Avaya Workforce Optimization

Thales KMS 6.0.2 Installation and Configuration Guide

Release 15.2

May 07, 2019
Revision 1.14

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by Avaya. You agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by You.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:
http://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE AVAYA GLOBAL SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO, OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS THE SOFTWARE (AS DEFINED IN THE AVAYA GLOBAL SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS), AND WHO PURCHASED THE LICENSE FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. REFER TO THE AVAYA SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS FOR INFORMATION REGARDING THE APPLICABLE LICENSE TYPES PERTAINING TO THE SOFTWARE.

All Rights Reserved

Avaya and/or its licensors retain title to and ownership of the Software, Documentation, and any modifications or copies thereof. Except for the limited license rights expressly granted in the applicable Avaya Global Software License Terms for Verint Software Products, Avaya and/or its licensors reserve all rights, including without limitation copyright, patent, trade secret, and all other intellectual property rights, in and to the Software and Documentation and any modifications or copies thereof. The Software contains trade secrets of Avaya and/or its licensors, including but not limited to the specific design, structure and logic of individual Software programs, their interactions with other portions of the Software, both internal and external, and the programming techniques employed.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for any Software that has distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Software, Documentation or on Avaya's website at: http://support.avaya.com/Copyright (or a successor site as designated by Avaya).

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Software is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, any Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

About this guide

The *Avaya Workforce Optimization Thales KMS 6.0.2 Installation and Configuration Guide* describes the installation and configuration of a single Thales Key Manager Server or multiple Thales Key Manager Servers in a high availability configuration.

Key features

- Compatible with all V15.2 HFR2 and higher version
- Simplified installation procedures

Intended audience

This guide is designed for:

- Any party responsible for planning and setting up systems.
- Anyone responsible for system security and system maintenance.

Document revision history

Revision	Description of changes
1.14	Added "Configure a backup schedule for Linux using the web application" to the Thales Key Manager Server backup and restore chapter. Added "Configure a backup schedule using the CLI" information to the Thales Key Manager Server backup and restore chapter.
1.13	Moved the "Install the signed certificate on the Thales KMS" step after the "Generate a certificate signing request" step in the "Workflow: Failover Thales KMS installation and configuration" topic. Moved content from "Server security modes" topic to "Prerequisites for the Thales KMS installation" topic. Clarified the wording in the step to load the Intermediate CA Certificate. "
1.12	Added "Unable to configure automatic backup" troubleshooting topic.

Revision	Description of changes
1.11	Added "Important information" section to the "Prerequisites for the Thales KMS installation" topic. Added that all backups are the responsibility of the customer to the "Thales Key Manager Server backup and restore" page. Added that the customer is responsible for maintaining wrapper keys to the "Backing up the Thales KMS" topic. Added "Email notifications" section to the "Backing up the Thales KMS" topic. Added that one custodian is recommended to the "Backing up the Thales KMS" topic. Added "Configuring email notifications" section to the Thales Key Manager Server administration appendix. Added "Configuring SNMP" section to the Thales Key Manager Server administration appendix. Added "Thales KMS software upgrade failed" troubleshooting topic. Changed "Recorder KMS service" to "KMS service". Added Step 3c to run checkport command for port 50000 and removed checkport command for port 50000 from step 4c from the "Primary server is not configured during failover registration" topic. Added maximum of 32 characters for the Organization field in the "Prerequisites for the Thales KMS installation" and the "Web server certificate fields" topics.
1.10	Added "Server security mode" topics in the Thales Key Management Server administration appendix.
1.09	Changed Upgrade Software "Browse" button to "Choose File" in the "Upgrade the server software" topic and the "Install the signed ceritifcate on the Thales KMS" topic. Added "0002:system$ up" command to step 2 in the "configure the network settings" topic. Changed country to geographic area for the gmttimezone set command in the "Configure the NTP, time zone, date and time" topic. Replaced ArchiveWS_IIS with IAF API KB from "Install the client on each V15.2 Application server.

Revision	Description of changes
1.08	Deleted the "up" command from step 1 of the "Disable DHCP" topic. Added that it is the customers responsibility to have the file share availability and enough memory when performing an automatic backup. Added the "Run the New Virtual Hard Disk Wizard" and the "Install the operating system and the Thales software" to the "Deploy the Thales KMS software on Hyper-V" topic. Changed "Recorder Tomcat" to "Recorder KMS service" in Install the client on each Application server, Generate the Thales KMS certificate authority, and the "Thales KMS registration failed" alarm topics. Removed IAF API KB number from "Install the client on each Application server.
1.07	Removed assigning users to a domain in the "Create a DSM administrative domain" topic.
1.06	The following changes are new with V15.2 HFR3: • Added "the status can be IN-USE, IDLE, or BLANK) to step 3 of the "Upgrade the server software" topic. • Updated with new document template.
1.05	Modified the "Generate a certificate signing request" to include "About certificate signing request files" and added a Related information sub-topic. Added a note to the "Create a shared secret" topic that step 1 can be skipped if only one domain exists. Removed adding users to a domain from the "Create a DSM administrative domain" topic. Created a separate topic named "Assign users to the Thales KMS administrative domain".
1.04	Changed the KB name from "Data Center API" to "IAF API" and added "or higher" to KB140216 in the "Install the client on each Application server" topic.
1.03	Moved "Upgrade the server software" after "Add Thales KMS administrator field descriptions". Added KB to "Install the client on each Application server" topic. Removed steps to switch domains in "Add agent key" topic. Added example time period to Validity Period field description in "Registration Shared Secret field descriptions" topic.
1.02	Replaced Application server client installation procedure in chapter 1.
1.01	Added the "Thales KMS administration" chapter with the following troubleshooting topics: • Unable to playback calls in an HA environment • "Thales KMS registration failed" alarm
1.00	Original document.

Thales Key Manager Server and client installation

The Thales Key Manager Server (Thales KMS) provides centralized management of data security policies and encryption keys that enable corporations to secure their data in virtual environments.

Install the Thales KMS software by completing the prerequisites and then deploying the software.

Naming conventions

- **Thales KMS** - Throughout this guide the server that provides key management is called the Thales KMS. The Thales documentation set refers to this server as the Data Security Manager (DSM). Please note that the Thales KMS and the DSM are the same servers.
- **(Avaya Contact Recorder Advanced) Protected host**, **Agent**, or **client**- The agent software is installed automatically on the Avaya Workforce Optimization Application servers, which are called protected hosts. In the Thales KMS system, **Application servers in the WFO suite are the only servers that connect to the Thales KMS**. Recorders request an encryption key from the Application server, not the Thales KMS.
- **(Avaya Contact Recorder) Protected host, Agent, or client** - The agent software is installed manually on each ACR server. Recorders request an encryption key directly from the Thales KMS.

Topics

Install the client on each V15.2 Application server or ACR server

The VAE client software and the IAF API KB must be loaded on all Application servers.

Avaya Contact Recorder Advanced (ACRA) Procedure

1. Download the latest IAF API KB from the portal or from your customer representative and then install the KB on the Application server.
2. Download the **VAEClient-15.2.x.xx ZIP** file from the portal or from your customer representative.
3. Extract the ZIP file to a folder.
4. Copy the extracted folder to an Application server.
5. On the Application server, open a command prompt as an administrator.
   a. From the **Start** menu, select **Programs** > **Accessories** > **Command Prompt**.
   b. Right-click the **Command Prompt** and select **Run as administrator**.
6. From the command prompt, access the folder containing the installation files.
7. From the command prompt, type **install.bat**.
8. Once the installation is complete. On the Application server, in Windows services, restart the Recorder KMS service.
9. Repeat step 1 through step 8 for the remaining Application servers.

Avaya Contact Recorder (ACR) Procedure

1. Download the ArchiveWS_IIS from the portal or from your customer representative.
2. Download the VAEClient installation from the portal or from your customer representative.
3. Install the KB and the client on the following servers.
   - each ACR server
   - each Application server if WFO is installed
4. For specific installation steps, refer to the *Avaya Contact Recorder Planning, Installation and Administration Guide*.

Prerequisites for the Thales KMS installation

Prior to installing the Thales KMS software, you must complete the prerequisite tasks. Tasks include, getting the Thales KMS installation file, recording the information needed to configure the software, and opening the necessary ports.

Equipment requirements

Refer to the *Customer Furnished Equipment (CFE) Guide* for minimum memory and hardware requirements.

Server security modes

The Thales KMS supports two modes, compatible and Suite B (also known as elliptic curve cryptography (ECC)).

- **Compatible mode**

  In compatible mode, all cipher suites are enabled and compatible with older clients that cannot use ECC (Suite B mode). Compatible mode uses RSA.

- **Suite B mode**

  Suite B is a set of publicly available cryptographic algorithms approved by the United States National Security Agency (NSA). The algorithms enhance security by adding up to 384-bit encryption to the communication between the following:

  - Web browser and Thales KMS
  - Thales KMS and clients
  - Between Thales KMS servers in a high-availability environment

  Using Suite B mode disables TLS 1.0/1.1 weak ciphers and RSA.

  When Suite B mode is configured, you must connect to the Thales KMS web application using Internet Explorer. Internet Explorer is the only browser that supports SHA384.

  Suite B is not used for data encryption.

  For information about configuring the mode, see Related topics.

Important information to provide after the installation

Once the installation is complete, provide the following information to the customer:

- The wrapper key used to create the backup. The wrapper key is required to restore from backup.
- The command-line interface "cliadmin" password.
- The web interface "admin" password.

It is the customer's responsibility to safeguard and retain the above information.

Procedure

1. If using VMware, obtain the Thales KMS Virtual Machine file (OVA) file. If using Hyper-V, obtain the Thales KMS ISO file. This file is used to deploy all the software required by the Thales KMS. The file is located on the ISO.

   All required installation packages are available on the Thales KMS ISO/DVD.

2 Obtain the latest Thales KMS patches released for the version you are installing. Patches are located on the ISO, or if required can be downloaded from VerintConnect.

3 Use the following table to record the information you need to install the software.

Description	Value
Thales KMS IP addresses and hostnames	
Primary Thales KMS static IP address	
Primary Thales KMS FQDN host name	
Secondary Thales KMS static IP address	
Secondary Thales KMS FQDN host name	
Certificate information	
Name of your organizational unit	
Name of your organization (up to 32 characters)	
Name of your city or locality Note: Do not use abbreviations.	
Two letter country code	

4 Open the necessary ports on the Thales KMS and the protected host computers (Application servers). For the latest information on port usage, see the *Firewall Ports Configuration Guide*.

Related topics

Activate ECC (Suite B) or compatible mode for all communications, page 81
Configure a client to use ECC (Suite B) for all communications, page 82
Create a wrapper key, page 55
Log on to the Thales KMS command-line interface, page 16
Log on to the Thales KMS web user interface, page 23

Deploy the Thales KMS software on VMware

The Thales KMS software is deployed using the Thales KMS Virtual Machine (OVA) template file. The template file includes all the software required by the Thales KMS.

Installation time

Approximately 30–45 minutes

Before you begin

Prerequisites for the Thales KMS installation, page 10

Procedure

1. Open the VMware vSphere client.
2. Click **File** > **Deploy OVF template**.
3. Click **Browse** and locate the OVA file.

   `vDSM-Vormetric-DSM-Virtual-Appliance-<version>.ova`
4. Select the OVA file, and then click **Next**.
5. On the **OVF Template Details** page, click **Next**.
6. On the **Name and Location** page, type a name for the virtual appliance, and then click **Next**.
7. On the **Storage** page, select a destination for the virtual appliance, and then click **Next**.
8. On the **Disk Format** page, select the type of provisioning based on the storage characteristics for your system, and then click **Next**.
9. On the **Ready to Complete** window, click **Finish**.
10. At the **Completed Successfully** message, click **Close**.
11. On the main screen of the vSphere Client, in the left pane, select the virtual appliance you just created and then click the power on icon in the tool bar.

    It takes approximately 30 minutes to provision the virtual machine and build the Thales KMS.
12. To monitor the output as the installation progresses, click the **Console** tab and click inside the console window.

Deploy the Thales KMS software on Hyper-V

The Thales KMS software is deployed using an ISO file. The file includes all the software required by the Thales KMS.

Installation time

Approximately 30–45 minutes

Before you begin

Prerequisites for the Thales KMS installation, page 10

Procedure: Run the New Virtual Hard Disk Wizard

1. Click **Start** > **Administrative Tools** > **Hyper-V Manager**.
2. From the **Action** pane, click **New**, and then click **Hard Disk**.
3. In the **New Virtual Hard Disk Wizard**, on the **Choose Disk Format** page, select **VHDX**, and then click **Next**.
4. On the **Choose Disk Type** page, select **Fixed size**, and then click **Next**.
5. On the **Specify Name and Location** page, specify the name of the virtual machine and where you want to store it. You will need the name and location when you run the New Virtual Machine Wizard.
6. On the **Configure Disk** page,
   a. Select **Create a new blank virtual hard disk**.
   b. Specify a size for the virtual hard disk based on the number of agents (Application servers) you plan to install. Refer to the *Customer Furnished Equipment Guide* for additional information.
   c. Click **Next**.
7. On the **Summary** page, review the settings, and then click **Finish**.

Procedure: Run the New Virtual Machine Wizard

1. Click **Start** > **Administrative Tools** > **Hyper-V Manager**.
2. From the **Action** pane, click **New**, and then click **Virtual Machine**.
3. In the **New Virtual Machine Wizard**, click **Next**.
4. On the **Specify Name and Location** page, specify the name of the virtual machine and where you want to store it.
5. On the **Specify Generation** page, select **Generation 1** for the virtual machine.


Generation 2 does not support CentOS 5.x.

6. On the **Assign Memory** page, specify a minimum of 4GB (which is 4000 MB) memory to run the guest operating system for the virtual machine.

   To prevent memory over commits, it is recommended that you disable the **Use Dynamic Memory for this virtual machine** option. This option is enabled by default.
7. On the **Configure Networking** page, connect the network adapter to an existing virtual switch to establish network connectivity. A second (optional) switch can be added later if desired.

   If you want to use a remote image server to install an operating system on your test virtual machine, select the external network.

8 On the **Connect Virtual Hard Disk** page, select **Use an existing virtual hard disk**. This is the virtual hard disk you created in step 4 of Procedure: Run the New Virtual Hard Disk Wizard, page 13.

9 On the **Summary** page, review the settings, and then click **Finish**.

Procedure: Install the operating system and the Thales software

1 From the Hyper-V Manager, select the virtual machine you created.

2 Right-click the virtual machine, and then click **Settings**.

3 Select the virtual DVD drive.

4 In the **Media** section, click **Browse** to navigate to the DSM ISO file location and select the file.

The ISO file name is **dsm-<version>.iso**.

5 Click **Apply**, and then click **OK**.

6 Select the virtual machine, and then click **Start**.

7 Connect to the virtual machine console.

Before you power on the virtual machine, make sure that the hard drive is set as first in the boot order.

8 Power on the machine to build the Thales KMS.

Chapter 2

Thales Key Manager Server configuration

Use the Thales KMS command-line interface (CLI) to configure network settings, set time and date, host name, and generate the Thales KMS Certificate Authority. Once the CLI procedures are complete, you will use the Thales KMS web application to complete the remaining configuration tasks.

Topics

Workflow: Thales KMS configuration using the command-line interface

Configure the Thales KMS using the command-line interface (CLI).

Workflow

1 Log on to the Thales KMS command-line interface, page 16

Before you can complete the preliminary Thales KMS configuration tasks, you must log on to the command-line interface (CLI).

2 Disable DHCP, page 18

Before you can assign a static IP address to the Thales KMS, you must disable DHCP on the eth0 interface.

3 Configure the network settings, page 18

Because the Thales KMS uses a static IP address, you must configure the network settings. The network settings are configured using the CLI.

4 Configure the NTP, time zone, date, and time, page 19

You must have the correct time set on your KMS(s) as this affects system functions such as protected host registration, log timestamps, high availability cluster synchronization, and certificate exchange. Although configuring a network time protocol (NTP) server is not mandatory, it is recommended.

5 Configure the host name, page 20

Configure the host name by entering the fully qualified domain name (FQDN) for the Thales KMS.

6 Generate the Thales KMS certificate authority, page 21

After completing the preliminary configuration, on the primary Thales KMS, generate the Thales KMS certificate authority (CA). The certificate is used to access the Thales KMS web interface.

Log on to the Thales KMS command-line interface

Before you can complete the preliminary Thales KMS configuration tasks, you must log on to the command-line interface (CLI).

Procedure

1 Log on to the Thales KMS CLI.

The CLI can be accessed using SSH if firewall port 22 is open.

2 Enter the default logon of **cliadmin**

3 Enter the default password of **cliadmin123**

4 If accessing the Thales KMS for the first time, read and then accept the license agreement and enter a new password.
   a. On the License Agreement screen, type **Y** to accept, and then press **Enter**.
   b. When prompted, enter a new password, and then press **Enter**.

Be sure to keep the new password stored in a safe location. You will need this password to access the CLI in the future.

Using the CLI

The Thales KMS Command-line interface (CLI) commands are grouped into categories and submenus. To run a submenu command, you must first access the category containing the submenu command.

List categories

From the CLI, to view a list of main menu categories, type a question mark (?), and then press Enter. The main menu with a list of categories is displayed.

Access a category

You must enter a category to execute the submenu commands in that category.

1 To access a category, type the category name or type just enough characters to uniquely identify the category, and then press **Enter**.
2 To display the submenu commands for that category, type a question mark (?).

