connect directly to the remote HTTP server. • Select **any** to allow SecureTransport to select the proxy connection using a network zone that enables an HTTP proxy. • Select **Default** to use the default network zone proxy configuration. If no default is network zone is defined, transfers from this transfer site fail. • Select a specific network zone to use the proxy configuration defined for that zone. For more information, see *Specify TM Server communication ports and IP address for protocol servers on SecureTransport Edge* on page 224.

Transfer settings

The following example shows the transfer settings for a Generic HTTP transfer site.



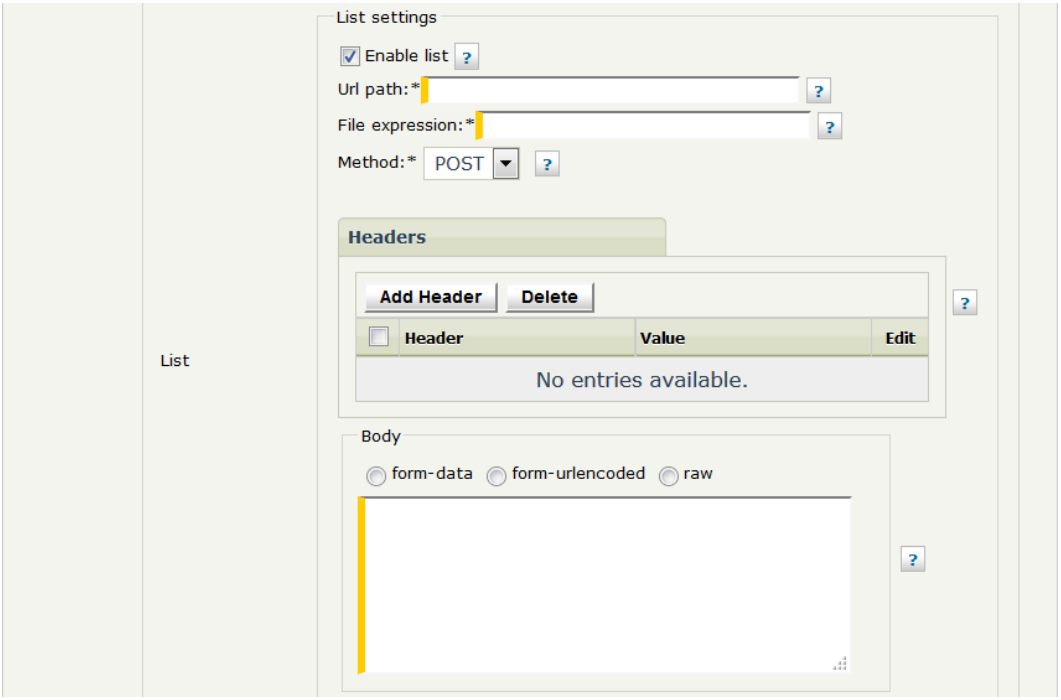
The following table describes the transfer settings for defining a Generic HTTP transfer site.

Field	Description
Transfer Settings	
Use HTTPS	A check box indicating if the connection should be secured or not. Deselect this check box to use HTTP instead of HTTPS.

Field	Description
Verify certificate for this Site	Select to verify that the remote system is trusted. This field is displayed when **Use HTTPS** is selected.
Enable FIPS Transfer Mode	Restrict HTTPS to use only FIPS 140-2 Level 1 certified cryptographic libraries. This field is displayed when **Use HTTPS** is selected. The sender and the recipient must use the ciphers and ciphers suites listed in *FIPS transfer mode* on page 983. If the sender and the recipient do not provide the required ciphers and ciphers suites SecureTransport does not complete the transfer.

List settings

The following example shows the list settings for a Generic HTTP transfer site.



The following table describes the list settings for defining a Generic HTTP transfer site.

Field	Description
List settings	

Field	Description
Enable list	A check box indicating if the Generic HTTP transfer site will operate in the single file download mode or will list files and then perform the download operation(s). If checked, the Generic HTTP transfer site will take as an input the result of the configured request and use it as a source for retrieving a list of files to be downloaded. It will then will use the *File download settings* to download each file from the list.

URL path	The HTTP server path that will be used to list files on the remote server:
	• A server absolute path when the partner is specified using a hostname (IP address) and port number.
	Example:
	`/list.php`
	• A server relative path when the partner is specified using an URL.
	Example:
	`list.php`
	The limited expression language can be used to specify the URL.
	Example:
	If the value in **Specify partner using URL** is `https://<host>:<port>/downloads/` and the value for **URL path** is `/list.php`, the final URI that will be resolved is `https://<host>:<port>/list.php`. This occurs because `/list.php` is an absolute path and not a relative path. If the value for **URL path** is `list.php`, the final URI that will be resolved is `https://<host>:<port>/downloads/list.php`.
	This field is displayed when **Enable list** is checked.

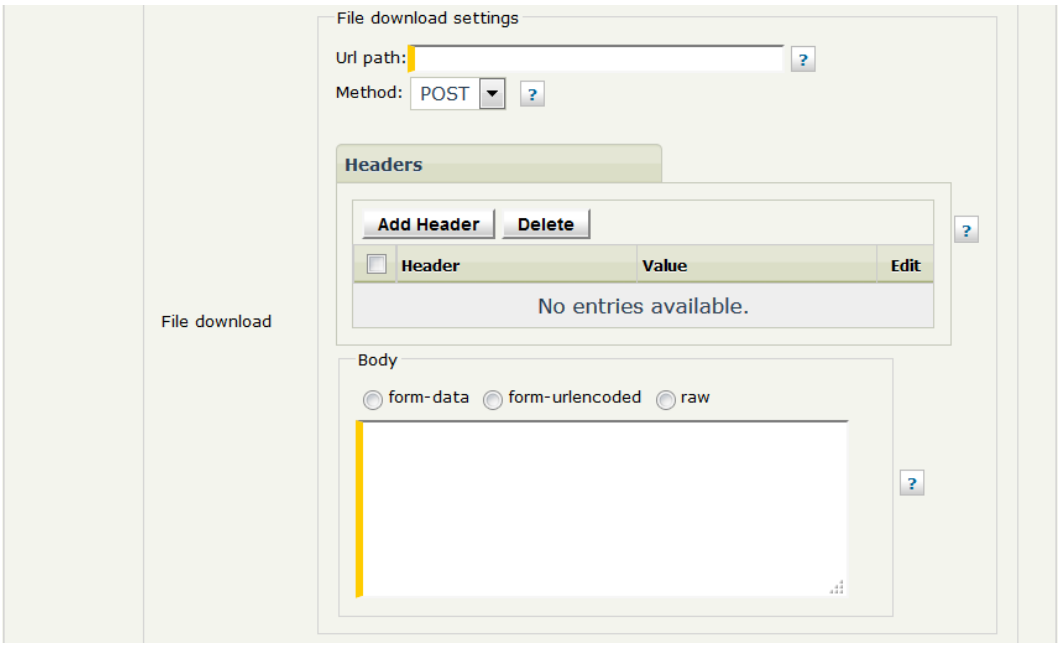
File expression	The expression for the file names that will be applied on the response for the list request to extract the files list. A Java regular expression and the SecureTransport expression language can be used to specify a pattern to match the files that need to be downloaded. It is possible to use () parenthesis in the file expression and everything within the parenthesis will be considered the file name. Example: Filename= `(/something/folder/file\\d.txt)` If they are not used, the matched expression will be the file name. The limited expression language can be used to specify the file name. This field is displayed when **Enable list** is checked.
Method	The HTTP method to be used for listing the files on the remote server. Either **GET** or **POST** can be selected. This field is displayed when **Enable list** is checked.

Field	Description
Headers	The HTTP headers that will be added in the HTTP request for listing files on the remote server. To add a header, click **Add Header** and complete the **Header** and **Value** fields. To edit a header, click the **Edit** ( ) icon and change the **Header** and **Value** fields. To delete a header, select the header to delete and click **Delete**. This Header option is displayed when **Enable list** is checked.

Body	The body of the request for listing files on the remote server. This field is displayed when the selected list Method is **POST**.
	The limited expression language can be used to specify the file name.
	The body can be any of the following types:
	• **form-data** - When selected the body will be transmitted as `multipart/form-data`.
	• **form-urlencoded** - When selected the body will be transmitted as `application/x-www-form-urlencoded`.
	• **raw** – When selected the body can be any text.
	Note When the selected body content type is **form-data** or **form-urlencoded** the body should be formed of key-value pairs on separate lines. Example:
	`param1=value1`
	`param2=value2`
	This field is displayed when **Enable list** is checked and **POST** is the selected Method.

File download settings

The following example shows the file download settings for a Generic HTTP transfer site.



The following table describes the file download settings for defining a Generic HTTP transfer site.

Field	Description
File download	
File download settings	

Field	Description

URL path	The HTTP server path used to download file(s):
	• A server absolute path when the partner is specified using a hostname (IP address) and port number.
	Example:
	`/download.php`
	• A server relative path when the partner is specified using an URL.
	Example:
	`download.php`
	If **Enable list** is checked, this URL will be used to download file(s) extracted from the list operation.
	The limited expression language can be used to specify the URL.
	The available environment variables are:
	• `${env['ts_relative_path']}` - The relative path of the file that will be downloaded.
	• `${env['ts_target']}` - The file name of the file that will be downloaded.
	Example:
	If the value in **Specify partner using URL** is `https://<host>:<port>/downloads/` and the value for **URL path** is `/download.php`, the final URI that will be resolved is `https://<host>:<port>/download.php`. This occurs because `/download.php` is an absolute path and not a relative path. If the value for **URL path** is `download.php`, the final URI that will be resolved is `https://<host>:<port>/downloads/download.php`.

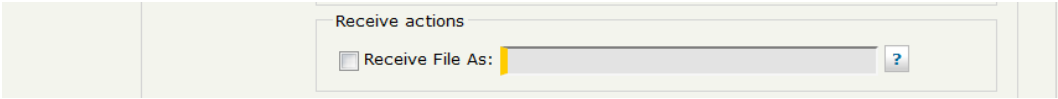
Method	The HTTP method to be used for the file download operation. Either **GET** or **POST** can be selected. If **Enable list** is checked, this method will be used when performing all download operations for the files listed on the remote server.
Headers	The HTTP headers that will be added in the HTTP download request. If **Enable list** is checked, these headers will be added in the all HTTP download requests for the files listed on the remote server. To add a header, click **Add Header** and complete the **Header** and **Value** fields. To edit a header, click the **Edit** () icon and change the **Header** and **Value** fields. To delete a header, select the header to delete and click **Delete**.

Field	Description

Body	The body of the download request. This field is displayed when the selected download Method is **POST**. If **Enable list** is checked, the body will be added in the all HTTP download requests.
	The limited expression language can be used to specify the body.
	The body can be any of the following types:
	• **form-data** - When selected the body will be transmitted as `multipart/form-data`.
	• **form-urlencoded** - When selected the body will be transmitted as `application/x-www-form-urlencoded`.
	• **raw** – When selected the body can be any text.
	The available environment variables are:
	• `${env['ts_content-disposition']}` - The value of the content disposition header presented from the remote HTTP server (if available).
	• `${env['ts_relative_path']}` - The relative path of the file that will be downloaded.
	• `${env['ts_target']}` - The file name of the file that will be downloaded.
	Note When the selected body content type is **form-data** or **form-urlencoded** the body should be formed of key-value pairs on separate lines. Example:
	`param1=value1`
	`param2=value2`

Receive actions

The following example shows the receive actions for a Generic HTTP transfer site.



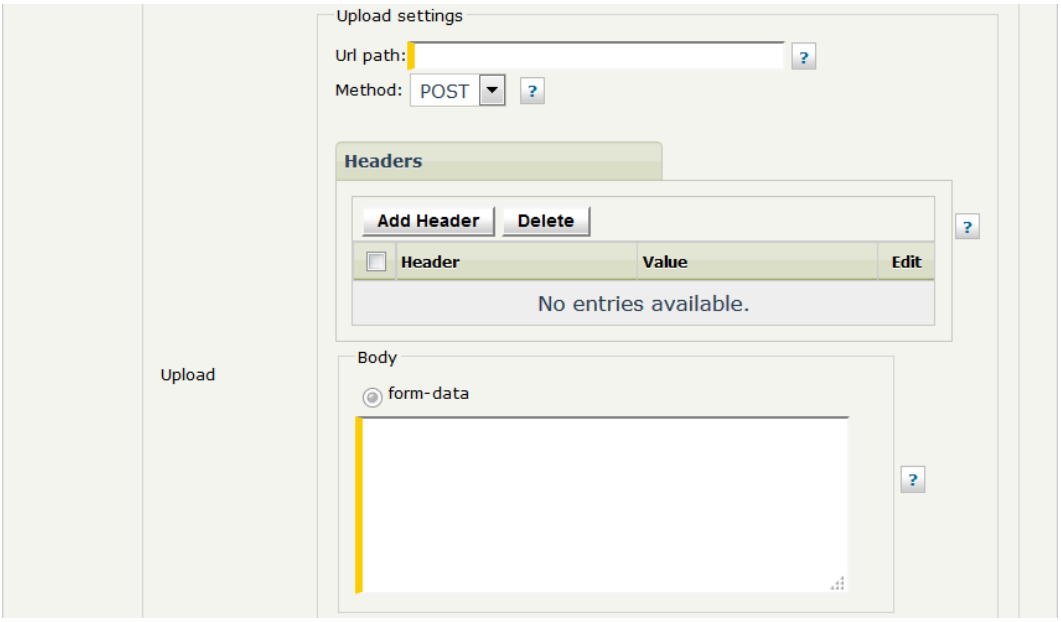
The following table describes the receive actions for defining a Generic HTTP transfer site.

Field	Description
Receive actions	

Field	Description
Receive File As	Select the check box to enable renaming the received file and to specify a value to be used to rename the file. The limited expression language can be used to specify the file name. Examples: • `${env['ts_content-disposition']}` • `${env['ts_relative_path']}` • `${env['ts_target']}` • `${env['ts_target']}_${random()}` • `${date('yyyyddMMHHmmss')}` The available environment variables are: • `${env['ts_content-disposition']}` - The value of content disposition header presented from the remote HTTP server (if available). • `${env['ts_relative_path']}` - The relative path of the file that will be downloaded. • `${env['ts_target']}` - The file name of the file that will be downloaded

Upload settings

The following example shows the upload settings for a Generic HTTP transfer site.



The following table describes the upload settings for defining a Generic HTTP transfer site.

Field	Description
Upload	
Upload settings	

URL path	The HTTP server path to be used for uploading files to the remote server:
	• A server absolute path when the partner is specified using a hostname (IP address) and port number.
	Example:
	`/upload.php`
	• A server relative path when the partner is specified using an URL.
	Example:
	`upload.php`
	The limited expression language can be used to specify the URL.
	The available environment variable is:
	• `${env['ts_target']}` - The file name of the file that will be uploaded.
	Example:
	If the value in **Specify partner using URL** is `https://<host>:<port>/uploads/` and the value for **URL path** is `/upload.php`, the final URI that will be resolved is `https://<host>:<port>/upload.php`. This occurs because `/upload.phpt` is an absolute path and not a relative path. If the value for **URL path** is `upload.php`, the final URI that will be resolved is `https://<host>:<port>/uploads/upload.php`.

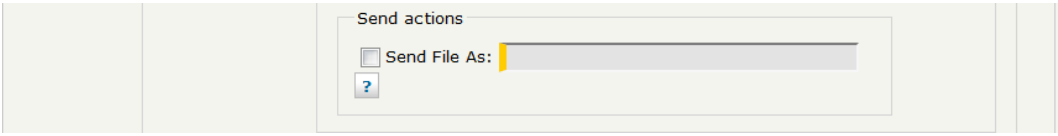
Method	The HTTP method used when uploading files to a remote server. Either **PUT** or **POST** can be selected. This field is displayed when **Enable list** is checked.
Headers	The HTTP headers that will be added in the HTTP request for upload. To add a header, click **Add Header** and complete the **Header** and **Value** fields. To edit a header, click the **Edit** ( ) icon and change the **Header** and **Value** fields. To delete a header, select the header to delete and click **Delete**.

Field	Description

Body	The body of the request for uploading files on the remote server. This option is displayed when the selected upload Method is **POST**.
	The limited expression language can be used to specify the body.
	The available environment variables are:
	• `${env['ts_target']}` - The file name of the file that will be uploaded.
	• `${env['ts_file_form_parameter_name']}` - The name of the form input element with file type on the remote server.
	The body can be of the following type:
	• **form-data** – When selected the body will be transmitted as a `multipart/form-data`.
	Note The body should be formed as key-value pairs on separate lines. Example:
	`param1=value1`
	`param2=value2`
	Example of how to use the environment variables in the body:
	`filename=${env['ts_target']}`
	`${env['ts_file_form_parameter_name']}=myDoc`

Send actions

The following example shows the send actions for a Generic HTTP transfer site.

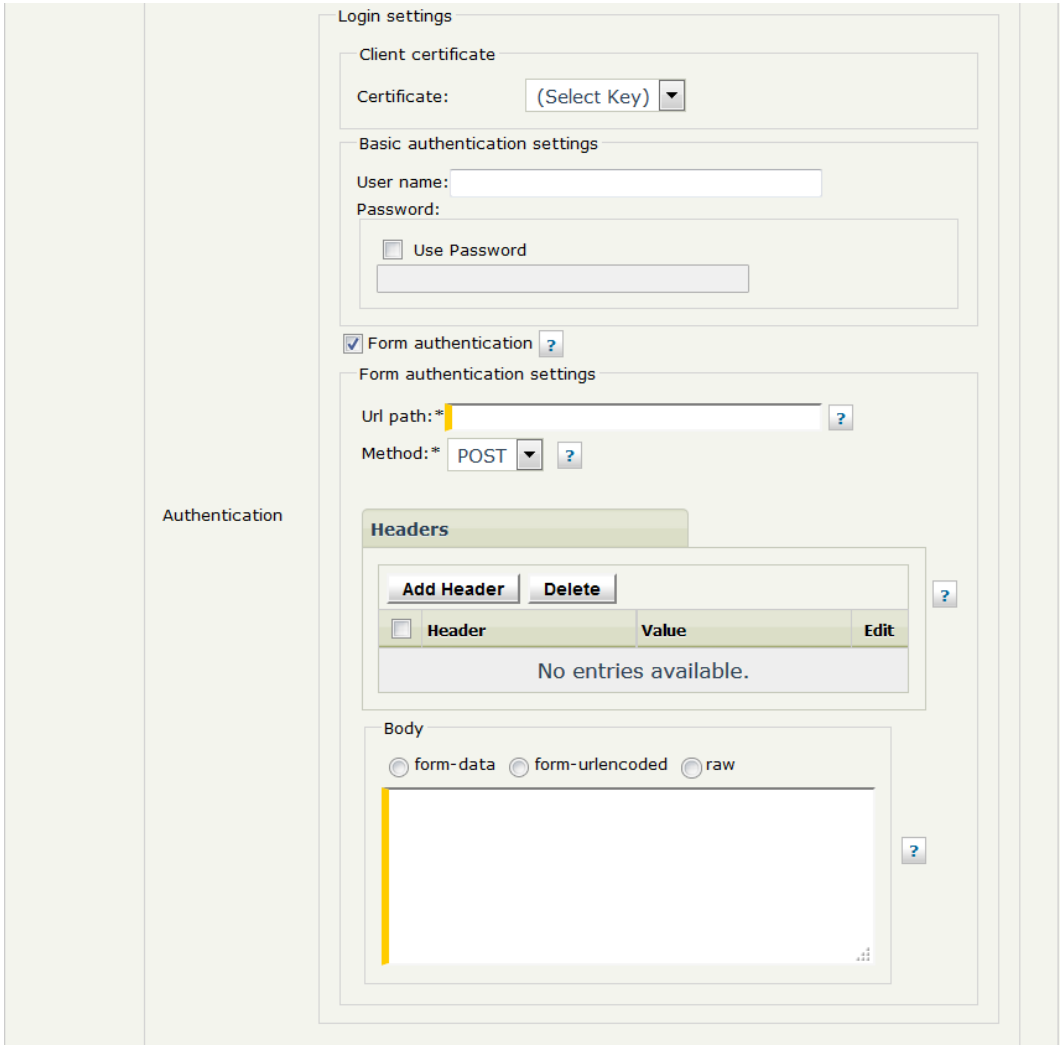


The following table describes the send actions for defining a Generic HTTP transfer site.

Field	Description
Send actions	
Send File As	Select the check box to send the file with a different name and specify the file name. The limited expression language can be used to specify the file name. The available environment variable is: • `${env['ts_target']}` - The file name of the file that will be sent. Examples: • `${env['ts_target']}` • `${env['ts_target']}_${random()}` • `${date('yyyyddMMHHmmss')}`

Login settings

The following example shows the login settings for a Generic HTTP transfer site.



The following table describes the login settings for defining a Generic HTTP transfer site.

Field	Description
Authentication	
Login Settings	
Client Certificate	
Certificate	The client certificate to be used for mutual authentication.
Basic authentication settings	

Field	Description
User name	The user name to be used to log into a remote HTTP server.
Use Password	Select to use a password to log into the remote HTTP server. Disabled when **Form authentication** is selected.
Password	Password used to log into the remote HTTP server. Disabled when **Form authentication** is selected.
Form authentication	Select to use form authentication. If **Form authentication** is enabled, the transfer site will use form authentication to connect to the remote HTTP server. If username and password in the *Basic authentication settings* pane are set, they will be mapped to the environment variables `${env['ts_form_auth_username']}` and `${env['ts_form_auth_password']}` and can be used in the body of the form authentication request.
Form authentication settings	

URL path	The HTTP server path used for sending the form authentication request:
	• A server absolute path when the partner is specified using a hostname (IP address) and port number.
	Example:
	`/form.php`
	• A server relative path when the partner is specified using an URL.
	Example:
	`form.php`
	The limited expression language can be used to specify the URL.
	Example:
	If the value in **Specify partner using URL** is `https://<host>:<port>/auth/` and the value for **URL path** is `/form.php`, the final URI that will be resolved is `https://<host>:<port>/form.php`. This occurs because `/form.php` is an absolute path and not a relative path. If the value for **URL path** is `form.php`, the final URI that will be resolved is `https://<host>:<port>/auth/form.php`.
	This field is displayed when **Form authentication** is checked.

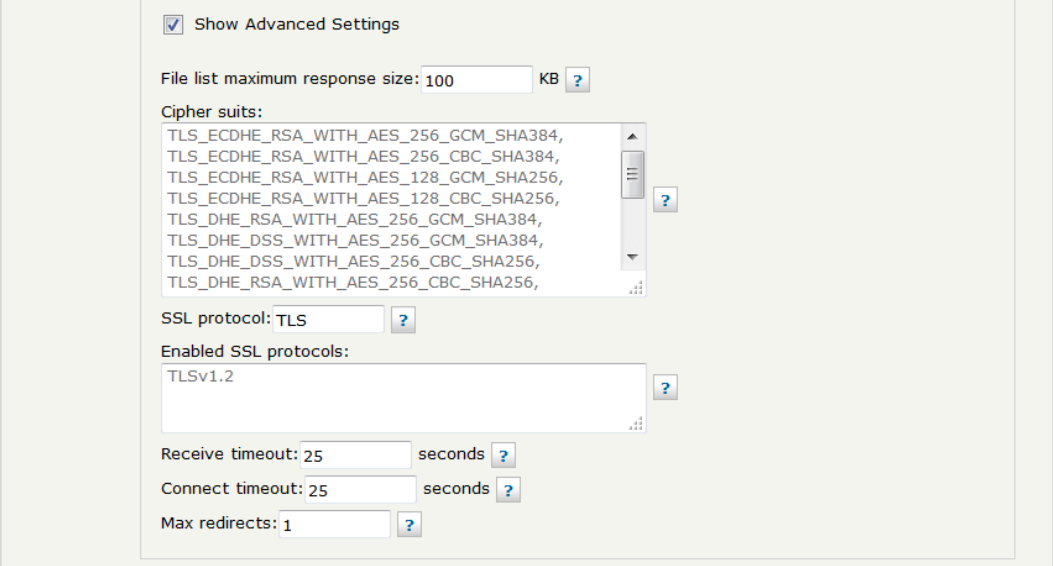
Method	The HTTP method to be used for the form authentication to the remote server. Either **GET** or **POST** can be selected. This field is displayed when **Form authentication** is checked.

Field	Description
Headers	The HTTP headers that will be added in the HTTP request for form authentication. To add a header, click **Add Header** and complete the **Header** and **Value** fields. To edit a header, click the **Edit** ( ) icon and change the **Header** and **Value** fields. To delete a header, select the header to delete and click **Delete**. Displayed when **Form authentication** is checked.

Body	The body of the form authentication request. This field is displayed when the selected authentication Method is **POST**.
	The limited expression language can be used to specify the body.
	The available environment variables are:
	`${env['ts_form_auth_username']}` - Represents the user name specified in the *Basic authentication settings* pane.
	`${env['ts_form_auth_password']}` - Represents the password specified in the *Basic authentication settings* pane.
	The body can be any of the following types:
	• **form-data** – When selected the body will be transmitted as `multipart/form-data`.
	• **form-urlencoded** – When selected the body will be transmitted as `application/x-www-form-urlencoded`.
	• **raw** – When selected the body can be any text.
	Note When the selected body content type is **form-data** or **form-urlencoded** the body should be formed as key-value pairs on separate lines.
	Example:
	`param1=value1`
	`param2=value2`
	Example of how to use the environment variables in the body:
	`user=${env['ts_form_auth_username']}`
	`password=${env['ts_form_auth_password']}`
	This field is displayed when **Form authentication** is checked.

Advanced settings

The following example shows the advanced settings for a Generic HTTP transfer site.



The following table describes the advanced settings for defining a Generic HTTP transfer site.

Field	Description
Advanced settings	
Show Advanced Settings	Select the check box to display the advanced settings.
File list maximum response size	The maximum size in KB of the file list response to handle. If the response exceeds this value, only the specified number of bytes will be processed. Example: If the response is 120 KB and the maximum size is set up to 100 KB, only the first 100 KB from the response will be processed. The default value is `100` KB. This field is displayed when **Show Advanced Settings** is checked.
Cipher suites	The cipher suites to be used for the SSL connection. The cipher suites must be comma separated. By default this set is populated with the cipher suites as defined in the `Https.SIT.Ciphers` configuration option. This field is displayed when **Show Advanced Settings** is checked.
SSL protocol	The SSL protocol to be used for the SSL connection. The default value is `TLS`. This field is displayed when **Show Advanced Settings** is checked.

Field	Description
Enabled SSL protocols	The enabled SSL protocols. The protocols must be comma separated. By default this list is populated with the SSL protocols as defined in the `Https.SIT.EnabledProtocols` configuration option. This field is displayed when **Show Advanced Settings** is checked.
Receive timeout	The socket timeout in seconds. Any non-zero time out will block the input stream associated with the socket for this amount of time. A timeout of zero is interpreted as an infinite timeout. The default value is `25` seconds. This field is displayed when **Show Advanced Settings** is checked.
Connect timeout	The connection timeout in seconds. A timeout of zero is interpreted as an infinite timeout. The connection will then block until established or an error occurs. The default value is `25` seconds. This field is displayed when **Show Advanced Settings** is checked.
Max redirects	The maximum number of redirects to be followed. The limit on the number of redirects is intended to prevent infinite loops. The default value is `1` redirect. This field is displayed when **Show Advanced Settings** is checked.

Sample configuration – List files and download

Sample configuration for a Generic HTTP transfer site to list specific files on an Apache HTTP server and download them:

Field	Description
General Settings	
Site Name	`GHTTP_list`
Site Type	Unspecified
Access Level	Private
Transfer Protocol	Generic-HTTP(S)
Server Settings	
Specify partner using hostname (IP address) and port number	Selected

Field	Description
Host	`10.232.15.114`
Port	`443`
Specify partner using URL	Not selected
Address	—
Network Zone	none
Transfer Settings	
Use HTTPS	Selected
Verify certificate for this Site	Not selected
Enable FIPS Transfer Mode	Not selected
List	
List settings	
Enable list	Selected
URL path	`/uploads`
File expression	`<a href=\"(([^?].*?)\">`
Method	GET
Headers	No headers
File download	
File download settings	
URL path	`${env['ts_relative_path']}/${env['ts_target']}`
Method	GET
Headers	No headers
Receive actions	
Receive File As	Not selected

Field	Description
Upload	
Upload settings	
URL path	—
Method	PUT
Headers	No headers
Send actions	
Send File As	Not selected
Authentication	
Login Settings	
Client Certificate	
Certificate	(Select Key) - No key selected
Basic authentication settings	
User name	`acc`
Use Password	
Password	
Form authentication	Not selected
Advanced settings	
Show Advanced Settings	Not selected

Sample configuration – Download file

Configuration for a Generic HTTP transfer site to download a file from an Apache HTTP server:

Field	Selection or entry
General Settings	

Field	Selection or entry
Site Name	GHTTP_download
Site Type	Unspecified
Access Level	Private
Transfer Protocol	Generic-HTTP(S)
Server Settings	
Specify partner using hostname (IP address) and port number	Selected
Host	10.232.14.182
Port	443
Specify partner using URL	Not selected
Address	—
Network Zone	none
Transfer Settings	
Use HTTPS	Selected
Verify certificate for this Site	Not selected
Enable FIPS Transfer Mode	Not selected
List	
List settings	
Enable list	Not selected
File download	
File download settings	
URL path	/download.txt
Method	GET
Headers	No headers

Field	Selection or entry
Receive actions	
Receive File As	Not selected
Upload	
Upload settings	
URL path	—
Method	PUT
Headers	No headers
Send actions	
Send File As	Not selected
Authentication	
Login Settings	
Client Certificate	
Certificate	(Select Key) - No key selected
Basic authentication settings	
User name	`acc`
Use Password	Selected
Password	
Form authentication	Not selected
Advanced settings	
Show Advanced Settings	Not selected

Sample configuration – Upload file

Configuration for a Generic HTTP transfer site to upload a file to an Apache HTTP server:

Field	Selection or entry
General Settings	
Site Name	`GHTTP_upload`
Site Type	Unspecified
Access Level	Private
Transfer Protocol	Generic-HTTP(S)
Server Settings	
Specify partner using hostname (IP address) and port number	Selected
Host	`10.232.14.182`
Port	`443`
Specify partner using URL	Not selected
Address	—
Network Zone	None
Transfer Settings	
Use HTTPS	Selected
Verify certificate for this Site	Not selected
Enable FIPS Transfer Mode	Not selected
List	
List settings	
Enable list	Not selected
File download	
File download settings	
URL path	—
Method	GET

Field	Selection or entry
Headers	No headers
Receive actions	
Receive File As	Not selected
Upload	
Upload settings	
URL path	`/upload.php`
Method	POST
Headers	Header = `header1` Value = `value1`

Body	Select **form-data**.
	`${env['ts_file_form_parameter_name']}=filename`
	`filename=${env['ts_target']}`

Send actions	
Send File As	Not selected
Authentication	
Login Settings	
Client Certificate	
Certificate	(Select Key) - No key selected
Basic authentication settings	
User name	`acc`
Use Password	Selected
Password	
Form authentication	Not selected
Advanced settings	

Field	Selection or entry
Show Advanced Settings	Not selected

Sample configuration – Push file to SecureTransport user using Form Authentication

Configuration for a Generic HTTP transfer site to push file to a SecureTransport user using form authentication:

Field	Description
General Settings	
Site Name	`GHTTP_form`
Site Type	Unspecified
Access Level	Private
Transfer Protocol	Generic-HTTP(S)
Server Settings	
Specify partner using hostname (IP address) and port number	Selected
Host	`10.232.15.114`
Port	`443`
Specify partner using URL	Not selected
Address	—
Network Zone	none
Transfer Settings	
Use HTTPS	Selected
Verify certificate for this Site	Not selected
Enable FIPS Transfer Mode	Not selected
List	

Field	Description
List settings	
Enable list	Not selected
File download	
File download settings	
URL path	—
Method	GET
Headers	No headers
Receive actions	
Receive File As	Not selected
Upload	
Upload settings	
URL path	`/api/v1.4/files?transferMode=BINARY`
Method	POST
Headers	Header=`Referer` Value=`123`

Body	Select **form-data**.
	`${env['ts_file_form_parameter_name']}=filename`
	`filename=${env['ts_target']}`

Send actions	
Send File As	Not selected
Authentication	
Login Settings	
Client Certificate	
Certificate	(Select Key) - No key selected

Field	Description
Basic authentication settings	
User name	`user1`
Use Password	Selected
Password	
Form authentication	Selected
Form authentication settings	
URL path	`/template/login`
Method	POST
Headers	Header=`User-Agent` Value=`Mozilla/5.0`

Body	Select **form-urlencoded**.
	`switch=Log In`
	`user=${env['ts_form_auth_username']}`
	`password=${env['ts_form_auth_password']}`

Advanced settings	
Show Advanced Settings	Not selected

Supported expression language

This topic outlines the limited expression language supported by Generic HTTP transfer sites.

Predefined variables

The predefined variable that is supported:

- `${timestamp}`

Predefined functions

The predefined functions that are supported:

- Functions related to a date. For example: `${date("yyyyMMdd")}`
- Functions related to a Random ID. For example: `${random()}`
- Functions related to a String representation. For example: `${concat('str', 'ing')}`

Note Expression variables and functions related to file name and the SecureTransport environment are not supported.

Added expression variables

On download and list, the following environment variables are added:

- `${env['ts_content-disposition']}` – If a remote HTTP server presents a content disposition header, its filename value will be preserved into this variable.
- `${env['ts_relative_path']}` – The relative path of the file that will be downloaded.
- `${env['ts_target']}` – The file name of the file that will be downloaded or uploaded.

On upload, the following environment variables are added:

- `${env['ts_target']}` – The file name of the file that will be downloaded or uploaded.
- `${env['ts_file_form_parameter_name']}` – Represents the name of the form input element with file type on the remote server.

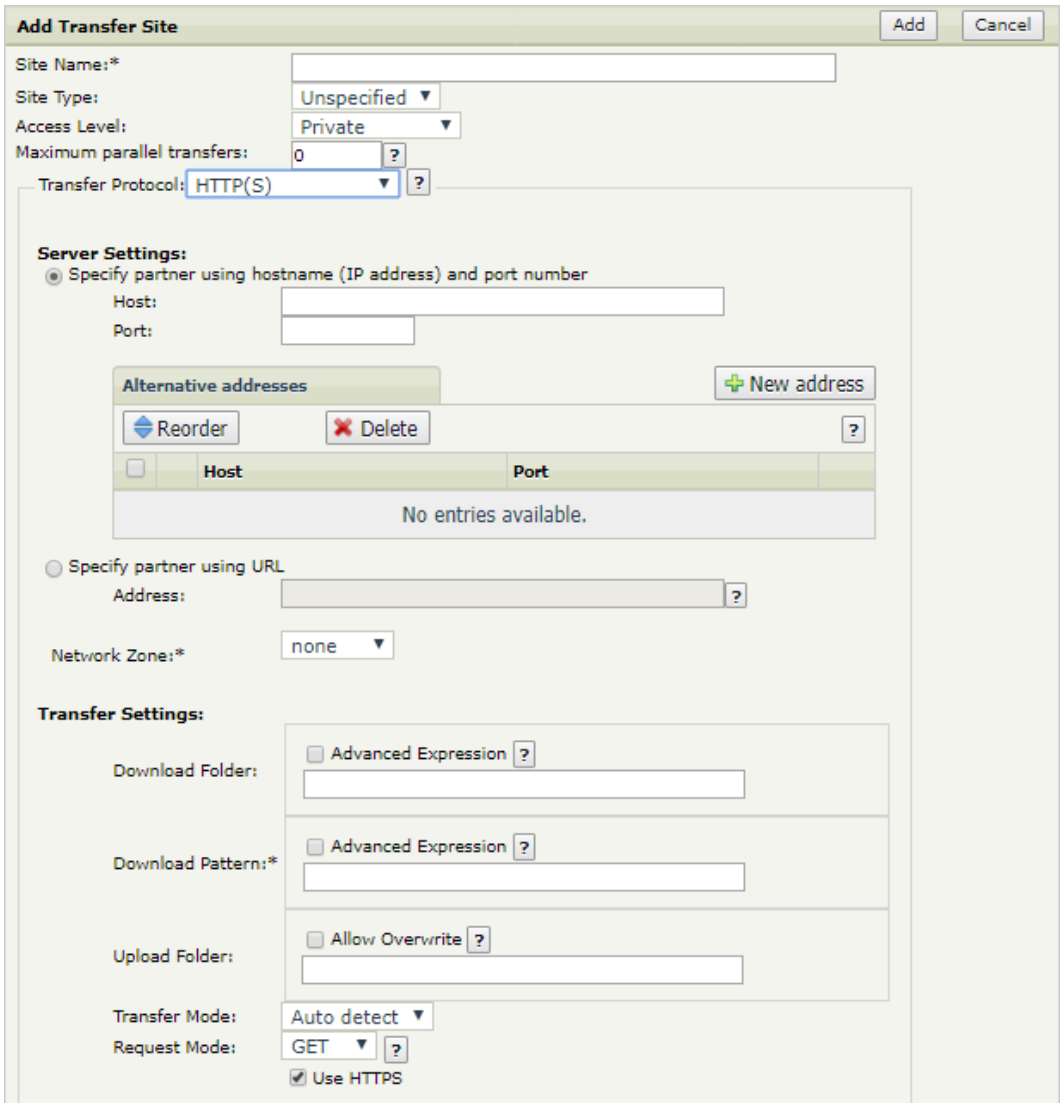
On form authentication, the following environment variables are added:

- `${env['ts_form_auth_username']}` – Represents the user name specified in the *Basic authentication settings* pane.
- `S{env['ts_form_auth_password']}` – Represents the password specified in the *Basic authentication settings* pane.

HTTP(S) transfer sites

SecureTransport Server provides support for guaranteed delivery and restart for transfers using the HTTP protocol when the remote server is a SecureTransport Server.

The following image presents a snippet of the *Add Transfer Site* page for a transfer site definition that uses the HTTP(S) transfer protocol.



The following table describes the HTTP(S) protocol options for a transfer site.

Field	Description
Server Settings	
Host	Select **Specify partner using hostname (IP address) and port number** to enable this field. Enter either the *host name* or *IP address* of the remote host to connect to for file transfers. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

Field	Description
Port	Select **Specify partner using hostname (IP address) and port number** to enable this field. Enter the port number on the remote host to be used for file transfers. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.;

Field	Description
Alternative addresses	Visibility of this option is controlled via a Server configuration option. This set of options allow you to add, delete and set a priority order of alternative endpoints. These endpoints act as backup alternatives to the configured Server-Port Site Settings and are particularly useful in cases of transfer failures. Specifying alternative endpoints as backup servers provides a way to temporarily reroute pending transfers and minimize the risk of transfer failure. As with the Server-Port site settings, the connection to each alternative endpoint is defined by its host name (or IP address) and port number. • To add an alternative server endpoint, click **New Address**. The Alternative Addresses table expands with a new row, that allows you to enter a hostname (or IP address), a port number and save these changes. • To delete an alternative server endpoint, select the corresponding check-box on the same row and click **Delete**. • To reorder the list of alternative endpoints, click **Reorder**. A new option (upward and downward arrow) appears next to each entry. You must hover with the mouse pointer over this newly appeared option and the mouse pointer will assume the "move" shape: a four-directional arrow pointer. This indicates which alternative endpoint is on focus. You can now drag & drop it up and down to the order number you want it at. Perform this action with other alternative endpoints until the list is ordered according to your needs. When you are done, click **Save Order** to keep the newly changed order. **Note** Visibility of this option is controlled with the value set for the `TransferSite.AlternativeAddresses.retryPolicy` configuration option. It allows you to set a "retry policy" with a list of alternative endpoints (presented in IP address: Port number pairs or hostname) you define on this screen. But before you are able to do so, you must go to **Operations > Server Configuration** and set the policy type using either of the following values: • `AllHostsOnEachRetry` – with this policy SecureTransport iterates through each endpoint, one by one, starting with the first in the list. If connection not successful, SecureTransport will continue trying each endpoint one after another until the maximum number of retries is reached. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `OneHostOnEachRetry` – with this policy SecureTransport tries to connect to the first endpoint in the list. If connection not successful, SecureTransport will continue trying that endpoint until the maximum number of retries is reached; and then will move to the next one in the list. Following that same pattern, SecureTransport will try each endpoint until success; or until end of list. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `Disabled` (default) – this is the default value that keeps the table with

Field	Description
	endpoints entirely hidden from view.
Address	Select **Specify partner using URL** to enable this field. Note that with this selection, the *Alternative addresses* grid moves under this option on the screen. Enter a URL that specifies the partner host. It can also include the port and a path (directory).
Network Zone	The network zone that defines the proxies to use for transfers through this site. • Select **none** to connect directly to the remote HTTP server. • Select **any** to allow SecureTransport to select the proxy connection using a network zone that enables an HTTP proxy. • Select **Default** to use the default network zone proxy configuration. If no default is network zone is defined, transfers from this transfer site fail. • Select a specific network zone to use the proxy configuration defined for that zone. For more information, see *Specify TM Server communication ports and IP address for protocol servers on SecureTransport Edge* on page 224.
Transfer Settings	
Download Folder	The folder on the remote server from which the file are transferred. If **Advanced Expression** is selected for Download Folder, the download folder is evaluated using expression language. To use the expression language to append dates: The download folder will be evaluated using the current date when the transfer site is being executed. For example `folder_20150130`. Example: `folder_${date("yyyyMMdd")}`
Download Pattern	The pattern used to match file names to determine whether a file is downloaded. Asterisk (`*`) matches zero or more characters and question mark (`?`) matches one character. If **Advanced Expression** is selected for Download Pattern, the download pattern is evaluated using expression language. To evaluate the download pattern using dates: The download pattern will be evaluated using the current date when the transfer site is being executed. For example `*_20150130.txt`. This will match all files ending with `_20150130.txt`. Example: `*_${date("yyyyMMdd")}.txt`

Field	Description
Allow Overwrite	Taken into account when the site is used by Send To Partner step. If checked the value of "Upload folder" will be overwritten with the value of "Overwrite upload folder". For more details see *Advanced Routing* on page 795.
Upload Folder	The folder on the remote server to which files are transferred.
Transfer Mode	Specify whether data is transferred as ASCII or binary. You can also choose to have SecureTransport automatically determine the correct transfer mode. For more information about automatically determining transfer mode, see *Transfer mode for server-initiated transfers* on page 702.
Use HTTPS	Deselect this check box to use HTTP instead of HTTPS.
Verify certificate for the Site	Select to verify that the remote system is trusted. This field is displayed when **Use HTTPS** is selected.
Enable FIPS Transfer Mode	Restrict HTTPS to use only FIPS 140-2 Level 1 certified cryptographic libraries. This field is displayed when **Use HTTPS** is selected. When you enable FIPS transfer mode, the panel expands with an additional field that lets you specify the desired set of cipher suites to be used in FIPS mode for server-initiated transfers through this site. By default, this set is populated with the cipher suites as defined in the `Https.FIPS.SIT.Ciphers` configuration option. You can add or remove cipher suites. The supported FIPS cipher suites from which you can select when adding a new one are listed in *FIPS transfer mode* on page 983. Note that both the sender and the recipient must use supported FIPS ciphers suites. Otherwise, the transfer will fail.
Site Login Credentials	
User Name	Username used to log in to the HTTP server. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Use Password	Select to use a password to log in to the HTTP server.
Password	Password used to log in to the HTTP server.
Certificate	A private certificate for SecureTransport to use to log in to the remote system. You can select a certificate or import a certificate. This field is displayed when **Use HTTPS** is selected. By default, the usage of expired X509 certificates is allowed for SIT transfers. To forbid it, set the `SIT.allowExpiredCertificates` to `false`.
Post-transmission Settings – Send Options	

Field	Description
Send File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name.
On Temporary Failure	A temporary failure can occur when the transfer is incomplete and a retry occurs. Select one of the three choices: **No Action**, **Delete Destination File**, or **Move File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete Destination File** removes the file from the new location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.
On Failure	A failure occurs when the transfer is incomplete and all retry attempts were unsuccessful. Select one of the three choices: **No Action**, **Delete Destination File**, or **Move File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete Destination File** removes the file from the new location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.
Post-transmission Settings – Receive Options	
Receive File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name when the transfer is received. You can use the SecureTransport-specific variable `${stenv.site_target}` which takes the value from the remote file path. See *Expression Language* on page 1020 for information on SecureTransport-specific variables.
On Failure	A failure occurs when the transfer is incomplete and all retry attempts were unsuccessful. Select one of the three choices: **No Action**, Delete Source File, or **Move File To**. Selecting **No Action** causes the file to stay in the original location. If another file with the same name is transferred to this location, the original file is overwritten. Selecting Delete Source File removes the file from the original location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files from and to provide an expression used to rename the file.

Field	Description
On Success	Select one of the three choices: **No Action**, Delete Source File, or **Move File To**. Selecting **No Action** causes the file to stay in the original location. If another file with the same name is transferred to this location, the original file is overwritten. Selecting Delete Source File removes the file from the original location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files from and to provide an expression used to rename the file.
Show Advanced SSL Settings	
Cipher suites	The set of cipher suites available with the current HTTPS transfer site for secure SIT connection. By default this set is populated with the cipher suites as defined in the `Https.SIT.Ciphers` configuration option. To reset to default values, click the button next to the tooltip.
Enabled SSL protocols	The available SSL protocols for secure SIT connection with the current HTTPS transfer site. By default this option uses the SSL protocols as defined in the `Https.SIT.EnabledProtocols` configuration option. To reset to default values, click the button next to the tooltip.

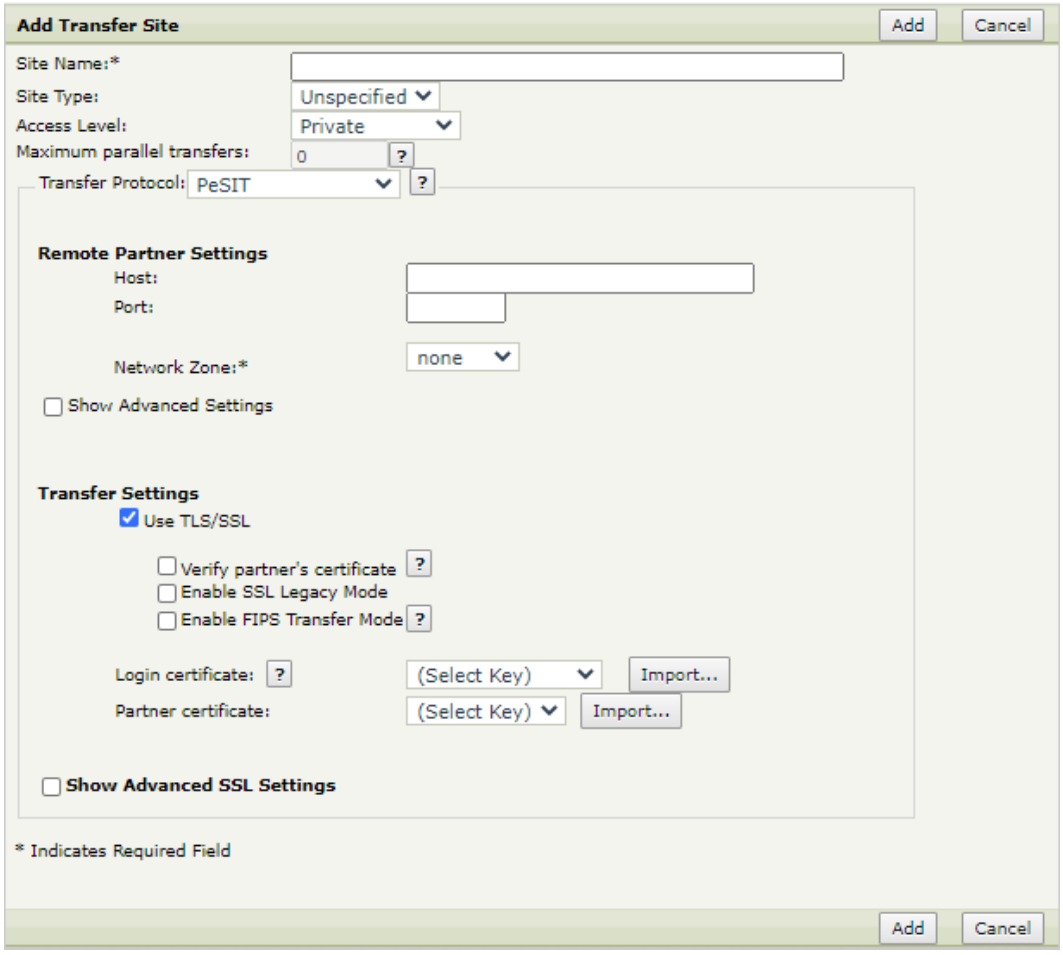
Note To preserve the original file name when using the **Move File To** option, use the `${stenv.target}` or `${stenv['target']}` expressions.

Note When Single Sign-On (SSO) for end-users is enabled, you can not transfer files over HTTP (S).

Note SecureTransport will not be able perform server initiated file pushes or pulls over HTTP to and from another SecureTransport instance if the second requires SSO authentication for the users as the HTTP transfer site cannot handle the SSO authentication.

PeSIT transfer sites

The following image is a snapshot of the *Add Transfer Site* page for a transfer site definition that uses the PeSIT transfer protocol.



Note When you select the **Show Advanced Settings** option, SecureTransport displays many additional fields, not visible on the screen above.

Unlike transfer sites for other transfer protocols, a PeSIT transfer site is also used for transfers initiated by the external PeSIT partner (considered client-initiated by SecureTransport). Only a **Site Name** value is required to define the partnership but it must not be used for transfers initiated by the SecureTransport server on which it is defined.

For a PeSIT transfer site, the **Site Name** designates the destination for an incoming routed transfer. For more information, see *Select a default PeSIT transfer site for routing* on page 571.

The following table describes the PeSIT protocol options for a transfer site.

Field	Description
Remote Partner Settings This group of options is displayed right below your selection of **Transfer Protocol**: PeSIT.	
Host	The host name or IP address of the remote server to connect to for file transfers. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

Field	Description
Port	The port on the remote server to be used for file transfers. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

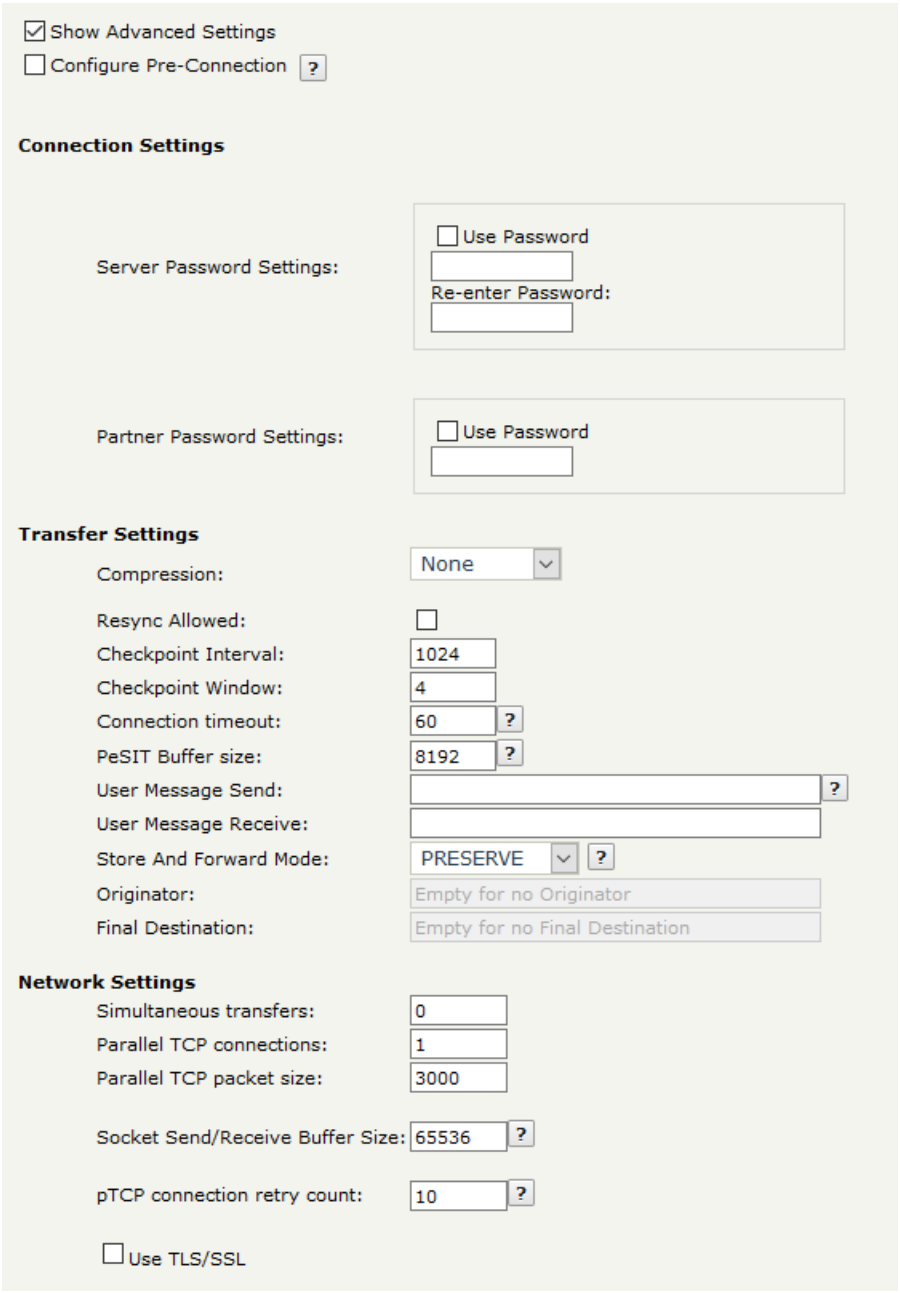
Field	Description
Alternative addresses	Visibility of this option is controlled via a Server configuration option. This set of options allow you to add, delete and set a priority order of alternative endpoints. These endpoints act as backup alternatives to the configured Server-Port Site Settings and are particularly useful in cases of transfer failures. Specifying alternative endpoints as backup servers provides a way to temporarily reroute pending transfers and minimize the risk of transfer failure. As with the Server-Port site settings, the connection to each alternative endpoint is defined by its host name (or IP address) and port number. • To add an alternative server endpoint, click **New Address**. The Alternative Addresses table expands with a new row, that allows you to enter a hostname (or IP address), a port number and save these changes. • To delete an alternative server endpoint, select the corresponding check-box on the same row and click **Delete**. • To reorder the list of alternative endpoints, click **Reorder**. A new option (upward and downward arrow) appears next to each entry. You must hover with the mouse pointer over this newly appeared option and the mouse pointer will assume the "move" shape: a four-directional arrow pointer. This indicates which alternative endpoint is on focus. You can now drag & drop it up and down to the order number you want it at. Perform this action with other alternative endpoints until the list is ordered according to your needs. When you are done, click **Save Order** to keep the newly changed order. **Note** Visibility of this option is controlled with the value set for the `TransferSite.AlternativeAddresses.retryPolicy` configuration option. It allows you to set a "retry policy" with a list of alternative endpoints (presented in IP address: Port number pairs or hostname) you define on this screen. But before you are able to do so, you must go to **Operations > Server Configuration** and set the policy type using either of the following values: • `AllHostsOnEachRetry` – with this policy SecureTransport iterates through each endpoint, one by one, starting with the first in the list. If connection not successful, SecureTransport will continue trying each endpoint one after another until the maximum number of retries is reached. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `OneHostOnEachRetry` – with this policy SecureTransport tries to connect to the first endpoint in the list. If connection not successful, SecureTransport will continue trying that endpoint until the maximum number of retries is reached; and then will move to the next one in the list. Following that same pattern, SecureTransport will try each endpoint until success; or until end of list. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `Disabled` (default) – this is the default value that keeps the table with endpoints entirely hidden from view.

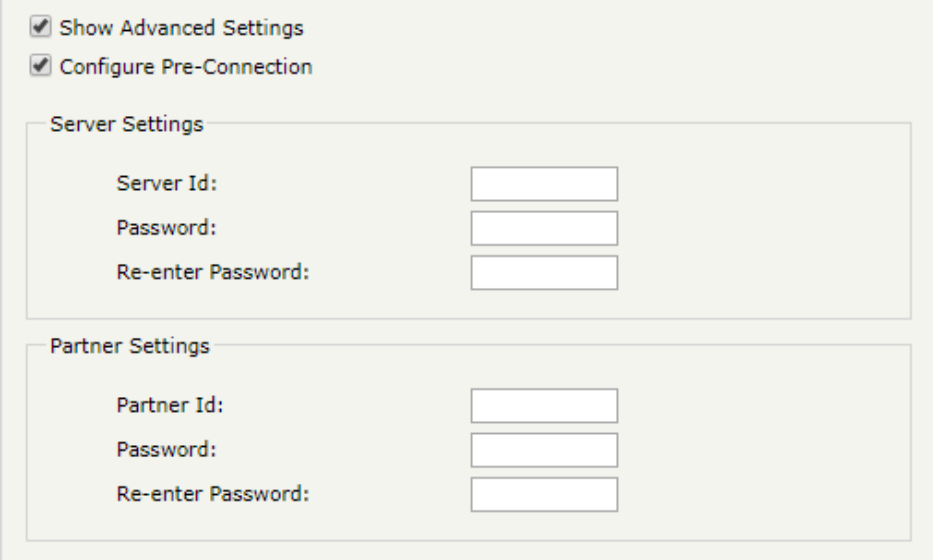
Field	Description
Network Zone	The network zone that defines the proxies to use for transfers through this site. • Select **none** to connect directly to the remote partner server. • Select **any** to allow SecureTransport to select the proxy connection using a network zone that enables an SOCKS5 proxy.SecureTransport • Select **Default** to use the default network zone proxy configuration. If no default is network zone is defined, transfers from this transfer site fail. • Select a specific network zone to use the proxy configuration defined for that zone. For more information, see *Specify TM Server communication ports and IP address for protocol servers on SecureTransport Edge* on page 224.
Transfer Settings Please note that the options described appear on display when the **Show Advanced Settings** option is **not** selected. When you select the **Show Advanced Settings** checkbox, these options are moved under **Network Settings**.	
Use TLS/SSL	Requires the use of TLS or SSL for communication with the partner server. When selected, additional fields appear on display.
Verify partner's certificate	Verify the TLS/SSL certificate of the partner site. This field is displayed when the **Use TLS/SSL** option is selected. When selected, SecureTransport verifies whether the server certificate of the partner is chained to a trusted root using the algorithm specified in `AgentServers.Ssl.trustAlgorithm` server configuration parameter and the certificates imported in the Trusted CAs store.
Enable SSL Legacy Mode	Requires the use of SSL Legacy mode for communication with the partner server. This field is displayed when the **Use TLS/SSL** option is selected.
Enable FIPS Transfer	Restrict PeSIT to use only FIPS 140-2 Level 1 certified cryptographic libraries. This field is displayed when the **Use TLS/SSL** option is selected. When you enable FIPS transfer mode, the panel expands with an additional field that lets you specify the desired set of cipher suites to be used in FIPS mode for server-initiated transfers through this site. By default, this set is populated with the cipher suites as defined in the `Pesit.FIPS.SIT.Ciphers` configuration option. You can add or remove cipher suites. The supported FIPS cipher suites from which you can select when adding a new one are listed in *FIPS transfer mode* on page 983. Note that both the sender and the recipient must use supported FIPS ciphers suites. Otherwise, the transfer will fail.
Login certificate	The local certificate to use when connecting to the partner site. By default, the usage of expired X509 certificates is allowed for SIT transfers. To forbid it, set the `SIT.allowExpiredCertificates` to `false`.

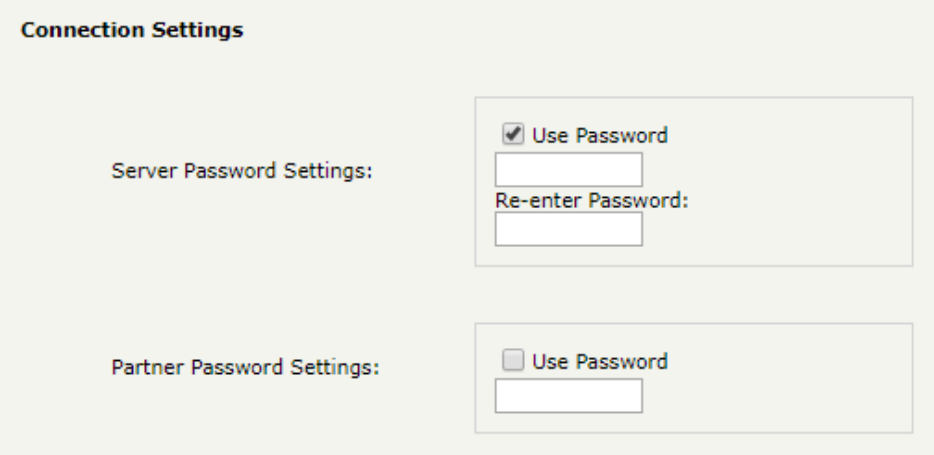
Field	Description
Partner certificate	The login certificate to use when authenticating the remote site.

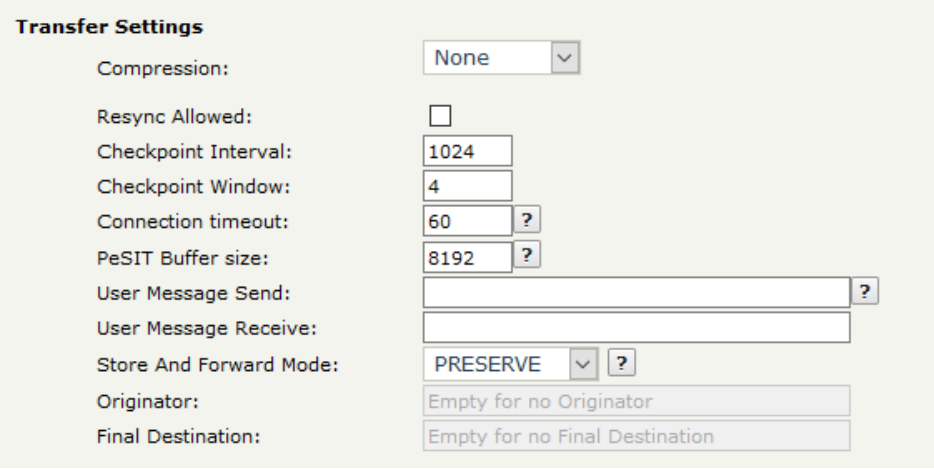
Advanced Settings

Scroll down to the bottom of the screen and select **Show Advanced Settings** to expand the screen with additional options.

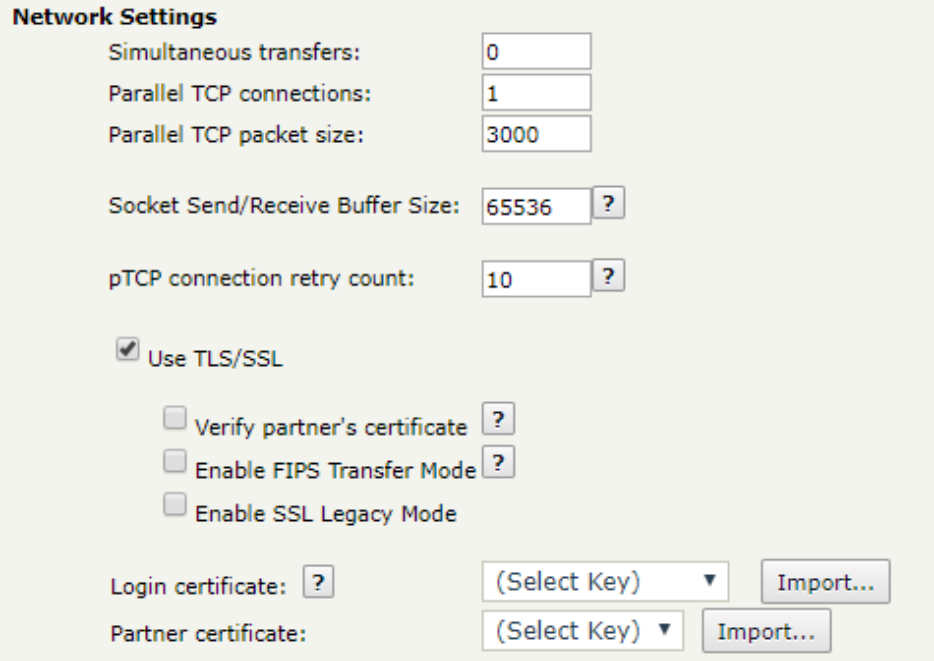


Field	Description
Pre-connection settings	You must have both **Show Advanced Settings** and **Configure Pre-Connection** selected for the following group of options to appear right below. PeSIT pre-connection settings allow you to map a *server ID* and *password* (Server Settings) to the corresponding client-side *partner ID* and *password* (Partner Settings). PeSIT pre-connection acts as a mechanism for additional verification prior to establishing a PeSIT connection.  By default, the **Configure Pre-Connection** checkbox is not selected. If you leave it this way, the following rules apply, depending on the SecureTransport role in Pre-Connection phase: • SecureTransport as *Server* – SecureTransport does not validate the received Partner ID and Partner Password. • SecureTransport as *Client* – SecureTransport sends to the target PeSIT Server the Account name as a Partner ID and the Connection Partner Password (if specified) as Partner Password. When you select the **Configure Pre-Connection** checkbox you must add either Server or Partner Settings, or both. In all cases, the Id field is required and the Password field is optional. With the input of Server or Partner Settings, the following rules apply, depending on the SecureTransport role in the Pre-Connection phase: • SecureTransport as *Server* – SecureTransport validates the received Partner ID and Partner Password against the configured Server ID and Server Password. • SecureTransport as *Client* – SecureTransport sends the configured Partner ID and Partner Password to the target PeSIT Server.
Server Settings	These options appear when you select **Pre-Connection settings**.

Field	Description
Server Id	The ID against which the Server validates the received Partner ID during Pre-Connection phase. It can contain any symbols (up to 8 characters). Leading or trailing spaces will be trimmed.
Password *(optional)*	The password against which the Server validates the received Partner password during Pre-Connection phase. It can contain any symbols (up to 8 characters). White spaces are not allowed. Leading or trailing spaces will be trimmed.
Re-enter Password	Retype the password you configure for pre-connection to your PeSIT server.
Partner Settings	These options appear when you select **Pre-Connection settings**.
Partner Id	The ID that the PeSIT client sends during Pre-Connection phase. It can contain any symbols (up to 8 characters). Leading or trailing spaces will be trimmed.
Password *(optional)*	The password that the PeSIT client sends during Pre-Connection phase. It can contain any symbols (up to 8 characters). White spaces are not allowed. Leading or trailing spaces will be trimmed.
Re-enter Password	Retype the password you configure for pre-connection to your PeSIT transfer site.
Connection Settings	
Server Password Setting	To use a server password, select **Use Password** and type the same password in both fields. The password is required when a remote partner connects to this Server and password authentication is used. Valid passwords are string values consisting of one to eight characters.

Field	Description
Partner Password Settings	To use a partner password, select **Use Password** and type the password in the field provided. The password is required when this Server connects to a remote partner. Valid passwords are string values consisting of one to eight characters.
Transfer Settings	These options appear when you select **Show Advanced Settings**. Please note that when you have not selected the **Show Advanced Settings** checkbox, a different group of options is presented, as described here. 
Compression	Enables horizontal online compression, vertical online compression, or both for transfers initiated by the SecureTransport Server. If the partner PeSIT server does not supports the selected compression, no compression is used for these transfers. SecureTransport support all types of compression for transfers initiated by the partner PeSIT server.
Resync Allowed	Enables dynamics resynchronization of exchanges during transfer, without interrupting the data exchange phase.
Checkpoint Interval	The maximum number of bytes in KB (equals 1024 bytes) that the sender may transmit between two consecutive checkpoints. Checkpoints are used to restart the transfer when required. A value of zero indicates no checkpoints. A value of 65535 indicates an undefined interval.
Checkpoint Window	The greatest difference allowed between the number of the last checkpoint transmitted and the number of the last checkpoint acknowledged. When this number of checkpoints are not acknowledged, the sender suspends data transmission until it receives a checkpoint acknowledgment. A value of zero indicates that no acknowledgments are required.

Field	Description
Connection Timeout	When SecureTransport acts as a client, the value of this field specifies the amount of time (in seconds) that SecureTransport will wait for an acknowledgment for a transfer. Default value: the value specified in the `Pesit.Client.Inactivity.Timeout` configuration option. Accepted values: positive integers. If specified, the Connection Timeout value overwrites the `Pesit.Client.Inactivity.Timeout` value.
PeSIT Buffer size	The size of the internal buffer for this transfer site in bytes. Valid values are 512 to 65535. A larger buffer improves performance. Specifies the maximum size of a PeSIT data element (PI 25). Should be greater than 800 bytes and less than 65535.
User Message Send	A string sent as PI 99 when the SecureTransport Server initiates a file transfer to the partner PeSIT server. The field may contain expressions. The tool tip lists valid expressions. If SecureTransport received the file using PeSIT, it retained the values of all the PeSIT PI codes as metadata and the PeSIT expression language variables contain those values. See also *Expression Language* on page 1020, especially *PeSIT variables* on page 1026. The string that results from the evaluation of the expression must be at most 512 characters long.
User Message Receive	A string included in messages sent when the SecureTransport Server initiates a file transfer from the partner PeSIT server. The field may contain expressions. The string that results from the evaluation of the expression must be at most 512 characters long.
Store and Forward Mode	Select the Store and Forward mode: **START_NEW** or **PRESERVE**. **Note** The Store and Forward mode selected here can be overwritten from the Send To Partner step settings.
Originator	• In case of SecureTransport initiating a new Store and Forward transfer, this property specifies the originator (PI61) of the transfer. **Note** The originator specified in the PeSIT transfer site can be overwritten from the Advanced Routing Send To Partner step setting **Originator**. • In case no value is specified in both this filed and the Advanced Routing Send To Partner step setting **Originator**, PI61 is blank. • When the PRESERVE store and forward mode is selected, this field is disabled as PI preserves the PI61 value.

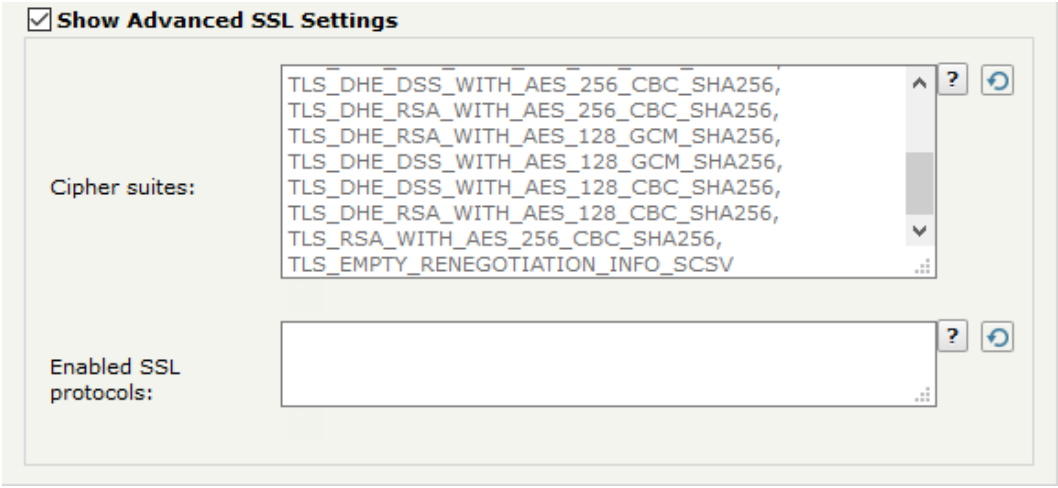
Field	Description
Final Destination	• In case of SecureTransport initiating a new Store and Forward transfer, this property specifies the final destination (PI62) of the transfer. **Note** The final destination specified in the PeSIT transfer site can be overwritten from the Advanced Routing Send To Partner step setting **Final Destination**. • In case no value is specified in both this field and the Advanced Routing Send To Partner step setting **Final Destination**, PI62 is blank. • When the PRESERVE store and forward mode is selected, this field is disabled as PI preserves the PI62 value.
Network Settings	These options appear when you select **Show Advanced Settings**.  **Note** The following settings: **Use TLS/SSL** onward are described here.
Simultaneous transfers	The maximum number of simultaneous transfers from this transfer site to remote PeSIT systems. A value of zero means no limit.
Parallel TCP connections	The number of TCP connections to make for parallel TCP (pTCP) to accelerate transfers.
Parallel TCP package size	The pTCP packet size in bytes.
Socket Send / Receive Buffer Size	The size of the pTCP buffers in bytes. Specifies the TCP Socket maximum send and receive buffer size in bytes. This setting corresponds to SO_SNDBUF and SO_RCVBUF socket parameters.

Field	Description
pTCP connection retry count	The number of attempts SecureTransport makes for each TCP connection for pTCP. When the value of the **Host** field is the address of load balancer for a remote PeSIT cluster, set this field to *connections* * (*nodes* - 1), where: • *connections* is the value of the **Parallel TCP Connections** field • *nodes* is the number of nodes in the remote PeSIT cluster SecureTransport reties the connections until all connections are with the same PeSIT remote server. It specifies the maximum times the SecureTransport will attempt to re-establish a connection with the remote server in case of "Unknown session" error. This is useful in cases where the remote partner is a PeSIT cluster, the address in the transfer site represents the load balancer in front of the PeSIT cluster and the individual nodes behind the Load Balancer are not accessible. In such environment, all connections have to arrive on the same partner node. Depending on the load balancing configuration different number of retries or no retries (sticky session LB configuration) might be required.

Note The options displayed below **pTCP connection retry count** are described here.

Advanced SSL Settings

Scroll down to the bottom of the screen and click the **Show Advanced SSL Settings** to expand the screen with additional options.



The following table provides brief description on the Advanced SSL Settings:

Field	Description
Show Advanced SSL Settings	

Field	Description
Cipher suites	The set of cipher suites available with the current PeSIT transfer site for secure SIT connection. By default this set is populated with the cipher suites as defined in the `Pesit.SIT.Ciphers` configuration option. To reset to default values, click the button next to the tooltip.
Enabled SSL protocols	The available SSL protocols for secure SIT connection with the current PeSIT transfer sites. By default this list is populated with the SSL protocols as defined in the `Pesit.SIT.EnabledProtocols` configuration option. To reset to default values, click the button next to the tooltip.

The following sectiion provides how-to instructions for selecting a default PeSIT transfer site for routing:

- *Select a default PeSIT transfer site for routing* on page 571

Select a default PeSIT transfer site for routing

SecureTransport implements PeSIT routing as an intermediate partner by sending a received file to a PeSIT transfer site specified as the destination of the PeSIT transfer.

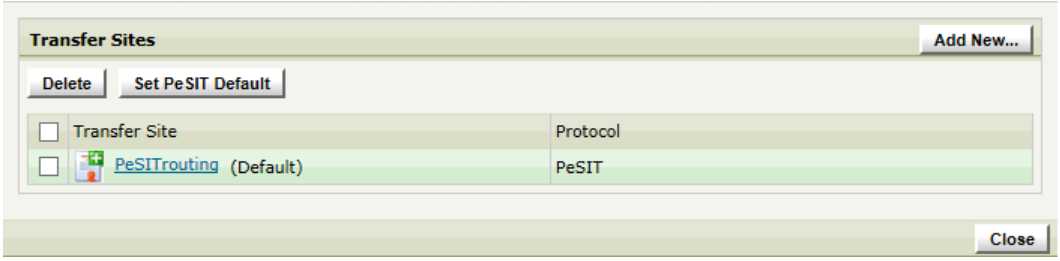
SecureTransport matches the specified destination to the names of the transfer sites for the account that receives the file. If a transfer site name matches, SecureTransport transfers the file to that site. No subscription is required. If no transfer site name matches and a default PeSIT transfer site is defined, SecureTransport transfers the file to that site.

If there is no default site, SecureTransport checks the **Routing Mode** value for the account. When set to **Reject**, the transfer is rejected before it starts. When set to **Accept**, the transfer is performed and the file is retained locally. If it is **Ignore**, a transfer that cannot be routed is ignored.

When SecureTransport routes a transferred file to a final PeSIT destination, SecureTransport includes PI 61 and PI 62.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account for which you want to set the default transfer site.
3. Click the **Transfer Site** tab.
4. Select the check box next to the name of the PeSIT transfer site to make the default.
5. Click **Set PeSIT Default**.

   The default is indicated in the transfer site list.

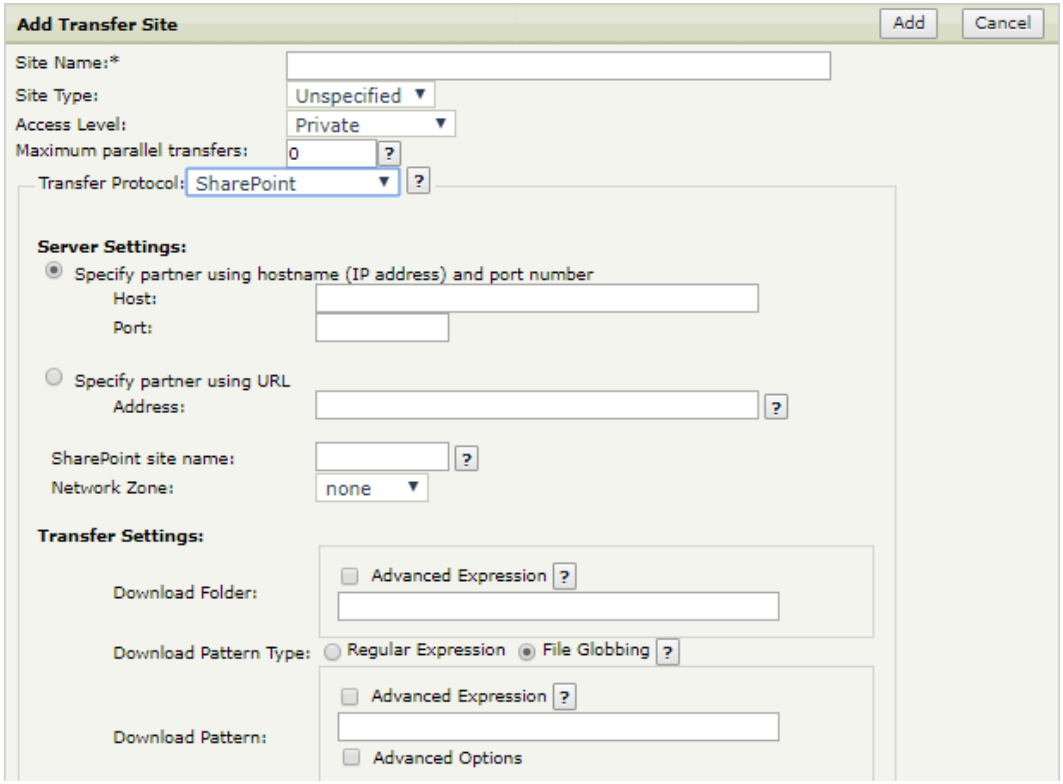


SharePoint transfer sites

The SharePoint transfer site supports pushes and pulls from SecureTransport to the SharePoint 2013 file system. The SharePoint transfer site can be used with Basic Application and Advanced Routing for PUSH and PULL server-initiated transfers (SIT). A user name and password are used for SharePoint file system authentication.

Note The Advanced Routing Send To Partner route step option **Overwrite Upload Folder** cannot be used for SharePoint transfers.

The following is the *Add Transfer Site* page for a transfer site definition that uses the SharePoint transfer protocol.



The following table describes the SharePoint protocol options for defining a transfer site.

Field	Description
Server Settings	
Specify partner using hostname (IP address) and port number	
Host	Host of SharePoint REST service.
Port	Port of SharePoint REST service.

Field	Description
Specify partner using URL	
Address	URL address of SharePoint REST service. Examples: • http://example.com • https://example.com:443 • https://example.com:443/websealjun/
SharePoint site name	The name of site where SharePoint document library lies.
Network Zone	Network zone for the transfer site. • **None** • **Any** • **Default**
Transfer Settings	
Download Folder	A folder on the SharePoint site from which files will be downloaded. This is the folder in which files will be looked up. The field will accept SecureTransport expression language input, controlled by the **Advanced Expression** checkbox.
Advanced Expression	When checked, the download folder is evaluated using the expression language. • Using it with dates. The download folder will be evaluated using the current date when the transfer site is being executed. For example: `folder_20150130`. `folder_${date("yyyyMMdd")}`
Download Pattern Type	Regular expression or file globing.

Regular Expression	When the syntax is **Regular Expression**, the String representation of the filename is matched against Perl5.003 regular expressions. Perl5 extended regular expressions are also supported. For example:
	• Matches files ending in `.xml` or `.txt`:
	`.*\.(xml|txt)`
	• Case insensitive match of `data.xml` file:
	`(?i)data\.xml`

Field	Description

File Globbing	When the pattern type is **File Globbing**, the String representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:
	• Matches files ending in `.xml`:
	`*.xml`
	• Matches file names starting with `foo.` that have a double character extension:
	`foo.??`
	• Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`:
	`*.[0-9]`
	• Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`:
	`*.[!0-9]`

Download Pattern	The pattern based on which files will be downloaded. After a LIST is performed, only files that match the pattern will be downloaded. The field will accept SecureTransport expression language input, controlled by the **Advanced Expression** checkbox.
Advanced Expression	When checked, the download pattern is evaluated using expression language. Also, when **Advanced Expression** is checked for Download Pattern, the input fields from Advanced Options menu will be evaluated using the expression language. • Using the download pattern with dates. The download pattern will be evaluated using the current date when the transfer site is being executed. For example: `*_20150130.txt`. This will match all files ending with `_20150130.txt`. `*_${date("yyyyMMdd")}.txt`
Advanced Options	An additional options section that allows downloading different file versions. When **Advanced Options** is selected, a new section will expand containing file versions related settings. Those settings will be used for forming the final download list. By default this section is hidden.

Field	Description
Download `specific|last|first X Any|Major|Minor` version(s) of the file	This setting is used for determining which file versions will be downloaded, based on their version labels and types. `X` would accept either a specific file version or a file version count. The following use cases are supported through this setting: • **Download "specific" "1.1" "Any" version of the file** – downloads a specific file version. • **Download "specific" "<empty value>" "Minor" versions of the file** – downloads all minor versions of the file. • **Download "specific" "<empty value>" "Major" versions of the file** – downloads all major versions of the file. • **Download "first" "<X>" "Any" versions of the file** – downloads the first X versions of the file, regardless if they are minor or major. • **Download "first" "<X>" "Minor" versions of the file** – downloads the first X MINOR versions of the file. Major versions are discarded. • **Download "first" "<X>" "Major" versions of the file** – downloads the first X MAJOR versions of the file. Minor versions are discarded. • **Download "last" "<X>" "Any" versions of the file** – downloads the last X versions of the file, regardless if they are minor or major. By default, it may be considered, that if only a Download Pattern is set for the transfer site, this exact use case is being executed – Download "last" "1" "Any" version of the file. • **Download "last" "<X>" "Minor" versions of the fil**e – downloads the last X MINOR versions of the file. Major versions are discarded. • **Download "last" "<X>" "Major" versions of the file** – downloads the last X MAJOR versions of the file. Minor versions are discarded. **Major versions** are in the following format – X.0 – for example 1.0, 2.0, 3.0, 6.0. **Minor versions** are in the following format X.Y, where Y is not equal to 0 – for example 1.2, 1.3, 4.5, 6.11.
Download file versions from `mm/dd/yyyy` to `mm/dd/yyyy`	Downloads all file versions within a specific time frame, regardless if versions are minor or major. If both the dates are the same, downloads all file versions from a specific day. Date fields are expression language based. Example: • `${date("MM/dd/yyyy")}`
Receive Post Actions	

Field	Description
Receive File As	Specify a value to receive the file with a different name. This is an expression language based field that can be used to download a file with different name. It should be configured when downloading different versions of the same file. The field is auto-populated with a default rename expression: `("${env['DXAGENT_TARGET]}_${env['DXAGENT_VERSIONLABEL']}")` Available environment variables: • `${env['DXAGENT_TARGET']}` • `${env['DXAGENT_VERSIONID']}` • `${env['DXAGENT_VERSIONLABEL']}` Examples: • `file_${random()}` • `${env['DXAGENT_TARGET']}_${env['DXAGENT_VERSIONID']}` • `${env['DXAGENT_TARGET']}_${env['DXAGENT_VERSIONLABEL']}`

On Failure	**No Action**
	Delete Source File - Deletes a file on SharePoint. This option is disabled when a different Advanced Options download other than the default one is set (Download **last 1 Any** version(s) of the file.).
	Delete File Version Only - Deletes the downloaded file version only from SharePoint. This option is disabled when the default download is set (Download **last 1 Any** version(s) of the file.) or using Advanced Download options is disabled.
	Move/Rename File To - Specify a full path value to rename the remote file on transmission failure or move it to a different remote folder. A limited expression language can be used to specify a file name/folder. This option is disabled when a different download than the default one (Download **last 1 Any** version(s) of the file.) is set.
	Examples:
	• Use current date as a file name.
	`${date('yyyyddMMHHmmss')}`
	• Use a random ID as a filename.
	`${random()}`
	Note Valid file or folder names cannot begin or end with a dot, cannot contain consecutive dots and cannot contain any of the following forbidden characters: **~ " # % & * : < > ? / \ { | }**

Field	Description

On Success	**No Action**
	Delete Source File - Deletes a file on SharePoint. This option is disabled when a different Advanced Options download other than the default one is set (Download **last 1 Any** version(s) of the file.).
	Delete File Version Only - Deletes the downloaded file version only from SharePoint. This option is disabled when the default download is set (Download **last 1 Any** version(s) of the file.) or using Advanced Download options is disabled.
	Move/Rename File To - Specify a full path value to rename the remote file on transmission success or move it to a different remote folder. A limited expression language can be used to specify a file name/folder. This option is disabled when a different download than the default one (Download **last 1 Any** version(s) of the file.) is set.
	Examples:
	• Use current date as a file name.
	`${date('yyyyddMMHHmmss')}`
	• Use a random ID as a filename.
	`${random()}`
	Note Valid file or folder names cannot begin or end with a dot, cannot contain consecutive dots and cannot contain any of the following forbidden characters: **~ " # % & * : < > ? / \ { | }**

Upload Folder	A folder on the SharePoint site where files will be uploaded. The field will accept SecureTransport expression language input, controlled by the **Advanced Expression** checkbox.
Advanced Expression	When checked the upload folder is evaluated using expression language. • Using it with dates. The upload folder will be evaluated using the current date when the transfer site is being executed. For example: `folder_20150130`. `folder_${date("yyyyMMdd")}`
Send Post Actions	

Field	Description
Send File As	Specify a value to send the file with a different name. The limited expression language can be used to specify a file name. Available environment variables: • `${env['DXAGENT_TARGET']}` Examples: • `file_${random()}` • `${env['DXAGENT_TARGET']}_${date ('yyyyddMMHHmmss')}` **Note** Valid file names cannot begin or end with a dot, cannot contain consecutive dots, and cannot contain any of the following forbidden characters: **~ " # % & * : < > ? / \ { | }**
On Success	**No Action** **Publish** - Publish the file with specified comment to SharePoint. Publishing a file, migrates the file from a minor version to a major version. The comment field is expression language based. Example: • Publish file and use the current date as publish comment. `${date('yyyyddMMHHmmss')}` **Note** The publish comment cannot contain any of the following forbidden characters: **~ " # % & * : < > ? / \ { | }**
Use HTTPS	Checked when HTTPS should be used for transfers.
Verify certificate for this Site	Verify certificate for the site when HTTPS is used for transfers.
Site Login Credentials	
User Name	Login name to be used for the SharePoint document library. If the user to authenticate with is in domain, then it is required to specify both the user and the domain in the username property as follows: `<domain name>\<user name>`. Otherwise specify only the username.
Password Settings	
Use Password	If checked, a password must be provided.
Password	The password to be used for the SharePoint document library.

The following provides information on the limited expression language supported by SharePoint transfer sites:

- *Supported expression language* on page 579

Supported expression language

This topic outlines the limited expression language supported by SharePoint transfer sites.

Predefined variables

The predefined variable that is supported:

- `${timestamp}`

Predefined functions

The predefined functions that are supported:

- Functions related to a date. For example: `${date("yyyyMMdd")}`
- Functions related to a Random ID. For example: `${random()}`
- Functions related to a String representation. For example: `${concat('str', 'ing')}`

Note Expression variables and functions related to file name and the SecureTransport environment are not supported.

Added expression variables

On download, the following environment variables are added:

- `${env['DXAGENT_ TARGET']}` – The name of the file being pulled.
- `${env['DXAGENT_ VERSIONLABEL']}` – The SharePoint file version label (1.0, 3.1, and so forth).
- `${env['DXAGENT_ VERSIONID']}` – The SharePoint file version ID (512, 1024, and so forth).

On upload, the following environment variable is added:

- `${env['DXAGENT_ TARGET]}` – The name of the file being pulled.

SSH transfer sites

Note SSH keys generated with DSA and RSA can be used to authenticate SSH transfer sites.

By default, a server-initiated transfer using SSH and a pattern with a wildcard character does not create an extra empty file. To allow a temporary zero-byte file to be created, set the `ZeroByteWildcardPullAllowed` server configuration parameter to `true`.

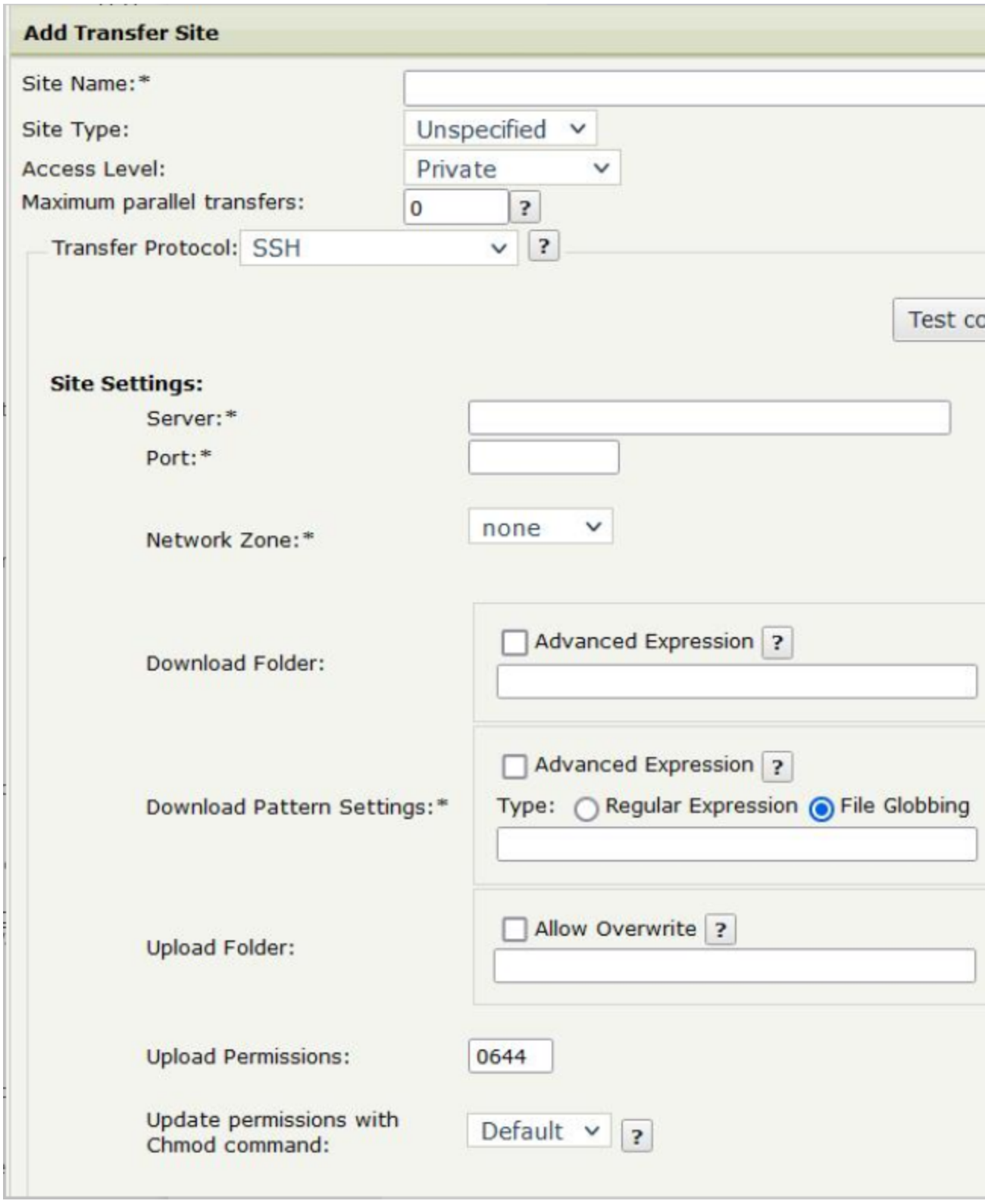
SSH Transfer Site options

Configuring a SSH protocol transfer site consists of making selections and completing fields for the following:

- *Site settings* on page 580
- *Transfer settings* on page 585
- *Site login credentials* on page 587
- *Network settings* on page 588
- *Test SSH Connection* on page 589
- *Post transmission send options* on page 590
- *Post transmission receive options* on page 592
- *Advanced SSL Settings* on page 594

Site settings

The following image presents a snippet of the *Site Settings* pane for a SSH transfer site:



The following table describes the site settings options for a SSH protocol transfer site.

Field	Description
Site Settings	
Server	The host name or IP address of the remote server to connect to for file transfers. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Port	The port on the remote server to be used for file transfers. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

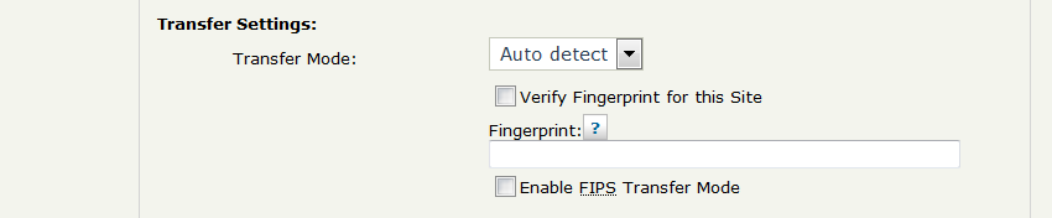
Field	Description
Alternative addresses	Visibility of this option is controlled via a Server configuration option. This set of options allow you to add, delete and set a priority order of alternative endpoints. These endpoints act as backup alternatives to the configured Server-Port Site Settings and are particularly useful in cases of transfer failures. Specifying alternative endpoints as backup servers provides a way to temporarily reroute pending transfers and minimize the risk of transfer failure. As with the Server-Port site settings, the connection to each alternative endpoint is defined by its host name (or IP address) and port number. • To add an alternative server endpoint, click **New Address**. The Alternative Addresses table expands with a new row, that allows you to enter a hostname (or IP address), a port number and save these changes. • To delete an alternative server endpoint, select the corresponding check-box on the same row and click **Delete**. • To reorder the list of alternative endpoints, click **Reorder**. A new option (upward and downward arrow) appears next to each entry. You must hover with the mouse pointer over this newly appeared option and the mouse pointer will assume the "move" shape: a four-directional arrow pointer. This indicates which alternative endpoint is on focus. You can now drag & drop it up and down to the order number you want it at. Perform this action with other alternative endpoints until the list is ordered according to your needs. When you are done, click **Save Order** to keep the newly changed order. **Note** Visibility of this option is controlled with the value set for the `TransferSite.AlternativeAddresses.retryPolicy` configuration option. It allows you to set a "retry policy" with a list of alternative endpoints (presented in IP address: Port number pairs or hostname) you define on this screen. But before you are able to do so, you must go to **Operations > Server Configuration** and set the policy type using either of the following values: • `AllHostsOnEachRetry` – with this policy SecureTransport iterates through each endpoint, one by one, starting with the first in the list. If connection not successful, SecureTransport will continue trying each endpoint one after another until the maximum number of retries is reached. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `OneHostOnEachRetry` – with this policy SecureTransport tries to connect to the first endpoint in the list. If connection not successful, SecureTransport will continue trying that endpoint until the maximum number of retries is reached; and then will move to the next one in the list. Following that same pattern, SecureTransport will try each endpoint until success; or until end of list. You can set the maximum retry value by editing the `EventQueue.maxRetryCount` configuration option. • `Disabled` (default) – this is the default value that keeps the table with

Field	Description
	endpoints entirely hidden from view.
Network Zone	The network zone that defines the proxies to use for transfers through this site. • Select **none** to connect directly to the remote SSH server. • Select **any** to allow SecureTransport to select the proxy connection using a network zone that enables an SOCKS5 proxy. • Select **Default** to use the default network zone proxy configuration. If no default is network zone is defined, transfers from this transfer site fail. • Select a specific network zone to use the proxy configuration defined for that zone. For more information, see *Specify TM Server communication ports and IP address for protocol servers on SecureTransport Edge* on page 224.
Download Folder	The folder on the remote server from which the file are transferred. Select download folder **Advanced Expression** to use expression language to evaluate the download folder. To use the expression language to append dates: The download folder will be evaluated using the current date when the transfer site is being executed. For example `folder_20150130`. Example: `folder_${date("yyyyMMdd")}`
Download Pattern Type	Select one of two types: **Regular Expression** or **File Globbing**. For regular expression syntax, see *Regular expressions* on page 1035. File globbing uses simple wildcards to specify a pattern. A question mark (`?`) matches any one character. An asterisk (`*`) matches any number of characters.

Field	Description
Download Pattern	The pattern used to match file names to determine whether a file is downloaded. Select download pattern **Advanced Expression** to use expression language to evaluate the download pattern. Using it together with **File Globbing** Pattern Type selected: The download pattern will be evaluated using the current date when the transfer site is being executed. For example `*_20150130.txt`. This will match all files ending with `_20150130.txt`. Example: `*_${date("yyyyMMdd")}.txt` Using it together with **Regular Expression** Pattern Type selected: The download pattern will be evaluated using the current date when the transfer site is being executed. For example `*[a-z]_20150130.txt`. This will match all files starting with any combination of letters from `a` to `z` and ending with `_20150130.txt`. Example: *[a-z]_${date("yyyyMMdd")}.txt
Allow Overwrite	Taken into account when the site is used by Send To Partner step. If checked the value of "Upload folder" will be overwritten with the value of "Overwrite upload folder". For more details see *Advanced Routing* on page 795.
Upload Folder	The folder on the remote server to which files are transferred.
Upload Permissions	Sets permission of the remote file during SFTP push. SecureTransport changes the file permissions as they are set in the SSH Transfer Site during the transfer.
Update Permissions with Chmod Command	Determines whether to use **`chmod`** or **`umask`** command to change file permissions. This setting overrides the global setting configured via the `Ssh.UpdateFilePermissionsWithChmodCommand` option. The possible values are: **Default** - The global setting is applied. **True** – The file permissions, specified in the SSH transfer site, are set after transfer ends with chmod. **False** – The file handler is opened with specified permissions. The file permissions are set with `umask`. There is **no need** to edit the Upload Permissions field - the correct format is automatically set.

Transfer settings

Transfer Settings pane for a SHH protocol transfer site:



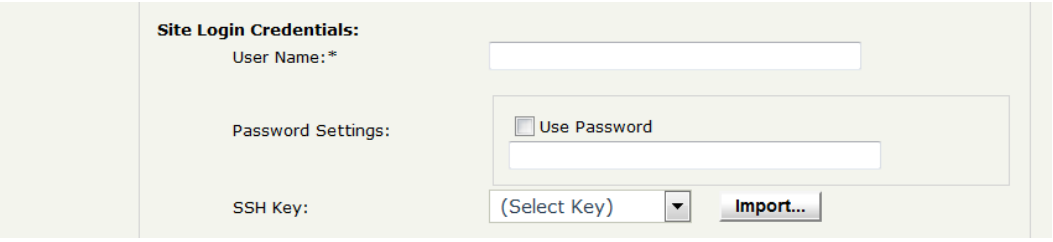
The following table describes the transfer settings options for a SSH protocol transfer site.

Field	Description
Transfer Settings	
Transfer Mode	Specify whether data is transferred as ASCII or binary. You can also choose to have SecureTransport automatically determine the correct transfer mode. For more information about automatically determining transfer mode, see *Client-initiated and server-initiated transfers* on page 701.
Verify Fingerprint for this Site	Select this check box to require SecureTransport to verify the fingerprint for the SSH key against the value you specify below. If the values do not match, the connection is refused.
Fingerprint	The value against which you want to verify the fingerprint from the remote server. If the partner SSH server has both DSA and RSA keys configured, the fingerprint that SecureTransport must verify for a server-initiated transfer depends on FIPS transfer mode. With FIPS transfer mode enabled, enter the fingerprint for the DSA key. With FIPS transfer mode disabled, enter the fingerprint for the RSA key. **Note** The fingerprint value must start with a formatted hashing algorithm name in the following format: `<hashing_algorithm>:<certificate_ssh_fingerprint_hash>` Examples: • `MD5:2d:d2:3d:32:d2:24:f2:2s:1a:2s:1a:23:af:e1:4s:3f` • `SHA-1:43:51:43:a1:b5:fc:8b:b7:0a:3a:a9:b1:0f:66:73:a8` • `SHA-256:12:5a:32:a1:5b:fc:8b:b7:00:a4:a9:b1:f0:88:73:c9`

Field	Description
Enable FIPS Transfer Mode	Restrict SSH to use only FIPS 140-2 Level 1 certified cryptographic libraries. When you enable FIPS transfer mode, the panel expands with the following fields that let you specify the desired set of SSH ciphers and algorithms for server-initiated transfers through this site: • FIPS cipher suites – allowed ciphers for server-initiated transfers through this site in FIPS mode. By default, this set is populated with the cipher suites as defined in the `Ssh.FIPS.SIT.Ciphers` configuration option. • FIPS allowed macs – allowed MAC algorithms for server-initiated transfers through this site in FIPS mode. By default, this set is populated with the MAC algorithms as defined in the `Ssh.FIPS.SIT.AllowedMacs` configuration option. • FIPS key exchange algorithms – allowed KEX algorithms for server-initiated transfers through this site in FIPS mode. By default, this set is populated with the KEX algorithms as defined in the `Ssh.FIPS.SIT.KeyExchangeAlgorithms` configuration option. • FIPS public keys – allowed public keys for server-initiated transfers through this site in FIPS mode. By default, this set is populated with the public keys as defined in the `Ssh.FIPS.SIT.PublicKeys` configuration option. All fields are editable. The supported FIPS ciphers and algorithms from which you can select when adding new ones are listed in *FIPS transfer mode* on page 983. Note that both the sender and the recipient must use FIPS-approved ciphers and algorithms supported by SecureTransport. Otherwise, the transfer will fail.

Site login credentials

Site Login Credentials pane for a SHH protocol transfer site:



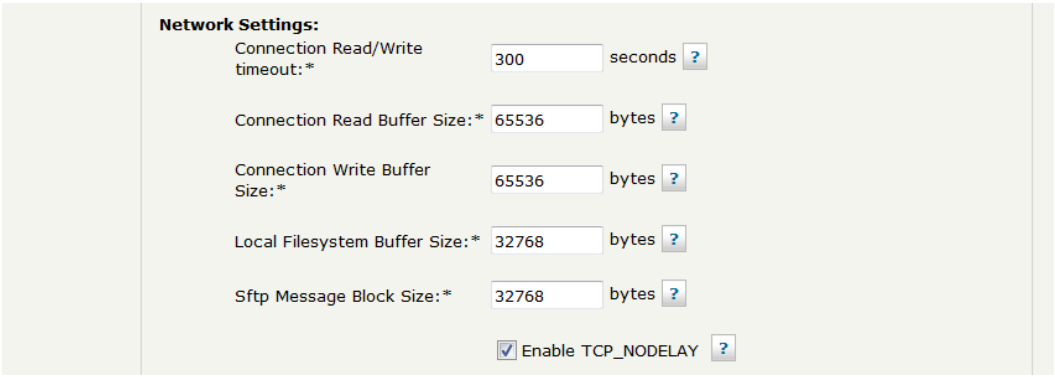
The following table describes the site login credentials options for a SSH protocol transfer site.

Field	Description
Site Login Credentials	

Field	Description
User Name	Username used to log in to the SSH server. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
Use Password	Select to use a password to log in to the SSH server.
Password	Password used to log in to the SSH server.
SSH Key	The certificate used to identify the user logging in. You can select a certificate or import a certificate. By default, the usage of SSH keys contained in expired X509 certificates is allowed for SIT transfers. To forbid it, set the `SSH.SIT.allowExpiredCertificates` to `false`.

Network settings

Network Settings pane for a SHH protocol transfer site:



The following table describes the network settings options for a SSH protocol transfer site.

Field	Description
Network Settings	
Connection Read/Write timeout	The maximum number of seconds the server waits to read a block of data from the partner server, or write a block of data to the partner server. If not specified, its value is 300 seconds. This option corresponds to the `SO_RVCTIMEO` and `SO_SNDTIMO` Socket options.

Field	Description
Connection Read Buffer Size	The size of the receive buffer in bytes used by the socket open for the transfer. It is used by the platform's networking code as a hint for the size to set the underlying network I/O buffers. Increasing the receive buffer size can increase the performance of network I/O for high-volume connections, while decreasing it can help reduce the backlog of incoming data. This value is also used to set the TCP receive window that is advertized to the remote peer. This option corresponds to the `SO_RCVBUF`. The value should be a positive integer.
Connection Write Buffer Size	The size of the send buffer in bytes used by the socket open for the transfer. It is used by the platform's networking code as a hint for the size to set the underlying network I/O buffers. This option corresponds to the `SO_SNDBUF`. The value should be a positive integer.
Local Filesystem Buffer Size	The size of the buffer in bytes used for reading from the local file system when performing the transfer.
SFTP Message Block Size	The SFTP block size value used for the transfer.
Enable TCP_ NODELAY	Enable or disable Nagle algorithm for the transfer.

Test SSH Connection

After you have filled in all the required settings, you can check if the connection between the transfer site and the remote partner is configured correctly. The test is performed based on the input on the transfer site page. The functionality is available for saved and non-saved transfer sites.

To initiate a test connection, click the **Test Connection** button located in the top-right corner of the configuration pane. Using the transfer site settings currently specified on the page, SecureTransport will to try to connect to the remote partner and display the result.

The *Result test connection* pane contains the following information:

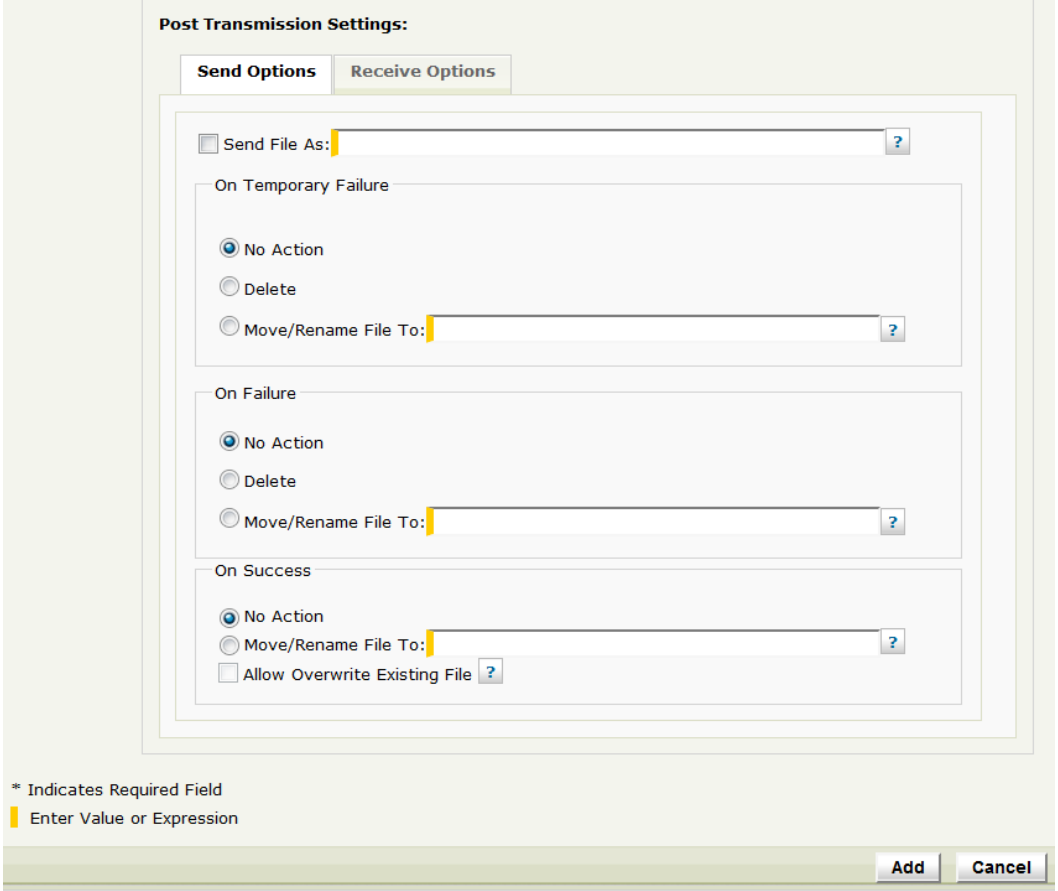
- `Connection status` – `success` or `failed`.
- `Fingerprint verification status` – `success`, `failed` or `not verified`.
    - `success` – the fingerprint verification during the test connection is successful.
    - `failed` – the fingerprint verification during the test connection failed.
    - `not verified` – the fingerprint verification is skipped during the test connection.
- `Fingerprint` – the fingerprint used in the test connection.
- `Cipher suite` – the name of the cipher suite used in the test connection.

- `HMAC` – hash-based message authentication codes used in the test connection.
- `Key exchange algorithms` – the KEX used in the test connection.
- `Public key` – the public key used in the test connection.
- `Send Buffer size` – the size of the send buffer in bytes `(SO_SNDBUF)` used in the test connection.
- `Receive Buffer size` – the size of the receive buffer in byte `(SO_RCVBUF)` used in the test connection.
- `Authentication status` – either `success` or `failed`.
- `SSH key alias` – the SSH key alias used in the test connection.
- `Session ID` – the Session ID associated with the test connection, represented as a link to the filtered Server Log entries.
- `Error details` – in the event of an error, displays detailed information on why the test connection failed.

Note The **Test Connection** option is also exposed as a REST API resource.

Post transmission send options

Post Transmission Settings - Send Options pane for a SHH protocol transfer site:



The following table describes the post transmission send settings options for a SSH protocol transfer site.

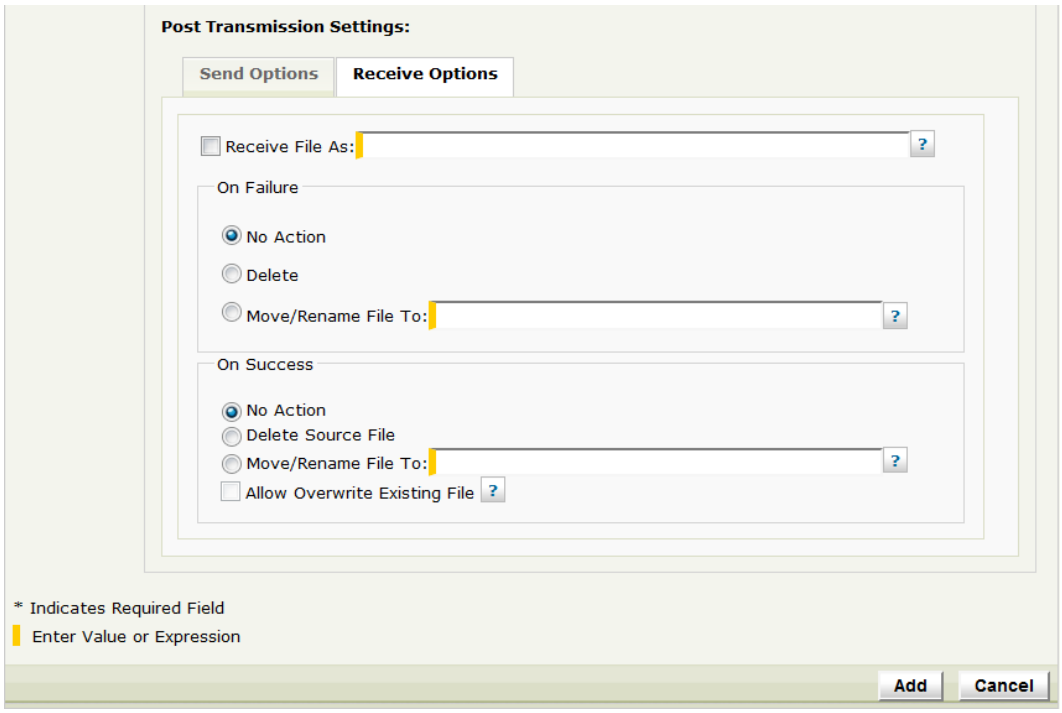
Field	Description
Send Options	
Send File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name.
On Temporary Failure	A temporary failure can occur when the transfer is incomplete and a retry occurs. Select one of the three choices: **No Action**, **Delete Destination File**, or **Move File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete Destination File** removes the file from the new location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.

Field	Description
On Failure	A failure occurs when the transfer is incomplete and all retry attempts were unsuccessful. Select one of the three choices: **No Action**, **Delete Destination File**, or **Move File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete Destination File** removes the file from the new location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.
On Success	Select one of the choices: **No Action**, or **Move File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file. Select **Allow Overwrite** to allow the file move to overwrite an existing file. If **Allow Overwrite** is not selected, a file transfer that attempts to overwrite an existing file fails.
Allow Overwrite Existing File	When enabled and the rename operation fails because the target file exists, SecureTransport will delete the target file and repeat the rename operation.

Note To preserve the original file name when using the **Move File To** option, use the `${stenv.target}` or `${stenv['target']}` expression.

Post transmission receive options

Post Transmission Settings - Receive Options pane for a SHH protocol transfer site:



The following table describes the post transmission receive settings options for a SSH protocol transfer site.

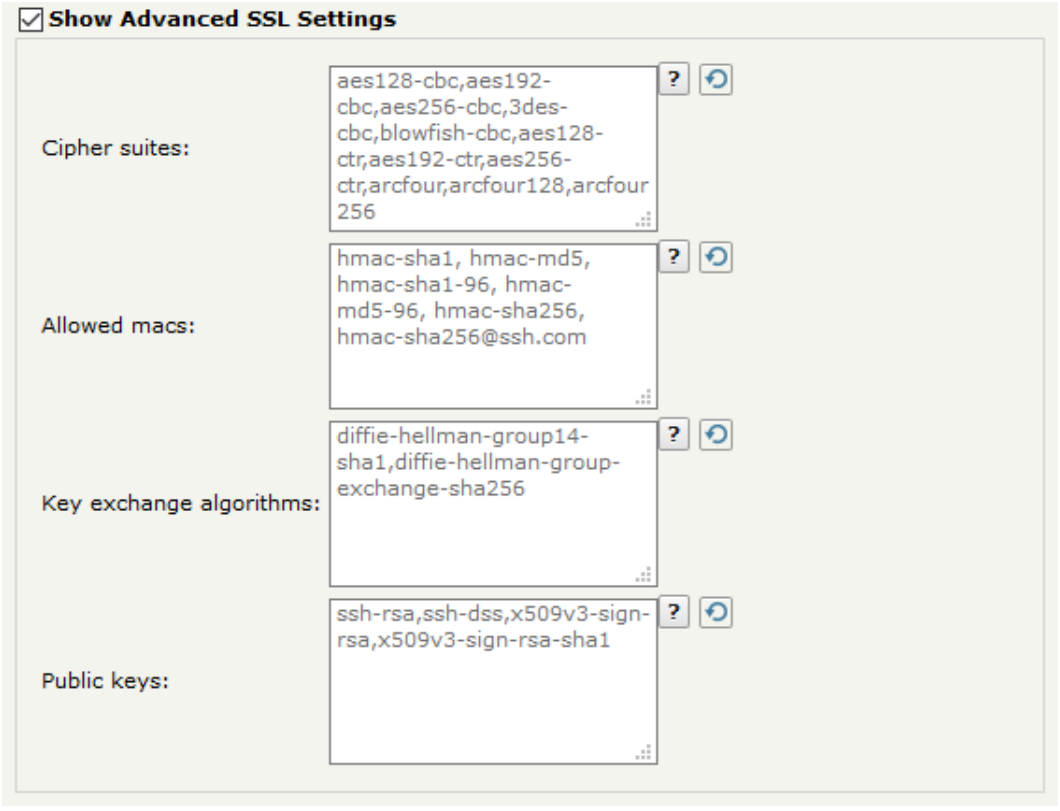
Field	Description
Receive Options	
Receive File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name when the transfer is received. You can use the SecureTransport-specific variable `${stenv.site_target}` which takes the value from the remote file path. see *Expression Language* on page 1020 for information on SecureTransport-specific variables.
On Failure	A failure occurs when the transfer is incomplete and all retry attempts were unsuccessful. Select one of the three choices: **No Action**, Delete Source File, or **Move File To**. Selecting **No Action** causes the file to stay in the original location. If another file with the same name is transferred to this location, the original file is overwritten. Selecting Delete Source File removes the file from the original location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files from and to provide an expression used to rename the file. To preserve the original file name you can use the SecureTransport-specific named variable `${stenv.target}`.

Field	Description
On Success	Select one of the three choices: **No Action**, **Delete Source File**, or **Move File To**. Selecting **No Action** causes the file to stay in the original location. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete Source File** removes the file from the original location. Selecting **Move File To** requires you to specify a directory in the location where you are transferring the files from and to provide an expression used to rename the file.
Allow Overwrite Existing File	When enabled and the rename operation fails because the target file exists, SecureTransport will delete the target file and repeat the rename operation.

Note To preserve the original file name when using the **Move File To** option, use the `${stenv.target}` or `${stenv['target']}` expression.

Advanced SSL Settings

Advanced SSL settings allow you to define Cipher suites and SSL protocols with your current SSH Transfer Site. Select **Show Advanced SSL Settings** to expand the pane with available options.



