axway

SecureTransport

Version 5.4

2 April 2024

Upgrade Guide

This documentation describes the following Axway software:

Axway SecureTransport 5.4

Revision history

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

SecureTransport version	Document revision number	Topics updated
5.4	5.4.01 – initial version	
5.4	5.4.02	New chapter added: *Migrate Windows Server 2012 to a later OS version* on page 26
5.4	5.4.02 - current version	*Recover your previous SecureTransport installation* on page 24 topic updated

Contents

Preface

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

- Upgrade tasks and upgrade prerequisites
- Upgrading SecureTransport from previous versions of 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.

Who should read this guide

This guide is intended for system administrators who upgrade SecureTransport. As a person responsible for upgrading SecureTransport, 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 upgrade 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 upgrading 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

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 plug-able information for the SecureTransport Pluggable Transfer Site and how to implement a Pluggable Transfer Site. It also provides Swagger REST API integration instructions and custom Address Book source implementation instructions and custom plugins/exits source implementation instructions.
- *SecureTransport Getting Started Guide* – This guide explains the initial setup and configuration of SecureTransport using the SecureTransport Administrator setup interface.
- *SecureTransport Installation Guide* – This guide explains how to install and uninstall SecureTransport on UNIX-based platforms and Microsoft Windows.
- *SecureTransport Release Notes* – This document contains information about new features and enhancements, information received after the finalization of the rest of the documentation, and a list of known and fixed issues.
- *SecureTransport Security Guide* – This guide provides security information necessary for the secure operation of the SecureTransport product.
- *SecureTransport Software Development Kit (SDK)* – A set of software development tools and examples that allow extending SecureTransport by consuming and implementing available APIs.
- *SecureTransport Upgrade Guide* – (This document) 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

Plan the upgrade 1

If you are responsible for upgrading an existing SecureTransport installation to SecureTransport 5.4, read this section to help you plan your upgrade activities.

Should I upgrade?

Before you upgrade, determine if upgrading is appropriate for your environment and production requirements:

- Review the SecureTransport Release Notes for:
  - New features
  - Fixed issues
  - Known limitations
- Evaluate the effort required for this upgrade. You should consider:
  - Length and impact of product down time
  - Basic upgrade effort
  - Specific actions that might be required due to incompatibilities or limitations. See *Incompatibilities* on page 10.
  - Initial validation and non-regression testing
  - Upgrading your different operating environments, for example, test, and preproduction

Minimum version requirement

To upgrade directly to SecureTransport 5.4, you must have SecureTransport 5.3.6 with the latest patch installed. See *Incompatibilities* on page 10 for a complete list of supported upgrade paths.

Upgrade methods

There is currently one method for upgrading to SecureTransport 5.4 from an earlier version:

- Apply an upgrade pack – When you apply the upgrade pack, the upgrade logic auto-detects and configures settings and prepares the upgraded installation for use without any additional configuration. This includes the upgrading of clustered implementations. For upgrade instructions using an upgrade pack, refer to *Upgrade* on page 17.

See *Incompatibilities* on page 10 to learn about incompatibilities between earlier versions of SecureTransport and this version.

Product downtime considerations

This section lists considerations and provides strategies for performing upgrades with the minimal disruption of your production processes.

Considerations:

- How much time does the upgrade require?
- What scheduling constraints exist?
- How long will it take to check the upgrade results?
- How long will it take to roll back to the previous state if the upgrade fails?

Strategies to reduce downtime:

- Review the upgrade prerequisites. Refer to *Upgrade prerequisites* on page 13.
- Upgrade during a low volume time period.

Acquire a license

A new license is not required when upgrading SecureTransport .

Download the upgrade pack

After reviewing *Incompatibilities* on page 10, go to the Axway support site and download the upgrade pack for your operating system.

Incompatibilities

This section describes incompatibilities and upgrade paths between SecureTransport 5.4 and:

- Other products that you may be using with previous versions.
- Earlier versions of SecureTransport.

The supported upgrade paths are:

SecureTransport version (Appliance Platform version)	Upgrade path	
	Prerequisites	**Upgrade Steps**
ST 5.2.1 SP9 (AP 6.7.0)	none	1. Remove ST 5.2.1 SP9 2. ST 5.3.0 GA (AP 6.7.1) 3. ST 5.3.0 Patch 14 (AP 6.7.1) 4. ST 5.3.1 GA (AP 7.0.1) 5. ST 5.3.3 GA (AP 7.0.1) 6. ST 5.3.6 GA (AP 7.1.1) 7. ST 5.4 GA (AP 7.1.1)
ST 5.2.1 any SP up to SP8 (AP 6.7.0)	Upgrade to ST 5.2.1 SP 8 (AP 6.7.0)	1. ST 5.3.0 GA (AP 6.7.1) 2. ST 5.3.0 Patch 14 (AP 6.7.1) 3. ST 5.3.1 GA (AP 7.0.1) 4. ST 5.3.3 GA (AP 7.0.1) 5. ST 5.3.6 GA (AP 7.1.1) 6. ST 5.4 GA (AP 7.1.1)
ST 5.3.0 any patch level (AP 6.7.1)	Upgrade to ST 5.3.0 latest patch (AP 6.7.1)	1. ST 5.3.1 GA (AP 7.0.1) 2. ST 5.3.3 GA (AP 7.0.1) 3. ST 5.3.6 GA (AP 7.1.1) 4. ST 5.4 GA (AP 7.1.1)
ST 5.3.1 any patch level (AP 7.0.0)	Upgrade to ST 5.3.1 latest patch (AP 7.0.0)	1. ST 5.3.3 GA (AP 7.0.1) 2. ST 5.3.6 GA (AP 7.1.1) 3. ST 5.4 GA (AP 7.1.1)
ST 5.3.3 any patch level (AP 7.0.1)	Upgrade to ST 5.3.3 latest patch (AP 7.0.1)	1. ST 5.3.6 GA (AP 7.1.1) 2. ST 5.4 GA (AP 7.1.1)
ST 5.3.5 any patch level (AP 7.0.3)	Upgrade to ST 5.3.5 RA latest patch (AP 7.0.3)	1. ST 5.3.6 GA (AP 7.1.1) 2. ST 5.4 GA (AP 7.1.1)
ST 5.3.6 any patch level (AP 7.1.1)	Upgrade to ST 5.3.6 latest patch (AP 7.1.1)	1. ST 5.4 GA (AP 7.1.1)

Review the upgrade information for older SecureTransport versions in Axway Support at SecureTransport documentation. Upgrade from ST 5.2.1 SP 9 to 5.4 (and any version) is not possible, as it would result in data loss. In case of questions, contact Axway Global Support at support.axway.com.

Notes:

- For a complete list of supported software, refer to **Axway and third-party software support** in the in the *SecureTransport Administrator's Guide*.
- On upgrade to SecureTransport 5.4, ciphers are added to and removed from the existing cipher sets. For the SecureTransport 5.4 list of ciphers, refer to **SecureTransport cipher suites** in the *SecureTransport Administrator's Guide*.

Upgrade prerequisites 2

Perform the following before you upgrade:

- If SecureTransport is already registered in Central Governance, disable integration from **Admin Tool > Setup > Central Governance**. Refer to the *SecureTransport Administrator's Guide*, Central Governance configuration.
- Review the *SecureTransport Installation Guide* to ensure your system meets all the pre-installation requirements and you have all the required information.
- Back up your existing SecureTransport installation. To back up your current SecureTransport deployment, follow a backup procedure applicable for your environment and make sure the backup is created at a time when all SecureTransport services are stopped. In the rare case of an upgrade procedure failure resulting in system instability of any kind, follow the upgrade recovery procedure.

