Secure Data

Integration Guide

Utimaco Atalla HSMs

utimaco®

Imprint

Copyright 2020	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	06/10/2025
Status	**PUBLISHED**
Document No.	IG-2025-0017

Table of Contents

1 Legal notices

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Except as specifically indicated otherwise, this document contains confidential information and a valid license is required for possession, use or copying. If this work is provided to the U.S. Government, consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

2 Trademark notices

Third-party brand and product names (including logos and icons) mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective owners.

3 Installing SecureData with Utimaco Atalla HSMs

A Hardware Security Module (HSM) is a physical device that can be installed on a network to derive cryptographic keys used to protect sensitive data. You can configure the Utimaco Atalla HSM to store the master secrets used to derive keys requested by SecureData key servers to protect and access data that is protected by SecureData. Keys derived from the master secrets are also used to protect sensitive data on the SecureData Management Console.

In addition to the Utimaco Atalla HSM, OpenText also supports Entrust nShield HSMs. A SecureData system can use either Atalla HSMs or nShield HSMs, but cannot use not both at the same time.

Atalla HSMs use a system image and configuration files designed specifically to work with

SecureData. After installing and configuring the Atalla HSMs, you configure the SecureData Appliances in your system to communicate with the HSMs. When communication is established, use the SecureData Management Console to create an Atalla HSM district.

Creating an Atalla HSM district initiates requests to create master secrets for cryptographic algorithms, including FPE, FFX, AES, IBE BF and IBE BB1. The request for creating master secrets is sent to the HSM via the Atalla HSM Connector. The Atalla Key Block (AKB) responses, returned by the HSM, contain the secrets encrypted with the Atalla HSM MFK (Master File Key). These secrets are stored in encrypted format in the SecureData Appliance.

When requests for keys are sent to a key server, it retrieves the encrypted secrets and any required public parameters from the SecureData Appliance. The key requests are then sent to the Atalla HSM via the Atalla HSM Connector. The HSM responses are returned to the Atalla HSM Connector, which routes them back to the key server from which the request

3.1 HSMs and SecureData

Hardware Security Modules (HSMs) are optional with SecureData, and provide an additional level of security in managing SecureData encryption keys. SecureData supports a limited set of off-cloud HSMs, and does not support current cloud HSMs.

When HSMs are integrated with the Key Servers, Master Secrets for the Security District—used to derive all keys for that Security District—are always encrypted by the HSMs. This means that keys for that Security District cannot be derived without connection to those HSMs. When HSMs are not used, Master Secrets are stored in the configuration database, encrypted by a Field Encryption Key (FEK).

In off-cloud, non-HSM deployments, FEKs are stored on the file system, meaning that a copy of the file system, VM, or container is sufficient to set up a Key Server that can derive customer keys.

With supported cloud service providers (CSPs), the FEK is stored in a native cloud key vault, with access controlled by appropriate cloud security administrators. This prevents an attacker using a copy of the file system, VM, or container to decrypt the configuration database and derive keys, because they will have no access to the FEK in the CSP's key vault.

However, this does not provide total protection from attack. SecureData administrators must be able to back up the configuration, including the Key Server, any time a configuration change is made, to allow recovery if the systems running the Key Servers are lost. This backup is initiated from the Management Console interface, and protected by a password, which the administrator records for use should a restore become necessary. Because SecureData can be used in a combination of off-cloud installation and one or more CSPs, such a backup must be usable on a system with no access to the cloud key vault, even if the backup was initiated from a cloud instance. This means that an attacker with a backup from a Management Console (and the password used for that backup) can use that backup to set up their own Key Servers and has the potential to derive customer keys.

When an HSM is in use, however, the Master Secrets are protected by the HSM, and are not directly available in the backup. Without access to the configured HSM, a Key Server, built from a backup obtained by an attacker, cannot be used to derive keys for those HSM-protected districts.

Because an HSM provides this additional level of protection, it is recommended, especially for cloud deployments, to use an HSM with SecureData. If an HSM is not used, customers must implement strict protocols to reduce the risk of an attacker gaining access to a backup (and password).

3.2 Getting Started

Before you begin the installation and configuration of an SecureData Appliance that uses an Atalla HSM, make sure you have access to the required equipment and documentation, and that the required infrastructure is in place.

3.2.1 Network TLS 1.2 Connection to SDA

SecureData 7.0.0 (and later) requires TLS 1.2 for communications between HSMs and SecureData services.

3.2.2 Redundancy

For redundancy, you can optionally configure multiple HSMs for a SecureData server.

To ensure the HSMs can act as clones of one another, all Atalla HSMs used by the SecureData server must be of the same type, running the same Atalla software version, and contain the same Master File Key (MFK).

3.2.3 Equipment

You must have access to the following equipment:

- Utimaco Atalla HSM AT1000 hardware, version 8.50

The Utimaco Atalla Ax160 HSM hardware is no longer supported by the manufacturer. Previous releases of SecureData Appliance function with these devices, and Version 7.0.1 is expected to function as well; however, no validation testing was done. We encourage you to work with your vendor to upgrade the HSM or to migrate your HSM data to a supported HSM version as soon as possible after upgrading to SecureData 7.0.1.

- Cables to connect the Utimaco Atalla HSM hardware to power and networking
- Medeco keys for opening the Atalla HSM front panel
- USB flash memory device (optional)
- Windows computer
- HP ElitePad tablet running Secure Configuration Assistant-3 (SCA-3) version 3.0
- (Optional) Docking station for the SCA-3 tablet
- Power cable for either the SCA-3 tablet or docking station
- Utimaco Atalla Secure Keypad (ASK)
- Cable to connect the ASK to the SCA-3 tablet or docking station
- Cable to connect the SCA-3 tablet or docking station to your Windows computer (if you are using the Remote Management Utility) or directly to the Atalla HSM
- At least three security administrator smart cards

- SecureData Appliance version 6.8.2 or later

3.2.4 Documentation

The instructions in this manual refer to the following Atalla and SecureData documentation:

- *Read Me First: Atalla HSM AT1000*
- *Installation and Operations Guide for the Atalla HSM AT1000* (chapters 3, 4, and appendix B)
- *Atalla Secure Configuration Assistant-3 User Guide*
- *SecureData Appliance Installation Guide* (chapters 1 and 2)