The following table describes the Advanced SSL Settings for a SSH protocol transfer site. Select the checkbox to expand the pane with available options.

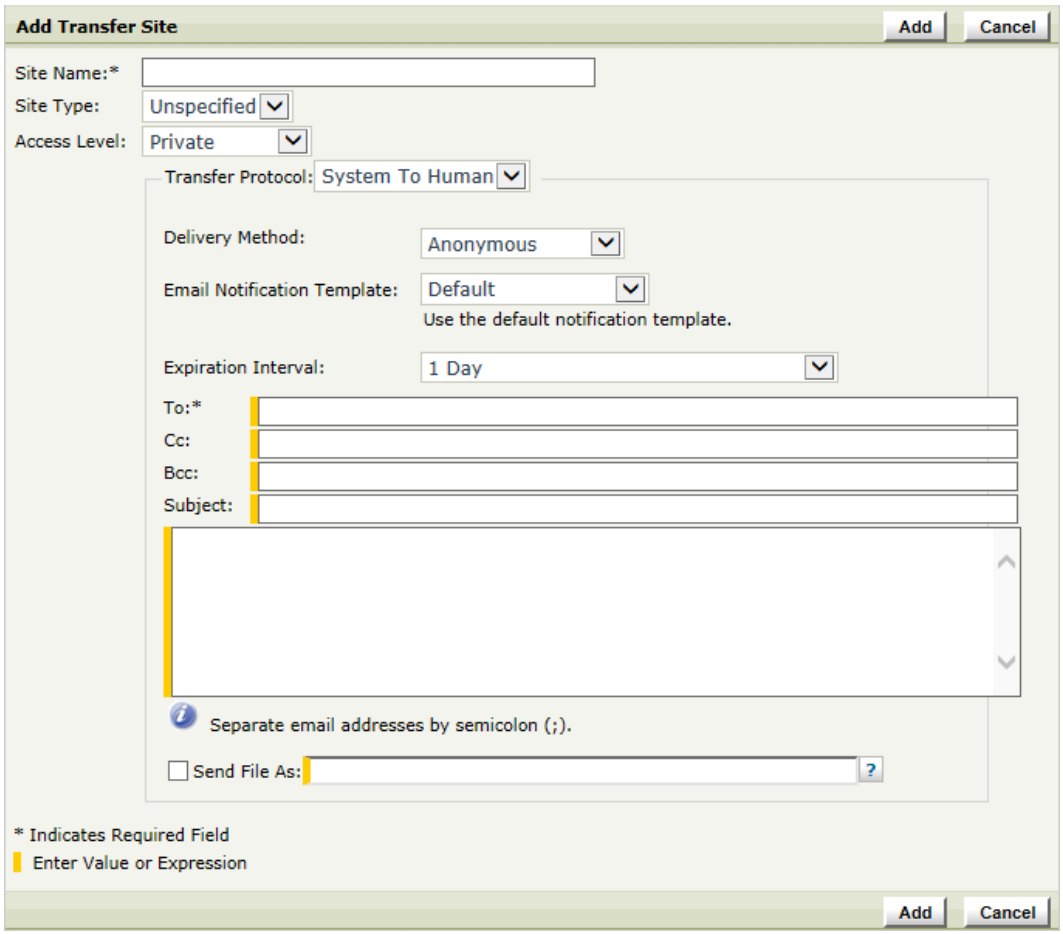
Field	Description
Show Advanced SSL Settings - select this check-box to expand the pane with available options.	
Cipher suites	The set of cipher suites for secure SIT connection with the current SSH transfer site. By default this set is populated with the cipher suites as defined in the `Ssh.SIT.Ciphers` configuration option. To reset to default values, click the button next to the tooltip.
Allowed macs	The set of allowed HMAC algorithms with the current SSH transfer site for secure SIT connection, presented in a comma-separated list. By default this list is populated with the supported MAC algorithms as defined in the `Ssh.SIT.AllowedMacs` configuration option.
Key exchange algorithms	The set of allowed key exchange algorithms with the current SSH transfer site for secure SIT connection, presented in a comma-separated list. By default this list is populated with the supported key exchange algorithms as defined in the `Ssh.SIT.KeyExchangeAlgorithms` configuration option.
Public keys	The set of allowed public key algorithms with the current SSH transfer site for secure SIT connection, presented in a comma-separated list. By default this list is populated with the supported public exchange algorithms as defined in the `Ssh.SIT.PublicKeys` configuration option.

System to Human transfer sites

You can use a System to Human transfer site to send files to email recipients. SecureTransport sends a notification email to the recipients from the email address specified in the **Email Contact** field of the user settings. If the email is not set, SecureTransport does not send the notification email and logs an error.

A recipient of a notification email retrieves the file based on the security level specified. In some cases, the recipient clicks a link in the notification email to retrieve the file. In other words, the recipient must log in to ST Web Client or one of the Axway Email Plug-ins and the user logs in to SecureTransport to retrieve the files. The notification email is from the email address specified in the **Email Contact** field of the user settings. If the email is not set, the If the security level allows, SecureTransport enrolls the user, creating an account.

The following is the *Add Transfer Site* page for a transfer site definition that uses the System to Human transfer protocol.



You can use hardcoded values, expressions in the supported expression language, or a combination of both to complete the fields indicated by a vertical yellow bar. For more information about expressions, see *Expression Language* on page 1020.

The following table describes the System to Human options for a transfer site.

Field	Description
Delivery Method	Controls user enrollment: • **Anonymous** – The recipient clicks a link in the email and can retrieve the files. • **Challenge** – When the recipient clicks the link in the email to retrieve the files, the recipient must answer a secret question correctly. • **Existing Account** – The recipient must have a SecureTransport accounts. • **Enroll Unlicensed** – SecureTransport enrolls the recipient as an unlicensed user, if necessary. • **Enroll Licensed** – SecureTransport enrolls the recipients as licensed users, if necessary.

Field	Description
Secret Question	This field is displayed when the **Delivery Method** is `Challenge`. Type the question that the email recipient must answer to retrieve the files.
Answer Re-enter Answer	These fields are displayed when the **Delivery Method** is `Challenge`. Type the answer to the question.
Email Notification Template	Select `Default` or an email template that SecureTransport uses to compose the file transfer notification and status emails. You specify the email templates on the *Mail Template Repository* page. You specify the default email notification template on the *AdHoc Settings* page.
Expiration Interval	The number of days before the message expires. The choices are: 1 Day, 7 Days, 30 Days, 60 Days, and Never.
To	Type values that can include expressions for the email addresses of the main recipients. Use a semicolon (`;`) to separate email addresses.
Cc	Type values that can include expressions for the email addresses of the copy recipients. Use a semicolon (`;`) to separate email addresses.
Bcc	Type values that can include expressions for the email addresses of the blind copy recipients. Use a semicolon (`;`) to separate email addresses.
Subject	Type a value that can include expressions for the subject of the file transfer emails.
Text	In the unlabeled email body field, type a value that can include expressions for the text of the notification emails.
Send File As	Select the check box to specify a file name. You can use the expression language to specify the criteria you want to match. The expression uses the criteria provided to create a new file name from the original file name. For example, when a file arrives in a H2S file transfer, SecureTransport renames the file by prepending a unique ID to the file name. If the file it routed to an H2S transfer site to forward it, the expression, `${stenv.target.replace('^.{66}', '')}`, removes the ID.

Manage transfer sites

Use the *Transfer Sites* page to create, edit, and delete transfer sites.

The following topics provide how-to instructions for managing transfer sites:

- *Create a transfer site* on page 598
- *Edit a transfer site* on page 599

- *Delete a transfer site* on page 599

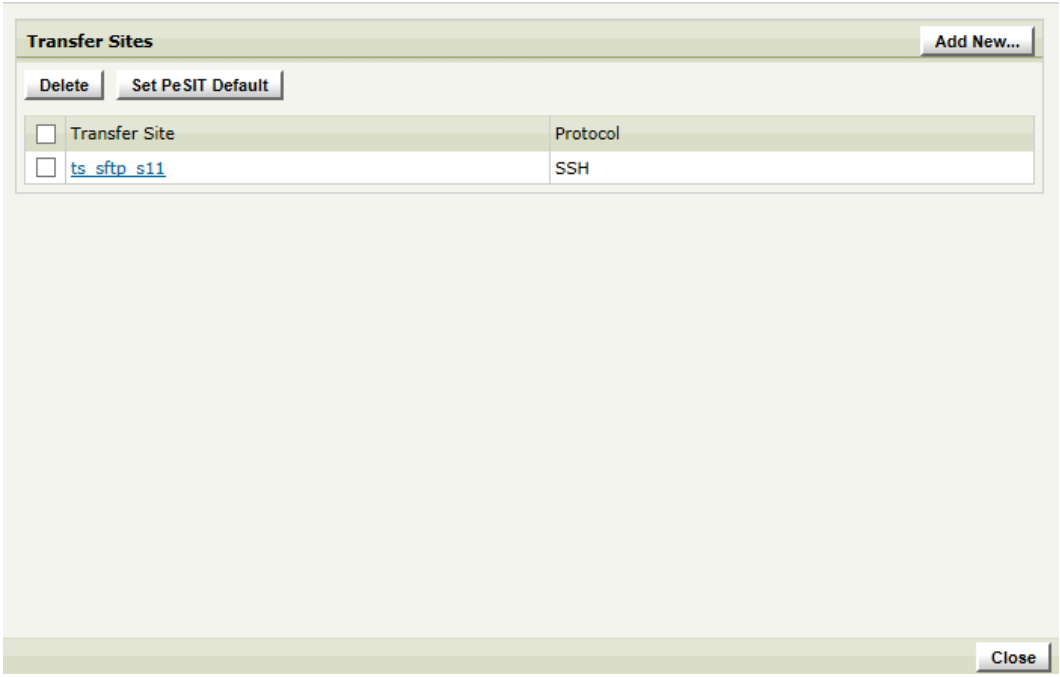
Create a transfer site

This topic provides a general procedure for creating a transfer site for an account. All supported protocols require custom settings. For details, see the reference topic for each protocol.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account to which you want to add a transfer site.

   The *Account Settings* page for that account is displayed.
3. Click **Transfer Sites**.

   The *Transfer Sites* page is displayed.



4. Click **Add New.**

   The *Add Transfer Site* page is displayed.
5. In the **Site Name** box, enter a unique name for the transfer site.
6. The Site Name is unique per account. Two sites could have the same names if they are associated with different accounts.
7. Select an **Site Type**. Use this parameter to differentiate between sites that transfer files internally and those that transfer files between partners. Choose from the following:
   - **Unspecified** – Default value. All transfer sites created using previous versions of SecureTransport have this value.
   - **Internal** – Transfers for this site occur within a single organization.
   - **Partner** – Transfers for this site occur between organizations.

8. Select the protocol that the transfer site uses for file transfers. The supported protocols are AS2, FTP(S), HTTP(S), SSH (SFTP and SCP), PeSIT, Connect:Direct, Folder Monitor, System to Human, Generic-HTTP(S), and SharePoint.
9. By default, the AS2 protocol settings are displayed first. This example displays the settings for creating an FTP(S) transfer site.
10. Edit the custom options depending on the selected transfer protocol.
11. Click **Add**

    The transfer site is added to the list of transfer sites available to the current account.

Edit a transfer site

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account that owns the transfer site to edit.
3. Click the **Transfer Sites** tab.
4. Click the name of the transfer site to edit.
5. The *Edit Transfer Site* page is displayed.

   Note Editing a transfer site does not affect transfers in progress, including transfers that are being retried.
6. Edit the desired settings for the transfer site.

   Note The *Edit Transfer Site* page is identical to the *Add Transfer Site* page for the corresponding protocol.
7. Click **Save**.

Delete a transfer site

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account that owns the transfer site to delete.
3. Click the **Transfer Sites** tab.
4. Select the check boxes next to the names of the transfer sites to delete.
5. Click **Delete**.

Pluggable Transfer Sites

Pluggable Transfer Sites (connectors) are custom plug-ins that can be deployed on the SecureTransport Server to allow sending and receiving files over various protocols.

Once deployed, the connector adds a new Transfer Site to the list of Transfer Sites available for the user accounts.

A collection of Transfer Site plug-ins for SecureTransport can be found in the AMPLIFY Repository.

Pluggable Transfer sites are deployed on all SecureTransport Server nodes, into the following folder `${FILEDRIVE_HOME}/plugins/transferSites`.

For more information on Pluggable Transfer sites, refer to the SecureTransport Developer's Guide.

Note When using expressions to configure a Pluggable Transfer site there is a difference in the variable spaces, depending on the account type – e.g.

- With standard User Accounts, the flow attributes of a file would be accessible with expression in the following format: `${ts['userVars.test']}`
  Note The `${ts['userVars.test']}` expression is applicable only for evaluating Upload folder and a post-transmission action (PTA); and does not work with Download folder and pattern.
- With User Account Templates, the flow attributes of a file would be accessible with expression in the following format: `${stenv['DXAGENT_SUBSCRIPTION_ATTR_userVars_folder']}`

Transfer profiles

Transfer profiles provide additional information for PeSIT transfers. A subscription that retrieves files from a PeSIT transfer site or sends files directly to a PeSIT transfer site can specify a transfer profile for that site to use when receiving or sending the files. If no transfer profile is specified, there must be a default transfer profile and it is used.

Because transfer profiles are used only with PeSIT transfers, the *Transfer Profiles* page is not available until a PeSIT transfer site exists.

The following topics describe how to manage transfer profiles:

- *Create a transfer profile* on page 600
- *Edit a transfer profile* on page 602
- *Delete a transfer profile* on page 603

Create a transfer profile

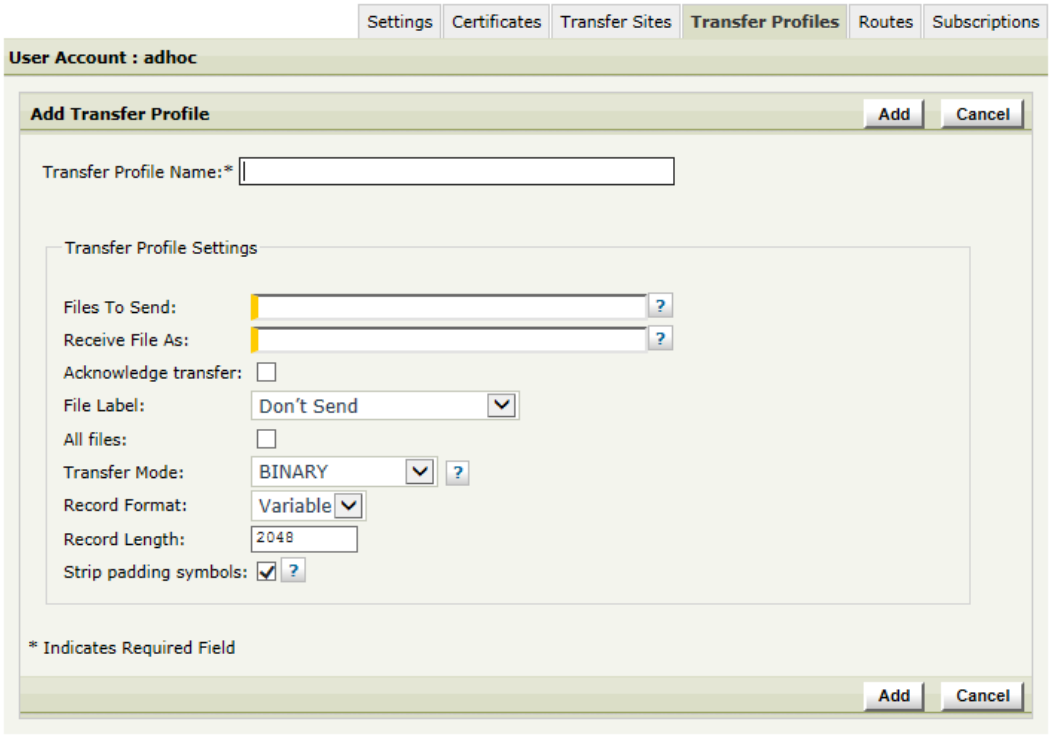
Use the following procedure to create a transfer profile.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account to which to add a transfer profile.

   The *Account Settings* page for that account is displayed.
3. Click the **Transfer Profiles** tab.

   The *Transfer Profiles* page is displayed.
4. Click **Add New.**

   The *Add Transfer Profile* page is displayed.



5. Enter the field values described in the following table.

Field	Description
Transfer Profile Name	The name you use to select the transfer profile in the subscription. If this name must matches the name of the IDF (PeSIT protocol PI 12) on a remote PeSIT partner for an transfer from the remote partner, this transfer profile is used.
Files To Send	Used to select the files to send when a partner site downloads. Relative to the user's home folder, so `/file` refers to a file in the home folder Any valid expression including PeSIT expressions For details, see *Expression Language* on page 1020.
Acknowledge Transfer	If this option is selected, a successful transfer is acknowledged by the receiving partner after the transfer finished and the transfer processing has been completed.

Field	Description
Receive Files As	Used to name the files received when files are transferred to SecureTransport. Relative to the user's home folder, so `/file` refers to a file in the home folder Any valid expression including PeSIT expressions. For details, see *Expression Language* on page 1020.
File Label	Controls whether the file name relative to the user's home folder is sent, the full file path and name is sent, or no file name is sent. Ignored when receiving files.
All files	If this option is selected, when SecureTransport initiates a download from the PeSIT partner, it gets all files whose names match the pattern. If this option is cleared, SecureTransport gets the first file with a matching file name.
Transfer Mode	`BINARY`, `ASCII`, `EBCDIC`, or `EBCDIC_NATIVE`. Use `EBCDIC_NATIVE` for files that use EBCDIC LF (0x25) as the end-of-line character.
Record Format	Fixed or Variable.
Record Length	Specifies the length of the records in bytes. Record Format and Record Length are only taken into account if the received or sent files do not have transfer metadata defined (PI31 and PI32).
Strip padding symbols	When **Strip padding symbols** is selected, the padding characters will be removed. This is the default behavior. When **Strip padding symbols** is not selected, the padding characters will not be removed. **Note** This is only applicable for incoming transfers when FIXED record format is set by the remote site. Padding symbols are added by the sending site. SecureTransport recognizes **null** when working in BINARY mode, **space** when in ASCII mode, and **@** when in EBCDIC or EBCDIC NATIVE modes.

6. Click **Add**.

   The new transfer profile is added to the list for the user.

Edit a transfer profile

Use the following procedure to edit a transfer profile.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account that owns the transfer profile to edit.

3. Click the **Transfer Profiles** tab.
4. Click the name of the transfer profile to edit.

   Note Editing a transfer profile does not affect transfers in progress, including transfers that are being retried.

5. Edit the desired settings for the transfer profile. For details about the fields, see *Create a transfer profile* on page 600.

   Note The *Edit Transfer Profile* page is identical to the *Add Transfer Profile* page.

6. Click **Save**.

Delete a transfer profile

Use the following procedure to delete a transfer profile.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the under the account that owns the transfer profile you want to delete.
3. Click the **Transfer Profiles** tab.
4. Select the check boxes next to the names of the transfer profiles to delete.
5. Click **Delete**.

Subscriptions

A subscription provides a functional connection between a user account and an application.

For each subscription, SecureTransport creates a subscription folder and stores and manages all files that are transferred or transformed as a result of the application activity. A single application can have subscriptions from multiple accounts and a single account can subscribe to multiple applications. An account can subscribe to new instances of the same application as long as each instance has a unique subscription folder name.

Additional transfer configurations are possible for subscriptions. Use subscriptions to trigger the execution of specific actions, defined in the respective application, when a subscription event occurs, such as an incoming file transfer in the dedicated subscription folder.

Note The application is not triggered if the file is uploaded into another folder first and is then moved or copied into the subscription folder.

The following topics describe how to manage subscriptions:

- *Encryption options* on page 604
- *Post-transmission actions* on page 605
- *Manage subscriptions* on page 607

Encryption options

SecureTransport can encrypt a file before transferring it. You can specify the following options for files you are uploading:

Encryption setting	Description
Encrypt File As	Determines if the file should be encrypted and if the encrypted file is saved to a different name, location, or both. You can use a file name expression.
Encrypt Using PGP Key	Determines if SecureTransport uses PGP to encrypt the file and which PGP key it uses.
Sign Using PGP Key	Determines if SecureTransport signs the file using a PGP key and which PGP key it uses.
Compression	Determines what type of compression is used. Choose from ZIP, ZLIB, or BZIP2. You can also choose to use no compression or to use preferred compression. Preferred compression methods and order of preference are determined by examining the recipient's PGP key. If the data compression method you choose is not among the recipient's preferred methods, it is possible that the recipient will not be able to access the data. You must also select the compression level: Fast, Normal, Good, or Best.
Encode Using ASCII Armor	Determines if SecureTransport uses ASCII armor encoding. ASCII armor refers to using binary-to-text encoding for plain text data.
Keep Original As	Determines if the original unencrypted file is saved to a different name, location, or both. You can use a file name expression.

You can also choose to decrypt encrypted files when you download them. Decryption includes the following options:

Decryption setting	Description
Decrypt PGP File As	Determines if the file should be decrypted and is the decrypted file is saved to a different name, location or both. You can use a file name expression.
Require Trusted Signature	Requires that the file contains a trusted signature or the transfer fails.

Decryption setting	Description
Require Encryption	Requires that the file is encrypted or the transfer fails.
Keep Original As	Determines if the original encrypted file is saved to a different name, location, or both. You can use a file name expression.

Note Files that were encrypted using ASCII armoring or data compression are automatically decrypted and decompressed when you decrypt the PGP file.

Post-transmission actions

Subscriptions can also be set up to trigger post-transmission actions for either outgoing or incoming files. Post-transmission actions can be used to move, delete, or rename files based on the success or failure of a transfer. Using these options you can prevent files from being overwritten by renaming them, delete failed transfers, or move transferred files to a different directory on the server. You can also delete a file on the remote server after it is transferred. An expression language is provided so you do not need to specify a file name but can use patterns to control the post-transmission actions.

The following post-transmission actions are provided:

Post-transmission setting	Description
Send Options	
On Failure	A failure occurs when the transfer is incomplete and all retry attempts were unsuccessful. Select one of the three choices: **No Action**, **Delete**, or **Move/Rename File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete** removes the file from the new location. Selecting **Move/Rename File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.
On Success	Select one of the three choices: **No Action**, **Delete**, or **Move/Rename File To**. Selecting **No Action** causes the file to stay in the new location with the file name you specified. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete** removes the file from the original location. Selecting **Move/Rename File To** requires you to specify a directory in the location where you are transferring the files to and to provide an expression used to rename the file.

Post-transmission setting	Description
Receive Options	
On Failure	A failure occurs when the transfer is incomplete and all retry attempts were unsuccessful. Select one of the three choices: **No Action**, **Delete**, or **Move/Rename File To**. Selecting **No Action** causes the file to stay in the original location. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete** removes the file from the original location. Selecting **Move/Rename File To** requires you to specify a directory in the location where you are transferring the files from and to provide an expression used to rename the file.
On Temporary Failure	A temporary failure can occur when the transfer is incomplete and a retry occurs. Select one of the three choices: **No Action**, **Delete**, or **Move/Rename File To**. Selecting **No Action** causes the file to stay in the original location. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Delete** removes the file from the original location. Selecting **Move/Rename File To** requires you to specify a directory in the location where you are transferring the files from and to provide an expression used to rename the file. On Temporary Failure is only available for server-initiated transfers
On Success	Select one of these choices: **No Action** or **Move/Rename File To**. Selecting **No Action** causes the file to stay in the original location. If another file with the same name is transferred to this location, the original file is overwritten. Selecting **Move/Rename File To** requires you to specify a directory in the location where you are transferring the files from and to provide an expression used to rename the file.

Note To preserve the original file name when using the **Move/Rename File To** option, use the `${stenv.target}` or `${stenv['target']}` expressions.

When using SecureTransport on the Windows platform and you are renaming a file for a post-transmission action, you cannot use the following characters: `* < > ? " / \ | :`.

Use URL encoding instead if you need to represent one of these characters for a remote post-transmission action.

If you are using SecureTransport on a UNIX-based platform, the following characters cannot be used: `/ . \`.

When using SecureTransport on the Windows platform and you configure a post-transmission action in a subscription to move a file from one drive partition to another, no folders are created on the new drive partition and the files are not moved.

Paths specified in post-transmission options are treated as either relative to the subscription folder or an absolute path starting from the subscription folder.

- Relative paths are resolved against the target location which might not be the subscription folder, but can be any of its subfolders. If you use ".." in the file name expression, the final destination cannot go up the folder tree past the subscription folder.
- Absolute paths are calculated as relative to the subscription folder. The final destination here is bound to the subscription folder even when the expression uses ".." one or more times.

Manage subscriptions

Use the *Subscriptions* pane of the *User Account* window to manage subscriptions.

The following topics provide how-to instructions for managing subscriptions:

- *Subscribe an account to an application* on page 607
- *Considerations for subscriptions and AS2 transfer sites* on page 615
- *Human to System type application* on page 615
- *Scheduled downloads and tasks* on page 616
- *Set up a scheduled transfer task for a subscription* on page 617
- *Retrieve files now* on page 618
- *Purge a subscription folder* on page 620
- *Unsubscribe an account from an application* on page 620
- *Unsubscribe an account and delete the subscription folder* on page 620

Subscribe an account to an application

Before creating a subscription for an account, you must create at least one application for the system.

Note PGP decryption and encryption paths, regardless of whether you use a relative or an absolute path type, are relative and restricted to the directory where the file resides.

Prerequisites

- Create an application. For details, see *Manage applications* on page 757.
- If the account is to have server-initiated transfers associated with it, you must create at least one transfer site for the account. For details, see *Transfer sites* on page 494.

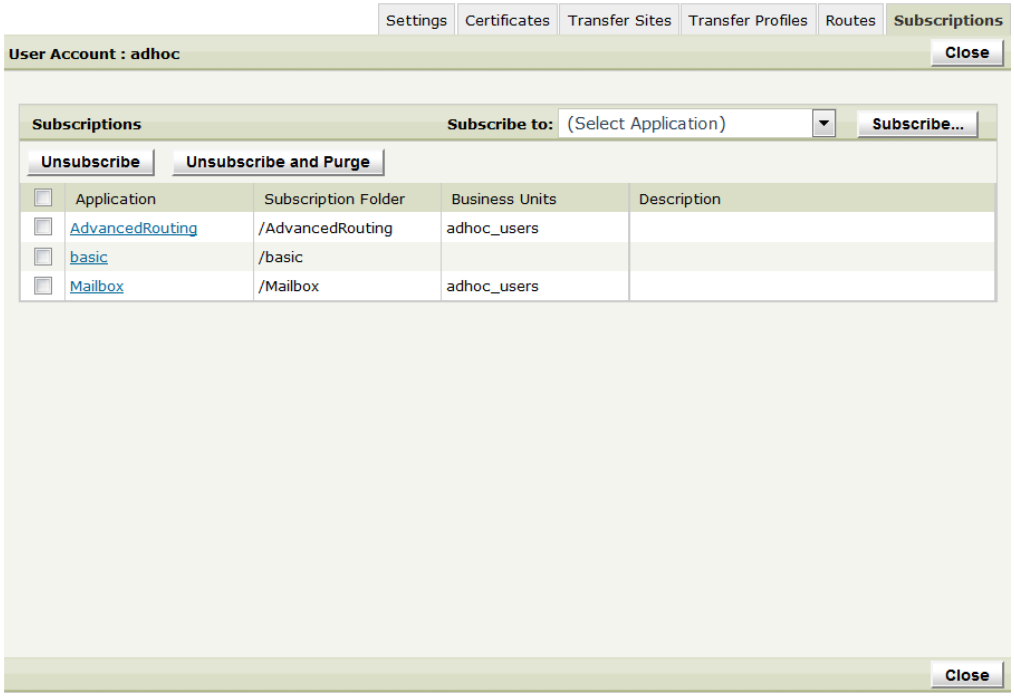
Workflow

1. *Select a user account* on page 608
2. *Configure general settings* on page 608
3. *Configure files received settings* on page 611
4. *Configure files sent settings* on page 613
5. *Complete the subscription* on page 615

Select a user account

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account for which you want to create a subscription.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Subscriptions** tab for the selected account.
4. Select the application you want to subscribe the account to from the **Subscribe to** list.



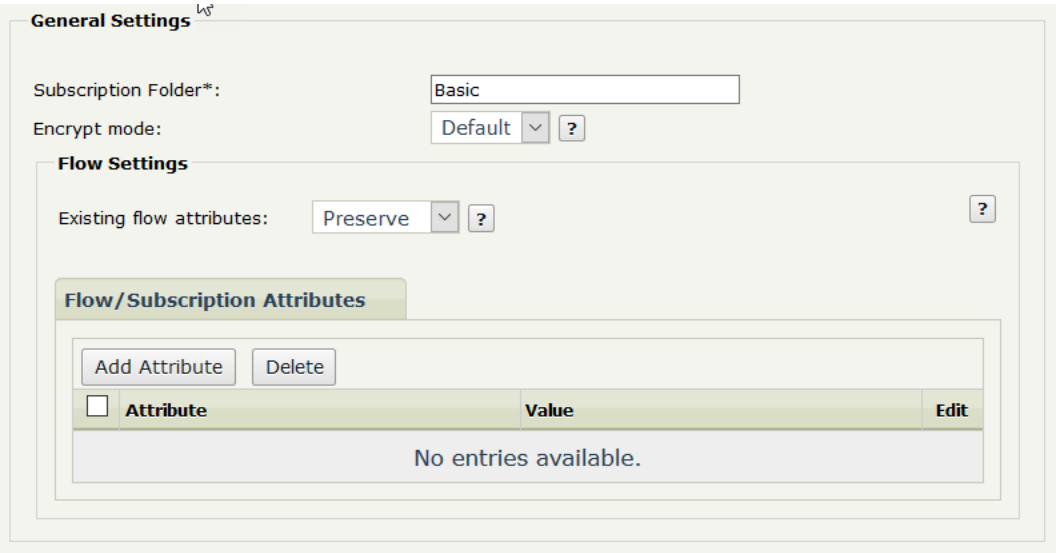
5. Click **Subscribe**.

   The settings page for the subscription is displayed.

   Note Some applications do not include all the fields described here.

Configure general settings

In the *General Settings* pane:



1. In the **Subscription Folder** field, type the full path to the subscription folder or use the default folder name. The subscription folder name can contain 254 characters or less.

   Note Axway does not recommend you to add leading or trailing space intervals to your subscription folder name as you may experience unexpected behavior with different SFTP / FTPS clients (although leading spaces are accepted with certain SFTP clients). You cannot use the following characters in the subscription folder name: `* < > ? " / \ | :`

2. Select the **Encrypt mode**. Selecting the **Encrypt mode** allows you to configure repository encryption for accounts at the per-subscription level. For additional information, refer to *Repository encryption certificate* on page 52.

   Select **Default** to inherit the encryption mode for the subscription folder from the account or the global settings.

   Select **Enable** to encrypt all files uploaded to the subscription folder.

   Select **Disable** to upload unencrypted files to the subscription folder.

   You can subscribe multiple accounts to the application. Some accounts may have repository encryption enabled for the subscription folder and others may have it disabled. As a result, the files uploaded from some accounts are encrypted while from other accounts the uploaded files are not encrypted.

   For example if:

   - **User1** has encryption **enabled** and is subscribed to **Shared Folder Application A**.
   - **User2** has encryption **disabled** and is subscribed to **Shared Folder Application B**.
   - **User3** is subscribed to both **Shared Folder Application A** and **Shared Folder Application B** and has encryption **enabled** for **Application A** and **disabled** for **Application B**.

   SecureTransport applies encryption to files that **User3** uploads and **User1** can download all files because they have repository encryption **enabled** for **Application A**. **User2** can only download unencrypted files because they have repository encryption setting **disabled** for **Application B**.

In this example, **User1** and **User3** can download all shared folder files because they have identical settings for repository encryption. **User1** and **User2** files are encrypted or not based on their repository encryption setting.

For example, three users are subscribed to a Shared Folder Application:

- **UserA** - Subscription repository encryption is set to **Enable**
- **UserB** - Subscription repository encryption is set to **Disable**
- **UserC** - Subscription repository encryption is set to **Disable**

Upload actions:

- **UserA** uploads a file to the subscription folder – The file is **encrypted**.
- **UserB** uploads a file to the subscription folder – The file is **unencrypted**.
- **UserC** uploads a file to the subscription folder – The file is **unencrypted**.

Result:

The subscription folder that the three users share contains both **unencrypted** and **encrypted** files.

Download actions:

- **UserA** can download all files from the subscription folder.
- **UserB** and **UserC** can only download unencrypted files from the subscription folder.

3. If you selected the Standard Router application type, Enter an ID in the **Subscriber ID** field.

   When the **Rename submitted files to include Subscriber ID** check box is selected during the application definition, the uploaded file is renamed before it is sent to the internal system. The file is renamed in the format `<ID> <FILE_NAME>` where `<ID>` is the `Subscriber ID` that is specified here for the current Subscription, and `<FILE_NAME>` is original file name. For details, see *Create a Standard Router application* on page 780.

4. In the *Flow Settings* pane, select the **Existing flow attributes**.

   If **Preserve** is selected, the attributes defined in the *Flow Attributes* pane will be applied only for newly received files which do not have associated flow attributes.

   If **Overwrite** is selected, the attributes defined in the *Flow Attributes* pane will overwrite any existing attributes for incoming files (for example, files published to this folder from another subscription folder).

   When **Append** is selected, only the attributes which are not defined for incoming files will be applied. Existing attributes will be preserved.

5. In the *Flow/Subscription Attributes* pane:

   a. To add an attribute, click **Add Attribute**. For additional information, refer to *Flow and subscription attributes* on page 175.

      Add Attribute enables the administrator to add custom properties (Key=Value). Flow attributes can be used for expression evaluation in Advanced Routing only when the application operates with files. Subscription attributes are bound to the subscription, therefore, they can be used for expression evaluation in all Advanced Routing fields.

Note Subscription attributes can be accessed using the following expression: `${subscription.attributes['userVars.ATTRIBUTE_NAME'].` Flow attributes can be accessed using the following expression: `${flow.attributes['userVars.ATTRIBUTE_NAME']}.`

Some examples of Attributes are:

Attribute	Value
userVars.1	internalEmail@axway.com
userVars.2	ReportsMonitor

To access attributes, see the following examples:

```
${account.attributes['userVars.1']}
```

```
${account.attributes['userVars.2']}
```

For example, the `account.attributes` is the selector for attributes of the account used to execute the current route - it has to be written exactly as shown.

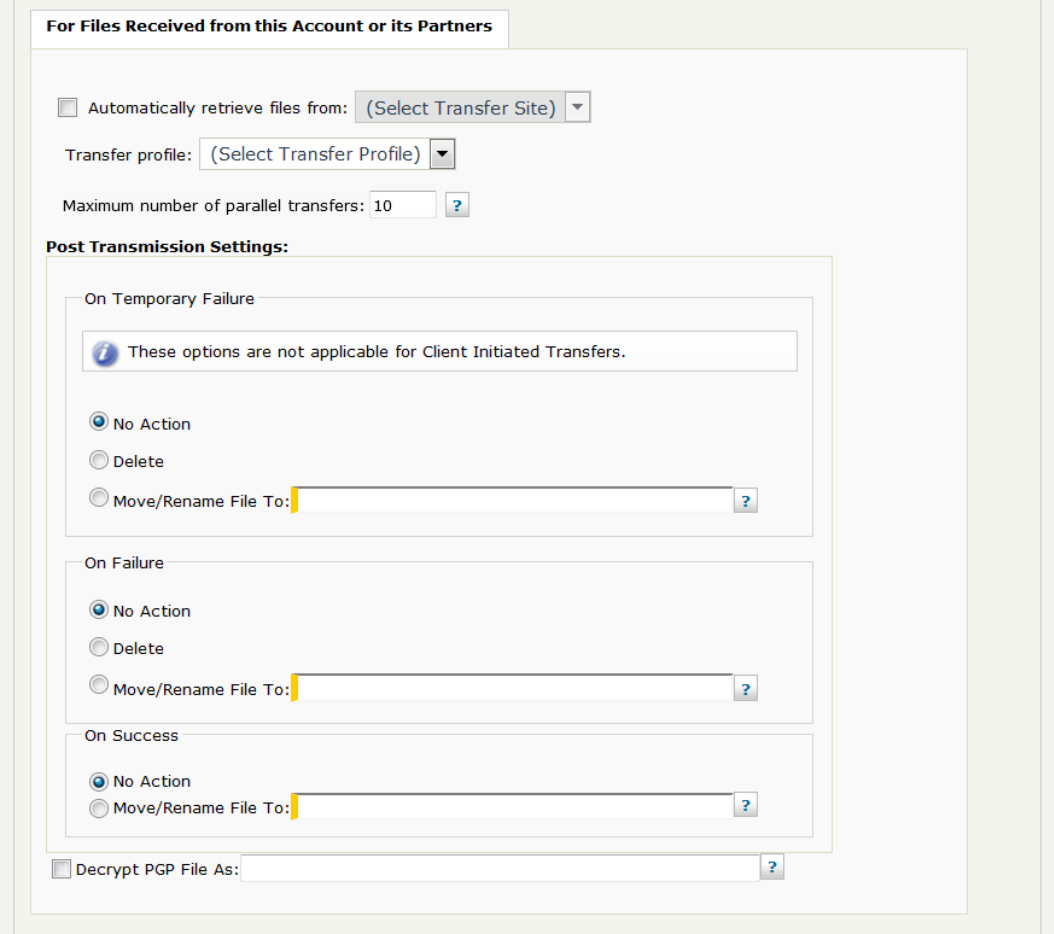
The `userVars.` prefix must be prepended to attribute name.

All this should be written as an EL expression: `${...}`

b. Click the attribute Save ( ) icon.

Configure files received settings

In the *For Files Received from this Account or its Partners* pane:



1. To set a schedule for automatic retrieval of the transferred files, select the **Automatically Retrieve Files From** check box and then select the respective transfer site from the drop down list. If you select a PeSIT transfer site, you can select a **Transfer Profile** from the list or leave the field empty to use the default PeSIT transfer profile. For more information, see *Transfer profiles* on page 600.

   The *Schedule* pane is displayed.

   A subscription that retrieves files from an AS2 transfer site does not use a schedule. To retrieve files from an AS2 transfer site, see *Considerations for subscriptions and AS2 transfer sites* on page 615.

   For a subscription that retrieves files from a Folder Monitor transfer site, to configure scheduled Folder Monitor operation, you must select **Set explicit FolderMonitor Schedule**.

2. (Optional) Click **Configure** in the *Schedule* pane to set up a future one time event or a recurring schedule.

   The *Configure Schedule* dialog box is displayed.

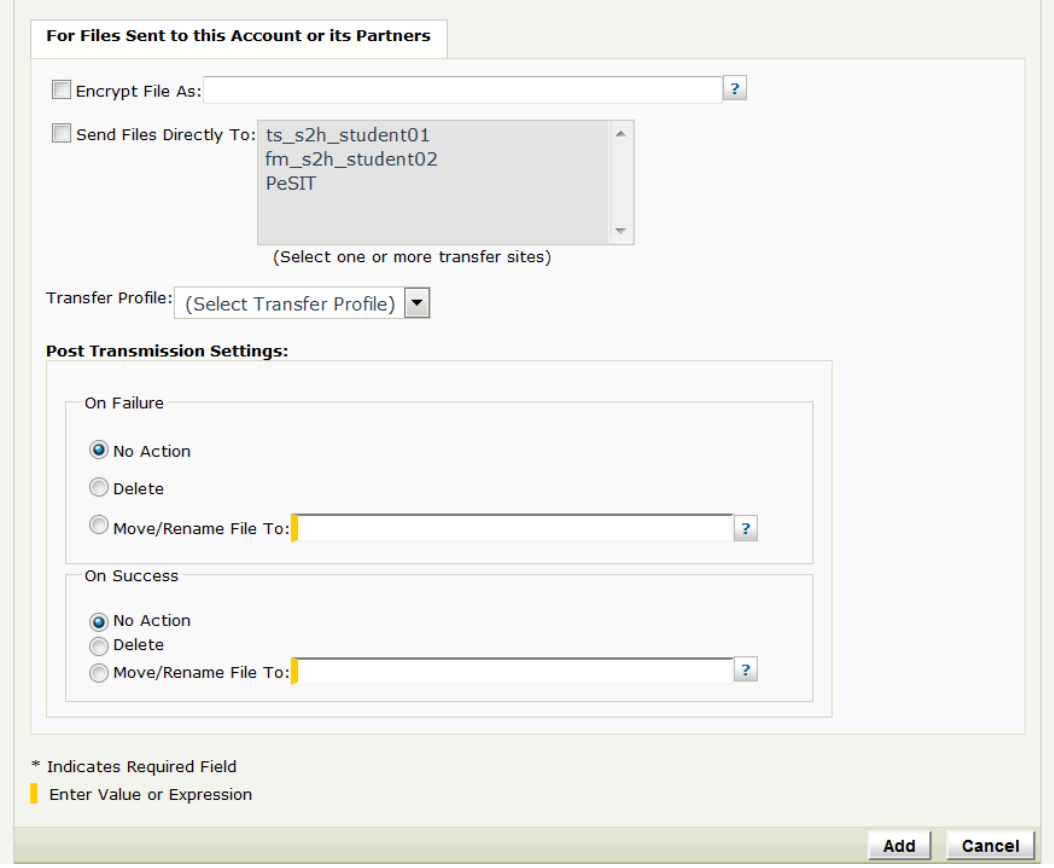
   Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

3. Specify the desired schedule. For details, see *Set up a scheduled transfer task for a subscription* on page 617.
4. (Optional) Enter the **Maximum number of parallel transfers**. If you enter a value greater than zero, SecureTransport executes only the specified number of transfers in parallel. If the value is null or zero, the maximum number of parallel transfers is limited by system capacity.

   The maximum number of parallel transfers limit is applied cluster wide. The limit for files transferred from the client will not be exceeded. Due to limitations in Standard Cluster communication mode, the parallel pulls limit can be exceeded when there are several connections. If you want to force the limit, then the `force.standart.cluster.sit.pulls.sync=true` system property should be added to the `start_tm_console`. Adding the property to the `start_tm_console` has a performance penalty due to increased cluster communication.
   Note that the `force.standard.cluster.sit.transfers.sync` value overrides the value of the `force.standart.cluster.sit.pulls.sync` property, used in previous SecureTransport versions for the same purposes.
5. (Optional) Click the **Retrieve Files Now** button to immediately trigger a one time file pull. For details, see *Retrieve files now* on page 618.
6. (Optional) In the *Post Transmission Settings* pane, set the failure and success options. For details, see *Post-transmission actions* on page 605.
7. To decrypt the transferred files, select **Decrypt PGP File As** and enter a file name or expression.
8. (Optional) Select or clear the **Require Trusted Signature** and **Require Encryption** options as needed for incoming transfers.
9. (Optional) Select **Keep Original As** to save the encrypted file. You can move the file to a different folder, rename the file, or both using either hard-coded text or by entering an expression.

Configure files sent settings

In the *For Files Sent to this Account or its Partners* pane:



1. Select or clear **Encrypt File As** for outgoing transfers. Enter a file name or an expression for the encrypted file.

   If you selected **Encrypt File As**, additional fields display. You must select either **Encrypt Using PGP Key** or **Sign using PGP Key** and select a PGP key.

2. Select or clear **Encrypt Using PGP Key** for outgoing transfers. If you turn this option on, you must select the PGP key used for encryption of outbound transfers from the list.

3. Select or clear **Sign using PGP Key** for outgoing transfers. If you turn this option on, you must select the PGP key used for signing of outbound transfers from the list.

4. (Optional) Select or clear **Use Data Compression** for outgoing transfers. If you turn this option on, you must select a data compression **Type** from the list. You must also select a **Compression Level**.

5. (Optional) Select or clear **Encode Using ASCII Armor** for outgoing transfers.

6. (Optional) Select **Keep Original As** to move the file to a different folder, rename the file, or both using either hard-coded text or by entering an expression.

7. (Optional) To set automatic sending of the files, select **Send Files Directly To** and choose one or more transfer sites from the drop-down list. Press either the Shift or Ctrl key while selecting the transfer sites to choose more than one site. All files in the outbox of the subscription folder are automatically sent to the selected transfer sites. If you select a PeSIT transfer site, you can select a **Transfer Profile** from the list or leave the field empty to use the default PeSIT transfer profile. For more information, see *Transfer profiles* on page 600.

Note Enable the `SendToSite` rules package to upload files without subscribing an account to an application. For more information, see .

8. (Optional) Under *Post Transmission Settings*, set the failure and success options.

Note If you configure two or more sites in **Send Files Directly To**, do not configure **Post Transmission Settings**.
If you select an AS2 transfer site, see *Considerations for subscriptions and AS2 transfer sites* on page 615.

Complete the subscription

To complete the subscription, Click **Add**.

Considerations for subscriptions and AS2 transfer sites

You can set independently the options to enable or disable automatic sending to and receiving files from an AS2 transfer site. For example, for a particular site, you can enable the **Automatically Retrieve Files From** option and disable the **Send Files Directly To** option.

Also, you can specify different AS2 transfer sites for each of the options. For example, you can send files directly to one AS2 transfer site and automatically receive files from a different AS2 transfer site.

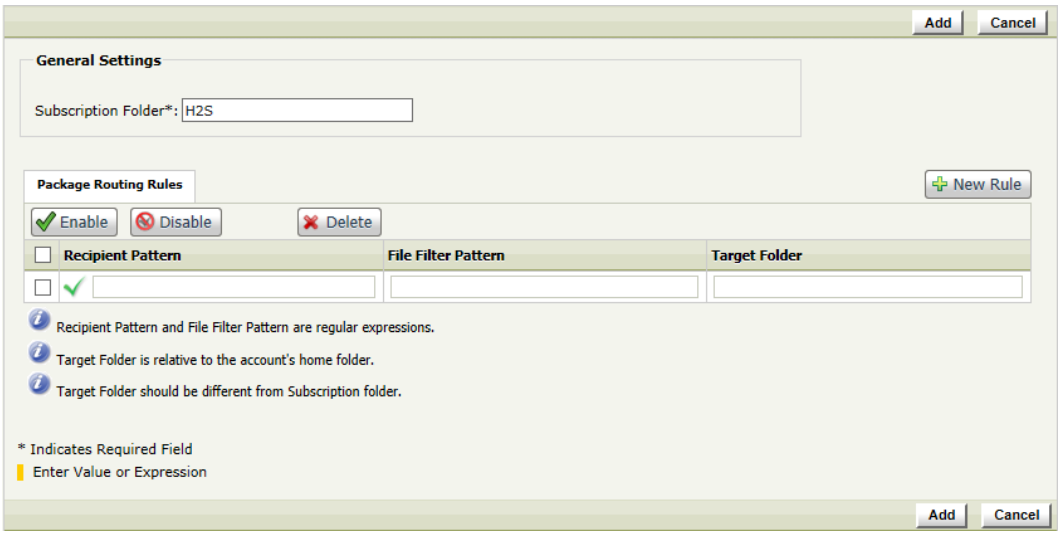
When you specify an AS2 transfer site in the **Automatically Retrieve Files From** list for a subscription, you cannot reuse the AS2 transfer site again in a different subscription.

If you specify an AS2 transfer site in the **Automatically Retrieve Files From** list for a subscription, the **On Temporary Failure** option is not displayed. This setting is not applicable for AS2 incoming transfers as they are never retried.

Human to System type application

Use a subscription to a Human to System type application to specify email addresses that represent destinations for files sent in emails from ST Web Client or from an email client using one of the Axway Email Plug-ins. When SecureTransport receives an email for one of these addresses, it process the files sent as you specify in the *Package Routing Rules* list in the subscription. SecureTransport applies all the rules that match the email.

Note An account can have at most one subscription to a Human to System type application.



1. In the **Subscription Folder** field, type the path to a folder that the application uses for temporary files or use the default folder name. The path is relative to the account home folder. The subscription folder name can contain 254 characters or less.
2. Create one or more package routing rules.
    a. Click **New Rule**.
    b. In the **Recipient Pattern** field, type a regular expression that matches the email addresses that this rule applies to. For example, `invoices@example\.com`.
    c. In the **File Filter Pattern** field, type a regular expression that matches the names of the files that this rules applies to. For example, `*\.xls`.
    d. In the **Target Folder** field, type the path to the folder that receives the files that arrive at a matching address and with a matching file name. The path is relative to the account home folder.

    Note For information about regular expressions, see *Regular expressions* on page 1035.

    The new rules are enabled by default.
3. Click **Add**.

Scheduled downloads and tasks

Use the scheduler functionality of SecureTransport to scheduled file downloads and tasks initiated by the server. You can schedule jobs to pull files from remote server in two ways, either per subscription or per application. You can access the scheduler page by creating or editing any application or subscription with a transfer site that supports scheduled transfers. Only file downloads can be scheduled.

When you create a scheduled transfer, for example, when creating a subscription connecting an account to an application where you are transferring files from a remote site or an internal system, you can set the following configuration options:

- Start Date and Time
- Perform the task once or perform recurring tasks at configurable regular intervals.
- Do not perform the scheduled task if it falls on a holiday.

Note The scheduler cannot be used for AS2 transfer sites.

Before queuing a new task, the server checks if a previous instance of same periodic task is still pending. If there is an instance of the same periodic scheduled task is pending, the new task is not scheduled.

If the server goes down and then restarts, the scheduler does not execute any scheduled tasks missed during the server down time.

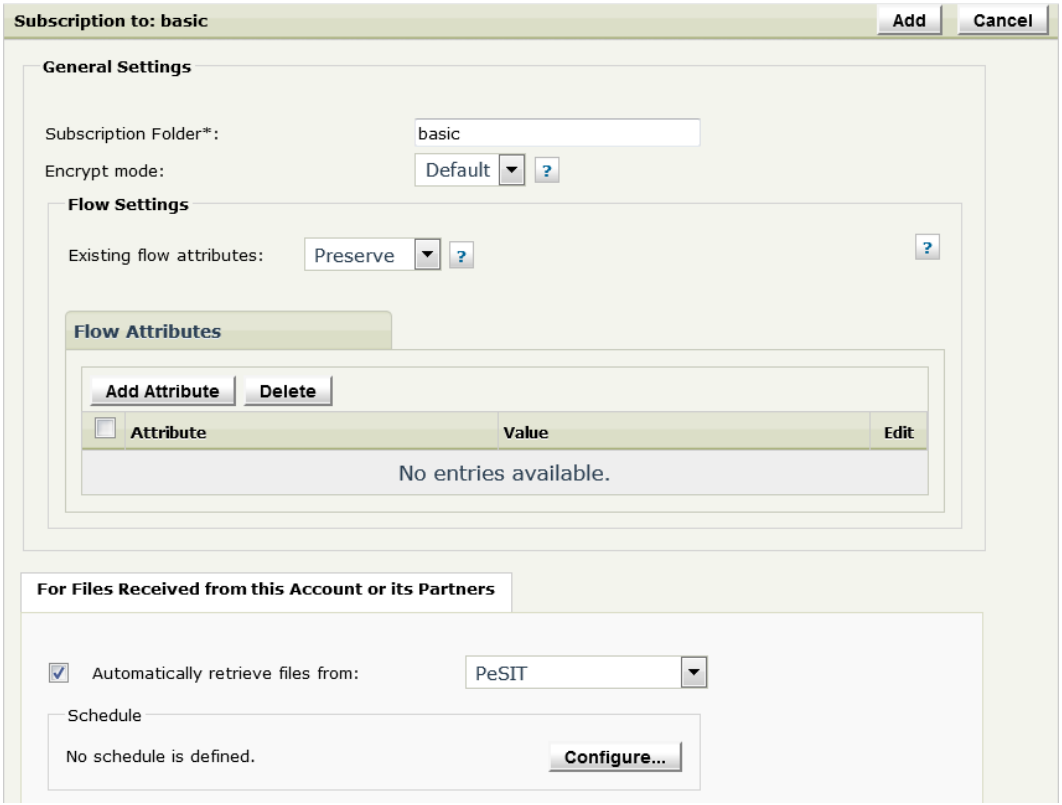
You can set up holiday dates and use them later when creating scheduled transfers or tasks.

Set up a scheduled transfer task for a subscription

When you subscribe a specific account to an application, depending on the transfer site protocol used you can schedule server-initiated downloads from a particular transfer site.

1. Click **Accounts > User Accounts** and click the account you want to subscribe.
2. Click **Subscriptions > Subscribe to <application_name>**.

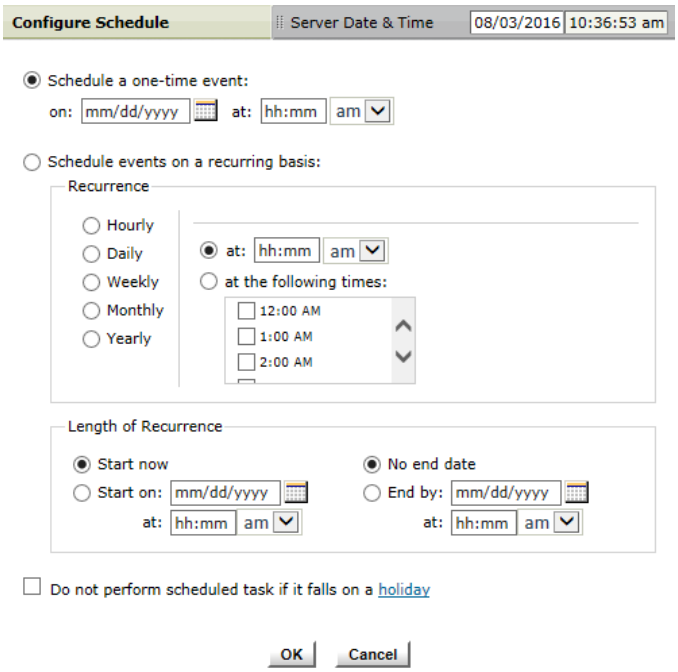
   The *Subscription to <application name>* page is displayed.



Note The **Schedule** pane is displayed only if the **Automatically retrieve files from:** check box is selected and a transfer site is selected.

3. To set the schedule conditions, click **Configure.**

   The *Configure Schedule* dialog box is displayed.



4. In the *Configure Schedule* dialog box, specify the desired conditions for the scheduled server-initiated download.

   To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

   Note If the schedule is set on a recurring basis, the **Recurrence** options dynamically change with respect to the recurrence condition: **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.
   If the server goes down for some time and restarts, the scheduler does not execute any scheduled tasks missed during the server down time.

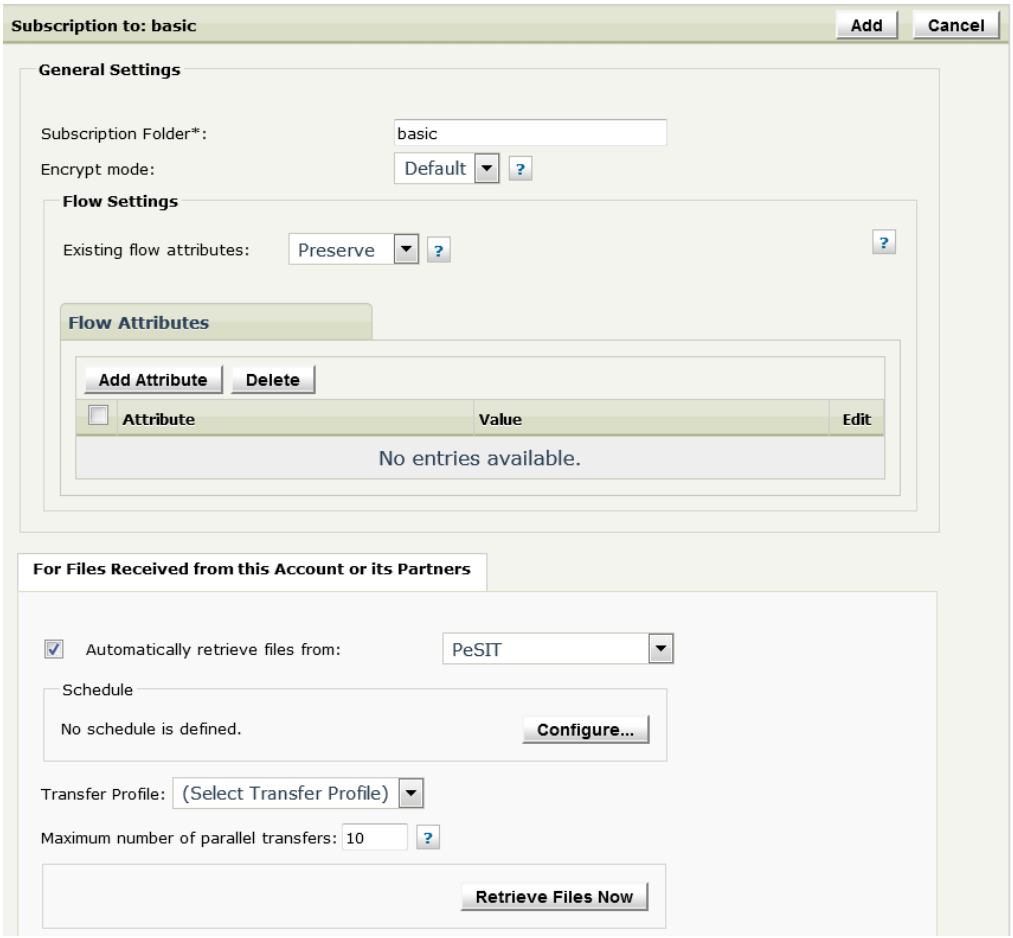
   Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

Retrieve files now

When you have already subscribed an account to an application, depending on the transfer site protocol used, you can initiate an immediate download from the selected transfer site by clicking the **Retrieve Files Now** button.

1. Click **Accounts > User Accounts** and click the account you want to subscribe.
2. Click **Subscriptions > Subscribe to <application_name>**.

The *Subscription to <application name>* page is displayed.



3. Select the **Automatically Retrieve Files From** check box and then select the respective transfer site from the drop down list. If you select a PeSIT transfer site, you can select a **Transfer Profile** from the list or leave the field empty to use the default PeSIT transfer profile. For more information, see *Transfer profiles* on page 600.

   The **Retrieve Files Now** button is displayed.

4. Click **Retrieve Files Now** to immediately trigger a one-time file pull.

   Note When the **Retrieve Files Now** is clicked, a one-time pull event is always triggered independent of the subscription being saved. If the subscription has just been created and a one-time pull event is executed, the subscription folder will be created by the runtime if it does not exist. Retrieve files now pulls can also be triggered from the REST API by account, transfer site, and destination folder.

   Note When the one-time pull event is triggered, the admin daemon will try to connect to the Transaction Manager until the maximum number of retry attempts is reached as specified by the `Streaming.Event.maxRetries` server configuration parameter. The period between each retry is specified by the

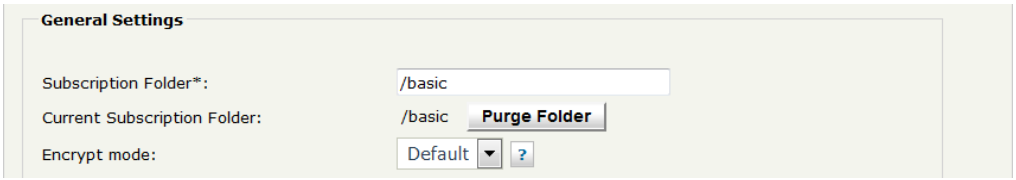
`Streaming.Event.idleTimeout` server configuration parameter. When the maximum number of retries is reached, the execution process finishes. For more information on server configuration parameters, refer to *View and change server configuration parameters* on page 315

.

Purge a subscription folder

You can delete the contents of the subscription folder specified for an account.

1. Click **Accounts > User Accounts** and click the account containing the subscription.
2. Click **Subscriptions** and click the subscription you want to edit.
3. Click **Purge Folder** to remove the contents of the current subscription folder.



4. A message asking you to confirm the deletion of the folder contents is displayed. Click **OK** to remove the folder contents or click **Cancel** to do nothing.

Note All files and directories (including other subscription directories) residing under the purged folder will be purged and deleted. The purged files and directories cannot be recovered.

Unsubscribe an account from an application

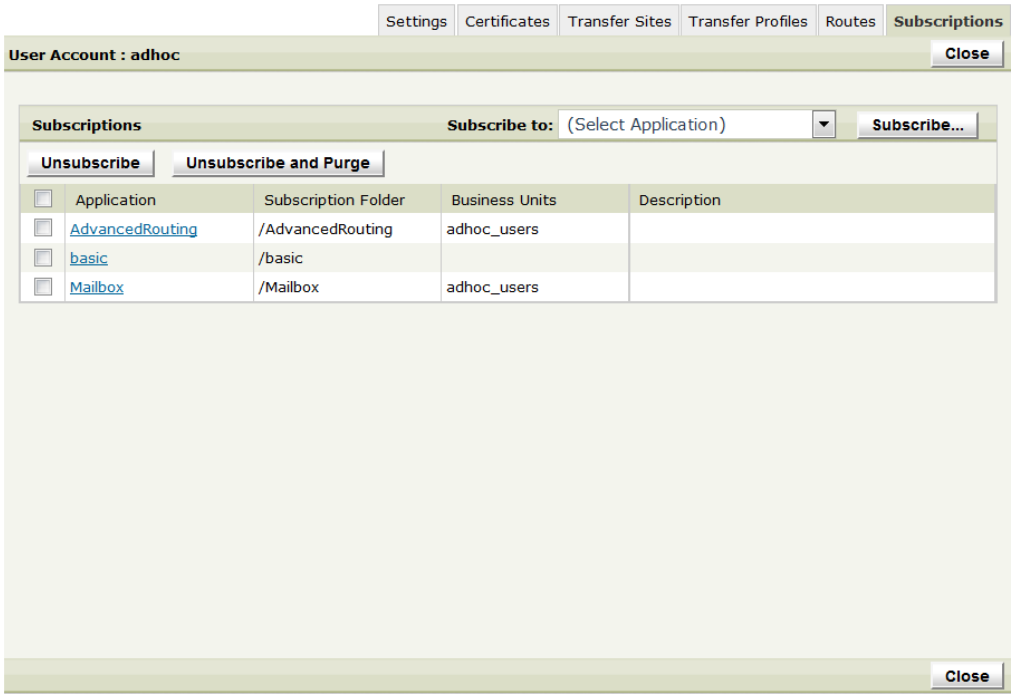
Use the following procedure to unsubscribe an account from an application.

1. Click **Accounts > User Accounts** and click the account containing the subscription.
2. Click the **Subscriptions** tab and select the check box next to the subscription you want to remove.
3. Click **Unsubscribe**. A message asking you to confirm the deletion of the subscription is displayed. Click **OK** to remove the folder contents or click **Cancel** to do nothing.

Unsubscribe an account and delete the subscription folder

You can remove a subscription and delete the associated subscription folder, including any subfolders.

1. Click **Accounts > User Accounts** and click the account containing the subscription.
2. Click the **Subscriptions** tab and select the check box next to the subscription you want to remove.



3. Click **Unsubscribe and Purge**. A message asking you to confirm the deletion of the subscription and the subscription folder is displayed. Click **OK** to remove the folder contents or click **Cancel** to do nothing.

Manage service accounts

Service accounts are internal accounts used for representing internal systems, as opposed to partner sites that are identified in SecureTransport by user accounts.

Note The Login Threshold Maintenance application does not function with service accounts.

Service accounts are defined and managed in the same way as user accounts, with the following exceptions and distinctions that you must consider when working with user accounts:

- The account settings, per-account transfer sites definition, and per-partner certificates are defined and managed identically to those of user accounts.
- Service accounts do not subscribe to applications using subscriptions. The functional connection between a service account and an application is called a *connector* and is defined at the application level. For this reason, the *Service Accounts* page does not contain a **Subscriptions** tab.
- Service accounts are internal to the system, and user accounts are external to the system.

The following topic describes how to export a single service account:

- *Export a single service account* on page 622

Export a single service account

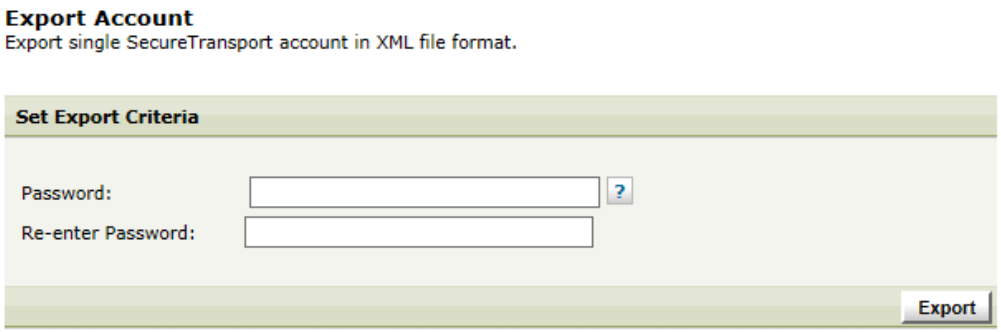
You can export a single service account to an XML file.

1. Select **Accounts > Service Accounts**.

   The *Service Accounts* page is displayed.

2. Select the account you want to export and click **Export an Account**.

   The *Export User Account* page is displayed.



3. Type a password in the **Password** field. This password is used to encrypt the sensitive information contained in the account. You use this password when you import the account to decrypt the sensitive information.
4. Retype the password in the **Re-enter Password** field.
5. Click **Export**. The account is exported to an XML file you can download to your local computer.

Duplicate an account

You can use an already created account as a template to create additional accounts with the same settings. Some information in each account must be unique to that account such as the name and the home folder. Items that must be unique have an asterisk by the field name.

Note A login certificate must be unique to a user and cannot be used on multiple accounts.

When you select **Duplicate Account** you are guided through the different pages where you can alter the user information, the transfer site and subscription details.

1. Open the user or service account you want to use as a template. On the Settings tab, click **Duplicate Account**.

   A *New Service Account* or *New User Account* page is displayed with a **Next** button at the bottom of the page.

2. Change the account name, home folder and any other user information you want to modify, such as the password. Click **Next** to continue

   If the account you are using as a template has a transfer site set up, the *Add Transfer Site* page is displayed.

3. Add a new transfer site, modify the existing settings, or click **Next** to continue without making any changes.

   If you did not add a transfer site, the *Subscriptions* page is displayed. Continue with step 5.

   If you added a transfer site, the *Transfer Profiles* page is displayed.

4. Add a new transfer profile, modify the existing settings, or click **Next** to continue without making any changes.

   The *Subscriptions* page is displayed.

   Note If you are duplicating a service account using a Standard Router application, only the transfer site and the certificates are copied to the new account.

5. Modify the subscription settings and click **Next** to continue.

   The new account is saved to the server and displayed on the *Settings* tab of the user account. The new account is disabled. Routes assigned to the duplicated account are also copied to the new account. If subscriptions are changed during duplication and they had routes assigned, the copied routes are assigned to respective changed subscriptions.

Note You will not be able to change the value in the *Route* drop-down menu while duplicating an account. You can the Route value afterwards via the *Subscriptions* tab in the newly created user account.

Control login name case sensitivity

You can avoid login errors caused by different treatment of the case sensitivity of user names for the different user types by setting server configuration parameters that control converting the case of login names and the case sensitivity of the names of a virtual users.

- **`Users.LoginNames.normalizedCaseInsensitiveUsername`**– Controls the conversion of user names entered during login. Valid values are:
  - `lower` – The user name is converted by mapping all alphabetic character to lower case. This is the default.
  - `upper` – The user name is converted by mapping all alphabetic character to upper case.
  - `none` – The user name is not converted.
- **`Users.LoginNames.virtualUserCaseSensitive`** – Controls whether the user name of a virtual user is case sensitive. Valid values are `true`, the default, or `false`.

The case sensitivity of login names is specified as follows, by user type:

- **Real users** – User names are case-sensitive on UNIX-based systems and case-insensitive on Windows systems.
- **Virtual users** – Case sensitivity depends on the parameter `Users.LoginNames.virtualUserCaseSensitive`. When the value of this parameter is `true`, login names must match configured user names exactly. When the value of this parameter is `false` and the value of `Users.LoginNames.normalizedCaseInsensitiveUsername` is `lower`, the

login name is converted and there must be no upper case letters in the configured user name. When the value of this parameter is `false` and the value of `Users.LoginNames.normalizedCaseInsensitiveUsername` is `upper`, the login name is converted and there must be no lower case letters in the configured user name. When the value of this parameter is `false` and the value of `Users.LoginNames.normalizedCaseInsensitiveUsername` is `none`, login names must match configured user names exactly.

- **LDAP users** – Case sensitivity depends on the **LDAP Common case** setting on the *LDAP Server* page. This setting specifies that an LDAP user name must be converted into upper or lower case before it is submitted for authentication. If the value of **LDAP Common case** is either `Upper` or `Lower`, the LDAP user name authentication is case insensitive. If the value of **LDAP Common case** is `None`, then case sensitivity is assumed. In other words, you must set **LDAP Common case** to either `Lower` or `Upper` to indicate that LDAP performs case insensitive match during login, even if it does not require normalization of the input string.
- **SiteMinder** – Case sensitivity depends on the `Siteminder.UserAttributesMap.commonCaseAttr` parameter on the *Server Configuration* page. Valid values are `disabled`, which causes case sensitive authentication, and `enabled`, which causes case insensitive authentication with the user name converted according to the value of `Users.LoginNames.normalizedCaseInsensitiveUsername`.

Password Reset

The SecureTransport Web Client users can reset their passwords if allowed by the administrator. If users have an email address configured in their SecureTransport account, they can reset their passwords from the *Login* page. If not, they must contact the SecureTransportadministrator to reset the password.

Note This functionality does not apply to LDAP or SSO users.

This functionality is controlled and configured by the following server configuration options, available on SecureTransport edge and backend servers in the Server configuration page in the Admin user interface:

PasswordReset.Enabled

Specifies if password reset is enabled. The default value for the setting is true.

PasswordReset.Interval

Specifies the minimum interval (in minutes) between two password reset requests for the same email. The value must be a positive integer. The default value for the setting is 60.

PasswordReset.LinkExpirationInterval

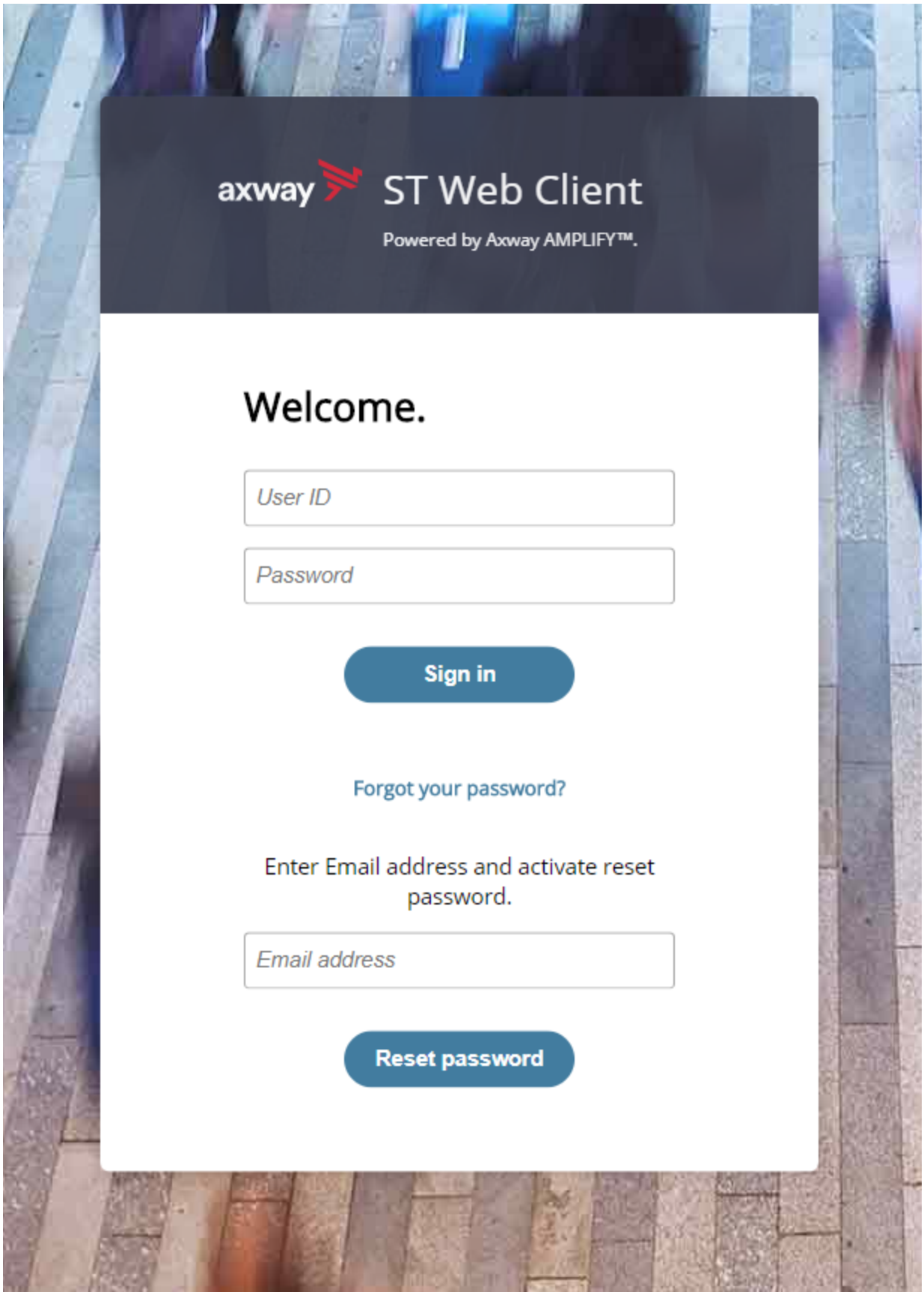
Specifies the time (in minutes) until the reset password link expires. The value must be a positive integer. The default value for the setting is 60.

PasswordReset.RequireUsername

If set to true, users will be asked for a username and an email while requesting a password reset. Otherwise, only email is required. Possible values are true/false. The default value for the setting is false.

Note Set all the password reset configuration options on all SecureTransport edge and backend servers in your setup to have identical values to avoid unexpected behaviour in a streaming setup. (Valid note for all server configuration options: PasswordReset.Enabled, PasswordReset.Interval, PasswordReset.LinkExpirationInterval, PasswordReset.RequireUsername)

To reset a password, an end user must click on the **Forgot your password?** link on the SecureTransport Web Client login page and the following window will be displayed:


axway
ST Web Client
Powered by Axway AMPLIFY™.
Welcome.
User ID
Password
Sign in
Forgot your password?
Enter Email address and activate reset password.
Email address
Reset password

A valid and unique email address must be provided.

Client password reset will not work if emails assigned to user accounts in SecureTransport are not unique.

SecureTransport sends an email with password reset instructions to the email address provided.

Once the user opens the link in the email, they are prompted to enter and confirm the new password in the displayed form.

If secret question service is enabled, the user must provide an answer to a secret question as part of the password reset process.

The user must fill in all the fields, save, and in case of success, log in with the new password.

Token

A token will be generated for authentication during the whole password reset process.

The token is encrypted with the SecureTransport Secret and bears its creation-time stamp and the account's email.

A token is expired if time, indicated by the `PasswordReset.LinkExpirationInterval` configuration option, has passed or if a password reset has occurred after the creation of the token.

The link sent via email will have the following structure: `https://<st_ip>/passwordReset?token=<encryptedString>`.

If the secret question feature is enabled in SecureTransport, the users must answer a secret question, which they have preciously set, before they can reset their password.

For more information on Secret Question Functionality, see *Configure a secret question* on page 627.

Configure a secret question

Enabling and configuring the optional secret question feature provides a secure challenge and response mechanism for resetting passwords. It also eliminates the security risks of replacing passwords with temporary ones and sending passwords via email.

If the secret question feature is enabled and their system administrator requires them to do so, end users must select and answer a secret question during their initial login. If the secret question feature is enabled and they are not required to select a secret question, end users may optionally select and answer a secret question. For additional information, refer to the *ST Web Client User Guide*.

As a system administrator, you can:

- *Enable or disable the secret question feature* on page 628
- *Set minimum length for the Secret question answer* on page 628
- *Set maximum number of answer attempts* on page 629
- *Configure a list of secret questions* on page 629
- *Require a user to select a new secret question* on page 630

If an end user forgets their password, they must:

1. Submit a password reset request through their email using the ST Web Client forgotten password mechanism.
2. Click the reset password link in the forgotten password email.
3. Answer the secret question correctly.
4. Provide and verify their new password.

For additional information on the end user password reset process, refer to the *ST Web Client User Guide*.

Enable or disable the secret question feature

By default the secret question feature is disabled. To enable the secret question feature:

1. Navigate to **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.
2. Search for the `Users.SecretQuestion.Enabled` configuration parameter.
3. Click the **Edit** ( ) icon in the *Edit* column.
4. Change the `Users.SecretQuestion.Enabled` configuration parameter to **true**.
5. Click the **Save** ( ) icon in the *Edit* column.

To disable the secret question feature:

Repeat steps 1 through 5, but set the configuration parameter to **false**.

For more information on changing server configuration parameters, refer to *View and change server configuration parameters* on page 315.

Set minimum length for the Secret question answer

To configure a minimum length for the Secret question answer:

1. Navigate to **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.
2. Search for the `Users.SecretAnswer.MinLength` configuration parameter.
3. Click the **Edit** ( ) icon in the *Edit* column.
4. Enter the desired minimum number of characters in the *Value* field. The default value is **0**.
5. Click the **Save** ( ) icon in the *Edit* column.

Note The `Users.SecretAnswer.MinLength` configuration option is available only on SecureTransport Server.

Set maximum number of answer attempts

To configure the maximum number of answer attempts:

1. Navigate to **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.
2. Search for the `Users.SecretQuestion.MaxAttempts` configuration parameter.
3. Click the **Edit** ( ) icon in the *Edit* column.
4. Enter the desired number of answer attempts in the *Value* field. The default value is **0**.
5. Click the **Save** ( ) icon in the *Edit* column.

For more information on changing server configuration parameters, refer to *View and change server configuration parameters* on page 315.

Configure a list of secret questions

To configure a list of secret questions:

1. Navigate to **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.
2. Search for the `Users.SecretQuestions` configuration parameter.
3. Click the **Edit** ( ) icon in the *Edit* column.
4. Update the `Users.SecretQuestions` list as desired. The secret questions must be separated by a hard return. The default secret questions are:
   - **What make was your first car or bike?**
   - **What is your father's middle name?**
   - **What is your mother's maiden name?**
   - **What is your school's mascot?**
   - **What is the name of your favorite fictional character?**
   - **What is your favorite teacher's name?**
   - **Where did you go on your first date?**
   - **What is your dog's name?**
   - **What is your dream occupation?**
5. Click the **Save** ( ) icon in the *Edit* column.

For more information on changing server configuration parameters, refer to *View and change server configuration parameters* on page 315.

Require a user to select a new secret question

To require a user to select and answer a new secret question, edit their user account and select **Require user to set new secret question on next login**. On the next login, the user must select and answer a new secret question before they can access the user interface. For additional information on editing user accounts, refer to *Edit user account settings* on page 468.

Advanced account administration 10

In addition to creating user and service accounts, you can control account access through additional tools such as account export and import, account templates, delegated administration, business units, and administrative roles.

The following topics describe advanced account administration:

- *Account export and import* on page 631
- *Manage administrator accounts* on page 644
- *Delegated administration* on page 651
- *Administrative roles* on page 655
- *Account templates* on page 661
- *Site templates* on page 681
- *System users* on page 687
- *Business units* on page 692
- *Display active users* on page 700
- *Client-initiated and server-initiated transfers* on page 701

Account export and import

SecureTransport 5.4 supports import from the following releases only, patched to the latest patch or service pack – 5.3.6, 5.3.5, 5.3.3, 5.3.1, 5.3.0, and 5.2.1. Accounts can be imported from export files produced by the same or another SecureTransport deployment.

SecureTransport provides a way to export or import all account information, such as account templates, user accounts, service accounts, business units, administrators, and site templates. Exported account template, user account, and service account information includes: user settings, transfer sites, transfer profiles, certificates, certificate requests, subscriptions, applications, business units, route packages, route package templates and their adjacent routes and steps, and those certificates that apply to all of the system.

You can use the command line interface or the Administration Tool to export and import the account information. Accounts can be exported to use as a template, to create a backup, to move from a test to a production environment, or to move from one platform to another.

Note Only a master administrator or a delegated administrator with the appropriate privileges can use the Administration Tool to import or export accounts. For more information, see *Delegated administration* on page 651. Any administrator who can access the server can use the command line to import or export accounts.

Information is exported to and imported from an XML file. This file can be edited and re-imported. Sensitive information such as private keys and passwords are encrypted during the export process, and you are asked to create a password to protect the sensitive information. When you import the account information, you are asked for the password to allow the sensitive information to be decrypted.

The following topics describe the account XML schema and how to edit the account XML schema. They also provide how-to instructions for exporting and importing accounts.

- *Account XML schema* on page 632
- *Edit an XML file* on page 632
- *Export and import accounts* on page 636

Account XML schema

SecureTransport provides an XML schema for importing and exporting account information. You can use this schema when creating an XML file that can be read by SecureTransport. You can also export an account and use the exported XML file as a template. The schema is located in the `<FILEDRIVEHOME>/conf/xmlExport.xsd` file.

Edit an XML file

Read the following information before editing an XML file:

- To change the password for the account, delete the `encryptedPassphrase` element and replace it with a `passphrase` element. Type the new account password using plain text.

  ```
  <passphrase>user3</passphrase>
  ```

  The password is encrypted during the import process.
- You can add or modify the information for a transfer site in its `site` element. Each setting that applies to all transfer sites has an element named for the setting. The information specific to the transfer protocol is represented by the `customProperties` element using the format `<entry key="`*`fieldname`*`">`*`value`*`</entry>` where *`fieldname`* is the name of the field in the transfer site, such as `port`, and *`value`* is the information entered for that field, such as `801`.
- You can add or modify the information for a transfer profile in its `Idf` element:

Field	Element	Valid values
Transfer Profile Name	name	Any valid string
Files To Send	sendMapping	Any valid string
Receive File As	receiveMapping	Any valid string
Acknowledge transfer	sendingAcknowledgmentEnabled	`false` `true`

File Label	fileLabelOption	`DONT_SEND`
		`SEND_FILENAME`
		`SEND_FILENAME_AND_PATH`

All files	multiSelect	`false` `true`

Transfer Mode	transferMode	`ASCII`
		`BINARY`
		`EBCDIC`

Record Format	recordFormat	`0` for Fixed `128` for Variable
Record Length	recordLength	Any valid positive integer

- To indicate that a transfer profile is the default, include the `<default>true</default>` element in the `Idf` element. Only one transfer profile can include this element.
- If you add or modify a subscription, make sure that the application is set up on the server where you are importing the XML file or that you are importing the appropriate application information in the same XML file.
- To modify an application name in a subscription, edit the following element:

  `<applicationReference>MySub</applicationReference>`
- You can change the account information of an existing account, or you can add new accounts to the file.
- When editing an account, you can modify the account information and use the existing `id` attribute in the `Account` element.
- When adding an account, include the following elements in a new `completeAccount` element. Do not include the `id` attribute.

```
<account authByEmail="false" unlicensed="false"
    isUnlicensedAllowedToReply="true" disabled="false" >
    <name>partner1</name>
    <type>user</type>
    <usrid>1001</usrid>
    <grpid>1003</grpid>
    <homeFolder>/home/users/partner1</homeFolder>
    <homeFolderAccessLevel>PUBLIC</homeFolderAccessLevel>
    <email>partner1@example.com</email>
    <phone>800-555-0199</phone>
    <htmlTemplateFolderPath>/html/skin/ric
</htmlTemplateFolderPath>
    <notes>Include ad hoc file transfer functions.</notes>
    <deliveryMethod>CUSTOM</deliveryMethod>
    <enrollmentTypes>CHALLENGED_LINK</enrollmentTypes>
    <implicitEnrollmentType>EXISTING_ACCOUNT</implicitEnrollmentType>
    <customAttributes>
        <customProperties>
            <entry key="encryptMode">unspecified</entry>
            <entry key="routingMode">reject</entry>
            <entry key="transferType">E</entry>
            <entry key="transfersWebServiceAllowed">false</entry>
        </customProperties>
        <localCertificates>
        </localCertificates>
        <partnerCertificates>
        </partnerCertificates>
        <userCertificates>
        </userCertificates>
    </customAttributes>
</account>
```

The elements correspond to the fields in the account *Settings* pane:

Field	Element	Valid values
Attributes		
Allow this account to login by email	authByEmail	`false` `true`

(none)	unlicensed	Is this an unlicensed user account?
		`false`
		`true`

Field	Element	Valid values

Allow reply to packages	isUnlicensedAllowedToReply	`false`
		`true`
		Always `true` of licensed accounts.

(none)	disabled	Is this user account disabled?
		`false`
		`true`

Elements		

Delivery Method	deliveryMethod	`DISABLED`
		`DEFAULT`
		`ANONYMOUS`
		`ACCOUNT_WITHOUT_ENROLLEMENT`
		`ACCOUNT_WITH_ENROLLMENT`
		`CUSTOM`

Enrollment Types	enrollmentTypes	If deliveryMethod is CUSTOM:
		`ANONYMOUS_LINK`
		`CHALLENGE_LINK`
		`EXISTING_ACCOUNT`
		`ENROLL_UNLICENSED`
		`ENROLL_LICENSED`

Implicit Enrollment Type	implicitEnrollmentType	One of the valid enrollment types. Do not include when the deliveryMethod is `DEFAULT` or the field value is None.

Home Folder Access	homeFolderAccessLevel	`PRIVATE`
		`PUBLIC`
		`BUSINESSUNIT`

Custom properties		
Encrypt Mode	encryptMode	`unspecified` `enabled`

Routing Mode	routingMode	`accept`
		`reject`
		`ignore`

Field	Element	Valid values

Account Type	transferType	`E`
		`I`
		`N`

Transfer Mode	transfersWebServiceAllowed	`false` `true`

Export and import accounts

Use the *Import or Export Accounts* page and command-line utilities to export and import SecureTransport accounts.

The following topics provide how-to instructions for exporting and importing accounts:

- *Export accounts using the Administration Tool* on page 636
- *Export accounts from the command line* on page 637
- *Import accounts using the Administration Tool* on page 642
- *Import accounts from the command line* on page 643

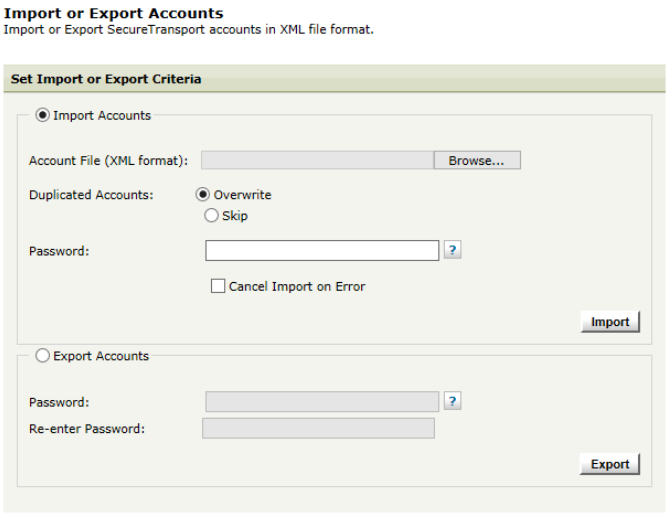
Export accounts using the Administration Tool

You can export accounts using the SecureTransport Administration Tool. When you use the *Import or Export Accounts* page, all the account information on the server is exported. This includes user accounts, service accounts, account templates, certificates, application instances, business units, administrators, administrative roles, site templates, route packages, and route package templates. To export a single account from the Administration Tool, see *Export a single user account* on page 470. To control which account information is exported, see *Export accounts from the command line* on page 637.

The exported file is written to the `<FILEDRIVEHOME>/var/tmp/export_accounts.xml` file. This file is overwritten every time you export account information.

1. Select **Accounts > Import/Export**.

   The *Import or Export Accounts* page is displayed.



2. Select **Export Accounts**.
3. Enter a password in the **Password** field, then type the same password in the **Re-enter Password** field. The password must contain at least eight characters.
4. Click **Export**. SecureTransport creates an export file in `<FILEDRIVEHOME>/var/tmp/export_accounts.xml` and displays a message indicating that the export was successful.

5. To save the exported account information to a new location, click **Download Exported Accounts**. A dialog box displays prompting you to **Save** or **Open** the XML file.

   Note You can download the exported file multiple times to the same or a new location. The Export Complete message with the **Download Exported Accounts** button remains, enabling you to download again, until you change tabs, select an option in the navigation bar at the left, or click **Back** twice.

6. (Optional) To refresh the *Import or Export Accounts* page, select **Accounts > Import/Export** or click **Back** twice.

Export accounts from the command line

Using the command line, you can export a single account or all the accounts. Exported account information includes: user accounts, administrators, administrative roles, transfer sites, site templates, transfer profiles, partner certificates, certificate requests, applications, subscriptions, and routes.

Run the `xml_export` utility in the `<FILEDRIVEHOME>/bin` directory from the command line to export account information into an XML file.

The form of the command is:

`./xml_export [options] [fileNameAndPath]` on a UNIX-based system

or

`xml_export [options] [fileNameAndPath]` on a Windows system

where *options* can be:

- `-help` means display the usage information and exit.
- `-acc=`*accountName* where *accountName* is the name of the account template, user or service account to export.
- `-adm=`*adminName* where *adminName* is the name of the administrator account to export.
- `-role=`*adminRoleName* where *adminRoleName* is the name of administrative role to export.
- `-bu=`*buName* where *buName* is the name of the business unit to export.
- `-st=`*stName* where *stName* is the name of the site template to export.
- `-crt=`*certName* where *certName* is the name of the certificate to export.
- `-app=`*appname* where *appName* is the name of the application to export.
- `-pwd=`*passwordFile* where *passwordFile* is a file containing the password used to encrypt or decrypt sensitive information stored in the XML file. The text in this file is not encrypted. You can create the file using any text editor. If you do not use this option, the utility prompts you to type the password in the command window.
- `-route=`*routeName* where routeName is the name of the route package template or global route package or orphan simple route to export.

and *fileNameAndPath* is the name and location of the XML file to write containing the exported data, such as `/user/XMLExport/ST_Acct_Export.XML`. If *fileNameAndPath* is not specified, `xml_export` writes the XML output to the standard output.

To export specific information, use only the option for the information you want. To export all items of one type, set the option to `*`, such as `-acc="*"`. To export all accounts, administrator accounts (including delegated administrators), administrative roles, business units, site templates, applications, and global certificates, do not use any of the `-acc`, `-adm`, `-role`, `-bu`, `-st`, `-crt`, or `-app` options.

Exporting a single account using the command line

When you export a single account the following items are not exported:

- Applications
- Business units
- Global certificates
- Site templates
- Route package templates

It is best to use the single account export to create an XML template for account import only.

1. On a UNIX-based system, change to the `<FILEDRIVEHOME>/bin` directory.
2. Type the following command:

   `./xml_export -acc=accountName fileNameAndPath` on a UNIX-based system

   or

   `xml_export -acc=accountName fileNameAndPath` on a Windows system

   where *`accountName`* is the name of the account template, user account, or service account you want to export and *`fileNameAndPath`* is the XML file name and location where you want to store the exported data.
3. When prompted, type a password for the exported information. This password is requested when you import the account from the file.
4. Confirm the password by typing it again when prompted.

   The XML file is created in the specified location.

Export information using a specific option

You can use the command line to export only the information for a specific option such as global certificates or application instances.

Export global certificates

1. On a UNIX-based system, change to the `<FILEDRIVEHOME>/bin` directory.
2. Type the following command:

   `./xml_export -crt=certName FileNameAndPath` on a UNIX-based system

   or

   `xml_export -crt=certName FileNameAndPath` on a Windows system

   where *`certName`* is the name of the global certificate you want to export or * to export all global certificates and *`FileNameAndPath`* is the XML file name and location where you want to store the exported data. Multiple certificates may use the same name.
3. When prompted, type a password for the exported information. This password is requested when you import the global certificates from the file.
4. Confirm the password by typing it again when prompted.

   The XML file is created in the specified location.

Export an application

1. On a UNIX-based system, change to the `<FILEDRIVEHOME>/bin` directory.
2. Type the following command:

   `./xml_export -app=appName FileNameAndPath` on a UNIX-based system

   or

`xml_export -app=appName FileNameAndPath` on a Windows system

where `appName` is the name of the application you want to export or * to export all the application instances and `FileNameAndPath` is the XML file name and location where you want to store the exported data.

3. When prompted, type a password for the exported information. This password is requested when you import the application from the file.
4. Confirm the password by typing it again when prompted.

   The XML file is created in the specified location.

Export a business unit

1. On a UNIX-based system, change to the `<FILEDRIVEHOME>/bin` directory.
2. Type the following command:

   `./xml_export -bu=buName FileNameAndPath` on a UNIX-based system

   or

   `xml_export -bu=buName FileNameAndPath` on a Windows system

   where `buName` is name of the business unit you want to export or * to export all the business units and `FileNameAndPath` is the XML file name and location where you want to store the exported data.
3. When prompted, type a password for the exported information. This password is requested when you import the business unit from the file.
4. Confirm the password by typing it again when prompted.

   The XML file is created in the specified location.

Export a site template

1. On a UNIX-based system, change to the `<FILEDRIVEHOME>/bin` directory.
2. Type the following command:

   `./xml_export -st=stName FileNameAndPath` on a UNIX-based system

   or

   `xml_export -st=stName FileNameAndPath` on a Windows system

   where `stName` is name of the site template you want to export or * to export all the site templates and `FileNameAndPath` is the XML file name and location where you want to store the exported data.
3. When prompted, type a password for the exported information. This password is requested when you import the site template from the file.
4. Confirm the password by typing it again when prompted.

   The XML file is created in the specified location.

Export a route package template, global route package, or orphan simple route

1. On a UNIX-based system, change to the `<FILEDRIVEHOME>/bin` directory.
2. Type the following command:

   `./xml_export -route=`*`routeName FileNameAndPath`* on a UNIX-based system

   or

   `xml_export -route=`*`routeName FileNameAndPath`* on a Windows system

   where `routeName` is the name of the route package template, global route package or orphan simple route you want to export or * to export all the route package instances and `FileNameAndPath` is the XML file name and location where you want to store the exported data.
3. When prompted, type a password for the exported information. This password is requested when you import the route from the file.
4. Confirm the password by typing it again when prompted.

   The XML file is created in the specified location.

Export all the information using the command line

You can generate an XML file that contains all the account, global and account certificate, application, business unit, delegated administrator, and site template information to use as a backup or to move information from a test environment to a production environment.

1. On a UNIX-based system, change to the `<FILEDRIVEHOME>/bin` directory.
2. Type the following command:

   `./xml_export `*`FileNameAndPath`* on a UNIX-based system

   or

   `xml_export `*`FileNameAndPath`* on a Windows system

   where *`FileNameAndPath`* is the XML file name and location where you want to store the exported data.
3. When prompted, type a password for the exported information. This password is requested when you import the information from the file.
4. Confirm the password by typing it again when prompted.

   The XML file is created in the specified location.

Note To save and restore delegated administrator accounts correctly, you must export and import both server configuration and accounts.

Import accounts using the Administration Tool

SecureTransport 5.4supports import from the following releases only, patched to the latest patch or service pack – 5.3.6, 5.3.5, 5.3.3, 5.3.1, 5.3.0, and 5.2.1. Accounts can be imported from export files produced by the same or another SecureTransport deployment.

You can import account information using the SecureTransport Administration Tool. The account information is imported as an XML file containing user settings, transfer sites, transfer profiles, account certificates, certificate requests, subscriptions, and route packages. You can also import business units, administrators, administrative roles, site template settings, applications, route package templates, and certificates. You must know the password assigned to the file when it was exported by SecureTransport. If you are creating an XML file from scratch, you must assign a password to the file.

1. Select **Accounts > Import/Export**.

   The *Import or Export Accounts* page is displayed.

2. Select **Import Accounts**.
3. Type the name of the XML file you are importing in the **File Account** field or click **Browse** and locate the file in your system.

   The system automatically validates the XML schema. If the schema is invalid, a warning message is displayed. For more information, see *Account XML schema* on page 632.

   If the XML document is valid, the import process starts.

4. In **Duplicated Accounts**, select **Overwrite** to overwrite the previous account settings or **Skip** to skip such accounts.

   If an account_export.xml, containing route templates instantiated by accounts with route packages, is imported with **Skip** option selected, to target SecureTransport Server, already configured with route templates, accounts and route packages, the corresponding imported route templates, accounts and route packages are rejected during the import if there are already objects with the same names in the target SecureTransport Server.

5. Type the password created for the exported account file in the **Password** field.
6. To stop the import process when an error occurs, select **Cancel Import on Error**.
7. Click **Import**.

   The import process begins. When the import is finished, a status message is displayed.

Account imports that fail upon import only report the first error. Once that error is fixed, it is possible another error might still be present that causes the import to fail. View the file `<FILEDRIVEHOME>/var/tmp/rejected_import_records.xml` to find the import error.

Import accounts from the command line

SecureTransport 5.4 supports import from the following releases only, patched to the latest patch or service pack – 5.3.6, 5.3.5, 5.3.3, 5.3.1, 5.3.0, and 5.2.1. Accounts can be imported from export files produced by the same or another SecureTransport deployment.

You can import accounts to move from one platform to another or to create a large number of accounts without creating them one at a time. Using an exported account as a template, you can create a list of new accounts that can be imported into SecureTransport.

Run the `xml_import` utility in the `<FILEDRIVEHOME>/bin` directory from the command line to import account information from an XML file. The utility has the following options and parameters:

The form of the command is:

`./xml_import [`*`options`*`]` *`FileNameAndPath`* on a UNIX-based system

or

`xml_import [`*`options`*`]` *`FileNameAndPath`* on a Windows system

where *`options`* can be:

- `-dup=[overwrite|skip]` where `overwrite` overwrites duplicate account entries and `skip` does not import duplicate accounts. If no option is specified, the default setting is `overwrite`.
- `-err=[continue|exit]` where `continue` continues importing the accounts when an error occurs and `exit` stops the utility when an error occurs. If no option is specified, the default setting is `exit`. Errors are written to the `admin.log` file
- `-pwd=`*`passwordFile`* where *`passwordFile`* is a file containing the password used to encrypt or decrypt sensitive information stored in the XML file. You can use this file instead of typing the password from the command line. The text in this file is not encrypted. You can create the file using any text editor.
- `-sync=[y|n]` where `y` synchronizes the imported accounts with all Servers in a Standard Cluster (SC) or Enterprise Cluster (EC) after the import and `n` only imports the accounts to the Server where the command is run. If no option is specified, the default setting is `y`.

  Use `-sync=n` to reduce the time to import large numbers of accounts or accounts with many transfer sites or other features. Then restart the Transaction Manager and the Administration Tool server on the other Servers in the Standard Cluster or Enterprise Cluster to synchronize.

  Note Synchronization requires that the Administration Tool server is running on all Servers in the cluster.

and *`FileNameAndPath`* is the location and file name of XML file containing the accounts you want to import, such as `/user/XMLExport/ST_Acct_Export.XML`.

Import accounts from an XML file

1. Make sure the Administration Tool server is running on all Servers in the Standard Cluster or Enterprise Cluster.
2. On a UNIX-based system, change to the `<FILEDRIVEHOME>/bin` directory.
3. Type the `xml_import` command.
4. Type the password for the XML file at the prompt.

   The accounts are imported into SecureTransport.

Note To restore administrator accounts exported from SecureTransport 5.1.0 SP3 or SecureTransport 5.2.1 SP3, SP4, or SP5 correctly, you must import server configuration before you import the accounts.

Set the location of the overwrite file

If you set the `dup` option to `overwrite`, and a specific account, certificate, template, or application cannot be imported, the information is written to the following location:

`<FILEDRIVEHOME>/var/tmp/rejected_import_records.xml`

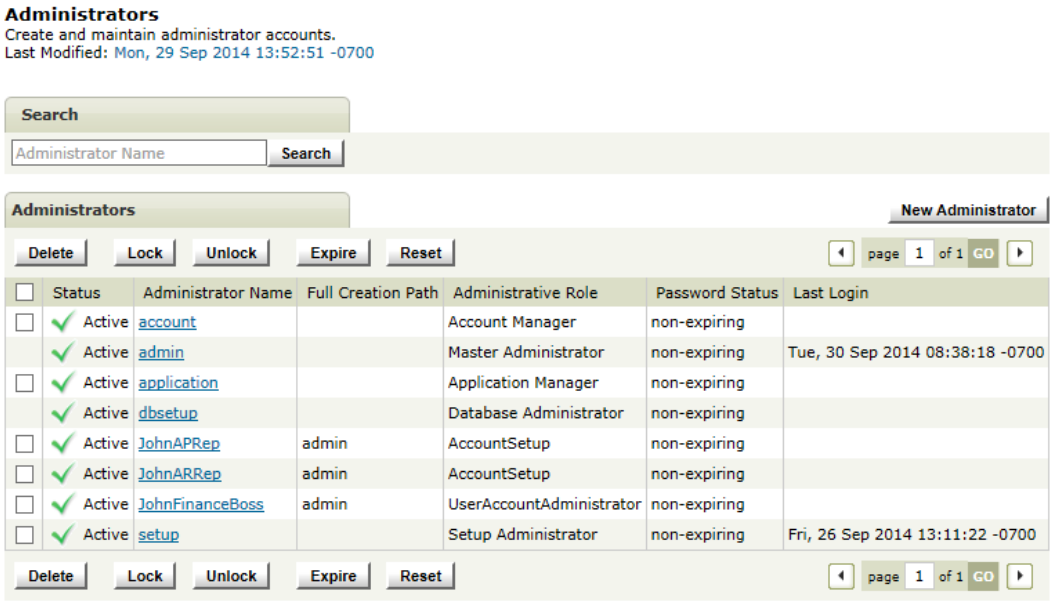
To store the overwrite information in a different directory relative to `<FILEDRIVEHOME>`, set the value of the `Directories.Directory.exportHome.path` parameter on the *Server Configuration* page to the relative path name for the directory. The default value is `/var/tmp`.

To store the overwrite information in a different directory not relative to `<FILEDRIVEHOME>`, clear the value of `Directories.Directory.exportHome.relative` and set the value of `Directories.Directory.exportHome.path` to the absolute path name for the directory.

Manage administrator accounts

Use the *Administrators* page to manage administrative accounts. You can create, edit, delete, and lock administrator accounts. You can also expire and reset administrator account passwords. If a custom hierarchical administration exists in an organization, you can specify different privileges for each administrator. Use the *Change Password* page to change your password even if you cannot edit accounts.

To display the *Administrators* page, select **Accounts > Administrators** in the Administration Tool. To show only administrators whose names match a character string, type the string in the field in the *Search* pane and click **Search**.



For each administrator, you can view the information described in the following table.

Field	Description
Status	Reports the current status of the administrator account: • **Active** – The account is neither locked nor expired. • **Expired** – Manual action or the expiration interval set the account as Expired. • **Locked** – Manual action or login failures set this account as Locked. The account might also be Expired.
Administrator Name	The name given to the Administrator account
Full Creation Path	Applies only to delegated administrators. Shows the path for the parent administrator. For example, the path might look like: `admin/deladmin1/subdeladmin1`.

Field	Description
Administrative Role	Role assigned to the administrator account. The predefined administrative roles are: • **Master Administrator** – Access to all menus, tabs and pages of the Administration Tool. Cannot be modified. • **Database Administrator** – Access to the *Database Setting* page only. Only the `dbsetup` administrator can have this role. Cannot be modified. • **Setup Administrator** – Access through the custom **Configure** menu to pages required to perform the post-installation tasks and setup operations described in the *SecureTransport Getting Started Guide*. Cannot be modified. • **Account Manager** – Access restricted to the *User Accounts*, *Unlicensed Users Accounts, Service Accounts*, *Templates*, and *Business Units* pages on the **Accounts** menu and all pages on the **Access** menu. • **Application Manager** – Access restricted to the pages on the **Service Accounts** and **Applications** menus. • **Delegated Administrator** – Configurable access to menus and data based on the function the administrator has within an organization.
Password Status	The password status is reported differently depending on whether or not password expiration is enabled on the *Admin Settings* page. If password expiration if enabled, this field shows one of the following: • the expiration date • the date the password expires • a reminder to change the password at the next login • non-expiring If password expiration if not enabled, this field shows one of the following: • the date the password was changed • a reminder to change the password at the next login • no change recorded Depending on your policy for these accounts, you can use the Reset function to mark the last password change time as the current time, or use the Expire function to force a password change at next login.
Last Login	Reports the last login attempt recorded. This is either the date and time of the last successful login, or if the last recorded activity was a failed login, the number of failures and the date and time.

The following topics provide how-to instructions for managing administrator accounts:

- *Add an administrator account* on page 647
- *Edit an administrator account* on page 648

- *Delete an administrator account* on page 649
- *Lock an administrator account* on page 650
- *Unlock an administrator account* on page 650
- *Expire an administrator account password* on page 650
- *Reset an expired administrator account password* on page 651
- *Change administrator password* on page 651

Add an administrator account

If you have access to the *Administrators* page, you can define multiple administrators with varied access privileges for SecureTransport administration. Master administrators and delegated administrators with the **Manage Administrators** privilege have access to the *Administrators* page by default.

1. Select **Accounts > Administrators**.

   The *Administrators* page is displayed.

2. Click **New Administrator**.

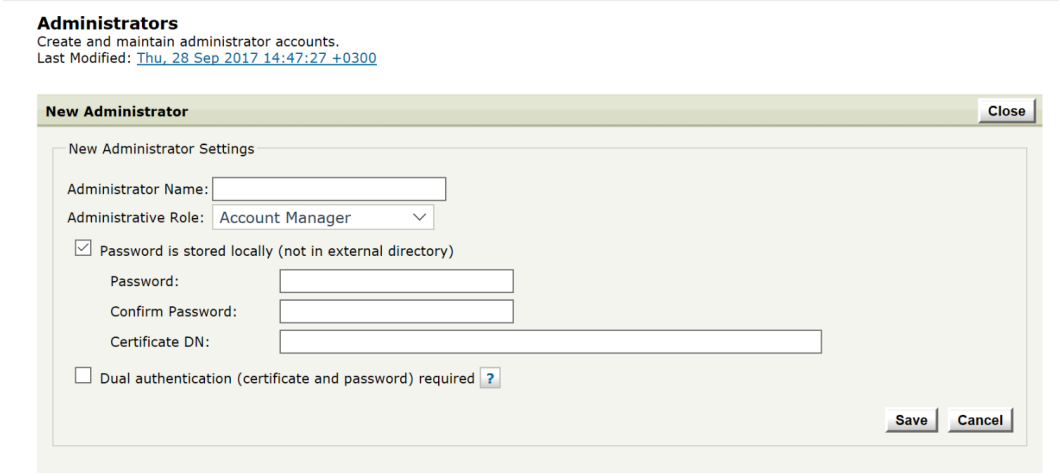
   The *New Administrator* page is displayed.

3. In the **Administrator Name** field, enter a name for the administrator. Administrator names are case-sensitive.
4. Select the **Administrative Role** for the new administrator.
5. Select **Password is stored locally (not in external directory)** to store the administrator password locally and not in an external directory. If this option is selected, completing the **Password** field is mandatory. If this option is not selected, the only mandatory parameters for creating an administrator are **Administrator Name** and **Administrative Role**.

   Note Uncheck this option in order for the current administrator to be able to log in, using an external authentication agent (SSO or authentication plug-in).

6. In the **Password** field, enter a password for the administrator. Passwords are case-sensitive.
7. In the **Confirm Password** field, type the password again to confirm it.
8. If you have enabled administrators to login using a client certificate on the *Admin Settings* page, the **Certificate DN** field and **Dual authentication** check box are displayed. If client certificates are required or to specify one for this administrator, complete the fields.
   a. In the **Certificate DN** field, type the Subject field value from the certificate.
   b. To require the administrator to use both a certificate and password, select **Dual authentication**. If you select this option, you must type the Distinguished Name in the **Certificate DN** field.
   c. In case the password stored locally is not checked, the Dual authentication will still be visible, allowing current administrator to be logged using dual-factor authentication by an external

d. In case the password stored locally is not checked, the Dual authentication will still be visible, allowing current administrator to be logged using dual-factor authentication by an external authentication agent (in this case the plug-in).
Note: This option will have no effort for SSO-authenticated administrators.



9. Click **Save** to add the administrator account.

   The new administrator is displayed in the list of administrators on the *Administrators* page.

Edit an administrator account

Note If you are using a Firefox browser, disable the auto complete function prior to editing an administrator account settings.

If you have access to the *Administrators* page, you can edit an Administrator account. Master administrators and delegated administrators with the **Manage Administrators** privilege are granted access to the *Administrators* page by default.

Account password stored locally

If the administrator account was created with **Password is stored locally (not in external directory)** selected and the account password is stored locally, use the following instructions to edit administrator account settings.

1. Select **Accounts > Administrators**.

   The *Administrators* page is displayed.

2. Click the administrator entry you want to edit.

   The *Edit Administrator* page is displayed.

3. Make any desired changes in the *Administrator Account Status* pane. You can lock the account, expire the administrator account password, or reset an expired password.
4. Make any desired changes to the fields in the *Edit Administrator Settings* pane.

   You can change the **Administrative Role** and the administrator password. If you have enabled administrators to login using a client certificate on the *Login Settings* page, you can change the **Certificate DN** field and **Dual authentication** check box. If the **Administrative Role** is set to Delegated Administrator, you can also modify the **Delegated Administrator Settings**.
5. Click **Save** to apply the changes.

Account password stored externally

If the administrator account was created with **Password is stored locally (not in external directory)** not selected and the account password is stored externally, use the following instructions to edit administrator account settings. This option will allow the administrator to be authenticated by an external authentication agent (Identity provider).

1. Select **Accounts > Administrators**

   The *Administrators* page is displayed.
2. Click the administrator entry you want to edit.

   The *Edit Administrator* page is displayed.
3. Make any desired changes in the *Administrator Account Status* pane. You can only lock and unlock the account.
4. Make any desired changes to the fields in the *Edit Administrator Settings* pane. You can only change the **Administrative Role**
   Note: If you have enabled administrators to log in using a client certificate on the **Login Settings** page, you can change the **Dual authentication** check box.
5. Click **Save** to apply the changes.

Delete an administrator account

If you have access to the *Administrators* page, you can remove an existing administrator account. Master administrators and delegated administrators with the **Manage Administrators** privilege are granted access to the *Administrators* page by default.

1. Select **Accounts > Administrators**.

   The *Administrators* page is displayed.
2. Select the check box for one or more administrators you want to delete.
3. Click **Delete**.

Lock an administrator account

You can lock an administrator account to remove or modify it or if you are not ready to make it active. Unlock the account when you want the administrator to have access to the server. You cannot lock the account of an administrator who is currently logged in.

1. Select **Accounts > Administrators**.

   The *Administrators* page is displayed.
2. Select the check box for one or more administrators you want to lock.
3. Click **Lock**.

   The **Status** column shows that the accounts are locked.

Unlock an administrator account

Use the following procedure to unlock an administrator account.

1. Select **Accounts > Administrators**.

   The *Administrators* page is displayed.
2. Select the check box for one or more administrators you want to unlock.
3. Click **Unlock**.

Expire an administrator account password

You can force the immediate expiration of the password for an administrator account. The administrator must set a new password upon the next log in. You cannot expire the password of an administrator who is currently logged in.

If you need to change the password for the administrate account that is currently logged in, edit the account or select **Change Password** from the **Accounts** menu.

1. Select **Accounts > Administrators**.

   The *Administrators* page is displayed.
2. Select the check box for one or more administrators for which you want to expire the passwords.
3. Click **Expire**, then click **Save** to apply the change.

Note When the password for the edited administrator is stored externally you can not expire their password.

Reset an expired administrator account password

You can cancel the password expiration and restore the current administrator account password. You can use Reset to cancel an expired administrator password until the administrator changes the password.

1. Select **Accounts > Administrators**.

   The *Administrators* page is displayed.

2. Select the check box for one or more administrators for which you want to reset the passwords.
3. Click **Reset**, then click **Save** to apply the change.

Note When the password for the edited administrator is stored externally, you cannot expire his password and therefore you cannot reset it.

Change administrator password

The *Change Password* page will not be displayed when authentication for the administrator is completed by an external agent.

Note If you are using a Firefox browser, disable the auto complete function prior to editing an administrator account password.

You can change your administrator password even if you cannot edit your administrator account by using the *Change Password* page. Use this page to view the last date and time the password was changed and to enter a new password.

1. Select **Accounts > Change Password**.

   The *Change Password* page is displayed.

2. Type the new password you want to use in the **Password** field.
3. Retype the new password in the **Confirm Password** field.
4. Click **Save**.

Delegated administration

SecureTransport provides a customizable administrator type called a *delegated administrator*. The delegated administrator works with specific user groups referred to as business units. User accounts, service accounts, account templates, unlicensed user accounts, and applications are divided into business unit groups and each user or service account, unlicensed user, and account template is assigned to only one business unit.

Each delegated administrator is assigned one or more business units that determine the user accounts, service accounts, unlicensed user accounts, account templates, and applications managed by that administrator. Tracking information is also displayed based on the business unit assigned.

When you log in to the SecureTransport Administration Tool as a delegated administrator, you see a subset of the menus and pages normally available. You are allowed to view the file transfer tracking information, accounts, and applications that are assigned to your business unit.

As a delegated administrators with the **Manage Administrators** privilege, you can create other delegated administrators and perform the following actions:

- Delegate to the new administrator any privileges that you have
- Assign your business unit or any child business unit to the new administrator

Maker and Checker

With SecureTrasnport version 5.3.8 and later, there are two additional available "roles" of the delegated administrator, defined by specific permissions: *Maker* and *Checker*.

- The Maker is a delegated administrator who can create and update user accounts. Accounts created by the Maker will remain in "Pending" verification status until further processing by a Checker.
- The Checker is a delegated administrator who can view in read-only mode all settings associated with an account. The Checker has the responsibility to review and accept or reject the newly created account by the Maker. In fact, these are the only actions the Checker privileges grant: the rest of the Checker permissions are read-only.

The concept of the Maker and Checker is to separate the responsibilities and duties of account creation and account approval. These two roles complement each other and the Checker acts as a second level of user account approval.

When you create a delegated administrator, you can either assign **Read Only** or **Checker Rights** or **Maker Rights**; or you could use any combination of the other available privileges.

Privilege	Description
Read Only	Allows the administrator to view the pages only. This administrator cannot make any changes. Use Read Only for auditing.
Checker Rights	Allows the administrator to inspect all settings of user, service and template accounts in an assigned business unit. The Checker administrator can also approve or reject accounts created by a Maker administrator in the assigned business unit.
Maker Rights	Allows the administrator to create user, service and template accounts in an assigned business unit. The Maker administrator can update all account settings before submitting the accounts for approval by Checker administrator.
Create Users	Allows the administrator to create new accounts for an assigned business unit outside of the Maker-Checker user creation flow.

Privilege	Description
Update Users	Allows the administrator to modify existing accounts for an assigned business unit outside of the Maker-Checker user creation flow.
HelpDesk Rights	Allows the administrator to change the password of users in an assigned business unit. The administrator can also enable or disable a user in the assigned business unit.
Audit Log Rights	Allows the delegated administrator to access Audit Log entries of actions performed by all administrators. When deselected, the administrator can access only the audit log entries of actions performed by their account and no one else's.
Manage Administrators	Allows the administrator to create, modify, and delete delegated administrators for an assigned business unit.
Manage Business Units	Allows the administrator to create, modify, and delete business units.
Manage Applications	Allows the administrator to create, modify, and delete applications other than Shared Folder type applications for an assigned business unit.
Manage Shared Folders Applications	Allows the administrator to create, modify, and delete Shared Folder type applications for an assigned business unit.
Manage Route Package Templates	Allows the administrator to create, modify, and delete route package templates. **Note** In order these privileges to take effect, the appropriate administrative role should be updated to allow access to the Routes Menu.
Manage 'External Script' Step	Allows the administrator to create, modify, and delete any **External Script** steps in a route belonging to route package or route package template. **Note** In order these privileges to take effect, the appropriate administrative role should be updated to allow access to the Routes Menu.
Manage 'Run as root external scripts'	Allows the administrator to modify the **Run as root administrator** External Script property. **Note** In order for these privileges to take effect, the administrator should have privilege to manage External Script step.
Manage Login Restriction Policies	Allows the administrator to create and maintain login restriction policies. They can also create and manage login restriction policy entries.

When each delegated administrator delegates privileges and assigns business unit to delegated administrators he creates, the result is a hierarchy of delegated administrators where those higher in the hierarchy can have greater responsibility and more privileges than those below them.

For example, a finance delegated administrator with permission for the finance business unit can create an audit delegated administrator who can view the Administration Tool pages and two other delegated administrators to administer business units within finance. The following diagram shows the hierarchy:

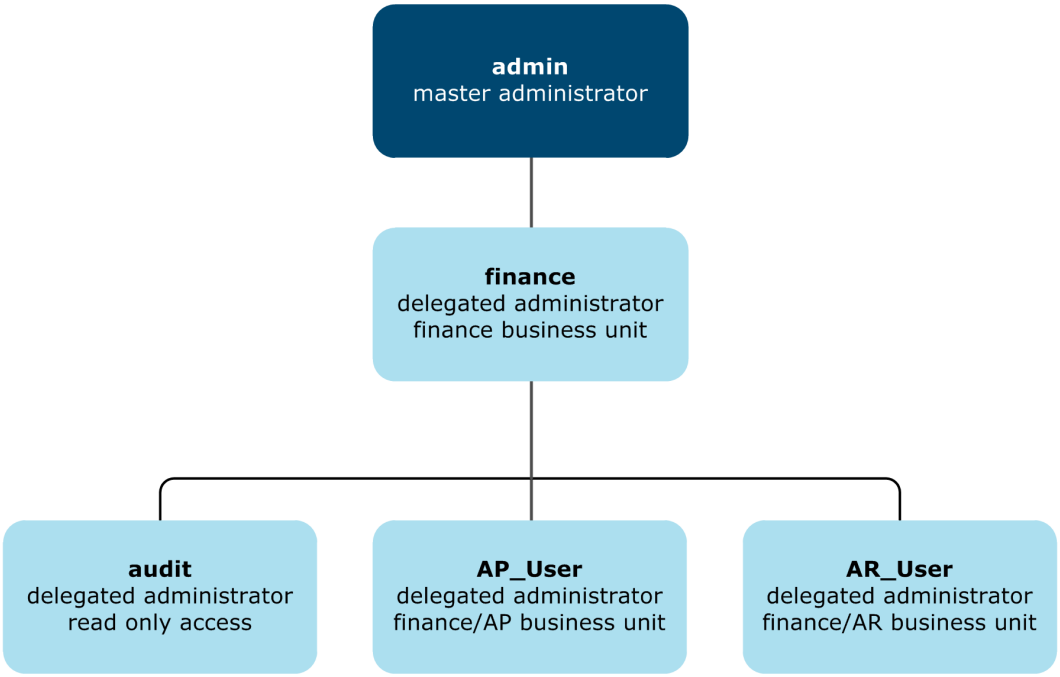


Figure 9. Example delegated administration hierarchy

The following topic describes how to create a delegated administrator:

- *Create a delegated administrator* on page 654 - Provides how-to instructions for creating a delegated administrator.

