axway

SecureTransport

Version 5.5

25 April 2024

Getting Started Guide

This documentation describes the following Axway software:

Axway SecureTransport 5.5 Modernized Standard Cluster (Beta)

Contents

Preface

This guide provides instructions for performing the initial setup and configuration of the SecureTransport software.

Use this documentation to:

- Install licenses
- Change the keystore password
- Generate certificates
- Generate or import certificate authority
- Perform initial database settings
- Perform initial setup of servers
- Exchange CA certificates
- Cleanup the setup account

This document describes how to set up and configure SecureTransport for basic operation. It assumes SecureTransport is already installed and ready to configure. If SecureTransport has not been installed or there are questions relating to the installation, see the *SecureTransport Installation Guide*.

The Setup Administrator account is used only for the initial post-installation configuration. Use the Setup Administrator account to configure key items needed for SecureTransport to function. These items are listed in the Starting Setup chapter of this guide. After the initial setup is complete, use the admin login for further configuration and future maintenance and changes. Refer to the *SecureTransport Administrator's Guide* for more information.

You can also export server configuration from a SecureTransport installation and import it into your new or upgraded installation. However, you cannot export licenses, so you must install them on a new server. Central Governance options are also not exported. See the topic on export and import of server configuration in the *SecureTransport Administrator's Guide*.

Who should read this guide

This document is intended for system administrators who perform the setup and initial configuration of the SecureTransport software. As the SecureTransport setup administrator, you must be able to work effectively with the operating system platform and network used by SecureTransport. You must have administrative privileges on any computers running Windows where you setup SecureTransport and appropriate access to systems that SecureTransport depends on, such as an external database and file system. Setup UNIX or Linux systems does require administrative privileges.

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

Available documentation

The following documentation is available for SecureTransport 5.5:

- *SecureTransport Administrator's 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 Appliance Guide* - provides the SecureTransport Appliance installation, configuration, and operation instructions. It also provides SecureTransport installation and upgrade instructions on Axway Appliances.
- *SecureTransport Capacity Planning Guide* – provides useful information when planning your production environment for SecureTransport.
- *SecureTransport Developer's Guide* – provides descriptions and usage instructions for implementing custom pluggable components in SecureTransport.
- *SecureTransport Getting Started Guide* – explains the initial setup and configuration of SecureTransport using the SecureTransport Administrator setup interface.
- *SecureTransport Installation Guide* – provides instructions for installing and uninstalling SecureTransport on UNIX-based platforms and Microsoft Windows.
- *SecureTransport on AWS Setup Guide* – provides a detailed overview and detailed instructions for setting up SecureTransport in the Amazon Web Services (AWS) Virtual Private Cloud (VPC).
- *SecureTransport on Azure Setup Guide* – provides a detailed overview and detailed instructions for setting up SecureTransport in the Microsoft Azure portal.
- *SecureTransport Upgrade Guide* – provides instructions for upgrading SecureTransport on UNIX-based platforms and Microsoft Windows.
- *SecureTransport Security Guide* – provides security information necessary for the secure operation of the SecureTransport product.
- *ST Web Client Configuration Guide* - describes how to configure and customize the ST Web Client user interface.
- *ST Web Client User Guide* – describes how to use the ST Web Client for end users.
- *SecureTransport Release Notes* – contains information about new features and enhancements in the current version of SecureTransport, as well as a comprehensive list of fixes and known issues.
- *SecureTransport Software Development Kit (SDK)* – a set of software development tools and examples that allow extending SecureTransport by consuming and implementing available APIs.
- *SecureTransport REST API documentation* – the portal published API documentation derived from the API swagger documents. To access the administrator and the end-user API documentation, go to docs.axway.com/category/api.

Accessibility and VPATs

- Axway Accessibility Conformance Report for SecureTransport 5.5 - Describes the SecureTransport accessibility features.

- Axway Accessibility Conformance Report for ST Web Client - Describes the ST Web Client accessibility features.

Visit docs.axway.com to view or download documentation.

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

Start working with SecureTransport

1

SecureTransport is part of the Axway family of managed file transfer (MFT) products. SecureTransport allows organizations to 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 manages 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*.

The following getting started topics are provided:

- *Initial configuration on page 9* - Describes the initial SecureTransport setup and configuration.
- *Install licenses on page 21* - Describes installing the SecureTransport licenses.
- *Change the keystore password on page 24* - Describes the keystore password and provides how-to instructions for changing the keystore password.
- *Generate or import a certificate authority on page 25* - Describes generating and or importing a certificate authority.
- *Generate certificates on page 28* - Describes generating certificates.
- *Database settings on page 33* - Describes the SecureTransport database settings.
- *Set up servers on page 35* - Describes setting up servers.
- *Exchange CA certificates on page 40* - Describes exchanging CA certificates.
- *Clean up the default administrative credentials on page 43* - Provides how-to instructions for cleaning up the setup account.
- *Setup test on page 44* - Provides the procedures for the initial test of the SecureTransport installation and setup.
- *Additional configuration tasks on page 49* - Provides a list of additional configuration tasks.

Initial configuration 2

For the initial configuration, SecureTransport provides a setup account with a default password. After the initial setup is completed, change the default setup password. Before beginning the setup of SecureTransport, review the following topics and checklists to ensure that the listed items are available:

- *SecureTransport Server checklists* on page 9 - Provides a list of items needed for the SecureTransport Server configuration.
- *SecureTransport Edge checklists* on page 14 - Provides a list of the items needed for the SecureTransport Edge server configuration.
- *Log into the server* on page 17 - Provides how-to instructions for logging into the server.
- *Setup steps* on page 18 - Provides a list and descriptions of the setup steps.
- *View server log messages* on page 19 - Provides how-to instructions for viewing server log messages.
- *View audit log messages* on page 20 - Provides how-to instructions for viewing audit log messages.

SecureTransport Server checklists

This section provides the SecureTransport Server checklists for root and non-root installations.

SecureTransport Server root installation checklist

The following items are needed for the SecureTransport Server root installation configuration:

Items	Your installation
SecureTransport Server IP address	
Core server license for SecureTransport Server	
Server feature license for SecureTransport Server	
Certificate Authority (CA) and certificate attributes	
Initial password for the root CA	

Items	Your installation	
Port settings	**Default**	**Your installation**
HTTP port	80	
HTTPS port	443	
HTTPS admin port	444	
HTTPS admin shutdown port	8005	
FTP/S port	21	
AS2 port for HTTP	10080	
AS2 port for HTTPS	10443	
AS2 shutdown port	8006	
SSH port	22	
PeSIT over Plain Socket port	17617	
PeSIT over Secured Socket port	17627	
PeSIT over Secured Socket (legacy) port	17637	
PeSIT over Secured Socket (legacy § comp) port	17657	
PeSIT over pTCP Plain Socket port	19617	
PeSIT over pTCP Secured Socket port	19627	
MariaDB / MySQL database port	33060	
Oracle database settings	**Default**	**Your installation**
Host		
Port	1521	
User Name		
Password		
Service Name		

Items	Your installation	
Use existing database schema	False	
Use secure connection	True	
Server Certificate DN		
Certificate Path		
PostgreSQL database settings	**Default**	**Your installation**
Host		
Port	5432	
User Name		
Password		
Database Name		
Use existing database schema	False	
Use secure connection	True	
Server Certificate DN		
Certificate File		
Microsoft SQL Server database settings	**Default**	**Your installation**
Host		
Port	1433	
Login Name		
Password		
Database Name		
Use existing database schema	False	
Use secure connection	True	
Server Certificate CN		
Certificate Path		

Note If port 22 is the default port for the operating system SSH service on your platform, to avoid conflicts change the port or disable the operating system service or choose a different port for SecureTransport SSH service. The default operating system SSH port for Axway appliances is 10022.

SecureTransport Server non-root installation checklist

The following items are needed for the SecureTransport Server non-root installation configuration:

Items	Your installation
SecureTransport Server IP address	
Core server license for SecureTransport Server	
Server feature license for SecureTransport Server	
Certificate Authority (CA) and certificate attributes	
Initial password for the root CA	

Port settings	Default	Your installation
HTTP port	8080	
HTTPS port	8443	
HTTPS admin port	8444	
HTTPS admin shutdown port	8005	
FTP/S port	8021	
AS2 port for HTTP	10080	
AS2 port for HTTPS	10443	
AS2 shutdown port	8006	
SSH port	8022	
PeSIT over Plain Socket port	17617	
PeSIT over Secured Socket port	17627	

Items	Your installation	
PeSIT over Secured Socket (legacy) port	17637	
PeSIT over Secured Socket (legacy § comp) port	17657	
PeSIT over pTCP Plain Socket port	19617	
PeSIT over pTCP Secured Socket port	19627	
MariaDB / MySQL database port	33060	
Oracle database settings	**Default**	**Your installation**
Host		
Port	1521	
User Name		
Password		
Service Name		
Use existing database schema	False	
Use secure connection	True	
Server Certificate DN		
Certificate Path		
PostgreSQL database settings	**Default**	**Your installation**
Host		
Port	5432	
User Name		
Password		
Database Name		
Use existing database schema	False	
Use secure connection	True	

Items	Your installation	
Server Certificate DN		
Certificate Path		
Microsoft SQL Server database settings	**Default**	**Your installation**
Host		
Port	1433	
Login Name		
Password		
Database Name		
Use existing database schema	False	
Use secure connection	True	
Server Certificate CN		
Certificate Path		

Note If port 8022 is the default port for the operating system SSH service on your platform, to avoid conflicts change the port or disable the operating system service or choose a different port for SecureTransport SSH service. The default operating system SSH port for Axway appliances is 10022.

