SecureTransport

Version 5.4

2 April 2024

Security Guide

This documentation describes the following Axway software:

Axway SecureTransport 5.4

Revision history

The following changes are added to the SecureTransport 5.4 Security Guide:

SecureTransport version	Document revision number	Topics added/updated
5.4	5.4.01 – initial version	
5.4	5.4.02	*SecureTransport cipher suites* on page 36 added
5.4	5.4.03	*Security best practices* on page 30 updated
5.4	5.4.04	*SecureTransport cipher suites* on page 36 updated
5.4	5.4.05	New topic added: *Security-related HTTP headers and policies* on page 25
5.4	5.4.06	*Security-related HTTP headers and policies* on page 25 updated with details on how to enable CSRF token protection
5.4	5.4.07 - current version	*SecureTransport cipher suites* on page 36 updated

Contents

Preface

This guide describes the secure development life cycle, certifications and compliance, security features, identity and access management (IAM), security configuration, and security best practices for the SecureTransport product.

Who should read this document

This guide is intended for system administrators responsible for network security and secure operations of the SecureTransport product.

Related documentation

SecureTransport provides the following documentation:

- *SecureTransport Administrator's Guide* – 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 document) 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 document) 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 knowledgebase 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

Training

Axway offers training across the globe, including on-site instructor-led classes and self-paced online learning. For details, go to training.axway.com

Security introduction 1

This guide provides instructions and recommendations to help you strengthen the security of SecureTransport. Security descriptions include:

- How the product was developed in a secure way
- A list of main security features
- Secure configuration parameters, including the Secure by Default configuration
- Identity and Access Management in this product
- Best practices to use this product in a secure way

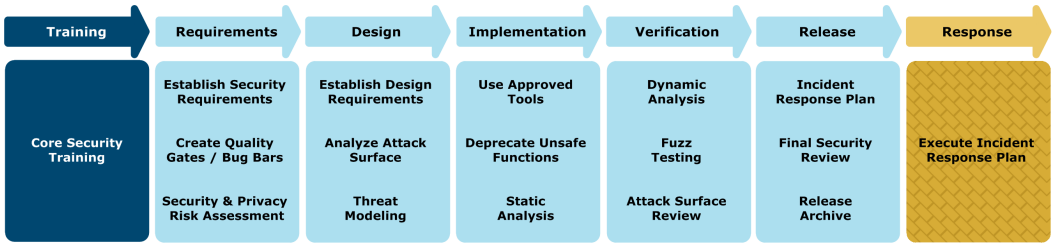
This document is targeted to the following audiences:

- Security teams in charge of auditing the security of the product
- Global network engineers
- Product administrators

Secure Development Lifecycle 2

Axway implements a Secure Development Lifecycle (SDL) in product development. A dedicated Axway team, the Product Security Group (PSG), manages the SDL in association with all the Research and Development (R&D) product teams.

The SDL consists of a set of standard phases and processes. In this spiral development model, requirements and design are frequently revisited to ensure that risks are assessed and eliminated. The following diagram illustrates the simplified Microsoft SDL model that Axway follows.



Axway development teams follow Agile practices and implement SDL processes and controls throughout the development lifecycle. For example, threat-modeling is an important part of the design phase and a final security review is required before product release. These processes and control points ensure that products meet the initial security requirements and pass the technical criteria established by PSG and the larger security community.

Development teams use a broad suite of industry-standard tools in the implementation and verification phases of the SDL. Teams run both static and dynamic analysis tools to identify potential code weaknesses and to discover security issues that could be exposed at run-time. The R&D Teams also run suites of attack surface tools and penetration testing tools on products to ensure that they meet gating criteria defined by PSG via the SDL. Teams also run other enhanced test scenarios required by our most security-conscious customers. Axway provides tool suite information and our customized usage profiles on request.

Axway's new product introduction (NPI) process supports the release of new products and major product revisions. This process requires a final security review that includes development and test artifacts. The NPI also ensures that the SDL is started early in development to optimize the delivery of secured products for you, our customer.

Certifications 3

This topic provides information about the certifications SecureTransport has received.

FIPS 140-2

SecureTransport 5.4 can be configured to use only FIPS 140-2 Level 1 certified cryptographic libraries. The FIPS certified cryptographic module SecureTransport uses is Security Builder® FIPS Java Module Version 2.8

Certification number: 1637

Date of certification: 08/24/2012

Other Certifications

SecureTransport5.4 also has the following certifications:

- AS2 certification, by Drummond Group

Security features 4

This product contains the following security features:

- Secure connections, see *Secure connections* on page 13
- Password management, see *Password management* on page 13
- Certificate management, see *Certificate management* on page 14
- Identity and access management, see *Identity and Access Management* on page 14
- Other security features, see *Other security features* on page 15

Secure connections

The following secure connections are available:

- Connections between the UI and the server are TLS secured.
- Outbound connection over any supported protocols (FTP, HTTP, AS2, PeSIT) can be SSL\TLS secured. SFTP and SCP implement Forward Secrecy and are secured via the SSH protocol by default.

  Note Cookies issued over HTTPS use the HTTP Strict Transport Security (HSTS) flag. Additionally, HSTS and HTTPOnly headers are added to the issued cookies for the administrator and end-user HTTP listeners.

- Inbound connections over any supported protocols can be TLS secured. SFTP and SCP use transport security by default and don't need to be secured explicitly.
- Connections to LDAP servers can be TLS secured.
- Connections to ICAP servers can be TLS secured.
- Connection to Sentinel can be TLS secured.
- When SecureTransport is integrated with Central Governance, the connection between both products is TLS secured using mutual authentication.
- Connections to external databases are TLS secured.

Password management

The following password features are available:

- Every user password is stored hashed (PBKDF2).
- Passwords for virtual users are salted using PBKDF2. The number of salt interations can be configured by changing the value of the `Security.Passwords.PBKDF2.Iterations` configuration parameter in the SecureTransport Administration Tool. The value default is 1000.

