axway

SecureTransport

Version 5.4

2 April 2024

Installation Guide

This documentation describes the following Axway software:

Axway SecureTransport 5.4

Revision history

The following changes are added to the SecureTransport 5.4 Installation guide:

SecureTransport version	Document revision number	Topics updated
5.4	5.4.01 – initial version	
5.4	5.4.02	Microsoft Windows Server 2016 and Microsoft Windows Server 2019 support added to the following topics: • *Install SecureTransport Server on Windows with the embedded database* on page 42 • *Install SecureTransport Server on Windows with an external database* on page 44 • *Supported operating systems* on page 26 • *Virtualization support* on page 13
5.4	5.4.03	• Oracle 18c support added to *Requirements for Oracle databases* on page 15 • Redundant items removed from *General prerequisites* on page 21
5.4	5.4.04	• *Silent installation of SecureTransport* on page 48 topic updated
5.4	5.4.05	The following topics have been edited for clarity: • *Install SecureTransport Server on Windows with an external database* on page 44 • *Install SecureTransport Server on Windows with the embedded database* on page 42
5.4	5.4.06	*General prerequisites* on page 21 updated
5.4	5.4.07 – current version	*General prerequisites* on page 21 updated with requirements for the `/tmp` directory

Contents

Preface **6**

Who should read this guide 6

Related documentation 7

Get more help 8

Training 8

1 Introduction **9**

About SecureTransport 9

Installation outline 9

2 Prerequisites **11**

Installation directory 11

Services 11

Server certificates 11

Administration accounts 11

Port numbers 12

Service packs and patches 13

System requirements 13

Virtualization support 13

Secret file 14

Database requirements 14

Requirements for Oracle databases 15

Data pump database management system 16

Requirements for Microsoft SQL Server databases 17

Database size in production 18

UNIX-based platforms 18

Supported operating systems 19

Minimum UNIX hardware requirements 19

Host name resolution 21

General prerequisites 21

Requirements for specific operating systems 21

Prerequisites for non-root installations 25

Windows platforms 25

Supported operating systems 26

Minimum Windows hardware requirements 26

3 Install **27**

UNIX-based platforms 27

Install SecureTransport to use the embedded database 28

Install SecureTransport Server in an Enterprise Cluster or to use an external database 33
Run SecureTransport as a service on UNIX-based platforms after non-root installation 40
Windows platforms 42
Install SecureTransport Server on Windows with the embedded database 42
Install SecureTransport Server on Windows with an external database 44
Cancel the Windows installation 48
Silent installation of SecureTransport 48
Configurable properties for silent installation 49
Recommendations for Clustered SecureTransport deployments 54
Silent file editor 55
Silent installation example file 56

4 Uninstall 59
Uninstall SecureTransport on UNIX-based systems 59
Uninstall SecureTransport on Windows 61

Preface

This guide provides instructions for installing the SecureTransport software and provides information on the following topics:

- Preinstallation tasks and installation prerequisites
- Installing SecureTransport or upgrading from previous versions of SecureTransport
- Performing post-installation tasks
- Uninstalling SecureTransport

These tasks are covered for all supported platforms: Axway Appliances, IBM AIX, Microsoft Windows, Oracle Linux, Oracle Solaris (previously Sun Solaris), Red Hat Enterprise Linux (RHEL), and SUSE Linux Enterprise Server (SLES).

This chapter provides general information about SecureTransport, a description of the documentation set, and contact information for obtaining technical support for SecureTransport.

This guide describes how to install SecureTransport and how to upgrade SecureTransport to the latest version. It also covers:

Installing – Describes how to perform a complete install as well as apply a service pack. See *Install* on page 27.

Uninstallation – Describes how you can uninstall SecureTransport using the Axway Installer. See *Uninstall* on page 59.

Who should read this guide

This guide is intended for system administrators who install SecureTransport on Axway appliance, Windows and UNIX-based platforms and perform its initial configuration. As the SecureTransport installer, you must have a working knowledge of system platforms and networks used by your SecureTransport instances. You must have administrative privileges on the computers where you will install SecureTransport and appropriate access to systems that SecureTransport depends on, such as an external database and file system. This guide is also intended for enterprise personnel involved in installing software and Axway Professional Services personnel. Familiarity with Axway products is recommended.

This guide presumes you have knowledge of:

- Your company's business processes and practices
- Your company's hardware, software, and IT policies
- The Internet, including use of a browser
- Azure Portal user interface and flows

Others who may find parts of this guide useful include network or systems administrators and other technical or business users.

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 pluggable 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

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

Introduction 1

This guide explains how to perform a full installation of SecureTransport and how to upgrade it to the latest version. It also describes how to uninstall SecureTransport.

The following topics provide a SecureTransport overview and outline the installation of SecureTransport:

- *About SecureTransport* on page 9 - Provides an overview of SecureTransport.
- *Installation outline* on page 9 - Provides an outline of instructions for installing SecureTransport.

About SecureTransport

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, 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.

For a complete description of SecureTransport features and components, refer to the *SecureTransport Administrator's Guide*.

Installation outline

The following is a brief outline of the Windows SecureTransport installation steps. For complete installation details and for appliance and UNIX installation steps, refer to *Install* on page 27

1. Download the SecureTransport software package file from support.axway.com.
2. Copy the software package file into a temporary folder.
3. Open the software package file.
4. Copy all files and folders in the software package file to a temporary location to extract the installation files.
5. In the temporary installer folder, run `setup64.exe`.
6. Click **Next** to proceed.
7. **Accept** the terms of the license agreement and click **Next** to proceed.

Note The installer should review all pages of the license agreement before clicking **Next**.

8. Enter the **Installation Directory** and click **Next**.
9. Select the module to install, **Server** or **Edge** and click **Next**.
10. Accept the default or enter the **Installation Directory** of SecureTransport and click **Next**.
11. Select the database to use.
12. Enter the settings according to the selected database and click **Next**.
13. Accept or modify the configuration settings and click **Next**.
14. Click **Install** to start the installation.
15. When the installation is complete, click **Next**.
16. Click **Finish** to exit the installer.

Prerequisites 2

Before you proceed, review the *SecureTransport Release Notes* for any updates to this preinstallation information or the installation and setup procedures.

Review the following information before starting the installer.

Installation directory

You must install SecureTransport on local disk storage. Installation on shared storage is not supported. (For more information, see the discussion in the *SecureTransport Administrator's Guide* of troubleshooting performance issues due to installation on a network drive.) All nodes in an Enterprise Cluster and a Standard Cluster must use the same local installation directory path name. The name of the SecureTransport installation directory cannot include the ~ character. For example, `/root/Axway/STServer` is valid, but `/root/Axway/ST~Server` is not valid.

Note Axway recommends installing SecureTransport in a directory path without spaces in the folder names. Other special characters in the folder names must also be avoided and the tilde (~) character cannot be used.

Note Since SecureTransport 5.2.1, SecureTransport server installation on a private SAN logical unit LUN is a supported configuration.

Services

After all components have been installed, the Admin service is started and, for installations that use the embedded database, the Database service is started. These services are configured according to your responses to the questions the installer asks during the installation procedure. These services are started so an administrator can configure SecureTransport before starting any additional services.

Server certificates

During installation, a temporary self-issued CA is generated, and then a temporary *admin* certificate, signed by this CA, is generated.

Administration accounts

The installer creates the following default accounts with a default user name and password:

- Master Administrator account "`admin/admin`".
- Setup Administrator "`setup/setup`" for the initial, one-time configuration of the system.
- Database Setup Administrator "`dbsetup/dbsetup`" for access to the *Database Setting* page when the database is not running.
- Account Manager "`account/account`" who can create and manage user access and export and import accounts.
- Application Manager "`application/application`" who can create service accounts and create and configure applications.

Note For better security, change the default passwords or disable the accounts that are not used.

Port numbers

The installer suggests the port numbers listed below for the SecureTransport server ports:

- MySQL database port number – `33060`

  This port is used for SecureTransport Edge, for SecureTransport Server Standard Clustering installations, and for SecureTransport Server stand-alone installations that use the embedded database. You can change this port after installation using the Administration Tool.

- Oracle database listener port number –`1521`

  This port is used for SecureTransport Server Enterprise Cluster installations that use an external Oracle database. You can change this port after installation using the Administration Tool.

- Microsoft SQL Server port number – `1433`

  This port is used for SecureTransport Server Enterprise Cluster installations that use an external Microsoft SQL Server database. You can change this port after installation using the Administration Tool.

- Admin port number – `444`

  This is the port that the web server for the Administration Tool listens to. You must specify the Admin port number in the URL when accessing the Administration Tool, using the form, `https://<hostname>:<Admin port>/`. If you are installing SecureTransport on a UNIX-based server to run as a non-root user, 8000 is added to port numbers that are below 1024, so the default Admin port number is 8444.

- Tomcat JK port number – `8009`

  This is the port that the Coyote JK Connector, the internal module of the admin server that handles the execution of servlets and JSP pages, listens to. It must be greater than 1024.

- Tomcat shutdown port number – `8005`

  This is the port on which the admin server waits for a shutdown command.

Note After installation, the SecureTransport admin server also uses port `8004` to communicate with the Tomcat application server. If port `8004` is in use by another process, change the `Admin.Http.Port` system configuration parameter on the *Server Configuration* page and stop and restart the admin server.

Service packs and patches

Check Axway Support at https://support.axway.com to determine if you need to apply any service packs or patch after you install SecureTransport and before you configure it. You can download the service pack and patch files to the system where you will install SecureTransport before you start the installation and apply them at the end of the installation without leaving the installer.

System requirements

The following are the system requirements for SecureTransport.

- Supported operating systems and versions. This also can include virtualization platforms.
- Supported databases types and versions.
- Hardware requirements, including RAM and disk space.
- Supported network storage (for example, network-attached storage (NAS) or storage area network (SAN) and supported file systems.
- Reference that describes the license keys required to perform the product installation.
- Supported browsers for the product.

Related topics

The following topics provide the SecureTransport installation prerequisites:

- *Virtualization support* on page 13 - Lists the virtualization support prerequisites.
- *Secret file* on page 14 - Describes the secret file prerequisites for SecureTransport Servers and SecureTransport Edges.
- *Database requirements* on page 14 - Lists the database requirements prerequisites.
- *UNIX-based platforms* on page 18 - Lists the UNIX-based platform prerequisites.
- *Windows platforms* on page 25 - Lists the Window platform prerequisites.

Virtualization support

SecureTransport 5.4 is supported in the following virtual environments:

- An IBM AIX 7.1, or 7.2 LPAR or WPAR
- An Oracle Solaris Zone in Oracle Solaris 10 or 11
- A virtual appliance running under VMware ESX(i) 5.0 or higher

- An Amazon Elastic Compute Cloud (EC2) virtual instance – an AMI, based on product appliance images, can be deployed on Amazon EC2 and Amazon VPC.
- A supported version of RHEL or SLES in any x86 virtual environment (see *Supported operating systems* on page 19)
- Microsoft Windows Server 2012 R2 (Standard/Datacenter) in any x86 virtual environment
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

A virtual environment must provide the minimum required virtual hardware. For details, see *Minimum UNIX hardware requirements* on page 19 and *Minimum Windows hardware requirements* on page 26.