SecureTransport Edge checklists

This section provides the SecureTransport Edge checklists for root and non-root installations.

SecureTransport Edge root installation checklist

The following items are needed for the SecureTransport Edge root installation configuration:

Items	Your installation
SecureTransport Edge IP address	
SecureTransport Server IP address or host name	

Items	Your installation	
Core server license for SecureTransport Edge		
Server feature license for SecureTransport Edge		
CA and certificate attributes		
Initial password for the root CA		
Port Settings	**Default**	**Your installation**
HTTP port	80	
HTTPS port	443	
HTTPS admin port	444	
HTTPS admin shutdown port	8005	
FTP/S port	21	
AS2 port for HTTP	10080	
AS2 port for HTTPS	10443	
SSH port	22	
PeSIT over Plain Socket port	17617	
PeSIT over Secured Socket port	17627	
PeSIT over Secured Socket (legacy) port	17637	
PeSIT over Secured Socket (legacy § comp) port	17657	
PeSIT over pTCP Plain Socket port	19617	
PeSIT over pTCP Secured Socket port	19627	
Database port	33060	
Proxy server port	1080	
Streaming Port Settings:	**Default**	**Your installation**
FTP	20021	

Items	Your installation
HTTP	20080
AS2	21080
SSH	20022
PeSIT	27617
ADMIN	20444

Note If port 22 is the default port for the operating system SSH service on your platform, to avoid conflicts change the port or disable the operating system service or choose a different port for SecureTransport SSH service. The default operating system SSH port for Axway appliances is 10022.

SecureTransport Edge non-root installation checklist

The following items are needed for the SecureTransport Edge non-root installation configuration:

Items	Your installation
SecureTransport Edge IP address	
SecureTransport Server IP address or host name	
Core server license for SecureTransport Edge	
Server feature license for SecureTransport Edge	
CA and certificate attributes	
Initial password for the root CA	

Port Settings	Default	Your installation
HTTP port	8080	
HTTPS port	8443	
HTTPS admin port	8444	
HTTPS admin shutdown port	8005	

Items	Your installation	
FTP/S port	8021	
AS2 port for HTTP	10080	
AS2 port for HTTPS	10443	
SSH port	8022	
PeSIT over Plain Socket port	17617	
PeSIT over Secured Socket port	17627	
PeSIT over Secured Socket (legacy) port	17637	
PeSIT over Secured Socket (legacy § comp) port	17657	
PeSIT over pTCP Plain Socket port	19617	
PeSIT over pTCP Secured Socket port	19627	
Database port	33060	
Proxy server port	1080	
Streaming Port Settings:	**Default**	**Your installation**
FTP	20021	
HTTP	20080	
AS2	21080	
SSH	20022	
PeSIT	27617	
ADMIN	20444	

Note If port 8022 is the default port for the operating system SSH service on your platform, to avoid conflicts change the port or disable the operating system service or choose a different port for SecureTransport SSH service. The default operating system SSH port for Axway appliances is 10022.

Log into the server

Log into your server with all checklist items readily available.

1. Open a browser.
2. Enter `https://<servername>:<portnumber>` where `<servername>` is the name or IP address of the server you want to configure and `<portnumber>` is the SSL port number you assigned to the Administration Tool during installation. The default port number is `444` or `8444` if SecureTransport is running as a non-root user.
3. Following the instructions for your browser, add a certificate exception for the SecureTransport instance.
4. Enter the setup user name and password. The default setup user name is `setup` and the default password is `setup`.

Setup steps

Before executing the setup steps, log into the Setup Administrator account. The Setup Administrator account is used for the initial, one-time configuration of the system.

There are seven steps involved in configuring SecureTransport for initial use. Complete the steps in the order listed to prevent conflicts.

1. **Install Licenses** – Install the core and feature licenses. This is the only step you perform on the second and subsequent servers in an Enterprise Cluster.
2. **Keystore Password** – Replace the default keystore password with one you create.
3. **Generate CA** – Regenerate the Internal CA used to sign other certificates.

   Alternately, you can import a CA certificate.
4. **Generate Certificates** – Generate certificates for each protocol server you are using, FTP, HTTP, etc.

   You can import server certificates. The certificates can be signed by any trusted authority.
5. **Database Settings** - Select the internal database port and configure the internal database password or setup an external database.
6. **Set Up Servers**– Set up the HTTP, FTP, SSH, AS2, and PeSIT protocol servers, the Transaction Manager (TM) server, and the Database server.

   The SecureTransport Edge server also supports a proxy (SOCKS) setup.
7. **Exchange Certificates** – Export and import CAs from SecureTransport Servers and SecureTransport Edge servers.

Shared Storage

Cluster environments of any type in an Enterprise or a Standard Cluster require Shared storage.

For more information about Standard and Enterprise Cluster models, refer to the *SecureTransport Administrator's Guide*.

Shared storage definition and configuration in SecureTransport

Since the data in the Shared Storage is used by all cluster nodes, they must have identical rights and simultaneous read/write access, while also providing consistency between the users' files.

Shared Storage must be mounted to the same location on all servers.

When creating a user account, the user's home folder must be the full path to the Shared Storage folder.

Setting up cluster with shared storage for the home folders of the user accounts

Windows

If the account home folder prefix is on a shared network, specify a real user that has access to it. You must either use SecureTransport impersonation functionality or use permissions sufficient for the network share to be accessed by local system users. The real user must be part of the domain, not a local user for one of the cluster nodes; otherwise the other nodes in the cluster cannot impersonate it to access the shared location.

For more information about creating and configuring a real user in Windows, refer to the *SecureTransport Administrator's Guide*.

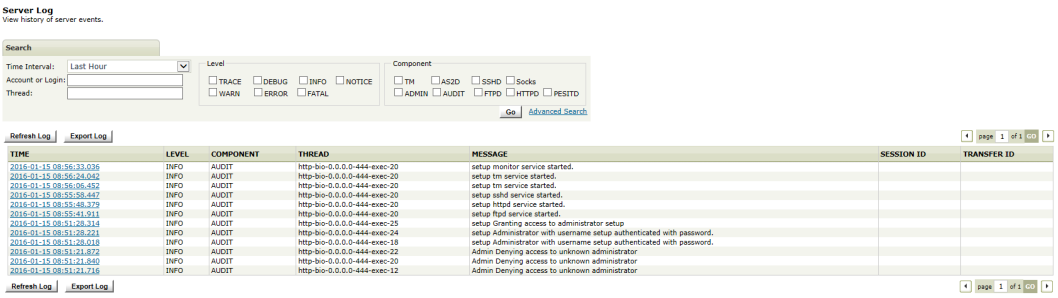
Linux

All user accounts must have access to the shared storage folder.

For more information about creating and configuring a real user in Linux, refer to the *SecureTransport Administrator's Guide*.

View server log messages

At any time during the setup process, you can view the log messages SecureTransport has generated by selecting **Server Log**.

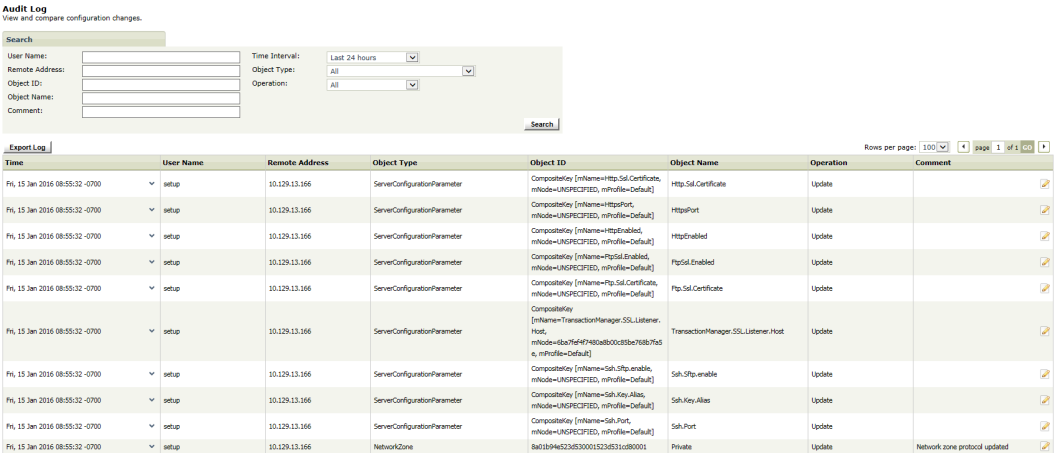


For more information about the server log, refer to the *SecureTransport Administrator's Guide*.