Example: Access the network menu

1 At the main menu prompt, type **network**, and then press **Enter**.
2 To list the submenu commands in the network category, type **?**.

Display usage and example input for submenu commands

Every submenu command has usage and example input. To display the usage and example input, type the command without a value.

Example: ping

1 At the main menu prompt, type **network**, and then press **Enter**.
2 To list the submenu commands in the network category, type **?**.
3 To display the usage information, type **ping**, and then press **Enter**.

```
0013:network$ ping
usage: ping IPADDRESS [ipv6]
0014:network$
```

Return to the previous menu

To return to the previous menu, type **up**, and then press **Enter**.

Related information

For additional information about navigating the CLI, see the *Vormetric Data Security Manager (DSM) Installation and Configuration Guide*.

Disable DHCP

Before you can assign a static IP address to the Thales KMS, you must disable DHCP on the eth0 interface.

Do *not* change the configuration on the eth1 interface. The eth1 interface is used to support backing up the software.

Procedure

1 Access the network command prompt, and turn off DHCP.

```
0000:vormetric$ network
0001:network$ ip dhcp release eth0 version 4
```

```
WARNING: Changing network ip address may disconnect your session and
will require the server software to be restarted. Continue? (yes|no)
[no]:yes
```

2 At the **Continue? (yes|no)** prompt, type **yes**.

```
DHCP operations may take some time, please wait....
SUCCESS: Please restart server software to pick up the changes.
```

3 Return to the main menu.

```
0002:network$ up
```

4 Using the CLI, from the main menu, access the system category and then restart the Thales KMS.

```
0000:vormetric$ system
0001:system$ restart
```

Configure the network settings

Because the Thales KMS uses a static IP address, you must configure the network settings. The network settings are configured using the CLI.

Procedure

1 Access the network command prompt, add the IP address, and then verify the settings.

```
0000:vormetric$ network
0001:network$ ip address init <IP address for Thales KMS>/<subnet mask 16 or
24> dev eth0
```

Example: ip address init 192.168.40.190/16 dev eth0

```
0002:network$ ip address show
0003:network$ up
```

2 Using the CLI, from the main menu, access the system category and then restart the Thales KMS.

```
0000:vormetric$ system
0001:system$ restart
0002:system$ up
```

3 Access the network command prompt, add the default gateway.

```
0000:vormetric$ network
0001:network$ ip route add default table main.table dev eth0 via <IP address for the default gateway>
```

Example: ip route add default table main.table dev eth0 via 192.168.0.254

```
0002:network$ ip route show
```

4 If applicable, configure DNS. At the network command prompt, set the primary DNS for the Thales KMS, and if multiple DNS are in use, set them. Set the search domain, and then return to the main menu.

```
0003:network$ dns dns1 <ip address for dns server 1>
0004:network$ dns dns2 <ip address for dns server 2>
0005:network$ dns search <search_domain>
0006:network$ dns show
0007:network$ up
```

Configure the NTP, time zone, date, and time

You must have the correct time set on your KMS(s) as this affects system functions such as protected host registration, log timestamps, high availability cluster synchronization, and certificate exchange. Although configuring a network time protocol (NTP) server is not mandatory, it is recommended.

Procedure

1 Access the maintenance command prompt, display the current ntpdate settings, add ntpdate server (s), and then activate the ntpdate server connection.

```
0000:vormetric$ maintenance
0001:maintenance$ ntpdate show
0002:maintenance$ ntpdate add <IP address or host name for the ntpdate server>
```

Example: ntpdate add time.nist.gov

```
0003:maintenance$ ntpdate on
```

2 Display a full list of time zones, display the time zone currently configured for this Thales KMS. If the time zone setting is incorrect, set the time zone where the Thales KMS is located.

```
0004:maintenance$ gmttimezone list
0005:maintenance$ gmttimezone show
0006:maintenance$ gmttimezone set <geographic area/city>
0007:maintenance$ up
```

3 If you did *not* change the time zone, you do not need to restart the Thales KMS. Skip to step 5.

If you changed the time zone, you must restart the Thales KMS. Continue to step 4.

4 Using the CLI, from the main menu, access the system category and then restart the Thales KMS.

```
0000:vormetric$ system
0001:system$ restart
```

5 If ntpdate sync was used, you do not need to complete this step. Continue to Configure the host name, page 20.

If ntpdate sync was *not* used, set the date and time and then verify the settings.

```
0000:system$ up
0001:vormetric$ maintenance
0002:maintenance$ date <mm/dd/yyyy>
0003:maintenance$ time <hh:mm:ss>
```

Where: hh is 00 to 23.

```
0004:maintenance$ date
0005:maintenance$ time
0006:maintenance$ up
```

Configure the host name

Configure the host name by entering the fully qualified domain name (FQDN) for the Thales KMS.

Rules

- The host name is case sensitive.
- The host name is the fully qualified domain name (FQDN) for the Thales KMS.
- The host name entered here must be the same name used on the domain name system (DNS).

Procedure

1 Access the system command prompt and then set the host name.

```
0000:vormetric$ system
0001:system$ setinfo show
0002:system$ setinfo hostname <FQDN>
0003:system$ up
```

2 Make sure that the host name is correct on the DNS.

Generate the Thales KMS certificate authority

After completing the preliminary configuration, on the primary Thales KMS, generate the Thales KMS certificate authority (CA). The certificate is used to access the Thales KMS web interface.

About the generate CA command

The generate CA command does the following, in the following order:

- Generates a new signer certificate
- Deletes the old signer certificate from the keystore
- Imports the new signer certificate into the keystore
- Generates a new certificate request from the existing Thales KMS certificate
- Signs the Thales KMS certificate with new CA
- Imports the new Thales KMS certificate into the keystore
- Restarts the Thales KMS

Regenerating a CA

Regenerating a CA makes certificates on the failover server and the agents (Application servers) invalid. Do the following:

- Re-sign certificates on the failover server.
- Cleanup and re-register each agent (Application server). To re-register, you must restart the "Recorder KMS service" on each Application server.

Procedure

1. Access the system prompt, and then start generating a new certificate.

   ```
   0000:vormetric$ system
   0001:system$ security genca
   ```

2. At the Continue prompt, type **yes**.
3. At the **Security Server host name** prompt, enter the fully qualified domain name entered in Configure the host name, page 20.

   Example: kms-vormetric.lab.local
4. Enter the information required to generate the certificate.
   a. Enter the **organization unit**, which is frequently a department or group name.
   b. Enter the **organization**, which is typically the company name.
   c. Enter the **city or locality** of the organization.
   d. Enter the **state or province** of the organization.
   e. Enter the **country code** in which the organization is located.
5. Return to the main menu.

   ```
   0002:system$ up
   ```

Workflow: Thales KMS configuration using the web interface

After completing the CLI configuration steps, you are ready to access the Thales KMS Management Console from a web browser. Use the web interface to complete the remaining configuration steps.

Workflow

1 Log on to the Thales KMS web user interface, page 23

You will log on to the Thales KMS web user interface using the default logon and password. After you log on for the first time, you are prompted to enter a new password. You will need this password to log on to the web interface. Be sure to keep the password in a safe location.

2 Upload the Thales KMS license file, page 23

When you log on to the Thales KMS for the first time, the dashboard displays "License not found." In addition, the only tabs that are available are the Dashboard and the System tabs. Once the license is uploaded, all the menu items available according to your license file are displayed.

3 Create Thales KMS administrative users, page 26

To create new Thales KMS administrative users, log on to the Thales KMS web application with a user that has a user type of System Administration.

4 Upgrade the server software, page 28

You can upgrade the Thales KMS software using the Thales KMS web application. The Thales KMS can hold up to two images. If you have two images on your system, you must delete the one that is not active before you can upload a new image.

5 Generate a certificate signing request, page 30

The Thales KMS can be configured to get certificates signed by an external Certificate Authority (CA). An external CA can be configured on a single node or a high availability (HA) system. Using an external CA is an optional procedure.

6 Install the signed certificate on the Thales KMS, page 33

Once you have received the signed certificate from the external CA, you are ready to import the signed certificate and the signer's certificate(s) to the Thales KMS.

7 Create a Thales KMS administrative domain, page 34

A Thales KMS administrative domain is a logical partition that is used to separate administrators, and the data they access, from other administrators. Administrative tasks are performed in each domain based on each administrator user type. A Thales KMS administrative domain is not related to a network domain.

8 Assign users to the Thales KMS administrative domain, page 37

Once the RecorderDomain is created, you are ready to assign administrators to the domain.

9 Add agent key, page 39

The Thales KMS web application is used to create agent keys, as a secure centralized repository for storing and retrieving third-party encryption keys.

10 Create a shared secret , page 40

Protected hosts (Application servers) are added and registered with the Thales KMS automatically. Before the protected hosts can be added and registered with the Thales KMS, a Thales KMS Administrator must create a registration password.

Log on to the Thales KMS web user interface

You will log on to the Thales KMS web user interface using the default logon and password. After you log on for the first time, you are prompted to enter a new password. You will need this password to log on to the web interface. Be sure to keep the password in a safe location.

Procedure

1 Open a web browser, using an HTTPS connection, enter the Thales KMS host name (if configured in DNS) or Thales KMS IP address.

If the URL does not work, port 443 could be blocked by a firewall. Specify port 8445 as shown in the following example:
https://vormetric.lab.local:8445

Since the website has not been secured yet, you will see a warning message. You can safely ignore the warning at this point in the procedure.
Example message: In Internet Explorer the warning message is "There is a problem with this website's security certificate."

2 Log on using the default user name and password.

Login: admin

Password: admin123

Related topics

For password criteria, see Verify web access (*Vormetric Data Security Manager (DSM) Installation and Configuration Guide*)

Upload the Thales KMS license file

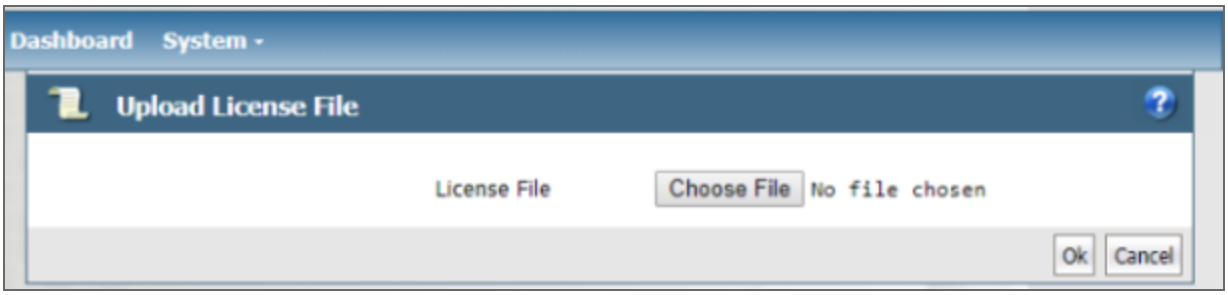
When you log on to the Thales KMS for the first time, the dashboard displays "License not found." In addition, the only tabs that are available are the Dashboard and the System tabs. Once the license is uploaded, all the menu items available according to your license file are displayed.

Procedure

1 Go to **System** > **License**.

2 On the **License** page, click **Upload License File**.

3 Enter the full path of the license file or click **Choose File** to locate and select the license file. The license file is included on the ISO.



4 Click **OK**.

5 Using the CLI, from the main menu, access the system category and then restart the Thales KMS.

```
0000:vormetric$ system
0001:system$ restart
```

Types of Thales KMS administrators

The Thales KMS implementation uses three administrative user types, which are *System Administrator*, *Domain Administrator*, and *Security Administrator*. Each administrator performs a specific set of administrative tasks. These administrative tasks are assigned to a user by assigning an administrative user type to the user.

Administrator authentication

For the different administrator accounts, the Thales KMS implements identity-based authentication using passwords.

Default administrative user types

- Thales KMS System Administrator - Operates outside domains. Creates domains and assigns administrators of the Domain Administrator role to the domains.
- Thales KMS Domain Administrators and Security Administrators - Performs every administrative task inside a domain.

Permissions for each user type

User type	Permissions
Thales KMS System Administrators Cannot perform security procedures in any domain.	Upgrade the Thales KMS software Back up and restore the Thales KMS database Add and delete all administrators Reset passwords for all administrators Add and delete all domains Assign one Domain Administrator to each domain Configure syslog server for system-level messages Install the license file Configure Thales KMS preferences View logs Configure High Availability (HA)
Thales KMS Domain Administrators Cannot remove domains or perform any domain security roles.	Domain administrative functions include: • Add and remove administrators (Domain, Security, All) to and from domains • Configure Security Administrator roles (Audit, Key, Policy, Host, Challenge & Response) • Configure syslog server for application-level messages • View Thales KMS preferences • View logs
Thales KMS Security Administrators Perform data protection work specified by their roles. Different roles allow them to create policies, configure hosts, audit data usage patterns, apply guard points, and do other duties.	Security administrative functions include: • Configure signature sets • Configure keys and key groups • Configure online and offline policies • Configure hosts and host groups • Assign host passwords (manually or generated) • Apply guard points • Share a host with another domain • Export the Thales KMS public key • Import symmetric keys • View Thales KMS preferences • View logs

Related topics

Create Thales KMS administrative users, page 26

Create Thales KMS administrative users

To create new Thales KMS administrative users, log on to the Thales KMS web application with a user that has a user type of System Administration.

Create these users

- *System Administrator* user type named *SystemAdministrator*
- *Domain Administrator* user type named *DomainAdministrator*
- *Security Administrator* user type named *SecurityAdministrator*

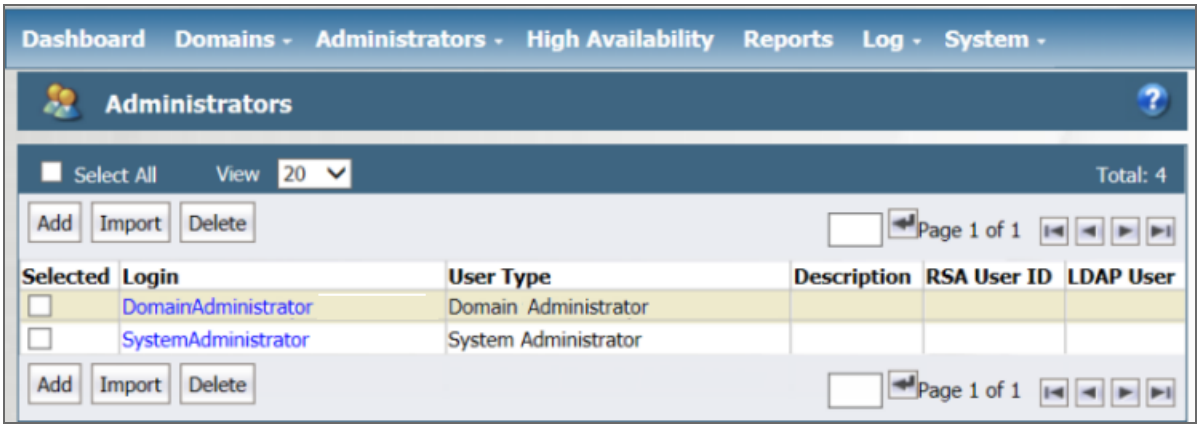
About administrative user passwords

After an administrative user is set up, the first time the administrator logs on, the administrator is prompted to enter a new password. The administrator should store the password in a safe location.

Procedure

1 Log on to the Thales KMS web application with a user type of System Administrator.

2 Click **Administrators**.



3 Add the SystemAdministrator user.
   a. Click **Add**.
   b. Select a **User Type** of **System Administrator**.
   c. Add the **SystemAdministrator** user and then complete the fields.
   d. Click **Ok**.

4 Add the DomainAdministrator user.
   a. Click **Add**.
   b. Select a **User Type** of **Domain Administrator**.
   c. Add the **DomainAdministrator** user and then complete the fields.

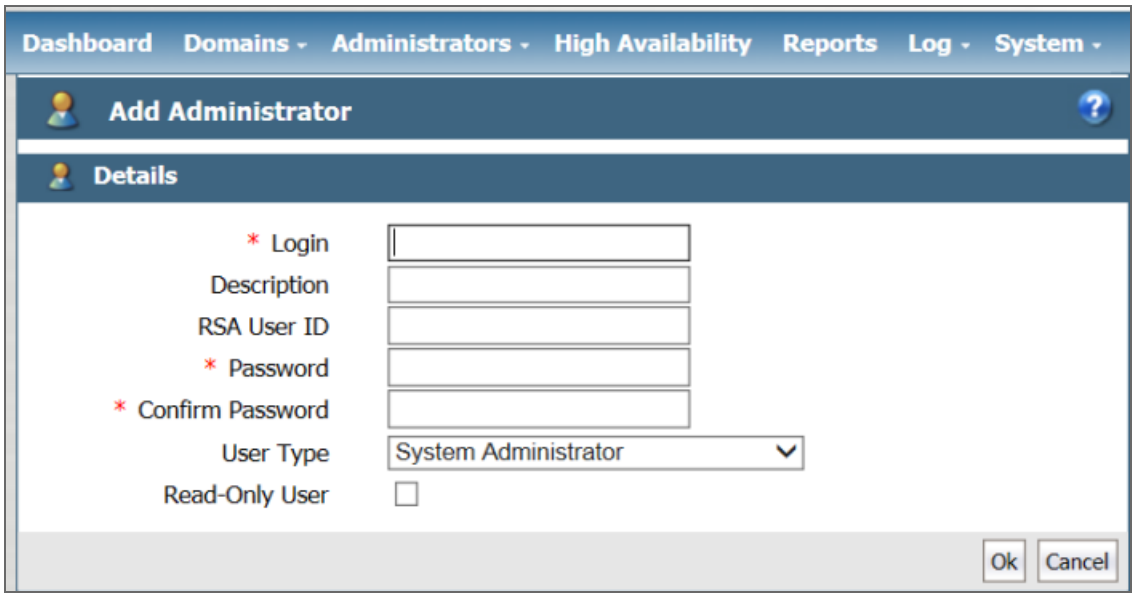
5 Add the SecurityAdministrator user.
   a. Click **Add**.
   b. Select a **User Type** of **Security Administrator**.
   c. Add the **SecurityAdministrator** user and then complete the fields.

