Enterprise Secure Key Manager

Enterprise Secure Key Manager v8.50.0

User’s Guide

utimaco®

Imprint

Copyright 2022 Utimaco IS GmbH
Germanusstr. 4
D-52080 Aachen
Germany

Phone AMERICAS +1-844-UTIMACO (+1 844-884-6226)
EMEA +49 800-627-3081
APAC +81 800-919-1301

Internet https://support.hsm.utimaco.com/

e-mail support@utimaco.com

Document Version 8.50.0

Date 2023-04-26

Status

Document No. 2021-0046

Table of Contents

1 What’s new in the ESKM v8 appliance

1.1 Summary of new ESKM software v8.50.0 features

ESKM v8.50.0 features can be summarized as follows:

- New WebUI support for Google Cloud External Key Manager
- Upgraded OpenSSL to OpenSSL 3.0.8
- Upgraded OpenSSH to OpenSSH 9.1
- ESKM now supports KMIP v3.0
- Virtual ESKM now supported on Hyper-V and KVM hypervisors
- New REST logging category for REST and Cloud logs
- Custom attribute support in REST API
- Fixed vulnerabilities and defects

⚠ For upgrading from ESKM v8.1, please follow the instructions in ESKM User's Guide (ESKM Appliance overview > Upgrading from a previous ESKM version).

⚠ Please refer FIPS mode changes (p. 373) in ESKM 8.50 user guide for the new restrictions related to FIPS mode.

1.2 Summary of new ESKM software v8.43.0 features

ESKM v8.43.0 features can be summarized as follows:

- Bring Your Own Key (BYOK) support for Microsoft Azure CSP
- New WebUI interface for BYOK Cloud integration
- Support for Google Cloud External KMS integration
- Fixed vulnerabilities and defects.

1.3 Summary of new ESKM software v8.42.0 features

Software v8.42.0 feature updates can be summarized as follows:

- Key import via REST API.
- Certificate signing via REST API.
- Random number generation via REST API.
- Get Custom attributes via REST API.
- Local user last access time update for REST API operations.
- Upgraded httpd and SNMP packages.
- Fixed vulnerabilities and defects.

1.4 Summary of new ESKM software v8.41.0 features

ESKM v8.41.0 features can be summarized as follows:

- Signing and verification via REST API.
    - Supported Key Algorithms: RSA-2048, RSA-3072, RSA-4096
    - Supported Padding: PSS, PKCS1
    - Supported Hashing Algorithms: SHA-256, SHA-512
- Hashing support via REST API.
    - Supported Algorithms: MD5, SHA-1, SHA-256, SHA-512
- KMIP Object creation via ESKM Management Console.
- Two NIC support for older vESKM releases via upgrader.
- What's New option in the ESKM Management Console.
- Fixed vulnerabilities and defects, including:
    - CVE-2022-0778

1.5 Summary of new ESKM software v8.4 features

ESKM v8.4 features can be summarized as follows:

- NIC Teaming support in ESKM appliances.
- Data Encryption and Decryption via REST API.
- LAN HSM support in ESKM L2 appliance.
- SSH public key authentication support for schedule backups.
- Enabled option to initiate schedule backups manually.
- Enabled option to download ESKM license usage and device information.
- Local user license type restricted for the following:
  - Server
  - KMIP
  - KMS
  - Custom
- SNMP trap and system log for scheduled backup failure.
- Bug Fixes.

1.6 Summary of ESKM software v8.3.2 features

ESKM v8.3.2 features can be summarized as follows:

- Fixed vulnerabilities and defects, including:
  - Log4j Vulnerability.

1.7 Summary of ESKM software v8.3.1 features

ESKM v8.3.1 features can be summarized as follows:

- Bug fixes including:
  - Key operation via REST is not disabled when all the enrolled HSMs are offline.

1.8 Summary of ESKM software v8.3 features

ESKM v8.3 features can be summarized as follows:

- REST API support for basic ESKM key operations.
- Server configuration support for REST and HSM Web UI.
- Service commands for REST service management.
- Bug fixes including
    - Intermediate CA signed certificates are not working for syslog TLS.
    - FIPS level is displayed incorrectly for custom key queries.

1.9 Summary of ESKM software v8.2 features

ESKM v8.2 features can be summarized as follows:

- Database support for ESKM users and groups
- Support for additive restore of ESKM users and groups
- Improved replication log messaging
- Reliability improvement for ESKM users/groups replication
- Bug fixes

1.10 Summary of new ESKM software v8.1 features

ESKM v8.1 features can be summarized as follows:

- New Utimaco hardware for ESKM FIPS level 2 appliance
- Added support for FIPS level 3 and level 4 ESKM appliances
- Improved cluster scalability and performance
- LCD based first time configuration support
- Support for HSM CLI commands

- Upgraded OpenSSH
- Fixed vulnerabilities and defects, including
  - Remove DH ciphers in SSH Kex algorithms
  - Updated the operating system packages
- ESKM connecting to unknown addresses after setting a DNS server
- ESKM is not responding through both NIC IPs when NIC2 IP is added without connecting ethernet cable
- Failure in sending ESKM backups via SCP
- Error in renaming ESKM CA name

1.11 Summary of new ESKM software v8.0 features

ESKM v8.0 features can be summarized as follows:

- First virtual ESKM release with OVA deployment image
- Initial 60 day trial period for vESKM installation
- Post trial licensing support for production environment
- Support for external HSM support (General purpose and CP5)
- New WebUI interface for HSM configuration
- Improved Security features
  - Disk Encryption
  - XFS file system
  - Stronger encryption algorithms

1.12 Management Console and CLI features

The following modifications have been made to the Management Console and CLI.

Table 1: Management Console and CLI modifications

Component	***Description***	***Relevant CLI command***
Public key authentication for CLI administrators	Public key technology can be used to authenticate administrators when they use the CLI to log in to the ESKM appliance via an SSH version 2 session, see SSH Public key authentication.	no administrator-keys show administrator-keys
KMIP SSL/TLS support	TLS 1.0, TLS 1.1 and TLS 1.2 protocol versions are individually selectable, see SSL options. Additional ciphers have been added, see SSL/TLS cipher order.	kmip cipherspec kmip cipherspec priority kmip ssl protocol show ssl
KMIP Server Authentication Settings	The KMIP server supports the ability to specify how clients are authenticated, see KMIP server authentication settings.	none
Server Certificate for web administration	A server certificate for web administration can be specified, see Remote administration settings.	show webadmin certificate set webadmin default certificate

Component	***Description***	***Relevant CLI command***
IPv6 support	Both the Management Console and the CLI can be accessed using IPv6 addresses. The ESKM appliance can be configured with an IPv6 address, see Network interface list. Both the KMS and KMIP servers can be configured to accept client connections via IPv6 addresses, see KMS server settings and KMIP server settings. Both the KMS and KMIP servers can be configured to accept client health check connections via IPv6 addresses, see Health check, and KMIP health check. These SCP file movement functions have been updated to support a remote host system that uses an IPv6 address: ▪ Backup, see Create backup: backup settings. ▪ Scheduled Backup, see Schedule backup. ▪ Restore, see Restore backup. ▪ Log transfer, see Log transfer. ▪ Log rotation, see Log rotation. ▪ Certificate import, see Importing a certificate. ▪ Certificate export, see Exporting a certificate with a private key. ▪ Software upgrade/install, see Software upgrade/install.	ipv6 enable ipv6 address no ipv6 address health check kmip-health check backup scheduled backup restore backup Transfer log file commands edit log rotation cert import software install edit community snmp agent

Component	***Description***	***Relevant CLI command***
	▪ Added IPv6 support for LDAP, Cluster, FIPS status, SNMP, Syslog, Static route and IP authorization, see • LDAP server configuration • FIPS status server • FIPS status server page • Static route list • Cluster configuration page • SNMP configuration • Syslog settings • IP authorization configuration	
SSL/TLS cipher suites	Removed weak ciphers suites for the KMS SSL/TLS connections	none
SSH Admin Maximum Login Attempts	The maximum number of authentication attempts permitted per connection can be specified, see Remote administration settings.	edit ras settings show ras settings
Session Timeout	The number of minutes the Management Console and CLI remain idle prior to logging off the user can be specified, see Remote administration settings	edit ras settings show ras settings
Selective backup for KMIP objects	KMIP objects to be included in a backup can be selectively specified, see Create backup.	backup

Component	***Description***	***Relevant CLI command***
SSH options	SSH Ciphers, MACs and KEX Algorithms can be enabled/disabled/prioritized, see SSH Configuration.	no ssh show ssh cipher ssh ssh priority ssh restore
SSL options	Added support for stronger TLS cipher suites to protect the KMS TLS communication. Removed 3DES symmetric cipher from SSL/TLS cipher list. See SSL/ TLS cipher order. Removed SSL 3.0 support. See SSL options.	SSL/TLS commands cipherspec priority kmip cipherspec priority
RAID Status	RAID Status is added in System health page, see RAID status	show system health
3072-bit certificate creation	Added support for 3072-bit certificate creation. ▪ Local CA, see Create local CA ▪ Certificate, see Create certificate	cert request local ca
Download ESKM query	Added support for download ESKM key query. See Download ESKM query	none

Component	***Description***	***Relevant CLI command***
SNMP	Added new algorithms (SHA-256, SHA-384, and SHA 512) under Auth Protocol. See ▪ SNMPv3 username list ▪ Create SNMP management station FIPS compliant added as new component. See ▪ SNMPv1/SNMPv2 community list ▪ SNMPv3 username list ▪ SNMP management station list	station edit station snmp username edit snmp username
Statistics	New operations added to KMIP server statistics. See KMIP statistics	none
FTP	Removed FTP support.	none

Component	***Description***	***Relevant CLI command***
Certificate and CA Configuration	Added ECDSA algorithms (ECDSA-P256, ECDSA-P384, ECDSA-512) in Certificate and CA creation. See ▪ Create certificate ▪ Create local CA Subject Alternative Name(s) added as a new option to certificates. See ▪ Certificate information ▪ Certificate installation ▪ Self-signed certificate ▪ Create certificate	local ca cert request
Log configuration	Added Syslog TLS settings in Log configuration. See ▪ Syslog TLS settings	no syslog tls show syslog tls syslog tls syslog test
Windows share	Added Windows share to Backup and Restore. See ▪ Create backup ▪ Restore backup ▪ Schedule backup	backup scheduled backup restore backup

Component	***Description***	***Relevant CLI command***
Local users	Added support for new Licensing schemes. See ▪ Local users ▪ Selected local user ▪ Last Access Time	user edit user no user show user

2 About this guide

This user guide provides information on the following topics.

- Performing configuration and operation tasks (p. 53)
- Maintaining the ESKM appliance (p. 164)
- Using the Management Console (p. 216)
- Using the command line interface (p. 569)
- Troubleshooting (p. 796)
- Utimaco Technical Support (p. 798)

For information on deploying a Virtual Enterprise Secure Key Manager, refer to the *Virtual Enterprise Secure Key Manager Deployment Guide*.

2.1 Intended audience

This guide is intended for system administrators with knowledge of:

- Data security administration
- Network configuration

2.2 Document conventions and symbols

Table 2: Document conventions

Convention	***Element***
Blue text: http://www.utimaco.com[1]	Cross-reference links, email addresses, website addresses

[1] http://www.utimaco.com/

Convention	***Element***
Bold text	- Keys that are pressed - Text typed into a GUI element, such as a box - GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	- File and directory names - System output - Code - Commands, their arguments, and argument values
`Monospace, italic` text	- Code variables - Command variables
`Monospace, bold` text	Emphasized monospace text

❗ Indicates an action that can potentially result in an irreversible configuration change or permanent loss of data.

❗ Indicates an action that can have consequences such as deletion of keys or changes to security settings.

ℹ Provides clarifying information or specific instructions.

⚠ Provides additional information.

2.3 Related documentation

The following documents provide related information:

- *Virtual Enterprise Secure Key Manager v8.50.0 Deployment Guide*
- *Enterprise Secure Key Manager v8.50.0 Release Notes*

2.4 Utimaco websites

For additional information, visit the following Utimaco website:

https://hsm.utimaco.com/products-hardware-security-modules/key-management/eskm/

OASIS websites

In addition to the Utimaco websites, visit the OASIS websites for more information on the Key Management Interoperability Protocol (KMIP) specification, usage guides, and profiles:

- https://www.oasis-open.org/standards
- https://wiki.oasis-open.org/kmip/KnownKMIPImplementations

2.5 Documentation feedback

Utimaco welcomes your feedback. To make comments and suggestions about product documentation, please send an email message to:

support@utimaco.com[2]

All submissions become the property of Utimaco.

[2] mailto:support@utimaco.com

3 ESKM Appliance overview

This chapter provides information about:

For information about installing an ESKM appliance, see the *ESKM Installation and Replacement Guide.*

3.1 ESKM features

The ESKM appliance is a complete solution for generating, storing, serving, controlling and auditing access to data encryption keys. It enables you to protect and preserve access to business-critical, sensitive, data-at- rest encryption keys, either locally or remotely.

The important features for this release include:

- Support for Utimaco and partner data protection solutions.
- High-availability, protected access to business-critical encrypted keys.
- Support for audit and compliance requirements, including PCI-DSS and HIPAA/ HITECH.
- Scalability for multiple data centers, hundreds of clients and millions of keys.
- FIPS 140-2 validation, supports the latest NIST guidance.
- Support for versions 1.0, 1.1, 1.2, 1.3, 1.4, 2.0 and 2.1 of the Key Management Interoperability Protocol (KMIP) open standard, enabling businesses to mix-and-match KMIP clients and servers.

3.2 Users, groups, and permissions

ESKM appliances support two types of protocols: KMS and KMIP. Permissions are rules that restrict or grant a user, access to an object, such as a key.

3.2.1 KMS permission model1

In the KMS permission model, by default, only the creator of the key has the permission to access the key. The KMS key owner has full permissions to perform any operation (exporting, deleting etc.) on the key over the ESKM XML protocol, if these capabilities are set during key creation. Membership to a KMS group is optional. If you grant a group access to a key, all the users in that group will be able to access the key (depending on the permissions). If the user is not a member of any group, but the group permissions are set by granting a group access to the user's key, then the users of that group are able to access the key.

3.2.2 KMIP permission model

The KMIP permission model controls access to KMIP-managed objects by group membership. This section covers the following topics:

- User groups and object groups (p. 38)
- Source groups and target groups (p. 40)
- Operation-based permissions (p. 45)

3.2.2.1 User groups and object groups

A KMIP group has a group type. The relevant group types relating to the KMIP permission model are user groups and object groups.

- A KMIP user group contains only users. All users must belong to at least one KMIP user group. User group membership is configured when creating a KMIP-enabled user. The administrator can change user group membership from either the Management Console or the CLI. All members of the same KMIP user group have exactly the same privileges. For example, two KMIP-enabled users, **Tape Library A** and **Tape Library B,** set their group membership to **Finance**. User **Tape Library A** has the same privileges as user **Tape Library B**. In addition, user **Tape Library B** has the same access privileges to all objects created by user **Tape Library A**.
- A KMIP object group contains only KMIP-managed objects, but no users. Since the KMIP permission model is group-based, all KMIP-managed objects in the same object group can be accessed by all users who have permission to access that group. Each KMIP-enabled user is configured with a default object group, which is the group that KMIP-managed objects created by this user will be placed in, if the **Object Group** property is not specified in the **Create** or **Register** request. The administrator cannot

transfer objects from one object group to another via the Management Console or the CLI. This can only be done via the KMIP protocol:

- To place an object in multiple object groups, specify the object groups in either the **Create** or **Register** operation in the **Object Group** attribute. The value specified in the **Object Group** attribute must exist prior to issuing the KMIP client operation; otherwise the operation will fail. Alternatively, use the **Add Attribute** KMIP client operation to add a new **Object Group** attribute to an existing KMIP-managed object.
- To remove an object from an existing object group, use the **Delete Attribute** KMIP client operation request. The restriction is that the object must belong to at least one object group, so that it can be accessed by at least one KMIP client. Hence, an attempt to remove the object from the last group will fail with a **Permission Denied** error.
- To change the membership of the object from one object group to another, either use the **Modify Attribute** KMIP client operation request, or use the **Delete attribute** KMIP client operation request to first delete the object from its existing group, followed by an **Add Attribute** KMIP client operation request to add the object to its new group. Due to the restriction that the object cannot be deleted from the last group that it belongs to, the second method will only succeed if the object already belongs to more than one group before the **Delete Attribute** KMIP client operation request.

The predefined object group named **default object group** is a special object group that is hidden from the KMIP client. Therefore:

- If a KMIP client issues a **Create** or **Register** operation request which contains an **Object Group** attribute with the value of *default object group*, the operation will succeed if there is sufficient permission to perform the request and if the request is correct. However, the **Get Attributes** operation will not return this **Object Group** attribute.
- If a KMIP client issues a **Create** or **Register** operation request which contains an **Object Group** attribute with any other value besides *default object group*, such as *engineering_objects*, the operation will succeed if there is sufficient permission to perform the request, the object group exists, and the request is correct. The **Get Attributes** operation will return this **Object Group** attribute. If the object group does not exist, the operation will fail with Permission Denied.

- If the KMIP client belongs to two object groups, the special object group named *default object group* and some other object group such as *engineering_objects*, the KMIP client Delete Attribute operation for either object group will fail. This is because the special object group named *default object group* is hidden from the user, and the *engineering_objects* object group is the only object group visible to the KMIP client. There is a restriction against deleting the object from the last object group that it belongs to.

3.2.2.2 Source groups and target groups

All KMIP group names must be unique. When you add a KMIP group, the server creates two groups: an object group and an associated user group. For example, if you add a KMIP group named Finance, the server creates an object group named Finance and also creates a user group named Finance_user. KMIP clients are configured to access object groups, not user groups.

In the KMIP permission model, permissions flow from a source group to a target group. In order for a user to be allowed to perform a KMIP operation on a managed object, that user must belong to a source group that has permissions to perform that operation in the target group to which the object is to be placed. The most common use case is that the source group is the user group, and the target group is the object group, although this is not always the case. You must configure KMIP-enabled users to be in a user group (the source group) that has privileges to perform operations in the default KMIP object group (the target group). The following example illustrates this use case. Note that the name of the user group has been changed from Tape_objects_user to Tape.

Two KMIP-enabled users, Tape Library A and Tape Library B, are configured to be members of a user group named Tape. The object group for both users Tape Library A and Tape Library B is Tape_objects. User group Tape is configured to have all permissions to operate on object group . User group is the source group, with privileges flowing to the target group Tape_objects. In this scenario, the source group is a user group, while the target group is an object group.

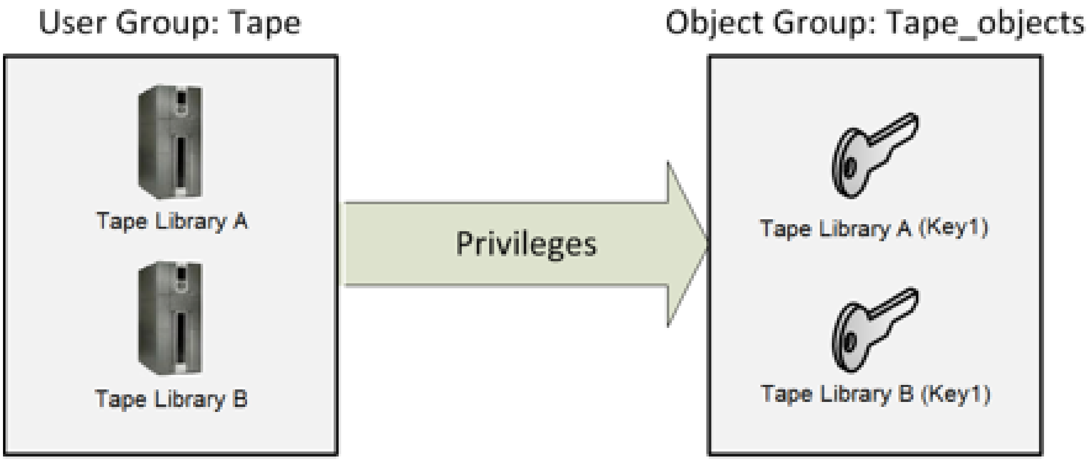


Figure 1 : Basic Source and Target Group Concepts

If the user **Tape Library A** issues a KMIP client **Create** request for a symmetric key named **Tape Library A (Key1)** without the Object Group attribute, that symmetric key will be created in the user's default KMIP object group, which is **Tape_objects**. Since the user **Tape Library B** is also a member of the user group **Tape**, and all members of the same user group have the same privileges, **Tape Library B** has the same access privileges as user **Tape Library A** for **Tape Library A (Key1)**.

If the user **Tape Library A** issues a KMIP client **Create** request for a symmetric key with the Object Group attribute specified as **Tape_objects**, the result will be the same as the above.

If the user **Tape Library B** issues a KMIP client **Create** request for a symmetric key named **Tape Library B (Key1)** without the Object Group attribute specified, that symmetric key will also be created in the object group **Tape_objects**, since this is also user **Tape Library B**'s configured default KMIP object group. Likewise, since the user **Tape Library A** is also a member of the user group **Tape** and all members of the same user group have the same privileges, **Tape Library A** has the same access privileges as user **Tape Library B** for **Tape Library B (Key1)**.

If the user **Tape Library A** issues a KMIP client **Create** request for a symmetric key with the Object Group attribute set to **Store_objects**, this request operation will fail, since user **Tape Library A** is not a member of any group that has access to the group **Store_objects**. User **Tape Library A** is only a member of the group **Tape**, which has no permissions to access the group **Store_objects**. Following are the two solutions to this issue.