Create a delegated administrator

Use the following procedure to create a delegated administrator.

1. Create or edit an administrator and set the **Administrative Role** to Delegated Administrator. The panel area expands with various additional Delegated Administrator Settings.
2. Select a **Parent Administrator**. This is the administrator who hierarchically stands on the higher level to the delegated administrator you are creating.
3. Select the business units you want to assign to the administrator, if required. Business Units can be added or modified through the *Business Units* page. Also, here you can only assign business units that are assigned to the Parent Administrator.

Note General rules of inheritance apply here: if the Business unit assigned to Delegated Administrator has one or more child business units, all those child business units will be also assigned to this Delegated Administrator. If the business unit does not have child, but another Delegated Administrator adds child on a later stage, the newly added child will be automatically assigned to the first Delegated Administrator. If the child Business Unit is removed from the parent Business Unit but continues to exist, the Delegated Administrator will not be assigned to it anymore.

4. Depending on the duties and responsibilities of your new delegated administrator, select either of the following options: **Read Only**, **Checker Rights** or **Maker Rights**.
    - Select **Read Only** to allow the delegated admin read-only access to the user management screens within the selected Business Units. This option deselects and disables editing of all the permission options that follow.
    - Select **Checker Rights** to allow the delegated admin Checker-only privileges. This option disables all additional permissions for user account creation and modification.
    - Select **Maker Rights** to allow the delegated administrator Maker-only privileges. This option preselects the **Create Users** and **Update Users** permissions. You can still edit HelpDesk and Manage rights.
5. If you do not any of the options in the previous step, you can still assign any of the available privilege options to the new delegated administrator.
6. Click **Save** to add the new administrator.

Administrative roles

When you create or edit an administrator account you can set an administrative role that defines the account's privileges and permissions in the Administration Tool. You can create multiple administrators whose account management capabilities are based on administrative roles you create. Each role can have different account management capabilities. Use the *Administrative Roles* page on the SecureTransport Server to create the roles and assign administrative privileges.

For each role, you control:

- Role type
- Permission to bounce servers
- Access to SecureTransport menus and submenus

The following topics describe and provide how-to instructions for managing administrative roles:

- *Predefined administrative roles* on page 656 - Lists the predefined administrative roles.
- *Add an administrative role* on page 659 - Provides how-to instructions for adding an administrative role.
- *Edit an administrative role* on page 661 - Provides how-to instructions for editing an administrative role.

Predefined administrative roles

The following administrative roles are predefined:

- **Master Administrator** – Access to all menus, tabs, and pages of the Administration Tool. Cannot be modified.
- **Database Administrator** – Access to the *Database Setting* page only. Access to the *Setup Oracle* page is not included when SecureTransport is running on the embedded database. Only the `dbsetup` administrator can have this role. Information is maintained in the file system so that `dbsetup` can log in to the Administration Tool when the database is not running. Cannot be modified.

  Note If, as the `dbsetup` administrator, you change your password, have your password expired, or have your account disabled or enabled while there is no connection to the database, that change is not recorded in the database. The next time you log in as the `dbsetup` administrator with the database connected, the change is overwritten by the information from the database.

- **Setup Administrator** – Access through the custom **Configure** menu to pages required to perform the post-installation tasks and setup operations described in the *SecureTransport Getting Started Guide*. Cannot be modified.
- **Account Manager** – Access restricted to the *User Accounts*, *Unlicensed User Accounts, Service Accounts*, *Templates*, and *Business Units* pages on the **Accounts** menu and all pages on the **Access** menu.
- **Application Manager** – Access restricted to the pages on the **Service Accounts** and **Applications** menus.
- **Delegated Administrator** – Configurable access to menus and data based on the function the administrator has within an organization. This administrator type is created by a master administrator or a parent delegated administrator.

The following table illustrates the access rights and restrictions of the default restriction levels for SecureTransport administrators. You can modify the access rights for the Account Manager, Application Manager, and Delegated Administrator roles:

Menus and Pages	Master Administrator	Setup Administrator	Account Manager	Application Manager	Delegated Administrator
Operations					
Server Control	P	P	—	—	—
Cluster Management	P	—	—	—	—

Menus and Pages		Master Administrator	Setup Administrator	Account Manager	Application Manager	Delegated Administrator
	Server Usage Monitor	P	—	—	—	—
	File Tracking	P	—	—	—	P
	Server Log	P	P	—	—	—
	Audit Log	P	P	—	—	P
	Server Configuration	P	—	—	—	—
	Support Tool	P	—	—	—	—
Setup						
	Certificates	P	P	—	—	—
	FTP Settings	P	—	—	—	—
	AS2 Settings	P	—	—	—	—
	SSH Settings	P	—	—	—	—
	Admin Settings	P	—	—	—	—
	PeSIT Settings	P	—	—	—	—
	AdHoc Settings	P	—	—	—	—
	Database Settings	P	P	—	—	—
	Axway Sentinel	P	—	—	—	—
	Server License	P	P	—	—	—
	Command Logging	P	—	—	—	—
	Transfer Logging	P	—	—	—	—
	Holiday Schedule	P	—	—	—	—

Menus and Pages	Master Administrator	Setup Administrator	Account Manager	Application Manager	Delegated Administrator
Miscellaneous	P	—	—	—	—
File Archiving	P	—	—	—	—
TM Settings	P	—	—	—	—
Network Zones	P	—	—	—	—
Authentication - All submenus	P	—	—	—	—
Account					
User Accounts	P	—	P	—	P
Unlicensed Users	P	—	P	—	P
Service Accounts	P	—	P	P	P
Import/Export	P	—	—	—	P
Administrators	P	—	—	—	P
Change Password	P	—	—	—	P
Manage Roles	P	—	—	—	—
Account Templates	P	—	P	—	P
Site Templates	P	—	P	—	P
System	P	—	—	—	P
Business Units	P	—	P	—	P
Active Users	P	—	—	—	—
Access—All submenus	P	—	P	—	—
Application—All submenus	P	—	—	P	P
Routes—All submenus	P	—	—	—	—

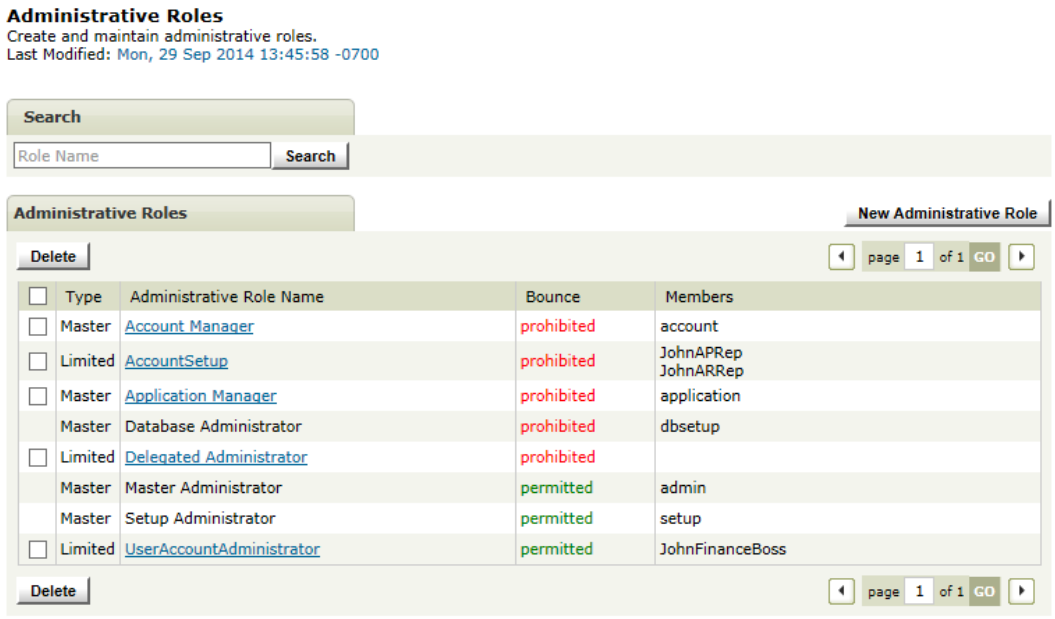
Add an administrative role

Note If you have been using a previous version of SecureTransport and you have upgraded to SecureTransport 5.3.1, only administrative roles which used to have full rights for the **Transaction Manager** tab (*Packages*, *Install Agents*, and *Install Functions*) will have permissions for *TM Settings* in the **Setup** tab.

Use the following procedure to add administrative role.

1. Select **Accounts > Manage Roles**.

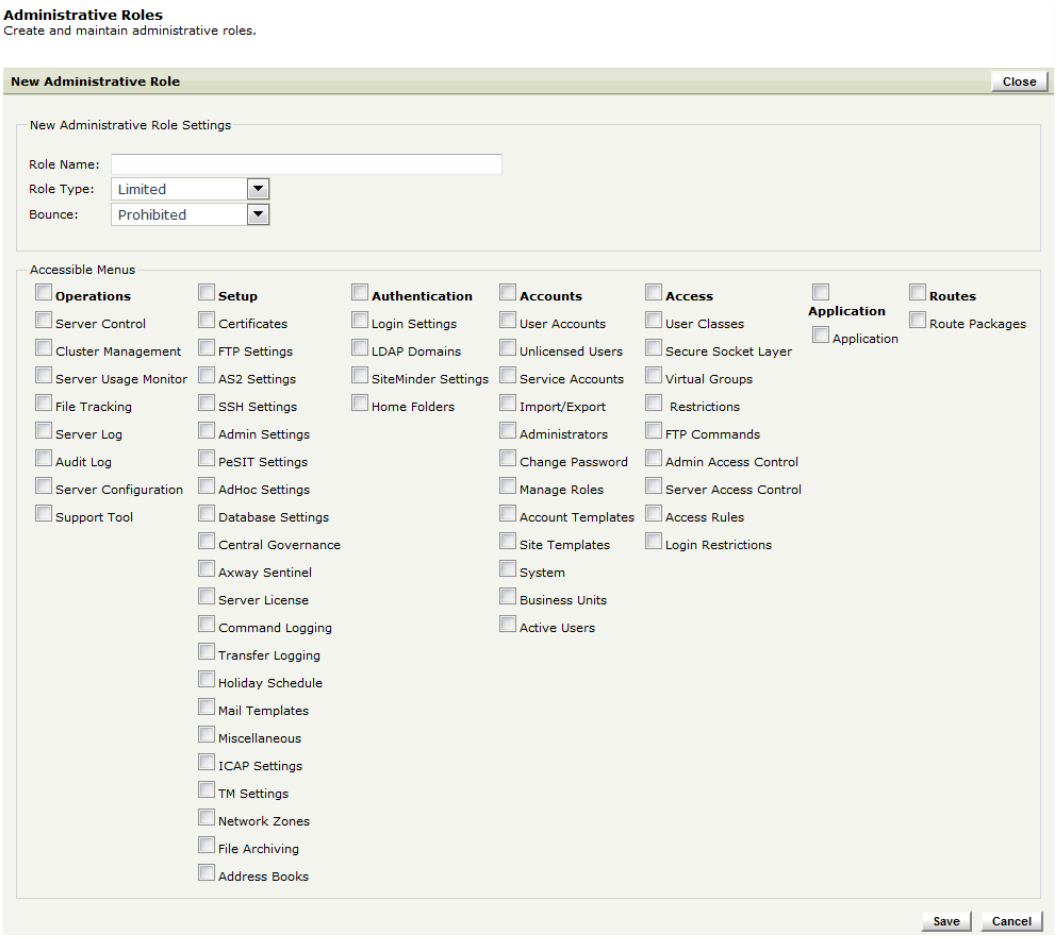
   The *Administrative Roles* page is displayed.



   If you do not see roles with Master in the Type column, you are logged on as a user with a limited role.

2. Click **New Administrative Role**.

   The *New Administrative Role* window is displayed.



3. Type the **Role Name**.
4. Select the **Role Type**.
    - Select **Master** to give this role complete privileges over the Administration Tool menus selected under **Accessible Menus** and access to all accounts and business units. Only an administrator whose role has Master type can select this.
    - Select **Limited** to enable limiting the business unit access and privileges for administrators with this role. The Delegated Administrator role has **Role Type** set to **Limited**. A user with a limited role and **Manage Roles** access cannot access Master roles or his own role. **Limited** is the default setting.
5. Select values from the **Bounce** drop-down list.
    - Select **Permitted** to enable administrators at this level to bounce (manually signal running server processes to reload their configurations) servers.
    - Select **Prohibited** to deny these same privileges. **Prohibited** is the default setting.

6. Under **Accessible Menus**, do the following:
   - Select the menus that the administrative role can access. Select the check box for the column heading to select all the menus in the column.
   - Clear the menus that the administrative role cannot access. Clear the check box for the column heading to clear all the menus in the column.
7. Click **Apply**.

   The new administrative role is added to the *Administrative Roles* page.

Edit an administrative role

Use the following procedure to edit an administrative role.

1. Select **Accounts > Manage Roles**.

   The *Administrative Roles* page is displayed.
2. Click the name of the administrative role you want to edit.

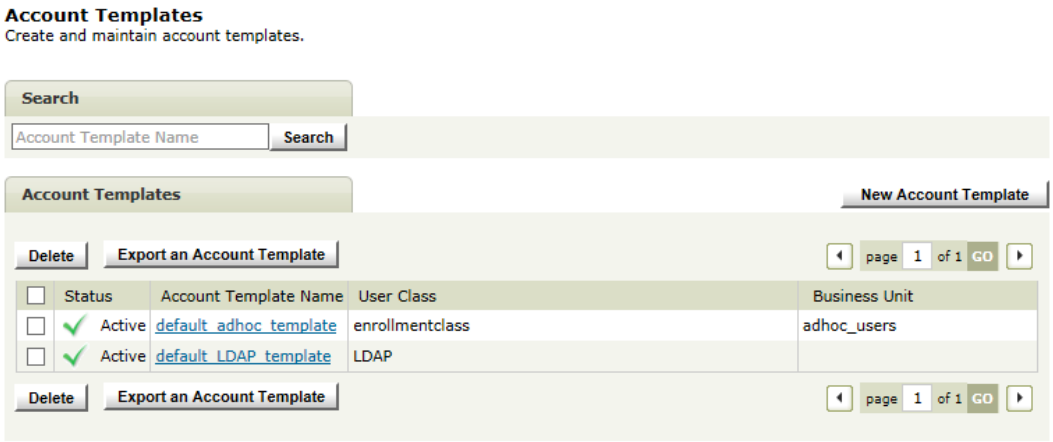
   The *Edit Administrative Role* dialog box is displayed.

   Note You cannot edit the Master Administrator, Setup Administrator, or Database Administrator roles or your own role.
3. Edit the values as necessary, and then click **Apply**.

   You are returned to the *Administrative Roles* page.

Account templates

You can create an account template that can be used by LDAP, SSO, or other external user repositories. Use account templates to avoid duplicating users between your user repository and SecureTransport. Account templates let SecureTransport use the user names and passwords that exist in external user repositories such as LDAP, SSO, Active Directory, or a third party database. SecureTransport does not need to synchronize with any external source. By using the value set in the User Class field, the account templates map the user in real time to SecureTransport.



The template uses the user class as a type of dividing mechanism, allowing you to create different templates for different user functions based on the User Class. A user can be assigned a User Class based on the following items: User Type, User Name, User Group, and From address (the IP address or host name of the logged in user). Create a specific user class for each external repository that you are using.

Templates can also be assigned a business unit.

The following topics describe how to assign external users to account templates and how to manage account template. They also list the account template required values.

- *Account templates and external users* on page 662
- *Account template required values* on page 663
- *Manage account templates* on page 663

Account templates and external users

SecureTransport assigns external users to the account template using the following steps:

1. Determine the User Class based on the already known values for the UID, GID, User Type, and IP address.
2. Compare the determined User Class with the defined User Class in all enabled external account templates. Since the User Class in the template can contain wildcards there might be more than one template that matches the User Class of the currently logged user. In this case, the templates are sorted alphabetically, and the first one is selected.
3. If the User Class matches the User Class of a template, SecureTransport tries to determine the new UID, GID, and Home Folder values as defined in the template. The templates can contain expressions in the supported expression language to dynamically select the UID, GID, or Home Folder. The result is one of the following:
    - If the system fails to determine even one of the required attributes (UID, GID, or Home Folder) from the template the user is *not* assigned to that template and the login fails.
    - If the system manages to determine all of the required attributes, the currently logged external user is assigned to the selected template.
    - If the User Class does not match any of the User Classes in the account template, the server treats the user as a regular external user.
4. If the user is assigned to a template, the UID, GID, and Home Folder are determined from the template, and the values used to determine the User Class are ignored. If the home folder of the user is missing, it is automatically created with the correct permissions.
5. After the external user is mapped to a template the user is automatically assigned a User Type of Virtual, the same as a regular user account.

Account template required values

Each template has several required values: **Account Template Name**, **User Class**, **UID**, **Group ID**, and **Change Home To**.

There are three ways to configure a template once you have specified the **User Class** and **Account Template Name**, and **Business Unit**:

- **Hardcoded values** – The values of the **UID**, **Group ID**, **Change Home To**, and **Notes** fields are explicitly specified in the template. In this scenario every external user mapped to the template uses the same home folder and has the same UID and Group ID (GID).
- **Expressions** – In this scenario the values of the **UID**, **Group ID**, **Change Home To**, and **Notes** fields are specified expressions in the supported expression language. Usually the values of the attributes are different for each external user.
- **Mixed** – Some values are hardcoded and some are expressions or text that includes hardcoded values and expressions. For example you can specify the **Change Home To** as `/tmp/users/${stenv['loginname']}` which means that the home folder of every external user is determined by adding the path `/tmp/users/` and the login name.

Directory path names in an account template are case sensitive.

Note If you configure the home directory of an account template that is used for LDAP or SSO users to include the user name in the home directory, and LDAP or SSO user whose user name contains one or more of the characters <, >, #, and \ or begins or ends with a space character cannot log in to SecureTransport. This is due to operating system limitation on file names. To allow such LDAP or SSO users to use an account template, use the UID or some other user-unique value to name the home directory.

Manage account templates

Use the *Account Templates* page to manage account templates.

The following topics provide example and how-to instructions for managing account templates:

- *Add an account template* on page 664
- *Enable an account template* on page 670
- *Disable an account template* on page 671
- *Certificates for an account template* on page 671
- *Configure transfer sites for an account template* on page 671
- *Configure transfer profiles for an account template* on page 672
- *Configure routes for an account template* on page 672
- *Configure subscriptions for an account template* on page 675
- *Examples of expressions in an account template* on page 677
- *Export an account template* on page 680

Add an account template

Use the following procedure to add an account template.

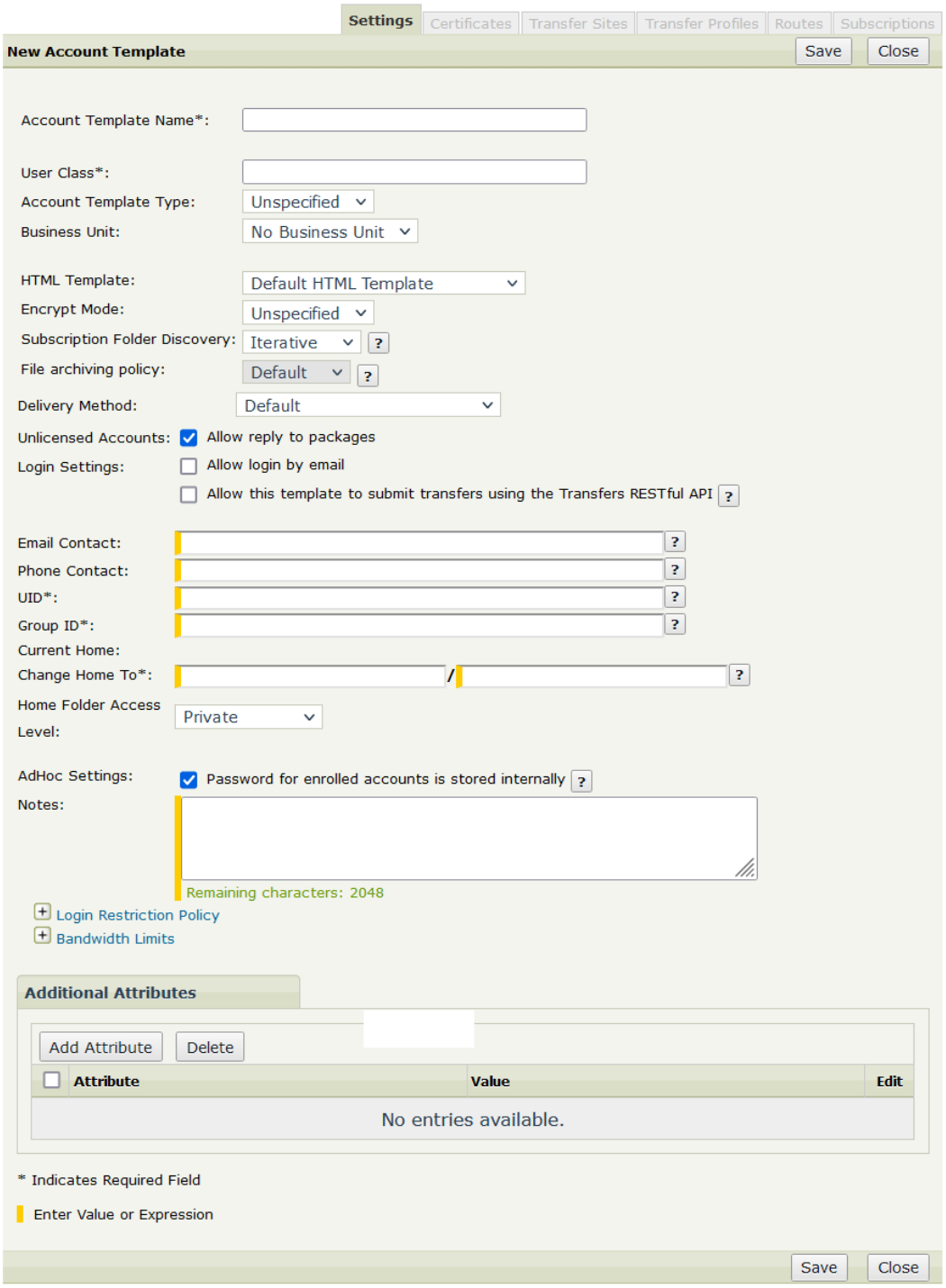
1. Select **Accounts > Account Templates**.

   The *Account Templates* page is displayed.

2. Click **New Account Template** to open a new account template.

   The *New Account Template* page is displayed.

   Note The *Address Book Settings* are only displayed if the Address Book feature is enabled (the value of the `AddressBook.Enabled` configuration option is set to **true**). For Address Book account level configuration instructions, refer to *Address Book account level configuration* on page 240.



Use hardcoded values, expressions in the supported expression language, or a combination of both to complete the fields for the account settings. Required fields are marked by an asterisk. Fields that accept either hardcoded values or expressions are indicated by a vertical yellow bar.

3. Enter a name for the template in the **Account Template Name** field.

4. Enter a pattern that uses question mark (`?`) to match one character and asterisk (`*`) to match any string of characters in the **User Class** field. This account template is associated with users in all classes whose names are matched by the pattern. For example, to associate the template with all users, enter `*`.
5. To place users in a **Business Unit**, select a business unit from the list. Leave the setting as `No Business Unit` if users are not part of a business unit.
6. To specify an HTML template to be used when users log in using the web client, select a value from the **HTML template** drop down.
7. Select **Encrypt Mode**.

   This field can enable repository encryption for users associated with this template.

   - **Unspecified** (default) – Repository encryption is enabled based on the `EncryptClass` user class evaluation.
   - **Enabled** – Repository encryption is enabled for users associated with this template.
8. Select **Subscription Folder Discovery**.

   This field determines the subscription folder discovery mode. For accounts with multiple subscriptions, the number of subscriptions and the target folder depth may impact performance.

   - **Iterable** (default): Subscription folder discovery is performed by iteration over all of the account's subscriptions while trying to match the target folder.
     Tip: choose this mode when the number of subscriptions is small and the target folder depth is large.
   - **Recursive**: Subscription folder discovery is performed by recursive traversal of the target folder hierarchy - the target folder is checked first and if no match is found, then its parent folder is checked. The process continues until a match is found or there are no more folders to check.
     Tip: choose this mode when the number of subscriptions is large and the target folder depth is shallow.
9. Select **File archiving policy**.

   This field determines the file archiving policy.

   - When **Default** is selected, then the following apply:
     1. If the account is assigned to a business unit, it will inherit its policy.
     2. Otherwise, the global archiving policy applies.
   - When **Enabled** is selected, file archiving will be enabled for this account.
   - When **Disabled** is selected, file archiving will be disabled for this account.

   Note:you cannot modify this option, if either of the following are true:

   - if the global file archiving policy is disabled, or
   - if this account is assigned to a business unit with **Allow File Archiving Policy modifying** unchecked.

10. The **Delivery Method** value controls the options that ST Web Client displays in the *User Access* window.
    - **Disabled** – The user cannot send files using ad hoc file transfers.
    - **Default** – Use the delivery method specified in the account template, if any, or in the **Default Package Delivery Method** field of the *AdHoc Setting* page.
    - **Anonymous** – The sender can choose Anonymous or Challenge.
    - **Account Without Enrollment** – The sender can choose Anonymous, Challenge, or Existing Account.
    - **Account With Enrollment** – The sender can choose Anonymous, Challenge, Existing Account, Enroll Unlicensed, or Enroll Licensed.
    - **Custom** – Select the allowed enrollment types in the **Enrollment Types** field. The sender can chose any of the selected enrollment types.
11. For a custom delivery method, select one or more allowed enrollment types in the **Enrollment Types** field:
    - **Anonymous** – The ad hoc file recipient receives a link to retrieve the files and is not enrolled as a user. The ST Web Client option is **Send attachment link only**.
    - **Challenge** – The ad hoc file recipient receives a link and must answer correctly a challenge question specified by the sender to retrieve the files. The recipient is not enrolled as a user. The ST Web Client option is **Protect attachment link with security question**.
    - **Existing Account** – Do not enroll ad hoc file recipients. Only existing users can receive files. The ST Web Client option is **Send to existing users only**.
    - **Enroll Unlicensed** – If the ad hoc file recipient does not have a user account, the recipient must enroll and create an account before retrieving the files. The ad hoc file recipient becomes an unlicensed user who can only reply once to the email and retrieve the files. Other user attributes are defined by the enrollment template. The ST Web Client option is **Allow recipients to enroll as new Unlicensed Users**.
    - **Enroll Licensed** – If the ad hoc file recipient does not have a user account, the recipient must enroll and create an account before retrieving the files. The ad hoc file recipient becomes a SecureTransport user with all the attributes specified in the default enrollment template. The ST Web Client option is **Allow recipients to enroll as new Full Licensed Users**.
12. The **Implicit Enrollment Type** value controls which option ST Web Client selects initially in the *User Access* window and which enrollment type is used by the Axway Email Plug-ins. The choices depend on the enrollment types enabled by the **Delivery Methods** and **Enrollment Types** fields.
13. Select **Allow reply to packages** in **Unlicensed Accounts** to allow an unlicensed user associated with this template to reply to emails.

14. Specify **Login Settings**.
    a. Select **Allow this account to login by email** to allow the user to log in using with the value of the **Email Contact** field as well as the **Login Name**. A user of one of the Axway Email Plug-ins must have **Allow this account to login by email** selected.
    b. Select **Allow this account to submit transfers using the ST RESTful API** to enable calls from the SecureTransport REST file transfer API authenticated with the credentials from this account. When this option is selected, the account will be allowed to trigger server initiated transfers using the Transfers RESTful API resource and retrieve the tracking information for these transfers.
15. Enter a value or expression for the **Email Contact**.

    When this email address is the recipient of an ad hoc file transfer email sent from ST Web Client or one of the Axway Email Plug-ins, SecureTransport determines that this user is the recipient. If the user is allowed to log in by email, this is the value used in the **User Name** field of the login page.

    Note You can access the SSO email attribute that was previously mapped to `fdxEmail` with the expression `${sess.STSESSION_SSO.email}`.

    Note Accessing Single Sign-On (SSO) attributes is not possible when using SSO with Kerberos authentication protocol. It is only possible with SAML.
16. Enter a value or expression for the **Phone Contact**.
17. Enter a value or expression for the numeric user ID of the user in the **UID** field.

    On Windows platforms, this field is named **Real User** and is optional.

    Note You can access the SSO UID attribute that was previously mapped to `fdxUid` with the expression `${sess.STSESSION_SSO.uid}`.

    Note Accessing Single Sign-On (SSO) attributes is not possible when using SSO with Kerberos authentication protocol. It is only possible with SAML.
18. Enter a value or expression for the numeric group ID for the user account in the **GID** field. The account uses the system access rights and privileges valid for this user group on the system.

    Note You can access the SSO GID attribute that was previously mapped to `fdxGid` with the expression `${sess.STSESSION_SSO.gid}`.

    Note Accessing Single Sign-On (SSO) attributes is not possible when using SSO with Kerberos authentication protocol. It is only possible with SAML.
19. Enter values or expressions for the home folder in the **Change Home To** fields for the account as an absolute path.

    Note You can access the SSO username attribute with the expression `${sess.STSESSION_SSO.userName}`.

    Note Accessing Single Sign-On (SSO) attributes is not possible when using SSO with Kerberos authentication protocol. It is only possible with SAML.

20. Select **Access Level**. The home folder access level determines whether and which other accounts are able to publish to the home folder of the current account.
    - **Private** – The access level is private. Only the current account is able to publish files to its home folder.
    - **Business Unit** – Account home folder access is limited to the account's business unit. The current account and all accounts in the current account's business unit can publish to this account's home folder.
    - **Public** – Access to the account is public. All accounts are able to publish to this account's home folder.

      Note Access level is applicable only when Advanced Routing feature is used. For more information see *Advanced Routing* on page 795.

21. Select **Password for enrolled accounts is stored internally** in **AdHoc Settings** to generate the account's password during enrollment. If **Password for enrolled accounts is stored internally** is not selected, no password will be generated and stored in the SecureTransport database. When a new account with external password is enrolled, SecureTransport will send out an email notification; but will not send a temporary password.

    Note For SSO end-users you need to uncheck this option.

22. Enter a value or expression for the text description of the user account in the **Notes** field.
23. Select the **Login Restriction Policy**. The Login Restriction Policy defines rules for allow or deny login to users based on the client IP or host and other conditions. For additional information, refer to *Login restrictions* on page 747.

    If a Login Restriction Policy is selected as the global default policy, it will be the inherited default selection for the user account.

    If a Login Restriction Policy is not selected as the global default policy and the Business Unit has a Login Restriction Policy selected, it will be the inherited default selection for the user account.

    If neither a global default Login Restriction Policy or a Business Unit Login Restriction Policy is selected, then the policy selected for the users account will be in effect.

    Note The default inherited Login Restriction Policy can be overridden by selecting a Login Restriction Policy from **On Account Template**.

24. In the *Bandwidth limits* pane select either **Bandwidth Limits Policy** to apply:
    - Default – the current account template inherits its bandwidth limits from the parent business unit or the global bandwidth
    - Custom – the panel expands with two additional options for you to configure: **Inbound limit** and **Outbound limit** (both values in kb/s per user)
    - Disabled – no bandwidth limits are applied to the users assigned to the current account template

25. To add an attribute, click **Add Attribute**. For additional information on Additional Attributes, refer to *Additional attributes* on page 175.
    a. Enter the attribute and value in the **Attribute** and **Value** fields.

       Add Attribute enables the administrator to add custom properties (Key=Value). Also the administrator will be able to access the custom properties (named Attributes) using any field in Advanced Routing.

       Some examples of Attributes are:

Attribute	Value
userVars.1	internalEmail@axway.com
userVars.2	ReportsMonitor

       To access attributes, see the following examples:

       ```
       ${account.attributes['userVars.1']}
       ```

       ```
       ${account.attributes['userVars.2']}
       ```

       For example, the `account.attributes` is the selector for attributes of the account used to execute the current route - it has to be written exactly as shown.

       The `userVars.` prefix must be prepended to attribute name.

       All this should be written as an EL expression: `${...}`

    b. Click the attribute Save ( ) icon.
26. Once you have completed the information in the *Settings* pane, click **Save** to create the account template.
27. To enable the account template, click **Enable Account Template**.

    Select the **Certificates**,**Transfer Sites**, **Transfer Profiles**, or **Subscriptions** tabs to add additional information to the template. Those pages are similar to the pages for an account, but permit expressions in some fields.
28. To return to the *Account Templates* page, click **Close** or select **Accounts > Account Templates**.

Enable an account template

Once you have created the template, you must enable it to use it.

1. Select **Accounts > Account Templates**.

   The *Account Templates* page is displayed.
2. Click the name of the template you want to enable to view the template settings.
3. Click **Enable Template** to make the template active.
4. To return to the *Account Templates* page, click **Close**.

Disable an account template

You can also disable an already created template.

1. Select **Accounts > Account Templates**.

   The *Account Templates* page is displayed.

2. Click the name of the template you want to enable to view the template settings.
3. Click **Disable Template** to make the template active.
4. To return to the *Account Templates* page, click **Close** or select **Accounts > Account Templates**.

Certificates for an account template

Like a user account, an account template can have partner certificates and private certificates. It cannot have login certificates.

For more information, see *Manage certificates* on page 476.

Configure transfer sites for an account template

Use the following procedure to configure transfer sites for an account template.

1. With the account template open, select **Transfer Sites** and click **Add New**.

   You must define the transfer site completely. Transfer sites in an account template do not support site templates.

2. Type a **Site Name**.
3. Select a **Site Type**.
4. In the **Add Transfer Site** box, select the **Transfer Protocol**.

   To comply with AS2 protocols, it is not available.

5. Type values or expressions for the required fields and the optional fields needed to define the transfer site.

   Transfer sites in an account template do not support server-initiated downloads, so the fields used for them are not displayed.

   You can use expressions in the fields indicated by a vertical yellow bar.

6. To use expressions for the check boxes, select **Advanced Expressions**, and, in each field that replaced a check box, type 1 for selected (true) or 0 for cleared (false) or an expression that evaluates to 0 or 1.

   Note The custom Pluggable Transfer Site feature does not support the use of the SecureTransport Expression Language (EL).

7. Click **Add** to save the transfer site.

For example, to select **Use FTPS** for the transfer site depending on the whether the `target` variable contains the string `class`, type the following in the **Use FTPS** field:

```
${stenv['target'].matches('.*class.*') ? '1' : '0'}
```

This expression tests the value of `target` and returns 1 if it contains the string `class`, 0 if not.

Note If an account template and its transfer site are defined using expressions, you cannot restart failed transfers for that account template using the **Resubmit** button on the *File Tracking* page.

Configure transfer profiles for an account template

An account template can have transfer profiles. You can use expressions in the **Files To Send** and **Receive Files As** fields.

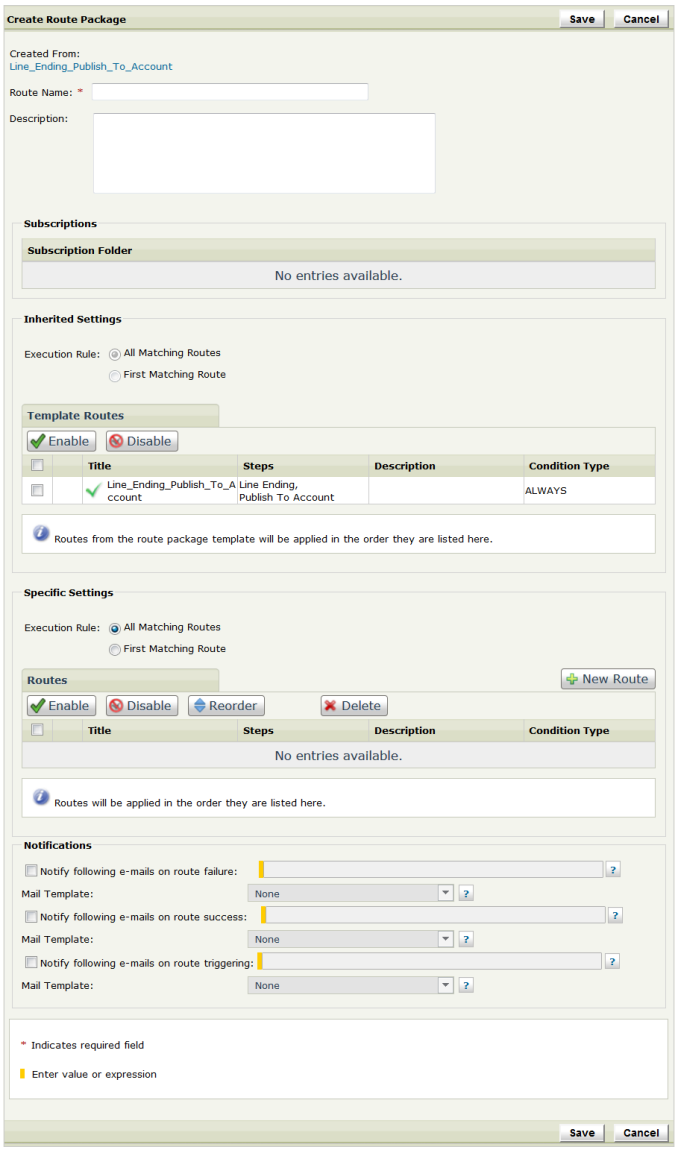
For more information, see *Transfer profiles* on page 600.

Configure routes for an account template

Prior to configuring a route for an account template, the account template should have an Advanced Routing application instance subscription. For account template subscription information, refer to *Configure subscriptions for an account template* on page 675 and to *Subscribe to Advanced Routing application* on page 821. Additionally, route package templates must be available for assignment. For information on creating and managing route package templates, refer to *Manage Route Package Templates* on page 806.

1. With the account template open, select **Routes**, select a route package template, and click **Assign Route**.

   The *Create Route Package* page is displayed. You can navigate to the *Edit Route Package Template* page for the selected route package template by clicking the **Created From** link.



2. In the **Route Name** field, type the desired name of the route. The route name can contain 254 characters or less.

   Note You cannot use the following characters in the route name: `* < > ? " / \ | :`

3. (Optional) Enter a **Description**.
4. In the *Subscriptions* pane:
   a. Click **Assign** to assign an available Advanced Routing application folder to the route.

      The Available Subscriptions page is displayed.

   b. On the *Available Subscriptions* page, select the checkbox for a folder from the

Subscriptions Folder list and click **OK** to assign a folder to the route.

The assigned folder is now listed in the *Subscriptions List*.

To unassign an application folder, select the checkbox for the folder and click **Unassign**.

5. In the *Inherited Settings* pane:
    a. Select the check box for a Template Route and click **Disable** to disable an enabled inherited route.
    b. Select the check box for a Template Route and click **Enable** to enable a disabled inherited route.

        Note The inherited Execution Rule cannot be changed.

6. In the *Specific Settings* pane:
    a. Determine the **Execution Rule**. Select either **All Matching Routes** (default) or **First Matching Route**.

        When **All Matching Routes** is selected, all matching Routes are executed. When **First Matching Route** is selected, only the first matching Route is executed.

    b. Click **New Route**.

        The *New Route Entry* page is displayed. For Route configuration information, refer to *Manage Routes* on page 812.

        You can also enable, disable, reorder, and delete Routes in the *Specific Settings* pane. For information on enabling, disabling, reordering, or deleting Routes, refer to *Manage Route Package Templates* on page 806.

7. In the *Notifications* pane:
    a. Select **Notify following e-mails on route failure** to be notified on route failure and enter a notification email address, a list of mail addresses, or an expression. For additional email configuration information, refer to *SMTP configuration* on page 183.
    b. Select the **Mail Template** from the menu to be used for route failure notifications. For email template configuration information, refer to *Mail templates* on page 173.
    c. Select **Notify following e-mails on route success** to be notified on route success and enter a notification email address, a list of mail addresses, or an expression. For additional email configuration information, refer to *SMTP configuration* on page 183.
    d. Select the **Mail Template** from the menu to be used for route success notifications. For email template configuration information, refer to *Mail templates* on page 173.
    e. Select **Notify following e-mails on route triggering** to be notified on route triggering and enter a notification email address, a list of mail addresses, or an expression. For additional email configuration information, refer to *SMTP configuration* on page 183.
    f. Select the **Mail Template** from the menu to be used for route triggering notifications. For email template configuration information, refer to *Mail templates* on page 173.
8. Click **Save**.

Configure subscriptions for an account template

1. With the account template open, select **Subscriptions**, select an application, and click **Subscribe**.

   Subscriptions in an account template do not support applications of type Standard Router, so they are not include in the drop-down list.

2. In the *Flow Settings* pane, select the **Existing flow attributes**.

   If **Preserve** is selected, the attributes defined in the *Flow Attributes* pane will be applied only for newly received files which do not have associated flow attributes.

   If **Overwrite** is selected, the attributes defined in the *Flow Attributes* pane will overwrite any existing attributes for incoming files (for example, files published to this folder from another subscription folder).

   When **Append** is selected, only the attributes which are not defined for incoming files will be applied. Existing attributes will be preserved.

3. In the *Flow/Subscription Attributes* pane:

   a. To add an attribute, click **Add Attribute**. For additional information, refer to *Flow and subscription attributes* on page 175.

   Add Attribute enables the administrator to add custom properties (Key=Value). Flow attributes can be used for expression evaluation in Advanced Routing only when the application operates with files. Subscription attributes are bound to the subscription, therefore, they can be used for expression evaluation in all Advanced Routing fields.

   Note Subscription attributes can be accessed using the following expression: `${subscription.attributes['userVars.ATTRIBUTE_NAME'].` Flow attributes can be accessed using the following expression: `${flow.attributes['userVars.ATTRIBUTE_NAME']}.`

   Some examples of Attributes are:

Attribute	Value
userVars.1	internalEmail@axway.com
userVars.2	ReportsMonitor

   To access attributes, see the following examples:

   ```
   ${account.attributes['userVars.1']}
   ```

   ```
   ${account.attributes['userVars.2']}
   ```

   For example, the `account.attributes` is the selector for attributes of the account used to execute the current route - it has to be written exactly as shown.

The `userVars.` prefix must be prepended to attribute name.

All this should be written as an EL expression: `${...}`

b. Click the attribute Save ( ) icon.

4. Type values or expressions for the required fields and the optional fields needed to define the subscription.

   Subscriptions in an account template do not support server-initiated downloads, so the fields used for them do not appear.

   You can use expressions in the fields indicated by a vertical yellow bar.

5. To use expressions for additional fields including the check boxes, select **Advanced Expressions**.

   The fields and check boxes are replaced by fields with a vertical yellow bar.

   - In each field that replaces a check box, type 1 for selected (true) or 0 for deselected (false) or an expression that evaluates to 0 or 1.
   - In the other fields, type a value or an expression that evaluates to the value required.

     In the **Compression Type** field for applications that have the **Encrypt File** option such as application of type Basic Application and Site Mailbox, type one of the following values that represent available compression algorithms or an expression that evaluates to one them:

Type	Value
Use preferred (algorithm obtained from PGP key)	-1
Uncompressed	0
ZIP	1
ZLIB	2
BZIP2	3

     In the **Compression Level** field, type an integer between 1 and 9, where 1 represents the least compressed but fastest level and 9 represents the most compressed but slowest level or an expression that evaluates to an integer between 1 and 9. The values that correspond to the levels available when **Advanced Expressions** is not selected are:

Level	Value
Fast	2
Normal	5
Good	7

Level	Value
Best	9

6. Click **Add** to add the subscription to the account template.

Examples of expressions in an account template

You can use expressions on the *Settings* pane, *Transfer Sites* pane, and *Subscription*s pane when creating an account template. The following examples show some of the expressions you can use.

The following table gives examples of expressions in account settings:

Field	Expression	Description
UID	`${sess['STSESSION_LDAP_DIR_uidNumber']}`	Returns the UID from the LDAP session.
GID	`${sess['STSESSION_LDAP_DIR_gidNumber']}`	Returns the GID from the LDAP session.
Home Folder	`${sess['STSESSION_LDAP_DIR_homeDirectory']}`	Returns the home folder specified in the LDAP session.
When you have attribute maps configured, you can use the following named variable expressions instead:		
UID	`${stenv.useruid}`	Returns the UID.
GID	`${stenv.usergid}`	Returns the GID.
HomeDir	`${stenv.homedir}`	Returns the home folder.
If the account template is for licensed or unlicensed users enrolled after receiving notification of an ad hoc file transfer:	If the account template is for licensed or unlicensed users enrolled after receiving notification of an ad hoc file transfer:	If the account template is for licensed or unlicensed users enrolled after receiving notification of an ad hoc file transfer:
Email Contact	`${stenv.recipient_email}`	Returns the email address for recipient of the ad hoc file transfer.

Field	Expression	Description
Home Folder	`${stenv.recipient_email}`	Returns the email address for recipient of the ad hoc file transfer to create a unique home folder.

The following table gives examples of expressions in transfer sites:

Field	Expression	Description
Upload Folder	`/upload/${stenv.loginname}`	Returns the subfolder based on the user login name in the upload folder.
User Name	`${stenv.loginname}`	Returns the user login name.
Certificate	`x509_${stenv.loginname}`	Returns the user login certificate.
With Advanced Expressions selected, you can use the following complex expressions:		
Upload Folder	`/${stenv['target'].replace('^(.*)_(.*)_(.*)$','$2')}` or `/upload/${stenv['target'].matches('.*\\.((jpg)|(gif)|(txt))$') ? stenv['target'].replace('^.*\\.((txt)\|(jpg)\|(gif))$','$1') : 'general/'}`	Returns the upload folder based on the match and replace expression criteria.
Enable SSL	`${stenv['target'].matches('^(ssl).*')}`	Returns a 0 (false) or 1 (true) based on the match criteria.

Note You can also use regular expressions such as `${stenv.target}` only to return the file name or `${filename(stenv.target)}-${random}` to change the file name.

The following table gives examples of expressions in subscriptions:

Field	Expression	Description
Subscription Folder	`mailbox_el_${stenv.useruid}`	Returns the folder using the UID.
	`${flow.attributes['userVars.ATTRIBUTE_NAME']}`	Returns the folder using the attribute name.

Field	Expression	Description
Receive Options Decrypt PGP File As:	`${stenv.loginname}_ ${embedded}`	Returns a file name based on the login name and the embedded file name.
Keep Original As:	`archive/${date ('yyyy.MM.dd')}/ ${filename (stenv.transformation_ input)}`	Returns the location and file name based on the date and the PGP file name.
With Advanced Expressions selected, you can use the following complex expressions:		
Send Options Send Files Directly To:	`${stenv.loginname}_ftp`	Returns a location based on the user login name.
Receive Options Decrypt PGP File:	`${stenv['target']. matches('.*((\\.pgp)| (\\.gpg)|(\\.asc))')}`	Returns a 0 (false) or 1 (true) based on the match criteria.
As:	`${empty embedded ? filename (stenv.transformation_ input).replace('(\\.pgp)| (\\.gpg)|(\\.asc)') : embedded}`	Returns the file name to which the decrypted file is saved.
Keep Original:	`1`	The value `1` represents true. SecureTransport recognizes the field as being selected.
As:	`archive/${date ('yyyy.MM.dd')}/ ${filename (stenv.transformation_ input)}`	Returns the file name based on the original PGP file name.
Use Data Compression	`${extension(filename (stenv.transformation_ input)) .matches('(\\.jpg)| (\\.mov)') ? 0 : 1}`	Returns a `0` when the file extension is `.jpg` or `.mov`. These file types are already compressed and do not require compression.

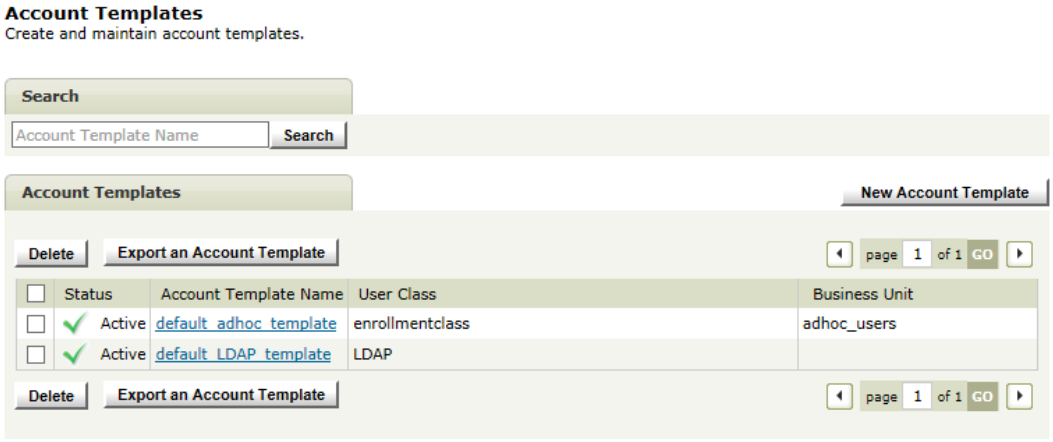
Field	Expression	Description
Compression Type	2	Compresses the file using ZLIB.
Compression Level	5	Compresses the file using the Normal setting.

Export an account template

You can export an account template to an XML file.

1. Select **Accounts > Account Templates**.

   The *Account Templates* page is displayed.



2. In the first column, select the account template to export.
3. Click **Export an Account Template**.

   The *Export Account* page is displayed.
4. Type a password in the **Password** field. This password is used to encrypt the sensitive information contained in the template account. You must use this password when you import the template account to decrypt the sensitive information.
5. Retype the password in the **Re-enter Password** field.
6. Click **Export**.
7. When the XML file with the exported account template is ready, click **Download Exported Accounts** and save the file to your local computer.

Site templates

You can create a site template for a Connect:Direct or a file services interface transfer site. You can use a Site templates to provide the information needed for many accounts in one place instead of creating a transfer site for each account. When you associate a transfer site with the template, that transfer site gets its properties from the site template. When you change the site template, the associated sites are changed.

You can associate the same template with multiple transfer sites in different accounts. If your account has more than one Connect:Direct or file services interface transfer site, you can reuse the same site template for each transfer site, or set up different site templates for each transfer site.

Site template properties are the same as those of a transfer site for the same protocol.

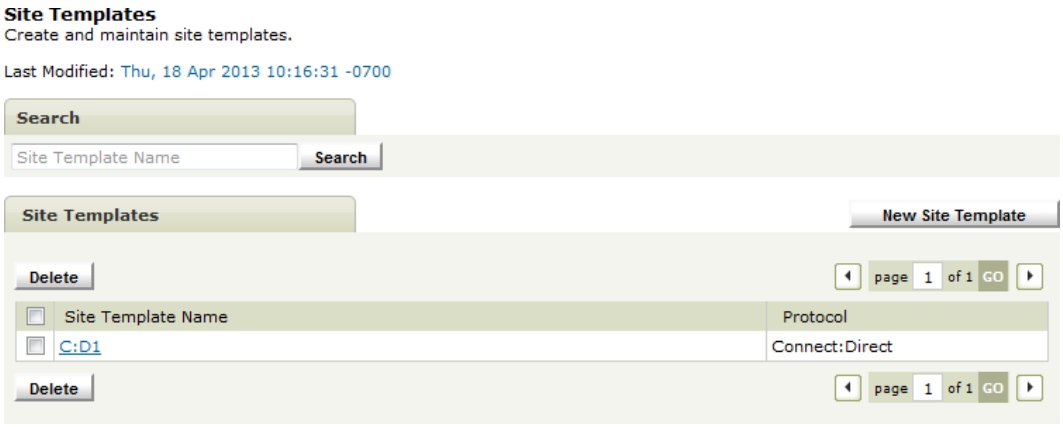
Note Support for the NDM protocol through a Connect:Direct transfer site does not replace or append your Connect:Direct license.

The following topics describe how to manage site templates and how to use a site template to define a transfer site:

- *Manage site templates* on page 681 - Provides how-to instructions for managing site templates.
- *Use a site template to define a transfer site* on page 685 - Provides how-to instructions for using a site template to define a transfer site.

Manage site templates

From the *Site Templates* page, you can create, search for, view, modify, and delete site templates.



The following topics provide how-to instructions for managing site templates:

- *Create a site template* on page 682
- *Search for a site template* on page 683
- *View a site template* on page 684

- *Modify a site template* on page 684
- *Delete a site template* on page 684

Create a site template

You can create site templates for Connect:Direct and file services interface sites.

A site template contains the same fields as the corresponding transfer site. Within those fields you can provide hardcoded values such as a server name or port number, or you can provide a placeholder parameter. You can specify an optional default value as part of a placeholder parameter. This default value can be changed after the site template is applied to a transfer site. When you select a site template while defining an account transfer site, you can provide values tailored for a specific transfer site in each field that specified a placeholder parameter.

Note You can create multiple site templates, but each site template must have a unique name.

SecureTransport provides a placeholder parameter you can use when you do not want to hard code values in the fields for the site template. A placeholder parameter is associated only with the site template where it is used. You can, however, specify different placeholder parameters for each site template you create. A placeholder parameter consist of two parts, the placeholder name and an optional default value. The format for entering a placeholder parameter is:

`%{PlaceholderName|DefaultValue}`

where `PlaceholderName` is the name of the placeholder parameter and `DefaultValue` is an optional default value assigned to a specific field.

Note If you are using the optional default value, it must be separated from the placeholder name by the | character.

For example, the placeholder parameter `%{ServerPort|456}` has both a placeholder name and a default value. In this example, the placeholder parameter is entered in the **Local server port** field and a server port number of 456 is used by all transfer sites that apply this site template and accept the default value.

Placeholder names can only contain the following characters: a-z, A-Z, 0-9, and the underscore (_). The first character of a placeholder name cannot be a digit. The default value can use any characters, but to include a right brace (`}`), precede it with a backslash (`\}`).

Placeholder examples:

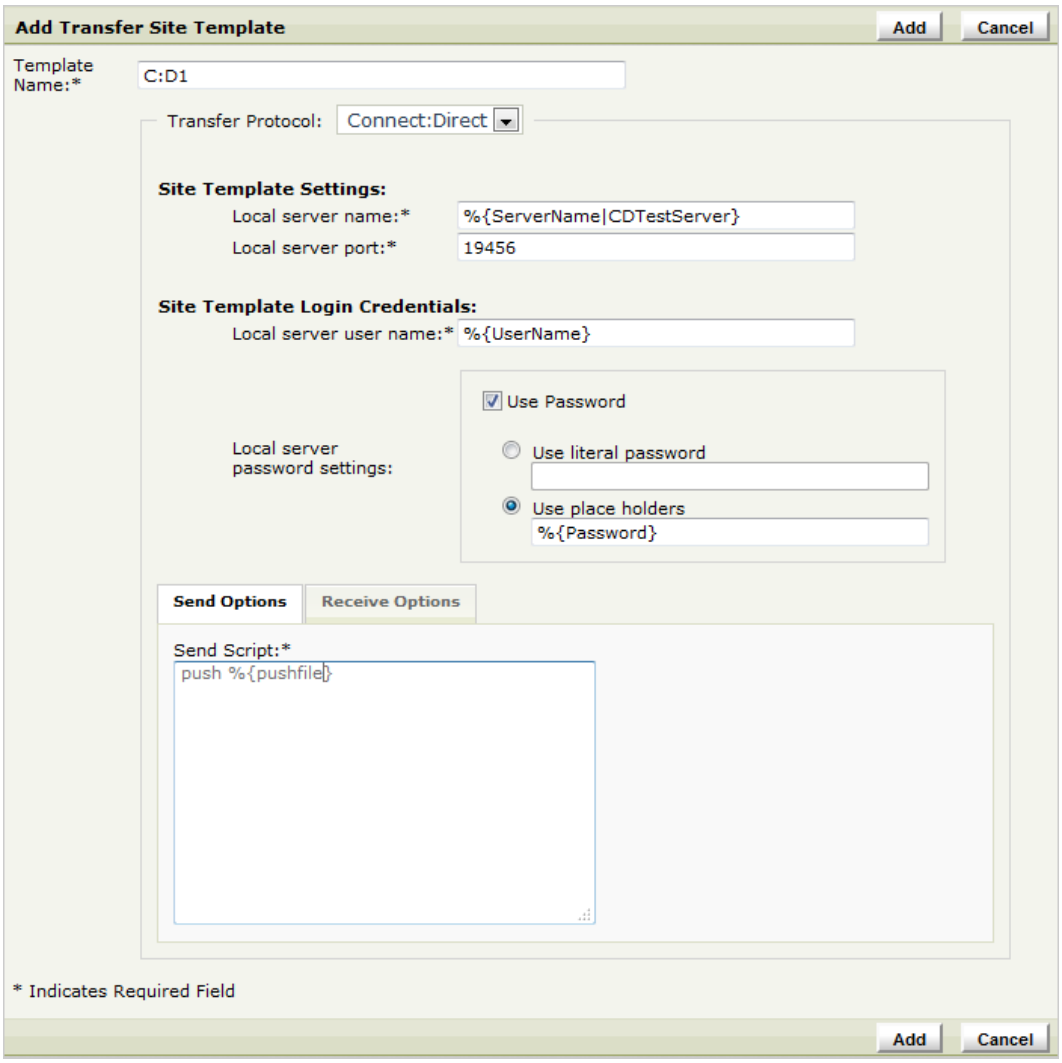
```
%{ServerPort|456}

pull %{pullTransferFile}
```

Note The placeholder parameter cannot include regular expressions.

1. Select **Accounts > Site Templates**.

   The *Site Templates* page is displayed.

2. Click **New Site Template** to create the template.



3. Type a site template name in the **Template Name** field.
4. Select Connect:Direct or the file services interface protocol from the **Transfer Protocol** list.
5. Complete the remaining fields for the transfer protocol you selected.

   Note You can use placeholder parameters or hardcoded values for each field or script. For more information about the fields, see *Connect:Direct transfer sites* on page 505 and *File services interface protocol transfer sites* on page 508.
   All the fields for the site template must have a value or a placeholder parameter.

6. Click **Add** to save the site template. Click **Cancel** to close the page without saving the site template.

Search for a site template

Use the following procedure to search for a site template.

1. Select **Accounts > Site Templates**.

   The *Site Templates* page is displayed.

2. In the *Search* pane, type all or part of a site template name and click **Search**. Wildcards are not accepted.

   All site templates that match the search criteria are displayed.

Note You can use individual characters to search for a template, such as typing a 1 to see all site templates that contain a 1 in the name. If you have site templates named NDM1, 1NDM, and NDM 1, all three site templates are displayed. If you have a fourth site template named NDM2, it is not displayed.

View a site template

Use the following procedure to view a site template.

1. Select **Accounts > Site Templates**.

   The *Site Templates* page is displayed.

2. Click the site template name. The *Edit Transfer Site Template* page is displayed. Use this page to view the site template settings.
3. Click **Save** or **Cancel** to return to the *Site Templates* page.

Modify a site template

Use the following procedure to modify a site template.

1. Select **Accounts > Site Templates**.

   The *Site Templates* page is displayed.

2. Click the site template name. The *Edit Transfer Site Template* page is displayed.
3. Modify any fields you want to change.
4. Click **Save** to return to the *Site Templates* page. Click **Cancel** to close the site template without saving the changes.

Delete a site template

Use the following procedure to delete a site template.

1. Select **Accounts > Site Templates**.

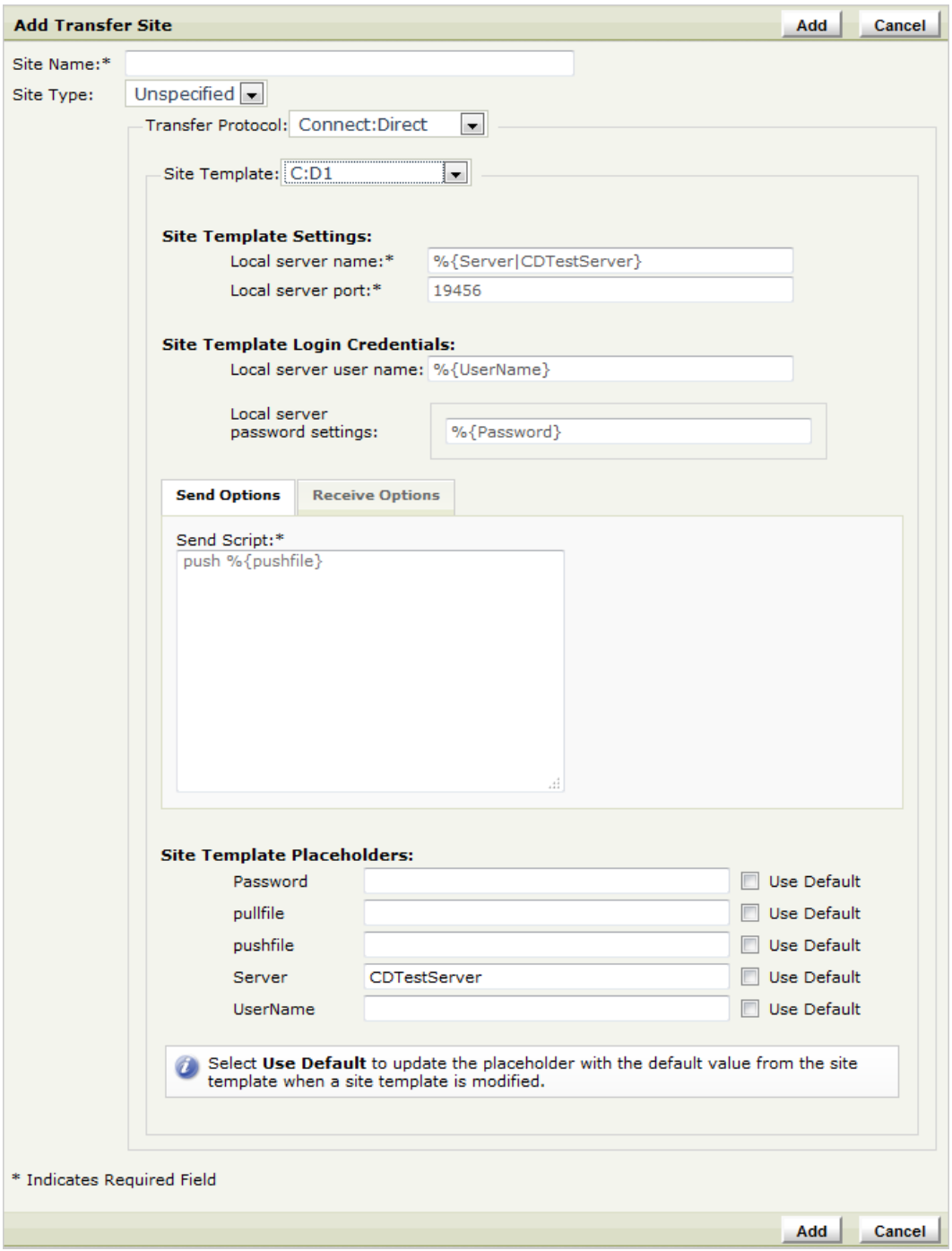
   The *Site Templates* page is displayed.

2. Select one or more site templates.
3. Click **Delete** to remove the site templates. A dialog box displays asking you to confirm the deletion. Click **OK** to continue or **Cancel** to stop.

Use a site template to define a transfer site

Use the following procedure to use a site template to define a transfer site.

1. Create or edit a Connect:Direct or file services interface protocol site as described in *Create a transfer site* on page 598 or *Edit a transfer site* on page 599.
2. In the **Site Template** field, select the site template from the drop-down list.
3. At the bottom of the page, type values for the **Site Template Placeholders**. If a default value was provided by the site template, you can modify it for this account.



(Optional) To have the placeholder default values automatically filled in when the site template is updated, select the **Use Default** check box for one or more placeholder parameters.

When you modify a site template, the changes are automatically applied to all transfer sites that use that template. For example:

- Add or remove a placeholder parameter adds or removes it to or from all associated transfer sites.
- Modify an optional default value of a placeholder parameter updates it in all associated sites that have the Use Default check box selected for that placeholder.
- Delete the default value of a placeholder parameter clears it in all associated sites that have the Use Default check box selected for that placeholder.

4. Click **Add** or **Save** to save your changes and close the *Add Transfer Site* or *Edit Transfer Site* page. Click **Cancel** to close the page without saving your changes.

System users

You can allow users who already have an account on the computer running SecureTransport to log in without creating a SecureTransport account by configuring the settings on the *Password Files* page in the Administration Tool. This page is only applicable for real users in SecureTransport.

The following topics describe real users and provide how-to instructions for managing password files:

- *Real users* on page 687 - Describes real system users.
- *Manage password files* on page 688 - Provides how-to instructions for managing password files.

Real users

Note Real users cannot be granted access to SecureTransport on non-root installations.

Real users are the users defined at the operating-system level. Access rights to the server file system for real users are based on the underlying operating system file access rights. Real users can be defined locally on the server (for instance, on a UNIX-based platform in `/etc/passwd`, or on Windows as a computer-specific local user) or on a network resource (NIS for UNIX or on a domain controller for Windows).

Set a home folder for each real user to ensure that the user is not logged into a randomly-selected directory when logging in to SecureTransport.

Note Real users can view the complete file system of the SecureTransport Server, regardless of the location of the home folder.

The following topics describe real users on UNIX and on Windows:

- *Real users on UNIX* on page 688
- *Real users on Windows* on page 688

Real users on UNIX

UNIX real users are the users defined in `/etc/passwd`, or in NIS. Real users are created at the system level. They can login using `telnet` or `rlogin`, in addition to FTP access only if their rights and permissions give them access.

Real users on Windows

Windows real users are created locally on the server or on the domain controller with the system controls. For Windows Server 2012 R2, Windows Server 2016 and Windows Server 2019, the system controls are accessed through **Control Panel > User Accounts > Add or remove user accounts**.

For more information on Windows users, refer to the Microsoft documentation.

Note Real users set up on the SecureTransport Edge are unable to log into either a SecureTransport Edge or SecureTransport Server. You must create a user account for each real user set up on a SecureTransport Edge to allow log ins.

Note If the account home folder prefix is on a shared network, specify a real user that has access to it. The real user must be part of the domain, not a local user for one of the cluster nodes; otherwise the other nodes in the cluster cannot impersonate it to access the shared location.

Note The specified real user needs to added in a password vault file. For more information, refer to *Add a user to a password vault* on page 690.

When SecureTransport is running on a Windows platform, the *Password Files* page provides an additional option to specify password vaults. A password vault stores user names and passwords of real users on Windows, is used to mimic virtual users on Windows, and is applicable only for Windows. See *Manage password files* on page 688

Manage password files

Use the *Password Files* page to add, enable, disable, and delete password entries for real users.

By default the *Password File List* contains a disabled entry for real users. On a UNIX-based system, you cannot delete this entry or add an entry. On Windows, you can delete the entry for real uses and add password vault entries. SecureTransport stores password vaults in the SecureTransport database.

The following topics provide how-to instructions for managing password files and password vaults:

- *Add password file entry* on page 689
- *Enable or disable password file entries* on page 689
- *Edit a password file entry* on page 689
- *Delete password file entries* on page 690
- *Add a user to a password vault* on page 690
- *Edit a user in a password vault* on page 691

- *Delete users from a password vault* on page 691
- *Purge a password vault* on page 691

Add password file entry

Use the following procedure to a password file entry.

1. Select **Accounts > System**.

   The *Password Files* page is displayed.

2. Click **Add Password File**.

   A new row is displayed in the table.

3. In the **Type** list, select `Real Users` or `Password Vault`.

   Note On UNIX-based platforms, `Real Users` is the only option in the **Type** list. On Windows platforms, there are two options: `Real Users` and `Password Vault`.

4. If you selected `Password Vault`, in the **Location** column, enter a Windows file path for the password vault.

   SecureTransport stores the password vault entries in the database and uses the value of the **Location** field to identify the password vault. SecureTransport does not create a file for the password vault.

5. Click the Save icon ( ) in the last column of the list.

Enable or disable password file entries

Once you have created the password file entry, you can enable it. You can disable entries you want to keep but not use.

1. Select **Accounts > System**.

   The *Password Files* page is displayed.

2. Select the entries to enable or disable.

3. Click **Enable** or **Disable**.

Edit a password file entry

Use the following procedure to edit a password file entry.

1. Click the Edit icon ( ) in the last column of the entry to edit.
2. Make changes in the **Type** or **Location** columns.
3. Click the Save icon ( ) in the last column.

Delete password file entries

If you no longer want to keep the password file entry, you can delete it.

1. Select **Accounts > System**.

   The *Password Files* page is displayed.
2. Select the entries to delete.
3. Click **Delete**.

   SecureTransport displays a confirmation dialog.
4. Click **OK** to delete the entries.

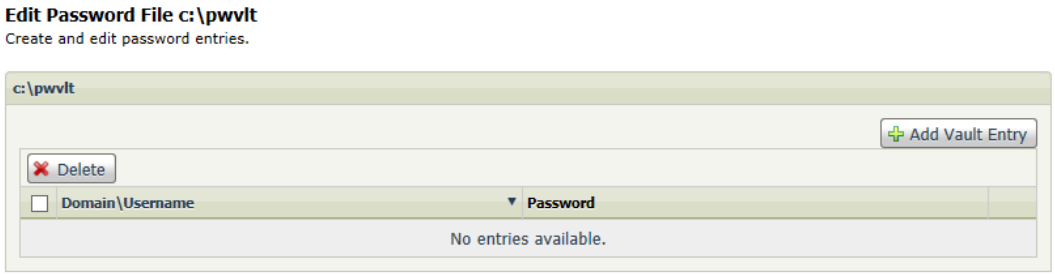
Add a user to a password vault

Use the following procedure to add a user to password vault.

1. Select **Accounts > System**.

   The *Password Files* page is displayed.
2. Click **Edit File** in the **File Action** column for the password vault entry.

   The *Edit Password File* page is displayed.



3. Click **Add Vault Entry**.

   A new row is displayed in the table.
4. In the **Domain\Username** column, type the domain or computer name and user name using one of the following formats:

   Domain\Username or *Computer\Username*

   where *Username* is the valid domain or computer user.
5. In the **Password** column, type the password of the user.
6. Click the Save icon ( ) in the last column of the list.

Note If the password is incorrect, or the specified user does not have the relevant Windows local or domain permissions, the addition of the user fails with an appropriate error message. If the reason is wrong permissions, contact the domain administrator.

Edit a user in a password vault

Use the following procedure to edit a user in a password vault.

1. Select **Accounts > System**.

   The *Password Files* page is displayed.

2. Click **Edit File** in the **File Action** column for the password vault entry.

   The *Edit Password File* page is displayed.

3. Click the Edit icon ( ) in the last column of the user to edit.

4. Make changes in the **Domain\Username** or **Password** columns.

5. Click the Save icon ( ) in the last column of the list.

Note If the password is incorrect, or the specified user does not have the relevant Windows local or domain permissions, the addition of the user fails with an appropriate error message. If the reason is wrong permissions, contact the domain administrator.

Delete users from a password vault

Use the following procedure to delete users from a password vault.

1. Select **Accounts > System**.

   The *Password Files* page is displayed.

2. Click **Edit File** in the **File Action** column for the password vault entry.

   The *Edit Password File* page is displayed.

3. Select the entries to delete.

4. Click **Delete**.

   SecureTransport displays a confirmation dialog.

5. Click **OK** to delete the users.

Purge a password vault

Use the following procedure to purge a password vault.

1. Select **Accounts > System**.

   The *Password Files* page is displayed.

2. Click **Purge File** in the **File Action** column for the password vault entry.

   SecureTransport immediately deletes the password vault from the database and deletes the entry from the *Password Files* page.

Business units

Use business units to encapsulate certain information necessary for transfers into a single entity. When you create accounts and templates, you can specify a business unit to represent a particular set of information about the transfer. When you create a delegated administrator, you can specify business units (including users assigned to that business unit) to be managed by the delegated administrator. For more information, see *Delegated administration* on page 651.

The information contained in a business unit includes business unit name, base folder, a parent business unit, whether administrators are allowed to modify the base folder or the home folder, and which HTML template to use when users belonging to this business unit log in using the web client.

The following topic describes how to manage business units:

- *Manage business units* on page 692 - Provides how-to instructions for managing business units.

Manage business units

Use the *Business Units* page to display a list of business units, search the list, delete business units, and invoke the editing process.

Use the *Business Units Settings* page to edit settings for a business unit.

Note Only master administrators and delegated administrators with permissions for managing business units can create and delete business units and modify business a business unit's properties.

The following topics provide how-to instructions for managing business units:

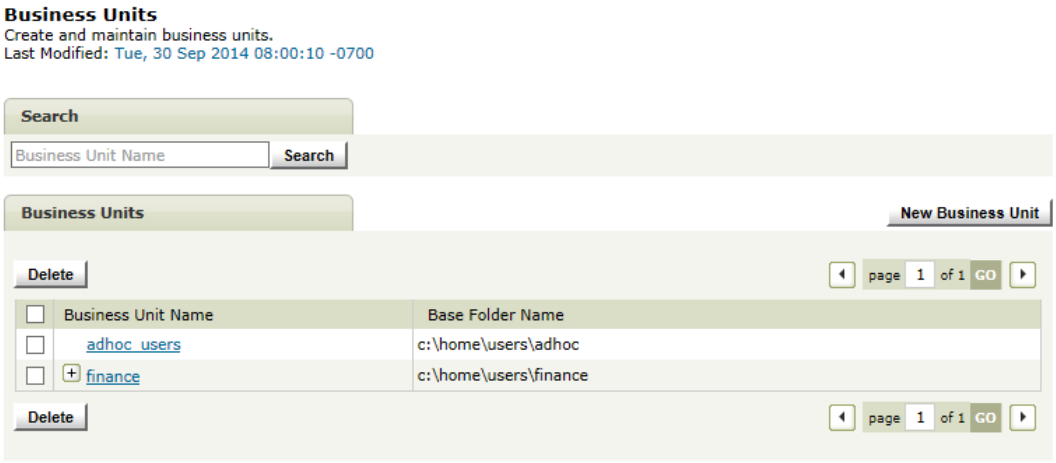
- *Display a list of business units* on page 692
- *Create or edit a business unit* on page 693
- *Delete a business unit* on page 700

Display a list of business units

Use the following procedure to display a list of business units.

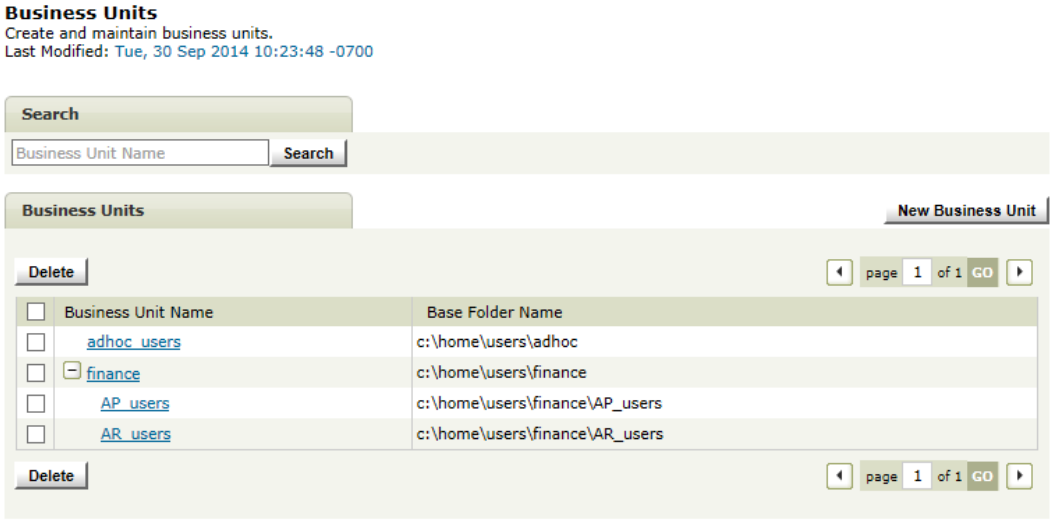
1. Select **Accounts > Business Units**.

   The *Business Units* page is displayed. Business units that have child business units associated with them are called *parent business units* and are displayed with a plus sign (+).



2. (Optional) To display child business units, click the plus sign next to a parent business unit.

   The child business units are displayed under their respective parent units.



Note Delegated administrators do not see business units as parents and children. All business units associated with a delegated administrator are displayed at the same level on the page.

Create or edit a business unit

Use the following procedure to create or edit a business unit.

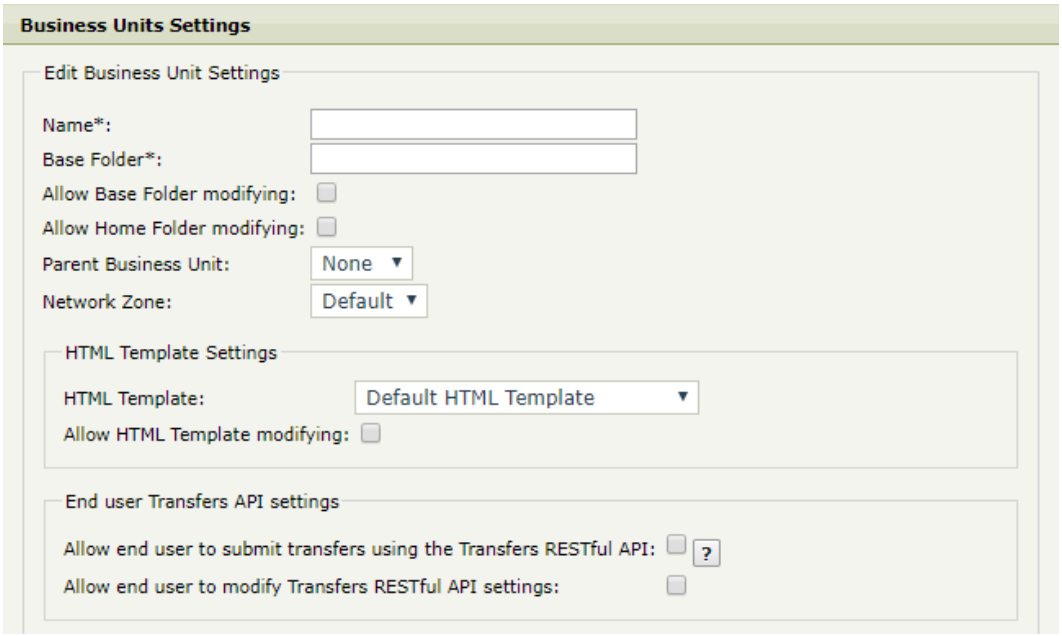
1. Select **Accounts > Business Units**.

   The *Business Units* page is displayed.

2. Click **New Business Unit** or click the name of the business unit you want to edit.

   The *Business Units Settings* page is displayed.

Note The *Address Book Settings* pane is only displayed if the Address Book feature is enabled (the value of the `AddressBook.Enabled` configuration option is set to **true**).



3. If you are creating a business unit, enter a value in the **Name** field.

   Note Business unit names are not case sensitive.

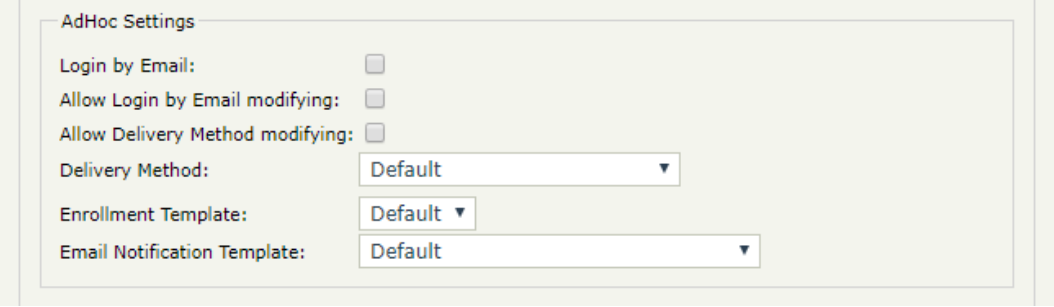
4. In the **Base Folder** field, specify a folder that is to contain the home directories of new accounts belonging to this business unit.
5. Select the **Allow Base Folder modifying** check box to allow administrators to change the base folder when creating an account.
6. Select the **Allow Home Folder modifying** check box to allow administrators to change the account name suffix when creating an account.
7. In the **Parent Business Unit** drop-down list, select the name of the parent business unit. If you do not want this business unit to be a child, select `None`, the default.

   Note If the Business unit assigned to Delegated Administrator has child Business unit, the child Business Unit will be also assigned to this Delegated Administrator. If Business unit does not have child, but another Delegated Administrator adds child, the newly added child will be automatically assigned to the first Delegated Administrator. If the child Business Unit is removed from the parent Business Unit but continues to exist, the Delegated Administrator will not be linked anymore.

8. In the **Network Zone** field, select the network zone that defines the public URL prefix for users in this business unit.
   - Select **Default** to use the setting in the default network zone.
   - Select a specific network zone to use the setting defined for that zone.

For more information, see *Manage the communication across Transaction Manager, protocol and proxy servers* on page 218.

9. *HTML Template Settings*: from the **HTML Template** drop-down, select the HTML template you want to use for accounts and account templates that belong to this business unit.
10. Select the **Allow HTML Template modifying** check box to allow administrators to change the HTML template when editing or creating an account for this business unit.
11. *End user Transfers API settings*: select **Allow this account to submit transfers using the Transfers RESTful API** to enable calls from the SecureTransport REST file transfer API authenticated with the credentials from accounts in the business unit. When this option is selected, the account will be allowed to trigger server initiated transfers using the Transfers RESTful API resource and retrieve the tracking information for these transfers.
12. Select **Allow end user to modify Transfers RESTful API settings** to allow a delegated administrator to modify this fields for users in the business unit.
13. Select **Login by email** to allow users in the business unit to log in using the value of the **Email Contact** field as well as the **Login Name**. A user of one of the Axway Email Plug-ins must be able to login by email.

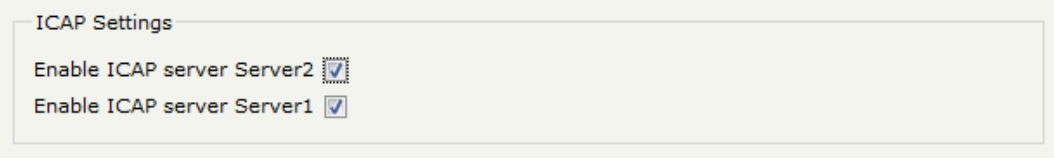


14. *AdHoc Settings*: select the **Allow Login by Email modifying** check box to allow administrators to change the **Allow this account to login by email** field when editing or creating an account for this business unit.
15. Select the **Allow Delivery Method modifying** check box to allow administrators to change the delivery method values when editing or creating an account for this business unit.
16. The **Delivery Method** value controls the options that ST Web Client displays in the *User Access* window.
    - **Disabled** – The user cannot send files using ad hoc file transfers.
    - **Default** – Use the delivery method specified in the account template, if any, or in the **Default Package Delivery Method** field of the *AdHoc Setting* page.
    - **Anonymous** – The sender can choose Anonymous or Challenge.
    - **Account Without Enrollment** – The sender can choose Anonymous, Challenge, or Existing Account.
    - **Account With Enrollment** – The sender can choose Anonymous, Challenge, Existing Account, Enroll Unlicensed, or Enroll Licensed.
    - **Custom** – Select the allowed enrollment types in the **Enrollment Types** field. The sender can chose any of the selected enrollment types.

17. For a custom delivery method, select one or more allowed enrollment types in the **Enrollment Types** field:
    - **Anonymous** – The ad hoc file recipient receives a link to retrieve the files and is not enrolled as a user. The ST Web Client option is **Send attachment link only**.
    - **Challenge** – The ad hoc file recipient receives a link and must answer correctly a challenge question specified by the sender to retrieve the files. The recipient is not enrolled as a user. The ST Web Client option is **Protect attachment link with security question**.
    - **Existing Account** – Do not enroll ad hoc file recipients. Only existing users can receive files. The ST Web Client option is **Send to existing users only**.
    - **Enroll Unlicensed** – If the ad hoc file recipient does not have a user account, the recipient must enroll and create an account before retrieving the files. The ad hoc file recipient becomes an unlicensed user who can only reply once to the email and retrieve the files. Other user attributes are defined by the enrollment template. The ST Web Client option is **Allow recipients to enroll as new Unlicensed Users**.
    - **Enroll Licensed** – If the ad hoc file recipient does not have a user account, the recipient must enroll and create an account before retrieving the files. The ad hoc file recipient becomes a SecureTransport user with all the attributes specified in the default enrollment template. The ST Web Client option is **Allow recipients to enroll as new Full Licensed Users**.
18. The **Implicit Enrollment Type** value controls which option ST Web Client selects initially in the *User Access* window and which enrollment type is used by the Axway Email Plug-ins. The choices depend on the enrollment types enabled by the **Delivery Methods** and **Enrollment Types** fields.
19. Select the **Enrollment Template** for this business unit. When a user is enrolled based on an ad hoc file transfer from a user in this business unit, the selected account template is used. You specify the default enrollment template on the *AdHoc Settings* page.
20. Select the **Email Notification Template** for this business unit. When a user is enrolled based on an ad hoc file transfer from a user in this business unit, the selected email notification template is used. You specify the default enrollment template on the *AdHoc Settings* page.
21. *Shared Folders Settings*: select the **Allow Shared Folders collaboration** check box to allow shared folders collaboration. This option is inherited from the business unit by the children of the business unit. When checked user accounts may collaborate using, creating, and sharing folders based on the following criteria:
    - If the user accounts are not in the same BU but they have common ancestor then the business unit setting of the lowest common ancestor is used for deciding if sharing is allowed or not.
    - If the user accounts are in one and the same business unit then the shared folder setting of the business unit is used for deciding if sharing is allowed or not.
    - If the user accounts have business units assigned but there is no common ancestor then the global setting is used for deciding if sharing is allowed or not. Refer to *View and change server configuration parameters* on page 315 for information on setting global parameters.

- If the owner account or the collaborator account (or both of them) has no assigned business unit then the global server setting is used for deciding if sharing is allowed or not. Refer to *View and change server configuration parameters* on page 315 for information on setting global parameters.

22. *ICAP Settings*: to enable of disable ICAP servers for a specific Business Unit, select **Enable ICAP scan with server 'servername'**, from the list of all ICAP servers in the **ICAP Settings**, and the specified ICAP server will be enabled for this particular Business Unit.
Note: Importing Legacy Business Unit Accounts (from any version before 5.4) will not import the Business Unit ICAP server selection/s. They must be manually activated after the import.



For ICAP server configuration information, refer to *ICAP settings* on page 187.

23. In the *File Archiving Settings* pane:
    a. Select the **File archiving policy** from the menu.
        - When **Default** is selected, business unit inherits either its parent's policy or the global archiving policy if it is a top level business unit.
        - When **Enabled** is selected, file archiving will be enabled for all accounts from this business unit.
        - When **Disabled** is selected, file archiving will be disabled for all accounts from this business unit.

            Note This option will be disabled if the **Enable File Archiving** option from the global *File Archiving* page is turned off.

    b. Select **Allow File archiving policy modifying** to enable modification of file archiving policy at the account level.
        - When **checked**, all the accounts that are assigned to this business unit can have their own file archiving policy.
        - When **unchecked**, the corresponding option in account settings page will be disabled and accounts will inherit business unit policy.

            Note This option will be disabled if the **Enable File Archiving** option from the global *File Archiving* page is turned off.

    c. Select the **Archive Folder** from the menu.
        - When **Default** is selected, the business unit inherits either its parent's folder or the global archiving folder if it is a top level business unit.
        - When **Custom** is selected, the business unit defines its archive folder.

            Note When you select this option, you must also provide archive folder absolute path.

Note This option will be disabled if the **Enable File Archiving** option from the global *File Archiving* page is turned off.

d. Select the **Encryption certificate** from the menu. The encryption certificate must be a local x.509 certificate. For information on adding local certificates, refer to *Manage local certificates and certificate signing requests* on page 54.

- When **Default** is selected, the business unit inherits either its parent's encryption certificate or the global encryption certificate if it is a top level business unit.
- When **Disabled** is selected, archived files for accounts in this business unit won't be encrypted.
- When **Custom** is selected, a dedicated encryption certificate can be selected for this business unit.

Note This option will be disabled if the **Enable File Archiving** option from the global *File Archiving* page is turned off.

Note The certificate cannot be deleted or overwritten when it is in use.

Note When you delete or overwrite a certificate which previously was used for encryption, all files encrypted with this certificate will be useless and cannot be restored.

e. Select the **Maximum file size to archive** from the menu.

- When **Default** is selected, business unit inherits either its parent's policy or the global file size limit policy if it is a top level business unit.
- When **Enabled** is selected, file size limit will be enabled for all accounts from this business unit.
- When **Disabled** is selected, file size limit will be disabled for all accounts from this business unit.

24. (Optional) When the Address Book feature is enabled, the *Address Book Settings* pane is displayed. To configure the business unit Address Book settings:

a. Select the Address Book source.

- **Default** - The business unit inherits either its parent's Address Book policy or the global Address Book policy if it is a top level business unit.
- **Custom** - A custom Address Book policy configuration will be set for this business unit only and the following will be configurable:
  1. Enable or disable Address Book sources for the business unit.
  2. Specify the parent groups for Address Book sources.
  3. Specify the domain for LDAP Address Book sources.
  4. Specify **All Business Units** or **User's own business unit** for local and custom Address Book sources.
- **Disabled** - The Address Book policy is set to disabled for this business unit.

b. Specify whether or not to Allow collaboration with non-Address Book recipients. If Address Book functionality is disabled, this setting does not affect user collaboration.

- When **checked**, accounts that use the Address Book policy defined on the business unit level will be allowed to send email packages and share folders with users that do not exist the defined Address Book.
- When **unchecked**, accounts that use the Address Book policy defined on the business unit level will be allowed to send email packages and share folders only with users that exist in the defined Address Book.

This business unit setting overrides the global Address Book policy setting for collaboration. This setting can be overridden on the account level if **Allow modifying of the 'Allow Address Book Collaboration' setting** is checked.

c. Specify whether or not to allow modification of the **Allow modifying of the Collaboration setting** setting.

- When **checked** accounts that use the Address Book policy defined in this business unit will be allowed to override the **Allow Address Book collaboration** setting specified here.
- When **unchecked** accounts that use the Address Book policy defined in this business unit will be not allowed to override the **Allow Address Book collaboration** setting specified here.

d. Specify whether or not to allow Address Book source settings modifying.

- When **checked** accounts that use the Address Book policy defined in this business unit will be allowed to override the Address Book Sources specified here.
- When **unchecked** accounts that use the Address Book policy defined on business unit will be not allowed to override the Address Book Sources specified here.

For additional Address Book business unit level configuration information, refer to refer to *Address Book business unit level configuration* on page 239.

25. In the *Login Restriction Policy* pane:

a. Select the **Business Unit Login Restriction Policy** from menu.

If None (No Restriction) is selected, the Global Login Restriction Policy (if configured) is the default Business Unit Login Restriction Policy.

If one of the configured Login Restriction Policies is selected, it becomes the default Business Unit Login Restriction Policy.

b. Select **Allow Login Restriction Policy modifying** to enable modifying of the Login Restriction Policy at the account level.

26. In the *Bandwidth limits* pane:

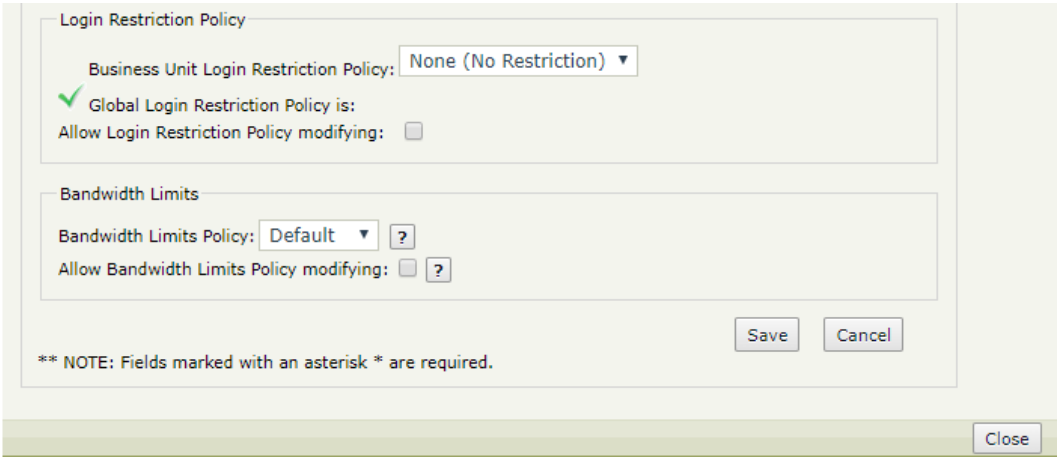
a. Select a **Bandwidth Limits Policy** to apply:

- Default – the current business unit inherits its bandwidth limits from the parent business unit or the global bandwidth
- Custom – the panel expands with two additional options for you to configure: **Inbound limit**

and **Outbound limit** (both values in kb/s per user)

- Disabled – no bandwidth limits are applied to the users assigned to the current business unit

b. Select **Allow Bandwidth Limits Policy modifying** and the bandwidth limits on the account template and accounts level will be applicable to the accounts assigned to the current business unit. Deselect this option and bandwidth limits on the account template and accounts level will not override the business unit bandwidth limits.



27. Click **Save**.

Delete a business unit

Use the following procedure to delete a business unit.

1. Before you delete a business unit, make sure that it is not associated with any account, administrator, application, or route and that it does not have any child business units.
2. Select **Accounts > Business Units**. The *Business Units* page is displayed.
3. Using the check boxes, select the business units to delete. To select or clear all the check boxes, select or clear the check box in the table header.
4. Click **Delete**. A confirmation window is displayed.
5. Click **OK** to delete the selected business units.

Display active users

Users who log in to the SecureTransport client are called *active users*. Use the *Active Users* page to view and search a list of the active users.

1. Select **Accounts > Active Users**.

   The Active Users list is displayed. A line for each user includes the user login name, the last time the user sent an ad hoc file transfer, and the last time the user accessed the server.

2. In the *Search* pane, enter a user login name and click **Search**.

Users that match your search criteria are displayed.

Note You can get the current number of active users by using REST API.

Client-initiated and server-initiated transfers

You can use SecureTransport to set up and execute server-initiated transfers. There are four types of transfers:

- **Client-initiated downloads** – A client application "pulls" a file from the SecureTransport Server.
- **Client-initiated uploads** – A client application "pushes" a file to the SecureTransport Server.
- **Server-initiated downloads** – The SecureTransport Server "pulls" a file from a remote server.
- **Server-initiated uploads** – The SecureTransport Server "pushes" a file to a remote server.

Client- and server-initiated transfers can be performed using any supported protocol. The protocol servers that handle client-initiated transfers run on the SecureTransport Server or on the SecureTransport Edge in the perimeter network (DMZ). The protocol clients that perform the server-initiated transfers run on the SecureTransport Server in the Transaction Manager server JVM and can connect out through a SOCKS5 Proxy on a SecureTransport Edge or through an HTTP proxy to a remote system. This allows the protocol clients to have direct access to the file system.

Note If the X509v3 certificate of your remote server contains extended key usage field, make sure it is configured to 'TLS Web Server Authentication'. Server-initiated transfers will always fail if the remote server certificate is configured with a X509v3 Extended Key Usage of 'TLS Web Client Authentication'.

Server-initiated transfers can be triggered by any of the following events, depending on the configuration of the transfer:

- A Folder Monitor
- A scheduler
- The arrival of a file

In addition to the protocols mentioned above, the Folder Monitor can be used for inbound and outbound file transfers.

- For outbound transfers, SecureTransport can copy the files to a specified folder.
- For inbound transfers, SecureTransport can monitor the folder for newly arrived files and use the event to trigger an application executing specific tasks.

Any server-initiated transfer requires an account to be subscribed to an application based on one of the application types: Standard Router, Site Mailbox, Shared Folder, Basic Application, File Transfer via File Service Interface, Human to System, or Advanced Routing. For detailed information about application types and applications, see *Applications* on page 756.

Note When setting up a server-initiated outbound transfer, make sure that the target folder exists. SecureTransport does not create the target folder on the remote system automatically.

The following topics describe managing client-initiated and server-initiated transfers:

- *Transfer mode for server-initiated transfers* on page 702
- *Transfer multiple files* on page 702
- *Configure retry parameters for server-initiated transfers* on page 703
- *Outgoing connections* on page 703
- *Authentication methods* on page 703
- *Server authentication* on page 704
- *Limitations for server-initiated transfers* on page 704
- *Encryption and server-initiated transfers* on page 705

Transfer mode for server-initiated transfers

Transfer mode for server-initiated transfers is determined by protocol and file content type.

For AS2, transfer mode is always binary. For all other protocols, including FTP(S), HTTP(S), and SFTP, SecureTransport uses the content-type of the file name to determine whether a transfer is text (ASCII) or binary (IMAGE).

If the content type is `text`, the file is transferred as text. If the content-type is not text, the file is transferred as binary.

Content-type is determined based on the file name extension. The default mapping for file name extension to content-type is stored in the file, `<FILEDRIVEHOME>/conf/mime.types`. Use the *Server Configuration* page to edit this file to change or add entries.

Transfer multiple files

SecureTransport allows a server-initiated transfer job to process a single file, a set of multiple files specified using wildcards in the file name, or a directory.

Note Except for with Folder Monitor type applications, wildcards in directory names and recursive directory traversal are not supported.

A single transfer request for transferring multiple files is defined at the beginning of the transfer process only. If the number of files happens to change during the transfer process, these changes are not reflected and the transfer of these additional/missing files or directories fails.

The SecureTransport system keeps track of the status of all the individual transfers. If a transfer fails, it is rescheduled for a later point in time until the retry limit value is exceeded.

Configure retry parameters for server-initiated transfers

When a server-initiated transfer fails, SecureTransport can automatically retry the transfer. By default, SecureTransport is configured to retry such a transfer five times at two-minute intervals. You can configure the retry count and interval by editing parameters on the *Server Configuration* page:

- `EventQueue.maxRetryCount` – The number of times SecureTransport retries a transfer. The default value is `5`.
- `EventQueue.retryDelayInterval` – The time in seconds that SecureTransport waits after a transfer fails before retrying it. The default value is `120`.
- `EventQueue.internalRetryDelayInterval` – The time in seconds that SecureTransport waits when a transfer cannot be started (for example, because all outbound connection to an FTP server are in use) before retrying it. The default value is `120`.

Outgoing connections

You can proxy outgoing connections using a SOCKS5 proxy running on a SecureTransport Edge or an HTTP proxy. You configure the use of a proxy by defining one or more network zones and making a selection in the transfer site. See *Manage the communication across Transaction Manager, protocol and proxy servers* on page 218 and the procedures for defining AS2, FTP, HTTP, PeSIT, and SSH transfer sites.

Note By default, when a proxy is configured, direct connections from the SecureTransport Backend are not permitted even in when the proxy is unreachable. To change the default behavior, set `Direct.Connection.When.Proxy.Down` server configuration parameter to **true**. For information on changing server configuration parameters, refer to *View and change server configuration parameters* on page 315.

If server-initiated transfers being performed using FTP(S) are passing through the SOCKS5 proxy, increase the value of the `Socks.Idle.Timeout` server configuration parameter on the SecureTransport Edge from 600000 to 7200000 milliseconds. This prevents the FTP control connection from timing out during the transfer. You must restart the SOCKS5 proxy server for this change to take effect.

Authentication methods

The following authentication methods are valid for connecting to a remote site for the different protocols.

Protocol	Authentication method
AS2	(no authentication)

Protocol	Authentication method
FTP	User name + password User name + password + certificate User name + certificate
HTTP	User name + password User name + password + certificate User name + certificate Certificate
SSO	User name + password (for more information see SSO Limitations)
PeSIT	(no authentication) User name + password User name + password + certificate User name + certificate
SSH	User name + password User name + password + SSH key User name + SSH key

Note If dual authentication is enabled, the key and password are required. If user classes are specified in Specific user classes, the key and password are required only for the specified classes.

You can configure the user name and password in the proxy configuration in a network zone node. See *Specify proxy settings in a network zone* on page 222.

Server authentication

SecureTransport provides an option to turn on the target server authentication for server-initiated transfers. This server-wide option is turned on by default and can be turned off using the *Transfer Sites* pane for a user account. For details, see *Manage transfer sites* on page 597.

To manage the list of trusted certificates for server authentication, use the *Certificates* page, accessible from the **Setup** menu in the Administration Tool. For details, see *Certificates* on page 50.

Limitations for server-initiated transfers

SecureTransport has the following limitations for server-initiated transfers:

- SecureTransport Server supports server-initiated transfers over HTTP only to remote sites running on another SecureTransport Server.
- Server-initiated transfers over FTPS from a streaming configuration with SecureTransport Edge to remote sites support only passive connection mode.

- When performing server-initiated uploads using the SSH protocol SecureTransport cannot always identify the remote operating system when the remote SSH server has version 3 or less.

  For ASCII mode SSH transfers, if the remote SSH server supports the newline (newline@vandyke.com) extension, SecureTransport correctly converts the end-of-line characters of the file.

  If the remote SSH server does not support the newline extension, SecureTransport can be configured to convert the end-of-line characters during server-initiated uploads based on the value of server configuration parameters. If the value of the `Ssh.EndOfLineConversion.enabled` server configuration parameter is true, SecureTransport uses the value of the `Ssh.EndOfLineConversion.type` server configuration parameter as the end-of-line sequence. Valid values are: `0x0A` (LF), `0x0D` (CR), and `0x0D0A` (CRLF). By default, the value of `Ssh.EndOfLineConversion.enabled` is `false` and the value of `Ssh.EndOfLineConversion.type` is `0x0D0A`.

  Whether or not the remote SSH server supports the newline extension, the remote server sees these transfers as BINARY mode.

  In all other cases of ASCII mode SSH server-initiated uploads and downloads, SecureTransport cannot identify the correct end-of-line characters to use. SecureTransport performs these transfers in BINARY mode and indicates this on the *File Tracking* page.

- The name of a file processed by a Folder Monitor transfer site cannot contain two or more of the following characters in sequence: `< > | : ? " * / \ % [ ] ~` (at the beginning of the file only).

Encryption and server-initiated transfers

When SecureTransport performs server-initiated transfers, it defines user classes by UID and GID only – no user name is specified. As a result, if you use `EncryptClass` for encrypting or decrypting transferred files and `EncryptClass` is defined only by user name, the following is true:

- Encrypted files transferred using a server-initiated upload are decrypted before the start of the transfer.
- Files transferred using a server-initiated download are transferred with encryption.

Access control 11

Use the Axway SecureTransport **Access** menu to configure how SecureTransport performs access control. Access control defines and restricts the rights of individuals to obtain data from, or place data onto, a storage device. Also, access control defines and restricts the rights of individuals to login. Access control changes are copied to all SecureTransport Servers in your Enterprise Cluster (EC).

Note If your SecureTransport deployment includes SecureTransport Edge servers in a peripheral network (DMZ), you must configure all the settings under the **Access** menu that are applicable to SecureTransport Edge exactly the same on both SecureTransport Edge and SecureTransport Servers.

The following topics describe the various methods to control access to SecureTransport:

- *User classes* on page 710
- *Secure Socket Layer access* on page 718
- *Virtual groups* on page 721
- *Filesystem restrictions* on page 723
- *Upload restrictions* on page 727
- *Download restrictions* on page 732
- *FTP command restrictions* on page 736
- *Protocol server access control* on page 738
- *User limits* on page 743
- *User and group access* on page 746
- *Login restrictions* on page 747

Pluggable authorization

SecureTransport Pluggable 0uthorization feature provides the option to add custom authorization logic by plugging it to the system. Existing SecureTransport Access Restrictions will be executed after any custom authorization logic. The FTP protocol is an exception, where the internal restrictions will be applied before the custom logic. Custom authorization will be applied for all protocols on client-initiated transfers.

SecureTransport will be executing any custom authorization on the following operations:

- Upload a file
- Download a file
- List content of a directory
- Change permissions (file or directory)

- Rename a file
- Delete a file
- Create a directory
- Delete a directory

The custom authorization attempt can be either successful or unsuccessful.

In case of success, SecureTransport will continue executing the set of applied Access Restrictions (if any). In case of authorization failure, the operation will not be executed.

Pluggable authorization also supports file filtering capabilities. All plug-in implementations are able to use SecureTransport specific environment data described in the Developer's Guide.

Before your custom plug-in can be configured and used, it must be deployed, registered, and then enabled in the Server Configuration.

Plug-in deployment

The custom authorization logic (plug-in) is packaged as .jar file that follows the set of conventions described in the Developer's Guide.

To deploy an authorization plug-in, place its JAR file in the `/<st_dir>/plugins/authorization/` directory, and restart the Admin and the TM daemons.

In a cluster environment, the plug-in should be deployed on all nodes, and the Admin service and the TM - restarted on all nodes.

Note The plug-in is applicable only on SecureTransport Server installation.

Plug-in registration

SecureTransport identifies the plug-in by the name of its JAR file. Plug-ins are discovered and registered at the Admin daemon start. Each authorization plug-in is added to the following configuration registry in the *Server configuration* page:

```
Plugins.Authorization.Registry
```

If the plug-in has a custom configuration, it is also added to the server configuration for the end users in the following format:

```
Plugins.Authorization.<plugin_name>.<config_option>
```

Note The plug-in configuration options are exported upon server configuration export. Before importing a server configuration with custom plug-in configuration options, the relative plug-ins must be deployed. Otherwise, their configuration options will not be imported.

Plug-in activation

After being registered, the authorization plug-ins are added to the Server Configuration, but they are disabled (have a hash symbol in front of their names). SecureTransport will not automatically activate a newly registered plug-in. To activate a plug-in, remove the # symbol from its name.

Only one authorization plug-in can be enabled at a time.

Note Plug-in activation does not require service restart.

Plug-in management

To undeploy a plug-in:

1. Delete the JAR file from the `/<st_dir>/plugins/authorization/` directory.

2. Restart the Admin and TM daemons.
The plug-in name is then removed from the registry along with its configuration options.

When you uninstall SecureTransport, the plug-ins JAR files are also removed.

To redeploy or update a plug-in:

1. Undeploy the existing plug-in.

2. After the Admin and TM daemon restart, go to the Server Configuration registry and make sure the plug-in is not present.

3. Deploy the new plug-in (version).

After the restart, the new plug-in is added to the authorization plug-in list.

Plug-in configuration

Successful plug-in usage depends on the plug-in implementation (check the Developer's guide for more details).

If you set up a Standard Cluster, and the steps in the Plug-in deployment section are not accomplished, this will not be considered as a correct configuration.

For example, in a Standard Cluster, if the jar file is not uploaded to the secondary node, the configuration will not be considered correct, and an error message will be displayed in the Server Log at startup.

Plug-in authorization notifications

On each of the operations authorized by a plug-in, the following messages are displayed in the Server log:

- On an INFO level: "Custom authorization plug-in <plugin_name> execution for <type_of_ operation> operation finished and it took: <estimated_execution_time> ms.”
- Custom authorization result:
    - On success, on a DEBUG level: "<plugin_name>'s with class <plugin_authorizer_impl> authorization successful. Result is <result_exitcode>, '<result_message>'"
    - On failure, on an INFO level: "<plugin_name>'s with class <plugin_authorizer_impl> authorization failed. Result is <result_exitcode>, '<result_message>'"
- On an Error level, when exception is thrown from the executing of any of the plug-in.

Note All data sent/ received to/from a plug-in will be available on a DEBUG log level.

Plug-in authorization considerations and special cases

The following considerations must be taken into account:

- Custom authorization plug-ins will be executed for client-initiated transfers only.
- Authorization will be executed for all protocols on any supported and applicable operation. Therefore, some protocols may not support particular operations (For example, directory listing) and the plug-in’s implementation will not be executed.
- For pluggable authorization, server-initiated transfers are out of the scope. However, if performing such transfers on one host only with a deployed plug-in (or in two hosts which both have plug-ins deployed), half of the transfer will be authorized against the plug-in. For one of the parties such transfer always appears (and it is) as a true client-initiated transfer since the SecureTransport protocol daemons receive a remote connections and perform user operations as it is in an ordinary client upload/download.
- Custom authorization will be executed before any internal SecureTransport upload/download/filesystem restrictions. An exception is the FTP protocol, where the internal SecureTransport restrictions are evaluated before the custom authorization.
- Advanced Routing transformation steps will not trigger custom authorization.
- Publish To Account routing step is excluded from custom authorization.
- Send To Partner routing step will be authorized in the receiving party if any custom plug-ins are deployed.

Plug-in file filtering capabilities

In addition, custom authorization supports plugging an implementation for filtering of directory content. Use this feature to restrict the view of some files for a particular user. Refer to the Developer's guide for more information regarding the file filtering extension.

Note Filtering is not applied for the directory content in **Mailbox** section in SecureTransport Web Client.

User classes

User classes define sets of SecureTransport users who share characteristics and privileges.

Use user classes to define the following access restrictions:

- SSL encryption
- Filesystem, upload and download
- FTP command
- Server
- User limits

You might also define user classes to support the following SecureTransport functions:

- The *Server Usage Monitor* page reports usage information by user class.
- On the *Setting* page, you define a FTP passive mode address rules for a user class.
- On the *Command Logging* page, you enable logging for a user class.
- On the *Transfer Logging* page, you enable logging for a user class.
- When you create an LDAP domain, you can define a DN filter for a user class.
- On the LDAP *Home Folders* page, you define the home folder prefix for a user class.
- When you create an account template, you specify the user class SecureTransport applies it to.
- You define a user class named `EncryptClass` to enable repository encryption for users.

To determine the user class for a user, SecureTransport evaluates the criteria for each user class in the sequence and puts the user in the first class that matches.

User classes are defined by the following values:

- **User type** – The user type can be *real*, *virtual*, or either
- **User name** – The user's login name
- **User group** – The account group for the user
- **From address** – The IP address or host name from which the user connects
- **Custom expression** – An expression comprised of values of SecureTransport user attributes and LDAP attributes as well as SSO attributes, constant values and patterns using arithmetic, comparison, string matching, logical, and conditional operations

You can use wildcard characters to define patterns in the **User name**, **User group**, and **From address** fields. Question mark (`?`) matches one character and asterisk (`*`) matches any string of characters.

Configure user classes on SecureTransport Server only.

The following topics describe and list the default user classes and custom expressions. The also provide how-to instructions for managing user classes.

- *Default user classes* on page 711
- *Custom expressions* on page 711
- *Manage user classes* on page 714

Default user classes

SecureTransport provides the following default user classes:

- **RealClass** – all users of type real, connecting from any host address (`*`)
- **VirtClass** – all users of type virtual, connecting from any host address (`*`)

If not other user classes are defined, all users are in one of the default user classes. You can use these user classes to create access and security settings. For example, you can prevent virtual users from uploading documents to the server. To define more specific access and security settings more specific sets of users, create custom user classes.

Note Classes that match Single Sign-On (SSO) accounts cannot be used with users with type Real.

Custom expressions

You can use the **Custom expression** field to define the user class based on the values of the following SecureTransport user and LDAP attributes.

The following user attributes are supported:

- `fdxUid` – User ID (UNIX-based systems only)
- `fdxGid` – Group ID
- `fdxHomeDir` – Home folder
- `fdxUserType` – User type
- `fdxShell` – User shell (UNIX-based systems only)
- `fdxSysUser` – Name of a local or domain user of the Windows server whose credentials SecureTransport uses to access the Windows files in the session (Windows only)
- Any custom SecureTransport user attribute defined in the LDAP domain. See *Define attribute mappings for a domain* on page 441.

The following variables that represent values from the SecureTransport LDAP domain that are supported:

- `LDAP_DOMAIN_ID` – Internal ID
- `LDAP_DOMAIN_NAME` – Value of the **Domain Name** field
- `LDAP_DN` – Value of the **Base DN** field
- `LDAP_AUTH_BY_EMAIL` – Value of the **Login by Email** field, `0` for `Disabled`, `1` for `Enabled`

The following variables that represent SSO values for SecureTransport that are supported:

- `SSO.idpId` – Identity provider Identification.
- `SSO.email` – SSO user email.
- `SSO.uid` – UID of the SSO user.
- `SSO.gid` – GID of the SSO user.
- `SSO.tenant` – SSO tenant.
- `SSO.homeDir` – Home directory of the SSO user.
- `SSO.userName` – SSO user username.

Note `UID`, `GID`, `Email` and `homeDir` SSO attributes should be mapped to SecureTransport as `fdxUid`, `fdxGid`, `fdxEmail`, `fdxHomeDir` attributes respectively.

The following variables that represent values from an already authenticated user in SecureTransport are supported:

- `DXAGENT_USERGID` - GID of the user
- `DXAGENT_USERUID` - UID of the user
- `DXAGENT_USEREMAIL` - user email
- `DXAGENT_BUSINESS_UNIT_NAME` - Business unit name
- `DXAGENT_ACCOUNT_NAME` - Account name
- `DXAGENT_ACCOUNT_ID` - Account ID
- `DXAGENT_USERLOGINTYPE` - Account login type
- `DXAGENT_ACCOUNT_PHONE` - Account telephone number
- `DXAGENT_ACCOUNT_NOTES` - Account notes
- `DXAGENT_ACCOUNT_UNLICENSED` - Account licensed property
- `DXAGENT_ACCOUNT_TYPE` - Account type: Unspecified, Internal, Partner
- `DXAGENT_ACCOUNT_DELIVERY_METHOD` - Adhoc delivery method
- `DXAGENT_ACCOUNT_IMPLICIT_ENROLLMENT` - Account implicit enrollment type
- `DXAGENT_HOMEDIR` - Account home directory

Note The attributes are not supported for users instantiated from account templates.

Note `DXAGENT` variables will not be evaluated for PeSIT, AS2 and Publish to Account transfers, as actual user login is not performed.

SecureTransport allows you to map an user based on their login type:

- To map a real user, use `DXAGENT_USERLOGINTYPE="REAL"`
- To map a virtual user, use `DXAGENT_USERLOGINTYPE="VIRTUAL"`
- To map a Siteminder user, use `DXAGENT_USERLOGINTYPE="SITEMINDER"`
- To map the a SSO user, you can use `DXAGENT_USERLOGINTYPE="SSO"`
- If you want to map the a LDAP user, you can use `DXAGENT_USERLOGINTYPE="LDAP"`

The following constants are supported:

- Numeric constants: `-5`, `100`, `.5`, `1.05`, `3.14159D`, `6.0221415e23`, `214748364`, `0xFFECDE5E`
- Character constants: `'a'`, `'\u0061'`, `'\t'`, `'\u0009'`, `'\n'`, `'\b'`, `'\r'`, `'\f'`, `'\\'`, `'\"'`
- String constants: `"Finance"`, `"US"`, `"^.*@finance\.example\.com$"`
- Logical constants: `true`, `false`
- Null constant: `null` (represents no value, so `fdxShell = null` is `true` if that `fdxShell` is not defined)

The following functions are supported:

- `isSet("A")` – true if there is a session variable named *A*
- `memberOf(A, B$collection)` – true if *A* is a member of the multivalued session variable *B*
- `toInt(A)` – converts *A* to an integer
- `toString(A)` – converts *A* to an string

SecureTransport evaluates the expression based on the following operator precedence from highest to lowest:

- Logical unary `not`
- Arithmetic unary + and −
- Arithmetic binary `*`, `/`, and `%` (integer remainder)
- Arithmetic binary + and −
- String concatenation +
- Numeric, date and string comparison >, >=, <, <=, and `like`
- Logical, numeric, date, and string comparison = and <>
- Logical `and`

- Logical `or`
- Conditional expression *A* `?` *B* `:` *C* (which has the value *B* if *A* is `true` or *C* if *A* is not `true`)

Use parentheses to group expressions and override the operator precedence.

SecureTransport dynamically converts numeric expressions to long integers, single-precision real numbers, or double-precision real numbers when it is necessary to evaluate an operator. When an operator requires a logical value, SecureTransport converts any value of a type other than logical to `false`.

The `like` operator matches its string left operand against a string right operand that is a Java regular expression. The result is `true` if the regular expression matches all of the left operand. The backslash (`\`) is the escape character Java regular expressions, so, in a regular expression, use two backslashes (`\\`) to match a backslash. See the examples.

The following expression checks for virtual users who are in one of three groups:

```
fdxUserType = "virtual" and (fdxGid = 1200 or fxdGid = 1400 or
fdxGid = 1500)
```

The following expression tests the prefix of the user home directory on a Windows system:

```
fdxHomeDir like "C:\\home\\users\\finance\\.*"
```

The following two expressions return the same result, checking the email address against different regular expressions depending on the UID:

```
fdxUid > 100 and fdxUid <= 200 and fdxEmail like
".*@finance\.example\.com" or fdxEmail like ".*@hr\.example\.com"
```

```
fdxEmail like (fdxUid > 100 and fdxUid <= 200 ?
".*@finance\.example\.com" : ".*@hr\.example\.com")
```

Manage user classes

Use the *User Classes* page to add, enable, disable, reorder, and delete user classes.