Related topics

Add Thales KMS administrator field descriptions, page 27

Add Thales KMS administrator field descriptions

Create Thales KMS administrators on the Add Administrator screen in the Thales KMS web application.



Field	Description
Login	Unique name for the administrator logon.
Description	(Optional) A phrase or string that helps identify the administration. Maximum characters: 256
RSA User ID	(Optional) RSA SecurID value configured by the RSA administrator. If in a local domain, this field is not available.
Password	Password the administrator uses to log on to the Thales KMS web application.
Confirm Password	The administrator will need the password entered here to log on to the web interface for the first time. The first time the administrator logs on, the page is redirected to the reset password page. The password must be reset at this time. Be sure to keep the password in a safe location.

Field	Description
User Type	User types are: • System Administrator • Domain Administrator • Security Administrator Default: System Administrator It is recommended that you use a separate login for each type of administrator.
Restrict to Domain	(displays for *Domain Administrator* user type only) The domain the administrator is limited to for operations. If domains are created that do not have an administrator assigned, these domains can be selected from the menu. Default: None
Read-Only User	An administrator with read-only access is not able to add, delete, or modify any settings on the Thales KMS. Read-only administrators are able to change their passwords and view the different settings per their type and the roles assigned to them. You can assign read-only privileges to any type of administrator—except for Local Domain administrators that are the first administrators to be assigned to a domain.

Related topics

Create Thales KMS administrative users, page 26

Upgrade the server software

You can upgrade the Thales KMS software using the Thales KMS web application. The Thales KMS can hold up to two images. If you have two images on your system, you must delete the one that is not active before you can upload a new image.

The web interface stops working during the upgrade. The Thales KMS restarts at the end of the upgrade, and then administrators must log on again.

Things you need to know

- If synchronization is in progress anywhere in the cluster, wait until it completes before you begin the upgrade.
- Do not change the Thales KMS configuration during the upgrade process. If multiple administrators are logged on to the web interface, make sure that they do not make any configuration changes during the upgrade process.
- Minimum patch build number required is **5148**.

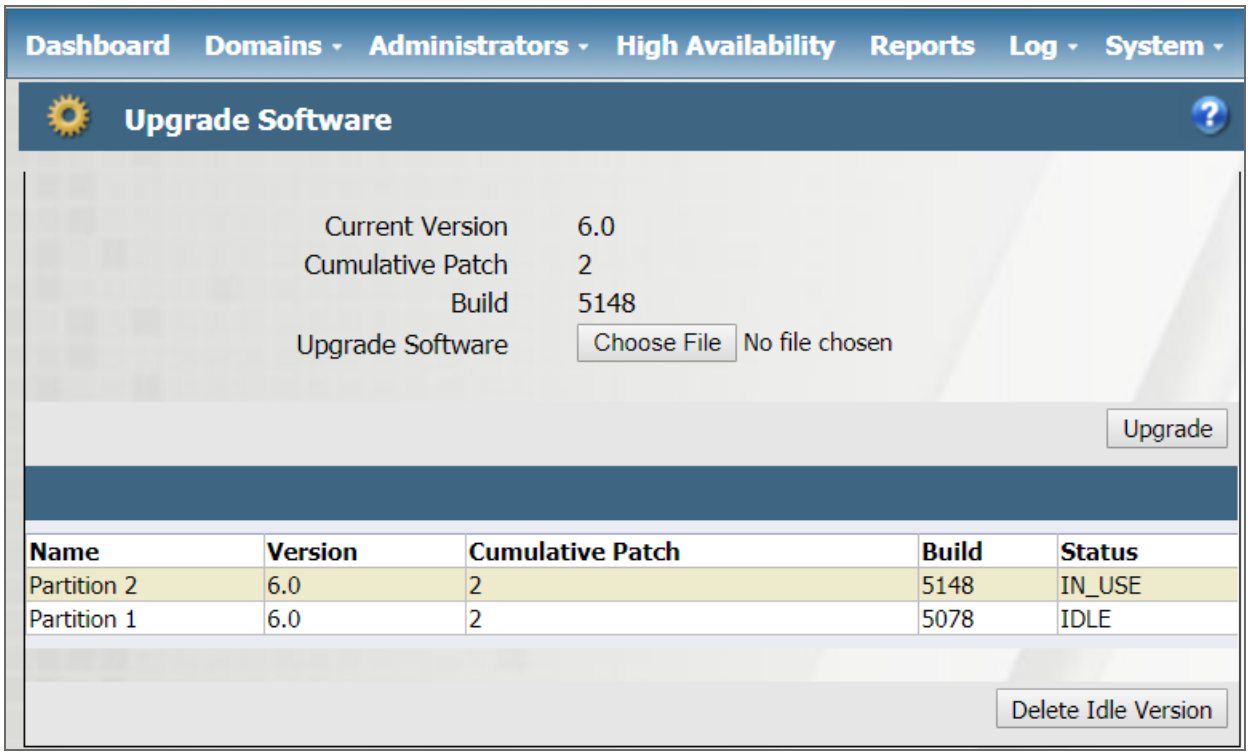
Before you begin

Back up the Thales KMS manually, page 59

Procedure

1 Log on to the Thales KMS web application as **SystemAdministrator**.

2 Click **System** > **Software Upgrade** > **Software Upgrade**.



3 If two software images are present (the status can be IN-USE, IDLE, or BLANK), click **Delete Idle Version** to delete the version not in use.

4 Click **Choose File**, and then select the upgrade file. The upgrade file is included on the ISO.

`VORMETRIC_upgrade_version_XXXXX.tar`

5 Click **Open**, and then click **Upgrade**.

6 Follow the directions on the screen.

7 After the upgrade is complete, refresh your browser to view the log in screen.

Do not close the upgrade browser/tab. If the upgrade seems like it is taking longer than expected, open a new browser window and try to access the Thales KMS.

8 Repeat the upgrade steps on the failover server.

Generate a certificate signing request

The Thales KMS can be configured to get certificates signed by an external Certificate Authority (CA). An external CA can be configured on a single node or a high availability (HA) system. Using an external CA is an optional procedure.

Working with an external CA

To configure the Thales KMS to work with an external CA, you need to have a valid account with an external CA that is network accessible. You also need instructions from the CA that explains how to transfer a Certificate Signing Request (CSR) file and a signed certificate file, to and from the Thales KMS.

About certificate signing request files

If the Thales KMS is running in Compatibility or Suite B mode, when you generate a CSR, the Thales KMS creates a .zip file containing two .pem files. See the following table to determine which file you need to get signed.

If the Thales KMS is operating in this mode...	Then get this file signed...
compatibility	tserver-csr.pem
Suite B	EC_tserver-csr.pem

Once you have received the signed Web server certificate, install the certificate on the Thales KMS.

Procedure

1 Log on to the primary Thales KMS web application as **SystemAdministrator**.

2 Click **System** > **Web Server Certificate**.

3 Click **CSR Generation**.

4 Click **Generate CSR**.

5 Name and then save the certificate signing request.
   a. On the **File Download** window, click **Save**.
   b. On the **Save As** window, enter the file name and path for the certificate request file.
      Default file name: servercasr_<hostname_YYYY_MM_DD_HHMM>.zip
   c. Click **Save**. The Download Complete window displays statistical information about the exported zip file, such as its location and size.
6 Extract the content from the zip file.
7 Make a note of the location of the pem file.
8 Submit the new CSR to a certificate authority for signing/approval.

To obtain valid certificates, be sure to follow the procedures of the CA. Each CA has different procedures to obtain the Root certificate, Intermediate certificate, and signed CSR certificate.

Once you have received the signed Web server certificate, install the certificate on the Thales KMS.

Related information

For information about elliptic curve cryptography (Suite B), perform an internet search and view a site such as Wikipedia.

Web Server Certificate fields

The Web Server Certificate page consists of multiple tabs. The Web Server Certificate Info tab displays status information about the existing Thales KMS certificate. The CSR Generation tab allows you to generate a certificate signing request (CSR) to send to a CA requesting signing/approval. The Install Certificates tab, once one or more signed certificates are received, is used to install the certificates.

Field	Description
Web Server Certificate Info	
Issued To	Displays a summary of the data required to generate a CSR, including Common Name (CN).
Issued By	Displays the CN of the Certificate Authority issuing the certificate.
Valid From	Displays the certificate start date and expiration date.
CSR Generation **Note:** Strings that contain a comma (,) are permitted. The use of single or double quotes in any field on the CSR Generation tab is not allowed.	
Host Name	Network name of the Thales KMS (up to 64 characters). It is possible to edit this field, however it is recommended that you do not change this name.

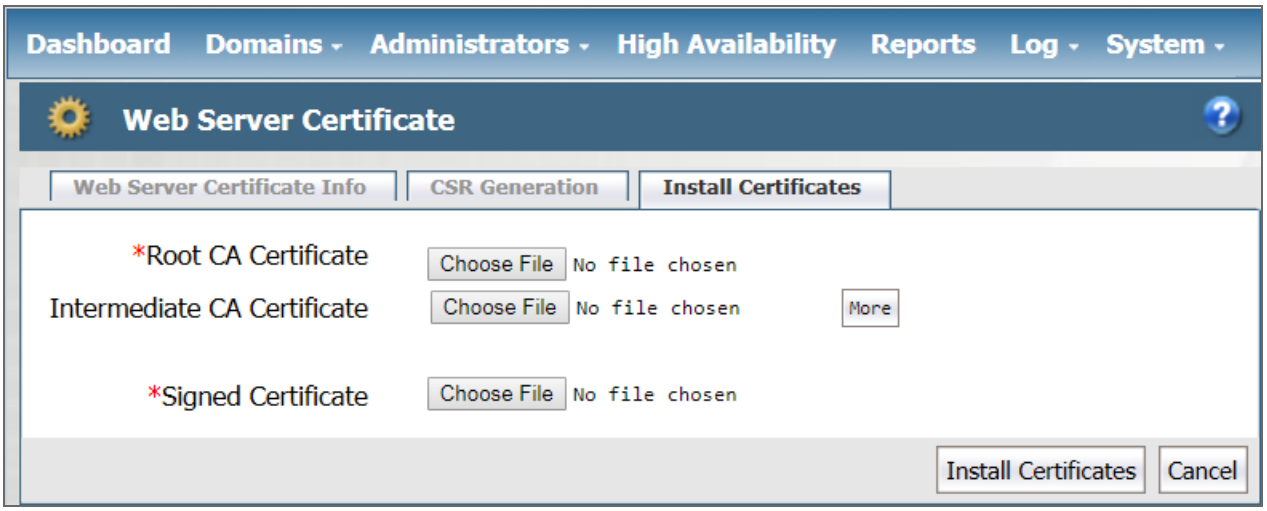
Field	Description
Organizational Unit	Typically a department or group name (up to 64 characters).
Organization	Typically the company name (up to 32 characters).
City or locality	Location of the Organization (up to 128 characters).
State or province	Location of the Organization. Refer to the external CA for format requirements. Some CAs will not accept an abbreviation for the name of the city or state (up to 128 characters).
Country Code	Abbreviation for the country where the Organizational Unit is located (up to 2 characters).

Install the signed certificate on the Thales KMS

Once you have received the signed certificate from the external CA, you are ready to import the signed certificate and the signer's certificate(s) to the Thales KMS.

Procedure

1. Log on to the Thales KMS web application as **SystemAdministrator**.
2. Click **System** > **Web Server Certificate**.
3. Click **Install Certificates**.



4. Load the Root CA Certificate.
   a. For the **Root CA Certificate** field, click the **Choose File** button.
   b. Select the root CA certificate from the external CA.
5. If the certificate is signed by the chain CA, then you must include the intermediate CA certificate.
   a. For the **Intermediate CA Certificate** field, click the **Choose File** button.
   b. Select the Intermediate CA certificate from the external CA.
6. If needed, load additional intermediate CA certificates.
   a. Click **More** to browse for additional Intermediate CA Certificates. You can select up to ten Intermediate CA Certificates.
7. Load the Signed Certificate.
   a. For the **Signed Certificate** field, click **Choose File**.

> When you copy any certificate, be sure to copy and paste the certificate just as it appeared originally. Make sure that there are no extra characters or leading spaces as this invalidates the certificate.

   b. (required) Select the Signed Certificate.

8 Click **Install Certificates**, and then click **OK**. The certificates are installed and the server is restarted. The restart takes several minutes.

During restart, do not close the browser. Do not select Back, Refresh, or the browser Stop buttons.

9 Verify the certificates.

a. After the server restarts, log on to the primary Thales KMS.

b. Click **System** > **Web Server Certificate**.

c. Click **Web Server Certificate Info**.

d. Check the following:

- If the Common Name (CN) entry in the Issued To and Issued By fields shows the same information, the current certificate is self-signed.
- If the CN entry in the Issued To and Issued By fields shows different values, the current certificate is not self-signed.

Create a Thales KMS administrative domain

A Thales KMS administrative domain is a logical partition that is used to separate administrators, and the data they access, from other administrators. Administrative tasks are performed in each domain based on each administrator user type. A Thales KMS administrative domain is not related to a network domain.

Types of administrative domains

- Global domain - Domain Administrators and Security Administrators that are assigned to a global domain are restricted to their assigned domains. The Administrators *can* be assigned to multiple domains.
- Restricted domain - Domain Administrators and Security Administrators assigned to a restricted domain are restricted to that particular domain. The Administrators *cannot* be assigned to multiple domains.

System Administrators are not members of domains. System Administrators can add and delete domains.

Domains and protected hosts

A domain is a group of one or more Thales KMS protected hosts under the control of an assigned Domain Administrator. Before a protected host can be administered, it must be placed in a domain.

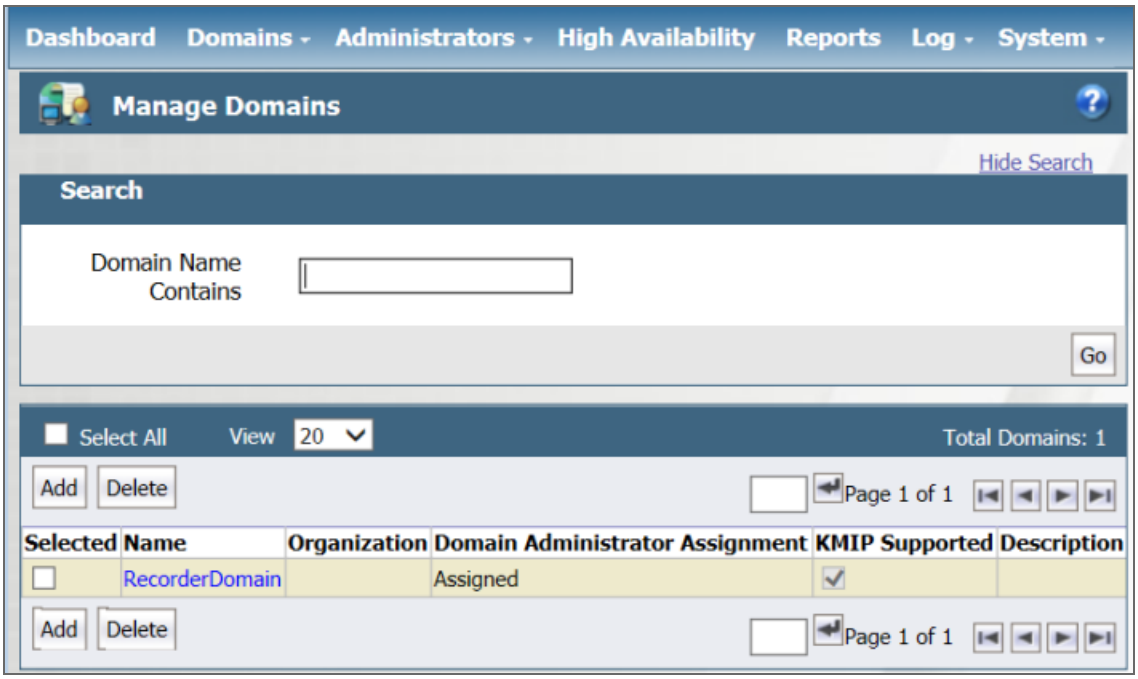
Create a domain

- Create a global domain named *RecorderDomain*

Procedure

1 Log on to the Thales KMS web application as **SystemAdministrator**.

2 Click **Domains** > **Manage Domains**.



3 Add the RecorderDomain.

a. On the **Manage Domains** page, click **Add**.

b. On the **Add Domain** page, on the **General** tab, name the domain **RecorderDomain**.

c. Complete the remaining fields, and then click **Ok**.