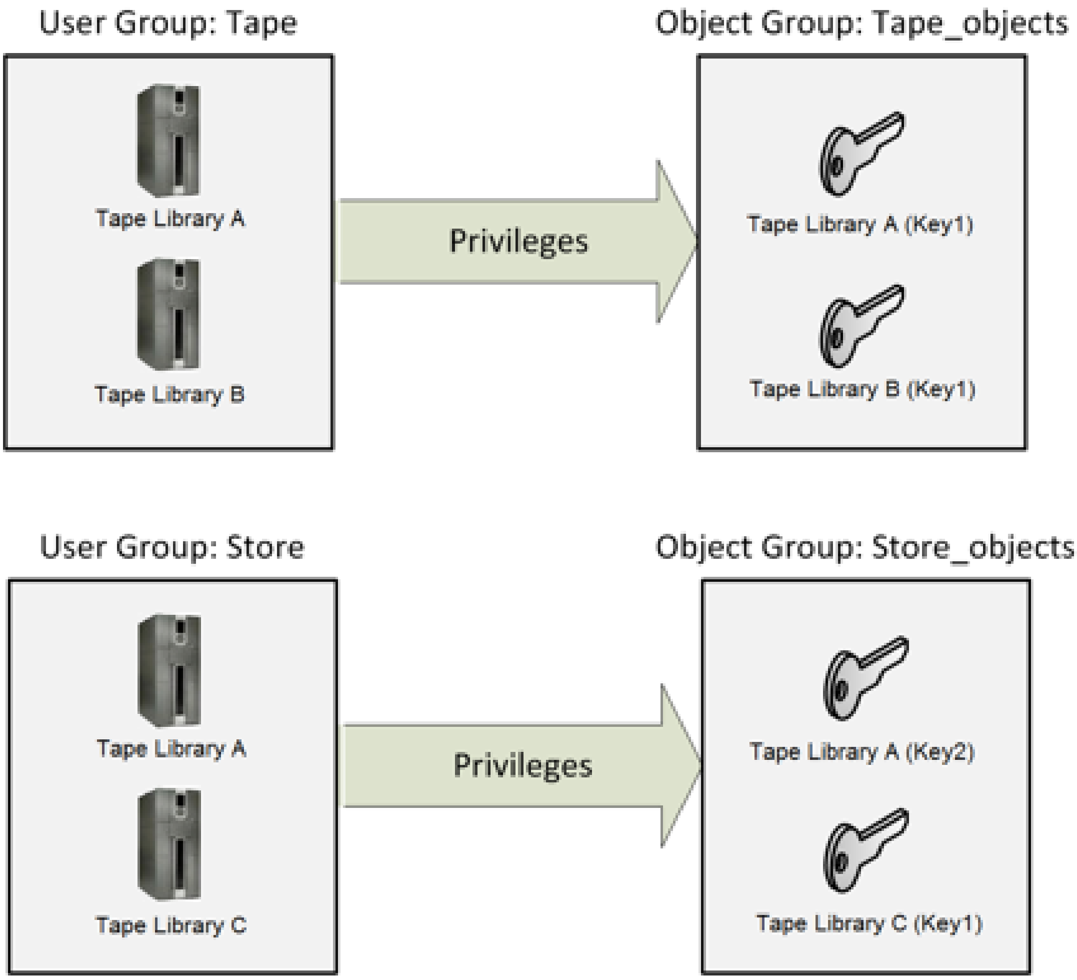


Figure 2 : Membership to multiple source groups

In this scenario there is an additional user group named **Store**, which is configured to have full access to object group **Store_objects**.

In order for KMIP-enabled user **Tape Library A** who is currently only a member of user group **Tape** to create objects in **Store_objects**, the user **Tape Library A** must be added to a group that has permissions to access the group **Store_objects**. Adding user **Tape Library A** to the user group **Store**, allows the **Create** request operation for a symmetric key named **Tape Library A (Key2)** with the Object Group attribute set to **Store_objects** to succeed. The newly created symmetric key will be a member of **Store_objects**.

Note the following:

- Since the user **Tape Library A** is now a member of user groups **Tape** and **Store**, both having full access privileges to object groups **Tape_objects** and **Store_objects** respectively, the user has full access privileges to all objects in both the object groups, **Tape_objects** and **Store_objects**.

- Since the user **Tape Library B** is only a member of the user group **Tape** and not of **Store**, the user will only be able to access objects in the group **Tape_objects**.
- Since the user **Tape Library C** is also member of the user group **Store**, both **Tape Library A** and **Tape Library C** will have identical privileges with respect to the group **Store_objects**. Therefore, if the user **Tape Library C** creates a symmetric key named **Tape Library C (Key1)** in Store_objects, the user **Tape Library A** will have the same access privileges to this object as the user **Tape Library C**.
- Each user has a default object group configured during user creation. If the user **Tape Library A**'s default object group is **Tape_objects**, then the only way that user **Tape Library A** can create objects in the **Store_objects** group is to issue a KMIP client request operation and explicitly specify the Object Group property as **Store_objects**.

In the use case where user **Tape Library C** is a member of the user group **Store** and is configured with a default KMIP object group of **Store_objects**, all KMIP client request operations sent by user **Tape Library C** will fail unless they have the Object Group attribute explicitly specified, since the only user group that **Tape Library C** is a member of is **Store**, which does not have permissions to access the object group **Tape_objects**.

Multiple target groups for a single source group

To allow the user **Tape Library A** to perform **Create** and other KMIP operations on object group **Store_objects,** you must give the user group **Tape** additional permissions, specifically by adding permissions from the source group **Tape** to the target group **Store_objects**, as illustrated in the following figure. In this scenario, users **Tape Library A**, **Tape Library B**, and **Tape Library C** all have identical privileges to access both target groups **Tape_objects** and **Store_objects**.

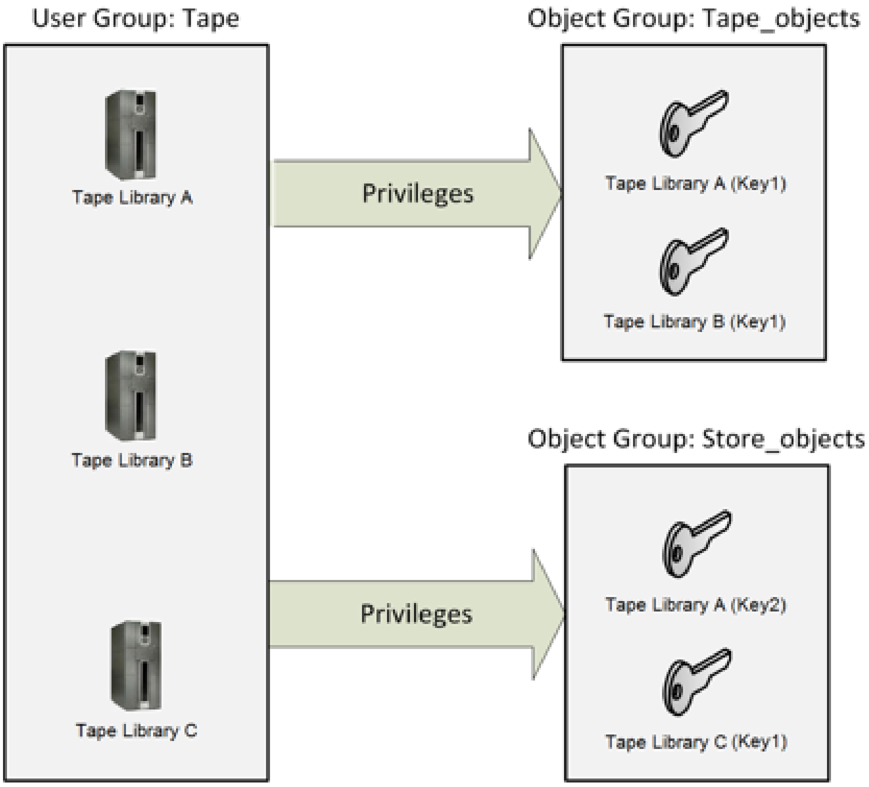


Figure 3 : Multiple target groups for a single source group

Merging source and target groups permissions

You have many individual user groups whose objects belong only to their own specific target group. For example:

- kmip_user1 is only a member of Group1_user and their objects exist only in Group1_objects.
- kmip_user2 is only a member of Group2_user and their objects exist only in Group2_objects.
- kmip_user100 is only a member of Group100_user and their objects exist only in Group100_objects.

You may encounter a situation in which each user requires access to the objects in all of the individual user's target groups. To accommodate this situation, create "common" user and target groups. In this case, perform the following steps:

1. Use the **Add** function in the Local Groups Configuration section to create the “common” user and target groups.

2. Use the **Add User** function to add each of the 100 KMIP users to this common user group’s group membership list.

3. Click the **Permissions** tab, and then click **Add** to add each KMIP user’s object group to the target group list.
   With this configuration, any user can access any object.

3.2.2.3 Operation-based permissions

The previous sections describe “privileges” in general terms. In the KMIP protocol, KMIP clients send requests for various operations to the KMIP server. These requests may be a **Create** operation to create a symmetric key, a **Register** operation to register a KMIP-managed object, a **Get Attributes** operation to retrieve attributes of a KMIP-managed object, a **Destroy** operation to destroy a KMIP-managed object, and so on. The KMIP permission model assigns privileges by operations. Therefore, in order for a user to be allowed to create a key, that user must have permission to perform the **Create** operation. Similarly, in order for a user to register a KMIP-managed object, that user must have permission to perform the **Register** operation.

Permissions are defined at the group level. For example, to retrieve an object the user must be a member of a group which has the **Get** permission enabled. To change the permissions of an existing group, see Modifying group permissions (p. 72).

3.3 Authentication mechanisms

There are two distinct authentication models:

- KMS authentication over XML protocol (p. 45)

- Authentication over KMIP protocol (p. 47)

3.3.1 KMS authentication over XML protocol

SSL/TLS is disabled in the default configuration of the ESKM XML protocol; the default port number for the XML protocol is 9000. Global keys can be created if the Owner Username field is left blank when creating a key via the Management Console.

An authenticated user has access to all global keys: all the keys owned by the user, and all keys accessible to groups to which the user belongs. In addition, a group of users can have an authorization policy assigned to it, which restricts the use of the keys accessible by that group to certain time periods or to certain operations per hour.

You can define a local users and groups list or use an LDAP server to centrally manage your users and groups.

3.3.1.1 Authentication options

The ESKM appliances provide many options with respect to security and authentication over the XML protocol. You can:

- Mandate SSL/TLS — You can choose between SSL/TLS connections and standard TCP connections; SSL/TLS connections are more secure since the data exchanged between client and server is encrypted.
- Allow global sessions — You can allow clients to access and create global keys without providing a valid username and password to the server.

⚠ Global sessions do not offer a high level of security.

- Disable global sessions — When you disable global sessions, all users are required to provide either a valid username and password combination, or a client certificate signed by a CA trusted by the appliance.
- Require client certificates — You can mandate that clients present a client certificate in order to establish an SSL/TLS connection to the server. This client certificate can be the sole means of authenticating to the server, or it can be used in tandem with a username and password.
- Enforce strong, two-factor authentication — You can take the “require client certificates” option one- step-further by having the ESKM appliance derive the username from the certificate. The username is then compared against the username provided in the authentication request. The user is authenticated only if the two usernames match and the password provided is correct.

Utimaco recommends that you enforce the most stringent security policy supported by the server. Such a security policy would mandate SSL/TLS, disallow global sessions, and enforce strong, two-factor authentication.

3.3.1.2 Key access and ownership

Keys can be created, using the ESKM XML protocol, as global keys or as keys owned by a particular user. When you assign group access permission for a key, all the users in that group (who have successfully authenticated to the ESKM appliance) can use that particular key.

When the client requests the server to generate a new key, it can specify that the key be exportable and/or deletable. An exportable key is one that a client can export from the ESKM appliance. An exportable key can be exported by the owner and any members of a group with the “Export” or “Full” permission for that key.

A deletable key is a key that the client can delete from the ESKM appliance. Only the owner of the key, or a member of the group that has “Full” permission access to the key, can delete the key.

Administrators with Keys and Authorization Policies access control can delete any key regardless of whether it is marked as deletable.

When the ESKM appliance is in FIPS-compliant mode, global key creation and use is not permitted.

3.3.2 Authentication over KMIP protocol

The KMIP server supports the KMIP authentication model which is used for clients communicating over the KMIP protocol.

The default port number for the KMIP protocol is 5696.

This authentication model is very different from the one used by clients over the ESKM XML protocol. Some of the differences are as follows:

- KMIP requires mutual authentication over the TLS protocol.

> ⚠ Sending unencrypted KMIP client requests over the standard TCP/IP protocol is not supported.

- There is no concept of global sessions in KMIP. The KMIP client cannot access keys without successfully authenticating with the KMIP server using one of the supported authentication mechanisms, see KMIP authentication mechanisms (p. 49).
- A client certificate is always required regardless of the KMIP authentication mechanism used. If the KMIP client chooses to use certificate-based authentication, the KMIP server matches the client certificate sent over the KMIP protocol with the one supplied during creation of the KMIP-enabled user, to determine the identity of the user and the user’s privileges. For KMIP clients using password authentication, the client must also provide a certificate for TLS authentication. In this case, the KMIP server determines the client identity based on the username or device identifier specified in the client request. The KMIP server uses the username/device identifier and the password to authenticate the user.

3.3.2.1 Key access and ownership

Unlike the ESKM XML protocol, the KMIP protocol does not support the concept of global keys. KMIP keys and other managed objects are always initially owned by the creator, although ownership can be changed by the system administrator using the Management Console. However, as discussed in the section Users, groups, and permissions (p. 37), permissions to access a particular key are determined by groups. All KMIP-enabled users who belong to the same user group as the key creator have the same privileges with respect to that KMIP object. The permission of a KMIP-enabled user to access KMIP-managed objects also depends on the object group(s) that the KMIP object belongs to, and whether there are privileges flowing from the source user group to the target object group.

KMS keys have three configurable attributes:

- Exportable
- Deletable
- Versioned

KMIP-managed objects have many other attributes. Some of the more common attributes are the following:

- Cryptographic algorithm
- Cryptographic length
- Digest
- Fresh
- Initial date
- Key format type
- Last change date
- Lease Time
- Name
- Object group
- Object type
- Original creation date
- State
- Unique identifier

The supported KMIP attributes depend on the version of the KMIP protocol being used. A full list of supported KMIP attributes can be found in the KMIP protocol specification. For KMIP-supported attributes, see Chapter 3 of KMIP Specification Version 1.4[3], published by OASIS.

3.4 KMIP authentication mechanisms

ESKM 4.1 and above support these KMIP protocol client authentication mechanisms:

- Certificate-based authentication (p. 50)
- Authentication using credential objects (p. 50)

[3] http://docs.oasis-open.org/kmip/spec/v1.4/kmip-spec-v1.4.pdf

Regardless of the authentication mechanism used, a client certificate must be provided for TLS authentication.

> Query operations used to interrogate ESKM appliance features and functions do not require authentication.

3.4.1 Certificate-based authentication

With certificate-based authentication, the KMIP client does not supply a credential structure in the KMIP client request. Instead, the client certificate used for TLS authentication is also used to determine the user identity.

3.4.1.1 Configuring KMIP-enabled users with certificates

A system administrator must first add the KMIP-enabled user and specify the client certificate before a KMIP client can send a request using certificate authentication. This task can be accomplished from either the Management Console or the CLI. The ESKM appliance stores this client certificate with the user properties in the KMIP user database. Unlike the ESKM XML protocol, which can derive the username from the certificate by extracting it from fields such as the Common Name, the KMIP protocol does not require that Common Name or any other field in the certificate to match the username. Instead, the raw certificate contents, sent in the KMIP client request, are compared with the certificate contents configured in the ESKM KMIP user database, and if the values are the same, the KMIP username is derived. Since the certificate contents are used to derive the username, the certificate must be unique. A single certificate cannot be shared by more than one KMIP-enabled user.

3.4.2 Authentication using credential objects

In addition to the certificate-based authentication, the KMIP protocol also provides client authentication using a Credential object. This is a structure used for client identification purposes and is managed by the appliance outside of the KMIP protocol. The Credential object contains two components:

- Credential type. ESKM appliances support two types of credentials:
    - Username and password credential authentication
    - Device credential authentication
- Credential value

The system administrator must use either the Management Console or the CLI to create a KMIP-enabled user with the matching username and password before either the username/ password or the device credential authentication will succeed.

3.4.2.1 Username and password credential authentication

If the Credential Type in the Credential is Username and Password (value 00000001), then the Credential Value in the KMIP client request will contain the Username and Password as text strings. For the authentication to succeed, the credential supplied in the KMIP client request must match the username and password that is configured in the ESKM appliance by the system administrator for a KMIP-enabled user.

3.4.2.2 Device credential authentication

If the Credential Type in the Credential is Device (value 00000002), the Credential Value is a structure that contains one, or a combination of, the following components:

- Device serial number
- Password
- Device identifier
- Network identifier
- Machine identifier
- Media identifier

The combination of these values must be unique.

For authentication using device credentials to succeed, the credentials must match the username and password that is configured in the ESKM appliance by the system administrator for a KMIP-enabled user. The username must be of the following format:

device-serial-number:device-identifier:network-identifier:machine-identifier:mediaidentifier

For example:

- device serial number = serial123
- device identifier = devid456
- network identifier = undefined (i.e. blank)

- machine identifier = machine1
- media identifier - undefined (i.e. blank)

The username configured is as follows:

```
serial123:devid456::machine1::
```

In addition, the password field in the credential structure must match the password configured for this KMIP-enabled user.

3.5 Upgrading from a previous ESKM version

Use the software upgrade feature in ESKM to upgrade your ESKM appliance to future versions, see Software upgrade/install (p. 203).

Please stop the KMS service in all cluster nodes OR disable any client registration that changes (add, modify or delete) the ESKM Users, before upgrading from **ESKM v8.1** in a cluster environment. Also, please take a full backup before upgrading.

> ⚠ Refrain from restoring backup(s) while the cluster nodes are being upgraded.

4 Performing configuration and operation tasks

This section includes procedures on the following topics:

4.1 Configuring ESKM services and port numbers

This section lists the ESKM services and their default port numbers. Configure your firewall to allow clients to connect to these ports and to access these services. The following table provides the Management Console functions and the Command Line Interface (CLI) commands that can be used to change the default port numbers.

Table 3: ESKM Services and Port Numbers

Service/Interface	***Default Port Number***	***Management Console Function***	***CLI Command***
Command Line Interface (SSH)	22	Remote administration settings (p. 505)	edit ras settings (p. 740)
ESKM Cluster	9001 9002	Cluster settings (p. 427)	n/a
FIPS Status	9081	FIPS status server (p. 381)	fips server (p. 647)
KMIP Health Check	9082	KMIP health check (p. 418)	kmip-health check (p. 657)
KMIP Server	5696	KMIP server settings (p. 411)	none
KMS Health Check	9080	Health check (p. 409)	health check (p. 657)
KMS Server	9000	KMS server settings (p. 400)	none
REST Server and HSM console	8443	REST server settings (p. 419) HSM Console (p. 764)	none

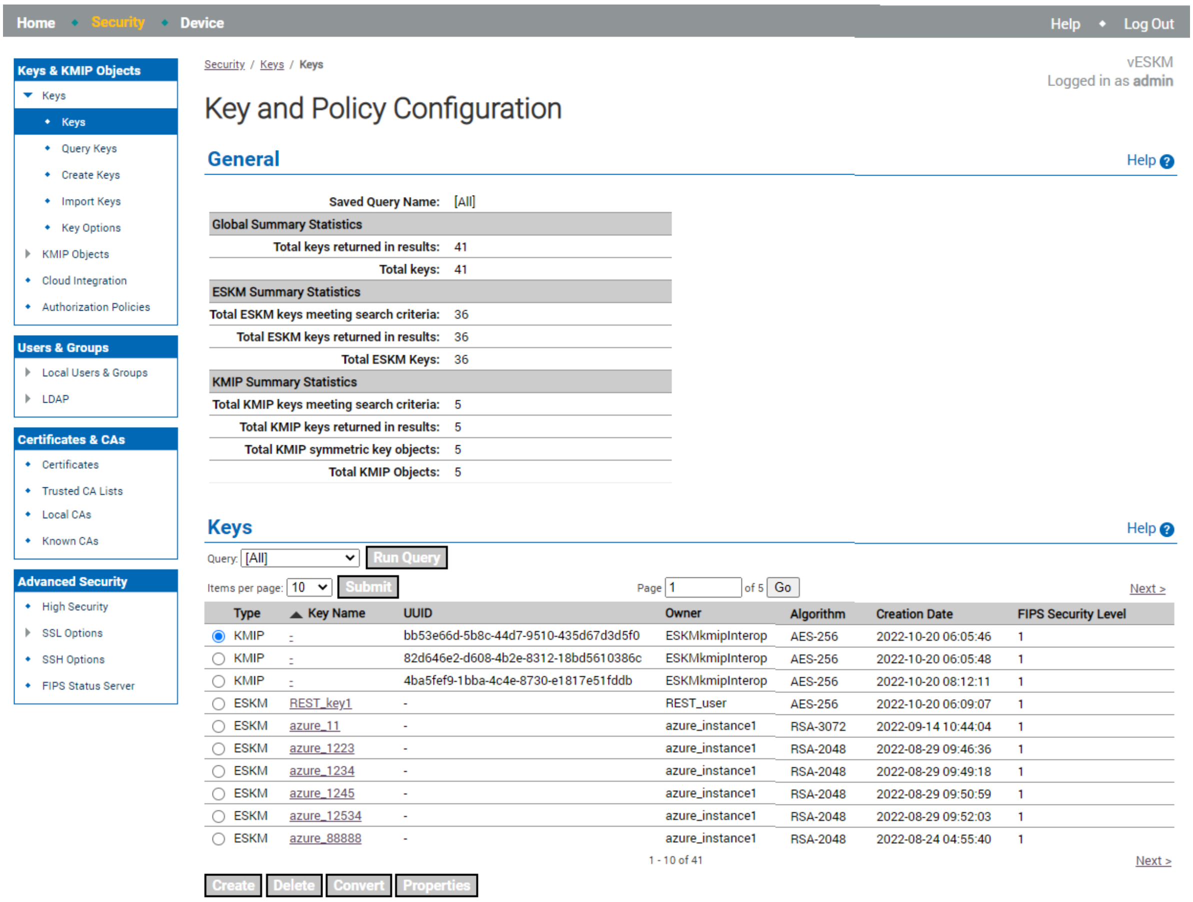
Service/Interface	***Default Port Number***	***Management Console Function***	***CLI Command***
LDAP	389, 636	LDAP user directory properties (p. 326)	ldap test administrators primary (p. 597)
Management Console (SSL/TLS)	9443	Remote administration settings (p. 505)	edit ras settings (p. 740)
SNMP Agent	161	SNMP agent settings (p. 455)	snmp agent (p. 721)
SNMP Management Station	162	SNMP management station list (p. 462)	station (p. 723)
Syslog	514	Syslog settings (p. 525)	system syslog (p. 679)
Google Cloud EKM	443	Cloud Integration (p. 763)	Refer Cloud Integration Guide (p. 763)

⚠ The port number assigned to each service or interface must be unique. The port numbers for certain well-known services cannot be changed. The ESKM appliance uses the following port numbers:

- NTP (port 123)
- SCP (port 22)

4.2 Key and policy procedures

This section describes the procedures to create and manage keys.