Axway provides support for Axway SecureTransport running in a virtual environment in an identical manner as with Axway SecureTransport running on any other supported x86-based systems without initially requiring the reproduction of issues on native hardware. If Axway suspects that the virtualization layer is the root cause of an incident, then the customer is required to contact the appropriate virtualization support provider to resolve the virtualization issue.

While Axway SecureTransport is expected to function properly in a virtual environment, there may be performance implications which can invalidate typical sizing and recommendations for Axway SecureTransport.

Secret file

The secret file (also called `taeh` file) contains randomly-generated data used by the SecureTransport system for encryption. It must be the same for all SecureTransport Servers or SecureTransport Edges in a cluster.

The installer creates the secret file (named `taeh`) when you install a stand-alone server or the first SecureTransport Server in a cluster. It is stored in the `<FILEDRIVEHOME>/bin/taeh` directory, where `<FILEDRIVEHOME>` is the directory where SecureTransport is installed.

For the second and subsequent servers of the cluster, you must copy the `taeh` file from the first cluster node before you install SecureTransport. Then you import the `taeh` file during server installation. After you configure the server, you cannot change the `taeh` file. Changing the secret file after the server is configured may corrupt certain encrypted configuration elements (local certificates, passwords, and so forth).

When you install SecureTransport on a second node in a cluster using an appliance, you are prompted for the remote server credentials and location of the secret file. The other server must be an appliance with SecureTransport installed and an OS-level SSH daemon running.

For details, see *General prerequisites* on page 21.

Database requirements

The following topics list the database requirements:

- *Requirements for Oracle databases* on page 15 - Lists the requirements for Oracle databases.
- *Data pump database management system* on page 16 - Provides configuration information for data pump database management.
- *Requirements for Microsoft SQL Server databases* on page 17 - Lists the requirements for Microsoft SQL Server databases.
- *Database size in production* on page 18 - Lists the database size in production.

Requirements for Oracle databases

- To support unicode characters in filenames and directories, the database should use AL32UTF8 encoding.
- SecureTransport can connect to external Oracle database over plain or secure connection.
- The Oracle database can use, but does not require, the Real Application Clusters (RAC) option.
- SecureTransport can use, but does not require, more than one Oracle database to store its data.
- Settings and parameters as follows:
    - Redo log groups: 3
    - Redo log file size: 500 MB (For more about redo log file use, see *Database size in production* on page 18.)
    - Gather optimizer statistics: Weekly or with any 10 percent change in the record count.
    - `DB_CACHE_SIZE`: 1 GB or larger. You should set this as high as possible to improve performance.
    - `OPEN_CURSORS`: at least 1000
    - `SHARED_POOL_SIZE`: 150 MB per node in the cluster
    - `PROCESSES`: 1000 or more

      For the external Oracle database, `hibernate.c3p0.max_size` and `hibernate.c3p0.min_size` is specified in `<FILEDRIVEHOME>/conf/configuration.xml`. The default value for `hibernate.c3p0.max_size` is 8 for each component, while the default value for `hibernate.c3p0.min_size` varies depending on the component. These two configuration items specify the connection pool size per component.
- The database must have the following tablespaces defined:
    - `ST_DATA` – configuration, such as account, sites, and certificates
    - `ST_FILETRACKING` – file tracking tables
    - `ST_SERVERLOG` – server log tables

      Note When you direct log data to separate databases, you must define the `ST_FILETRACKING` tablespace in the database for the transfer log and the `ST_SERVERLOG` tablespace in the database for the server log.

  Set `AUTOEXTEND ON` for all tablespaces and datafiles.

See *Database size in production* on page 18 for information you can use to set initial sizes for the tablespaces. Give the user unlimited quota on all tablespaces.

- The database must have a user defined who has been granted the following system privileges (*directly* and not through a role):
  - `CREATE OPERATOR`
  - `CREATE PROCEDURE`
  - `CREATE SEQUENCE`
  - `CREATE SESSION`
  - `CREATE TABLE`
- The default tablespace for the database user must be `ST_DATA`.

During the installation, you need the following information:

- Host name, IP address, or SCAN name of the database server in case Oracle RAC is utilized
- Listener port number
- Database user name and password
- Service name
- Axway Installer supports encryption up to TLS 1.1 and does not support TLS 1.2. If you want to configure your SecureTransport installation to connect to your Oracle database using TLS 1.2, you can configure the database to accept connections using either no encryption or TLS 1.1 (and earlier) during the installation process. After a successful installation, you can secure the connection to your Oracle database using TLS 1.2.
  To accomplish that, stop all SecureTransport services, reconfigure the Oracle database to accept connection over TLS 1.2 only and start SecureTransport again. Make sure that you have listed TLSv1.2 under *Enabled Protocols* in the **Setup > Database Settings** configuration page.
- If the database is used over secure connection, you will also need the database server certificate signer or JKS keystore which contains it in order to trust the connection. In addition, the optional parameter **Distinguished Name (DN)** can be provided and installer will verify the provided information against the database certificate's DN. If it is not provided, the installer will not check the certificate DN and will trust any.

Data pump database management system

Before installation, you can set the `DATA_PUMP` system environment variable to either **false** or **true** depending upon if you want to *disable* or *enable* the data pump. By default, if data pump system environment variable is not set, the data pump will be enabled and export database functionality procedures will be deployed.

Execute the following command to set the `DATA_PUMP` system environment variable to false:

```
export DATA_PUMP=false
```

When the DATA_PUMP system environment variable is set to **false**, the installer will detect that the data pump is disabled and a warning message will be displayed in the install.log file with the following content:

```
DEBUG [external_db_configuration] 2016-07-05 15:47:25,761 EEST WARN [main]
com.tumbleweed.st.server.appframework.util.OracleDatabaseConfigurator -
DataPump capabilities are disabled. The configuration will proceed without
deploying the data pump procedures.
```

When the data pump disabled, the installer will not deploy the database procedures to export partitions. Microsoft SQL Server to Oracle database migrations will assume that the target database and user have data pump available. When deploying on multiple databases, all databases inherit the same data pump behavior as the first one. On upgrade, also valid for all patches and service packs, data pump will be enabled by default and you cannot change it.

Requirements for Microsoft SQL Server databases

- The database must have the READ_COMMITED_SNAPSHOT option set to ON

  To check if option is enabled, execute the following query:

  SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = *yourdatabase*

  If it is not set, you can set it by executing the following:

  ALTER DATABASE *yourdatabase* SET READ_COMMITTED_SNAPSHOT ON

- The database must have the following filegroups defined with at least one file in each filegroup:
  - ST_DATA – configuration, account, sites, and certificates (the default filegroup)
  - ST_FILETRACKING – file tracking tables
  - ST_SERVERLOG – server log tables

    Note You cannot direct log data to separate Microsoft SQL Server databases.

- Two new filegroups needs to be created: ST_FILETRACKING_ARCHIVE and ST_SERVERLOG_ARCHIVE. They are used only if SecureTransport is installed using Microsoft SQL Server Enterprise Edition, and transfer and log entry maintenance applications are configured to export data. Also the database user needs write permissions on the export directory. The database user should be granted Backup database and Backup log permissions. Backup log permission is only required only if the database is configured in Full recovery model.
- The default filegroup for the database user must be ST_DATA.
- The database must have a user defined that is mapped to the login that SecureTransport will use to access the database.
- The authentication mode for the user must be Microsoft SQL Server Authentication.

- The user must be a member of the following database roles:
  - `db_datareader`
  - `db_datawriter`
  - `db_ddladmin`

  For example, the `db_owner` user has the required permissions.

Note In addition to the current required roles for SQL Server you have to add a data definition language admin (ddladmin) role. The ddladmin can apply changes to the database schema. The ddladmin role is required during patch installation (when the patch changes the schema), upgrade, service pack installations and fresh installations.

During the installation, you need the following information:

- Database access port number
- Database user name and password
- Database name
- If the database is used over secure connection, you will also need the database server certificate signer or JKS keystore which contains it in order to trust the connection. In addition, the optional parameter **Common Name (CN)** can be provided and installer will verify the provided information against the database certificate's CN. If it is not provided, the installer will not check the certificate CN and will trust any.

Database size in production

The *Database size in production* topic has been removed from the *SecureTransport 5.4 Installation Guide* and has been added as part of the *SecureTransport 5.4 Capacity Planning Guide*.

UNIX-based platforms

Review the following topics before you install SecureTransport on a UNIX-based system:

- *Supported operating systems* on page 19 - Lists the supported UNIX-based operating systems and updates.
- *Minimum UNIX hardware requirements* on page 19 - Lists the minimum UNIX hardware requirements.
- *Host name resolution* on page 21 - Provides how to instructions for resolving the host name.
- *Requirements for specific operating systems* on page 21 - Lists the requirements for specific operating systems.
- *General prerequisites* on page 21 - Lists the general prerequisites.
- *Prerequisites for non-root installations* on page 25 - Lists the prerequisites for non-root installations.

Supported operating systems

All SecureTransport Servers in a cluster must run on the same operating system. All SecureTransport Edge servers that synchronize configuration must run on the same operating system. However, in a multitier security deployment, the operating system for SecureTransport Server systems can be different from the operating system for the SecureTransport Edge systems.

SecureTransport is a 64-bit application and requires a 64-bit version of the supported operating systems. The embedded MySQL database runs as a 32-bit process when SecureTransport is installed in an IBM AIX environment. On all the other supported 64-bit operating systems the embedded MySQL database runs as a 64-bit process.

For a full list of supported operating systems and updates, refer to Axway and third-party software support.

For virtual platforms, see *Virtualization support* on page 13.

Minimum UNIX hardware requirements

SecureTransport runs on any computer or virtual environment capable of running the supported version of the operating system. The computer or virtual environment requires a functional network connection.

The following table provides the minimum hardware requirements needed to install SecureTransport:

Platform	Architecture	RAM for 64-bit OS
IBM AIX	IBM POWER	8 GB
Oracle Enterprise Linux	x86_64	8 GB
Oracle Solaris	SPARC	8 GB
Red Hat Enterprise Linux	x86_64	8 GB
SUSE Linux Enterprise Server	x86_64	8 GB

During SecureTransport installation, approximately 20 GB of free disk space is temporarily required for the extracted installer and SecureTransport files. The files are removed when the installation completes. If the installation fails, you can reclaim the disk space by removing the `/tmp/AxwayTemp`*`timestamp`* directory.

During SecureTransport upgrade, the `/tmp` directory requires an additional 20 GB of free space for a total of approximately 40 GB of free space needed to upgrade. The additional `/tmp` directory space is not required for fresh installations or during normal operations.

Alternatively, prior the upgrade, the `TEMPORARY_DIR` environment variable, pointing to a directory with sufficient space, can be exported to be used during the installation or upgrade.

To install and run SecureTransport, the OS must be able to allocate at least 8 GB of memory to SecureTransport. On UNIX-based platforms, you can limit the system resources available using `ulimit` or similar commands.