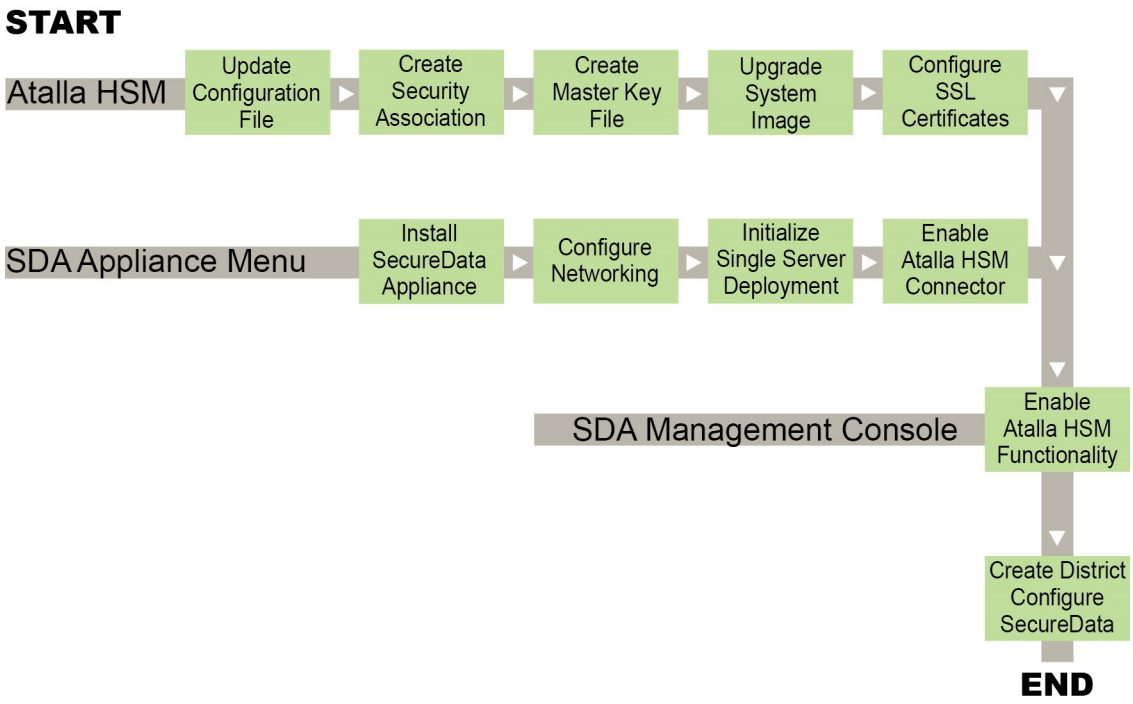
3.2.5 Infrastructure

The instructions in this manual assume that your infrastructure includes the following:

- Power and networking are available to each SecureData Appliance.
- Power and networking are available to each Atalla HSM used with the SecureData Appliance.
- An IP address has been allocated for each SecureData Appliance and each Atalla HSM
- (Optional) If you are using the SCA-3 Remote Management Utility on your Windows computer, the firewall rules allow a connection between the Windows machine and the Atalla HSM.
- Purchase the appropriate license (there are 3 tiers: 280 TPS, 1080 TPS, and 10,000 TPS)

3.2.6 Workflow

The following diagram shows the workflow for the installation and configuration steps.



3.3 Atalla AT1000 HSM Version 8.50

Firmware Version 8.50 for Utimaco Atalla AT1000 HSM includes configuration adjustments to caching made specifically to improve performance with SecureData. OpenText recommends version 8.36 or later of Atalla AT1000 firmware for use with SecureData. For information on upgrading Atalla firmware with SecureData 6.x, see Migrate SecureData (to 7.0.0) With Atalla Software version 8.30 or later.

SecureData 6.8 and AT1000 8.30 are the minimum required versions for AES districts support. However, OpenText recommends AT1000 version 8.36 or later for better performance.

3.3.1 Configure for Version 8.50

With firmware version 8.50, there are two configuration setting changes to make.

- Set the number of sockets according to the number of Key Servers in your SecureData deployment. The number of sockets are set in the Atalla HSM Connector Configuration Menu in the SecureData Main Menu (vsappconfig). See Configure the SecureData Appliance.

- Update the `MAX_CLIENTS_ASCII=` parameter of the config.prm file to specify 64. See Update the Configuration File.

4 Prepare the Atalla HSM

Before you begin configuring the SecureData software to work with one or more Utimaco Atalla HSMs, configure each HSM as described in the Atalla HSM documentation. The information in this section includes specific instructions that you follow instead of or in addition to those provided in the following Atalla manuals:

- *Read Me First: Atalla HSM AT1000*
- *Installation and Operations Guide for the Atalla HSM AT1000*
- *Atalla Secure Configuration Assistant-3 User Guide*

4.1 Overview

Complete the following high-level steps to prepare each Atalla HSM for use with SecureData. This process assumes that you have already followed the instructions in Chapter 3, "Hardware Installation" in the *Installation and Operations Guide for the Atalla HSM AT1000 manual*.

1. Obtain the configuration and documentation files from the OpenText Software Support website.
2. Update the configuration file and copy it to the USB device.
3. Create the security association and an Master File Key (MFK). If your AT1000s are running version 8.30 and later, you must create an MFK with AES encryption (AMK).
4. If you need to copy image and certificate template files to the Atalla HSM USB device, see the `Atalla_HSM_AT1000_UserDocs_v8.XX.zip` file for information.
5. Configure SSL on the Atalla HSM for mutual authentication with the SecureData Appliance.
6. If you are upgrading or have already upgraded AT1000(s) to software version 8.30 or later, see Migrate SecureData (to 7.0.0) With Atalla Software version 8.30 or later for important information on the upgrade process.

4.2 Get Atalla HSM Files

To configure the Atalla HSM, you must edit the `config.prm file`. You must download the `config.prm` configuration file and documentation from the Utimaco Support website. An Utimaco Support account is required.

4.3 Update the Configuration File

Follow the instructions in the “Software Configuration” chapter of the Installation and Operations Guide for the Atalla HSM AT1000. Use a text editor, such as notepad, to update the [TCPIP] section of the `config.prm` file.

The [STARTUP] section of the config.prm file must include the IMAGE=A8.XX parameter, where XX is the version you are configuring.

- Update the `IPADDR=` parameter to specify the IP address of the Atalla HSM.
- Update the `NETMASK=` parameter to specify the IP subnet mask, which controls the range of

host IP addresses for the Atalla HSM.

- Update the `GATEWAY=` parameter to specify the IP address of the gateway for the SecureData Appliance if it is on a different network than the Atalla HSM.
- Update the `PORT_ASCII=` parameter to specify the port number at which the Atalla HSM will accept commands. The preset value is 7000.
- Update the `MAX_CLIENTS_ASCII=` parameter to specify how many connections can be opened between all SecureData Appliances and the Atalla HSM. Use the default value of 16 if you have a maximum of 3 Appliances. Increase this value by 5 for each additional Appliance that will connect to the Atalla HSM. OpenText recommends the maximum value of 64.

If you are connecting to Atalla AT1000 HSMs with firmware version 8.36, set this value to 64.

- (Optional) Update the preset `RECONNECT=no` parameter value to RECONNECT=yes to allow faster reconnection from a specific Appliance in the event of network connectivity issues.
- Update the `PORT_STATUS=` parameter to specify the port number to which system log files and error files are written. This parameter does not have a default value. The preset value is 7001.
- Update the `PORT_MANAGEMENT=` parameter to specify the port number on which the HSM will accept management commands from a remote SCA-3. The preset value is 7005.

- Make sure that the `PROTOCOL_ASCII=TLS` and `REQUIRE_CLIENT_CERT=yes` parameters are included.
    - Add the `ALLOWIP= parameter` to limit the IP addresses that can access the Atalla HSM. You must include the IP address of the Appliance that runs the Management Console, and all remote host Appliances that run Key Servers. For example, if your system includes a dedicated Management Console and two Key Servers, you must specify the three IP addresses for the ALLOWIP= parameter. Separate each IP address with a comma and space, as shown in the following example.
    `ALLOWIP=192.168.1.20, 192.168.1.21, 192.168.1.22`

After you update the file with the information required for connecting with the SecureData Appliance, save the file to the Atalla HSM USB device. You must use config.prm as the file name.