Certificate management

Certificate management can either be performed internally in the product or using Central Governance or with a supported Hardware Security Module (HSM) with several limitations.

Central Governance

Certificates generated by Central Governance and deployed in SecureTransport by flows with mutual authentication, are stored in the JKS keystore persisted in the database. The revocation list and certificate path are not checked.

Central Governance is responsible for managing such certificates. For example, when a certificate has expired, it must be re-generated by Central Governance and the flow using it must be re-deployed.

HSM

SecureTransport supports HSM key management of local certificates. Storing any other type of certificates on HSM is not supported. Only the FTP and HTTP protocol servers can be configured with HSM support.

When not using HSM or Central Governance

Certificates are stored in JKS keystore persisted in the database.

- The revocation list and certificate path are not checked.

Identity and Access Management

Identity and Access Management can either be performed internally in the product using SSO (SiteMinder) or LDAP.

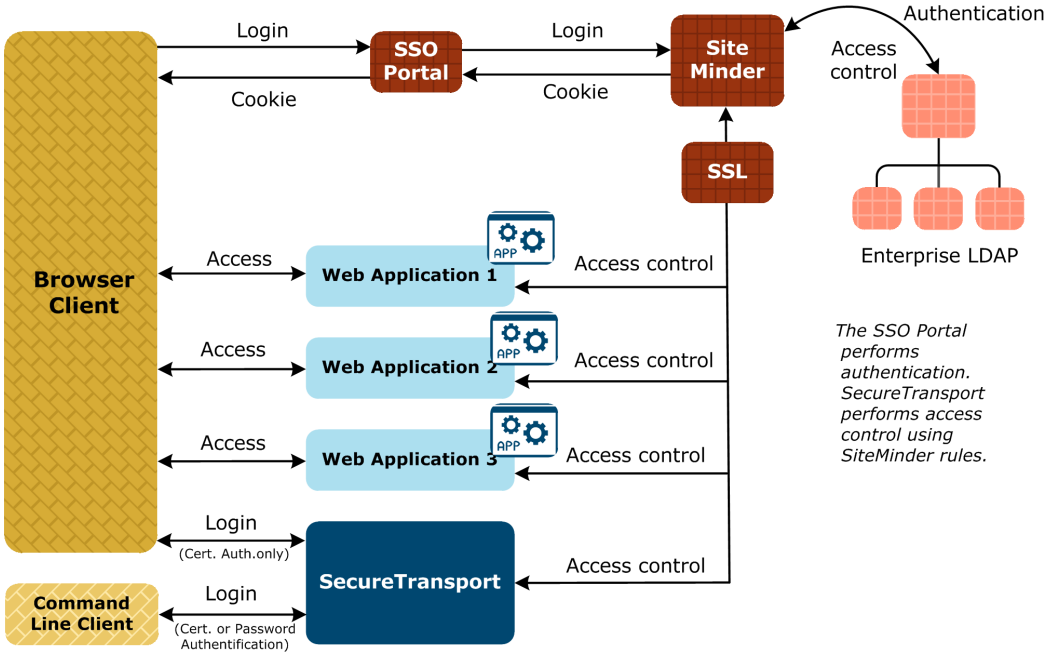
Internally

The following features are available:

- Passwords are stored internally in the database and are hashed using PBKDF2.
- Flexible access restrictions and permission can be configured on per user basis or on a larger scale – user classes and group id.

SiteMinder

SecureTransport can be integrated into a SiteMinder SSO environment and use SiteMinder to authenticate and authorize all supported client protocols. For more information, refer to the *SiteMinder integration* chapter in the *SecureTransport Administrator's Guide*.



LDAP

SecureTransport can be configured to use Lightweight Directory Access Protocol (LDAP) servers to authenticate users and to set up the user session. For more information, refer to the *LDAP integration* chapter in the *SecureTransport Administrator's Guide*.

Other security features

The following features are available:

- ICAP - For more information, refer to the *ICAP settings* section in the *Setup* chapter of the *SecureTransport Administrator's Guide*.
- Email/SNMP/Sentinel notifications on various events - For more information, refer to the *Manage accounts* chapter in the *SecureTransport Administrator's Guide*.

- DMZ support - For additional information, refer to the *Transaction Manager protocol and proxy server communication section* in the *Setup* chapter of the *SecureTransport Administrator's Guide*.

Identity and access management 5

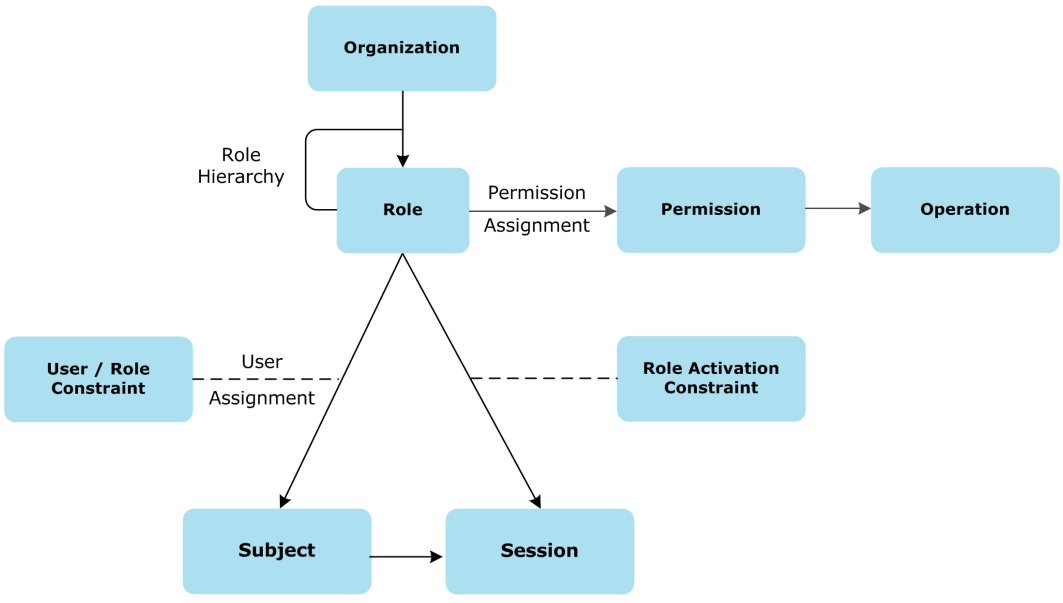
This topic describes what is available in Identity and Access Management and includes the following:

- *The RBAC model* on page 17 - Describes the RBAC model.
- *Available resources and actions* on page 18 - Lists the available resources and actions.
- *Predefined privileges* on page 19 - Lists the predefined privileges.
- *Predefined default roles* on page 20 - Lists the predefined default roles.

The RBAC model

This product implements an RBAC model to manage identity and access control. This model is based on the concept that there are actually few roles within an organization, and instead of assigning access to each individual resource, the permission can be assigned to roles, and then those roles assigned to users. This process makes it much easier to manage permissions. It is not necessary to review the complete list of users each time a new resource is added, but only to review the list of roles. In the same way it is not necessary to review the complete list of resources each time a new user is added, but only to review the list of roles.

The following diagram illustrates an RBAC model.



The following describes how the RBAC model works:

- A role is a list of permissions (or privileges).
- A permission is the right to execute one or multiple actions on one resource.
- When using a permission, it becomes an operation.
- Roles can be grouped to create hierarchical roles.
- Roles belong to an organization.
- When assigning a role to a subject (or user), it is possible to create a User/Role constraint to limit the scope of the role for this subject.
- To define these constraints, attributes can be associated with Resources.
- When the subject starts using a role, a session is created. When creating the session, it is possible to limit the scope of the role for this particular session through a role activation constraint.

For example:

- A role is delegated administrator
- Permissions are Manage Business Units
- Operations on resource are: Create, Read, Update, Delete
- A resource is a Business Unit
- The User/Role constraint is a concrete Delegated Administrator
- The constraint is added when assigning this role to a subject (User)

Available resources and actions

The following is a list of available resources in SecureTransport for administrator accounts. Included for each object are associated actions and a description.

Resource	Description	Resource actions
Accounts	Manage accounts and users	View, Modify
Application	Manage applications	View, Modify
Configuration	Manage configuration	View, Modify
Routes	Manage routes	View, Modify
Logging	Manage server logs	View

Predefined privileges

SecureTransport provides the following predefined privileges. For additional information on the predefined privileges, refer to the *Administrative roles* section in the *Advanced account administration* chapter of the *SecureTransport Administrator's Guide*.

Privilege	Description	Actions
account	Account Manager	View, Modify
admin	Master Administrator	Unlimited permissions
application	Application Manager	View, Modify
dbsetup	Database Administrator	View, Modify
setup	Setup Administrator	View, Modify
routes	Routes Manager	View, Modify

Account manager

This role enables the Account and Access menus. Users with this role can perform all tasks on the menus. This role groups the following privileges:

- Manage user accounts, service accounts, site and account templates, and business units
- Manage user classes and filesystem restrictions

Application manager

The role enables the Account and Application menus. Users with this role can perform all tasks on the Application menu and one task on the Account menu. This role groups the following privileges:

- Manage service accounts
- Manage applications

Database administrator

This role enables the Setup menu. Users with this role can manage database connection settings. This role groups the following privileges:

- Manage DB connection settings such as host, port, and password

Setup administrator

This role enables the Configuration menu. Users with this role can perform post-installation tasks. This role groups the following privileges:

- Install licenses
- Change default keystore password
- Regenerate CA and certificates
- Configure database settings

Master administrator

This role enables all the menus. Users with this role have unlimited authority to perform all tasks.

Delegated administrator

This role is customizable and enables different menus depending on its configuration. Users with this role can perform various tasks on specific user groups know as business units.

Predefined default roles

SecureTransport has two predefined roles:

Master administrator role - Has full permissions over SecureTransport and is represented by the following default administrator account:

- Master administrator (admin/admin)

Limited administrator role - The permissions of the limited administrators are represented by the following default administrator accounts:

- Account manager (account/account) - limited to account management
- Application manager (application/application) - limited to application management
- Database administrator (dbsetup/dbsetup) - limited to administering databases
- Setup administrator (setup/setup) - limited to performing the initial setup of SecureTransport

For additional information on the predefined default roles, refer to the *Administrative roles* section in the *Advanced account administration* chapter of the *SecureTransport Administrator's Guide*.