Note Ensure the resources allowed include at least 8 GB of memory.

The following topics provide the minimum UNIX hardware requirements:

- *Viewing memory limits* on page 20
- *Changing memory limits* on page 20

Viewing memory limits

You can view the memory limitations using the command `ulimit -a`. These limitations need to be adjusted for the `root` user for the installation to run correctly and for the user running SecureTransport if a non-root install is done. After installation, only the user running SecureTransport should be able to allocate that much memory.

Changing memory limits

To change these limits, different commands are used for each UNIX-based platform.

To set system resource limits on AIX:

1. At the command line, type `smitty users` and press Enter.
2. From the menu, select `Change / Show Characteristics of a User`.

   Ensure that `Soft DATA segment` and `Hard DATA segment` allows more than 1 GB of memory. For best results, set these options to unlimited (`-1`).

To set system resource limits on RHEL:

1. Modify the file `/etc/security/limits.conf`. Use the following setting to allow more than 1 GB of memory:

   ```
   <username> hard memlock 1048576
   ```

2. Reboot the computer.

To set system resource limits on Oracle Solaris:

- To change the memory limit, use the `projmod` command to set the `rcap.max-rss` attribute in the `/etc/project` file:

  ```
  projmod -s -K rcap.max-rss=<MemoryInGB> db
  ```

  where `<MemoryInGB>` is the amount of memory such as `10GB`.

Host name resolution

For SecureTransport to run, the host name of the server must resolve to its actual IP address, not the loopback address (127.0.0.1).

1. Use `nslookup` to check the IP address for the server.
2. If the IP address returned is not the actual IP address of the server, check `/etc/hosts` and remove any entry that maps the host name to the loopback address and check the IP address again.
3. If the IP address returned is not correct, check your the operating system name resolution settings, correct any errors, and check the IP address again.
4. If the IP address returned is not correct, add an entry to `/etc/hosts` that maps the host name to the correct IP address.

General prerequisites

Review the following information before starting the installer:

- Make sure the umask is 022.
- The `/tmp` folder must have enough free space and the necessary permissions to execute the binaries. SecureTransport shows errors and fails if `/tmp` is mounted with the `noexec` flag. To resolve the problem, remount the temp location with "exec" permission using the command:

  ```
  mount -o remount,exec /tmp
  ```

  Alternatively, export the temporary directory to another location that already has executable permissions. Before you upgrade, set the environment variable `TEMPORARY_DIR` to the new tmp directory: `export TEMPORARY_DIR= <new_tmp_path>`.
- All SecureTransport Servers in a cluster must use the same installation path, such as `/opt/Axway/SecureTransport`.
- Copy the `taeh` file from the systems running the primary server in a Standard Cluster or the first server in the Enterprise Cluster to the system where you will install the subsequent server.

Requirements for specific operating systems

Review the information for your operating system before starting the installer.

The following topics provide requirements for specific operations systems:

- *Requirements for specific operating systems* on page 21
- *AIX requirements* on page 22
- *Oracle Linux / RHEL / CentOS requirements* on page 23

- *SLES requirements* on page 24
- *Solaris requirements* on page 25

Prior to installing SecureTransport on UNIX operating systems, you must install an unzip utility of your choice.

AIX requirements

Complete the following tasks before installing SecureTransport on IBM AIX.

Increase file size limit

There is a default 1 GB limit on the size of files on AIX. The 1GB file size limit must be removed by editing the `/etc/security/limits` file. Change the default to:

```
fsize = -1
```

You can also use AIX System Management Interface Tool (SMIT) to change the file size limit.

1. Enter `smitty users`.
2. From the menu, select `Change / Show Characteristics of a User`.

   Ensure that `Soft FILE size` is set to unlimited (`-1`).

By default, a JFS filesystem created on AIX has a limit of 2 GB. For best results, create a JFS filesystem with large file support.

Check and set ARG_MAX

Before installing SecureTransport, ensure the `ARG_MAX` setting is correct. It must be at least 9. For best results, use 256 or higher, up to 1024.

1. Check the ARG_MAX setting by typing the following:

   ```
   getconf ARG_MAX
   ```

2. If the value is less than 1048576, run the following command as the root user:

   ```
   chdev -l sys0 -a ncargs=256
   ```

Allow larger socket buffers

For Enterprise Clustering, SecureTransport Server requires larger socket buffers than the default. Use the following commands to allow larger socket buffers:

```
/usr/sbin/no -p -o rfc1323=1
/usr/sbin/no -p -o sb_max=4194304
```

Change maximum bundle size

For Enterprise Clustering, use the following commands to change the maximum bundle size:

```
/usr/sbin/no -p -o udp_recvspace=4194304
/usr/sbin/no -p -o udp_sendspace=65536
```

Check and set locale

Use the following command to check the locale:

```
locale
```

If the output does not include `LC_CTYPE=en_US.UTF-8`, change the locale to `EN_US.UTF-8` using the Manage Language Environment menu in SMIT. Be sure that EN_US.UTF-8 locale is installed on your system

Oracle Linux / RHEL / CentOS requirements

The following tasks must be completed before installing SecureTransport on Oracle Linux, Red Hat Enterprise Linux or CentOS.

Note A 64-bit Perl interpreter and a 64-bit Perl `Data::Dumper` module are required for installing SecureTransport with an embedded MySQL database. The Perl interpreter and the Perl `Data::Dumper` module can be removed after a successful installation. The Perl interpreter and `Perl Data::Dumper` are required when upgrading SecureTransport with an embedded MySQL database. If your SecureTransport Server is running on RedHat Enterprise Linux 6.x, be sure that you have the `numactl` package installed.

Install package

To install SecureTransport on RHEL systems, you need to install the following packages:

- 32-bit `glibc.i686` library package (provides `ld-linux.so.2`)
- 32-bit `zlib` library package
- 64-bit `libaio` library package

The packages are available on the operating system installation media or from the Red Hat Network website.

Allow larger socket buffers

For Enterprise Clustering, SecureTransport Server requires larger socket buffers than the default. Add the following lines to the `/etc/sysctl.conf` file to allow larger socket buffers:

```
net.core.rmem_max=2096304
net.core.wmem_max=2096304
net.ipv4.tcp_moderate_rcvbuf=1
```

Then run the following command to apply the settings immediately:

```
sysctl -p
```

Increase the maximum number of file descriptors

SecureTransport requires more than the default number of file descriptors. Add the following line to the `/etc/sysctl.conf` file:

```
fs.file-max = 65536
```

Then run the following command to apply the settings immediately:

```
sysctl -p
```

SLES requirements

The following tasks must be completed before installing SecureTransport on SUSE Linux Enterprise Server:

- Perform a Minimal System SLES installation. Do not install the X Window System.
- Install the following packages:
  - `unzip` (to unpack the installation package)
  - `numactl`
  - `which`
  - `glibc-32bit`
  - `libz1-32bit`
- Install the Server Base System pattern.
- If AppArmor is installed, disable it as follows:
  1. Start YaST.
  2. Select **System > System Services(Runlevel)**.
  3. Select **Expert Mode**.
  4. Select `boot.apparmor` and click **Set/Reset > Disable the service**.
  5. Click **Finish** to exit the YaST Runlevel tool.
- *Increase the maximum number of file descriptors* on page 24

Solaris requirements

Complete the following task before installing SecureTransport on Oracle Solaris.

Note Install Platform Information and Control Library (PICL). If it's not installed the performance of SecureTransport may not be optimal.

Note When you install SecureTransport on a Solaris zone, be sure that the `xcu4` package (`pkg://solaris/system/xopen/xcu4`) is installed on the Solaris installation zone.

Allow larger socket buffers

For Enterprise Clustering, SecureTransport Server requires larger socket buffers than the default. Use the following command to allow larger socket buffers:

```
ndd -set /dev/udp udp_max_buf 2096304
```

Prerequisites for non-root installations

If you are installing SecureTransport for a non-root execution, consider the following information before starting the installer:

- The installation process should be started with the non-root user, defined in the `/etc/passwd` file and have a valid shell that allows login and command execution. For example, `/sbin/nologin` is not a valid shell, but `/bin/bash` is a valid shell.
- Increase the resources available to the shell of the non-root user:
  - open files
  - max user process

  You can check the values of these limits by using `ulimit -a`. Set them to minimum **65536** or higher.
- The SecureTransport installation routine calls crontab to set up some entries for log rotation and process monitoring. To tell the installer to skip the calls to crontab:

  `export INSTALL_CRON=false`

Windows platforms

You must meet these prerequisites before installing SecureTransport 5.4 on Windows platforms:

- Make sure you have administrative privileges on the machine where you want to install SecureTransport Server or Edge.

Note Local Administrator credentials are required to install SecureTransport. Installation by an LDAP user with Administrator privileges is not supported.

- Make sure any antivirus software running on the computer is disabled. Leaving the antivirus software running can cause the install to fail.
- You have installed Microsoft Visual C++ 2010 SP1 Redistributable Package (x64). Download the package here.

The following topics provide additional Windows platform prerequisite information:

- *Supported operating systems* on page 26 - Lists the supported Windows operating systems.
- *Minimum Windows hardware requirements* on page 26 - Lists the minimum Windows hardware requirements.

Supported operating systems

All SecureTransport Servers in a cluster must run on the same operating system. All SecureTransport Edge servers that synchronize configuration must run on the same operating system. However, in a multitier security deployment, the operating system for SecureTransport Server systems can be different from the operating system for the SecureTransport Edge systems.

SecureTransport is a 64-bit application.

For a full list of supported operating systems and updates, refer to Axway and third-party software support.

For virtual platforms, see *Virtualization support* on page 13.

Minimum Windows hardware requirements

SecureTransport requires an x86_64 processor with 2 cores and 8 GB RAM.

Install 3

SecureTransport 5.4 uses the Axway Installer for new installations. The following topics provide the procedures for installing SecureTransport:

- *UNIX-based platforms* on page 27 - Provides instructions for installing SecureTransport on UNIX-based platforms.
- *Windows platforms* on page 42 - Provides instructions for installing SecureTransport on Windows-based platforms.
- *Silent installation of SecureTransport* on page 48 - Provides instructions for silent installation of SecureTransport deployments

UNIX-based platforms

This topic explains how to install SecureTransport on UNIX-based platforms.

SecureTransport 5.4 uses the Axway Installer in console mode for new installations on UNIX-based platforms. To navigate through the wizard, use the following commands:

- To go to the next dialog, type `Next`, `N`, or `n` or press Enter if the installer prompts you with `>Next`.
- To go to the previous dialog, type `Previous`, `P`, or `p`.
- To exit the installation type `Quit`, `Q`, or `q`.

For field values, use the following:

- To edit an option, select it by typing its number from a list and enter the new value.
- To accept a value, press Enter.

The following topics provide the how to instructions for installing SecureTransport on UNIX-based platforms:

- *Install SecureTransport to use the embedded database* on page 28 - Provides how to instructions for installing SecureTransport to use the embedded database.
- *Install SecureTransport Server in an Enterprise Cluster or to use an external database* on page 33 - Provides how to instructions for installing SecureTransport Server in an Enterprise Cluster or to use an external database.
- *Run SecureTransport as a service on UNIX-based platforms after non-root installation* on page 40 - Provides how to instructions for running SecureTransport as a service on UNIX-based platforms.