The following topics provide user class examples and how-to instructions for managing user classes:

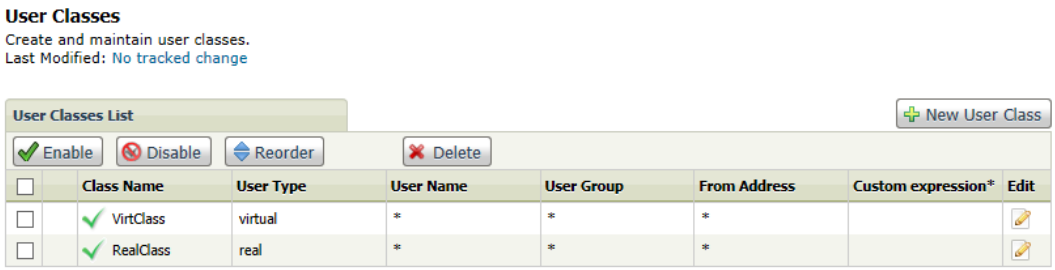
- *Add a user class* on page 714
- *Enable or disable a user class* on page 716
- *Edit a user class* on page 716
- *Reorder user classes* on page 716
- *Delete a user class* on page 716
- *User class examples* on page 717

Add a user class

Use the following procedure to add a user class.

1. Select **Access > User Classes**.

   The *User Classes* page is displayed.



2. Click **New User Class**. A new line is displayed in the *User Classes List*.
3. In the **Class Name** field, enter the name for the user class to create.

   If the name is not unique, SecureTransport uses only the first user class with that name in the *User Class List*.
4. In the **User Type** field, select the predefined user type for the user class.

   Note Because of the different ways SecureTransport treats the path name specification of the download or upload directory for real and virtual users when download or upload restrictions are defined, you should avoid selecting `*` to match all users.
5. In the **User Name** field, enter one of the following:
   - The user name, such as the UNIX-based system login name, the Windows user name, virtual user name, LDAP user name, SiteMinder, or Single Sign-On (SSO) user name.

     On Windows, type either a `username`, *`COMPUTERNAME`*`\username`, or *`DOMAIN`*`\username`.
   - A pattern using `*` and `?` to include matching users. For example, `*` includes all users.

     Only one pattern is allowed.
6. In the **User Group** field, enter one of the following:
   - The name or numerical GID of the group assigned to the user. If all characters are numeric, the value is a GID. Otherwise, it is group name. On Windows, the value can be either the Windows security identifier (SID) of the group or the GID from the `group` file.
   - An asterisk (`*`) to include users in all groups.
7. In the **From Address** field, enter a host name, a host name pattern, an IP address, or subnet specification. For valid values, see *IP addresses and host names* on page 1032.

   Only one host name, an IP address, or subnet specification is allowed.
8. To define the user class using other user attributes or LDAP attributes, enter a **Custom expression**. See *Custom expressions* on page 711.
9. Click the Save icon ( ) in the **Edit** column.

   The status of a new user class is set to Disabled.

Note To cancel an add operation, select **Access > User Classes** again.

Enable or disable a user class

Use the following procedure to enable or disable a user class.

1. Select **Access > User Classes**.

   The *User Classes* page is displayed.
2. In the *User Classes List*, select the check box for each user class to modify.
3. Click **Enable** or **Disable**.

   The icons in the **Class Name** column change to indicate the status of the classes.

Edit a user class

Use the following procedure to edit a user class.

1. Select **Access > User Classes**.

   The *User Classes* page is displayed.
2. In the *User Classes List*, click the Edit icon ( ) in the **Edit** column for the user class entry to edit.
3. Make the required changes to the fields in the row.
4. Click the Save icon ( ) in the **Edit** column.

Note To cancel an edit operation, select **Access > User Classes** again.

Reorder user classes

If a user belongs to multiple classes, SecureTransport categorizes the user as belonging to the first matching class in the *User Classes List*.

If two or more user classes have the same name, SecureTransport processes only the first of those classes in the *User Classes List*.

1. Select **Access > User Classes**.

   The *User Classes* page is displayed.
2. In the *User Classes List*, click **Reorder**.

   Up and down arrows are displayed in a column before the **Class Name** column in the *User Classes List*.
3. Drag the rows of the *User Classes List* to the required order.
4. Click **Save Order**.

Note To cancel a reorder operation, select **Access > User Classes** again.

Delete a user class

Use the following procedure to delete a user class.

1. Select **Access > User Classes**.

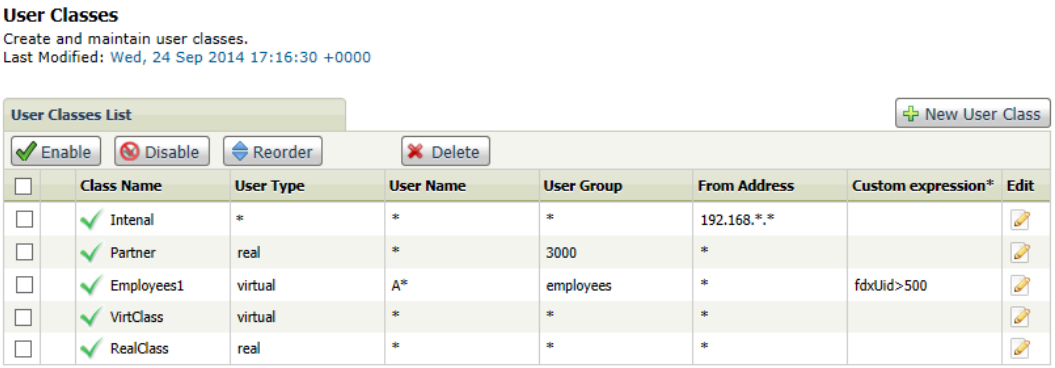
   The *User Classes* page is displayed.

2. In the *User Classes List*, select the check box for each user class to delete.
3. Click **Delete**.
4. Click **OK** in the confirmation dialog box.

Note If you delete a user class, it is best to remove all references to that user class from all access rules. SecureTransport ignores access rules that reference an undefined user class.

User class examples

The following example illustrates some sample user class entries.



The following table summarizes the user classes and describes their functions.

User class	Definition
Internal	Includes users of any type, name, or group, who connect from IP address that start with `192.168`.
Partner	Includes users of real type with GID 3000 who do not connect from IP address that start with `192.168`.
Employees1	Includes users of virtual type whose user name begins with `A`, are in the `employees` user group, have user ID greater than or equal to 500, and do not fall into the Internal class.
VirtClass	Includes all virtual users who do not fall into the Internal or Employee1 classes.
RealClass	Includes all real users who do not fall into the Partner class.

Because the default RealClass and VirtClass include all users, all SecureTransport users are in one of the four classes.

Secure Socket Layer access

The Secure Socket Layer (SSL) is the security protocol used by SecureTransport to encrypt communication between the server and its clients. SSL requires the server to have a certificate, which is exchanged with the client during the SSL handshake. SSL allows the client to have a certificate that is presented to the server and can be used to authenticate the SecureTransport user as an alternative to authenticating the user through a password. SSL is also used by SecureTransport to transfer files securely.

Based on user class, encryption (SSL) can be set as optional or mandatory.

- If SSL is mandatory, the SecureTransport Server only accepts SSL connections. If SSL is not enabled at the client end, SecureTransport refuses the connection.
- If SSL is optional, then both SSL and non-SSL connections are enabled. If the client requests an SSL connection, then it is negotiated. Otherwise, SecureTransport accepts the connection to proceed without encryption. If the client certificate verification is enabled, SecureTransport checks the validity and authenticity of the certificate presented by the client. If SSL is optional and the client requests SSL, but the client certificate verification fails, the client is allowed to log in with a user name and password.

If your SecureTransport deployment includes SecureTransport Edge servers in a peripheral network (DMZ), you should configure SSL access exactly the same on both SecureTransport Edge and SecureTransport Server.

The following topics describe SSL and SSH authentication and provide how-to instructions for managing SSL access:

- *SSL and SSH* on page 718 authentication
- *Manage SSL access* on page 719

SSL and SSH

SSH provides mutual authentication. The client authenticates the server and the server authenticates the client. The data transferred between the client and server is encrypted.

For SSH server authentication, a key is assigned to the SSH server. As part of the connection handshake, the SSH client verifies the server key by checking whether the user has successfully connected to the server in the past. If a user is connecting to the server for the first time, the SSH client asks the user to confirm that the SSH server key and accept it before connecting to the server.

Generally, the SSH protocol provides three methods of authenticating clients: keyboard-interactive authentication, password authentication, and public key authentication. All types of client authentication are supported by SecureTransport.

Note SSH authentication is based on the public key, while SSL authentication is based on certificates. A certificate includes a public key, but it also includes information about the entity to which the key belongs.

In SecureTransport, keys are always managed in the form of certificates. Server keys are associated with Local Certificates. For details, see *Manage local certificates and certificate signing requests* on page 54.

You can assign a local server certificate to the SSH server. The key contained in the certificate is used to establish the SSH connection. Similarly, SSH client keys are associated with login certificates. For details, see *Certificate types* on page 51.

The Secure Socket Layer configuration includes an option to control the use of client certificates in SSL. This option also applies to the use of SSH client keys as described in *Manage SSL access* on page 719.

Note If SecureTransport is deployed with SecureTransport Edge Server installed in a peripheral network (DMZ), you must configure the SSL access control settings on both the SecureTransport Edge and the SecureTransport Server. The settings can be the same to require the same secure connection for both types of installation or they might differ. For example, HTTP and FTP servers on the SecureTransport Server might be intended for internal use only and be protected by the firewall. In this case, the SecureTransport Server can be set up to not require SSL, depending on the organization's policy.

Manage SSL access

Use the *Secure Socket Layer* page to add, enable, disable, reorder, or delete SSL encryption entries.

Note To enable or disable SSL for HTTP transfers, you must modify the **HTTP Server** settings on the *Server Control* page. If you select **Enable HTTPS**, SecureTransport uses SSL with the HTTP connections. If you do not select **Enable HTTPS**, SecureTransport does not use SSL with HTTP connections. For more information, see *Manage the HTTP server* on page 254.

The following topics provide how-to instructions for managing SSL access:

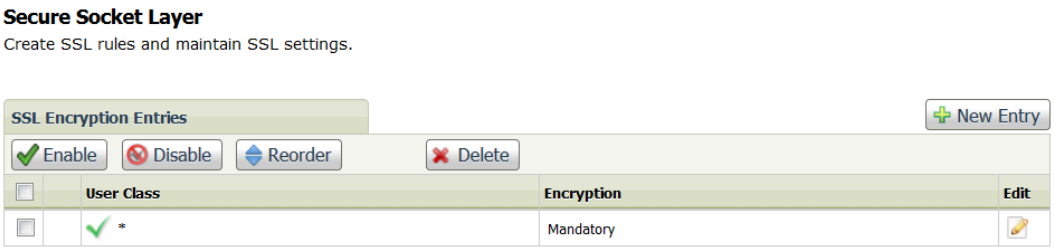
- *Add an SSL users encryption entry* on page 719
- *Enable or disable an encryption entry* on page 720
- *Edit an encryption entry* on page 720
- *Reorder encryption entries* on page 721
- *Delete an encryption entry* on page 721

Add an SSL users encryption entry

You can define SSL encryption settings based on user classes.

1. Select **Access > Secure Socket Layer**.

   The *Secure Socket Layer* page is displayed.



2. At *SSL Encryption Entries*, click **New Entry**. A new line is displayed in the *User Classes List*.
3. Select a **User Class**. The user class must already be defined in the *User Classes* page. Asterisk (`*`) means all users.
4. Select an **Encryption** option for the user class. The two option types are: `Mandatory` and `Optional`.
5. Click the Save icon ( ) in the **Edit** column.

   Note When using certificate-based authentication on Windows with real users, add the real user to the password vault to log in without being prompted for a password. For more information, see *Real users* on page 687.

Note To cancel an add operation, select **Access > Secure Socket Layer** again.

Enable or disable an encryption entry

Use the following procedure to enable or disable an encryption entry.

1. Select **Access > Secure Socket Layer**.

   The *Secure Socket Layer* page is displayed.
2. Under *SSL Encryption Entries*, select the check box for each entry to modify.
3. Click **Enable** or **Disable**.

   The icons in the **User Class** column change to indicate the status of the entries.

Edit an encryption entry

Use the following procedure to edit an encryption entry.

1. Select **Access > Secure Socket Layer**.

   The *Secure Socket Layer* page is displayed.
2. Under *SSL Encryption Entries*, click the Edit icon ( ) in the **Edit** column for the entry to edit.
3. Make the required changes to the fields in the entry.
4. Click the Save icon ( ) in the **Edit** column.

Note To cancel an edit operation, select **Access > Secure Socket Layer** again.

Reorder encryption entries

SecureTransport applies the first entry in the *SSL Encryption Entries* that matched the user class of the user. So, for SecureTransport to use them, you want the more specific entries before the more general entries in the list.

1. Select **Access > Secure Socket Layer**.

   The *Secure Socket Layer* page is displayed.

2. Under *SSL Encryption Entries*, click **Reorder**.

   Up and down arrows are displayed in a column before the **User Class** column in the *SSL Encryption Entries*.

3. Drag the rows of the *SSL Encryption Entries* to the required order.
4. Click **Save Order**.

Note To cancel a reorder operation, select **Access > Secure Socket Layer** again.

Delete an encryption entry

Use the following procedure to delete an encryption entry.

1. Select **Access > Secure Socket Layer**.

   The *Secure Socket Layer* page is displayed.

2. Under *SSL Encryption Entries*, select the check box for each entry to delete.
3. Click **Delete**.
4. Click **OK** in the confirmation dialog box.

Virtual groups

Every user on a UNIX-based system has a user ID and a group ID. UNIX-based systems use these IDs to set process and file permissions. You can define certain groups as virtual users. Any user who is a member of a virtual group becomes a virtual user whether or not they are included in the virtual password file.

Configure virtual groups on SecureTransport Server only.

For how-to instructions for managing virtual groups, refer to *Manage virtual groups* on page 1.

Manage virtual groups

Use the *Virtual Groups* page to add, enable, disable, or delete SSL virtual group entries.

The following topics provide how-to instructions for managing virtual groups:

- *Add a virtual group* on page 722
- *Enable or disable a virtual group* on page 722
- *Edit a virtual group* on page 722
- *Delete a virtual group* on page 723

Add a virtual group

Use the following procedure to add a virtual group.

1. Select **Access > Virtual Groups**.

   The *Virtual Groups* page is displayed.

2. At *Virtual Groups List*, click **New Entry**. A new line is displayed in the *Virtual Groups List*.

3. In the **Virtual Group Name** field, enter the name or the group ID (GID) of the group.
4. Click the Save icon ( ) in the **Edit** column.

   The status of a new virtual group is set to Disabled.

Note To cancel an add operation, select **Access > Virtual Groups** again.

Enable or disable a virtual group

Use the following procedure to enable or disable a virtual group.

1. Select **Access > Virtual Groups**.

   The *Virtual Groups* page is displayed.

2. In the *Virtual Groups List*, select the check box for each user class to modify.
3. Click **Enable** or **Disable**.

   The icons in the **Virtual Group Name** column change to indicate the status of the classes.

Edit a virtual group

Use the following procedure to edit a virtual group.

1. Select **Access > Virtual Groups**.

   The *Virtual Groups* page is displayed.

2. In the *Virtual Groups List*, click the Edit icon ( ) in the **Edit** column for the virtual group entry to edit.

3. Make the required changes to the **Virtual Group Name** field.
4. Click the Save icon ( ) in the **Edit** column.

Note To cancel an edit operation, select **Access > Virtual Groups** again.

Delete a virtual group

Use the following procedure to delete a virtual group.

1. Select **Access > Virtual Groups**.

   The *Virtual Groups* page is displayed.
2. In the *Virtual Groups List*, select the check box for each user class to delete.
3. Click **Delete**.
4. Click **OK** in the confirmation dialog box.

Filesystem restrictions

Use the *Filesystem* pane of the *Restrictions* page to control rights for specific user classes to modify files and directories on the SecureTransport server.

The order of the entries in the list in the *Filesystem* pane of the *Restrictions* page is important because SecureTransport applies the filesystem restrictions starting with the last in the list and proceeding to the first. Once the user class for the user filesystem is established, SecureTransport applies the last entry for that user class or for all user classes (*) that has a file pattern that matches the filesystem. If no entry matches, SecureTransport allows access to the filesystem.

For each user class, put the entries with more general paths before those with more specific paths. For example, to allow users to download from the `/outgoing` directory only, put an entry that allows downloads from that path after an entry that denies download from all locations (*).

Operations that can be allowed or denied are:

- **Delete a File** – Specifies whether or not users from the specified user class may delete files on the SecureTransport Server.
- **Rename a File** – Specifies whether or not users from the specified user class may rename files on the SecureTransport Server.
- **Overwrite a File** – Specifies whether or not users from the specified user class may overwrite existing files on the SecureTransport Server.
- **Make a Directory** – Specifies whether or not users from the specified user class may create directories on the SecureTransport Server.
- **Remove a Directory** – Specifies whether or not users from the specified user class may remove directories from the SecureTransport Server.
- **Change File Mode** – Specifies whether or not users from the specified user class may change file access permissions on the SecureTransport Server. This option is applicable only for UNIX.

- **Change Umask** – Specifies whether or not users from the specified user class may change the access permissions mask for new files being uploaded to the SecureTransport Server. This option is applicable only for UNIX.

  Note The SecureTransport Server is compliant with the SFTP protocol specification and does not apply a umask to the mode bits if they are specified by the client. If the mode bits are not specified by the client, the umask is applied based on the configuration of the `Users.DefaultUmask` option.

  Note If the SecureTransport `Users.DefaultUmask` configuration option is set to some value, that value is used for the umask. If the `Users.DefaultUmask` configuration option is empty, the operating system's umask is used.

- **Access a File/Directory** – Specifies whether or not users from the specified user class have access to files or directories on the SecureTransport Server.

Note When a ST Web Client user moves a file using cut and paste, SecureTransport checks the filesystem Rename a File permission. SecureTransport does not check the upload restrictions in this case.

The `Restrictions.OrderOfApplication` server configuration option defines the order of application for filesystem and upload and download restrictions. There are two available values for the option:

- **legacy** (default) - rules are applied from bottom to top
- **new** - rules are applied from top to bottom

Configure filesystem restrictions on SecureTransport Server only.

For how-to instructions for managing filesystem restrictions, refer to *Manage filesystem restrictions* on page 724.

Manage filesystem restrictions

Use the *Filesystem* pane of the *Restrictions* page to add, enable, disable, or delete filesystem restriction entries.

Note SecureTransport applies filesystem restrictions starting with the last in the list and proceeding to the first. When you create two or more restrictions with the same action and that apply to the same users and the same path, make sure to put an entry with a more general path above one with a more specific path.

The following topics provide how-to instructions for managing filesystem restrictions:

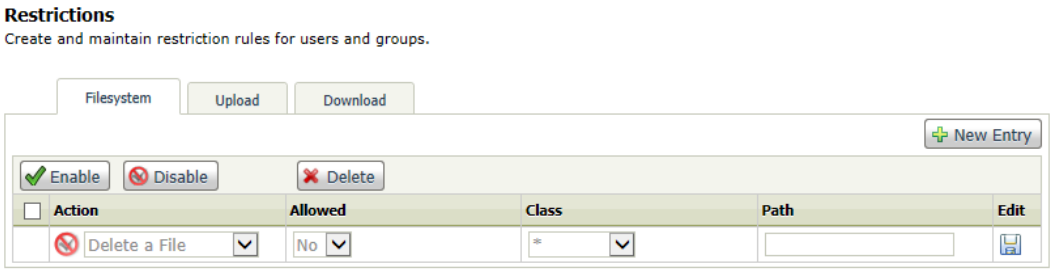
- *Add a filesystem restriction* on page 725
- *Enable or disable a filesystem restriction* on page 726
- *Edit a filesystem restriction* on page 726
- *Delete a filesystem restriction* on page 726
- *Example filesystem restriction* on page 727

Add a filesystem restriction

Use the following procedure to add a filesystem restrictions.

1. Select **Access > Restrictions**.
2. Click the **Filesystem** tab.

   The *Filesystem Restrictions* pane is displayed.
3. Click **New Entry**. A new line is displayed in the list.



4. Select an **Action** from the list. For description of the options, see *Filesystem restrictions* on page 723.
5. In the **Allowed** field, select **No** to deny the action or **Yes** to allow it.
6. In the **Class** field, select a user class. Asterisk (`*`) means all users.
7. In the **Path** field, type the path of the directory for which the restriction applies.

   Specify the path relative to the file system root for the user. For a real user, the file system root is the operating system root. For a virtual user, the file system root is the user's home directory.

   On Windows, you must use a POSIX path. Specify drives as `/drives/c` and `/drives/d` instead of `C:\` and `D:\`.

   You can use UNIX-style wildcard characters to apply restrictions for an entire directory. Path entries must contain both a forward slash and the asterisk wildcard (`/*`) to allow or deny everything. For example, on Windows, to prevent deletion of the contents of the `C:\temp` directory, specify `/drives/C/temp/*` as the path. In this example, specifying `/drives/C/temp` only prevents the directory itself from being deleted, not its contents.
   With SecureTransport version 5.4, two new parameters are introduced with Filesystem restrictions: `{s}` and `{i}`. These two options are used as prefixes to regular expressions and their purpose is to match the Path in case sensitive (`{s}`)or case insensitive (`{i}`) manner.

- `{i}` matches Path in an expression in a case-insensitive fashion.
  Example use: Delete a File action of files that match the expression `{i}/*.xml` will delete any xml file, regardless of filename extension case: whether it is XML, xml or XmL.
- `{s}` matches all files in an expression in a case-sensitive fashion.
  Example use: Delete a File action of files that match the expression `{s}/*.TXT` will only delete files with TXT extension (uppercase, as defined in the expression) and will not delete files with .txt extension (lowercase, not defined in the expression).

Note Along with the two regular expression prefixes, a dedicated configuration option is introduced: `Restrictions.pathIgnoreCases`. When it is set to `false`, all expressions that do not use the `{i}` or `{s}` prefixes will match the path in case-sensitive manner. Respectively, when set to `true`, all expressions without the `{i}` or `{s}` prefixes will match in case-insensitive manner.

8. Click the Save icon ( ) in the **Edit** column.

   SecureTransport adds the new entry at the top of the list. The status of a new entry is set to Disabled.

Note To cancel an add operation, select **Access > Restrictions** again.

Enable or disable a filesystem restriction

Use the following procedure to enable or disable a filesystem restriction.

1. Select **Access > Restrictions**.
2. Click the **Filesystem** tab.

   The *Filesystem Restrictions* pane is displayed.
3. Select the check box for each entry to modify.
4. Click **Enable** or **Disable**.

   The icons in the **Action** column change to indicate the status of the classes.

Edit a filesystem restriction

Use the following procedure to edit a filesystem restriction.

1. Select **Access > Restrictions**.
2. Click the **Filesystem** tab.

   The *Filesystem Restrictions* pane is displayed.
3. Click the Edit icon ( ) in the **Edit** column for the entry to edit.
4. Make the required changes to the fields.
5. Click the Save icon ( ) in the **Edit** column.

Note To cancel an edit operation, select **Access > Restrictions** again.

Delete a filesystem restriction

Use the following procedure to delete a filesystem restriction.

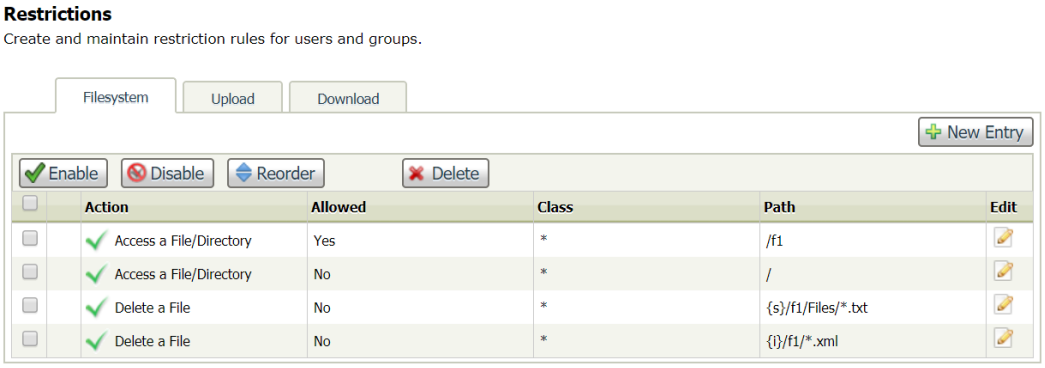
1. Select **Access > Restrictions**.
2. Click the **Filesystem** tab.

   The *Filesystem Restrictions* pane is displayed.
3. Select the check box for each entry to delete.

4. Click **Delete**.
5. Click **OK** in the confirmation dialog box.

Example filesystem restriction

The following example supplies some examples for Filesystem restrictions.



- The first condition defines access to the `/f1` folder only.
- The second condition restricts access to the root folder.
- The third condition deletes all entirely lowercase TXT files in the `/f1/Files` folder and omits all other case variations (for example,.TxT and .TXT files will not be deleted with this expression). Also, in case there is a `/f1/files` path, its content will remain untouched by this expression since it exactly matches the `/f1/Files` path.
- The fourth condition deletes all XML files in the `/f1` folder (.XML, .xml, .XmL, etc.).

Upload restrictions

Use upload restrictions to allow or deny permission for users to upload files based on user class. For each user class, you can specify upload permissions and, for UNIX-based systems, the value of the owner, group and access permissions of the uploaded file.

The order of the entries in the list in the *Upload* pane of the *Restrictions* page is important because SecureTransport applies the upload restrictions starting with the last in the list and proceeding to the first. Once the user class for the user uploading the file is established, SecureTransport applies the last entry for that user class or for all user classes (*) that has a file pattern that matches the file to be uploaded. If no entry matches, SecureTransport allows the upload.

For each user class, put the entries with more general paths before those with more specific paths. For example, to allow users to upload to the `/incoming` directory only, put an entry that allows uploads to that path after an entry that denies upload to all locations (*).

Note For metadata file upload for a protocol implemented using the file services interface, the IP address is not used to choose the user class. The upload restrictions defined for the first user class that matches the user type, name, and group control these transfers.

Configure upload restrictions on SecureTransport Server only.

For how-to instructions for managing upload restrictions, refer to *Manage upload restrictions* on page 728.

Manage upload restrictions

Use the *Upload* pane of the *Restrictions* page to add, enable, disable, reorder, or delete upload restriction entries. Using upload restrictions, for each user class, you can allow or deny permission to upload files based on the destination and set the owner, group, or file system permission (mode) of the uploaded file on a UNIX-based system.

The following topics provide how-to instructions for managing upload restrictions:

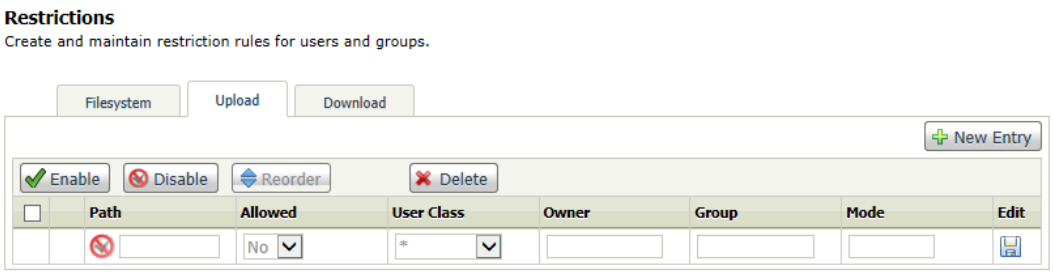
- *Add an upload restriction* on page 728
- *Enable or disable an upload restriction* on page 731
- *Edit an upload restriction* on page 731
- *Reorder upload restrictions* on page 731
- *Delete an upload restriction* on page 1

Add an upload restriction

Use the following procedure to add an upload restriction.

1. Select **Access > Restrictions**.
2. Click the **Upload** tab.

   The *Upload Restrictions* pane is displayed.
3. Click **New Entry**. A new line is displayed in the list.



4. Complete the fields in the following table.

Field	Description
Path	The file name or directory you want to apply a restriction to. Specify the path relative to the file system root for the user. For a real user, the file system root is the operating system root. For a virtual user, the file system root is the user's home directory. On Windows, you must use a POSIX path. Specify drives as `/drives/c` and `/drives/d` instead of `C:\` and `D:\`. You can use UNIX-style wildcard characters to apply restrictions for an entire directory and its subdirectories. Path entries must contain both a forward slash and the asterisk wildcard (`/*`) to deny or allow everything. Specifying `/temp` applies the restriction only to the directory itself, not its contents. To apply the restriction to the directory and its contents, you must specify `/temp/*`. For example, if you specify `/drives/C/temp` as the path and allow uploads, uploading will be allowed but Owner, Group, and Mode will not be applied to the uploaded file. To apply Owner, Group, and Mode or to allow uploads to subdirectories of `/temp`, you must specify `/drives/C/temp/*` as the path. With SecureTransport version 5.4, two new parameters are introduced with Filesystem restrictions: `{s}` and `{i}`. These two options are used as prefixes to regular expressions and their purpose is to match the Path in case sensitive (`{s}`)or case insensitive (`{i}`) manner. • `{i}` matches Path in an expression in a case-insensitive fashion. Example use: Access to path that matches the expression `{i}/*.xml` will allow the user to upload any xml file, regardless of filename extension case: whether it is XML, xml or XmL. • `{s}` matches all files in an expression in a case-sensitive fashion. Example use: Access to path that matches the expression `{s}/*.TXT` will allow the user to upload only files with TXT extension (uppercase, as defined in the expression) and will not be able to upload files with .txt extension (lowercase, not defined in the expression). Along with the two regular expression prefixes, a dedicated configuration option is introduced: `Restrictions.pathIgnoreCases`. When it is set to `false`, all expressions that do not use the `{i}` or `{s}` prefixes will match the path in case-sensitive manner. Respectively, when set to `true`, all expressions without the `{i}` or `{s}` prefixes will match in case-insensitive manner.
Allowed	Select **Yes** or **No** based on whether you want to restrict uploading.

Field	Description
User Class	Select a user class. Asterisk (`*`) means all users.
Owner	(UNIX-based systems only) User ID to be set for the uploaded file when **Allowed** is **Yes**. When the `Users.Uploads.RestrictionsApplication` server configuration parameter is set to `limited`, the value of this field is ignored if the file mode is set by the client. The `Users.Uploads.RestrictionsApplication` server configuration parameter default value is: `limited` When the `Users.Uploads.RestrictionsApplication` server configuration parameter is set to `full`, the value of this field is always applied.
Group	(UNIX-based systems only) Group name or ID to be set for the uploaded file when **Allowed** is **Yes**. When the `Users.Uploads.RestrictionsApplication` server configuration parameter is set to `limited`, the value of this field is ignored if the file mode is set by the client. The `Users.Uploads.RestrictionsApplication` server configuration parameter default value is: `limited` When the `Users.Uploads.RestrictionsApplication` server configuration parameter is set to `full`, the value of this field is always applied.
Mode	(UNIX-based systems only) File access permissions to be applied to the uploaded file when **Allowed** is **Yes**. When the `Users.Uploads.RestrictionsApplication` server configuration parameter is set to `limited`, the value of this field is ignored if the file mode is set by the client. The `Users.Uploads.RestrictionsApplication` server configuration parameter default value is: `limited` When the `Users.Uploads.RestrictionsApplication` server configuration parameter is set to `full`, the value of this field is always applied. If you leave this field empty, the file mode set by the client is applied regardless of the value of `Users.Uploads.RestrictionsApplication` server configuration parameter.

5. Click the Save icon ( ) in the **Edit** column.

   The status of a new entry is set to Disabled.

Note To cancel an add operation, select **Access > Restrictions** again.

Enable or disable an upload restriction

Use the following procedure enable or disable an upload restriction.

1. Select **Access > Restrictions**.
2. Click the **Upload** tab.

   The *Upload Restrictions* pane is displayed.
3. Select the check box for each entry to modify.
4. Click **Enable** or **Disable**.

   The icons in the **Path** column change to indicate the status of the classes.

Edit an upload restriction

Use the following procedure to edit an upload restriction.

1. Select **Access > Restrictions**.
2. Click the **Upload** tab.

   The *Upload Restrictions* pane is displayed.
3. Click the Edit icon ( ) in the **Edit** column for the entry to edit.
4. Make the required changes in the fields.
5. Click the Save icon ( ) in the **Edit** column.

Note To cancel an edit operation, select **Access > Restrictions** again.

Reorder upload restrictions

Use the following procedure to reorder upload restrictions.

1. Select **Access > Restrictions**.
2. Click the **Upload** tab.

   The *Upload Restrictions* pane is displayed.
3. Click **Reorder**.

   Up and down arrows are displayed in a column before the **Path** column.
4. Drag the rows of the entries to the required order.
5. Click **Save Order**.

Note To cancel a reorder operation, select **Access > Restrictions** again.

Delete an upload restriction

Use the following procedure to delete an upload restriction.

1. Select **Access > Restrictions**.
2. Click the **Upload** tab.

   The *Upload Restrictions* pane is displayed.
3. Select the check box for each entry to delete.
4. Click **Delete**.
5. Click **OK** in the confirmation dialog box.

Download restrictions

Use download restrictions to allow or deny permission for users to download files based on user class. For each user class, you can specify upload permissions that allow or deny the user the ability to view, create, or modify files and directories.

The order of the entries in the list in the *Download* pane of the *Restrictions* page is important because SecureTransport applies the download restrictions starting with the last in the list and proceeding to the first. Once the user class for the user downloading the file is established, SecureTransport applies the last entry for that user class or for all user classes (*) that has a file pattern that matches the file to be downloaded. If no entry matches, SecureTransport allows the download.

For each user class, put the entries with more general paths before those with more specific paths. For example, to allow users to download from the `/outgoing` directory only, put an entry that allows downloads from that path after an entry that denies download from all locations (*).

Configure download restrictions on SecureTransport Server only.

For how-to instructions for managing download restrictions, refer to *Manage download restrictions* on page 1.

Manage download restrictions

Use the *Download* pane of the *Restrictions* page to add, enable, disable, reorder, or delete download restriction entries.

The following topics provide how-to instructions for managing download restrictions:

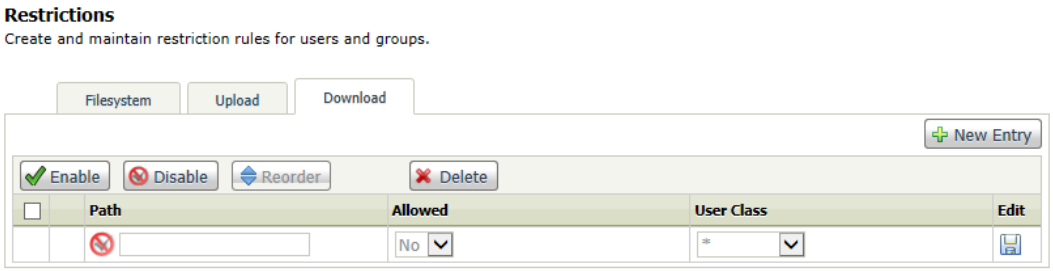
- *Add a download restriction* on page 732
- *Enable or disable a download restriction* on page 735
- *Edit a download restriction* on page 735
- *Reorder download restrictions* on page 735
- *Delete a download restriction* on page 736

Add a download restriction

Use the following procedure to add a download restriction.

1. Select **Access > Restrictions**.
2. Click the **Download** tab.

   The *Download Restrictions* pane is displayed.
3. Click **New Entry**. A new line is displayed in the list.



4. Complete the fields in the following table.

Field	Description
Path	The file name or directory you want to apply a restriction to. Specify the path relative to the file system root for the user. For a real user, the file system root is the operating system root. For a virtual user, the file system root is the user's home directory. On Windows, you must use a POSIX path. Specify drives as `/drives/c` and `/drives/d` instead of `C:\` and `D:\`. You can use UNIX-style wildcard characters to apply restrictions for an entire directory and its subdirectories. Path entries must contain both a forward slash and the asterisk wildcard (`/*`) to deny or allow everything. For example, on Windows, to prevent deletion of the contents of the `C:\temp` directory, specify `/drives/C/temp/*` as the path. In this example, specifying `/drives/C/temp` applies the restriction only to the directory itself, not its contents. With SecureTransport version 5.4, two new parameters are introduced with Filesystem restrictions: `{s}` and `{i}`. These two options are used as prefixes to regular expressions and their purpose is to match the Path in case sensitive (`{s}`)or case insensitive (`{i}`) manner. • `{i}` matches Path in an expression in a case-insensitive fashion. Example use: Access to path that matches the expression `{i}/*.xml` will allow the user to download any xml file, regardless of filename extension case: whether it is XML, xml or XmL. • `{s}` matches all files in an expression in a case-sensitive fashion. Example use: Access to path that matches the expression `{s}/*.TXT` will allow the user to download only files with TXT extension (uppercase, as defined in the expression) and will not be able to download files with .txt extension (lowercase, not defined in the expression). Along with the two regular expression prefixes, a dedicated configuration option is introduced: `Restrictions.pathIgnoreCases`. When it is set to `false`, all expressions that do not use the `{i}` or `{s}` prefixes will match the path in case-sensitive manner. Respectively, when set to `true`, all expressions without the `{i}` or `{s}` prefixes will match in case-insensitive manner.
Allowed	Select **Yes** or **No** based on whether you want to restrict downloading.
User Class	Select a user class. Asterisk (`*`) means all users.

5. Click the Save icon ( ) in the **Edit** column.

   The status of a new entry is set to Disabled.

Note To cancel an add operation, select **Access > Restrictions** again.

Enable or disable a download restriction

Use the following procedure to enable or disable a download restriction.

1. Select **Access > Restrictions**.
2. Click the **Download** tab.

   The *Download Restrictions* pane is displayed.
3. Select the check box for each entry to modify.
4. Click **Enable** or **Disable**.

   The icons in the **Path** column change to indicate the status of the classes.

Edit a download restriction

Use the following procedure to edit a download restriction.

1. Select **Access > Restrictions**.
2. Click the **Download** tab.

   The *Download Restrictions* pane is displayed.
3. Click the Edit icon ( ) in the **Edit** column for the entry to edit.
4. Make the required changes in the fields.
5. Click the Save icon ( ) in the **Edit** column.

Note To cancel an edit operation, select **Access > Restrictions** again.

Reorder download restrictions

Use the following procedure to reorder download restrictions.

1. Select **Access > Restrictions**.
2. Click the **Download** tab.

   The *Download Restrictions* pane is displayed.
3. Click **Reorder**.

   Up and down arrows are displayed in a column before the **Path** column.
4. Drag the rows of the entries to the required order.
5. Click **Save Order**.

Note To cancel a reorder operation, select **Access > Restrictions** again.

Delete a download restriction

Use the following procedure to delete a download restriction.

1. Select **Access > Restrictions**.
2. Click the **Download** tab.

   The *Download Restrictions* pane is displayed.
3. Select the check box for each entry to delete.
4. Click **Delete**.
5. Click **OK** in the confirmation dialog box.

FTP command restrictions

The SecureTransport FTP server uses a number of standard and extended FTP commands. You can restrict individual FTP commands for specified user classes. By default, the page includes entries that allow all listed commands for all users.

To allow an FTP command for some users and restrict it for others, create two or more entries and reorder them so that the more restrictive rule comes before the less restrictive rules.

If your SecureTransport deployment includes SecureTransport Edge servers in a peripheral network (DMZ) and if you need different restrictions for users who connect using SecureTransport Edge and using SecureTransport Server, you can configure FTP command restrictions differently.

The following topics describe the FTP SITE command and the how-to instructions for managing FTP command restrictions:

- *FTP SITE command* on page 736
- *Manage FTP command restrictions* on page 736

FTP SITE command

Some FTP `SITE` commands that SecureTransport accepts are handled differently than the other FTP commands. The `SITE VERS`, `SITE AUTH` and `SITE FEAT` commands are not listed even though SecureTransport accepts those commands. Those commands must always be allowed, because Axway Secure Client depends on the responses of those commands to determine the capabilities of SecureTransport Server. SecureTransport restricts the `SITE HELP` command based on the setting for the `HELP` command.

Manage FTP command restrictions

Use the *FTP Commands* page to allow or restrict individual FTP commands for specified user classes.

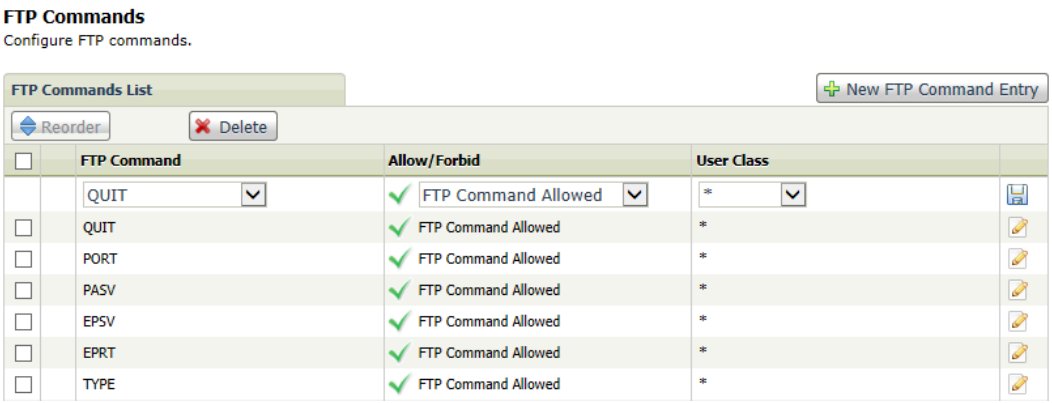
The following topics provide how-to instructions for managing FTP command restrictions:

- *Add an FTP command entry* on page 737
- *Edit an FTP command entry* on page 737
- *Reorder FTP command entries* on page 738
- *Delete an FTP command entry* on page 738

Add an FTP command entry

Use the following procedure to add an FTP command entry.

1. Select **Access > FTP Commands**.
2. The *FTP Commands* page is displayed.
3. Click **New FTP Command Entry**. A new line is displayed in the list.



4. Select an **FTP Command** to allow and restrict.
5. In the **Allow/Forbid** field, select **FTP Command Allowed** or **FTP Command Forbidden**.
6. Select the **User Class**. Asterisk (*) means all users.
7. Click the Save icon () in the **Edit** column.

   The new entry is added before the existing entries for that FTP command.

Note To cancel an add operation, select **Access > FTP Commands** again.

Edit an FTP command entry

Use the following procedure to edit an FTP command entry.

1. Select **Access > FTP Commands**.

   The *FTP Commands* page is displayed.
2. Click the Edit icon () in the **Edit** column for the entry to edit.
3. Make the required changes in the fields.
4. Click the Save icon () in the **Edit** column.

Note To cancel an edit operation, select **Access > FTP Commands** again.

Reorder FTP command entries

SecureTransport applies the FTP restrictions for each command in the order they are displayed in the list. To restrict an FTP command for some users and allow it for others, create two or more entries and reorder them with the most restrictive commands first.

1. Select **Access > FTP Commands**.

   The *FTP Commands* page is displayed.

2. Click **Reorder**.

   Up and down arrows are displayed in a column before the **FTP Command** column for the FTP commands that have two or more entries.

3. Drag the rows of the entries to the required order.

   You can reorder the entries for only one FTP command each time you click **Reorder**.

4. Click **Save Order**.

Note To cancel a reorder operation, select **Access > FTP Commands** again.

Delete an FTP command entry

Use the following procedure to delete an FTP command entry.

1. Select **Access > FTP Commands**.

   The *FTP Commands* page is displayed.

2. Select the check box for each entry to delete.
3. Click **Delete**.
4. Click **OK** in the confirmation dialog box.

Note You cannot delete the last entry for each FTP command.

Protocol server access control

You can limit access to the SecureTransport Administration Tool, FTP, and HTTP servers to specified hosts by defining access rules.

When a client attempts to connect to the SecureTransport Administration Tool or either of the protocol servers, the server looks up the address and, if reverse DNS lookup is enabled, the host name of the computer the client is connecting from and for protocol servers, the user class and applies the access rules to allow or deny access.

If your SecureTransport deployment includes SecureTransport Edge servers in a peripheral network (DMZ) and if you need different Administration Tool access control for administrators who use the Administration Tool for SecureTransport Edge and for SecureTransport Server, you can configure Administration Tool access control differently.

Configure protocol server access control on SecureTransport Server only.

Note Protocol server access restrictions do not work for SiteMinder logins.

The following topics describe access rule ordering and provide how-to instructions for enabling host names for access control and managing protocol server access:

- *Access rule order* on page 739
- *Enable host names for access control* on page 739
- *Manage protocol server access* on page 740

Access rule order

You set the order that the server applies the access rules. Using rule order and multiple rules, you can implement detail access control.

If you select *Allow then Deny* rule order, the server denies access to a computer if:

- It is not explicitly specified in an allow rule

  or

- It is explicitly specified in a deny rule.

With *Allow then Deny*, if the IP address or host name of a computer is not specified in either an allow rule or a deny rule, the server denies access. So, the default is no access.

A more general deny rule overrides a more specific allow rule, so to allow access from an entire subnet or range of IP addresses and deny access from specific hosts, select *Allow then Deny* and define an allow rule for the subnet or range of IP addresses and deny rules for each host.

Note Be careful not to deny access to the Administration Tool from all computers. If you select *Allow then Deny* rule order and delete all admin access control rules, no computer can access the Administration Tool. If this happens, contact Axway Global Support.

If you select *Deny then Allow* rule order, the Administration Tool server allows access to a computer if:

- It is not explicitly specified in a deny rule

  or

- It is explicitly specified in an allow rule.

With *Deny the Allow*, if the IP address or host name of a computer is not specified in either an allow rule or a deny rule, the server allows access. So, the default is access.

A more general allow rule overrides a more specific deny rule, So to deny access from an entire subnet or range of IP addresses and allow access from specific hosts, select *Deny the Allow* and define an deny rule for the subnet or range of IP addresses and allow rules for each host.

Enable host names for access control

To use host names in the **Address** field of rules that control access to the Administration Tool, FTP, HTTP, and SSH servers, enable reverse DNS lookup for those severs.

Note Enabling reverse DNS lookup might reduce the server's performance because DNS lookups involve a series of requests through the DNS name server tree.

To enable DNS lookups for FTP, HTTP, and SSH servers, use **Reverse DNS Lookups** on the *Miscellaneous Options* page.

The following topics provide how-to instructions for enabling reverse DNS lookups:

- *Enable reverse DNS lookups for the Administration Tool server* on page 740
- *Enable reverse DNS lookups for the FTP, HTTP, or SSH server* on page 740

Enable reverse DNS lookups for the Administration Tool server

Use the following procedure to enable reverse DNS lookups for the Administration Tool server.

1. Select **Operations > Server Configuration**.

   The *Server Configuration* page is displayed.
2. To enable reverse DNS lookups for the Administration Tool server, search for the `Admin.ReverseDNSLookup` parameter and set it to `true`.
3. Bounce the server.

Enable reverse DNS lookups for the FTP, HTTP, or SSH server

Use the following procedure to enable reverse DNS lookups for the FTP, HTTP, or SSH servers.

1. Select **Setup > Miscellaneous**.

   The *Miscellaneous Options* page is displayed.
2. In the **Reverse DNS Lookups** list, select `Reverse DNS lookups enabled`.
3. Click **Apply**.

Manage protocol server access

Define any number of rules in the *Admin Access Control* page control access to the SecureTransport Administration Tool. Define any number of rules in the *Server Access Control* page to control access to the FTP and HTTP servers.

The following topics provide how-to instructions for managing protocol server access:

- *Add an access rule* on page 741
- *Enable or disable an access rule* on page 741
- *Edit an access rule* on page 742
- *Delete an access rule* on page 742

- *Change the order that rules are applied* on page 742
- *Server access rules example* on page 742

Add an access rule

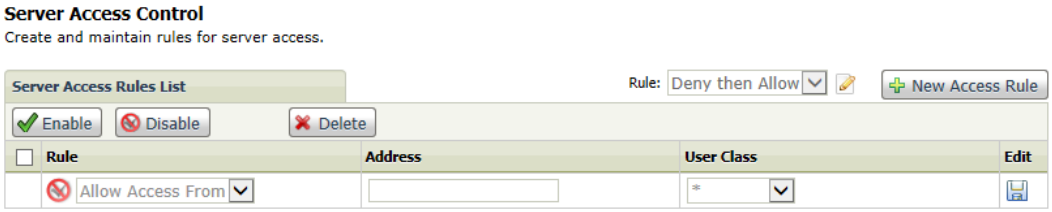
Use the following procedure to add an access rule.

1. Select **Access > Admin Access Control** or **Access > Server Access Control**.

   The *Admin Access Control* or *Server Access Control* page is displayed.

   The initial configuration allows access to the Administration Tool from all computers.

2. Click **New Access Rule**. A new line is displayed in the list.



3. In the **Rule** field, select an access permission. The types of access permissions available are:
   - Allow Access From
   - Deny Access From
4. In the Address field, enter a host name, an IP address, or a value that represents a range of IP addresses to apply the rule. For valid IP addresses and values for IP address ranges, see *IP addresses and host names* on page 1032.

   Only one host name, IP address, or IP address range value is allowed. A host name pattern is not valid.

5. For a server access rule, select a **User Class**. Asterisk (*) means all users.
6. Click the Save icon ( ) in the **Edit** column.

   The status of a new entry is set to Disabled.

Note To cancel an add operation, select **Access > Admin Access Control** or **Access > Server Access Control** again.

Enable or disable an access rule

Use the following procedure to enable or disable an access rule.

1. Select **Access > Admin Access Control** or **Access > Server Access Control**.

   The *Admin Access Control* or *Server Access Control* page is displayed.

2. Select the check box for each rule to modify.
3. Click **Enable** or **Disable**.

   The icons in the **Rule** column change to indicate the status of the classes.

Edit an access rule

Use the following procedure to edit an access rule.

1. Select **Access > Admin Access Control** or **Access > Server Access Control**.

   The *Admin Access Control* or *Server Access Control* page is displayed.
2. Click the Edit icon ( ) in the **Edit** column for the rule to edit.
3. Make the required changes in the fields.
4. Click the Save icon ( ) in the **Edit** column.

Note To cancel an edit operation, select **Access > Admin Access Control** or **Access > Server Access Control** again.

Delete an access rule

Use the following procedure to delete an access rule.

1. Select **Access > Admin Access Control** or **Access > Server Access Control**.

   The *Admin Access Control* or *Server Access Control* page is displayed.
2. Select the check box for each rule to delete.
3. Click **Delete**.
4. Click **OK** in the confirmation dialog box.

Change the order that rules are applied

Use the following procedure to change the order that access rules are applied.

1. Select **Access > Admin Access Control** or **Access > Server Access Control**.

   The *Admin Access Control* or *Server Access Control* page is displayed.
2. Click the Edit icon ( ) to the right of the **Rule** list.
3. Select a rule order. The available rule orders are:
   - Deny then Allow
   - Allow then Deny
4. Click the Save icon ( ) to the right of the **Rule** list.

Server access rules example

The following example uses an IP address pattern to specify a range of IP addresses as described in *IP addresses and host names* on page 1032. It denies access to all computers except those in the 198.160.123 subnet.

User limits

Use user limit entries to limit the number of concurrent users who can connect to the SecureTransport FTP and HTTP servers. The limit you define applies to each protocol server, if you limit the users from a user class to 10, 10 users can connect concurrently to the FTP server and 10 can connect to the HTTP server. You can also specify a time range and days of the week to apply the limit.

If your SecureTransport deployment includes SecureTransport Edge servers in a peripheral network (DMZ) and if you need different user limits for users who connect using SecureTransport Edge and using SecureTransport Server, you can configure user limits differently. For example, you can allow access to users who connect to SecureTransport Server from your internal network during a time you restrict access to users who connect using SecureTransport Edge.

SecureTransport applies all user limits defined for all users or for the user class that the user is in. If no user limit applies to the user, the user can connect to the FTP and HTTP servers. However, connections might be limited by licenses or hardware or network capacity.

User limits do not apply to protocol servers other than FTP and HTTP.

For how-to instructions for managing user limits, refer to *Manage user limits* on page 743.

Manage user limits

Use the *User Limits* pane of the *Access Rules* page to add, enable, disable, reorder, or delete user limits. Using user limits, you can set the maximum number of users who can log in to SecureTransport for each user class. You can also specify the days and time the limit is in effect.

The following topics provide how-to instructions for managing user limits:

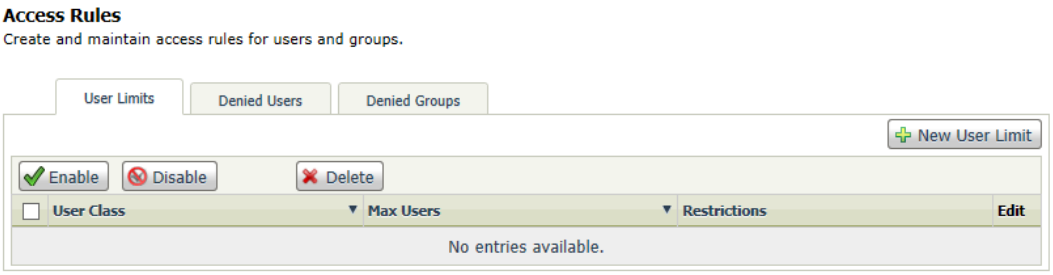
- *Add a user limit* on page 743
- *Enable or disable a user limit* on page 745
- *Edit a user limit* on page 745
- *Delete a user limit* on page 745

Add a user limit

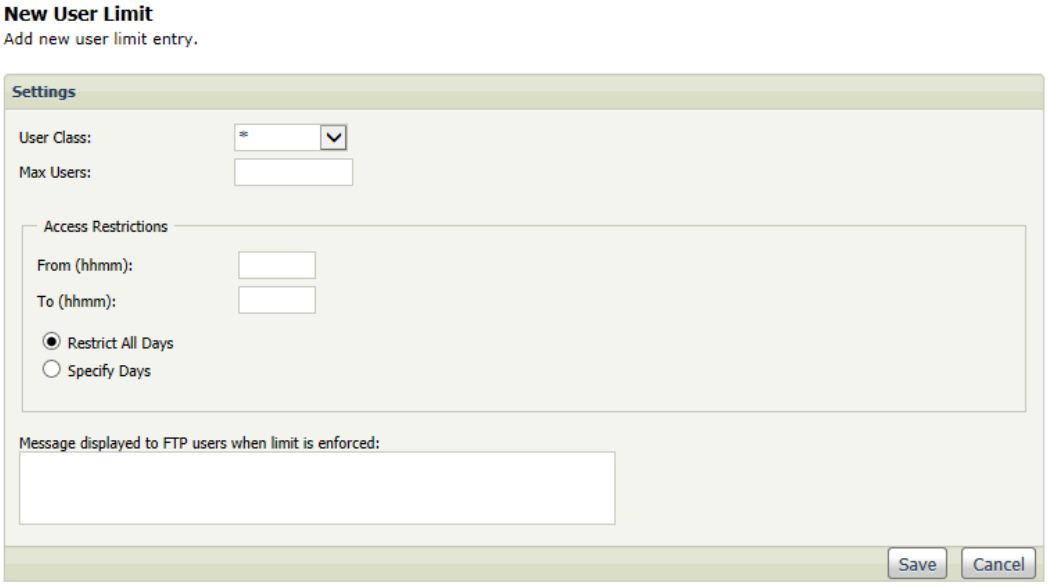
Use the following procedure to add a user limit.

1. Select **Access > Access Rules**.
2. Click the **User Limits** tab.

   The *User Limits* pane is displayed.



3. Click **New User Limit**. The *New User Limit* page is displayed.



4. Select a **User Class**. Asterisk (*) means all users.
5. Type the maximum number of concurrent users for that class.

   Note SecureTransport applies the user limit separately for each protocol. For example, if the maximum users for a user class is 50, SecureTransport allows a maximum of 50 concurrent connections to the FTP server and 50 connections to the HTTP server.

6. Under *Access Restrictions*, to specify the start and end times for SecureTransport to apply the restriction, enter the time in 24-hour format in the **From** and **To** fields. To specify that SecureTransport apply the restriction all the time, leave the **From** and **To** fields empty.
7. Under *Access Restrictions*, to specify the days of the week for SecureTransport to apply the restriction, click **Specify Days** and select the days. To specify that SecureTransport apply the restriction on all days, click **Restrict All Days**.
8. In the field provided, enter a message to be displayed when a user tries to connect to the FTP server and is denied access due to this user limits restriction.
9. Click **Save.**

The *User Limits* pane of the *Access Rules* page is displayed with the new user limit listed. The status of a new user limit is set to Disabled.

Enable or disable a user limit

Use the following procedure to enable or disable a user limit.

1. Select **Access > Access Rules**.
2. Click the **User Limits** tab.

   The *User Limits* pane is displayed.
3. Select the check box for each entry to modify.
4. Click **Enable** or **Disable**.

   The icons in the **User Class** column change to indicate the status of the classes.

   The *User Access* page is displayed.

Edit a user limit

Use the following procedure to edit a user limit.

1. Select **Access > Access Rules**.
2. Click the **User Limits** tab.

   The *User Limits* pane is displayed.
3. Click the Edit icon ( ) in the **Edit** column for the entry to edit. The *User Limit* page is displayed.
4. Make the required changes in the fields.
5. Click **Save.**

   The *User Limits* pane of the *Access Rules* page is displayed with the user limit updated.

Delete a user limit

Use the following procedure to delete a user limit.

1. Select **Access > Access Rules**.
2. Click the **User Limits** tab.

   The *User Limits* pane is displayed.
3. Select the check box for each user limit to delete.
4. Click **Delete**.
5. Click **OK** in the confirmation dialog box.

User and group access

Use this configuration to deny access to SecureTransport to individual users and to users who are members of a group.

By default, the rules deny access to the user `root` and the group `daemon`.

User and group access restrictions apply only to the FTP and HTTP servers.

If your SecureTransport deployment includes SecureTransport Edge servers in a peripheral network (DMZ) and if you need different user and group access for users who connect using SecureTransport Edge and using SecureTransport Server, you can configure user and group access rules differently.

For how-to instructions for managing user and group access, refer to *Manage user and group access* on page 746

Manage user and group access

Use the *Denied Users* pane and the *Denied Groups* pane of the *Access Rules* page to add and remove user and groups that SecureTransport prevents from connecting to the FTP and HTTP servers.

Every group listed as a denied group must be defined at the operating system level so that SecureTransport can determine the group name from the GID in the user account.

The following topics provide how-to instructions for managing user and group access:

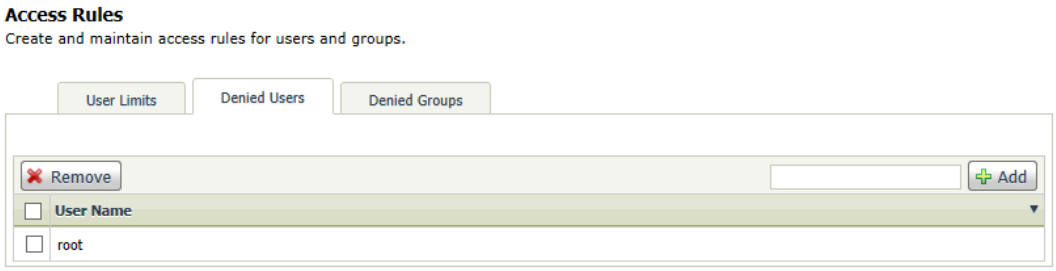
- *Add a user or group to the denied list* on page 746
- *Remove users or groups from the denied list* on page 747

Add a user or group to the denied list

Use the following procedure to add a user or group to the denied list.

1. Select **Access > Access Rules**.
2. Click the **Denied Users** tab or the **Denied Groups** tab.

   The *Denied Users* or *Denied Groups* pane is displayed.



3. Enter in the field to the left of the **Add** button a user name for denied users or a group name or group ID (GID) for denied groups.

4. Click **Add**.
5. The user or group is added to the denied list.

Remove users or groups from the denied list

Use the following procedure to remove users or groups from the denied list.

1. Select **Access > Access Rules**.
2. Click the **Denied Users** tab or the **Denied Groups** tab.

   The *Denied Users* or *Denied Groups* pane is displayed.
3. Select the check box for each user or group to remove.
4. Click **Remove**.
5. Click **OK** in the confirmation dialog box.

Login restrictions

Login restrictions define and restrict the rights of individuals to log in to SecureTransport Servers or SecureTransport Edges through the configuration and use of login restriction policies. The configured login restriction policies are applicable to user accounts, account templates, and business units in a hierarchical inheritance and precedence order.

The login restriction policy inheritance order is:

1. If a policy is not defined on the account or account template level, then the policy of the associated business unit is used.
2. If a policy is not defined either on the account or account template level or on the business unit level, but a default policy is set, then the default policy applies.
3. If no policy is set on the account or template, business unit, or default levels, then access is not restricted.

The login restriction policy precedence order is:

1. If a policy is defined on the account or account template Level, then it takes precedence over the policy assigned on the business unit level.
2. If no policy is defined on the account or account template Level, then the policy assigned on the business unit level takes precedence.

A single user restriction policy can be selected and set as the default policy. The default policy is the suggested user restriction policy when creating a new business unit, account, or account template but it also applies to users that do not have a corresponding user account and do not match an account template. This enables login restrictions to be defined even for external users who do not have any account definition inside SecureTransport.

Refer to the following topics to manage user accounts, account templates, and business units:

- *User accounts* on page 453
- *Manage account templates* on page 663
- *Manage business units* on page 692

Refer to the following topics to create login restriction policies and manage login restrictions :

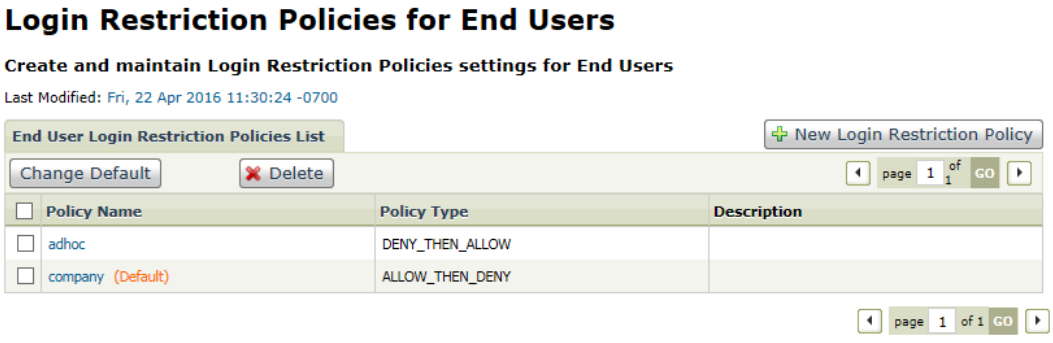
- *Create Login Restriction Policy entries* on page 751
- *Manage Login Restriction Policies* on page 748

Manage Login Restriction Policies

Login restrictions limit access to SecureTransport Servers and SecureTransport Edges through the evaluation of `ALLOW_THEN_DENY` and `DENY_THEN_ALLOW` Login Restriction Policies for end users. The following table describes the evaluation result for different types of Login Restriction Policies.

Match	ALLOW_THEN_DENY	DENY_THEN_ALLOW
Match Allow only	Request allowed	Request allowed
Match Deny only	Request denied	Request denied
No match	Default to second directive: Denied	Default to second directive: Allowed
Match both Allow and Deny	Final match controls: Denied	Final match controls: Allowed

To access and manage the Login Restriction Policies, select **Access > Login Restrictions** in the SecureTransport Administration Tool. The *Login Restriction Policies for End Users* page will be displayed. Use the *Login Restriction Policies for End Users* page to create and maintain Login Restriction Policies.



The following topics provide how-to instructions for managing Login Restriction Policies:

- *Adding Login Restriction Policies* on page 749
- *Editing a Login Restriction Policy* on page 749

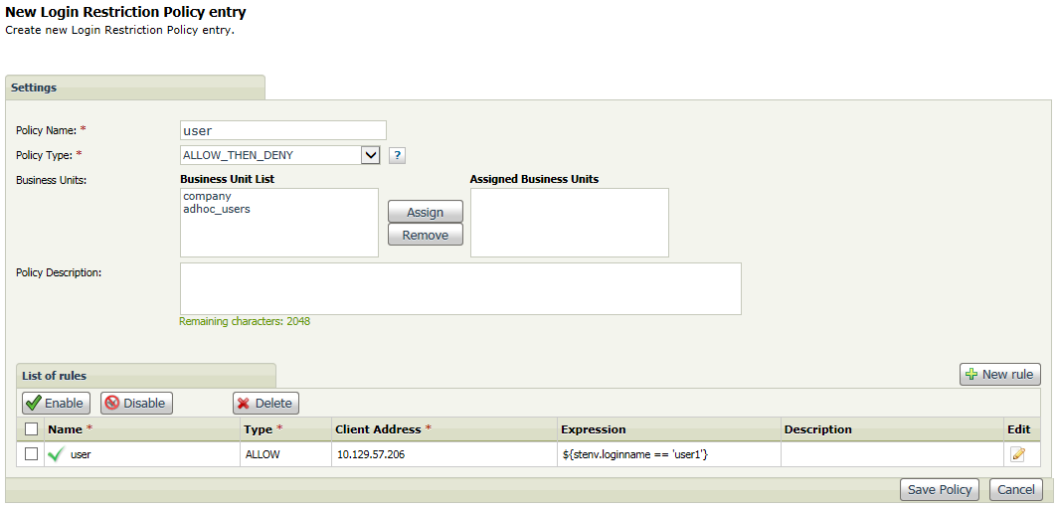
- *Changing the default Login Restriction Policy* on page 750
- *Deleting Login Restriction Policies* on page 750

Adding Login Restriction Policies

Use the following instructions to add a new Login Restriction Policy:

1. Click **New Login Restriction Policy**.

   The *New Login Restriction Policy entry* page will be displayed.



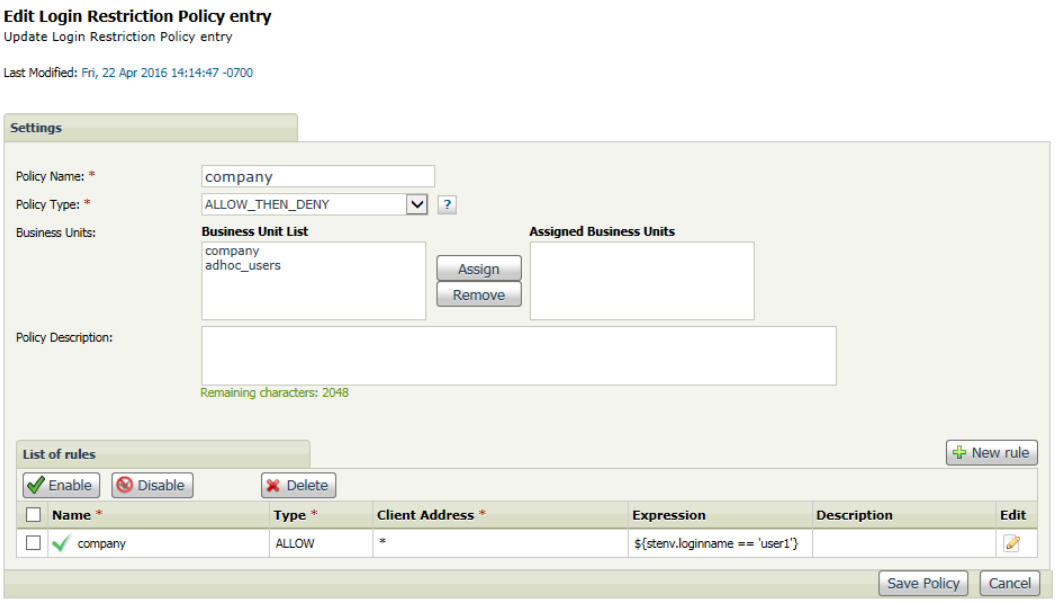
2. Refer to *Creating a Login Restriction Policy* on page 751 for instructions on creating a new Login Restriction Policy.

Editing a Login Restriction Policy

Use the following instructions to edit an existing Login Restriction Policy:

1. Click on the Policy Name to edit the selected Login Restriction Policy.

   The *Edit Login Restriction Policy entry* page will be displayed.



2. Refer to *Editing a Login Restriction Policy* on page 752 for instructions on editing an existing Login Restriction Policy.

Changing the default Login Restriction Policy

Use the following instructions to change the default Login Restriction Policy:

1. Select the desired Login Restriction Policy to make the default policy using the *Policy Name* checkbox.
2. Click **Change Default**.

The selected Login Restriction Policy is now the default policy. The default Login Restriction Policy is indicated by the addition of (default) to the policy name.

You can also unselect the default Login Restriction Policy use the following instructions:

1. Select the current default Login Restriction Policy using the *Policy Name* checkbox.
2. Click **Change Default**.

The selected Login Restriction Policy is no longer the default policy and no Login Restriction Policies are set as the default policy.

Deleting Login Restriction Policies

Use the following instructions for delete a Login Restriction Policy:

1. Select the desired Login Restriction Policy to delete using the *Policy Name* checkbox.
2. Click Delete.
3. Confirm the deletion of the selected Login Restriction Policy.

Create Login Restriction Policy entries

The following topics provide the instructions for creating and editing Login Restriction Policies. The instructions for adding, editing, enabling, disabling, and deleting policy rules are also provided.

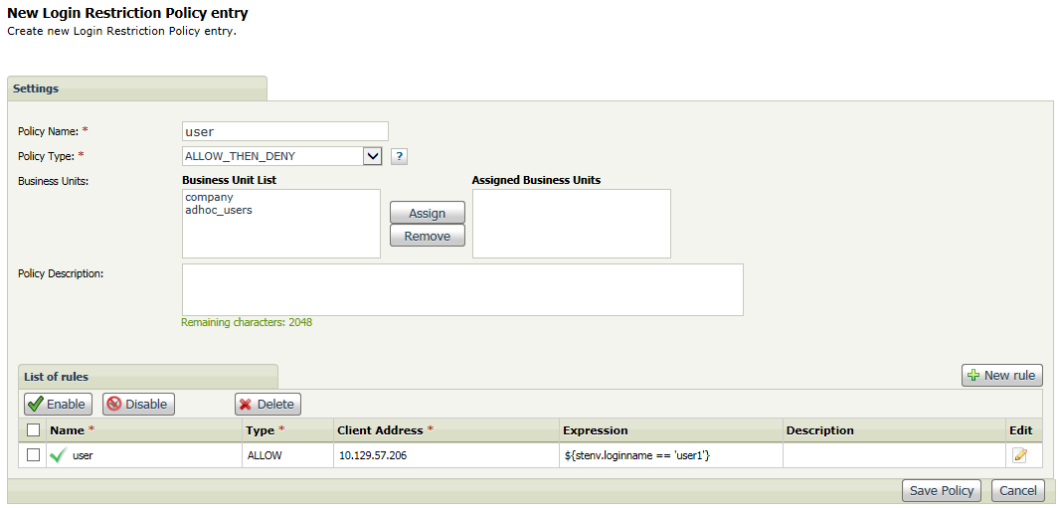
- *Creating a Login Restriction Policy* on page 751
- *Editing a Login Restriction Policy* on page 752
- *Adding a policy rule* on page 752
- *Editing a policy rule* on page 755
- *Enabling a policy rule* on page 755
- *Disabling a policy rule* on page 755
- *Deleting a policy rule* on page 755

Creating a Login Restriction Policy

Use the following instructions to create a Login Restriction Policy:

1. Click **New Login Restriction Policy** on the *Login Restriction Policies for End Users* page.

   The New Login Restriction Policy entry page is displayed.



2. Enter a **Policy Name**.
3. Select a **Policy Type**.

   If the selected Login Restriction Policy Type is `ALLOW_THEN_DENY`, then login access is **denied** by default unless some **ALLOW** rule matches and no **DENY** rule matches.

   If the selected Login Restriction Policy Type is `DENY_THEN_ALLOW`, then login access is **allowed** by default unless some **DENY** rule matches and no **ALLOW** rule matches.
4. (Optional) **Assign Business Units** to the Login Restriction Policy.
5. (Optional) Enter a **Policy Description**.

6. Add Policy Rules to the Login Restriction Policy.

   For instructions on adding Policy Rules to the Login Restriction Policy, refer to *Adding a policy rule on page 752*.

   Note Policy Rules are enabled by default.

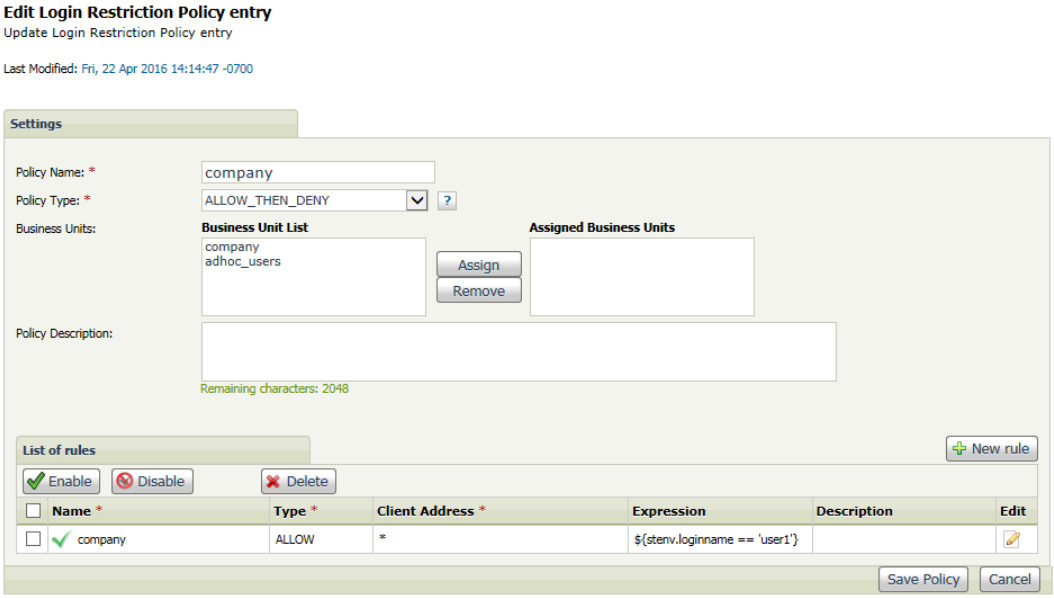
7. Click **Save Policy**.

Editing a Login Restriction Policy

Use the following instructions to edit an existing Login Restriction Policy:

1. Click on the Policy Name to edit the selected Login Restriction Policy on the *Login Restriction Policies for End Users* page.

   The *Edit Login Restriction Policy entry* page will be displayed.



2. Make the desired edits to the selected Login Restriction Policy.

   For additional information, refer to *Creating a Login Restriction Policy on page 751*.

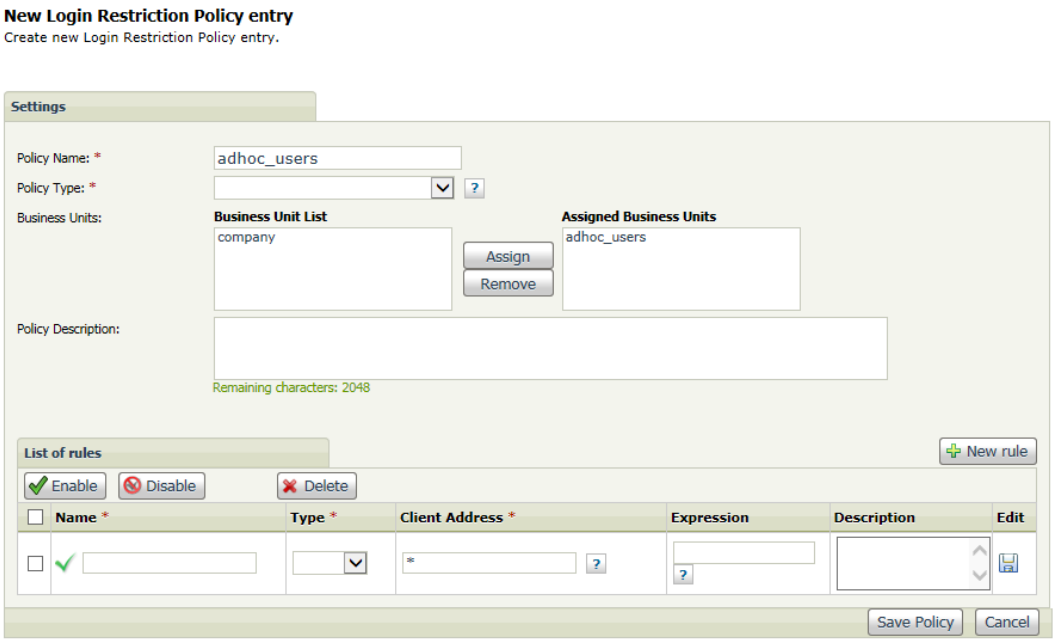
3. Click **Save Policy**.

Adding a policy rule

Use the following instructions to add a policy rule to Login Restriction Policy.

1. Click **New Rule**.

   The **New Rule** fields open on *List of Rules* pane.



2. Enter a policy rule **Name**.
3. Select a policy rule **Type**.

   If `Allow` is selected, the policy rule is set to **Allow** the Client Address.

   If `Deny` is selected, the policy rule is set to **Deny** the Client Address.
4. Enter a **Client Address** for the policy rule. Valid client address types are:
   - **Allow All**: Use asterisk (*) to allow all client addresses.
   - **IPv4 address**: Use an exact IPv4 to specify a single host.

     Examples:

     `172.23.34.45;127.0.0.1;`
   - **IPv6 address**: Use an exact IPv6 to specify a single host (two colons (::) can represent one sequence of zero bits).

     Examples:

     `FC00:1234:56:0:0:0:AB:EF;FC00:1234:56::AB:EF;::1`
   - **IPv4 CIDR**: Classless Inter-Domain Routing (CIDR) notation specifies an IPv4 address and a number of significant bits separated by a slash (`/`). Use CIDR notation to represent a range of IP addresses.

     Examples:

     `172.23.34.0/24` represents `172.23.34.0` through `172.23.34.255`
   - **IPv6 CIDR**: Classless Inter-Domain Routing (CIDR) notation specifies an IPv6 address and a number of significant bits separated by a slash (/). Use CIDR notation to represent a range of IP addresses.

     Examples:

`FC00:1234:56::/120` represents `FC00:1234:56::` through `FC00:1234:56::FF`

- **Specific host name**: Use a literal host name to represent a single host where host names are valid. The host name must resolve to a valid IPv4 or IPv6 address.

  Example:

  `appserver.example.com`

- **Wild-carded host name using the character * as wildcard**: Use a host name pattern that uses asterisk (`*`) to represent one or more characters. The pattern specifies any host whose name matches.

  Examples:

  `*.example.com`; `example.*`

5. (Optional) Enter an **Expression** for the policy rule.

   Specify an expression using SecureTransport expression language. Use the following named variable sets:

   - `${sess['variable']}`
   - `${env['variable']}, ${stenv['variable']}, or ${stenv.variable}`

   If such expression is specified, then a rule will be considered to match if both client address matches and expression evaluates to true.

   If such expression is not specified then it is not taken into account. Just the client address is considered.

   Example:

   `${stenv.loginname =='user1'}`

   You can create a rule that limits the possible concurrent open sessions by a user. To do this, you must use the `currentSessions`variable and evaluate it against the threshold value you set in your rule.
   Example:

   `${currentSessions <= 3}` - this example puts a session limit of up to 3 current sessions per user

   Note To restrict user logins to a specific Edge server or a network zone, we can use two variables:

   - The `DXAGENT_CLIENTADDR` variable effectively represents an Edge server hostname (or an IP address depending on the network setup) and is always present when connecting through an Edge server. It can be used in LRP expressions as `{stenv.clientaddr} or ${sess.clientaddr}`.

- When connecting through an Edge server, the value of the `DXAGENT_EDGEID` variable is taken from the configuration option `EdgeId`. This configuration option is defined by a SecureTransport administrator and is valid for FTP and HTTP daemons only. It can be used in LPR expressions as `{stenv.edgeid} or ${sess.edgeid}`.

When a user logs in through the Private zone (that is through Backend protocol daemons), these variables are not available in the environment, and in this case the only valid expression is `${empty sess.clientaddr} or ${empty sess.edgeid}`.

You may use custom HTTP headers in LRP expressions, where the name of the HTTP header must be capitalized and all dashes must be replaced by underescores.
For example: ${env['DXAGENT_HTTP_X_FORWARDED_FOR'] == '10.10.10.10'}

6. (Optional) Enter a **Description** for the policy rule.
7. Click the **Save** ( ) icon.

Editing a policy rule

Use the following instructions to edit a policy rule:

1. Click the **Edit** ( ) icon for the policy rule.
2. Make the desired changes to the policy rule. For additional information, refer to *Adding a policy rule* on page 752.
3. Click the **Save** ( ) icon.

Enabling a policy rule

Use the following instruction to enable a policy rule or rules:

1. Select the policy rule or rules to enable using the **Policy Rule** check boxes.
2. Click **Enable**.

Disabling a policy rule

Use the following instruction to disable a policy rule or rules:

1. Select the policy rule or rules to disable using the **Policy Rule** check boxes.
2. Click **Disable**.

Deleting a policy rule

Use the following instruction to delete a policy rule or rules:

1. Select the policy rule or rules to delete using the **Policy Rule** check boxes.
2. Click **Delete**.
3. Confirm the policy rule or rules deletion.

Applications 12

This section introduces Axway SecureTransport applications and describes how to use the Applications menu features of the SecureTransport Administration Tool.

Application overview

In SecureTransport, *applications* are sets of workflow you can create to perform file processing, including the following:

- Transform data
- Schedule file transfers
- Route files
- Monitor shared folder monitoring across user accounts
- Trigger sequential sets of actions

An application is defined as an instance of a set of workflow called an *application type*. Once you have defined an application, you create a connection between an application and one or more *accounts*. Such a connection is defined through a *subscription*.

SecureTransport ships with the following built-in application types:

- **Archive Maintenance** – Automatically deletes archived files based on a schedule you define.

  See *Create an Archive Maintenance application* on page 760.
- **Audit Log Maintenance** – Automatically deletes Audit log records that are older than a specified number of days or months (6 months by default). You can schedule how often to run this application and configure it to optionally export these records prior to deletion.

  See *Create an Audit Log Maintenance application* on page 763.
- **Axway Sentinel Link Data Maintenance** – Removes all SentinelLinkData entries to files that do not exist anymore, based on a schedule you define.

  See *Create an Axway Sentinel Link Data Maintenance application* on page 765.
- **Axway Transfer CFT** – Enables Axway Transfer CFT to push files to SecureTransport.

  See *Create an Axway Transfer CFT application* on page 766.
- **Basic Application** – Processes server-initiated transfers and performs data transformations.

  See *Create a Basic Application* on page 767.
- **File Transfer via File Services Interface** – Processes metadata files sent from another system for a protocol implemented using the file services interface.

  See *Create a File Transfer via File Services Interface application* on page 768.

- **Human to System** – Provides a way to route H2S file transfers.

  See *Create a Human to System application* on page 769.

- **Log Entry Maintenance** – Automatically deletes Server log records that are older than a specified number of days, hours or minutes (1 day by default). You can schedule how often to run this application and configure it to optionally export these records prior to deletion.

  See *Create a Log Entry Maintenance application* on page 770.

- **Login Threshold Maintenance** – Unlocks accounts locked according to the selected "Lock account after N successful logins" option in the *Account settings* and sends a report to specified email contacts.

  See *Create a Login Threshold Maintenance application* on page 774.

- **Package Retention Maintenance** – Deletes expired file packages from ad hoc file transfers.

  See *Create a Package Retention Maintenance application* on page 776.

- **Shared Folder** – Provides shared data storage between accounts.

  See *Create a Shared Folder application* on page 778.

- **Site Mailbox** – Similar to Basic application, however with dedicated outbox and inbox folders for files transfers using a transfer site. This application is recommended for AS2 transfer sites.

  See *Create a Site Mailbox application* on page 779.

- **Standard Router** – Provides basic options to automate flows for file transformations, routing and transfers between an account and internal systems.

  See *Create a Standard Router application* on page 780.

- **Advanced Routing** – Provides options to create complex automated flows for file transformations, routing and transfers between different participants, partner systems, and applications.

  See *Advanced Routing* on page 795.

- **Transfer Log Maintenance** – Automatically deletes Transfer log records that are older than a specified number of days (30 days by default). You can schedule how often to run this application and configure it to optionally export these records prior to deletion.

  See *Create a Transfer Log Maintenance application* on page 786.

- **Unlicensed Accounts Maintenance** – Deletes inactive unlicensed user accounts older than a specified number of days (60 days by default). You can schedule how often to run this application.

  See *Create a Unlicensed Accounts Maintenance application* on page 792.

Manage applications

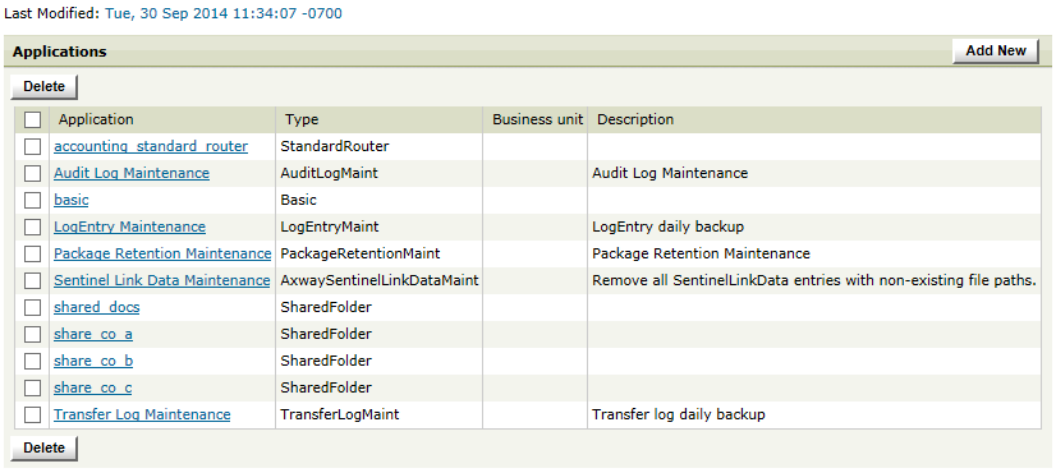
This short subtopic provides brief instructions on how to access, edit, and delete already created applications.

At the bottom of this section you will find links for creating every application.

Access applications

Use the **Application** menu to access applications.

The following example shows the main page that opens from the menu:

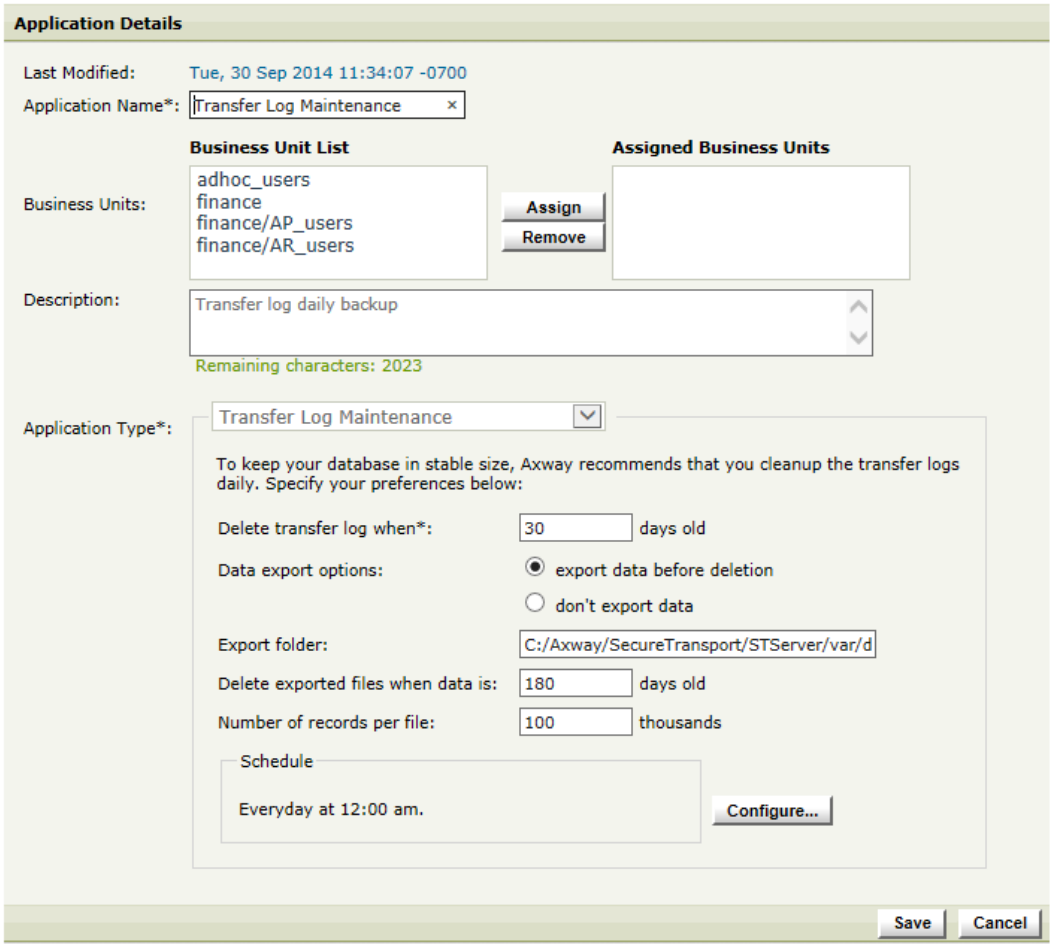


The *Applications* page lists all the applications available currently on the system. Use it to add, delete, view, and edit applications.

View or edit an application

Use the following procedure to view or edit an application.

1. Select **Application**. The *Applications* page is displayed.
2. Click the name of the application you want to view or edit. The *Application Details* page the application you selected is displayed.



3. View or edit the information displayed.

   The *Application Details* page varies for the different application types. It dynamically displays the attributes for the respective application type. You can edit all the standard settings of an application, except application type.

4. If you edit the information, click **Save** to preserve the changes.

Delete an application

Use the following procedure to delete an application.

1. Select **Application**. The *Applications* page is displayed.
2. Select the check box for the application you want to delete.
3. Click **Delete**.
4. When prompted, confirm that any subscription to this application will be lost.

Note When you delete an application, all subscriptions to this application are removed.

Create applications

Every application in SecureTransport must be based on an application type. Currently, SecureTransport supports 16 application types. The following topics describe the specific attributes and considerations for and how to create applications of each application type:

- *Create an Archive Maintenance application* on page 760
- *Create an Audit Log Maintenance application* on page 763
- *Create an Axway Sentinel Link Data Maintenance application* on page 765
- *Create an Axway Transfer CFT application* on page 766
- *Create a Basic Application* on page 767
- *Create a File Transfer via File Services Interface application* on page 768
- *Create a Human to System application* on page 769
- *Create a Log Entry Maintenance application* on page 770
- *Create a Login Threshold Maintenance application* on page 774
- *Create a Package Retention Maintenance application* on page 776
- *Create a Shared Folder application* on page 778
- *Create a Site Mailbox application* on page 779
- *Create a Standard Router application* on page 780
- *Create a Transfer Log Maintenance application* on page 786
- *Create a Unlicensed Accounts Maintenance application* on page 792

For instructions on creating an Advanced Routing application, see *Create Advanced Routing application* on page 805.

Create an Archive Maintenance application

The Archive Maintenance application automatically deletes archived files based on a schedule you define.

You must enable the `ArchiveMaintApp` rules package in the Transaction Manager before you can use an Archive Maintenance application. For more information, see *Manage rules packages* on page 207.

The configuration for an Archive Maintenance application is stored in the database.

Note If the database partition feature is not available because the export database feature is not installed, a warning message will be displayed. For additional information, refer to the *SecureTransport Installation Guide*.

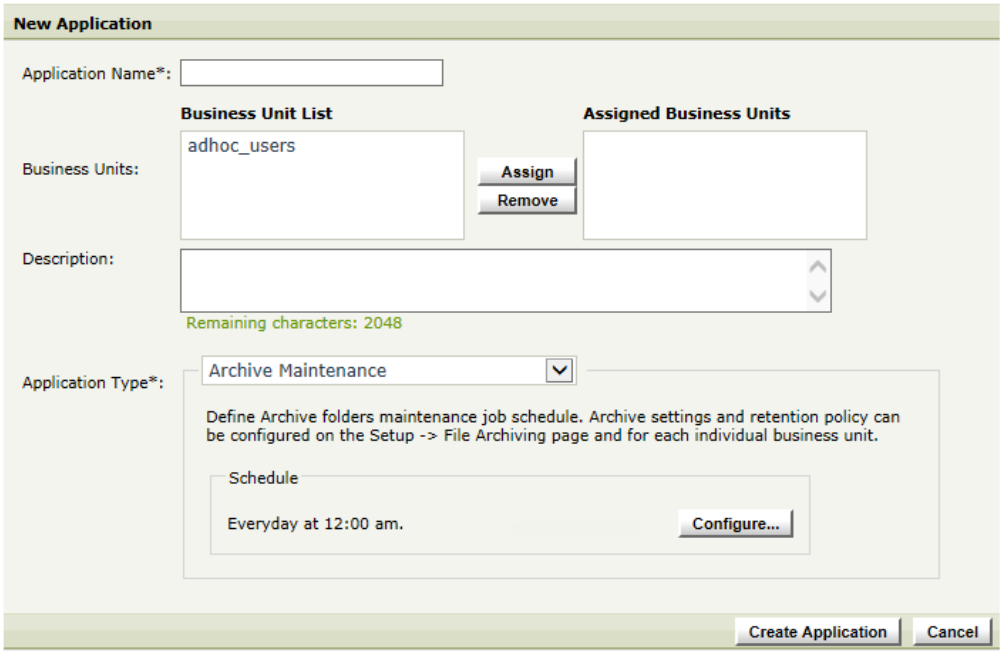
The Archive Maintenance application defines the file archiving maintenance job schedule. Archive settings and retention policy can be configured on the **Setup > File Archiving** page and for each individual business unit.

For information on configuring the file archiving global configuration, refer *File archiving global configuration* on page 213.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Archive Maintenance** from the mandatory **Application Type** list.



3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

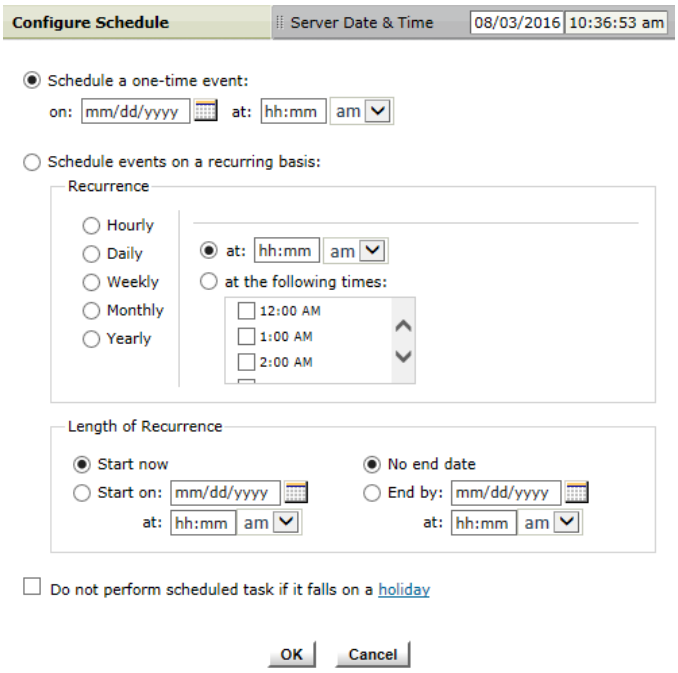
   Note The application name cannot include any forward slash (/) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.

5. (Optional) Enter an application **Description**.

6. (Optional) In the *Schedule* pane, click **Configure** to schedule a future task or to schedule a series of future tasks.

   The *Configure Schedule* dialog box is displayed.



7. Set a recurring schedule for some period of time less than or equal to the value you specified in the **Delete preserved files when** fields. Deletes files older than the options set for the **Delete archived files after** field on the global *File Archiving* page.

   To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

   Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

   For information on working with the SecureTransport scheduler , see *Scheduled downloads and tasks* on page 616. Click **OK** when finished setting the schedule.

8. Click **Create Application**.

   To use the Archive Maintenance application, make sure that the `ArchiveMaintApp` and the `ArchiveAgent` rules packages are enabled in the *Rules Packages* page.

Enable Multithreading

When the Archive maintenance application is to process a large number of files, it can be executed multi-threaded. To enable multithreading, set the number of threads to execute file deletion in the `FileArchiving.DeleteFiles.ProcessingThreads` configuration option.

Increasing the number of threads increases the load on the storage on which the application operates. The number of threads should not exceed 16.

Set maximum run time

Occasionally, if the Archive Maintenance application is processing a large number of files, it may not be able to finish until the next scheduled occurrence. In this case, it may be advisable to specify the maximum time (in minutes) that you expect the application to run in the `FileArchiving.DeleteFiles.MaximumProcessingTime` configuration option. If you set it to `0`, the application continues to run until it completes.

Create an Audit Log Maintenance application

The Audit Log Maintenance application automatically deletes Audit log records that are older than a specified number of days or months (6 months by default). You can schedule how often to run this application and configure it to optionally export these records prior to deletion.

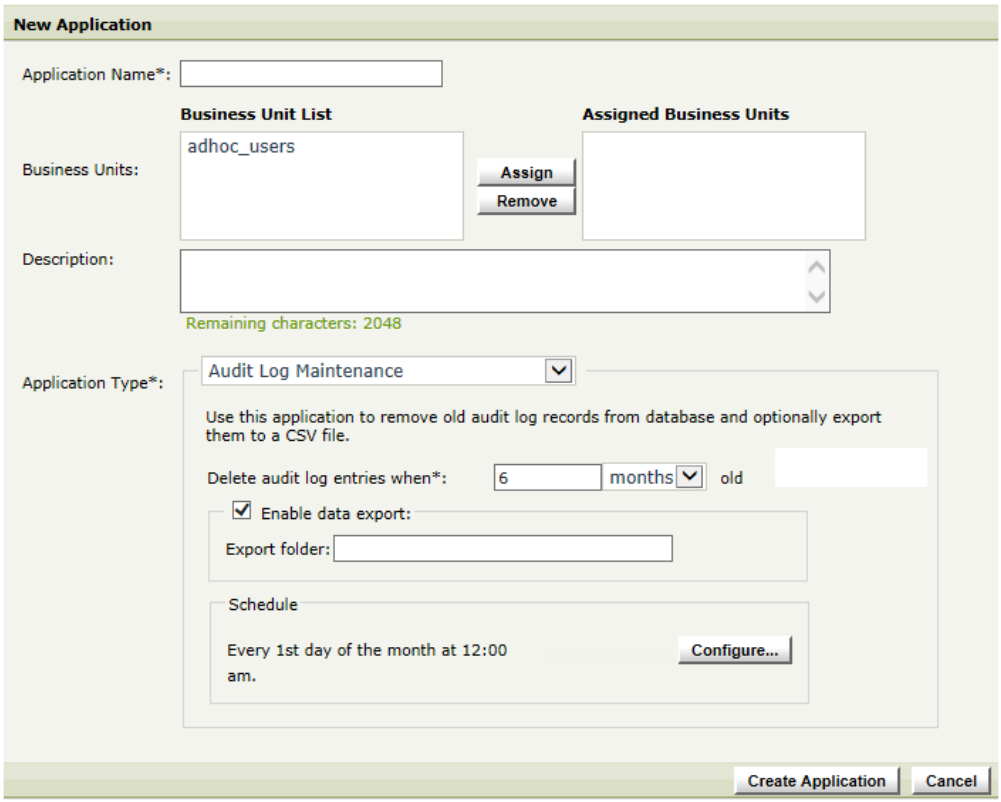
Make sure that the `AuditLogMaintApp` rules package is enabled in the Transaction Manager before you enable an Audit Log Maintenance application. For more information, see *Manage rules packages* on page 207.

Use the following procedure to create an Audit Log Maintenance application.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Audit Log Maintenance** from the mandatory **Application Type** list.



3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (/) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.

   Note As with all applications, assigning business units to the application controls which delegated administrators can manage the application. It does not control which log entries Transfer Log Maintenance processes.

5. (Optional) Enter an application **Description**.

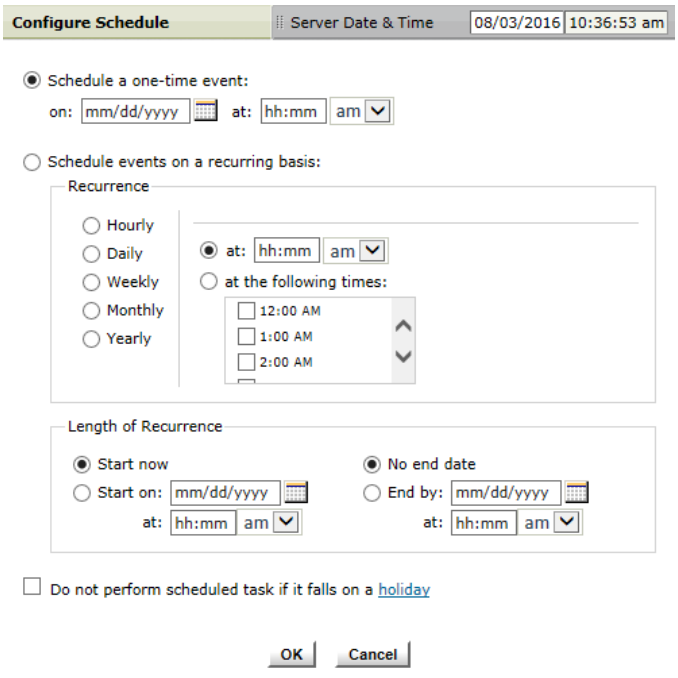
6. In the **Delete audit log entries when** field, specify in days or months how old transfer log entries will be when they are deleted. This field is mandatory.

   You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

7. To export the deleted audit log entries to a file before they are deleted, select **Enable data export**, and, in the **Export folder** field, specify where the export files are stored. You must enter a full directory path.

8. (Optional) In the *Schedule* pane, click **Configure** to schedule a future task or to schedule a series of future tasks.

   The *Configure Schedule* dialog box is displayed.



   To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

For information on working with the SecureTransport scheduler , see *Scheduled downloads and tasks* on page 616. Click **OK** when finished setting the schedule.

9. Click **Create Application**.

- *Manage applications* on page 757

Create an Axway Sentinel Link Data Maintenance application

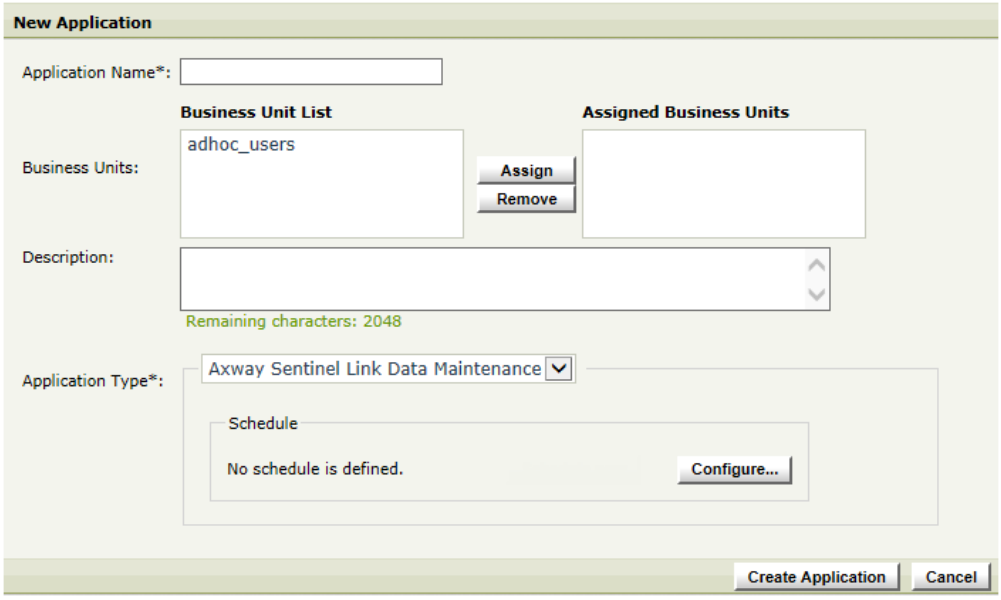
The Axway Sentinel Link Data Maintenance application removes all SentinelLinkData entries to files that do not exist anymore, based on a schedule you define.

Use the following procedure to create an Axway Sentinel Link Data Maintenance type application.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Axway Sentinel Link Data Maintenance** from the mandatory **Application Type** list.



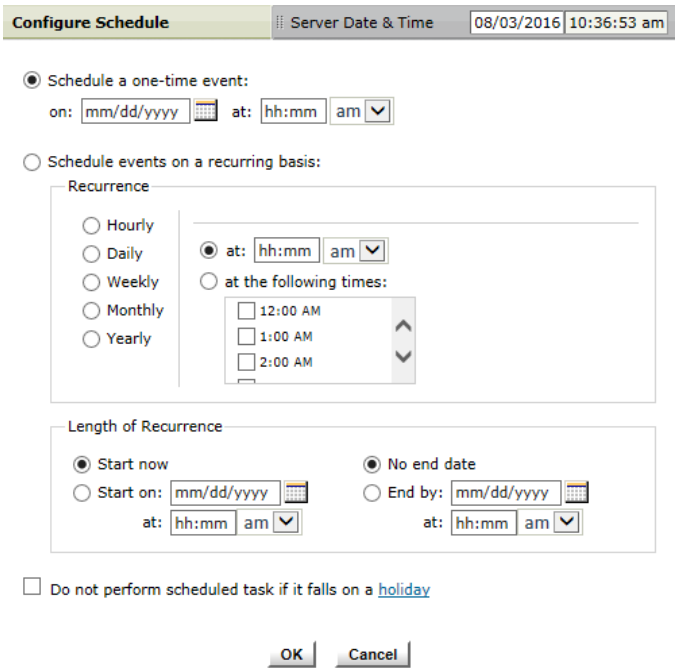
3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (/) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.

5. (Optional) Enter an application **Description**.
6. (Optional) In the *Schedule* pane, click **Configure** to schedule a future task or to schedule a series of future tasks.

   The *Configure Schedule* dialog box is displayed.



   To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

   Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

   Define the schedule for Sentinel link data maintenance. For information on working with the SecureTransport scheduler, see *Scheduled downloads and tasks* on page 616. Click **OK** when finished setting the schedule.
7. Click **Create Application**.

Create an Axway Transfer CFT application

The Axway Transfer CFT application enables Axway Transfer CFT to push files to SecureTransport.

You must enable the `AxwayTransferCFT` rules package in the Transaction Manager before you can use an Axway Transfer CFT application. For more information, see *Manage rules packages* on page 207.

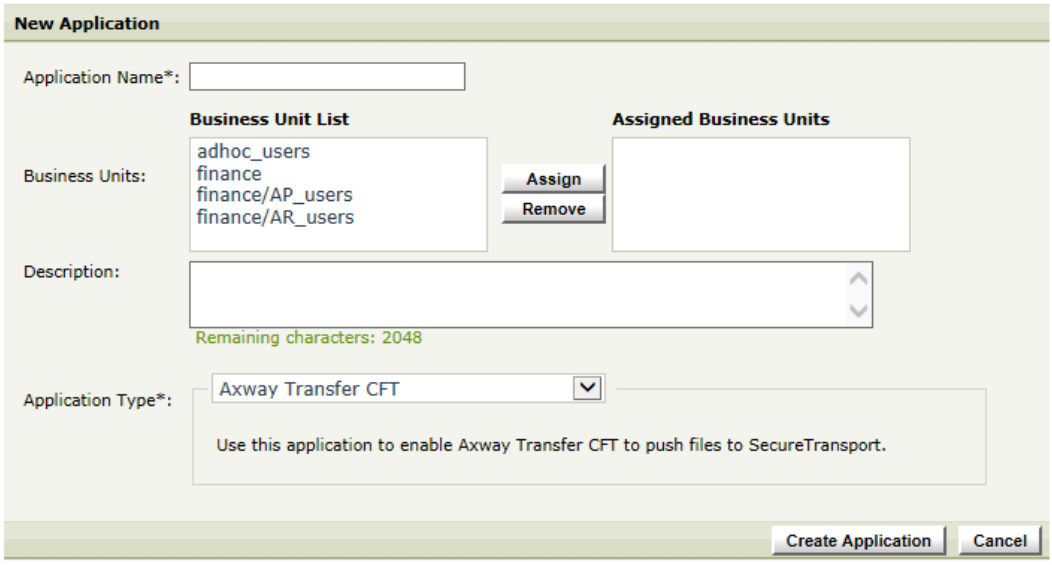
Note This application is not needed for Transfer CFT communication and is used only for legacy configurations.

Use the following procedure to create an Axway Transfer CFT application.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Axway Transfer CFT** from the mandatory **Application Type** list.



3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (`/`) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.

5. (Optional) Enter an application **Description**.

6. Click **Create Application**.

Create a Basic Application

The Basic Application performs server-initiated transfers and data transformations without file routing.

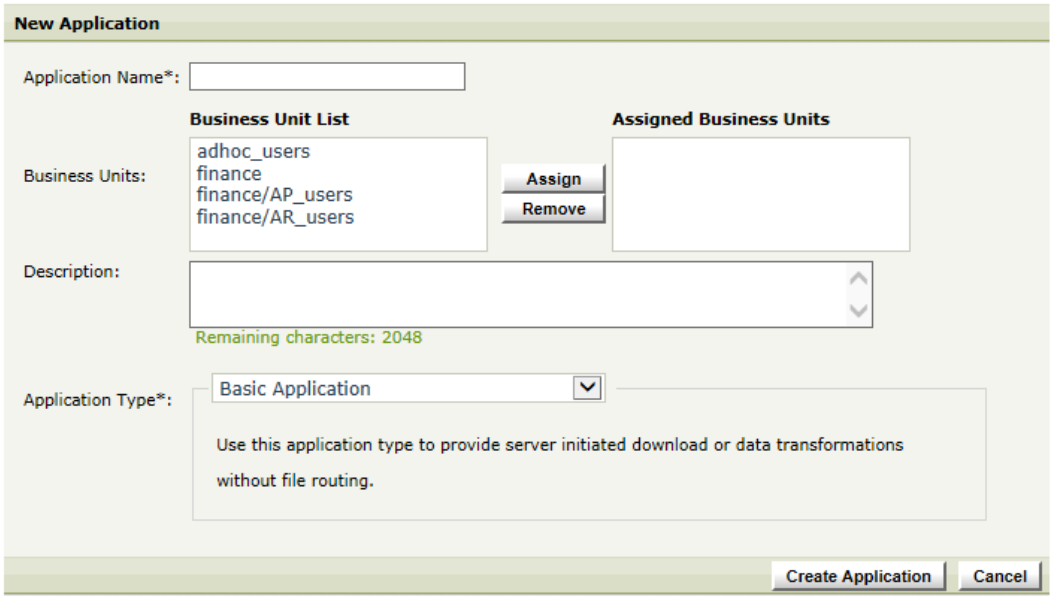
You must enable the `BasicApp` rules package in the Transaction Manager before you can use a Basic Application. For more information, see *Manage rules packages* on page 207.

Use the following procedure to create a Basic Application application.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Basic Application** from the mandatory **Application Type** list.



3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (`/`) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.
5. (Optional) Enter an application **Description**.
6. Click **Create Application**.

Create a File Transfer via File Services Interface application

The File Transfer via File Services Interface application processes metadata files sent from another system for a protocol implemented using the file services interface.

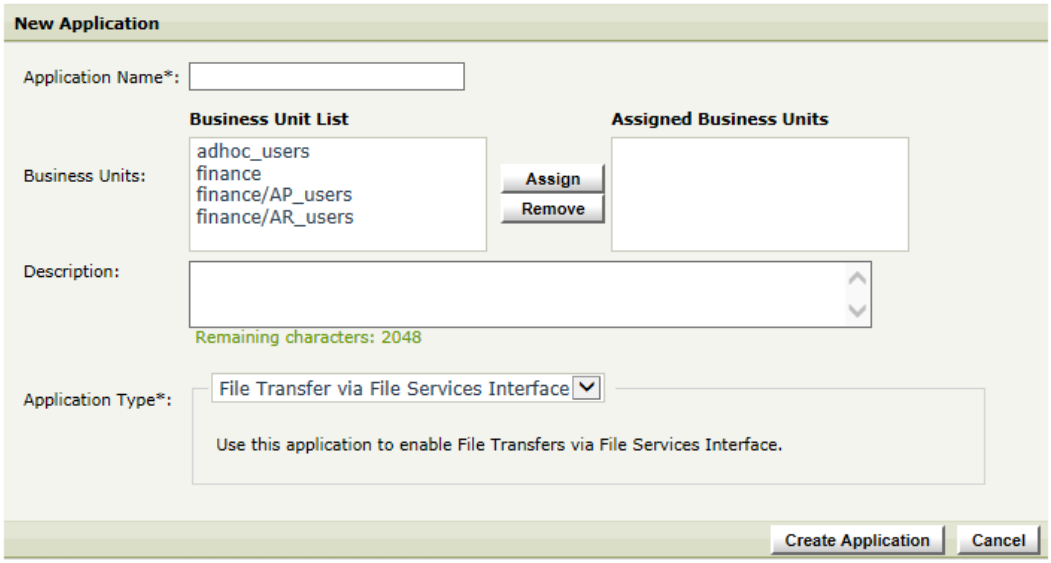
You must enable the `FileServicesInterface` rules package in the Transaction Manager before you can use a File Transfer via File Services Interface application. For more information, see *Manage rules packages* on page 207.

Use the following procedure to create a File Transfer via File Services Interface application.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **File Transfer via File Services Interface** from the mandatory **Application Type** list.



3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (`/`) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.
5. (Optional) Enter an application **Description**.
6. Click **Create Application**.

For more information about configuring transfers using a file services interface protocol, see *File services interface transfers* on page 958.

Create a Human to System application

The Human to System application provides a way to route H2S file transfers.

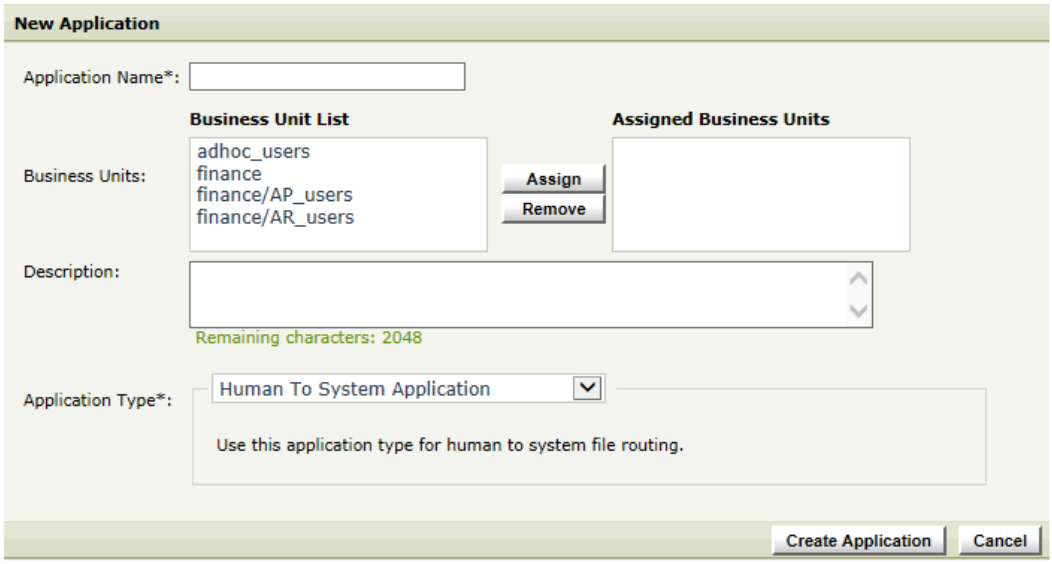
You must enable the `HumanSystem` rules package in the Transaction Manager before you can use a Human to System application. For more information, see *Manage rules packages* on page 207.

Use the following procedure to create a Human to System application.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Human To System Application** from the mandatory **Application Type** list.



3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (`/`) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.
5. (Optional) Enter an application **Description**.
6. Click **Create Application**.

Create a Log Entry Maintenance application

The Log Entry Maintenance application automatically deletes Server log records that are older than a specified number of days, hours or minutes (1 day by default). You can schedule how often to run this application and configure it to optionally export these records prior to deletion.

You must enable the `LogEntryMaintApp` rules package in the Transaction Manager before you can use a Log Entry Maintenance application. For more information, see *Manage rules packages* on page 207.

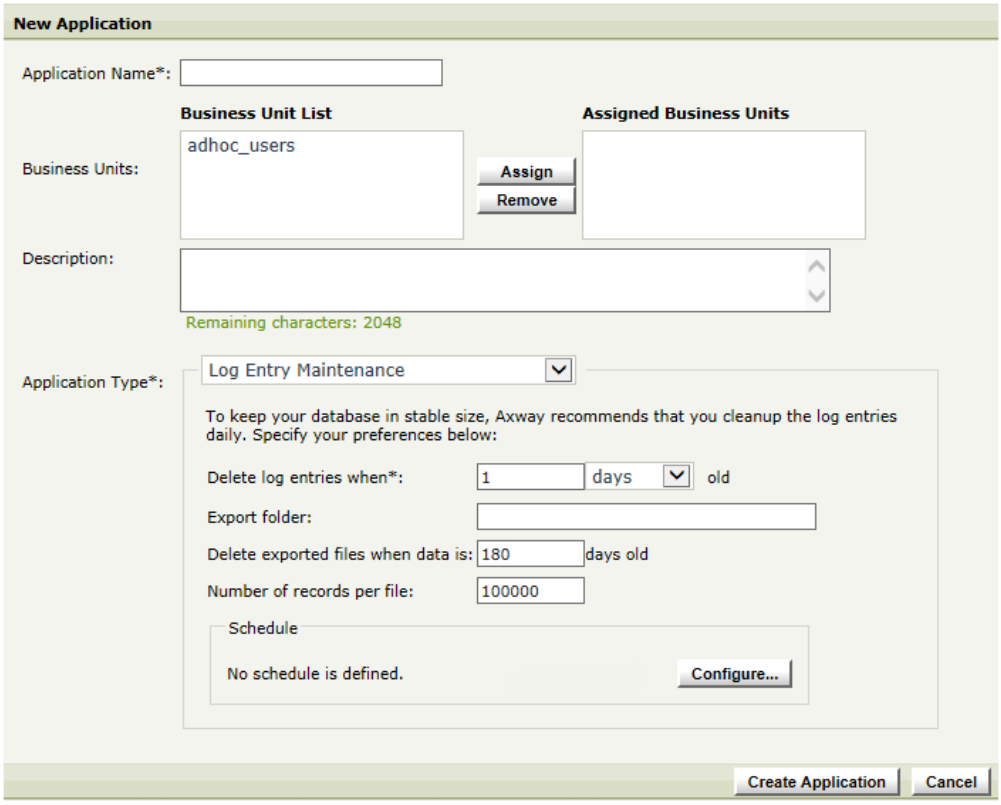
Use the following procedure to create a Log Entry Maintenance application.