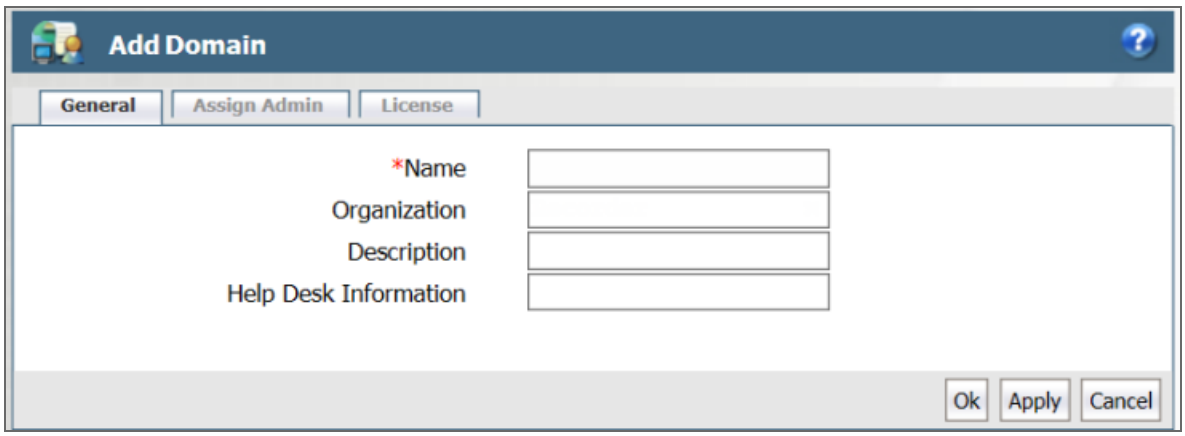
When configuring Security in Enterprise Manager, you must enter the same Domain Name entered here.

Related topics

Add Domain field descriptions, page 36

Add Domain field descriptions

The Add Domain page is used to add Thales KMS domains and then assign administrators to the domain. A protected host cannot be administered until it is placed in a Thales KMS domain.



Field	Description
General tab	
Name	Thales KMS domain name. Maximum characters: 64 The entry in the **Name** field must be the same name entered in the Domain field in Enterprise Manager.
Organization	(Optional) Name of the organization responsible for or administered by this Thales KMS domain.
Description	(Optional) Phrase or string of characters that identifies the Thales KMS domain. Maximum characters: 256
Help Desk Information	(Optional) The telephone number to call to get the response string for challenge-response authentication. Default: "Please contact a Security Server administrator for a response." The term Security Server refers to the Thales KMS.
Assign Admin tab	
The Assign Admin tab shows a list of administrators who have the required permissions to be the first administrator in a domain. You can assign only one administrator when you assign the first administrator to a domain. Later, that administrator can log on to the domain and add other administrators.	

Related topics

Create a Thales KMS administrative domain, page 34

Related information

Configure encryption management *(Security Configuration Guide)*

Assign users to the Thales KMS administrative domain

Once the RecorderDomain is created, you are ready to assign administrators to the domain.

Assign users to the Thales KMS administrative domain

- Assign the *DomainAdministrator* login to the *RecorderDomain*
- Assign the *SecurityAdministrator* login to the *RecorderDomain*

Before you begin

Create a Thales KMS administrative domain, page 34

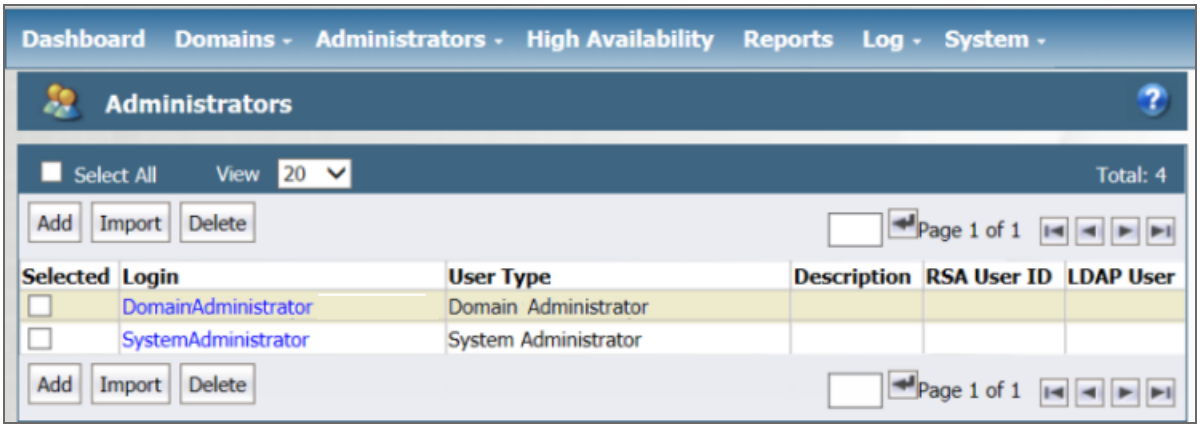
Procedure

1 Assign the DomainAdministrator login to the RecorderDomain. Only users with a role of domain displays.

a. Logged on to the Thales KMS web application as **SystemAdministrator**, click **Domains** > **Manage Domains**.

b. Click the **RecorderDomain** name.

c. Click the **Assign Admin** tab.



d. In the Selected column, click the option for the **DomainAdministrator** login.

e. Click **Ok**.

2 Assign the SecurityAdministrator login to the RecorderDomain.

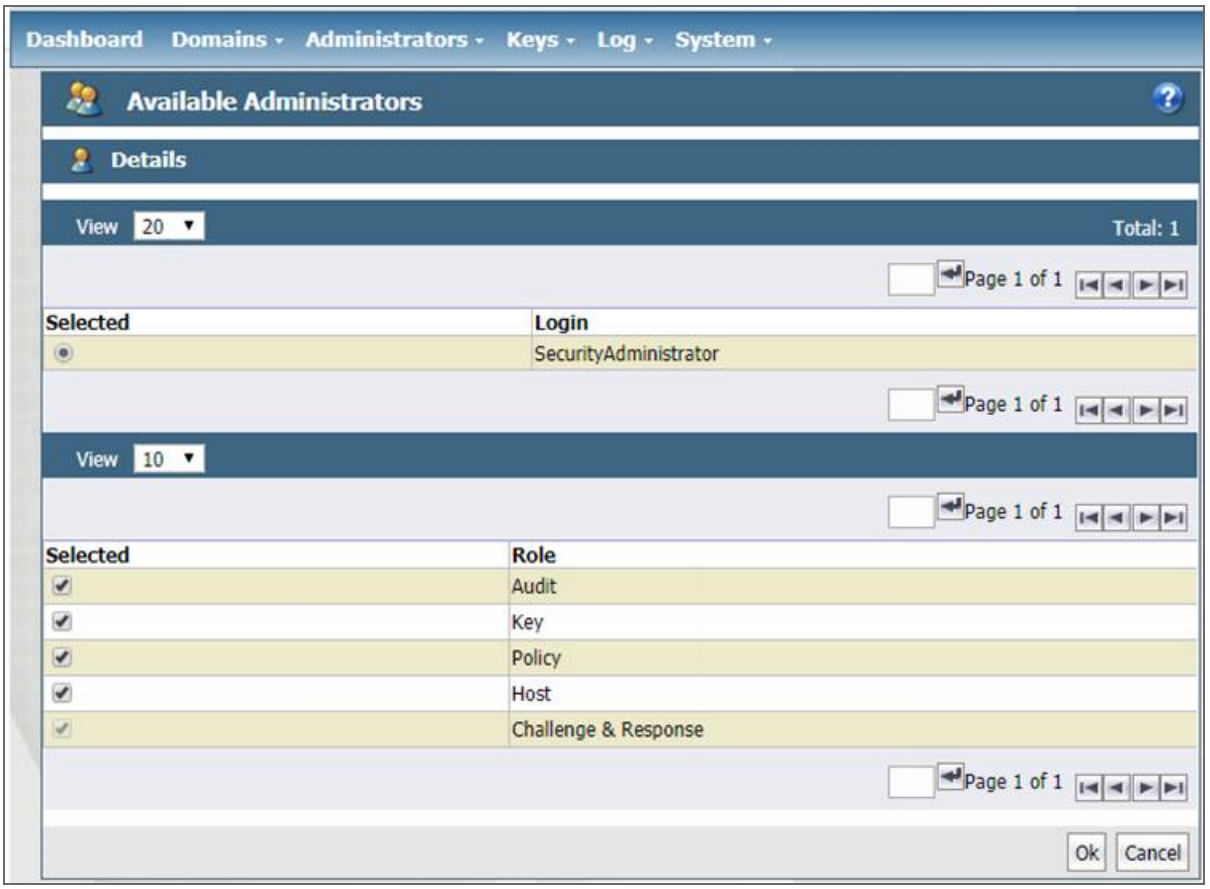
a. Log on to the Thales KMS web application as **DomainAdministrator**.

b. Click **Administrators** > **Domain**.

c. Click **Add to Domain**.

d. Select the **SecurityAdministrator** login.

e. Select all roles.



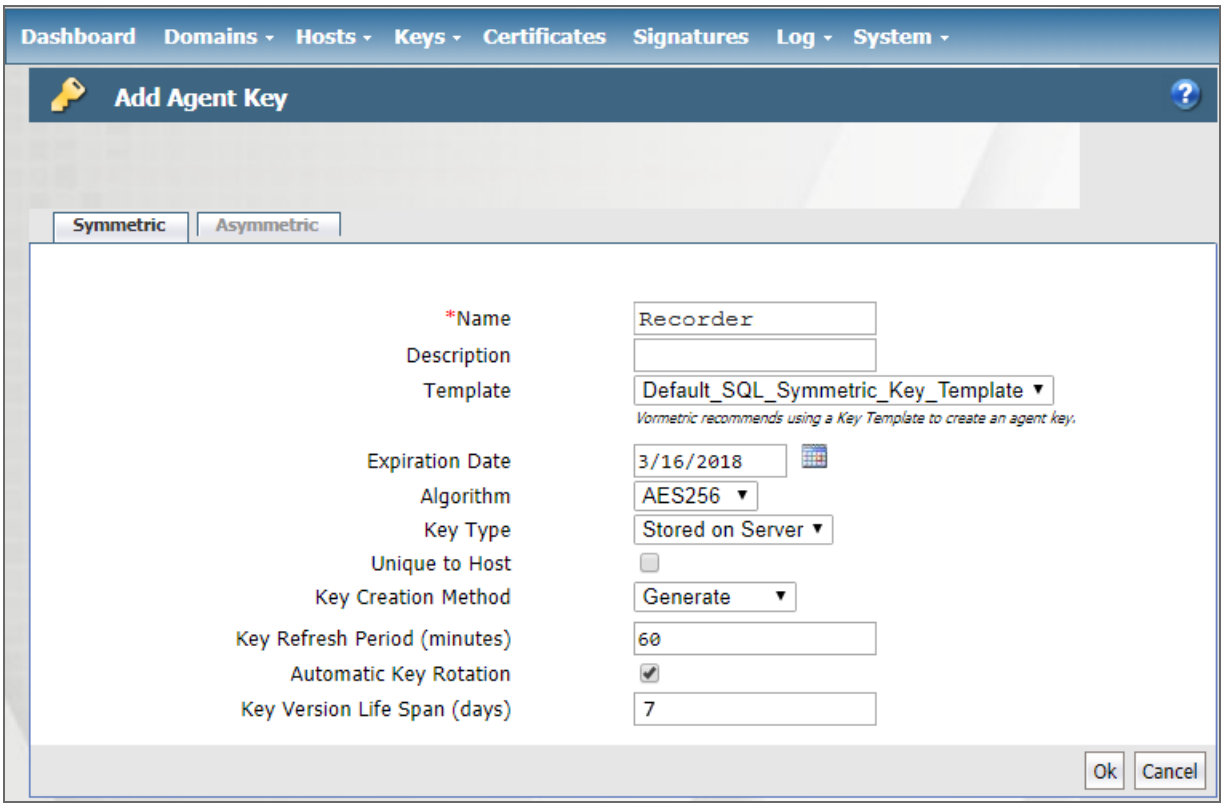
f. Click **Ok**.

Add agent key

The Thales KMS web application is used to create agent keys, as a secure centralized repository for storing and retrieving third-party encryption keys.

Procedure

1. Log on to the Thales KMS web application as **SecurityAdministrator** with *Key* role permissions.
2. Click **Keys** > **Agent Keys** > **Keys**.
3. Click **Add**.
4. Click the **Symmetric** tab.
5. It is important that the fields are completed as described in Add agent key field descriptions, page 39.



6. Click **Ok**.

Related information

Configure encryption management *(Security Configuration Guide)*

Add agent key field descriptions

The Thales KMS enables you to manually create symmetric keys using a pre-defined key template. The key template is used to create keys of a specific type with specific attributes.

Field	Description
Name	The name of the key. This field is mandatory. The entry in the **Name** field must be the same name entered in the Encryption Key Class field in Enterprise Manager. (ACR only) The Name *must be* lowercase "recorder."
Description	(Optional) Phrase or string that helps you identify the key.
Template	Always select **Default_SQL_Symmetric_Key_Template**.
Expiration Date	Date the key expires. Set the date in which the first version of the key will expire. For example, if your key rotation period is one day, then this date is set to tomorrow's date.
Algorithm	Always select **AES256**.
Key Type	The location for the generated key. Always select **Stored on Server**. Stored on Server keys are downloaded to non-persistent memory on the host. Each time the key is needed, the host retrieves the key from the Thales KMS. Stored on Server requires a constant network connection to the Thales KMS.
Unique to Host	This check box must be cleared.
Key Creation Method	This field must be set to the default, which is **Generate**. The key is generated automatically using a random seed.
Key Refresh Period (minutes)	The refresh period, in minutes. Values are from 1 to 44640 minutes, with 10080 minutes as the default value. When set outside of a domain (on the General Preferences page, System tab), the refresh period is applied globally, that is for all keys. Recommended setting: 5 minutes
Automatic Key Rotation	Always select this check box. The key is automatically rotated based on the expiry date and the period defined in the Key Version Life Span option.
Key Version Life Span (days)	This field is displayed once you enable the Automatic Key Rotation check box. This option specifies the frequency in which the keys are rotated, in days. Recommended setting: 7 days

Create a shared secret

Protected hosts (Application servers) are added and registered with the Thales KMS automatically. Before the protected hosts can be added and registered with the Thales KMS, a Thales KMS Administrator must

create a registration password.

Procedure

1 Log on to the Thales KMS web application as **SecurityAdministrator**.

2 Switch to the **RecorderDomain** domain.

   a. Go to **Domains** > **Switch Domains**.

   b. In the Selected column, click the option for the domain you want.

   c. Click **Switch to domain**.

If only one domain exists in the system, skip this step and continue to step 3

3 Click **Hosts** > **Registration Shared Secret** > **Registration Shared Secret**.

4 On the **Registration Shared Secret** page, complete the fields.

   - Create the **Registration Shared Secret** or automatically generate the password.

The entry in the **Shared Secret Key** field in Enterprise Manager must be the same as the password entered in the **Registration Shared Secret** field.

   - In the **Validity Date** field, enter an expiration date that is far into the future.
   - Make sure that the "Require that hosts are first added" check box is *not* selected.

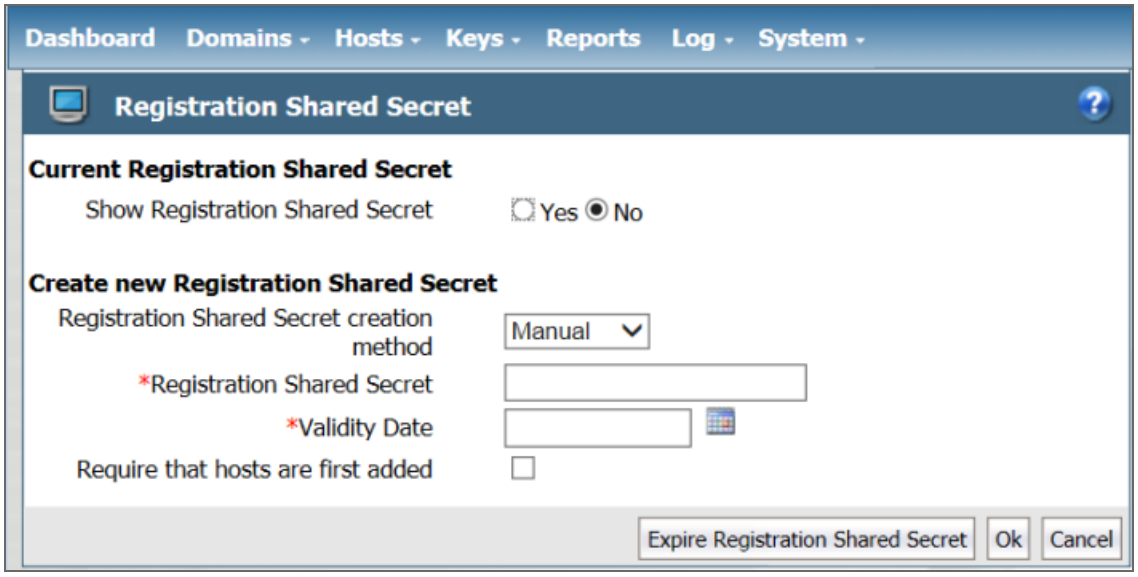
5 Click **Ok**.

Related topics

Registration Shared Secret field descriptions, page 42

Registration Shared Secret field descriptions

The Registration Shared Secret page is used to create a registration password for a domain or host group. The registration password is required to use the shared secret method to add and register protected hosts with the Thales KMS.



Field	Description
Current Registration Shared Secret	
Show Registration Shared Secret	Displays the secret when Yes is selected. Default: No This field does not display if the registration shared secret feature is not used.
Create new Registration Shared secret	
Registration Shared creation method	Create the shared secret yourself or automatically generate the password.