  Note Security settings must also be backed up and reapplied after upgrade. The `jdk.certpath.disabledAlgorithms` and `jdk.tls.disabledAlgorithms` parameters in the `Java/lib/security/java.security` file must be backed up and reapplied.

  Note Transaction Manager rules and the `<FILEDRIVEHOME>/brules/conf/brules.xml` settings file must also be backed and reapplied after upgrade.

  Note If scripts in `<FILEDRIVEHOME>/bin/start_*` are modified, these changes are not preserved during an upgrade. You must back up the modified files and reapply applicable changes to the respective scripts after the upgrade.

- If your SecureTransport installation uses an external database, upgrade the database prior to upgrading SecureTransport. Refer to the documentation for your database for the procedure on upgrading the external database.

  Note Prior to upgrading the external database, backup the database. Refer to the documentation for your database (Microsoft SQL Server or Oracle) for the procedure on backing up the external database.

- Make sure the port number for Tomcat JK2 is greater than 1024. (The default value is 8009.)

  Check the following locations for the port numbers:

  - In `<FILEDRIVEHOME>/tomcat/admin/conf/server.xml` find `Connector port=` and `jmvRoute`.

  If the Tomcat JK2 port number shown is less than or equal to 1024, change all occurrences to a number greater than 1024.

- To ensure your previous version of SecureTransport is not running, execute the following command to stop all services:

  ```
  <FILEDRIVEHOME>/bin/stop_all
  ```

- Check for leftover running processes and `.pid` files in the `<FILEDRIVEHOME>/var/run` folder.
- During a chained upgrade 5.2.1 > 5.3.1 > 5.3.3 > 5.3.6 > 5.4, remove the `<AxwayHome>/Installer/xercesImpl-2.6.2.jar` file before launching the SecureTransport 5.3.6 upgrade.
- Move all folders and folders in the `<FILEDRIVEHOME>/var/db/hist/*` directory to outside the `<FILEDRIVEHOME>` path. The high volume of files in the history folders could significantly slow down the upgrade process.

For Windows upgrade, also perform the following:

- Make sure the Cygwin console and all Cygwin tools installed with your previous SecureTransport installation, including the Cygwin `cron` service, are closed. Check the **Users** tab in the Windows Task Manager to make sure no one else is using Cygwin. If necessary, close the Cygwin console and tools manually.
- Make sure that no folder in `<FILEDRIVEHOME>` or `<FILEDRIVEHOME>\..\cygwin` is in use or open in Windows Explorer or in a command window and that no file in those folders is in use or open in any application. Close Windows Explorer and any other application accessing the folders in question. Make sure no SecureTransport services, including Cygwin, are running
- Make sure you have installed the Microsoft Visual C++ 2010 SP1 Redistributable Package (x64). Download the package here.
- While it is not recommended to have antivirus software running on the same deployment as SecureTransport, in case you are running as such, please make sure the antivirus software is stopped and disabled during the upgrade. Leaving the antivirus software running can cause the upgrade to fail.

For IBM AIX appliance upgrades, also perform the following:

- Log onto the IBM AIX appliance as a superuser and execute the following commands:

  ```
  no -o udp_recvspace=65000
  ```

  ```
  no -o udp_sendspace=65000
  ```

The following topic provides how-to instructions for backing up the existing installation:

- *Back up the existing installation before upgrading* on page 14 - Provides how-to instructions for backing up the existing installation before upgrading.

Back up the existing installation before upgrading

Back up your previous installation on UNIX-based platforms before upgrading.

For UNIX-based platforms including appliances:

1. Stop all the SecureTransport services.

   `<FILEDRIVEHOME>/bin/stop_all`

2. Verify the all services are stopped by checking for running processes and `.pid` files in the `<FILEDRIVEHOME>/var/run` directory. In order to assure no processes are left running even in the rare case of missing files, check the process tree with the appropriate OS tools for running processes before proceeding.
3. Back up the SecureTransport directory by tarring the files or using another backup method. Name the backup archive `SecureTransport.tar`.

   Your backup must include the following files:

   - All files in `<FILEDRIVEHOME>`
   - The following file in the `/etc` directory and its subdirectories if present: `/etc/rc.d/init.d/rc.stransport`
   - The files in the `/etc` directory that end with the installation name (You can use the `find /etc -name "*<installation name>" -print` command to find those files.) The result of this command may be empty if you are using non-root deployment, please proceed if this is the case.
   - The root `crontab` file or, for a non-root installation, the `crontab` file of the user who runs SecureTransport
4. Back up the Axway Installer directory by tarring the files or using another backup method. Name the backup archive `Axway Installer.tar`.
5. If an external database is used, the external database must be backed up according the appropriate vendor's specific instructions.

For Windows:

1. Stop all the SecureTransport services.

   `<FILEDRIVEHOME>\bin\stop_all`

   You can also open CMD as an administrator and run `stop_all`.
2. Verify the all services are stopped by checking for running processes and `.pid` files in the `<FILEDRIVEHOME>\var\run` directory. In order to assure no processes are left running even in the rare case of missing files, check the process tree with the appropriate OS tools for running processes before proceeding.

3. Back up Windows registry entries. Run `regedit.exe`.
   a. Select each of the following registry entries:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Axway Software
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
    CurrentVersion\Uninstall\
    Axway_Installer_4.8.0 SecureTransport01
HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\services\cygwin_cron
HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\services\AxwaySecureTransport*
```

   where `AxwaySecureTransport*` represents all the registry entries that start with `AxwaySecureTransport`.
   b. Right click each entry, select **Export > Export Registry File**, and save the registry entry to a safe location.
   c. When you are finished backing up the registry entries, exit `regedit`.
4. Back up files of the existing SecureTransport installation and installation information by copying the contents of the following directories, preserving the subdirectory structure, to a ZIP file or some other backup. Name the backup archive `SecureTransport.zip`.