Note You can also use the `log_export` command-line utility to export server log entries.

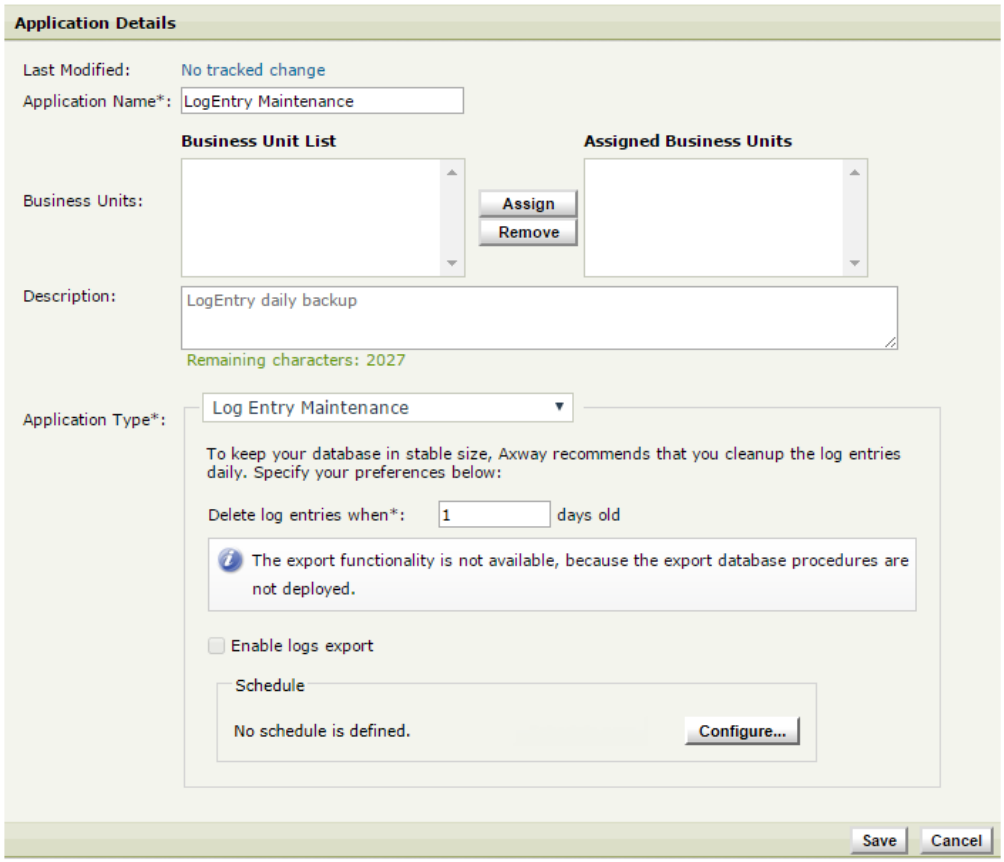
1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Log Entry Maintenance** from the mandatory **Application Type** list.



For an external Oracle database where the export functionality is not available, the following page is displayed.



Note When your server uses an Oracle database, the **Export folder** and **Number of records per file** fields is not displayed. Instead, SecureTransport uses a partitioned table for the log entries. Your Oracle DBA can implement data export using Oracle functionality.

Note When your server uses an Oracle database and the export database procedures are not deployed, the **Enable logs export** checkbox is disabled and following message is displayed: "The export functionality is not available, because the export database procedures are not deployed."

Note The granularity of Oracle databases are in days.

3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (/) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.
5. (Optional) Enter an application **Description**.
6. In the **Delete log entries when** field, specify how old log entries will be when they are deleted in terms of days, hours, or minutes.

You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

7. In the **Export folder** field, specify where the export files are stored. You must enter a full directory path. If you are exporting from an Oracle database, you must fill in the name of the directory defined in the Oracle database (for example, `ST_DMPDIR`). On the Oracle Server:
   a. Create the directory where the logs will be exported and make sure that the Oracle user has permissions.
   b. Log in into Oracle as SYSDBA and create the `ST_DMPDIR` directory using the following syntax:

      ```
      CREATE DIRECTORY ST_DMPDIR AS '/YOUR_DIRECTORY_HERE';
      ```

   c. Grant all privileges on the directory to the ST user:

      ```
      GRANT ALL PRIVILEGES ON DIRECTORY ST_DMPDIR TO ST_
      DATABASE_USER
      ```

   d. Grant create table privileges to the ST user:

      ```
      GRANT CREATE TABLE TO ST_DATABASE_USER;
      ```

   If you are exporting from a Microsoft SQL Enterprise Edition database, you must complete the following steps on the database server:
   a. Create an export directory on the Microsoft SQL Server.
   b. Create a new filegroup:

      ```
      ALTER DATABASE databaseuser ADD FILEGROUP [ST_SERVERLOG_
      ARCHIVE]
      ```

   c. Create a file:

      ```
      ALTER DATABASE databaseuser
           ADD FILE
           (NAME = N'ST_SERVERLOG _ARCHIVE_databaseuser',
           FILENAME = N'<EXPORT_DIR>\ST_SERVERLOG_ARCHIVE_
      databaseuser.ndf',
           SIZE = 10MB,
           MAXSIZE = 100MB,
           FILEGROWTH = 1MB)
           TO FILEGROUP [ST_SERVERLOG_ARCHIVE]
      GO
      ```

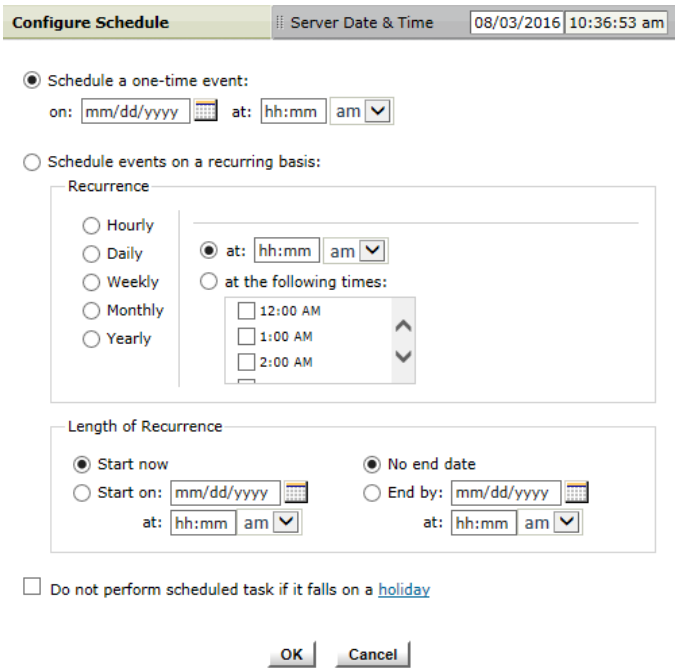
   d. Grant all permissions on the `<EXPORT_DIR>` directory created in step "a" to the database user.
   e. Grant the database user **Backup database** and **Backup log** permissions.

      Note The **Backup log** permission is only required if the database is in **Full recovery mode**.

8. In the **Delete exported files when data is: ____ days old** field, specify when SecureTransport deletes old exported log entry data.

9. In the **Number of records per file** field, specify the maximum number of records that can exist in an exported file. When this value is exceeded, SecureTransport starts to export the server log entries in a new file.
10. (Optional) In the *Schedule* pane, click **Configure** to schedule a future task or to schedule a series of future tasks.

    The *Configure Schedule* dialog box is displayed.



    To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

    Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

    For information on working with the SecureTransport scheduler , see *Scheduled downloads and tasks* on page 616. Click **OK** when finished setting the schedule.
11. Click **Create Application**.

Create a Login Threshold Maintenance application

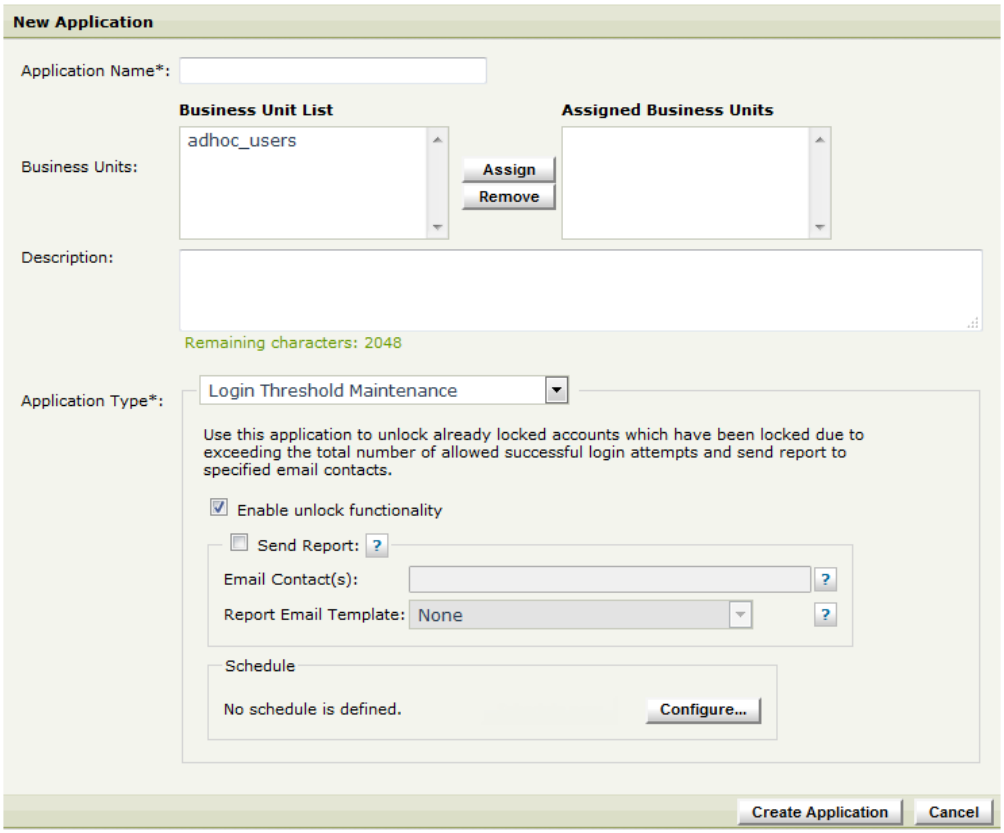
The Login Threshold Maintenance application unlocks accounts locked according to the selected "Lock account after N successful logins" option in the *Account settings* and sends a report to specified email contacts.

Use the following procedure to create a Login Threshold Maintenance application.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Login Threshold Maintenance** from the mandatory **Application Type** list.



3. Enter an unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (/) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.

5. (Optional) Enter an application **Description**.

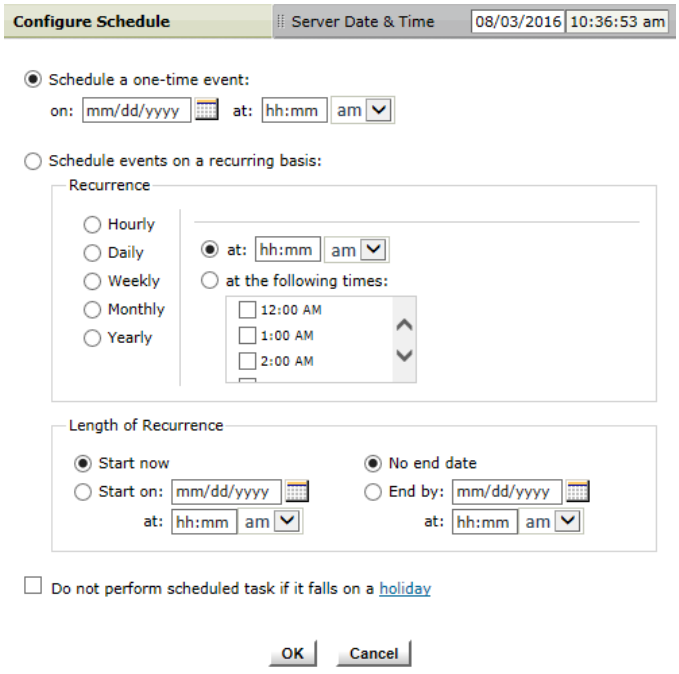
6. (Optional) Select **Enable unlock functionality**. **Enable unlock functionality** is selected by default.

7. (Optional) Select **Send Report**. If **Send Report** is selected, a report will be sent to the specified email addresses.

   - If **Enable unlock functionality** is selected, the report will contain a list of unlocked users.
   - If **Enable unlock functionality** is not selected, the report will contain a list of locked, due to login threshold functionality, users.

8. Enter the email address or addresses to deliver the report to in the **Email Contact(s)** field. Email addresses can be separated by either a comma or a semicolon.
9. Select the email template for the report from the **Report Email Template** list. The `LoginThresholdReport.xhtml` template is the default template for the Login Threshold Maintenance application.
10. (Optional) In the *Schedule* pane, click **Configure** to schedule a future task or to schedule a series of future tasks.

    The *Configure Schedule* dialog box is displayed.



    To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

    Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

    For information on working with the SecureTransport scheduler , see *Scheduled downloads and tasks* on page 616. Click **OK** when finished setting the schedule.
11. Click **Create Application**.

Create a Package Retention Maintenance application

The Package Retention Maintenance applicaiton deletes expired file packages from ad hoc file transfers.

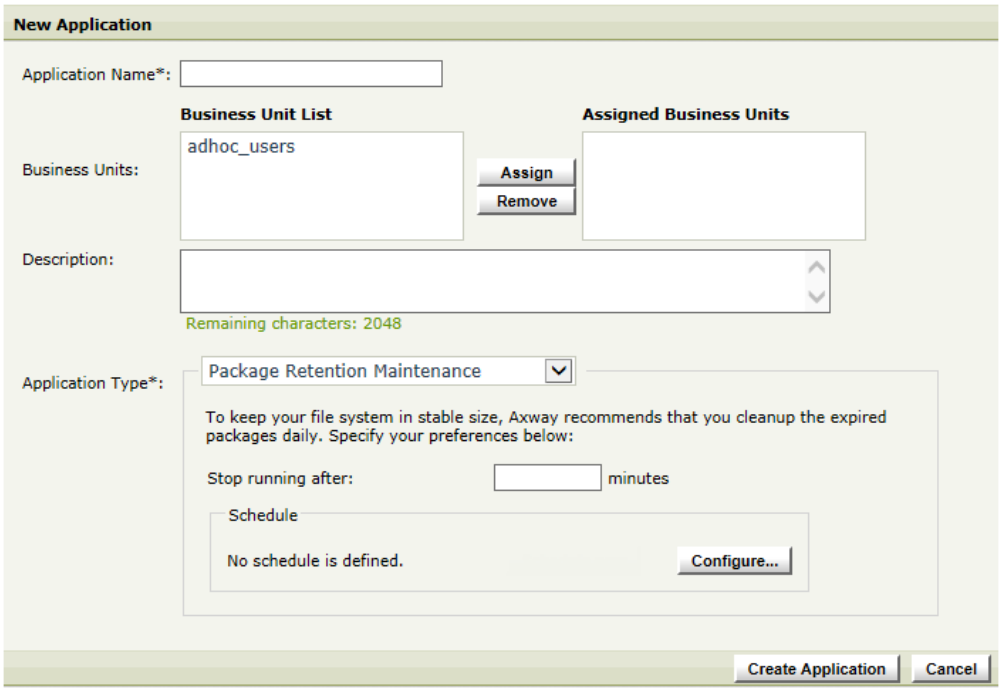
You must enable the `PackageRetentionMaintApp` rules package in the Transaction Manager before you can use a Package Retention Maintenance application. For more information, see *Manage rules packages* on page 207.

Use the following procedure to create a Package Retention Maintenance application.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Package Retention Maintenance** from the mandatory **Application Type** list.

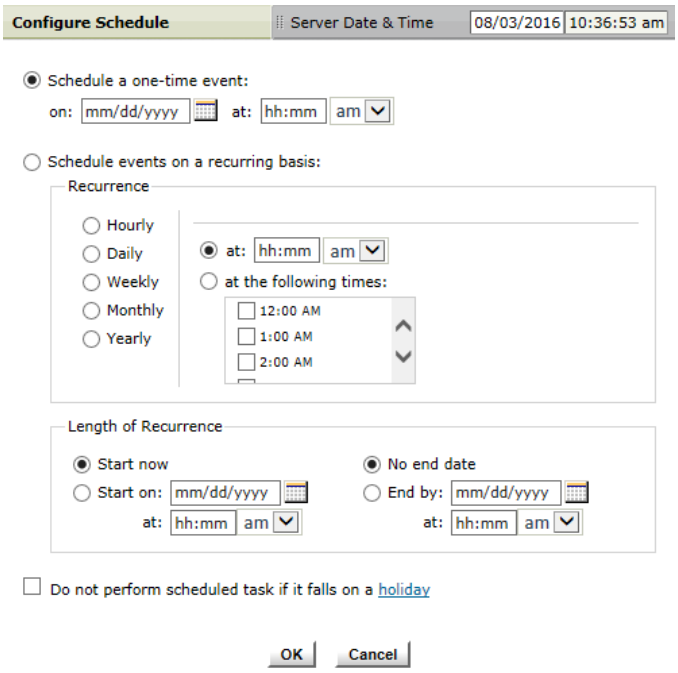


3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (`/`) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.
5. (Optional) Enter an application **Description**.
6. In the **Stop running after: _____ minutes** field, enter the maximum number of minutes the application runs each time it is started.
7. (Optional) In the *Schedule* pane, click **Configure** to schedule a future task or to schedule a series of future tasks.

   The *Configure Schedule* dialog box is displayed.



To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

For information on working with the SecureTransport scheduler , see *Scheduled downloads and tasks* on page 616. Click **OK** when finished setting the schedule.

8. Click **Create Application**.

Create a Shared Folder application

The Shared Folder application provides shared data storage between accounts.

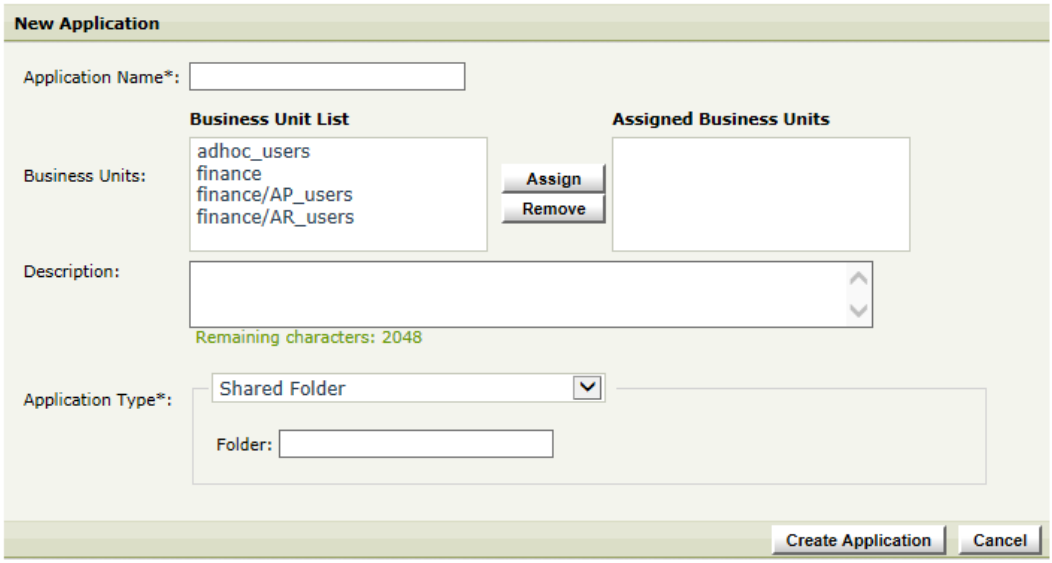
You must enable the `SharedFolder` rules package in the Transaction Manager before you can use a Shared Folder application. For more information, see *Manage rules packages* on page 207.

All users of a shared folder must be either repository encryption users or not repository encryption users.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Shared Folder** from the mandatory **Application Type** list.



3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (`/`) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.
5. (Optional) Enter an application **Description**.
6. In the **Folder** field, type the full path of the folder that you want to share for the accounts that subscribe to the new application.

   You cannot use the following characters in the folder path or name: `* < > ? " / \ | :`

   Note Under Windows, you use Windows-style paths when you specify a shared folder. Denote drives as `C:\` and `D:\`.

7. Click **Create Application**.

Create a Site Mailbox application

The Site Mailbox application is similar to the Basic application, however with dedicated outbox and inbox folders for files transfers using a transfer site. This application is recommended for AS2 transfer sites.

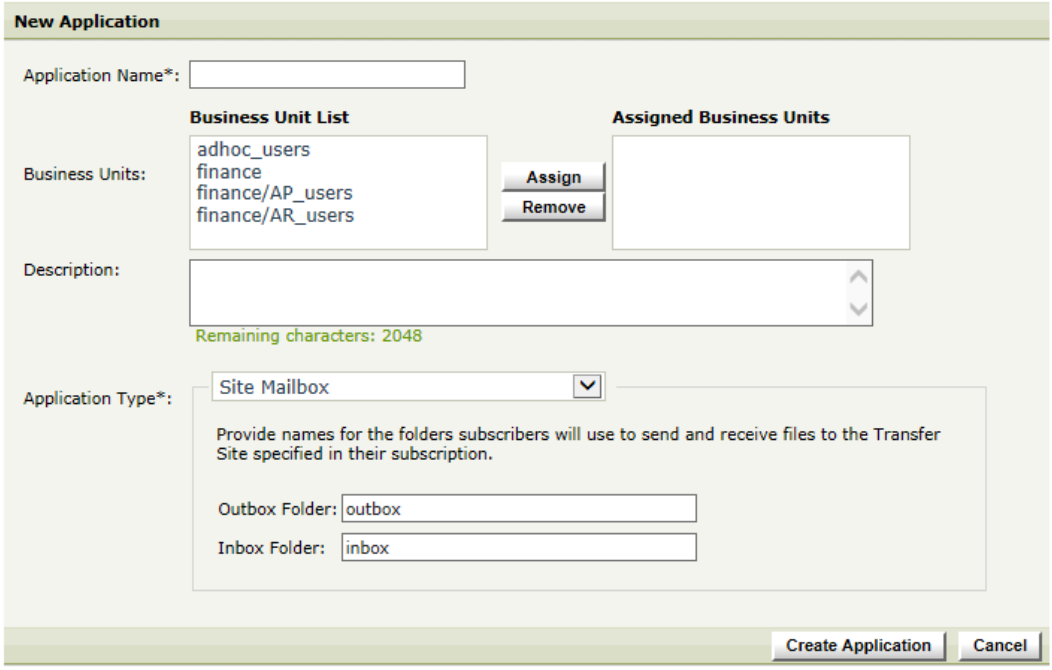
You must enable the `SiteMailbox` rules package in the Transaction Manager before you can use a Site Mailbox application. For more information, see *Manage rules packages* on page 207.

When a user account is subscribed to the Site Mailbox application, there are four subscription settings possible. Require Valid Signature and Require File Encryption are applied to the subscription folder for both incoming and outgoing transfers. Encrypt Files and Sign Files are applied only for the outgoing transfers

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Site Mailbox** from the mandatory **Application Type** list.



3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (`/`) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.

5. (Optional) Enter an application **Description**.

6. Under **Outbox Folder**, type the name of the folder subscribers use to send files. The default value is `outbox`.

7. Under **Inbox Folder**, type the name of the folder subscribers use to receive files. The default value is `inbox`.

8. Click **Create Application**.

Create a Standard Router application

The Standard Router application provides basic options to automate flows for file transformations, routing and transfers between an account and internal systems.

You must enable the `StandardRouter` rules package in the Transaction Manager before you can use a Standard Router application. For more information, see *Manage rules packages* on page 207.

Use the following procedure to create a Standard Router application.

Note A Standard Router application triggers a schedule, even if it is not subscribed to a user account.

When a Standard Router application is used, a file integrity check of receipts generated generates a message that there was no successful MDN comparison in the following cases:

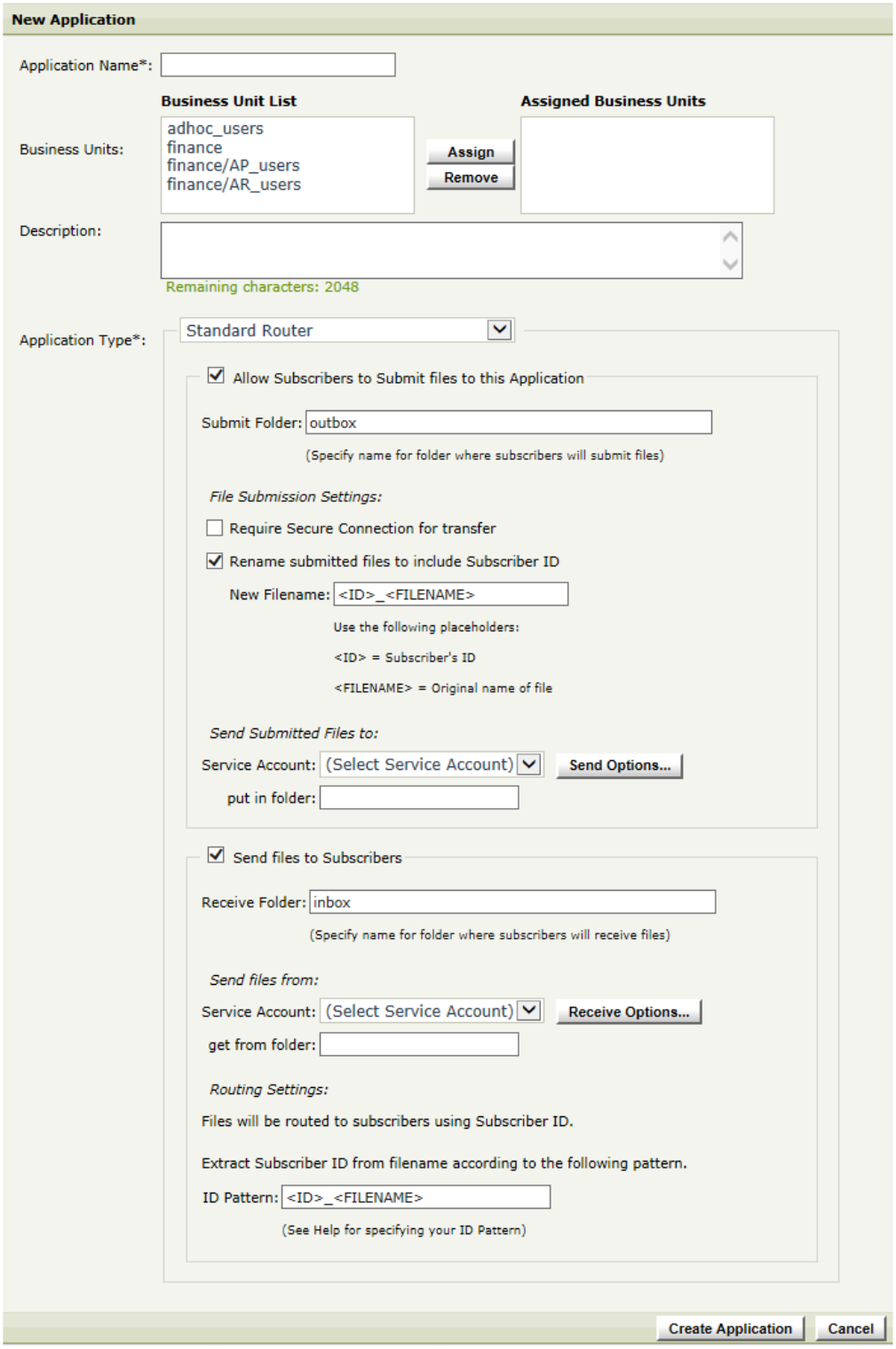
- When a file is uploaded in the user account outbox folder: The file is moved to the submit folder of the service account.
- When the service account pulls a file from its transfer site: The file is moved from the receive folder of the service account to the inbox folder of the user account.

Note You can set up the Standard Router as a one-way configuration by selecting only one of the two choices: **Allow Subscribers to Submit files to this Application** or **Send files to Subscribers**. When you set up a one-way configuration, you do not need to specify a folder.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Standard Router** from the mandatory **Application Type** list.



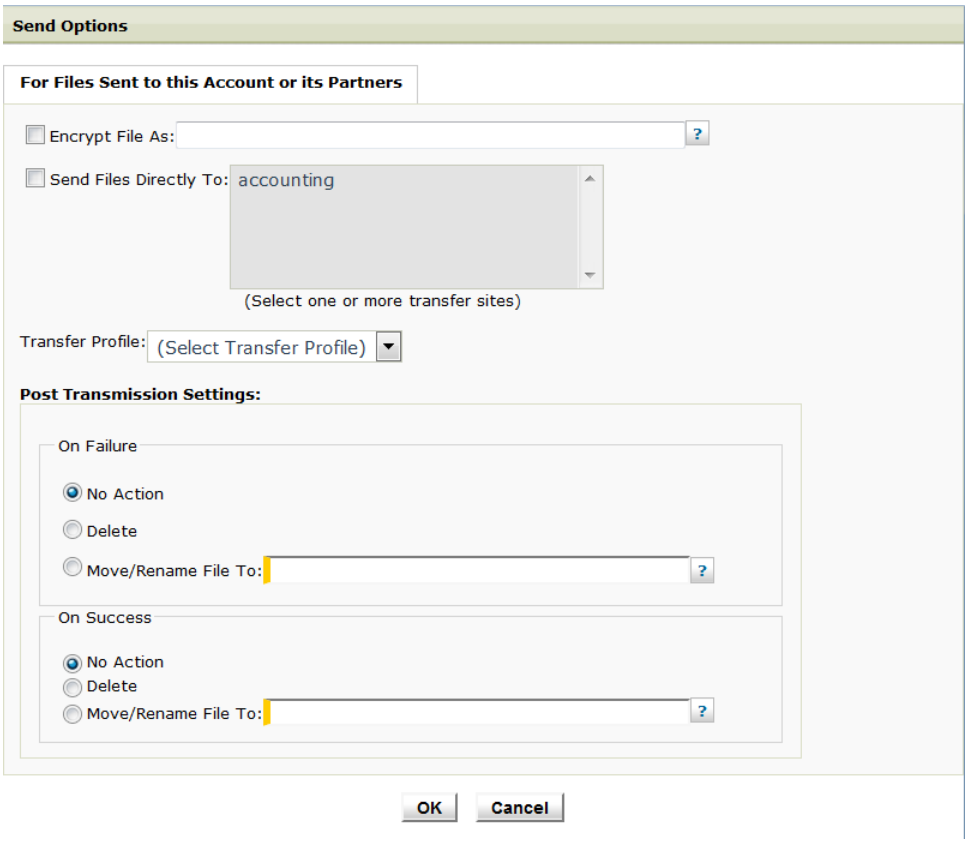
3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (/) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.
5. (Optional) Enter an application **Description**.
6. (Optional) Select **Allow Subscribers to Submit files in this Application** to permit incoming file transfers from the subscriber parties to the application. If you enable this option, continue specifying values for the parameters in the pane.
    a. In the **Submit folder** field, type the name of the folder where incoming transferred files are submitted via subscriptions. The application only processes files stored in the submit folder. Any files stored outside the submit folder are not routed for transferring. The submit folder is created as a sub-folder of the subscription folder. The subscription folder is specified during the creation of the respective subscription. For details, see *Transfer sites* on page 494.
    b. In the **File Submission Settings** group, select the **Require Secure Connection for transfer** option to enable SSL for the incoming transfers.
    c. In the **File Submission Settings** group, select the **Rename submitted files to include Subscriber ID** option to add a prefix to the file name identifying the sender before it is sent to the internal system. The subscriber ID is specified during the creation of the respective subscription. For details, see *Transfer sites* on page 494.

       Then, in the **New Filename** field, define the format of the new file name. By default, the file is renamed in the format `<ID> <FILENAME>` where, `<ID>` is the Subscriber ID specified when the subscription is created and `<FILENAME>` is the original name of the transferred file.

       The use of the placeholders, `<ID>` and `<FILENAME>`, in the new file name format is mandatory. The character you use to separate `<ID>` from `<FILENAME>` must not be included in the `<ID>` string.
    d. In **Service Account**, select a service account to which you want to send submitted files.
    e. In the **put in folder** field, type the name of the folder to be used by the service account you specified.
    f. (Optional) Click **Send Options** to display the *Send Options* dialog box.



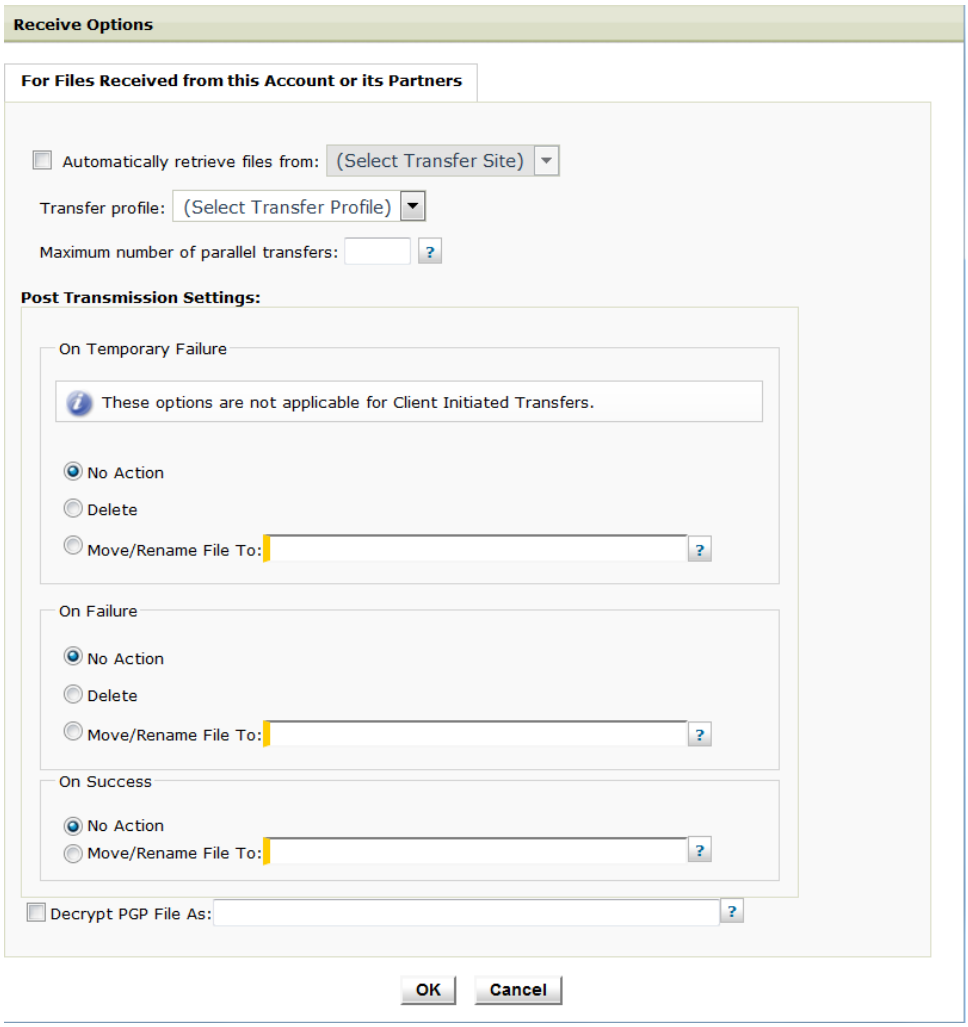
Define the settings for sending files to the service account. Choose one or more of the following options, and then click **OK** in the *Send Options* dialog box.

Encrypt File As – Select this check box to require that files submitted are encrypted.

Send files directly to <transfer site> – Select this check box to send files directly to the transfer site you select from the drop-down list.

Post Transmission Settings – Select which action you want SecureTransport to take when the transfer fails or succeeds.

7. (Optional) Select the **Send files to Subscribers** check box to permit outgoing file transfers from the application to the subscribed parties. If you enable this option, continue specifying values for the parameters in the pane.
    a. In the **Receive folder** field, type the name of the folder where outgoing transferred files are submitted to the subscriber. The receive folder is created as a sub-folder of the subscription folder.
    b. Select a service account to receive files from in the **Service Accounts** list.
    c. In the **get from folder** field, type the name of the folder to be used by the service account you specified.
    d. (Optional) Click **Receive Options** to display the *Receive Options* dialog box and configure the settings for receiving files from this service account. Choose one or more of the following options and enter the maximum number of parallel transfers, and then click **OK** in the *Receive Options* dialog box.



Automatically retrieve files from – Select this check box and select a transfer site from the drop-down list to automatically retrieve files from the transfer site when they arrive.

Maximum number of parallel transfers – Enter a number to limit the number parallel transfers. If you enter a value greater than zero, SecureTransport executes only the specified number of transfers in parallel. If the value is null or zero, the maximum number of parallel transfers is limited by system capacity.

Post Transmission Settings – Select which action you want SecureTransport to take when the transfer has a temporary failure, a permanent failure, or succeeds.

Decrypt PGP File As – Select this check box to require that files are decrypted after the transfer is complete.

e. In the **Routing Settings** group, specify a pattern in the **ID Pattern** box to define the ID of the subscriber to whom files are routed. By default, the pattern is `<ID>_<FILENAME>` where, `<ID>` is a regular expression corresponding to the Subscriber ID specified when the subscription is created and `<FILENAME>` is the original name of the transferred file.

The use of the placeholders, `<ID>` and `<FILENAME>`, in the new file name format is mandatory.

8. Click **Create Application**.

Create a Transfer Log Maintenance application

The Transfer Log Maintenance automatically deletes Transfer log records that are older than a specified number of days (30 days by default). You can schedule how often to run this application and configure it to optionally export these records prior to deletion.

You must enable the `TransferLogMaintApp` rules package in the Transaction Manager before you can use a Transfer Log Maintenance application. For more information, see *Manage rules packages* on page 207.

Use the following procedure to create a Transfer Log Maintenance application.

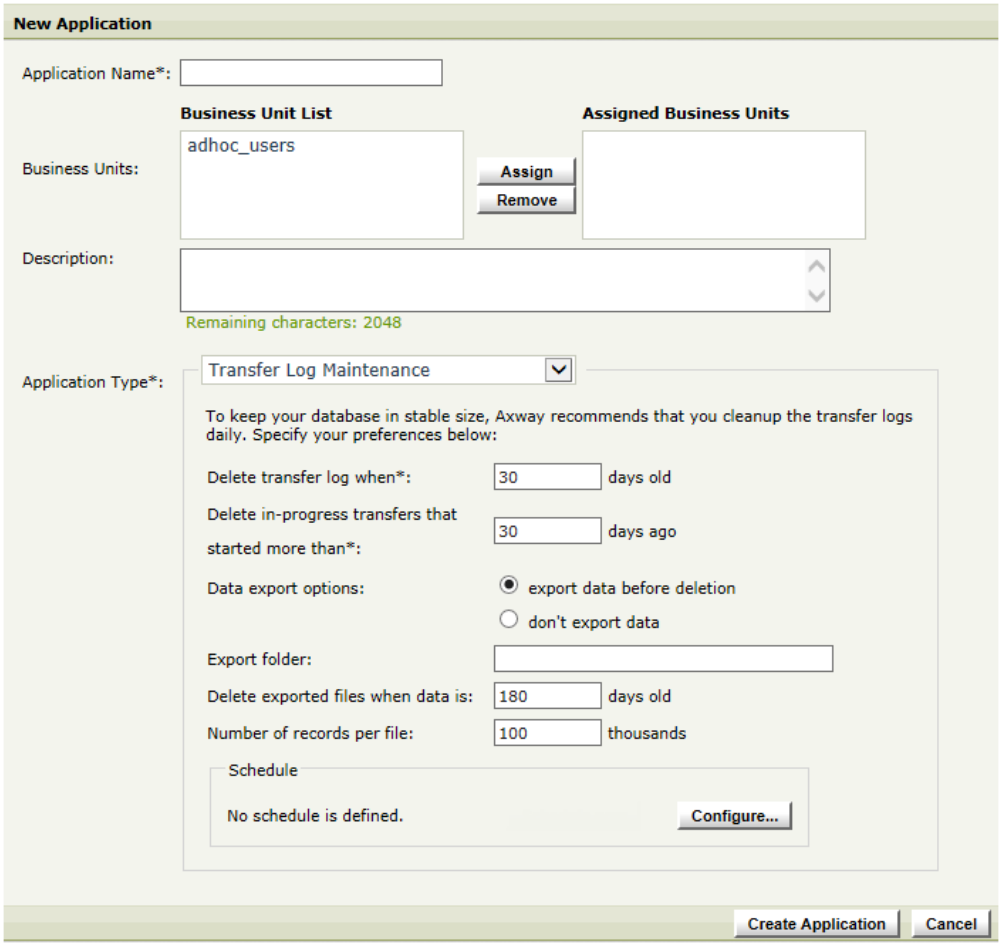
Note You can also use the `log_export` command-line utility to export transfer log entries.

1. Select **Application** and click **Add New**.

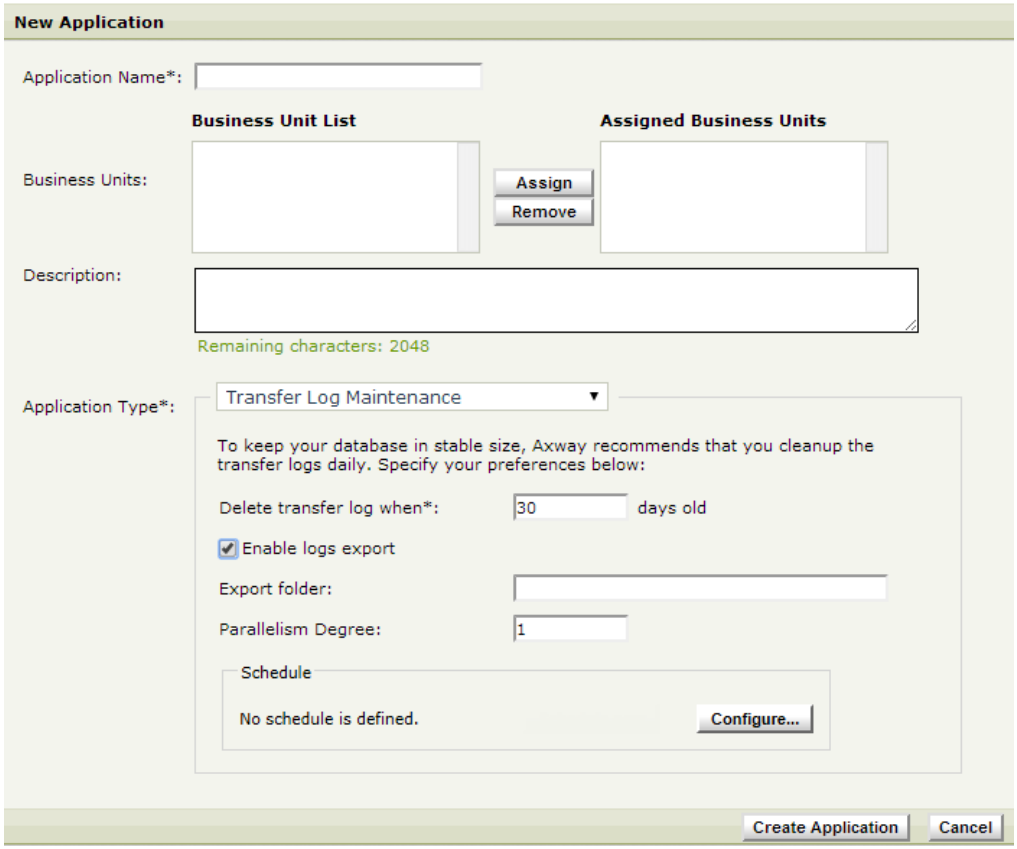
   The *New Application* page is displayed.

2. Select **Transfer Log Maintenance** from the mandatory **Application Type** list.

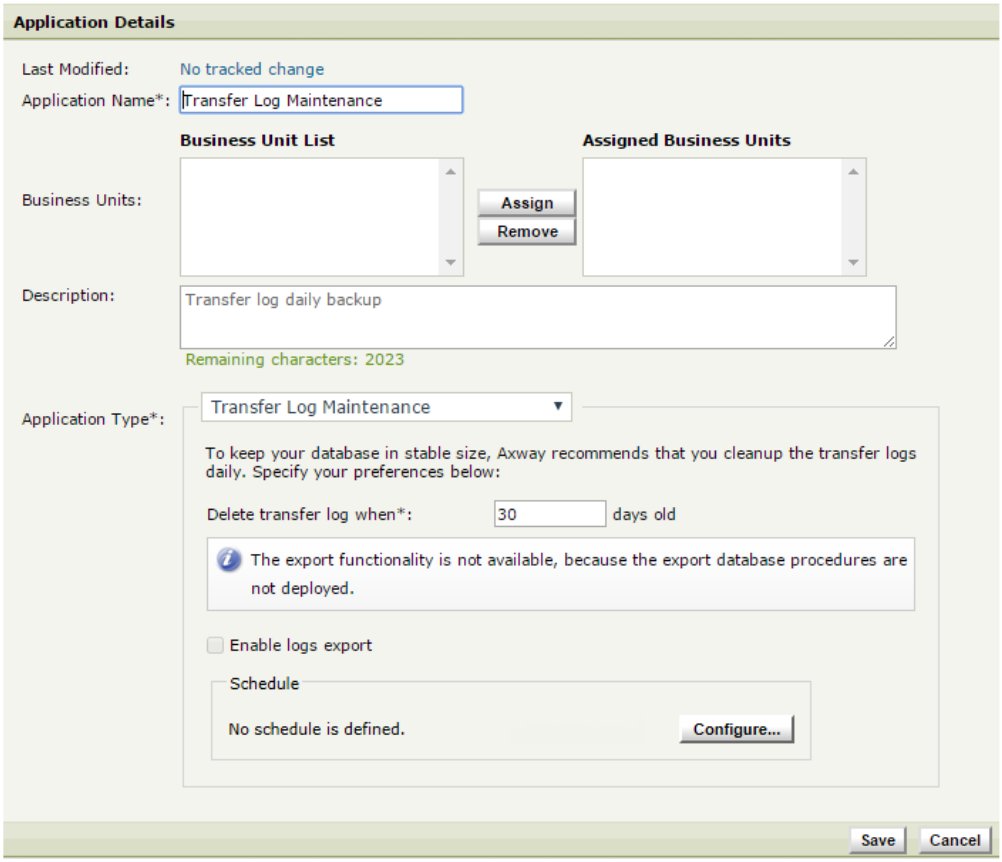
   For an embedded database or an external Microsoft SQL Server database, the following page is displayed.



For an external Oracle database, the following page is displayed.



For an external Oracle database where the export functionality is not available, the following page is displayed.



Note When the server uses an Oracle database, the data export option and related fields are not displayed. Instead, SecureTransport uses a partitioned table for the log entries. Your Oracle DBA can implement data export using Oracle functionality.

Note When your server uses an Oracle database and the export database procedures are not deployed, the **Enable logs export** checkbox is disabled and following message is displayed: "The export functionality is not available, because the export database procedures are not deployed."

3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (/) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.

   Note As with all applications, assigning business units to the application controls which delegated administrators can manage the application. It does not control which log entries Transfer Log Maintenance processes.

5. (Optional) Enter an application **Description**.

6. In the **Delete transfer log when _____ days old** field, specify how old transfer log entries will be when they are deleted. The application computes the age of transfer log entries to midnight of the day it is run. For example, if the value of this field is `1` and the application runs at 4:00 AM., the application deletes entries created before midnight on at the beginning of the previous day. It does not delete entries created between midnight and 4:00 AM. on the previous day. This field is mandatory.

   You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   If your server uses an Oracle database, continue with step 8.

7. To export logs from an embedded database or an external Microsoft SQL Server database, select **export data before deletion**.

   a. In the **Export directory** field, specify where the export files are stored. You must enter a full directory path. If you are exporting from a Microsoft SQL Enterprise Edition database, you must also complete the following steps on the database server:

      i. Create an export directory on the Microsoft SQL Server.

      ii. Create a new filegroup:

      ```
      ALTER DATABASE databaseuser ADD FILEGROUP [ST_
      FILETRACKING_ARCHIVE]
      ```

      iii. Create a file:

      ```
      ALTER DATABASE databaseuser
           ADD FILE
           (NAME = N'ST_FILETRACKING_ARCHIVE_databaseuser',
           FILENAME = N'<EXPORT_DIR>\ST_FILETRACKING_ARCHIVE_
      databaseuser.ndf',
           SIZE = 10MB,
           MAXSIZE = 100MB,
           FILEGROWTH = 1MB)
           TO FILEGROUP [ST_FILETRACKING_ARCHIVE]
      GO
      ```

      iv. Grant all permissions on the `<EXPORT_DIR>` directory created in step "i" to the database user.

      v. Grant the database user **Backup database** and **Backup log** permissions.

      Note The **Backup log** permission is only required if the database is in **Full recovery mode**.

   b. In the **Delete exported files when data is: _____ days old** field, type the period of time (in days) exported files remain in the export directory before they are deleted. If you leave this field empty or specify zero, SecureTransport does not delete the files.

   c. In the **Number of records per file: _____ thousands** field, specify the maximum number of records (in thousands) that can exist in an exported file. When this value is exceeded, SecureTransport starts to export the transfer log entries in a new file.

8. To export logs from an external Oracle database, select **Enable logs export**.
    a. In the **Export folder** field, specify where the export files are stored. You must fill in the name of the directory defined in the Oracle database (for example, `ST_DMPDIR`). On the Oracle Server:
        i. Create the directory where the logs will be exported and make sure that the Oracle user has permissions.
        ii. Log in into Oracle as SYSDBA and create the `ST_DMPDIR` directory using the following syntax:

        ```
        CREATE DIRECTORY ST_DMPDIR AS '/YOUR_DIRECTORY_HERE';
        ```

        iii. Grant all privileges on the directory to the ST user:

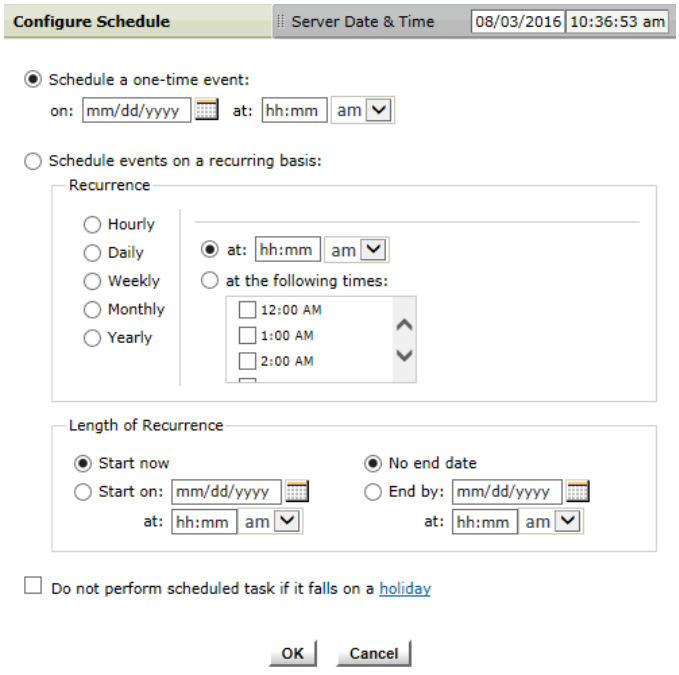
        ```
        GRANT ALL PRIVILEGES ON DIRECTORY ST_DMPDIR TO ST_DATABASE_USER
        ```

        iv. Grant create table privileges to the ST user:

        ```
        GRANT CREATE TABLE TO ST_DATABASE_USER;
        ```

    b. In the **Parallelism Degree** field, specify the number of processors to use during an export operation. You can specify any value for one to the number of processors available on the server. You can limit the effect of the export on database performance by limiting the number of processors used.
9. (Optional) In the *Schedule* pane, click **Configure** to schedule a future task or to schedule a series of future tasks.

    The *Configure Schedule* dialog box is displayed.



To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

For information on working with the SecureTransport scheduler , see *Scheduled downloads and tasks* on page 616. Click **OK** when finished setting the schedule.

10. Click **Create Application**.

Create a Unlicensed Accounts Maintenance application

The Unlicensed Accounts Maintenance application deletes inactive unlicensed user accounts older than a specified number of days (60 days by default). You can schedule how often to run this application.

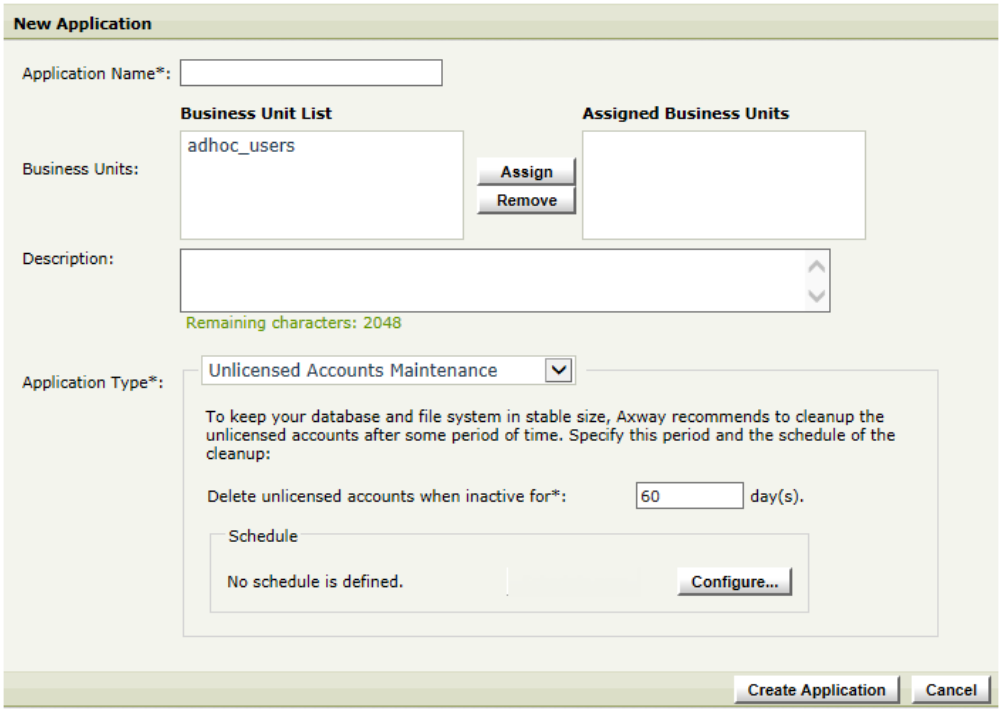
You must enable the `UnlicensedAccountMaintApp` rules package in the Transaction Manager before you can use a Unlicensed Account Maintenance application. For more information, see *Manage rules packages* on page 207.

Use the following procedure to create an Unlicensed Accounts Maintenance application.

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select **Unlicensed Accounts Maintenance** from the mandatory **Application Type** list.



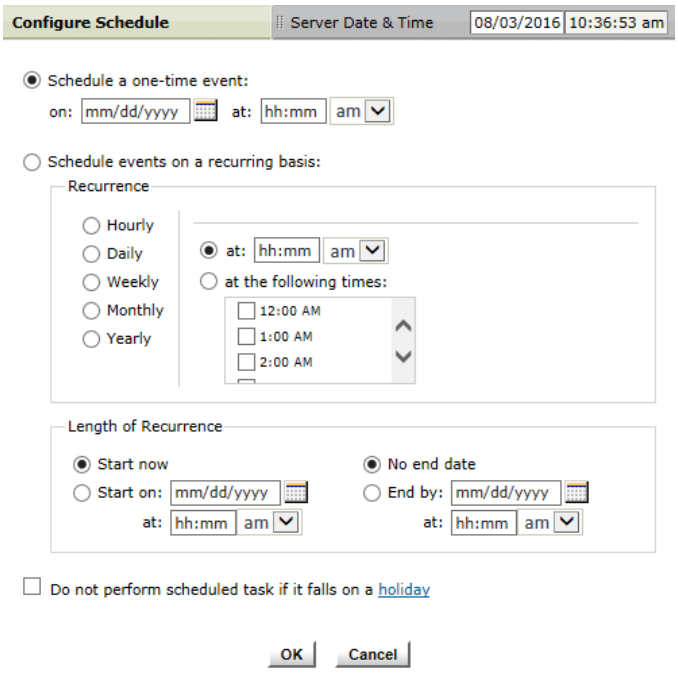
3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (/) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you have created. For details, see *Business units* on page 692.
5. (Optional) Enter an application **Description**.
6. In the **Delete unlicensed accounts when inactive for** field, specify how long in days an unlicensed account must be inactive before it is deleted.

   You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
7. (Optional) In the *Schedule* pane, click **Configure** to schedule a future task or to schedule a series of future tasks.

   The *Configure Schedule* dialog box is displayed.



To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

Note If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

For information on working with the SecureTransport scheduler , see *Scheduled downloads and tasks* on page 616. Click **OK** when finished setting the schedule.

8. Click **Create Application**.

Advanced Routing 13

This chapter provides detailed information about the Advanced Routing concepts and procedures. You will learn various instruction on how to create Advanced Routes, subscribe user accounts to Advanced Routing applications and assign route package templates to user accounts.

In addition to configuration descriptions, you will be able to observe some example basic and advanced use cases.

The final topics of this chapter also contain instructions for Advanced Routing best practices and troubleshooting.

Advanced Routing overview

Advanced Routing (AR) provides a mechanism for multiple routing and transformation iterations over one or more files. As the name suggests, it allows the SecureTransport administrator to create diverse patterns for file transformations and movement (routing) across different partner systems and internal entities. UI-wise, Advanced Routing is a standard SecureTransport *application*: in order to use it, either an account or account template must subscribe to it.

Advanced Routing (AR) is the most complex application, both in terms of configuration and possible use cases. Using it involves concepts and terminology that are entirely AR-specific. In order to take advantage of these concepts, you must first understand the aspects of AR and the great multitude of file transfer scenarios it covers.

What can Advanced Routing do?

AR allows you to configure complex sets of actions (called *route steps*) to apply on one or more files during a transfer process. Route steps are divided into two categories: *transformation* (modification) and *routing* (transferring) of files.

- *Transformation* of files – this includes several predefined file modifications: you configure in what way you to modify (transform) a file. For example, you can apply PGP encryption/decryption, compression/decompression, character replacement or renaming of filenames, etc.
- *Routing* of files – this is a definition of the AR file transfer: you configure where you want to send your file.

Each transformation or routing is defined as a *step* in a *route*. For example, if you want to 1)encrypt a file, 2)send it to the subscription folder of a selected account and then 3)decrypt it, you must perform one step per each action, three in total. These three steps form the route.

Summary: Route steps are *definitions for actions* you apply to one or more files in a specific order. A set of route steps forms a route.

Advanced Routing allows you to add more routes if you need to. You decide how many steps you'll have in each of your routes. Theoretically, your route package can include as many steps as you want; however, it is not recommended to have too many as it might adversely affect performance.

For best UI experience, it is recommended that you understand the terminology introduced with AR.

Advanced Routing glossary of terms

The following terms and concepts are introduced with Advanced Routing:

- **Route and route steps**

  Advanced Routing provides advanced transformation and routing capabilities to file transfers. Each transformation and movement of files is performed in a *route*. A route is a set of (route) steps which are consecutively executed. The order of step execution is defined in the routes and the eventual processing of steps is triggered by predefined conditions. Only AR file transfers use steps. You can have multiple steps defined in a route. Each step performs either of the two possible actions: file *transformation* or file *routing*.

  Note that both Transformation and route execution can be based on file path/name patterns or other environment variables

- **Step conditions**

  Each step you define has a triggering condition associated with it. You can trigger step execution either by using EL or always (unconditionally).

- **Route package**

  A collection of routes defines a route package. The routes in a package process the file in parallel: this means that no order in route execution is defined. Route package is performed on the Account level and is an instance of the Route Package Template.

- **Route Package Template**

  The Route Package Template is used for adding a route package per account. You can define the Business units a package template will be available to: only accounts part of the specified Business units will be able to use route packages as defined in the Route Package Template.

Now that you know some basic AR-specific terms, you can learn more about triggering conditions that launch a file transfer through the route steps.

Triggering conditions and events

When specific predefined conditions are met, the route kicks off and its steps are performed in the predefined order. These conditions are triggered by specified events. As with routing steps, conditions are wrapped in routes as part of a *Route Package Template* or *Route Package*.

As an administrator, you define the conditions which will trigger transformation and routing processing or both over one or more files. Those conditions or steps are stored in a Route Package or Route Package Template. In order to reuse already defined steps, you must add them to a *Route Package Template*. In contrast, one or more steps which are specific for a particular user can be defined in a *Route Package*.

Advanced Routing processing can be triggered by the following events:

- Successful client upload
- Failed client upload
- Successful client download
- Failed client download
- Successful server pull
- Temporarily failure of a server pull
- Failed server pull - Also applies to failed wildcard and individual file pulls

Advanced Routing setup overview

The following list represents the setup stages that a SecureTransport administrator must go through in order to configure an AR instance.

- Create a route package template
- Create AR application
- Create a route package instance from the route package template
- Subscribe account to AR application to trigger the route

As noted above, you must have an account (or an account template) in order to create a subscription to the AR application. You can have multiple AR applications that cover different use cases for different groups of users. Additionally, you can create and AR delegated administrator to administer all AR configurations and file transfers.

As you can see, setup itself introduces some AR-specific concepts. The route package template, the route package instance and the route itself are all different forms of the same concept: a reusable configuration that is easily upgradable when necessary. You will better understand their purpose when you learn a bit more about the logic incorporated into each AR flow.

Advanced Routing features

Advanced Routing offers the following features:

- Conditioning
    - Transformation and route execution can be based on file path/name patterns or other environment variables
- Transformations
    - PGP Encryption, PGP Decryption, Compress, Decompress, Line Ending, External Script, Encoding Conversion, Characters Replace, Line Padding, Line Truncating, Line Folding, and Rename transformations
    - Multiple transformation execution (for example, Decompress > PGP Decryption >

Compress)

- Renaming
  - Routings
    - File routing to transfer sites, accounts (including virtual and LDAP ones), and file system through Publish To Account and Send To Partner
    - Renaming and deleting
    - Overwrite upload folder - optional setting for the new upload folder name which overwrites the one configured in Transfer site settings
  - Tracking and notifications
    - File Tracking integration
    - Sentinel integration
    - Email notifications on routing and transformation successes, failures, and triggering
  - Extensive Expression Language support
  - Post routing, post transformation, and post processing actions
  - Ability to specify and overwrite transformation and routing steps on an account basis
  - Distributed execution of the routes in a Standard Cluster or Enterprise Cluster

The following topics provide detailed info about different aspects of Advanced Routing :

- *Order of configuration* on page 798
- *Configuration* on page 800
- *Transformations* on page 829
- *Route steps* on page 875
- *Operation* on page 894
- *Advanced Routing best practices* on page 917
- *Custom Expression Language functions and variables* on page 921
- *Troubleshoot Advanced Routing* on page 947

Order of configuration

This topic provides instructions for configuring Advanced Routing, presented in steps. It also provides a brief overview of each configuration item.

Business units can be created prior to configuring the Route Package Template. For configuration information, see *Create or edit a business unit* on page 693.

Optionally, an Advanced Routing administrator can be created. For configuration information, see *Advanced Routing delegated administrator* on page 800 and to *Create a delegated administrator* on page 654.

The Advanced Routing feature should be configured in the following order:

1. Create user account (or account template) or use an existing one. See Create user accounts on page 1 and *User accounts* on page 453.
2. Create Advanced Routing application. See *Create Advanced Routing application* on page 805.
3. Create Route Package Template. See *Create route package template* on page 1.
4. Assign Route Package Template to the account from Step 1. See *Assign Route Package Template* on page 818.
5. Subscribe to the Advanced Routing application. See *Subscribe to Advanced Routing application* on page 1.

Create Advanced Routing administrator

In order to setup an administrator dedicated to managing the Advanced Routing application and Route Package Templates it is necessary to create an Advanced Routing administrator with file tracking, accounts, applications, mail templates, and routes privileges. See *Advanced Routing delegated administrator* on page 800 for more.

Create user accounts

In order to subscribe an account to an Advanced Routing application instance, start off by creating a SecureTransport user account or account template (or use an existing one). For information on creating user accounts, see *Create a user account* on page 456. See *Manage account templates* on page 663 for more.

Create Advanced Routing application

Navigate to the **Application** tab and click **Add New**. Specify the preferred **Application Name** for the Advanced Routing application instance. Select *Advanced Routing* from the **Application Type** combo box. See *Create Advanced Routing application* on page 805.

Create Route Package Template

Navigate to the **Routes** tab and click **New Route Package Template**. Specify the preferred **Route Package Template Name** for the Route Package Template, determine assigned business units, enter a route template description, determine execution routes, add transformation and routing steps, and determine notifications.

Assign Route Package Template

You must subscribe the selected user to the Advanced Routing application prior to assigning the user a Route Package Template. To assign the user a Route Package Template, navigate to **Accounts > User Accounts**, select the desired user account, and then select the **Routes** tab for the selected

account. From the *Routes* tab, select the desired Route Package Template from the **Route Package Template** list and then click **Assign Route**. The *Create Route Package* screen is displayed with a link to the selected Route Package Template under the **Created From** label. For more details on assigning a Route Package Template, see *Assign Route Package Template* on page 818.

Subscribe to Advanced Routing application

To subscribe a user account to the Advanced Routing application, navigate to **Accounts > User Accounts**, select the desired user account, and then select the **Subscriptions** tab for the selected account. From the **Subscriptions** tab, select *Advanced Routing* from the **Subscribe to** list and click **Subscribe**. For additional details on subscribing to the Advanced Routing application, see *Subscribe to Advanced Routing application* on page 821. For details on managing subscriptions, see *Manage subscriptions* on page 607.

Configuration

This topic provides the step-by-step instructions for creating delegated administrator accounts, user accounts, applications, and templates for Advanced Routing. It also includes step-by-step instructions for adding an Advanced Routing application, subscribing to the Advanced Routing application, and assigning a Route Package Template.

The following topics provide how-to instructions for configuring Advanced Routing:

- *Advanced Routing delegated administrator* on page 800
- *Create user accounts* on page 804
- *Create Advanced Routing application* on page 805
- *Manage Route Package Templates* on page 806
- *Manage Routes* on page 812
- *Assign Route Package Template* on page 818
- *Subscribe to Advanced Routing application* on page 821

Advanced Routing delegated administrator

The configuration of a delegated administrator for Advanced Routing requires creating an Advanced Routing administrator role and creating an Advanced Routing administrator with the specified administrator settings. The following topics provide the configuration details for creating the role of Advanced Routing administrator and assigning the role to the Advanced Routing administrator.

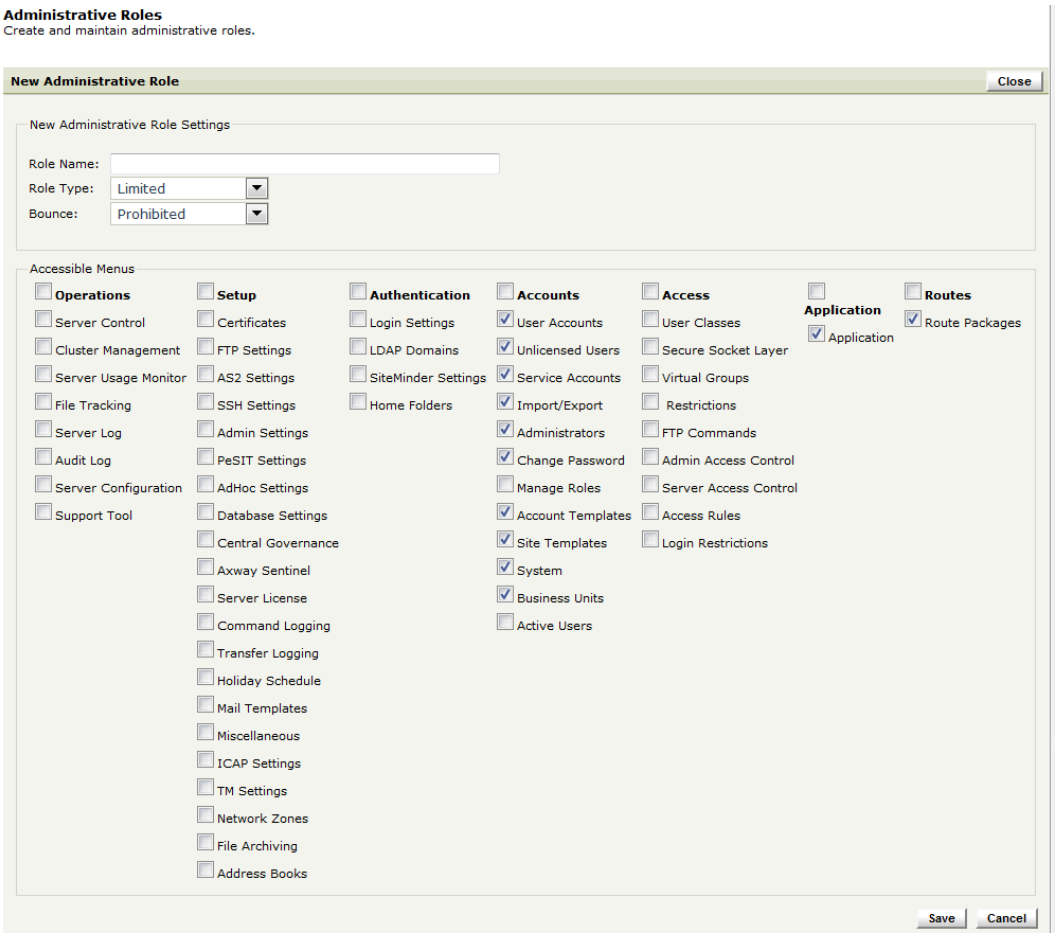
The following topics provide how-to instructions for creating an Advanced Routing administrator role and creating an Advanced Routing administrator:

- *Create Advanced Routing administrator role* on page 801
- *Create Advanced Routing administrator* on page 802

Create Advanced Routing administrator role

For details on creating administrative roles, refer to *Administrative roles* on page 655. The Advanced Routing administrator role should be created with the same settings as a delegated administrator plus the selection of *Route Packages* as shown in the following table and figure.

Function	Selections
Role Name:	Advanced Routing Administrator
Role Type:	Limited
Bounce:	Prohibited
Accessible Menus	
Operations	No selections
Setup	Mail Templates
LDAP	No selections
Accounts	User Accounts, Unlicensed Users, Service Accounts, Import/Export, Administrators, Change Password, Account Templates, Site Templates, System. Business Units
Access	No selections
Application	Application
Routes	Route Packages



Create Advanced Routing administrator

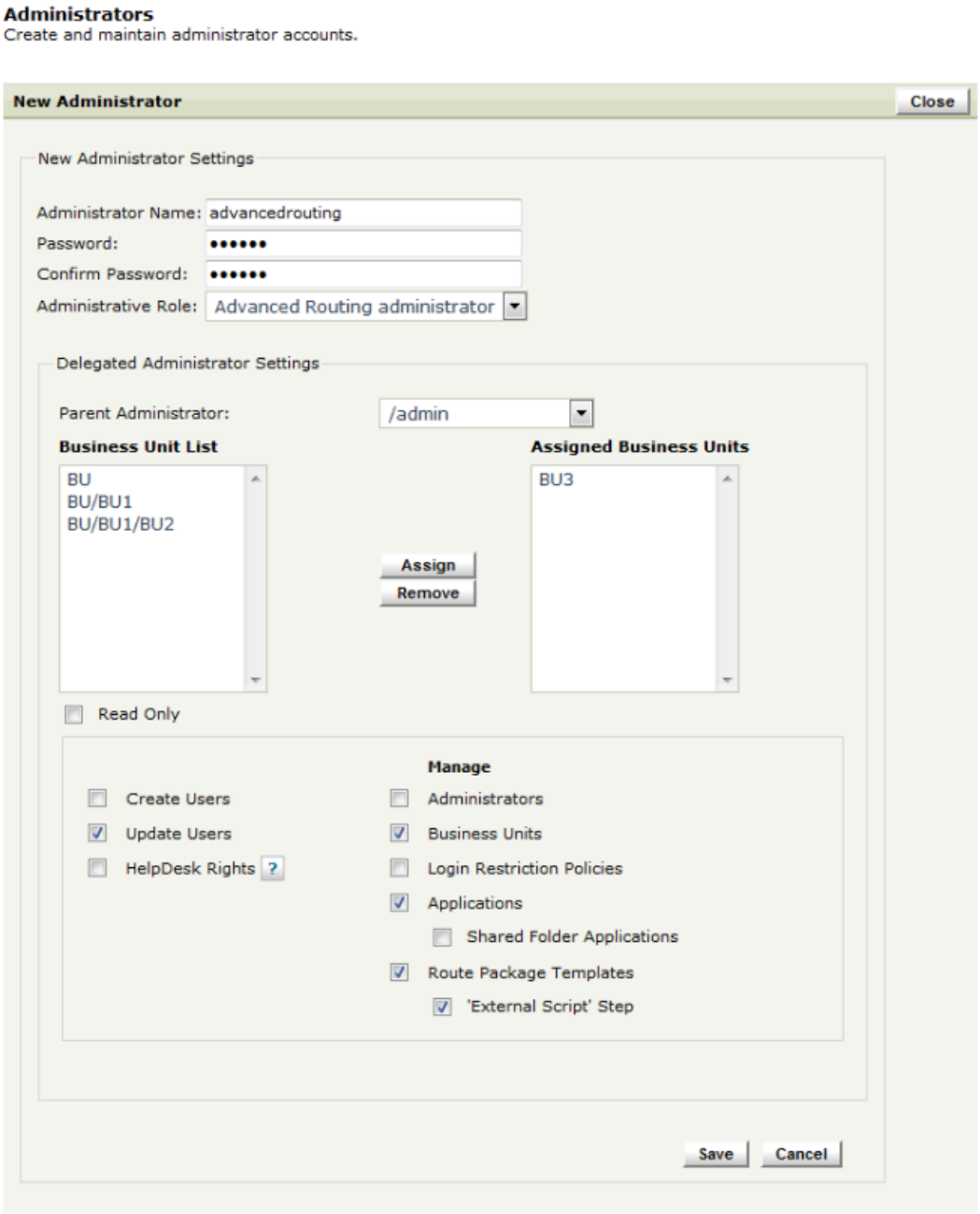
For details on creating administrators, refer to *Manage administrator accounts* on page 644. An Advanced Routing administrator should be created with settings as shown in the following table and figure.

Note At least one business unit must be assigned to the Advanced Routing administrator.

Function	Selections
Administrator Name:	User determined
Password:	User determined
Confirm Password:	Must match password entry
Administrative Role:	Advanced Routing Administrator

Function	Selections
Parent Administrator:	/admin
Assigned Business Units	User determined - At least one Business Unit should be assigned
Advanced Routing Administrator Selections	Update Users, Business Units, Applications, Route Package Templates, 'External Script' Step

Note Manage Route Package Templates and Manage 'External Script' Step must be selected.

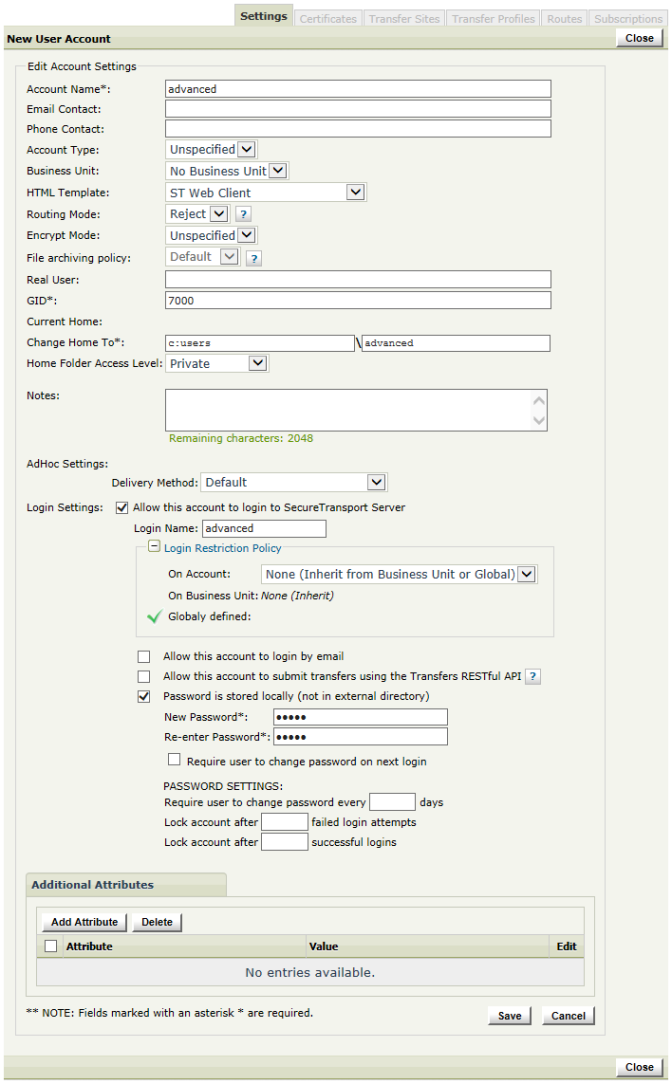


Create user accounts

For details on creating user accounts, refer to *User accounts* on page 453. Accounts which have advanced routes can be created using the instructions for adding user accounts.

Note The *Home Folder Access Level* property (which specific to Advanced Routing functionality) defines whether or not files can be routed to the account's home folder.

The following figure shows an example of an account which has advanced routes assigned.

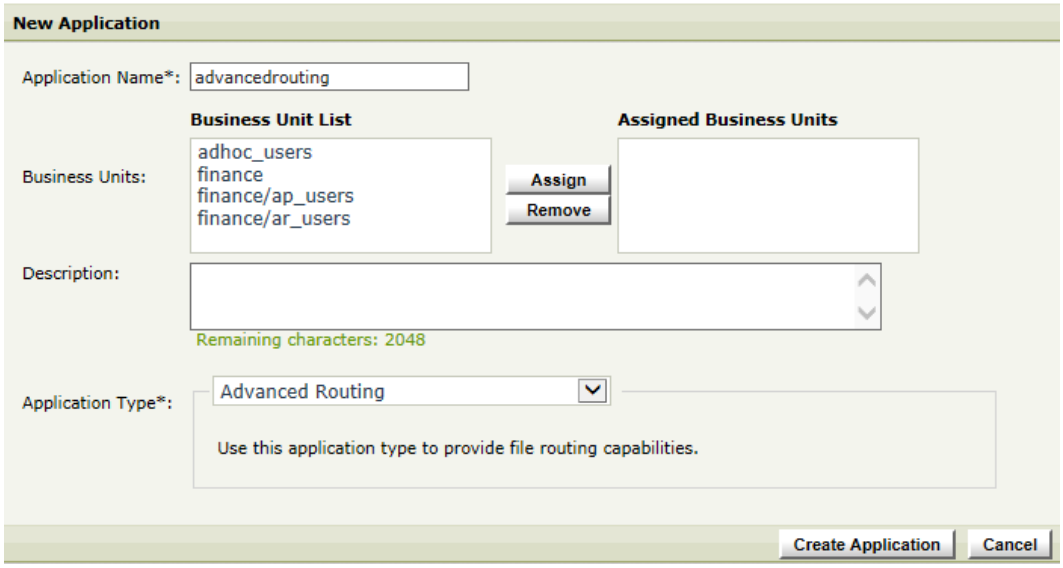


Create Advanced Routing application

1. Select **Application** and click **Add New**.

   The *New Application* page is displayed.

2. Select Advanced Routing from the mandatory **Application Type** list.



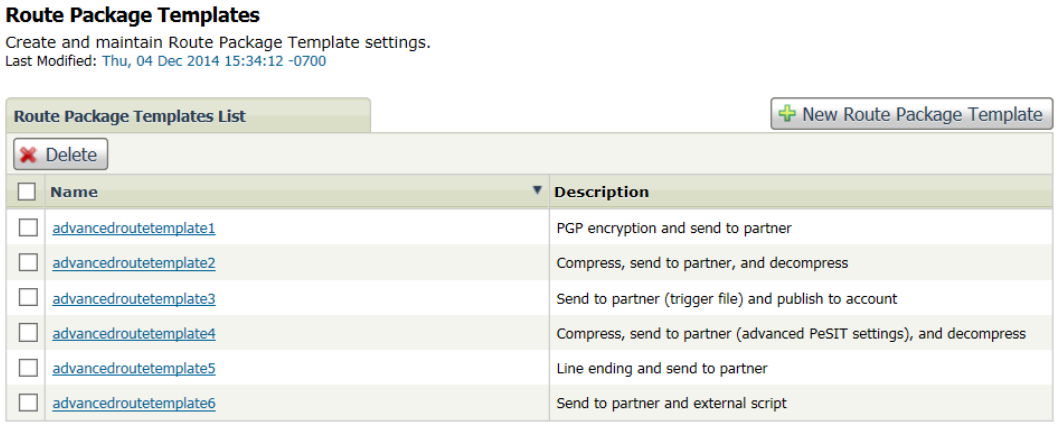
3. Enter a unique **Application Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.

   Note The application name cannot include any forward slash (/) characters.

4. (Optional) Use the **Assign** and **Remove** buttons to assign business units for the application. The **Business Unit List** contains the names of business units you create. For details, see *Business units* on page 692.
5. (Optional) Enter an application **Description**.
6. Click **Create Application**.

Manage Route Package Templates

Use the *Route Package Templates* page to manage route package templates. Route package templates can be created, edited, and deleted from the *Route Package Templates* page. To display the *Route Package Templates* page, select **Routes > Route Packages**.



If you have access to the *Route Package Templates* page, you can create, edit, and delete route package templates. Master administrators and limited administrators with the Manage Route Package Templates privilege have access to the *Route Package Templates* page by default.

The following topics provide how-to instructions for managing Route Package Templates:

- *Add Route Package Template* on page 807
- *Edit Route Package Template* on page 809
- *Enable Route* on page 811
- *Disable Route* on page 811
- *Reorder Routes* on page 811
- *Delete Route* on page 811
- *Delete Route Package Template* on page 811

Add Route Package Template

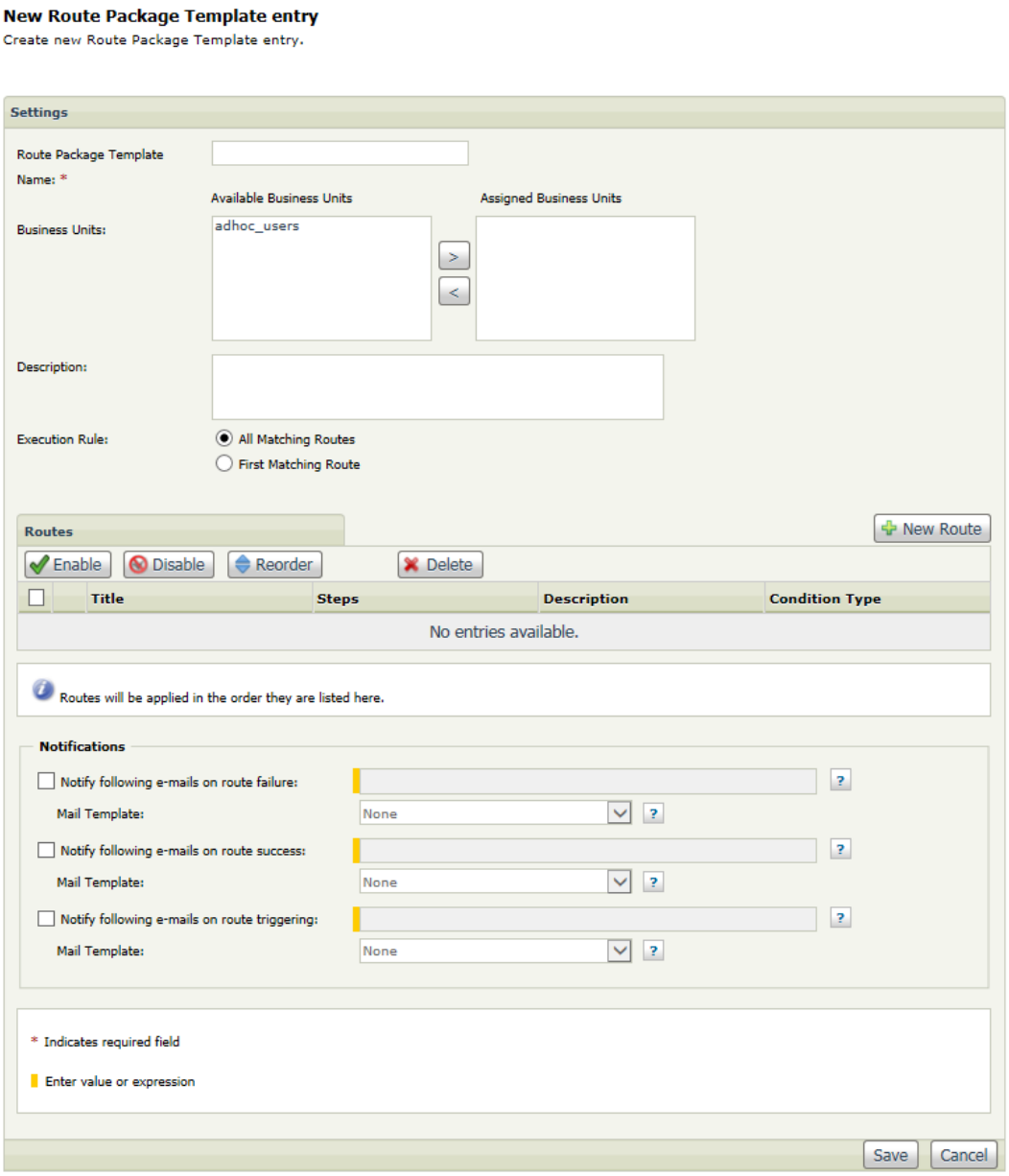
Use the following procedure to add a Route Package Template.

1. Select **Routes >Route Packages**.

   The *Route Package Template* page is displayed.

2. Click **New Route Package Template**.

   The *New Route Package Template Entry* page is displayed.



3. Enter a unique **Route Package Template Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
4. (Optional) Use the **Left** and **Right** buttons to assign business units to the Route Package Template. The **Business Unit List** contains the names of business units you create. For details, *Business units* on page 692.
5. (Optional) Enter a **Description**.
6. Determine the **Execution Rule**. Select either **All Matching Routes** (default) or **First Matching Route**.

   When **All Matching Routes** is selected, all matching routes are executed. When **First Matching Route** is selected, only the first matching route is executed.
7. Click **New Route**.

The *New Route Entry* page is displayed. For route entry configuration information, refer to *Manage Routes* on page 812.

8. Determine email **Notifications**. As a prerequisite the SMTP settings must be configured by navigating to **Setup > Miscellaneous > SMTP Configuration** in the Administration Tool. For additional SMTP configuration information, refer to *SMTP configuration* on page 183. Additionally, in order to add email notifications the administrator must have access to Mail Templates, otherwise this selection is disabled. Mail Templates access is configurable through the Administrative role settings. For additional administrative role configuration information, refer to *Manage administrator accounts* on page 644.
    a. Select **Notify following e-mails on route failure** to be notified on route failure and enter a notification email address, a list of mail addresses, or an expression. For additional email configuration information, refer to *SMTP configuration* on page 183.
    b. Select the **Mail Template** from the menu to used for route failure notifications. For email template configuration information, refer to *Mail templates* on page 173.
    c. Select **Notify following e-mails on route success** to be notified on route success and enter a notification email address, a list of mail addresses, or an expression. For additional email configuration information, refer to *SMTP configuration* on page 183.
    d. Select the **Mail Template** from the menu to used for route failure notifications. For email template configuration information, refer to *Mail templates* on page 173.
    e. Select **Notify following e-mails on route triggering** to be notified on route triggering and enter a notification email address, a list of mail addresses, or an expression. For additional email configuration information, *SMTP Configuration* on page 1
    f. Select the **Mail Template** from the menu to used for route triggering notifications. For email template configuration information, *Mail templates* on page 173
9. Click **Save**.

You can add, enable, disable, reorder, and delete Routes as part of creating or adding a Route Package Template. For information on adding Routes, refer to *Manage Routes* on page 812. For information on enabling, disabling, reordering, or deleting Routes, refer to *Enable Route* on page 811, *Disable Route* on page 811, *Reorder Routes* on page 811, and *Delete Route* on page 811.

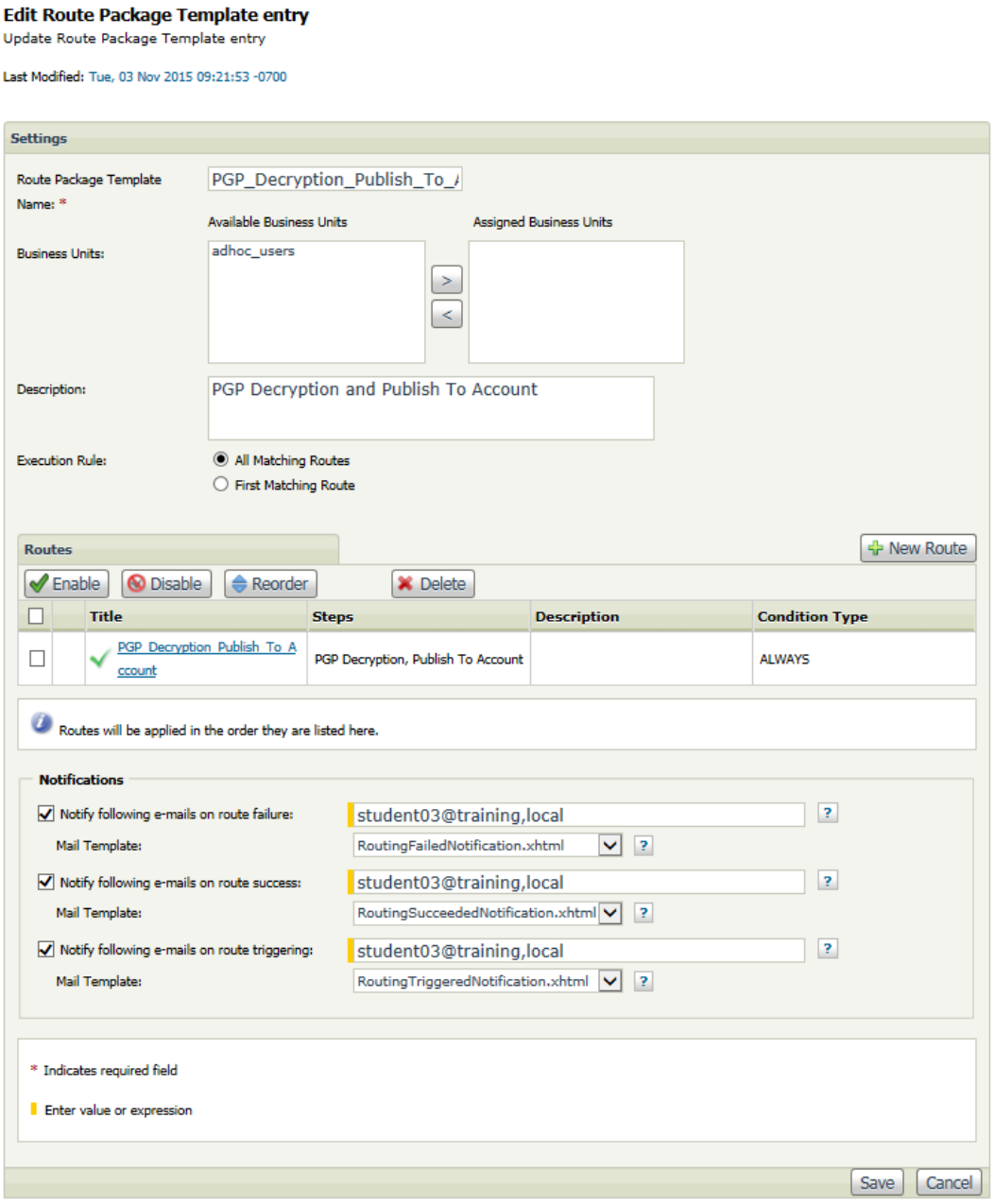
Edit Route Package Template

Use the following procedure to edit a Route Package Template.

1. Select **Routes >Route Packages**.

   The *Route Package Template* page is displayed.
2. Click on the name of the Route Package Template to edit in the *Route Package Templates List*.

   The *Edit Route Package Template Entry* page is displayed.



3. Edit the information displayed. To edit a route, click on the name of the Route and refer to *Manage Routes* on page 812.
4. Click **Save** to apply the changes.

Note You can add, enable, disable, reorder, and delete Routes as part of editing a Route Package Template. For information on adding Routes, refer to *Manage Routes* on page 812. For information enabling, disabling, reordering, or deleting Routes, refer to *Enable Route* on page 811, *Disable Route* on page 811, *Reorder Routes* on page 811, and *Delete Route* on page 811.

Enable Route

Use the following procedure to enable a Route.

1. Select the Route to enable from the *Routes* list.
2. Click **Enable**.

   The selected Route is enabled and a Enabled icon ( ) is displayed next to the selected Route name.

Disable Route

Use the following procedure to disable a Route.

1. Select the Route to disable from the *Routes* list.
2. Click **Disable**.

   The selected Route is disabled and a Disabled icon ( ) is displayed next to the selected Route name.

Reorder Routes

Use the following procedure to reorder the Routes

1. Click **Reorder**.

   A Reorder tool ( ) appears for each Route in the *Routes* list.
2. Use the Reorder tool ( ) to move the Routes in the *Routes* list into the desired order.
3. Click **Save Order**.

Delete Route

Use the following procedure to delete a Route.

1. Select the Route to delete from the *Routes* list.
2. Click **Delete**.
3. When prompted, confirm that you would like to delete the selected Route.

Delete Route Package Template

Use the following procedure to delete a Route Package Template.

1. Select **Routes >Route Packages**.

   The *Route Package Template* page is displayed.

2. Select the check box for the Route Package Template to delete from the *Route Package Templates List*.
3. Click Delete.
4. When prompted, confirm that you would like to delete the selected Route Package Template.

Manage Routes

If you have access to the *Route Package Templates* page, you can create, edit, and delete Routes as part of managing Route Package Templates. You can also add, edit, enable, disable, reorder, and delete Route steps.

The following topics provide how-to instructions for managing Routes:

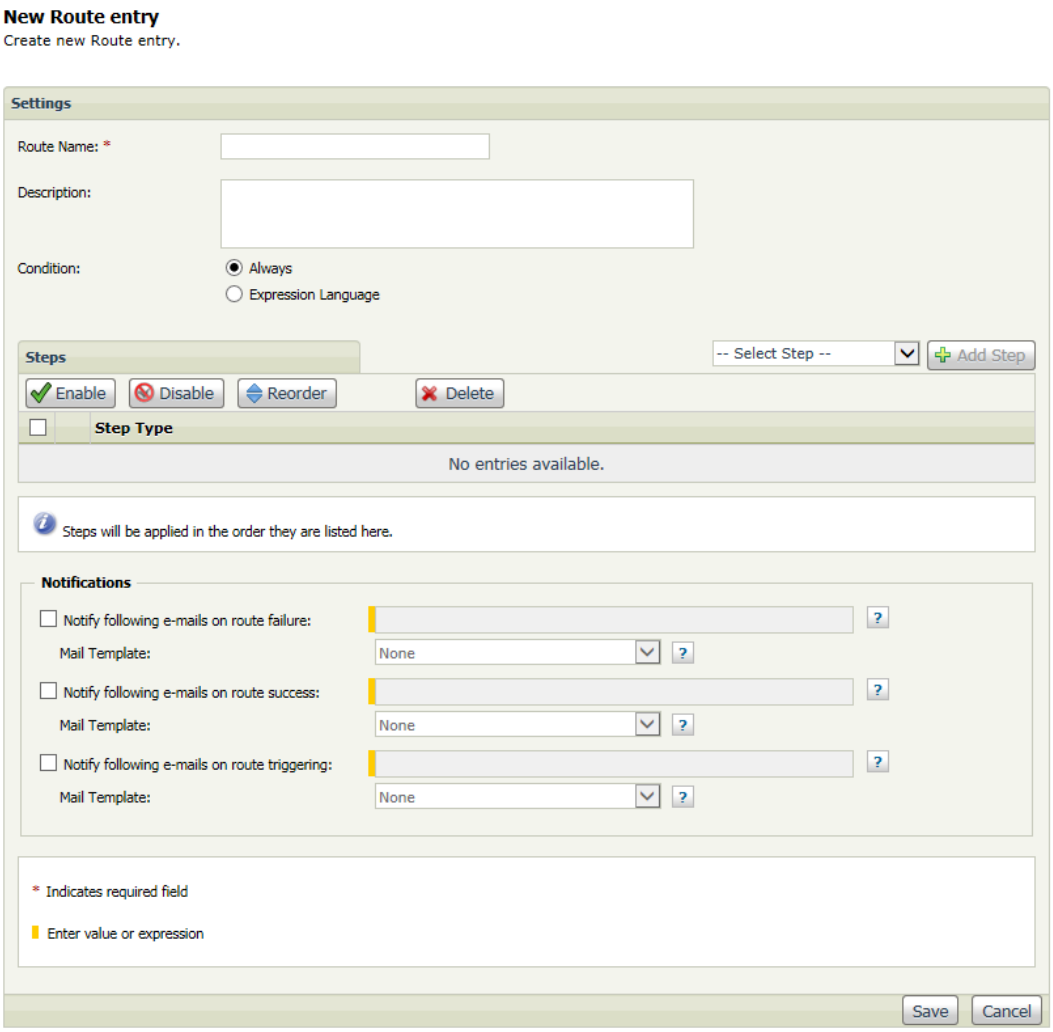
- *New Route* on page 812
- *Edit Route* on page 815
- *Enable Step* on page 816
- *Disable Step* on page 817
- *Reorder Steps* on page 817
- *Delete Step* on page 817
- *Delete Route* on page 817

New Route

Use the following procedure to create a Route.

1. From the *Route Package Template Entry* page, click **New Route**.

   The *New Route Entry* page is displayed.



2. Enter a unique **Route Name**. You cannot enter spaces-only values in this field. For more information, see *Spaces in required fields* on page 464.
3. (Optional) Enter a **Description**.
4. Determine the **Condition**. Select either **Always** (default) or **Expression Language**.

   When **Always** is selected, the trigger condition is always used. When **Expression Language** is selected, the trigger condition is based on the expression entered in the *Expression Language* field.

   Expression Language should be used to define the route trigger condition.

   Examples:

   Files uploaded only through a specific protocol:

   ```
   ${session.protocol eq 'http'}
   ```

   Files uploaded from specific partner over PeSIT:

   ```
   ${pesit.pi.senderID.toLowerCase() eq 'partner'}
   ```

5. Select steps (**Transformation** or **Routing**) from the *Select Step* menu and click **Add Step**. Refer to the following tables for **Transformation** or **Routing** configuration information.

Transformation	Configuration Reference
PGP Encryption	*PGP Encryption* on page 829
PGP Decryption	*PGP Decryption* on page 835
Compress	*Compress* on page 838
Decompress	*Decompress* on page 842
Line Ending	*Line Ending* on page 846
External Script	*External Script* on page 850
Encoding Conversion	*Encoding Conversion* on page 853
Characters Replace	*Characters Replace* on page 856
Line Padding	*Line Padding* on page 861
Line Folding	*Line Folding* on page 869
Line Truncating	*Line Truncating* on page 865

Routing	Configuration Reference
Publish To Account	*Publish To Account* on page 875
Send To Partner	*Send To Partner* on page 881

6. Determine email **Notifications**. In order to add email notifications the administrator must have access to Mail Templates, otherwise this selection is disabled. Mail Templates access is configurable through the Administrative role settings. For additional administrative role configuration information, refer to *Manage administrator accounts* on page 644.
    a. Select **Notify following e-mails on route failure**. You need to have configured SMTP settings on the **Administration Tool > Setup > Miscellaneous > SMTP Configuration** page (notify email, mail relay and SMTP port). The *Notify following e-mails on route failure* field supports EL and you can enter:
        - An email address
        - An expression, for example `ldap.attributes.mail`, `${account.name}`, `${account.email}`.
        - A list of email addresses (delimiters depend on the SMTP server)

        For additional email configuration information, refer to *SMTP configuration* on page 183.

b. Select the **Mail Template** from the menu to used for route failure notifications. For email template configuration information, refer to *Mail templates* on page 173.

c. Select **Notify following e-mails on route success** to be notified on route success and enter a notification email address, mail relay, or SMTP port in the field. For additional email configuration information, refer to *SMTP configuration* on page 183.

d. Select the **Mail Template** from the menu to used for route failure notifications. For email template configuration information, refer to *Mail templates* on page 173.

e. Select **Notify following e-mails on route trigger** to be notified on route trigger and enter a notification email address, mail relay, or SMTP port in the field. For additional email configuration information, refer to *SMTP configuration* on page 183

f. Select the **Mail Template** from the menu to used for route trigger notifications. For email template configuration information, refer to *Mail templates* on page 173.

7. Click **Save**.

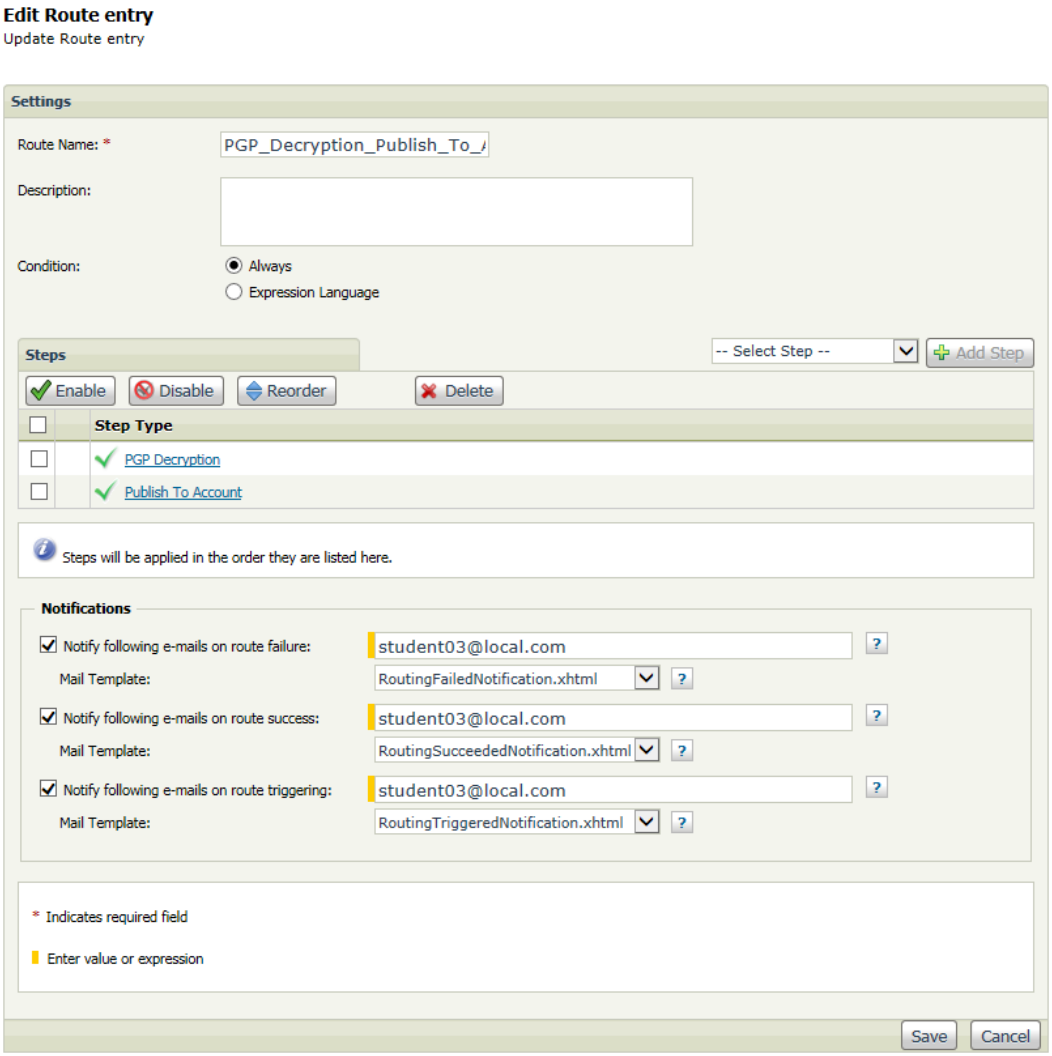
Note You can edit, enable, disable, reorder, and delete Route Steps as part of adding a Route. For information about enabling, disabling, reordering, or deleting Route Steps, refer to *Enable Step* on page 816, *Disable Step* on page 817, *Reorder Steps* on page 817, and *Delete Step* on page 817.

Edit Route

Use the following procedure to edit a Route.

1. From the *Route Package Template Entry* page, click on the name of the Route to edit in the *Routes* list.

   The *Edit Route Entry* page is displayed.



2. Edit the information displayed. To edit a Route Step, click on the name of the Route Step and refer to *Transformations* on page 829 to edit Transformations and to *Route steps* on page 875 to edit Route Steps.
3. Click **Save** to apply the changes.

Note You can edit, enable, disable, reorder, and delete Route Steps as part of editing a Route. For information about enabling, disabling, reordering, or deleting Route Steps, refer to *Enable Step* on page 816, *Disable Step* on page 817, *Reorder Steps* on page 817, and *Delete Step* on page 817.

Enable Step

Use the following procedure to enable a Route step.

1. Select the Step to enable from the *Steps* list.
2. Click **Enable**.

The selected Route Step is enabled and an Enabled icon ( ) is displayed next to the selected Step name.

Disable Step

Use the following procedure to disable a Route step.

1. Select the Step to disable from the *Steps* list.
2. Click **Disable**.

   The selected Step is disabled and a Disabled icon ( ) is displayed next to the selected Step name.

Reorder Steps

Use the following procedure to reorder Route steps.

1. Click **Reorder**.

   A Reorder tool ( ) appears for each Step in the *Steps* list.
2. Use the Reorder tool ( ) to move the Steps in the *Steps* list into the desired order.
3. Click **Save Order**.

Delete Step

Use the following procedure to delete a Route step.

1. Select the Step to delete from the *Steps* list.
2. Click **Delete**.
3. When prompted, confirm that you would like to delete the selected Step.

Delete Route

Use the following procedure to delete a Route.

1. From the *Route Package Template Entry* page, select the check box for the Route to delete in the *Routes* list.
2. Click **Delete**.
3. When prompted, confirm that you would like to delete the selected Route.

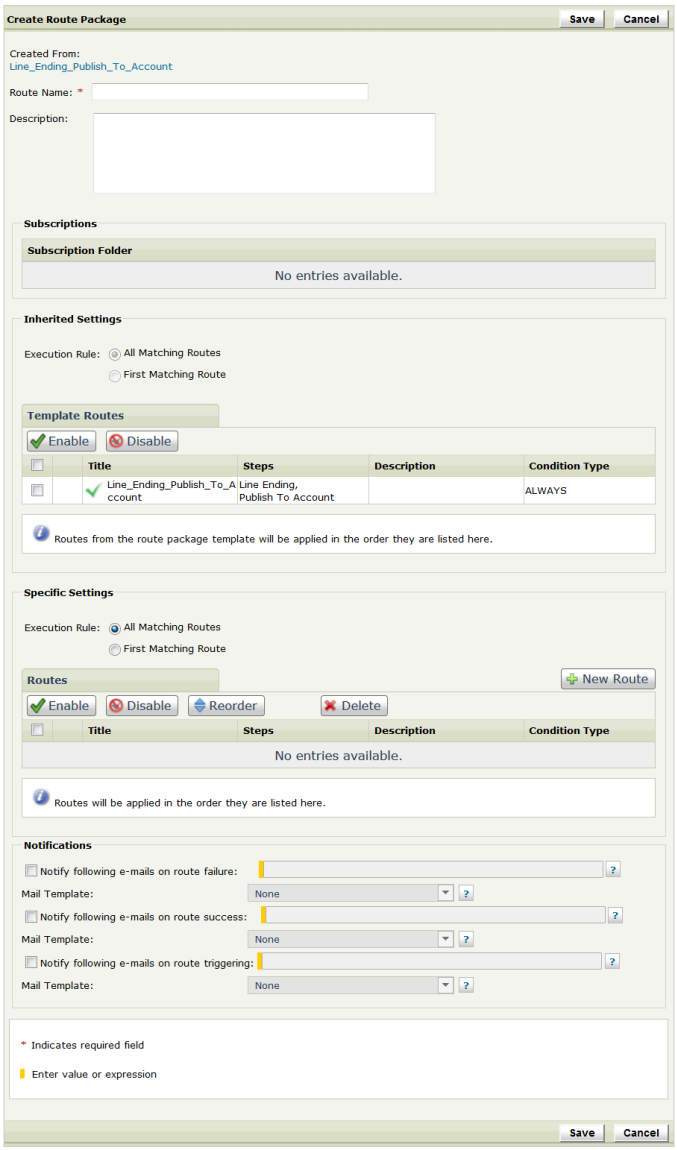
Assign Route Package Template

To assign a Route Package Template to a user account or account template, you must create at least one Route Package Template prior to assigning a route to a user account or account template. For configuration details on managing and creating Route Package Templates, refer to *Manage Route Package Templates* on page 806.

1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click the name of the account that you want to assign a route.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Routes** tab for the selected account.
4. Select the desired Route Package Template from the **Route Package Template** list.
5. Click **Assign Route**.

   The *Create Route Package* page is displayed. You can navigate to the *Edit Route Package Template* page for the selected Route Package Template by clicking the **Created From** link.



6. In the **Route Name** field, type the desired name of the route. The route name can contain 254 characters or less.

   Note You cannot use the following characters in the route name: `* < > ? " / \ | :`

7. (Optional) Enter a **Description**.
8. In the *Inherited Settings* pane:
   a. Select the check box for a Template Route and click **Disable** to disable an enabled inherited route.
   b. Select the check box for a Template Route and click **Enable** to enable a disabled inherited route.

      Note The inherited Execution Rule cannot be changed.

Note If an inherited route is disabled in the Route Package Template, it cannot be enabled from the *Inherited Settings* pane. Also, inherited routes cannot be reordered or deleted from the *Inherited Settings* pane.

9. In the *Specific Settings* pane:
    a. Determine the **Execution Rule**. Select either **All Matching Routes** (default) or **First Matching Route**.

    When **All Matching Routes** is selected, all matching Routes are executed. When **First Matching Route** is selected, only the first matching Route is executed.

    b. Click **New Route**.

    The *New Route Entry* page is displayed. For Route configuration information, refer to *Manage Routes* on page 812.

    You can also edit, enable, disable, reorder, and delete Routes in the *Specific Settings* pane. For information on enabling, disabling, reordering, or deleting Routes, refer to *Manage Route Package Templates* on page 806.

10. In the *Notifications* pane:

    As a prerequisite the SMTP settings must be configured by navigating to **Setup > Miscellaneous > SMTP Configuration** in the Administration Tool. For additional SMTP configuration information, refer to refer to *SMTP configuration* on page 183. Additionally, in order to add email notifications the administrator must have access to Mail Templates, otherwise this selection is disabled. Mail Templates access is configurable through the Administrative role settings. For additional administrative role configuration information, refer to refer to *Manage administrator accounts* on page 644.

    a. Select **Notify following e-mails on route failure** to be notified on route failure and enter a notification email address, list of addresses, or expression in the field. For additional email configuration information, refer to *SMTP configuration* on page 183.

    b. Select the **Mail Template** from the menu to used for route failure notifications. For email template configuration information, refer to *Mail templates* on page 173.

    c. Select **Notify following e-mails on route success** to be notified on route success and enter a notification email address, list of addresses, or expression in the field. For additional email configuration information, refer to *SMTP configuration* on page 183.

    d. Select the **Mail Template** from the menu to used for route success notifications. For email template configuration information, refer to *Mail templates* on page 173.

    e. Select **Notify following e-mails on route trigger** to be notified on route trigger and enter a notification email address, mail relay, or SMTP port in the field. For additional email configuration information, refer to *SMTP configuration* on page 183.

    f. Select the **Mail Template** from the menu to used for route triggering notifications. For email template configuration information, refer to *Mail templates* on page 173.

11. Click **Save**.

Subscribe to Advanced Routing application

To use Advanced Routing features, you must subscribe a user account or account template to an Advanced Routing application.

Prerequisites

- Create an Advanced Routing application. For instructions on creating an Advanced Routing application, see *Create Advanced Routing application* on page 805.
- Create at least one transfer site for the selected user account. For instructions on creating a transfer site, see *Transfer sites* on page 494.
- Assign at least one route to the selected user account. For instructions on assigning a Route Template Package, see *Assign Route Package Template* on page 818.

Workflow

1. *Select a user account* on page 821
2. *Configure general settings* on page 821
3. *Configure post transmission actions* on page 823
4. *Complete the subscription* on page 829

Select a user account

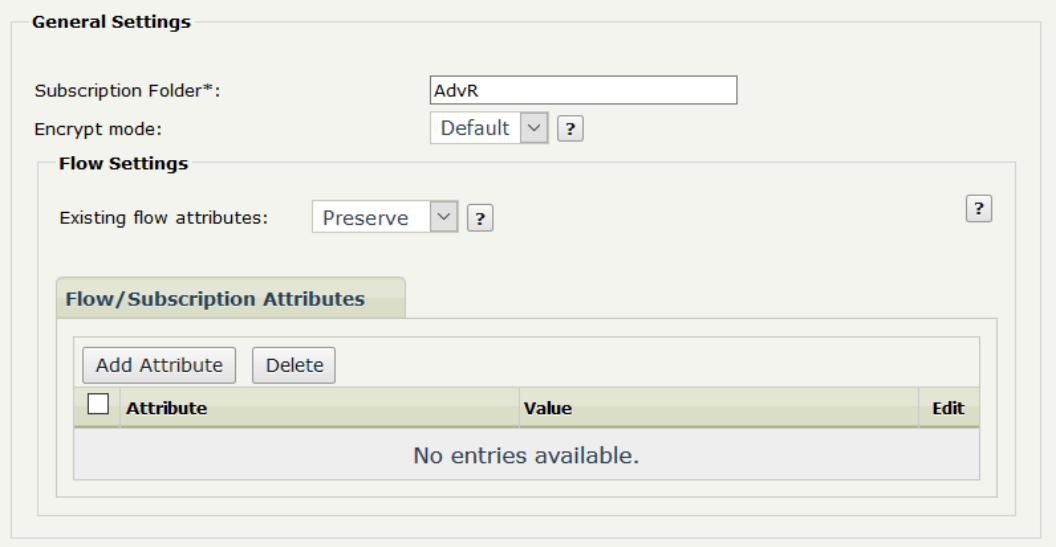
1. Select **Accounts > User Accounts**. The *User Accounts* page is displayed.
2. Click on the name of the account that you want to subscribe to the Advanced Routing application.

   The *User Account Settings* page is displayed with details for the selected account.
3. Click the **Subscriptions** tab for the selected account.
4. Click **Subscribe**.

   The settings page for the subscription is displayed.

Configure general settings

In the *General Settings* pane:



1. In the **Subscription Folder** field, type the full subscription folder path under the user's home folder. The subscription folder name can contain up to 254 characters.

   Note You cannot use the following characters in the subscription folder name: * < > ? " \ | :

2. Select the **Encrypt mode**. Selecting the **Encrypt mode** allows you to configure repository encryption for accounts at the per-subscription level. For additional information, refer to *Repository encryption certificate* on page 52.

   Select **Default** to inherit the encryption mode for the subscription folder from the account or the global settings.

   Select **Enable** to encrypt all files uploaded to the subscription folder.

   Select **Disable** to upload unencrypted files to the subscription folder.

   Note Files that are transferred via Advanced Routing or Standard Routing will be encrypted or not based on the target subscription folder repository encryption setting.

   For additional subscription folder repository encryption information, refer to *Configure general settings* on page 608.

3. In the *Flow Settings* pane, select the **Existing flow attributes**.

   If **Preserve** is selected, the attributes defined in the *Flow Attributes* pane will be applied only to newly received files which do not have associated flow attributes.

   If **Overwrite** is selected, the attributes defined in the *Flow Attributes* pane will overwrite any existing attributes for incoming files (for example, files published to this folder from another subscription folder).

   When **Append** is selected, only the attributes which are not defined for incoming files will be applied. Existing attributes will be preserved.

4. In the *Flow/Subscription Attributes* pane:

   a. To add a flow or a subscription attribute, click **Add Attribute**. For additional information, refer to *Flow and subscription attributes* on page 175.

   Add Attribute allows you to add custom properties as Key=Value pairs. Flow attributes can be used for expression evaluation in Advanced Routing only when the application operates with files. Subscription attributes are bound to the subscription, therefore, they can be used for expression evaluation in all Advanced Routing fields.