Field	Description
Registration Shared Secret	If entering the password manually, the password criteria are: • Does not have repeating characters • Uses at least 1 upper and 1 lowercase character • Uses at least 1 special character The entry in the **Registration Shared Secret** field must be the same as the password entered in the Shared Secret Key field in Enterprise Manager.
Validity Period	In MM/DD/YY format, enter the period in which the shared secret is valid. For the system to work without manual intervention, the validity period should be set to a date far into the future. For example, 5 years in the future.
Require that hosts are first added	Do *not* select the Require that hosts are first added option. When selected, you must add the host to the Thales KMS database with the Registration Allowed check box enabled before you install and configure the agent.

Related topics

Create a shared secret , page 40

Related information

Configure encryption management *(Security Configuration Guide)*

Configure the Key Management Server settings *(Enterprise Manager Configuration and Administration Guide)*

Verify host communication with the Thales KMS

Verify that the host can communicate with the Thales KMS. To silently register the host with the Thales KMS, connectivity is required.

Procedure

1. Log on to the Application server.
   a. Search for the Command Prompt program.
   b. In the search results list, right-click the **Command Prompt** program, and then click **Run as administrator**.
2. From the Command Prompt, verify that the host can communicate with the Thales KMS.

   ```
   ping <Thales KMS_host_name or FQDN>
   ```

Chapter 3

Thales Key Manager Server High Availability installation and configuration

You must have two Thales KMSs installed on the network to create a high availability system—a primary Thales KMS and a failover Thales KMS.

Topics

Workflow: Failover Thales KMS installation and configuration

The High Availability configuration consists of two Thales KMSs—one Thales KMS installation acts as the primary Thales KMS and the other becomes the failover Thales KMS.

After the primary and failover KMSs initial configuration, all configuration settings occur on the primary Thales KMS only. Changes after the installation and configuration includes changes to administrators, hosts, keys, and policies. Configuration changes and updates on the primary Thales KMS is pushed to the failover Thales KMS at set intervals.

Generating new keys

Since the failover Thales KMS is in read-only mode, the failover Thales KMS will *not* issue new keys. New keys can only be generated by the primary Thales KMS.

Workflow

Install the software on the failover Thales KMS

1 Prerequisites for the Thales KMS installation, page 10

Prior to installing the Thales KMS software, you must complete the prerequisite tasks. Tasks include, getting the Thales KMS installation file, recording the information needed to configure the software, and opening the necessary ports.

2 Deploy the Thales KMS software on VMware, page 12

The Thales KMS software is deployed using the Thales KMS Virtual Machine (OVA) template file. The template file includes all the software required by the Thales KMS.

Or

Deploy the Thales KMS software on Hyper-V, page 13

The Thales KMS software is deployed using an ISO file. The file includes all the software required by the Thales KMS.

Configure the software using the CLI on the failover Thales KMS

3 Log on to the Thales KMS command-line interface, page 16

Before you can complete the preliminary Thales KMS configuration tasks, you must log on to the command-line interface (CLI).

4 Disable DHCP, page 18

Before you can assign a static IP address to the Thales KMS, you must disable DHCP on the eth0 interface.

5 Configure the network settings, page 18

Because the Thales KMS uses a static IP address, you must configure the network settings. The network settings are configured using the CLI.

6 Configure the NTP, time zone, date, and time, page 19

You must have the correct time set on your KMS(s) as this affects system functions such as protected host registration, log timestamps, high availability cluster synchronization, and certificate exchange. Although configuring a network time protocol (NTP) server is not mandatory, it is recommended.

7 Configure the host name, page 20

Configure the host name by entering the fully qualified domain name (FQDN) for the Thales KMS.

8 Generate the Thales KMS certificate authority, page 21

After completing the preliminary configuration, on the primary Thales KMS, generate the Thales KMS certificate authority (CA). The certificate is used to access the Thales KMS web interface.

High availability configuration using the web interface and the CLI

9 Log on to the Thales KMS web user interface, page 23

You will log on to the Thales KMS web user interface using the default logon and password. After you log on for the first time, you are prompted to enter a new password. You will need this password to log on to the web interface. Be sure to keep the password in a safe location.

10 Upload the Thales KMS license file, page 23

When you log on to the Thales KMS for the first time, the dashboard displays "License not found." In addition, the only tabs that are available are the Dashboard and the System tabs. Once the license is uploaded, all the menu items available according to your license file are displayed.

11 Back up the Thales KMS manually, page 59

In case you need to roll back the Thales KMS upgrade, you must create a wrapper key, export the key, and then perform a system level backup.

12 Upgrade the server software, page 28

You can upgrade the Thales KMS software using the Thales KMS web application. The Thales KMS can hold up to two images. If you have two images on your system, you must delete the one that is not active before you can upload a new image.

13 Generate a certificate signing request, page 30

The Thales KMS can be configured to get certificates signed by an external Certificate Authority (CA). An external CA can be configured on a single node or a high availability (HA) system. Using an external CA is an optional procedure.

14 Install the signed certificate on the Thales KMS, page 33

Once you have received the signed certificate from the external CA, you are ready to import the signed certificate and the signer's certificate(s) to the Thales KMS.

15 Designate the primary and failover Thales KMSs , page 48

The failover Thales KMS must be added to the primary Thales KMS. In addition, the primary Thales KMS must be added to the failover Thales KMS.

16 Register the failover Thales KMS with the primary Thales KMS, page 49

For a new installation, the convert2failover command is used to reinitialize the failover Thales KMS.

17 Configure replication on the primary Thales KMS, page 52

After the failover Thales KMS is configured, you need to configure the primary Thales KMS to replicate its information to the new failover Thales KMS.

Designate the primary and failover Thales KMSs

The failover Thales KMS must be added to the primary Thales KMS. In addition, the primary Thales KMS must be added to the failover Thales KMS.

Before you begin

Before high availability can be configured, verify the following procedures are complete:

- The signed certificate is installed on the *primary* and *failover* Thales KMS.
- The primary and failover Thales KMS server names are case sensitive. Use the server name display in the CLI to determine the server name.

To display the server name, do the following:

- Log on to the failover Thales KMS CLI.
- Access the system command prompt, and then display the system information.

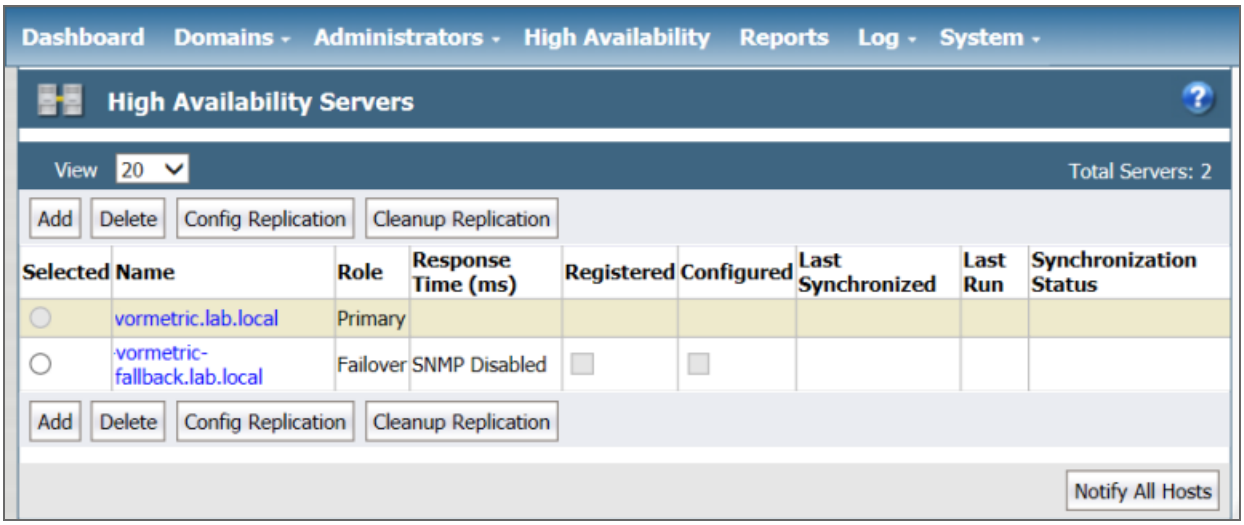
```
0000:vormetric$ system
0001:system$ setinfo show
```

- Repeat for the primary Thales KMS.

Use the host name value identified here when configuring high availability for the failover and primary Thales KMS.

Procedure

1. Add the failover Thales KMS to the primary Thales KMS.
   a. On the primary Thales KMS, log on to the Thales KMS web application as **SystemAdministrator**.
   b. In the menu bar, click **High Availability**.
   c. Click **Add**.
   d. On the **Add High Availability Server** window, in the **Server Name** field, enter the host name or FQDN of the failover Thales KMS. Use the host name identified in Before you begin.
   e. Click **OK**.



Register the failover Thales KMS with the primary Thales KMS

For a new installation, the convert2failover command is used to reinitialize the failover Thales KMS.

Before you begin

- The primary and failover Thales KMS server names are case sensitive. Use the server name display in the CLI to determine the server name.

To display the server name, do the following:

- Log on to the primary Thales KMS CLI.
- Access the system command prompt, and then display the system information.

```
0000:vormetric$ system
0001:system$ setinfo show
```

Procedure

1 On the failover Thales KMS, log on to the Thales KMS CLI.

2 Using the CLI, from the main menu, access the ha category and reinitialize the failover Thales KMS.

```
0001:vormetric$ ha
0002:ha$ convert2failover
```

Output similar to the following is displayed.

```
WARNING: This server will now be converted to a failover server.
Make sure the primary server is running and has this server on its
failover server list.
This may take several minutes. After converting to failover, you must
configure replication for this failover server from the primary
server.
After HA is set up, make sure all the cluster server nodes are in the
same suiteb mode.
Continue? (yes|no)[no]:
```

3 At the Continue? prompt, type **yes**, and then complete the following prompts:

a. **Primary Security Server host name:**

Type the hostname or FQDN of the primary Thales KMS identified in Before you begin.

b. **Primary Security Server system administrator name:**

Type the name of an administrator of type System Administrator or All that is configured on the primary Thales KMS.

c. **Primary Security Server system administrator password:**

Type the administrator's password.

d. **Enter the host name of this computer. This will be used by Agents to talk to this Security Server.**

Type the hostname or FQDN of the failover Thales KMS.

4 The primary Thales KMS uses the following information for key and certificate generation.

a. **What is the name of your organizational unit? []**

b. **What is the name of your organization? []**

c. **What is the name of your City or Locality? []**

d. **What is the name of your State or Province? []**

e. **What is your two-letter country code? [US]**

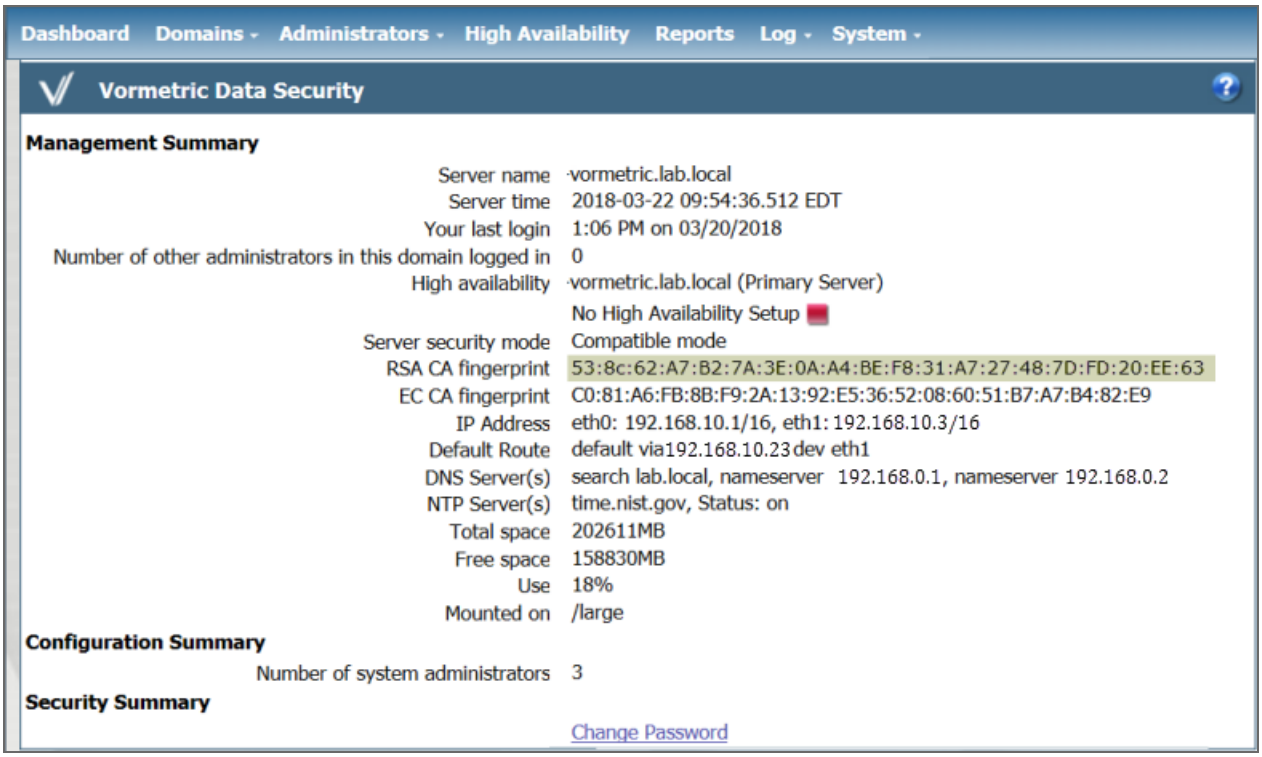
5 Type **yes** to continue. The installation utility creates certificates, completes the installation process, and then starts the Thales KMS. This may take a few minutes.

Output similar to the following is displayed.

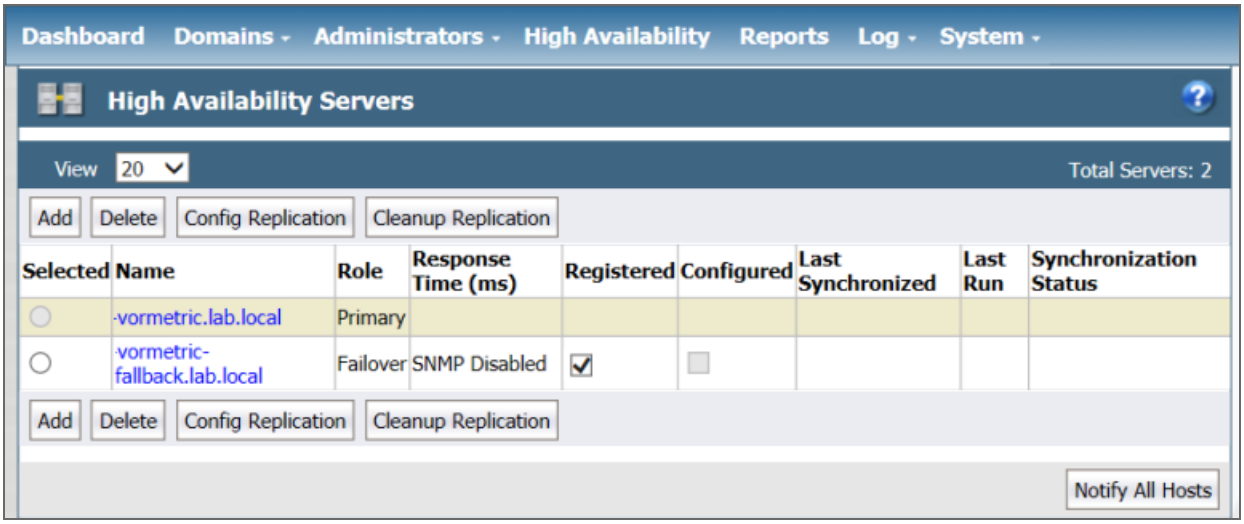
```
Primary_Server=sys1.mycompany.com
CAs_
Fingerprint=53:8C:62:A7:B2:7A:3E:0A:A4:BE:F8:31:A7:27:48:7D:FD:20:EE:
63
Ensure the fingerprint listed above matches the one on the primary
Security Server web console dashboard.
SUCCESS: convert server to failover server. The server is started.
Please verify the fingerprint
0003:ha$
```

6 On the primary Thales KMS, log on to the Thales KMS web interface as **SystemAdministrator**.

a. Click the **Dashboard** tab.
b. Match the fingerprint from the output (shown in yellow in step 5) on the primary Thales KMS with the RSA CA fingerprint on the Dashboard.



c. Click the **High Availability** tab.
d. In the row for the failover Thales KMS, verify the **Registered** check box is selected.