Install SecureTransport to use the embedded database

Use this installation procedure to install SecureTransport on UNIX-based platforms where the installation will use the embedded database server:

- Stand-alone SecureTransport Server
- SecureTransport Server in a Standard Cluster
- SecureTransport Edge

Check the pre-installation information and prerequisites before you install.

This procedure assumes that SecureTransport is not installed on the system. Only one instance of SecureTransport Server or SecureTransport Edge is supported in a production environment. To upgrade an existing installation, refer to the *SecureTransport Upgrade Guide*.

1. Log in to the system as the user who will run SecureTransport.
2. Copy the Axway Installer file into a temporary directory and navigate to that temporary directory.
3. Extract the installation files using the following commands:

   ```
   unzip SecureTransport_5.4.0_Install_<OS>-<processor>_<buildNumber>.zip
   ```

   where the placeholders represent the following:

   - `<OS>` is the operating system: `aix` (for IBM AIX), `linux` (for Linux), or `sun` (for Oracle Solaris).
   - `<processor>` is the type of processor running the operating system: `power-64`, or `sparc-64`, or `x86-64`.
   - `<BuildNumber>` is the actual build number listed in the installer executable file, for example, `BN1234`.
4. Enter the following commands to run the Axway Installer:

   ```
   ./setup.sh -m console
   ```

   The installer initializes and displays a welcome message and a prompt.

   ```
   Initialization in progress
   ..............

   ----------------------------------------
   Welcome
   ----------------------------------------
   Welcome to the Axway Installer wizard for SecureTransport Server and
   SecureTransport Edge.
   ```

```
This wizard will install SecureTransport Server or SecureTransport
Edge on your computer.
Next (type Next or N or n): to go to next Dialog
Previous (type Previous or P or p): to go to previous Dialog
Quit (type Quit or Q or q): to abort
If you want to delete a field value, use the Space bar or the Tab key.
During installation, all values or choices must be validated by
pressing Enter.
Enter (Next, Quit).
>Next
```

5. Press Enter.

   The installer will display the license agreement page by page. After each one there is a **Press ENTER to continue** prompt. After all license agreement pages are displayed, the installer displays the license agreement and the following prompt (for accepting or rejecting the license agreement):

```
[1] I accept the terms of the license agreement.
[2] I do not accept the terms of the license agreement.
Enter a number [1-2] to select an option or (Previous, Quit).
:>2
```

6. Enter 1 to accept the license agreement. Enter 2 to reject the license agreement and cancel the installation (default).

   The installer displays a prompt for the Axway installation directory:

```
----------------------------------------
Installation directory
----------------------------------------
Specify the directory where you want to install the products and
documentation.
1: Installation Directory:           /<userHome>/Axway
Enter 1 to select an option or (Next, Previous, Quit).
:>Next
```

   where <userHome> represents the home directory of the user running the installation.

7. To change a value, enter the number for the value.

   The installer displays a prompt for you to enter a new value.

8. Enter the new value.

   The value of the Installation Directory field must be an absolute path. The installer installs its files, including files required to update and uninstall SecureTransport 5.4, in the directory that you specify in this step and uses that directory as the parent directory in the default values of the SecureTransport installation directory. You specify the SecureTransport installation directory in a later step.

The installer displays the installation type choice:

```
----------------------------------------
Modules
----------------------------------------
Select the modules you want to install, then type Next to continue the
 configuration.

Axway SecureTransport V5.4:
1 :[x] Server
2 :[ ] Edge
Enter a number[1-2] (Next, Previous, Quit)
:>Next
```

9. To install SecureTransport Server, accept the default. To install SecureTransport Edge, enter `2` and confirm that Edge is selected when the installer displays the prompt again.

   The installer displays a prompt for the SecureTransport installation directory:

```
----------------------------------------
Installation directory
----------------------------------------
To specify the directory where the product is installed, type the path
directly, or press Enter to select the displayed default.
1: Select the installation directory for SecureTransport:
<AxwayHome>/SecureTransport
Press 1 to change the selected option or (Next, Previous, Quit).
:>Next
```

   where `<AxwayHome>` is the directory you specified in the previous installation directory step.

10. Accept the default or change the directory name.

    Do not use the directory where you copied the installer files. All SecureTransport Servers in a cluster or SecureTransport Edges that are synchronized must use the same installation directory. The name of the SecureTransport installation directory cannot contain space characters, the tab character, or the ~ character. For example, `/root/Axway/STServer` is valid, but `/root/Axway/ST Server` is not.

    This installation directory is referred to as `<FILEDRIVEHOME>` throughout this document and other SecureTransport documents.

    If you are installing SecureTransport Edge, the installer displays the embedded port number prompt shown in the next step.

    If you are installing SecureTransport Server, the installer displays the database selection prompt:

```
----------------------------------------
```

```
Database settings
--------------------------------------
[1] Embedded Database (MySQL)
[2] External Oracle Database
[3] External Microsoft SQL Server Database
Enter a number [1-3] to select an option or (Previous, Quit).
:>1
```

11. Press Enter to accept the default, the embedded database.

    Note For installation using an external database, see *Install SecureTransport Server in an Enterprise Cluster or to use an external database* on page 33.

    The installer displays the embedded port number prompt:

```
---------------------------------------


Database settings
---------------------------------------
Provide the settings for the MySQL database:
1: Port: 33060


Press 1 to change the selected option or (Next, Previous, Quit).
:>Next
```

12. Enter `1` to select a new port number for the embedded database installed by SecureTransport or accept the default setting.

    The installer displays the default SecureTransport ports, nightly log rotation, and import secret file configuration:

```
---------------------------------------
Configuration
---------------------------------------
  Select the options that you want to enable:
  SecureTransport Ports
1: SSL Admin UI Port:           444
2: Tomcat Shutdown Port:        8005
3: Enable Nightly Log Rotation: true
  Import Secret File
To synchronize the configuration of this ST Server with another ST
Server you must import the same secret file (located on the remote ST
Server at: <installation path>/bin/taeh). Otherwise, leave the field
empty to generate a new secret file.
4: Secret File Path:

 Enter a number [1-4] to select an option or (Next, Previous, Quit).
:>Next
```

13. Accept or modify the default configuration.

The information required is:

- **SSL Admin UI Port** – The port used to connect to the Administration Tool. When you install SecureTransport as a non-root user, the default value for Admin port number is 8444.
- **Tomcat Shutdown Port** – The port used to shut down the Tomcat server
- **Enable Nightly Log Rotation** – Select if you want the system to perform automatic backup and purging of log files on a nightly basis. When this feature is enabled, SecureTransport Server backups log files, generated on the respective day, and creates a new one for the subsequent day. The server takes a back up and creates a new log file at 23:59 or 00:00 hours, depending on the log file type. This option is enabled by default. You can enable or disable the nightly log rotation after installation. For more information, see the *SecureTransport Administrator's Guide*, Server Log Rotation Scheduling.
- **Secret File Path** – The path to the secret file you copied from another SecureTransport Server installation to this system, if blank, the installer creates a secret file (See *Secret file* on page 14.)

When you have modified these values as required for your installation, press Enter.

The installer prepares the installation execution and displays its last prompt:

```
----------------------------------------
Installation execution
----------------------------------------
All selected products are ready to install. Type Next to start
installing. If not, type Previous to make changes.
Enter (Next, Previous, Quit).
>Next
```

14. Press Enter to start the installation.

    The installer displays progress messages as it completes the installation tasks.

    When the installation is complete, the installer displays:

```
Installation successful


----------------------------------------


Summary
----------------------------------------
The information below summarizes the installation status. Refer to
install.log for more details.

------------------------------------------------------------
Axway_Installer_V4.8.0
Installed in /opt/TMWD/Axway/
Axway_Installer_4.8.0_SP3 has been applied successfully.
------------------------------------------------------------
```

```
Product: SecureTransport_V5.4
Installed in /opt/Axway/SecureTransport
------------------------------------------------------------
Enter a number [1-2] to select an option.

[1]Finish installation
[2]Update the installed products
:>1
```

15. Press Enter to exit the installer or select update mode to apply patches or service packs without leaving the installer.

The installer also creates a log file, `<AxwayHome>/install.log`.

After successfully installing SecureTransport, you must perform a number of post-installation steps, such as applying your SecureTransport licenses, and enabling, configuring, and starting the SecureTransport services. For more information, see the *SecureTransport Getting Started Guide*.

Install SecureTransport Server in an Enterprise Cluster or to use an external database

Note The SecureTransport Enterprise Cluster installation will fail if the database password contains the dollar sign (`$`) and other special characters.

Use this installation procedure to install SecureTransport on UNIX-based platforms where the installations will use an external database server:

- SecureTransport Server in an Enterprise Cluster
- Stand-alone SecureTransport Server when an external Oracle or Microsoft SQL Server database server is otherwise required

To use an external database, either in single or in multi-node environment, you need a license for the Enterprise Clustering (EC) option.

Check the pre-installation information and prerequisites before you install.

All the nodes of a SecureTransport Enterprise Cluster share the same database schema and use the same installation directory and secret (`taeh`) file. The installer creates that schema when you install the first server in the cluster. You can have the installer create the `taeh` file or import an existing file for the first server in the cluster. You must copy and import the `taeh` file to the second and subsequent servers in the cluster before you install. For more information, see *Secret file* on page 14.

This procedure assumes that SecureTransport is not installed on the system. Only one instance of SecureTransport Server or SecureTransport Edge is supported in a production environment. To upgrade an existing installation, refer to the *SecureTransport Upgrade Guide*.

1. Log in to the system as the user who will run SecureTransport.
2. Copy the Axway Installer file into a temporary directory and navigate to that temporary directory.

3. Extract the installation files using the following commands:

```
unzip SecureTransport_5.4_Install_<OS>-<processor>_<buildNumber>.zip
```

where the placeholders represent the following:

- <OS> is the operating system: aix (for IBM AIX), linux (for Linux), or sun (for Oracle Solaris).
- <processor> is the type of processor running the operating system: power-64, or sparc-64, or x86-64.
- <BuildNumber> is the actual build number listed in the installer executable file, for example, BN1234.