```
C:\Axway\SecureTransport
```

5. Back up the Axway home directory. Name the backup archive `Axway Installer.zip`.
6. If an external database is used, the external database must be backed up according the appropriate vendor's specific instructions.

Upgrade 3

This topic describes the upgrade procedures for SecureTransport 5.4.

The upgrade procedure will require downtime, so make sure you plan for it.

The following topics describe the upgrade procedures:

- *Upgrade prerequisites* on page 13 - Lists the SecureTransport upgrade prerequisites.
- *Upgrade SecureTransport on a UNIX-based platform* on page 17 - Provides how-to instructions for upgrading SecureTransport on a UNIX-based platform or Axway Appliance.
- *Upgrade SecureTransport on Windows* on page 18 - Provides how-to instructions for upgrading SecureTransport on Windows.
- *Upgrade in Streaming, Standard Cluster, and Enterprise Cluster environments* on page 21 - Provides how-to instructions for upgrading in Streaming, Standard Cluster, and EC environments.
- *After you upgrade SecureTransport* on page 23 - Provides cleanup and access instructions after you upgrade SecureTransport.

Upgrade SecureTransport on a UNIX-based platform

Note If you are using an external database, the external database must be upgraded to a supported version prior to upgrading SecureTransport to version 5.4 or a new instance of the respective database should be deployed and you should migrate the existing SecureTransport data to the new instance. Refer to the documentation for your database for the upgrade or migration procedure. If additional information is needed, contact your database vendor's support.

For **ROOT** installation, run the upgrade with ROOT user. After the upgrade finishes all binaries (both SecureTransport and Axway Installer) should be owned by the ROOT user.

For **NON-ROOT** installation, run the upgrade with NON-ROOT user. Attempts to run the upgrade with root user will be successful and no error message will be returned to you. However after the upgrade the permissions on installation files will be wrong and your installation will be corrupt.

Note If you are upgrading an Axway Appliance, refer to the *SecureTransport Appliance Guide*.

Note If you are upgrading from SecureTransport 5.2.1, use the following steps to upgrade the platform:
- Upgrade the platform to 7.0.1.
- Create file /usr/platform/etc/appliance_id containing appliance model (use 4810 or another corresponding appliance model for a hardware appliance or VMWARE for a virtual appliance).
- Continue with the upgrade.

1. Log on with the user that owns SecureTransport services.
2. Download and copy the SecureTransport installer into a temporary directory.

   ```
   SecureTransport_5.4_UP1-from-5.3.6_<OS>-<processor>_<BuildNumber>.jar
   ```

   Where the variables represent the following:

   - `<OS>` is the operating system: `aix` (for IBM AIX) or `linux` (for RHEL and SUSE).
   - `<processor>` is the type of processor running the operating system: `power`, `sparc`, or `x86-64`.
   - `<BuildNumber>` is the actual build number listed in the installer executable file, for example, `Build1234`.

     Note Do not place the binaries in the same folder where Axway Installer is installed.

3. Navigate to the Axway Installer directory in your existing SecureTransport installation and run the following command to apply the update pack:

   ```
   ./update.sh -i <path to the update pack named
   SecureTransport_5.4_UP1-from-5.3.6_<OS>-<processor>_
   <BuildNumber>.jar>
   ```

   Note Do not run more than one instance of the SecureTransport installer on a system at one time. The upgrade fails when more than one instance is running.

   Note After this step, the SecureTransport instance will be upgraded to 5.4.

When the installation is complete, a success message appears.

Note When the installer completes the installation, it will start all services except for TM. TM will need to be manually restarted. Also, all custom TM rules are disabled and need to be manually enabled.

The log file will be the `<AxwayHome>/install.log` of the Axway Installer.

Upgrade SecureTransport on Windows

Note If you are using an external database, the external database must be upgraded to a supported version prior to upgrading SecureTransport to version 5.4 or a new instance of the respective database should be deployed and you should migrate the existing SecureTransport data to the new instance. Refer to the documentation for your database for the upgrade or migration procedure. If additional information is needed, contact your database vendor's support.

The following topics provide instructions for upgrading an existing SecureTransport installation:

Upgrade from SecureTransport 5.3.6 or above using the console

On Microsoft Windows using the console mode:

1. Execute the following command to stop all services:

   `stop_all`

2. Verify that the Cygwin console and all Cygwin tools, including the Cygwin `cron` service, are closed.
3. Download the file `SecureTransport_5.4_UP1-from-5.3.6_win-x86-64_<BuildNumber>.jar`.

   Where the variable represent the following:

   - `<BuildNumber>` is the actual build number listed in the installer executable file, for example, BN1234.
4. Navigate to the Axway Installer directory from your existing SecureTransport installation and run the following command to apply the update pack:

   ```
   update64.exe -i <path to the first update pack named SecureTransport_
   5.4_UP1-from-5.3.6_win-x86-64_<BuildNumber>.jar
   ```

   Note After Step 3 completes, the SecureTransport instance will be upgraded to 5.4.

When the installation is complete, a success message appears.

Note When the installer completes the installation, it will start all services except for TM. TM will need to be manually restarted. Also, all custom TM rules are disabled and need to be manually enabled.

The log file will be the `<AxwayHome>/install.log` of the Axway Installer.

Upgrade from SecureTransport 5.3.6 or above using the GUI

For Microsoft Windows using GUI mode:

1. Execute the following command to stop all services:

   `stop_all`

2. Verify that the Cygwin console and all Cygwin tools, including the Cygwin `cron` service, are closed.
3. Download the file `SecureTransport_5.4_UP1-from-5.3.6_win-x86-64_<BuildNumber>.jar`.

   Where the variable represent the following:

   - `<BuildNumber>` is the actual build number listed in the installer executable file, for example, BN1234.
4. Select **Start > All Programs > Axway Software > Axway *<installation_name>* > Update**.

   The Axway Installer starts in update mode and displays the *Welcome* page.
5. Click **Next**.

   The installer displays the *Updates management* page.
6. Click **Select file**.

   The installer displays the *Select update file* window.
7. Browse to and select the `SecureTransport_5.4_UP1-from-5.3.6_win-x86-64_<BuildNumber>.jar` file and click **Open**.
8. Click **Next**.

   The installer displays the *Ready to update* page.
9. Click **Update** to begin the update process.

   The installer displays a confirmation window.
10. If you have stopped all SecureTransport processes, click **Yes**.

    The installer displays the *Update in Progress* page.

    When the update is complete, the installer displays the *Update completed* page.
11. Click **Next**.

    The installer displays the *Summary* page.
12. Click **Finish** to exit the installer.

    Note After Step 11 completes, SecureTransport will be updated to version 5.4.

When the installation is complete, a success message appears.

Note When the installer completes the installation, it will start all services except for TM. TM will need to be manually restarted. Also, all custom TM rules are disabled and need to be manually enabled.

The log file will be the `<AxwayHome>/install.log` of the Axway Installer.

Upgrade in Streaming, Standard Cluster, and Enterprise Cluster environments

This section describes the options for upgrading in Streaming, Standard Cluster, and Enterprise Cluster (EC) environments.

Note If you are using an external database, the external database must be upgraded to a supported version prior to upgrading SecureTransport to version 5.4 or a new instance of the respective database should be deployed and you should migrate the existing SecureTransport data to the new instance. Refer to the documentation for your database for the upgrade or migration procedure. If additional information is needed, contact your database vendor's support.

Streaming

In a streaming environment, stop all of the protocol servers and services on all of the SecureTransport Edges before you start upgrading. Update the SecureTransport Server (backend) first and then update the SecureTransport Edges. Once the upgrades are completed, restart all servers and edges.

Note Verify that an edge and server on different versions are never started together.

Standard Cluster

In a Standard Cluster environment, stop all of the protocol servers and services on all of the nodes before you start updating.

For Standard Clusters the following two options for upgrade are supported:

- Option 1 (recommended)
    - Stop the nodes and upgrade the nodes one at a time. After a node is upgraded, stop all SecureTransport services on the node and proceed with the upgrade of the next node in the cluster. Start all SecureTransport services only after the upgrade is applied on all the nodes in the cluster.
    - After all node upgrades are finished, do a manual sync. Only after you have completed a manual sync will you have functional and operating cluster.
- Option 2:
    - Dis-join the cluster before the upgrade by changing the cluster mode and deleting the node entries in the servers file. For details, refer to the *Remove a server from an active/active cluster* section in the *SecureTransport Administrator's Guide*.
    - Then upgrade all the nodes as standalone installations.
    - Once the upgrades are completed, join the cluster back together and do a manual sync. The cluster is considered upgraded and running only after the successful manual sync. For details, refer to the *Remove a server from an active/active cluster* section in the *SecureTransport Administrator's Guide*.

Enterprise Cluster

The upgrade of an Enterprise Cluster (EC) consists of upgrading the nodes.

The following Enterprise Cluster upgrade option is supported:

- Stop the nodes and upgrade the nodes one at a time. After a node is upgraded, stop all SecureTransport services on the node and proceed with the upgrade of the next node in the cluster. Start all SecureTransport services only after the upgrade is applied on all the nodes in the cluster.

After you upgrade SecureTransport 4

For non-root installations, verify that all crontab entries are for the user running the SecureTransport installation (this is the user as set in the `STuser.txt` file in your `FILEDRIVEHOME` directory).

Additionally, you need to establish the Transaction Manager protocol and proxy server communication by starting the protocol servers and services on the SecureTransport Edges. For additional information, refer to the *SecureTransport Administrator's Guide*.

Notes:

- After upgrade to SecureTransport5.4, when a proxy is configured, direct connections from the SecureTransport Backend are not permitted even when the proxy is unreachable. To change the default behavior, set the `Direct.Connection.When.Proxy.Down` server configuration parameter to **true**. For information on changing server configuration parameters, refer to **View and change server configuration parameters** in the *SecureTransport 5.4 Administrator's Guide*.
- In SecureTransport 5.3.3 there is a structural change of database tables related to File Tracking. The data related to file transfers made before upgrade, should be migrated to the new tables created after upgrade to SecureTransport 5.3.3 for them to be visible in File Tracking for SecureTransport 5.3.3 and above. If the migration is skipped, all the details related to the file transfers made before the upgrade will NOT be visible on the Administration Tool *File Tracking* page. For more information, refer to **Migration of File Tracking entries after upgrade** in the *SecureTransport 5.4 Installation Guide*.
- After upgrading from SecureTransport 5.3.6 Patch 37 and later to SecureTransport 5.4, you must manually remove the duplicate JDBC driver, as follows:

    1. Go to `FDH/bin/` and use the `stop_all` command to stop all services.
    2. Go to `FDH/lib/jars/external/` and remove the file `ojdbc8.jar`.

        Note This process is applicable to both SecureTransport Server and SecureTransport Edge so you must repeat these steps for each node in your Server and Edge clusters.

Recover your previous SecureTransport installation 5

Note After a successful upgrade to SecureTransport 5.4, there is no revert / downgrade path: the only way to roll back to a previous SecureTransport version deployment is to restore it from backup.

If the upgrade fails, you can recover your backed-up SecureTransport 5.3.6 installation. Make sure you uninstall SecureTransport 5.4 before you attempt to recover.

1. For a SecureTransport Server using an external Oracle database, restore the database using standard Oracle procedures. For a SecureTransport Server using an external Microsoft SQL Server database, restore the database using standard Microsoft procedures.
2. Expand the `SecureTransport.zip` file created during the backup procedure and extract the files into the original installation folder of your previous SecureTransport installation.
3. Expand the `Axway Installer.zip` file created during the backup procedure and extract the files into the original installer folder of your previous installation.
4. Run `regedit.exe` to start the 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
   ```