Key and Policy Configuration

General

Saved Query Name:	[All]
Global Summary Statistics	
Total keys returned in results:	41
Total keys:	41
ESKM Summary Statistics	
Total ESKM keys meeting search criteria:	36
Total ESKM keys returned in results:	36
Total ESKM Keys:	36
KMIP Summary Statistics	
Total KMIP keys meeting search criteria:	5
Total KMIP keys returned in results:	5
Total KMIP symmetric key objects:	5
Total KMIP Objects:	5

Keys

Query: [All]

Items per page: 10

Page 1 of 5

	Type	▲ Key Name	UUID	Owner	Algorithm	Creation Date	FIPS Security Level
●	KMIP	-	bb53e66d-5b8c-44d7-9510-435d67d3d5f0	ESKMkmipInterop	AES-256	2022-10-20 06:05:46	1
○	KMIP	-	82d646e2-d608-4b2e-8312-18bd5610386c	ESKMkmipInterop	AES-256	2022-10-20 06:05:48	1
○	KMIP	-	4ba5fef9-1bba-4c4e-8730-e1817e51fddb	ESKMkmipInterop	AES-256	2022-10-20 08:12:11	1
○	ESKM	REST_key1	-	REST_user	AES-256	2022-10-20 06:09:07	1
○	ESKM	azure_11	-	azure_instance1	RSA-3072	2022-09-14 10:44:04	1
○	ESKM	azure_1223	-	azure_instance1	RSA-2048	2022-08-29 09:46:36	1
○	ESKM	azure_1234	-	azure_instance1	RSA-2048	2022-08-29 09:49:18	1
○	ESKM	azure_1245	-	azure_instance1	RSA-2048	2022-08-29 09:50:59	1
○	ESKM	azure_12534	-	azure_instance1	RSA-2048	2022-08-29 09:52:03	1
○	ESKM	azure_88888	-	azure_instance1	RSA-2048	2022-08-24 04:55:40	1

1 - 10 of 41

Figure 4 : Key and Policy Configuration

This section explains the following processes:

- Creating a key (p. 57)
- Importing a key (p. 58)
- Setting group permissions for a key (p. 59)
- Downloading an RSA key (p. 60)
- Deleting a key (p. 61)

4.2.1 Creating a key

⚠ This section is applicable only to KMS keys. KMIP keys can only be created using KMIP client Create and Create Key Pair request operations, not via the Management Console.

To create a KMS key:

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2. Navigate to the **Create Key** section on the **Key and Policy Configuration** page (**Security** > **Keys** > **Create Keys**).

3. Enter a unique KMS key name in the **Key Name** field. KMS and KMIP keys have different name-spaces. Therefore, a KMS key can have the same name as another KMIP key, but it cannot have the same name as another KMS key.

4. Enter a value in the **Owner Username** field to assign a specific owner or leave this value blank to create a global key. If an owner is listed for the key, only that user can access the key, unless you set up group permissions. Global keys can be accessed by all users.

5. Select an Algorithm.

6. To make the key deletable by the owner or members of the group with “Full” permission to access the key, select **Deletable**. Deletable global keys are deletable by all users.

7. To make the key exportable from the ESKM appliance, select **Exportable**. An exportable key can be exported by its owner and by members of a group with “Export” or “Full” permission for the key. An exportable global key is exportable by all users.

8. To allow multiple versions of the key, select **Versioned Key Bytes**. Each key version has unique key bytes, but shared key metadata (key name, algorithm, permissions, etc.).

9. To copy permission settings from an existing key, select **Copy Group Permissions From**.

10. Click **Create**.

Create a backup immediately after creating a key. There is no way to recover a key that has not been backed up.

4.2.2 Importing a key

This section is applicable only to KMS keys. KMIP keys can only be imported using KMIP client Register request operation, not via the Management Console.

To import a KMS key:

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2. Navigate to the Import Keys section on the Key and Policy Configuration page (**Security** > **Keys** > **Import Keys**).

3. Enter a unique key name in the **Key Name** field.

4. Enter a value in the **Owner Username** field to assign a specific owner or leave this value blank to create a global key. If an owner is listed for the key, only that user can access the key, unless you set up group permissions. Global keys can be accessed by all users.

5. Select an Algorithm.

6. To make the key deletable by the owner or members of the group with “Full” permission to access the key, select **Deletable**. Deletable global keys are deletable by all users.

7. To make the key exportable from a non-FIPS ESKM appliance, select **Exportable**. To export a key from a FIPS-compliant ESKM appliance, TLS must be enabled. An exportable key can be exported by its owner and by members of a group with “Export” or “Full” permission for the key. An exportable global key is exportable by all users.

8. Paste the key bytes in the **Key** field. Asymmetric keys must be imported in PEM-encoded ASN.1 DER-encoded PKCS #1 format, and both the public and private keys must be imported. Symmetric keys must be in Base 16 format, and in the case of DES keys, parity bits must be properly set.

9. Click **Import**.

> ⚠ The ESKM appliance does not import keys that are known to be weak, such as 64-bit DES. In addition, the parity bits must be set properly; otherwise, the appliance returns an error.

4.2.3 Setting group permissions for a key

> ⚠ This section is applicable only to KMS keys, not KMIP keys.

Prior to setting group permissions, you must create a group. If your group permissions use an authorization policy, you must also create that authorization policy before continuing.

To set the group permissions for a key:

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2. Navigate to to the Keys section of the Key and Policy Configuration page (**Security** > **Keys**). Select the key for which you want to create permissions.

3. Go to the **Group Permissions** section on the **Permissions** tab.
4. Click **Add**.
5. Enter a group name in the **Group** field.
6. Select **Always** or choose an Authorization Policy for the export operation.
7. Select either **Always** or **Never** for the Full permission attribute.
8. Click **Save**.
9. Click **Add** to create permissions for additional groups.

4.2.4 Downloading an RSA key

> ⚠ Downloading an RSA key using the Management Console is applicable to KMS keys only. To download KMIP public keys and other managed objects, use the KMIP client Get request operation.

To download an RSA key:

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.
2. Navigate to the **Keys** section of the **Key and Policy Configuration** page (**Security** > **Keys**). Select the RSA key.
3. Go to the **Public Key** section.
4. Click **Download Public Key** to download the public portion of the RSA key.

4.2.5 Deleting a key

To delete a key:

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2. Navigate to the Keys section of the Key and Policy Configuration page (**Security** > **Keys**).

3. Select the key, and then click **Delete**.

> The steps above apply to both KMS and KMIP keys. Only KMIP symmetric key objects can be deleted from the **Keys** section of the **Key and Policy Configuration** page. To delete other KMIP-managed objects, perform the below steps.

1. Go to the **Security** > **KMIP Objects** page.

2. Select the key, and then click **Delete**.

4.2.6 Purging destroyed KMIP objects

> This section is applicable to destroyed KMIP objects. This action purges destroyed objects which reside on all ESKM appliances in a cluster.

The KMIP client **Destroy** request operation sets the KMIP-managed object state to Destroyed, but does not physically remove the managed object from the ESKM appliance. You may want to periodically purge destroyed KMIP objects to free up storage space on the appliance.

To purge destroyed KMIP-managed objects:

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

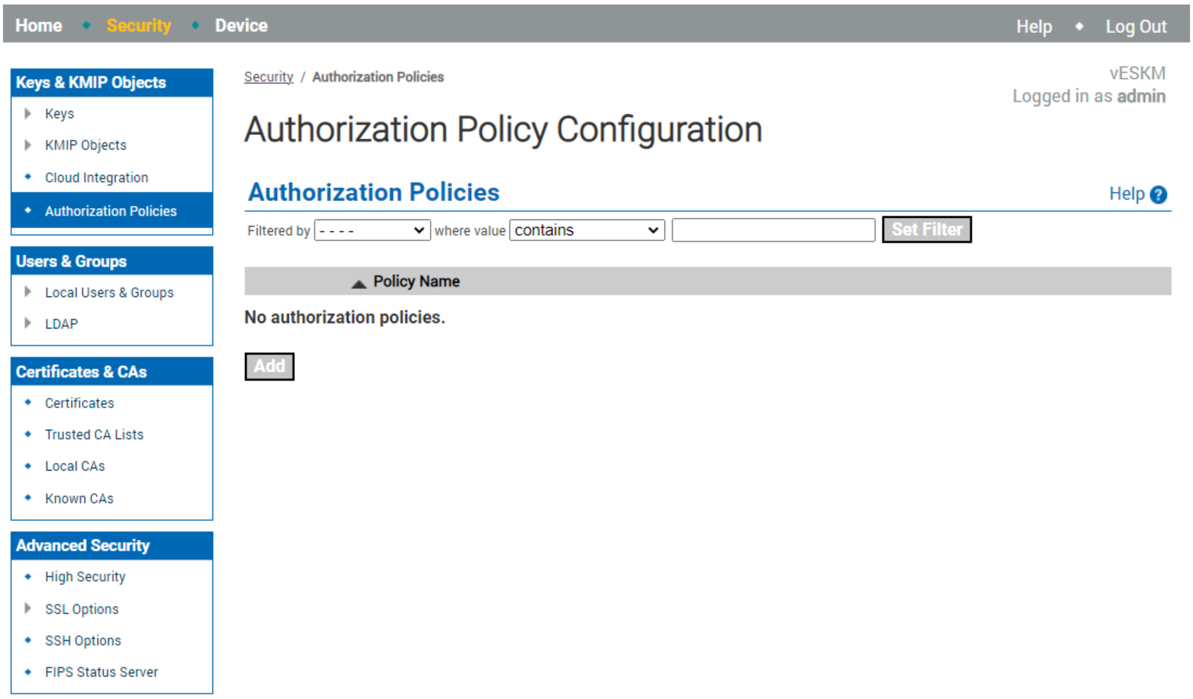
2. Navigate to the KMIP Objects Configuration section (**Security** > **KMIP Objects**).

3. Click **Purge Destroyed Objects**.

4.3 Authorization policy procedures

Authorization policies are applicable only to KMS keys, not KMIP keys.

This section describes the procedures you will follow when creating and managing authorization policies.



Authorization Policy Configuration

Authorization Policies

No authorization policies.

Figure 5 : Authorization Policies

This section explains the following processes:

- Creating an authorization policy (p. 63)

- Deleting an authorization policy (p. 63)

4.3.1 Creating an authorization policy

To create an authorization policy:

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2. Navigate to the Authorization Policies section of the Authorization Policy Configuration page (**Security** > **Authorization Policies**).

3. Click **Add**.

4. Enter a **Policy Name**.

5. Click **Save**.

6. Select the Policy to access on the **Authorization Policy Configuration** page.

7. Click **Edit** to establish a rate limit using the **Maximum Operations per Hour** field, and then click **Save**.

8. Click **Add** to establish a time limit using the **Start Day**, **Start Time**, **End Day**, and **End Time** fields.

9. Click **Save**. Repeat this step to set multiple usage periods.

4.3.2 Deleting an authorization policy

To delete an authorization policy:

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

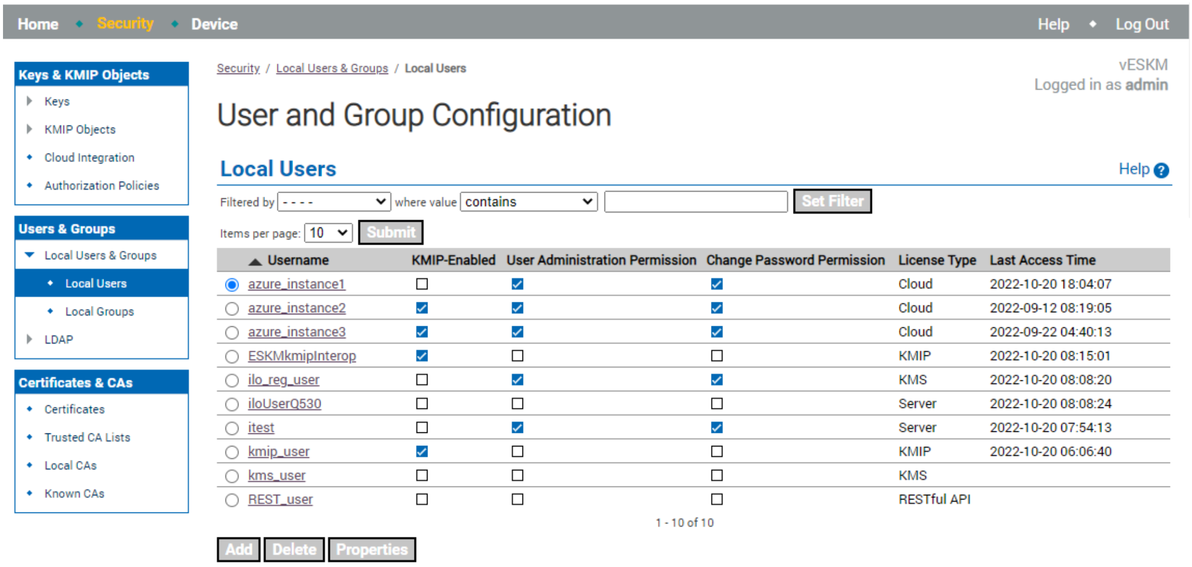
2. Navigate to the Authorization Policies section of the Authorization Policy Configuration page (**Security** > **Authorization Policies**).

3. Select a Policy Name.

4. Click **Delete**.

4.4 User and group procedures

This section describes the procedures you will follow when creating and managing local users and groups.



User and Group Configuration

Local Users

Filtered by - - - - where value contains

Items per page: 10

Username	KMIP-Enabled	User Administration Permission	Change Password Permission	License Type	Last Access Time
● azure_instance1	□	☑	☑	Cloud	2022-10-20 18:04:07
○ azure_instance2	☑	☑	☑	Cloud	2022-09-12 08:19:05
○ azure_instance3	☑	☑	☑	Cloud	2022-09-22 04:40:13
○ ESKMkmipInterop	☑	□	□	KMIP	2022-10-20 08:15:01
○ ilo_reg_user	□	☑	☑	KMS	2022-10-20 08:08:20
○ iloUserQ530	□	□	□	Server	2022-10-20 08:08:24
○ itest	□	☑	☑	Server	2022-10-20 07:54:13
○ kmip_user	☑	□	□	KMIP	2022-10-20 06:06:40
○ kms_user	□	□	□	KMS	
○ REST_user	□	□	□	RESTful API	

1 - 10 of 10

Figure 6 : User and Group Configuration

This section explains the following processes:

- Creating a group (p. 65)
- Creating a user (p. 66)
- Adding a user to a group (p. 69)
- Modifying a user (p. 69)
- Removing a user from a group (p. 71)
- Deleting a user (p. 71)

- Deleting a group (p. 72)

To efficiently add users to the ESKM appliance, Utimaco recommends that you first create the user group; then, when you create a user, you can specify the group(s) to which the user belongs.

> User accounts and groups can be managed locally on the ESKM appliance and shared among the other ESKM appliances in the cluster. This is the preferred method, as this maintains the Federal Information Processing Standards (FIPS) compliance for the ESKM appliances. User accounts and groups can also be managed centrally.

4.4.1 Creating a group

When you create a KMIP group, the ESKM appliance uses the name you specify to create a KMIP object group, and also automatically creates a KMIP user group which has the suffix "_user" appended to it. For example, if you create a KMIP group named "Finance", the server creates a KMIP object group named "Finance", and also a KMIP user group named "Finance_user". You can change these names if necessary. For more information on this topic, see User groups and object groups (p. 38).

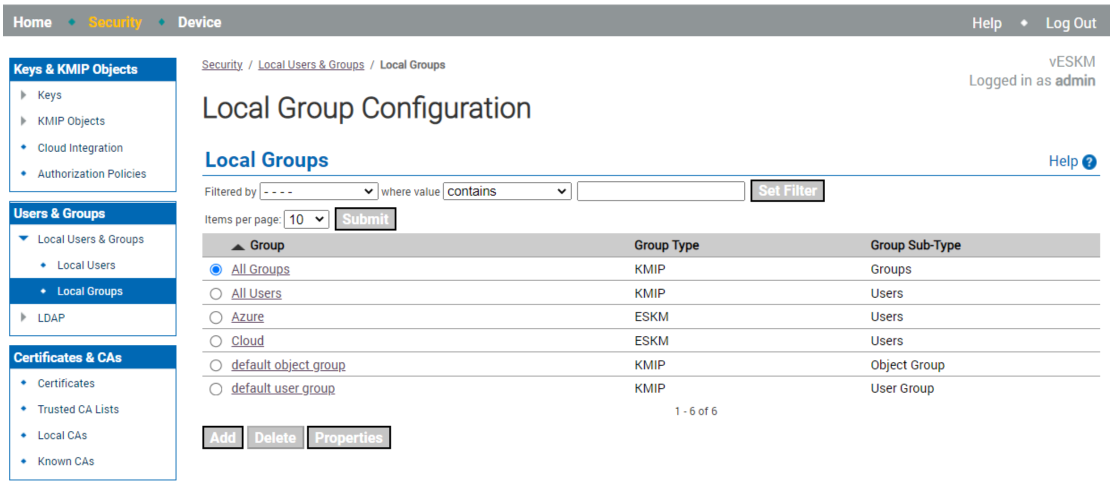
> KMS group names must begin with a letter. Names can only contain letters, numbers, hyphens, underscores, and periods.
>
> KMIP group names can begin with either a letter or a number. Names can only contain letters, numbers, colons, spaces, hyphens, underscores, and periods.

To create a group:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the Local Groups section of the User and Group Configuration page (**Security** > **Local Users & Groups** > **Local Groups**).

3. Click **Add**.



Local Group Configuration

Local Groups

Filtered by - - - - where value contains

Items per page: 10

	Group	Group Type	Group Sub-Type
●	All Groups	KMIP	Groups
○	All Users	KMIP	Users
○	Azure	ESKM	Users
○	Cloud	ESKM	Users
○	default object group	KMIP	Object Group
○	default user group	KMIP	User Group

1 - 6 of 6

Figure 7 : Local Groups

4. Enter a name in the **Group** field.

5. Choose the group type, either ESKM or KMIP.

6. If you chose ESKM as the group type, click **Save**. If you chose KMIP as the group type, click **Next**. At the next screen, you can change the KMIP user and group names if necessary.

7. Click **Save**.

You can now add users to the group.

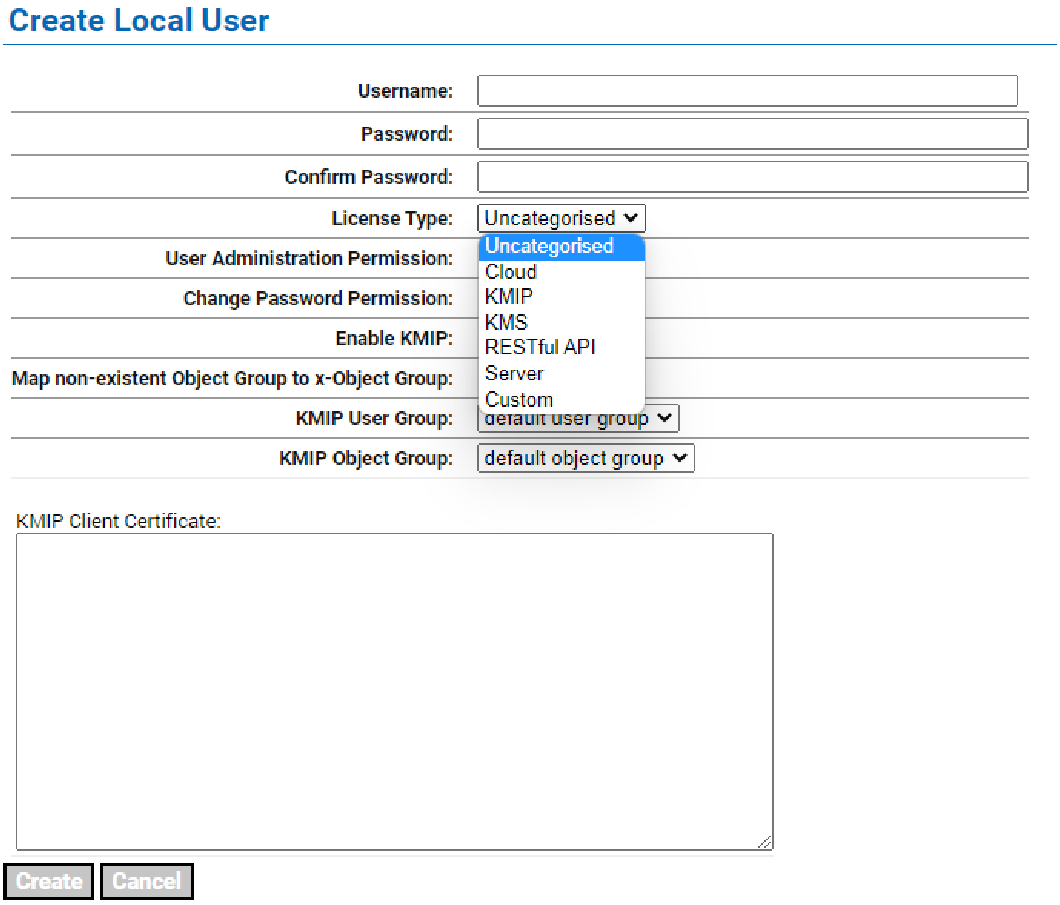
4.4.2 Creating a user

To create a user:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to to the Local Users section of the User and Group Configuration page (**Security** > **Local Users & Groups** > **Local Users** > **Local Users**).

3. Click **Add**.
   The **Create Local User** window appears.



Create Local User

Username:	
Password:	
Confirm Password:	
License Type:	Uncategorised
User Administration Permission:	
Change Password Permission:	
Enable KMIP:	
Map non-existent Object Group to x-Object Group:	
KMIP User Group:	default user group
KMIP Object Group:	default object group

KMIP Client Certificate:

Figure 8 : Create Local User

4. Enter a username and password and enter the password again in the **Confirm Password** field.

5. Select the appropriate **License Type** from the drop down.

6. To give this user the ability to create, modify, and delete users and groups via the ESKM XML interface, select **User Administration Permission**.