4. Enter the following command to run the Axway Installer:

```
./setup.sh -m console
```

The installer initializes and displays a welcome message and a prompt.

```
Initialization in progress
........

----------------------------------------
Welcome
----------------------------------------
Welcome to the Axway Installer wizard for SecureTransport Server and
SecureTransport Edge.
This wizard will install SecureTransport Server or SecureTransport
Edge on your computer.
Next (type Next or N or n): to go to next Dialog
Previous (type Previous or P or p): to go to previous Dialog
Quit (type Quit or Q or q): to abort
If you want to delete a field value, use the Space bar or the Tab key.
During installation, all values or choices must be validated by
pressing Enter.
Enter (Next, Quit).
>Next
```

5. Press Enter.

The installer will display the license agreement page by page. After each one there is a **Press ENTER to continue** prompt. After all license agreement pages are displayed, the installer displays the license agreement and the following prompt (for accepting or rejecting the license agreement):

```
[1] I accept the terms of the license agreement.
[2] I do not accept the terms of the license agreement.
```

```
Enter a number [1-2] to select an option or (Previous, Quit).
:>2
```

6. Enter 1 to accept the license. Enter 2 to reject the license and cancel the installation (default).

   The installer displays a prompt for the Axway installation directory:

```
----------------------------------------
Installation directory
----------------------------------------
Specify the directory where you want to install the products and
documentation.
1: Installation Directory:           /<userHome>/Axway
Enter 1 to select an option or (Next, Previous, Quit).
:>Next
```

   where <userHome> represents the home directory of the user running the installation.

7. To change a value, enter the number for the value.

   The installer displays a prompt for you to enter a new value.

8. Enter the new value.

   The value of the Installation Directory field must be an absolute path. The installer installs its files, including files required to update and uninstall SecureTransport 5.4, in the directory that you specify in this step and uses that directory as the parent directory in the default values of the SecureTransport installation directory. You specify the SecureTransport installation directory in a later step.

   The installer displays the installation type choice:

```
----------------------------------------
Modules
----------------------------------------
Select the modules you want to install, then type Next to continue the
 configuration.

Axway SecureTransport V5.4:
1 :[x] Server
2 :[ ] Edge
Enter a number[1-2] (Next, Previous, Quit)
:>Next
```

9. Press Enter to accept the default, SecureTransport Server.

   The installer displays a prompt for the SecureTransport installation directory:

```
----------------------------------------
```

```
Installation directory
----------------------------------------
To specify the directory where the product is installed, type the path
directly, or press Enter to select the displayed default.
1: Select the installation directory for SecureTransport:
<AxwayHome>/SecureTransport
Press 1 to change the selected option or (Next, Previous, Quit).
:>Next
```

where <AxwayHome> is the directory you specified in the previous installation directory step.

10. Accept the default or change the directory name.

    Do not use the directory where you copied the installer files. All SecureTransport Servers in a cluster must use the same installation directory. The name of the SecureTransport installation directory cannot contain space characters, the tab character, or the ~ character. For example, /root/Axway/STServer is valid, but /root/Axway/ST Server is not.

    This installation directory is referred to as <FILEDRIVEHOME> throughout this document and other SecureTransport documents.

    The installer displays the database selection prompt:

```
----------------------------------------

Database settings
----------------------------------------
Select the database to use:
[1] Embedded Database (MySQL)
[2] External Oracle Database
[3] External Microsoft SQL Server Database
Enter a number [1-3] to select an option or (Previous, Quit).
:>1
```

11. Select the external database type for SecureTransport to use.

    Note For installation using the embedded database, see *Install SecureTransport to use the embedded database* on page 28.

    If you selected Microsoft SQL Server, continue with step 14.

12. If you selected Oracle, the installer displays the Oracle database settings:

```
----------------------------------------

Database settings
----------------------------------------
Provide the settings for the Oracle database:
1: Host:
2: Port:                          1521
3: User Name:
```

```
4: Password:
5: Service Name:
6: Use existing database schema: false
7: Use secure connection: true
8: Server Certificate DN:
9: TrustStore File Path:
Enter a number [1-9] to select an option or (Next, Previous, Quit).
:>Next
```

13. Supply the required Oracle database settings:
    - **Host** – The FQDN or IP address of the Oracle system or cluster
    - **Port** – The number of 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 to the Oracle server or cluster
    - **Use secure connection** - When true, database connection will be established over a secure connection. True is the default value.
    - **Server Certificate DN** (Optional) - Server certificate DN value. If provided, the installer will explicitly match the provided value against the certificate provided by the database server.
    - **TrustStore File Path** - PEM or DER file, or JKS (Java Key Store) keystore containing the trusted certificates needed by the installer to establish a chain of trust.

    Continue with step 15.
14. If you selected Microsoft SQL Server, the installer displays the Microsoft SQL Server database settings:

```
----------------------------------------
Database settings
----------------------------------------
Provide the settings for the Microsoft SQL server database:
1: Host:
2: Port:                        1433
3: Login Name:
4: Password:
5: Database Name:
6: Use existing database schema: false
7: Use secure connection: true
8: Server Certificate CN:
9: TrustStore File Path:
Enter a number [1-6] to select an option or (Next, Previous, Quit).
:>Next
```

Supply the required Microsoft SQL Server database settings:

- **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
- **Login Name** – The name of the user authorized to create the SecureTransport schema and populate it
- **Password** – The password for the user, not displayed
- **Database Name** – Used to connect to the Microsoft SQL Server
- **Use secure connection** - When true, database connection will be established over a secure connection. True is default value.
- **Server Certificate CN** (Optional) - Server certificate CN value. If provided, the installer will explicitly match the provided value against the certificate provided by the database server. If not provided, the installer will trust any.
- **TrustStore File Path** - PEM or DER file, or JKS (Java Key Store) keystore containing the trusted certificates needed by the installer to establish chain of trust.

15. The database connection information must be the same for all SecureTransport Servers in a cluster.

    The value for **Use existing database schema** depends on whether you are installing the SecureTransport on a stand-alone server or the first server of an Enterprise Cluster, or on another clustered server:

    - If you are installing the first server in a cluster or a stand-alone server, accept the default so that the installer creates the database schema.
    - If you are installing the second or a subsequent server in the cluster, set **Use existing database schema** to `true` to use the database schema created when you installed the first server.

    When you have entered all the settings, press Enter to accept the values.

    The installer tests the connection to the database. If the installer cannot connect, it displays an error message and you must correct the database settings.

16. When the installer verifies the database connection, it displays the default SecureTransport ports, nightly log rotation, and import secret file configuration:

```
----------------------------------------
Configuration
----------------------------------------
  Select the options that you want to enable:
  SecureTransport Ports
1: SSL Admin UI Port:           444
2: Tomcat Shutdown Port:        8005
3: Enable Nightly Log Rotation: true
  Import Secret File
To synchronize the configuration of this ST Server with another ST
```

```
Server you must import the same secret file (located on the remote ST
Server at: <installation path>/bin/taeh). Otherwise, leave the field
empty to generate a new secret file.
4: Secret File Path:

 Enter a number [1-4] to select an option or (Next, Previous, Quit).
:>Next
```

17. Accept or modify the default settings.

    If you selected **Use existing database schema** for the second or subsequent server in an Enterprise Cluster, the following three fields are not available.

    - **SSL Admin UI Port** – The port used to connect to the Administration Tool. When you install SecureTransport as a non-root user, the default value for Admin port number is 8444.
    - **Tomcat Shutdown Port** – The port used to shut down the Tomcat server

    The following field is always available:

    - **Enable Nightly Log Rotation** – Select if you want the system to perform automatic backup and purging of log files on a nightly basis. When this feature is enabled, SecureTransport Server backups log files, generated on the respective day, and creates a new one for the subsequent day. The server takes a back up and creates a new log file at 23:59 or 00:00 hours, depending on the log file type. This option is enabled by default. You can enable or disable the nightly log rotation after installation. For more information, see the *SecureTransport Administrator's Guide*.
    - **Secret File Path** – The path to the secret (`taeh`)file you copied to this system. If you leave it blank, the installer creates a new secret file.

      If you are installing the first server in an Enterprise Cluster, you can specify a secret file or have the installer create one. Before you install SecureTransport on the other cluster nodes, you must copy the secret file to those systems.

      If you are installing the second or a subsequent server in the cluster, you must use the secret file you copied from the first server. See *Secret file* on page 14.

    When you have modified these values as required for your installation, press Enter.

    The installer prepares the installation execution and displays its last prompt:

```
----------------------------------------
Installation execution
----------------------------------------
All selected products are ready to install. Type Next to start
installing. If not, type Previous to make changes.
Enter (Next, Previous, Quit).
>Next
```

18. Press Enter to start the installation.

    The installer displays progress messages as it completes the installation tasks.

When the installation is complete, the installer displays:

```
Installation successful

---------------------------------------

Summary
---------------------------------------
The information below summarizes the installation status. Refer to
install.log for more details.

-------------------------------------------------------------
Axway_Installer_V4.8.0
Installed in /root/Axway/
Axway_Installer_4.8.0_SP3 has been applied successfully.
-------------------------------------------------------------
Product: SecureTransport_V5.4
Installed in /root/Axway/SecureTransport/
-------------------------------------------------------------
Enter a number [1-2] to select an option.

[1]Finish installation
[2]Update the installed products
:>1
```

19. Press Enter to exit the installer or select update mode to apply patches or service packs without leaving the installer.

The installer also creates a log file, `<AxwayHome>/install.log`.

After successfully installing SecureTransport, you must perform a number of post-installation steps, such as applying your SecureTransport licenses, and enabling, configuring, and starting the SecureTransport services. For more information, see the *SecureTransport Getting Started Guide*.

Run SecureTransport as a service on UNIX-based platforms after non-root installation

To run SecureTransport as a service, you must log on as root and manually register it.

The following topics provide how to instructions for running SecureTransport as a service:

- *AIX* on page 40
- *Oracle Linux and RHEL* on page 41
- *SLES* on page 41

AIX

Use the following procedure to run SecureTransport as a service on AIX platforms:

1. Log on as root.
2. Edit `<FILEDRIVEHOME>/bin/utils/rc.AIX` and
   a. Replace `@FILEDRIVEHOME@` with the SecureTransport installation directory you specified during the installation.
   b. Replace `@USER@` with the name of the user who installed SecureTransport and will run it.
3. Run the following commands:

```
 cp <FILEDRIVEHOME>/bin/utils/rc.AIX /etc/rc.stransport
chmod 755 /etc/rc.stransport
```

4. Edit /etc/rc.tcpip and add the following line at the end of the file:

```
[ -f /etc/rc.stransport ] && sh /etc/rc.stransport start
```

Oracle Linux and RHEL

Use the following procedure to run SecureTransport as a service on Oracle Linux and RHEL platforms:

1. Log on as root.
2. Edit `<FILEDRIVEHOME>/bin/utils/rc.Linux` and
   a. Replace `@FILEDRIVEHOME@` with the SecureTransport installation directory you specified during the installation.
   b. Replace `@USER@` with the name of the user who installed SecureTransport and will run it.
3. Run the following commands:

```
cp <FILEDRIVEHOME>/bin/utils/rc.Linux /etc/init.d/rc.stransport
chmod 755 /etc/init.d/rc.stransport
chkconfig --add "rc.stransport"
```

SLES

Use the following procedure to run SecureTransport as a service on SLES platforms:

1. Log on as root.
2. Edit `<FILEDRIVEHOME>/bin/utils/rc.SLES` and
   a. Replace `@FILEDRIVEHOME@` with the SecureTransport installation directory you specified during the installation.
   b. Replace `@USER@` with the name of the user who installed SecureTransport and will run it.
3. Run the following commands:

```
cp <FILEDRIVEHOME>/bin/utils/rc.SLES /etc/rc.d/rc.stransport
chmod 755 /etc/rc.d/rc.stransport
chkconfig --add "rc.stransport"
```

Windows platforms

This topic explains how to install SecureTransport on Windows. SecureTransport 5.4 uses the Axway Installer in console mode or dialogs for new installations. The pages of the Axway Installer wizard on Windows are the same as the dialogs of the Axway Installer in console mode on UNIX-based platforms.