Note When you log into the Administration Tool using the admin account, you can access this page by selecting **Operations > Server Log**.

View audit log messages

At any time during the setup process, you can view the log messages that audit changes to the SecureTransport configuration by selecting **Audit Log**.



For more information about the audit log, refer to the *SecureTransport Administrator's Guide*.

Note When you log into the Administration Tool using the admin account, you can access this page by selecting **Operations > Audit Log**.

Install licenses 3

Setup step 1 requires you to install your licenses: *core server license* and *features license*.

The *core server license* specifies the number of accounts allowed and the number of ad hoc users allowed. It also limits the license to a specified host and date range. The *features license* limits the type of external database server and specifies if the AS2, SSH, and Connect:Direct protocols are allowed, if SiteMinder integration is allowed, if the Enterprise Cluster (EC) option is included, and the number of Enterprise Cluster nodes allowed.

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

Contact Axway Global Support to obtain text files containing the core server license and the features license for your authorized features. For contact information, see *Get more help* on page 7.

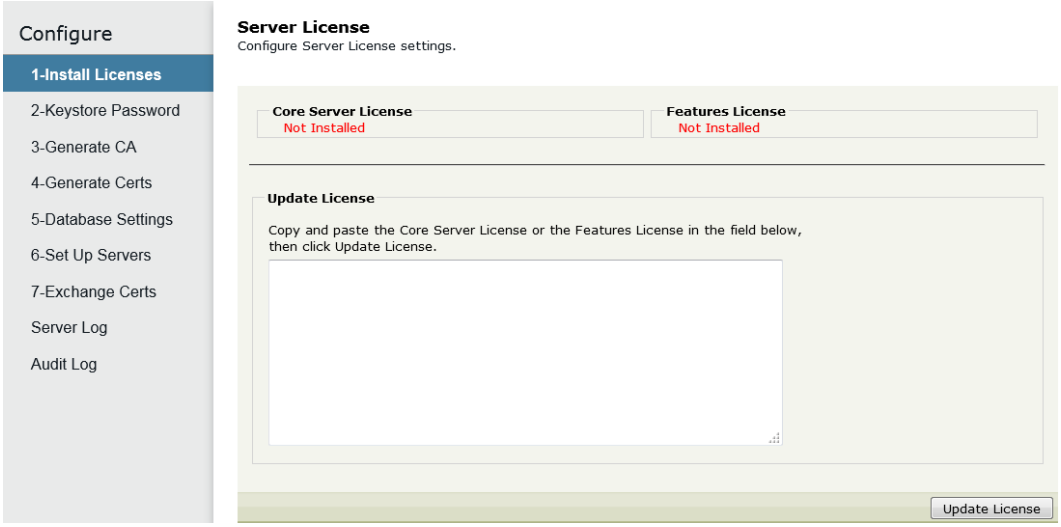
Note The installation of licenses is the only setup step you perform on the second and subsequent servers in an Enterprise Cluster.

Install server license

Use the **Server License** page to install SecureTransport licenses.

1. Select **Configure > 1-Install Licenses**.

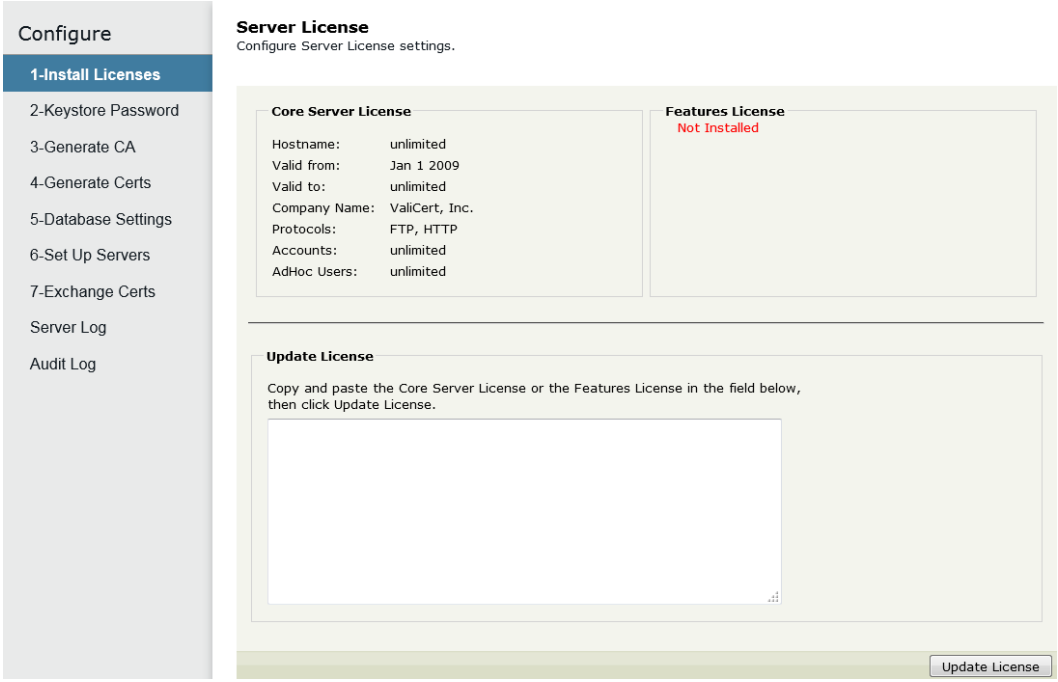
   The *Server License* page is displayed.



2. Open the text file containing the core server license information.
3. Copy the entire contents of the file to the clipboard.

4. Paste the copied contents of the file into the **Update License** text area and click **Update License**.

   The core server license information is displayed.



Ad hoc user license

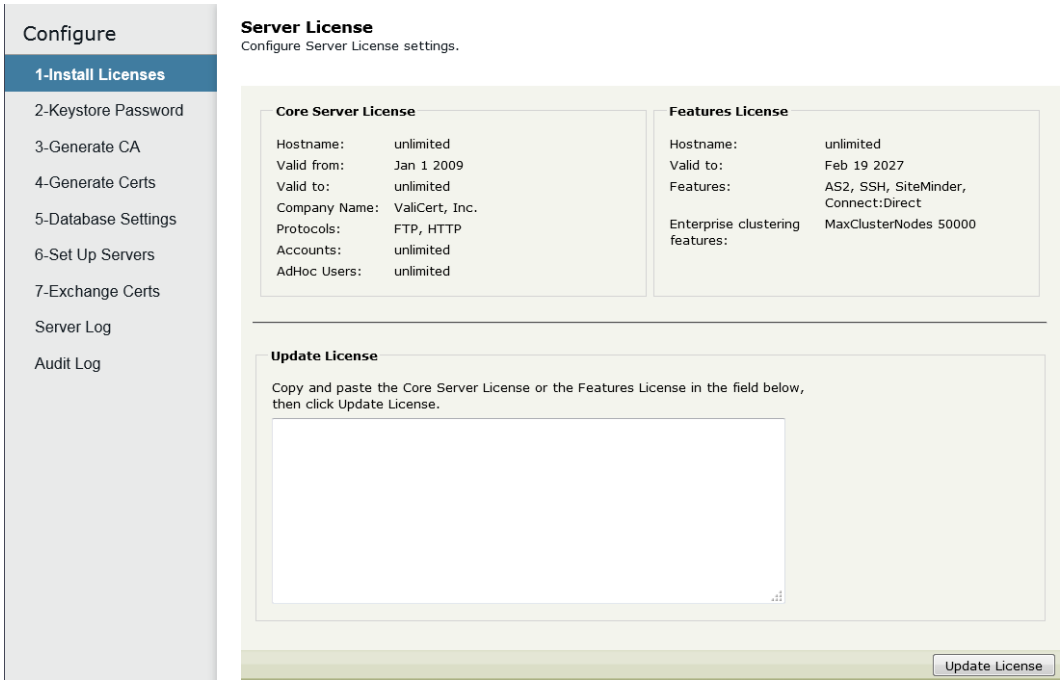
Ad hoc users is a feature, part of the core server license. Ad hoc users have the capability to compose, send, reply to, or forward email messages using ST Web Client. There are four categories of ad hoc user licenses:

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

Install features license

1. Open the text file containing the feature server license information.
2. Copy the entire contents of the file to the clipboard.
3. Paste the copied contents of the file into the **Update License** text area and click **Update License**.

   The features license information is displayed.



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

Change the keystore password 4

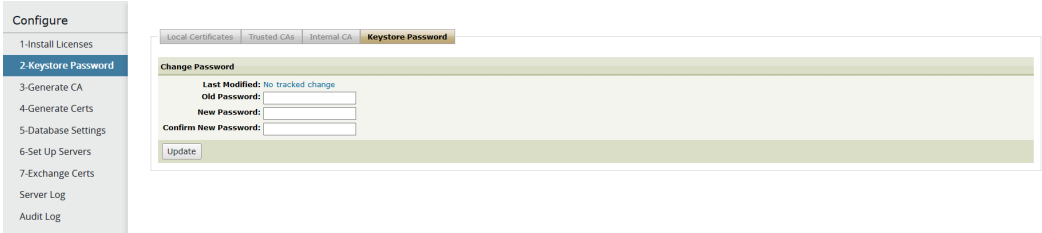
Setup step 2 requires you to change the default keystore password.