7. To give this user the ability to change their own password via the ESKM XML interface, select **Change Password Permission**. Users with User Administration Permission selected automatically have this ability.

8. The **Enable KMIP** check box is checked by default. This gives the user the ability to communicate with the ESKM appliance either via the ESKM XML interface or via KMIP interface. To prevent this user from communicating via KMIP interface, un-check the **Enable KMIP** check box.

   The following settings apply only to KMIP-enabled users. If the **Enable KMIP** box is unchecked, these settings are grayed out and therefore cannot be set.

   a. The interoperability option **Map non-existent Object Group to x-Object Group** is unchecked by default. Some non-standard KMIP clients require this option to be checked for interoperability. The standard KMIP behavior is to fail the KMIP client request if an Object Group attribute has an object group name that does not exist on the ESKM appliance. If this option is checked, and the KMIP client specifies an object group name that does not exist, the Object Group attribute is mapped to the x-Object Group custom attribute, and the request succeeds. Setting this option will only enable this feature for this user. To enable this feature for all KMIP-enabled users, see Interoperability (p. 307).

   b. Select the **KMIP User Group** from the drop-down box. This is the name of the KMIP user group that this user will be a member of upon creation. Subsequently, this user can be added to more or other KMIP user groups or removed from existing groups via the **Local Groups Properties** page. To ensure that this KMIP-enabled user has the privileges to create KMIP objects, in either the default object group or the object groups specified in the KMIP client request, this KMIP-enabled user must be a member of a user group that has the correct privileges to create objects in these object groups. For more information see **KMIP permission model** (p. 38).

   c. Select the **KMIP Object Group** from the drop-down box. This is the name of the group to which all of the objects that the KMIP user creates belong.

   d. If a client certificate will be used to authenticate the KMIP client to the ESKM appliance, paste the contents of the PEM-encoded client certificate into the

KMIP Client Certificate field. The -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines are optional.

9. Click **Create.**

4.4.3 Adding a user to a group

To add a user to a group:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the **Local Groups** section of the User and Group Configuration page (**Security** > **Local Users & Groups** > **Local Groups**).

3. Select a Group, and then click **Properties**, or click the group name to access the ESKM User List or the KMIP Group Membership List section.

4. To add an ESKM user, click **Add**, and then enter the username in the **Username** field. To add a KMIP-enabled user, click **Add User**, and then select a KMIP-enabled user from the Name drop-down list.

5. Click **Save**.

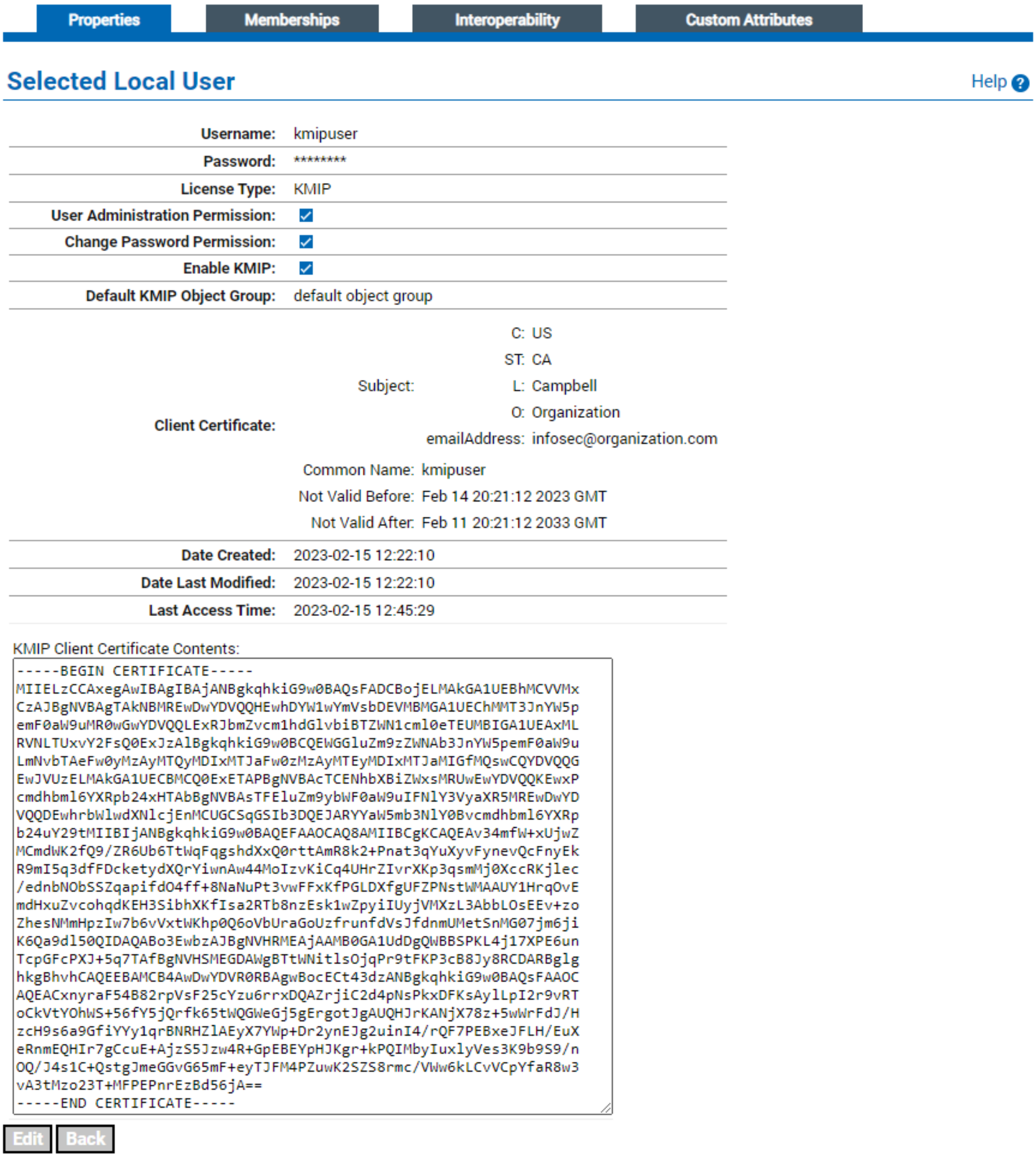
4.4.4 Modifying a user

To change any of the properties of a user:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the **Local Users** section of the User and Group Configuration page (**Security** > **Local Users & Groups** > **Local Users**).

3. Select the underlined username of the user to modify. The **User and Group Configuration** window appears.



Selected Local User

Username:	kmipuser
Password:	********
License Type:	KMIP
User Administration Permission:	☑
Change Password Permission:	☑
Enable KMIP:	☑
Default KMIP Object Group:	default object group
Client Certificate:	Subject: C: US ST: CA L: Campbell O: Organization emailAddress: infosec@organization.com Common Name: kmipuser Not Valid Before: Feb 14 20:21:12 2023 GMT Not Valid After: Feb 11 20:21:12 2033 GMT
Date Created:	2023-02-15 12:22:10
Date Last Modified:	2023-02-15 12:22:10
Last Access Time:	2023-02-15 12:45:29

KMIP Client Certificate Contents:

```
-----BEGIN CERTIFICATE-----
MIIELzCCAxegAwIBAgIBAjANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcm1hdGlvbiBTZWN1cml0eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9u
LmNvbTAeFw0yMzAyMTQyMDIxMTJaFw0zMzAyMTEyMDIxMTJaMIGfMQswCQYDVQQG
EwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCENhbXBiZWxsMRUwEwYDVQQKEwxP
cmdhbml6YXRpb24xHTAbBgNVBAsTFEluZm9ybWF0aW9uIFNlY3VyaXR5MREwDwYD
VQQDEwhrbWlwdXNlcjEnMCUGCSqGSIb3DQEJARYYaW5mb3NlY0Bvcmdhbml6YXRp
b24uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv34mfW+xUjwZ
MCmdWK2fQ9/ZR6Ub6TtWqFqgshdXxQ0rttAmR8k2+Pnat3qYuXyvFynevQcFnyEk
R9mI5q3dfFDcketydXQrYiwnAw44MoIzvKiCq4UHrZIvrXKp3qsmMj0XccRKjlec
/ednbNObSSZqapifdO4ff+8NaNuPt3vwFFxKfPGLDXfgUFZPNstWMAAUY1HrqOvE
mdHxuZvcohqdKEH3SibhXKfIsa2RTb8nzEsk1wZpyiIUyjVMXzL3AbbLOsEEv+zo
ZhesNMmHpzIw7b6vVxtWKhp0Q6oVbUraGoUzfrunfdVsJfdnmUMetSnMG07jm6ji
K6Qa9dl50QIDAQABo3EwbzAJBgNVHRMEAjAAMB0GA1UdDgQWBBSPKL4j17XPE6un
TcpGFcPXJ+5q7TAfBgNVHSMEGDAWgBTtWNitlsOjqPr9tFKP3cB8Jy8RCDARBglg
hkgBhvhCAQEEBAMCB4AwDwYDVR0RBAgwBocECt43dzANBgkqhkiG9w0BAQsFAAOC
AQEACxnyraF54B82rpVsF25cYzu6rrxDQAZrjiC2d4pNsPkxDFKsAylLpI2r9vRT
oCkVtYOhWS+56fY5jQrfk65tWQGWeGj5gErgotJgAUQHJrKANjX78z+5wWrFdJ/H
zcH9s6a9GfiYYy1qrBNRHZlAEyX7YWp+Dr2ynEJg2uinI4/rQF7PEBxeJFLH/EuX
eRnmEQHIr7gCcuE+AjzS5Jzw4R+GpEBEYpHJKgr+kPQIMbyIuxlyVes3K9b9S9/n
OQ/J4s1C+QstgJmeGGvG65mF+eyTJFM4PZuwK2SZS8rmc/VWw6kLCvVCpYfaR8w3
vA3tMzo23T+MFPEPnrEzBd56jA==
-----END CERTIFICATE-----
```

Each tab at the top of the window shows categories of settings assigned to that user. For more information about each setting, see Creating a user (p. 66).

4. Click **Edit**. The properties of the selected user become editable.

5. Make the required modifications to the user.

6. Click **Save**. The user has now been modified.

4.4.5 Removing a user from a group

To perform any operation on a key, a user must be a member of a group that has permission to manage the key.

To remove a user from a group:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the Local Groups section of the User and Group Configuration page (**Security > Local Users & Groups > Local Groups**).

3. Select a Group, and then click **Properties**, or click the group name to access the ESKM User List or the KMIP Group Membership List section.

4. Select the **Username**, and then click **Delete**.

4.4.6 Deleting a user

If you discover that you erroneously deleted a user, you can recreate that user. After recreating the user, you must manually add the user to the groups to which the user belonged previously.

You cannot delete a user if the user is a key owner

To delete a user:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the Local Users section of the User and Group Configuration page (**Security > Local Users & Groups > Local Users**).

3. Select the **Username**, and then click **Delete**.

4.4.7 Deleting a group

Prior to deleting a KMIP user group, you must first delete all KMIP-enabled users from the group. Similarly, to delete a KMIP object group, you must first delete all KMIP objects from the KMIP object group.

To delete a group:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the Local Groups section of the User and Group Configuration page (**Security** > **Local Users & Groups** > **Local Groups**).

3. Select the **Group**, and then click **Delete**.

❗ When a group is deleted, the group permission is also deleted from the key. Re-adding the group will not give back the group permission to the key.

4.4.8 Modifying group permissions

Permissions are defined for the group, not the user. Any user in the group can perform all of the operations assigned to the group of which they are a member. Normally you define the group permissions when you create the group. However as user requirements change, you can change the permissions of the group. For example, the user group does not have the **Get** permission enabled and a user in the group needs the

Get permission to retrieve an object.
Before you can modify the permissions, you must first determine the user's default target and source groups.

To determine the user's target object group:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.
2. Navigate to the Local Users section of the User and Group Configuration page (**Security** > **Local Users & Groups** > **Local Users**).
3. Select the **Username** and then click **Properties**. The value in the **Default KMIP Object Group** is the user's target object group.

⚠ The user may be a member of multiple user groups and therefore have access to multiple target object groups. Click **Memberships** to see a list of all target object groups which the user can access.

To determine the user's source group:

1. Click the **Memberships** tab, and then click on the user's target object group (the value from step 3 above). The **Source Group**: field displays the user's source group.

To edit the permissions of the user's target object group:

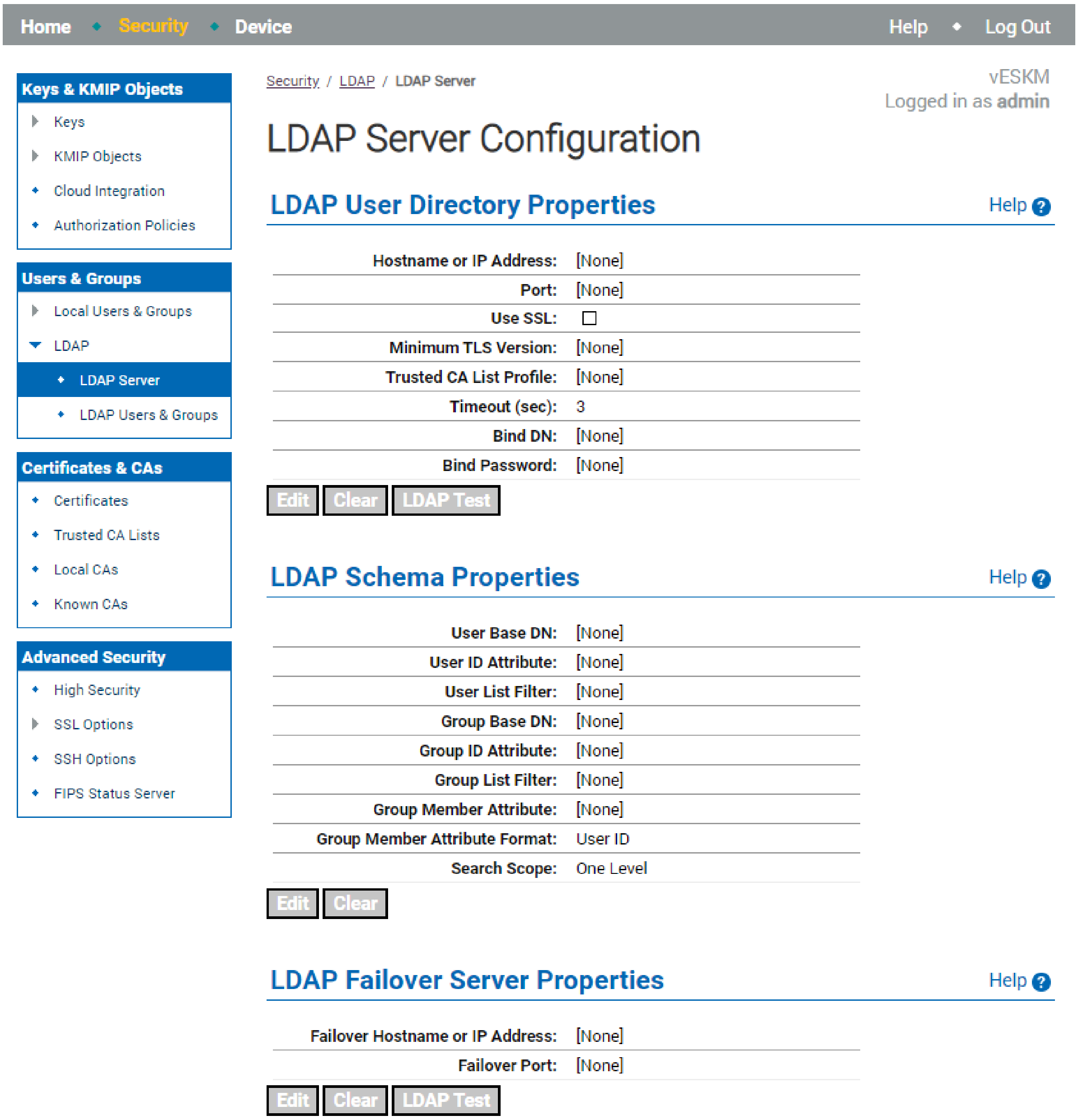
1. Navigate to the Local Groups section of the User and Group Configuration page (**Security** > **Local Users & Groups** > **Local Groups**).
2. Select the user's source group name (the value from step 1 under To determine the user's source group (p. 72)) and then click **Properties**.
3. Click the **Permissions** tab, select the user's target object group name (the value from step 3 under To determine the user's target object group (p. 72)), and then click **Permissions**.

4. Confirm that the **Source Group** and **Target Group** fields, (located in the Target Group Permissions section) contain the correct group names.

5. Click **Edit**, adjust the user’s target object group permissions as necessary, and then click **Save**.

4.5 LDAP server procedures

This section describes the procedures you will follow when managing LDAP servers.



LDAP Server Configuration

LDAP User Directory Properties

Hostname or IP Address:	[None]
Port:	[None]
Use SSL:	□
Minimum TLS Version:	[None]
Trusted CA List Profile:	[None]
Timeout (sec):	3
Bind DN:	[None]
Bind Password:	[None]

LDAP Schema Properties

User Base DN:	[None]
User ID Attribute:	[None]
User List Filter:	[None]
Group Base DN:	[None]
Group ID Attribute:	[None]
Group List Filter:	[None]
Group Member Attribute:	[None]
Group Member Attribute Format:	User ID
Search Scope:	One Level

LDAP Failover Server Properties

Failover Hostname or IP Address:	[None]
Failover Port:	[None]

Figure 9 : LDAP Server Configuration

This section explains the following processes:

- Setting up the LDAP user directory (p. 76)
- Testing the LDAP user directory connection (p. 77)
- Setting up the LDAP schema (p. 77)
- Setting up an LDAP failover server (p. 77)

- Testing the LDAP failover server connection (p. 78)

⚠ LDAP users are only supported for ESKM users communicating over the ESKM XML protocol.

4.5.1 Setting up the LDAP user directory

To set up the LDAP user directory:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.
2. Navigate to the LDAP User Directory Properties section of the LDAP Server Configuration page (**Security** > **LDAP** > **LDAP Server**).
3. Click **Edit**.
4. Enter the **Hostname or IP Address**, and then enter the **Server Port**.
5. If you are using SSL/TLS, check **Use SSL**, enter the **Minimum TLS Version**, and **Trusted CA List** Profile.
6. Enter the number of seconds to wait for the LDAP server during connections in the **Timeout** field.
7. Enter the **Bind DN** (distinguished name) and **Bind Password**.
8. Click **Save**.

⚠ On a FIPS-compliant appliance, selecting a Minimum TLS version earlier than TLS 1.2, will make the appliance non-FIPS-compliant.

4.5.2 Testing the LDAP user directory connection

To test the LDAP user directory connection:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the LDAP User Directory Properties section of the LDAP Server Configuration page (**Security** > **LDAP** > **LDAP Server**).

3. Click **LDAP Test**.

4.5.3 Setting up the LDAP schema

To set up the LDAP schema:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the LDAP Schema Properties section of the LDAP Server Configuration page (**Security** > **LDAP** > **LDAP Server**).

3. Click **Edit**.

4. Enter the values for your LDAP schema.

5. Click **Save**.

4.5.4 Setting up an LDAP failover server

To set up an LDAP failover server:

1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the LDAP Failover Server Properties section of the LDAP Server Configuration page (**Security** > **LDAP** > **LDAP Server** > **LDAP Failover Server Properties**).

3. Click **Edit**.

4. Enter the **Failover Server IP or Hostname** and **Failover Server Port**.

5. Click **Save**.

4.5.5 Testing the LDAP failover server connection

To test the LDAP failover server connection:

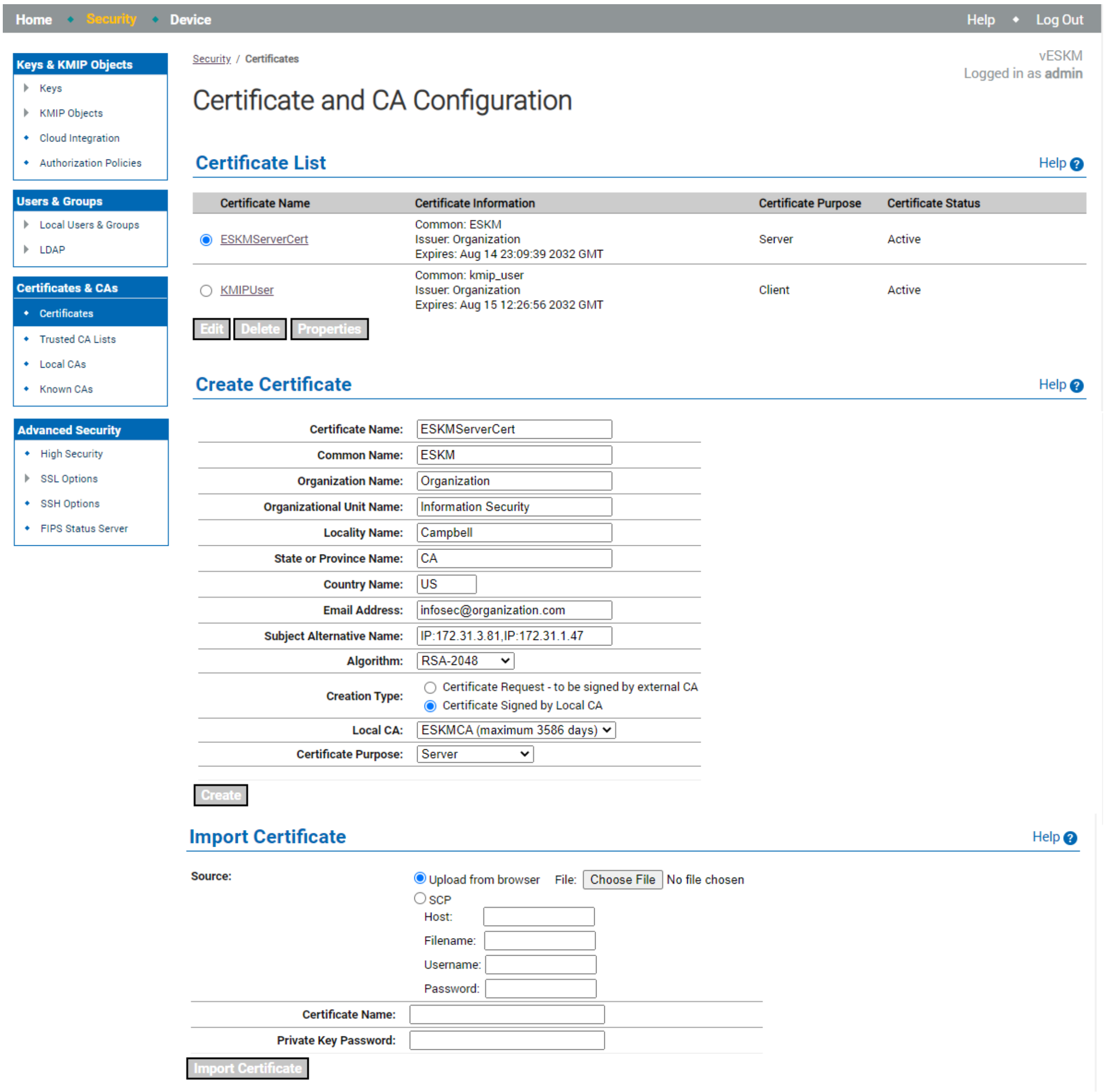
1. Log in to the Management Console as an administrator with Users, Groups, and LDAP access control.