Related topics

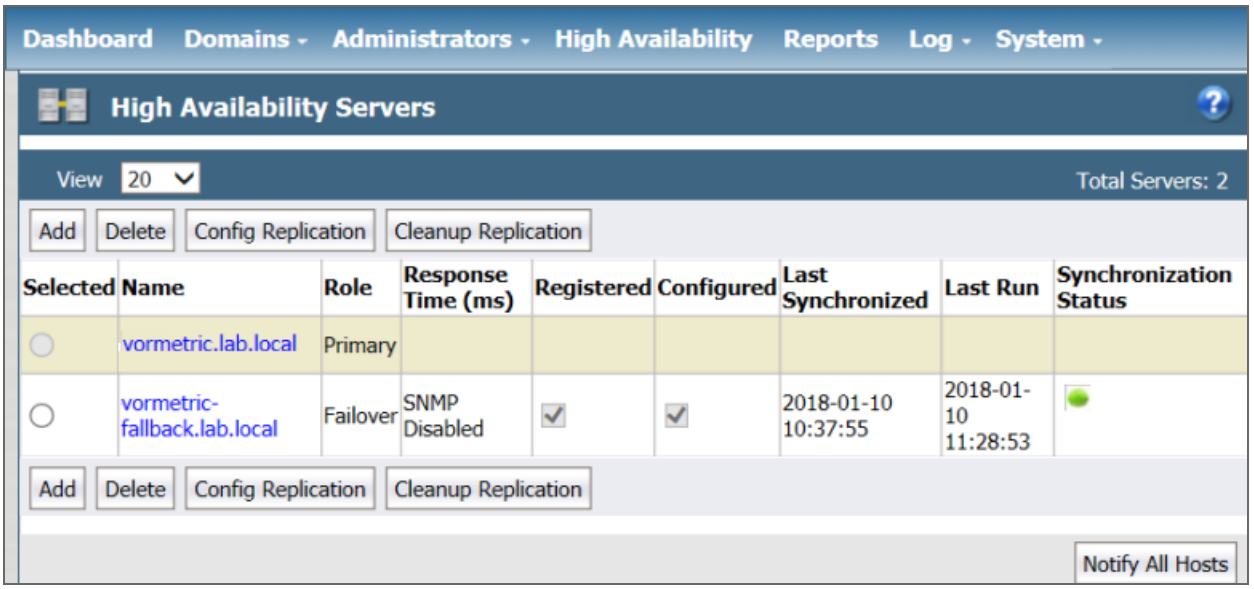
Primary server is not configured during failover registration, page 77

Configure replication on the primary Thales KMS

After the failover Thales KMS is configured, you need to configure the primary Thales KMS to replicate its information to the new failover Thales KMS.

Procedure

1. Log on to the primary Thales KMS web application as **SystemAdministrator**.
2. Click the **High Availability** tab.
3. Under **Selected**, select the failover Thales KMS.
4. Click **Config Replication**.
5. Click **OK** to continue. Once the configuration is complete, the Configured check box for the failover Thales KMS is enabled.



6. Click **Notify All Hosts**.
7. For the failover server, verify the **Synchronization Status** field shows a green circle. The green circle indicates that the failover Thales KMS is synchronized with the primary Thales KMS.

Thales Key Manager Server backup and restore

Backup and recovery procedures for the Thales KMS is essential to maintaining your system. If a backup and recovery mechanism is not in place, some or all encryption keys might be lost. If encryption keys are lost, recordings encrypted with the lost keys cannot be used.

All backups are the sole responsibility of the customer IT department. The customer is responsible for scheduling and maintaining an automatic backup.

Topics

Backing up the Thales KMS

A backup of the Thales KMS is a snapshot of a Thales KMS configuration at a point in time. When a backup is restored, the Thales KMS web interface displays the same information captured at the time the backup was originally made. Any changes made after the last backup are not restored.

Backup types

There are two types of back ups that can be performed on the Thales KMS. The backup types are system-level backup and domain-level backup. This guide provides instructions for performing system-level backups.

About system-level backups

System-level backup
System administrators create the backup.
Configuration information for the complete Thales KMS system is backed up, including the following: • web server certificate • certificates • system preferences • log preferences • users • domains • hosts • encryption keys • signatures • policies • GuardPoints • license information, including all configuration information in all domains
Thales KMS users are backed up.
GuardPoints and host-sharing information is backed up.

What is not backed up?

System-level configuration such as network and timezone settings are *not* backed up. These settings remain unchanged after a restore operation.

Wrapper key

Thales KMS backup files are encrypted with a wrapper key to keep them secure. This wrapper key must be created, or imported from a previous create operation, before creating a backup. The same wrapper key used to encrypt a backup is also required to restore that Thales KMS backup.

Hand over the wrapper key to the customer. The wrapper key stays in the custody of the customer. The key is required to restore backup data in case of disaster.

Key shares

For additional security, wrapper keys can be broken up into key shares—pieces of a wrapper key. These key shares can then be divided among two or more custodians. Each custodian must contribute their key share to assemble a complete wrapper key.

For example, you can break up the wrapper key among a total of five custodians and set the minimum number of required custodians at two. When the wrapper key is required, at least two of the custodians must contribute their key share to assemble a complete wrapper key.

It is recommended that you have one custodian only.

Email notifications

You can set up an email alert to notify the appropriate people if a FATAL or ERROR message is generated during the backup. See Related topics for a link to the instructions.

Related topics

Configuring email notifications, page 73
Create a wrapper key, page 55
Workflow: Schedule automatic Thales KMS backups, page 1
Back up the Thales KMS manually, page 59

Create a wrapper key

Thales KMS backup files are encrypted with a wrapper key to keep them secure. This wrapper key must be created, or imported from a previous create operation, before creating a backup. The same wrapper key used to encrypt a backup is also required to restore that Thales KMS backup.

Regardless of the type of backup that will be performed (automatic or manual), a wrapper key is required.

Procedure

1. Log on to the Thales KMS web application as **SystemAdministrator**.
2. Create a wrapper key.
   a. Click **System** > **Wrapper Keys**.
   b. In the **Wrapper Keys** window, from the **Operation** menu, click **Create**.
   c. Click **Apply**. A confirmation key message stating that the key exists is displayed.
   d. On the warning box, click **Ok**.
3. Export the wrapper key.
   a. In the **Wrapper Keys** window, in the **Operation** list, click **Export**.
   b. Set a number for the **Minimum Custodians Needed** and the **Total Number of Custodians**.

      This setting splits the wrapper key value among multiple custodians. If only a single administrator is to control the wrapper key, enter a value of 1 in both fields.
   c. Select the check box next to the Thales KMS administrator(s) who will serve as custodians for the wrapper key shares. Only administrators of type System Administrator are listed. Any of these administrators, except for the default initial log-on administrator *admin*, can be selected as a custodian.

d. Click **Apply**. The generated wrapper key or key shares are exported and are visible on the Dashboard.

4 Ask each administrator to securely store a copy of their unique key.

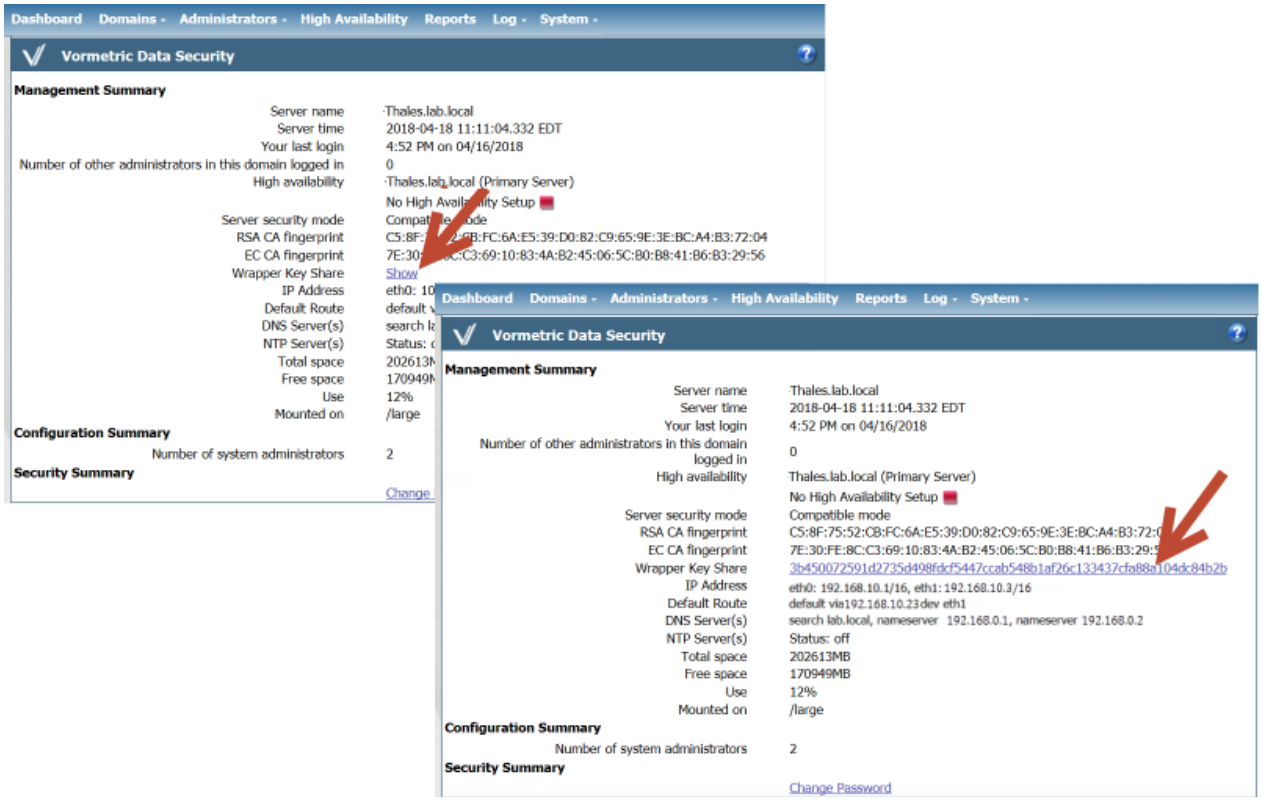
a. Log on to the Thales KMS web application using their user name. The user type is System Administrator.

b. Click **Dashboard**.

c. The Wrapper Key Share displayed in the Dashboard is a toggle. Click **Show** to display the wrapper key share value. Click **Wrapper Key Share** value to display the string **Show**.

The key share displays beneath the fingerprint for the CA.

Be sure to store the wrapper key in a safe location. The same wrapper key used to create the backup is required to restore the backup.



What to do next

Workflow: Schedule automatic Thales KMS backups, page 1

Or

Back up the Thales KMS manually, page 59

Configure a backup schedule for Linux using the web application

Use the Automatic Backup page to create a daily or weekly schedule to automatically back up a Thales KMS configuration to a target host that is running Linux.

About the authorized keys file

You will create an authorized keys file on the Thales KMS and then copy the file to the target host. The authorized keys file is a public key that is used to authenticate the SCP user. The file allows the user to access the target host without a password.

Before you begin

- Create a wrapper key, page 55
- It is the customers responsibility to verify that the file share is available and has enough memory.

Procedure

1 Create the authorized keys file using the Thales KMS web application.
   a. Log on to the Thales KMS web application as **SystemAdministrator**.
   b. Click **System** > **Backup and Restore** > **Automatic Backup**.
   c. Enter the settings for the **Automatic Backup Schedule**.
   d. In the **Active Settings** field, select **SCP**.
   e. To download the **authorized keys** file, click on the **Click to Export** hyperlink. You will copy the authorized keys file to the target host later in this procedure.

2 Copy the authorized keys file from the Thales KMS to the target host.
   a. On the target host, create a username that will be used to copy the backup file from the Thales KMS to the target host.

      You will enter this username in the Thales KMS web application later in this procedure.
   b. Log on to the target host using the username you just created.
   c. Create a backup directory.

      ```
      # mkdir KMS_Backup
      ```
   d. Change to the .ssh directory for the username that will copy the backup file.

      ```
      # cd /root/.ssh/
      ```
   e. Copy the **authorized keys** file from the Thales KMS to the **/home/<username>/.ssh** folder on the target host.
   f. List the contents of the directory in long form, including hidden files.

      ```
      # ls -al
      ```

      Output similar to the following is displayed:

```
total 12
drwx------. 2 root root 48 May 11 2019 .
dr-xr-x---. 15 root root 4096 May 28 11:38 ..
-rw-r--r--. 1 root root 402 May 11 2019 authorized_keys
-rw-r--r--. 1 root root 1577 Feb 21 11:30 known_hosts
```

3 In the Thales KMS web application, on the **Automatic Backup** page, complete the remaining **External File Server** fields:

- Directory in which to store the backup files on the target host.
- User name that will be used to copy the backup files to the target host.

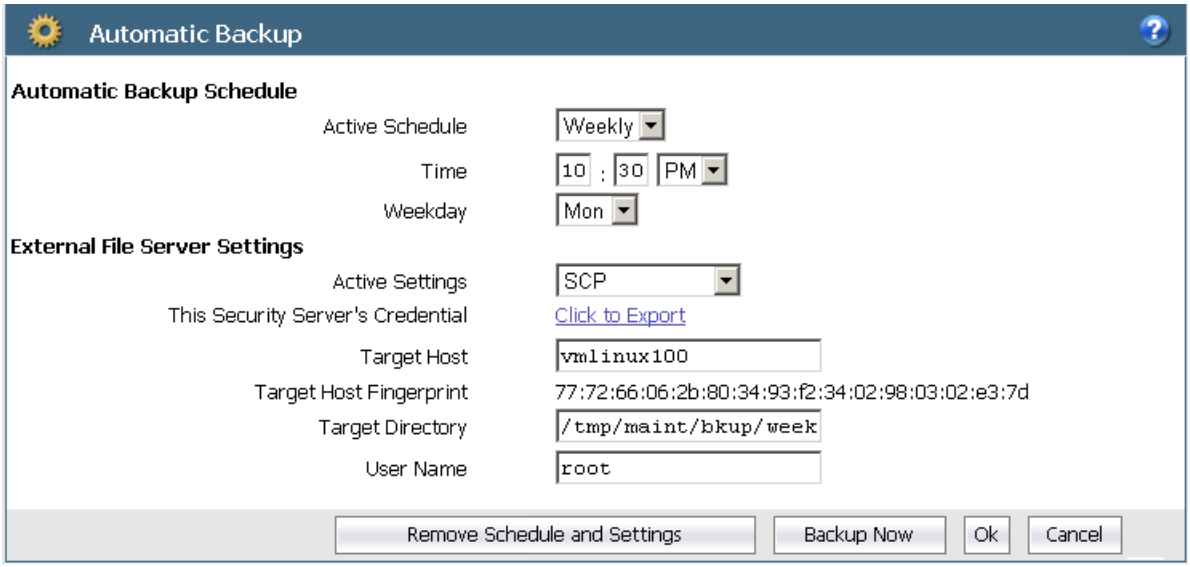
Related topics

Automatic backup field descriptions for Linux, page 58

Automatic backup field descriptions for Linux

The fields required to back up the Thales KMS to a target host that is running Linux is described.

SCP example



Automatic backup schedule

Field	Description
Active Schedule	The frequency in which the Thales KMS is backed up. Options are weekly and daily.

Field	Description
Time	The time, in 12-hour format, in which the backup takes place. The time is relative to the Thales KMS system clock.
Weekday	The day of the week in which the Thales KMS backup takes place.

External file server settings for secure copy protocol (SCP)

Field	Description
Active Settings	The mode in which to copy the generated backup file to the target host. The selected mode determines the configuration parameters that display. Select SCP. Note: To use the SCP mode, SSH must be configured on the target host.
This Security Server's Credential	To download the Thales KMS public key, click this option. Copy the public key onto the target host and into ~/user/.ssh/authorized_keys. The Thales KMS public key is required to use SCP to copy the backup file to the external file server.
Target Host	The host name, IP address, or FQDN of the destination system.
Target Host Fingerprint	The fingerprint of the Thales KMS public key that is currently on the target host. The fingerprint is retrieved from the target host and displayed in the Automatic Backup page during a backup. You can verify if the public key on the target host is current by comparing the key in ~/user/.ssh/authorized_keys on the target host with the key generated by Click to Export.
Target Directory	On the destination system, the full directory path in which to copy the backup file.
User Name	The name of the user to perform the copy operation. The name must be a valid user on the target host. Copy the public key into the ~/.ssh/authorized_keys file in the home directory of the user you specify in this field.

Back up the Thales KMS manually

In case you need to roll back the Thales KMS upgrade, you must create a wrapper key, export the key, and then perform a system level backup.

Before you begin

Create a wrapper key, page 55

Procedure

1 Back up the current Thales KMS configuration.

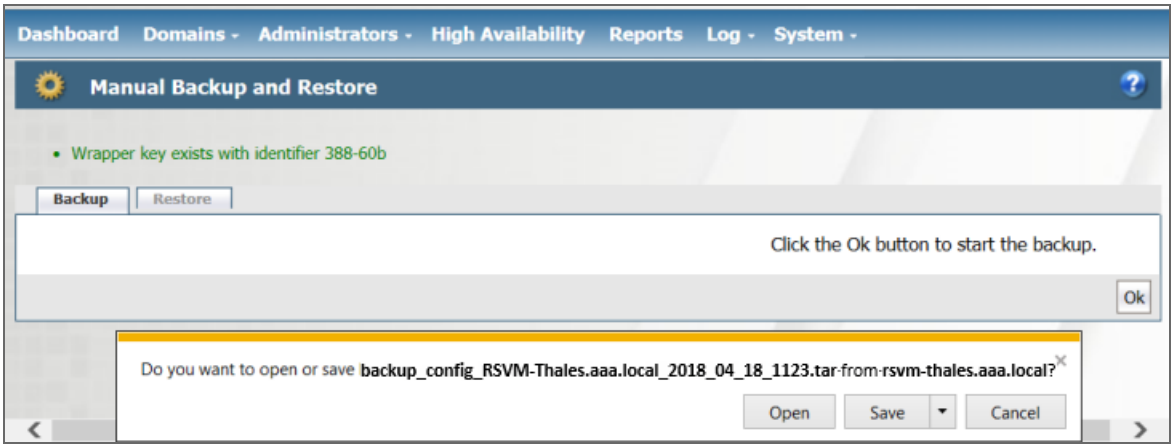
a. Log on to the Thales KMS web application as **SystemAdministrator**.

b. Click **System** > **Backup and Restore** > **Manual Backup and Restore**.

c. On the **Manual Backup and Restore** page, click the **Backup** tab.

d. Click **Ok**.

e. On the file download box, click **Save**. Save the file to a secure location that you are sure will still be accessible if the Thales KMS fails.