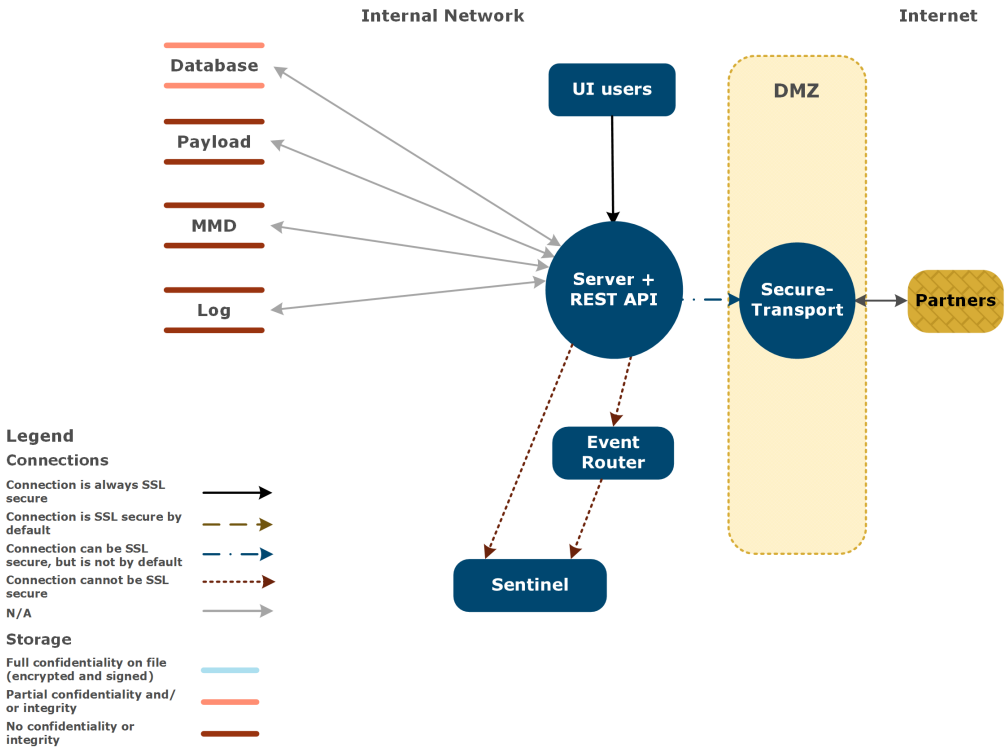
Configuration 6

The following topics contain configuration information:

- *Security architecture* on page 21 - Describes the SecureTransport security architecture.
- *Security configuration* on page 22 - Provides how-to instructions for configuring security.
- *Secure by default configuration* on page 25 - Describes the SecureTransport default security configuration.
- *Product certificates* on page 29 - Lists the product certificates.

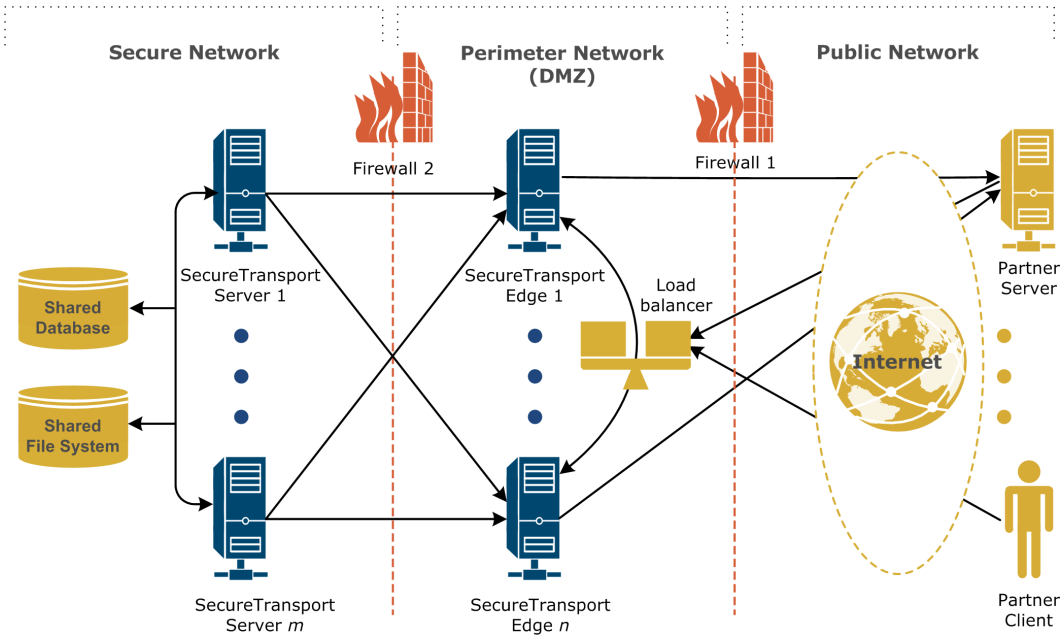
Security architecture

Global architecture of SecureTransport as identified in the Threat Modeling process.



For the database in the diagram, sensitive parameters, such as passwords and keys, are encrypted.

An Enterprise Cluster diagram.



Security configuration

For information on how to configure SecureTransport security, refer to the *Setup* chapter in the *SecureTransport Administrator's Guide*.

How to implement connection with Central Governance

There is secured communication between SecureTransport and Central Governance.

To establish the secured communication, follow these steps.

1. Ensure an administrator with master or limited role exists which can authenticate against the Administration Tool using a certificate.
    a. In the Administration Tool, navigate to **Setup > Admin Settings**.
    b. Under *Certificate Settings*, enable and configure administrator login using client certificates depending on the security level you want.
2. Configure SecureTransport integration with Central Governance:
    a. Navigate to **Setup > Central Governance** and configure the following in the *Central Governance Settings* pane:
        - **Host**: The fully qualified domain name (FQDN) or IP address of the computer where Central Governance is running.
        - **Port**: The port on which Central Governance is running.

- **Name**: Agent name set while configuring Central Governance.
- **Shared Secret**: Shared secret set while configuring Central Governance (it is stored encrypted in the SecureTransport database).

b. Navigate to **Setup > Central Governance** and configure the following in the *SecureTransport Settings* pane:

- **Product Identifier**: Unique and logical identifier 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 all XFB_Transfer Tracked Objects in Sentinel events.
- **Administrator Name**: The delegated or master administrator account. It will be used by Central Governance to log in to the Administration Tool.
- **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.)
- **Local Bind Port**: The local port through which the communication channel to Central Governance will be established. (For example, 5701.)

The following is a brief description of the authentication process after the initial configuration is complete and the agent is started:

1. The public part of the SecureTransport CA is exported and then imported in the CG/Passport trusted store.
2. The SecureTransport plug-in generates a client certificate.
3. The public part of the Central Governance CA is imported into SecureTransport.
4. The certificate DN is configured to the delegated or master administrator selected for the communication.