SecureTransport contains a keystore of encrypted X509 and PGP private and public keys created and used within SecureTransport. A default keystore password is set during installation. For greater security, change the keystore password from the default one before you generate an internal certificate.

Follow these steps to change the keystore password:

1. Select **Configure > 2-Keystore Password**.

   The *Keystore Password* pane is displayed.



2. Enter the old keystore password in the **Old Password** field. Leave this field empty if this is the first time you are changing the keystore password and SecureTransport uses the default.
3. Enter a new password and re-enter the password in the **Confirm New Password** field.
4. Click **Update** to change the password.

   A message in the **Keystore Password** tab confirms that the password was changed successfully.

Note When you log in to the Administration Tool using the admin account, you can access this page by selecting **Setup > Certificates > Keystore Password**.

Generate or import a certificate authority

5

Setup step 3 requires you to create or import a new internal certificate authority (CA) before you can generate certificates for services.

Generate a permanent internal CA

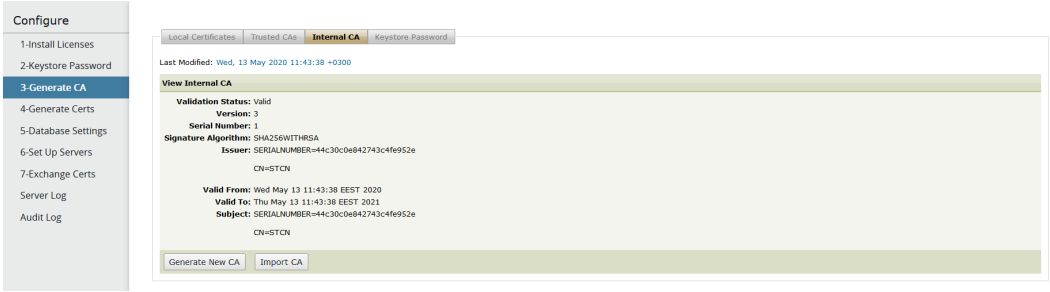
SecureTransport uses digital certificates for many security functions. These certificates can either be self-issued, meaning they are issued by the SecureTransport Server or signed by a third party, such as an external company like Verisign or a corporate CA. During the installation process, SecureTransport installs a default self-issued CA.

This step regenerates the self-signed Internal CA with a new password and with Distinguished Name (DN) attributes specific to an organization. You can use the Internal CA to sign local certificates that you generate in Step 4.

Note When you log in to the Administration Tool using the admin account, you can access this page by selecting **Setup > Certificates > Internal CA**.

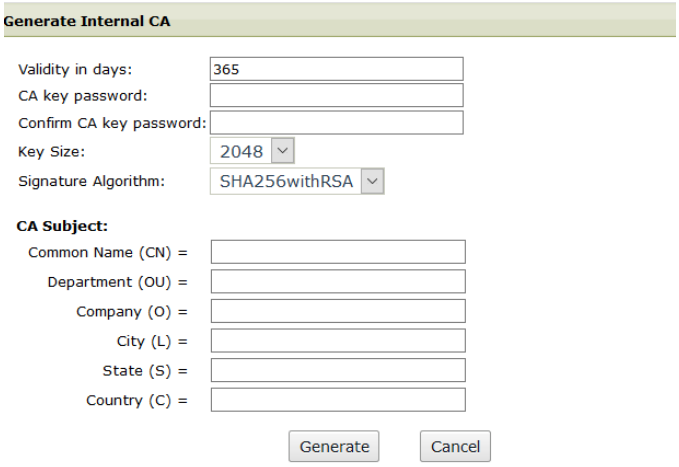
1. Select **Configure > 3-Generate CA**.

   SecureTransport displays the *Internal CA* pane.



2. Click **Generate New CA**.

   SecureTransport displays *Generate Internal CA* page.



3. Enter the required information for the internal certificate.

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

   - **Validity in days** – the number of days the certificate is valid. The default is 365 days.
   - **CA key password** – the private key password used to unlock the certificate.
   - **Confirm CA key password** – the private key password must be entered again for confirmation.
   - **Key Size** – a number representing the size of the generated key, expressed in bits. Possible values are 1024, 2048 (default), 3072, or 4096 bits.
   - **Signature Algorithm** – the selection of the signature signing hashing algorithm. Possible values are SHA1withRSA, SHA256withRSA (default), SHA384withRSA, and SHA512withRSA.
   - **Common Name** – a description of the certificate. Do not use the host name or the fully qualified domain name (FQDN) of the server without additional identifying text.
   - **Department** – the organizational unit represented by the CA.
   - **Company** – the organization represented by the CA.
   - **City** – the name of the locality where the CA is located.
   - **State** – the name of the state or province where the CA is located.
   - **Country** – the name of the country where the CA is located.

4. Click **Generate**.

Import an external CA

Optionally, you can also import an external certificate. Ensure the certificate is valid and configured to validate certificates before you import it. SecureTransport does not check the validity of the certificate.

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

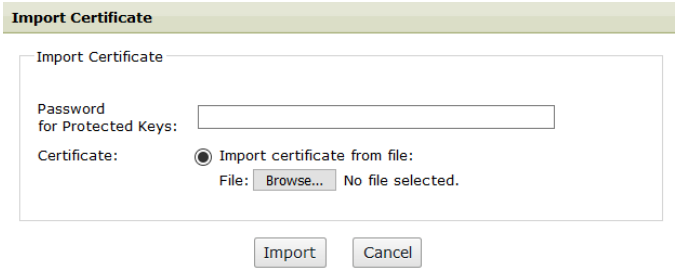
Note SecureTransport protocol servers and services do not require restart after importing, overwriting, or deleting a trusted certificate.

1. Select **Configure > 3-Generate CA**.

   SecureTransport displays the *Internal CA* pane.

2. Click **Import CA**.

   SecureTransport displays the *Import Certificate* page.



3. Enter a password in the field provided. The password is required.

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

4. Specify the certificate by browsing to the PKCS#12 (PEM/DER) file.

5. Click **Import**.

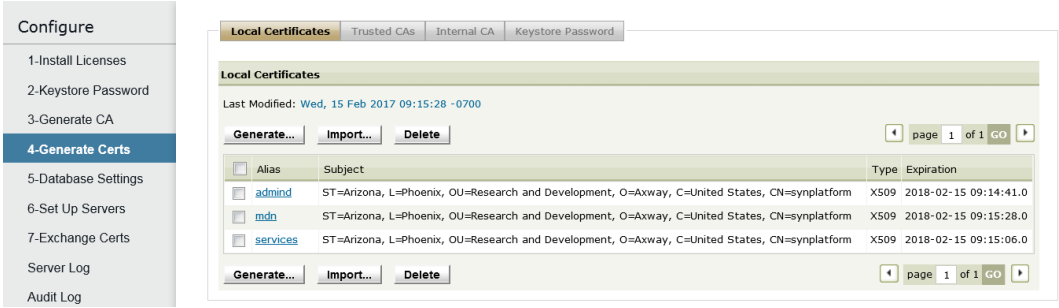
Now, SecureTransport uses the imported certificate as Internal CA and signs all certificates generated using that CA.

Note For more information, refer to the topic on importing an external CA in the *SecureTransport Administrator's Guide*.

Generate certificates 6

Step 4 requires you to generate the server certificates that SecureTransport uses.

Select **Configure > 4-Generate Certs** to generate local, self-issued server certificates. Generated certificates are assigned RSA keys.



Note When you log in to the Administration Tool using the admin account, you can access this page by selecting **Setup > Certificates > Local Certificates**. To import a certificate, refer to the *SecureTransport Administrator's Guide*.

SecureTransport can use certificates for multiple purposes. For example, the FTPD certificate is commonly used for securing FTPS connections. Separate certificates and aliases can be used for each protocol. The httpd certificate is commonly signed by a public CA so that external users, especially those using a web browser to access the system, will trust the certificate. The other certificates are either internal to the product or only used by the Administrators; they can be signed by the internal CA. A temporary admind certificate is generated as part of the installation process so you can log in for initial setup.

To use a certificate signed by an external CA, refer to the *SecureTransport Administrator's Guide* for information about the Import function.

SecureTransport certificates

The following tables list the certificates commonly used with SecureTransport, although the default SecureTransport configuration only requires that the `admind` and `mdn` certificates use those exact aliases.

For a SecureTransport Server installation, generate the following certificates as needed:

Alias	Required/Optional	Certificate use
`admind`	Required	An SSL server certificate for users connecting to the web administration system. Replaces the temporary one generated during installation.
`ftpd`	Optional	An SSL server certificate for users connecting to transfer files.
`httpd`	Optional	An SSL server certificate for users connecting to transfer files.
`mdn`	Optional	A certificate used to sign the MDN receipts. The `mdn` alias is used by the AS2 protocol for sending receipts. SecureTransport also generates MDN receipts for transfers for other protocols, but retains them locally and does not send the receipts to the customer.
`repencrypt` (or other)	Optional	A certificate used to encrypt and decrypt SecureTransport repository data. For more information, refer to the *SecureTransport Administrator's Guide*.
`streaming`	Optional	A certificate used to secure the streaming between the server and the edge.