The default file name is:

`backup_config_<Thales KMS name>_yyyy_mm_dd_hhmm.tar`

Where **`<Thales KMS name>`** is the FQDN of the Thales KMS being backed up.

2 Using the steps in this procedure, back up the failover Thales KMS.

Restore from backup

In the event of a software crash recovery or system changes, a Thales KMS backup can be used to restore the hosts, encryption keys, policies, as well as other configuration information of a Thales KMS.

Following a restore operation, the Thales KMS configuration in the web application is replaced by the configuration stored in the backup copy. Any new encryption keys, policies, hosts, and GuardPoints added since the last backup are overwritten and lost.

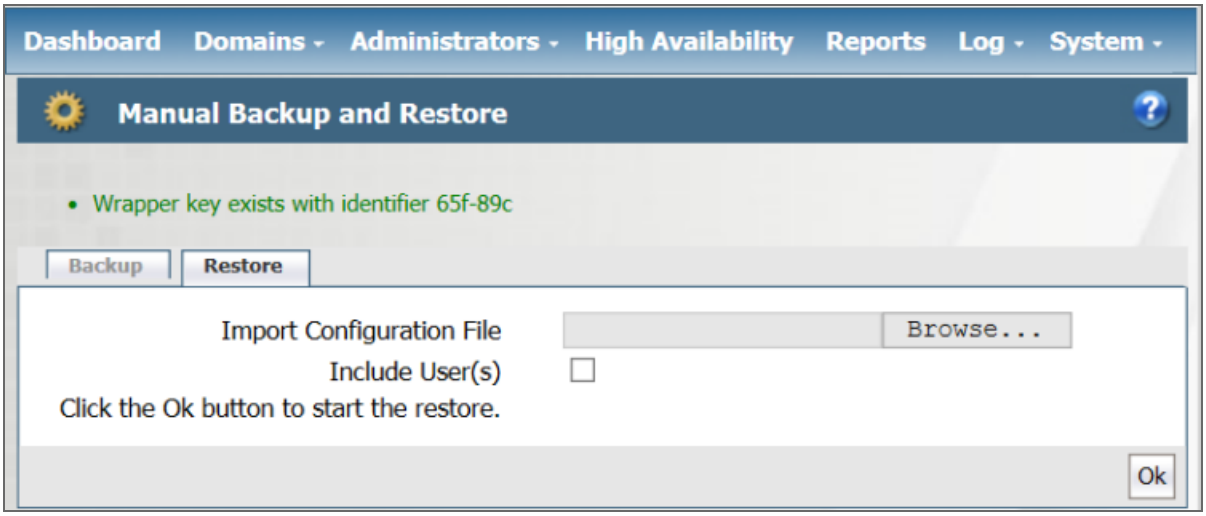
A system level backup can be restored to the same Thales KMS or another Thales KMS.

Before you begin

Prior to backing up the software, if you created key shares from the wrapper key, get the key shares from the custodians. A key share must be imported for at least as many times specified by the Minimum Number of Custodians value when the wrapper key was exported.

Procedure

1 Import the wrapper keys used to create the backup.
   a. Log on to the Thales KMS web application as **SystemAdministrator**.
   b. Click **System** > **Wrapper Keys**.
   c. In the **Wrapper Keys** window, in the **Operation** list, click **Import**.
   d. Click **Add**.
   e. Get a key share and paste it into the Key Share text field, and then click **Ok**.
      If you have chosen to have more than one custodian for the wrapper key shares, repeat step e for each administrator selected as a key custodian.
   f. Click **Apply** to finish importing the wrapper key.
2 Restore the backup file.
   a. Click **System** > **Backup and Restore** > **Manual Backup and Restore**.
   b. Click the **Restore** tab.



c. Click **Browse**, and then locate and select the backup file you want to restore.
d. If restoring a system level backup, and you want to restore users, select **Include User(s)**.
e. Click **OK**.

   A dialog box opens and tells you that the session will be terminated and you will have to log back in.
f. Click **OK**.
g. Wait a minute before starting another web application session.
h. Open the Thales KMS web application and verify that the configuration is restored correctly.

Thales Key Manager switch over procedure - Disaster recovery

If a disaster occurs that destroys the primary Thales KMS, you can promote the failover Thales KMS to the primary Thales KMS. The failover Thales KMS then operates as the primary Thales KMS.

If the failover Thales KMS is *not* promoted to primary and a new Application server is added to the enterprise, the new Application server cannot register with the failover Thales KMS. Since the Application server is not registered, the Application server cannot retrieve keys.

Topics

Convert a failover Thales KMS to a primary Thales KMS

Generally, the reason for converting a failover Thales KMS to a primary Thales KMS is because the primary is no longer operational. Converting the failover Thales KMS to the primary Thales KMS is useful when you do not have a current backup of the primary Thales KMS. The failover Thales KMS contains the same database information as the primary Thales KMS at the time the failover Thales KMS was last synchronized.

Procedure

1. Run the convert2primary command.
   a. Log on to the failover Thales KMS CLI.
   b. Using the CLI, access the high availability category and convert the failover Thales KMS to the primary Thales KMS.

      ```
      0001:vormetric$ ha
      0002:ha$ convert2primary
      ```

      ```
      WARNING: We will now convert this failover server to primary server.
      This may take several minutes. Continue? (yes|no)[no]:
      ```

   c. At the **Continue?** prompt, type **yes**.

      ```
      SUCCESS: convert server to primary server. The server is restarted.
      ```

2. Log on to the new primary Thales KMS web application as **SystemAdministrator**.
3. **On the Application servers, in Enterprise Manager, change the primary Thales KMS to the new primary Thales KMS**.

Related information

Workflow: Configure data-at-rest-encryption *(Security Configuration Guide)*

Appendix B

Thales Key Manager Server administration

Thales KMS administration describes tasks that are not necessarily part of the initial Key Manager Server setup, but are tasks that you may need to perform after your system is installed.

Topics

Configuring SNMP

Simple Network Management Protocol (SNMP) is a full-featured protocol that is used to manage and monitor network nodes like hosts and routers. The specific attributes of network nodes that can be managed and monitored by SNMP are configured as objects in a Management Information Base (MIB). The Thales KMS can be enabled as an SNMP agent and then monitored by SNMP servers using the set of MIB objects described.

Overview

The Thales KMS supports SNMP version 1 or 2. SNMP is not used to manage Thales KMSs. A small set of MIB objects is provided with which to query Thales KMS configuration and status information.

The primary Thales KMS database is replicated to the failover Thales KMS in a high availability cluster, distributing the same SNMP configuration to the failover server. Therefore, SNMP servers that can query the primary Thales KMS can also query each failover Thales KMS with the same community string.

Polling the primary and failover Thales KMSs

When the Thales KMS receives an SNMP GET request from an SNMP server, the Thales KMS locates the Object IDentifier (OID) entry in the MIB and returns its value to the SNMP server.

If SNMP is enabled on the primary Thales KMS, the primary Thales KMS polls itself and the failover Thales KMS using an SNMP GET request at five-minute intervals. The response time for the failover Thales KMS is displayed in the High Availability Servers window in milliseconds. If SNMP is disabled, the Response Time column displays "SNMP Disabled". If the failover Thales KMS cannot be reached, the Response Time column displays "Not Reachable".

SNMP traps

SNMP traps are not supported at this time and cannot be configured on the Thales KMS.

Enable SNMP on the Thales KMS

You can define the SNMP community string with which to query the Thales KMS.

About the SNMP Access Control List

If the SNMP Access Control List (ACL) is empty, SNMP requests from any IP address is acknowledged. If the SNMP ACL is defined to allow only certain IP addresses (for example, 10.1.2.3) or IP address blocks (for example, 10.1.2.*) to go through, the Thales KMS only acknowledges requests from IP addresses specified in the SNMP ACL.

The community string and IP address are the only credentials used to verify the legitimacy of the SNMP request. The community string is typically set to a factory default value of “public.” This string must be the same for all devices in the same group for SNMP monitoring to function. For security reasons, the Network Administrator should change the community string from “public” to a custom value.

We recommend that you do not enable SNMP on the Thales KMS unless it is required, as this could pose a security risk. If you do enable SNMP on the Thales KMS, we recommend that you use an SNMP ACL to restrict access to this service, and change the default community string from 'public' to a custom value.

SNMP in a high-availability environment

The failover Thales KMS in a high availability cluster shares the same SNMP configuration as the primary Thales KMS. Enable SNMP listening on the primary Thales KMS and SNMP listening is enabled on the failover Thales KMS.

The community string that you enter is applied to the primary Thales KMS and the failover Thales KMS in the high-availability cluster. This means that an SNMP server that is allowed to query the primary Thales KMS can also query the failover Thales KMS in the high-availability cluster.

If the failover Thales KMS in a high-availability configuration does not respond to SNMP requests, restart the failover Thales KMS to resolve the issue.

Ports

GET requests can be sent to port 161 or port 7025.

Procedure

1. Log on to the Thales KMS web application with a user type of System Administrator.

   Do not enter a domain.
2. Go to **System** and then click **SNMP**.
3. On the **Configuration** tab, select **SNMP Enabled** to make the Thales KMS listen for SNMP queries.
4. In the **SNMP Community String** field, enter the community string or password the SNMP servers will use to query the Thales KMS.
5. Click **Apply**.

   Once SNMP is enabled, the Thales KMS responds to requests from any SNMP server unless a preferred SNMP server is specified in the Access Control List. Once the IP address of a SNMP server is specified in the Access Control List, the Thales KMS only responds to that SNMP server.

Add SNMP servers

Configure the SNMP servers that are allowed to query the Thales KMS in the SNMP window, Access Control List tab.

Port types

SNMP servers can access the Thales KMS using TCP or UDP.

Using wildcards in the IP Address field

The IP Accress field supports the use of a wild-card in the 4th octet.

Example: 10.1.2.*

Procedure

1. Go to **System** and then click **SNMP**.

2 Click the **Access Control List** tab.

3 In the **IP Address** field, enter the IP address of the SNMP server to be granted access.

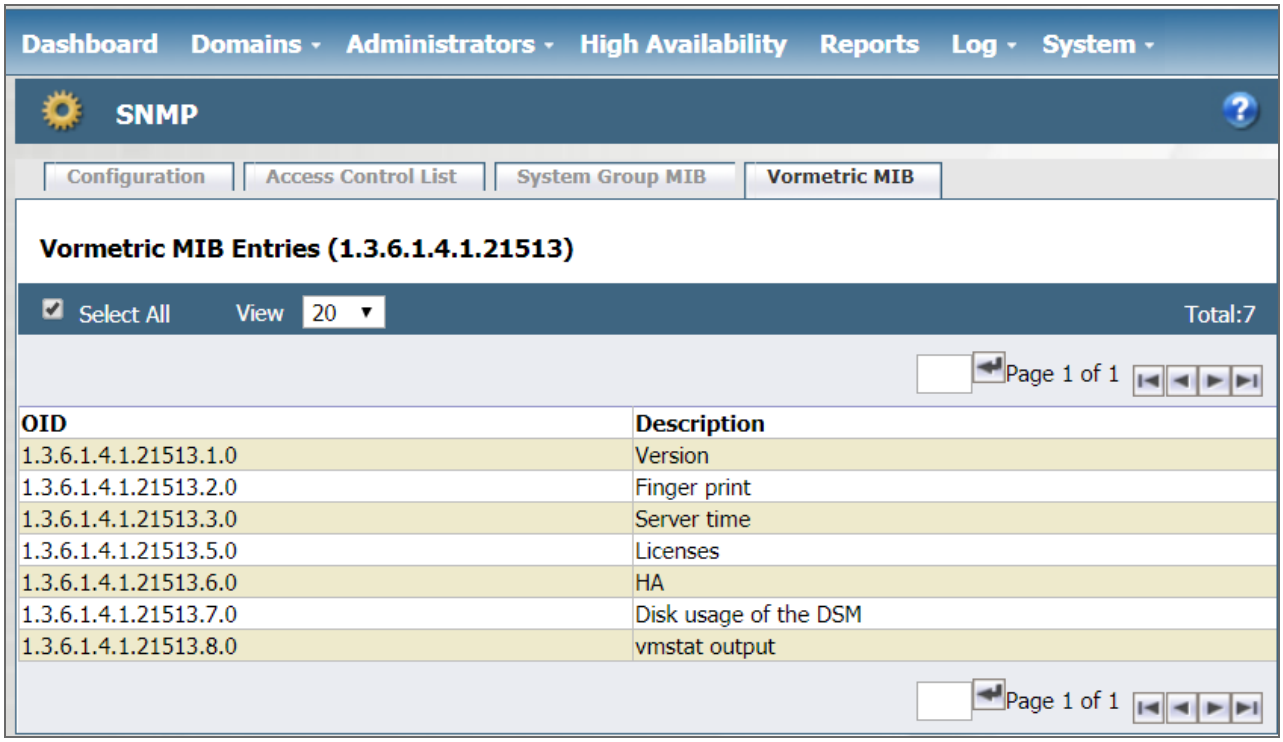
Host names and fully qualified domain names (FQDN) are not supported.

4 Click **OK**.

Once an SNMP server is added to the list of allowed servers, a corresponding log entry is created. The log entry indicates that an SNMP server is added to the Access Control List.

Thales KMS-specific SNMP information

The Vormetric MIB tab displays the Thales KMS-specific OIDs that can be queried by an SNMP server. The OIDs cannot be manually changed. The OID values are dynamic and change based on the Thales KMS state and configuration.



Thales KMS OIDs

The OIDs in the Vormetric group MIB begin with 1.3.6.1.4.1.21513. The following table lists the Vormetric OIDs and their purpose.

OID	SNMP object type	Description
1.3.6.1.2.1.1.4.0	sysContact	The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is a zero-length string. Maximum length is 256 characters.
1.3.6.1.2.1.1.6.0	sysLocation	The physical location of this node (for example, telephone closet, third floor). If the location is unknown, the value is a zero-length string. Maximum length is 256 characters.
1.3.6.1.4.1.21513.2.0		Returns the fingerprint of the current Thales KMSdeployment. The fingerprint is also displayed in the Thales KMSweb interface *Dashboard* window.
1.3.6.1.4.1.21513.3.0		Returns the time and date on the Thales KMS at the time of the SNMP query.
1.3.6.1.4.1.21513.5.0		Returns the following: • Agent type (FS or Key agent) • License installation state (true or false) for each agent type • License expiration date for each installed license The preceding information is also displayed in the Thales KMSweb interface *License* window.
1.3.6.1.4.1.21513.6.0		Returns the name of each node in a Thales KMS high-availability cluster configuration.
1.3.6.1.4.1.21513.7.0		Returns disk usage information for each file system mounted on the Thales KMS. Information returned is the equivalent of running the following CLI command: **`df -hk -B 1024K`**
1.3.6.1.4.1.21513.8.0		Returns Thales KMS process, memory, paging, I/O, and CPU usage information. Information returned is the equivalent of running the following CLI command: **`vmstat`**

Example SNMP queries

The example SNMP queries were made on a Red Hat Enterprise Linux Server, release 6.0, using SNMPv2.

Display Thales KMS contact information

```
# snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.2.1.1.4.0
SNMPv2-MIB::sysContact.0 = STRING: Vormetric Customer Support at 1-877-267-3247
#
```

Display the physical location of the Thales KMS

```
# snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.2.1.1.6.0
SNMPv2-MIB::sysLocation.0 = STRING: 2545 N. 1st St., San Jose, CA
#
```

Display the Thales KMS version number

```
# snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.1.0
SNMPv2-SMI::enterprises.21513.1.0 = STRING: "5.3.0.1616"
#
```

Display the Thales KMS fingerprint

```
# snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.2.0
SNMPv2-SMI::enterprises.21513.2.0 = STRING:
"D2:48:EF:E4:A2:B0:59:8C:5F:DB:9D:3B:30:41:0B:EE:BD:07:8D:67"
#
```

Display the current date and time on the Thales KMS

```
# snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.3.0
SNMPv2-SMI::enterprises.21513.3.0 = STRING: "2015-08-18 20:56:53.135 PDT"
#
```

Display the Thales KMS license configuration

```
# snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.5.0
SNMPv2-SMI::enterprises.21513.5.0 = STRING: "FS max # of agents: 30000;
Expires: Dec-31-2015; Key max # of agents: 30000; Expires: Dec-31-2015; FS
max # of agents: 30000; ; Key max # of agents: 30000; FS max # of agents:
30000; Max hours: 1000000; Key max # of agents: 30000; Max hours: 1000000;
Key vault enabled: true; Multi-domain enabled: true; max # of domains:
20000; Issued to: DSM522-Performance-2015-12-31"
#
```

Display the Thales KMS high availability configuration

```
# snmpget -c public -v 2c 10.3.48.239:7025 1.3.6.1.4.1.21513.6.0
SNMPv2-SMI::enterprises.21513.6.0 = STRING: "Failover: sys15123.com;
Primary: sys48239.com; "
#
```

Display the mounted file systems and their disk usage

```
# snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.7.0
SNMPv2-SMI::enterprises.21513.7.0 = STRING: "

 Filesystem                    IM-        Used    Available   Use%   Mounted
                               blocks                                on

 /dev/mapper/vg_sys48001-lv_   50269      3006    44703       7%     /
 root

 tmpfs                         1917       1       1917        1%     /dev/shm

 /dev/sda1                     477        38      414         9%     /boot

 /dev/mapper/vg_sys48001-lv_   45867      15185   28346       35%    /home
 home

#
```

Display Thales KMS system usage information

```
# snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.8.0
SNMPv2-SMI::enterprises.21513.8.0 = STRING: "
procs --------memory------------------ ---swap- -----io---- ---system--- ------
-------cpu----------
 r b swpd    free     buff     cache     si  so  bi  bo   in  cs  us  sy  id   wa  st
 0 0 51040   130248   228572   1777640   0   0   1   12   11  4   0   0   100  0   0
#
```

Configuring email notifications

The Email Notification feature allows you to add, delete, enable, and disable groups of email addresses to be notified of error messages, key expiration, or certificate expiration. You may want to add three email notification groups, one for each use case.