How to implement connection with Outlook Add-in

In order to connect Outlook Add-in to SecureTransport using HTTPS protocol, at least one of the cipher suites provided by Axway Outlook Add-in has to be enabled. For example: `TLS_RSA_WITH_AES_256_CBC_SHA`

Note Remember to keep all cipher suites separated by commas.

1. In the Administration Tool, navigate to **Operations > Server Configurations**.
2. Search for parameter: `Http.Ssl.EnabledCipherSuites`
3. Click the **Edit** () icon.
4. Add `TLS_RSA_WITH_AES_256_CBC_SHA` at the end of the cipher suite list.
5. Click the **Save** () icon.
6. Restart the HTTP service.

How to implement connection with Transfer CFT over PeSIT (SSL)

In order to configure PeSIT over SSL connection between Transfer CFT and SecureTransport, a cipher suite supported by Transfer CFT has to be enabled. For example: `TLS_RSA_WITH_AES_256_CBC_SHA`

Note Remember to keep all cipher suites separated by commas.

1. In the Administration Tool, navigate to **Operations > Server Configurations**.
2. Search for parameter: `Pesit.Listeners.Ssl.enabledCipherSuites`
3. Click the **Edit** () icon.
4. Add `TLS_RSA_WITH_AES_256_CBC_SHA` at the end of the cipher suite list.
5. Click the **Save** () icon.
6. Restart the PeSIT service.

For Server Initiated Transfers, the cipher also has to be added to the `Pesit.SIT.Ciphers` parameter.

How to implement connection with an older version of SecureTransport

In order to implement a connection with an older version of SecureTransport at least one cipher on SecureTransport 5.3.6 must match with the ciphers on the older version of SecureTransport.

For server-initiated transfers:

1. In the Administration Tool, navigate to **Operations > Server Configurations**.
2. Search for parameter based on the protocol used (FTP, HTTP, AS2, PeSIT): `<protocol>.SIT.Ciphers`
3. Click the **Edit** () icon.
4. Add a cipher in common with the older version of SecureTransport at the end of the cipher suite list.
5. Click the **Save** () icon.
6. Restart Transaction Manager.

Optionally, for SecureTransport servers using MD5 with RSA signature algorithm for local certificates, go to the `java.securty` file and enable the use of signature certificates.

For client-initiated transfers:

1. In the Administration Tool, navigate to **Operations > Server Configurations**.
2. Search for parameter based on the protocol used (FTP, HTTP, AS2, PeSIT): `<protocol>.Listeners.Ssl.enabledCipherSuites`
3. Click the **Edit** () icon.
4. Add a cipher in common with the older version of SecureTransport at the end of the cipher suite list.
5. Click the **Save** () icon.
6. Restart the protocol service.

Optionally, for SecureTransport servers using MD5 with RSA signature algorithm for local certificates, go to the `java.securty` file and enable the use of signature certificates.

Secure by default configuration

SecureTransport is secured by default after initial setup and configuration. You must explicitly assign a certificate alias for the protocol servers you need secured. The default configuration for TLS protocols and ciphers is secure and should not be changed unless specifically instructed. Currently, SecureTransport supports the TLSv1, TLSv1.1, and TLSv1.2 protocols. SSLv2 and SSLv3 protocols are deemed insecure and are not enabled by default. For a successful handshake between the server and the client, both must have a matching TLS/SSL protocol and at least one ciphersuite affiliated with that protocol. The `TLS_EMPTY_RENEGOTIATION_INFO_SCSV` pseudo ciphersuite must be present when performing negotiations via TLSv1 and TLSv1.1 to legacy partners.

SecureTransport has a variety of configuration options that you can use to set up HTTP security headers, redirect and referrer validation, and thus, protect against cross-site scripting (XSS), clickjacking and other code injection attacks. For more information, see *Security-related HTTP headers and policies on page 25*.

Security-related HTTP headers and policies

This topic presents a list of the most important security-related HTTP headers and their dedicated configuration options in SecureTransport. Setting up these headers in the SecureTransport server configuration protects you against many common attacks, including cross-site request forgery, cross-site scripting, clickjacking, etc. Some of these options are not enabled by default as they are not always appropriate and should be configured per business case.

Note Changing the value of a configuration option for the Administration Tool server requires Admin service restart to take effect; changing the value of a configuration option for an HTTP server requires HTTP server restart to take effect.

Referer header validation

Referer is an optional request header that contains the address of the source page from which a request is coming. To defend against CSRF attacks, you can configure SecureTransport to validate the Referer header in incoming HTTP requests against a whitelist of trusted domains. To enable the Referer validation, specify the acceptable header values in the following configuration options:

- `WebServices.Admin.Referer.Whitelist` - whitelist for Admin API web services
- `WebServices.Public.Referer.Whitelist` - whitelist for Public API web services

Both configuration options accept regular expressions. The default value for both is **""** (empty), meaning any referrer is allowed.

Also, you can use the `Http.Security.ReferrerPolicy` configuration option to specify the value of the Referrer-Policy header for the HTTP daemon. This header determines what information is sent in the Referer header in an outgoing request. The 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. When no value is set, the browser's default is used.

For more information on each directive and its meaning, see MDN Web Docs and Google Developers.

Redirect validation

For additional protection against Open Redirect vulnerabilities, you can configure SecureTransport to allow redirection only to a specified list of domains. To enable this feature, specify the domains that you consider trusted in the `Http.RedirectWhiteList` option. You can either list them explicitly or use a regular expression. Adding a domain to the whitelist results in redirects to this domain and its sub-domains being allowed. The default value of the option is `(^/)`, meaning all domains starting with / are allowed. Redirects to domains that are not whitelisted will be rejected with a 403 error message.