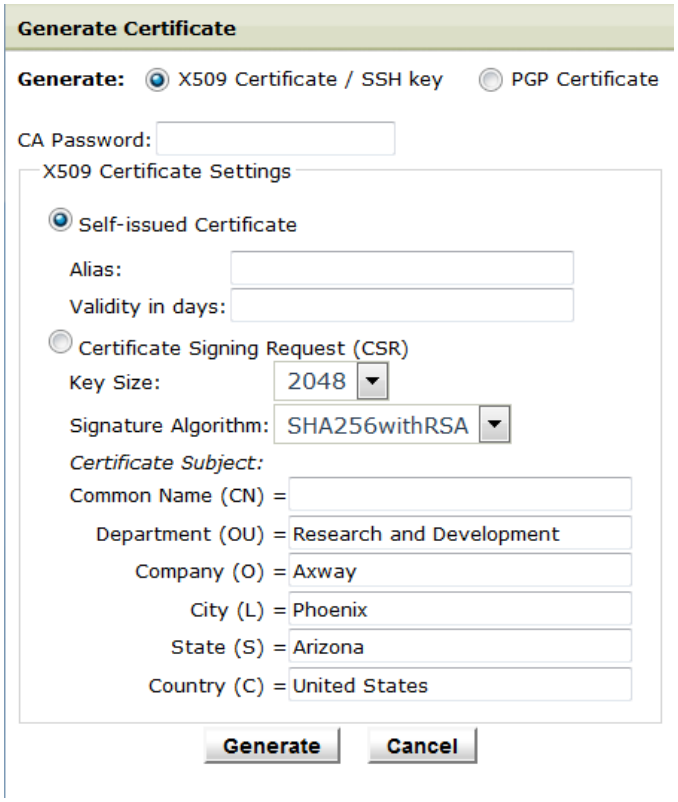
For a SecureTransport Edge installation, generate the following certificates as needed:

Alias	Required/Optional	Certificate use
`admind`	Required	An SSL server certificate for users connecting to the web administration system. Replaces the temporary one generated during installation.
`ftpd`	Optional	An SSL server certificate for users connecting to transfer files.
`httpd`	Optional	An SSL server certificate for users connecting to transfer files.
`streaming`	Optional	A certificate used to secure the streaming between the server and the edge.

These certificates can be signed by the internal SecureTransport CA, generated in the previous setup step. For more information, see *Generate or import a certificate authority on page 25*.

The following procedure is used to generate a self-issued certificate. For information about generating a Certificate Signing Request (CSR), refer to the *SecureTransport Administrator's Guide*.

1. Select **Configure > 4-Generate Certs**.
2. Click **Generate** to create a certificate.



3. Select the certificate type: **X509 Certificate / SSH key**.
4. Enter the **CA key password** – the password of the Internal CA private key.
5. Select **Self-issued Certificate**. Enter the required information for the self-issued certificates.

   Self-issued certificates require the **Certificate Subject** information. For self-issued certificates, enter the following information:

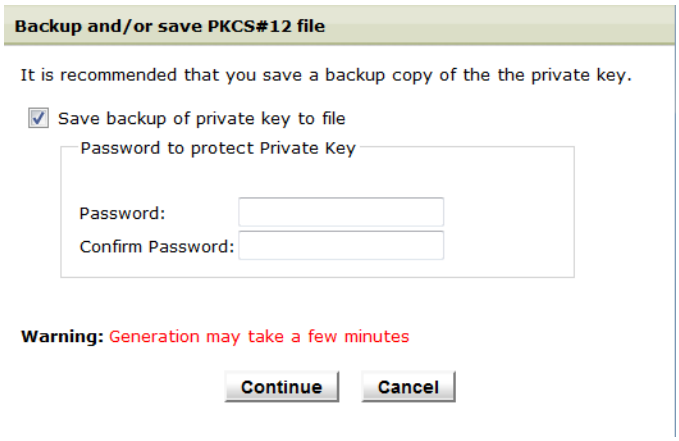
   - **Alias** – the name that identifies the certificate.

     If an alias that is already assigned to another certificate is used, a dialog box is displayed asking if you want to overwrite the original certificate. Be sure to enter the appropriate alias for the new certificate. If you are sure you want to replace the original certificate with the new one, click **Overwrite**. Click **Cancel** to discard the new certificate and keep the original one. You are returned to the **Generate Certificate** dialog box to make changes.
   - **Validity in days** – the number of days the certificate is valid.

- **Key Size** – a number representing the size of the generated key, expressed in bits. Possible values are 1024, 2048 (default), 3072, or 4096 bits.
- **Signature Algorithm** – the selection of the signature signing hashing algorithm. Possible values are SHA1withRSA, SHA256withRSA (default), SHA384withRSA, and SHA512withRSA.
- **Common Name** – a description of the certificate. Should be the external address that the users will access to ensure that browsers recognize it as a valid certificate. It can be the address itself but it also can be a load-balancer (LB) address. Do not use the same CN as is used in the Certificate Authority.
- **Department** – the organizational unit represented by the certificate.
- **Company** – the organization represented by the certificate.
- **City** – the name of the locality where the certificate is located.
- **State** – the name of the state or province where the certificate is located.
- **Country** – the name of the country where the certificate is located.

If you want to create a Certificate Signing Request (CSR), refer to the *SecureTransport Administrator's Guide* for more information.

6. Click **Generate**.
   a. If you are generating a certificate with the same alias as an existing certificate, confirm that you want to overwrite the existing one.
   b. (Optional) Select **Save backup of private key to file** if you want to save a copy of the private key.



   c. Enter a password in the **Password** field, enter it again in the **Confirm Password** field, and click **Continue**.
   d. When asked to open or save the file, click **Save** and select a location on the local file system.

      A message displays indicating that the certificate was successfully saved.
7. Click **Close**.

After generating a new `admind` certificate, you must restart the admin service.

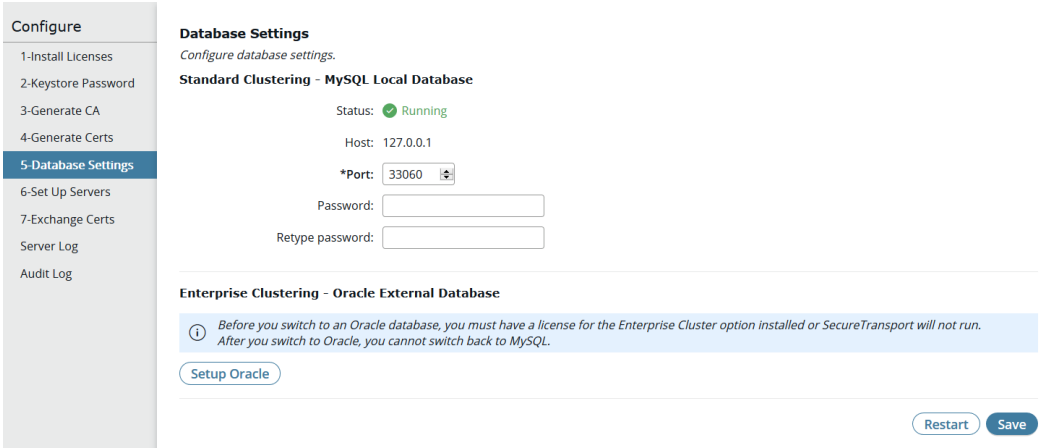
Note Never delete the `admind` certificate, instead overwrite it when you need to replace it. The `admind` certificate must be present, valid, and chained to a trusted root or the admind service will not start.

Database settings 7

If you are using the embedded database, select **Configure > 5-Database Settings** to perform the following tasks:

- Change the port or password for the embedded database for a SecureTransport Edge or a SecureTransport Server
- Migrate data from the embedded database to an external database

To change a stand-alone or clustered SecureTransport Server to different Oracle database or to direct log data to separate external Oracle databases, refer to the *SecureTransport Administrator's Guide*.



Note When you log in to the Administration Tool using the admin account, you can access this page by selecting **Setup > Database Settings**.

Change the embedded database port or password

If this SecureTransport installation uses the embedded database, the database has the default password `tumbleweed` after installation. To secure the system, change the database password. You can also change the database port.