Example of the `config.prm` File

```
[[CONFIG]]

[STARTUP]

IMAGE=A8.50

[TCPIP]

IPADDR=192.168.1.100

NETMASK=255.255.0.0

GATEWAY=192.168.1.1

PORT_ASCII=7000

MAX_CLIENTS_ASCII=64

RECONNECT=no

PORT_STATUS=7001

PORT_MANAGEMENT=7005

PROTOCOL_ASCII=TLS

REQUIRE_CLIENT_CERT=yes ALLOWIP=192.168.1.20, 192.168.1.21, 192.168.1.22

[[SNMP]]

[SNMP]
```

```
[[LOG]]

[LOG]
```

4.3.1 Copy the Configuration File to the USB

To copy the configuration file:

1. Insert the USB flash memory device in the Windows computer that contains the files downloaded from the OpenText Software Support website.
2. Copy the modified `config.prm` file to the root directory of the USB flash memory device.
3. Use the front panel key pad to enable the USB port.
4. Insert the USB device into the USB port located next to the power and system health LEDs.
5. Confirm you want to transfer the config.prm file. It is uploaded to the server and new configuration is set.
6. Confirm and remove the USB when prompted by the Front Panel LCD.
7. Confirm the new IP addresses are correct via the Front Panel LCD.

4.4 Create Security Association and Master File Key (MFK)

Before an Atalla HSM can work with SecureData, you must create the security association with at least three security administrator smart cards. This procedure requires a Secure Configuration Assistant-3 (SCA-3) that is connected to an Utimaco Atalla Secure Keypad (ASK), and a set of at least three security administrator smart cards. You can connect the SCA-3 directly to an Atalla HSM, or you can connect it to a Windows computer using the Remote Management Utility for a remote connection to the Atalla HSM.

If you are using the Remote Management Utility on a Windows computer that is on a different network than the Atalla HSM, you might need to open the port used for communication to the SCA-3 (as specified by the PORT_MANAGEMENT= parameter of the config.prm file) on your firewall.

See Chapter 2, “Connect the SCA-3 to an HSM or personal computer” in the *Atalla Secure Configuration Assistant-3 Users Guide* for details.

After creating the security association, you can create the Master File Key (MFK) using at least two of the security administrator cards.

OpenText recommends creating the MFK using AES encryption. If you have upgraded your Atalla AT1000(s) to version 8.30 or later, you MUST create an AES MFK (AMK) before you can upgrade SecureData to version 6.8 and later. See Migrate SecureData (to 7.0.0) With Atalla Software version 8.30 or later.

Detailed instructions for creating the security association and MFK are available in chapters 3 and 4 of the Atalla Secure Configuration Assistant-3 Users Guide. The following steps provide an overview of the sections that you must complete. The name of the step corresponds to the title of the section.

1. Personalize the smart card.

   This sub-section is in Chapter 3, “Initialize the HSM.” Follow the instructions in this sub-section to enter a user name and PIN for at least three security administrator smart cards. This step is successfully completed for each card when the PIN is required each time the card is inserted into the Atalla Secure Key Pad.

2. Do one of the following:

   - Create the security association and define the SCA use policy

     This sub-section is in Chapter 3, “Initialize the HSM.” Follow the instructions in this subsection if this is the first Atalla HSM being installed in an environment. This step is successfully completed when the SCA-3 displays the following:

     Create New Security Association Transaction Results:

     The security administrator smart card was successfully added to the new security association!

     The connected HSM was successfully added to the new security association

   - Add a HSM to a security association.

This sub-section is in Chapter 3, “Initialize the HSM.” Follow the instructions in this subsection if this is not the first Atalla HSM being installed in the environment. This step is successfully completed when the SCA-3 displays the following:

> Add HSM to Security Association Transaction Results:
>
> The connected HSM was successfully added to the existing security association

The security association cryptographically links security administrator smart cards to the Atalla HSM. The administrators who hold at least two of the administrator smart cards must be present to insert the card and enter the PIN.

3. HSM time adjustment.

   This sub-section is in Chapter 4, “Define the HSM security policy.” Follow the instruction in this sub-section to check the clock time on each Atalla HSM and adjust the time, if needed. This step is successfully completed when the HSM system time displays correctly when you tap the HSM status icon on the SCA-3.

4. Define the MFK key components.

   This sub-section is in Chapter 3, “Initialize the HSM.” Follow the instructions in this sub-section to define the MFK components and their values on the security administrator smart cards. The minimum number of key components that can be combined to form a MFK is two. The maximum number is equal to the number of security administrators that create the security association. After you define a component, the Atalla Secure Keypad displays the key component value. Record this value because this is the only time that the value is displayed in cleartext.

   This step is successfully completed for each card when the SCA-3 displays the component check digits for the key component.

5. Send a key component to the HSM

   This sub-section is in Chapter 3, “Initialize the HSM.” Follow the instructions in this subsection to push the MFK components from the security administrator smart cards to an Atalla HSM in the security association. Once the Atalla HSM has received the correct number of key components, it creates the MFK and check digits, and stores them in non-volatile memory.

This step is successfully completed when the SCA-3 Current Transaction window displays the following:

```
Send Key to HSM

Transaction Results:

The key was successfully defined in the HSM!

Key Type: MFK

Key Check Digits: <digit_value>
```

To ensure that encrypted SecureData master secrets generated on one Atalla HSM can be used on another, all Atalla HSMs in the cluster must contain the same MFK.

4.5 Backup Operator Group Smart Cards

After you have created the administrator smart cards, it is a good idea to create a set of Backup Operator Group smart cards so that a known state of the Atalla HSM can be quickly restored.

Security Administrators use their smart cards and the SCA-3 to create a Backup Operator Group.

The group contains a number of Backup Operator smart cards (2 to 20 cards) in the group. Each Backup Operator smart card receives a share of a secret key. Backup Operator Group configuration data consists of the security association, Master File Key (MFK), Pending Master File Key (PMFK) and the HSM security policy. Once the group is created, a file which is encrypted under the secret key containing the current HSM security policy is written to the encrypted hard drive on the HSM.

When it comes time to initialize a replacement HSM, the USB drive that has the file of the encrypted security policy is installed in the replacement HSM. When the HSM is powered on, the required number of Backup Operator smart card users use the SCA-3 to initialize the HSM.

For complete information on Backup Operator smart cards, refer to Chapter 6 of the *Atalla Secure Configuration Assistant-3 User Guide*.

On the first power-on, wait 10 minutes for the software update sequence to complete before attempting to establish communications with the Atalla HSM. After the initial successful software update, when the Atalla HSM is powered on, it will complete the system startup sequence in approximately 6-10 minutes.

4.6 Configure SSL

After you initialize the Atalla HSM and create the MFK, you must install a certificate signed by a Certificate Authority (CA) and the root certificate of the CA on each Atalla HSM. The SecureData Appliance requires TLS 1.2 for communication with the Atalla HSM. See the "TLS Configuration" appendix of the *Installation and Operations Guide for the Atalla HSM AT1000* for details about the files used in the following procedure.