CSRF token protection

Using a CSRF token (also known as synchronizer token) is one of the most popular and recommended methods to prevent Cross-site Request Forgery. SecureTransport has built-in protection: it generates a CSRF token for each active user session and verifies that the token in the received request matches the token stored in the session. By default, the CSRF token protection is disabled. To enable it, set the following options to `true`:

- `Webservices.Admin.CsrfToken.enabled` for the Administration Tool server
- `Webservices.Http.CsrfToken.enabled` for the HTTP server

When CSRF token protection is enabled, in order to use the REST API while reusing the same session, you need to make an authentication request to the `/myself` resource to obtain the CSRF token from the csrfToken response header. The token must be passed with every subsequent request for the current session using the `csrfToken` header.

X-XSS-Protection

According to how this header is set, if a cross-site scripting attack is detected, the browser will either sanitize the page (remove the unsafe parts) or prevent rendering of the page. To specify the X-XSS-Protection header in server responses, edit the following configuration options to specify an appropriate value:

- `Admin.Security.XSSProtection` for the Administration Tool server
- `Http.Security.XSSProtection` for the HTTP server

Possible values:

- `0` – Disables the XSS filtering.
- `1` – Enables the XSS filtering. If a cross-site scripting attack is detected, the browser will sanitize the page (remove the unsafe parts).
- `1; mode=block` – Enables XSS filtering. Instead of sanitizing, the browser will prevent rendering of the page if an attack is detected.
- `1; report=<report-uri>` – Enables XSS filtering. If a cross-site scripting attack is detected, the browser will sanitize the page and report the violation using the CSP report-uri directive.

Cache-Control

This header lets you control the caching of specific web pages. In SecureTransport, you can define the caching policy for the Administration Tool pages via the `Admin.ControlCaching` server configuration option. It accepts the following values:

- `true`– Default; The request cashing is enabled.
- `false`– The Cache-Control directive is set to `no-cache, no-store` on all static and non-static requests.

Note When requests are not being cached, performance degradation may occur.

Server

The Server header may expose information like your server platform and software. You can remove or limit the content of the header by editing the following server configuration options:

- `Admin.ServerHeaderTokens`configures the Admin server response header. The possible values are `Full`, `Prod`, `OS`, `None`. The default value is `Full`.
- `Http.ServerHeaderTokens` configures the HTTP server response header. The possible values are `Full`, `Prod`, `OS`, `None`. The default value is `Full`.
- `As2.ServerHeaderTokens` configures the AS2 server response header. The possible values are `Full`, `None`. The default value is `Full`.

where

- `Full`– The header field shows the product name, build number, and the operating system (with the result being, for example, `Server: SecureTransport 5.5 (build: 1111) - Linux)`.
- `Prod`– The header field shows the product name, *SecureTransport*.
- `OS`– The header field shows the operating system on which SecureTransport is running (with the result being, for example, `Server: Linux`)
- `None`– Depending on the Jetty version, the Server header is not displayed or its field is empty.

Content-Security-Policy

This header defines content sources that are approved, permitting the browser to load them. To configure your server to return the Content-Security-Policy HTTP header, use the following server configuration options:

- `Admin.Security.ContentSecurityPolicy` for the Administration Tool server
- `Http.Security.ContentSecurityPolicy` for the HTTP server

Possible values for both configuration options are:

- `default-src 'self'`
- `style-src 'self' 'unsafe-inline'`
- `script-src 'self' 'unsafe-eval' 'unsafe-inline'`

For more information on each directive, see the CSP Quick Reference Guide.

Note Content Security Policy is not supported in Internet Explorer 11.

Strict-Transport-Security (HSTS)

This header forces the browser to use only secure (HTTPS) connections. To set the HSTS on SecureTransport, use the following server configuration options:

- `Admin.Security.Hsts.enabled` – Enables/disables HSTS for the Administration Tool server. Boolean, the default is `true`.
- `Admin.Security.Hsts.max-age` –The max-age directive in the HSTS header for the Administration Tool server, in seconds. The default is `15768000` (6 months).
- `Http.Security.Hsts.enabled` – Shows whether HSTS is enabled for the HTTP Server or not. The value of this configuration option depends on the selection of the **Enable HSTS** checkbox in **Operations->Server Control**. Boolean, the default is `true` which means that HSTS is enabled and an HSTS response will always be sent, redirecting the plain HTTP connection to HTTPS.
- `Http.Security.Hsts.max-age` – The max-age directive in the HSTS header for the HTTP server, in seconds. The default is `15768000` (6 months).

X-Frame-Options

This header provides clickjacking protection by not allowing the loading of a page within a frame or iframe. To configure SecureTransport to send the X-Frame-Options header, set the `Admin.Security.FrameOptions` configuration option to one of the following values:

- `deny`– The browser will block the resource from loading in a frame.
- `sameorigin`– The browser will only load the resource in a frame if the request originated from the same site

X-Content-Type-Options

Configuring your server to return the X-Content-Type-Options response header set to `nosniff` will instruct browsers that support MIME sniffing to use the server-provided Content-Type and not interpret the content as a different content type. Use the following configuration options:

- `Admin.Security.ContentTypeOptions` for the Administration Tool server
- `Http.Security.ContentTypeOptions` for the HTTP server

Expect-CT

The Expect-CT header identifies the usage of wrongly issued certificates for a site and allows sites to decide on reporting and/or enforcement of Certificate Transparency requirements. The header has effect on HTTPS connections only.

To configure the ST Web Client to respond with Expect-CT header, use the `Http.Security.ExpectCT` server configuration option. It accepts a semicolon- (;) or comma-separated list of the Expect-CT header directives: `max-age=<age>; enforce; report-uri=<uri>`. The `report-uri=<uri>` and `enforce` directives are optional. Depending on their presence, Expect-CT will only report violations, enforce compliance to the Certificate Transparency policy, or both report and enforce.

Examples:

- To enforce Certificate Transparency for an hour, set the server configuration value to `max-age=3600; enforce`.
- To enforce Certificate Transparency for 12 hours and report violations to www.st-report.com, set the server configuration value to:
- `max-age=43200; enforce; report-uri="https://www.st-report.com/"`

Product certificates

The Java applet, including the signed jar, has been removed from the current version of SecureTransport (5.3.6) and Web Access Plus has been replaced by ST Web Client.