   Note Subscription attributes can be accessed using the following expression: `${subscription.attributes['userVars.ATTRIBUTE_NAME'].` Flow attributes can be accessed using the following expression: `${flow.attributes['userVars.ATTRIBUTE_NAME']}.`

   Some examples of attributes are:

Attribute	Value
userVars.1	internalEmail@axway.com
userVars.2	ReportsMonitor

   To access attributes, see the following examples: `${account.attributes['userVars.1']}${account.attributes['userVars.2']}` For example, the `account.attributes` is the selector for attributes of the account used to execute the current route - it must be written exactly as shown.The `userVars.` prefix must be prepended to the attribute name .All this should be written as an EL expression: `${...}`

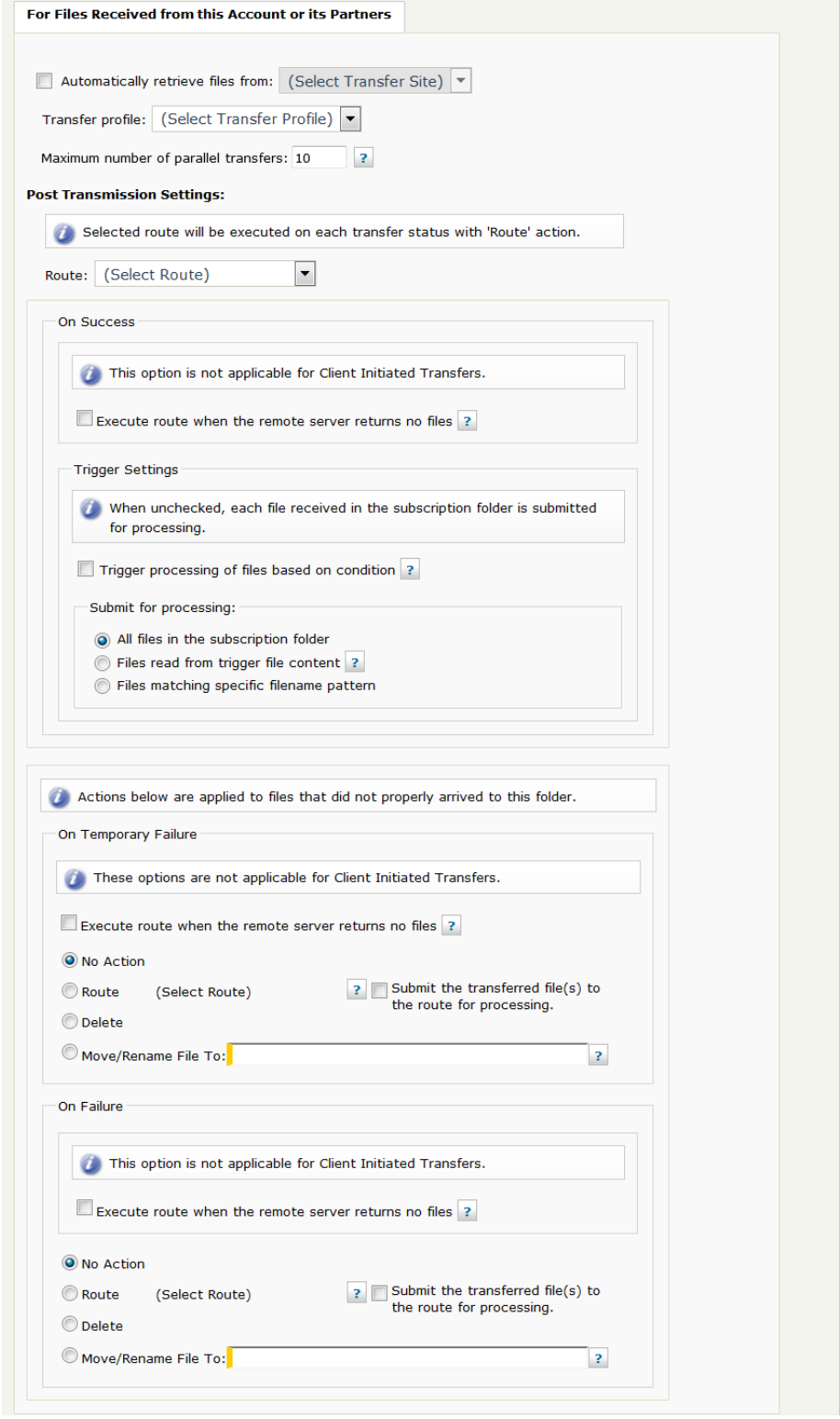
   b. Click the **Save** () icon.

Configure post transmission actions

Configuring the post transformation actions is divided into selecting the post transformation actions, the post client download actions, and the post routing settings.

Select the post transformation actions

In the *For Files Received from this Account or its Partners* pane:



1. To set a schedule for automatic retrieval of files from a remote server, select the **Automatically Retrieve Files From** check box and then select the transfer site from the drop-down list. If you select a PeSIT transfer site, you can select a **Transfer Profile** from the list or leave the field

empty to use the default PeSIT transfer profile. For more information, see *Transfer sites* on page 494.

The *Schedule* pane and the **Retrieve Files Now** button are displayed.

If subscription retrieves files from a Folder Monitor transfer site, to configure a scheduled Folder Monitor operation, you must select **Set explicit FolderMonitor Schedule**.

2. Click **Configure** in the *Schedule* pane to set up a future one time event or a recurring schedule.

   The *Configure Schedule* dialog box is displayed.

3. In the *Configure Schedule* dialog box, specify the desired conditions for the scheduled server-initiated file retrieval.

   To schedule an immediate recurrent task, select **Schedule events on a recurring basis** and then select **Start now** in the *Length of Recurrence* pane. The task will begin on the next minute.

   Note If the schedule is set on a recurring basis, the **Recurrence** options dynamically change with respect to the recurrence condition: **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.

   If the server goes down and restarts, the scheduler will not execute any scheduled tasks missed during the server down time.

   If you configure a schedule and save it after the scheduled start time, the task will not be executed. You must save your configured schedule before the scheduled start time.

4. (Optional) Enter the **Maximum number of parallel transfers**. If you enter a value greater than zero, SecureTransport executes only the specified number of transfers in parallel. If the value is null or zero, the maximum number of parallel transfers is limited by system capacity.

   The maximum number of parallel transfers limit is applied cluster wide. The limit for files transferred from the client will not be exceeded. Due to limitations in Standard Cluster communication mode, the parallel pulls limit can be exceeded when there are several connections. If you want to force the limit, then the `force.standart.cluster.sit.pulls.sync=true` system property should be added to the `start_tm_console`. Adding the property to the `start_tm_console` has a performance penalty due to increased cluster communication.
   Note that the `force.standard.cluster.sit.transfers.sync` value overrides the value of the `force.standart.cluster.sit.pulls.sync` property, used in previous SecureTransport versions for the same purposes.

5. (Optional) Click the **Retrieve Files Now** button to immediately trigger a one time file pull.

   Note When the one-time pull event is triggered, the admin daemon will try to connect to the Transaction Manager until the maximum number of retry attempts is reached as specified by the `Streaming.Event.maxRetries` server configuration parameter. The period between each retry is specified by the `Streaming.Event.idleTimeout` server configuration parameter. When the maximum number of retries is reached, the execution process

finishes. For more information on server configuration parameters, refer to *View and change server configuration parameters* on page 315.

6. In the *Post Transmission Settings* pane, select the **Route**. The selected route will be executed on files uploaded to the subscription folder.
7. In the *On Success* pane, to execute the selected route when the server does not return any, select the **Execute route when the remote server returns no files** check box. The selected route will be executed when directory listing is successful but there are no files matching the download pattern.
8. To trigger processing of files based on a specific condition, select the **Trigger processing of files based on condition** check box.

   When **unchecked**, each file received in the subscription folder is submitted for processing.

   When **checked**, processing of the files in the subscription folder will be triggered upon a specific condition.
9. Enter the trigger condition in the **Trigger condition** field.

   Example:

   To trigger file processing when the file the extension trigger arrives:

   ```
   ${stenv['target'].matches('.*.trigger')?1:0}
   ```
10. Select the files to submit for processing.

    If **All files in the subscription folder** (default) is selected, all files in the subscription folder are processed except for the trigger file.

    If **Files read from trigger file content** is selected, data file names will be read from trigger file content. Each file name should be on new line. The whitespace characters before and after the file names are discarded. Also lines containing only whitespace characters are not considered as files.

    Trigger file format:

    ```
    file1.txt

    file2.txt

    file3.png
    ```

    If **Files matching specific filename pattern** is selected, the files matching the defined filename pattern will be processed.

    The expression language can be used to specify the filename pattern.

    Examples:

    All text files - with `.txt` extension:

    ```
    *.txt
    ```

    All files that have names same as the trigger file name without extension.

    ```
    ${basename(stenv['target'])}.*
    ```

11. In the *On Temporary Failure* pane, select the option for temporary failed transfers. The temporarily failed transfers will be retried. The temporary failure option is not applicable for Client Initiated Transfers.

    Note The following actions are applied to files that did not properly arrive in the designated folder.

    If **No Action** is selected, no actions take place on the temporarily failing files.

    If **Route** is selected, the selected route will be triggered. By default, the route will be triggered without the temporarily failing files. Select **Submit the transferred file(s) to the route for processing** to perform transformations on the temporarily failing files inside the selected route.

    If **Delete** is selected, the temporarily failing files are deleted.

    If **Move/Rename File To** is selected, you are required to specify a directory in the location where you are transferring the temporarily failing files to and to provide an expression to rename the files.

12. In the *On Failure* pane, select the permanent failure option.

    Note The following actions are applied to files that did not properly arrive in the designated folder.

    If **No Action** is selected, no actions take place on the failed files.

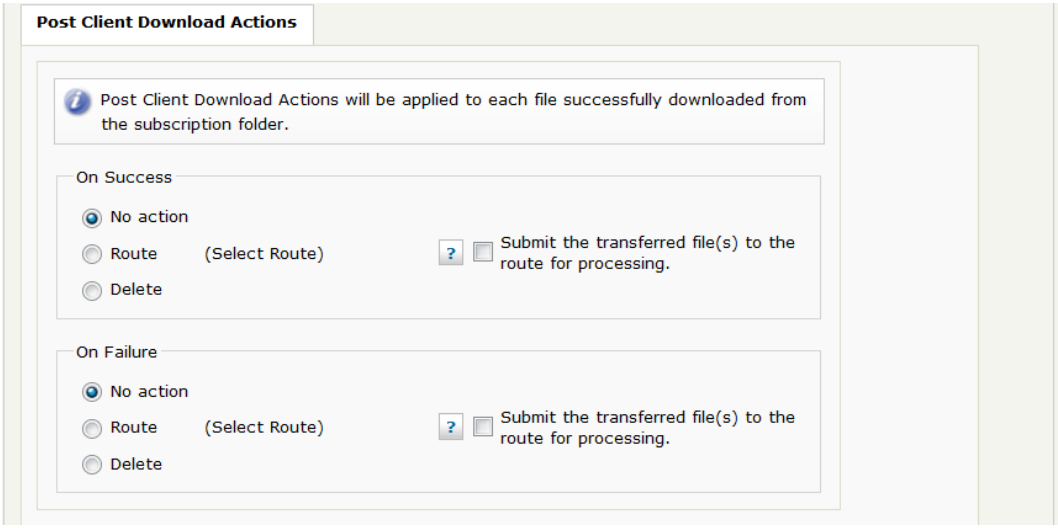
    If **Route** is selected, the selected route will be triggered. By default, the route will be triggered without the failed files. Select **Submit the transferred file(s) to the route for processing** to perform transformations on the failed files inside the selected route.

    If **Delete** is selected, the failed files are deleted.

    If **Move/Rename File To** is selected, you are required to specify a directory in the location where you are transferring the failed files to and to provide an expression to rename the files.

Select the post client download actions

In the *Post Client Download Actions* pane:



Note Post Client Download Actions will be applied to each file downloaded from the subscription folder.

1. In the *On Success* pane, select the action to take place for each successful client download.

   If **No Action** is selected, no actions take place on the downloaded files.

   If **Route** is selected, the selected route will be triggered. By default, the route will be triggered without the files that are being downloaded. Select **Submit the transferred file(s) to the route for processing** to perform transformations on the files that are being downloaded inside the selected route.

   If **Delete** is selected, after a file is successfully downloaded by the client, it is deleted from the Advanced Routing subscription folder.

2. In the *On Failure* pane, select the action to take place for each failed client download.

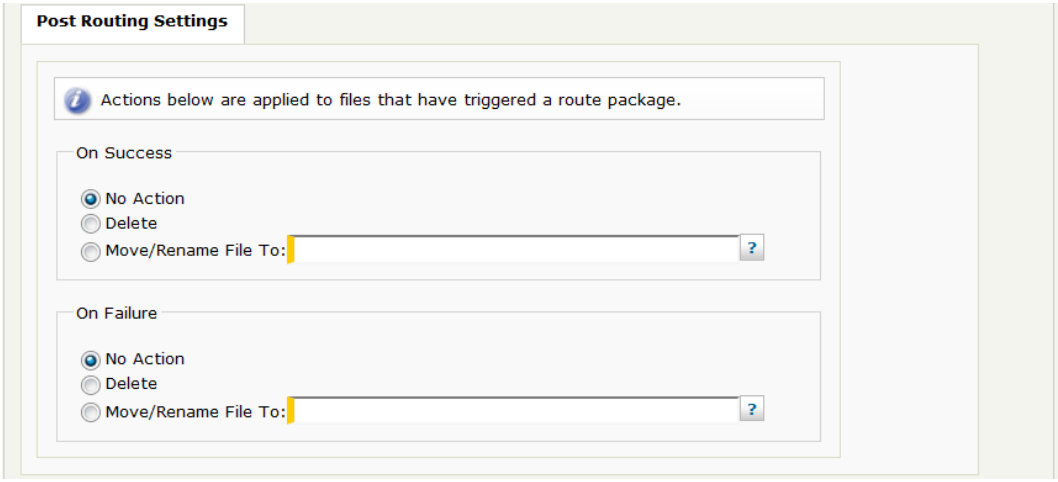
   If **No Action** is selected, no actions take place on the files that failed downloading.

   If **Route** is selected, the selected route will be triggered. By default, the route will be triggered without the files that are being downloaded. Select **Submit the transferred file(s) to the route for processing** to perform transformations on the files that are being downloaded inside the selected route.

   If **Delete** is selected, after a file download by the client fails, the file is deleted from the Advanced Routing subscription folder.

Select the post routing actions

In the *Post Routing Settings* pane:



Note The Post Routing Settings actions are applied to files that have triggered a route package.

1. In the *On Success* pane, select the action to take place for each file that successfully triggered a route.

   If **No Action** is selected, no actions take place on the files that successfully triggered a route.

   If **Delete** is selected, the files that successfully triggered a route are deleted.

If **Move/Rename File To**is selected, you are required specify a directory in the location where you are transferring the files to that successfully triggered a route and to provide an expression rename the files.

2. In the *On Failure* pane, select the action to take place for each file that failed to trigger a route.

   If **No Action** is selected, no actions take place on the files that failed to trigger a route.

   If **Delete** is selected, the files that failed to trigger a route are deleted.

   If **Move/Rename File To**is selected, you are required specify a directory in the location where you are transferring the files to that failed to trigger a route and to provide an expression rename the files.

Complete the subscription

To complete the Advanced Routing subscription, click **Add**.

Transformations

This topic includes detailed configuration information for the transformation routing steps. Detailed configuration information is provided for the available transformations with Advanced Routing steps.

The following topics provide detailed how-to instructions for configuring different transformations:

- *PGP Encryption* on page 829
- *PGP Decryption* on page 835
- *Compress* on page 838
- *Decompress* on page 842
- *Line Ending* on page 846
- *External Script* on page 850
- *Encoding Conversion* on page 853
- *Characters Replace* on page 856
- *Line Padding* on page 861
- *Line Truncating* on page 865
- *Line Folding* on page 869
- *Rename* on page 873

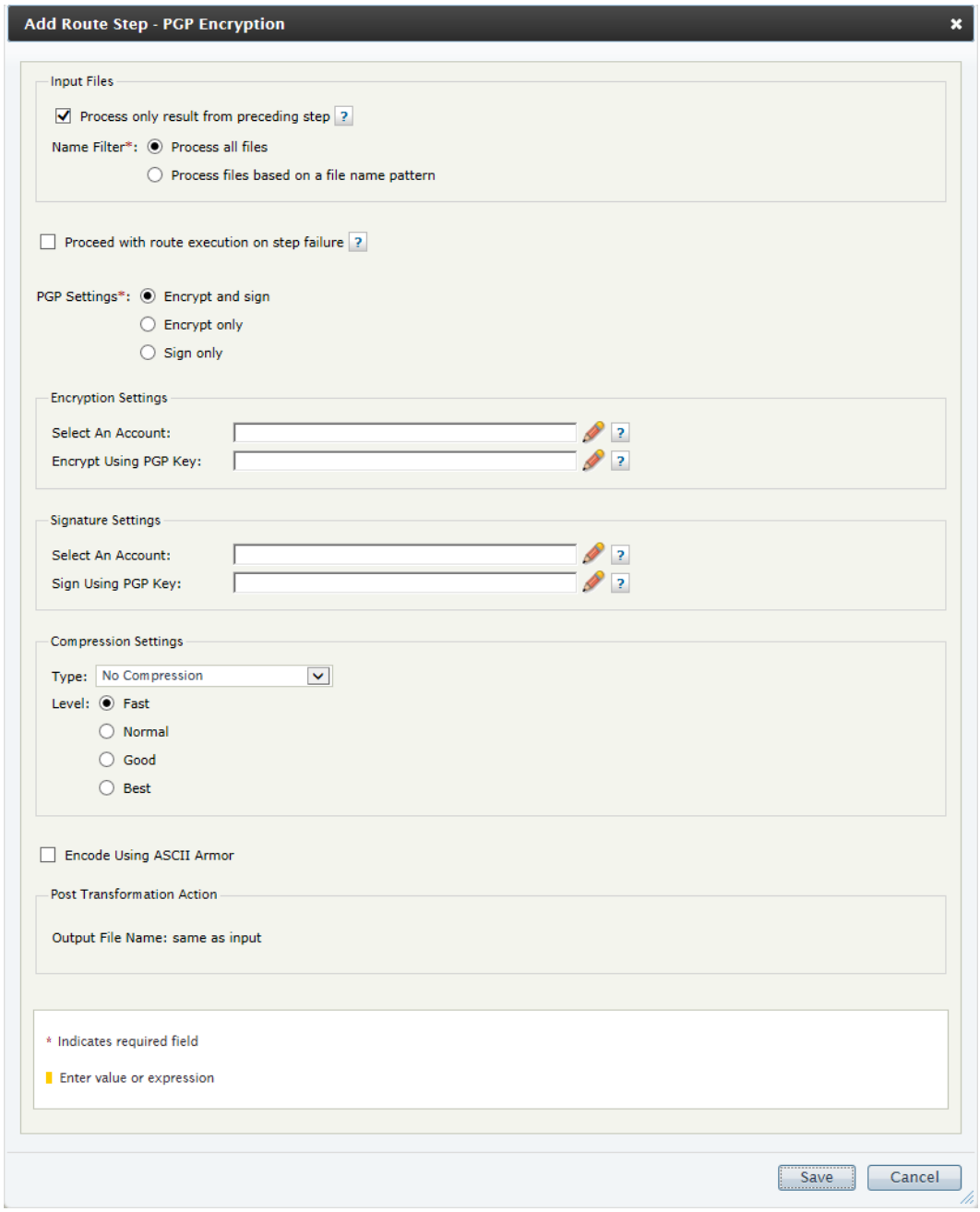
PGP Encryption

The PGP Encryption transformation step enables the encryption and signing of designated files as part of a route. To add a PGP Encryption transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Select PGP settings, including encryption and signature settings as determined by selected PGP setting.
4. Set compression level and type.
5. Determine whether or not to ASCII armor encode transformed files.
6. Determine post transformation actions.

Note Steps 1 and 3 are mandatory. All other steps are optional.

The following figure provides an example of the PGP Encryption transformation step.



Note The buffer size for PGP encryption and decryption is controlled by the `Pgp.BufferSize` server configuration option.

The following topics provide configuration details for the PGP Encryption transformation step:

- *Input Files* on page 832
- *Proceed with route execution on step failure* on page 833
- *PGP Settings* on page 833
- *Encryption Settings* on page 833
- *Signature Settings* on page 834

- *Compression Settings* on page 834
- *Encode using ASCII Armor* on page 835
- *Post transformation action* on page 835

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

The Name Filter can either be set to process all files forwarded by the selection of *Process only result from preceding step* or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*. If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed. If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression pattern are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

  ```
  *.[!0-9]
  ```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

```
.*\.(xml|txt)
```

- Case insensitive match of `data.xml` file.

```
(?i)data\.xml
```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

If *Proceed with route execution on step failure* is not checked, the processing stops on the first failed file if there are several files being transformed by the step. The route execution also stops.

Proceed with route execution on step failure is not checked by default.

PGP Settings

The PGP setting can be encrypt and sign, encrypt only, or sign only. If *Encrypt and sign* is selected, the files being processed by the route step are encrypted and signed. If *Encrypt only* is selected, the files being processes by the route step are encrypted but not signed. If *Sign only* is selected, the files being processed by the route step are signed but not encrypted.

Encryption Settings

The encryption settings consist of selecting an account and the PGP key to use for encryption.

Select an account

Either an account name or an Expression Language (EL) string can be specified to determine the recipient based on the environment information (such as filename).

The *Select an account* field has auto-completion which shows a list of existing accounts containing the same letter.

Once an account is selected its publicly available PGP certificates are populated in the *Select an account* field. The certificates can be public for all SecureTransport accounts, or public for an account assigned to the same Business Unit.

If an account name is unknown (for example, expression based) its PGP certificates are determined at run time. PGP certificates can be expression based as well.

Encrypt using PGP key

A PGP Encryption key can be selected from PGP Public Keys (within the selected account) or by entering an expression string. The access level of PGP keys is determined by the select access level. The PGP key selected access level can be private, business unit, or public.

Wild card symbols ('*' and '?') can be used when specifying the PGP key alias (for example, `.*-pgp`). If multiple keys match the pattern the first one is picked up and used.

Signature Settings

The signature settings consist of selecting the account and the PGP key to use for signing.

Select an account

Either an account name or an EL string can be specified to determine the recipient based on the environment information (such as filename).

The *Select an account* field has auto-completion which shows a list of existing accounts containing the same letter.

Once an account is selected its publicly available PGP certificates are populated in the *Select an account* field. The certificates can be public for all SecureTransport accounts, or public for an account assigned to the same Business Unit.

If an account name is unknown (for example, expression based) its PGP certificates are determined at run time. PGP certificates can be expression based as well.

Sign using PGP key

A PGP signature key can be selected from PGP Public Keys (within the selected account) or by entering an expression string.

Wild card symbols ('*' and '?') can be used when specifying the PGP key alias (for example, `.*-pgp`). If multiple keys match the pattern the first one is picked up and used.

Compression Settings

The compression settings consist of selecting the type and level of compression.

Type

The types of compression that can be selected are:

- No Compression
- Use Preferred
- ZIP

- ZLIB
- BZIP2

Level

The levels of compression that can be selected are:

- Fast
- Normal
- Good
- Best

Encode using ASCII Armor

If *Encode using ASCII Armor* is checked, the files processed by the route step are ASCII armor encoded.

Post transformation action

The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

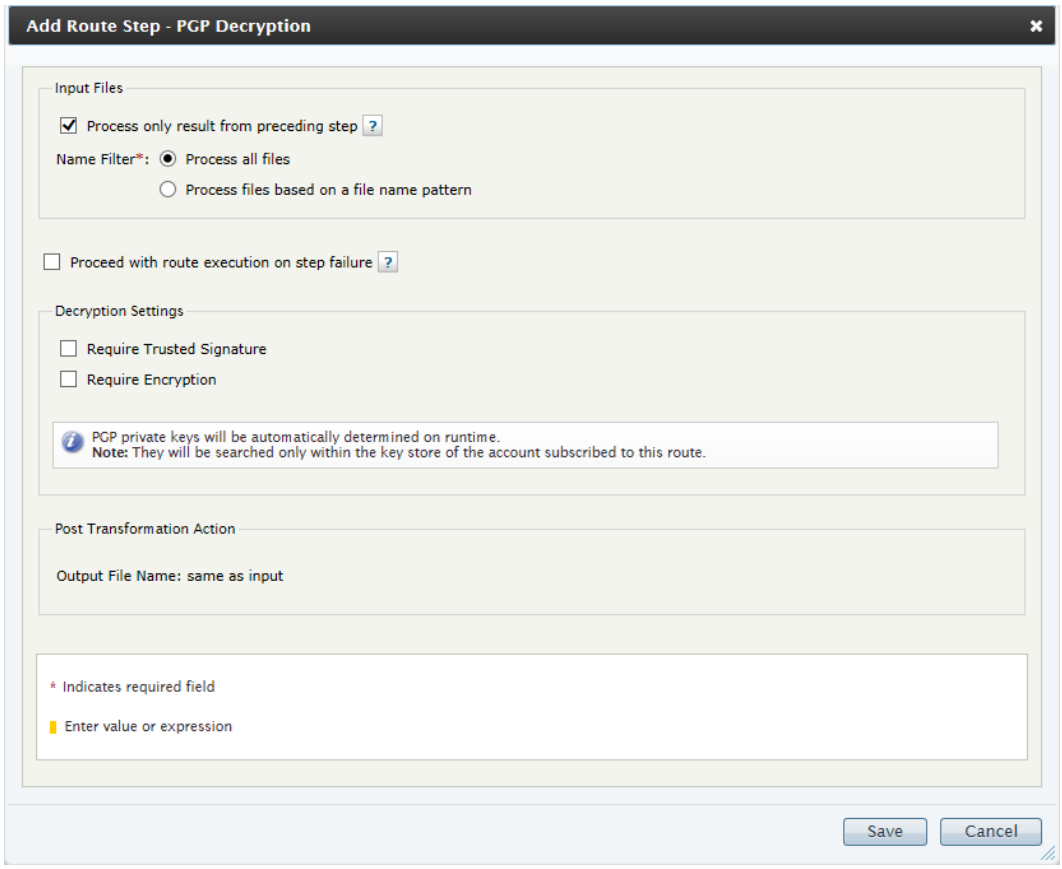
PGP Decryption

The PGP Decryption transformation step enables the decryption and signature verification of designated files as part of a route. To add a PGP Decryption transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Select decryption settings.
4. Determine post transformation actions.

Note Step 1 is mandatory. All other steps are optional.

The following figure provides an example of a PGP Decryption transformation step.



Note The buffer size for PGP encryption and decryption is controlled by the `Pgp.BufferSize` server configuration option.

The following topics provide configuration details for the PGP Decryption transformation step:

- *Input Files* on page 836
- *Proceed with route execution on failure* on page 837
- *Decryption Settings* on page 838
- *Post transformation action* on page 838

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

The Name Filter can either be set to process all files forwarded by the selection of *Process only result from preceding step* or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*. If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed. If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression pattern are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

  ```
  *.[!0-9]
  ```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

  ```
  .*\.(xml|txt)
  ```

- Case insensitive match of `data.xml` file.

  ```
  (?i)data\.xml
  ```

Proceed with route execution on failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

If *Proceed with route execution on step failure* is not checked, the processing stops on the first failed file if there are several files being transformed by the step. The route execution also stops.

Proceed with route execution on step failure is not checked by default.

Decryption Settings

The two selections for decryption settings are:

- Require Trusted Signature
- Require Encryption

PGP private keys are automatically determined on runtime.

Note PGP private and public keys are only searched for within the key store of the account subscribed to this route.

Require Trusted Signature

If *Require Trusted Signature* is selected, the transformation of the designated file or files requires a PGP partner key for signature verification. If a signature is required, but the file is not signed, the signature verification fails. If encryption is required but the file is not encrypted, the PGP Decryption fails. If both trusted signature and encryption are required but the file is neither encrypted or signed, the decryption fails. PGP Decryption step also fails if there is a problem with the certificate selected (not valid, expired, not signed, and so forth).

Require Encryption

If *Require Encryption* is selected, the transformation of the designated file or files requires a PGP private key for decryption.

Post transformation action

The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

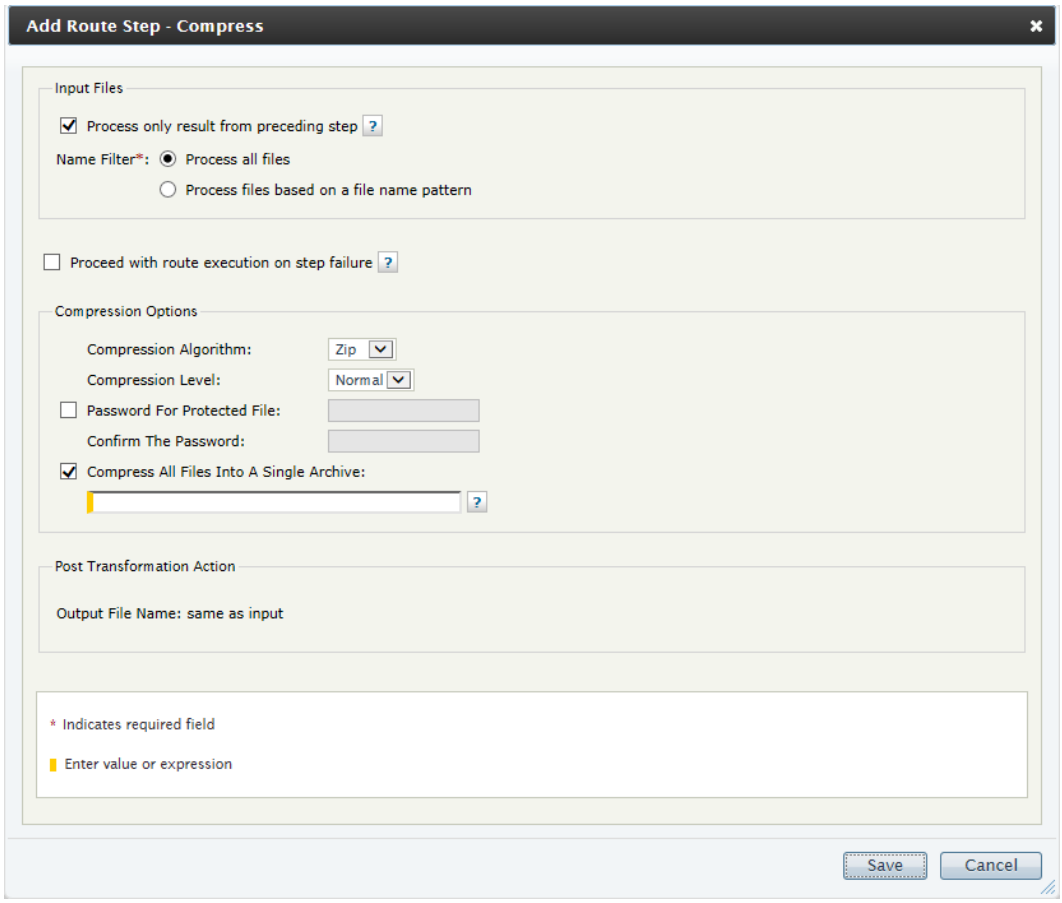
Compress

The Compress transformation step enables the compression of designated files as part of a route. To add a compression transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Select compression options.
4. Determine post transformation actions.

Note Step 1 is mandatory. All other steps are optional.

The following figure provides an example of a Compress transformation step.



The following topics provide configuration details for the Compress transformation step:

- *Input Files* on page 839
- *Proceed with route execution on step failure* on page 841
- *Compression Options* on page 841
- *Post transformation action* on page 842

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

The Name Filter can either be set to process all files forwarded by the selection of *Process only result from preceding step* or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*. If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed. If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression pattern are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

  ```
  *.[!0-9]
  ```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

  ```
  .*\.(xml|txt)
  ```

- Case insensitive match of `data.xml` file.

  ```
  (?i)data\.xml
  ```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Compression Options

The compression options consists of determining compression algorithm and level for designated files. The compression options also include determining whether or not the compressed files is password protected and whether or not the designated files are compressed into a single archive.

Note Password protection is only available for the ZIP compression algorithm.

Note Compressing all files into a single archive **is not** available for the GZIP compression algorithm.

Compression algorithm

The selectable compression algorithms are:

- ZIP
- JAR
- TAR
- GZIP

The compression of `tar.gz` archives require two separate Compress steps. The first one to archive files in a tar archive and the second one to compress the tar archive into a gzip archive.

Compression level

The selectable compression levels are:

- Store
- Fastest
- Fast
- Normal
- Good
- Better
- Best

As compressed file size decreases (from store to best), the time to compress increases.

Password for protected file

Note Password protection is only available for the ZIP compression algorithm.

If *Password for protected file* is selected, enter the desired password.

Confirm the password

If *Password for protected file* is selected, confirm the desired password.

Compress all files into a single archive

Note Compressing all files into a single archive **is not** available for the GZIP compression algorithm.

If **Compress all files into a single archive** is selected, all designated files are compressed into a single archive. An EL expression should be used to define the single archive name.

Example:

- Target file name, containing timestamp:

```
archive-${timestamp}.zip
```

If **Compress all files into a single archive** is not selected, each input file is compressed in a separate archive which is named as the input file (including extension) and with an algorithm specific extension added: `.zip`, `.jar`, `.tar`, or `.gz`

Post transformation action

The output file names will be the same as the input file names and with an algorithm specific extension added unless **Compress all files into a single archive** is selected. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873. If **Compress all files into a single archive** is selected then the output file name is designated by the EL expression.

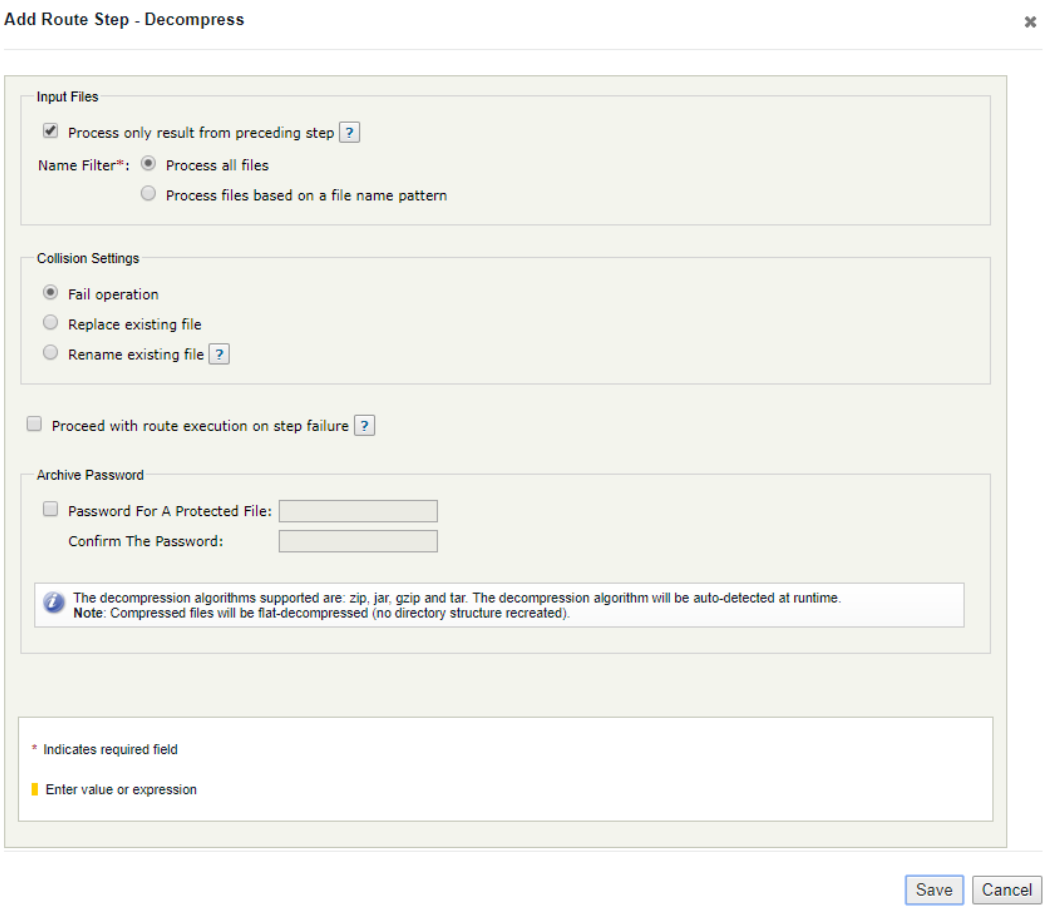
Decompress

The Decompress transformation step enables the decompression of designated archived files as part of a route. To add a Decompress transformation step to a Route Package Template, take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Select decompression options.
4. Determine post transformation actions.

Note Step 1 is mandatory. All other steps are optional.

The following figure provides an example of a Decompress transformation step.



The following topics provide configuration details for the Decompress transformation step:

- *Input Files* on page 843
- *Collision settings* on page 844
- *Proceed with route execution on step failure* on page 845
- *Archive Password* on page 845
- *Post transformation action* on page 846

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

The Name Filter can either be set to process all files forwarded by the selection of *Process only result from preceding step* or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*. If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed. If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression pattern are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

  ```
  *.[!0-9]
  ```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

  ```
  .*\.(xml|txt)
  ```

- Case insensitive match of `data.xml` file.

  ```
  (?i)data\.xml
  ```

Collision settings

The Collision settings determine how an archive containing a file with the same name is handled.

The following options are available:

- **Fail operation** - Default setting. A file with the same name as the archive prevents its extraction; an error is reported, and the step fails.
- **Replace existing file** - When set, the archive member is extracted into a file with the same name, and the archive is deleted.
- **Rename existing file** - When set, name collisions are resolved automatically by appending *(new copy <number>)* to the extracted archive member that shares its name with the archive. The archive name remains unchanged.
  For example:
  - When an archive named *myFile* contains a file named *myFile*, the archived file will be renamed to *myFile (new copy 1)*.
  - If a file with a name *myFile (new copy 1)* already exists, the extracted file will be renamed to *myFile (new copy 2)*.

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Archive Password

Archive Password consists of entering and confirming the archive password if *Password for a protected file* is selected.

Note Password protection is only available for the ZIP compression algorithm.

The decompression algorithms supported are:

- ZIP
- JAR
- GZIP
- TAR

The decompression algorithm is auto-detected at runtime.

All `tar.gz` archives require two separate Decompress steps. The first one to extract the tar from gzip archive and the second one to decompress the gzip archive.

Note Compressed files are flat-decompressed (no directory structure is recreated).

If there is a file with the same name in different folders inside the archive, only one of them is extracted.

For example:

If an archive.zip file contains two folders (`folder1` and `folder2`) and each of the folders contains a file named `file.txt` (`folder1\file.txt` and `folder2\file.txt`), only one copy of `file.txt` is extracted.

Password for a protected file

If *Password for protected file* is selected, enter the archive password.

Confirm the password

If *Password for protected file* is selected, confirm the archive password.

Post transformation action

The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

Line Ending

The Line Ending transformation step enables converting line ending formats as part of a route.

Note Currently, the Line Ending transformation accepts Unicode or ASCII as an input, or mixed input when the custom line ending format is selected.

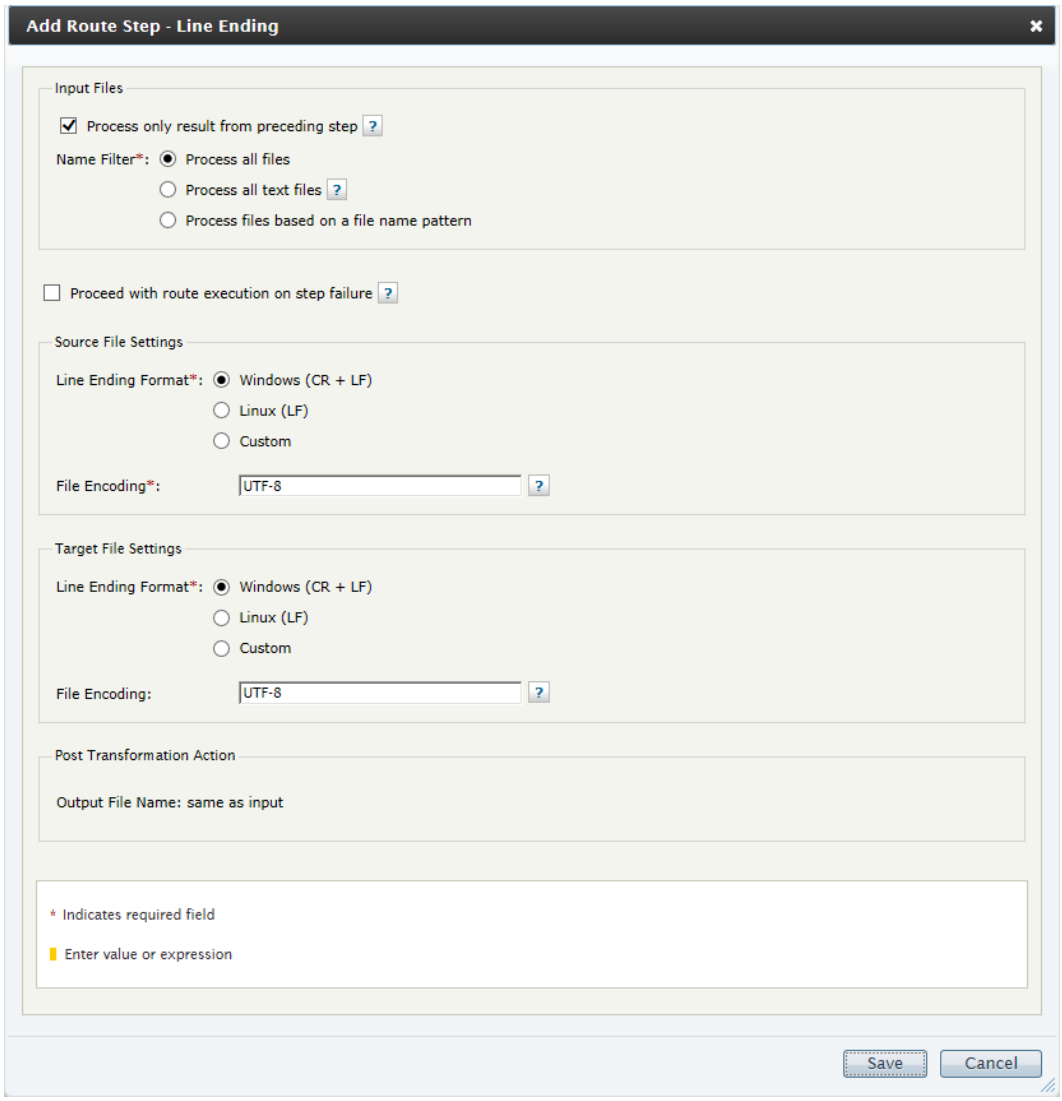
Note If the encoding a file is changed to IBM500, IBM037, or IBM424; the line ending of the input file should be LF and not CRLF. The CR is preserved in some cases and a new line appears between every original line.

To add a Line Ending transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Select source file setting options.
4. Select target file setting options.
5. Determine post transformation actions.

Note Steps 1, 3, and 4 are mandatory. All other steps are optional.

The following figure provides an example of a Line Ending transformation step.



The following topics provide configuration details for the Line Ending transformation step:

- *Input Files* on page 847
- *Proceed with route execution on step failure* on page 849
- *Source file settings* on page 849
- *Target file settings* on page 850
- *Post transformation action* on page 850

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

Name filtering can either be set to process all files, process all text files, or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*.

If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed.

If *Process all text files* is selected, all text files forwarded by the selection of *Process only result from preceding step* are processed.

Text file selection is determined based on the file extension and the MIME type that corresponds to that extension. MIME types are defined in the `mime.types` configuration file located in:

Administrator's Tool > Server Configuration > Configuration Files

Furthermore, some MIME types can be defined as text by configuring the `AdvancedRouting.TextMimeSubtypes` server configuration option. For example, to configure the `application/xml` MIME type to be treated as text, add `xml` to the server configuration option.

If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression all files forwarded by the selection of *Process only result from preceding step* are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

```
*.[!0-9]
```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

```
.*\.(xml|txt)
```

- Case insensitive match of `data.xml` file.

```
(?i)data\.xml
```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Source file settings

The source file settings consists of selecting a source file line ending format and encoding.

Line ending format

The selectable line ending formats are:

- Windows (CR + LF)
- Unix (LF)
- Custom

If *Custom* is selected, specify line ending characters in ASCII or Unicode format (\uXXXX). The hex encoded value of the line ending is any character `\n`, `\r`, and the combination of both. The custom line ending char in Unicode notation:

- Windows:

```
\u000d\u000a
```

- *nix, MacOS:

```
\u000a
```

- Mainframe:

```
\u0025
```

File encoding

The file encoding format can be selected from a long list of available formats. Start typing the desired file encoding format in the field and select the desired file encoding format from the list. For a supported list of source and target encodings, refer to encoding.doc.html.

Target file settings

The target file settings consists of selecting a target file line ending format and encoding.

Line ending format

The selectable line ending formats are:

- Windows (CR + LF)
- Unix (LF)
- Custom

If *Custom* is selected, the hex encoded value of the line ending character must be specified. The hex encoded value of the line ending is any character `\n`, `\r` combination of both. The custom line ending char in Unicode notation:

- Windows:

  ```
  \u000d\u000a
  ```

- *nix, MacOS:

  ```
  \u000a
  ```

- Mainframe:

  ```
  \u0025
  ```

File encoding

The file encoding format can be selected from a long list of available formats. Start typing the desired file encoding format in the field and select the desired file encoding format from the list.

Post transformation action

The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

External Script

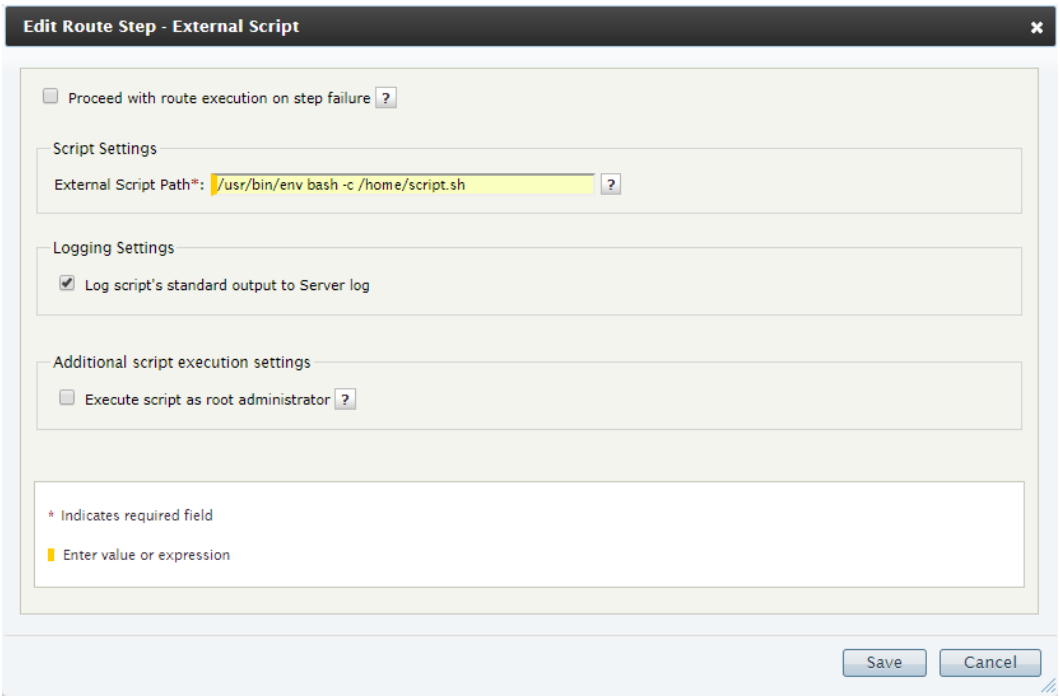
Note The External Script transformation does not function with repository encryption.

The External Script transformation step enables adding the execution of external script as part of a route. To add an External Script transformation step to a Route Package Template take the following steps:

1. Determine whether or not to proceed with route execution on step failure.
2. Select the external script path.
3. Determine whether or not to log the external script's standard output to the server log.
4. Select whether or not to run scripts as the root administrator.

Note Step 2 is mandatory. All other steps are optional.

The following figure provides a configured example of an External Script transformation step.



The following topics provide configuration details for the External Script transformation step:

- *Proceed with route execution on step failure* on page 851
- *Script Settings* on page 852
- *Logging Settings* on page 852
    - Log script's standard output to Server log
    - Run as root for external script

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Script Settings

The script settings consist of the selecting the external script path.

External script path

The external script path is an absolute path to external script.

Example script expressions:

- For *nix environment:

```
/usr/bin/env bash -c
"${FILEDRIVEHOME}/bin/agents/example.sh ${date
('yyyyMMdd')} ${currentfulltarget}
${transfer.transferredBytes} ${routing.originalFiles}"
```

- For Windows environment:

```
cmd /c ${FILEDRIVEHOME}\bin\agents\example.bat ${date
('yyyyMMdd')} ${currentfulltarget}
${transfer.transferredBytes} ${routing.originalFiles}
```

Logging Settings

The logging settings consists of determining whether or not the external script's standard output is logged to the server log.

Log script's standard output to Server log

If *Log script's standard output to Server log* is selected, the external script's standard output is logged to the server log.

Run as root for external script

External script steps can be configured to run scripts as a root administrator for each individual step instance.

When running scripts as a system superuser, scripts have the ability to execute the full scope of commands, thus exposing the system in the hands of the writer of the script.

General recommendation is to avoid using this option or to use it with caution.

By default, the option is unchecked.

For more information, refer to the SecureTransport Security Guide.

Note Running scripts as root is not default behavior. Enabling it makes possible running commands to which the routing step might not have permissions to execute otherwise.

Note This option is available to administrators with sufficient level of permission only. By default, master and account administrators can manage the option. For delegated administrator privileges, see Delegated administration.

Note When running scripts from the external script routing step, the execution environment might not have full scope of environment variables initialized. The script writer is responsible to properly export and initialize the necessary environment in the script itself before the actual script execution specifics.

Note The option is applicable only for root and non-Windows deployments.

Encoding Conversion

The Encoding Conversion transformation converts the character encoding of an input file to another configured encoding. Both source file encoding and output file encoding must be configured in the transformation step settings.

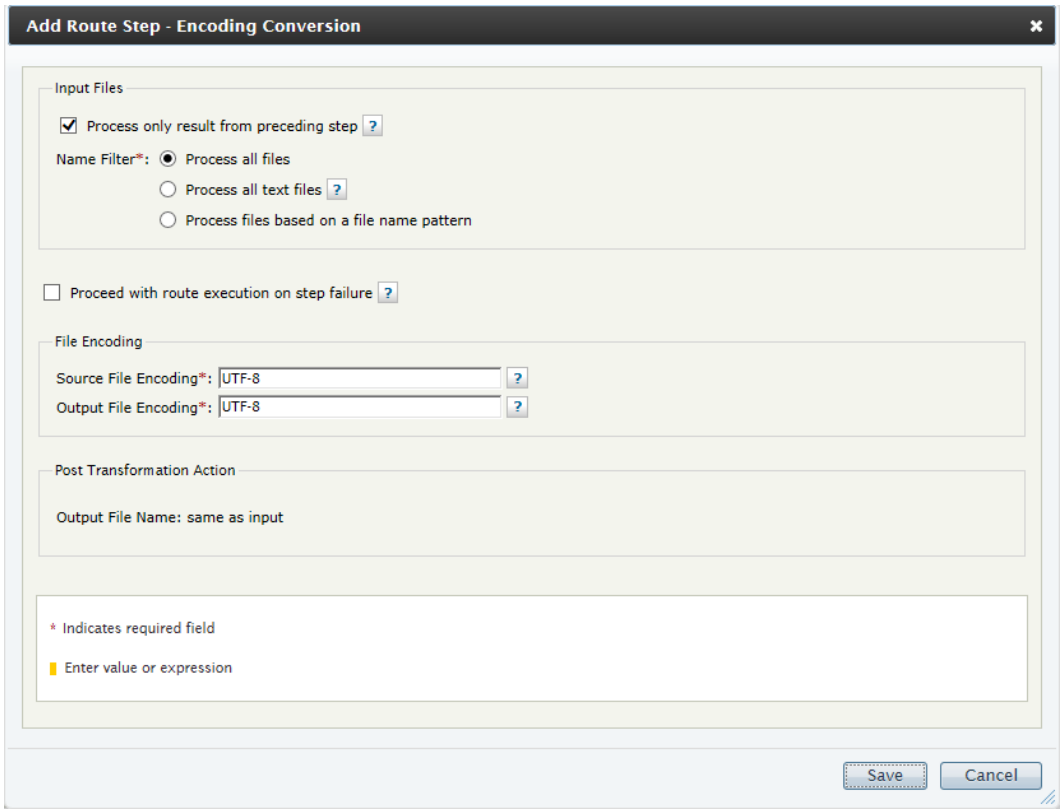
Note If the encoding a file is changed to IBM500, IBM037, or IBM424; the line ending of the input file should be LF and not CRLF. The CR is preserved in some cases and a new line appears between every original line. If the line ending is not LF, a Line Ending step can used before the Encoding Conversion step.

To add an Encoding Conversion transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Select source file encoding option.
4. Select output file encoding option.
5. Determine post transformation actions.

Note Steps 1, 3, and 4 are mandatory. All other steps are optional.

The following figure provides an example of an Encoding Conversion transformation step.



The following topics provide configuration details for the Encoding Conversion transformation step:

- *Input Files* on page 854
- *Proceed with route execution on step failure* on page 856
- *File encoding* on page 856
- *Post transformation action* on page 856

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

Name filtering can either be set to process all files, process all text files, or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*.

If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed.

If *Process all text files* is selected, all text files forwarded by the selection of *Process only result from preceding step* are processed.

Text file selection is determined based on the file extension and the MIME type that corresponds to that extension. MIME types are defined in the `mime.types` configuration file located in:

Administrator's Tool > Server Configuration > Configuration Files

Furthermore, some MIME types can be defined as text by configuring the `AdvancedRouting.TextMimeSubtypes` server configuration option. For example, to configure the `application/xml` MIME type to be treated as text, add `xml` to the server configuration option.

If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression all files forwarded by the selection of *Process only result from preceding step* are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

  ```
  *.[!0-9]
  ```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

```
.*\.(xml|txt)
```

- Case insensitive match of `data.xml` file.

```
(?i)data\.xml
```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

File encoding

Both source file encoding and output file encoding must be configured.

Source file encoding

Encoding of the file that will be transformed specified by the name of a SecureTransport supported character set. The **Source file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Output file encoding

Encoding of the file that will be produced specified by the name of a SecureTransport supported character set. The **Output file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Post transformation action

The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

Characters Replace

Note Currently, the Character Replace transformation accepts Unicode or ASCII as an input, or mixed input for the **Find** and **Replace** fields.

Note If the encoding a file is changed to IBM500, IBM037, or IBM424; the line ending of the input file should be LF and not CRLF. The CR is preserved in some cases and a new line appears between every original line. If the line ending is not LF, a Line Ending step can used before the Characters Replace step.

Note The comma (,) symbol can be used in ASCII only as a separator and not as find criteria. For find criteria, the comma (,) symbol can only be used in Unicode.

The Characters Replace transformation has two working modes. Only one mode can be active at a time.

Find/Replace mode

The Characters Replace transformation will search the input file for character sequences matching the specified search sequences and if a match is found it will be replaced with the replace character sequence. The search and replace character sequences are specified in the transformation step settings. More than one search sequence can be configured separating the sequences with a comma character.

This mode can be configured in one of two ways:

1. The number of find sequences is one or greater. The replace sequence is only 1.

   Multiple find sequences are specified separated with commas (,) and only a single replace sequence. In this case all find sequences have the same corresponding replace sequence. The transformation will search the input file for matches to the specified find sequences. If multiple sequences match the same text for replacement, only the first sequence that is found to fully match the text will be replaced.

   Note Empty replace sequence is a valid configuration. If such is specified, when a search match is found the matching sequence will effectively be removed from the file content.

2. The number of find and replace sequences is the same.

   In this case each find character sequence has its own replace character sequence. The correlation between find and replace sequences is based on their position in the configuration (the first find sequence corresponds to the first replace sequence, the second find to the second replace and so on).

   The transformation will search the input file for matches to the specified search sequences. When a match to a find sequence is found, it will be replaced by its own corresponding replace sequence. If multiple sequences match the same text for replacement, only the first sequence that is found to fully match the text will be replaced.

Find/Line strip

The Characters Replace transformation will strip all file lines starting with a specified search character sequence. The search character sequence is specified in the transformation step settings. More than one search sequence can be configured separating the sequences with a comma character.

The transformation will search the input file for matches at the start of each row to the specified find sequences. If a match is found, the row will be removed from the file content.

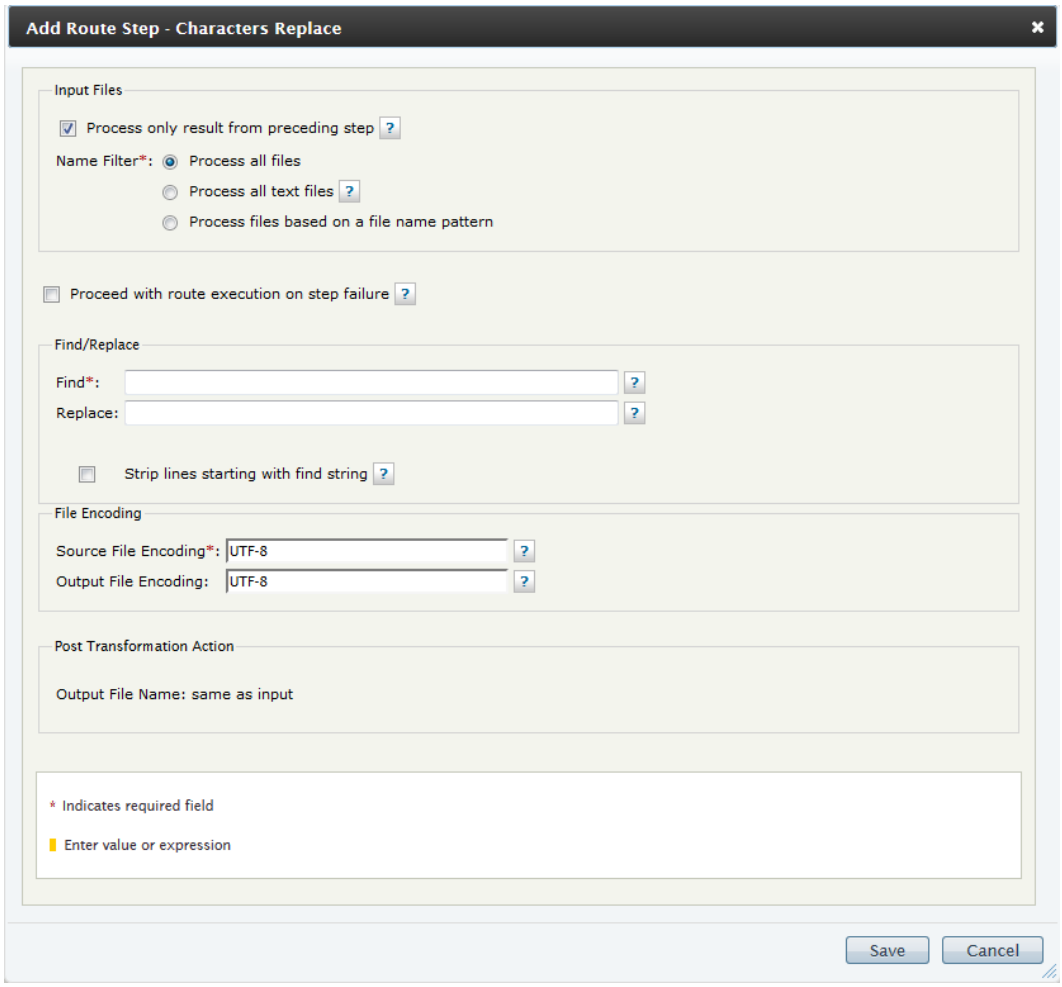
Characters Replace configuration

To add a Characters Replace transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Determine the working mode. If Find/Replace mode, complete the **Find** and **Replace** fields. If Find/Line strip mode, select **Strip lines starting with find string.** and complete the **Find** field.
4. Select source file encoding option.
5. Select output file encoding option.
6. Determine post transformation actions.

Note Steps 1, 3, and 4 are mandatory. All other steps are optional.

The following figure provides an example of a Characters Replace transformation step.



The following topics provide configuration details for the Replace transformation step:

- *Input Files* on page 859
- *Proceed with route execution on step failure* on page 860
- *Find/Replace mode* on page 860
- *Find/Line strip* on page 861

- *File encoding* on page 861
- *Post transformation action* on page 861

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

Name filtering can either be set to process all files, process all text files, or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*.

If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed.

If *Process all text files* is selected, all text files forwarded by the selection of *Process only result from preceding step* are processed.

Text file selection is determined based on the file extension and the MIME type that corresponds to that extension. MIME types are defined in the `mime.types` configuration file located in:

Administrator's Tool > Server Configuration > Configuration Files

Furthermore, some MIME types can be defined as text by configuring the `AdvancedRouting.TextMimeSubtypes` server configuration option. For example, to configure the `application/xml` MIME type to be treated as text, add `xml` to the server configuration option.

If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression all files forwarded by the selection of *Process only result from preceding step* are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

  ```
  *.[!0-9]
  ```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

  ```
  .*\.(xml|txt)
  ```

- Case insensitive match of `data.xml` file.

  ```
  (?i)data\.xml
  ```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Find/Replace mode

If Find/Replace mode, complete the **Find** and **Replace** fields.

Find

Specify the find character sequence. Unicode notation (\uXXXX) can be used. Multiple find character sequences separated with a comma (,) can be specified.

Note Comma must be Unicode encoded (\002c) if used in the find sequence.

Replace

Specify the replace character sequence. Unicode notation (\uXXXX) can be used. Multiple replace character sequences separated with a comma (,) can be specified. The number of replace sequences must be equal to the number of find sequences or just a single sequence.

Note Leaving this field blank is a valid configuration. Empty replace sequence is treated as an empty character.

Note Comma must be Unicode encoded (\002c) if used in the replace sequence.

Find/Line strip

If Find/Line strip, select **Strip lines starting with find string.** and complete the **Find** field.

File encoding

The source file encoding must be configured. Configuring the output file encoding is not mandatory. If it is not set, the output file encoding will be the same as the source file encoding.

Source file encoding

Encoding of the file that will be transformed specified by the name of a SecureTransport supported character set. The **Source file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Output file encoding

Encoding of the file that will be produced specified by the name of a SecureTransport supported character set. The **Output file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Post transformation action

The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

Line Padding

The Line Padding transformation will pad input text file lines to a configured length "X" with a configured character "C". If a file line length is longer than or equal to "X" number of characters then the line will be outputted to the result file without change. If a line length is shorter than "X" number of characters, then it will be padded out with character "C" to the length "X".

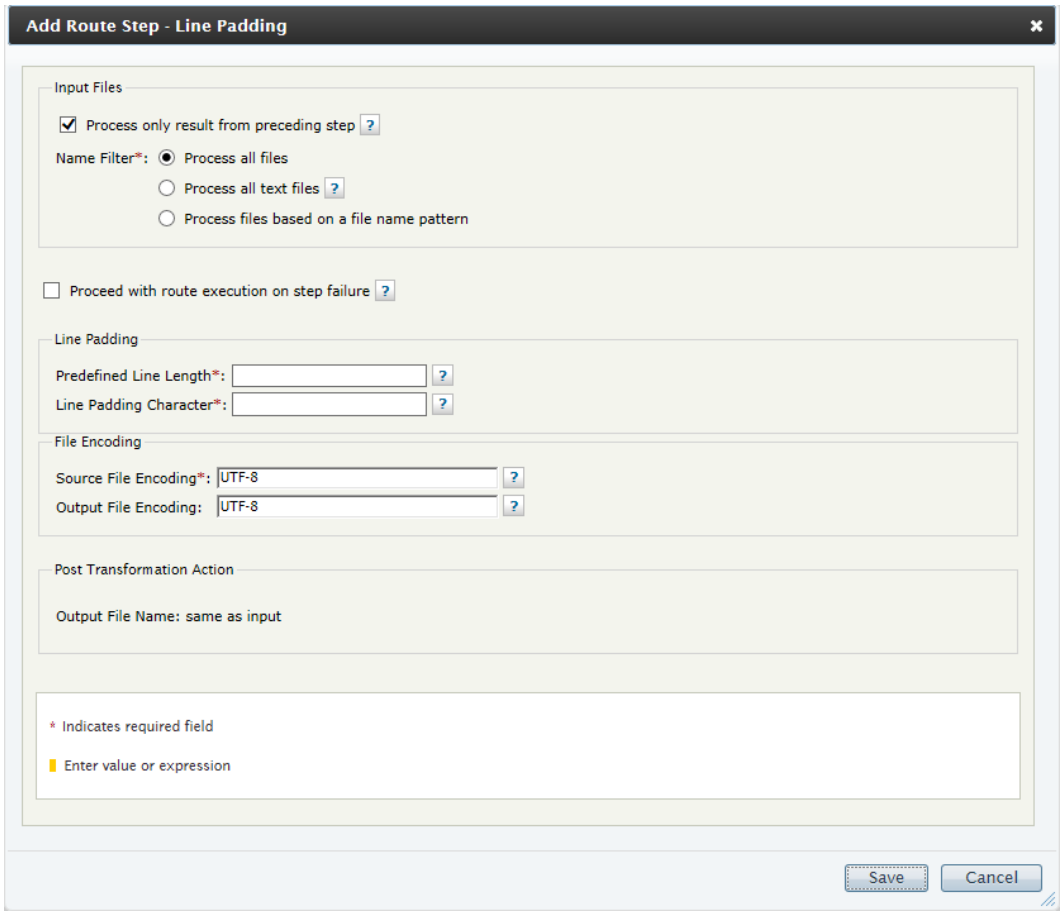
To add a Line Padding transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Determine line padding length.
4. Determine line padding character.
5. Select source file encoding.

6. Select output file encoding.
7. Determine post transformation actions.

Note Steps 1, 3, 4, and 5 are mandatory. All other steps are optional.

The following figure provides an example of a Line Padding transformation step.



The following topics provide detailed Line Padding transformation configuration information:

- *Input Files* on page 862
- *Proceed with route execution on step failure* on page 864
- *Line Padding* on page 864
- *File encoding* on page 864
- *Post transformation action* on page 865

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

Name filtering can either be set to process all files, process all text files, or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*.

If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed.

If *Process all text files* is selected, all text files forwarded by the selection of *Process only result from preceding step* are processed.

Text file selection is determined based on the file extension and the MIME type that corresponds to that extension. MIME types are defined in the `mime.types` configuration file located in:

Administrator's Tool > Server Configuration > Configuration Files

Furthermore, some MIME types can be defined as text by configuring the `AdvancedRouting.TextMimeSubtypes` server configuration option. For example, to configure the `application/xml` MIME type to be treated as text, add `xml` to the server configuration option.

If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression all files forwarded by the selection of *Process only result from preceding step* are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

```
*.[!0-9]
```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

```
.*\.(xml|txt)
```

- Case insensitive match of `data.xml` file.

```
(?i)data\.xml
```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Line Padding

Both the line padding length and line padding character must be configured.

Line padding length

The line padding length must be specified in number of characters. The maximum line padding length is 1024 characters.

Line padding character

The line padding character is specified in Unicode format with `\uXXXX` where `XXXX` is the hexadecimal representation of the characters. Only one character is accepted.

File encoding

The source file encoding must be configured. Configuring the output file encoding is not mandatory. If it is not set, the output file encoding will be the same as the source file encoding.

Source file encoding

Encoding of the file that will be transformed specified by the name of a SecureTransport supported character set. The **Source file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Output file encoding

Encoding of the file that will be produced specified by the name of a SecureTransport supported character set. The **Output file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Post transformation action

The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

Line Truncating

The Line Truncating transformation will truncate each line of input text file to a maximum length. The maximum length is specified in the transformation step settings. If a file line length is shorter than or equal to the configured maximum truncate length, then the line will be outputted to the result file without change. If a line length is longer than the configured maximum length "X" then only the first "X" number of characters will be outputted to the result file.

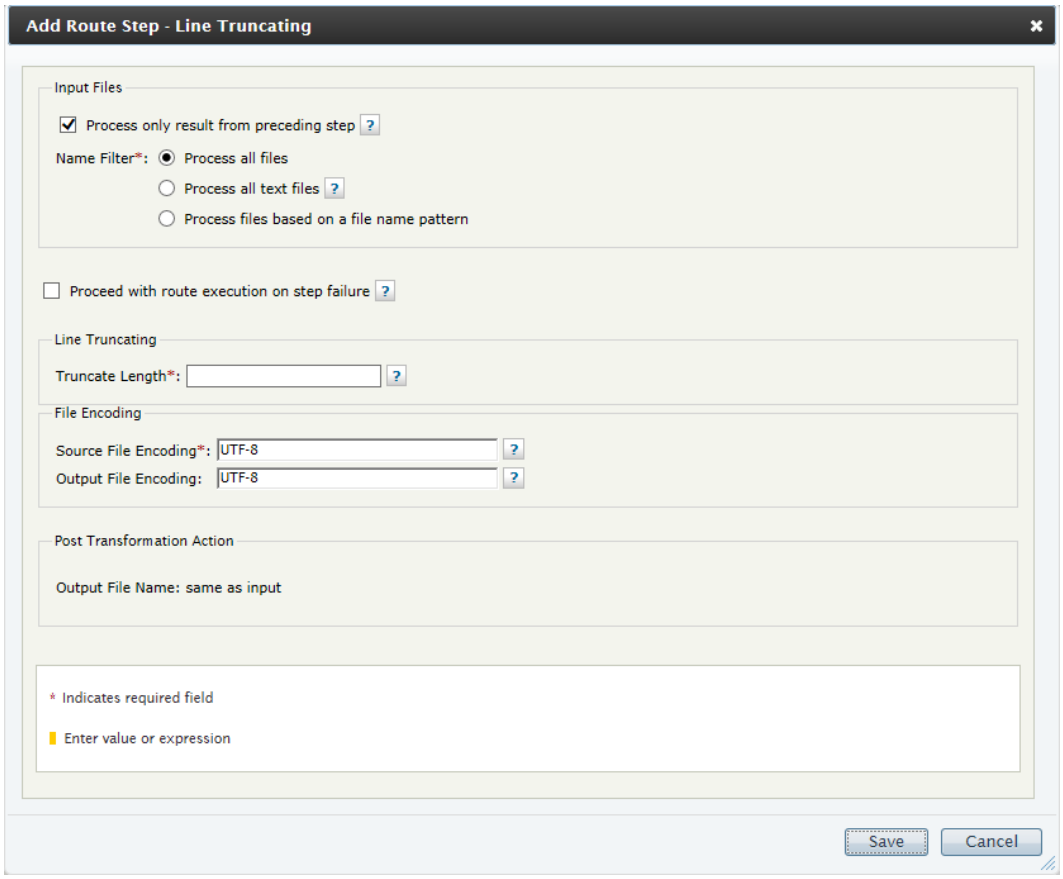
Note If the encoding a file is changed to IBM500, IBM037, or IBM424; the line ending of the input file should be LF and not CRLF. The CR is preserved in some cases and a new line appears between every original line. If the line ending is not LF, a Line Ending step can used before the Line Truncating step.

To add a Line Truncating transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Determine truncate length.
4. Select source file encoding.
5. Select output file encoding.
6. Determine post transformation actions.

Note Steps 1, 3, and 4 are mandatory. All other steps are optional.

The following figure provides an example of a Line Truncating transformation step.



The following topics provide configuration details for the Line Truncating transformation step:

- *Input Files* on page 866
- *Proceed with route execution on step failure* on page 868
- *Line truncating* on page 868
- *File encoding* on page 868
- *Post transformation action* on page 868

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

Name filtering can either be set to process all files, process all text files, or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*.

If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed.

If *Process all text files* is selected, all text files forwarded by the selection of *Process only result from preceding step* are processed.

Text file selection is determined based on the file extension and the MIME type that corresponds to that extension. MIME types are defined in the `mime.types` configuration file located in:

Administrator's Tool > Server Configuration > Configuration Files

Furthermore, some MIME types can be defined as text by configuring the `AdvancedRouting.TextMimeSubtypes` server configuration option. For example, to configure the `application/xml` MIME type to be treated as text, add `xml` to the server configuration option.

If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression all files forwarded by the selection of *Process only result from preceding step* are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

  ```
  *.[!0-9]
  ```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

```
.*\.(xml|txt)
```

- Case insensitive match of `data.xml` file.

```
(?i)data\.xml
```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Line truncating

The truncate length must be configured.

Truncate length

Maximum file line truncate length as specified in number of characters. The maximum number of characters is **TBD**.

File encoding

The source file encoding must be configured. Configuring the output file encoding is not mandatory. If it is not set, the output file encoding will be the same as the source file encoding.

Source file encoding

Encoding of the file that will be transformed specified by the name of a SecureTransport supported character set. The **Source file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Output file encoding

Encoding of the file that will be produced specified by the name of a SecureTransport supported character set. The **Output file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Post transformation action

The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

Line Folding

The Line Folding transformation will break file lines to a maximum width specified in number of characters. The maximum file width is specified in the transformation step settings. If a file line exceeds the maximum width, the extra characters will be moved to the next line. The moved extra characters are moved to a line of their own and not appended in front of the next line.

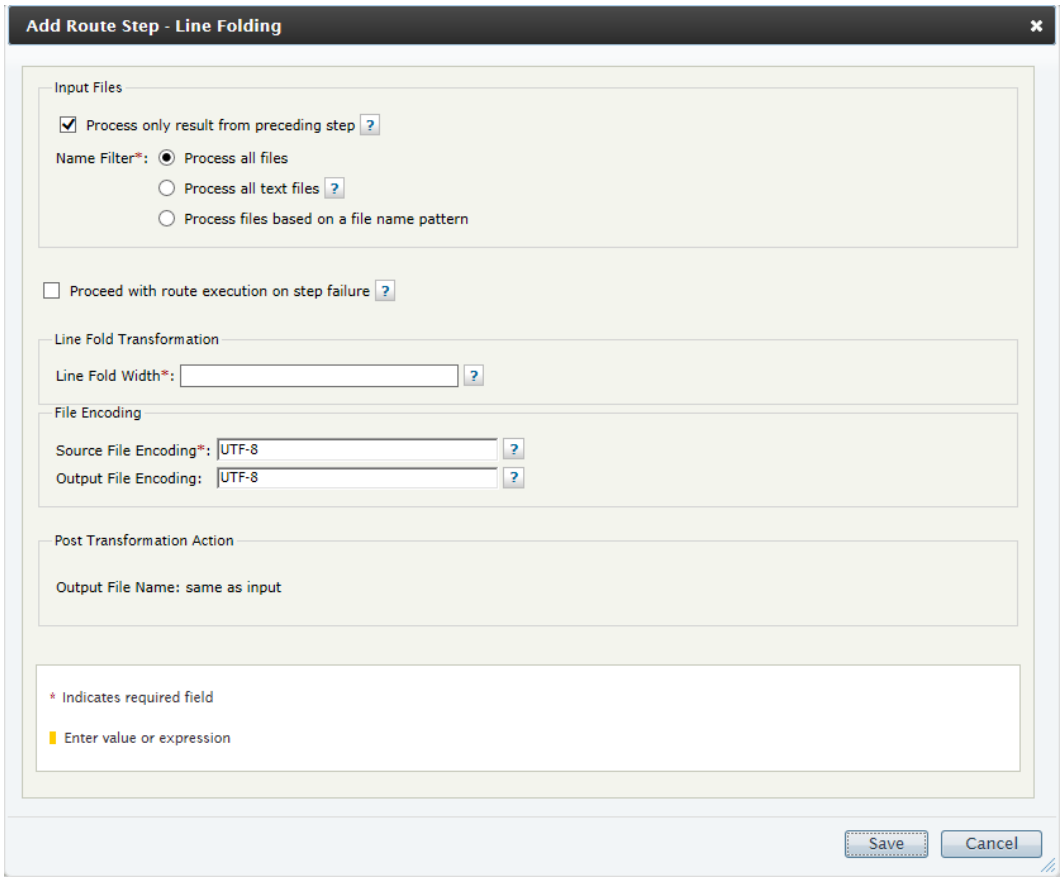
Note If the encoding a file is changed to IBM500, IBM037, or IBM424; the line ending of the input file should be LF and not CRLF. The CR is preserved in some cases and a new line appears between every original line. If the line ending is not LF, a Line Ending step can used before the Line Folding step.

To add a Line Folding transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Determine file fold width.
4. Select source file encoding.
5. Select output file encoding.
6. Determine post transformation actions.

Note Steps 1, 3, and 4 are mandatory. All other steps are optional.

The following figure provides an example of a Line Folding transformation step.



The following topics provide configuration details for the File Folding transformation step.:

- *Input Files* on page 870
- *Proceed with route execution on step failure* on page 872
- *File fold transformation* on page 872
- *File encoding* on page 872
- *Post transformation action* on page 872

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

Name filtering can either be set to process all files, process all text files, or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*.

If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed.

If *Process all text files* is selected, all text files forwarded by the selection of *Process only result from preceding step* are processed.

Text file selection is determined based on the file extension and the MIME type that corresponds to that extension. MIME types are defined in the `mime.types` configuration file located in:

Administrator's Tool > Server Configuration > Configuration Files

Furthermore, some MIME types can be defined as text by configuring the `AdvancedRouting.TextMimeSubtypes` server configuration option. For example, to configure the `application/xml` MIME type to be treated as text, add `xml` to the server configuration option.

If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression all files forwarded by the selection of *Process only result from preceding step* are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

  ```
  *.[!0-9]
  ```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

```
.*\.(xml|txt)
```

- Case insensitive match of `data.xml` file.

```
(?i)data\.xml
```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

File fold transformation

The file fold width must be configured.

File fold width

Maximum allowed file line width as specified in number of characters. The maximum number of characters is 1024.

File encoding

The source file encoding must be configured. Configuring the output file encoding is not mandatory. If it is not set, the output file encoding will be the same as the source file encoding.

Source file encoding

Encoding of the file that will be transformed specified by the name of a SecureTransport supported character set. The **Source file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Output file encoding

Encoding of the file that will be produced specified by the name of a SecureTransport supported character set. The **Output file encoding:** field has an auto-complete function that lists matching SecureTransport supported character sets.

Post transformation action

The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

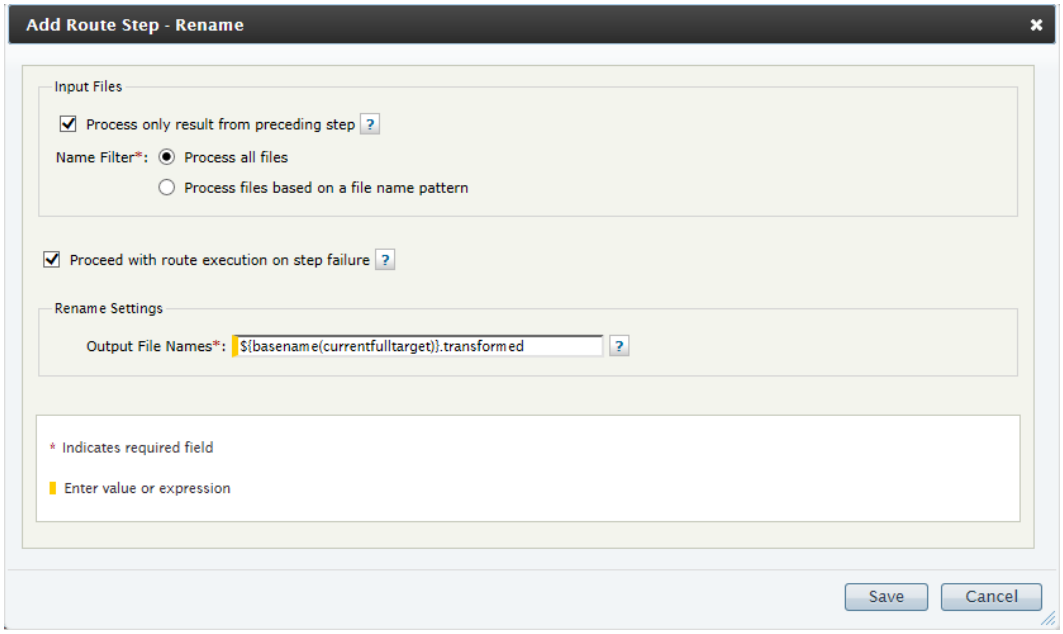
Rename

The Rename transformation step enables the renaming of a designated file or files as part of a route. To add a Rename transformation step to a Route Package Template take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Determine output file names.

Note Step 1 and 3 are mandatory. Step 2 is optional.

The following figure provides a configured example of a rename transformation step.



The following topics provide configuration details for the Rename transformation step:

- *Input Files* on page 873
- *Proceed with route execution on step failure* on page 875
- *Rename* on page 873

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

The Name Filter can either be set to process all files forwarded by the selection of *Process only result from preceding step* or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*. If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed. If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression pattern are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

  ```
  *.[!0-9]
  ```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

  ```
  .*\.(xml|txt)
  ```

- Case insensitive match of `data.xml` file.

  ```
  (?i)data\.xml
  ```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Rename settings

The rename settings determine the naming of the output file or files.

Output file names

The output file or files are renamed according to the expression entered in the *Output File Names* field. All input files are renamed based on the configured expression.

Examples:

- New filename based on the current filename:

  ```
  ${basename(currentfulltarget)}.transformed
  ```

- New filename bases on the original filename with a timestamp:

  ```
  ${basename(currentfulltarget)}.${timestamp}.${extension
  (currentfulltarget)}
  ```

The path of the new file (if any) will be stripped off and only the filename will be left.

Route steps

This topic includes detailed configuration information for the Publish To Account and Send To Partner route steps.

The purpose of routing steps is to move successfully transformed files out of the sandbox folder. It is highly recommended that each route terminates with at least one routing step (either Publish To Account or Send To Partner), otherwise the transformed file will not reach its destination and will be deleted when the route execution finishes.

The following topics provide detailed route step configuration information:

- *Publish To Account* on page 875
- *Send To Partner* on page 881

Publish To Account

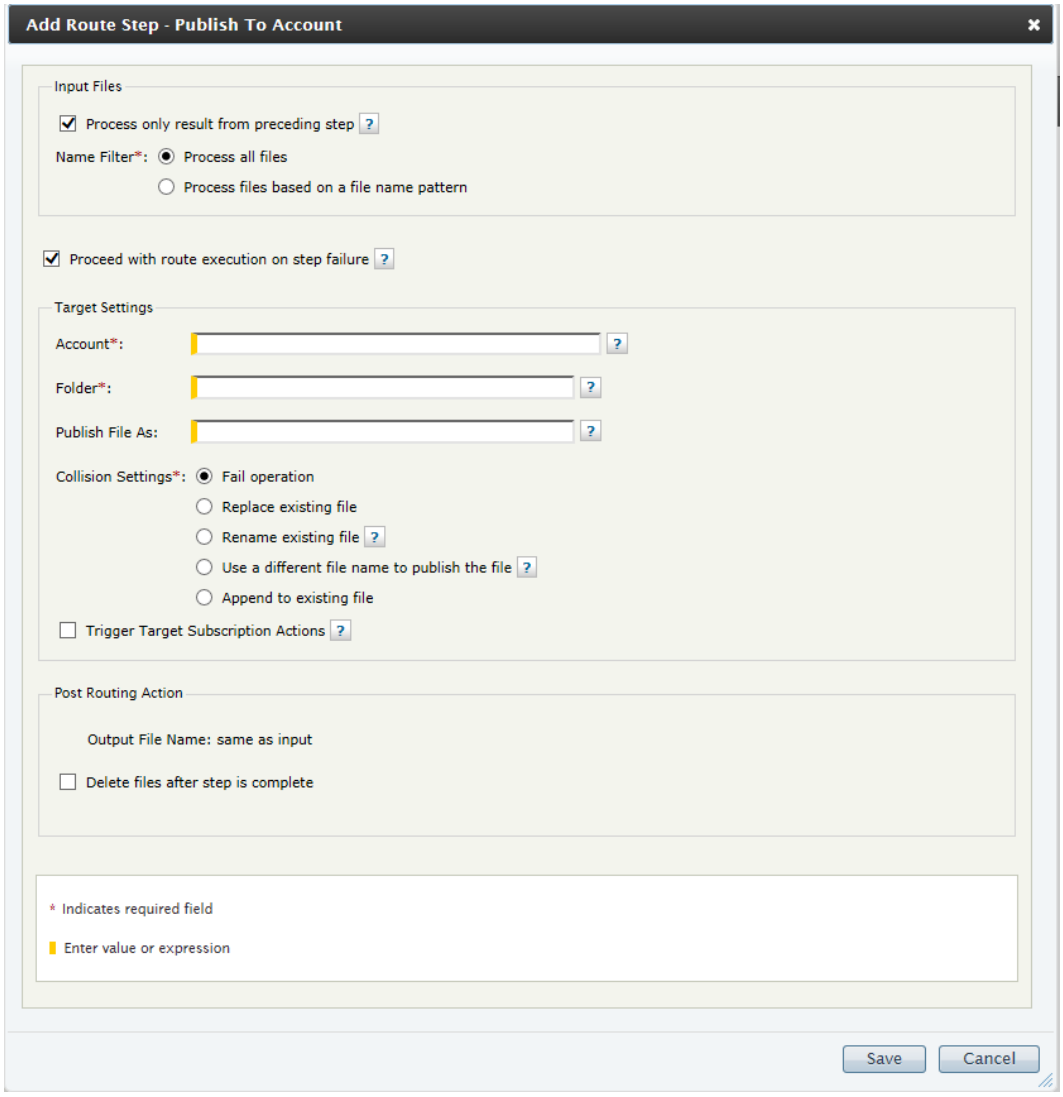
The Publish To Account routing step enables publishing files to a specified account as part of a route. To add Publish To Account to a Route Package Template or Route Package take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Enter and select the target settings.
4. Determine post routing actions.

Note Steps 1 and 3 are mandatory. All other steps are optional.

Note Publish To Account is used only to publish files to accounts which belong to the same SecureTransport Server. The administrator is not able to publish files to accounts managed by other products including other instances of SecureTransport Server. To avoid this restriction the administrator could use a Send To Partner routing step instead. For more information refer to *Send To Partner* on page 881.

The following figure provides an example of a Publish To Account routing step.



The following topics provide detailed Publish To Account route step configuration information:

- *Input Files* on page 877
- *Proceed with route execution on step failure* on page 878
- *Target Settings* on page 878
- *Post Routing Action* on page 880

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

The Name Filter can either be set to process all files forwarded by the selection of *Process only result from preceding step* or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*. If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed. If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression pattern are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

  ```
  *.[0-9]
  ```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

```
*.[!0-9]
```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

```
.*\.(xml|txt)
```

- Case insensitive match of `data.xml` file.

```
(?i)data\.xml
```

Proceed with route execution on step failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Target Settings

The target settings consists of selecting the account and the folder location to which to publish the designated files. The settings also include determining the name of the published file and selecting how to handle collisions.

Account

This is the account to publish the file(s) to. You can specify either an account name or use an EL expression to determine the recipient based on the environment information (such as filename). If no account with such name exists SecureTransport will try to match an account by its login name (either virtual or external user).

The *Account* field has auto-completion which shows a list of existing accounts containing the same search term.

Note Auto-completion will suggest account names and user (login) names.

Note Publish To Account could publish files only to internal (virtual, unlicensed or service) users or external ones using an existing account template.

Note In order to publish files to an external account (real, LDAP account, or SiteMinder), the administrator must specify the login name of this account (not the name of the account template which will be used).

Note You can access the first value of a given SSO attribute with name `attributeName` with the expression `${sso.attributes['attributeName'][0]}`.

Folder

This is the folder in the designated account to publish the file to. If the folder doesn't exist, it is automatically created. A folder name can be specified or an EL expression can be used to determine the folder based on the environment information. The folder name is a relative path to the home folder of the specified account.

Note A file will be successfully published to the specified folder only if the home folder of the designated account has a proper home folder access level. For more details see *User accounts* on page 453 and *Advanced Routing* on page 795.

Note You can access the first value of a given SSO attribute with name `attributeName` with the expression `${sso.attributes['attributeName'][0]}`.

Publish file as

This is the name of the published file. If this field is not empty, the file is published with the specified name. An EL script can also be used to specify a file name.

Examples:

- New file name based on the current filename (since the transformation might have change it):

  ```
  ${basename(currentfulltarget)}.sent
  ```

- New file name based on the original filename with a timestamp:

  ```
  ${basename(transfer.target)}.${timestamp}.${extension
  (transfer.target)}
  ```

- You can access the first value of a given SSO attribute with name `attributeName` with the expression `${sso.attributes['attributeName'][0]}`.

Note The path of the new file (if any) is stripped off and only the filename is left.

Collision settings

The collision setting determines the course of action to take in the event of duplicate file names. The possible collision settings are:

- Fail operation
- Replace existing file
- Rename existing file
- Use a different file name to publish the file
- Append to existing file

Replace existing file

With replace of existing file, there is a dedicated configuration option `AdvancedRouting.PublishToAccount.allowSelfOverwrite`. It allows (or disallows) the overwrite of files with the same name when source and destination is the same. Note that this option is available with Patch 48 and later.

Rename existing file

Renames the existing file with the following pattern:

If file name is `myFile.txt`, after renaming the file name is `myFile (old copy 1).txt`

If this file already exists, after renaming the file name is `myFile (old copy 2).txt`

Note If the file doesn't have an extension, the name transformation is the same but without the extension - `myFile (old copy 1).`

Use different file name to publish the file

Uses a different name to publish the file. The name is derived from the name specified in the *Publish file as* field as follows:

If file name is `myFile.txt`, after renaming the file name is `myFile (new copy 1).txt`

If this file already exists, after renaming the file name is `myFile (new copy 2).txt`

Note If the file doesn't have an extension, the name transformation is the same but without the extension - `myFile (new copy 1).`

Trigger target subscription actions

This option allows administrators to define the behavior if the target folder is a subscription or other special folder.

If it is unchecked (by default) - no further processing in the target folder is done.

If it is checked - the post processing actions defined in the target folder are executed.

Post Routing Action

If *Delete files after step is complete* is selected, the files processed by the route step are deleted.

Note The output file names will be the same as the input file names. To change the file names, use a Rename transformation step. See *Rename* on page 873.

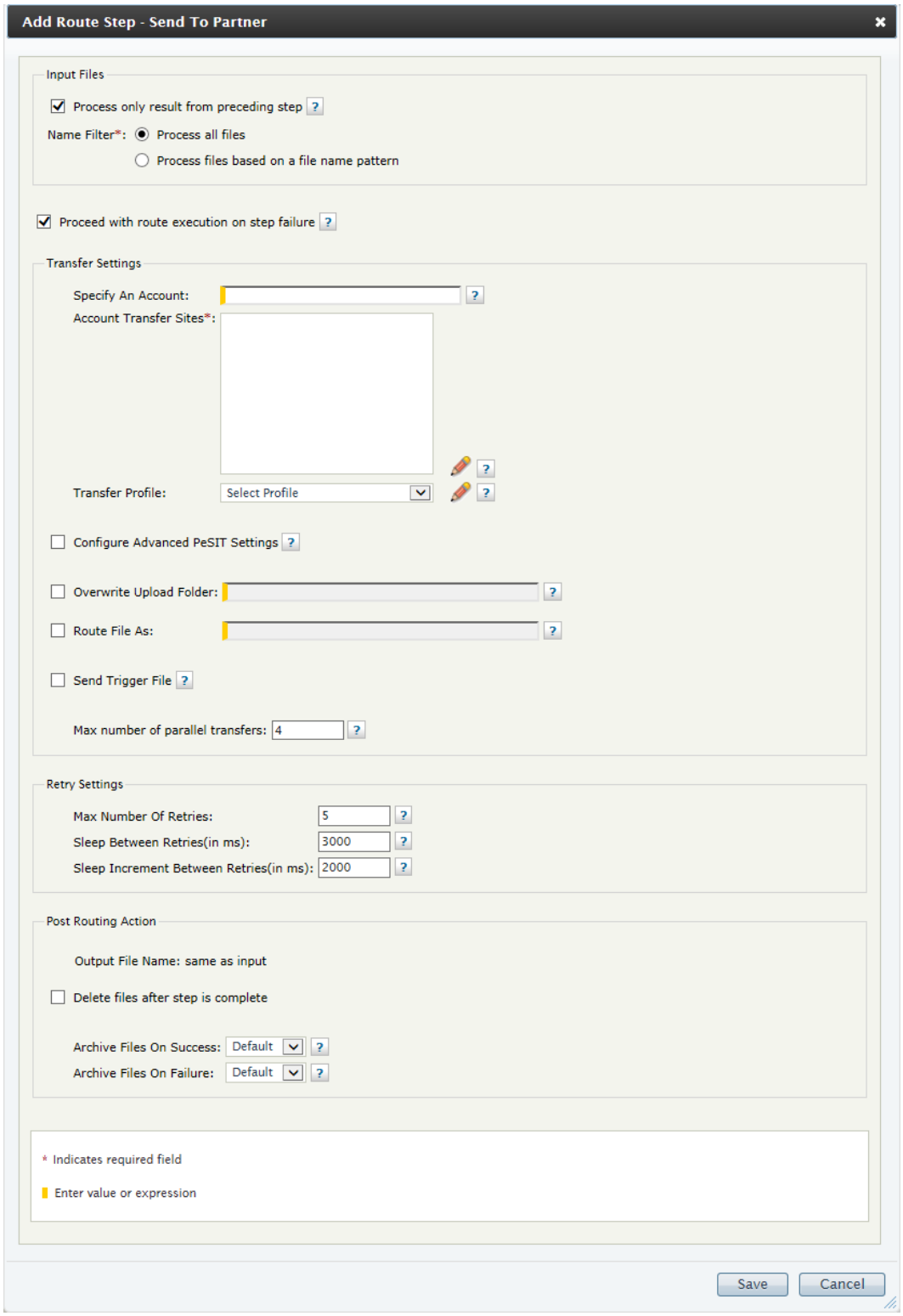
Send To Partner

The Send To Partner routing step enables routing to a specified partner account as part of a route. To add a Send To Partner routing step to a Route Package Template or Route Package take the following steps:

1. Designate file filtering.
2. Determine whether or not to proceed with route execution on step failure.
3. Configure transfer settings.
4. Configure retry settings.
5. Determine post routing actions.

Note Steps 1 and 3 are mandatory. All other steps are optional.

The following figure provides an example of a Send To Partner routing step.



The following topics provide detailed Send To Partner route step configuration information:

- *Input Files* on page 883
- *Proceed with route execution on failure* on page 884

- *Transfer Settings* on page 884
- *Configure advanced PeSIT settings* on page 885
- *Overwrite upload folder* on page 888
- *Route files as* on page 888
- *Send trigger file* on page 888
- *Retry settings* on page 891
- *Post Routing Action* on page 892

Input Files

The Input Files settings consist of the selection *Process only result from preceding step* and determining the Name Filter.

Process only result from preceding step

When *Process only result from preceding step* is **enabled** only files produced by the preceding step will be used as input for this step.

When *Process only result from preceding step* is **disabled** or this is the first step all current working files will be used as input for this step.

Note The Name Filter settings will also be applied on a given set of input files.

Name Filter

The Name Filter can either be set to process all files forwarded by the selection of *Process only result from preceding step* or process files based on a designated filename pattern forwarded by the selection of *Process only result from preceding step*. If *Process all files* is selected, all files forwarded by the selection of *Process only result from preceding step* are processed. If *Process files based on a filename pattern* is selected, only the files that match the file globbing or regular expression pattern are processed.

Filename patterns

Filename pattern matching supports `glob` and `regexp` syntax expressions.

When the designated pattern type is *File Globbing* then the `String` representation of the filename is matched using a limited pattern language that resembles regular expressions but with a simpler syntax. For example:

- Matches files ending in `.xml`.

  ```
  *.xml
  ```

- Matches file names starting with `foo.` that have a double character extension.

  ```
  foo.??
  ```

- Matches file names ending in `.1`, `.2`, `.3`, `.4`, `.5`, `.6`, `.7`, `.8`, `.9`, `.0`.

```
*.[0-9]
```

- Matches file names having a single character extension different from `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`.

```
*.[!0-9]
```

When the designated syntax is *Regular Expression* then the `String` representation of the filename is matched against a `Perl5.003` regular expressions. Perl5 extended regular expressions are also supported. For example:

- Matches files ending in `.xml` or `.txt`.

```
.*\.(xml|txt)
```

- Case insensitive match of `data.xml` file.

```
(?i)data\.xml
```

Proceed with route execution on failure

If *Proceed with route execution on step failure* is checked, the route execution continues even if the step execution fails.

Transfer Settings

The transfer setting consist of specifying an account, selecting account transfer sites, and selecting a transfer site profile.

Specify an account

The *Specify an account* field, is used to specify the account who holds the information (transfer site) about the recipient of the file. Either an account name, login name, or EL expression can be used to determine the recipient based on the environment information (such as filename).

The *Specify an account* field has auto-completion which shows a list of existing accounts containing the same search term.

Once an account is selected its transfer sites are populated in the select box. The population is possible only if the account name matches the login name of the user.

If an account name is unknown (for example, expression based) or the login name does not match the account name, its transfer sites are determined at runtime. Transfer sites can be expression based as well.

Account template names shouldn't be used in this field. The transfer sites which belong to the template will be populated but the step will fail. When using account templates, the value of this field should be the login name.

Note Auto-completion will suggest account names and user (login) names.

Note You can access the first value of a given SSO attribute with name `attributeName` with the expression `${sso.attributes['attributeName'][0]}`.

Account transfer sites

Transfer sites can either be existing transfer sites retrieved from the account selected or expression based ones.

To use an expression, click the edit icon ( ) next to the select box and enter the expression in field.

Expression for specifying the sites allows both EL and the wild card symbols - '*' and '?'.

Example:

If expression like `${account.name}-HTTP-*` is specified this would match all transfer sites (within the account selected) such as:

- `jsmith-HTTP-Partner1`
- `jsmith-HTTP-Partner2`
- `etc.`

Note Only transfer sites with proper access level will be listed. For more details see *Transfer sites* on page 494.

Transfer profile

Transfer profile property is used only if the transfer site is of type PeSIT. Otherwise, it is ignored.

When the transfer profile is specified by using an EL expression there are three possible cases:

1. EL expression does not match any account transfer profiles - the default transfer profile is used then.
2. EL expression matches more than one transfer profile - the default transfer profile is used.
3. EL expression matches exactly one transfer profile - the matched transfer profile is used.

The transfer profile can be selected from the listed ones or an EL expression can be used. To use an expression, click the edit icon ( ) next to the select menu and enter the expression in field.

Configure advanced PeSIT settings

If *Configure advanced PeSIT settings* is selected, the advanced PeSIT settings can be configured. The advanced PeSIT settings consist of selecting the store and forward mode, specifying the virtual file name and data encoding, and configuring the record length, file label, final destination, and user message.

Note PeSIT settings are only used for transfers over PeSIT.

Store and forward mode

The store and forward mode selections are:

- START_NEW
- PRESERVE

The *PRESERVE* store and forward mode preserves the current store and forward transfer (if any). The transfer will fail if the PeSIT transfer site is used for sending files that were received via a protocol other than PeSIT.

The *START_NEW* store and forward mode initiates a new store and forward transfer and the current transfer (if any) is acknowledged.

Virtual file name

The *Virtual file name* field is used to overwrite the virtual file name (PI12) predefined in the transfer profile. To preserve the predefined virtual file name, either leave the field empty or enter the EL expression `${pesit.file.filename}`.

This configuration parameter corresponds to the **IDF** parameter in Axway Transfer CFT.

Data encoding

Data encoding selections are:

- ASCII
- EBCDIC
- BINARY
- EBCDIC_NATIVE

The *Data encoding* field is used to overwrite the data encoding (PI16) predefined in the transfer profile.

To preserve the predefined data encoding, do not make a data encoding selection or use the EL expression `${pesit.pi.dataEncoding}`. To use the EL expression, click the Edit icon ( ) next to the select menu and enter the expression in field.

This configuration parameter corresponds to the **FCODE** parameter in Axway Transfer CFT.

Record format

Record format selections are:

- Variable
- Fixed

In *START_NEW* transfer mode, the **Record format** field is used to overwrite the record format (PI31) predefined in the transfer profile.

In *PRESERVE* transfer mode, the **Record format** field defines PI31. It can be an empty value, EL expression `${pesit.pi.recordFormat}`, or a numeric value. When the **Record format** field is empty and the file was originally received over PeSIT, the Record format (PI31) is preserved from the original file transfer. If file is received over a different protocol, the Record format (PI31) is preserved from the transfer profile.

This configuration parameter corresponds to the **FRECFM** parameter in Axway Transfer CFT.

Record length

In *START_NEW* transfer mode, the **Record length** field is used to overwrite the record format (PI32) predefined in the transfer profile.

In *PRESERVE* transfer mode, the **Record length** field defines PI32. It can be an empty value, EL expression `${pesit.pi.recordLength}`, or a numeric value. When the **Record length** field is empty and the file was originally received over PeSIT, the Record length (PI32) is preserved from the original file transfer. If file is received over a different protocol, the Record length (PI32) is preserved from the transfer profile.

This configuration parameter corresponds to the **FRECL** parameter in Axway Transfer CFT.

File label

The *File label* field is used to overwrite the file label (PI37) predefined in the transfer profile.

To preserve the predefined file label, either leave the field empty or enter the EL expression `${pesit.pi.fileLabel}` in the field.

This configuration parameter corresponds to the **NFNAME** parameter in Axway Transfer CFT.

Originator

The *Originator* field is used to overwrite the original sender (PI61) of the transfer.

To preserve the originator of the previous transfer, enter the EL expression `${pesit.pi.originalSenderID}`. in the field.

To make a Store and Forward PeSIT transfer specify the originator and choose the intermediate partner (**IPART** parameter in Axway Transfer CFT) in the transfer site list.

Note Originator can only be changed when Store and Forward mode is set to `START_NEW`.

Final Destination

The *Final Destination* field is used to overwrite the final destination (PI62) of the transfer.

To preserve the final destination of the previous transfer, enter the EL expression `${pesit.pi.finalDestinationID}` in the field.

To make a Store and Forward PeSIT transfer specify the final destination and choose the intermediate partner (**IPART** parameter in Axway Transfer CFT) in the transfer site list.

Note Final destination can only be changed when Store and Forward mode is set to `START_NEW`.

User message

The *User message* field is used to overwrite the predefined user message (PI99) in the PeSIT transfer site. To preserve the predefined user message, either leave the field empty or enter the EL expression `${pesit.pi.serviceParam}` in the field.

This configuration parameter corresponds to the **PARM** parameter in Axway Transfer CFT.

Overwrite upload folder

If Overwrite upload folder is selected, the value specified is used to overwrite the upload folder configured in the transfer site settings (if allowed in the transfer site).

Note The upload folder must be created on the target file system. Otherwise, the sending of the trigger file could fail.

Note The upload folder of a custom Pluggable Transfer Site cannot be overwritten.

An EL expression can be used to specify the new upload folder.

Example: You can access the first value of a given SSO attribute with name `attributeName` with the expression `${sso.attributes['attributeName'][0]}`.

Route files as

If *Route files as* is selected, the entry in the field overwrites *Send File As* property which is set in the transfer site. An EL expression can be used to specify a route files as name.

Examples:

- New file name based on the current filename (since the transformation might have changed it):

  ```
  ${basename(currentfulltarget)}.sent
  ```

- New file name based on the original filename with a timestamp:

  ```
  ${basename(transfer.target)}.${timestamp}.${extension
  (transfer.target)}
  ```

Note You can access the first value of a given SSO attribute with name `attributeName` with the expression `${sso.attributes['attributeName'][0]}`.

Note The path of the new file (if any) is stripped off and only the filename is left.

Send trigger file

If *Send trigger file* is selected, a designated trigger file is sent to the transfer site after successful routing of files. To designate the trigger file, name the trigger file, determine whether or not to send a trigger file for each transferred file, and create the trigger file content. To complete the configuration

of the trigger file, select the trigger file destinations by specifying a destination account, selecting account transfer sites, selecting the transfer profile (if applicable), and determining whether or not to overwrite the upload folder.

Note The trigger file is created after the successful transfer of a file or files. The trigger file exists only in the sandbox folder. The trigger file is deleted right after it was successfully transferred to the trigger destination or destinations.

Note The *Max number of parallel transfers* and *Retry settings* are applied for both the data file and the trigger file.

Trigger file name

The *Trigger file name* field is used to name the trigger file to be sent to the transfer site after the successful routing of file(s). EL expressions are supported.

Examples:

- New file name based on the current filename (since the transformation might have changed it):

  ```
  ${basename(currentfulltarget)}.sent
  ```

- New file name based on the original filename with a timestamp:

  ```
  ${basename(transfer.target)}.${timestamp}.${extension
  (transfer.target)}
  ```

- You can access the first value of a given SSO attribute with the name `attributeName` with the expression `${sso.attributes['attributeName'][0]}`.

Note Send File as option, in the site used to send the trigger file, is ignored and the name of the trigger file remains unchanged. Though, other Post Transmission Settings, if any, are applied over the name of the trigger file.

Send trigger file for each transferred file

If *Send trigger file for each transferred file* is selected, a trigger file is sent after each successful routing of a data file to the transfer site. If this option is not selected, one trigger file is sent after all transformed files are successfully routed to the transfer site.

Note If *Send trigger file for each transferred file* is not selected and the sending of one or more of the transformed files fails, the trigger file is not sent even though most of the files were successfully transferred.

Trigger file content

The *Trigger file content* field is used to specify the content of the trigger file. EL expressions are supported.

If the content is not specified an empty (zero byte) trigger file is sent.

`\n\r` (CRLF) is used as a line separator for the content of the trigger file.

Trigger files destinations

To specify a trigger file destinations, specify the destination account, select account transfer sites and transfer profile (if applicable), and determine whether or not to overwrite the upload folder.

Specify an account

The Specify an account field, is used to specify the account who holds information (transfer site) about the trigger destination. Either an account name, login name, or EL expression can be used to determine the recipient based on the environment information (such as filename).

The *Specify an account* field has auto-completion which shows a list of existing accounts containing the same search term.

Once an account is selected its transfer sites are populated in the select box. The population is only possible if the account name matches the login name of the user.

If an account name is unknown (for example, expression based) or the login name does not match the account name, its transfer sites are determined at runtime. Transfer sites can be expression based as well.

Account template names should not be used in this field. The transfer sites which belong to the template will be populated but the step will fail. When using account templates, the value of this field should be the login name.

Note Auto-completion will suggest account names and user (login) names.

Account transfer sites

Transfer sites can either be existing transfer sites retrieved from the account selected or expression based ones.

To use an expression, click the Edit icon ( ) next to the select box and enter the expression in field.

Expression for specifying the sites allows both EL and the wild card symbols - '*' and '?'.

Example:

If expression like `${account.name}-HTTP-*` is specified this would match all transfer sites (within the account selected) such as:

- `jsmith-HTTP-Partner1`
- `jsmith-HTTP-Partner2`
- `etc.`

Note Only transfer sites with proper access level will be listed. For more details see *Transfer sites* on page 494.

Transfer profile

Transfer profile property is used only if the transfer site is of type PeSIT. Otherwise, it is ignored.

When the transfer profile is specified by using an EL expression there are three possible cases:

1. EL expression does not match any account transfer profiles - the default transfer profile is used then.
2. EL expression matches more than one transfer profile - the default transfer profile is used.
3. EL expression matches exactly one transfer profile - the matched transfer profile is used.

The transfer profile can be selected from the listed ones or an EL expression can be used. To use an expression, click the Edit icon ( ) next to the select menu and enter the expression in field.

Overwrite upload folder

If Overwrite upload folder is selected, the specified value is used to overwrite the upload folder configured in the transfer site settings (if allowed in the transfer site).

An EL expression can be used to specify the new upload folder.

Note The upload folder must be created on the target file system. Otherwise, the sending of the trigger file could fail.

Max number of parallel transfers

The entry in the *Max number of parallel transfers* field determines the maximum number of parallel transfers for each route used for both the data file and trigger file, if configured. The default number of maximum parallel transfers is 4 which means you cannot have more than 4 concurrent transfer connections at a time. Note that files are processed one by one but are published in bulk to the configured transfer sites.

No retries are triggered if the reason for the failure is permanent (for example, the wrong credentials are specified in the transfer site being used).

The following topics provide instructions and descriptions for managing transfer sites that can have alternate endpoints:

- *Transfer site properties* on page 495 - Describes transfer site properties.
- *AS2 transfer sites* on page 497 - Describes AS2 transfer site configuration.
- *FTP(S) transfer sites* on page 515 - Describes FTP(S) transfer site configuration.
- *HTTP(S) transfer sites* on page 552 - Describes HTTP(S) transfer site configuration.
- *PeSIT transfer sites* on page 559 - Describes PeSIT transfer site configuration.
- *SSH transfer sites* on page 579 - Describes SSH transfer site configuration.

Retry settings

The retry settings allow you to configure the maximum number of retries, the sleep time between retries (a static delay), and the sleep increment between retries (an incremental delay). Those settings are used for both the data file and trigger file, if configured.

Note If your Send To Partner step uses Transfer Sites that have alternative endpoints configured, the Retry settings apply in accordance with the retry policy as set in the `TransferSite.AlternativeAddresses.retryPolicy` configuration option. This server configuration can have either of the following values:

- `Disabled` (default) – this is the default retry policy and it applies globally to all Transfer sites. This configuration prevents you from configuring alternative endpoints to Transfer sites.
- `AllHostsOnEachRetry` – with this policy SecureTransport iterates through each endpoint, one by one, starting with the first one in the list. If connection not successful, SecureTransport will continue trying each endpoint one after another until the maximum number of retries is reached. You can configure alternative endpoints only for AS2, HTTP(S), FTP(S), SSH and PeSIT transfer sites.
- `OneHostOnEachRetry` – with this policy SecureTransport tries to connect to the first endpoint in the list. If connection not successful, SecureTransport will continue trying that endpoint until the maximum number of retries is reached; and then will move to the next one in the list. Following that same pattern, SecureTransport will try each endpoint until success; or until end of list. You can configure alternative endpoints only for AS2, HTTP(S), FTP(S), SSH and PeSIT transfer sites.

Max number of retries

Enter an integer number to define the countdown value of the *Max Number of Retries* of failed transfers (5 by default). Entering the retry flow occurs only in the case of a transfer fail.

Sleep between retries

Enter an integer number to define the *Sleep Between Retries* to add a delay (in milliseconds) between consecutive retries (3000 milliseconds by default).

Sleep increment between retries

Enter an integer number to define the *Sleep Increment Between Retries* to add an incremental delay (in milliseconds) between retries (2000 milliseconds by default). Being incremental, this delay grows with each next retry, so use with caution.

Post Routing Action

The post routing action selections determine what actions occur once the route step is completed. The post routing actions include deleting and archiving files.

Note Post routing actions are not performed over the trigger file, since this file has already been deleted except when File Archiving is enabled. When File Archiving is enabled, the trigger file will be archived as a normal file. For information on the global configuration of File Archiving (including enabling File Archiving), refer to *File archiving global configuration* on page 213.

Note The post routing actions are executed in the sandbox folder only.

Note Post routing actions are executed for successfully transferred data files only. If the transfer fails (permanently or reaches its maximum number of retries), post routing actions are not executed except when File Archiving is enabled. When File Archiving is enabled, the selected *Archive Files On Failure* action will occur. For information on the global configuration of File Archiving (including enabling File Archiving), refer to *File archiving global configuration* on page 213.

Note The output file names will be the same as the input file names. To change the file names use a Rename transformation step. To configure a Rename transformation step, refer to *Rename* on page 873.

Delete files after step is complete

If *Delete files after step is complete* is selected, the files processed by the route step are deleted.

Archive files on success

The *Archive Files On Success* selection determines how the files are backed up in the configured archive folder if the step execution succeeds.

- If **Default** is selected, the files will archive the files based on the account configuration.
- If **Enable** is selected, the files will always be archived.
- If **Disable** is selected, the files will not be archived.

Note The *Archive Files On Success* selection will only be visible if File Archiving is enabled. For information on the global configuration of File Archiving (including enabling File Archiving), refer to *File archiving global configuration* on page 213.

Note In order for the administrator to be able to resubmit successful outbound transfers initiated by the Send To Partner step, you must have the *Archive Files On Success* set to enabled.

Archive files on failure

The *Archive Files On Failure* selection determines how the files are backed up in the configured archive folder if the step execution fails.

- If **Default** is selected, the files will archive the files based on the account configuration.
- If **Enable** is selected, the files will always be archived.
- If **Disable** is selected, the files will not be archived.

Note The *Archive Files On Failure* selection will only be visible if File Archiving is enabled. For information on the global configuration of File Archiving (including enabling File Archiving), refer to *File archiving global configuration* on page 213.

Note In order for the administrator to be able to resubmit failed outbound transfers initiated by the Send To Partner step, you must have the *Archive Files On Success* set to enabled.

Operation

This topic describes basic and complex use cases. Use cases provide customer oriented examples of Advanced Routing configurations.

The following basic use cases are described:

- PGP Decryption and Publish To Account
- Line Ending and Publish To Account
- Send To Partner
- Compress and Send To Partner
- Decompress and Publish To Account
- External Script and Send To Partner
- Send To Partner (PeSIT)

The advanced use cases are described:

- Route files based on file name extension
- PGP Decryption, PGP Encryption (partner's certificate), and send to multiple partners
- Decompress and Send to Partner (Trigger File Output)

The following topics describes the basic and advanced use cases:

- *Basic use cases* on page 894
- *Advanced use cases* on page 908

Basic use cases

An overview, prerequisites, flow configuration steps, and flow of events of the following basic use cases are provided:

- *PGP Decryption and Publish To Account* on page 895 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the PGP Decryption and Publish To Account use case.
- *Line Ending and Publish To Account* on page 896 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the Line Ending and Publish To Account use case.
- *PGP Encryption and Send To Partner* on page 898 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the PGP Encryption and Send To Partner use case.
- *Compress and Send To Partner* on page 900 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the Compress and Send To Partner use case.
- *Decompress and Publish To Account* on page 902 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the Decompress and Publish To Account use case.
- *External Script and Publish To Account* on page 903 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the External Script and Publish To Account use case.

- *Send To Partner (PeSIT)* on page 906 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the Send To Partner (PeSIT) use case.

PGP Decryption and Publish To Account

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the PGP Decryption and Publish To Account use case:

- *Overview* on page 895
- *Prerequisites* on page 895
- *Steps to configure the flow* on page 895
- *Flow of events* on page 896

Overview

PGP decrypt each incoming file and publish the files to the local account.

Prerequisites

- Create a Route Package Template. For instructions on creating a Route Package Template, refer to *Add Route Package Template* on page 807.
- Create an Advanced Routing application instance. For instructions on creating an Advanced Routing application instance, refer to *Create Advanced Routing application instance* on page 1.
- Create an user account in SecureTransport. For instructions on creating an user account, refer to *User accounts* on page 453.
- Generate or import a private PGP key which is used for decryption. For instructions on generating or importing a private PGP key, refer to *Generate a PGP private certificate* on page 492or *Import an X509 or PGP private certificate* on page 492.

Steps to configure the flow

1. Create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.
    a. Configure the subscription folder.
    b. (Optional) configure the rest of the settings.
    c. Click **Add** when done.
2. Navigate to the *Routes* tab of the created account and assign a new route package to the account by choosing the created Route Package Template and clicking the **Assign Route** button. For assigning a route configuration details, refer to *Assign Route Package Template* on page 818.
3. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 1.

4. Create a new route by clicking the **New Route** button in the *Specific Settings* pane. For route configuration details, refer to *New Route* on page 812.
    a. Configure the new route's name and (optionally) description.
    b. Add and configure a PGP Decryption step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For PGP Decryption configuration details, refer to *PGP Decryption* on page 835.
        i. (Optional) Enable **Require Encryption** and/or **Require Trusted Signature**.
        ii. Click **Save** when done.

        Note The PGP Decryption step automatically detects the PGP private key for decrypting the content. The step only searches in the account key store.

    c. Add and configure a Publish to Account step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For Publish To Account configuration details, refer to *Publish To Account* on page 875.
        i. Uncheck **Proceed with route execution on step failure**.
        ii. Select an account to publish to (for example, the current account).
        iii. Select a folder to publish the file to (for example, the subscription folder configured in Step 1).
        iv. (Optional) Configure the rest of the settings.
        v. Click **Save** when done.
5. Save the route and the route package.

Flow of events

1. A PGP encrypted file is uploaded via any protocol to the Advanced Routing subscription folder.
2. The Advanced Routing application triggers the route.
3. The uploaded file is decrypted and published to the specified folder.

Note Upon completion of the route there will be two files present – the PGP encrypted (original) file and the PGP decrypted file. To automatically remove the PGP encrypted file, select **Post Processing Action > On Success > Delete** in the subscription settings.

Note Publishing the PGP decrypted file in Advanced Routing subscription folder does not trigger the route execution once again, because *Trigger target subscription actions* is **unchecked**.

Line Ending and Publish To Account

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the Line Ending and Publish To Account use case:

- *Overview* on page 897
- *Prerequisites* on page 897

- *Step to configure the flow* on page 897
- *Flow of events* on page 898

Overview

Transform end-of-line characters of each incoming file and publish the file to the local account.

Prerequisites

- Create a Route Package Template. For Route Package Template creation details, refer to *Add Route Package Template* on page 807.
- Create an Advanced Routing application instance. For Advanced Routing application instance creation details, refer to *Create Advanced Routing application* on page 805.
- Create a SecureTransport user account. For user account creation details, refer to *User accounts* on page 453.