2. Navigate to the LDAP Failover Server Properties section of the LDAP Server Configuration page (**Security** > **LDAP** > **LDAP Server** > **LDAP Failover Server Properties**).

3. Click **LDAP Test**.

4.6 Certificate procedures

This section describes the procedures you will follow to create, install, and download certificates.



Certificate and CA Configuration

Certificate List

	Certificate Name	Certificate Information	Certificate Purpose	Certificate Status
●	ESKMServerCert	Common: ESKM Issuer: Organization Expires: Aug 14 23:09:39 2032 GMT	Server	Active
○	KMIPUser	Common: kmip_user Issuer: Organization Expires: Aug 15 12:26:56 2032 GMT	Client	Active

Create Certificate

Certificate Name:	ESKMServerCert
Common Name:	ESKM
Organization Name:	Organization
Organizational Unit Name:	Information Security
Locality Name:	Campbell
State or Province Name:	CA
Country Name:	US
Email Address:	infosec@organization.com
Subject Alternative Name:	IP:172.31.3.81,IP:172.31.1.47
Algorithm:	RSA-2048
Creation Type:	○ Certificate Request - to be signed by external CA ● Certificate Signed by Local CA
Local CA:	ESKMCA (maximum 3586 days)
Certificate Purpose:	Server

Import Certificate

Source: ● Upload from browser File: No file chosen
○ SCP
Host:
Filename:
Username:
Password:

Certificate Name:
Private Key Password:

Figure 10 : Certificates

This section explains the following processes:

- Creating a certificate (p. 80)
- Creating a certificate request (p. 80)
- Creating a server certificate (p. 81)
- Creating a client certificate (p. 82)
- Creating a self-signed certificate (p. 83)

- Installing a certificate (p. 84)
- Installing a certificate chain (p. 85)
- Downloading a certificate (p. 86)

4.6.1 Creating a certificate

To create a certificate:

1. Log in to the Management Console as an administrator with Certificates access control.

2. Navigate to the Create Certificate section of the Certificate and CA Configuration page (**Security** > **Certificates**).

3. Enter the **Certificate Name**, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, **Subject Alternative Name**, and select an **Algorithm** for the certificate.

4. Select **Creation Typ**e as “Certificate Signed by Local CA”.

5. Select a **Local CA**.

6. Select a **Certificate Purpose**.

7. Click **Create**.

4.6.2 Creating a certificate request

1. Log in to the Management Console as an administrator with Certificates access control.

2. Navigate to the Create Certificate section of the Certificate and CA Configuration page (**Security** > **Certificates**).

3. Enter the **Certificate Name**, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, **Subject Alternative Name**, and select an **Algorithm** for the certificate.

4. Select **Creation Type** as "Certificate Request".

5. Click **Create**.

The new request appears in the Certificate List with the status **Request Pending**.

4.6.3 Creating a server certificate

Before the ESKM appliance can respond to SSL/TLS requests from a client application, it must be configured with at least one server certificate. If your ESKM appliance will be communicating with KMIP-enabled clients, Utimaco highly recommends that, in addition to the server certificate you create for the KMS server, you should also create a separate server certificate for the KMIP server.

> ⚠ To generate a valid certificate, you must have a certificate authority to sign the certificate request. You can create local CAs on the ESKM appliance, and use those CAs to sign the certificate requests. Otherwise, you will need to create a certificate request and use an external CA to sign the request.

The following steps assume that you have already created a local CA.

To create a server certificate for the ESKM appliance:

1. Log in to the Management Console as an administrator with Certificates access control.

2. Navigate to the Create Certificate section of the Certificate and CA Configuration page (**Security** > **Certificates**).

3. Enter the **Certificate Nam**e, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, **Subject Alternative Name**, and select an **Algorithm** for the certificate.

4. Select “Certificate Signed by Local CA” as **Creation Type**.

5. Select a **Local CA.**

6. Select “Server” as **Certificate Purpose**.

7. Click **Create**. The new certificate appears in the Certificate List.

8. Click **Save**.

The certificate appears as “Certificate Active” in the Certificate List. The certificate can now be used in to establish SSL/TLS connections with client applications.

4.6.4 Creating a client certificate

To create a client certificate for the ESKM appliance:

1. Log in to the Management Console as an administrator with Certificates access control.

2. Navigate to the Create Certificate section of the Certificate and CA Configuration page (**Security** > **Certificates**).

3. Enter the **Certificate Name**, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, **Subject Alternative Name**, and select an **Algorithm** for the certificate.

4. Select “Certificate Signed by Local CA” as **Creation Type**.

5. Select a **Local CA**.

6. Select “Client” as **Certificate Purpose**.

7. Click **Create**. The new certificate appears in the Certificate List.

8. Click **Save**.

The certificate appears as “Certificate Active” in the Certificate List. Refer to the client user guide for instructions on installing the client certificate.

4.6.5 Creating a self-signed certificate

The ESKM appliance allows you to test self-signed certificates. This allows you to avoid getting a certificate request signed by a local CA, or a CA on another ESKM appliance. Self-signed certificates can be presented to client applications just like any other certificate.

> ℹ A self-signed certificate should be used for testing purposes only. Any attempt to connect with an ESKM appliance using a test self-signed certificate sends a warning to the client browser.

To create a self-signed certificate:

1. Log in to the Management Console as an administrator with Certificates access control.

2. Navigate to the Create Certificate section of the Certificate and CA Configuration page (**Security** > **Certificates**).

3. Enter the **Certificate Name**, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, **Subject Alternative Name**, and select an **Algorithm** for the certificate.

4. Select “Certificate Request” as **Creation Type**.

5. Click **Create**. The certificate request will appear in the Certificate List section on the top of the page.

6. Select the certificate request, and then click **Properties** to access the Certificate Request Information section.

7. Click **Create Self Sign Certificate**.

8. Enter the duration for which the certificate will be valid in the **Certificate Duration** field.

9. Click **Create**. The ESKM appliance performs the following steps:
   a. The certificate request is copied into a new certificate request called `<certificate_name>-selfsign`.
   b. The ESKM appliance transforms `<certificate_name>-selfsign` into an active certificate by generating a self-signed certificate.
   c. The self-signed certificate is presented as an Active Certificate in the Certificate List.

⚠ The ESKM appliance keeps time based on the universal standard of GMT/UTC and provides for clock error up to one full day difference from the date of the certificate start.

4.6.6 Installing a certificate

Prior to installing a certificate, you must have a copy of the certificate response from the CA.
To install a certificate:

1. Log in to the Management Console as an administrator with Certificates access control.

2. Navigate to the Certificate List section of the Certificate and CA Configuration page (**Security** > **Certificates**).

3. Select the certificate request, and then click **Properties** to access the Certificate Request Information section.

4. Click **Install Certificate**.

5. Paste the certificate response from the CA into the **Certificate Response** field on the Certificate Installation page.

6. Click **Save**.

The ESKM appliance verifies the validity of the newly installed certificate. If determined to be valid, the certificate appears in the Certificate List with a status of "Certificate Active".

4.6.7 Installing a certificate chain

When the server certificates are signed with an intermediate CA, it might be necessary for an ESKM appliance to send multiple certificates to enable the client to verify the server certificate. Multiple certificates contained in one certificate are called a certificate chain. A client connecting to a forwarding rule that uses such a chain receives all certificates in the chain.

Certificate chains can be installed on the ESKM appliance from the Certificate Installation page.

To install a certificate chain:

1. Log in to the Management Console as an administrator with Certificates access control.

2. Navigate to the Certificate List section of the Certificate and CA Configuration page (**Security** > **Certificates**).

3. Select the certificate, and then click **Properties** to access the Certificate Information section.

4. Click **Install Certificate** to access the Certificate Installation page.

5. Append the intermediate CA certificate to the server certificate received from the CA. The combined certificates should be displayed in the **Certificate Response** field.

6. Click **Save**.

4.6.8 Downloading a certificate

To download a certificate:

1. Log in to the Management Console as an administrator with Certificates access control.

2. Navigate to the Certificate List section of the Certificate and CA Configuration page (**Security** > **Certificates**).

3. Select the **Certificate Name**, and then click **Properties** to access the Certificate Information section.

4. Click **Download**.

4.7 Certificate authority procedures

This section describes the procedures you will follow when creating and managing certificate authorities. The following processes are explained:

- Adding a CA certificate to the trusted CA list (p. 87)
- Removing a CA certificate from the trusted CA list (p. 87)
- Creating a new trusted CA list profile (p. 88)
- Deleting a trusted CA list profile (p. 89)
- Signing certificate requests with a local CA (p. 89)
- Viewing the certificates signed by a local CA (p. 90)
- Downloading a local CA (p. 90)

- Creating a local CA (p. 91)
- Deleting a local CA (p. 91)
- Creating a self-signed root CA (p. 92)
- Creating an intermediate CA request (p. 92)
- Installing a CA certificate (p. 94)
- Removing a CA certificate (p. 94)

4.7.1 Adding a CA certificate to the trusted CA list

To add a CA certificate to the trusted CA list:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Trusted Certificate Authority List Profiles section of the Certificate and CA Configuration page (**Security** > **Trusted CA Lists**).

3. Select a profile, and then click **Properties** to access the Trusted Certificate Authority List section.

4. Click **Edit**.

5. Click the **Add** button to move available CAs to the Trusted CA list.

6. Click **Save**.

4.7.2 Removing a CA certificate from the trusted CA list

To remove a CA certificate to the trusted CA list:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Trusted Certificate Authority List Profiles section of the Certificate and CA Configuration page (**Security** > **Trusted CA Lists**).

3. Select a profile, and then click **Properties** to access the Trusted Certificate Authority List section.

4. Click **Edit**.

5. Click the **Remove** button to move CAs from the Trusted CA list.

6. Click **Save**.

4.7.3 Creating a new trusted CA list profile

To create a new trusted CA list profile:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Trusted Certificate Authority List Profiles section of the Certificate and CA Configuration page (**Security** > **Trusted CA Lists**).

3. Click **Add**.

4. Enter a new Profile Name.

5. Click **Save**. This creates a new entry on the list of profile.

6. Select the profile, and then click **Properties** to access the Trusted Certificate Authority List section.

7. Click **Edit**.

8. Click the **Add** button to move available CAs to the Trusted CA list.

9. Click **Save**.

4.7.4 Deleting a trusted CA list profile

To delete a trusted certificate authority list profile:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Trusted Certificate Authority List Profiles section of the Certificate and CA Configuration page (**Security** > **Trusted CA Lists**).

3. Select a profile, and then click **Delete**.

> ⚠ You cannot delete a trusted CA list profile if it used by the Web Administration, KMS or KMIP service. In addition, you cannot delete the default profile.

4.7.5 Signing certificate requests with a local CA

To sign certificate requests with a local CA:

1. Generate a certificate request on the machine where the client application resides. If you are signing a certificate for another ESKM appliance, then generate the certificate request on that appliance. If you are signing a certificate for a client application, the documentation that accompanies the client application should explain how to create a new certificate request.

2. Navigate to the Local Certificate Authority List section of the Certificate and CA Configuration page (**Security** > **Local CAs**).

3. Select the CA, and then click **Sign Request**.

4. Set Certificate Purpose to **Server** if this certificate is used by an ESKM appliance, or set the purpose to **Client** if this certificate is used by a client application. If the certificate

will be used for both server and client authentication, set the Certificate Purpose to **Server and Client**.

5. Paste the certificate request generated by the client application into the certificate request field.

6. Click **Sign Request**.
   The newly signed certificate is displayed.

7. Install the certificate on the client application or the ESKM appliance.
   The certificate can now be used to establish SSL/TLS sessions.

⚠ The maximum duration for a certificate signed by a local CA is determined by the value of the **Maximum User Certificate Duration** field for that CA.

4.7.6 Viewing the certificates signed by a local CA

To view all of the certificates signed by a local CA:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Local Certificate Authority List section of the Certificate and CA Configuration page (**Security** > **Local CAs**).

3. Select a certificate authority, and then click **Show Signed Certs** to access the Signed Certificates section.

Alternatively, you can access the Signed Certificates section by clicking the **Show Signed Certs** button on the CA Certificate Information section.

4.7.7 Downloading a local CA

To download a local CA:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Local Certificate Authority List section of the Certificate and CA Configuration page (**Security** > **Local CAs**).

3. Select a certificate authority, and then click **Download** to download the CA to your local workstation.

Alternatively, you can download the certificate authority by using the **Download** button on the CA Certificate Information section.

4.7.8 Deleting a local CA

To delete a local CA:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Local Certificate Authority List section of the Certificate and CA Configuration page (**Security** > **Local CAs**).

3. Select a certificate authority.

4. Click **Delete**.

4.7.9 Creating a local CA

To create a local certificate authority:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Create Local Certificate Authority section of the Certificate and CA Configuration page (**Security** > **Local CAs**).

3. Enter the **Certificate Authority Name**, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, and select an **Algorithm**.

4. Select either Self-signed Root CA or Intermediate CA Request as the **Certificate Authority Type**.

5. Click **Create**.

4.7.10 Creating a self-signed root CA

To create a self-signed root CA:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Create Local Certificate Authority section of the Certificate and CA Configuration page (**Security** > **Local CAs**).

3. Enter the **Certificate Authority Name**, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, and select an **Algorithm**.

4. Select Self-signed Root CA as the **Certificate Authority Type**.

5. Click **Create**.

4.7.11 Creating an intermediate CA request

To create an intermediate CA request:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.

2. Navigate to the Create Local Certificate Authority section of the Certificate and CA Configuration page (Security > Local CAs).

3. Enter the Certificate Authority Name, Common Name, Organization Name, Organizational Unit Name, Locality Name, State or Province Name, Country Name, Email Address, and select an Algorithm.

4. Select Intermediate CA Request as the Certificate Authority Type.

5. Click Create. The new request appears in the Local Certificate Authority List section with the status CA Certificate Request Pending.

6. Go to the Local Certificate Authority List section of the Certificate and CA Configuration page (Security > Local CAs).

7. Select the CA Certificate Request, and then click Properties to access the CA Certificate Information section.

8. Copy the CA certificate request text*.

9. Sign this request with another CA. Copy the signed certificate text.

10. Go back to the Local Certificate Authority List section.

11. Select the CA Certificate Request, and then click Properties to access the CA Certificate Information section.

12. Click Install Certificate.

13. Paste the text of the signed CA certificate into the Certificate Response field.

14. Click Save.

The CA certificate appears in the Local Certificate Authority List with a status of “Certificate Active”.

*Be sure to include the first and last lines (-----BEGIN CERTIFICATE REQUEST... and ...END CERTIFICATE REQUEST-----)

4.7.12 Installing a CA certificate

Prior to installing a CA certificate, you must have a copy of the CA certificate on your local workstation.

To install a CA certificate:

1. Log in to the Management Console as an administrator with Certificate Authorities access control.
2. Navigate to the Install CA Certificate section of the Certificate and CA Configuration page (**Security** > **Known CAs**).
3. Enter a value for the **Certificate Name** and paste the CA certificate text in the **Certificate** field.
4. Click **Install**. The CA will be added to the CA Certificate list.

4.7.13 Removing a CA certificate

To remove a CA certificate:

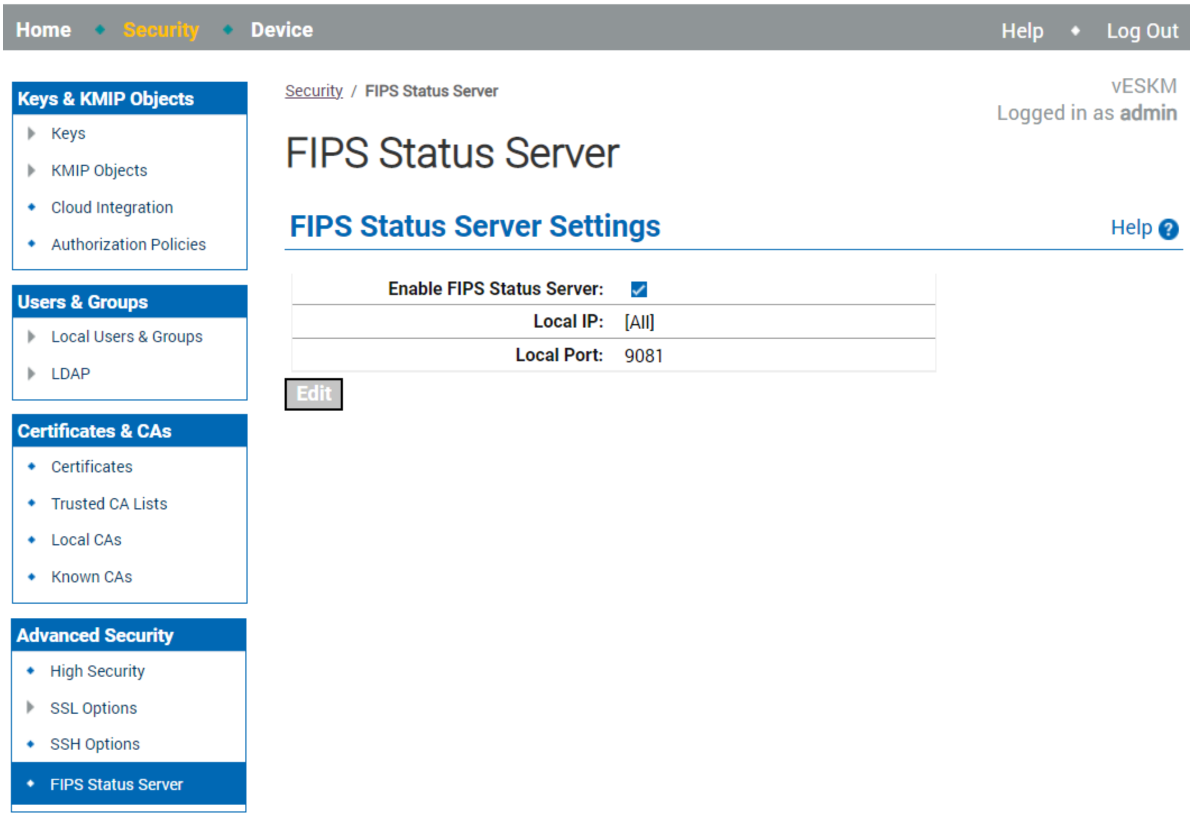
1. Log in to the Management Console as an administrator with Certificate Authorities access control.
2. Navigate to the CA Certificate List section of the Certificate and CA Configuration page (**Security** > **Known CAs**).

3. Select a CA certificate.

4. Click **Delete**.

4.8 FIPS status server procedures

This section describes the procedures you will follow when managing the ESKM FIPS Status Server.



Enable FIPS Status Server:	☑
Local IP:	[All]
Local Port:	9081

Figure 11 : FIPS Status Server settings

This section the following processes:

- Enabling the FIPS status server (p. 96)
- Viewing the FIPS status report (p. 96)

4.8.1 Enabling the FIPS status server

> ⚠ View the Security Protocols enabled on your Internet Browser. You must enable TLS to access the Management Console when the ESKM appliance is operating in FIPS-compliant mode.

To enable the FIPS Status Server:

1. Log in to the Management Console as an administrator with SSL/TLS, Advanced Security, and KMS Server access controls.

2. Go to the FIPS Status Server page (**Security** > **FIPS Status Server**).

3. Click **Edit**.

4. Select **Enable FIPS Status Server**.

5. Select the **Local IP** address from the list or select **[All]**.

6. Enter the Local Port of the FIPS Status Server on which the appliance "listens", or accept the default port value of 9081.