SMTP server

Until the SMTP server is configured, the "SMTP server not set" message is displayed.

Workflow

1. Configure the SMTP server and port, page 73

   To send email notifications, the SMTP server and port must be configured.
2. Enable email notifications, page 73

   You can automatically send email notifications to a set of administrators if the Thales KMS generates a serious log message, such as during a system backup.

Configure the SMTP server and port

To send email notifications, the SMTP server and port must be configured.

Procedure

1. Log on to the Thales KMS web application as **SystemAdministrator**.
2. Go to **System** > **Email Notification**.
3. On the **Email Notification** page, click the **SMTP Server** tab.
4. In the **SMTP Server** field, enter the host name or IP address of the SMTP server that sends email notifications.
5. In the **SMTP Server Port** field, enter the SMTP server port number.
6. Click **Apply**.

Enable email notifications

You can automatically send email notifications to a set of administrators if the Thales KMS generates a serious log message, such as during a system backup.

Procedure

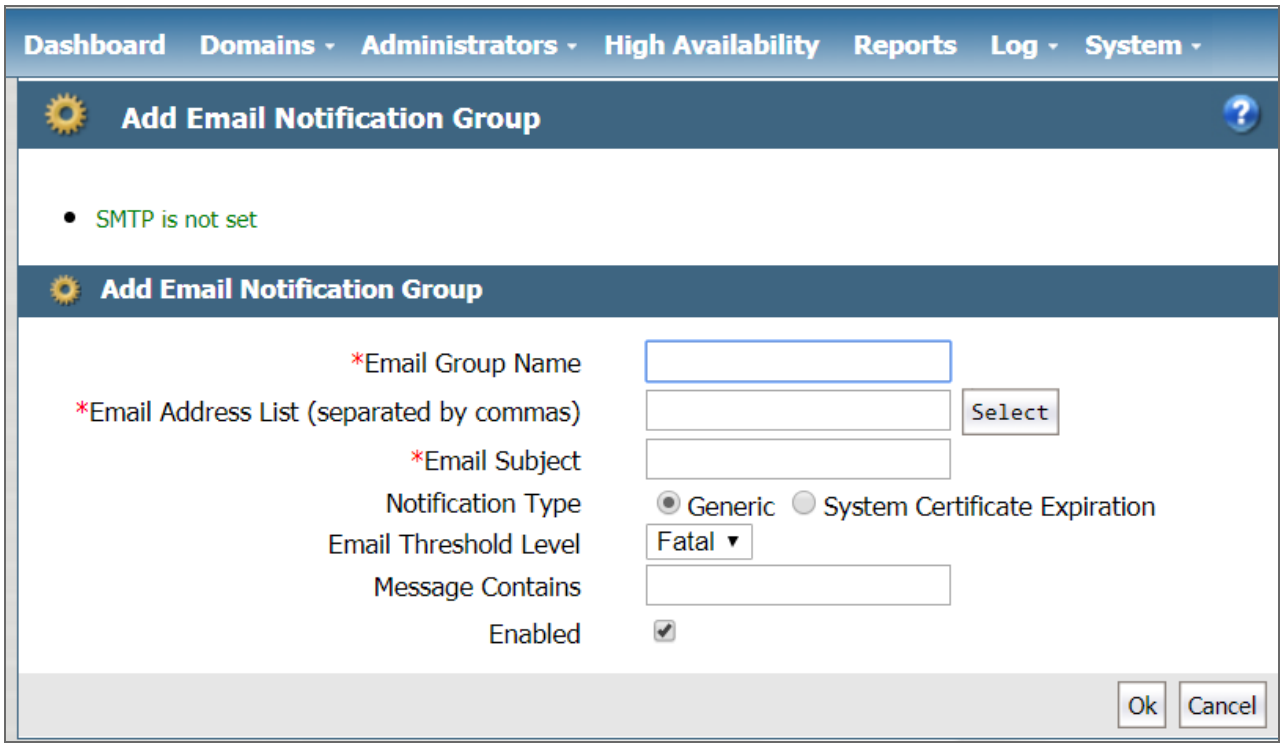
1. Go to **System** and then click **Email Notification**.
2. On the **Email Notification List** tab, click **Add**.
3. Complete the fields.
4. Click **Ok**.

Related topics

Add Email Notification Group field descriptions, page 74

Add Email Notification Group field descriptions

Configure email notifications to be notified about log messages whose threshold level is FATAL or ERROR.



Field	Description
Email Group Name	Name of the email group which will receive the email notification. Email Groups are per domain. You can set up email groups for domains of System, Security, Domain, Domain/Security and All Administrators.
Email Address List	Email addresses that will receive this email notification. Separate addresses with commas. If LDAP is configured, you can select addresses from your LDAP address book by pressing Select. If LDAP is not configured, you can enter your login and password to access it.
Email Subject	Text to display on the subject line of the email message.

Field	**Description**
Notification Type	Choices are: • Generic - Sends an email when the Thales KMS generates a log message that matches the value set in the Email Threshold Level field. This option is visible inside and outside of a domain. • Key Expiration - Sends email about expiration dates for Vormetric Encryption Keys and vaulted keys. This option is visible inside a domain. Emails are sent according to the following schedule: - once 90 days before expiration - once 60 days before expiration - once 30 days before expiration - once 15 days before expiration - every day within 7 days before expiration - once 7 days after expiration • Certificate Expiration - Sends email about expiration dates for vaulted certificates. This option is visible inside a domain. Email are sent according to a schedule. Certificate Expiration uses the same schedule as Key Expiration. See Key Expiration for the schedule. For email notifications about backup issues, select Generic.
Email Threshold Level	If the Thales KMS generates a log message with a severity of the specified threshold level, an email notification is generated. Options are ERROR or FATAL. FATAL includes both ERROR and FATAL messages.
Message Contains	A string filter that works with the Email Threshold Level. Only messages containing this string are sent as an email notification. If blank, then all messages meeting the threshold criteria are sent.
Enabled	When selected, enables email notifications to the group. To turn off email notifications to the group, clear the checkbox.

Troubleshooting

The following topics include resolutions to specific issues.

Unable to playback calls in an HA environment

Issue

In a high-availability (HA) environment, a call cannot be played back.

Symptom

In an HA environment where the primary Thales KMS is down, calls recorded with older keys cannot be played.

Background

In a Thales KMS HA environment, the following occurs:

1. The Thales agent that is installed on the Application server tries to get the key from the primary Thales KMS.
2. If the attempt to retrieve the key from the primary Thales KMS times out (which may range from 40-80 seconds), the Thales agent gets the key from the failover Thales KMS.

Resolution

Wait approximately one minute, and then try to replay the call again. The wait time allows the attempt to retrieve the key from the primary Thales KMS to time out and then retrieve the key from the failover Thales KMS.

"Thales KMS registration failed" alarm

Issue

The "Thales KMS Registration Failed" alarm is raised after KMS service is restarted.

Symptoms

The most likely reason the alarm was raised is because the Thales KMS that is configured in Enterprise Manager is down. While the Thales KMS is down you may see the symptoms described below if KMS service is restarted on an Application server.

- **Playback fails** – due to an issue on the Thales KMS, both new and old calls cannot be retrieved. This is a known issue.
- **Newly added Application servers fail to retrieve keys** – When the primary Thales KMS (configured in Enterprise Manager) is down, new Application servers cannot register with the

Thales KMS. Since the new Application server cannot register with the primary Thales KMS, key retrieval fails.

- **Newly added Recorders fail to encrypt calls** – Since Application servers may fail to register with the primary Thales KMS while it is down, newly added Recorders will fail to encrypt the calls.

Resolution

Do one of the following:

- Promote the failover Thales KMS to primary. See "Related topics" for a link to instructions.
- Turn on the primary Thales KMS.

Related topics

Convert a failover Thales KMS to a primary Thales KMS, page 64

Primary server is not configured during failover registration

Issue

When running the convert2failover command during the High Availability configuration, a message indicates the following:

- Connection to the primary Thales KMS failed.
- Configuration for the primary server failed.

Symptom

The following message is displayed after running the convert2failover command.

```
Warning: This will overwrite all keystores on this failover server!
ERROR failed to make SSL connection: Connection timed out (Connection
timed out)
ERROR: Server converted to Failover Server, but failed to config
primary server
```

Resolution

1. Have the high-availability configuration steps in Thales Key Manager Server High Availability installation and configuration, page 45 been followed correctly?
2. Verify that port 8080 is bidirectional.
   a. Log on to the primary Thales KMS CLI.
   b. Access the network command prompt, and run the ping command using the failover Thales KMS fully qualified domain name (FQDN).

      ```
      0000:vormetric$ network
      0001:network$ ping <failover_FQDN>
      ```

   c. From the network command prompt, run the ping command using the failover Thales KMS IP address.

      ```
      0002:network$ ping <failover_IP_address>
      ```

Example: ping commands

```
0006:vormetric$ network
0007:network$ ping vormetric.lab.local
PING vormetric.lab.local (192.168.40.194) 56(84) bytes of data.
64 bytes from vormetric.lab.local (192.168.40.194): icmp_seq=1 ttl=64 time=0.279 ms
64 bytes from vormetric.lab.local (192.168.40.194): icmp_seq=2 ttl=64 time=0.404 ms
64 bytes from vormetric.lab.local (192.168.40.194): icmp_seq=3 ttl=64 time=0.279 ms
64 bytes from vormetric.lab.local (192.168.40.194): icmp_seq=4 ttl=64 time=0.289 ms
64 bytes from vormetric.lab.local (192.168.40.194): icmp_seq=5 ttl=64 time=0.279 ms
64 bytes from vormetric.lab.local (192.168.40.194): icmp_seq=6 ttl=64 time=0.237 ms

--- vormetric.lab.local ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 0.237/0.294/0.404/0.054 ms
ping SUCCESS
0008:network$ ping 192.168.40.194
PING 192.168.40.194 (192.168.40.194) 56(84) byes of data.
64 bytes from 192.168.40.194: icmp_seq-1 ttl=64 time=0.302 ms
64 bytes from 192.168.40.194: icmp_seq-2 ttl=64 time=0.410 ms
64 bytes from 192.168.40.194: icmp_seq-3 ttl=64 time=0.255 ms
64 bytes from 192.168.40.194: icmp_seq-4 ttl=64 time=0.351 ms
64 bytes from 192.168.40.194: icmp_seq-5 ttl=64 time=0.470 ms
64 bytes from 192.168.40.194: icmp_seq-6 ttl=64 time=0.271 ms

--- 192.168.40.194 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
Rtt min/avg/max/mdev = 0.255/0.344/0.470/0.080 ms
Ping SUCCESS
```

3 Check the status and availability of port 8080 and then port 50000.

a. Logged on to the primary Thales KMS CLI, from the network command prompt, run the checkport command. When running the command, use the failover Thales KMS IP address, port 8080, and a timeout of 10 seconds.

`0003:network$ checkport <failover_IP_address> 8080 timeout 10`

b. From the network command prompt, run the checkport command using the failover Thales KMS FQDN, port 8080, and a timeout of 10 seconds.

`0004:network$ checkport <failover_FQDN> 8080 timeout 10`

Example: checkport commands

```
0007:vormetric$ network
0008:network$ checkport 192.168.40.194 8080 timeout 10
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: connected to 192.168.40.194:8080.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.

SUCCESS: invoked chckport(nc) command.
0009:network$ checkport vormetric.lab.local 8080 timeout 10
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: connected to 192.168.40.194:8080.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.

SUCCESS: invoked chckport(nc) command.
0010:network$
```

c. Check the status and availability of port 50000.

0005:network$ checkport <failover_IP_address> 50000 timeout 10

0006:network$ checkport <failover_FQDN> 50000 timeout 10

4 Check the connection from the failover Thales KMS to the primary Thales KMS.

a. Log on to the failover Thales KMS CLI.

b. Access the network command prompt and run the ping command twice.

0000:vormetric$ network

0001:network$ ping <primary_FQDN>

0002:network$ ping <primary_IP_address>

c. Check the status and availability of port 8080.

0003:network$ checkport <primary_IP_address> 8080 timeout 10

0004:network$ checkport <primary_FQDN> 8080 timeout 10

5 If an error displayed during any of the previous steps, then the ports are not open between the primary Thales KMS and the failover Thales KMS. If an error displayed:

a. Open the ports.

b. Reconfigure the failover Thales KMS.

Related topics

Register the failover Thales KMS with the primary Thales KMS, page 49

Thales KMS software upgrade failed

Issue

When using Internet Explorer to run the Thales KMS web user interface, the Thales KMS software upgrade failed.

Resolution

Use Firefox or Chrome to run the Thales KMS web user interface while upgrading the software.

Unable to configure automatic backup

Issue

Configuring automatic backup fails.

Symptom

When configuring the Thales KMS automatic backup schedule, the following message is displayed:

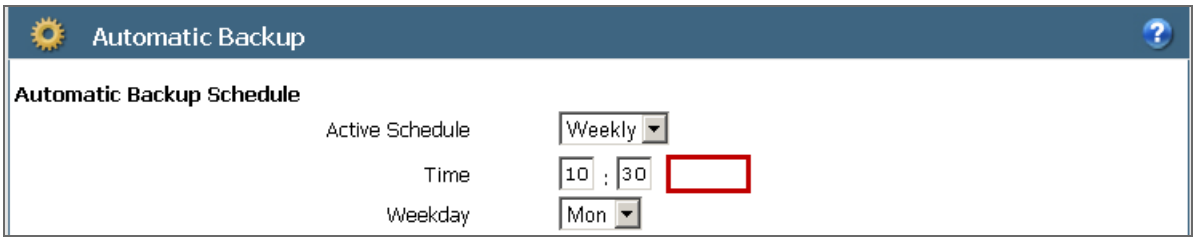
```
This operation did not complete. The application experienced an internal
error.
```

Any attempts to modify the automatic backup policy or create a new policy fails with the same error message.

Background

The error displays if a non-US English language web browser is used. The issue is that the web console uses a 12-hour clock, but the AM/PM selections are not available on the Automatic Backup screen.

1. Go to **System** > **Backup and Restore** > **Automatic Backup** .
2. Verify that the AM/PM selections are *not* available for the **Time** field.



Resolution

1. From your web browser, do the following:
   a. Change the browser language to **English (United States)**. Refer to your browser documentation for information about changing language preferences.
   b. Remove any language except for English (United States).
2. Restart the web browser and connect to the Thales KMS web application.
3. Configure the automatic backup.

Related topics

Configure a backup schedule for Linux using the web application, page 57

Activate ECC (Suite B) or compatible mode for all communications

Using the command-line interface (CLI), you can configure the mode to use in your environment. Modes are Suite B or compatible.

Procedure

1. If Suite B mode, verify that the clients can reach ports 8446 and 8447 on the Thales KMS.
2. Log on to the Thales KMS CLI. If in an HA environment, log on to the primary Thales KMS CLI.
3. Activate Suite B or compatibility mode.
   a. Access the system command prompt, and change to Suite B or compatible mode.

      ```
      0000:vormetric$ system
      0001:system$ security suiteb set [suiteb | compatible]
      ```

      ```
      WARNING: After setting to <suiteb or compatible> mode, the security
      server software will be restarted automatically! Continue? (yes|no)
      [no]:yes
      ```

      Example: Activate Suite B mode

      ```
      0001:system$ security suiteb set suiteb
      ```

      Example: Activate compatible mode

      ```
      0001:system$ security suiteb set compatible
      ```

   b. At the **Continue? (yes|no)** prompt, type **yes**.
   c. Confirm the configuration.

      ```
      0002:system$ security suiteb show
      ```

      ```
      Example:
      Current mode is: suiteb
      SUCCESS: showed suite b mode
      ```
4. If in an HA environment, log on to the failover Thales KMS CLI.
5. On the failover Thales KMS, repeat step 3.

Related topics

For information about the server security modes, see Prerequisites for the Thales KMS installation, page 10

Configure a client to use ECC (Suite B) for all communications

You can configure a specific client to only use ECC (Suite B mode) to communicate with the Thales KMS.

Procedure

1. Make sure that the client can reach the following Thales KMS ECC ports:
   - 8446
   - 8447
2. Block the client from outbound traffic to the following Thales KMS RSA ports:
   - 8443
   - 8444

   If blocking the ports does not work, then you can re-register the client. When you re-register the client, a dialog with ECC ports is displayed.