Step to configure the flow

1. Create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.
    a. Configure the subscription folder.
    b. (Optional) Configure the rest of the settings.
    c. Click **Add** when done.
2. Navigate to the *Routes* tab of the created account and assign a new route package to the account by choosing the created Route Package Template and clicking the **Assign Route** button. For assigning a route configuration details, refer to *Assign Route Package Template* on page 818.
3. Assign the subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 1.
4. Create a new route by clicking the **New Route** button in the *Specific Settings* pane. For route configuration details, refer to *New Route* on page 812.
    a. Configure the new route's name and (optionally) description.
    b. Add and configure a Line Ending step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For Line Ending configuration details, refer to *Line Ending* on page 846.
        i. Select the source line ending format (for example, **Custom -> \u0025** for Mainframe end-of-line characters).
        ii. Select source file encoding (for example, **X-ORACLE-WE8EBCDIC500**).
        iii. Select target line ending format (for example, **Linux(LF)**).

iv. Select target file encoding (for example, **US-ASCII**).

v. (Optional) Configure the rest of the options.

vi. Click **Save** when done.

c. Add and configure a Publish to Account step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For Publish To Account configuration details, refer to *Publish To Account* on page 875.

i. Uncheck **Proceed with route execution on step failure**.

ii. Select an account to publish to (for example, the current account).

iii. Select a folder to publish the file to (for example, the subscription folder configured in Step 1).

iv. Enter the following expression in the *Publish file as* field:

```
${basename(transfer.target)}.us-ascii${extension
(transfer.target)}
```

This expression transforms the original file name by adding `.us-ascii` before the filename extension. For example, for file `incoming.txt` the result is `incoming.us-ascii.txt`.

v. (Optional) Configure the rest of the settings.

vi. Click **Save** when done.

5. Save the route and the route package.

Flow of events

1. A file with **\u0025** end-of-line character and **WE8EBCDIC500** file encoding is uploaded via any protocol to the Advanced Routing subscription folder.
2. The Advanced Routing application triggers the route.
3. The uploaded file's end-of-line character is changed to **LF** and the file's encoding is changed to **US-ASCII**.

Note In the end there are two files present – the incoming (original) file and transformed file. To automatically remove the incoming file, select **Post Processing Action -> On Success -> Delete** in the subscription settings.

Note Publishing the transcoded file in Advanced Routing subscription folder does not trigger the route execution once again, because *Trigger target subscription actions* is **unchecked**.

PGP Encryption and Send To Partner

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the PGP Encryption and Send To Partner use case:

- *Overview* on page 899
- *Prerequisites* on page 899

- *Step to configure the flow* on page 899
- *Flow of events* on page 900

Overview

PGP encrypt each incoming file and route the file to a remote transfer site.

Prerequisites

- Create a Route Package Template. For Route Package Template creation details, refer to *Add Route Package Template* on page 807.
- Create an Advanced Routing application instance. For Advanced Routing application instance creation details, refer to *Create Advanced Routing application* on page 805.
- Create SecureTransport user account. For user account creation details, refer to *User accounts* on page 453.
- Create a remote transfer site. For remote transfer site creation details, refer to *Create a transfer site* on page 598.
- Generate or import a Partner PGP key which is used for encryption. For instructions on generating or importing a partner PGP key, refer to *Generate a partner PGP key* on page 477or *Import a partner PGP key* on page 479.

Step to configure the flow

1. Create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.
    a. Configure the subscription folder.
    b. (Optional) Configure the rest of the settings.
    c. Click **Add** when done.
2. Navigate to the *Routes* menu of the created account and assign a new route package to the account by choosing the created Route Package Template and clicking the **Assign Route** button. For assigning a route configuration details, refer to *Assign Route Package Template* on page 818.
3. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 1.
4. Create a new route by clicking the **New Route** button in the *Specific Settings* pane. For route configuration details, refer to *New Route* on page 812.
    a. Configure the new route's name and (optionally) description.
    b. Add and configure a PGP Encryption step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For PGP Encryption configuration details, refer to *PGP Encryption* on page 829.

i. Select the **Encrypt only** option.

ii. Configure an account from which to select PGP certificate for encryption (for example, the current account).

iii. Select a PGP certificate for encryption from that account. PGP certificate can be specified by alias, EL or wild card symbols. If more that one certificate matches the pattern, the first one is used.

iv. Click **Save** when done.

a. Add and configure a Send To Partner step by selecting it from the *-- Select Step --* drop-down menu and clicking the **Add Step** button. For Send To Partner configuration details, refer to *Send To Partner* on page 881.

i. Uncheck **Proceed with route execution on step failure**.

ii. Select the account which contains the target transfer site (or select **Use current account**).

iii. Select the transfer site from the selected account to send the file to.

iv. Click **Save** when done.

5. Save the route and the route package.

Flow of events

1. A file is uploaded via any protocol to the Advanced Routing subscription folder.
2. The Advanced Routing application triggers route.
3. The uploaded file is encrypted and sent to the remote transfer site.

Compress and Send To Partner

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the Compress and Send To Partner use case:

- *Overview* on page 900
- *Prerequisites* on page 900
- *Steps to configure the flow* on page 901
- *Flow of events* on page 902

Overview

Compress multiple incoming files and route the archive to a remote transfer site.

Prerequisites

- Create a Route Package Template. For Route Package Template creation details, refer to *Add Route Package Template* on page 807.

- Create an Advanced Routing application instance. For Advanced Routing application instance creation details, refer to *Create Advanced Routing application* on page 805.
- Create a SecureTransport user account. For user account creation details, refer to *User accounts* on page 453.
- Create a remote transfer site. For remote transfer site creation details, refer to *Create a transfer site* on page 598.

Steps to configure the flow

1. Create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.
    a. Configure the subscription folder.
    b. To await multiple files, configure a condition (for example, trigger file) on which to submit the files to the route.
    c. (Optional) Configure the rest of the settings.
    d. Click **Add** when done.
2. Navigate to the *Routes* tab of the created account and assign a new route package to the account by choosing the created Route Package Template and clicking the **Assign Route** button. For assigning a route configuration details, refer to *Assign Route Package Template* on page 818.
3. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 1.
4. Create a new route by clicking the **New Route** button in the *Specific Settings* pane. For route configuration details, refer to *New Route* on page 812.
    a. Configure the new route's name and (optionally) description.
    b. Add and configure a Compress step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For Compress configuration details, refer to *Compress* on page 838.
        i. Choose name for the archive (for example, `archive-${timestamp}.zip`).
        ii. (Optional) Configure the rest of the settings.
        iii. Click **Save** when done.
    c. Add and configure a Send To Partner step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For Send To Partner configuration details, refer to *Send To Partner* on page 881.
        i. Uncheck **Proceed with route execution on step failure**.
        ii. Select the account which contains the target transfer site (or select **Use current account**).
        iii. Select the transfer site from the selected account to send the file to.
        iv. Click **Save** when done.

5. Save the route and the route package.

Flow of events

1. Multiple files are uploaded via any protocol to the Advanced Routing subscription folder.
2. The trigger file (file with `.trigger` extension) is uploaded to the subscription folder.
3. The Advanced Routing application triggers the route.
4. The uploaded files are compressed into single zip archive and sent to the remote transfer site.

Decompress and Publish To Account

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the Decompress and Publish To Account use case:

- *Overview* on page 902
- *Prerequisites* on page 902
- *Steps to configure the flow* on page 902
- *Flow of events* on page 903

Overview

Decompress incoming archives and publish the result files to the local account.

Prerequisites

- Create a Route Package Template. For instructions on creating a Route Package Template, refer to *Add Route Package Template* on page 807.
- Create an Advanced Routing application instance. For instructions on creating an Advanced Routing application instance, refer to *Create Advanced Routing application instance* on page 1.
- Create a SecureTransport user account. For instructions on creating an user account, refer to *User accounts* on page 453.

Steps to configure the flow

1. Create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.
    a. Configure the subscription folder.
    b. (Optional) Configure the rest of the settings.
    c. Click **Add** when done.

2. Navigate to the *Routes* tab of the created account and assign a new route package to the account by choosing the created Route Package Template and clicking the **Assign Route** button. For assigning a route configuration details, refer to *Assign Route Package Template* on page 818.
3. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 1.
4. Create a new route by clicking the **New Route** button in the *Specific Settings* pane. For route configuration details, refer to *New Route* on page 812.
    a. Configure the new route's name and (optionally) description.
    b. Add and configure a Decompress step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For Decompress configuration details, refer to *Decompress* on page 842.
        i. (Optional) Configure the available options.
        ii. Click **Save** when done.

            Note The Decompress step automatically detects the archive type.

    c. Add and configure a Publish to Account step by selecting it from the -- *Select Step* --drop-down menu and clicking the **Add Step** button. For Publish To Account configuration details, refer to *Publish To Account* on page 875.
        i. Uncheck **Proceed with route execution on step failure**.
        ii. Select an account to publish to (for example, the current account).
        iii. Select a folder to publish the file to (for example, the subscription folder configured in Step 1).
        iv. (Optional) Configure the rest of the settings.
        v. Click **Save** when done.
5. Save the route and the route package.

Flow of events

1. An archive is uploaded via any protocol to the Advanced Routing subscription folder.
2. The Advanced Routing application triggers the route.
3. The uploaded archive is decompressed and published to the specified folder.

Note In the end the subscription folder contains the archive file and the decompressed files. To automatically remove the archive file, select **Post Processing Action > On Success > Delete** in the subscription settings.

Note Publishing the decompressed files in Advanced Routing subscription folder does not trigger the route execution once again, because *Trigger target subscription actions* is **unchecked**.

External Script and Publish To Account

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the External Script and Publish To Account use case:

- *Overview* on page 904
- *Prerequisites* on page 904
- *Step to configure the flow* on page 904
- *Script example* on page 905
- *Flow of events* on page 906

Overview

Compress incoming files by leveraging an external script and publish the result archive to the local account.

Prerequisites

- Download and install 7zip on your SecureTransport machine.
- Create a Route Package Template. For instructions on creating a Route Package Template, refer to *Add Route Package Template* on page 807.
- Create an Advanced Routing application instance. For instructions on creating an Advanced Routing application instance, refer to *Create Advanced Routing application instance* on page 1.
- Create a SecureTransport user account. For instructions on creating an user account, refer to *User accounts* on page 453.

Step to configure the flow

1. Create a script with the following contents that uses 7zip to compress the incoming files.
    a. Modify the third line of the script and set the correct path to the *7z* executable.
    b. Name the script `7zip-compress.sh`.
    c. Ensure the script is accessible by SecureTransport. For this example, it needs to be deployed in the `/bin/agents` subfolder of the SecureTransport installation folder.
2. Create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.
    a. Configure the subscription folder.
    b. To await multiple files, configure a condition (for example: trigger file) on which to submit the files to the route.
    c. (Optional) Configure the rest of the settings.
    d. Click **Add** when done.
3. Navigate to the *Routes* tab of the created account and assign a new route package to the account by choosing the created Route Package Template and clicking the **Assign Route** button. For assigning a route configuration details, refer to *Assign Route Package Template* on page 818.

4. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 2.
5. Create a new route by clicking the **New Route** button in the *Specific Settings* pane. For route configuration details, refer to *New Route* on page 812.
    a. Configure the new route's name and (optionally) description.
    b. Add and configure an External Script step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For External Script configuration details, refer to *External Script* on page 850.
        i. Specify the external script path and arguments as follows:

        ```
        /bin/sh -C ${FILEDRIVEHOME}/bin/agents/7zip-compress.sh archive-${timestamp}.7z
        ```

        ii. Select **Log script's standard output to Server log**.
        iii. (Optional) Configure the rest of the settings.
        iv. Click **Save** when done.
    c. Add and configure a Publish to Account step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For Publish To Account configuration details, refer to *Publish To Account* on page 875.
        i. Uncheck **Proceed with route execution on step failure**.
        ii. Select an account to publish to (for example, the current account).
        iii. Select a folder to publish the file to (for example, the subscription folder configured in Step 2).
        iv. (Optional) Configure the rest of the settings.
        v. Click **Save** when done.
6. Save the route and the route package.

Script example

```
#!/bin/sh

SEVENZIP="<path to '7z' executable>"

if [ "X${ST_ACCOUNT_HOME}" = "X" ]; then
        echo "ST_ACCOUNT_HOME environment variable not set, aborting."
        exit 1
fi

# Dump the environment in the account home folder
env > ${ST_ACCOUNT_HOME}/dumpenv.${$}
```

```
if [ ! -x $SEVENZIP ]; then
        echo "\"$SEVENZIP\" does not exist or is not an executable,
aborting."
        exit 2
fi

# Go to the sandbox folder
cd $SANDBOX_FOLDER

# Keep track of the files that will be archived to delete them later
FILELIST=`ls`

$SEVENZIP a $1 *
exitcode=$?

if [ $exitcode -ne 0 ]; then
        echo "Failed to compress files \"$FILELIST\", aborting."
        exit $exitcode
fi

# Delete the archived files
for file in $FILELIST ;
do
rm -f $file;
done
```

Flow of events

1. Multiple files are uploaded via any protocol to the Advanced Routing subscription folder.
2. The trigger file (file with `.trigger` extension) is uploaded to the subscription folder.
3. The Advanced Routing application triggers the route.
4. The uploaded files are compressed into a single 7zip archive and published to the subscription folder.

Note In the end there will be several files present in the subscription folder – the input files, the trigger file, and the archive. To automatically remove the input files and the trigger file, select **Post Processing Action > On Success > Delete** in the subscription settings.

Note Publishing the archive file in Advanced Routing subscription folder does not trigger the route execution once again, because *Trigger target subscription actions* is **unchecked**.

Send To Partner (PeSIT)

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the Send To Partner (PeSIT) use case:

- *Overview* on page 907
- *Prerequisites* on page 907
- *Steps to configure the flow* on page 907
- *Flow of events* on page 908

Overview

Each incoming file is routed to a remote transfer site over PeSIT and the file is archived to a local folder.

Prerequisites

- Create a Route Package Template. For Route Package Template creation details, refer to *Add Route Package Template* on page 807.
- Create an Advanced Routing application instance. For Advanced Routing application instance creation details, refer to *Create Advanced Routing application* on page 805.
- Create a SecureTransport user account. For user account creation details, refer to *User accounts* on page 453.
- Create a PeSIT transfer site to route the file to. For PeSIT transfer site creation details, refer to *PeSIT transfer sites* on page 559.
- Create a transfer profile that is used for the transfer. For transfer profile configuration details, refer to *Transfer profiles* on page 600.
- Create a Folder Monitor transfer site that is used to archive the incoming files. For Folder Monitor transfer site configuration details, refer to *Folder Monitor transfer sites* on page 511.

Steps to configure the flow

1. Create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.
    a. Uncheck **Proceed with route execution on step failure**.
    b. Configure the subscription folder.
    c. (Optional) Configure the rest of the settings.
    d. Click **Add** when done.
2. Navigate to the *Routes* tab of the created account and assign a new route package to the account by choosing the created Route Package Template and clicking the **Assign Route** button. For assigning a route configuration details, refer to *Assign Route Package Template* on page 818.
3. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 1.

4. Create a new route by clicking the **New Route** button in the *Specific Settings* pane. For route configuration details, refer to *New Route* on page 812.
    a. Configure the new route's name and (optionally) description.
    b. Add and configure a Send to Partner step by selecting it from the *-- Select Step --* drop-down menu and clicking the **Add Step** button. For Send To Partner configuration details, refer to *Send To Partner* on page 881.
        i. Select the account which contains the target transfer site (or select **Use current account**).
        ii. Select the created PeSIT transfer site.
        iii. Select the created Transfer Profile.
        iv. Optionally, configure the **Advanced PeSIT Settings**. For example, to trigger Store and Forward:
            I. Click the **Configure advanced PeSIT settings** checkbox.
            II. Set the *Final Destination* field to the desired final destination.
        v. (Optional) Configure the rest of the step's settings.
        vi. Click **Save** when done.
    c. Add and configure a Send To Partner step by selecting it from the *-- Select Step --* drop-down menu and clicking the **Add Step** button. For Send To Partner configuration details, refer to *Send To Partner* on page 881.
        i. Select the account which contains the Folder Monitor transfer site (or select **Use current account**).
        ii. Select the Folder Monitor transfer site from the selected account.
        iii. Click **Save** when done.
5. Save the route and the route package.

Flow of events

1. A file is uploaded via any protocol to the Advanced Routing subscription folder.
2. The Advanced Routing application triggers route.
3. The uploaded file is routed to the remote PeSIT transfer site and after that is archived to the folder specified in the Folder Monitor transfer site.

Note To compress the file before sending it to the archive folder, add a Compress step before the second Send To Partner step.

Advanced use cases

An overview, the prerequisites, and the flow of events of the following advanced use cases are provided:

- *Route files based on file name extension* on page 909 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the route files based on file name extension use case.
- *PGP Encryption (partner's certificate) and send to multiple partners* on page 911 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the PGP Encryption (partner's certificate) and send to multiple partners use case.
- *Decompress and Send to Partner (trigger file output)* on page 914 - Provides the overview, prerequisites, flow configuration steps, and flow of events for the Decompress and Send to Partner (Trigger File Output) use case.

Route files based on file name extension

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the route files based on file name extension use case:

- *Overview* on page 909
- *Prerequisites* on page 909
- *Step to configure the flow* on page 909
- *Flow of events* on page 911

Overview

Identify the Routing Destination based on filename following the convention `<routing-destination>_<filename>`. The custom Expression Language function `extract('some_string', '_', 2)` is utilized since it splits the given string to tokens based on a delimiter.

Prerequisites

- Create a Route Package Template. For Route Package Template creation details, refer to *Add Route Package Template* on page 807.
- Create an Advanced Routing application instance. For Advanced Routing application instance creation details, refer to *Create Advanced Routing application* on page 805.
- Create a SecureTransport user account. For user account creation details, refer to *User accounts* on page 453.
- Create two remote transfer sites (for example, named **partner1** and **partner2**) which are used as routing destinations. For remote transfer site creation details, refer to *Create a transfer site* on page 598.

Step to configure the flow

1. Create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.

a. Configure the subscription folder.

b. (Optional) Configure the rest of the settings.

c. Click **Add** when done.

2. Navigate to the *Routes* tab of the created account and assign a new route package to the account by choosing the created Route Package Template and clicking the **Assign Route** button. For assigning a route configuration details, refer to *Assign Route Package Template* on page 818.
3. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 1.
4. Configure the *Execution Rule* of the route package to be **First Matching Route**.
5. Create a new route by clicking the **New Route** button in the *Specific Settings* pane. For route configuration details, refer to *New Route* on page 812.
   a. Configure the new route's name (for example, **Partner 1**) and (optionally) description.
   b. Configure the *Route Condition* to be **Expression Language** and enter the following in the expression field:

      ```
      ${extract(basename(transfer.target),'_',1) eq 'partner1'}
      ```

   c. Add and configure a Send To Partner step by selecting it from the *-- Select Step --* drop-down menu and clicking the **Add Step** button. For Send To Partner configuration details, refer to *Send To Partner* on page 881.
      i. Select the account which contains the target transfer site (or select **Use current account**).
      ii. Select the transfer site from the selected account to send the file to (for example, **partner1**).
      iii. Select **Route file as** and enter the following expression:

      ```
      ${extract(basename(transfer.target),'_',1)}
      ```

      This expression extracts the *<routing-destination>* from the filename (for example, `partner1_incoming.txt` returns `partner1`).
      iv. Click **Save** when done.
6. Create another route by clicking the **New Route** button in the *Specific Settings* pane.
   a. Configure the new route's name (for example **Partner 2**) and (optionally) description.
   b. Configure the *Route Condition* to be **Expression Language** and enter the following in the expression field:

      ```
      ${extract(basename(transfer.target),'_',1) eq 'partner2'}
      ```

   c. Add and configure a Send To Partner step by selecting it from the *-- Select Step --* drop-down menu and clicking the **Add Step** button.
      i. Select the account which contains the target transfer site (or select **Use current account**).
      ii. Select the transfer site from the selected account to send the file to (for example, **partner2**).

iii. Select Route file as and enter the following expression:

```
${extract(basename(transfer.target),'_',2)}
```

This expression extracts the *<filename>* from the filename (for example, `partner2_incoming.txt` returns `incoming`).

iv. Click **Save** when done.

7. Save the route package.

Flow of events

1. A file named `partner1_filename.txt` is uploaded to the Advanced Routing subscription folder.
2. Advanced Routing application is triggered and `partner1` is extracted from the filename.
3. Route **Partner 1** is triggered. Route **Partner 2** is skipped.
4. File is routed to the transfer site **partner1**.
5. A file named `partner2_filename.txt` is uploaded to the Advanced Routing subscription folder.
6. The Advanced Routing application is triggered and `partner2` is extracted from the filename.
7. Route **Partner 1** is skipped. Route **Partner 2** is triggered.
8. File is routed to the transfer site **partner2**.

PGP Encryption (partner's certificate) and send to multiple partners

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the PGP Encryption and send to multiple partners use case:

- *Overview* on page 911
- *Prerequisites* on page 911
- *Steps to configure the flow* on page 912
- *Flow of events* on page 914

Overview

Pull files from multiple sources and route the incoming files to multiple partners after PGP encrypting the files with the partner's PGP certificate.

Prerequisites

- Create an Advanced Routing application instance. For Advanced Routing application instance creation details, refer to *Create Advanced Routing application* on page 805.

- Create two partner accounts (for example, accounts with names **partner1** and **partner2**). For user account creation details, refer to *User accounts* on page 453.
    - Create transfer site in each account to be used as a routing destination to the respective partner.

      Note Modify the access level of the transfer sites to be **Public**, so these transfer sites can be used in routes defined outside of this account.
    - Generate or import a partner PGP certificate in each account that is used for encrypting the files before routing them to the partner

      Note Modify the access level of the certificates to be **Public**, so these certificates can be used in routes defined outside of this account.
- Create two local accounts (for example, accounts with name **local1** and **local2**) and transfer sites (for example, named **target1** and **target2**) which are used as source for pulling. For user account creation details, refer to *User accounts* on page 453.

Steps to configure the flow

1. Create a Route Package Template by navigating to **Routes** and clicking **New Route Package Template**. For Route Package Template creation details, refer to *Add Route Package Template* on page 807.
    a. Configure the new Route Package Template's name and (optionally) description.
    b. Create a new route by clicking the **New Route** button. For route configuration details, refer to *New Route* on page 812.
        i. Configure the new route's name (for example, **Partner 1**) and (optionally) description.
        ii. Add and configure a PGP Encryption step by selecting it from the *-- Select Step --* drop-down menu and clicking the **Add Step** button. For PGP Encryption configuration details, refer to *PGP Encryption* on page 829.
            I. Select the **Encrypt only** option.
            II. Select the first partner account.
            III. Select the PGP certificate for encryption from that account.
            IV. Click **Save** when done.
        iii. Add and configure a Send To Partner step by selecting it from the *-- Select Step --* drop-down menu and clicking the **Add Step** button. For Send To Partner configuration details, refer to *Send To Partner* on page 881.
            I. Uncheck **Proceed with route execution on step failure**.
            II. Select the first partner account which contains the target transfer site.
            III. Select the transfer site from the selected account to send the file to.
            IV. Click **Save** when done.

c. Save the route and create a new one by clicking the **New Route** button.

i. Configure the new route's name (for example, **Partner 2**) and (optionally) description.

ii. Add and configure a PGP Encryption step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button.

I. Select the **Encrypt only** option.

II. Select the second partner account.

III. Select the PGP certificate for encryption from that account.

IV. Click **Save** when done.

iii. Add and configure a Send To Partner step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button.

I. Uncheck **Proceed with route execution on step failure**.

II. Select the second partner account which contains the target transfer site.

III. Select the transfer site from the selected account to send the file to.

IV. Click **Save** when done.

d. Save the Route Package Template.

2. Go to the first local account (**local1**) and create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.

a. Configure the subscription folder.

b. Select **Automatically Retrieve Files From** checkbox and choose the transfer site to pull files from (the one created as a prerequisite).

c. Configure a schedule for pulling the files.

d. (Optional) Configure the rest of the settings.

e. Click **Add** when done.

3. Navigate to the *Routes* tab of the same account and assign a new route package to the account by choosing the Route Package Template created in Step 1 and clicking the **Assign Route** button.

a. Configure the new route package's name and (optionally) description.

b. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 2.

c. Click **Save** when done.

Note There's no need to create routes within the route package as the routes inherited from the Route Package Template are sufficient for the current use case.

4. Go to the second local account (**local2**) and create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button.

a. Configure the subscription folder.

b. Select **Automatically Retrieve Files From** checkbox and choose the transfer site to pull files from (the one created as a prerequisite).

c. Configure a schedule for pulling the files.

d. (Optional) Configure the rest of the settings.

e. Click **Add** when done.

5. Navigate to the *Routes* tab of the same account and assign a new route package to the account by choosing the route template package created in Step 1 and clicking the **Assign Route** button.

a. Configure the new route package's name and (optionally) description.

b. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 2.

c. Click **Save** when done.

Note There's no need to create routes within the route package as the routes inherited from the Route Package Template are sufficient for the current use case.

Flow of events

1. A scheduled SIT pull is triggered as configured in account **local1's** subscription.
2. The files from the remote site are downloaded in the local subscription folder and the Advanced Routing application is triggered.
3. Files are processed by the two routes configured in the Route Package Template:
   - The first route PGP encrypts the file with the certificate imported in **partner1** account and routes the file to **partner1**.
   - The second route PGP encrypts the file with the certificate imported in **partner2** account and routes the file to **partner2**.
4. A scheduled SIT pull is triggered as configured in account **local2's** subscription.
5. The files from the remote site are downloaded in the local subscription folder and the Advanced Routing application is triggered.
6. Files are processed by the two routes configured in the Route Package Template:
   - The first route PGP encrypts the file with the certificate imported in **partner1** account and routes the file to **partner1**.
   - The second route PGP encrypts the file with the certificate imported in **partner2** account and routes the file to **partner2**.

Decompress and Send to Partner (trigger file output)

The following topics provide the overview, prerequisites, configuration steps, and flow of events for the Decompress and Send To Partner with trigger file output use case:

- *Overview* on page 915
- *Prerequisites* on page 915
- *Steps to configure the flow:* on page 915
- *Flow of events* on page 916

Overview

Decompress incoming archives, send the result files to two remote transfer sites and send a trigger file to one of them.

Prerequisites

- Create a Route Package Template. For Route Package Template creation details, refer to *Add Route Package Template* on page 807.
- Create an Advanced Routing application instance. For Advanced Routing application instance creation details, refer to *Create Advanced Routing application* on page 805.
- Create an SecureTransport user account. For user account creation details, refer to *User accounts* on page 453.
- Create remote transfer sites which are used as routing destinations (for example, **Partner 1 (FTP)** and **Partner 2 (HTTP)**). For remote transfer site creation details, refer to *Create a transfer site* on page 598.

Steps to configure the flow:

1. Create and configure a subscription to the Advanced Routing application by navigating to the account's *Subscriptions* tab and clicking the **Subscribe...** button. For Advanced Routing subscription configuration details, refer to *Subscribe to Advanced Routing application* on page 821.
    a. Configure the subscription folder.
    b. (Optional) Configure the rest of the settings.
    c. Click **Add** when done.
2. Navigate to the *Routes* tab of the created account and assign a new route package to the account by choosing the created Route Package Template and clicking the **Assign Route** button. For assigning a route configuration details, refer to *Assign Route Package Template* on page 818.
3. Assign a subscription to the new route package by selecting **Assign** in the *Subscriptions* pane and selecting the subscription created in Step 1.
4. Create a new route by clicking the **New Route** button in the *Specific Settings* pane. For route configuration details, refer to *New Route* on page 812.
    a. Configure the new route's name and (optionally) description.
    b. Add and configure a Decompress step by selecting it from the *-- Select Step --* drop-down menu and clicking the **Add Step** button. For Decompress configuration details, refer to *Decompress* on page 842.

i. (Optional) Configure the available options.

ii. Click **Save** when done.

Note The Decompress step automatically detects the archive type.

c. Add and configure a Send To Partner step by selecting it from the -- *Select Step* -- drop-down menu and clicking the **Add Step** button. For Send To Partner configuration details, refer to *Send To Partner* on page 881.

i. Uncheck **Proceed with route execution on step failure**.

ii. Select the account which contains the target transfer sites (or select **Use current account**).

iii. Select the transfer sites from the selected account to send the files to (for example, **Partner 1 (FTP)** and **Partner 2 (HTTP)**).

iv. Select **Send trigger file**.

v. Specify trigger file name (for example, `${timestamp}.trigger`).

vi. (Optional) Specify **Trigger file content** if the remote system expects trigger file with content.

Note You can use the `${transferredfilenames}` environment variable to specify the trigger file contents. This way the trigger file contains all files transferred by the step and each file is on a new line. The trigger file contains the original file names of the transferred files even if rename have been configured in the transfer site. `\r\n` (CRLF) is used as a line separator for the content of the trigger file.

vii. Select an account and a transfer site to send the trigger file to. Usually these are the same as the ones configured in Step ii and Step iii.

viii. Click **Save** when done.

5. Save the route and the route package.

Flow of events

1. An archive file is uploaded to the Advanced Routing subscription folder. The archive contains two files named `text1.txt` and `text2.txt`.
2. The Advanced Routing application is triggered and the archive is processed by the route.
3. The archive is decompressed – `text1.txt` and `text2.txt` are the resulting files.
4. The files are routed to the selected transfer sites (**Partner 1 (FTP)** and **Partner 2 (HTTP)**).
5. A trigger file is generated with name `<current timestamp>.trigger` (for example, `1334851799648.trigger`) with contents:
   - `text1.txt`
   - `text2.txt`
6. The trigger file is routed to **Partner 1 (FTP)** transfer site only.

Advanced Routing best practices

This topic emphasizes a number of important Advanced Routing usage tips by describing the process flow of some complex scenarios.

The following Advanced Routing best practices are described:

- *Chain of route execution* on page 917
- *Inherited settings vs. Specific Settings* on page 918
- *Skipped transformation* on page 918
- *Transformation on multiple files* on page 919
- *Route failure* on page 919
- *Transformed file as the input to the next step* on page 920
- *Routing to multiple transfer sites* on page 920

Chain of route execution

The following Advanced Routing steps are configured:

- Route 1:
  - Transformation 1: Compression
  - Routing 1: Publish To Account
- Route 2
  - Transformation 1: Compression
  - Transformation 2: PGP Encryption
  - Routing 1: Send To Partner

The uploaded file triggers Route 1 and Route 2 in the specified order. The execution of Route 1 compresses the original file and routes the transformed (compressed) file to an account for publishing. The execution of Route 2 compresses the original file, PGP encrypts the compressed file, and routes the transformed (compressed and PGP encrypted) file to a partner transfer site.

Each route works with a copy of the original file. During the route execution the copy of the original file is passed from step to step. See *Transformed file as the input to the next step* on page 920 for more information.

Note Execution of the routes is sequential, not simultaneous.

Note It is highly recommended that the last step of every route is a routing step (Send To Partner or Publish To Account). The reason is that only routing steps can move (send or publish) the transformed file or files outside of the sandbox folder. Having only transformation steps properly transforms the file in the sandbox folder, but when the route terminates the transformed files is deleted along with the sandbox folder.

Related topics:

- *Inherited settings vs. Specific Settings* on page 918
- *Skipped transformation* on page 918
- *Transformation on multiple files* on page 919
- *Route failure* on page 919
- *Transformed file as the input to the next step* on page 920
- *Routing to multiple transfer sites* on page 920

Inherited settings vs. Specific Settings

The following Advanced Routing steps are configured:

- Inherited Settings:
    - Route 1:
        - Transformation 1: Compression
        - Routing 1: Publish To Account
- Specific Settings:
    - Route 2:
        - Transformation 1: PGP Encryption
        - Routing 1: Send To Partner

The uploaded file triggers Route 1 (Inherited Settings) and Route 2 (Specific Settings). The Inherited Settings compress the original file and routes the transformed (compress) file to an account for publishing. The Specific Settings PGP encrypt the original file and routes the transformed (PGP encrypted) file to a partner transfer site.

The Inherited Settings have a higher priority than the Specific Settings.

Note It is highly recommended that the last step of every route is a routing step (Send To Partner or Publish To Account). The reason is that only routing steps can move (send or publish) the transformed file or files outside of the sandbox folder. Having only transformation steps properly transforms the file in the sandbox folder, but when the route terminates the transformed files are deleted along with the sandbox folder.

Skipped transformation

The Advanced Routing routes are configured:

- Route 1:
    - Transformation 1: PGP Decryption where **Require Encryption** is not selected
    - Route 1: Publish To Account

- Route 2:
    - Transformation 1: Line Ending where **Process files based on a filename pattern** is selected
    - Route 1: Send To Partner

A clear text file is uploaded. Route 1 is triggered. The PGP Decryption transformation is skipped since **Require Encryption** is not selected. The clear text file is published successfully. A file is uploaded that does not match the configured filename pattern. Route 2 is triggered. The Line Ending transformation is skipped since the filename pattern was not recognized and routes the original file to partner transfer site.

Note PGP Decryption, Decompression, and Line Ending transformations have optional behaviors that enables them to pass along files that are not eligible for transformation.

Note Even though transformation steps could be skipped, it is highly recommended that the last step of every route will be a routing step (Send To Partner or Publish To Account). Only routing steps can route the transformed file outside of the sandbox folder.

Transformation on multiple files

The following Advanced Routing routes are configured:

- Route 1:
    - Transformation 1: Decompress
    - Transformation 2: PGP Decryption where **Require Encryption** is not selected
    - Routing 1: Publish To Account
- Route 2:
    - Routing 2: Send To Partner

A compressed file, containing both PGP encrypted and clean files, is uploaded. Route 1 is triggered. Transformation 1 decompresses the file and multiple files are passed on to Transformation 2. The PGP encrypted files are decrypted and the clean files are left as they are. The PGP decrypted and clean files are routed to the Publish to Account destination. Route 2 is triggered and originally uploaded compressed file is pushed to the partner transfer site.

Note If **Proceed with route execution on step failure** is not selected for the PGP Decryption (Route 1, Transformation 2) and PGP Decryption fails on any file, the whole transformation chain is considered failed. Any further operations withing the route are not executed. Any successfully transformed files (until the failure point) are left on the file system. Any files that are in the sandbox folder are lost. Only files published by Send To Partner or Publish To Account route steps are available.

Route failure

The following Advanced Routing routes are configured:

- Route 1:
    - Transformation 1: Decompress
    - Transformation 2: PGP Decryption where **Require Encryption** is selected and **Proceed with route execution on step failure** is not selected
    - Routing 1: Publish To Account
- Route 2:
    - Routing 1: Send To Partner

A compressed file, containing both PGP encrypted and clean files, is uploaded. Route 1 is triggered. Transformation 1 decompresses the file and multiple files are passed on to Transformation 2. The PGP encrypted files are decrypted but since some of the files are in plain text the step execution fails (because **Require Encryption** is selected). Since **Proceed with route execution on step failure** is not selected the whole transformation chain is considered failed and any further processing within Route 1 is not executed, which means that Routing 1 (Publish To Account) is not executed (even though there are successfully decrypted files). Although other routes (if any) defined in the chain are executed. That's why Route 2 is triggered and the originally uploaded compressed file is pushed to the partner site.

Note By default all routing steps (Send To Partner and Publish To Account) are configured to be processed even though one or more files have failed to be sent or published, though all transformation steps (PGP Encryption, PGP Decryption, and so forth) are configured to fail even if only one file transformation has failed.

Note If route execution fails, any successfully transformed files (until the failure point) are left in the sandbox folder. Any files that are in the sandbox folder are lost. Only files published by the Send To Partner or Publish To Account route steps are available.

Transformed file as the input to the next step

The following Advanced Routing routes are configured:

- Route 1:
    - Transformation 1: Line Ending where **Rename output files** is not selected
    - Routing 1: Publish To Account

A text file is uploaded. Route 1 is triggered. Transformation 1 performs a Line Ending transformation over the file. The name of the file is not modified because **Rename output files** is not selected and the Line Ending transformation does not automatically modify the file name. The transformed file is the input for the next step, that's why the transformed file is routed to the Publish To Account destination.

Note When **Rename output files** is selected, the transformed file is renamed in the sandbox folder only. The original file in the subscription folder is not transformed.

Routing to multiple transfer sites

The following Advanced Routing route is configured:

- Route 1:
    - Routing 1: Send To Partner where multiple transfer sites belonging to a single account are selected

A file is uploaded. Route 1 is triggered. The file is sent to all transfer sites. If any of the transfers temporarily fail, only the failed transfers are automatically retried. There are no retries if the transfer permanently fails.

Note When routing to multiple transfer sites, it is recommended the **Route file as** be set using an Expression Language expression, containing `${timestamp}` or `${random()}` so it's transformed to an unique value for each of the transfers.

Note Unlike automatic retries when an ordinary subscription folder is used to send files directly to a transfer site, with the Advanced Routing feature the administrator is not able to control the automatic retries using *Cancel* or *Resubmit* buttons.

Custom Expression Language functions and variables

This topic lists custom Expression Language (EL) functions and variables that can be used within the Advanced Routing file processing. For information on additional Expression Language expressions, refer to *Expression Language* on page 1020.

Exceptional case: absolute path to sandbox folder in EL expressions

Problem summary: With SecureTransport deployments on Windows Server, attempts to use a configured absolute path to sandbox location in an EL expression may fail and return an error.

Problem details:

1. You set an absolute path value for the sandbox location in the '`AdvancedRouting.sandboxFolderLocation`' server configuration option.
2. You configure use of EL expressions: set the '`AdvancedRouting.sandboxFolderLocation.expressionLanguage`' configuration option to '`true`'.
3. When you attempt to use an expression (for example'`\\10.232.2.103\Shared\sandbox\${env['DXAGENT_ACCOUNT_TYPE']}`'), you might get errors in the Server Log.

Possible cause: The issue is configuration based and relates to the allowed remote storage for 'Users' to create symbolic links (configurable in 'secpol.msc' where 'Users' must be added in - *Security Settings > Local Policies > User Rights Assignment > 'Create symbolic links'*). The problem occurs only in the case when the user's home folder and the sandbox custom folders are both set to one or more remote storage machines.

Solution: This problem might occur because by default remote to remote symbolic links are disabled. You can enable it with `fsutil`.

```
C:\Windows\system32>fsutil behavior query SymlinkEvaluation
    Local to local symbolic links are enabled.
    Local to remote symbolic links are enabled.
    Remote to local symbolic links are disabled.
    Remote to remote symbolic links are disabled.
C:\Windows\system32>fsutil behavior set SymlinkEvaluation R2R:1
C:\Windows\system32>fsutil behavior query SymlinkEvaluation
    Local to local symbolic links are enabled.
    Local to remote symbolic links are enabled.
    Remote to local symbolic links are disabled.
    Remote to remote symbolic links are enabled.
Be sure to run fsutil from elevated command prompt.
```

The following topics provide detailed lists of the custom Expression Language functions and variables that can be used within the Advanced Routing file processing:

- *Session related EL expressions* on page 922
- *Predefined EL functions* on page 926
- *Account related EL expressions* on page 927
- *LDAP related EL expressions* on page 929
- *PeSIT related EL expressions* on page 930
- *Routing related EL expressions* on page 936
- *Special routing variables* on page 937
- *STFS PeSIT related EL expressions* on page 937
- *Transfer related EL expressions* on page 943
- *Trigger related EL expressions* on page 945
- *User related EL expressions* on page 946
- *HTTP header EL expressions* on page 946 that can be used within the Advanced Routing file processing
- *Accessing Single Sign-On (SSO) attributes* on page 391

Session related EL expressions

The following table lists the session related variables along with their corresponding Agent environment variables, as well as EL expression examples:

Routing EL expression / Agent Env Variable	Example usage
session.protocol DXAGENT_PROTOCOL	${session.protocol eq 'http'} - will return true
session.workDir DXAGENT_PWD=/	${concat(transfer.targetDir.substring (0,1), leadingFolder(session.workDir)) eq transfer.targetDir} - returns true
session.workDirFull DXAGENT_PWD_RESOLVED	${session.workDirFull.substring(13,15) eq account.businessUnit.name} - returns true
session.remoteAddress DXAGENT_REMOTEADDR	${session.remoteAddress eq session.remoteHost}
session.remoteHost DXAGENT_REMOTEHOST	${session.remoteHost.matches('10.*')}
session.streamingClient DXAGENT_CLIENT	${session.streamingClient eq 'httpd'} ${extract (session.streamingClient,'d',1) eq session.protocol}
session.isSSL DXAGENT_SECURE_DATA	${session.isSSL} ${!session.isSSL}
session.transferDirection DXAGENT_TYPE	The direction of the transfer configuration. Values: • 0 indicates a transfer from an account to the application. • 1 indicates a transfer from the application to an account.
session.timestampOutgoingEnd DXAGENT_TIMESTAMP_OUTGOING_END	${session.timestampOutgoingEnd} - the timestamp for events with outgoing type and trigger end.
session.logFileName DXAGENT_LOGFILENAME	${session.logFileName} - the log file name. This will be used by runas utility on Unix to redirect stderr.
session.edgeId DXAGENT_EDGEID	${session.edgeId} - the identifier of the current SecureTransport Edge. The Edge identification string is set in the protocol server's configuration file(s).

Routing EL expression / Agent Env Variable	Example usage
session.subscriptionFolder DXAGENT_SUBSCRIPTION_FOLDER	${session.subscriptionFolder} - the subscription folder in the form of a POSIX-style path relative to the user home directory. This value represents the client path.
session.applicationType DXAGENT_APPLICATION_TYPE	${session.applicationType} - a string that identifies application type.
session.applicationName DXAGENT_APPLICATION_NAME	${session.applicationName} - the name of the application instance.
session.applicationNotes DXAGENT_APPLICATION_NOTES	${session.applicationNotes} - notes associated with the application instance.
session.siteUploadFolder DXAGENT_SITE_ATTR_UPLOAD_FOLDER	${session.siteUploadFolder} - the upload folder specifies the directory on the remote server where the uploaded files are placed.
session.siteUsername DXAGENT_SITE_ATTR_USERNAME	${session.siteUsername} - the username presented to the remote server for authentication; optional Site attribute.
session.siteHost DXAGENT_SITE_ATTR_HOST	${session.siteHost} - the remote host represented by the site. If absent, the site does not establish a connection to the remote host. An example of that is the Folder Monitor site.

Agent Env Variable	Routing EL expression	Example
DXAGENT_PROTOCOL	session.protocol	${session.protocol eq 'http'} - will return true
DXAGENT_PWD=/	session.workDir	${concat (transfer.targetDir.substring(0,1), leadingFolder (session.workDir)) eq transfer.targetDir} - returns true

Agent Env Variable	Routing EL expression	Example
DXAGENT_PWD_RESOLVED	session.workDirFull	${session.workDirFull.substring(13,15) eq account.businessUnit.name} - returns true
DXAGENT_REMOTEADDR		${session.remoteAddress eq session.remoteHost}
DXAGENT_REMOTEHOST	session.remoteHost	
DXAGENT_CLIENT	session.streamingClient	
DXAGENT_SECURE_DATA	session.isSSL	
DXAGENT_TYPE	session.transferDirection	
	session.timestampOutgoingEnd	
DXAGENT_LOGFILENAME	session.logFileName	
DXAGENT_EDGEID	session.edgeId	
DXAGENT_SUBSCRIPTION_FOLDER	session.subscriptionFolder	
DXAGENT_APPLICATION_TYPE	session.applicationType	${session.applicationType} - a string that identifies application type.
DXAGENT_APPLICATION_NAME	session.applicationName	${session.applicationName} - the name of the application instance.

Agent Env Variable	Routing EL expression	Example
DXAGENT_APPLICATION_NOTES	session.applicationNotes	${session.applicationNotes} - notes associated with the application instance.
DXAGENT_SITE_ATTR_UPLOAD_FOLDER	session.siteUploadFolder	${session.siteUploadFolder} - the upload folder specifies the directory on the remote server where the uploaded files are placed.
DXAGENT_SITE_ATTR_USERNAME	session.siteUsername	${session.siteUsername} - the username presented to the remote server for authentication; optional Site attribute.
DXAGENT_SITE_ATTR_HOST	session.siteHost	${session.siteHost} - the remote host represented by the site. If absent, the site does not establish a connection to the remote host. An example of that is the Folder Monitor site.

Predefined EL functions

The following table lists predefined EL functions and descriptions.

Syntax	Description
${variable.toUpperCase()}	Converts a given string to upper case only characters. **Usage:** ${transfer.target.toUpperCase()}
${variable.toLowerCase()}	Converts a given string to lower case only characters. **Usage:** ${transfer.target.toLowerCase()}
${variable.substring(beginIndex,endIndex)}	Returns a substring for a given string. The substring begins at the specified beginIndex and extends to the character at index endIndex - 1. Thus, the length of the substring is calculated as endIndex-beginIndex. **Usage:** ${transfer.target.substring(0,5)}
${extract(variable, delimiter, position)}	Splits given string to tokens based on a delimiter. **Usage:** ${extract('payroll_Axway_21457584375.txt', '_', 2)} returns Axway

Syntax	Description
`${leadingFolder(path)}`	For given directory/file path returns only the parent folder. **Usage:** • `${leadingFolder('/opt/TMWD/st51')}` - returns `'opt'`, • `${leadingFolder('/opt')}` - returns `'opt'`, • `${leadingFolder('/')}` - returns `'/'`
`${parentFolder(path)}`	For given directory/file path returns path to the parent folder. **Usage:** • `${parentFolder('/opt/TMWD/st51')}` - returns `'/opt/TMWD'` • `${parentFolder('/')}` - returns `'/'` • `${parentFolder('/usr/file.txt')}` - returns `'/usr'`
`${dayOffset(format, offset)}`	Returns a date representing today's date with the offset of the days parameter. **Usage:** • `${dayOffset('yyMMdd', '-5')}` - returns 10th if today is 15th of August formatted as per the specified format parameter - `120810`. • `${dayOffset('yyMMdd', '+7')}` - returns 22th if today is 15th of August formatted as per the specified format parameter - `120822`. • `${dayOffset('ddMMyy', '+1')} ge '090414'}`

Account related EL expressions

The following table provides the account related EL expressions.

Agent Env Variable	Routing EL expression	Example
DXAGENT_ACCOUNT_ATTR_*	account.attributes ['ATTRIBUTE_NAME']	${account.attributes ['templateClass'].toUpperCase() eq 'AdClass'.toUpperCase()} - returns true ${account.attributes ['transfersWebServiceAllowed']} - returns either false or true
DXAGENT_ACCOUNT_DELIVERY_METHOD	account.deliveryMethod	${account.deliveryMethod. toLowerCase() == 'custom' }
DXAGENT_ACCOUNT_DISABLED	account.disabled	${account.disabled != '0'} - returns true
DXAGENT_ACCOUNT_EMAIL	account.email	${!empty account.email}
DXAGENT_ACCOUNT_ENROLLMENT	account.enrollment	${account.enrollment.toLowerCase() eq 'existing_account'}
DXAGENT_ACCOUNT_HTMLTEMPLATE	account.htmlTemplate	${account.htmlTemplate.substring (11,14) eq 'sm6'}
DXAGENT_ACCOUNT_ID	account.id	${ !empty account.id}
DXAGENT_BUSINESS_UNIT_NAME	account.businessUnit.name	${account.businessUnit.name eq 'bu'} - returns true
DXAGENT_BUSINESS_UNIT_ID	account.businessUnit.id	${ !empty account.businessUnit.id}
DXAGENT_ACCOUNT_NAME	account.name	${account.name eq 'template-routes'} - returns true

Agent Env Variable	Routing EL expression	Example
DXAGENT_ ACCOUNT_NOTES	account.notes	${ !empty account.notes}
DXAGENT_ ACCOUNT_PHONE	account.phone	${ !empty account.phone}
DXAGENT_ ACCOUNT_TYPE	account.type	${account.type eq 'template'} ${account.type != 'service'}
DXAGENT_ HOMEDIR	account.home	${parentFolder (transfer.targetDirFull) eq account.home}
DXAGENT_ ACCOUNT_ IMPLICIT_ ENROLLMENT	account. implicit Enrollment	${account.implicitEnrollment. toLowerCase().matches ('.*account')}
	account.attributes ['userVars.xxx']	Access additional attribute of an account with name xxx.

LDAP related EL expressions

The following table provides the LDAP related EL expressions.

Agent Env Variable	Routing EL expression	Example
STSESSION_ LDAP_DOMAIN_ ID	ldap.domainId	${ldap.domainId == '<domain id>'}
STSESSION_ LDAP_DOMAIN_ NAME	ldap.domainName	${ldap.domainName eq 'ad'} - will return true
STSESSION_ LDAP_DN	ldap.dn	${ldap.dn.toLowerCase ().matches('.*dc=st1.*')} - will return true

Agent Env Variable	Routing EL expression	Example
STSESSION_LDAP_AUTH_BY_EMAIL	ldap.authByEmail	${ldap.authByEmail gt 0}
STSESSION_LDAP_DIR.*	ldap.attributes.*	
STSESSION_LDAP_DIR_mail	ldap.attributes.mail	${ldap.attributes.mail.matches('usert.*') ? 1 : 0} - will return 1

PeSIT related EL expressions

The following table provides the PeSIT related EL expressions.

Agent Env Variable	Routing EL expression	Description
DXAGENT_PESIT_FILE_DESTINATION	pesit.file.destination	Provides the file destination.
DXAGENT_PESIT_FILE_FILENAME	pesit.file.filename	Provides the file name.
DXAGENT_PESIT_FILE_ORIGINATOR	pesit.file.originator	Provides the originator of the file.
DXAGENT_PESIT_FILE_RECEIVER	pesit.file.receiver	Provides the receiver for the file.
DXAGENT_PESIT_FILE_SENDER	pesit.file.sender	Provides the sender of the file.
DXAGENT_PESIT_FILE_FILETYPE	pesit.file.filetype	Provides a description of the file type.
DXAGENT_PESIT_FILE_TRANSFERID	pesit.file.transferID	Provides the transfer ID of the file.

Agent Env Variable	Routing EL expression	Description
DXAGENT_PESIT_PI_CRC	pesit.pi.crc	Provides the cyclic redundancy check (CRC) parameters in the message body. Example: Outgoing ${!pesit.pi.crc}
DXAGENT_PESIT_PI_DIAGCODE	pesit.pi.diagCode	Provides the diagnostic code parameters in the message body. Example: Outgoing ${pesit.pi.callerID.toLowerCase() eq account.user.loginName}
DXAGENT_PESIT_PI_senderID	pesit.pi.senderID	Provides the sender identification parameters in the message body. Example: ${pesit.pi.senderID.toLowerCase() eq 'target'}
DXAGENT_PESIT_PI_receiverID	pesit.pi.receiverID	Provides the receiver identification parameters in the message body. Example: ${pesit.pi.receiverID.toLowerCase() eq account.name}
DXAGENT_PESIT_PI_callerPassword	pesit.pi.callerPassword	Provides the caller password parameters in the message body.
DXAGENT_PESIT_PI_serverPassword	pesit.pi.serverPassword	Provides the server password parameters in the message body.
DXAGENT_PESIT_PI_version	pesit.pi.version	Provides the version parametes in the message body. Example: Outgoing ${pesit.pi.version == 2}

Agent Env Variable	Routing EL expression	Description
DXAGENT_PESIT_PI_exchangeBufferSize	pesit.pi.exchangeBufferSize	Provides the exchange buffer size parameters in the message body. Example: ${!empty pesit.pi.exchangeBufferSize}
DXAGENT_PESIT_PI_totalRecords	pesit.pi.totalRecords	Provides the number of total records parameter in the message body.
DXAGENT_PESIT_PI_fileOrganization	pesit.pi.fileOrganization	Provides the file organization parameter in the message body. Example: ${pesit.pi.fileOrganization == 0}
DXAGENT_PESIT_PI_recordLength	pesit.pi.recordLength	Provides the record length parameter in the message body. Example: ${pesit.pi.recordLength == 2048}
DXAGENT_PESIT_PI_keyLength	pesit.pi.keyLength	Provides the key length parameter in the message body
DXAGENT_PESIT_PI_allocationUnit	pesit.pi.allocationUnit	Provides the number of allocation units parameter in the message body. Example: ${pesit.pi.allocationUnit == 0}
DXAGENT_PESIT_PI_creationDateTime	pesit.pi.creationDateTime	Provides the creation date and time parameter in the message body. Example: ${!empty pesit.pi.creationDateTime}
DXAGENT_PESIT_PI_originalSenderID	pesit.pi.originalSenderID	Provides the original sender identification parameter in the message body. Example: Store ${pesit.pi.originalSenderID eq 'CFT1'}

Agent Env Variable	Routing EL expression	Description
DXAGENT_PESIT_PI_msgData	pesit.pi.msgData	Provides the message data parameter in the message body.
DXAGENT_PESIT_PI_checkPointInterval	pesit.pi.checkPointInterval	Provides the check point interval parameter in the message body. Example: ${pesit.pi.checkPointInterval == 1024}
DXAGENT_PESIT_PI_checkPointWindow	pesit.pi.checkPointWindow	Provides the check point window parameter in the message body. Example: ${pesit.pi.checkPointWindow == 4}
DXAGENT_PESIT_PI_fileType	pesit.pi.fileType	Provides the file type parameter in the message body. Example: ${pesit.pi.fileType == 0}
DXAGENT_PESIT_PI_fileName	pesit.pi.fileName	Provides the file name parameter in the message body. Example: ${pesit.pi.fileName.toLowerCase() eq 'idf'}
DXAGENT_PESIT_PI_transferID	pesit.pi.transferID	Provides the transfer identification parameter in the message body. Example: ${!empty pesit.pi.transferID}
DXAGENT_PESIT_PI_fileAttributes	pesit.pi.fileAttributes	Provides the file attributes parameter in the message body.
DXAGENT_PESIT_PI_restart	pesit.pi.restart	Provides the restart parameter in the message body. Example: Outgoing ${!pesit.pi.restart}

Agent Env Variable	Routing EL expression	Description
DXAGENT_PESIT_PI_dataEncoding	pesit.pi.dataEncoding	Provides the data encoding parameter in the message body. Example: ${pesit.pi.dataEncoding lt 3}
DXAGENT_PESIT_PI_priority	pesit.pi.priority	Provides the priority parameter in the message body. Example: ${pesit.pi.priority == 1}
DXAGENT_PESIT_PI_restartCheckPoint	pesit.pi.restartCheckPoint	Provides the restart check point parameter in the message body.
DXAGENT_PESIT_PI_cancelCode	pesit.pi.cancelCode	Provides the cancel code parameter in the message body.
DXAGENT_PESIT_PI_checkPointNumber	pesit.pi.checkPointNumber	Provides the check point number parameter in the message body.
DXAGENT_PESIT_PI_compressed	pesit.pi.compressed	Provides the compression parameter in the message body. Example: Outgoing ${!pesit.pi.compressed}
DXAGENT_PESIT_PI_compressionType	pesit.pi.compressionType	Provides the compression type parameter in the message body. Example: ${pesit.pi.compressionType eq 3}
DXAGENT_PESIT_PI_accessType	pesit.pi.accessType	Provides the access type parameter in the message body.
DXAGENT_PESIT_PI_resyncAllowed	pesit.pi.resyncAllowed	Provides the resync allowed parameter in the message body. Example: Outgoing ${pesit.pi.resyncAllowed == 0}

Agent Env Variable	Routing EL expression	Description
DXAGENT_PESIT_PI_totalBytes	pesit.pi.totalBytes	Provides the total bytes parameter in the message body.
DXAGENT_PESIT_PI_diagnosticText	pesit.pi.diagnosticText	Provides the diagnostic text parameter in the message body.
DXAGENT_PESIT_PI_recordFormat	pesit.pi.recordFormat	Provides the record format parameter in the message body. Example: ${pesit.pi.recordFormat eq 128}
DXAGENT_PESIT_PI_fileLabel	pesit.pi.fileLabel	Provides the file label parameter in the message body. Example: ${pesit.pi.fileLabel eq transfer.target}
DXAGENT_PESIT_PI_keyOffset	pesit.pi.keyOffset	Provides the key offset parameter in the message body.
DXAGENT_PESIT_PI_allocationSize	pesit.pi.allocationSize	Provides the allocation size parameter in the message body. Example: ${pesit.pi.allocationSize == 195}
DXAGENT_PESIT_PI_extractionDateTime	pesit.pi.extractionDateTime	Provides the extraction date and time parameter in the message body.
DXAGENT_PESIT_PI_finalDestinationID	pesit.pi.finalDestinationID	Provides the final destination identification parameter in the message body. Example: Store and Forward ${pesit.pi.finalDestinationID eq 'CFT2'}

Agent Env Variable	Routing EL expression	Description
DXAGENT_PESIT_PI_serviceParam	pesit.pi.serviceParam	Provides the service parameter in the message body. Example: ${pesit.pi.serviceParam eq 'X'}

Routing related EL expressions

The following table presents the routing related EL expressions.

Routing EL expression	Description
routing.routePackageId	The ID of current Route Package. **Example:** ${routing.routePackageId.matches ('<id>')}
routing.routePackageSandboxFolder	The master working directory of current execution of a Route Package; located in ${user_home_dir}/.stfs/objects/${routePackageId(0,2)}/${routePackageId(3)}/; . The directory is same during route recovery and it is persisted with the event. **Example:** ${!routing.routePackageSandboxFolder}
routing.executeRouteSandboxFolder	The working directory of current Execute Route (it is a subdirectory of ${routing.routePackageSandboxFolder}). **Example:** ${parentFolder (routing.executeRouteSandboxFolder) eq routing.routePackageSandboxFolder}
${routing.originalFiles}	List of file paths being selected for processing from the Subscription folder.
${routing.targetFiles}	List of file paths to process in current Execute Route sandbox (these are copies of ${routing.originalFiles}; located in ${routing.executeRouteSandboxFolder}).
routing.triggeredWithoutPayload	Determines if the Route was triggered without any file(s) available for processing. This is determined by the *Submit the transferred file(s) to the route for processing.* check boxes on the Advanced Routing subscription page. Possible values are true or false.

Special routing variables

The following table provides the special routing variables.

Variable	Description
`${currentfulltarget}`	Contains the path to the file in sandbox folder that is currently processed by a transformation or routing step. Used in PGP Encryption transformation steps and in Send to Partner and Publish To Account routing steps. Also, used in the Rename output file of Transformation steps. The expression is evaluated to the absolute file path of the file being processed.
`${transformedfilename}`	Denotes the name of current transformed file. Used mainly in PGP and Compression steps (Transformation steps). Used in the *Rename output file to* pane.
`${transferredfilename}`	Denotes the name of last transferred file. It can be the same as ${currentfulltarget} or changed by using "Route file as"/"Publish file as" settings. Used in Routing steps (Publish/SendToPartner) in *Post Routing Action Rename* pane.
`${transferredfilenames}`	Contains the list of names of currently transferred files by the Send To Partner step. Files which were not processed by the Send To Partner step (because of the File Filter criteria) are not on this list. This variable should be used only in the *Trigger file content* field.

STFS PeSIT related EL expressions

The following table provides the STFS PeSIT related EL expressions.

Agent Env Variable	Routing EL expression	Description
`pesitPIEnvVariables`		

Agent Env Variable	Routing EL expression	Description
DXAGENT_ PESIT_PI_ senderID	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_senderID']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_senderID']}	Provides the sender identification parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ senderID'] eq 'PARTNER-PESIT'}
DXAGENT_ PESIT_PI_ record Length	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_recordLength']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ recordLength']}	Provides the record length parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ recordLength'] eq '2048'}
DXAGENT_ PESIT_PI_ allocation Unit	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_allocationUnit']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ allocationUnit']}	Provides the allocation unit parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ allocationUnit'] eq '0'}
DXAGENT_ PESIT_PI_ fileName	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_fileName']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_fileName']}	Provides the file name parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ fileName'].matches ('IDF.*')}

Agent Env Variable	Routing EL expression	Description
DXAGENT_ PESIT_PI_ service Param	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_serviceParam']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ serviceParam']}	Provides the service parameter in the message body. Examples: No PI99 ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ serviceParam'] eq null} With PI99 ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ serviceParam'].matches ('AloAlo')}
DXAGENT_ PESIT_PI_ receiverID	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_receiverID']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ receiverID']}	Provides the receiver identification parameter in the message body. Examples: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ receiverID'] eq 'U1'} ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ receiverID'].matches ('U.*')}
DXAGENT_ PESIT_PI_ priority	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_priority']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_priority']}	Provides the priority parameter in the message body. Examples: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ priority']} - will be evaluated to {1} which is the priority value ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ priority']==1} - will be evaluated to true

Agent Env Variable	Routing EL expression	Description
DXAGENT_ PESIT_PI_ data Encoding	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_dataEncoding']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ dataEncoding']}	Provides the data encoding parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ dataEncoding'] eq '1'}
DXAGENT_ PESIT_PI_ record Format	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_recordFormat']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ recordFormat']}	Provides the record format parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ recordFormat']==0}
DXAGENT_ PESIT_PI_ fileLabel	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_fileLabel']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_fileLabel']}	Provides the file label parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ fileLabel'].matches ('file.*')}
DXAGENT_ PESIT_PI_ original SenderID	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_originalSenderID']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ originalSenderID']}	Provides the original sender identification parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ originalSenderID'] eq null}

Agent Env Variable	Routing EL expression	Description
DXAGENT_ PESIT_PI_ final Destination ID	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_finalDestinationID']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ finalDestinationID']}	Provides the final destination identification parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ finalDestinationID'] eq null}
DXAGENT_ PESIT_PI_ creation DateTime	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_creationDateTime']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ creationDateTime']}	Provides the creation date and time parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ creationDateTime'] gt '140611093656'}
DXAGENT_ PESIT_PI_ transferID	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_transferID']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ transferID']}	Provides the transfer identification parameter in the message body. Example: ${!empty stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ transferID']}
DXAGENT_ PESIT_PI_ compression Type	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_compressionType']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ compressionType']}	Provides the compression type parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ compressionType']==3}

Agent Env Variable	Routing EL expression	Description
DXAGENT_ PESIT_PI_ exchange BufferSize	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_exchangeBufferSize']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ exchangeBufferSize']}	Provides the exchange buffer size parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ exchangeBufferSize'] lt '8192'}
DXAGENT_ PESIT_PI_ record Length	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_recordLength']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ recordLength']}	Provides the record length parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ recordLength'] < 512}
DXAGENT_ PESIT_PI_ file Organizatio n	${stfs.attributes. pesitPIEnvVariables['DXAGENT_ PESIT_PI_recordLength']} ${stfs.attributes ['pesitPIEnvVariables'] ['DXAGENT_PESIT_PI_ recordLength']}	Provides the file organization parameter in the message body. Example: ${stfs.attributes. pesitPIEnvVariables ['DXAGENT_PESIT_PI_ fileOrganization'] eq '0'}
recordsLength		
	${stfs.attributes.recordsLengt h} ${stfs.attributes ['recordsLength']}	Provides the record length parameter in the message body. Example: ${stfs.attributes ['recordsLength'].match es('[I@.*')}
endOfLineSymbol		
	${stfs.attributes.endOfLineSym bol} ${stfs.attributes ['endOfLineSymbol']}	Provides the end of line symbol parameter in the message body. Example: ${stfs.attributes ['endOfLineSymbol']. matches('n.*')}

Transfer related EL expressions

The transfer related EL expressions are derived from the use case where:

- A LDAP user has an account template (*template-routes*) which is:
  - Subscribed to an Advanced Routing application - *ba*) and assigned:
    - Subscription folder - (*/ba*)
    - Business unit - (*bu*)
    - Account home folder -

      ```
      /home/vusers/bu/user
      ```

    - Account email address -

      ```
      usert@axway.int
      ```

    - LDAP domain - *ad*

The user logs in over HTTPS and uploads a file

```
partner_certificate.crt
```

in the subscription folder under its home folder.

The following table provides the transfer related EL expressions from the use case.

Agent Env Variable	Routing EL expression	Example
DXAGENT_CORE_ID	transfer.coreId	${transfer.coreId eq "390bedec-c82e-45aa-afc2-1b78d846732d"}
DXAGENT_TARGETPATH	transfer.targetDirFull	${parentFolder (transfer.targetDirFull) eq account.home}
DXAGENT_TRANSFERRED_BYTES	transfer.transferredBytes	${transfer.transferredBytes ge 20}
DXAGENT_TRANSFER_STATUS_START_TIME	transfer.startTime	${transfer.startTime lt transfer.endTime}
DXAGENT_TIMESTAMP_INCOMING_END	transfer.endTime	${transfer.endTime gt transfer.startTime}

Agent Env Variable	Routing EL expression	Example
DXAGENT_ XFERTYPE	transfer.xferType	${transfer.xferType eq "A"} ${transfer.xferType eq "I"}
DXAGENT_ TARGETDIR	transfer.targetDir	${concat (transfer.targetDir.substring (0,1), leadingFolder (session.workDir)) eq transfer.targetDir} - returns true
DXAGENT_ FULLTARGET	transfer.targetFull	${filename (transfer.targetFull).matches ('part.*.crt')} - returns true ${extension(transfer.target) eq extension(filename (transfer.targetFull))} - returns true
DXAGENT_TARGET	transfer.target	${transfer.target.matches ('.*.crt') ? 1 : 0} - will return 1 ${extract(basename (transfer.target),'_',1) eq 'partner1'} - will return true ${basename (transfer.target).replace('(.*)_ (.*)', '$2_$1') eq 'certificate_ partner')
DXAGENT_TYPE		

Additional transfer related expressions

The following table provides additional transfer related EL expressions.

Routing EL expressions	Description
transfer.trigger	Determines the transfer trigger. Values: • server_pull - If the routing was started by a server initiated pull. • client_download - If the routing was started by a client download. • client_upload - If the routing was started by a client upload.

Routing EL expressions	Description
`transfer.status`	Determines the transfer status. Values: • `success` - If the routing was started by a success. • `failure` - If the routing was started by a failure. • `temporary_failure` - If the routing was started by a temporary failure.

Trigger related EL expressions

The following table provides the trigger related EL expressions.

Routing EL expression	Example
`string getFileContent (string filePath, int beginIndex, int length, string charset)`	Returns a string that is a sub-string of the file's content. Example: When the file contains `1234567890` the `getFileContent (file, 1, 3, "UTF8")` will return `234`.
`string getFileContentTail (string filePath, int beginIndex, int length, string charset)`	Returns a string that is a sub-string of the file's content. The reading of the file begins at the end. Example: When the file contains `1234567890` the `getFileContentTail (file, 1, 3, "UTF8")` will return `789`.
`byte[] getFileContentBytes (string filePath, int offset, int length)`	Reads up to the specified number of bytes of data starting from a specified offset into an array of bytes from the beginning of the file. An attempt is made to read as many bytes as possible, but a smaller number may be read.
`byte[] getFileContentBytesTail (string filePath, int offset, int length)`	Reads up to the specified number of bytes of data from a specified offset into an array of bytes starting from the end of the file. An attempt is made to read as many bytes as possible, but a smaller number may be read.

The functions which return a string can be used in Expressions and Predicates for route triggering, as well as in other fields in which the expression language is supported.

The functions which return bytes cannot be used in Expressions and Predicates for route triggering. The extraction of file is used for file content composition (for example, trigger file content in a Send To Partner route step).

Note When functions which return bytes are used in trigger file content, they cannot be combined with string functions, because bytes will be written.

Note The `filePath` parameter must contain an absolute path and should be written under home folder of the user who is triggering the corresponding route.

User related EL expressions

The following table provides the user related EL expressions.

Agent Env Variable	Routing EL expression	Example
DXAGENT_ LOGINNAME	account.user.loginName	${account.user.loginName. matches('.*usert.*') ? 1 : 0} - will return 1
DXAGENT_ USERTYPE	account.user.type	${account.user.type.matches ('virtual') } - will return true
DXAGENT_ USERCLASS	account.user.className	${account.user.class eq 'AdClass'}
DXAGENT_ NATIVEUSER	account.user. nativeUserName	
DXAGENT_ USERGID	account.user.uid	${account.user.uid gt '1000'}

HTTP header EL expressions

The following table provides the HTTP header EL expressions.

Agent Env Variable	Routing EL expression	Example
DXAGENT_HTTP_*	http.headers. HEADER_NAME	
DXAGENT_HTTP_ HOST	http.headers. HOST	${http.headers.HOST.matches('.*')}
DXAGENT_HTTP_ USER_AGENT	http.headers. USER_AGENT	${extract(http.headers.USER_AGENT,'/',1) eq 'Mozilla'}

Agent Env Variable	Routing EL expression	Example
DXAGENT_HTTP_REFERER	http.headers.REFERER	${concat(concat('https://',http.headers.HOST),':444').matches(http.headers.REFERER)}
DXAGENT_HTTP_CONTENT_LENGTH	http.headers.CONTENT_LENGTH	${http.headers.CONTENT_LENGTH eq transfer.transferredBytes}
DXAGENT_HTTP_CONTENT_TYPE	http.headers.CONTENT_TYPE	
DXAGENT_HTTP_ACCEPT_LANGUAGE	http.headers.ACCEPT_LANGUAGE	
DXAGENT_HTTP_FEATURES	http.headers.FEATURES	
DXAGENT_HTTP_CONTENT_RANGE	http.headers.CONTENT_RANGE	
DXAGENT_HTTP_ACCEPT	http.headers.ACCEPT	
DXAGENT_HTTP_ORIGIN	http.headers.ORIGIN	
DXAGENT_HTTP_CONNECTION	http.headers.CONNECTION	
DXAGENT_HTTP_ACCEPT_ENCODING	http.headers.ACCEPT_ENCODING	
DXAGENT_HTTP_CONTENT_DISPOSITION	http.headers.CONTENT_DISPOSITION	

Troubleshoot Advanced Routing

This topic outlines the specific troubleshooting steps for Advanced Routing as well as some general troubleshooting approach recommendations.

The following troubleshooting procedures are provided:

- *General troubleshooting steps* on page 948 - Provides general Advanced Routing troubleshooting steps.
- *Debug logging* on page 948 - Describes debug logging.

- *Log into a file* on page 948 - Provides how-to instructions for logging into a file.
- *AR fails while copying the file to sandbox* on page 949 - Provides a solution for the problem

General troubleshooting steps

Should you encounter any problems with Advanced Routing, take the following steps:

1. Check if the observed behavior is listed in the *Advanced Routing best practices* on page 917 topic.
2. Check if the observed issue is listed in the *Known Issues* topic of the *SecureTransport Release Notes*.
3. Restart the failing sever(s) or client(s).
4. Reproduce the issue with Debug Logging enabled if applicable. Refer to the *Debug logging* on page 948 topic for instructions.
5. Collect the debug log files, screen shots, or any other data related to the issue and contact Axway Support at support.axway.com.

Debug logging

SecureTransport stores log messages in the SecureTransport database. The contents of log messages can be viewed on the *Server Log* page. To access and view the *Server Log* page, select **Operations > Server Log**. For complete information on viewing, searching, and exporting logs, refer to *Server log* on page 304.

Log into a file

By default, all logs are saved in the SecureTransport database and can be explored from the SecureTransport Administration Tool. To save logs to a file, edit `$FILEDRIVEHOME/conf/tm-log4j.xml` and add the following lines after the last appender block.

```
<appender name="FileBasedLog"
class="com.tumbleweed.st.server.logging.DailyRollingFileAppender">
    <param name="File" value="/opt/TMWD/SecureTransport/var/logs/file-based_
log.log" />
    <param name="Append" value="true" />
    <param name="DatePattern" value="'.'yyyy-MM-dd" />
    <param name="RotateDirectory"
value="/opt/TMWD/SecureTransport/var/db/hist/logs" />
     <layout class="org.apache.log4j.PatternLayout">
         <param name="ConversionPattern" value="%d %p [%t] %c - %m%n" />
    </layout>
</appender>
```

Make sure to change the *File* and *RotateDirectory* values to meet your environment set-up.

When ready, restart the SecureTransport TM service for the change to take effect.

AR fails while copying the file to sandbox

Problem: In a cluster environment where one node uploads files and another node processes Advanced Routing, a route could fail with a transient error.

Possible cause: Once a file is uploaded in an AR subscription folder, it is copied from the subscription folder to the sandbox folder. If the shared storage synchronization does not happen on time, the second node does not "see" the file in the subscription folder uploaded on another node. As a result, a "no such file" error occurs and the route fails while copying the file to the sandbox folder.

Solution: In this case, retrying the failed operation more times or/and for longer intervals may solve the issue. SecureTransport uses an exponential backoff algorithm for retries: it increases the waiting time between the consecutive retries after each retry failure following the logic:

The first retry is after 1 x `retryTime`, the second retry is after 2 x `retryTime`, the third after 3 x `retryTime` and so on until the configured number of `retries` is reached.

where

- `retries` is the maximum number of retry attempts for failed AR file processing operations configured in the `com.axway.st.server.fs.ar.file.processing.retries` parameter (10 by default).
- `retryTime` is the delay of the first retry and the growth rate between attempts configured in the `com.axway.st.server.fs.ar.file.processing.retryTime` parameter. (100 ms by default).

With the default values, SecureTransport retries 10 times: the first retry happens in 100 ms, the second after 200, the third after 300, and so on. This sets a deadline of 5.5 seconds for SecureTransport to retry a failed AR file processing operation.
For example, if the number of retries is limited to 20, and the delay is set to 200 ms, the retries happen in 200, 400, 600, 800,...., 4000 ms. So, the total amount of time for retrying is 42 seconds.
The benefits of changing these parameters are dependent on the shared storage type and its performance

To customize the AR file processing retry logic, add the following in the `<FILEDRIVEHOME>/bin/start_tm_console` file and edit the values to fit your needs:

```
JAVA_OPTS="-Dcom.axway.st.server.fs.ar.file.processing.retries=10
$JAVA_OPTS"
```

```
JAVA_OPTS="-
Dcom.axway.st.server.fs.ar.file.processing.retryTime=100 $JAVA_
OPTS"
```

Configuring asynchronous MDN receipts with AS2 transfers

MDN (Message Disposition Notification) receipts serve to warrant data integrity and non-repudiation in the underlying protocol, in this case AS2. Asynchronous AS2 MDN receipts are communicated in separate request from transfers, and this behavior requires specific setup for correct processing in advanced routes. It is possible to use Advanced Routing (AR) for AS2 file transfers using asynchronous MDN receipts but the available options require special out-of-the-box approaches which serve as *workarounds*. To better understand the logic of each workaround, it is important to understand where the concepts in AR and asynchronous exchange of MDN receipts differ and where they intercept.

AS2 MDN receipts overview

The AS2 protocol requires a bi-directional partnership to be created: you must define the partner's server on your side, and the partner defines your server on theirs. This creates several use cases with this partnership and the AS2 MDN receipts configuration differs depending on the actual usage.

It is possible to use the partnership only in one direction - to send files to a partner or receive files from them (files that partner sends you). In this case the AS2-MDN is configured only for one side of the partnership.

For two-way, bi-directional communication between partners, the asynchronous AS2-MDN receipts have to be configured on both ends, for both inbound and outbound directions.

The asynchronous AS2-MDN receipt is sent in a separate HTTP or HTTPS TCP/IP connection and is similar to an inbound transfer from a partner.

SecureTransport Applications for AS2 transfers

In SecureTransport, the setup that handles AS2 transfers can be an instance of Site Mailbox, the Basic Application or the Advanced Routing application types. A user account must be subscribed to either of these applications to be able to send / receive files over the AS2 protocol.

AR uses Route setup for outbound transfers

With Advanced Routing, the configuration for outbound transfers is part of the Routes, not the Subscription. This presents a problem with AS2 transfers and the asynchronous MDN receipts due to the way SecureTransport relates the received receipts to the transfers: via the Subscription.

In the cases with e.g. Site Mailbox and Basic Application, the Subscription holds the configuration for the outbound transfers, so when SecureTransport receives a MDN, it can relate to the proper subscription and validate the MDN. With Advanced Routing, however, when a file is sent to partner via AS2 in a Route, and the MDN is returned by the partner, SecureTransport is unable to locate the Subscription the MDN belongs to and throws an error:

```
org.openas2.partner.PartnershipNotFoundException: AS2 site <AS2-sitename>
is not used for sending in any subscription.
```

This is a direct consequence of the design of the Advanced Routing. However, this behavior can be fixed using special scenarios in which you can combine AR with other applications to achieve AS2 transfers when asynchronous MDN receipts are required.

- Scenario 1: Combine AR with Basic application (outbound transfers only)
- Scenario 2: Combine AR with two Basic application instances (one for inbound and one for outbound transfers)
- Scenario 3: Combine AR with both SiteMailbox application (for both inbound and outbound transfers)

Scenario 1: Combine AR and Basic application for outbound transfers

This approach uses a combination of an Advanced Routing instance and one Subscription to the Basic Application. Configure Advanced Routing to receive files and send them to an AS2 Site. A dummy Basic Application will be added (and subscribed to a different folder) to facilitate correct MDN processing for outbound transfers in AR. In essence, the Advanced Routing application will be used to send the files, while the Basic Application will only be used for receiving the asynchronous MDN receipts.

Setup specifics

With this setup, you must configure:

- One AS2 Transfer Site (in the user account).
- An Advanced Routing instance with a Route that uses an AS2 Transfer Site to send the files in a Send To Partner step. In the subscription to this application, you must set that AS2 Transfer Site in the **Automatically retrieve files from** option. The Subscription must use a dedicated Subscription folder.
- A Basic application with a the subscription that contains the following settings: **Send files directly to** the same AS2 Transfer Site. The Subscription must use another Subscription folder (different from the one above).

Note Even though the AS2 Site is selected in the **Send files directly to** Subscription option, it is not practically used to send files.

Use case

This setup is good only for outbound transfers with asynchronous AS2-MDN. If your partner sends you an AS2 message (i.e. a file) you will return it back to them as the Route will be triggered from the AR subscription. This problem can be avoided if the route in the subscription sends the file to an

internal server instead of to the partner AS2 Transfer Site (in the Advanced Routing Send To Partner step). If you wish to be able to send files outbound with this use case, you need another Advanced Routing instance with a route that uses an AS2 Transfer Site to send the files in a Send To Partner step, but without specifying **Automatically retrieve files from** Subscription option.

Scenario 2: Combine AR and Basic application for both inbound and outbound transfers

This approach is similar to the one from above with outbound transfers. This time you must also configure another Basic application for inbound transfers.

Basically, here you use Advanced Routing in one Subscription, and two (dummy) Subscriptions with Basic Application. Each of the three is subscribed to a separate folder once again. The AR is used to do the actual file transfers outbound, while one of the BA Subscriptions is used to receive the files, while the other one is taking care of receiving the asynchronous MDN receipts and "bridging the gap" between the MDN receipts and the Subscriptions.

Setup specifics

With this setup, you must configure:

- One AS2 Transfer Site (in the user account).
- An Advanced Routing instance with a Route that uses an AS2 Transfer Site to send the files in a Send To Partner step. The Subscription must use a dedicated Subscription folder.
- One "outbound" Basic application that uses the same AS2 Transfer Site. In the subscription to this application, you must set that AS2 Transfer Site in the **Send files directly to** option. The Subscription must use a second, different Subscription Folder.
- One "inbound" Basic application, that uses the same AS2 Transfer Site. In the subscription to this application, you must set that AS2 Transfer Site in the **Automatically retrieve files from** option. The Subscription must use a third, different Subscription folder.

Use case

This setup is good for both inbound and outbound transfers with asynchronous AS2-MDN.

Scenario 3: Combine AR for outbound and SiteMail for inbound transfers

This approach combines the use of Advanced Routing with Site Mailbox application to achieve for both inbound and outbound transfers.

Basically, here you use Advanced Routing in one Subscription. A dummy Site Mailbox application will be added (and subscribed to a different folder) to facilitate correct MDN processing in AR. In essence, the Advanced Routing will be used to send files and the Site Mailbox application will only be receiving the files and the asynchronous MDN receipts.

Setup specifics

- One AS2 Transfer Site (in the user account).
- An Advanced Routing instance with a Route that uses an AS2 Transfer Site to send the files in a Send To Partner step. The Subscription must use a dedicated Subscription folder.
- A Site Mailbox application, that uses the same AS2 Transfer Site. In the subscription to this application, you must select that AS2 Transfer Site in both the **Send files directly to** and **Automatically receive files from** Subscription options. The Subscription must use a second, different Subscription Folder.

Use case

This setup is good for both inbound and outbound transfers with asynchronous AS2-MDN.

AS2 transfers 14

Axway SecureTransport supports AS2 (Applicability Statement 2) is the industry standard for Internet-based data exchange.

Use the SecureTransport AS2-certified solution to exchange data with any trading partner using an AS2-interoperable solution over the Internet. AS2 simplifies communication by reducing the number of technologies an organization must support and manage. It would be cost prohibitive for small business partners to exchange data electronically with large organizations that use a different data transport standard. The AS2 standard allows organizations, both large and small, to implement one solution for data exchange with all business partners using an AS2 solution.

The AS2 standard secures data with S/MIME (Secure/Multipurpose Internet Mail Extensions) over HTTP (Hypertext Transfer Protocol) or HTTPS (secure HTTP over SSL), also using MDN (Message Disposition Notification). AS2 provides synchronous, real-time transmission of data with immediate message delivery notice.

Note In Windows, file names of files transferred using the AS2 protocol are limited to 255 characters.

The following topics describe the SecureTransport AS2 implementation:

- *AS2 implementation* on page 954
- *Synchronous and asynchronous receipts* on page 955
- *AS2 and application framework: Architecture and workflow* on page 955
- *SecureTransport AS2 server: Setup overview* on page 956

AS2 implementation

Companies that conduct Business-to-Business (**B2B**) Electronic Commerce can use SecureTransport Server to send business documents to their business partners using the AS2 protocol.

The SecureTransport AS2 server provides security by utilizing encryption and signing. The server sends a document that is signed and encrypted to the partner using digital certificates that are agreed upon between the server and the target partner.

The partner checks the signature of the document and sends a signed MDN receipt to acknowledge that the transfer succeeded. MDN is an Internet messaging format used to transmit a receipt. MDN is used interchangeably with receipt. MDN is a receipt. This MDN signature is used to prove that the original document was sent from the SecureTransport AS2 server to the partner in a process called non-repudiation.

Note The use of signing, encryption, and MDN receipts are optional AS2 features that are decided when businesses enter into a partnership.

The following topics describe the SecureTransport AS2 implementation:

- *Synchronous and asynchronous receipts* on page 955
- *AS2 and application framework: Architecture and workflow* on page 955
- *SecureTransport AS2 server: Setup overview* on page 956

Synchronous and asynchronous receipts

A synchronous receipt is returned to the sender during the same HTTP session as the sender's original message. An asynchronous receipt is returned to the sender on a different communication session than the sender's original message session.

The synchronous receipt is sent as an HTTP response to an HTTP POST or as an HTTPS response to an HTTPS POST. This form of AS2-MDN is called synchronous because the AS2-MDN is returned to the originator of the POST on the same TCP/IP connection.

The asynchronous AS2-MDN is sent on a separate HTTP or HTTPS TCP/IP connection. Logically, the asynchronous AS2- MDN is a response to an AS2 message. However, at the transfer-protocol layer, assuming that no HTTP pipe lining is used, the asynchronous AS2-MDN is delivered on a unique TCP/IP connection, distinct from that used to deliver the original AS2 message. When handling an asynchronous request, the HTTP response MUST be sent back before the MDN is processed and sent on the separate connection.

When an asynchronous AS2-MDN is requested by the sender of an AS2 message, the synchronous HTTP or HTTPS response returned to the sender prior to terminating the connection *must* be a transfer-layer response indicating the success or failure of the data transfer. The format of such a synchronous response *may* be the same as that response returned when no AS2-MDN is requested.

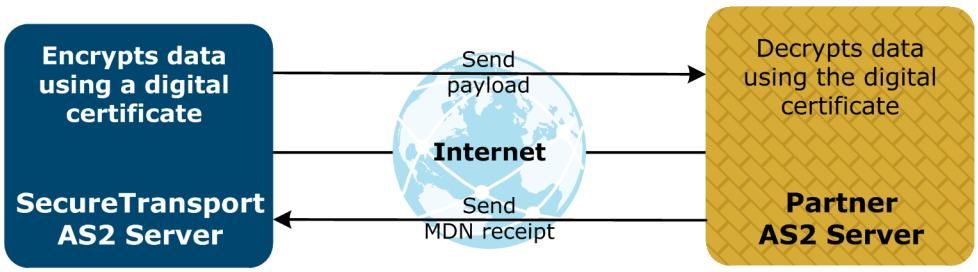


Figure 10. AS2 receipt

AS2 and application framework: Architecture and workflow

AS2 transfers can be handled by an AS2 application, which is an instance of the generic Site Mailbox application type. The AS2 Site Mailbox application can perform inbound and outbound transfers from and to the same AS2 site. To this end, the respective account is subscribed to the AS2 Site Mailbox

application and the subscription is associated with the AS2 site that is set up during the definition of the transfer site of the account. The application outgoing and incoming subfolders are called by default `outbox` and `inbox`.

Some basic application framework concepts, relating to the AS2 implementation in SecureTransport, are outlined here.

The following topics describe the architecture and workflow of AS2 and the application framework:

- *Application for AS2* on page 956
- *AS2 site* on page 956

Application for AS2

The particular AS2 application that handles AS2 transfers can be an instance of the Site Mailbox application type or the Basic or Advanced Routing application types. To be able to transfer files over the AS2 protocol, the user account must be subscribed to the AS2 application and the subscriptions must have the AS2 site defined.

The AS2 application must have an outgoing subfolder `outbox` and an incoming subfolder `inbox`.

AS2 site

AS2 partnership holds a description of local and remote parties which participate in AS2 transfers. Besides identification information (local and remote IDs and remote address), the partnership holds information about data transformation of payload and MDN requirements.

The SecureTransport architecture, implemented by the application framework, introduces the site concept. A SecureTransport site has all the necessary attributes to connect to the AS2 site and transfer the contents. The only partnerships items that are not a part of the SecureTransport site specification are the following:

- **Subfolder** – an attribute of subscription between the AS2 user account and the AS2 Site Mailbox application.
- **Username** – an attribute of the user account for AS2.

Note AS2 site does not support server-initiated inbound transfers (server pull).

For details, see *Manage applications* on page 757.

SecureTransport AS2 server: Setup overview

This topic outlines the overall steps required to set up SecureTransport for AS2 transfers. To setup SecureTransport Server for AS2, complete these steps:

1. Configure the AS2 server control settings. See *Manage the AS2 server* on page 255.
2. Configure the AS2 settings. See *Manage the AS2 server* on page 255.
3. Configure an HTTP proxy (optional). See *Specify proxy settings in a network zone* on page 222.

4. Start Transaction Manager and AS2 servers. See *Server control* on page 250.
5. Create a SiteMailbox application or a Basic or Advanced Routing application. See *Manage applications* on page 757.
6. Create a user account. See *Create a user account* on page 456.
7. In the user account, create a AS2 transfer site using the AS2 protocol. During this step you specify the AS2 local and remote sites in the transfer site definition. See *AS2 transfers* on page 954.
8. In the user account, create a subscription to the `SiteMailbox` application or to the Basic or Advanced Routing application and specify the AS2 transfer site. See *Subscribe an account to an application* on page 607.

File services interface transfers 15

A developer can use the Axway SecureTransport file services interface feature to implement a protocol that can use a shared file system and a transferred metadata file.

The following topics describe file services interface transfers:

- *File services interface overview* on page 958
- *Receive files using a file services interface protocol* on page 959
- *Send files using a file services interface protocol* on page 963

File services interface overview

For SecureTransport to receive a file using the file services interface, the external system must copy the file into the shared file system. The external system then sends the parameters for the transfer in the metadata file using another protocol.

To perform a file services interface transfer, the external server:

1. Copies the file to transfer to a location in the shared folder.
2. Construct a metadata file that specifies the parameters of the transfer.
3. Upload the metadata file into the subscription folder of an application of type File Transfer via File Services Interface.

The SecureTransport Server:

1. Reads the specification of the transfer from the metadata file.
2. Copies the transferred file from the shared directory to the locations specified in the metadata file.
3. Deletes the metadata file.
4. Deletes the transferred file from the shared directory, if specified in the metadata file.

When SecureTransport sends a file using the file services interface, it calls a connector process configured by the developer which pushes the file to the remote server.

Receive files using a file services interface protocol

For SecureTransport to receive files sent by another system using a file services interface protocol, you must set up access to a shared directory, create an application, and subscribe an account to that application.

1. Determine which shared directory the systems are to use to transfer the files and make it accessible from both systems.
2. Perform the procedure in *Create a File Transfer via File Services Interface application* on page 768.
3. Create or identify an account to receive the metadata files from the other system. For details, see *Create a user account* on page 456.
4. Subscribe that account to the file services interface application. For details, see *Subscribe an account to an application* on page 607.

When the remote system transfers the metadata file to the subscription folder, the file services interface application reads it and processes the transferred file based on its contents.

The following topics describe the metadata file and the location of the transferred file:

- *Metadata file* on page 959 - Lists and describes the elements in the XML metadata file.
- *Location of the transferred file* on page 962 - Describes the location of the transferred file.

Metadata file

The metadata file is an XML file that contains a `Transfer` element. The elements in the following table must be included in the `Transfer` element unless noted as optional:

Element	Description	Valid values	Notes
`SourceFileLocation`	Path to the transferred file	Full path name or path relative to `RemoteSharePath`	See *Location of the transferred file* on page 962.
`RemoteSharePath`	Path to the shared directory on the remote system	Full path name	Optional. SecureTransport uses this to determine the location of the transferred file. See *Location of the transferred file* on page 962.

Element	Description	Valid values	Notes
`LocalSharePath`	Path to the shared directory on the SecureTransport system	Full path name	Optional. Optional for transfers to SecureTransport. SecureTransport uses this to determine the location of the transferred file. See *Location of the transferred file* on page 962.
`CycleID`	Processing cycle identifier for the file transfer	Any valid cycle ID	SecureTransport uses this cycle ID in events reported to Axway Sentinel.
`Protocol`	Name of a file services interface protocol	Any protocol defined in the file services interface protocol registry	SecureTransport displays the corresponding display name in Protocol column of the *File Tracking* page and in events it sends to Axway Sentinel.
`Mode`	File transfer mode	`A` for ASCII or `I` for binary	
`Recipients`	Container for `Recipient` elements	N/A	Optional. Contains any number of `Recipient` elements.
`Recipient`	A recipient for the file	N/A	Optional. Contains a `Name` element and, optionally, a `Path` element

Element	Description	Valid values	Notes
`Name`	Login name of a SecureTransport account to receive the file	Any existing account login name	
`Path`	Path to the directory where SecureTransport copies the file, relative to the account home folder	Path to any directory in the home folder of the named account	Optional. The default is the home folder of the account.
`Parameters`	Container for `Parameter` elements	N/A	Optional. Contains any number of `Parameter` elements.
`Parameter`	A parameter	N/A	Optional. Contains a `Key` element and, optionally, a `Value` element.
`Key`	Key ID for the parameter	Any string	
`Value`	Value of the parameter	Any string	Optional.

The following is an example of a metadata file:

```
<?xml version="1.0" encoding="UTF-8"?>
<Transfer>
   <SourceFileLocation>/opt/shared/incoming/report-20110704
      </SourceFileLocation>
   <CycleId>2162164</CycleId>
   <Protocol>T3Direct</Protocol>
   <Mode>I</Mode>
   <Recipients>
      <Recipient>
         <Name>acctng</Name>
         <Path>/incoming/reports</Path>
      </Recipient>
```

```
         <Recipient>
         <Name>audit</Name>
      <Path>/incoming/check</Path>
      </Recipient>
   </Recipients>
   <Parameters>
      <Parameter>
         <Key>status</Key>
         <Value>complete</Value>
      </Parameter>
   </Parameters>
</Transfer>
```

Location of the transferred file

For files pushed to SecureTransport from a remote system, use `SourceFileLocation` and optionally `RemoteSharePath` and `LocalSharePath` to specify the location of the transferred file:

- If `RemoteSharePath` or `LocalSharePath` is not specified, `SourceFileLocation` is the location of the transferred file on the SecureTransport system.
- If `RemoteSharePath` and `LocalSharePath` are specified and `SourceFileLocation` starts with `RemoteSharePath`, then SecureTransport replaces `RemoteSharePath` with `LocalSharePath` to determine the location of the transferred file on the SecureTransport system.
- If `RemoteSharePath` and `LocalSharePath` are specified and `SourceFileLocation` does not start with `RemoteSharePath`, then SecureTransport concatenates `LocalSharePath` and `SourceFileLocation` to determine the location of the transferred file on the SecureTransport system.

For files pushed to a remote system from SecureTransport, `LocalSharePath` must be specified. Use `SourceFileLocation` and optionally `RemoteSharePath` to specify the location of the transferred file:

If `RemoteSharePath` is specified, SecureTransport concatenates `LocalSharePath`, a unique directory name, `RemoteSharePath`, a unique file prefix, and `SourceFileLocation` to determine the location of the transferred file on the SecureTransport system.

If `RemoteSharePath` is not specified, SecureTransport concatenates `LocalSharePath`, a unique directory name, a unique file prefix, and `SourceFileLocation` to determine the location of the transferred file on the SecureTransport system.

Send files using a file services interface protocol

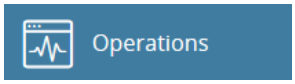
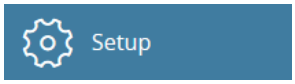
For SecureTransport to send files to another system using a file services interface protocol, you must create a transfer site for a file services interface protocol, and subscribe to an application that sends files to that site.

1. Create or identify an account to send files to the other system. For details, see *Create a user account* on page 456.
2. Create a transfer site in that account that references the file services interface protocol. For details, see *File services interface protocol transfer sites* on page 508.
3. Subscribe that account to an application configured to send files to that transfer site. For details, see *Subscribe an account to an application* on page 607.

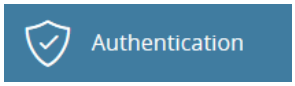
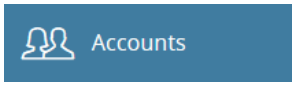
When the application sends a file to the transfer site, SecureTransport finds the information for the protocol in the protocol registry and calls a program configured for the protocol to perform the transfer.

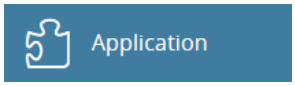
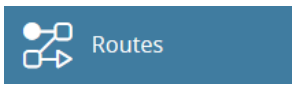
Appendix A: Administration Tool features checklist

Most Administration Tool features are present in Axway SecureTransport Server, but not all of those are available in the Administration Tool for SecureTransport Edge. The following table lists all available features within the Administration Tool for both SecureTransport Edge and SecureTransport Server.

Administration Tool features		SecureTransport Edge	SecureTransport Server
Operations Menu 		P	P
	Server Control	P	P
	Cluster Management	P	P
	Server Usage Monitor	P	P
	File Tracking	—	P
	Server Log	P	P
	Audit Log	P	P
	Server Configuration	P	P
	Support Tool	P	P
Setup Menu 		P	P
	Certificates	P	P
	FTP Settings	P	P

Administration Tool features	SecureTransport Edge	SecureTransport Server
AS2 Settings	P	P
SSH Settings	P	P
Admin Settings	P	P
PeSIT Settings	P	P
AdHoc Settings	—	P
Database Settings	P	P
Central Governance	—	P
Axway Sentinel/DI	—	P
Server License	P	P
Allowed ST Servers	P	—
Command Logging	P	P
Transfer Logging	P	P
Holiday Schedule	—	P
Mail Templates	—	P
Miscellaneous	P	P
ICAP Settings	—	P
TM Settings	—	P
File Archiving	—	P
Network Zones	P	P

Administration Tool features	SecureTransport Edge	SecureTransport Server
Address Books	—	P (If enabled on the *Server Configuration* page.)
Authentication Menu 	P	P
Login Settings	P	P
LDAP Domains	—	P
SiteMinder Settings	—	P
User Type Ranges	—	P (UNIX-based servers only)
Home Folders	—	P
Accounts Menu 	P	P
User Accounts	—	P
Unlicensed Accounts	—	P
Service Accounts	—	P
Import/Export	—	P
Administrators	P	P
Change Password	P	P
Manage Roles	—	P
Account Templates	—	P
System	—	P

Administration Tool features		SecureTransport Edge	SecureTransport Server
	Business Units	—	P
	Active Users	—	P
Access Menu		P	P
	User Classes	—	P
	Secure Socket Layer	P	P
	Virtual Groups	—	P
	Restrictions	—	P
	FTP Commands	P	P
	Admin Access Control	P	P
	Server Access Control	—	P
	Access Rules	P	P
	Login Restrictions	—	P
Application 		—	P
	Application	—	P
Routes 		—	P
	Route Packages	—	P

Appendix B: Troubleshoot common problems

The following topics discuss the most common issues that can occur when using SecureTransport. If you are still having issues after following the procedures in this topic, contact Axway Global Support for further assistance. For more information, see *Get more help* on page 31.

- *Communication problems* on page 968
- *Servers do not start* on page 970
- *Cannot log in as a client* on page 972
- *FTP does not work through the firewall* on page 976
- *PeSIT file transfers fail over TLSv1 Legacy for certain ciphers* on page 977 - Provides how-to instructions for eliminating cipher problems with PeSIT file transfers from a MFT product to SecureTransport over TLSv1 Legacy.
- PeSIT file transfer from SecureTransport to another MFT product fail over TLSv1 Legacy for certain ciphers - Provides how-to instructions for eliminating cipher problems with PeSIT file transfers from SecureTransport to another MFT product over TLSv1 Legacy.
- *Performance issues* on page 978 - Provides procedures for troubleshooting performance issues.
- *Troubleshooting I/O problems* on page 981 - Provides procedures for troubleshooting I/O issues on GlusterFS.

Communication problems

When the SecureTransport Server and the SecureTransport Edge are unable to communicate with each other, you can follow the procedures below. The main symptom of a communication problem is the inability to log into the server from the client. Each topic explains how to troubleshoot the system to determine if you are experiencing one of these common problems. Make sure that you check each item in the order listed.

1. **Clock Settings** – Verify that the clock settings for the servers are correct.
2. **Trust Establishment** – Check the log files for errors that can occur between SecureTransport Server and SecureTransport Edge
3. **Connectivity** – Make sure that the correct IP addresses are listed.

The following topics provide lists of what to check for communication problems:

- *Clocks out of sync* on page 969 - Provides a list of what to check for clocks out of sync issues.
- *Trust establishment issues* on page 969 - Provides a list of what to check for trust establishment

issues.

- *Connectivity* on page 970 - Provides a list of what to check for connectivity issues.

Clocks out of sync

If the clock on both the SecureTransport Server and SecureTransport Edge are out of sync, the two servers might not be able to communicate correctly. Verify that both systems are set for the same time and date.

If you are using the Windows platform, the SecureTransport Edge might not be in the same domain, but in a workgroup instead. If this is the case, the SecureTransport Edge does not use the Windows Time Service and you must manually verify that the clocks are in sync.

When using a UNIX-based platform, make sure that the time formats and time zones are the same. If they are not the same, the imported CA certificate might have a different "valid from" date and time, and are considered invalid until the server reach the listed date and time.

For an Enterprise Cluster (EC), the clocks of all servers must be synchronized.

Trust establishment issues

If the certificates are not configured correctly for both the SecureTransport Server and the SecureTransport Edge, trust might not be properly established between the two systems. Try the following procedures to verify your trust settings.

- To establish trust between SecureTransport Server and SecureTransport Edge, you need to exchange Trusted CA certificates. Exchanging certificates consists of:
    - Saving the CA certificate for SecureTransport Server to a file on a local system and importing the file to the SecureTransport Edge using the SecureTransport Administration Tool.
    - Saving the CA certificate for SecureTransport Edge to a file on a local system and importing the file to the SecureTransport Server using the SecureTransport Administration Tool.

To export or import a CA certificate, see *Manage trusted CAs* on page 61.

Common certificate errors

If certificates are not correctly imported or the certificate has expired, you might see ERROR-level entries regarding SSL handshaking in the server log on the SecureTransport Server such as:

```
com.valicert.brules.eventmonitor - SSL handshake failed
```

Specific issues that can cause an error include:

- SecureTransport Server CA certificate is not imported into Edge.
- SecureTransport Edge CA certificate is not imported into Server.

- SecureTransport Server CA certificate is expired.
- SecureTransport Edge CA certificate is expired.
- SecureTransport Server certificate is expired.
- SecureTransport Edge certificate is expired.

Use **Setup > Certificates** to view the certificates and monitor expiration dates on a regular basis.

Connectivity

Communication issues can arise when IP addresses are not recognized properly. Use the following procedures to check your connectivity settings.

- Make sure that the correct IP addresses are listed for the SecureTransport Server and SecureTransport Edge in the `hosts` file. For details, see *Incorrect host name and IP address in the host file* on page 971.
- Make sure that the network zones on the SecureTransport Server and SecureTransport Edge are correct and consistent.
- Make sure that the SecureTransport Server is listed as an allowed server on the SecureTransport Edge.
- Make sure that the `Streaming.TrustedAliases` server configuration parameter is set correctly. For more information, see *Secure the communication between the TM server and the protocol servers* on page 225.
- Make sure that the firewall is configured correctly. For more information on configuring the firewall, see *Firewall settings* on page 1008.

Servers do not start

If a SecureTransport protocol or TM server does not start, check the following topics to troubleshoot the problem. Make sure you check each item in the order listed.

1. **SSL Certificate** – Verify that the SSL certificate is properly configured for the server.
2. **Conflicting Port Numbers** – Verify that the port number assigned to the server is not in use elsewhere.
3. **Host Name** – Look in the server host file for an entry for each host name with the correct IP address.

The following topics provide lists of what to check for when servers do not start:

- *No SSL certificate configured for the server* on page 971 - Provides how-to instructions for verifying that a SSL certificate is configured for the server.
- *Conflicting port numbers* on page 971 - Provides how-to instructions for verifying port assignments and eliminating conflicting port assignments.

- *Incorrect host name and IP address in the host file* on page 971 - Provides how-to instructions for verifying IP address and host name assignments.

No SSL certificate configured for the server

Verify that the SSL certificate configured for the server has not expired. If the certificate is valid, use the following procedure to make sure that the SSL certificate is properly configured for the server that is not starting.

1. Select **Operations > Server Control**.
2. For each server, select an appropriate certificate alias from the **SSL Key Alias** list.
3. At the bottom of the page, click **Update**.
4. Restart each server for which you changed the certificate.

In a synchronized configuration, the certificate aliases must match on the primary and the secondary nodes, or after synchronizing, the link between the server and the certificate is broken.

Conflicting port numbers

Make sure the port number assigned to the server is not in use elsewhere, such as the operating system SSH server using port 22. To check the port, open the SecureTransport Administration Tool and select **Operations > Server Control**. Verify that the ports assigned to the FTP Server, the HTTP server, the AS2 Server, the SSH server, and the PeSIT Server are not in use by other servers.

Incorrect host name and IP address in the host file

Verify that the correct IP addresses are in the `hosts` file for each system running SecureTransport. Look in the hosts file for an entry for each host name with the correct IP address. This file is located in the `/etc` directory on UNIX-based systems. The `hosts` file can be found in the `WINNT\System32\drivers` directory on Windows Server.

Entries in the hosts file have the following format:

```
127.0.0.1 localhost.localdomain localhost
```

If the entry is not present, create it. If there is an entry, make sure that it has the correct IP address listed. Entries should have the primary alias for each IP address first, followed by the aliases for all other interfaces. You should also verify that your DNS is set up correctly. For more information, see *DNS settings* on page 979.

Cannot log in as a client

If you attempt to login to SecureTransport and the login fails despite using a correct user name and password, try the following topics to troubleshoot the problem. Make sure that you check each item in the order listed.

1. **License Issues** – Verify that the required licenses are installed and current.
2. **Connection to Server** – Verify that the client system can communicate with the server and that no other client is experiencing a problem.
3. **Authentication** – Check the LDAP or SiteMinder settings.
4. **LDAP** – Verify that the LDAP configuration is set correctly.
5. **Unable to use file system commands such as ls** – make sure that you have plenty of hard drive space available.
6. **Unable to log in to SecureTransport Edge, but can log in to SecureTransport Server** – Make sure that the certificates for Edge and Server match.
7. **Client certificate authentication fails** – Make sure that you do not have two Root CA certificates in the "Trusted Certificates" keystore with an identical DN specified.
8. **Logged in to client with reduced functionality** – Make sure that you are using the required browser and that the required features are installed and enabled.
9. **Session terminates due to CSRF protection** – Add the client to the white list.

The following topics provide procedures for troubleshooting client log in problems:

- *License issues* on page 973 - Provides how-to procedures for troubleshooting license issues.
- *Connectivity to server failed* on page 973 - Provides how-to procedures for troubleshooting connectivity issues.
- *SiteMinder issues* on page 973 - Provides how-to procedures for troubleshooting SiteMinder issues.
- *LDAP issues* on page 974 - Provides how-to procedures for troubleshooting LDAP issues.
- *File system commands not functional* on page 974 - Provides how-to procedures for troubleshooting file system command functionality issues.
- *Cannot log in to SecureTransport Edge* on page 975 - Provides how-to procedures for troubleshooting SecureTransport Edge log in issues.
- *Client certificate authentication fails* on page 975 - Provides how-to procedures for troubleshooting client certificate authentication issues.
- *Logged in to client with reduced functionality* on page 975 - Provides how-to procedures for troubleshooting client reduced functionality issues.
- *Session terminates due to CSRF protection* on page 975 - Provides how-to procedures for troubleshooting session termination issues due to CSRF protection.

License issues

If you get an error indicating that the license is expired or that there is no license available for ad hoc users, verify that the license is installed and within the validity period. Use the following procedure to verify that your license is still valid.

To view server licenses:

1. Open the SecureTransport Administration Tool and select **Setup > Server License**.
2. Verify that the license is installed and not expired by checking the **Core Server License** for the FTP and HTTP servers, user accounts, and ad hoc users and the **Features License** for AS2, SSH, and Connect:Direct protocols and the SiteMinder feature.
3. If your license has passed the expiration date, contact Axway Global Support to renew it. For details, see *Get more help* on page 31.

For each license type, the validity period is given in the **Valid from** and **Valid to** fields. Check the following items if your license is valid.

- Make sure that you are using the correct IP address to connect to the server from the client.
- Make sure that your server's clock is set correctly.
- If you experience a license error, log in to the SecureTransport Administration Tool, select **Operations > Server Log**, and look in the following log entries for the exact error code and description.
    - AS2: AS2D
    - FTP or FTPS logins (secure or nonsecure): FTPD
    - HTTP or HTTPS logins: HTTPD
    - PeSIT transfer: TM
    - SiteMinder: TM
    - SSH: SSHD
    - Transaction Manager: TM

Connectivity to server failed

SecureTransport Server and SecureTransport Edge must be able to communicate with each other properly. Make sure that the following settings are configured correctly.

- **DNS Settings** – For details, see *DNS settings* on page 979.
- **Firewall** – For details, see *Firewall settings* on page 1008.

SiteMinder issues

Check the SiteMinder settings to make sure that authentication is configured correctly.

To view the SiteMinder settings:

1. Open the SecureTransport Administration Tool on the SecureTransport Server and select **Setup**.
2. Select **SiteMinder Settings**. Verify that the following settings are correct: IP Address, Authorization Port, Authentication Port, Accounting Port, Agent Name, Shared Secret, Maximum Connections, Connection Timeout, File Storage Root Path, Default Home Directory, Default Local User ID, and Default Local Group ID.

LDAP issues

Common LDAP problems are incorrect LDAP configuration, incorrect service account credentials, and an inability to access LDAP through the firewall. Check the following setting in the SecureTransport Administration Tool to troubleshoot problems:

- Make sure that the credentials LDAP can search through are correct for each user unable to login from the client. If the users are connecting to an Active Directory (AD) LDAP server, the Bind DN and Password need to be specified. AD does not allow anonymous binds. Verify that the user has the correct user name and password and is entering the correct information into the client.
- For Windows-based systems, make sure that the LDAP SysUser is set correctly to a local or domain user that has the necessary permissions on the directory. The LDAP SysUser must be present in the password vault.
- Make sure that the correct LDAP port, generally 389 or 3268, is available to SecureTransport in the firewall.
- Check that for each LDAP-based user, the settings allow the user to obtain the UID/GID (UNIX-based systems only), user type, and home directory either from the LDAP directory (using attribute mapping) or through the user defaults. Make sure that the user home directory exists and has the correct permissions. You can set up a login agent for this purpose.
- Make sure that you use the correct LDAP Protocol version. SecureTransport supports version 2 and version 3. Make sure that the LDAP server is the same version as the one selected in the SecureTransport Administration Tool on the *LDAP Server* page.
- Try using the `ldapsearch` command from the command line. If the command fails, you might have an incorrect search query or insufficient credentials.
- If you are not using attribute mapping, make sure that the home directory exists in the LDAP User Default and that the entry is enabled. For more information, see *LDAP logins* on page 427.

File system commands not functional

If you are unable to log in or file system commands such as `ls` or `dir` do not work correctly, the server might be low or out of disk drive space on the installation volume. Free up additional disk space and try logging in again.

Cannot log in to SecureTransport Edge

If you are unable to log in to a SecureTransport Edge, but you can log into the SecureTransport Server directly, make sure that the Internal CA certificate matches the local certificates created for the protocol servers.

Also make sure that your SecureTransport Server and SecureTransport Edge have exchanged certificates as appropriate.

Client certificate authentication fails

If you have two Root CA certificates in the "Trusted Certificates" keystore with an identical DN specified, you might not be able to log into SecureTransport. SecureTransport searches for the first certificate that matches the DN of the Certificate Authority. If a match is found, then SecureTransport does not continue to search. When two or more CA certificates with the same DN exist, the correct CA might never be selected.

Make sure that all CA certificates have unique DN values.

Logged in to client with reduced functionality

To get access to the full functionality of the following SecureTransport clients, you must use the listed web browser, have the listed features enabled, and have the related software installed.

For both the SecureTransport Browser Client and ST Web Client:

- The web browser must have JavaScript enabled.

For the SecureTransport Browser Client basic functionality:

- Supported web browsers are listed in *Axway and third-party software support* on page 39.

For the SecureTransport Browser Client Web Client Control:

- Supported web browsers are listed in *Axway and third-party software support* on page 39.

For the ST Web Client:

- Supported web browsers are listed in *Axway and third-party software support* on page 39.

Session terminates due to CSRF protection

SecureTransport implements token-based cross-site request forgery (CSRF) protection. This prevents a user who is logged in to a SecureTransport web client from causing unwanted modification of user data, such as uploading or deleting a file, by opening a malicious web page or clicking a crafted link in another browser tab or window. When the CSRF protection detects a violation, SecureTransport marks the session as expired and logs out the user.

If an HTTP client identifies itself with a User-Agent string, SecureTransport matches the string against a white list of clients represented by a Perl-compatible regular expression. If the User-Agent string matches, SecureTransport does not perform CSRF protection. By default, the white list is `(^SecureTransport|^Axway/SecureClient|^Axway/EndPoint|Java|^curl/|^Jakarta Commons\-HttpClient)`.

To configure a different white list, save the regular expression in the `Http.UserAgentWhiteList` server configuration parameter. To exclude another client from CSRF protection, add a pattern that matches the User-Agent string for that client to the regular expression. For example, to exclude Wget in addition to the clients in default, set the value of the `Http.UserAgentWhiteList` server configuration parameter to `(^SecureTransport|^Axway/SecureClient|^Axway/EndPoint|Java|^curl/|^Jakarta Commons\-HttpClient|^Wget)`. If the value of the `Http.UserAgentWhiteList` server configuration parameter is empty, SecureTransport uses the default white list.

FTP does not work through the firewall

If you are having a problem using FTP through a firewall, use the following topics to help you troubleshoot the problem. Make sure you check each item in the order listed.

1. **Firewall Rules** – Verify that the firewall rules open the ports specified for using FTP.
2. **Passive Port Range** – Make sure the passive port range is configured correctly.
3. **Check Point Firewalls** – Make sure you set up the Check Point firewall to use bidirectional transfers.

The following topics provide procedures for troubleshooting FTP protocol firewall issues:

- *Firewall rules prevent the port from opening* on page 976 - Provides procedures for troubleshooting port opening firewall rule issues.
- *Passive port range is not defined in the firewall* on page 976 - Provides procedures for troubleshooting port definition firewall issues.
- *Check Point firewall is not configured for bidirectional transfers* on page 977 - Provides procedures for troubleshooting Check Point firewall bidirectional transfer issues.

Firewall rules prevent the port from opening

Make sure the rules for your firewall open the ports specified for using FTP. For more information, see *Firewall settings* on page 1008.

Passive port range is not defined in the firewall

Configure the passive mode port range in your firewall if you are planning on using passive FTP. The passive range is defined on the SecureTransport Server and must be made available on the firewall. To set the passive range on the SecureTransport Server, open the SecureTransport Administration

Tool and select **Setup > FTP Settings**. Configure the port range in the *FTP Passive Mode* pane of the page.

Firewalls with no stateful inspection must make this port range explicitly available. Firewalls that support stateful inspection can define the port range dynamically. To ensure proper operation, the FTP control channel must not be encrypted. If you are using a third-party secure FTP client, use Clear Command Channel (CCC).

If you are using Axway Secure Client, you can use firewall-friendly Tunnel mode.

Note Because the Axway Secure Client firewall-friendly Tunnel mode uses SSL v3, you cannot use it for FTPS in FIPS transfer mode.

Check Point firewall is not configured for bidirectional transfers

The symptoms of incorrectly configured bidirectional FTP transfers include:

- The error message `message_info violated unidirectional connection` in the Check Point log viewer
- Bidirectional FTP data connections getting dropped

These symptoms can occur because bidirectional FTP data connections are not allowed by default. Bidirectional FTP data connections are not considered as safe since the data connection is interactive and the connection changes the basic way FTP works.

Check Point firewalls need to be configured to use bidirectional transfers. In the Check Point NG firewall (AI R55 and higher), set the FTP connection to FTP_BASIC. This allows bidirectional communications and sets the firewall to allow commands not terminated with a new line.

PeSIT file transfers fail over TLSv1 Legacy for certain ciphers

A change to CBC ciphers in SecureTransport made in response to CVE-2011-3389 causes older version of Transfer CFT and other PeSIT clients to fail to transfer files from and to a SecureTransport server over TLSv1 Legacy. These clients fail because they do have the update or have other deficiencies in their SSL implementations.

Note The following workarounds enable the file transfer between these clients and SecureTransport but both are considered insecure and using any is at your own risk.

Failed PeSIT file transfers to SecureTransport

To enable the transfer of files to SecureTransport, disable the fix in SecureTransport by adding the following Java option in `<FILEDRIVEHOME>/bin/start_pesitd`:

```
JAVA_OPTS="-Djsse.enableCBCProtection=false $JAVA_OPTS"
```

Failed PeSIT file transfers from SecureTransport

To enable SecureTransport to transfer files to such clients, disable the fix by adding the following Java option in <FILEDRIVEHOME>/bin/start_tm_console:

```
JAVA_OPTS="-Djsse.enableCBCProtection=false $JAVA_OPTS"
```

Performance issues

When SecureTransport performance is reduced from previous levels or is not consistent your expectations, use the checklist below to troubleshoot the issue and determine if performance can be improved. Make sure you check each item in the order listed.

1. Evaluate performance issues – Investigate factors that might result in reduced performance.
2. DNS Settings – Verify that the DNS settings for the servers are correct by using `nslookup` in Windows or UNIX-based systems.
3. Firewall Settings – Verify that the firewall is configured properly for SecureTransport and that no other application is also experiencing a firewall problem.
4. System Resources – Look at the memory and CPU usage for any other services running on the same computer.
5. Installation Drive – To avoid performance problems, always install SecureTransport on a local disk drive.
6. Log Level – Check the log level.

The following topics provide how-to procedures for evaluating and troubleshooting performance issues:

- *Evaluate performance issues* on page 979 - Provides how-to procedures for evaluating performance issues.
- *DNS settings* on page 979 - Provides how-to procedures for troubleshooting DNS settings issues.
- *Firewall issues* on page 980 - Provides how-to procedures for troubleshooting firewall issues.
- *Other services using to much CPU or memory* on page 980 - Provides how-to procedures for troubleshooting CPU and memory usage issues.
- *Installation on network drive* on page 981 - Provides how-to procedures for troubleshooting drive issues.
- *Debug log output slows computer* on page 981 - Provides how-to procedures for troubleshooting debug log output issues.

Evaluate performance issues

Before considering configuration changes to improve performance, investigate factors that might result in reduced performance. Consider the following factors:

- How many transfers have occurred during recent typical and peak transfer periods? Has the number of transfers increased from the levels before the performance problems were observed?
- How many concurrent users or partner sessions are transferring files during recent typical and peak transfer periods? Has the number of user or sessions increased from the levels before the performance problems were observed?
- Is your organization no longer meeting service level agreements with your customers?

If performance issues are due to increased workload, perhaps increasing slowly over time, evaluate implementing a cluster or adding a server to an existing cluster to accommodate the additional workload.

DNS settings

Try the following procedures to verify that your DNS settings are not causing performance to deteriorate.

- Verify that the DNS settings for the servers are correct by using `nslookup` in Windows or UNIX-based systems. If the `nslookup` returns an error you need to reconfigure your DNS settings. If `nslookup` times out, make sure that the firewall allows port 53 UDP/TCP.
- Reverse DNS lookups are used to resolve an IP address into a fully qualified domain name. The domain name is used for logging purposes and for applying access rules that specify a host name instead of an IP address. Reverse DNS lookups might cause server performance to deteriorate since a series of requests through the DNS name server tree is made each time.

  To disable reverse DNS lookups for the FTP, HTTP, and SSH servers:

  1. Open the SecureTransport Administration Tool in a web browser and log in as the administrator.
  2. Select **Setup > Miscellaneous**.
  3. For **Reverse DNS Lookups**, choose `Reverse DNS lookups disabled`.
  4. Click **Apply**.

  To disable DNS lookups for Administration Tool server:

  1. Open the SecureTransport Administration Tool in a web browser and log in as the administrator.
  2. Select **Operations > Server Configuration**.
  3. Search for the `Admin.ReverseDNSLookup` system configuration parameter.
  4. Click the Edit icon ( ) in the **Edit** column, type `Off` in the **Value** column, and click the Save icon ( ) in the **Edit** column.

5. Restart the server.

- If you need to use reverse DNS lookups, make sure that the DNS path is not blocked by a firewall. Firewalls can block the DNS path when SecureTransport is in the peripheral network (DMZ). Try one of the following workarounds to allow access through the firewall:
  - Allow SecureTransport access to port 53 TCP/UDP.
  - Include a hosts file entry for every computer using the Administration Tool.
  - Connect to the Administration Tool through a proxy, and put a host file entry for just the proxy.
- In some cases, SecureTransport performs NIS lookups for users and groups, even when real users are disabled in SecureTransport. If there is a large number of users defined in NIS, server performance can deteriorate. To work around the issue, take the computer out of NIS.