Security best practices 7

When using this product, follow these security best practices:

- Always use TLS secured connections; see *Secure connections* on page 30.
- Don't use the sample certificates provided with the installation of the product; see *Sample certificates* on page 31.
- Don't use self-signed certificates; see *Self-signed certificates* on page 31.
- Maintain a list of users with privileged access; see *Privileged access user list* on page 31.
- Limit as much as possible number of Internet access points; see *Internet access limitation* on page 31.
- Have the correct procedure to upgrade the product; see *Correct upgrade procedure* on page 32.
- Don't define generic or anonymous users; see *Generic or anonymous users* on page 32.
- Be sure to enforce a reasonably strong password policy; see *Password policy* on page 32.
- Make sure default authentication accounts are disabled or deleted; see *Default authentication account* on page 32.
- Always change default passwords after installation; see *Default passwords* on page 33.
- Limit your remote connections; see *Remote connections* on page 33.
- SecureTransport supports configurations for logging, audit, and alerting; see *Logging, audit, and alerts rules* on page 33.
- Protect your sensitive files and databases; see *Sensitive files and databases* on page 34.
- Use cryptographically strong protocols and ciphers; see *Use cryptographically strong protocols and ciphers* on page 34.
- Use basic authorization and Base64 encoding of username and password; see *Password encoding and BASIC authentication* on page 34.
- If you are deploying plug-ins, keep in mind that they may have their security settings.
- Use External Script routing step with caution; see *External Script execution* on page 35.

Secure connections

Axway deems it mandatory that all connections with external networks be secure and secure connections are recommended for internal connections. For example, connections between an SSO proxy and an application must always be SSL/TLS-secured with mutual authentication to avoid anyone connecting with the proxy header without any credentials.

Sample certificates

Axway provides sample certificates with the product. These certificates should be used for test purposes only. As soon as the product goes live, or as soon as real data is managed by the product, you must use your own certificates. Using sample certificates is a security risk as all Axway customers have the same certificates with the same private keys.

The following sample certificates are delivered with the product. These certificates should be used only for test purposes and must be replaced with your own certificates as soon as possible. These certificates are self-signed. They expire within a month after installation.

- Internal CA (alias – ca)
- Administrator UI (alias – admind)

Self-signed certificates

Using self-signed certificates may also be a security risk for many reasons, including:

- Anyone can generate his own certificate and you need a very secure process to receive/send these certificates to make sure they are coming from the right partner. When using CA-signed certificates, you can rely on the CA.
- If self-signed certificates are not securely stored, anyone can change them. CA-signed certificates also must be securely stored, but no one can change them.
- There is no way to revoke self-signed certificates.

Privileged access user list

To be customized for every product depending on predefined privileges.

Maintain a list of users with privileged access. At a minimum, maintain a list of administrators and a list of users with access to multiple functions.

Internet access limitation

As much as possible, limit the number of internet access points. Do not open useless Internet connections and limit interconnections with external networks as much as possible. This reduces the risk of external attacks and makes it easier to audit the product.

Correct upgrade procedure

In the event of a possible vulnerability discovered in the product, you must be able to apply the patch or service pack as soon as possible. Make sure you have the correct procedure to complete the upgrade. Always use the latest version of the product, if possible, as it contains fixes to known vulnerabilities.

Generic or anonymous users

The term "generic users" means that the password is shared among multiple specific users. This makes it easier for an attacker to retrieve this password. In addition, the procedure to change shared passwords can be complicated and risky. In case of an incident, these generic or anonymous users make it impossible to determine who completed the erroneous action.

Password policy

Password policy refers to size and complexity of the password, as well as to all the rules to manage this password. The size and complexity is important. The policy should define that the length be a minimum of 8 characters, contain a mix of alphabetic characters with numbers and special characters, and be case-sensitive.

Your password policy:

- Must force passwords to be changed periodically.
- Should prohibit reuse of a password before n number of different passwords and within a certain period of time.
- Must define how the password is created differently from the old one (such as: at least a certain number of different characters).
- Must limit the number of failed attempts.

Default authentication account

The product is delivered with the following default administrators:

- Master administrator (admin/admin)
- Account manager (account/account)
- Application manager (application/application)
- Database administrator (dbsetup/dbsetup)
- Setup administrator (setup/setup)

Your first task after login with this user must be to create your own administrator account and to delete the default one, or at least change the default administrator password.

Default passwords

The product is delivered with the following default passwords:

- Keystore password (tumbleweed)
- Database password (tumbleweed)

Remote connections

You should limit your remote connections in the following ways:

- If no one needs to access the product remotely, make sure that the UI ports are closed in your firewall.
- If someone needs to connect remotely only occasionally, set a procedure to open the port only on demand.
- If there are regular remote users, make sure that the connections are as secure as possible, such as using HSTS or VPN.

Logging, audit, and alerts rules

SecureTransport supports configurations for logging, audit, and alerting.

1. SecureTransport has its own mechanisms for logging, auditing, and alerting. They are represented by the following features:
    - Audit Log (**Operations > Audit Log**) - Provides the administrator with information about the configuration changes in SecureTransport. The administrator is able to get information about the entities that changed the database, as well as information about the exact time the changes happened.
    - Server Log (**Operations > Server Log**) - Provides log messages from the following SecureTransport components: the Transaction Manager (TM) and the processes that implement the FTP, HTTP, SSH (SCP and SFTP), AS2 , PeSIT, and SOCKS5 protocols, the Administration Tool interface (ADMIN), and auditing.
    - File Tracking (**Operations > File Tracking**) - Provides log of the statuses and attributes for each transfer.
    - Email notifications (Refer to *SecureTransport Administrator's Guide* for additional information.)
2. SecureTransport integrated with Axway Sentinel - Once SecureTransport is configured to send file transfer and processing events to Sentinel, data is collected and displayed on a dashboard.