7. Click **Save**.

4.8.2 Viewing the FIPS status report

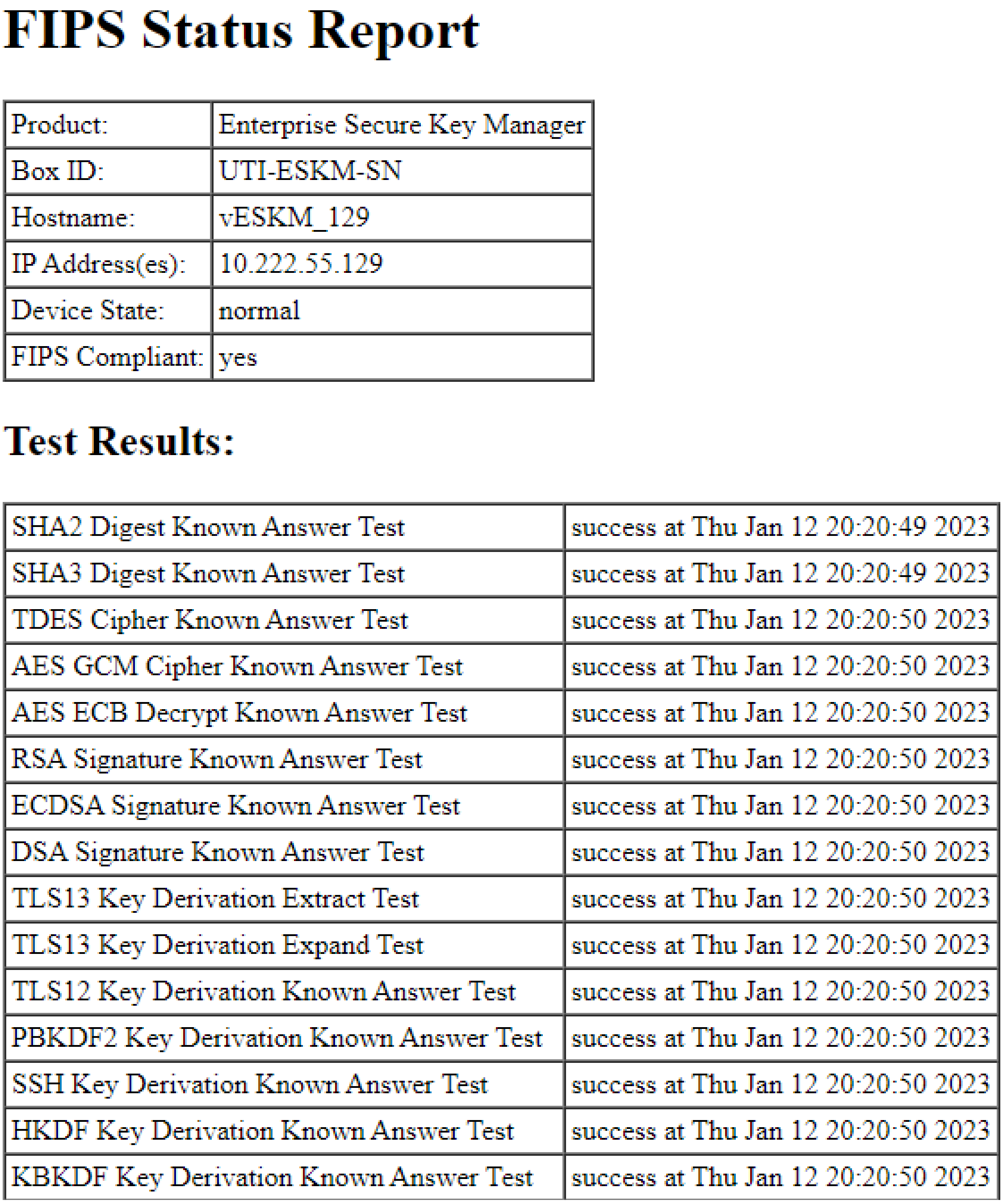
To view the FIPS Status Report:

1. Locate the IP and port of the status report by either using the Management Console or the CLI.
   By default, the location is **<ESKM IP>:9081/status.html**.
    a. Using the Management Console: Log in to the Management Console and navigate to the FIPS Status Server page (**Security > Advanced Security > FIPS Status Server**).

b. Using the CLI: Log in to the CLI and enter the command <show fips server (p. 650)>.

2. View the FIPS Status Report through a web browser: Go to the IP and port using http; for example, http://192.168.12.20:9081/status.html.

The following report appears.

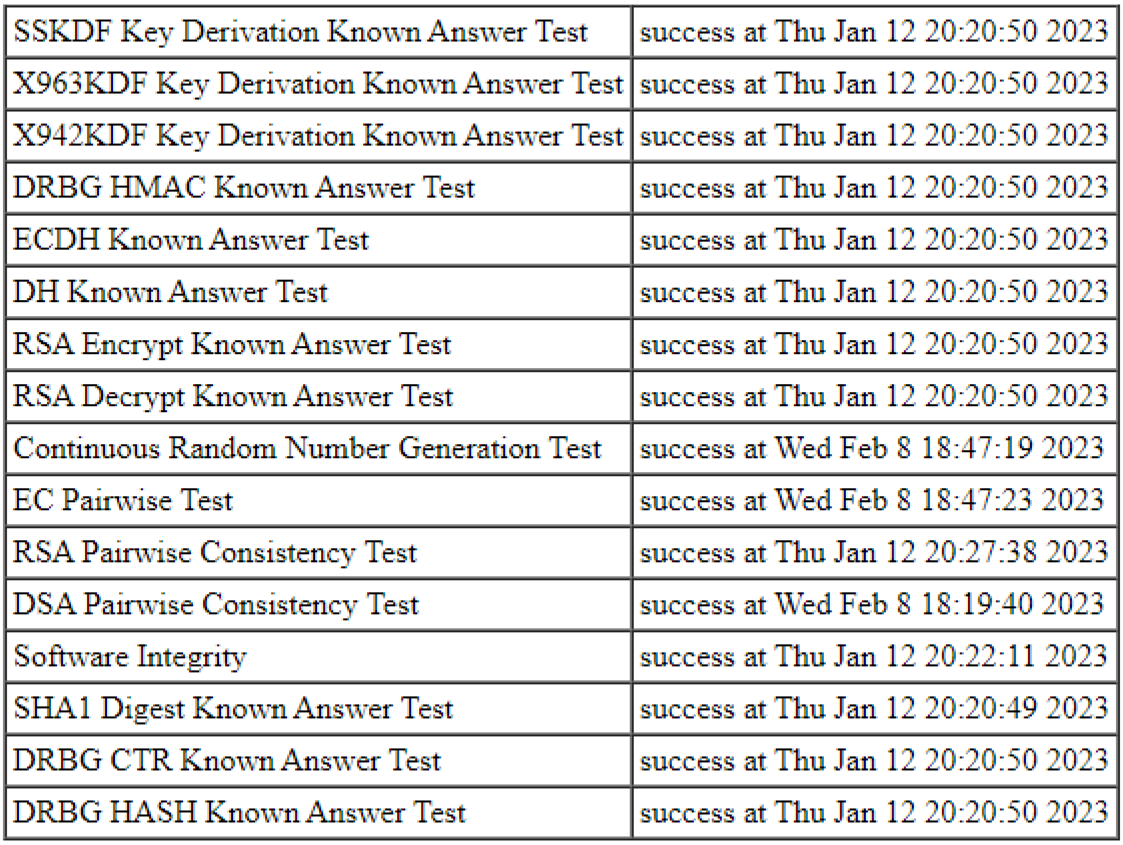


FIPS Status Report

Product:	Enterprise Secure Key Manager
Box ID:	UTI-ESKM-SN
Hostname:	vESKM_129
IP Address(es):	10.222.55.129
Device State:	normal
FIPS Compliant:	yes

Test Results:

SHA2 Digest Known Answer Test	success at Thu Jan 12 20:20:49 2023
SHA3 Digest Known Answer Test	success at Thu Jan 12 20:20:49 2023
TDES Cipher Known Answer Test	success at Thu Jan 12 20:20:50 2023
AES GCM Cipher Known Answer Test	success at Thu Jan 12 20:20:50 2023
AES ECB Decrypt Known Answer Test	success at Thu Jan 12 20:20:50 2023
RSA Signature Known Answer Test	success at Thu Jan 12 20:20:50 2023
ECDSA Signature Known Answer Test	success at Thu Jan 12 20:20:50 2023
DSA Signature Known Answer Test	success at Thu Jan 12 20:20:50 2023
TLS13 Key Derivation Extract Test	success at Thu Jan 12 20:20:50 2023
TLS13 Key Derivation Expand Test	success at Thu Jan 12 20:20:50 2023
TLS12 Key Derivation Known Answer Test	success at Thu Jan 12 20:20:50 2023
PBKDF2 Key Derivation Known Answer Test	success at Thu Jan 12 20:20:50 2023
SSH Key Derivation Known Answer Test	success at Thu Jan 12 20:20:50 2023
HKDF Key Derivation Known Answer Test	success at Thu Jan 12 20:20:50 2023
KBKDF Key Derivation Known Answer Test	success at Thu Jan 12 20:20:50 2023

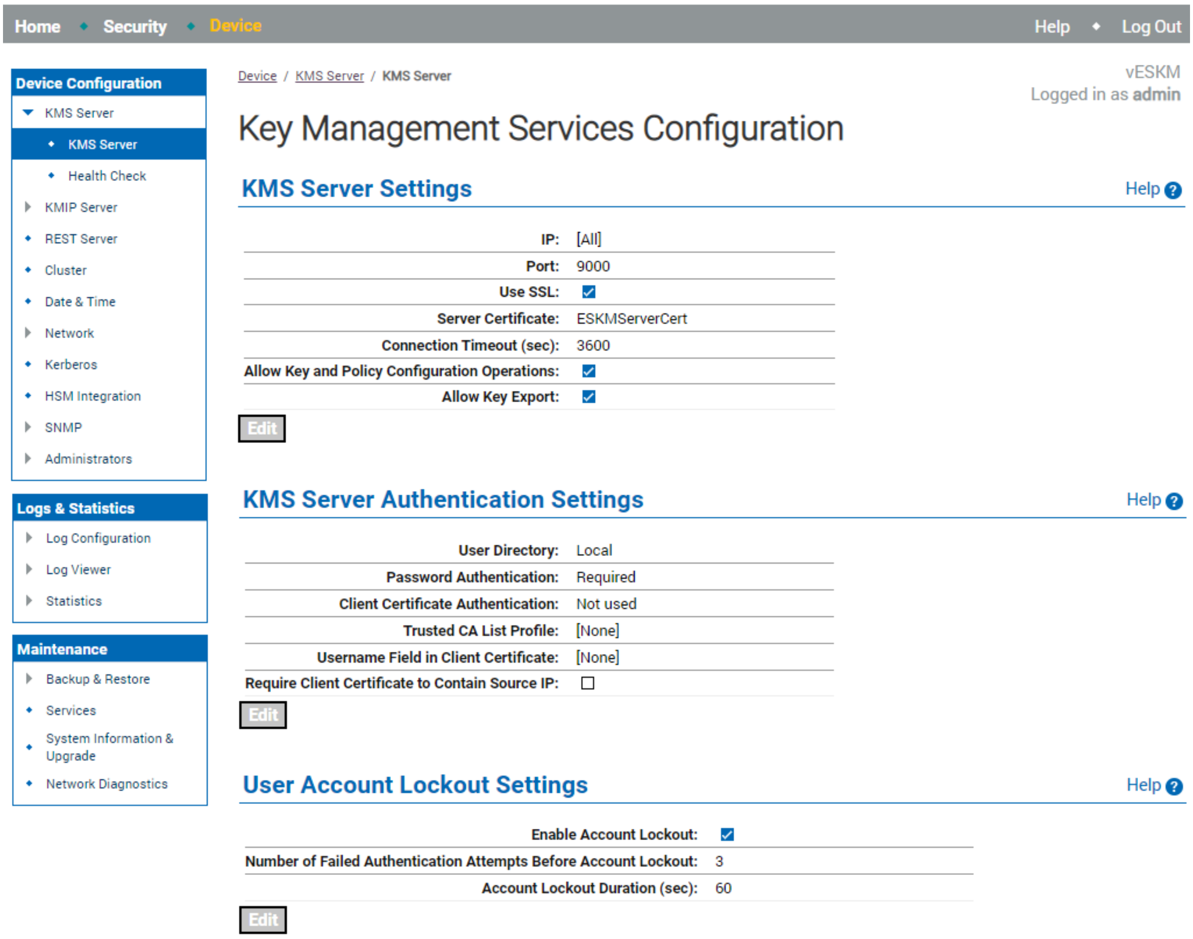


SSKDF Key Derivation Known Answer Test	success at Thu Jan 12 20:20:50 2023
X963KDF Key Derivation Known Answer Test	success at Thu Jan 12 20:20:50 2023
X942KDF Key Derivation Known Answer Test	success at Thu Jan 12 20:20:50 2023
DRBG HMAC Known Answer Test	success at Thu Jan 12 20:20:50 2023
ECDH Known Answer Test	success at Thu Jan 12 20:20:50 2023
DH Known Answer Test	success at Thu Jan 12 20:20:50 2023
RSA Encrypt Known Answer Test	success at Thu Jan 12 20:20:50 2023
RSA Decrypt Known Answer Test	success at Thu Jan 12 20:20:50 2023
Continuous Random Number Generation Test	success at Wed Feb 8 18:47:19 2023
EC Pairwise Test	success at Wed Feb 8 18:47:23 2023
RSA Pairwise Consistency Test	success at Thu Jan 12 20:27:38 2023
DSA Pairwise Consistency Test	success at Wed Feb 8 18:19:40 2023
Software Integrity	success at Thu Jan 12 20:22:11 2023
SHA1 Digest Known Answer Test	success at Thu Jan 12 20:20:49 2023
DRBG CTR Known Answer Test	success at Thu Jan 12 20:20:50 2023
DRBG HASH Known Answer Test	success at Thu Jan 12 20:20:50 2023

Figure 12 : FIPS Status Report

4.9 KMS server procedures

The KMS server is the component of the ESKM appliance that manages communications between the appliance and the client(s). This section describes the procedures you will follow when managing the KMS server.



Key Management Services Configuration

KMS Server Settings

IP:	[All]
Port:	9000
Use SSL:	☑
Server Certificate:	ESKMServerCert
Connection Timeout (sec):	3600
Allow Key and Policy Configuration Operations:	☑
Allow Key Export:	☑

KMS Server Authentication Settings

User Directory:	Local
Password Authentication:	Required
Client Certificate Authentication:	Not used
Trusted CA List Profile:	[None]
Username Field in Client Certificate:	[None]
Require Client Certificate to Contain Source IP:	□

User Account Lockout Settings

Enable Account Lockout:	☑
Number of Failed Authentication Attempts Before Account Lockout:	3
Account Lockout Duration (sec):	60

Figure 13 : KMS Configuration

This section explains the following processes:

- Configuring the IP address and port number (p. 100)
- Enabling SSL (p. 100)
- Configuring the connection timeout (p. 101)
- Enabling key and policy configuration by client applications (p. 101)
- Enabling the LDAP server (p. 102)
- Enabling password authentication (p. 103)
- Enabling client certificate authentication (p. 103)
- Configuring the user account lockout settings (p. 104)

4.9.1 Configuring the IP address and port number

Specify the IP address and port number for the KMS Server on the ESKM appliance.

To specify the IP address and port number:

1. Log in to the Management Console as an administrator with KMS Server access control.
2. Navigate to the KMS Server Settings section of the Key Management Services Configuration page (**Device** > **KMS Server** > **KMS Server Settings**).
3. Click **Edit**.
4. Select **IP**, and then select either [All] or one or more IP addresses.
5. Input the port number in the **Port:** field.
6. Click **Save**.

4.9.2 Enabling SSL

Prior to enabling SSL, you must have a server certificate available for use by the KMS Server.

To enable SSL:

1. Log in to the Management Console as an administrator with KMS Server access control.
2. Navigate to the KMS Server Settings section of the Key Management Services Configuration page (**Device** > **KMS Server** > **KMS Server Settings**).
3. Click **Edit**.
4. Select **Use SSL**

5. Select a certificate in the **Server Certificate** field.

6. Click **Save**.

See SSL options (p. 389) for more information on configuring SSL and TLS.

4.9.3 Configuring the connection timeout

The connection timeout value (in seconds) specifies how long client connections can remain idle before the KMS Server begins closing them. The default value is 3600; the maximum value is 7200 (2 hours). Specifying a value of 0 means that the KMS Server will not close client connections due to inactivity.

To configure the connection timeout:

1. Log in to the Management Console as an administrator with KMS Server access control.

2. Navigate to the KMS Server Settings section of the Key Management Services Configuration page (**Device** > **KMS Server** > **KMS Server Settings**).

3. Click **Edit**.

4. Input a value in the **Connection Timeout**: field.

5. Click **Save**.

4.9.4 Enabling key and policy configuration by client applications

Enabling key and policy configuration by client applications permits the following actions:

- create and delete key
- import key
- create, delete and modify operations of users and groups

To enable key and policy configuration by client applications:

1. Log in to the Management Console as an administrator with KMS Server access control.
2. Navigate to the KMS Server Settings section of the KMS Configuration page (**Device** > **KMS Server** > **KMS Server Settings**).
3. Click **Edit**.
4. Select **Allow Key and Policy Configuration Operations**.
5. Click **Save**.

⚠ If SSL/TLS is not enabled, enabling Allow Key and Policy Configuration Operations takes the ESKM appliance out of FIPS compliance.

4.9.5 Enabling the LDAP server

To enable the LDAP server:

1. Log in to the Management Console as an administrator with KMS Server access control.
2. Navigate to the KMS Server Authentication Settings section of the KMS Server Configuration page (**Device** > **KMS Server** > **KMS Server Authentication Settings**).
3. Click **Edit**.
4. Select **LDAP** in the **User Directory** field.
5. Click **Save**.

⚠ Enabling the LDAP server takes the ESKM appliance out of FIPS compliance.

4.9.6 Enabling password authentication

To enable password authentication:

1. Log in to the Management Console as an administrator with KMS Server access control.

2. Navigate to the KMS Server Authentication Settings section of the KMS Server Configuration page (**Device** > **KMS Server** > **KMS Server Authentication Settings**).

3. Click **Edit**.

4. Select **Required** in the **Password Authentication** field.

5. Click **Save**.

4.9.7 Enabling client certificate authentication

To enable client certificate authentication:

1. Log in to the Management Console as an administrator with KMS Server access control.

2. Navigate to the KMS Server Authentication Settings section of the KMS Server Configuration page (**Device** > **KMS Server** > **KMS Server Authentication Settings**).

3. Click **Edit**.

4. Select either **Used for SSL Session only** or **Used for SSL session and username** in the **Client Certificate Authentication** field.

5. Select a profile list in the **Trusted CA List Profile** field. The ESKM appliance uses this profile when verifying that the client certificate is signed by a CA trusted by the ESKM appliance.

6. Use the **Username Field in Client Certificate** field to specify which field in the client certificate must contain a valid username. This setting is optional.
7. Select **Require Client Certificate to Contain Source IP** to specify that the client certificate must contain the client's IP address in the `subjectAltName` field. This setting is optional.
8. Click **Save**.

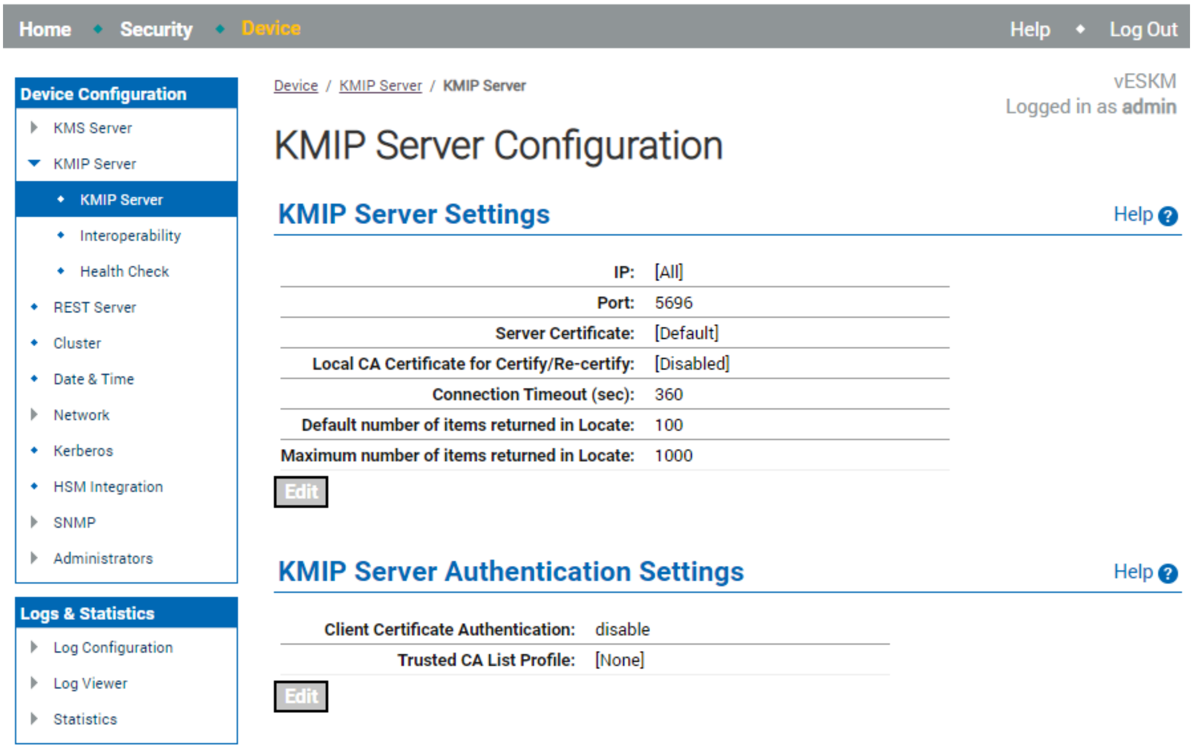
4.9.8 Configuring the user account lockout settings

To configure the user account lockout settings:

1. Log in to the Management Console as an administrator with KMS Server access control.
2. Navigate to the User Account Lockout Settings section of the KMS Server Configuration page (**Device** > **KMS Server** > **User Account Lockout Settings**).
3. Click **Edit**.
4. Select **Enable Account Lockout** to prevent a user from logging in to the server for a given duration after a specified number of failed login attempts.
5. Enter a value in the **Number of Failed Authentication Attempts Before Account Lockout** field.
6. Enter a value in the **Account Lockout Duration** field. This is the period of time during which the account is not available during lockout.
7. Click **Save**.

4.10 KMIP server procedures

The KMIP server is the component of the ESKM appliance that manages communications between the appliance and the KMIP-enabled clients.



KMIP Server Configuration

KMIP Server Settings

IP:	[All]
Port:	5696
Server Certificate:	[Default]
Local CA Certificate for Certify/Re-certify:	[Disabled]
Connection Timeout (sec):	360
Default number of items returned in Locate:	100
Maximum number of items returned in Locate:	1000

KMIP Server Authentication Settings

Client Certificate Authentication:	disable
Trusted CA List Profile:	[None]

Figure 14 : KMIP Server Configuration

This section describes the procedures you will follow when managing the KMIP server. The following processes are explained:

- Configuring the IP address and port number (p. 106)
- Configuring TLS (p. 106)
- Configuring a Local CA for KMIP certify and re-certify operations (p. 107)
- Configuring the default number of items returned in locate (p. 107)
- Configuring the maximum number of items returned in locate (p. 108)
- Configuring KMIP client certificate authentication (p. 108)
- Configuring KMIP server certificate (p. 109)

⚠ Changing the KMIP server configuration causes the KMIP server service to restart.