Firewall issues

To eliminate any possible firewall settings that can affect performance, check the following:

- Make sure the ports SecureTransport uses are set correctly. If your firewall uses passive mode, make sure that you are using Clear Command Channel (CCC) or Firewall Friendly mode.
- Verify that no other applications are experiencing problems with the firewall.
- The Transaction Manager has a timeout value that allows connections to close before the firewall can close them. Make sure the timeout setting in `<FILEDRIVEHOME>/brules/conf/brules.xml` on the SecureTransport Server is a lower value than the timeout setting for the firewall. Look for the following setting in the Event Monitor element in the file:

  ```
  <!-- single simple value, timeout in seconds -->
  <client timeout="900"/>
  ```

  Change the setting to be smaller than the value of the firewall timeout.

Other services using to much CPU or memory

One possible reason performance deteriorates can be caused by other services using too many system resources. Perform the following procedures to fine tune performance.

- Look at the memory and CPU usage for any other services running on the same computer. If you turn off all the SecureTransport services, but you still see high memory usage, you might need to add more memory or assign a dedicated memory amount to SecureTransport. If the CPU usage is still too high, you need to move some of the services to another computer or turn them off. If you can configure the services to use less CPU resources, do so.

Because SecureTransport is a CPU-intensive application, during peak demand times, it can consume most or all of the CPU resources. This can reduce the performance of other services. To provide

sufficient processor resources for SecureTransport and other services, allocate a computer with higher processing power to SecureTransport. For example, employ a computer with multiple processors.

Installation on network drive

The SecureTransport Server and Edge must access disk files and the database on disk for all file transfer and processing actions. If SecureTransport is installed on a network or shared drive, application performance depends on network throughput and processes from other computers accessing the drive.

SecureTransport installation on a network drive, regardless of its performance characteristics, is not supported. To avoid performance problems, always install SecureTransport on a local disk drive.

Debug log output slows computer

You might need to set the log level for one or more of the SecureTransport logs configured in files in the `<FILEDRIVEHOME>/conf/` directory to `debug` to produce a detailed log for problem isolation. If you leave a log set to `debug`, it can produce a very large volume of log output. Because this keeps the database and disk busy, it can affect the performance of all processes running on the computer.

- Always reset the log level after using `debug` to gather log information for problem isolation.
- Never set a log level to `debug` for routine operation.

Troubleshooting I/O problems

Problem summary: An I/O error may occur when a large number of write or read operations are happening simultaneously. As a result, SecureTransport may fail to retrieve file attributes or decrypt repository encrypted files when sending them outbound, for example. The issue is observed mainly in cluster environments with GlusterFS.

Possible cause: Read/write operations may require more time.

Solution: In this case, retrying failed read/write operations more times or/and for longer intervals may solve the issue. SecureTransport uses an exponential backoff algorithm for retries: it increases the waiting time between the consecutive retries after each retry failure following the logic:

The first retry is after 1 x `retryTime`, the second retry is after 2 x `retryTime`, the third after 3 x `retryTime` and so on until the configured number of `retries` is reached.
where

- `retries` is the maximum number of retry attempts for failed read/write operations configured in the `com.axway.st.server.fs.attributes.read.retries` parameter (10 by default).
- `retryTime` is the delay of the first retry and the growth rate between attempts configured in the `com.axway.st.server.fs.attributes.read.retryTime` parameter. (100 ms by default).

With the default values, SecureTransport retries 10 times: the first retry happens in 100 ms, the second after 200, the third after 300, and so on. This sets a deadline of 5.5 seconds for SecureTransport to retry a failed read/write operation.
For example, if the number of retries is limited to 20, and the delay is set to 200 ms, the retries happen in 200, 400, 600, 800,...., 4000 ms. So, the total amount of time for retrying is 42 seconds.
The benefits of changing these parameters are dependent on the shared storage type and its performance

To customize the read/write retry logic, add the following in the `<FILEDRIVEHOME>/bin/start_tm_console` file and edit the values to fit your needs:

```
JAVA_OPTS="-Dcom.axway.st.server.fs.attributes.read.retries=10
$JAVA_OPTS"
```

```
JAVA_OPTS="-Dcom.axway.st.server.fs.attributes.read.retryTime=100
$JAVA_OPTS"
```

Appendix C: FIPS transfer mode

For file transfers using the AS2 (SSL), FTPS, HTTPS, PeSIT (SSL, legacy SSL), or SSH (SFTP and SCP) protocols, you can restrict the Axway SecureTransport Server to use only FIPS 140-2 Level 1 certified cryptographic libraries. This requires the sender and the recipient (clients and partner servers) to use only approved algorithms, ciphers, and cipher suites and assures that the entire transfer is secure at FIPS 140-2 Level 1.

For a complete list of supported ciphers and algorithms that be used in FIPS mode, see *Advertised ciphers and cipher suites in FIPS mode* on page 984

As an administrator, you can customize the list of allowed TLS cipher suites or SSH ciphers and algorithms at the following levels:

- per protocol server (in the server settings). For more information about client-initiated transfers, see *Server control* on page 250.
- for server-initiated transfers through a specific transfer site (in the transfer site configuration)
- for server-initiated transfers over a specific protocol (via dedicated server configuration options)

  For more information about server-initiated transfers, see *Transfer sites* on page 494.

Note Because Axway Secure Client firewall-friendly Tunnel Mode uses SSL v3, you cannot use it for FTPS in FIPS transfer mode.

Also note, Oracle and IBM JREs might have different list of security ciphers so this will probably result in different list of ciphers on AIX.

The following topics describe the FIPS certified cryptographic libraries and list the FIPS compliant ciphers and cipher suites, supported by SecureTransport:

- *FIPS-certified cryptographic libraries* on page 983
- *Advertised ciphers and cipher suites in FIPS mode* on page 984

FIPS-certified cryptographic libraries

SecureTransport 5.4 uses the following cryptographic library in FIPS transfer mode:

- Security Builder® FIPS Java Module Version 2.8, FIPS 140-2 Validation Certificate No. 1637 – Used for all server-initiated and client-initiated transfers.

Advertised ciphers and cipher suites in FIPS mode

In Federal Information Processing Standard (FIPS) transfer mode, SecureTransport 5.4 advertises the following ciphers, cipher suites, or algorithms in the order given. The remote system must use one of them for the file transfer to succeed.

FIPS-compliant TLS cipher suites

In FIPS mode, SecureTransport supports the following ciphers suites for communication over FTPS, HTTPS, AS2, and PeSIT protocols:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

Note From the list of supported algorithms, some are considered as not secure enough and are listed in the `<FILEDRIVEHOME>/jre/lib/security/java.security` file. If you insist on using any of them, you must manually remove their corresponding entries under `jdk.tls.disabledAlgorithms` and restart the node.

FIPS-compliant ciphers and algorithms for SSH communication

In FIPS mode, SecureTransport supports the following ciphers and algorithms for the SSH daemon and server-initiated transfers:

FIPS-compliant ciphers

- aes256-cbc
- aes192-cbc
- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

FIPS-compliant key exchange algorithms

- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group-exchange-sha1

FIPS-compliant MAC algorithms

- hmac-sha256
- hmac-sha256@ssh.com
- hmac-sha512
- hmac-sha512@ssh.com
- hmac-sha1
- hmac-sha1-96
- hmac-sha2-256
- hmac-sha2-512

FIPS-compliant public key algorithms

- ssh-rsa
- ssh-dss
- x509v3-sign-rsa
- x509v3-sign-rsa-sha1

Appendix D: Command line utilities

The Axway SecureTransport Server includes several utility files that allow users to manually perform functions like installing a license file, stopping a server, and starting a server. These files are scripts on UNIX and batch files (`.bat`) on Windows. The utility files are located in the `<FILEDRIVEHOME>/bin` directory.

Utility files on page 987 provides a summary of the utilities and their functions.

Note If an alias is used to install SecureTransport, use the `-A` option for any other commands for the server on UNIX. For example, to stop all servers for a SecureTransport installation with an alias as `myserver` on UNIX, use the following command:

```
./stop_all -A myserver
```

On Windows, you do not need to use the `-A` option. Instead, use the following command:

```
stop_all
```

For instructions on how to control servers from the command line, refer to *Control the servers* on page 987

Control the servers

If a private key is specified for a server during installation and the server needs to be stopped or restarted, you must type the password for the private key. If the password is entered incorrectly during the boot process, use the Ctrl+C keyboard combination to stop the boot process and then restart the server.

Utility files

SecureTransport includes the utility files listed in the following table:

Utility file	Description
`bounce`	Bounces the SecureTransport protocol servers. If run on a primary server of a cluster, it will also bounce all the secondary servers.
`collect_ support_ information`	Collects information for Axway Global Support as specified on the *Support Tool Configuration* page.
`gencsr`	Generates a key pair and the associated certificate request file. Users can submit the CSR file to a CA to get a CA-issued certificate.

Utility file	Description
`log_export`	Export server log or File Tracking (transfer log) entries from the database in CSV or DBF format.
`mkadmin`	Adds a new administrator account or changes the password of an existing administrator account. Changes are automatically synchronized across all servers in a Standard Cluster or Enterprise Cluster, unless the `-sync=n` option is present.
`repconv`	Updates repository encryption by decrypting files encrypted in a previous version of SecureTransport and encrypting them for the current version. Can also change the cipher algorithm and certificate SecureTransport uses to encrypt files and decrypt files and folders. **Note** On Windows systems, the repconv tool cannot process files with special characters in their names (such as Japanese, Chinese, or Cyrillic characters). **Note** Starting with SecureTransport 5.4 Patch 32, Axway is deprecating "repconv" utility ability to convert any files encrypted by pre-5.2 SecureTransport releases to SecureTransport 5.2 (and later) repository encryption. After installing SecureTransport 5.4 Patch 32, users will no longer be able to convert files encrypted by pre-5.2 SecureTransport releases to SecureTransport 5.2 (and later) repository encryption. SecureTransport customers who still have files encrypted by pre-5.2 SecureTransport releases, are required to convert those to current SecureTransport repository encryption prior applying SecureTransport 5.4 Patch 32. The "repconv" utility decrypt and encrypt features continue to work as previously did with SecureTransport 5.4 Patch 32.
`show_ports`	Displays the ports on which the servers are configured to run.
Start scripts	
`start_admin`	Starts the Administration Tool server.
`start_all`	Starts all SecureTransport servers.
`start_as2d`	Starts the AS2 server.
`start_db`	Starts the embedded database server.
`start_ftpd`	Starts the FTP server.
`start_httpd`	Starts the HTTP server.

Utility file	Description
`start_pesitd`	Starts the PeSIT server.
`start_sshd`	Starts the SSH server.
`start_tm`	Starts Transaction Manager.
Stop scripts	
`stop_admin`	Stops the Administration Tool server.
`stop_all`	Stops all SecureTransport servers.
`stop_as2d`	Stops the AS2 server.
`stop_db`	Stops the embedded database server.
`stop_ftpd`	Stops the FTP server.
`stop_httpd`	Stops the HTTP server.
`stop_tm`	Stops Transaction Manager.
`stop_pesitd`	Stops the PeSIT server.
`stop_sshd`	Stops the SSH server.
Status scripts **Note** In order for the status scripts to work, you need to have the admin server up an running.	
`status_ftpd`	Checks the status of the FTP server.
`status_ socks`	Checks the status of the SOCKS5 proxy. Only available on Edge.
`status_httpd`	Checks the status of the HTTP server. The following example is applicable to `status_ftpd` as well: you can expect the same messages with either in the place of `status_httpd`. • `status_httpd` returns `'httpd is disabled'`, when all http listeners are disabled. • `status_httpd` returns `'httpd is functional'`, when at least one http listener is enabled, and it is functional. • `status_httpd` returns `'httpd is down'`, when at least one http listener is enabled, and it is stopped or it is not functional.

Utility file	Description
`status_as2d`	Checks the status of the AS2 server.
`status_pesitd`	Checks the status of the PeSIT server.
`status_sshd`	Checks the status of the SSH proxy. The following example is applicable to `status_as2d` and `status_pesitd` as well: you can expect the same messages with either in the place of `status_sshd`. • `status_sshd` returns `'sshd is disabled'`, when all ssh listeners are disabled, and there are no functional listeners. • `status_sshd` returns `'sshd is functional'`, when at least one SSH listener is functional. • `status_sshd` returns `'sshd is down'`, when at least one SSH listener is enabled, and there are no functional SSH listeners.
`status_admin`	Checks the status of the Admin server.
`status_tm`	Checks the status of the Transactional manager.
`status_db`	Checks the status of the Database. The following example is applicable to `status_admin`, `status_socks`, and `status_tm` as well: you can expect the same messages with either in the place of `status_db`. • `status_db` returns `'db is functional'`, when the service is functional. • `status_db` returns `'db is down'`, when the service is not functional.

Note SecureTransport includes several utilities that are used internally. All the utility files are stored in the `<FILEDRIVEHOME>/bin` or `<FILEDRIVEHOME>/bin/utils` directory.

Note In case of low disk space do not start servers.

Command line directory or file listing

This subsection discusses file listing specifics in SecureTransport and also supplies examples and usage details.

The `ls -l` command is the standard file/directory listing command that returns all files and directories contained in the directory where you run it. You can also specify a *subdirectory listing*, using `ls -l <directory_name>` or a *file listing*, using `ls -l <file_name>`.

The returned output contains all contained files and directories is in the following format:

```
[Permissions] [ST_nlink] [UID] [GID] [File_Size] [Date] [File_Name]
```

The following table includes the descriptions and specifics of each output parameter:

Utility file	Description
`Permissions`	The read-write-execute permissions for the current file.
`ST_nlink`	Represents the number of hard links to the file. Output of `ls -l <file_name>`, returns either as '`0`' or '`?`' for the `ST_nlink` value. This behavior applies to deployments on any supported OS.
`UID`	The User ID. When listing (file and folder) performed over SFTP on Windows, this value is always presented as a 0.
`GID`	The Group ID. When listing (file and folder) performed over SFTP on Windows, this value is always presented as a 0.
`File_Size`	The size of a file. Use the `Stfs.Encryption.ListDecryptedSize` server configuration option to specify which file size, the original (decrypted) or the encrypted file size, to be reported for encrypted files. The option is available in both SecureTransport Server and Edge, and should be set to the same value on both. The default value is `false`, meaning the encrypted file size is displayed. When the option is set to `true`, the original file size (taken from the STFS attribute) is reported. Due to the STFS attribute checks, performance degradation may occur.
`Date`	For a file, the returned value when that file was last modified; for a directory, it is the returned value for when that directory was created.
`File_Name`	The name and extension of the respective file.

A valid return line would look like this:

```
rw-rr--r-- 1 100 1001 1024 Aug 19 08:46 samplelog.txt
```

Appendix E: Server logs

The following topics lists the log files maintained by Axway SecureTransport and provide details for each log file:

- *Log file list* on page 992
- *Log output details* on page 995

Log file list

SecureTransport writes to several log files in multiple locations. These files can be used to monitor SecureTransport processes and identify any issues that can occur. Some messages are logged directly to the database and are visible in the *Server Log* page. For more information, see *Server log* on page 304.

You can open log files in a text editor to review them and to find specific messages.

The following table describes the log files used by SecureTransport and provides the location and a brief description of each file. Several log files share the same name. When viewing the table, make sure that you note the location of the log file you want to find.

File name	Directory	Description
`audit.log`	`<FILEDRIVEHOME>/var/logs/admin`	Records failed administrator login attempts, embedded database restart from Administrative tool, and database configuration change events for either the embedded or external database.
`catalina.out`	`<FILEDRIVEHOME>/tomcat/admin/logs`	Records unhandled exceptions in Java components in the Administration Tool and information about the servlets, including information about errors.
`catalina.out`	`<FILEDRIVEHOME>/tomcat/as2/logs`	Records AS2 protocol connection unhandled exceptions and information about the servlets, including information about errors.

File name	Directory	Description
cmdlog	<FILEDRIVEHOME>/var/logs	Records FTP commands and arguments that are sent by FTP clients after they connect successfully.
migration.log	<FILEDRIVEHOME>/var/logs	Records information generated during database migration from the embedded database to an Oracle database.
monitor_*.out	<FILEDRIVEHOME>/var/logs	Records monitor server output in a separate file for each monitored server.
mysql_error.log	<FILEDRIVEHOME>/var/logs	Records information about the embedded database for SecureTransport Edge and SecureTransport Server deployments that use the embedded database. Not used in deployments that use an external database.
mysql_slow_query.log	<FILEDRIVEHOME>/var/logs	Lists queries that took longer than a given time to execute for SecureTransport Edge and SecureTransport Server deployments that use the embedded database. The file name and time limit are configurable in mysql.conf. Not used in deployments that use an external database.
serverlog-fallback.log	<FILEDRIVEHOME>/var/logs/admin	Records server log messages when the server log database fails for either the embedded or external database.
tm.stdout.log	<FILEDRIVEHOME>/var/logs	Records standard output from Transaction Manager processes.
tm_agent_error.log	<FILEDRIVEHOME>/var/logs	Records errors about Transaction Manager operations and in-process agents.

File name	Directory	Description
tools.log	<FILEDRIVEHOME>/var/logs	Records warnings and errors from internal SecureTransport components.
AxwaySecureTransportAdmin_SecureTransport.log	<FILEDRIVEHOME>/../cygwin/var/log	A Windows-specific log file where information about the AxwaySecureTranportAdmin_5.3.0 service is recorded.
AxwaySecureTransportAS2d_SecureTransport.log	<FILEDRIVEHOME>/../cygwin/var/log	A Windows-specific log file where information about the AxwaySecureTranportAS2d service is recorded.
AxwaySecureTransportFTPd_SecureTransport.log	<FILEDRIVEHOME>/../cygwin/var/log	A Windows-specific log file where information about the AxwaySecureTranportFTPd service is recorded.
AxwaySecureTransportHTTPd_SecureTransport.log	<FILEDRIVEHOME>/../cygwin/var/log	A Windows-specific log file where information about the AxwaySecureTranportHTTPd service is recorded.
AxwaySecureTransportSSHd_SecureTransport.log	<FILEDRIVEHOME>/../cygwin/var/log	A Windows-specific log file where information about the AxwaySecureTranportSSHd service is recorded.
AxwaySecureTransportPeSITd_SecureTransport.log	<FILEDRIVEHOME>/../cygwin/var/log	A Windows-specific log file where information about the AxwaySecureTransportPeSITd service is recorded.
AxwaySecureTransportTM_SecureTransport.log	<FILEDRIVEHOME>/../cygwin/var/log	A Windows-specific log file where information about the AxwaySecureTransportTM (Transaction Manager) service is recorded.

File name	Directory	Description
`AxwaySecureTransport Database_ SecureTransport.log`	`<FILEDRIVEHOME>/ ../cygwin/var/log`	A Windows-specific log file where information about the `AxwaySecureTransport MYSQL` (embedded database) service is recorded when it is used.
`xferlog`	`<FILEDRIVEHOME>/ var/logs`	Records information about FTP(S), HTTP(S), SFTP, AS2, Connect:Direct, Folder Monitor, and PeSIT transfers. For more information, see *Track file transfer activity* on page 290 and *Configure transfer log* on page 170.

Log output details

The following topics provide the log file output details:

- *Log4j files* on page 995 - Provides the details of the log4j files.
- *Database log files* on page 997 - Provides the details of database log files.
- *FTPD log file* on page 997 - Provides the details of the FTPD log file.
- *Admin log file* on page 998 - Provides the details of the admin log file.
- *General log files* on page 998 - Provides the details of the general log files.
- *Modify the log4j files* on page 1001 - Provides how-to instructions for changing the log4j files.
- *Redirect log4j output from the database* on page 1003 - Provides how-to instructions for redirecting the log4j output from the database.
- *Control log fallback from database to file* on page 1005 - Provides how-to instructions to control log fallback from the database to a file.
- *Server log rotation scheduling* on page 1006 - Provides how-to instructions for scheduling server log rotation.

Log4j files

A number of the log files and some log output to the database use the log4j format. For more information, refer to the log4j documentation on the Apache web site.

Unless otherwise specified, by default, the logs are in the following format:

```
%d %p [%t] %c - %m
```

where:

- `%d` is the date
- `%p` is the error level
- `%t` is the thread ID
- `%c` is the Java class name
- `%m` is the log message

You might also find Java stack traces in these logs. Axway Global Support can use these to determine the cause of a particular error condition.

The following table log4j configuration files in `<FILEDRIVEHOME>/conf`, the log output they control, and the default destinations.

Configuration file name	Log output	Destinations

`admin-log4j.xml`	Administration Tool server	Database
		`audit.log`
		`migration.log`

`as2d-log4j.xml`	AS2 Server	Database `xferlog`
`ftpd-log4j.xml`	FTP Server	Database `xferlog`
`httpd-log4j.xml`	HTTP Server	Database `xferlog`
`pesitd-log4j.xml`	PeSIT Server	Database `xferlog`
`socks-log4j.xml` (Only on SecureTransport Edge)	SOCKS5 proxy	Database
`sshd-log4j.xml`	SSH Server	Database `xferlog`
`tm-log4j.xml` (Only on SecureTransport Server)	TM Server internal agents	Database `xferlog`
`tools-log4j.xml`	Data migration Export/import Various components	Database Java console `tools.log`

In an Enterprise Cluster (EC), when the database does not accept log messages fast enough and the queue becomes full, the servers listed in the table store their log messages in a buffer file until the database can accept them. See *Control log fallback from database to file* on page 1005.

The behavior for each server is controlled by the following parameters in their respective log4j files:

- `queueAwaitDefaultTimeout`: Time in milliseconds to wait for the queue to free up when full (default 5000 milliseconds)
- `queueAwaitMinTimeout`: Minimum time in milliseconds of the queue wait period (default 50 milliseconds)
- `queueAwaitFactor`: Factor used to adjust queue wait time (default 1000). This value is divided by the number of events that have not been saved in the database, and the result is subtracted from the current timeout to get the time to wait until the next event is sent to database. If the result is less than the `queueAwaitMinTimeout` value, `queueAwaitMinTimeout` is used instead.

With a larger value of `queueAwaitFactor`, future events do not wait as long and the system is more responsive. With a smaller value, future events wait longer before they are sent to the database so the load on the database is reduced and the system response might be reduced.

next-event-await-period = maximum(`queueAwaitMinTimeout`, *last-event-await-period* - `queueAwaitFactor` / *number-of-events*)

With the default values for the parameters, the initial value of *next-event-await-period* is 5000 milliseconds. When there are 2 events that have not been saved to the database, the time to wait is reduced by 1000/2 = 500 milliseconds until it reaches 50 milliseconds.

When database communication returns to normal and the database starts to accept log messages again, *next-event-await-period* is reset to `queueAwaitDefaultTimeout` and *number-of-events* is reset to zero.

```
date time [process ID]: username: command
```

Database log files

These log files exist on SecureTransport Edge systems and on SecureTransport Server systems that use the embedded MySQL database.

mysql_error.log – This log file contains the messages from the embedded database server. The log file contains information indicating when `mysqld` was started and stopped and also any critical errors that occur while the server is running. For more information on MySQL, refer to the documentation of the error log on the MySQL Developer Zone website.

mysql_slow_query.log – This log file contains SQL statements that took more than `long_query_time` seconds to execute. For more information on MySQL, refer to the documentation of the slow query log on the MySQL Developer Zone website.

FTPD log file

cmdlog – This log file contains the FTP commands and arguments that are sent by FTP clients after they connect successfully. (Thus, it does not show the USER and PASS commands.) Note that this log is not enabled by default. For more information, see *Configure FTP command log* on page 166.

The format of this file is:

`<calendar_time> <PID> <user_name> <command>`

Where:

`<current_time>` - The current local time, for example Tue Feb 24 14:28:01

`<PID>` - The process ID

`<user_name>` - Account name

`<command>` - FTP command and (optional) target file name

The possible FTP commands are listed under `Ftp.Commands` configuration option.

The default path of the **cmdlog** file is `<filedrivehome>/var/logs` and is configurable trough the `Ftp.CommandLogging.File` configuration option.

Admin log file

audit.log – This log file contains information on configuration changes made by Java components of the SecureTransport Administration Tool and database starts and stops. When the configuration changes are logged to the database (the default), failed administrator login attempts and database starts, stops, and configuration changes are still logged to this file.

The format and content of this file is controlled by the `<FILEDRIVEHOME>/conf/admin-log4j.xml` file. This file uses the log4j format. By default, the logs are in the following format:

`%d %s %m`

Where:

- `%d` is the date
- `%s` is the subcomponent
- `%m` is the log message

admin_tomcat<date>.log – This log file contains Tomcat-specific error messages. The file contains the Java stack traces for the errors.

General log files

xferlog – This log file contains information about uploads and downloads for all protocols.

The xferlog file records information about all the AS2, FTP(S), HTTP(S), PeSIT, SFTP, Connect:Direct, and Folder Monitor transfers made with SecureTransport Server and Edge. This information is also stored in the database.

Each server entry is composed of a single line of the format shown below. All fields are separated by spaces.

The field separator character in the xferlog file is by default a " " (space). To avoid breaking the external parsers, when the name of a transferred file contains spaces, the separator character can now be made a configurable parameter.

Note To configure your own delimiter, add `<param name="delimiter" value="{value}"/>` as a property of `com.tumbleweed.st.server.logging.xferlog.XferLogLayout` in all log4j files (`ftpd-log4j.xml, as2d-log4j.xml, sshd-log4j.xml, pesitd-log4j.xml, httpd-log4j.xml and tm-log4j.xml`).

For example:

```
<appender name="XferLogAppender"
class="com.tumbleweed.st.server.logging.xferlog.XferLogAppender">
<param name="File" value="/root/Axway/SecureTransport/var/logs/xferlog" />
<param name="Append" value="true" />

<layout class="com.tumbleweed.st.server.logging.xferlog.XferLogLayout">
<param name="DateFormat" value="EEE MMM dd HH:mm:ss yyyy" />
<param name="delimiter" value=";" />
```

```
<current_time> <transfer_time> <remote_host> <file_size> <file_name> <transfer_
mode> <transfer_security> <direction> <access_mode> <user_name> <server_name> 0
*
```

The fields are defined in the following:

- `<current_time>` – The current local time, for example, `Wed Oct 24 10:53:34 2012`. The format is *`DDD MMM dd hh:mm:ss YYYY`*, where:
  - *`DDD`* – Day of the week
  - *`MMM`* – Month
  - *`dd`* – Day of the month
  - *`hh`* – Hour
  - *`mm`* – Minutes
  - *`ss`* – Seconds
  - *`YYYY`* – Year
- `<transfer_time>` – Total time for the transfer, rounded off to seconds.
- `<remote_host>` – Remote host name or IP address.

Note When a user logs in/out or performs file transfers behind a proxy or a load balancer, an additional IP address is listed: the originating IP address of the user account. In such case, the Remote Host displays the IP address of the proxy/load balancer followed by the user's original IP address. Note that when the user is not behind a proxy/load balancer, the original IP address is displayed with the Remote Host parameter, with no additional IP address.

- `<file_size>` – Number of bytes transferred.
- `<file_name>` – (for example: `/home/jdoe/somefile`): For virtual and anonymous users, the path given is relative to their home directory. For real users, it's relative to the filesystem root.

  Note If you use a File Download or File Upload agent (such as the streaming agents) to handle the file transfer, the path will be preceded by `STOR:` (for uploads) or `RETR:` (for downloads).

- `<transfer_mode>` – A single character indicating the type of transfer:
  - `a` – ASCII transfer
  - `b` – Binary transfer
- `<transfer_security>` – A single character indicating the level of security:
  - `s` – Secure (SSL-based)
  - `n` – Non-secure

    Note In the 2.x versions of SecureTransport (and the 2.x and 3.x versions of SecureTransport for Windows), the value of this field is always _ regardless of whether security was used.

- `<transfer_status>` – A single character indicating the upload or download status:
  - Uploads – `i` for OK, `j` for error, and `k` for aborted
  - Downloads – `o` for OK, `p` for error, and `q` for aborted

    Note Under HTTP/S and SSH , user aborts are treated as errors. The reason is that for FTP, the abort condition is indicated by an explicitly received ABOR command. Any other data socket reset is considered a failure. Since SSH and HTTP don't have a control connection, they resort to interpreting a socket reset as a failure. There isn't any trace of an abort being present for SSH and HTTP protocol daemons. This also includes the guaranteed delivery extension for HTTP. Therefore, the client side aborts are displayed in the `xferlog` (and FileTracking) as inbound and outbound errors rather than inbound and outbound aborts. For SSH uploads there is an additional peculiarity: With a native SFTP Linux client, unless a kill ABRT of the child SSH process is completed, a transfer interrupt on the client side with Ctrl +C would cause `SSH_FXP_CLOSE` to be sent to SecureTransport, indicating FULL "successful" transfer. In this case, an "interrupted " SSH client transfer will be shown in FileTracking and the `xferlog` as successful.

- `<access_mode>` – A single character indicating the type of user access:
  - `a` - Anonymous
  - `r` – Real or virtual user
- `<user_name>` - E-mail address, as given at the password prompt, for anonymous users (for example: `jdoe@foo.com`); username for real or virtual users (for example: `jdoe`).

- `<server_name>` – Type of server used to make the transfer (transport protocol):
  - `ad-hoc`
  - `as2`
  - `c:d` (Conect:Direct)
  - `folder` (Folder Monitor)
  - `ftp`
  - `http`
  - `pesit`
  - `ssh`
- A zero (`0`)
- An asterisk (`*`)

Note The zero and asterisk are inserted as authentication method and authenticated user id respectively for compatibility with the `wu-ftp` log format.

The following is an example of a typical log entry:

```
Wed Jan 11 10:55:13 2006 3 10.191.2.33 5873
/drives/c/home/Virtual/vuser/avatar.jpg b s i r vuser http 0 *
```

Note On Windows, it is not possible to modify existing cron jobs or to use cron to run any jobs other than those SecureTransport jobs documented in these topics. Instead, use the Windows Task Scheduler.

tools.log – This log4j-format log file records warnings and error from internal SecureTransport components. The format and content of this file is controlled by the `<FILEDRIVEHOME>/conf/tools-log4j.xml` file.

For example, importing accounts using command-line tool might produce the following message:

```
2010-11-16 00:56:14,505 PST WARN [main]
com.tumbleweed.st.server.appframework.sql.SessionFactoryManagerImpl - Component
type '' is unknown. Using TOOLS configuration.
```

Modify the log4j files

You can set up the rotation of several log files based on the file size by editing the files listed under *Log4j files* on page 995.

Configure Log rotation to a file per file-size

In this example, the configuration file is the TM log: `<FILEDRIVEHOME>/conf/tm-log4j.xml`. The example uses *`FILEDRIVEHOME`* instead of `<FILEDRIVEHOME>` to represent the SecureTransport installation directory to avoid confusion with the syntactic use of pointed brackets in XML.

Change:

```
<appender name="ServerLog"
class="com.tumbleweed.st.server.logging.DailyRollingFileAppender">
  <param name="File" value="FILEDRIVEHOME/STServer/var/logs/tm.log" />
  <param name="Append" value="true" />
  <param name="RotateDirectory" value="FILEDRIVEHOME/STServer/var/db/hist/logs"
/>
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="%d %p [%t] %c - %m%n" />
  </layout>
</appender>
```

To:

```
<appender name="ServerLog" class="org.apache.log4j.RollingFileAppender">
  <param name="File" value="FILEDRIVEHOME/STServer/var/logs/tm.log" />
  <param name="MaxFileSize" value="10485760" />
  <param name="Append" value="true" />
  <param name="DatePattern" value="'.'yyyy-MM-dd" />
  <param name="MaxBackupIndex" value="5" />
  <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d %p [%t] %c - %m%n" />
  </layout>
</appender>
```

You can use any of the log4j file appenders. `com.tumbleweed.st.server.logging.DailyRollingFileAppender` supports the `RotateDirectory` parameter. If you use the Apache `RollingFileAppender`, the file rotates into the same directory as the original file with a `".n"` suffix appended to the filename, where `"n"` is an integer number up to the `MaxBackupIndex` value. You need to use another method to move the backup log files from `<FILEDRIVEHOME>/var/logs`.

Note For another way to manage log file rotation, see *Create a Log Entry Maintenance application* on page 770.

Attach logger to a non-blocking asynchronous appender

In some cases when the log messages are directed to a flat file, the rotation of the file might take a considerable amount of time during which certain SecureTransport processes (including user log-in) are unavailable. This might happen, for example, when rotating a large log to a file which is hosted on a remote location.

In this case, you might consider attaching the rotating log to an asynchronous appender which is explicitly defined as not-blocking. To achieve this, use the following example:

```
<appender name="ServerLog" class="org.apache.log4j.AsyncAppender">
  <param name="BufferSize" value="20000" />
  <param name="blocking" value="false" />
  <param name="LocationInfo" value="false"/>
  <appender-ref ref="AsyncAppender" />
</appender>
<appender class="com.tumbleweed.st.server.logging.DailyRollingFileAppender"
name="AsyncAppender">
  <param name="File" value="/opt/mysql54/Axway/SecureTransport/var/logs/tm.log"
/>
  <param name="Append" value="true" />
  <param name="DatePattern" value="'.'yyyy-MM-dd" />
  <param name="RotateDirectory" value="/mnt/logs/" />
  <layout class="org.apache.log4j.PatternLayout">
  <param name="ConversionPattern" value="%d %p [%t] %c - %m%n" />
  </layout>
</appender>
```

Redirect log4j output from the database

As listed in *Log4j files* on page 995, some log output is directed to both the `xferlog` file and the database.

If you set any log level to `debug` or `all`, SecureTransport produces many log messages which can overload the database. Do not log to the database for log level `debug` or `all`.

Note When server log messages are stored in the database, they are displayed in the *Server Log* page. When you store the log messages in a file, they are not displayed in the *Server Log* page.

To direct the log messages being stored in the database to a file, modify the `ServerLog` appender for each relevant file. The example uses `FILEDRIVEHOME` instead of `<FILEDRIVEHOME>` to represent the SecureTransport installation directory to avoid confusion with the syntactic use of pointed brackets in XML. Replace the `<FILEDRIVEHOME>` with the actual installation path to the SecureTransport home folder in the XML configuration file.

Change:

```
<appender name="ServerLog" class="org.apache.log4j.db.DBAppender">
    <param name="locationInfo" value="true"/>
    ...
    <connectionSource
class="com.tumbleweed.st.server.logging.STDataSourceConnectionSource">
        <dataSource class="com.mchange.v2.c3p0.ComboPooledDataSource">
            ...
        </dataSource>
    </connectionSource>
    <filter class="org.apache.log4j.filter.MapFilter">
    </filter>
    <filter class="com.tumbleweed.st.server.logging.STLog4JNDCFilter">
        <param name="ComponentName" value="AS2D"/>
    </filter>
</appender>
```

Note The `dataSource` settings are different for each configuration file.

To:

```
<appender name="ServerLog"
    class="com.tumbleweed.st.server.logging.DailyRollingFileAppender">
    <param name="File" value="FILEDRIVEHOME/var/logs/tm.log"/>
    <param name="Append" value="true"/>
    <param name="DatePattern" value="'.'yyyy-MM-dd"/>
    <param name="RotateDirectory"
        value="FILEDRIVEHOME/var/db/hist/logs"/>
    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%d %p [%t] %c - %m%n"/>
    </layout>
</appender>
```

In the `admin-log4j.xml` file there is an additional appender called `AuditLogAppender`. Change appender from:

```
<appender name="AuditLogAppender"
    class="com.tumbleweed.st.server.logging.db.STDBAppender">
    <param name="locationInfo" value="true"/>
    <param name="maxLoggingEventQueueSize" value="10000"/>
    <param name="fallbackLogger" value="ServerLogFallback"/>
    <param name="databaseStatusCheckupDelay" value="60"/>
    <param name="databaseCheckupTimeout" value="30"/>

    <!-- WARNING - changing the id area may cause deletion of existing
        logs and crash of the appender! -->
```

```
    <param name="idAreaBegin" value="-40000000000"/>
    <param name="idAreaEnd" value="-30000000000"/>

    <!-- Connection pool parameters -->
    <param name="driverClass" value="com.mysql.jdbc.Driver"/>
    <param name="initialPoolSize" value="5"/>
    <param name="maxPoolSize" value="25"/>
    <param name="minPoolSize" value="5"/>
    <param name="acquireIncrement" value="5"/>
    <param name="maxStatements" value="4000"/>

    <filter class="com.tumbleweed.st.server.logging.STLog4JNDCFilter">
        <param name="ComponentName" value="AUDIT"/>
    </filter>
</appender>
```

To:

```
<appender name="AuditLogAppender"
    class="com.tumbleweed.st.server.logging.DailyRollingFileAppender">
    <param name="File" value="FILEDRIVEHOME/var/logs/admin/audit.log"/>
    <param name="Append" value="true" />
    <param name="DatePattern" value="'.'yyyy-MM-dd" />
    <param name="RotateDirectory"
        value="FILEDRIVEHOME/var/db/hist/logs/admin"/>
    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%d %p [%t] %c - %m%n" />
    </layout>
</appender>
```

Control log fallback from database to file

If the embedded or external database stops accepting log messages, SecureTransport directs the messages to `<FILEDRIVEHOME>/var/logs/admin/serverlog-fallback.log`.

You can control this behavior by setting the following parameters for each server in `<FILEDRIVEHOME>/conf/configuration.xml`:

- When the embedded database is used, the `hibernate.c3p0.timeout` attribute of the component for each server controls the timeout after which an idle connection will be removed from the pool. The default value is 30 minutes.
- When an external Oracle database is used, the `hibernate.connection.oracle.jdbc.ReadTimeout` attribute of the component for each server controls the read timeout, how long to wait for a response from the database before failing a query, for all TCP sockets to the database. The default is five minutes.

- When an external database is used, the `hibernate.c3p0.checkoutTimeout` attribute of the component for each server controls the Database connect timeout, how long to wait for a connection to be established. The default is five minutes.

Server log rotation scheduling

Note For another way to schedule server log rotation, see *Create a Transfer Log Maintenance application* on page 786 and *Create a Log Entry Maintenance application* on page 770.

Log files are rotated so that you do not lose any information because you have reached a file size limit. The log rotation schedule for log4j files is specified in the log4j configuration files. All other log files are rotated on a regular schedule as directed by a log rotation scheduling tool. You can modify the log rotation schedule by editing the root `crontab` file. (For details, refer to `man 5 crontab`.)

On UNIX-based systems, the root `crontab` file is located in the `/var/spool/cron/crontabs/root` directory for Oracle Solaris and AIX or the `/var/spool/cron/root` directory for Linux. These paths are under the system root directory, not `<FILEDRIVEHOME>`. Use the `crontab -e` command to edit this file while logged in as root; it opens the file in the vi editor.

On Windows, it is not possible to modify existing cron jobs or to use cron to run any jobs other than the predefined SecureTransport jobs. Use the Task Scheduler or some other method to schedule server log rotation.

Note If SecureTransport is installed to run a non-root user, the `crontab` file is named after the non-root user.

The schedule fields in this file, and the allowable values for each one, are:

- Minutes 0-59
- Hours 0-23
- Day of Month 1-31
- Month 1-12 (or name)
- Day of Week 0-7, where Sunday is 0 or 7 (or name)

So the format looks like the following:

```
<Minutes> <Hours> <Day of Month> <Month> <Day of Week> <path to rotate
script> >> <path to output file> 2>&1
```

A `*` character in any field means all legal values. For example, a `*` in the Day of Week field configures the rotation schedule to run every day of the week. You can also use multiple elements separated by commas in any field, where an element is either a single number (such as `4`) or a range of numbers separated by a hyphen (such as `4-8`). For more information, run `man 5 crontab`.

To disable a rotate job, put a `#` character at the beginning of the line that calls it.

Rotation job examples

The following examples are shown for UNIX-based platforms.

The default rotate job as defined during installation runs every night at 11:59 PM:

```
59 23 * * * "/opt/Axway/SecureTransport/bin/rotate"
```

To run the job every Sunday at midnight:

```
0 0 * * 0 "/opt/Axway/SecureTransport/bin/rotate"
```

To run the job every eight hours at midnight, 8:00 A.M., and 4:00 P.M. on Monday through Friday:

```
0 0,8,16 * * 1-5 "/opt/Axway/SecureTransport/bin/rotate"
```

Appendix F: Firewall settings

The SecureTransport client and server software is frequently used in conjunction with network firewalls, designed to permit access only to authorized protocols and possibly specific source networks, hosts, or users. Firewalls provide essential protection from hackers, corporate raiders, and other types of access that are unauthorized or should be restricted.

A firewall refers to a hardware, software, or combination product that provides stateful inspection or filtering functionality only. There are other types of network devices, such as proxy servers and caching stores that can provide these functions as well, but these devices are not covered in the following topics.

One frequently deployed firewall is the Check Point FireWall-1 product (VPN-1), produced by Check Point Software Technologies Ltd. Other popular products include the Cisco PIX, Symantec Enterprise Firewall (Raptor), and Network Associates Gauntlet firewalls.

The following topics provide how-to instructions for enabling bidirectional connections and configuring ports, descriptions and lists of the firewall rules.

- *Enable bidirectional connections in a firewall* on page 1008
- *Configure firewall ports* on page 1009
- *Firewall rules* on page 1011

Enable bidirectional connections in a firewall

If you are using FTP for file transfers, you might need to configure your firewall to use bidirectional FTP transfers. Bidirectional FTP data connections might not be enabled in your firewall by default. Bidirectional FTP data connections are not considered as safe since the data connection is interactive and the connection changes the basic way FTP works.

The following topics provide how-to instructions for enabling bidirectional connections:

- *Check Point firewall* on page 1009 - Provides how-to instructions for enabling bidirectional connections on a Check Point firewall.
- *Cisco PIX firewall* on page 1009 - Provides how-to instructions for enabling bidirectional connections on a Cisco PIX firewall.
- *Raptor firewall* on page 1009 - Provides how-to instructions for enabling bidirectional connections on a Raptor firewall.

Check Point firewall

To enable Check Point firewalls, in Check Point NG firewalls (AI R55 and higher), set the FTP connection to FTP_BASIC. This allows bidirectional communications and sets the firewall to allow commands not terminated with a newline.

The Check Point firewall must allow bidirectional communication. It must not enforce new line termination.

As the Check Point documentation states, the FTP_BASIC protocol type was introduced in the Check Point R55 NG AI. If you apply it to the FTP object, it enforces a reduced set of the FTP security checks done by the regular FTP protocol type. The following checks are not enforced by FTP_BASIC:

- That every packet is terminated with a newline character, so that the PORT command is not split across packets.
- Bidirectional traffic on the data connection is not allowed, as it can be used improperly.

Note FTP_BASIC also disables FTP BOUNCE protection and so can be viewed as potentially less secure. This, as well as a more secure method to disable the newline check (FTP PACKET check) are described in Check Point Secure Knowledge SK27122.

Cisco PIX firewall

Cisco PIX firewalls do not interoperate properly with SecureTransport FTP connections when "stateful inspection" is enabled for the FTP protocol. Disable stateful inspection for the FTP protocol accordingly.

Raptor firewall

Raptor Firewalls prior to version 6.5 do not accept the AUTH command. Upgrading to version 6.5 resolves this problem.

Configure firewall ports

The exact list of ports to open depends on which SecureTransport functions you use. For example, if you do not enable FTP connections to your server, then you can disregard the ports listed below for FTP.

The following lists show the ports that SecureTransport can use. The values given are the defaults. You can reconfigure SecureTransport after installation to use different values.

The following topics list firewall ports that need to be open:

- *Communication between the outside and SecureTransport Edge* on page 1010 - Lists the firewall ports that need to be open for communication between the outside and SecureTransport Edge.

- *Communication between SecureTransport Server and SecureTransport Edge* on page 1010 - Lists the firewall ports that need to be open for communication between SecureTransport Server and SecureTransport Edge.
- *Communication between SecureTransport Server and an internal network* on page 1011 - Lists the firewall ports that need to be open for communication between SecureTransport Server and an internal network.
- *Internal SecureTransport communication* on page 1011 - Lists the firewall ports that need to be open for internal SecureTransport communication.

Communication between the outside and SecureTransport Edge

These ports must be opened on your external firewall to allow communication between the outside world and your proxy (SecureTransport Edge) server.

- 20 – FTP (secure and non-secure) active-mode data channel
- 21 – FTP (secure and non-secure) control channel (For secure connections, the firewall must allow bidirectional communication.)
- 22 – SSH (SFTP and SCP)
- 80 – HTTP
- 443 – HTTPS
- 444 – Administration Tool (HTTPS)
- 10080 – AS2 (non-SSL)
- 10443 – AS2 (SSL)
- 17617 – PeSIT (non-SSL)
- 17627 – PeSIT over secure socket (non–Transfer CFT compatible)
- 17637 – PeSIT over secure socket (CFT compatible)
- 19617 - PeSIT over pTCP plain socket
- 19627 - PeSIT over pTCP Secured Socket
- User-defined range – FTP (secure and non-secure) passive-mode data channel

Communication between SecureTransport Server and SecureTransport Edge

These port must be open between the private network and the peripheral network (DMZ) for the Transaction Manager Server on SecureTransport Server to connect to the protocol servers on SecureTransport Edge. The protocol is the SecureTransport secure streaming protocol.

- 20021 – FTP Server
- 20022 – SSH Server

- 20080 – HTTP Server
- 20444 – Administration Tool server
- 21080 – AS2 Server
- 27617 – PeSIT Server

Communication between SecureTransport Server and an internal network

All of the ports used for communication between the outside and SecureTransport Edge can be used for user connections originating within your internal network. The following ports might be used for interfacing with infrastructure components:

- 389 or 3268 – LDAP
- 1305 – Axway Sentinel
- 1344 - ICAP
- 1433 - Microsoft SQL Server database (default)
- 1521 – Oracle database (default)
- 44441 – SiteMinder Accounting
- 44442 – SiteMinder Authentication
- 44443 – SiteMinder Authorization

Internal SecureTransport communication

- 7800 thorough 7802 – Hibernate second-level cache
- 8005 – Tomcat shutdown
- 8006 – AS2 shutdown
- 8009 – Tomcat JK connector
- 33060 – MySQL database
- 44431 – Standard Cluster (SC) server synchronization and heartbeat

Ports used for communication outside the firewall (for the servers that you plan to use), might need firewall rules set up so that they are accessible only from certain subnets. For example, allowing internal users to connect using both plain and secure HTTP, while requiring external users to use HTTPS, by opening port 80 only for a certain subnet, while keeping 443 open unconditionally.)

Firewall rules

You can use the firewall rules in the following tables for active/active (load-balanced) or active/passive (failover) Standard Clusters and Enterprise Clusters.

Note For a non-streaming deployment with active/active or active/passive systems, skip the rules for port 1080. For a non-streaming setup with only a single machine, also skip the Standard Clustering rules. The Destination Port values listed are the default values or ranges used by SecureTransport.

The following topics list the firewall rules:

- *Protocol rules* on page 1012 - Lists the firewall protocol rules.
- *Authentication rules* on page 1015 - Lists the firewall authentication rules.
- *Administration rules* on page 1015 - Lists the firewall administration rules.
- *TM server communication rules* on page 1016 - Lists the firewall Transaction Manager server communication rules.
- *Server transfer rules* on page 1017 - Lists the firewall server transfer rules.
- *Standard Cluster rules* on page 1017 - Lists the firewall Standard cluster rules.
- *Enterprise Cluster rules* on page 1017 - Lists the firewall Enterprise Cluster rules.
- *Protocol rules - outbound from SecureTransport Edge* on page 1018 - Lists the firewall protocol rules for outbound communication from the SecureTransport Edge.

Protocol rules

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
1	Internet	Secure-Transport Edge Virtual IP (load balancer)	FTP(S)	21	← (in-bound)	Client FTP(S) control channel
2	Internet	Secure-Transport Edge Virtual IP (load balancer)	FTP(S)	1024 to 65535 (Actual port range is specified on the Remote Server.)	→ (out-bound)	Client FTP(S) data channel, active mode
3	Internet	Secure-Transport Edge Virtual IP (load balancer)	FTP(S)	1024 to 65535 (Actual port range is specified on the Edge.)	← (in-bound)	Client FTP(S) data channel, active mode

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
4	Internet	Secure-Transport Edge Virtual IP (load balancer)	HTTP	80	← (in-bound)	Client web access (non-secure)
5	Internet	Secure-Transport Edge Virtual IP (load balancer)	HTTPS	443	← (in-bound)	Client web access (secure)
6	Internet	Secure-Transport Edge Virtual IP (load balancer)	SSH	22	← (in-bound)	Client SSH access
7	Internet	Secure-Transport Edge Virtual IP (load balancer)	AS2 (SSL)	10443	← (in-bound)	Partner AS2 access (secure)
8	Internet	Secure-Transport Edge Virtual IP (load balancer)	AS2 (non-SSL)	10080	← (in-bound)	Partner AS2 access (non-secure)
9	Internet	Secure-Transport Edge Virtual IP (load balancer)	PeSIT over plain socket	17617	← (in-bound)	Partner PeSIT access (non-secure)
10	Internet	Secure-Transport Edge Virtual IP (load balancer)	PeSIT over secured socket (non–Transfer CFT Compatible)	17627	← (in-bound)	Partner PeSIT access (non-secure)

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
11	Internet	Secure-Transport Edge Virtual IP (load balancer)	PeSIT over secured socket (Transfer CFT Compatible)	17637	← (in-bound)	Partner PeSIT access (non-secure)
12	Internet	Secure-Transport Edge Virtual IP (load balancer)	PeSIT over pTCP plain socket	19617	← (in-bound)	Partner PeSIT access (non-secure)
13	Internet	Secure-Transport Edge Virtual IP (load balancer)	PeSIT over pTCP secured socket	19627	← (in-bound)	Partner PeSIT access (non-secure)
14	Trusted (secure network)	Secure-Transport Edge	HTTPS	444	← (in-bound)	SecureTransport Administration Tool (if access is required through the firewall)
15	Secure-Transport Server	Mail server for outgoing mail	SMTP (TCP)	25	→ (out-bound)	Ad hoc file transfer email notifications from ST Web Client
16	Secure-Transport Server	SNMP Masters	SNMP (UDP)	162	→ (out-bound)	SNMP monitoring

For a streaming deployment with one SecureTransport Edge and one SecureTransport Server there is no load balancer, so substitute the real IP address of the SecureTransport Edge for the IP address of the load balancer in the Group Destination column for rules 1 through 13.

For outbound AS2 transfers or asynchronous MDN receipts for inbound AS2 transfers, define outbound rules for ports 10080 and 10443. If the AS2 listener is on the SecureTransport Server and an SOCKS5 proxy is on the SecureTransport Edge, define these rules on the firewall between the SecureTransport Edge and the SecureTransport Server. Otherwise, define these rules on the firewall between the SecureTransport Edge and the Internet.

For internal users to upload or download files to SecureTransport, they must log into the SecureTransport Server directly using HTTP(S) or FTP(S). So those ports from the secure network to the SecureTransport Server must be open. In some installations, access is only through a proxy. In this case secure network requires access to the Proxy server.

Both FTP and FTPS use port 20 for the data channel in active mode. If preferred, you can define a passive-port range instead, and set up a similar rule for that range of ports. Both FTP and FTPS use port 21 for the control channel. For more details, see *Passive port range is not defined in the firewall* on page 976.

HTTP access is optional. To disable HTTP, do not define rule 4.

If the SMTP server that handles ad hoc file transfer email notifications from ST Web Client is in the secure network, do not define rule 15.

Authentication rules

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
17	Secure-Transport Server	Trusted (secure network)	SiteMinder	44441	➔ (out-bound)	SiteMinder Accounting
18	Secure-Transport Server	Trusted (secure network)	SiteMinder	44442	➔ (out-bound)	SiteMinder Authentication
19	Secure-Transport Server	Trusted (secure network)	SiteMinder	44443	➔ (out-bound)	SiteMinder Authorization
20	Secure-Transport Server	Trusted (secure network)	LDAP	389 or 3268	➔ (out-bound)	LDAP user lookup and authentication

Administration rules

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
21	Trusted (secure network)	Secure-Transport Server	HTTPS	444	← (inbound)	SecureTransport Administration Tool

TM server communication rules

Network zones define the server ports that the TM Servers running on SecureTransport Servers in the secure network connect to on the SecureTransport Edge servers running in the peripheral network (DMZ). See *Communication across Transaction Manager, protocol, and proxy servers* on page 215.

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
22	Secure-Transport Servers	Secure-Transport Edge (FTP Server)	TCP over SSL	20021	➔ (out-bound)	Transaction Manager streaming protocol
23	Secure-Transport Servers	Secure-Transport Edge (HTTP Server)	TCP over SSL	20080	➔ (out-bound)	Transaction Manager streaming protocol
24	Secure-Transport Servers	Secure-Transport Edge (AS2 Server)	TCP over SSL	21080	➔ (out-bound)	Transaction Manager streaming protocol
25	Secure-Transport Servers	Secure-Transport Edge (SSH Server)	TCP over SSL	20022	➔ (out-bound)	Transaction Manager streaming protocol
26	Secure-Transport Servers	Secure-Transport Edge (PeSIT Server)	TCP over SSL	27617	➔ (out-bound)	Transaction Manager streaming protocol
27	Secure-Transport Servers	Administration Tool server	TCP over SSL	20444	➔ (out-bound)	Transaction Manager streaming protocol

Do not define these rules in a deployment with no SecureTransport Edge. Define only the rules for the protocols you are using.

Note that in SecureTransport Edge deployment, port 20444 (used by the Administration Tool server) must always be open.

Server transfer rules

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
28	Secure-Transport Servers	Secure-Transport Edge	SOCKS	1080	→ (out-bound)	SOCKS5 proxy for server-initiated transfers (out-bound)

Do not define rule 28 for a deployment with no SecureTransport Edge.

Standard Cluster rules

The following rules are required for a Standard Cluster (SC).

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
29	Secure-Transport Servers	Secure-Transport Servers	Proprietary	44431	←→ (server-to-server)	Server synchronization and heartbeat
30	Secure-Transport Servers	Secure-Transport Servers	HTTPS	444	←→ (server-to-server)	Synchronization

Enterprise Cluster rules

The following rules are required for a Enterprise Cluster (EC). The cluster cache manager uses the first free port starting at 8088.

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
31	Secure-Transport Servers	Secure-Transport Servers	TCP and UDP	8088 through 8093	←→ (server-to-server)	Cluster cache management

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
32	Secure-Transport Servers	Secure-Transport Servers	TCP	7	←→ (server-to-server)	Coherence TcpRing/IpMonitor death detection

Protocol rules - outbound from SecureTransport Edge

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
33	Secure-Transport Edge	Internet	FTP(S)	1024 to 65535 port range specified on the Edge	← (inbound)	Server FTP (S) data channel, active mode
34	Secure-Transport Edge	Internet	FTP(S)	1024 to 65535 port range specified on the client server	→ (out-bound)	Server FTP (S) data channel, passive mode
35	Secure-Transport Edge	Internet	FTP(S)	21	→ (out-bound)	Server FTP (S) data channel
36	Secure-Transport Edge	Internet	HTTP	80	→ (out-bound)	Server HTTP data channel
37	Secure-Transport Edge	Internet	HTTPS	443	→ (out-bound)	Server HTTPS data channel
38	Secure-Transport Edge	Internet	SSH	22	→ (out-bound)	Server SSH data channel
39	Secure-Transport Edge	Internet	AS2	Specified in the transfer site	→ (out-bound)	Server AS2 data channel

#	Group source	Group destination	Protocol	Destination port	Direction	Purpose
40	Secure-Transport Edge	Internet	PeSIT	Specified in the transfer site	➔ (out-bound)	Server PeSIT data channel

If you disable the default HTTP port by not defining rule 4, do not define rule 36.

Define rules 39 and 40 for each port specified for the partnerships in the transfer sites.

Appendix G: Expression Language

This appendix provides information about the syntax for the expressions used for post-transmission actions, PGP, and account templates supported by Axway SecureTransport.

The following topics list and provide Expression Language variables and functions:

- *Expression Language overview* on page 1020
- *Expression Language operators* on page 1021
- *Predefined variables* on page 1021
- *Predefined functions* on page 1022
- *SecureTransport specific named variable sets* on page 1025
- *PeSIT variables* on page 1026
- *Advanced Routing EL functions and variables* on page 1029
- *Match and replace functions* on page 1029
- *Expression examples* on page 1029

Expression Language overview

Many features of SecureTransport use expressions. The expression language SecureTransport uses is based on the Sun JSP Expression Language. Only the syntax listed in this appendix is supported by SecureTransport, any other syntax is not guaranteed to function properly.

The following SecureTransport features can use the expression language:

- Transfer site post-transmission actions
- Subscription post-transmission actions
- PGP
- Account templates

Note If an account template and its transfer site are defined using expressions, you cannot restart failed transfers for that account template using the **Resubmit** button on the *File Tracking* page.

This appendix provides a list of the supported syntax with examples.

Note When creating expressions that use file paths you must use the forward slash (/) regardless of the platform where the file path is located. For example, instead of writing `c:\tmp\${stenv['loginname']}`, write `c:/tmp/${stenv['loginname']}`.

Expression Language operators

The following operators are supported:

Operator	Description
`[ ]` and `.`	Used to refer to attributes of an object or items in collection.
`+`, `-`, `*`, `/` or `div`, `%` or `mod`	Arithmetic Operators. Both binary and unary operators are supported
`==` or `eq`, `!=` or `ne`, `<` or `lt`, `>` or `gt`, `<=` or `le`, `>=` or `ge`	Relational Operators. provides ability to compare values
`&&` or `and`, `||` or `or`, `!` or `not`	Logical Operators
empty	Empty Operator
`? :`	Conditional Operator

Parentheses can be used in combination with the operators to change precedence.

SecureTransport evaluates operators using the following precedence order, listed from highest to lowest and left to right:

- `[ ] .`
- `( )`
- - (unary) `not ! empty`
- `* / div % mod`
- `+` - (binary)
- `< > <= >= lt gt le ge`
- `== != eq ne`
- `&& and`
- `|| or`
- `? :`

Predefined variables

SecureTransport supports the following predefined variables:

Name	Syntax	Description
Time Stamp	`${timestamp}`	Returns the UNIX epoch time in milliseconds as a decimal integer.
PGP Embedded File Name	`${embedded}`	The original file name embedded in the PGP encoded file. This value is defined after a PGP encoded file is decrypted. If the file was not PGP encoded, returns an empty string.

Predefined variable examples

The following table shows examples of the predefined variables:

Name	Example usage	Example return value
Time Stamp	`${timestamp}`	`1345652729052`
PGP Embedded File Name	`${embedded}`	`original-file-name.txt`

Predefined functions

SecureTransport supports the following predefined functions:

Name Syntax	Description
Date `${date()}` or `${date(`*`date-and-time-pattern`*`)}`	Returns the current date and time. The *date-and-time pattern* is the same format defined in the Java class `java.text.SimpleDateFormat`. If no format is specified then the output is the default date format in the current locale.
dayOffset `${dayOffset ('yymmdd', 'var1')}`	Returns the current date and time with `var1` days added or subtracted as an offset.
Random ID `${random()}`	Creates a pseudo-random string using both letters and numbers. Format is a 32 byte hex string.
String Concatenation `${concat (`*`var1`*`, `*`var2`*`)}`	Creates a new string concatenating the two variables together.

Name Syntax	Description
Substring `${substring (variable, beginIndex,endIndex)}`	Returns a substring for a given string. The substring begins at the specified `beginIndex` and extends to the character at index `endIndex` - 1. Thus, the length of the substring is `endIndex-beginIndex`.
Force Exception`${error()}` or `${error(message)}`	Throws an exception error. If `${error(message)}` is used, a message is returned with the error. This message is logged along with the exception.
File Name`${filename (variable)}`	Returns the target file name with the extension, but without the path to the file.
File Basename`${basename (variable)}`	Returns the target file name without the extension or path to the file.
File Extension`${extension (variable)}`	Returns the target file extension, including the dot. If there is no extension, an empty string is returned.
`${resolve()}`	Removes any occurrence of ., or . in a file path. This function works with POSIX style paths only. If the resolved path is null, empty or returns a `/`, an error is returned.

Predefined function examples

The following table shows examples of the predefined functions:

Name	Example usage	Example return value
Date (default)	`${date()}`	`June 22, 2012 1:42:04 AM`
Date (formatted)	`${date('EEEE, M-d H:m')}`	`Friday, 6-22 1:42`

Name	Example usage	Example return value
DayOffset	`${dayOffset('yymmdd', '-1')}`	`${dayOffset('yyMMdd', '-5')}` - returns 10th if today is 15th of August formatted as per the specified format parameter - `120810`. `${dayOffset('yyMMdd', '+7')}` - returns 22th if today is 15th of August formatted as per the specified format parameter - 120822. `${dayOffset('ddMMyy', '+1') ge '090414'}`
Random ID	`${random()}`	`C7F2119AAECEACCDE16C496C96FEEE39`
String Concatenation	`${concat('str', 'ing')}`	`string`
Substring	`/${substring (stenv.loginname,0,1)}` where `stenv.loginname` is interoperable with `env ['DXAGENT_LOGINNAME']`	`string`
Force Exception	`${error()}`	`com.tumbleweed.util. expressions. InvalidExpressionException Caused by: java.lang.Exception: Unspecified error`
Force Exception (with a specific error message)	`${error(*message*)}`	`com.tumbleweed.util. expressions. InvalidExpressionException Caused by: java.lang.Exception: An error has occurred in this part of the process!`
Full File Name	`${filename($file)}`	`filename.txt`
File Basename	`${basename($file)}`	`filename`

Name	Example usage	Example return value
File Extension	`${extension($file)}`	`.txt`
Path Resolution	`${resolve('.././path')}`	path
Path Resolution with Error	`${resolve('../../..')}`	`com.tumbleweed.util.expressions.InvalidExpansionException: Invalid path resolution: /`
Path Resolution with Error	`${resolve('\\')}`	`com.tumbleweed.util.expressions.InvalidExpansionException: Path must not contain '\' character`

SecureTransport specific named variable sets

Named variable sets separate variables into logical groups. Named variable sets use the following syntax:

`${name['variable']}`

or

`${name.variable}`

SecureTransport uses the following named variable sets:

- `${sess['variable']}` – used with SecureTransport session variables including LDAP
- `${env['variable']}`, `${stenv['variable']}`, or `${stenv.variable}` – used with SecureTransport predefined environment variables
- `${pesit['variable']}` – used with SecureTransport PeSIT variables described in *PeSIT variables* on page 1026

LDAP session variables can be used with the `sess` named variable set. You can also develop an agent that contains the session variables you want to use. All session variables must be prefixed with `STSESSION_`.

The `env` named variable set contains the entire environment, including any non- SecureTransport-specific variables. Environment variables accessed using `stenv` are preprocessed to remove the `DXAGENT_` prefix, and upper case characters are converted to lower case characters. For example, to use the environment variable `DXAGENT_TARGET`, write the following expression:

`${env['DXAGENT_TARGET']}`

or use the `stenv` named variable set and access the variable as:

```
${stenv['target']} or ${stenv.target}
```

SecureTransport-specific named variable set examples

The following table shows examples of SecureTransport-specific named variables:

Example	Example return value
`${sess['STSESSION_LDAP_DIR_homeDirectory']}`	`/home/user1`
`${sess['STSESSION_LDAP_DN']}`	`cn=john,ou=People,dc=tp,dc=axway,dc=com`
`${sess['STSESSION_LDAP_DIR_uidNumber']}`	`1000`
`${env['DXAGENT_HOMEDIR']}`	`/home/user2`
`${stenv['homedir']}`	`/home/user2`
`${env['DXAGENT_FULLSOURCE']}`	`/st/monitor/download/test.xml`
`${stenv['fullsource']}`	`/st/monitor/download/test.xml`
`${stenv.rawsource}`	`AS2OriginalFile`
`${stenv.site_target}`	`OriginalFile`

PeSIT variables

The following expressions are valid in transfer profiles:

Expression	PeSIT PI code
`${pesit.crc}`	PI 1

Expression	PeSIT PI code
${pesit.diagCode}	PI 2
${pesit.callerID}	PI 3
${pesit.senderID}	PI 3
${pesit.serverID}	PI 4
${pesit.receiverID}	PI 4
${pesit.version}	PI 6
${pesit.checkPointInterval}	PI 7
${pesit.checkPointWindow}	PI 7
${pesit.fileType}	PI 11
${pesit.fileName}	PI 12
${pesit.transferID}	PI 13
${pesit.fileAttributes}	PI 14
${pesit.restart}	PI 15
${pesit.dataEncoding}	PI 16
${pesit.priority}	PI 17
${pesit.restartCheckPoint}	PI 18
${pesit.cancelCode}	PI 19
${pesit.checkPointNumber}	PI 20
${pesit.compressed}	PI 21
${pesit.compressionType}	PI 21
${pesit.accessType}	PI 22
${pesit.resyncAllowed}	PI 23

Expression	PeSIT PI code
`${pesit.exchangeBufferSize}`	PI 25
`${pesit.totalBytes}`	PI 27
`${pesit.totalRecords}`	PI 28
`${pesit.diagnosticText}`	PI 29
`${pesit.recordFormat}`	PI 31
`${pesit.recordLength}`	PI 32
`${pesit.fileOrganization}`	PI 33
`${pesit.fileLabel}`	PI 37
`${pesit.keyLength}`	PI 38
`${pesit.keyOffset}`	PI 39
`${pesit.allocationUnit}`	PI 41
`${pesit.allocationSize}`	PI 42
`${pesit.creationDateTime}`	PI 51
`${pesit.extractionDateTime}`	PI 52
`${pesit.originalSenderID}`	PI 61
`${pesit.finalDestinationID}`	PI 62
`${pesit.msgData}`	PI 91
`${pesit.serviceParam}`	PI 99
`${pesit.accountName}`	—
`${pesit.datetime}`	—
`${pesit.details}`	—

Note The expressions `${pesit.originalSenderID}` and are `${pesit.finalDestinationID}` are set only for routed transfers.

Advanced Routing EL functions and variables

For a complete listing of the Advanced Routing Expression Language (EL) functions and variables, refer to *Custom Expression Language functions and variables* on page 921.

Match and replace functions

The expression language match and replace functions can match a regular expression or replace it.

The syntax for the replace operation is:

```
${variable.replace(<match RE>, <replace RE>)}
```

If the match succeeds, the value is the string with the matched string replaced.

The syntax for a match operation is:

```
${variable.matches(<match RE>)}
```

If the match succeeds, the value is `true`. If it does not, the value is `false`.

Note The match operation returns a logical value that can be used with relational or conditional operators.

For more about regular expressions, see *Regular expressions* on page 1035.

Regular expression examples

The following table shows several examples of using the match and replace operations with regular expressions.

Name	Example	Example return value
Match	`${foo.matches('fo*')}`	`true`
Replace	`${foo.replace('f(.*)', 'm$1')}`	`moo`

Expression examples

This topic provides additional examples on expression usage. In this topic, sample variable values are given to show how various expressions can use the information. The examples provided in this topic apply to:

- Transfer site post-transmission actions
- Subscription post-transmission actions

- PGP
- Account templates

For a complete listing of the Advanced Routing Expression Language (EL) functions and variables, refer to *Custom Expression Language functions and variables* on page 921.

Expression variables and examples

The following table provides the variable names and values that are used in the subsequent examples:

Variable name	Value
DXAGENT_LOGINNAME	stuser
DXAGENT_HOMEDIR	/home/users/stuser
DXAGENT_TARGET	document_12.txt
DXAGENT_TARGETPATH	/home/users/stuser
DXAGENT_TRANSFORMATION_INPUT	/home/users/stuser/PGP/encrypted.pgp

Note The variable DXAGENT_TRANSFORMATION_INPUT is only available from within a PGP transformation agent. Expressions using this variable do not evaluate correctly in other cases. In the example using this variable, assume that the original file name before encryption is original_12.txt.

The following table shows additional examples of the different expressions available for use in SecureTransport:

Example variable name	Example return value
${env['DXAGENT_TARGET']}	document_12.txt
${stenv['target']}	document_12.txt
${stenv["target"]}	document_12.txt
Prefix${stenv["target"]}.newext	Prefixdocument_12.txt.newext
${stenv.targetpath}	/home/users/stuser
${basename(stenv.target)}	document_12

Example variable name	Example return value
`${extension(stenv.target)}`	`txt`
`${filename (stenv.target).replace(' [0-9]','z').replace(' [*&_]','-')}`	`document-zz.txt`
`${basename(stenv.target)}-${random}.${extension (stenv.target)}`	`document_12-C7F2119AAECEACCDE16C496C96FEEE39.txt`
`${stenv.loginname.replace ('st', 'SecureTransport-')}`	`SecureTransport-user`
`${stenv.target.matches ('.*.txt') ? 1 : 0}`	`1`
`${stenv.target.matches ('.*.pgp') ? 1 : 0}`	`0`
`${stenv.transformation_input.matches('\*.pgp') ? 1 : 0}`	`1`
`${embedded}`	`original_12.txt`
`${basename(embedded)}-${timestamp}.${extension (embedded)}`	`original_12-1345652729052.txt`
`${basename(embedded)}-${date('yyyy.MM.dd_hhmmss')}.${extension (embedded)}`	`original_12-2012.08.22_162529.txt`
`${resolve(concat (stenv.homedir, '../..'))}`	`/home`
`${empty var ? error ('Missing Variable') : var}`	Either the value of `$var` or an exception

Appendix H: IP addresses and host names

This appendix describes valid syntax for IP addresses and host names you can use with Axway SecureTransport. In fields in the Administration Tool, you enter an IP address or host name to represent a host or server, a pattern to represent a range of IP address, or a pattern that SecureTransport matches against input data.

For details on the IP address and host name syntax formats, refer to *IP address and host name syntax* on page 1032

IP address and host name syntax

In SecureTransport, you can specify a host address in any of the following formats:

- Exact IPv4 or IPv6 address
- Range of address using Classless Inter-Domain Routing (CIDR) notation
- Range of address using IPv4 address and netmask
- Patten matching an IPv4 address
- Exact host name
- Pattern matching a host name

The following topics IP address and host name syntax usage:

- *Exact IPv4 or IPv6 address* on page 1032
- *Range of address using Classless Inter-Domain Routing notation* on page 1033
- *Range of address using IPv4 address and subnet mask* on page 1033 -
- *Patten matching an IPv4 address* on page 1033
- *Exact host name* on page 1034
- *Pattern matching a host name* on page 1034

Exact IPv4 or IPv6 address

Use an exact IPv4 or IPv6 address to specify a single server. In IPv6 addresses, two colons (`::`) can represent one sequence of zero bits.

Examples of valid values include the following:

- `172.23.34.45`
- `127.0.0.1`
- `FC00:1234:56:0:0:0:AB:EF`
- `FC00:1234:56::AB:EF`
- `::1`

Range of address using Classless Inter-Domain Routing notation

Classless Inter-Domain Routing (CIDR) notation specifies an IPv4 or IPv6 address and a number of significant bits separated by a slash (`/`). In other contexts, CIDR notation is used to specify an IP address and a subnet. For SecureTransport, use CIDR notation to represent a range of IP addresses.

Examples of valid values include the following:

- `172.23.34.0/24` represents `172.23.34.0` through `172.23.34.255`
- `FC00:1234:56::/120` represents `FC00:1234:56::` through `FC00:1234:56::FF`

Range of address using IPv4 address and subnet mask

Use an IPv4 address and a subnet mask separated by a colon (`:`) to represent a range of IPv4 addresses.

Examples of valid values include the following:

- `172.23.34.0:255.255.255.0` represents `172.23.34.0` through `172.23.34.255`
- `172.56.67.128:255.255.255.224` represents `172.56.67.128` through `172.56.67.159`

Patten matching an IPv4 address

Use an IPv4 address pattern to represent a range of IPv4 addresses. Use an asterisk (`*`) to match any sequence of octal digits.

Examples of valid values include the following:

- `172.23.34.*` represents `172.23.34.0` through `172.23.34.255`
- `172.56.*.*` represents `172.56.0.0` through `172.56.255.255`

Exact host name

Use a literal host name to represent a single host where host names are valid. The host name must resolve to a valid IPv4 or IPv6 address.

Pattern matching a host name

Use a host name pattern that uses asterisk (`*`) to represent one or more characters and question mark (`?`) to represent one character. The pattern specifies any host whose name matches. A host name pattern is valid for values that SecureTransport uses to match a host name, for example, in a user class definition.

Examples of valid values include the following:

- `*.example.com`
- `mail?.example.edu`
- `int?*`

Appendix I: Regular expressions

This appendix provides information about the syntax for regular expressions supported by Axway SecureTransport.

For matching file names with the glob pattern method, SecureTransport uses `org.apache.oro.text.GlobCompile` class. We can refer to its GlobCompiler Class javaDoc which describes the following syntax:

- `*` - Matches zero or more instances of any character.
- `?` - Matches one instance of any character.
- `[...]` - Matches any of characters enclosed by the brackets. *** and ? lose their special meanings within a character class. Additionally if the first character following the opening bracket is a ! or a ^, then any character not in the character class is matched. A between two characters can be used to denote a range. A at the beginning or end of the character class matches itself rather than referring to a range. A] immediately following the opening [matches itself rather than indicating the end of the character class, otherwise it must be escaped with a backslash to refer to itself.
- / - A backslash matches itself in most situations. But when a special character such as a *** follows it, a backslash escapes the character, indicating that the special character should be interpreted as a normal character instead of its special meaning.
- All other characters match themselves.

Examples:

- `[a-c]test*` – matches file name which include any of the letters "a", "b" or "c" , followed by the string "test". The asterisk * character means that any character(s) can follow the word "test".
- `[^a-c]d?` – matches file names which do not include any of the letters "a", "b" or "c", followed by the a single instance of the letter "d".
- `*a*` – matches file names which include any sequence of characters, which include the letter "a".
- `\*dir` – matches path names that include the string "dir".

The following topics describe the components of SecureTransport regular expressions:

- *Regular expression characters* on page 1036
- *General character classes* on page 1036
- *Predefined character classes* on page 1036
- *Boundary matches* on page 1038
- *Regular expression closures* on page 1039
- *Logical and grouping operators* on page 1039
- *Back references* on page 1040

Regular expression characters

The following table shows the variables and characters allowed within the regular expressions.

Character	Meaning
unicodeChar	Matches any identical Unicode character
\	Used to quote a meta-character (such as *)
\\	Matches a single '\' character
\0*nnn*	Matches a given octal character
\x*hh*	Matches a given 8-bit hexadecimal character
\\u*hhhh*	Matches a given 16-bit hexadecimal character
\t	Matches an ASCII tab character
\n	Matches an ASCII newline character
\r	Matches an ASCII return character
\f	Matches an ASCII form feed character

General character classes

You can specify a character class to match a set of characters.

Character class	Meaning
[abc]	Matches any character between the brackets
[a-zA-Z]	Use hyphen (-) to specify ranges of characters
[^abc]	Matches any character not specified

Predefined character classes

There is a set of predefined character classes. The following table explains these.

Character class	Meaning
`.`	Matches any character other than newline
`\w`	Matches a "word" character, alphanumeric plus underscore (_)
`\W`	Matches a non-word character
`\s`	Matches a whitespace character
`\S`	Matches a non-whitespace character
`\d`	Matches a digit character
`\D`	Matches a non-digit character
`[:alnum:]`	Alphanumeric characters *
`[:alpha:]`	Alphabetic characters *
`[:blank:]`	Space and tab characters *
`[:cntrl:]`	Control characters *
`[:digit:]`	Numeric characters *
`[:graph:]`	Characters that are printable and are also visible. (A space is printable, but not visible, while an "`a`" is both.) *
`[:javastart:]`	Start of a Java identifier *
`[:javapart:]`	Part of a Java identifier *
`[:lower:]`	Lower-case alphabetic characters *
`[:print:]`	Printable characters (characters that are not control characters) *
`[:punct:]`	Punctuation characters (characters that are not letter, digits, control characters, or space characters) *
`[:space:]`	Space characters (for example, space, tab, and form feed) *
`[:upper:]`	Upper-case alphabetic characters *
`[:xdigit:]`	Characters that are hexadecimal digits *

Character class	Meaning
\p{Alnum}	Alphanumeric characters †
\p{Alpha}	Alphabetic characters †
\p{Blank}	Space and tab characters †
\p{Cntrl}	Control characters †
\p{Digit}	Numeric characters †
\p{Graph}	Characters that are printable and are also visible. (A space is printable, but not visible, while an "a" is both.) †
\p{Lower}	Lower-case alphabetic characters †
\p{Print}	Printable characters (characters that are not control characters) †
\p{Punct}	Punctuation characters (characters that are not letter, digits, control characters, or space characters) †
\p{Space}	Space characters (for example, space, tab, and form feed) †
\p{Upper}	Upper-case alphabetic characters †
\p{Xdigit}	Characters that are hexadecimal digits †

* For regular expressions used with the Transaction Manager rule ~ (match) operator see LDAP domain DN filter (see *Manage DN filters for a domain* on page 442).

† For all other regular expressions.

Boundary matches

The following table defines boundary matches.

Character class	Meaning
\^	Matches only at the beginning of a line
\$	Matches only at the end of a line
\b	Matches only at a word boundary
\B	Matches only at a non-word boundary

Note Transaction Manager automatically places a "`\^`" at the beginning of the search string and a "`\$`" at the end of the search string. If you do not want to anchor the regular expression, you must add "`.*`" to the beginning or end:
`.*regex.*`

Regular expression closures

These match a series of characters by matching the pattern they follow zero or more time.

Character class	Meaning
`P*`	Matches the pattern `P` zero or more times
`P+`	Matches the pattern `P` one or more times
`P?`	Matches the pattern `P` zero or one times
`P{n}`	Matches the pattern `P` exactly `n` times
`P{n,}`	Matches the pattern `P` at least `n` times
`P{n,m}`	Matches the pattern `P` at least `n` but not more than *m* times.

All closure operators (`*`, `+`, `?`, `{n,m}`) are *greedy* by default, meaning that they match as many characters of the string as possible without causing the overall match to fail.

A *reluctant* closure matches as few characters of the string as possible without causing the overall match to fail. To specify a reluctant closure, append a `?` to the closure pattern. Valid patterns are `P*?`, `P+?`, and `P??`.

Logical and grouping operators

Use these items to match a sequence of characters and indicate subexpressions.

Operator	Meaning
`AB`	Matches pattern `A` followed by pattern `B`
`A|B`	Matches either pattern `A` or pattern `B`
`(A)`	Groups pattern `A` as a subexpression for other operations or for back references

Back references

Use the following character classes to refer back to subexpressions in patterns and in replacement strings.

Character class	Meaning
\1	Back reference to 1st parenthesized subexpression
\2	Back reference to 2nd parenthesized subexpression
\3	Back reference to 3rd parenthesized subexpression
\4	Back reference to 4th parenthesized subexpression
\5	Back reference to 5th parenthesized subexpression
\6	Back reference to 6th parenthesized subexpression
\7	Back reference to 7th parenthesized subexpression
\8	Back reference to 8th parenthesized subexpression
\9	Back reference to 9th parenthesized subexpression

Appendix J: Velocity email notification package

The following topics describe how to set up and configure the Velocity email notification package:

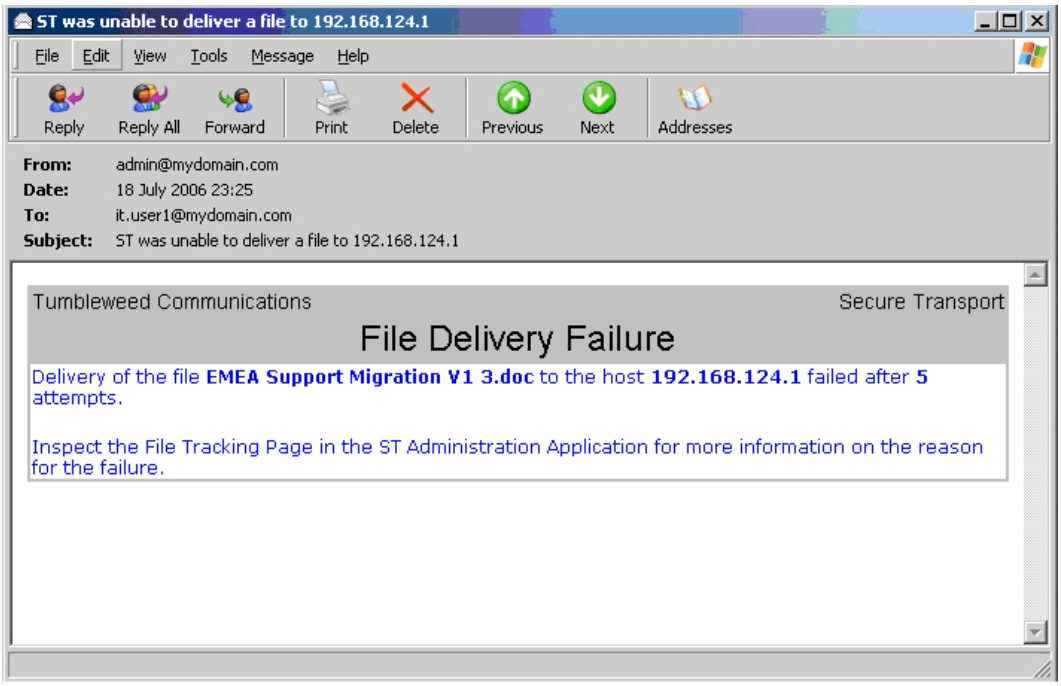
- *Email notification overview* on page 1041
- *Velocity overview* on page 1042
- *Configure the ServerTransferNotify rules package* on page 1043
- *Customize the email notification templates* on page 1044
- *Velocity troubleshooting* on page 1046

Email notification overview

There are four benefits of using this package:

- It generates HTML rather than plain text notifications.
- It utilizes notification templates that allow SecureTransport variables to be used as substitution tokens.
- The notification templates also contain meta-data to allow customizations of the email subject line and the SMTP envelope headers
- It supports attachments making it easy to attach a target file.

The following example shows what an email generated using the Velocity Email Notification package can look like:



There are many scenarios in SecureTransport which might require generating a notification. This package contains examples that show how to generate a notification when:

- A server upload delivery exhausts its retry count.
- A sender or recipient needs to be notified when a file upload or download completes

However this package is easy to use in almost any scenario.

Velocity overview

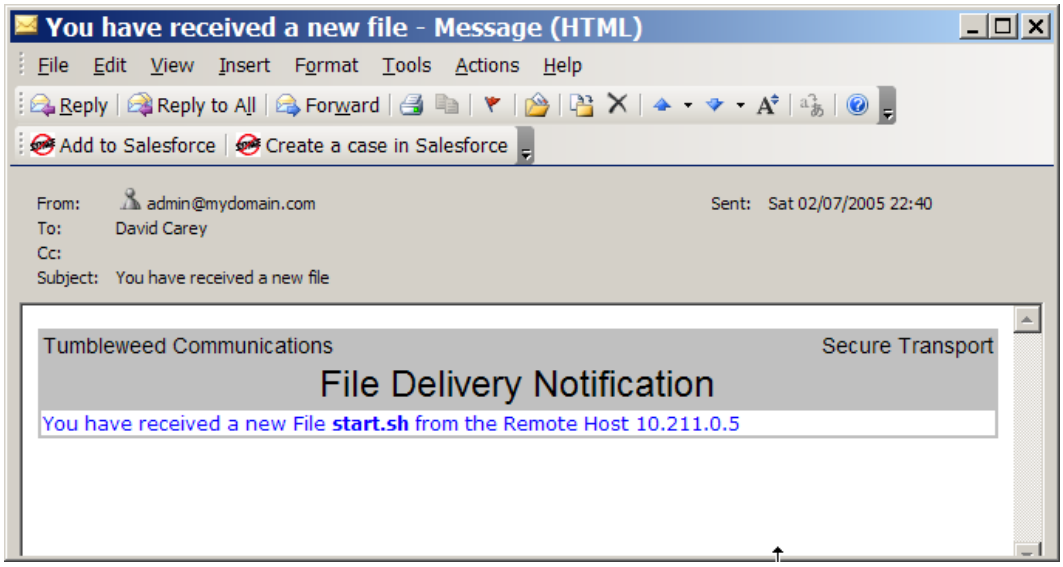
Velocity is an open source template engine provided by the Jakarta Apache Project. It uses the Velocity Template Language (VTL) which provides an easy and simple way to incorporate dynamic content in an HTML email.

VTL uses *references* to embed dynamic content into an HTML email and a variable is one type of reference. This makes it an ideal technology for integrating with the SecureTransport Server SDK as the variables can be mapped to the set of SecureTransport environment variables.

The following HTML code snippet shows a VTL statement that can be embedded in an HTML email notification generated by SecureTransport:

```
<tr id="areabody" bgcolor="white">
   <td colspan="2">
      You have received a new File <b>$DXAGENT_TARGET</b> from the
      Remote Host $DXAGENT_REMOTEHOST
   </td>
</tr>
```

When generated, the email notification displays something like the following example:



For more information, refer to the Apache Velocity Project website.

Configure the ServerTransferNotify rules package

The `ServerTransferNotify` package rule, when enabled, handles only cases where the transfer fails after it is started. The `ServerTransferNotify` rules package ships with one rule, also named `ServerTransferNotify`. This rule is configured to send an email if the server initiated upload or download operation exhausts the last retry or encounters a permanent failure.

If the SecureTransport administrator needs a way to handle all cases like wrong login credentials and both permanent and temporary failures, the following modifications can to be done:

1. Select **Setup > TM Settings** to display the *TM Settings* page.
2. Locate and disable the `ServerTransferNotify` rule package by selecting it and clicking **Disable**.
3. Locate the `FTPTransfer` rule package, select it, and click **Export** to export the package to modify it.
4. Using an external XML editor, modify the `FTPTransfer` rule package to include the following:

```
IF ( ( EventType <equal> Server Transfer - Pull OR EventType <equal>
Server Transfer - Push ) AND DXAGENT_SITE_PROTOCOL <equal> ftp ) THEN {
id=1 streaming(none)
In-process> com.tumbleweed.st.server.ftp.agent.FtpTransferAgent (
Impersonation="true" ) id=2 executeafter(1) streaming(none)
In-process> com.tumbleweed.st.server.tm.agents.RetryAgent (
Impersonation="true", dontretry="0 1 2 4 5", internalretry="6" ) id=3
```

```
executeafter(2) streaming(none)
In-process> com.tumbleweed.st.server.tm.agents.Continue ( continue="2 3 4
5" ) id=4 executeafter(3) streaming(none)
In-process> com.tumbleweed.st.server.mailer.agent.EmailNotification (
messagetemplate:-PushDeliveryFailure.xhtml, mailserver=<mailserver>,
mailfrom=<sender_email>, mailto=<recipient_email> ) }
```

5. Save the modified `FTPTransfer` rule package.
6. Import the modified `FTPTransfer` rule package into the *TM Settings* page by clicking **Import**.
7. Browse to the select the modified `FTPTransfer` rule package.
8. Select **Overwrite existing**.
9. Click **Import**.
10. Select the modified `FTPTransfer` rule package, and click **Enable**.

This procedure can be repeated on the `HttpTransfer`, `PesitTransfer`, and `SSHTransfer` rule packages.

Customize the email notification templates

The templates are located in `<FILEDRIVEHOME>/conf/mailer-templates`. You can customize the email notification template with any text or HTML editor. An HTML editor is recommended because you can use it to preview the notification before deploying it in SecureTransport.

There are seven prerequisite fields that must be set in the XHTML email notification template.

- `$subject` — The subject line for the email
- `$mailfrom` — Who the email is coming from
- `$mailto` — Who the email is going to
- `$mailserver` — The name of the local SMTP mail server that will be used to deliver the email
- `$mailserverport` — The TCP port on the SMTP server to connect to.
- `$smtpUser` — A user to be used when authenticating to an SASL-enabled SMTP server.
- `$smtpPassword` — Authentication password for the user specified in the `smtpUser` field.

The following code example shows an XHTML file with the prerequisites set:

```
<?xml version="1.0" encoding="windows-1252"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
   "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<!-- #set( $subject = "ST was unable to deliver a file to
   $DXAGENT_SITE_ATTR_HOST") -->
```

```
<!-- #set( $mailfrom = "admin@example.com") -->
<!-- #set( $mailto = $DXAGENT_ACCOUNT_EMAIL) -->
<!-- #set( $mailserver = "mail.example.com") -->
<!-- #set( $mailserverport = "25") -->
<!-- #set( $smtpUser = "user") -->
<!-- #set( $smtpPassword = "password") -->
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <meta http-equiv="Content-Type" content="text/html;
      charset=windows-1252" />
</head>
<body>
   <table border="0" bgcolor="#C0C0C0" width="100%">
      <tr id="areatop">
         <td style="text-align: left">Axway</td>
         <td style="text-align: right">SecureTransport</td>
      </tr>
      <tr id="areatopmain">
         <td colspan="2" align="center">
            File Delivery Failure
         </td>
      </tr>
      <tr id="areabody" bgcolor="white">
         <td colspan="2">
            Delivery of the file <b>$DXAGENT_TARGET</b> to the
host
            <b>$DXAGENT_SITE_ATTR_HOST</b> failed after
            <b>$DXAGENT_PERSISTED_EVENT_RETRY_COUNT</b>
attempts.
            <p>Inspect the File Tracking Page in the ST
Administration Tool
            for more information on the reason for the
failure.</p>
         </td>
      </tr>
   </table>
</body>
</html>
```

Note You can hard code the values directly into the email notification template or you can use any SecureTransport environment variable. In the previous example the `mailfrom` address is hard coded into the template, but the `mailto` address is calculated at runtime from the `$DXAGENT_ACCOUNT_EMAIL` variable.
Any value set in the Invocation Parameter for the TM rule overrides the value set in the notification template.

Velocity troubleshooting

To add additional logging of email notifications events, edit the `tm-log4j.xml` file in the `<FILEDRIVEHOME>/conf/` directory and add the following code where the original `appender` elements are located:

```
<appender name="AgentLog"
   class="com.tumbleweed.st.server.logging.DailyRollingFileAppen
der">
   <param name="File" value="/opt/TMWD/SecureTransport/var/logs/
      stx-agent.log" />
   <param name="Append" value="true" />
   <param name="DatePattern" value="'.'yyyy-MM-dd" />
   <param name="RotateDirectory"
      value="/opt/TMWD/SecureTransport/var/db/hist/logs" />

   <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d %p [%t] %c -
%m%n" />
   </layout>
</appender>
```

Add the following code at the end of the file:

```
<logger name="com.tumbleweed.st.server.util.mailer"
additivity="false">
   <level value="debug" />
   <appender-ref ref="AgentLog" />
</logger>
<logger name="javax.mail" additivity="false">
   <level value="debug" />
   <appender-ref ref="AgentLog" />
</logger>
<logger name="org.apache.commons.mail" additivity="false">
   <level value="debug" />
   <appender-ref ref="AgentLog" />
</logger>
```

This configuration creates the log file named `stx-agent.log` in the `<FILEDRIVEHOME>/SecureTransport/var/logs/` directory when SecureTransport is restarted.

Restart SecureTransport

Use the following procedure to restart SecureTransport.

1. Go to `<FILEDRIVEHOME>/bin` and execute `./stop_all`.
2. When the prompt returns, execute `./start_all`.

The file `stx-agent.log` logs all events for email notifications.

Appendix K: SSO filter mapping

An Identity Provider can return attributes attached to the authenticated user. A mapping using this attributes may be executed by the SSO agent before they are transmitted to the application.

Two kinds of mapping are supported: *Rename* mapping and *Filter* mapping.

Rename mapping

With this mapping, you can rename an attribute from the Identity Provider, keeping its value.

Filter mapping

This mapping creates output attributes when a filter matches the input attributes from the Identity Provider.

Note Currently, the output attribute value is fixed. It cannot take the value from an input attribute.

Filter syntax

Only a subset of the full syntax is supported as described below. A filter consists of one or more criteria. If more than one criterion exist in one filter definition, they can be concatenated by logical operators.

Criteria

The criteria have to be put in parentheses. A criteria can only be an equality.

Example:

```
(givenName=Sandra)
```

Operators

The logical operators are always placed in front of the criteria. The whole term have to be put in parentheses.

AND Operator

`(&(criteria1)(criteria2))` means: criteria1 AND criteria2

With more than two criteria: `(&(criteria1)(criteria2)(criteria3)(criteria n)`

OR Operator

`(|(criteria1)(criteria2))` means: criteria1 OR criteria2

With more than two criteria: `(|(criteria1)(criteria2)(criteria3)(criteria n))`

NOT Operator

`(!(criteria1)` means NOT criteria1

Nested Operators

`(&(|(criteria1) (criteria2))(|(criteria3) (criteria4)))` means : (criteria1 OR criteria2) AND (criteria3 OR criteria4)

Examples

Rename the *user* attribute to *username*:

```
<Mappings>
    <RenameMapping source="user" target="username"/>
</Mappings>
```

Add two attributes when the name attribute from the Identity Provider is set to Bob:

```
<Mappings>
    <FilterMapping>
        <Filter>(name=Bob)</Filter>
        <OutputAttribute name="role">SPRole</OutputAttribute>
        <OutputAttribute name="user">Bob</OutputAttribute>
    </FilterMapping>
</Mappings>
```

Appendix L: Sample SSO configuration file for administrators

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- This is a sample file for SSO configuration for Admin component. -->
<SSOConfiguration>

    <!--
         Configures certificate validation. Validates the Service Provider and
Identity Providers certificates specified in its configuration. Validation
happens at start-up and at regular intervals. Optional.
    -->
    <!--
         Attributes:
         1) trustStoreInitializer - Set
com.axway.st.server.sso.impl.TrustStoreInitializer value for
trustStoreInitializer in order to use SecureTransport trust store. Recommended
value: com.axway.st.server.sso.impl.TrustStoreInitializer
         2) delayBetweenValidations - Defines at which interval certificates
validation occurs, in hours. Default value is 3 hours.
    -->
    <CertificateValidation
            trustStoreInitializer="com.axway.st.server.sso.impl.TrustStoreInitializer"
            delayBetweenValidations="3">
    </CertificateValidation>

    <!-- Configures the service provider. -->
    <!--
    Main attributes:
        entityId - Sets the unique identifier of the service provider. This
identifier is sent to the Identity Provider so it can know who is requesting an
authentication or a logout. This identifier is used by the Identity Provider to
differentiate what Service Provider is requesting an authentication or a
logout.
        filteredUri - Specifies the URI of the authentication process entry
point. The value must be /*
        logoutUri - Specifies the URI which triggers logout process. The value
must be /logout.
        logoutRedirectUri - Specifies the URI to redirect to the initial logout
message generated. In turn that message will be redirected to a Identity
Provider. The value must be /coreadmin/.
        keystoreInitializer - Configures key store to use. That key store keeps
key-pairs taking part in authentication process. Set
com.axway.st.server.sso.impl.KeyStoreInitializer value in order to use
SecureTransport local key store.
        keyAlias - Specifies key alias of the private key used to decrypt SAML
```

```
messages and assertions and to sign SAML messages and assertions.
        sessionIdCookieName - Sets the name of the cookie to store the SSO
session identifier if sessions are managed by the SSO module.
     -->
    <ServiceProvider
            entityId="st.sso.admin"
            filteredUri="/*"
            logoutUri="/logout"
            logoutRedirectUri="/coreadmin"
keystoreInitializer="com.axway.st.server.sso.impl.KeyStoreInitializer"
            keyAlias="ssokey"
            sessionIdCookieName="STAdminSsoCookie"
            useAppSessions="false"
            >

        <!-- Specifies an entry points for receiving SAML Assertions from the
Identity Provider. The below tags are recommended. -->
        <AssertionConsumerService
binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
location="/saml2/sso/post/j_security_check"/>
        <AssertionConsumerService
binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
location="/saml2/sso/redirect/j_security_check"/>
        <AssertionConsumerService
binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-PAOS"
location="/saml2/sso/paos/j_security_check"/>
        <SingleLogoutService
binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
location="/saml2/slo/post/j_security_check"/>
        <SingleLogoutService
binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
location="/saml2/slo/redirect/j_security_check"/>

        <!-- Features tag is optional - Here are the default values -->
        <Features>

            <!-- Configures the session cookie whether to be set with Secure
flag. Recommended value: true. -->
            <Feature key="secure-cookie" value="true" />

            <!--
                 Type of unique identifier generator to use to assign ids to
SAML messages. The value must be com.axway.st.server.sso.impl.UIDGenerator
            -->
            <Feature key="uid-generator"
value="com.axway.st.server.sso.impl.UIDGenerator" />
        </Features>

        <!--
            Identity Provider resolution provides support for choosing the
right Identity Provider based on configuration and run-time metadata. If such
```

```
resolution is not present, the first Identity Provider is selected among ones
specified under IdentityProviders element below.
            The supported ways to do that are by:
            1) Query parameter provided by a user request (see the example
below).
            2) Header value provided by a user request. An example follow:
                <Header name="idp_id">
                    <Mapping value="keycloakIdp"
entityId="https://st.keycloak.axway.int/" />
                    <Mapping value="shibbolethIdp"
entityId="https://st.shibboleth.axway.int/" />
                </Header>
                In the example above if a user authentication request has
header with name 'idp_id' and corresponding value equals to 'keycloakIdp', then
Identity Provider with entityId equals to https://st.keycloak.axway.int/ will
be chosen to authenticate the user agent.
           Note: Only one of these way can be done.
        -->
        <IdentityProviderResolution>
            <!--
                 Identity provider mapping using a query parameter. The name of
query parameter resolution will be searched for in request parameters during
runtime and its value should match to the value attribute of a Mapping element.
If both query parameter name and value match, then corresponding entityId is
used to select Identity Provider.
                 Examples:
                         1) https://localhost/?idp_id=keycloakIdp in the below
case will match the Identity provider with
entityId=https://st.keycloak.axway.int/
                         2) https://localhost/?idp_id=shibbolethIdp in the
below case will match the Identity provider with
entityId=https://st.shibboleth.axway.int/
             -->
            <QueryParameter name="idp_id">
                <!-- Note: The name of the query parameter/header should match
the value of the ST configuration option
LoginSettings.Admin.SSO.idpResolverKey. -->
                <!-- Note: Ensure the name of the query parameter/header to be
different than ST configuration option LoginSettings.Admin.SSO.localIdpId in
order to be able to configure selection of ST as local authentication provider
and SSO Identity Providers. -->
                <Mapping value="keycloakIdp"
entityId="https://st.keycloak.axway.int/" />
                <Mapping value="shibbolethIdp"
entityId="https://st.shibboleth.axway.int/" />
            </QueryParameter>
        </IdentityProviderResolution>

        <!--
```

```
            This element is optional.
            Tenant resolution provides support for choosing the right Identity
Provider based on configuration and run-time metadata. If both tenant
resolution and identity provider resolutions are present, then tenant
resolution takes precedence. Tenants are defined inside Identity Providers so
resolving the IdP in turn will resolve a tenant.
            The supported ways to do that are by:
            1) QueryParameter
                <QueryParameter name="idp_id">
                    <Mapping tenant="Axway"
entityId="https://st.keycloak.axway.int/" />
                    <Mapping tenant="Sopra"
entityId="https://st.shibboleth.axway.int/" />
                </QueryParameter>
            2) Header (example below)
            Notes:
                  1) Only one of these way can be done.
                  2) Header evaluation takes precedence on query parameter one.
                  3) If mapping is not present, IdentityProviderResolution is
used.
                     If IdentityProviderResolution is not present first listed
IdP is used.
        -->
        <TenantResolution>
            <!-- Note: The name of the query parameter/header should match the
value of the ST configuration option LoginSettings.Admin.SSO.idpResolverKey. --
>
            <!-- Note: Ensure the name of the query parameter/header to be
different than ST configuration option LoginSettings.Admin.SSO.localIdpId in
order to be able to configure selection of ST as local authentication provider
and SSO Identity Providers. -->
            <Header name="idp_id">
                <Mapping tenant="Axway"
entityId="https://st.keycloak.axway.int/" />
                <Mapping tenant="Sopra"
entityId="https://st.shibboleth.axway.int/" />
            </Header>
        </TenantResolution>
    </ServiceProvider>

    <!-- Identity provider definitions. Configures various aspects of
interaction with identity providers. -->
    <IdentityProviders>
        <!-- A SAML sample IdP definition. -->
        <!--
        Main attributes:
            entityId - Sets the unique identifier of the service provider. This
identifier is sent to the Identity Provider so it can know who is requesting an
authentication or a logout. Add here EntityDescriptor entityID value, from the
idpMetadata.xml
            metadataUrl - Specify the relative location of the metadata file.
```

```
Specifies a relative location of the metadata file to sso-admin.xml file.
                     NOTE: ST does not support the metadata URL to be a HTTP
site.
            verifyAssertionExpiration - Turn on/off verification of the
validity period of assertions. Consider to set to false if service provider and
identity provider times are not synchronized. Default: true.
            sign - If set to true, all SAML messages and their assertions sent
by the service provider will be signed. There are a couple of features (see
below) for fine-grained control of signing. Optional - if not present, default
value is false.
            userNameAttribute - Sets the name of the identity provider
attribute that provides the user name.
         -->

         <!-- Sample Keycloak Identity provider definition. -->
        <SamlIdentityProvider
                entityId="https://st.keycloak.axway.int/"
                metadataUrl="./keycloak-idp-metadata.xml"
                verifyAssertionExpiration="false"
                sign="true">

            <!-- Mappings tag is optional -->
            <Mappings>
                <!-- NOTE: SecureTransport does not support the attribute
mapping for Admin component. -->
            </Mappings>

            <!-- Features control specific behavior of SAML message processing. -->
            <Features>
                <!-- Allows interaction with the IdP by plain HTTP. Default:
false. -->
                <Feature key="saml-allow-http-connection" value="false"/>

                <!-- Allows unsigned assertions in messages received from the
Identity Provider. Default: false. -->
                <Feature key="saml-allow-unsigned-assertion" value="false"/>

                <!--
                    Enable or disable the signature verification of the
metadata file and the certification path of the certificate used to sign. Set
to false if metadata file is not signed. Default: true.
                -->
                <Feature key="saml-verify-metadata-signature" value="false"/>

                <!--
                    Enable or disable signing of Authentication Request
messages. Presence of this feature and its value overrides the meaning of sign
attribute of IdentityProvider element above.
                -->
                <Feature key="saml-sign-authnrequest" value="true"/>

                <!--
                    Enable or disable signing of Logout Request messages.
Presence of this feature and its value overrides the meaning of sign attribute
of IdentityProvider element above.
```

```
                 -->
                <Feature key="saml-sign-logoutrequest" value="true"/>

                <!--
                    Enable or disable signing of Logout Response messages.
Presence of this feature and its value overrides the meaning of sign attribute
of IdentityProvider element above.
                -->
                <Feature key="saml-sign-logoutresponse" value="true"/>

            </Features>
        </SamlIdentityProvider>

        <!-- Sample Shibboleth Identity provider definition. -->
        <SamlIdentityProvider
                entityId="https://st.shibboleth.axway.int/"
                metadataUrl="./shibboleth-idp-metadata.xml"
                verifyAssertionExpiration="false"
                userNameAttribute="urn:oid:0.9.2342.19200300.100.1.1"
                sign="true" >

            <!-- Mappings tag is optional -->
            <Mappings>
                <!-- NOTE: SecureTransport does not support the attribute
mapping for Admin component. -->
            </Mappings>

            <!-- Features control specific behaviour of SAML message
processing. -->
            <Features>
                <!-- Allows interaction with the IdP by plain HTTP. Default:
false. -->
                <Feature key="saml-allow-http-connection" value="false"/>

                <!-- Allows unsigned assertions in messages received from the
Identity Provider. Default: false. -->
                <Feature key="saml-allow-unsigned-assertion" value="false"/>

                <!--
                    Enable or disable the signature verification of the
metadata file and the certification path of the certificate used to sign. Set
to false if metadata file is not signed. Default: true.
                -->
                <Feature key="saml-verify-metadata-signature" value="false"/>

                <!--
                    Enable or disable signing of Authentication Request
messages. Presence of this feature and its value overrides the meaning of sign
attribute of IdentityProvider element above.
                -->
                <Feature key="saml-sign-authnrequest" value="true"/>

                <!--
                    Enable or disable signing of Logout Request messages.
Presence of this feature and its value overrides the meaning of sign attribute
of IdentityProvider element above.
```

```
                 -->
                <Feature key="saml-sign-logoutrequest" value="true"/>
                <!--
                    Enable or disable signing of Logout Response messages.
Presence of this feature and its value overrides the meaning of sign attribute
of IdentityProvider element above.
                -->
                <Feature key="saml-sign-logoutresponse" value="true"/>
            </Features>
        </SamlIdentityProvider>
    </IdentityProviders>
</SSOConfiguration>
```

Appendix M: Sample SSO configuration file for end-users

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- This is a sample file for SSO configuration for End-user component. -->
<SSOConfiguration>

    <!--
         Configures certificate validation. Validates the Service Provider and
Identity Providers certificates specified in its configuration. Validation
happens at start-up and at regular intervals. Optional.
    -->
    <!--
         Attributes:
         1) trustStoreInitializer - Set
com.axway.st.server.sso.impl.TrustStoreInitializer value for
trustStoreInitializer in order to use SecureTransport trust store. Recommended
value: com.axway.st.server.sso.impl.TrustStoreInitializer
         2) delayBetweenValidations - Defines at which interval certificates
validation occurs, in hours. Default value is 3 hours.
    -->
    <CertificateValidation
trustStoreInitializer="com.axway.st.server.sso.impl.TrustStoreInitializer"
            delayBetweenValidations="3">
    </CertificateValidation>

    <!-- Configures the service provider. -->
    <!--
    Main attributes:
        entityId - Sets the unique identifier of the service provider. This
identifier is sent to the Identity Provider so it can know who is requesting an
authentication or a logout. This identifier is used by the Identity Provider to
differentiate what Service Provider is requesting an authentication or a
logout.
        filteredUri - Specifies the URI of the authentication process entry
point. The value must be /*
        logoutUri - Specifies the URI which triggers logout process. The value
must be /logout.
        logoutRedirectUri - Specifies the URI to redirect to the initial logout
message generated. In turn that message will be redirected to a Identity
Provider. The value must be /logoutRedirect.
        keystoreInitializer - Configures key store to use. That key store keeps
key-pairs taking part in authentication process. Set
com.axway.st.server.sso.impl.KeyStoreInitializer value in order to use
SecureTransport local key store.
        keyAlias - Specifies key alias of the private key used to decrypt SAML
```

```
messages and assertions and to sign SAML messages and assertions.
        sessionIdCookieName - Sets the name of the cookie to store the SSO
session identifier if sessions are managed by the SSO module.
     -->
    <ServiceProvider
            entityId="st.sso.enduser"
            filteredUri="/*"
            logoutUri="/logout"
            logoutRedirectUri="/logoutRedirect"
            keystoreInitializer="com.axway.st.server.sso.impl.KeyStoreInitializer"
            keyAlias="ssokey"
            sessionIdCookieName="STEndUserSsoCookie"
            useAppSessions="false"
            >

        <!-- Specifies an entry points for receiving SAML Assertions from the
Identity Provider. The below tags are recommended. -->
        <AssertionConsumerService
binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
location="/saml2/sso/post"/>
        <AssertionConsumerService
binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
location="/saml2/sso/redirect"/>
        <AssertionConsumerService
binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS"
location="/saml2/sso/paos"/>
        <SingleLogoutService
binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
location="/saml2/slo/post"/>
        <SingleLogoutService
binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
location="/saml2/slo/redirect"/>
        <!-- Features tag is optional - Here are the default values -->
        <Features>

            <!-- Configures the session cookie whether to be set with Secure
flag. Recommended value: true. -->
            <Feature key="secure-cookie" value="true" />

            <!--
                 Type of unique identifier generator to use to assign ids to
SAML messages. The value must be com.axway.st.server.sso.impl.UIDGenerator
            -->
            <Feature key="uid-generator"
value="com.axway.st.server.sso.impl.UIDGenerator" />
        </Features>

        <!--
            Identity Provider resolution provides support for choosing the
right Identity Provider based on configuration and run-time metadata.
```

```
            If such resolution is not present, the first Identity Provider is
selected among ones specified under IdentityProviders element below.
            The supported ways to do that are by:
            1) Query parameter provided by a user request (see the example
below).
            2) Header value provided by a user request. An example follow:
                <Header name="idp_id">
                    <Mapping value="keycloakIdp"
entityId="https://st.keycloak.axway.int/" />
                    <Mapping value="shibbolethIdp"
entityId="https://st.shibboleth.axway.int/" />
                    <Mapping value="kerbIdP" entityId="kerberos" />
                </Header>
                In the example above if a user authentication request has
header with name 'idp_id' and corresponding value equals to 'keycloakIdp', then
Identity Provider with entityId equals to https://st.keycloak.axway.int/ will
be chosen to authenticate the user agent.
           Note: Only one of these way can be done.
        -->
        <IdentityProviderResolution>
            <!--
                 Identity provider mapping using a query parameter. The name of
query parameter resolution will be searched for in request parameters during
runtime and its value should match to the value attribute of a Mapping element.
If both query parameter name and value match, then corresponding entityId is
used to select Identity Provider.
                 Examples:
                         1) https://localhost/?idp_id=keycloakIdp in the below
case will match the Identity provider with
entityId=https://st.keycloak.axway.int/
                         2) https://localhost/?idp_id=shibbolethIdp in the
below case will match the Identity provider with
entityId=https://st.shibboleth.axway.int/
                         3) https://localhost/?idp_id=kerbIdP in the below case
will match the Identity provider with entityId=kerberos
             -->
            <QueryParameter name="idp_id">
                <!-- Note: The name of the query parameter/header should match
the value of the ST configuration option
LoginSettings.EndUser.SSO.idpResolverKey. -->
                <!-- Note: Ensure the name of the query parameter/header to be
different than ST configuration option LoginSettings.EndUser.SSO.localIdpId in
order to be able to configure selection of ST as local authentication provider
and SSO Identity Providers. -->
                <Mapping value="keycloakIdp"
entityId="https://st.keycloak.axway.int/" />
                <Mapping value="shibbolethIdp"
entityId="https://st.shibboleth.axway.int/" />
                <Mapping value="kerbIdP" entityId="kerberos" />
            </QueryParameter>
        </IdentityProviderResolution>
```

```
        <!--
            This element is optional.
            Tenant resolution provides support for choosing the right Identity
Provider based on configuration and run-time metadata.
            If both tenant resolution and identity provider resolutions are
present, then tenant resolution takes precedence.
            Tenants are defined inside Identity Providers so resolving the IdP
in turn will resolve a tenant.
            The supported ways to do that are by:
            1) QueryParameter
                <QueryParameter name="idp_id">
                    <Mapping tenant="Axway"
entityId="https://st.keycloak.axway.int/" />
                    <Mapping tenant="Sopra"
entityId="https://st.shibboleth.axway.int/" />
                    <Mapping tenant="Apple" entityId="kerberos" />
                </QueryParameter>
            2) Header (example below)
            Notes:
                  1) Only one of these way can be done.
                  2) Header evaluation takes precedence on query parameter one.
                  3) If mapping is not present, IdentityProviderResolution is
used.
                     If IdentityProviderResolution is not present first listed
IdP is used.
        -->
        <TenantResolution>
            <!-- Note: The name of the query parameter/header should match the
value of the ST configuration option LoginSettings.EndUser.SSO.idpResolverKey.
-->
            <!-- Note: Ensure the name of the query parameter/header to be
different than ST configuration option LoginSettings.EndUser.SSO.localIdpId in
order to be able to configure selection of ST as local authentication provider
and SSO Identity Providers. -->
            <Header name="idp_id">
                <Mapping tenant="Axway"
entityId="https://st.keycloak.axway.int/" />
                <Mapping tenant="Sopra"
entityId="https://st.shibboleth.axway.int/" />
                <Mapping tenant="Apple" entityId="kerberos" />
            </Header>
        </TenantResolution>
    </ServiceProvider>

    <!-- Identity provider definitions. Configures various aspects of
interaction with identity providers. -->
    <IdentityProviders>
        <!--
        Main attributes:
            entityId - Sets the unique identifier of the service provider. This
```

```
identifier is sent to the Identity Provider so it can know who is requesting an
authentication or a logout. Add here EntityDescriptor entityID value, from the
idpMetadata.xml
            metadataUrl - Specify the relative location of the metadata file.
Specifies a relative location of the metadata file to sso-enduser.xml file.
                        NOTE: ST does not support the metadata URL to be a HTTP
site.
            configurationUrl - should be an absolute path to Kerberos
configuration file.
                        NOTE: ST does not support the configuration URL to be a
network path.
            verifyAssertionExpiration - Turn on/off verification of the
validity period of assertions. Consider to set to false if service provider and
identity provider times are not synchronized. Default: true.
            sign - If set to true, all SAML messages and their assertions sent
by the service provider will be signed. There are a couple of features (see
below) for fine-grained control of signing. Optional - if not present, default
value is false.
            userNameAttribute - Sets the name of the identity provider
attribute that provides the user name.
         -->

         <!-- Sample Keycloak Identity provider definition. -->
        <SamlIdentityProvider
                entityId="https://st.keycloak.axway.int/"
                metadataUrl="./keycloak-idp-metadata.xml"
                verifyAssertionExpiration="false"
                sign="true">

            <!-- Mappings tag is optional -->
            <Mappings>
                <!-- Filter mapping is optional. -->
                <FilterMapping>
                    <Filter>(department=426 AXW RD SOFIA)</Filter>
                    <OutputAttribute name="role">Developer</OutputAttribute>
                </FilterMapping>

                <!-- With this mapping, you can rename an attribute from the
Identity Provider, keeping its value. -->
                <!--
                     A system attributes mapping.
                     For email, UID, GID and homeDir ST expects the following
renaming.
                -->
                <RenameMapping source="email" target="fdxEmail" />
                <RenameMapping source="uid" target="fdxUid" />
                <RenameMapping source="gid" target="fdxGid" />
                <RenameMapping source="homeDir" target="fdxHomeDir" />
                <!-- Custom attributes mapping examples (optional).-->
                <RenameMapping source="department" target="department" />
                <RenameMapping source="username" target="username" />
                <RenameMapping source="full name" target="fullName" />
                <RenameMapping source="last name" target="lastName" />
```

```
            </Mappings>

            <!-- Features control specific behavior of SAML message processing.
-->
            <Features>
                <!-- Allows interaction with the IdP by plain HTTP. Default:
false. -->
                <Feature key="saml-allow-http-connection" value="false"/>

                <!-- Allows unsigned assertions in messages received from the
Identity Provider. Default: false. -->
                <Feature key="saml-allow-unsigned-assertion" value="false"/>

                <!--
                    Enable or disable the signature verification of the
metadata file and the certification path of the certificate used to sign. Set
to false if metadata file is not signed. Default: true.
                -->
                <Feature key="saml-verify-metadata-signature" value="false"/>

                <!--
                    Enable or disable signing of Authentication Request
messages. Presence of this feature and its value overrides the meaning of sign
attribute of IdentityProvider element above.
                -->
                <Feature key="saml-sign-authnrequest" value="true"/>

                <!--
                    Enable or disable signing of Logout Request messages.
Presence of this feature and its value overrides the meaning of sign attribute
of IdentityProvider element above.
                 -->
                <Feature key="saml-sign-logoutrequest" value="true"/>

                <!--
                    Enable or disable signing of Logout Response messages.
Presence of this feature and its value overrides the meaning of sign attribute
of IdentityProvider element above.
                -->
                <Feature key="saml-sign-logoutresponse" value="true"/>

            </Features>
        </SamlIdentityProvider>

        <!-- Sample Shibboleth Identity provider definition. -->
        <SamlIdentityProvider
                entityId="https://st.shibboleth.axway.int/"
                metadataUrl="./shibboleth-idp-metadata.xml"
                verifyAssertionExpiration="false"
                userNameAttribute="urn:oid:0.9.2342.19200300.100.1.1"
                sign="true" >

            <!-- Mappings tag is optional -->
            <Mappings>
                <!-- Filter mapping is optional. -->
```

```
                <FilterMapping>
                    <Filter>(department=R&amp;amp;D)</Filter>
                    <OutputAttribute
name="rolename">Developer</OutputAttribute>
                </FilterMapping>
                <!-- A system attributes mapping. -->
                <RenameMapping source="email" target="fdxEmail" />
                <RenameMapping source="uid" target="fdxUid" />
                <RenameMapping source="gid" target="fdxGid" />
                <RenameMapping source="homeDir" target="fdxHomeDir" />
                <!-- Custom attributes mapping (optional).-->
                <RenameMapping source="department" target="department" />
                <RenameMapping source="username" target="username" />
                <RenameMapping source="full name" target="fullName" />
                <RenameMapping source="last name" target="lastName" />
            </Mappings>

            <!-- Features control specific behaviour of SAML message
processing. -->
            <Features>
                <!-- Allows interaction with the IdP by plain HTTP. Default:
false. -->
                <Feature key="saml-allow-http-connection" value="false"/>

                <!-- Allows unsigned assertions in messages received from the
Identity Provider. Default: false. -->
                <Feature key="saml-allow-unsigned-assertion" value="false"/>

                <!--
                    Enable or disable the signature verification of the
metadata file and the certification path of the certificate used to sign. Set
to false if metadata file is not signed. Default: true.
                -->
                <Feature key="saml-verify-metadata-signature" value="false"/>

                <!--
                    Enable or disable signing of Authentication Request
messages. Presence of this feature and its value overrides the meaning of sign
attribute of IdentityProvider element above.
                -->
                <Feature key="saml-sign-authnrequest" value="true"/>

                <!--
                    Enable or disable signing of Logout Request messages.
Presence of this feature and its value overrides the meaning of sign attribute
of IdentityProvider element above.
                 -->
                <Feature key="saml-sign-logoutrequest" value="true"/>

                <!--
                    Enable or disable signing of Logout Response messages.
Presence of this feature and its value overrides the meaning of sign attribute
of IdentityProvider element above.
                -->
```

```
                <Feature key="saml-sign-logoutresponse" value="true"/>
            </Features>
        </SamlIdentityProvider>
        <!-- A Kerberos IdP sample definition. -->
        <KerberosIdentityProvider
                entityId="kerberos"
configurationUrl="C:/Axway/SecureTransport/STServer/conf/sso/krb5-login.conf">
        </KerberosIdentityProvider>
    </IdentityProviders>
</SSOConfiguration>
```