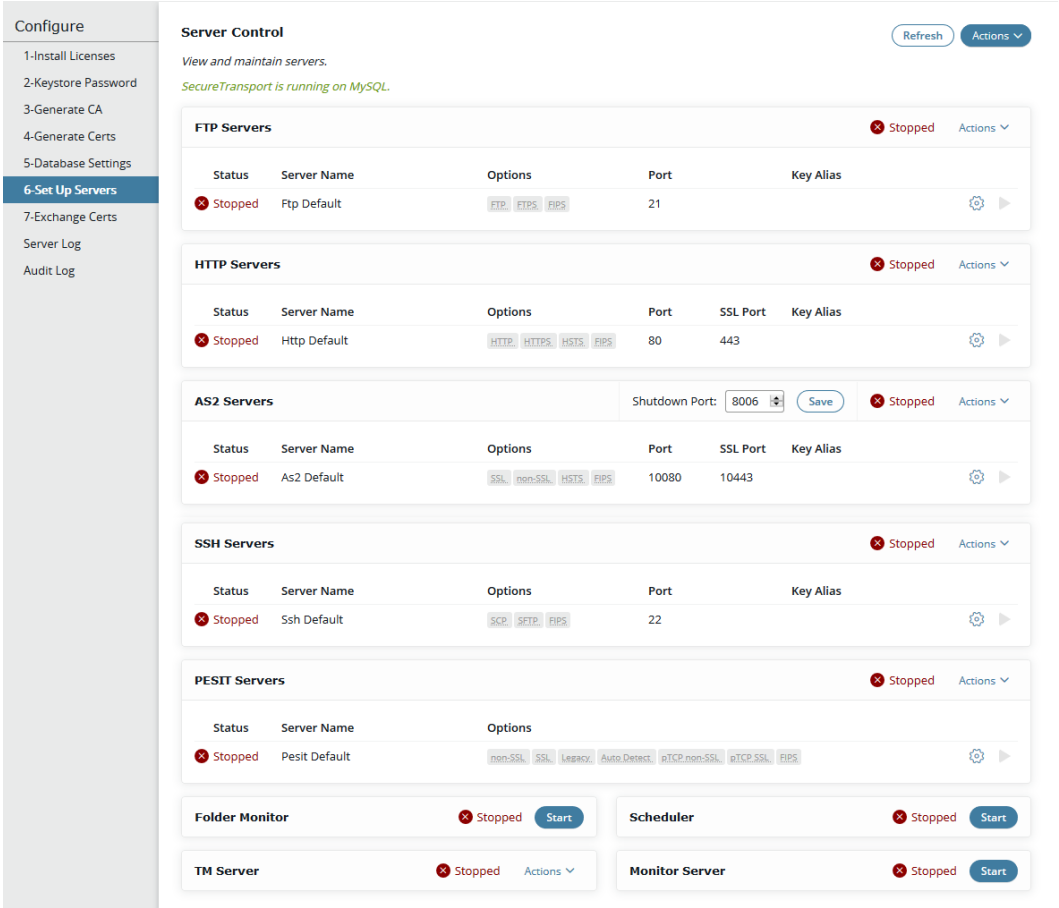
1. Select **Configure > 5-Database Settings**.
2. Under *Standard Clustering - MySQL Local Database* or *Standard Clustering - MariaDB Local Database*, type the new port number in the **Port** field.
3. Under *Standard Clustering - MySQL Local Database* or *Standard Clustering - MariaDB Local Database*, type the new password in both the **Password** and **Retype Password** fields.

4. Click **Save**.
5. If you changed the port, click **Restart Database Now**.

Set up servers 8

Setup step 6 requires you to define the settings for HTTP, FTP, AS2, SSH, PeSIT, and TM Server.

The **Configure > 6-Set Up Servers** page displays the FTP, HTTP, AS2, SSH, PeSIT, TM, and Monitor server settings. You can use this page to change the protocol ports, specify the protocol SSL key aliases, enable and disable services, and start or stop the services. When you are setting up an Edge server, you can also configure the Proxy server settings. When logged in as the Setup Administrator on SecureTransport Server, the following settings are displayed:



Note When you log in to the Administration Tool using the admin account, you can access this page by selecting **Operations > Server Control**. For more information about managing the servers, refer to the *SecureTransport Administrator's Guide*.

Set the SSL key alias

When you set up FTPS, HTTPS, AS2 (SSL), SSH, or PeSIT, you select a key alias to specify the certificate to use to secure the communications. You create the alias on Setup step 4 - Generate certificates. For more information, see *Generate certificates* on page 28.

Set the FIPS transfer mode

For client-initiated transfers using the AS2, FTPS, HTTPS, SSH (SFTP/SCP), or PeSIT protocols, you can select **Enable FIPS Transfer Mode** to restrict the SecureTransport server to use only FIPS 140-2 Level 1 certified cryptographic libraries. This mode requires the sender and the recipient (clients and partner servers) to use only the approved algorithms, ciphers, and cipher suites listed in the *SecureTransport Administrator's Guide* and assures that the entire transfer is secure at FIPS 140-2 Level 1.

Note If FIPS transfer mode is enabled for a protocol server, however the respective client does not provide the required FIPS cipher or cipher suite, SecureTransport will not complete the transfer.

Configure FTP servers

To use FTP in non-streaming environments, specify the FTP settings for the SecureTransport Server. In streaming environments, specify the FTP settings for the SecureTransport Edge.

1. Select **Enable FTP**. Additionally, if needed, select **Enable FTPS**.
2. If FTP is already running on port 21 (8021) at the OS level, change the **FTP Port** to use a port number other than the default setting of 21 for root installations and 8021 for non-root installations.

   Note Additionally, to avoid a port conflict, disable FTP at the OS level or assign it a different port number instead of changing the port number in SecureTransport.

3. If you enabled FTPS, select an **SSL Key Alias** from the drop-down list, for example, **ftpd**.
4. If you enabled FTPS, to restrict FTPS connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** checkbox.
5. Click **Start**.

Note Configuring the FTP servers does not enable plain FTP. By default, the Secure Socket Layer (SSL) is enabled for all protocols. To enable plain FTP, an SSL user rule with encryption optional must be created. For information on creating SSL user rules, refer to the *SecureTransport Administrator's Guide*.

Configure HTTP servers

To use HTTP, specify the HTTP settings for both the SecureTransport Edge and SecureTransport Server.

1. Select one or both of **Enable HTTP** and **Enable HTTPS**. If you select Enable HTTPS, by default **Enable HSTS** will also be selected. You can also deselect **Enable HSTS** once **Enable HTTPS** is selected. When HSTS is enabled, a HSTS response will always be sent, redirecting the plain HTTP connection to HTTPS. Enabling HSTS requires a HTTP server restart.
2. The default HTTP port number is 80 for root installations and 8080 for non-root installations. The default HTTPS port number is 443 for root installations and 8443 for non-root installations. If a default port is in use, SecureTransport displays a message and you must change the **Port** to use a port number other than the default setting.
3. If you enabled HTTPS, select an **SSL Key Alias** from the drop-down list, for example, **httpd**.
4. If you enabled HTTPS, to restrict HTTPS connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** checkbox.
5. Click **Start**.

Configure AS2 servers

If an AS2 license is available, enable the AS2 service. Specify the AS2 settings on both SecureTransport Server and SecureTransport Edge.

1. Select **Enable AS2 (non-SSL)** and/or **Enable AS2 (SSL)**. If you select **Enable AS2 (SSL)**, by default **Enable HSTS** will also be selected. You can also deselect **Enable HSTS** once **Enable AS2 (SSL)** is selected. When HSTS is enabled, a HSTS response will always be sent, redirecting the plain AS2 connection to SSL. Enabling HSTS requires a AS2 server restart.
2. Enter a port for each protocol you enabled.
3. If you enabled AS2 (SSL), select an **SSL Key Alias** from the drop-down list.
4. If you enabled AS2 (SSL), to restrict AS2 (SSL) connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** checkbox.
5. In the **AS2 Shutdown Port field,** enter a shutdown port for AS2 server.
6. Click **Start**.

Configure SSH servers

If you are using SSH, specify the SSH settings for both the SecureTransport Edge and SecureTransport Server.

1. Select **Enable Secure File Transfer Protocol (SFTP)** and/or **Enable Secure Copy (SCP)**.
2. Enter a port to assign.

3. If the operating system SSH server is using port 22, assign a different port number. To avoid a port conflict, you can disable SSH at the OS level or assign it a different port number instead of changing the port number in SecureTransport. By default, the operating system SSH port for Axway appliances is 10022.
4. Select an **SSH Key Alias** from the drop-down list.
5. To restrict SSH (SFTP/SCP) connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** checkbox.
6. Click **Start**.

To view the SSH Server Public Key Fingerprint, click **View Fingerprint**.

Note **View Fingerprint** does not work until a key alias has been assigned and the page is updated.

Configure PeSIT servers

If you are using PeSIT, specify the PeSIT server settings for both the SecureTransport Edge and SecureTransport Server.

1. Select one or more of the PeSIT transmission options:
   - **Enable PeSIT over Plain Socket** – Select to enable non-secure PeSIT transfers.
   - **Enable PeSIT over Secured Socket** – Select to enable secure PeSIT transfers.
   - **Enable PeSIT over pTCP Plain Socket** – Select to enable non-secure PeSIT transfers over pTCP.
   - **Enable PeSIT over pTCP Secured Socket** – Select to enable secure PeSIT transfers over pTCP.
   - **Enable PeSIT over Secured Socket (Legacy)** – Select to enable transfers with remote partners using SSL Legacy.
   - **Enable PeSIT over Secured Socket (legacy § comp)** – Select to enable the automatic detection of the used SSL/TLS mode (Legacy or Comp) when SecureTransport acts as a server.
2. If you are not using the default port, type a port for each option you selected.
3. If you enabled either SSL option, select an **SSL Key Alias** from the drop-down list.
4. If you enabled either SSL option, to restrict PeSIT SSL connections to FIPS 140-2 Level 1 certified cryptographic libraries, select the **Enable FIPS Transfer Mode** checkbox.
5. Click **Start**.