If you are not in the same location as the AT1000 HSM, you can use the Remote Management Utility HSM File feature to move the files in this procedure between the Atalla HSM USB device and your Windows computer. See Chapter 8, "Remote Management Utility" in the *Atalla Secure Configuration Assistant-3 User Guide*. You can also use the Remote HSM Restart feature of the SCA-3 to restart the Atalla HSM. See the "Remote HSM Restart" section in Chapter 4 of the *Atalla Secure Configuration Assistant-3 User Guide*.

To configure SSL on Atalla HSM:

1. Receive the serverreq.pem file from the certificates_server directory on the RMU Manage Files tab and move it to a location where it can be signed by your CA.
2. Get the serverreq.pem file signed by your CA.
3. Open the signed server certificate in a Certificate Viewer application and display the CN= value, located in the Subject field. Make note of this value for use when configuring SSL for the Atalla HSM Connector service.
4. Send the signed server certificate to the file named servercert.pem in the certificates_server directory using the RMU. This requires confirmation from two or more Atalla security administrator cards.
5. Send the root certificate or chain of certificates, obtained from your CA, to a file named `trustedca.pem` in the certificates_ca folder using the RMU. This requires confirmation from two or more Atalla security administrator cards. The order of the certificates provided in a certificate chain is important. The certificate of the CA that signed the server

certificate must be the first certificate in the file, followed by Intermediate certificates in descending order. The last certificate in the file is the root CA certificate.

This step assumes that you use the same CA to sign the server certificate and the certificate generated by the SecureData Appliance.

6. Power cycle the Atalla HSM and wait 10 minutes for the system to start. The Atalla HSM system log will have messages similar to the following:

2017 Aug 24 22:23:39 [notice] - [Host Listener] Successfully processed

"config.prm" file

2017 Aug 24 22:23:39 [notice] - [Host Listener] Successfully copied

"config.prm" as "last-known-good-config.prm"

2017 Aug 24 22:23:39 [notice] - [System] Synchronizing server time and date with ACS

2017 Aug 24 22:23:42 [notice] - [System] Server time adjustment complete

2017 Aug 24 22:23:42 [notice] - [Host Listener] ACS Configuration process completed successfully.

2017 Aug 24 22:23:52 [notice] - [Host Listener] Atalla HSM has started successfully.

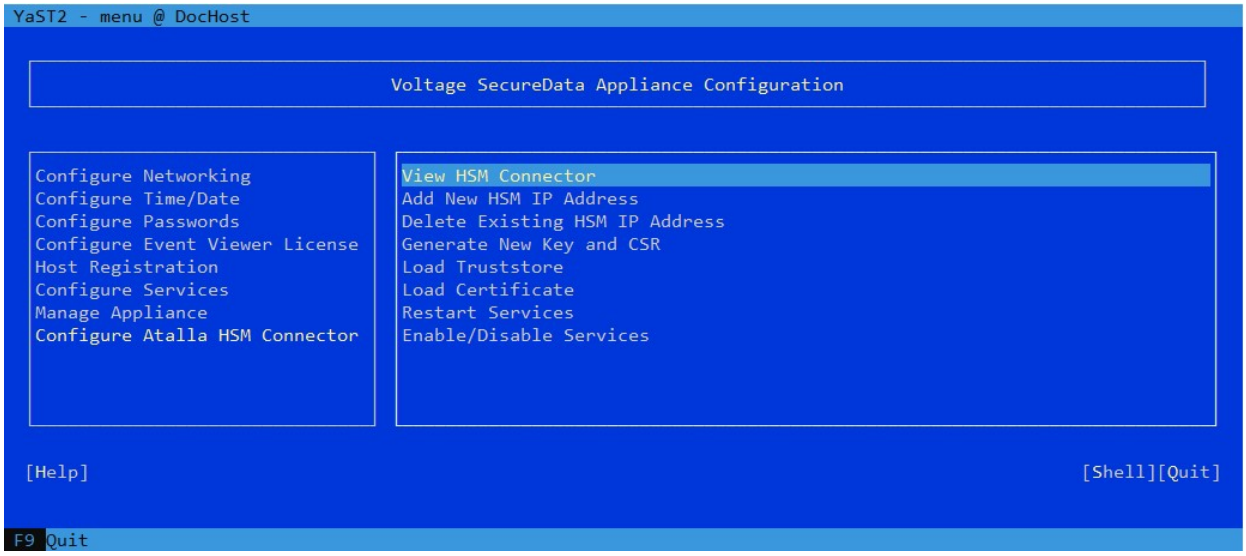
These messages indicate that you are ready to configure the SecureData Appliance.

5 Configure the SecureData Appliance

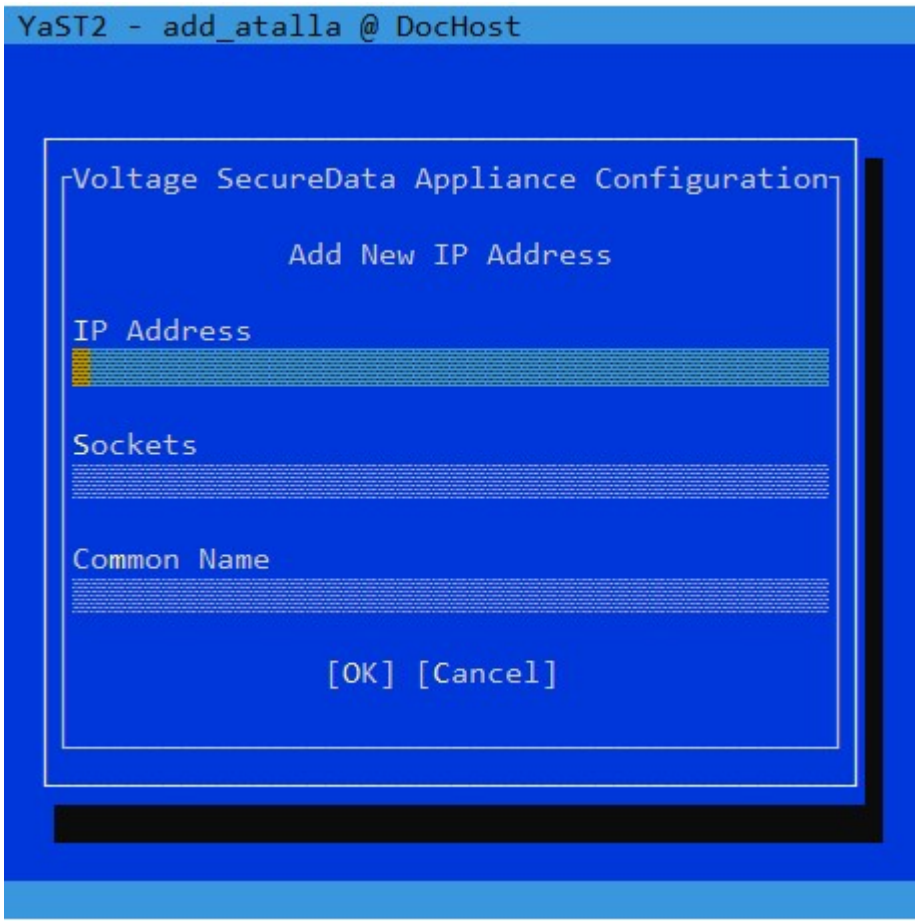
Communication between Utimaco Atalla HSMs and the SecureData Appliances is mediated by the Atalla HSM Connector. It distributes key requests from Key Servers to the HSMs in the cluster to ensure that the load is balanced among the HSMs. The Atalla HSM Connector also detects failed HSMs and redirects requests to the remaining active HSMs. Each SecureData Appliance includes the Atalla HSM Connector software, which is disabled by default.