5. Restore the registry entries that you backed up. To import a registry entry into the Windows registry, double-click the name of the respective `.reg` files you saved when you backed up your installation.
6. Make sure the file `cygwin1.dll` is included in your PATH environment variable. For example:

   ```
   C:\Axway\SecureTransport\cygwin\bin
   ```

7. Make sure the folder `STServer\bin` is included in your PATH environment variable. For example:

   ```
   C:\Axway\SecureTransport\STServer\bin
   ```

8. Install the SecureTransport services:
   - To install the services on a SecureTransport Server installation, navigate to the folder `STServer\bin`, located in the SecureTransport installation folder, and double-click the following files:

```
install_ftpd_service.com
install_httpd_service.com
install_sshd_service.com
install_tm_service.com
install_admin_service.com
install_as2d_service.com
install_pesitd_service.com
```

- To install SecureTransport services on a SecureTransport Edge installation, navigate to the folder `STServer\bin`, located in the SecureTransport installation folder, and double-click the following files:

```
install_ftpd_service.com
install_httpd_service.com
install_sshd_service.com
install_admin_service.com
install_as2d_service.com
```

9. Install Cygwin `cron`:
   a. Navigate to the `cygwin\bin` folder in the SecureTransport installation folder and double-click the `cygwin.bat` file to start the Cygwin shell.
   b. In the Cygwin shell, execute the following command:

```
cygrunsrv -I cygwin_cron -d \"Cygwin cron\" -p /usr/sbin/cron \
    -a -D -f \"Cygwin Cron\"
```

10. Reboot your system and start all SecureTransport services. For more information, refer to the *SecureTransport Administrator's Guide*.

Migrate Windows Server 2012 to a later OS version 6

This chapter provides detailed step-by step procedures on migrating SecureTransport 5.4 installed on Microsoft Windows Server 2012 to a later Windows Server version: either 2016 or 2019. The following topics cover different SecureTransport 5.4 deployments.

Note The topics described will refer to your existing SecureTransport 5.4 on Windows Server 2012 deployment as the *original* deployment. Your future SecureTransport 5.4 (on either Windows Server 2016 or Windows Server 2019) deployment is referred to as the *new* deployment.

Instructions in these topics pertain to SecureTransport 5.4 only. If you are using a previous version of SecureTransport, follow the upgrade procedures as provided in this guide.

In the listed topics, to avoid confusion, the following terminology is introduced:

- The current SecureTransport deployment on Windows Server 2012 is also referred to as the *original* deployment.
- Similarly, your future deployment (Windows Server 2016 or Windows Server 2019) is also referred to as the *new* deployment.

Standalone installation with MySQL

This topic provides steps to a successful migration of a standalone SecureTransport5.4 on Windows Server 2012 to Windows Server 2016 or Windows Server 2019.

The migration procedure requires you to form a Standard cluster and take advantage of its capability of synchronizing global configurations and accounts across nodes.

Note The migration procedure to Windows Server 2016 is the same as that to Windows Server 2019. To avoid repetition, instructions herein will discuss migration steps to Windows Server 2016. You can follow these same steps when migrating to Windows Server 2019.

Prerequisites

- Back up your existing SecureTransport installation. To back up your current SecureTransport deployment, follow a backup procedure applicable for your environment and make sure the backup is created at a time when all SecureTransport services are stopped.

Note Please keep in mind that migrating SecureTransport with embedded database to Windows Server 2016 will not migrate the Transfer, Server and Audit log information. This information can be backed up prior to the migration.

Migration procedure

Follow the steps below to replace the original SecureTransport Server (standalone installation) deployed on Windows Server 2012, with one on Windows Server 2016.

1. Install a new node of SecureTransport5.4 (vanilla installation, no patches) on Windows Server 2016 using the `taeh` file from the one on Windows Server 2012.
    - Make sure that the host names and IP addresses of all servers are in the host files of all servers. Use the lookup command to verify that the host names of all servers resolve on all hosts.
    - Select the computer that is to serve as the primary server. This must be the Windows Server 2012 node from which the configuration is to be replicated.
2. Make sure that the patch level of the new SecureTransport deployment (on Windows Server 2016) matches that of the original one (on Windows Server 2012). For example, if the original deployment has Patch 22 installed, you must perform the necessary steps to upgrade the new vanilla SecureTransport installation to Patch 22 as well.
3. Manually re-apply and reconfigure all previously applied customizations, for example:
    - plugins from the …`\STServer\plugins\` folder
    - start/stop scripts
    - configurations in `configuration.xml`
    - configurations in `mysql.conf`
    - JVM heap size
    - multi-protocol listeners
    - all local server configurations (i.e. network zones) and all Local Server configuration parameters: in the SecureTransport Administration Tool, go to **Operation > Server Configuration** and select the **Local Parameters** checkbox on the new Windows Server 2016 SecureTransport deployment.

Note Please make sure no configuration files (i.e. `configuration.xml`) are copied across the nodes. All Server Configuration parameters will sync automatically when the cluster is formed.

4. Make sure you have a feature license that permits the necessary number of nodes for the migration procedure. In case your license does not allow you to add new machines to the existing environment, contact Axway Global Support and request a temporary license. Do not forget to restart all services after the new license is applied.
5. Follow the below steps of forming a Standard Cluster between the SecureTransport on Windows Server 2012 and the one on Windows Server 2016.