3. SecureTransport integrated with Central Governance - Sentinel is part of the Central Governance product. Once SecureTransport is integrated with Central Governance, the Sentinel configuration is applied in SecureTransport.

Sensitive files and databases

You must protect your sensitive files and databases. The configuration file contains information that can be useful to a hacker. Even if part of this information is encrypted, access to this file must be restricted by your local access management. Only the product and one or two administrators should have access to this file in any mode (read, update, and delete).

The file containing the password used to generate encryption keys must be protected as well. This file is encrypted, but access to this file should only be granted to the product.

The product database also contains sensitive data; you should also prohibit access to this database from any other tools or applications using the API, with the exception of one or two administrators.

Use cryptographically strong protocols and ciphers

Refrain from using protocols and ciphers that are deemed insecure by today's industry standards. At the time of this writing SSLv3 does not provide enough security and should not be used. Instead TLSv1.2 (preferred), TLSv1.1, or TLSv1 should only be used. Stream ciphers such as RC4 should also be avoided. For example, RC4 is known to be susceptible to cryptographic attacks.

Password encoding and BASIC authentication

Basic authentication and Base64 encoding of username and password are required but can be exploited if not properly configured. Use of BASIC authentication by itself, is not a vulnerability; however, when combined with other factors such as not using TLS and improper no-cache response headers, it can be exploited.

If the server is configured to use TLS, the HTTP header containing the BASIC authentication header will be encrypted. If TLS is not enabled, then Base64 will provide absolutely no protection, nor was it designed to do so. It is essential however, that when BASIC authentication is used, that self-signed certificates are not. A certificate from a trusted CA is the only adequate protection of BASIC authentication credentials. Also, login attempts should be limited when using BASIC authentication.

BASIC authentication should not be enabled by default for API authentication; but should be an option, in order to integrate the API with existing systems.

External Script execution

Advanced Routing External Script step provides the functionality to run a script from the underlying file system. Since version 5.4, the External Script routing step exposes a property in the form of a checkbox which adds extra functionality in the external script execution.

By default, when running SecureTransport as an operating system superuser ("root"), external scripts are executed with impersonating the user account which has triggered the routing step, thus limiting the set of commands and scripts which can be run due to the lack of permissions.

When enabling the "Execute script as root administrator" checkbox, SecureTransport will use the system superuser to run the specified script and will not impersonate the user account.

Note SecureTransport administrators must be fully aware that running external scripts with operating system superuser permissions grants privileges to execute a full scope of commands which might harm the server irrevocably.

Axway recommends running external scripts without root permissions.

SecureTransport cipher suites 8

The following topics provide the SecureTransport cipher suites:

AS2 daemon

The following are the AS2 daemon (`As2.Listeners.Ssl.enabledCipherSuites`):

- 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

AS2 server initiated transfer

The following are the AS2 SIT (`As2.SIT.Ciphers`):

- 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

FTP daemon

The following are the FTP daemon (`Ftp.Listeners.Ssl.enabledCipherSuites`):

- 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

FTP server initiated transfer

The following are the FTP SIT (`Ftps.SIT.Ciphers`):

- 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

HTTP daemon

The following are the HTTP daemon (`Http.Ssl.EnabledCipherSuites`):

- 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

HTTP server initiated transfer

The following are the HTTP SIT (`Https.SIT.Ciphers`):

- 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

PeSIT daemon

The following are the PeSIT daemon (`Pesit.Listeners.Ssl.enabledCipherSuites`):

- 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

SSH daemon and server initiated transfer

The following are the ciphers and algorithms for both SSH daemon and SSH SITs:

SSH2 (default) ciphers

- aes128-ctr
- aes192-ctr
- aes256-ctr
- 3des-cbc
- blowfish-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- arcfour
- arcfour128
- arcfour256
- 3des-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com

SSH1 ciphers

- ssh1-des
- ssh1-3des

MACs

- hmac-sha1
- hmac-md5

- hmac-sha1-96
- hmac-md5-96
- hmac-sha256
- hmac-sha256@ssh.com
- hmac-sha512
- hmac-sha512@ssh.com
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha2-512-etm@openssh.com
- hmac-ripemd160-etm@openssh.com
- hmac-md5-etm@openssh.com
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-256-96
- hmac-sha1-etm@openssh.com
- hmac-ripemd160
- hmac-ripemd160@openssh.com
- hmac-sha2-512-96

Public keys

- ssh-dss
- ssh-rsa
- x509v3-sign-rsa
- x509v3-sign-dss
- x509v3-sign-rsa-sha1
- x509v3-ssh-rsa
- x509v3-ssh-dss
- x509v3-ecdsa-sha2-nistp256
- x509v3-ecdsa-sha2-nistp384
- x509v3-ecdsa-sha2-nistp521
- x509v3-rsa2048-sha256
- ssh-rsa-cert-v01@openssh.com
- ssh-dss-cert-v01@openssh.com
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- rsa-sha2-256
- rsa-sha2-512

KEXs

- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp512
- diffie-hellman-group14-sha256
- diffie-hellman-group15-sha512
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group18-sha512
- diffie-hellman-group14-sha1
- diffie-hellman-group17-sha512
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group1-sha1
- curve25519-sha256@libssh.org
- rsa1024-sha1
- rsa2048-sha256

Admin

The following are the Admin (`Admin.EnabledCipherSuites`):

- 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

Sentinel

The following are the Sentinel (`AxwaySentinel.SecureConnection.EnabledCipherSuites`):

- 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_RSA_WITH_AES_256_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

Streaming

The following are the Streaming (`Streaming.EnabledCipherSuites`):

- TLS_RSA_WITH_AES_256_CBC_SHA256

Transaction Manager

The following is the TM (Tm.CipherSuites):

- TLS_RSA_WITH_AES_256_CBC_SHA256