To enable the Atalla HSM Connector service on the SecureData Appliance:

1. Complete all installation and configuration steps described in Chapter 1 and Chapter 2 of the *SecureData Appliance Installation Guide*.
2. On the Appliance running the Management Console, navigate to Configure Atalla HSM Connector.



3. Use Down Arrow key to highlight Add New HSM IP Address, and press Enter.



4. Type the IP address of the Atalla HSM.
5. Tab to the Sockets field, and enter the number of connections needed to the Atalla HSM at that address. Integers from 2 and 64 are valid. Do not configured more sockets than the value of `MAX_CLIENTS_ASCII` in the `config.prm` file of the HSM. See Update the Configuration File. If you are connecting to HSMs running firmware version 8.30 or earlier, set two sockets for each Key Server. If you are connecting to HSMs running firmware version 8.36 or later, refer to the table below to set the number of sockets.

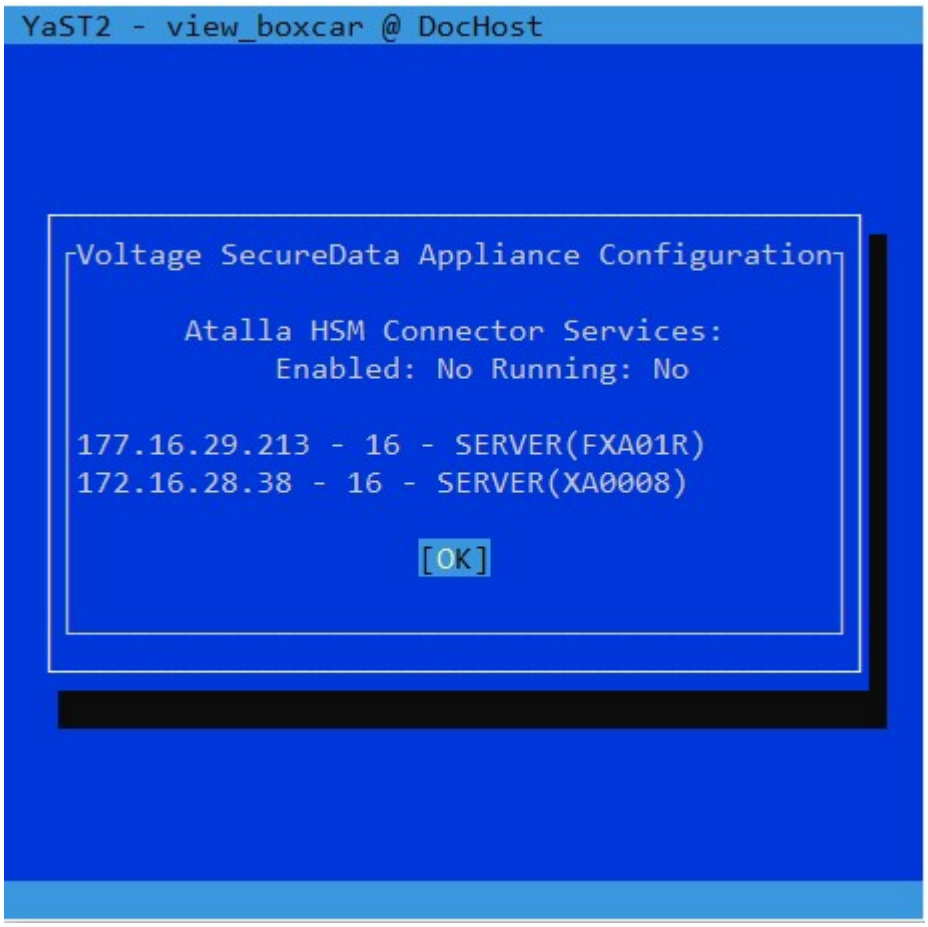
Number of Key Server(s)	1	2	3	4	5
If MC gets key requests	16	10	6	5	4

If MC does not get key requests	N/A	MC: 2 Others: 16	MC: 2 Others: 9	MC: 2 Others: 6	MC: 2 Others: 5

To ensure the HSMs can act as clones of one another, all Atalla HSMs used by the SecureData server must be of the same type, running the same Atalla software version, and contain the same Master File Key (MFK).

6. Tab to the `Common Name` field and enter the value (without any leading or trailing white spaces) obtained as the `CN= value` in the Atalla HSM server certificate, in Step 3 in the section Configure SSL, then choose OK.
7. On the dialog asking if you want to add another IP address, do one of the following:

- If you are configuring the Appliance to work with multiple Atalla HSMs, choose Yes, and then repeat Step 4 to Step 6 to enter the IP address, number of sockets, and Common Name for each Atalla HSM.
- If you have entered all of the required IP addresses, choose No to return to the Atalla HSM Connector IP Address Configuration Menu, which displays the list of all IP addresses and the associated CN value and number of sockets specified for each one.



- If you are replacing or upgrading an Ax160 to AT1000, perform the following steps to make sure the new Atalla HSM contains the same MFK to support the existing districts:
    a. Backup the MFK from the existing Ax160.
    b. Disable the **HSM** checkbox from the Management Console.
    c. Restart the vsmgmt service and deploy.
    d. Add the new Atalla IP address.
    e. Restore the MFK you backed up in step a to the new Atalla HSM.
    f. Enable the **HSM** checkbox from the Management Console.
    g. Restart the vsmgmt service and deploy.

8. Choose **Back** to return to the Atalla HSM Connector Configuration Menu. A message displays with a reminder to restart the Atalla Connector Services. However, you do not need to restart the services until after you have configured SSL settings.
9. Navigate to **Generate New Key and CSR**.

10. Enter the Distinguished Name for the certificate request. The DN field is pre-populated with the value `/CN=<host_name>`, where `<host_name>` is the Hostname value that you used in the **Configure DNS and Hostname** dialog when you initially configured the Appliance.
11. Choose **OK**, then choose **OK** again to dismiss the message that shows the location of the `atalla.csr` file.

12. Download the atalla.csr file from the /root/atalla directory of the Appliance.
13. Get the CSR signed by your CA and obtain a copy of the root CA certificate.

Make sure to sign the CSR with Client or Client/Server Purpose.