Prerequisites for Synchronization

- The SecureTransport administrator account names and passwords on the new SecureTransport deployment must be the same as those on the original SecureTransport deployment.
- When certificate authentication is enabled for the administrator accounts, `Cluster.DynamicSync.adminName` and `Cluster.DynamicSync.keyAlias` configuration options must be set on all nodes manually.
- The SecureTransport installation path of the new SecureTransport deployment must be the same as that on the original one.
- The `taeh` file on the new SecureTransport deployment must be the same as that on the original one.
- The certificate for encrypting cluster communications specified in the `Cluster.Crypto.Alias` server configuration parameter on the new SecureTransport deployment must be the same as that on the original one.
- The internal CAs on all nodes must be trusted by all other nodes. You can import the same internal CA on all nodes using a SecureTransport generated certificate or an external one.
- All the SecureTransport server certificates must be issued by a common CA.
- Each server must be hosted on a different computer or virtual machine.
- All the servers in an active/active cluster must be in the same LAN.
- All servers in a cluster must have their clocks set to the same time.
- The TM Server must be running on all servers.
- All database settings on the new SecureTransport deployment must be identical to that on the original one.

Cluster formation steps

a. Make sure that Transaction Manager (TM) servers are stopped on all SecureTransport servers.

b. On the primary and the secondary server, list both servers in the `<FILEDRIVEHOME>\lib\admin\config\servers` configuration file. List the primary server first and continue with the secondary server.

Note The `<FILEDRIVEHOME>\lib\admin\config\servers` file must be the same on all machines in your cluster. You can create it on one SecureTransport server and copy it to the other.

c. On the primary server, generate a local certificate for encrypting cluster communications.

d. On the primary server, export the certificate in `.p12` format protected with a password.

e. Import the certificate on the secondary server.

f. On the primary and the secondary server, configure encryption for cluster communications. On the *Server Configuration* page of each node, change the value of the `Cluster.Crypto.Alias` server configuration parameter to the alias of the certificate.

g. On the primary server and the secondary server, activate the cluster. On the *Server Configuration* page of each node, change the value of the `Cluster.mode` parameter to **active**.

h. Start the TM server on the primary server and wait until it promotes itself as a primary server.

i. Check for a `'becomePrimary is called.'` message in the Server Log of the primary node.

j. Start the TM server on the other server in the cluster and wait for it to go online.

k. Check for a `'The machine <machine>/<IP> goes online.'` message in Server Log of the secondary node.

6. Synchronize the secondary server manually using the SecureTransport Administration Tool of the primary server.

Note Wait for the synchronization to complete successfully. The duration of the sync will depend on the amount of the data that will be synced.

7. Manually verify that the data is successfully synced to the new node (parameters, accounts, certificates should be present on the new node).

8. On both nodes set the `Cluster.mode` parameter to **disabled** and comment the entries in the `servers` file located in `<FILEDRIVEHOME>\lib\admin\config\`.

9. Power off the original node on Windows Server 2012.

10. Change the IP address of the new SecureTransport on Windows Server 2016 deployment to the IP address previously occupied by the original deployment on Windows Server 2012.

11. Re-add your existing (original) license if a temporary one was used and restart all services on the new SecureTransport installation on Windows Server 2016.

Related Topis:

- *Standalone with External Database* on page 30
- *Standard Cluster environment with MySQL* on page 32
- *Enterprise Cluster environment with external database* on page 36
- *Edge installation with MySQL* on page 38
- *Edge installation with MySQL when part of a synchronized cluster* on page 41

Standalone with External Database

This topic provides instructions for migrating a standalone SecureTransport 5.4 deployment on Windows Server 2012 to Windows Server 2016 or Windows Server 2019.

The migration procedure requires you to use the external database of your existing (original) deployment (on Windows Server 2012) to acquire all original global configurations and account information.

Note The migration procedure to Windows Server 2016 is the same as that to Windows Server 2019. To avoid repetition, instructions herein will discuss migration steps to Windows Server 2016. You can follow these same steps when migrating to Windows Server 2019.

Prerequisites

- Back up your existing SecureTransport installation. To back up your current SecureTransport deployment, follow a backup procedure applicable for your environment and make sure the backup is created at a time when all SecureTransport services are stopped. It is recommended that you perform a full database backup.
- All Windows Server 2016 machines must be added to the same Domain.
- The time set on the Windows Server 2016 machine must be the same as the time on Windows Server 2012 machine where your current SecureTransport is installed. The time settings (clocks) on all machines in the network must be synchronized.
- The new Windows Server 2016 machine must have access to the network storage that the Windows Server 2012 machine is using.

Migration procedure

Follow the steps below to replace a SecureTransport installation on Windows Server 2012 (standalone installation, with external database) with one on Windows Server 2016.

1. Install SecureTransport Server 5.4 (vanilla installation, no patches) on Windows Server 2016 using the `taeh` file from the one on Windows Server 2012 and use the existing database schema.

2. The SecureTransport installation path must be the same on all servers.
3. Make sure that the patch level of the new SecureTransport deployment (on Windows Server 2016) matches that of the original one (on Windows Server 2012). For example, if the original deployment has Patch 22 installed, you must perform the necessary steps to upgrade the new vanilla SecureTransport installation to Patch 22 as well.
4. Manually re-apply and reconfigure all previously applied customizations, for example:
    - plugins from the …`\STServer\plugins\` folder
    - start/stop scripts
    - configurations in `configuration.xml`
    - JVM heap size
    - multi-protocol listeners
    - all local server configurations (i.e. network zones) and all Local Server configuration parameters: in the SecureTransport Administration Tool, go to **Operation > Server Configuration** and select the **Local Parameters** checkbox on the new Windows Server 2016 node.

Note Please make sure no configuration files (i.e. `configuration.xml`) are copied between the two machines.

5. Make sure you have a feature license that permits the necessary number of nodes for the migration procedure. In case your license does not allow you to use more machines, contact Axway Global Support and request a temporary license. Do not forget to restart all services after a new license is applied.
6. Start the SecureTransport Administration Tool server on Windows Server 2016 machine
7. Log in to the SecureTransport Administration Tool (on Windows Server 2016) as the admin user and install the license.

Note In case the current SecureTransport environment uses separate Oracle databases, they have to be added manually in *Database Settings* page.

8. Restart all SecureTransport services on Windows Server 2016 machine.
9. Make sure that all global server configuration options are present on the new installation on Windows Server 2016.
10. Manually add all local server configuration options from the original SecureTransport (on Windows Server 2012) to the new SecureTransport installed on Windows Server 2016.
11. Stop the original Windows Server 2012 machine.
12. Stop all services on SecureTransport on Windows Server 2016.
13. Change the IP address of Windows Server 2016 to the one of the powered off Windows Server 2012.
14. Start all services on SecureTransport on Windows Server 2016.
15. Wait until the new SecureTransport deployment goes online.
16. Re-add your existing (original) license if a temporary one was used and restart all services on your new SecureTransport deployment (on Windows Server 2016).

Related Topics:

- *Standalone installation with MySQL* on page 26
- *Standard Cluster environment with MySQL* on page 32
- *Enterprise Cluster environment with external database* on page 36
- *Edge installation with MySQL* on page 38
- *Edge installation with MySQL when part of a synchronized cluster* on page 41

Standard Cluster environment with MySQL

This topic provides instructions for migrating SecureTransport 5.4 Server (part of a Standard cluster deployment) on Windows Server 2012 to Windows Server 2016 or Windows Server 2019.

The migration procedure requires you to add your new SecureTransport Server deployment (on Windows Server 2016 or Windows Server 2019) as a secondary server to the Standard cluster (replacing the old one) and take advantage of its capability to sync global configurations and accounts across nodes.

Note The migration procedure to Windows Server 2016 is the same as that to Windows Server 2019. To avoid repetition, instructions herein will discuss migration steps to Windows Server 2016. You can follow these same steps when migrating to Windows Server 2019.

Prerequisites

- Back up your existing SecureTransport installation. To back up your current SecureTransport deployment, follow a backup procedure applicable for your environment and make sure the backup is created at a time when all SecureTransport services are stopped.