4.10.1 Configuring the IP address and port number

Specify the IP address and port number for the KMIP Server on the ESKM.

To specify the IP address and port number:

1. Log in to the Management Console as an administrator with KMIP Server access control.
2. Navigate to the KMIP Server Settings section of the KMIP Server Configuration page (**Device** > **KMIP Server** > **KMIP Server Settings**).
3. Click **Edit**.
4. Select **IP**, and then select either [All] or one or more IP addresses.
5. Input the port number in the **Port:** field.
6. Click **Save**.

4.10.2 Configuring TLS

KMIP requires TLS. You must have a server certificate available for use by the KMIP Server, see Creating a server certificate (p. 81).

To configure TLS:

1. Log in to the Management Console as an administrator with KMIP Server access control.
2. Navigate to the KMIP Server Settings section of the KMIP Server Configuration page (**Device** > **KMIP Server** > **KMIP Server Settings**).

3. Click **Edit**.
4. Select a certificate in the **Server Certificate** field.
5. Click **Save**.

4.10.3 Configuring a Local CA for KMIP certify and re-certify operations

The KMIP certify and re-certify operations require a Local CA to sign a certificate request. To create a local CA, see Creating a local CA (p. 91).

To specify the name of the Local CA that the KMIP server will use to sign certificate requests:

1. Log in to the Management Console as an administrator with KMIP Server access control.
2. Go to the KMIP Server Settings section of the KMIP Server Configuration page (**Device** > **KMIP Server** > **KMIP Server Settings**).
3. Click **Edit**.
4. Select a Local CA in the **Local CA Certificate for Certify/Re-certify** field.
5. Click **Save**.

4.10.4 Configuring the default number of items returned in locate

This value specifies the default number of items returned in a KMIP client Locate request operation, if a value is not specified by the client. The default value is 100.

To configure the default number of items returned:

1. Log in to the Management Console as an administrator with KMIP Server access control.

2. Navigate to the KMIP Server Settings section of the KMIP Server Configuration page (**Device** > **KMIP Server** > **KMIP Server Settings**).

3. Click **Edit**.

4. Input a value in the **Default number of items returned in Locate** field. The minimum value is 10, the maximum value is 1000.

5. Click **Save**.

4.10.5 Configuring the maximum number of items returned in locate

This value specifies the maximum number of items returned in a KMIP client Locate request operation. Even if a value is specified by the client in the KMIP Locate operation request, the number of items returned will not exceed this value. The default value is 1,000.

To configure the maximum number of items returned:

1. Log in to the Management Console as an administrator with KMIP Server access control.

2. Navigate to the KMIP Server Settings section of the KMIP Server Configuration page (**Device** > **KMIP Server** > **KMIP Server Settings**).

3. Click **Edit**.

4. Input a value in the **Maximum number of items returned in Locate** field.

5. Click **Save**.

4.10.6 Configuring KMIP client certificate authentication

To enable client certificate authentication:

1. Log in to the Management Console as an administrator with KMIP Server access control.

2. Navigate to the KMIP Server Authentication Settings section of the KMIP Server Configuration page (**Device** > **KMIP Server** > **KMIP Server Authentication Settings**).

3. Click **Edit**.

4. Select **Enable** in the **Client Certificate Authentication** field.

5. Select a profile list in the Trusted **CA List Profile** field. The ESKM appliance uses this profile when verifying that the client certificate is signed by a CA trusted by the ESKM appliance.

6. Click **Save**.

4.10.7 Configuring KMIP server certificate

To select a configured server certificate:

1. Log in to the Management Console as an administrator with KMIP Server access control.

2. Navigate to the KMIP Server Settings section of the KMIP Server Configuration page (**Device** > **KMIP Server** > **KMIP Server Settings**).

3. Click **Edit**.

4. Select a configured server certificate in the **Server Certificate** field. The configured server certificate is selected from the list to replace the default server certificate.

5. Click **Save**.

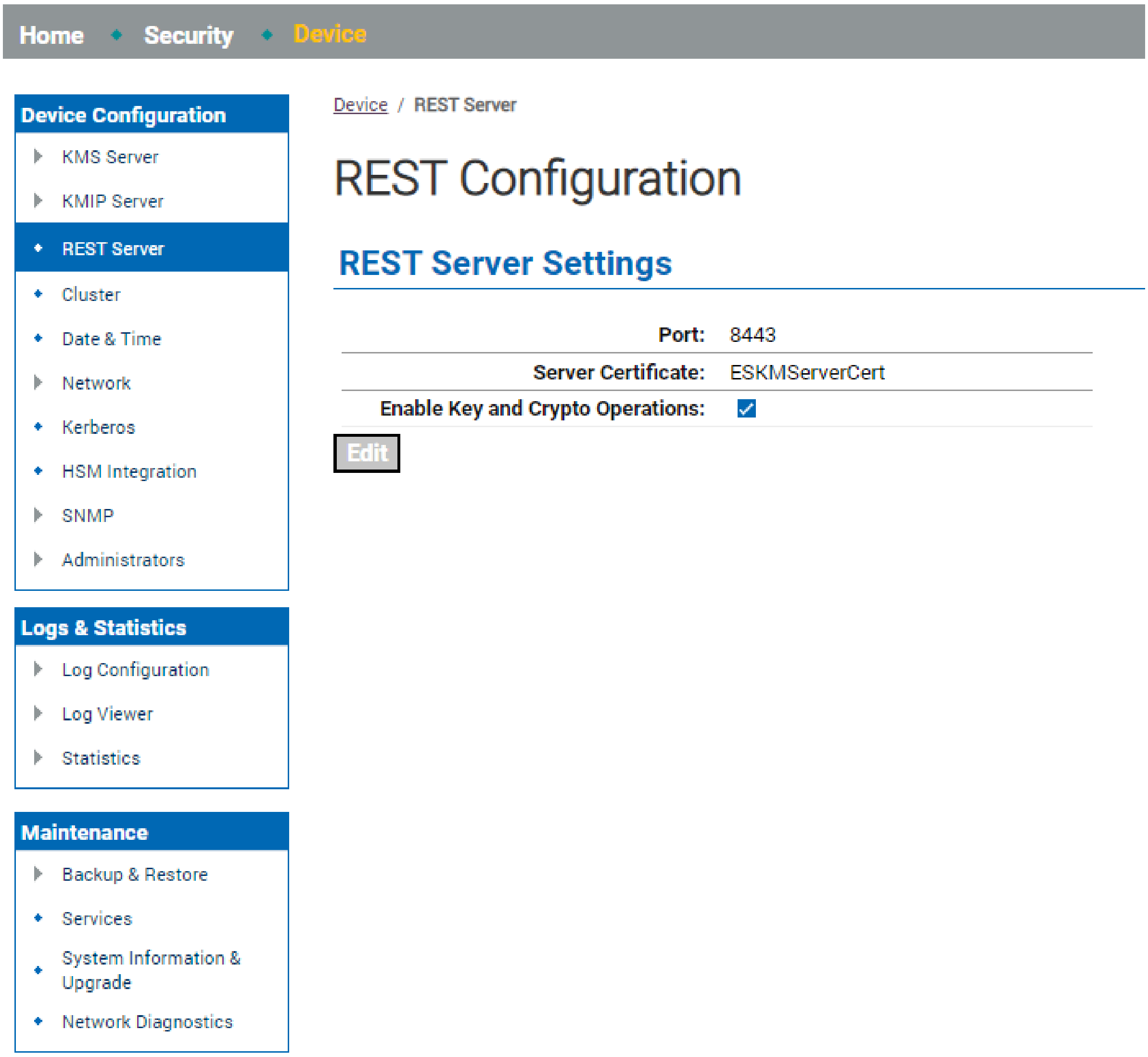
⚠ KMIP requires mutual authentication. After configuring the KMIP server, enable KMIP client certificate authentication. The KMIP client certificate authentication status is disabled by default.

4.11 REST server procedures

Clients can communicate with the ESKM appliance using REST APIs. REST commands can be used for cryptographic key management. Refer *ESKM RESTful API Reference* for information on the various ESKM REST methods.

⚠ Keys created via REST interface can also be accessed using KMS.

The REST server of the ESKM appliance manages communication (using REST APIs) between the appliance and the client.



Port:	8443
Server Certificate:	ESKMServerCert
Enable Key and Crypto Operations:	☑

Figure 15 : Rest Server Settings

> To modify the REST Server Settings, REST Server Access Control should be enabled for the administrator.

This section explains the following processes:

- Configuring the Port number (p. 112)
- Configuring REST Server Certificate (p. 112)
- Enabling Key and Crypto Operations (p. 113)

❗ Changing the configuration restarts the REST service which may take a while. Key operations will not be available while the service restarts. The configuration also applies to the HSM Configuration UI.

HSM Web Console

The REST configuration also applies to the HSM Configuration UI. The **Port** and the **Server Certificate** changes in the **REST Server Settings** section are reflected in the HSM web console as well (refer Using the HSM Web Console (p. 764)). Changing the **REST Configuration** may cause the HSM to be unavailable for a few seconds.

4.11.1 Configuring the Port number

Specify the port number for the REST Server on the ESKM appliance.

To specify the port number:

1. Log in to the Management Console as an administrator with REST Server access control.
2. Navigate to the **REST Server Settings** section of the REST Configuration page (**Device** > **Rest Server**).
3. Click **Edit**.
4. Enter the port number in the **Port** field, (the default port number is 8443).
5. Click **Save**.

4.11.2 Configuring REST Server Certificate

By default, the REST Server uses the system-generated server certificate. The default server certificate can be replaced from the REST Server Settings section. A server certificate must be available for use by the REST Server, see Creating a server certificate (p. 81).

To configure REST Server Certificate:

1. Log in to the Management Console as an administrator with REST Server access control.

2. Navigate to the **REST Server Settings** section of the REST Configuration page (**Device** > **Rest Server**).

3. Click **Edit**.

4. Select a server certificate from the **Server Certificate** drop-down list. The selected certificate will replace the default server certificate.

5. Click **Save**.

Utimaco strongly recommends replacing the default system-generated server certificate.

After configuring the Server Certificate, the user will not be able to change the certificate back to the system-generated default server certificate.

4.11.3 Enabling Key and Crypto Operations

Enabling key and crypto operations in the **REST Server Settings** section allows the client applications to do cryptographic key management using REST commands.

To enable key operations

1. Log in to the Management Console as an administrator with REST Server access control.

2. Navigate to the **REST Server Settings** section of the REST Configuration page (**Device** > **Rest Server**).

3. Click **Edit**.

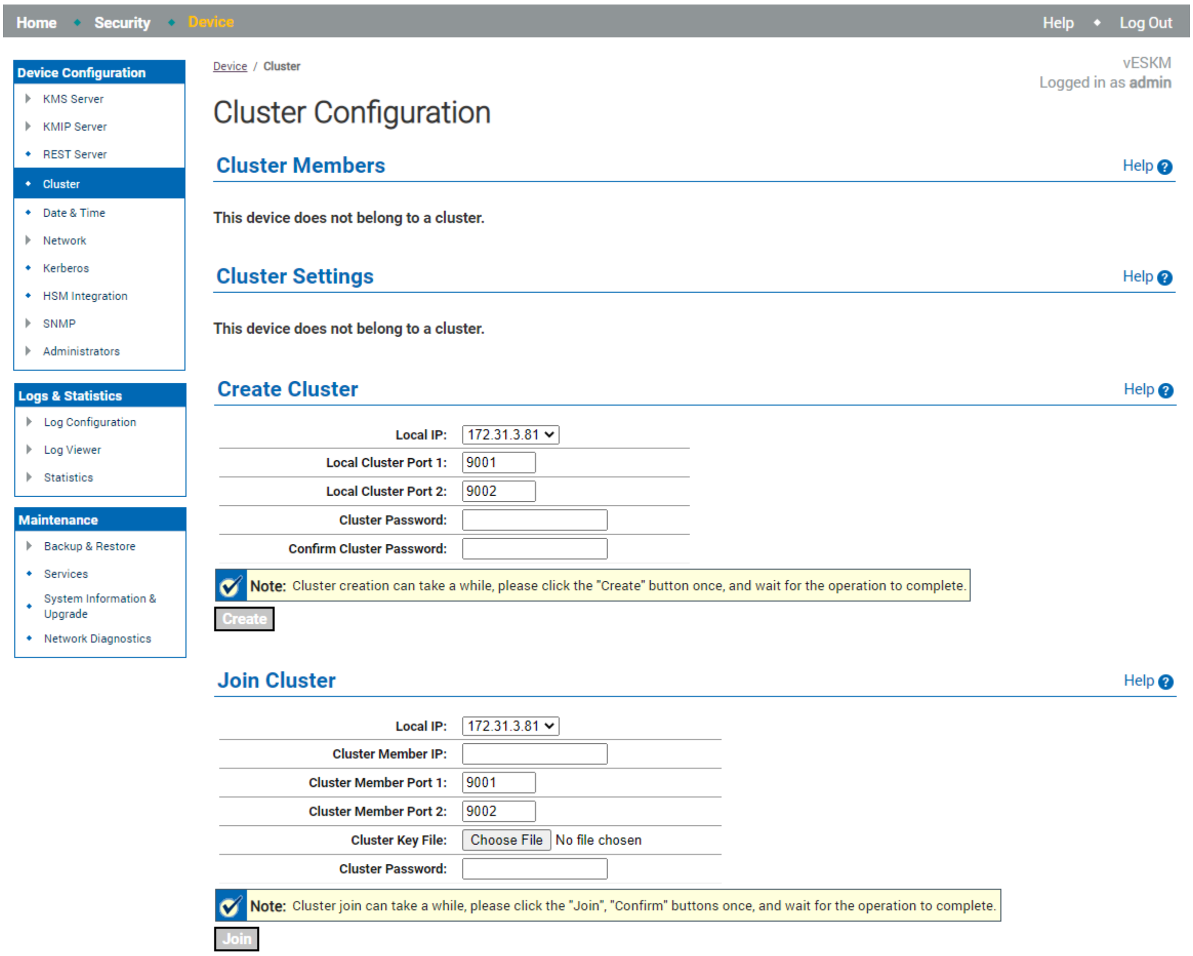
4. Select **Enable Key and Crypto Operations**.

5. Click **Save**.

Changing the configuration restarts the REST service which may take a while. Key and Crypto operations will not be available while the service restarts. Also, this configuration applies to the HSM Configuration UI.

4.12 Clustering procedures

This section describes the procedures you will follow when creating and managing clusters.



Cluster Configuration

Cluster Members

This device does not belong to a cluster.

Cluster Settings

This device does not belong to a cluster.

Create Cluster

Local IP:	172.31.3.81
Local Cluster Port 1:	9001
Local Cluster Port 2:	9002
Cluster Password:	
Confirm Cluster Password:	

Note: Cluster creation can take a while, please click the "Create" button once, and wait for the operation to complete.

Join Cluster

Local IP:	172.31.3.81
Cluster Member IP:	
Cluster Member Port 1:	9001
Cluster Member Port 2:	9002
Cluster Key File:	Choose File No file chosen
Cluster Password:	

Note: Cluster join can take a while, please click the "Join", "Confirm" buttons once, and wait for the operation to complete.

Figure 16 : Cluster Configuration

This section explains the following processes:

A cluster enables multiple ESKM appliances to share configuration settings. Any changes made to these values on one cluster member are replicated to all members within the same cluster. This enables you to immediately share configuration changes with other ESKM appliances.
If you only have one ESKM appliance, skip this section.

> ❗ Utimaco recommends that ESKM appliances be configured in a cluster, for high availability and for disaster recovery scenarios. If an unclustered appliance fails, all data from the last backup to the point of failure is lost.
>
> Utimaco strongly recommends performing frequent backups.

4.12.1 Creating a cluster

You create a cluster on one ESKM appliance and then join other ESKM appliance members to that cluster.

To create a cluster:

1. Select an ESKM appliance to be the first cluster member. This appliance cannot currently be a member of a cluster.
2. Log in to the Management Console as an administrator with Cluster access control.

3. Go to the Create Cluster section on the Cluster Configuration page (**Device** > **Cluster**).

4. Enter the **Local IP**, **Local Cluster Port 1**, **Local Cluster Port 2**, and **Cluster Password**.

5. Click **Create**.

4.12.2 Joining a cluster

Before joining a cluster, make sure that the ESKM appliance does not already belong to another cluster.

> ⚠ All ESKM appliances in a cluster must be running the same major version of software.
>
> For example, it is not possible to cluster ESKM appliances with ESKM v4, ESKM v4.1, and ESKM v4.2 appliances.
>
> Adding multiple ESKM appliances to a cluster is a sequential process. Ensure the first appliance is successfully added to the cluster before attempting to add the next appliance to the cluster.

To join a cluster:

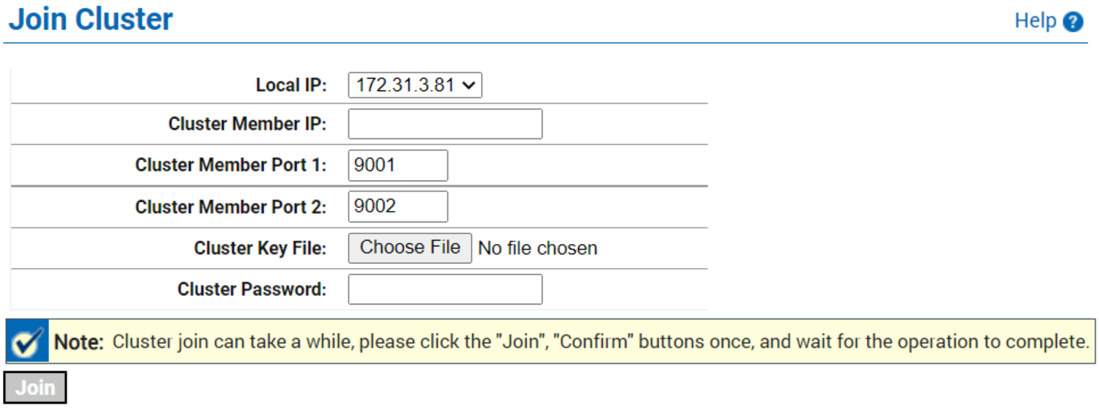
1. Log in to the Management Console of a current cluster member as an administrator with Cluster access control.

2. Go to the Cluster Settings section of the Cluster Configuration page (**Device** > **Cluster**).

3. Click **Download Cluster Key** to save the key on your workstation’s local file system. The cluster key contains authentication information used when passing information between cluster members. Utimaco recommends using a unique name each time you download a cluster key.

4. Log in to the ESKM appliance, which you want to add to the cluster.

5. Navigate to the **Join Cluster** section on the Cluster Configuration page.



Join Cluster

Local IP:	172.31.3.81
Cluster Member IP:	
Cluster Member Port 1:	9001
Cluster Member Port 2:	9002
Cluster Key File:	Choose File No file chosen
Cluster Password:	

Note: Cluster join can take a while, please click the "Join", "Confirm" buttons once, and wait for the operation to complete.

Figure 17 : Join Cluster

6. Enter the **Local IP**, **Cluster Member IP**, **Cluster Member Port 1**, **Cluster Member Port 1** and **Cluster Password**.
   The **Cluster Password** was set when first establishing the primary node in the cluster. For more information about initial configuration, see the *vESKM Deployment Guide*.

7. Browse to and enter the location of the downloaded cluster key in the **Cluster Key File** field.

8. Click **Join**. Post clicking the Join button, the following warning message is displayed.

Joining to the cluster will delete all existing keys on the “joining node” and acquire keys and configuration from the “local node”. Security settings may be changed causing this device to be taken out of FIPS compliance.

An internal backup of all keys and configuration will be made automatically. This backup can be restored using the cluster password.

- Click **Confirm** to join with the “joining node” .

⚠ If the cluster configuration specifies a KMIP server certificate that does not exist on the ESKM appliance joining the cluster, a warning message displays, indicating that the KMIP server cannot start. To resolve this issue, create a KMIP server certificate with the same name as the KMIP server certificate specified in the cluster configuration.

⚠ If the cluster configuration specifies a REST server certificate that does not exist on the ESKM appliance joining the cluster, the communication via REST API will not work. To resolve this issue, create a server certificate with the same name and save the same certificate in REST Server configuration.

- When all ESKM appliances have joined the cluster, you can delete the cluster key from the local file system on your workstation.

4.12.3 Synchronizing with a cluster member

To synchronize with a cluster member:

1. Log in to the Management Console that will be updated as an administrator with Cluster access control.

2. Navigate to the Cluster Members section of the Cluster Configuration page (**Device** > **Cluster**).

3. Select the appliance from which you will copy configuration settings.

4. Click **Synchronize With** and confirm this action. As part of the synchronization, the ESKM appliance creates an automatic synchronization backup before installing the new configuration.

! Synchronizing the local appliance with the cluster overwrites the existing configuration, which may include keys. You can access the overwritten information using the synchronization backup. If you have any keys that exist only on the local ESKM appliance, use the backup and restore features to copy them to another appliance before synchronizing the local appliance with the cluster.

4.12.4 Configuring SSL/TLS in a cluster

When using SSL/TLS in a cluster, the replication settings must include KMS Server settings, KMIP Server settings, and all cluster members must use a server certificate with the same name, as indicated in the KMS Server Settings and KMIP Server Settings sections. The contents of those server certificates should be unique.

To configure SSL/TLS for a cluster:

1. Log in to the Management Console as an administrator with Certificate and CA access control.
2. Navigate to the Create Certificate section on the Certificate and CA Configuration page (**Device** > **Cluster** > **Cluster Configuration**).
3. Create a certificate signed by a local CA.
4. Repeat steps 1, 2, and 3 for each ESKM appliance in the cluster*.
5. Select an ESKM appliance with configuration settings that you can push out to the other appliances in the cluster.
6. Navigate to the **KMS Server Settings** section on the KMS Configuration page.
7. Click **Use SSL**, and then set **Server Certificate** to the newly created certificate.
8. Click **Save**, and then confirm your changes. Once you confirm the settings, they will be replicated to the other cluster members. No automatic synchronization backup will occur.
9. Navigate to the **KMIP Server Settings** section on the KMIP Server Configuration page.