14. Upload the root CA certificate file to the following location on the Appliance:

    `/root/atalla/truststore.pem`

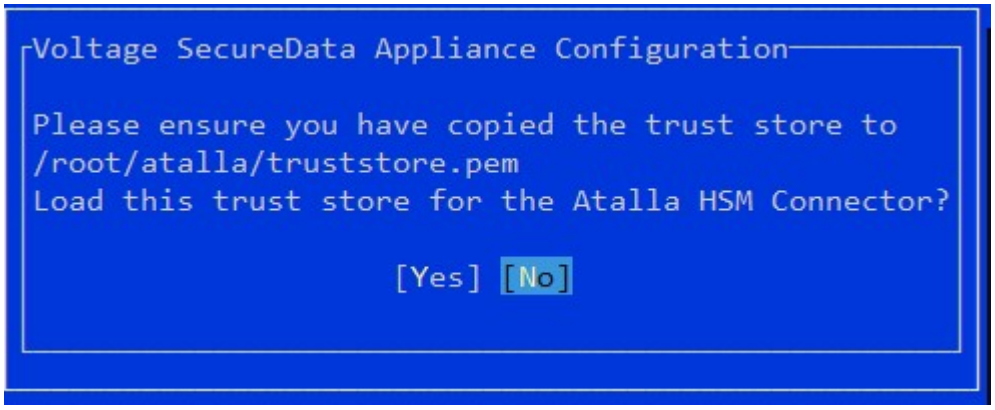
This step assumes that you use the same CA to sign the server certificate and the certificate generated by the SecureData Appliance.

- If you have a CA chain, you can include the CA chain in the truststore.pem in the following order:
    a. CA that signs the client certificate
    b. Intermediate certificates
    c. Root CA

15. Upload the signed certificate file to the following location on the Appliance:

`/root/atalla/atalla.cer`

16. Choose **Load Truststore**.



17. Choose **Yes** to confirm that the `truststore.pem` file is in the correct location and ready to be loaded, then choose No to dismiss the confirmation dialog.
18. Choose **Load Certificate**.

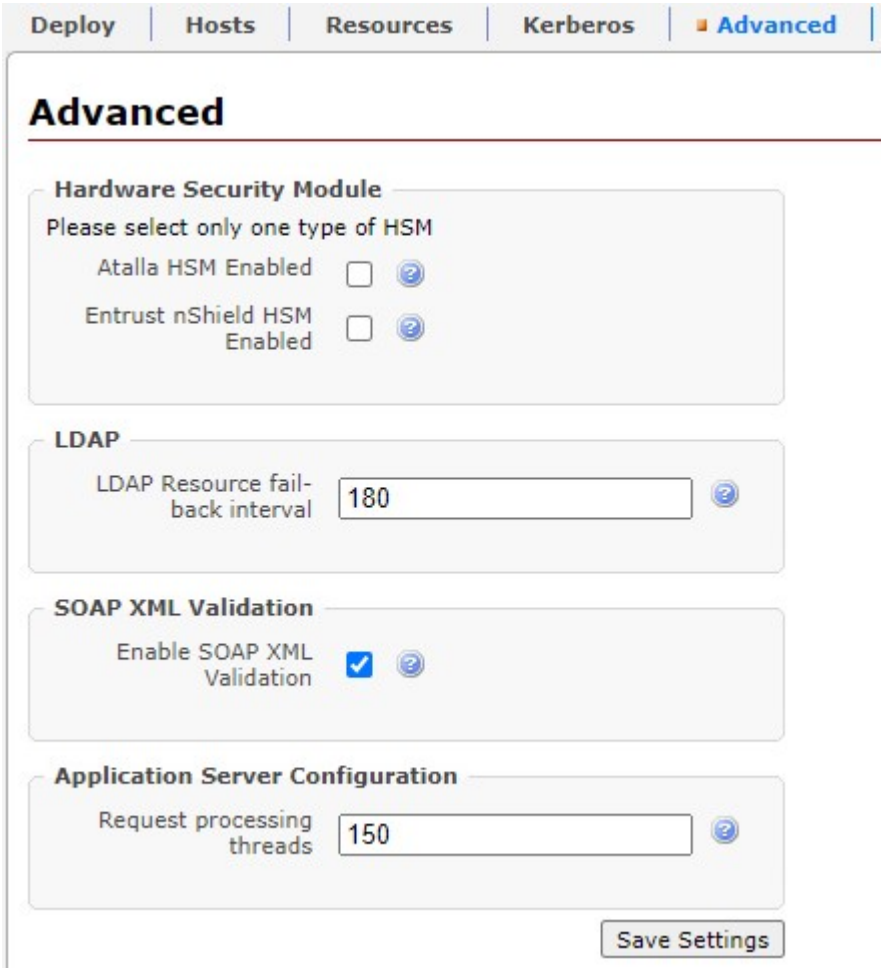
19. Choose **Yes** to confirm that the certificate is in the correct location and you are ready to load it for use with the Atalla HSM, then choose OK to dismiss the confirmation dialog.
20. Choose **Back** to return to the Atalla HSM Connector Configuration Menu
21. Choose **Enable/Disable** Services and then choose Yes to confirm that you want to enable Atalla HSM Connector services.
22. If you have not already done so, verify that the time on the Appliance is correct, and if needed, set the Date/Time manually or from the NTP server.
23. Complete Step 1 to Step 22 for each Appliance that serves as a remote host running a Key Server.

6 Enable Atalla HSM on the Management Console

Before you can create a district that uses the Utimaco Atalla HSM, you must enable it on the Management Console.

To enable SecureData to use an Atalla HSM:

1. Verify that each Key Server is connected to an Atalla HSM, as described in Configure the SecureData Appliance.
2. On the Management Console, navigate to the System > Advanced tab. The Advanced Configuration page opens.



3. Click the **Atalla HSM Enabled** check box.

You cannot enable this check box if the Entrust nShield HSM Enabled check box is already enabled. If any Entrust nShield districts already exist, you must remove them before you can enable Atalla HSMs.

This setting controls whether or not the Management Console and Key Server use the Atalla HSM for cryptographic operations. When enabled, the master secrets are stored in the HSM and are used to generate encryption/decryption keys that are sent directly to the client. After this setting is enabled, any new districts that are created use the HSM to generate the master secret key data.

This setting affects only the creation of new districts and whether the Management Console database settings are encrypted using the HSM. Key derivation operations in the Key Server for these districts also use the HSM. Enabling the Atalla HSM does not change existing software-based districts and they are not converted to be HSM districts. If any HSM districts are in the district list, the district list includes an HSM column to indicate which districts are HSM-based and which are software-based.

This setting also controls how the Management Console protects sensitive settings, such as shared secrets in its settings database. If Atalla HSM support is enabled, then these settings are encrypted using the Atalla HSM; otherwise they are encrypted in software.

If the Appliance on which the Management Console is running is not configured to use Atalla HSMs, then attempting to enable HSM support gives an error. If an HSM-enabled district is deployed to a remote host that does not support Atalla HSMs, an error occurs when attempting a key request for that district.

If the system was originally configured with the **Atalla HSM Enabled** check box disabled (unchecked), and an HSM-district is restored or imported, you must "bounce" (uncheck, save, check, save) the restored check box setting to ensure HSM FEK is being used. On the System > Advanced page, clear the **Atalla HSM Enabled** check box and click Save Settings, and then select the **Atalla HSM Enabled** check box and click **Save Settings**.