For information about more PeSIT settings, refer to the *SecureTransport Administrator's Guide*.

Start the Transaction Manager server on SecureTransport Server

The Transaction Manager (TM) server runs on SecureTransport Server. To start it, click the corresponding *Actions* dropdown list and select **Start**.

Start the Monitor server

The Monitor server checks that the SecureTransport services are running and restarts them if they terminate. However, the Monitor server does not restart a service if a dependent service is not running. The Monitor server can run on SecureTransport Server or SecureTransport Edge.

To start it, click the corresponding **Start** button.

Configure the Proxy Server on SecureTransport Edge

On the SecureTransport Edge, specify the port for the SecureTransport proxy server. The proxy port is used by SecureTransport Server to handle outgoing connections passed through a SecureTransport Edge.

1. Enter a port number to assign for a **Proxy Port**.
2. Click **Start**.

For the remaining proxy configuration on the SecureTransport Server and the SecureTransport Edge, refer to the *SecureTransport Administrator's Guide*.

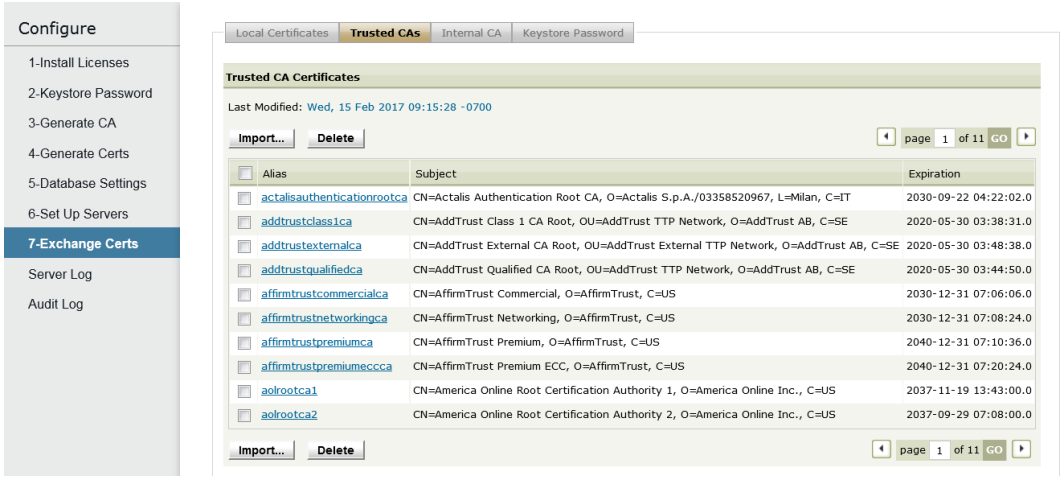
Exchange CA certificates 9

The Setup step 7 pertains only to a two-tier architecture, where both a SecureTransport Edge and SecureTransport Server are being configured.

In a two-tier deployment, the SecureTransport Edge and SecureTransport Server authenticate each other through the use of certificates. These certificates have already been created and specified in previous steps. In this step, a trust relationship between the two servers must be set up. This setup involves exchanging certificates between SecureTransport Edge and SecureTransport Server.

To complete this step, you must be able to access both the SecureTransport Server and SecureTransport Edge Administration Tool. Use a separate browser window to open each Administration Tool.

Note When you log in to the Administration Tool using the admin account, you can access this page by selecting **Setup > Certificates > Trusted CAs**.

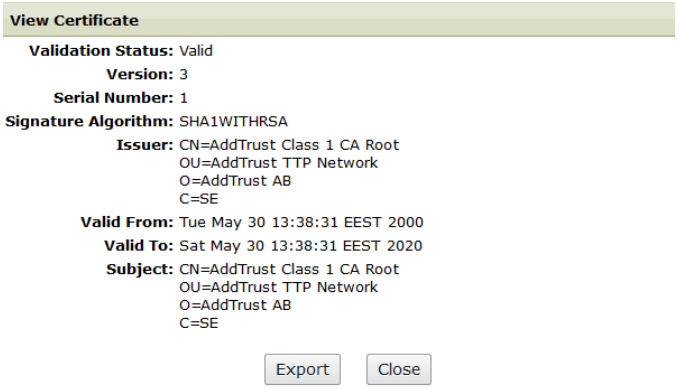


Export the SecureTransport Server or Edge CA certificate

Use the following steps to export the CA certificate from the SecureTransport Server or Edge.

1. Go to **Configure > 7-Exchange Certs**.
2. From the list of trusted CAs, click the alias that matches the CA certificate set up for the SecureTransport Server or Edge in **Configure > 2-Generate CA**.

   The *View Certificate* dialog box is displayed.



3. Click **Export** in the *View Certificate* dialog box.
4. Save the file to a location in the local system.
5. Click **Close**.

If necessary, you can import the CA certificate file to Edge (or SecureTransport Server, where applicable).

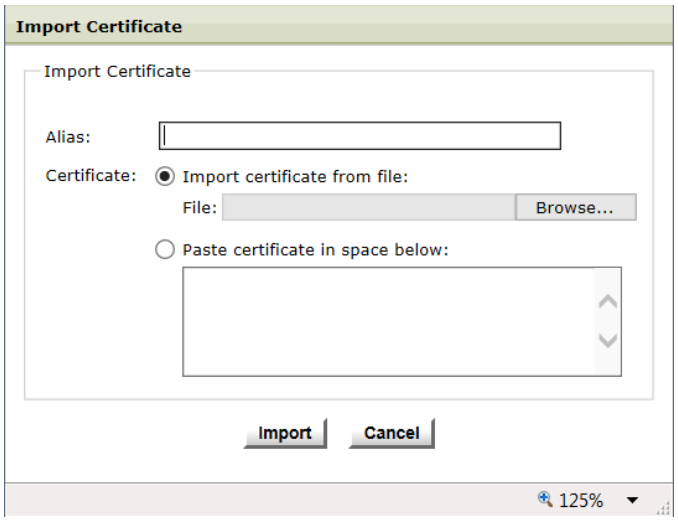
Import the SecureTransport Server or Edge CA certificate

A X509 certificate can be imported as a trusted CA in the form of a X509 DER or PEM encoded file. Make sure the certificate is valid and configured to validate certificates before you import it. The CA attribute in the X509v3 extension section of the certificate must be true.

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

Use the following steps to import the CA certificate from the SecureTransport Server to the SecureTransport Edge or vice versa.

1. Go to **Configure > 7-Exchange Certs**.
2. Click **Import**. The *Import Certificate* dialog box is displayed.



3. Enter an **Alias** for the imported certificate. Ensure the alias is unique and different from any other trusted CA aliases
4. To import the certificate file:
   a. Select **Import certificate from file** and click **Browse** to locate the file on your local system.

      Or select **Paste certificate in space below** to copy and paste the certificate contents.

   b. Click **Import** to import the certificate to the Edge server.
5. Click **Close** in the *Import Certificate* dialog box.

   The newly imported certificate appears in the **Trusted CA Certificates** list.

The following topics provide how-to instructions for importing and exporting SecureTransport Server and Edge CAs:

- *Export the SecureTransport Server CA certificate* on page 1 - Provides how-to instructions for exporting the SecureTransport Server CA certificate.
- *Import the SecureTransport Server CA certificate* on page 1 - Provides how-to instructions for importing the SecureTransport Server CA certificate.
- *Export the SecureTransport Edge CA certificate* on page 1 - Provides how-to instructions for exporting the SecureTransport Edge CA certificate.
- *Import the SecureTransport Edge CA certificate* on page 1 - Provides how-to instructions for importing the SecureTransport Edge CA certificate.

Clean up the default administrative credentials 10

The initial configuration of SecureTransport is now complete. As a final step, clean up the default administrative credentials either by changing the password or by deleting the administrator accounts that are not required. You can use the master administrator account for additional configuration tasks.

1. Log out of the Administration Tool.
2. Log in using the default user name, `admin` and default password `admin`.
3. Change the default password for the `admin` account.
4. Select **Accounts > Administrators**.
5. For each of the accounts: `account`, `setup` and `application`, take one of the following actions to improve security:
   - Remove the account by clicking the checkbox next to it and then **Delete**.
   - Change the password for the account by clicking the administrator entry and setting the desired password in the *Administrator Account Status* panel.
6. Change the default password for the `dbsetup` administrator account. It is stored on the filesystem and not in the database so that `dbsetup` can log in to the Administration Tool when the database is not running.

For more information on the **Accounts > Administrators** settings, refer to the *SecureTransport Administrator's Guide*.