You cannot install more than one instance of SecureTransport on a Windows server. You can install one instance of either SecureTransport Server or SecureTransport Edge.

The following topics provide how to instructions for installing SecureTransport on Windows platforms and canceling a Windows installation:

- *Install SecureTransport Server on Windows with the embedded database* on page 42
- *Install SecureTransport Server on Windows with an external database* on page 44
- *Cancel the Windows installation* on page 48

Install SecureTransport Server on Windows with the embedded database

Use this procedure to install SecureTransport on Windows in all cases where it uses the embedded database server:

- Stand-alone SecureTransport Server
- SecureTransport Server in a Standard Cluster
- SecureTransport Edge

Before you install SecureTransport, check the pre-installation information and prerequisites.

This procedure assumes that SecureTransport is not installed on the system. Only one instance of SecureTransport Server or SecureTransport Edge is supported in a production environment. To upgrade an existing installation, refer to the *SecureTransport Upgrade Guide*.

During the installation, do not close any console windows that are opened.

1. Download the SecureTransport installation package for Windows from Axway Support. Note that the installation packages are different for Microsoft Windows Server 2012 and Microsoft Windows Server 2016/2019.
    - If you are installing SecureTransport on Windows Server 2012, download `SecureTransport_5.4_Install_win-x86-64_<buildNumber>.zip`
    - If you are installing SecureTransport on Windows Server 2016 or 2019, download `SecureTransport_5.4.0_Install_Win2016-2019_win-x86-64_<buildNumber>.zip`

      where `<BuildNumber>` is the actual build number, for example, `BN1234`.

2. Extract the zip file into a directory on the same drive where you are going to install SecureTransport. The name of the extracted folder is `SecureTransport_5.4_Install_win-x86-64`.
3. In the extracted folder, run the `setup64.exe` executable to begin the installation process.
4. The installer loads and displays the *Welcome* page. Click **Next** to proceed.
5. Read and accept the terms of the license agreement to continue.
   (Optional) Click Print to print out a copy of the license agreement.
6. Specify the **Installation Directory** to which the installer files to be deployed. It must reside on the same drive as the installation files. You can enter a custom location by using its absolute path.

   Note The directory path must not contain the tilde (~) character. Also, we recommend using a directory path without special characters and spaces

   This is the location where the installer installs its files, including files required to update and uninstall SecureTransport 5.4. It is also used as a parent directory of the SecureTransport default installation location.

   Click **Next** to continue.
7. Select the module or modules to install, **Server** or **Edge** and click **Next**.
8. Specify a location to install SecureTransport. By default, SecureTransport is installed in a sub-directory of the Axway Installer installation directory (specified at step 6). You can either accept the default or specify a new location following the requirements:
   - The SecureTransport installation directory must be specified using an absolute path. It must not contain the tilde (~) character; letters and digits are acceptable.
   - It must reside on the same drive as the SecureTransport installation files.
   - The SecureTransport installation directory and the Axway Installer components must never be in the same directory.

   SecureTransport Server is installed in the `STServer` sub-directory of the specified installation directory. The SecureTransport installation directory is referred to as `<FILEDRIVEHOME>` throughout the product documentation.

   Click **Next** to continue.
9. If you selected **Edge**, the installer displays another *Database settings* page. Continue with step 11.
10. If you selected **Server**, to install SecureTransport Server in a Standard Cluster or as a stand-alone Server using an embedded database, select **Embedded Database (MySQL)** and click **Next**.
11. Set the port for the embedded database, and click **Next**.

12. Accept or modify the configuration settings.
    - **SSL Admin UI Port** – default 444
    - **Tomcat Shutdown Port** – default 8005
    - **Enable Nightly Log Rotation** – Select if you want the system to perform automatic backup and purging of log files on a nightly basis. When this feature is enabled, SecureTransport Server backups log files, generated on the respective day, and creates a new one for the subsequent day. The server takes a back up and creates a new log file at 23:59 or 00:00 hours, depending on the log file type. This option is enabled by default. You can enable or disable the nightly log rotation after installation - see the *SecureTransport Administrator's Guide* for more information.
    - **Secret File Path**– The path to the `taeh` secret file you copied to this system. If blank, the installer creates a new secret file.

      If you are installing the first server in a cluster, you can specify a secret file or have the installer create one. Before you install SecureTransport on the other cluster nodes, you must copy the secret file to those systems.

      If you are installing the second or a subsequent server in the cluster, you must use the secret file you copied from the first server. See *Secret file* on page 14.

    Click **Next** to continue.
13. On the *Ready to install* page, click **Install** to start the installation.

    The installation process can take several minutes to complete.
14. When the installation procedure is complete, the installer displays the *Installation completed* page. Click **Next** to see summary information about your SecureTransport installation.
15. Click **Finish** to exit the installer.

    You can click **Update** to install patches or service packs without leaving the installer. Refer to the Readme files for the patches or service packs.

The installer also creates a log file, `<AxwayHome>/install.log`.

After successfully installing SecureTransport, you must perform a number of post-installation steps, such as updating your SecureTransport license, enabling, configuring, and starting the SecureTransport services. For more information, see the *SecureTransport Getting Started Guide*.

Install SecureTransport Server on Windows with an external database

Use this installation procedure to install SecureTransport on Windows Server where the installation will use an external database server:

- SecureTransport Server in an Enterprise Cluster
- Stand-alone SecureTransport Server when an external Oracle or Microsoft SQL Server database server is otherwise required

To use an external database, you need a license for the Enterprise Clustering (EC) option.

Check the pre-installation information and prerequisites before you install.

All the nodes of a SecureTransport Enterprise Cluster share the same database schema and use the same installation directory and secret (`taeh`) file. The installer creates that schema when you install the first server in the cluster. You can have the installer create the `taeh` file or import an existing secret file for the first server in the cluster. You must copy the `taeh` file to the second and subsequent servers in the cluster before you install. For more information, see *Secret file* on page 14.

This procedure assumes that SecureTransport is not installed on the system. Only one instance of SecureTransport Server or SecureTransport Edge is supported in a production environment. To upgrade an existing installation, refer to the *SecureTransport Upgrade Guide*.

During the installation, do not close any console windows that are opened.

1. Download the SecureTransport installation package for Windows from Axway Support. Note that there are different installation packages for Microsoft Windows Server 2012 and Microsoft Windows Server 2016/2019.
    - If you are installing SecureTransport on Windows Server 2012, download `SecureTransport_5.4_Install_win-x86-64_<buildNumber>.zip`
    - If you are installing SecureTransport on Windows Server 2016 or 2019, download `SecureTransport_5.4.0_Install_Win2016-2019_win-x86-64_<buildNumber>.zip`

      where `<BuildNumber>` is the actual build number, for example, `BN1234`.
2. Extract the ZIP file to a location on the same drive where you are going to install SecureTransport. The name of the extracted folder is `SecureTransport_5.4_Install_win-x86-64`.
3. In the extracted folder, run the `setup64.exe` executable to begin the installation process.
4. The installer loads and displays the *Welcome* page. Click **Next** to proceed.
5. Read and accept the terms of the license agreement to continue.

   (Optional) Click **Print** to print out a copy of the license agreement.
6. Specify the **Installation Directory** to which the installer files to be deployed. It must reside on the same drive as the installation files. You can enter a custom location by using its absolute path.

   Note The directory path must not contain the tilde (~) character. Also, we recommend using a directory path without special characters and spaces.

   In the directory that you specify in this step, the installer installs its files, including the files required to update and uninstall SecureTransport 5.4. The directory is used as the parent directory of the SecureTransport default installation location.

   Click **Next** to continue.
7. On the *Modules* page, click **Next** to install the default Server module.
8. Specify a location to install SecureTransport. By default, SecureTransport is installed in a sub-directory of the Axway Installer installation directory (specified at step 6). You can either accept the default or specify a new location following the requirements:

- The SecureTransport installation directory must be specified using an absolute path. It must not contain the tilde (~) character; letters and digits are acceptable.
- It must reside on the same drive as the SecureTransport installation files.
- The SecureTransport installation directory and the Axway Installer components must never be in the same directory.

The installer installs SecureTransport into the `STServer` directory in this installation directory. The SecureTransport installation directory is referred to as `<FILEDRIVEHOME>` throughout this document and other SecureTransport documents.

Click **Next** to continue.

9. On the *Database settings* page, select either **External Oracle Database** or **External Microsoft SQL Server Database** and click **Next**.
10. Supply the database settings.

    Note The database settings must be the same for all SecureTransport Servers in a cluster.

    If you selected Oracle, the *Database settings* page displays the following settings:

    - **Host** – The FQDN or IP address of the Oracle system or cluster
    - **Port** – The number of the port used to access the server or cluster, 1521 is the default
    - **Login 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 to the Oracle server or cluster
    - **Use secure connection** - When selected, the database connection will be established over a secure connection. The default value is: **true**
    - **Server Certificate DN** (Optional) - This is the Server certificate DN value. If provided, the installer will explicitly match the provided value against the certificate provided by the database server.
    - **TrustStore File Path** - PEM or DER file, or JKS (Java Key Store) keystore containing the trusted certificates needed by the installer to establish a chain of trust.

    If you selected Microsoft SQL Server, the *Database settings* page displays the following settings:

    - **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 create the SecureTransport schema and populate it
    - **Password** – The password for the user, not displayed
    - **Database Name** – Used to connect to the Microsoft SQL Server
    - **Use secure connection** - When selected, the database connection will be established over a secure connection. The default value is: **true**

- **Server Certificate CN** (Optional) - This is the Server certificate CN value. If provided, the installer will explicitly match the provided value against the certificate provided by the database server. If not provided, the installer will trust any.
- **TrustStore File Path** - PEM or DER file, or JKS (Java Key Store) keystore containing the trusted certificates needed by the installer to establish a chain of trust.

11. Select **Use existing database schema** depending on whether you are installing the SecureTransport on a stand-alone server or the first server of an Enterprise Cluster, or on another clustered server:
    - If you are installing the first server in a cluster or a stand-alone server, do not select **Use existing database schema**. The installer creates the database schema and the `taeh` file.
    - If you are installing the second or a subsequent server in the cluster, select **Use existing database schema** to use the database schema created when you installed the first server.

    Click **Next**.

    The installer tests the connection to the database. If the installer cannot connect, it displays an error message and you must correct the database settings.
12. When the installer verifies the database connection, it displays the *Configurations* page.