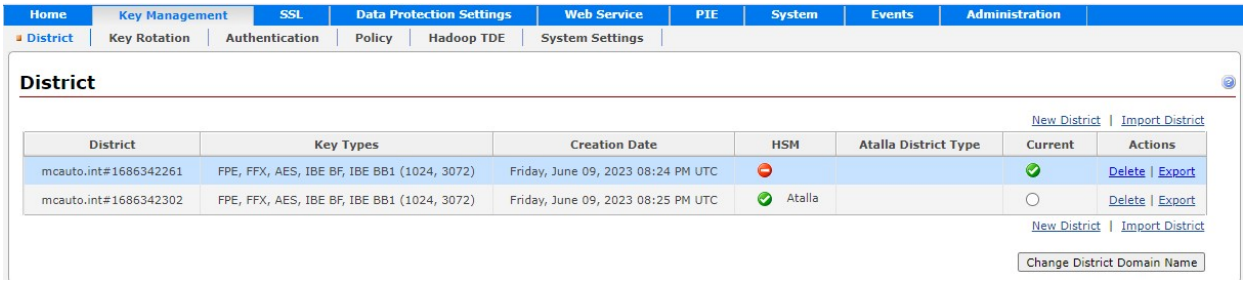
4. Click **Save Settings**.
5. Click the **Key Management** tab. The **District** page opens.
6. If your system does not have a district set, specify the domain name for the district, then click **Set District Domain Name**. If your system already includes a district, the district domain name is already set and you do not need to complete this step.

7. Click the **New District** link.

If the system already has an existing district, a message displays to confirm that you want to create a new district and to specify whether to set the new district as the current district.

Leave the "**Set the new district as current district**" check box selected, then click OK.

A message displays at the top of the District page, indicating that the new district is being generated. This process can take several minutes. When the process completes, the District page displays the new district. The page includes a column labeled HSM, showing that the district is for use with the Atalla HSM.



If the MFK is encrypted with **AES**, AES is displayed in the **Atalla District Type** column.

8. Complete the remaining initial configuration steps on the Management Console (creating an authentication method and obtaining an SSL certificate). See “Getting Started” in the *SecureData Administrator Guide* for details.

9. Click the **System** tab, then click **Deploy**.

You cannot successfully deploy a cluster unless an Atalla HSM is configured to work with every Appliance that has the Key Management service enabled.

6.1 Monitor HSM Status

After you have enabled Atalla HSM support, the Management Console begins monitoring the status of the HSM that it is connected to, as well as the status of each remote host that is configured to use the HSM. The initial status of each HSM is queried immediately after the HSM is enabled on the Management Console. After this initial query, each Appliance that is configured to use an HSM is contacted every 60 seconds, and the status of the HSM (which can be Available, Unavailable, or Failed) is logged as an event.

All HSM status changes are logged to the console.log, and are aggregated as events that can be queried, using the Events tab in the Management Console. See the *SecureData Administrator Guide* for the list of Management Console events.

6.2 Disable the HSM on the Appliance

The Management Console uses the HSM to protect the sensitive settings in its settings database while the HSM is in use. If the HSM is no longer needed, it still must be used one more time to decrypt these settings.

If you no longer want to use the Atalla HSM to derive SecureData keys, the HSM must remain connected until you have disabled the setting on the Management Console. To disable the setting:

1. Navigate to the **System > Advanced** page of the Management Console
2. Clear the **Atalla HSM Enabled** checkbox.
3. Click **Save Settings** to apply this setting.

The Management Console now uses keys from a non-HSM district to protect its settings. The Atalla HSM is no longer used, and can be disconnected from the SecureData system.

7 Migrate SecureData (to 7.0.0) With Atalla Software version 8.30 or later

SecureData 7.0.0 supports Utimaco Atalla HSM AT1000 hardware, version 8.50. Before you begin your migration to SDA to 7.0.0, review the SDA migration steps in the Installation Guide and review the HSM integration requirements in Getting Started.

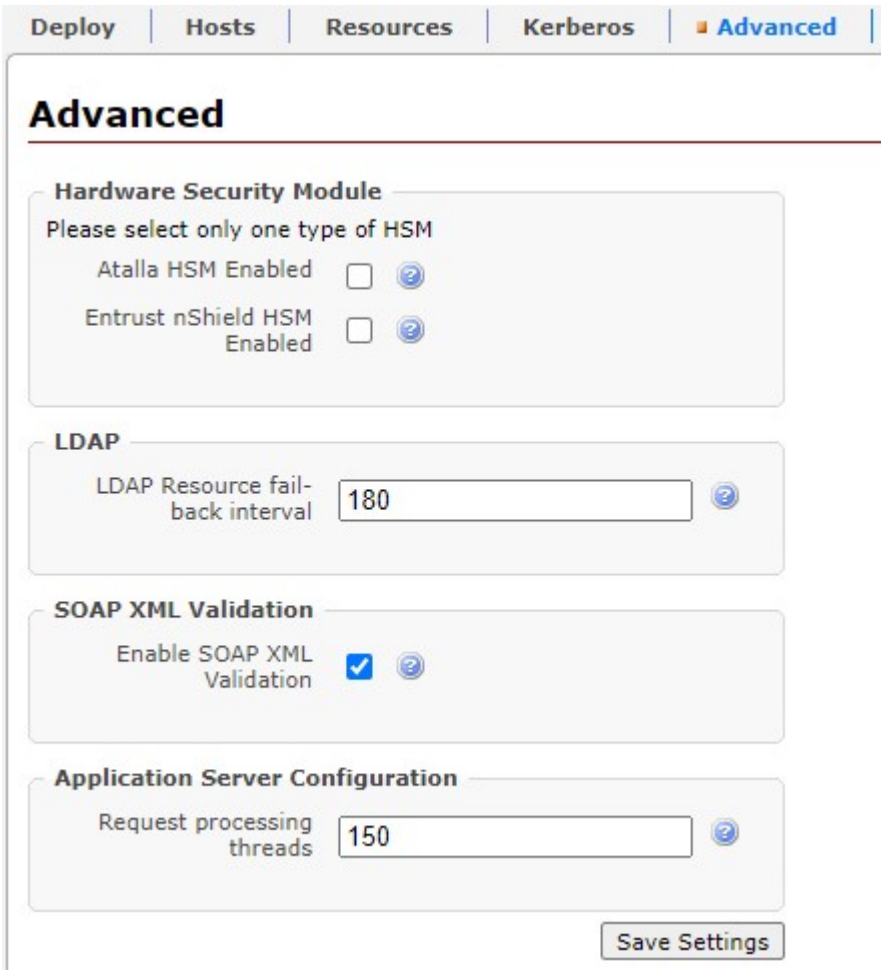
Support for using AES districts with Utimaco Atalla AT1000 HSM version 8.30 was added in SecureData 6.8. The minimum supported versions are SecureData version 6.8 and HSM AT1000 version 8.30.

If you are upgrading or migrating a SecureData appliance with a version older than 6.8, and HSM AT1000 version that is older than version 8.20, you must update SecureData before updating your HSM.

If your SecureData appliance and AT1000 HSM are running newer software than the minimum supported versions, you can update in any order.