Note Please keep in mind that migrating SecureTransport with embedded database to Windows Server 2016 will not migrate the Transfer, Server and Audit log information. This information can be backed up prior to the migration.

Migration procedure

Follow the steps below to replace the original SecureTransport Server (as part of a Standard cluster) deployed on Windows Server 2012, with one on Windows Server 2016.

1. Install 2 new SecureTransport 5.4 (vanilla installation, no patches) instances on Windows Server 2016 using the `taeh` file from the original one on Windows Server 2012.
    - Make sure that the host names and IP addresses of all servers are in the host files of all servers. Use the lookup command to verify that the host names of all servers resolve on all hosts.

- Select the machine that is to serve as the primary server. This must be the Windows Server 2012 node from which the configuration is to be replicated.

2. Make sure that the patch level of the new SecureTransport deployment (on Windows Server 2016) matches that of the original one (on Windows Server 2012). For example, if the original deployment has Patch 22 installed, you must perform the necessary steps to upgrade the new vanilla SecureTransport installation to Patch 22 as well.
3. Manually re-apply and reconfigure all previously applied customizations, for example:
   - plugins from the …`\STServer\plugins\` folder
   - start/stop scripts
   - configurations in `configuration.xml`
   - configurations in `mysql.conf`
   - JVM heap size
   - Multi-protocol listeners
   - all local server configurations (i.e. network zones) and all Local Server configuration parameters: in the SecureTransport Administration Tool, go to **Operation > Server Configuration** and select the **Local Parameters** checkbox on the new Windows Server 2016 node.

Note Please make sure no configuration files (i.e. `configuration.xml`) are copied across the nodes. All Server Configuration parameters will sync automatically when the cluster is formed.

4. Make sure you have a feature license that permits the necessary number of nodes for the migration procedure. In case your license does not allow you to add new machines to the existing environment, contact Axway Global Support to request a temporary license. Do not forget to restart all services after the new license is applied.
5. On the existing Standard Cluster nodes (Windows Server 2012) – stop the TM servers.
6. On the Primary node – edit the `<FILEDRIVEHOME>\STServer\lib\admin\config\servers` file – remove the Secondary server and add one of the new SecureTransport on Windows Server 2016. On the original secondary server (Windows Server 2012), set the `Cluster.mode` parameter to **disabled**, then comment the entries in the `servers` file located in `<FILEDRIVEHOME>\lib\admin\config\` and restart all services. This will run as standalone and will take the load during the migration procedure.
7. Follow the below steps of forming a Standard Cluster between the original SecureTransport (on Windows Server 2012) and the one on Windows Server 2016:

Prerequisites for Synchronization

- The SecureTransport administrator account names and passwords must be the same across all servers.
- When certificate authentication is enabled for the administrator accounts, the `Cluster.DynamicSync.adminName` and `Cluster.DynamicSync.keyAlias` configuration options must be manually set on all SecureTransport Server nodes.
- The SecureTransport installation path must be the same on all servers.
- The `taeh` file must be the same on all servers.
- The certificate for encrypting cluster communications specified in the `Cluster.Crypto.Alias` server configuration parameter must be the same on all servers.
- The internal CAs on all nodes must be trusted by all other nodes. You can import the same internal CA on all nodes using a SecureTransport generated certificate or an external one.
- All the SecureTransport server certificates must be issued by a common CA.
- Each server must be hosted on a different computer or virtual machine.
- All the servers in an active/active cluster must be in the same LAN.
- All servers in a cluster must have their clocks set to the same time.
- The TM Server must be running on all servers.
- All database settings must be identical on all the servers.

Cluster formation steps

a. Make sure that Transaction Manager (TM) servers are stopped on all machines.

b. On the primary and the secondary server, list both servers in the `<FILEDRIVEHOME>\lib\admin\config\servers` configuration file. List the primary server first and continue with the secondary servers in the order you want them promoted to primary server in the event of failover.

Note The `<FILEDRIVEHOME>\lib\admin\config\servers` file must be the same on all machines in your cluster. You can create it on one server and copy it to the others.

c. On the primary server, generate a local certificate for encrypting cluster communications.

d. On the primary server, export the certificate in `.p12` format protected with a password.

e. Import the certificate on each secondary server.

f. On the primary and the secondary server, configure encryption for cluster communications. On the Server Configuration page, change the value of the `Cluster.Crypto.Alias` server configuration parameter to the alias of the certificate.

g. On the primary server and all secondary servers, activate the cluster. On the *Server Configuration* page, change the value of the `Cluster.mode` parameter to **active**.

h. Start the TM server on the primary server and wait until it promotes itself as a primary server.

i. Check for a `'becomePrimary is called.'` message in the Server Log of the primary node.

j. Start the TM server on the other server in the cluster and wait for it to go online.

k. Check for a `'The machine <machine>/<IP> goes online.'` message in Server Log of the secondary node.

8. Synchronize the secondary server manually from the Administration Tool of the primary server.

Note Wait for the synchronization to complete successfully. The duration of the sync will depend on the amount of the data that will be synced.

9. Manually verify that the data is successfully synced to the new node (parameters, accounts, certificates should be present on the new node).
10. On both nodes set the `Cluster.mode` parameter to **disabled** and comment the entries in the `servers` file located in `<FILEDRIVEHOME>\lib\admin\config\`.
11. Edit the `servers` file located in `<FILEDRIVEHOME>\lib\admin\config\` on Windows Server 2016 machine - set its IP address on first position and the IP of the other SecureTransport Windows Server 2016 - on the second position.
12. Repeat the previous point on the other SecureTransport Windows Server 2016 machine.
13. Start all services on both SecureTransport instances.
14. Follow the *Prerequisites for Synchronization* and the *Cluster formation steps* as described above in order to form Standard Cluster with both SecureTransport instances on Windows Server 2016.
15. At this point you have a fully functioning Standard cluster on Windows Server 2016.
16. Power off the nodes on Windows Server 2012.
17. Change the IP addresses of the nodes on Windows Server 2016 to the corresponding ones, previously occupied by the nodes on Windows Server 2012.
18. Re-add your existing (original) license if a temporary one was used and restart all services on the node on Windows Server 2016.

Related Topics:

- *Standalone installation with MySQL* on page 26
- *Standalone with External Database* on page 30
- *Enterprise Cluster environment with external database* on page 36
- *Edge installation with MySQL* on page 38
- *Edge installation with MySQL when part of a synchronized cluster* on page 41

Enterprise Cluster environment with external database

This topic provides instructions for migrating SecureTransport5.4 Server on Windows Server 2012 deployment (as part of an Enterprise cluster with Oracle or MSSQL database) to Windows Server 2016 or Windows Server 2019.

The migration procedure requires you to add your new SecureTransport Server deployment (on Windows Server 2016 or Windows Server 2019) to the Enterprise cluster and take advantage of its capability to sync global configurations and accounts across nodes.

Note The migration procedure to Windows Server 2016 is the same as that to Windows Server 2019. To avoid repetition, instructions herein will discuss migration steps to Windows Server 2016. You can follow these same steps when migrating to Windows Server 2019.

Prerequisites

- Back up your existing SecureTransport installation. To back up your current SecureTransport deployment, follow a backup procedure applicable for your environment and make sure the backup is created at a time when all SecureTransport services are stopped. It is recommended that you perform a full database backup.
- All Windows Server 2016 machines must be added to the same Domain.
- The time of the Windows Server 2016 machine must be the same as the time on Windows Server 2012 machine where your current SecureTransport is installed. The time settings (clocks) on all machines in the network must be synchronized.
- All new Windows Server 2016 machines must have access to the network storage that the Windows Server 2012 machines are using.

Migration procedure

Follow the steps below for adding a new node on Windows Server 2016 to the existing SecureTransport Cluster on Windows Server 2012.