    If you selected **Use existing database schema** for the second or subsequent server in an Enterprise Cluster, you cannot changes the values of the following three fields.
    - **SSL Administration Tool Port** – default 444
    - **Tomcat Shutdown Port** – default 8005

    The following field is always available:
    - **Enable Nightly Log Rotation** – Select if you want the system to perform automatic backup and purging of log files on a nightly basis. When this feature is enabled, Server backups log files, generated on the respective day, and creates a new one for the subsequent day. The server takes a back up and creates a new log file at 23:59 or 00:00 hours, depending on the log file type. This option is enabled by default. You can enable or disable the nightly log rotation after installation - see the *SecureTransport Administrator's Guide* for more information.
    - **Secret File Path**– The path to the `taeh` secret file you copied to this system. If blank, the installer creates a new secret file.

      If you are installing the first server in an Enterprise Cluster, you can specify a secret file or have the installer create one. Before you install SecureTransport on the other cluster nodes, you must copy the secret file to those systems.

      If you are installing the second or a subsequent server in the cluster, you must use the secret file you copied from the first server. See *Secret file* on page 14.

    Click **Next** to continue.
13. On the *Ready to install* page, click **Install** to start the installation. The installer displays the *Installation in progress* page which shows the progress of the installation.

    The installation process can take several minutes to complete.

14. Once the SecureTransport installation has completed, the installer displays the *Installation completed* page. Click **Next** to see summary information about your SecureTransport installation.
15. Click **Finish** to exit the installer.

    You can click **Update** to install patches and service packs without leaving the installer. Refer to the readme files for the patches or service packs.

The installer also creates a log file, `<AxwayHome>/install.log`.

After successfully installing SecureTransport, you must perform a number of post-installation steps, such as updating your SecureTransport license, enabling, configuring, and starting the SecureTransport services. For more information, see the *SecureTransport Getting Started Guide*.

Cancel the Windows installation

You can cancel the installation by clicking **Quit**.The installer opens a confirmation window and proceeds according to your response.

Note If you quit while the installation is in progress, no rollback will be performed and the already installed content must be manually deleted.

Silent installation of SecureTransport

There is an option to perform a silent installation of SecureTransport of either Server or Edge to properly fit standalone or clustered deployments.

The current topic provides the basic step-by-step procedure for performing silent installation and includes the following subtopics:

- *Configurable properties for silent installation* on page 49 - contains a detailed list of configurable parameters and their properties, including the ones which are specific to your database deployments
- *Recommendations for Clustered SecureTransport deployments* on page 54
- *Silent file editor* on page 55 - contains a basic set of instructions for using the dedicated silent file editor tool, part of the SecureTransport installation package

The silent installation process requires you to pass though a few steps:

1. Start the SecureTransport installation in normal mode.
2. Complete the installer dialog screens up until the point of installation (for example, before clicking **Install**). This will add two `.properties` files:
    - `Install_Axway_Installer_<installer-version>.properties`
    - `Install_SecureTransport_<st-version>.properties`

3. Create a copy of each of the two `.properties` files under `<installation_root_directory>\SilentFile\<date_and_time>_install\` to a temp folder for later reuse.
4. Quit the installation in normal mode.
5. Edit `Install_Axway_Installer_<installer-version>.properties` and make sure to have the following declaration line included:

```
IncludeFiles.SecureTransport = Install_SecureTransport_V5.5.properties
```

6. Edit `Install_SecureTransport_<st-version>.properties` and make sure to have correct input for the minimum number of configurable properties. Scroll down to see the Configurable properties you'll need to configure for successful for all pertinent properties. To facilitate the editing process, see Silent file editor, part of the current topic as well.
7. Run the installation with the following switches for silent install:
8. `# ./setup.sh -s /path/to/Install_Axway_Installer_<version>.properties`

Note Use the Axway Installer properties file for the silent install, not the SecureTransport properties file.

Note Always provide the full path to the properties file, instead of a relative one.

Configurable properties for silent installation

Note The following list does not contain all configurable but only the ones you'll need to set for silent installation in different SecureTransport deployments. Please make sure to remove any empty valued properties as leaving these properties blank might adversely affect your silent installation!

The following table presents some useful configuration properties you can edit to perform silent installation of SecureTransport in the `Install_SecureTransport_<st-version>.properties` file:

Property	Description / Example
`Component.Version` *string*	The SecureTransport version to install example: `5.4`
`Component.InstallerVersion` *string*	The version of the Axway installer example: `4.8.0`
`Server` *boolean*	A flag which specifies if you're installing SecureTransport Server. Must be set to `false` when installing SecureTransport Edge.

Property	Description / Example
`Edge` *boolean*	A flag which specifies if you're installing SecureTransport Edge. Must be set to `false` when installing SecureTransport Server.
`externalDBUseExistingSchema` *boolean*	A flag which specifies if you're using an external database. Not applicable to SecureTransport Edge installation. **Important!** In a LEC deployment using an external database (Oracle or MSSQL), you must configure this value to `false` with the first Server node and to `true` all subsequent Server deployments in your LEC.

Note This table does not include all installation properties but just the ones you would need to edit in order to perform silent installation.

MySQL-specific configurable properties

The following table presents some database configuration properties you must configure, depending on your selected database implementation.

Property	Description / Example
`dbType` *enum*	The database to install: `useMySQLLocal` with mySQL databases
`mySQLPort` *integer*	Listener port of your mySQL database: `33060` by default
`mySQLPort.Type` *enum*	A flag identifying the mySQL listener port type: set to `IPPortOwner`
`mySQLPort.Max` *integer*	Upper threshold of mySQL port range example: `65535`
`mySQLPort.Min` *integer*	Lower threshold of mySQL port range example: `1024`

Oracle-specific configurable properties

The following table presents some Oracle database configuration properties you must configure, depending on your selected database implementation.

Property	Description / Example
`dbType` *enum*	The database to install: `useOracleExternal` with Oracle databases
`oracleHost` *string*	Database hostname or IP address: for example `oracle.localdomain.com`
`oracleHost.Type` *enum*	A flag identifying if you are using HostName or IP address for your database: either `HostName` or `IPaddress`
`oraclePort` *integer*	Listener port of your Oracle database: `1521` by default
`oraclePort.Type` *enum*	A flag identifying the listener port number format Example: `Integer`
`oracleUserName` *string*	The name of the database user account Example: `st_user`
`oraclePassword` *string*	The Oracle database encrypted password: for correct behavior, set the `oraclePassword.Format` property to `AES128`
`oraclePassword.Format` *enum*	The encryption format of your database password: `AES128` Do not change this value!
`oracleServiceName` *enum*	Service name of Oracle database: `orcl`
`externalDBUseExistingSchema` *boolean*	A flag specifying whether to use existing external DB schema or not. Its value must be the same as the one with the `oracleUseExistingSchema` property: either `true` or `false`
`oracleUseExistingSchema` *boolean*	A flag specifying whether to use existing Oracle DB schema or not: `true` or `false`
`oracleUseSecureConnection` *boolean*	A flag specifying whether to use SSL encryption for DB connection:`true` or `false`
`oracleCertificateDN` *string*	Distinguished name as specified in your SSL certificate

Property	Description / Example
`OracleTrustStoreFilePath` *string*	Path to DB public certificate in X.509 format
`OracleTrustStoreFilePath.Type` *enum*	Type of SSL certificate: set this value to `File`
`externalDBUseSecureConnection` *boolean*	A flag that specifies whether to use SSL encrypted communication to your external database. Its value must be the same as the one of the `oracleUseSecureConnection` property: either `true` or `false`
`externalDBCertificateName` *string*	Distinguished name as specified in your SSL certificate. This value must be the same as the one with the `oracleCertificateDN`
`externalDBTrustStore` *string*	Path to DB public certificate in X.509 format

MSSQL-specific configurable properties

The following table presents some MSSQL database configuration properties you must configure, depending on your selected database implementation.

Property	Description / Example
`dbType` *enum*	The database to install: `useMSSQLExternal` with MSSQL databases
`mssqlHost` *enum*	Database hostname or IP address Example: `sqlserver.localdomain.com`
`mssqlHost.Type` *enum*	A flag identifying if you are using HostName or IP address for your database: either `HostName` or `IPaddress`
`mssqlPort` *integer*	Listener port of your MSSQL database: `1433` by default
`mssqlPort.Type` *enum*	A flag identifying the listener port number format Example: `Integer`
`mssqlLoginName` *string*	The name of the database user account Example: `st_user`

Property	Description / Example
`mssqlPassword` *string*	The MSSQL database encrypted password: for correct behavior, set the `mssqlPassword.Format` property to `AES128`
`mssqlPassword.Format` *enum*	The encryption format of your database password: `AES128`. If you are using the silent file editor (recommended), your database password will be encrypted. Do not change this value!
`mssqlDatabaseName` *string*	Name of MSSQL database: `mssql_db4`
`mssqlUseExistingSchema` *boolean*	A flag specifying whether to use existing MSSQL DB schema or not. : `true` or `false`
`externalDBUseExistingSchema` *boolean*	A flag specifying whether to use existing external DB schema or not. Its value must be the same as the one with the `mssqlUseExistingSchema` property: either `true` or `false`
`mssqlUseSecureConnection` *boolean*	A flag specifying whether to use SSL encryption for DB connection: `true` or `false`
`mssqlCertificateDN` *string*	Distinguished name as specified in your SSL certificate
`MssqlTrustStoreFilePath` *string*	Path to DB public certificate in X.509 format
`MssqlTrustStoreFilePath.Type` *enum*	Type of SSL certificate: set this value to `File`
`externalDBUseSecureConnection` *boolean*	A flag that specifies whether to use SSL encrypted communication to your external database. Its value must be the same as the one of the `mssqlUseSecureConnection` property: either `true` or `false`
`externalDBCertificateName` *string*	Distinguished name as specified in your SSL certificate. This value must be the same as the one with the `mssqlCertificateDN`
`externalDBTrustStore` *string*	Path to DB public certificate in X.509 format

Recommendations for Clustered SecureTransport deployments

This subtopic contains instructions and tips to aid you to successful silent installations of SecureTransport (Server and Edge) in clustered deployments:

- Standard Cluster
- Large Enterprise Cluster (LEC) with external databases

Please observe the listed info before proceeding with silent installations of your cluster nodes.

Silent installation on Standard Cluster nodes

With Standard Cluster, after you perform silent installation on your first node, you can re-use the `Install_SecureTransport_<st-version>.properties` file for silent installation of all other nodes.

Standard Cluster works with an embedded MySQL database only and no additional edits are required.

Silent installation on Large Enterprise Cluster nodes

Large Enterprise Cluster (LEC) deployments offer the use of external databases which adds some additional steps in performing successful silent installation on all nodes.

To simplify this process, we can separate the SecureTransport Server deployments apart from the SecureTransport Edge deployments.

The big difference is in the fact that Server nodes are in LEC deployment (using an external database) while Edge nodes are in Standard Cluster deployment (using an embedded MySQL database).