To migrate to SecureData 7.0.0 before upgrading AT1000(s) to 8.30 and later:

1. Create backups of your SecureData system and current Atalla AT1000 configuration.
2. Follow migration steps in the Installation Guide to migrate your SDA to 7.0.0.
3. Upgrade your AT1000(s) to version 8.30 (or later version).
4. If it does not already exist, configure an AES MFK (AMK) on the AT1000(s).
5. On the SecureData Management Console, disable and save, then enable and save the Atalla HSM Enabled check box. This is necessary to ensure HSM FEK is being used. On the System > Advanced page, clear the Atalla HSM Enabled check box and click Save Settings, and then select the Atalla HSM Enabled check box and click Save Settings.



6. Deploy the changes. The FEK is now protected by the AT1000 HSM AMK.

For existing SecureData environments being migrated to Version 7.0.0, the AT1000 (s) with software version 8.30 and later require both your existing 3DES MFK to support existing districts and an AES MFK (AMK) for new district creation on SecureData 7.0.0.

7.1 Installing New AT1000s with Version 8.30 and Later Software

If you are replacing or adding an AT1000 running a version prior to 8.30 with new AT1000(s) that are running 8.30 or later, you must restore the 3DES MFK used to create existing districts (districts created prior to version 6.7) and create an AES MFK to support new district creation. To restore 3DES MFK, either create the same 3DES MFK or restore the 3DES MFK from the old AT1000.

All Atalla HSMs used by SecureData must be running the same Atalla software version.

Backing up and restoring the 3DES MFK is also important when you are upgrading to AT1000 HSMs from Ax160 HSMs.

7.2 Replacing or Upgrading Atalla HSM from Ax160 to AT1000

The Utimaco Atalla Ax160 HSM is no longer in support. We provide a migration for SecureData districts generated with Ax160 to AT1000. Contact OpenText Support for information.

If you are replacing or upgrading an Atalla HSM from version Ax160 to version AT1000, perform the following steps to make sure the new Atalla HSM contains the same MFK to support the existing districts:

1. Back up the MFK from the existing Ax160. Refer to the Atalla HSM and Atalla Secure Configuration Assistant-3 (SCA-3) documents for this operation.
2. Disable the HSM check box from the Management Console. Go to System > Advanced., then clear (disable) the Atalla HSM Enabled check box and click Save Settings.
3. Restart the **vsmgmt** service and deploy.
4. Restore the MFK you backed up in Step 1 to the new or upgraded Atalla HSM. Refer to Atalla HSM and Atalla Secure Configuration Assistant-3 (SCA-3) documents for this operation.
5. If you are upgrading from Ax160 to AT1000, generate an AES MFK (AMK) on AT1000 prior to adding this HSM to the SDA.
6. Add the new Atalla IP address to the SDA.
7. Enable the HSM check box from the Management Console. Go to System > Advanced., then select (enable) the Atalla HSM Enabled check box and click Save Settings.
8. Restart the **vsmgmt** service and deploy.

8 Troubleshooting

This section provides information to help troubleshoot issues with HSMs in your SecureData environment. Refer to the Utimaco Atalla documentation for troubleshooting your HSM product.

- Boxcar Fails with SSL Error
- SDA Events for HSMs

8.1 Boxcar Fails with SSL Error

If Boxcar fails to start during configuration and returns an SSL error, you can use the command below to test the SSL connection between a client and the HSM.

```
cd /opt/boxcar

openssl s_client -connect <HSM-IP>:7000 \

-CAfile truststore.pem \

-cert boxcar.pem \

-pass pass:`grep "^PARAM BOXCAR-CLIENT-PASSPHRASE" params|awk ' {print $3}'`
```

where <HSM-IP> is the IP address of the HSM.

Example

```
openssl s_client -connect 10.10.242.14:7000 \

-CAfile truststore.pem \

-cert boxcar.pem \

-pass pass:`grep "^PARAM BOXCAR-CLIENT-PASSPHRASE" params|awk ' {print $3}'`
```

8.2 SDA Events for HSMs

The following table identifies SecureData events for HSMs. For additional SecureData events, see the *SecureData Administrator Guide*.

SecureData Events for HSMs

Event Number	SDA Component or Console Module	Level	Event Text	Description or Workaround
3080	Key Management	4	Converted HSM district.	
3081	Key Management	6	Failed to convert HSM district.	
3082	Key Management	4	Generating IBE BF Parameters	Occurs when creating a new HSM district.
3083	Key Management	4	Generating IBE BB 1024 Parameters	Occurs when creating a new HSM district.
3087	Key Management	4	Generating IBE BBX 3072 Parameters	Occurs when creating a new HSM district.
3088	Key Management	4	Generating AES Parameters	Occurs when creating a new HSM district.
3089	Key Management	4	Generating TDES Parameters	Occurs when creating a new HSM district.
3090	Key Management	4	Generating FPE Parameters	Occurs when creating a new HSM district.

6823	Remote Deployer	6	Failed to check Atalla HSM status on remote host	The Atalla HSM Connector is disabled or down on a remote host
6824	Remote Deployer	6	Unable to parse JSON object for Atalla HSM status check	
6842	HSM	2	Checking HSM status on remote host	The beginning message that indicates the start of the checking interval for the HSM status check.
6843	HSM	4	Host with HSM connected to management console	A new host, for which HSM is configured, is added to the Management Console.
6844	HSM	4	Host with HSM disconnected from management console	A host with HSM configured has been removed from the Management Console
6845	HSM	4	HSM added to host	One or more new HSMs have been configured to an existing host
6846	HSM	4	HSM removed from host	An HSM has been removed from an existing host

6847	HSM	4	HSM became available at host	One or more HSMs have changed from another state to "Available"
6848	Remote Deployer	6	HSM became unavailable at host	One or more HSMs have changed from "Available" to "Not Available" or "Failed".

SecureData Events for HSMs, continued

Event Number	SDA Component or Console Module	Level	Event Text	Description or Workaround
6849	HSM	4	Started HSM status checker	The beginning message that indicates that the HSM status checker has started.
6850	Remote Deployer	4	Atalla HSM has been enabled	The Atalla HSM monitor is starting
6852	Remote Deployer	6	Failed to check Atalla HSM status on local host	The Atalla HSM Connector is disabled or down on the local host

6917	Key Management	4	PIE wrapped mode unsupported.	
8013	Secret	4	Fetch new master key	Occurs when enabling / disabling HSM on the System > Advanced tab of the Management Console
8014	Secret	4	Create new master key	Occurs when enabling/ disabling HSM on the System > Advanced tab of the Management Console
8015	Secret	4	Re-encrypt field encryption key	Occurs when enabling/ disabling HSM on the System > Advanced tab of the Management Console
8314	Core	8	HSM inaccessible	HSM machine not reachable.
8317	Core	4	Initialized field encryption key	aws_enabled=True/False azure_enabled=True/False atalla_hsm_enabled=True/ False hsm_enabled=True/ False
9401	System	4	Modified HSM settings.	
9402	System	8	Error modifying HSM settings.	

91030	Key Server	5	Generating IBE key via HSM.	Derive IBE key from HSM if HSM enabled.
91030	Key Server	5	Generating Symmetric key via HSM.	Derive Symmetric key from HSM, if HSM-enabled.