1. Install SecureTransport Server 5.4 (vanilla installation, no patches) on Windows Server 2016 using the `taeh` file from the one on Windows Server 2012 and use the existing database schema
2. The SecureTransport installation path must be the same on all servers
3. Make sure that the patch level of the new SecureTransport deployment (on Windows Server 2016) matches that of the original one (on Windows Server 2012). For example, if the original deployment has Patch 22 installed, you must perform the necessary steps to upgrade the new vanilla SecureTransport installation to Patch 22 as well.
4. Manually re-apply and reconfigure all previously applied customizations, for example:

- plugins from the …\STServer\plugins\ folder
- start/stop scripts
- configurations in configuration.xml
- JVM heap size
- multi-protocol listeners
- all local server configurations (i.e. network zones) and all Local Server configuration parameters: in the SecureTransport Administration Tool, go to **Operation > Server Configuration** and select the **Local Parameters** checkbox on the new Windows Server 2016 node.

Note Please make sure no configuration files (i.e. configuration.xml) are copied across the nodes.

5. Make sure you have a feature license that permits the necessary number of nodes for the migration procedure. In case your license does not allow you to add new machines to the existing EC, contact Axway Global Support and request a temporary license. Do not forget to restart all services after the new license is applied.
6. Log in to the SecureTransport Administration Tool on the running SecureTransport server on Windows Server 2012 as the admin user. Go to the *Cluster management* page and add the Windows Server 2016 machine to the cluster by entering its IP address.
7. Start the Administration Tool server on Windows Server 2016 machine.
8. Log in to the SecureTransport Administration Tool (on Windows Server 2016) as the admin user and install the license.
9. In case the current SecureTransport environment uses separate Oracle databases, they have to be added manually in the *Database Settings* page.
10. Restart all SecureTransport services on the Windows Server 2016 machine.
11. Make sure all nodes in the Enterprise cluster are online and synchronized.
12. Make sure that all global server configuration options are present in the newly added node after the synchronization.
13. Manually add all local server configuration options (i.e. network zones) and all Local Server configuration parameters in the SecureTransport Administration Tool: go to **Operation > Server Configuration** and select the **Local Parameters** checkbox on the new Windows Server 2016 node.
14. Stop the original Windows Server 2012 machine.
15. Log in to the SecureTransport Administration Tool of the second SecureTransport node (on Windows Server 2012), go to *Cluster Management* page and remove the IP address of the machine that was powered off from the Servers table.
16. Stop all services on SecureTransport on Windows Server 2016.
17. Change the IP address of Windows Server 2016 to the one of the powered off Windows Server 2012.
18. Add the IP address from step 17 again to the cluster.
19. Start all services on SecureTransport on Windows Server 2016.

20. Wait until the node goes online.
21. Log in the SecureTransport Administration Tool and go to the *Cluster management* page
22. Remove the original IP address of the Windows Server 2016 machine from the cluster.
23. Re-add your existing (original) license in case a temporary one was used and restart all services on the new node (on Windows Server 2016).

Repeat the same steps for all other SecureTransport Server nodes from the Enterprise cluster.

Related Topics:

- *Standalone installation with MySQL* on page 26
- *Standalone with External Database* on page 30
- *Standard Cluster environment with MySQL* on page 32
- *Edge installation with MySQL* on page 38
- *Edge installation with MySQL when part of a synchronized cluster* on page 41

Edge installation with MySQL

This topic provides instructions for migrating SecureTransport5.4 Edge with MySQL database on Windows Server 2012 deployment to Windows Server 2016 or Windows Server 2019.

The migration procedure requires you to form a synchronized cluster of Edges with your new SecureTransport Edge deployment (on Windows Server 2016 or Windows Server 2019) and the original one (on Windows Server 2019) and take advantage of the cluster capability to sync global configurations and accounts across nodes.

Note The migration procedure to Windows Server 2016 is the same as that to Windows Server 2019. To avoid repetition, instructions herein will discuss migration steps to Windows Server 2016. You can follow these same steps when migrating to Windows Server 2019.

Prerequisites

- Back up your existing SecureTransport installation. To back up your current SecureTransport deployment, follow a backup procedure applicable for your environment and make sure the backup is created at a time when all SecureTransport services are stopped.

Note Please keep in mind that migrating SecureTransport Edge to Windows Server 2016 will not migrate the Server and Audit log information. This information can be backed up prior to the migration.

Migration procedure

Perform the below procedure for each of the SecureTransport Edges when not in a synchronized cluster.

1. Install a new SecureTransport5.4 Edge (vanilla installation, no patches) on Windows Server 2016 using the `taeh` file from the one on Windows Server 2012.
    - Make sure that the host names and IP addresses of all servers are in the host files of all servers. Use the lookup command to verify that the host names of all servers resolve on all hosts.
    - Select the computer that is to serve as the primary server. This must be the Windows Server 2012 node from which the configuration is to be replicated.
2. Make sure that the patch level of the new SecureTransport deployment (on Windows Server 2016) matches that of the original one (on Windows Server 2012). For example, if the original deployment has Patch 22 installed, you must perform the necessary steps to upgrade the new vanilla SecureTransport installation to Patch 22 as well.
3. Manually re-apply and reconfigure all previously applied customizations, for example:
    - plugins from the …`\STServer\plugins\` folder
    - start/stop scripts
    - configurations in `configuration.xml`
    - configurations in `mysql.conf`
    - JVM heap size
    - multi-protocol listeners
    - all local server configurations (i.e. network zones, allowed SecureTransport Servers) and all Local Server configuration parameters in the SecureTransport Administration Tool: go to **Operation > Server Configuration** and select the **Local Parameters** checkbox on the new Windows Server 2016 node.

Note Please make sure no configuration files (i.e. `configuration.xml`) are copied across the nodes. All Server Configuration parameters will sync automatically when the cluster is formed.

4. Make sure you have a feature license that permits the necessary number of nodes for the migration procedure. In case your license does not allow you to add new machines to the existing environment, contact Axway Global Support and request a temporary license. Do not forget to restart all services after the new license is applied.
5. Follow the below steps of forming a Cluster between the SecureTransport Edge on Windows Server 2012 and the one on Windows Server 2016.

Prerequisites for Synchronization

- The `<FILEDRIVEHOME>\lib\admin\config\servers` configuration file is correct and identical on all SecureTransport Edge servers.
- The `<FILEDRIVEHOME>\var\tmp\sentinel_primary` file exists on the primary SecureTransport Edge only.
- A shared common `taeh` file is used on all servers.
- Each server is hosted on a different computer or VM.
- All servers use the same installation path.
- All the servers are on the same LAN.
- The primary administrator user ID is the same on all servers and all have the same password.
- The clocks are set to the same time on all servers.
- The internal CAs on all servers is trusted by all other servers. You can import the same internal CA on all servers.
- All database settings must be identical on all edges.
- Only files used for server configuration are configured for synchronization.
- All the server certificates are issued by a common CA.

Cluster formation steps

a. Exchange CA certificates between all servers.

b. On the primary and the secondary server, list all the servers in the `<FILEDRIVEHOME>\lib\admin\config\servers` configuration file. List the primary server first and continue with the secondary server.

Note The `<FILEDRIVEHOME>\lib\admin\config\servers` file must be the same on all machines in your cluster. You can create it on the primary server and copy it to the secondary one.

c. On the primary server, create a file named `<FILEDRIVEHOME>\var\tmp\sentinel_primary`

Note To create the file, you can create an empty file with no file extension in Windows. The file must have 0 bytes.

d. Log out of the primary SecureTransport Edge server and log in again. Make sure that the server is identified as the primary server and that the **Synchronize All** and **Bounce All** buttons are displayed.

e. Synchronize the secondary server manually from the Administration Tool of the primary server.