SecureTransport Server nodes in LEC

When using external databases (Oracle or MSSQL) you must make sure the correct values are added to the respective properties, as listed in the following table:

Database	First node	Every following node

Oracle	`oracleUseExistingSchema = false`
	
	`externalDBUseExistingSchema = false`
		`oracleUseExistingSchema = true`
		`externalDBUseExistingSchema = true`
		`SecretFilePath = <path_to_taeh_file>`

Database	First node	Every following node
MSSQL	mssqlUseExistingSchema = false externalDBUseExistingSchema = false	mssqlUseExistingSchema = true externalDBUseExistingSchema = true SecretFilePath = <path_to_taeh_file>

SecureTransport Edge nodes in Standard Cluster

Follow the instructions as stated above in the *Silent installation on Standard Cluster nodes* on page 54 subsection. There are no additional steps in terms of silent installation.

Silent file editor

The Silent file editor is a tool dedicated to editing your SecureTransport `.properties` file and it is located in Tools/SilentFileEditor directory of the product distributive.

Before using the silent file editor you must export the `JAVA_HOME` variable containing path to supported version of JRE.

Usage

The following syntax is used:

```
./SilentFileEditor.sh silent_file_path key value -u key value_to_be_encrypted -c
```

Here is typical example of silent file editor usage:

```
./SilentFileEditor.sh $ST_SILENT_FILE_PATH InstallDir $ST_INSTALLDIR -u
mssqlPort $DB_PORT_NUMBER -u mssqlLoginName $DB_USER -u mssqlPassword $DB_
USER_PASSWORD -c mssqlDatabaseName $DB_NAME -u mssqlHost $DB_HOSTNAME -u
```

Where:

- `$ST_SILENT_FILE_PATH` is the path to silent file
- `$ST_INSTALLDIR` is the path where SecureTransport should be installed
- `$DB_PORT_NUMBER` is the database port number
- `$DB_USER` is the database username
- `$DB_USER_PASSWORD` is the database password in plaintext. Use `-c` to encrypt it. Use `-u` to update it.
- `$DB_NAME` is the database name
- `$DB_HOSTNAME` is the database hostname

Notes

- Silent file editor is only setting plain or encrypted values to keys.
- Silent file editor cannot add new keys.
- Silent file editor does not check if the name of the key is valid.

Related topics

See *Silent installation example file* on page 56

Silent installation example file

This subsection contains example configuration files used in SecureTransport silent installation:

- Axway Installer configuration file: `Install_Axway_Installer_V4.8.0.properties`
- SecureTransport silent installation configuration file: `Install_SecureTransport_V5.4.properties`

Install_Axway_Installer_V4.8.0.properties

The following example provides and example of the Axway Installer configuration file:

```
Component = Axway_Installer

Component.ComponentType = ComponentPack

Component.Parent =

Component.Version = 4.8.0

Component.SourceDiskNumber = 1

Component.LongName = Axway

DocumentationIndexRelativePath = Installer_4.5.x_
InstallationPrerequisitesGuide_allOS_en/index.htm

AxwaySupportURL = https://support.axway.com/

IntegrationDir = Axway_Installer_V4.8.0

IntegrationDir.Type = Directory

InstMode = Install

InstMode.Default = Install

CreationDate = 27-10-2009 11:23

CreationDate.Type = Date

CreationDate.Format = dd-MM-yyyy HH:mm

InstallMode = Standard

DVDLocation =
```

```
LevelOfExpertise = 1
LevelOfExpertise.Show = true
LevelOfExpertise.Level = 3
InstallDir = /opt/axway/
InstallationLogicalName = SecureTransport01
AllAxwayComps32 = false
AllAxwayComps64 = true
IncludeFiles =
IncludeFiles.SecureTransport = ST_PROPERTIES_FILE
```

Install_SecureTransport_V5.4.properties

The following example provides and example of the SecureTransport silent installation configuration file:

```
Component = SecureTransport
Component.LongName = Axway SecureTransport
Component.Version = 5.4
Component.Parent = Axway_Installer
Component.ComponentType = ComponentPack
Component.FileIdent = ST
Component.SupportedOS = aix-power-64;linux-x86-64;sun-sparc-64;win-x86-64
Component.SourceDiskNumber = 1
Component.InstallerVersion = 4.5.2
Component.AllowSpaceInDirectoryName = true
Component.RootUser = Indifferent
Component.LimitedCluster = NoCluster
Component.ConfigureMode = false
Component.Implementation = Java
Component.PreferredJavaVersion = 7
CreationDate = 07-08-2014 18:03
CreationDate.Type = Date
CreationDate.Format = dd-MM-yyyy HH:mm
IntegrationDir = SecureTransport_V5.4
IntegrationDir.Type = Directory
SelectedBitArchitecture = 64
```

```
InstMode = Install
SecureTransport = true
SecureTransport.Type = Module
SecureTransport.ModuleType = Installed
SecureTransport.LogicalName = SecureTransport
SecureTransport.ParentName = null
SecureTransport.Title = Axway SecureTransport V5.4
Server = true
Server.Type = Module
Server.ModuleType = Installed
Server.LogicalName = Server
Server.ParentName = SecureTransport
Server.Title = Server
Edge = false
Edge.Type = Module
Edge.ModuleType = NotInstalled
Edge.LogicalName = Edge
Edge.ParentName = SecureTransport
Edge.Title = Edge
InstallDir = /opt/axway/SecureTransport/
userName = root
isNonRootInstall = false
dbType = useMySQLLocal
mySQLPort = 33060
mySQLPort.Type = IPPortOwner
mySQLPort.Max = 65535
mySQLPort.Min = 1024
externalDBUseExistingSchema = false
sslAdminPort = 444
sslAdminPort.Type = Integer
tomcatShutdownPort = 8005
tomcatShutdownPort.Type = Integer
enableLogRotation = true
SecretFilePath =
```

Uninstall 4

The following topics describe how to uninstall SecureTransport on all platforms.

- *Uninstall SecureTransport on UNIX-based systems* on page 59 - Provides how to instructions for uninstalling SecureTransport on UNIX-based systems.
- *Uninstall SecureTransport on Windows* on page 61 - Provides how to instructions for uninstalling SecureTransport on Windows-based platforms.

Uninstall SecureTransport on UNIX-based systems

This section explains how to uninstall SecureTransport from the Axway appliance or any of the supported UNIX-based platforms.

The following error messages may occur and be placed in the `uninstall.log` during the uninstall of SecureTransport:

- `<Axway installer folder>/synInstall/scripts/utils.sh: line 743: [: -gt: unary operator expected`
- `<Axway installer folder>/synInstall/scripts/utils.sh: line 746: [: too many arguments`

They are expected and will not cause an uninstall failure.

If you are uninstalling from the Axway appliance, you can use the Appliance Console Menu to proceed. Refer to the *SecureTransport Appliance Guide*.

Note In a cluster environment, stop all of the protocol servers and services on the node you want to uninstall and remove this node from the cluster before you uninstall it. For details refer to the *SecureTransport Administrator's Guide*.

1. Log in to the system as the user who installed and runs SecureTransport.
2. Use the `<FILEDRIVEHOME>/bin/stop_all` command to stop all SecureTransport services.
3. Navigate to the Axway Installer directory of your installation and run the uninstaller script by typing the following on the command line:

```
./uninstall.sh
```

Note If you want to run the uninstallation procedure in non-interactive mode, you should run `./uninstall.sh -a`.

The Axway Installer initializes and displays a welcome message and a prompt.

```
Initialization in progress .......

----------------------------------------
Welcome
----------------------------------------
Welcome to the Axway Installer wizard for SecureTransport
Server and SecureTransport Edge.
This wizard will install SecureTransport Server or
SecureTransport Edge on your computer.
Next (type Next or N or n): to go to next Dialog
Previous (type Previous or P or p): to go to previous Dialog
Quit (type Quit or Q or q): to abort
If you want to delete a field value, use the Space bar or
the Tab key. During installation, all values or choices must
be validated by pressing Enter.
Enter (Next, Quit).
>Next
```

4. Press Enter to continue.

   The installer prepares the uninstallation execution and displays the following prompt:

```
Please wait while execution process is being prepared!

----------------------------------------
Uninstallation execution
----------------------------------------
All selected products are ready to uninstall. Type Next to start
uninstalling. If not, type Previous to make changes.
Enter (Next, Previous, Quit).
>Next
```

5. Press Enter to continue.

   The installer displays the following confirmation prompt:

```
Uninstall in progress...
Confirmation
Warning: Before proceeding, ensure that the products you want to
uninstall are stopped.
Do you want to continue?
```

```
Confirm this operation [y/n]
```

6. Type `y` and press Enter to continue.

   The installer displays progress messages as it completes the uninstallation tasks.

   When the installer has uninstalled SecureTransport and the Axway Installer, it displays:

```
Uninstallation successful

---------------------------------------
Summary
---------------------------------------
The information below summarizes the uninstallation status. Refer to
install.log for more details.

-----------------------------------------------------------------------
Product: SecureTransport_V5.4 Uninstalled from <FILEDRIVEHOME>
-----------------------------------------------------------------------
```

7. If you were running SecureTransport as a service, as described in *Run SecureTransport as a service on UNIX-based platforms after non-root installation* on page 40:
   - On AIX:
     a. Remove `/etc/rc.stransport`.
     b. Edit `/etc/rc.tcpip` and delete the `[ -f /etc/rc.stransport ] && sh /etc/rc.stransport start` line.
   - On Oracle Linux and RHEL – Remove `/etc/init.d/rc.stransport`.
   - On SLES – Remove `/etc/rc.d/rc.stransport`.
   - On Solaris:
     a. Remove `/etc/rc.d/rc.stransport`.
     b. Remove the `/etc/rc3.d/S98stransport` symbolic link.

Uninstall SecureTransport on Windows

This section explains how to uninstall SecureTransport from Windows.

Note When uninstalling SecureTransport in Microsoft Windows environments, Axway registry entries may be left behind. It is safe to manually remove the Axway registry entries left behind.

If registry entries are left behind, run `regedit.exe` to start the Microsoft Windows registry and delete the following registry entries:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Axway Software
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
    Uninstall\Axway_Installer_4.8.0 SecureTransport01
```

Note In a cluster environment, stop all of the protocol servers and services on the node you want to uninstall and remove this node from the cluster before you uninstall it. For details refer to the *SecureTransport Administrator's Guide*.

1. Prior to uninstallation, stop all SecureTransport processes and make sure that no SecureTransport files or directories are in use and that the Cygwin console and all Cygwin tools and services installed with your previous SecureTransport installation are closed. If necessary, close the Cygwin console and tools manually.
2. Select **Start > Programs > Axway Software > Uninstall**.

   The installer loads and displays the *Welcome* page.
3. Click **Next** to proceed. The installer displays the *Ready to uninstall* page.
4. Click **Uninstall** to start the uninstallation. The installer displays a confirmation dialog.
5. If you have stopped all SecureTransport and related services as described in step 1, click **Yes**. The installer displays the *Uninstall in progress* page which shows the progress of the uninstallation.
6. When uninstallation is complete, the installer displays the *Uninstall completed* page.
7. Click **Next**. The installer displays the *Summary* page.
8. Click **Finish** to close the installer.

Note You can also use the Add/Remove Programs option in the Control Panel to uninstall SecureTransport Server or Edge or navigate to the Axway Installer installation folder and start `uninstall64.exe`.