Note Once you have made the configuration changes using the Administration Tool, run `stop_all` to stop all SecureTransport services, then run `start_all` to restart them. For information on stopping and starting SecureTransport services, refer to the *SecureTransport Administrator's Guide*.

Setup test 11

To test your setup, follow these simple steps:

1. Create a test account
2. Access test account
3. Transfer test file
4. Verify file transfer

Create test account

The first task to test the SecureTransport installation and initial configuration is to create a test user account.

1. Log into the Administration Tool as an administrator.
2. Select **Accounts > User Accounts**.
3. Click **New Account**.

   The *New User Account* page is displayed. The New User Account page shown is from a SecureTransport instance running on Windows. The *Real Users* field is the *UID* field for a SecureTransport instance running on UNIX.
4. Enter or select the following information.

Configurable item	Enter or select
Account Name:	Test
Email Contact:	test@axway.com
Phone Contact:	[blank]
Account Type:	Unspecified
Business Unit:	No Business Unit
HTML Template:	ST Web Client
PeSIT Routing Mode:	Reject
Encrypt Mode:	Unspecified

Configurable item	Enter or select
File archiving policy	Default
Real User (Windows):	[blank]
UID (UNIX):	6000
GID:	7000
Current Home:	
Change Home To*:	c:\home\users\Test
Change Home To* (UNIX):	/home/users/Test
Home Folder Access Level:	Private
Notes:	[blank]
Adhoc Settings	
Delivery Method:	Default
Login Settings:	[checked]
Login Name:	Test
Allow this account to login by email	[unchecked]
Allow this account to submit transfers using the Transfers RESTful API	[unchecked]
Password is stored locally (not in external directory)	[checked]
New Password*:	axway
Re-enter Password*:	axway
Require user to change password on next login	[unchecked]
Require user to set new secret question on next login	[unchecked]
Password Settings:	
Require user to change password every ___ days	[blank]

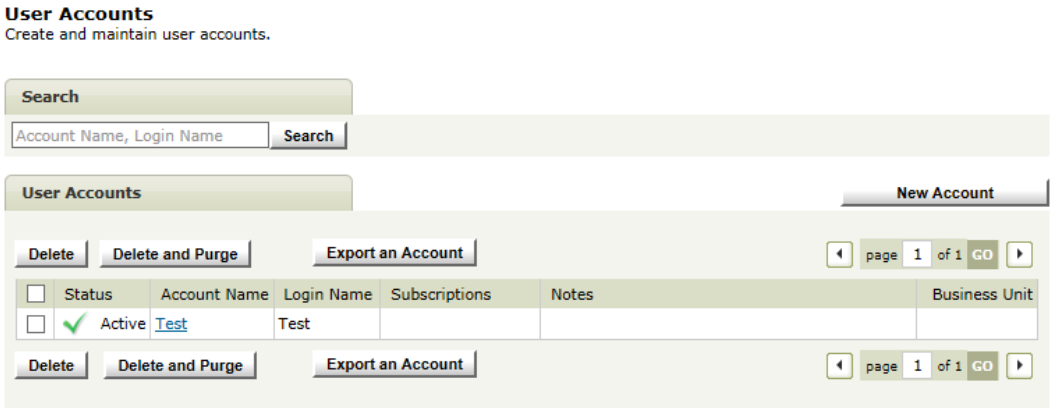
Configurable item	Enter or select
Lock account after ___ failed login attempts	[blank]
Lock account after ___ successful logins	[blank]
Additional Attributes	
Add Attribute	
Attribute	userVars.1
Value	test2@axway.com

5. Click **Save**.

   The *User Account: Test* page is displayed.

6. Click **Close**.

   Observe that the **Test** user account was added to the *User Accounts* page.



Access test account

The second task is to access the test account using the ST Web Client.

1. From your Internet browser, enter the HTTPS address to the SecureTransport installation using the IP address of the SecureTransport installation.

   Note If the default port (443) is used for HTTPS protocol, it is not necessary to enter the port number since it is the standard port for the HTTPS protocol. If a non-standard port number is used for HTTPS protocol, you must enter the port number.

2. Following the instructions for your browser, add a certificate exception for the ST Web Client instance.

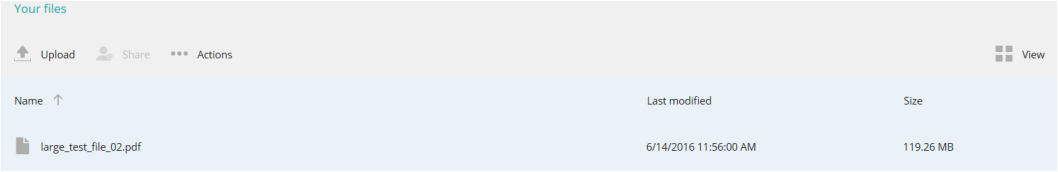
   The *ST Web Client Login* page is displayed.

3. Enter **User ID:** *Test* and **Password:** *axway*.
4. Click **Log in**.

Transfer test file

The third task is to transfer a test file.

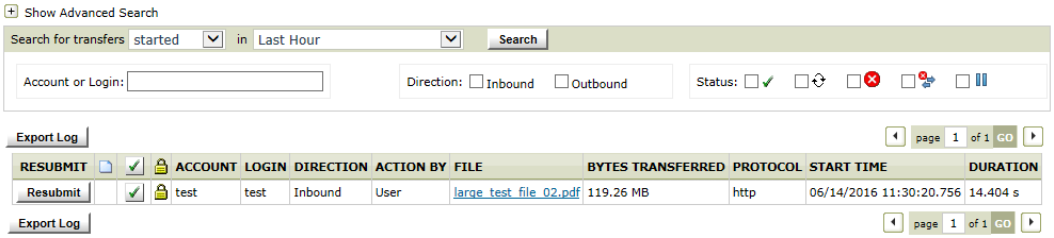
1. Click **Upload**.
2. Navigate to a test file to upload and click **Open**.
3. Verify that the test file appears on the *Your files* list.



Verify file transfer

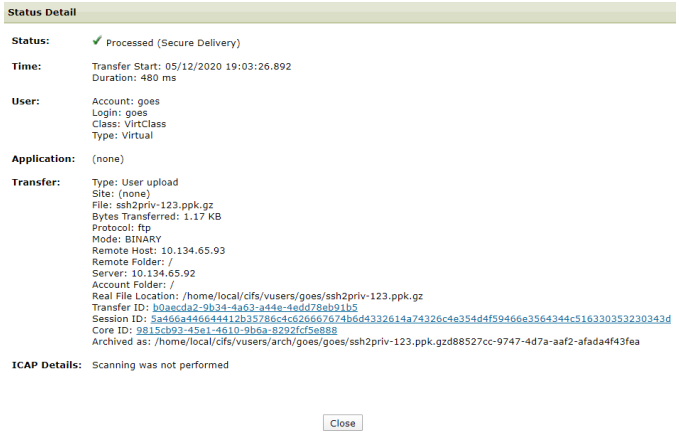
The fourth and final task is to verify the file transfer.

1. Log in to the SecureTransport installation as an administrator.
2. Navigate to **Operations > File Tracking**.
3. Verify that the test file was successfully uploaded.



4. Click the Check icon (✓) or click the **File Name** to review the details of the file transfer.

   The *Status Detail* page is displayed.



Status Detail

Status: ✔ Processed (Secure Delivery)

Time: Transfer Start: 05/12/2020 19:03:26.892
Duration: 480 ms

User: Account: goes
Login: goes
Class: VirtClass
Type: Virtual

Application: (none)

Transfer: Type: User upload
Site: (none)
File: ssh2priv-123.ppk.gz
Bytes Transferred: 1.17 KB
Protocol: ftp
Mode: BINARY
Remote Host: 10.134.65.93
Remote Folder: /
Server: 10.134.65.92
Account Folder: /
Real File Location: /home/local/cifs/vusers/goes/ssh2priv-123.ppk.gz
Transfer ID: b0aecda2-9b34-4a63-a44e-4edd78eb91b5
Session ID: 5a466a446644412b35786c4c626667674b6d4332614a74326c4e354d4f59466e3564344c516330353230343d
Core ID: 9815cb93-45e1-4610-9b6a-8292fcf5e888
Archived as: /home/local/cifs/vusers/arch/goes/goes/ssh2priv-123.ppk.gzd88527cc-9747-4d7a-aaf2-afada4f43fea

ICAP Details: Scanning was not performed

Close

5. Click **Close** when you are finished reviewing the transfer status details.

Additional configuration tasks

12

You must complete the SecureTransport configuration using the Administration Tool menus available to the `admin` user. Among the next configuration tasks you might need to perform are:

- Configure Transaction Manager server and SecureTransport Edge protocol server and proxy communication
- Configure your Standard Cluster or Enterprise Cluster
- Configure the FTP, AS2, SSH and PeSIT servers
- Set up integration with your LDAP server, CA SiteMinder, or Axway Sentinel
- Create additional user and service accounts

For information on these and other configuration and maintenance tasks, refer to the *SecureTransport Administrator's Guide*.