Note Wait for the synchronization to complete successfully. The duration of the sync will depend on the amount of the data that will be synced.

6. Manually verify that the data is successfully synced to the new node (parameters, administrators, certificates should be present on the new node).
7. On both nodes comment the entries in the `servers` file located in `<FILEDRIVEHOME>\lib\admin\config\`
8. On the primary node remove the previously created `sentinel_primary` file located in `<FILEDRIVEHOME>\var\tmp\`
9. Power off the original node on Windows Server 2012.
10. Change the IP address of the node on Windows Server 2016 to the IP address previously occupied by the node on Windows Server 2012.
11. Re-add your existing (original) license if a temporary one was used and restart all services on the node on Windows Server 2016.

Related Topics:

- *Standalone installation with MySQL* on page 26
- *Standalone with External Database* on page 30
- *Standard Cluster environment with MySQL* on page 32
- *Enterprise Cluster environment with external database* on page 36
- *Edge installation with MySQL when part of a synchronized cluster* on page 41

Edge installation with MySQL when part of a synchronized cluster

This topic provides instructions for migrating SecureTransport 5.4 Edge on Windows Server 2012 deployment (as part of a synchronized cluster) to Windows Server 2016 or Windows Server 2019.

The migration procedure requires you to add your new SecureTransport Edge deployment (on Windows Server 2016 or Windows Server 2019) to a synchronized cluster of Edges and take advantage of the cluster capability to sync global configurations and accounts across nodes.

Note The migration procedure to Windows Server 2016 is the same as that to Windows Server 2019. To avoid repetition, instructions herein will discuss migration steps to Windows Server 2016. You can follow these same steps when migrating to Windows Server 2019.

Prerequisites

- Back up your existing SecureTransport installation. To back up your current SecureTransport deployment, follow a backup procedure applicable for your environment and make sure the backup is created at a time when all SecureTransport services are stopped.

Note Please keep in mind that migrating SecureTransport Edge to Windows Server 2016 will not migrate the Server and Audit log information. This information can be backed up prior to the migration.

- If migrating SecureTransport Edges in a synchronized cluster, perform the below procedure for each set of two nodes (one old and one new, the new replaces the old one).

Note Alternatively if all of the nodes have the same local settings you can add a new node on Windows Server 2016 to the existing synchronized cluster (to sync and replace the old Primary), after which add all other nodes on Windows Server 2016 to the synchronized cluster and resync.

Migration procedure

1. Install a new SecureTransport 5.4 Edge (vanilla installation, no patches) on Windows Server 2016 using the `taeh` file from the one on Windows Server 2012.
    - Make sure that the host names and IP addresses of all servers are in the host files of all servers. Use the lookup command to verify that the host names of all servers resolve on all hosts.
    - Select the computer that is to serve as the primary server. This must be the Windows Server 2012 node from which the configuration is to be replicated.
2. Make sure that the patch level of the new SecureTransport deployment (on Windows Server 2016) matches that of the original one (on Windows Server 2012). For example, if the original deployment has Patch 22 installed, you must perform the necessary steps to upgrade the new vanilla SecureTransport installation to Patch 22 as well.
3. Manually re-apply and reconfigure all previously applied customizations, for example:
    - plugins from the …`\STServer\plugins\` folder
    - start/stop scripts
    - configurations in `configuration.xml`
    - configurations in `mysql.conf`
    - JVM heap size
    - multi-protocol listeners
    - all local server configurations (i.e. network zones, allowed SecureTransport Servers) and all Local Server configuration parameters in the SecureTransport Administration Tool: go to **Operation > Server Configuration** and select the **Local Parameters** checkbox on the new Windows Server 2016 node.

Note Please make sure no configuration files (i.e. `configuration.xml`) are copied across the nodes. All Server Configuration parameters will sync automatically when the cluster is formed.

4. Make sure you have a feature license that permits the necessary number of nodes for the migration procedure. In case your license does not allow you to add new machines to the existing environment, contact Axway Global Support and request a temporary license. Do not forget to restart all services after the new license is applied.

5. On all Windows Server 2012 Edge nodes comment the entries in the `servers` file located in `<FILEDRIVEHOME>\lib\admin\config\` so that the edges will no longer remain synched.
6. Follow the below steps of forming a Cluster between the SecureTransport Edge on Windows Server 2012 and the one on Windows Server 2016.

   Perform these steps for the corresponding set of nodes:

   - on one hand the node from which the configuration will be copied. This is the primary one on Windows Server 2012.
   - on the other the node which will receive the old configuration. This is the new primary one on Windows Server 2016, which will replace the old one on Windows Server 2012.

   Prerequisites for Synchronization

   - The `<FILEDRIVEHOME>\lib\admin\config\servers` configuration file is correct and identical on all SecureTransport Edge servers.
   - The `<FILEDRIVEHOME>\var\tmp\sentinel_primary` file exists on the primary SecureTransport Edge only.
   - A shared common `taeh` file is used on all servers.
   - Each server is hosted on a different computer or VM.
   - All servers use the same installation path.
   - All the servers are on the same LAN.
   - The primary administrator user ID is the same on all servers and all have the same password.
   - The clocks are set to the same time on all servers.
   - The internal CAs on all servers is trusted by all other servers. You can import the same internal CA on all servers.
   - All database settings must be identical on all edges.
   - Only files used for server configuration are configured for synchronization.
   - All the server certificates are issued by a common CA.

   Cluster formation steps

   a. Exchange CA certificates between all servers.
   b. On the primary and the secondary server, list all the servers in the `<FILEDRIVEHOME>\lib\admin\config\servers` configuration file. List the primary server first and continue with the secondary servers.

   Note The `<FILEDRIVEHOME>\lib\admin\config\servers` file must be the same on all machines in your cluster. You can create it on the primary server and copy it to the others.

c. On the primary server, create a file named `<FILEDRIVEHOME>\var\tmp\sentinel_primary`

Note To create the file, you can create an empty file with no file extension in Windows. The file must have 0 bytes.

d. Log out of the primary SecureTransport Edge server and log in again. Make sure that the server is identified as the primary server and that the **Synchronize All** and **Bounce All** buttons on the *Server Control* page are displayed.

e. Synchronize the secondary server manually from the Administration Tool of the primary server.

Note Wait for the synchronization to complete successfully. The duration of the sync will depend on the amount of the data that will be synced.

7. Manually verify that the data is successfully synced to the new node (parameters, administrators, certificates should be present on the new node).
8. On both nodes comment the entries in the `servers` file located in `<FILEDRIVEHOME>\lib\admin\config\`.
9. On the primary node remove the previously created `sentinel_primary` file located in `<FILEDRIVEHOME>\var\tmp\`
10. Power off the original node on Windows Server 2012.
11. Change the IP address of the node on Windows Server 2016 to the IP address previously occupied by the node on Windows Server 2012.
12. Restart all services on the node on Windows Server 2016.
13. For all secondary nodes, follow steps 1 through 4, make sure the new node meets the *Prerequisites for Synchronization* on page 43, and then follow steps 10 through 12.
14. After each node has been successfully replaced by its corresponding Windows Server 2016 node, uncomment the entries in the `servers` file located in `<FILEDRIVEHOME>\lib\admin\config\` on all nodes.
15. Restart all services on all nodes.
16. Synchronize the secondary servers manually from the SecureTransport Administration Tool of the primary server.
17. Re-add your existing (original) license if a temporary one was used and restart all services.

Related topics:

- *Standalone installation with MySQL* on page 26
- *Standalone with External Database* on page 30
- *Standard Cluster environment with MySQL* on page 32
- *Enterprise Cluster environment with external database* on page 36
- *Edge installation with MySQL* on page 38