10. Set the Server Certificate to the newly created certificate.

11. Click **Save**, and then confirm your changes. Once you confirm the settings, they will be replicated to the other cluster members. No automatic synchronization backup will occur.

> *For each certificate, you must use the same name, and all the certificates should be signed by the same CA.

4.12.5 Removing an appliance from a cluster

Before removing an ESKM appliance from a cluster, be sure to configure the client so that it will no longer attempt to use the appliance.

To remove an ESKM appliance from a cluster:

1. Log in the Management Console of the appliance that will be removed from the cluster as an administrator with Cluster access control.

2. Navigate to the Services List section (**Device** > **Services**) and stop both the KMS and KMIP services.

3. Navigate to the Cluster Settings section of the Cluster Configuration page (**Device** > **Cluster**).

4. Click **Remove From Cluster**.

> Perform a restore default configuration in case you want to rejoin the node back to a cluster.

4.12.6 Upgrading a cluster

A cluster can be upgraded by upgrading one ESKM appliance at a time. After all of the ESKM appliances are running the new software, you can configure the replication settings as needed.

> ⚠ Utimaco recommends that you do not make configuration changes while upgrading a cluster. Utimaco recommends stopping KMS and KMIP services, quiescing client operations, and taking backups for all cluster members before upgrading the software. Consult Utimaco Technical Support (p. 798) for upgrade planning, software, and documentation before starting an upgrade.

To upgrade a cluster:

1. Log in to the Management Console as an administrator with Software Upgrade access control.

2. Upgrade the software on the ESKM appliance.

3. Repeat steps 1 and 2 for each additional ESKM appliance in the cluster.

4.12.7 Deleting a cluster

A cluster is deleted when the last ESKM appliance is removed from the cluster.

To delete a cluster:

1. Log in the Management Console of the appliance, that will be removed from the cluster, as an administrator with Cluster access control.

2. Navigate to the Services List section (**Device** > **Services**), and then stop the KMS and KMIP services.

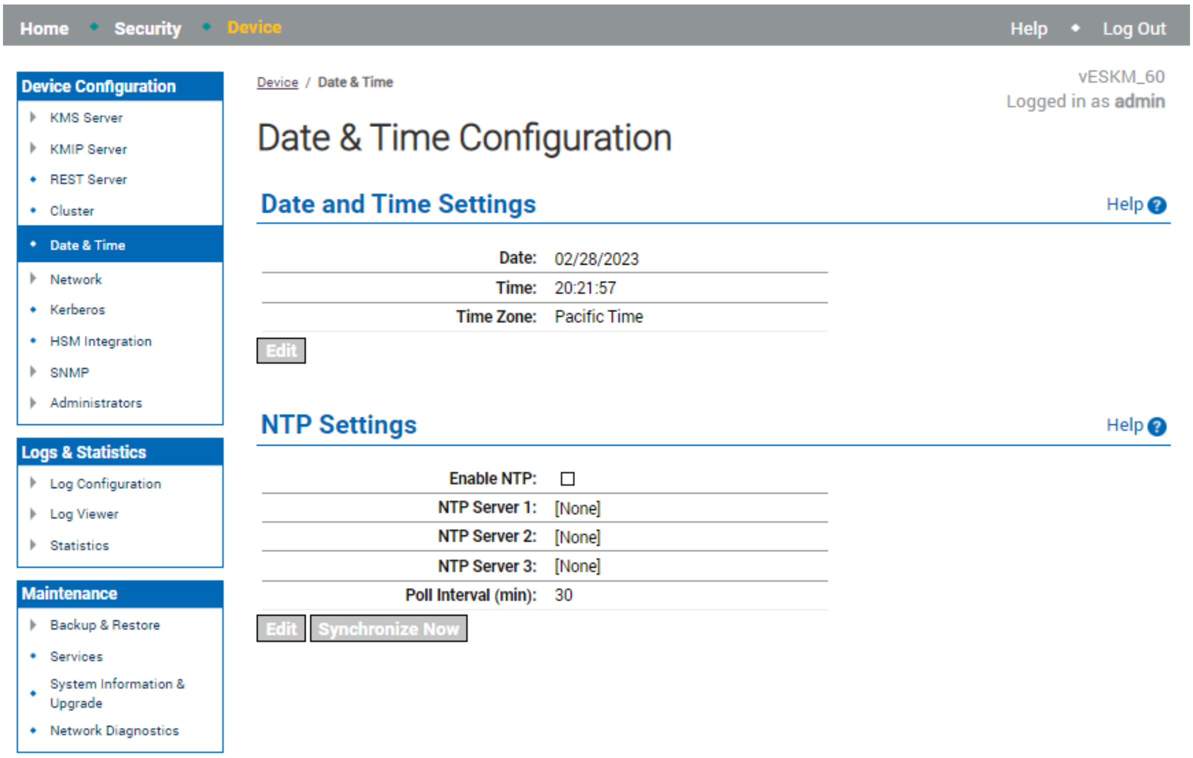
3. Navigate to the Cluster Settings section of the Cluster Configuration page (**Device** > **Cluster**)

4. Click **Remove From Cluster**.

5. Repeat these steps for each additional ESKM appliance in the cluster.

4.13 Date and time procedures

This section describes the procedures to follow when managing date and time settings on the ESKM appliance and configuring NTP connections.



Date & Time Configuration

Date and Time Settings

Date: 02/28/2023
Time: 20:21:57
Time Zone: Pacific Time

NTP Settings

Enable NTP: □
NTP Server 1: [None]
NTP Server 2: [None]
NTP Server 3: [None]
Poll Interval (min): 30

This section explains the following processes:

- Setting the date and time (p. 122)
- Configuring an NTP server connection (p. 123)
- Manually synchronizing with an NTP server (p. 124)

4.13.1 Setting the date and time

To set the date and time on the ESKM appliance:

1. Log in to the Management Console as an administrator with Network and Date/Time access control.

2. Navigate to the Date and Time Settings section of the Date and Time Configuration page (**Device** > **Date & Time**).

3. Click **Edit**.

4. Modify the **Date**, **Time**, and **Time Zone** fields as needed.

5. Click **Save**.

4.13.2 Configuring an NTP server connection

To configure an NTP server connection:

1. Log in to the Management Console as an administrator with Network and Date/Time access control.

2. Navigate to the NTP Settings section of the Date and Time Configuration page (**Device** > **Date & Time**).

3. Click **Edit**.

4. Select **Enable NTP**.

5. Enter the IP addresses of the NTP servers in the **NTP Server** fields.

6. Specify the frequency (in minutes) with which the ESKM appliance will poll the NTP servers. If you enter a value that is not a multiple of 5, the ESKM appliance will round down to the nearest multiple of 5.

7. Click **Save**.

4.13.3 Manually synchronizing with an NTP server

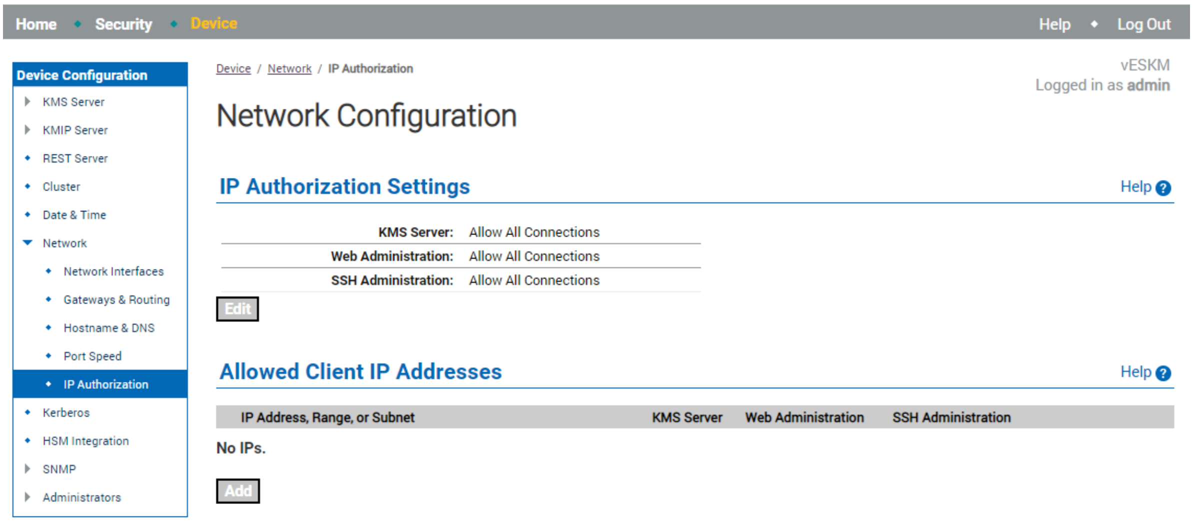
The ESKM appliance automatically synchronizes with the NTP server according to the Poll Interval value indicated in the NTP section.

To manually synchronize with an NTP server:

1. Log in to the Management Console as an administrator with Network and Date/Time access control.
2. Navigate to the NTP Settings section of the Date and Time Configuration page (**Device** > **Date & Time**).
3. Click **Synchronize Now**.

4.14 IP authorization procedures

This section describes the procedures you will follow when configuring IP authorization.



Network Configuration

IP Authorization Settings

KMS Server:	Allow All Connections
Web Administration:	Allow All Connections
SSH Administration:	Allow All Connections

Allowed Client IP Addresses

IP Address, Range, or Subnet	KMS Server	Web Administration	SSH Administration

No IPs.

Figure 18 : Network Configuration

4.14.1 Specifying which clients can connect to the ESKM

The IP authorization feature enables you to control which clients can connect to the ESKM appliance and what services they can access.

⚠ The KMIP server does not support IP Authorization.

To specify which ESKM clients can connect to the ESKM appliance:

1. Log in to the Management Console as an administrator with Network and Date/Time access control.

2. Navigate to the Allowed Client IP Addresses section of the Network Configuration page (**Device** > **Network** > **IP Authorization**).

3. Click **Add**.

4. Enter a single IP address, a range of addresses, or a subnet in the **IP Address**, **Range**, or **Subnet** field.

5. Select the services that will be available to this client using the **KMS Server**, **Web Administration**, and **SSH Administration** fields.
   You can grant access to various features but you cannot explicitly deny access to a specific client. In the event that a specific IP is listed individually and as part of a group, that IP address acquires the sum of
   listed permissions.

6. Click **Save**.

7. Repeat steps 3 through 6 as needed.

8. Click **Edit** on the IP Authorization Settings section.

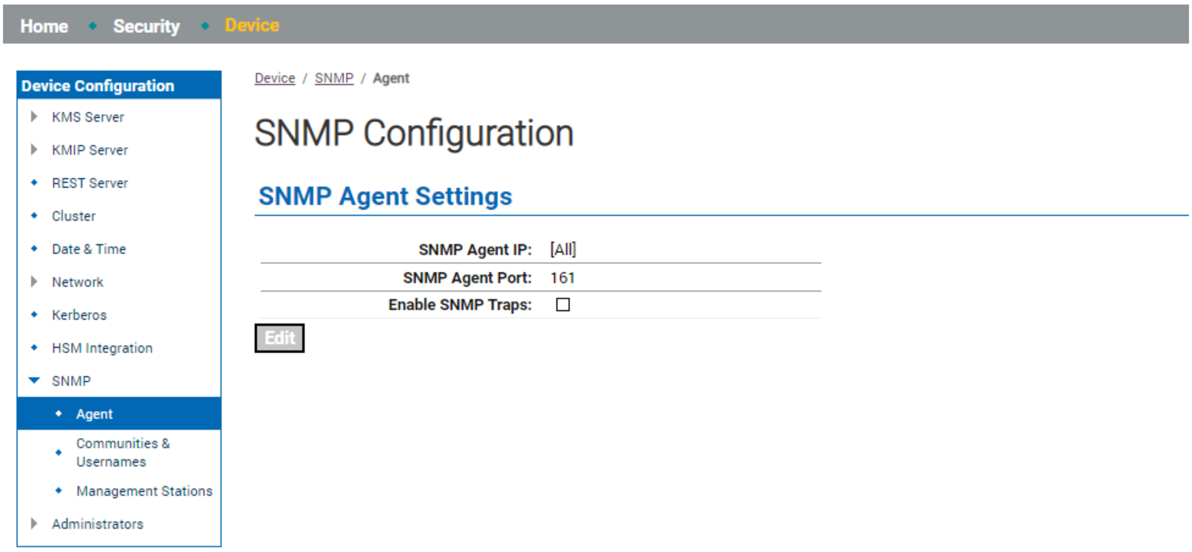
9. To grant access to all clients, select **Allow All Connections**. To grant access to only the clients listed in the Allowed Client IP Addresses section, select **Only Allow IPs Specified Below**. Repeat this step for each service as needed.

10. Click **Save**.

> When updating this feature from the Management Console, the ESKM appliance ensures that the current administrator IP address maintains its web administration permissions.

4.15 SNMP procedures

This section describes the procedures you will follow when configuring the ESKM appliance for Simple Network Management Protocol (SNMP).



SNMP Configuration

SNMP Agent Settings

SNMP Agent IP:	[All]
SNMP Agent Port:	161
Enable SNMP Traps:	□

Figure 19 : SNMP Configuration

This section explains the following processes:

- Configuring SNMPv1/v2
- Configuring SNMPv3

4.15.1 Configuring SNMPv1/v2

The ESKM appliance supports all three versions of SNMP. From a configuration standpoint, SNMPv1/v2 are treated as a unit, and SNMPv3 is treated separately. Please note that the ESKM SNMP agent is capable of providing the following SNMP functionality:

- It enables the Network Management System (NMS) to access Management Information Base (MIB)s on the ESKM appliance.

- It initiates trap messages to the NMS

You can configure the ESKM SNMP agent to provide either piece of functionality or both pieces. Both pieces of functionality are optional.

To configure an ESKM agent to communicate with an NMS running SNMPv1/v2 software:

1. Configure the agent at the **SNMP Agent Settings** section.
2. Create a community at the **SNMPv1/SNMPv2 Community List** section to enable the NMS to access the Enterprise MIBs.
3. Define an NMS at the **Create SNMP Management Station** section if you want the ESKM appliance to initiate trap messages to the NMS. You only have to provide values for the first five fields. The fields that are used for SNMPv3 are clearly marked as v3 only.

4.15.2 Configuring SNMPv3

The ESKM appliance supports all three versions of SNMP. From a configuration standpoint, SNMPv1/v2 are treated as a unit, and SNMPv3 is treated separately. The ESKM SNMP agent is capable of providing the following SNMP functionality:

- It enables the NMS to access the MIBs on the ESKM appliance
- It initiates trap messages to the NMS

You can configure the ESKM SNMP agent to provide either piece of functionality or both pieces. Both pieces of functionality are optional.

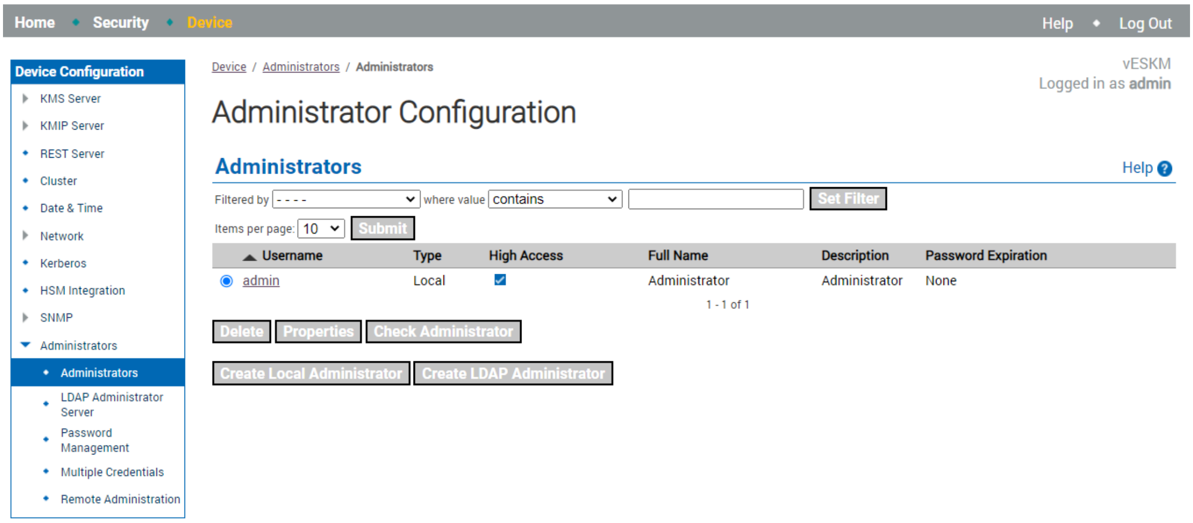
To configure an ESKM SNMP agent to communicate with an NMS running SNMPv3 software:

1. Configure the agent at the **SNMP Agent Settings** section.
2. Create an SNMPv3 username at the **SNMPv3 Username List** section to enable the NMS to access the Enterprise MIBs.

3. Define an NMS at the **Create SNMP Management Station** section if you want the ESKM appliance to initiate trap messages to the NMS. The fields required for defining an SNMPv3 NMS depend on the combination of authorization and privacy you choose.

4.16 Administrator procedures

This section describes the procedures you will follow when creating and managing administrator accounts.



Administrator Configuration

Administrators

Help
Filtered by - - - - where value contains Set Filter
Items per page: 10 Submit

	Username	Type	High Access	Full Name	Description	Password Expiration
●	admin	Local	☑	Administrator	Administrator	None

1 - 1 of 1

Figure 20 : Administrator Configuration

This section explains the following processes:

- Creating an administrator (p. 128)
- Deleting an administrator (p. 130)

For more information about administrators and access controls, see Administrator overview (p. 473).

4.16.1 Creating an administrator

Use the Administrators section to view the list of administrators, modify an administrator, view properties assigned to a specific administrator, or manage administrator passwords.

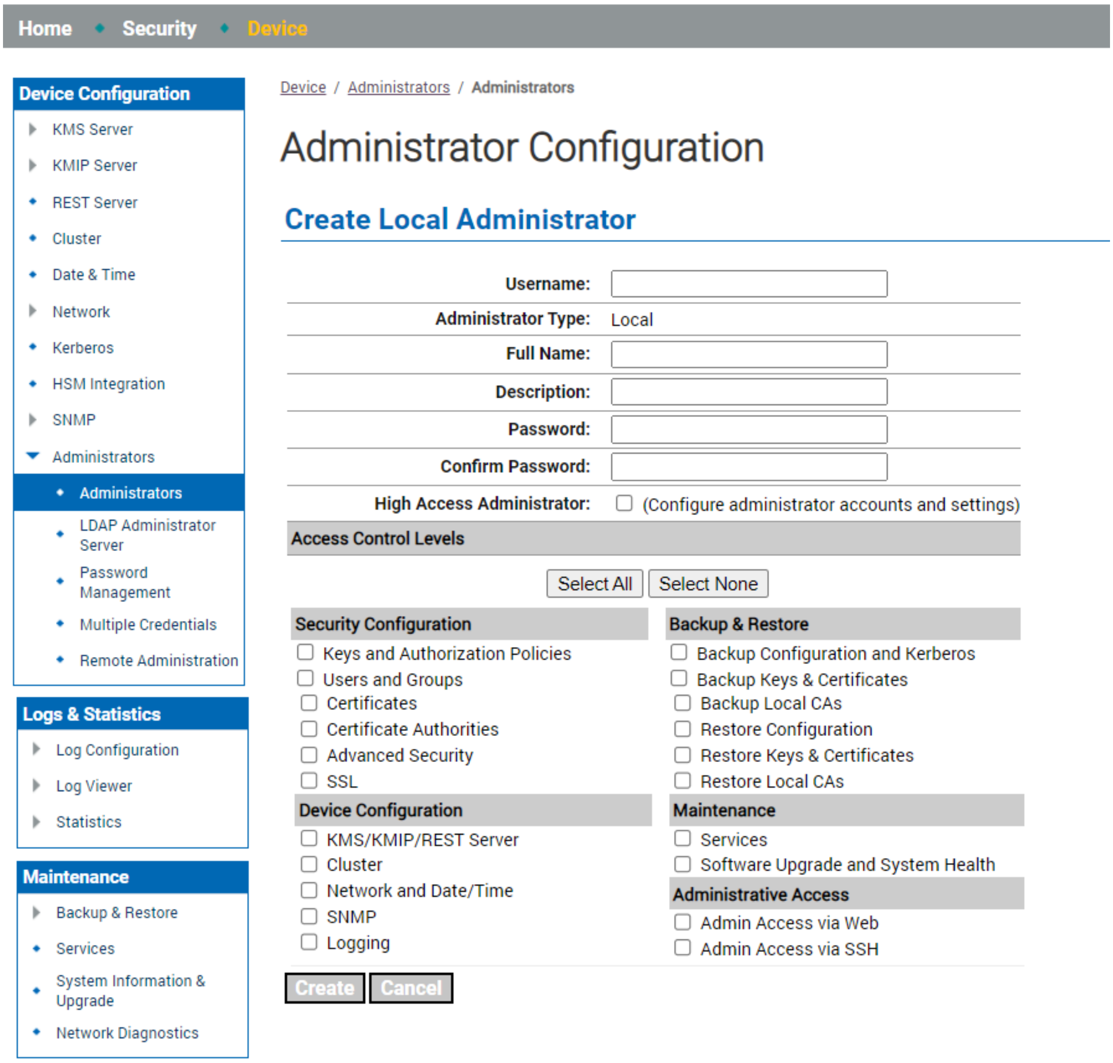
To create an administrator account:

1. Log in the Management Console as an administrator with Administrators access control.

2. Navigate to the Create Administrator section on the Administrator Configuration page (**Device** > **Device Configuration** > **Administrators** > **Administrators**).

3. Click **Local Administrator** or **LDAP Administrator**, depending on the administrator type you want to create. (For more information about LDAP Administrator, see LDAP administrators (p. 478).)

4. Enter values and access controls in the prompted fields.



Administrator Configuration

Create Local Administrator

Username:

Administrator Type: Local

Full Name:

Description:

Password:

Confirm Password:

High Access Administrator: □ (Configure administrator accounts and settings)

Access Control Levels

Security Configuration
- □ Keys and Authorization Policies
- □ Users and Groups
- □ Certificates
- □ Certificate Authorities
- □ Advanced Security
- □ SSL

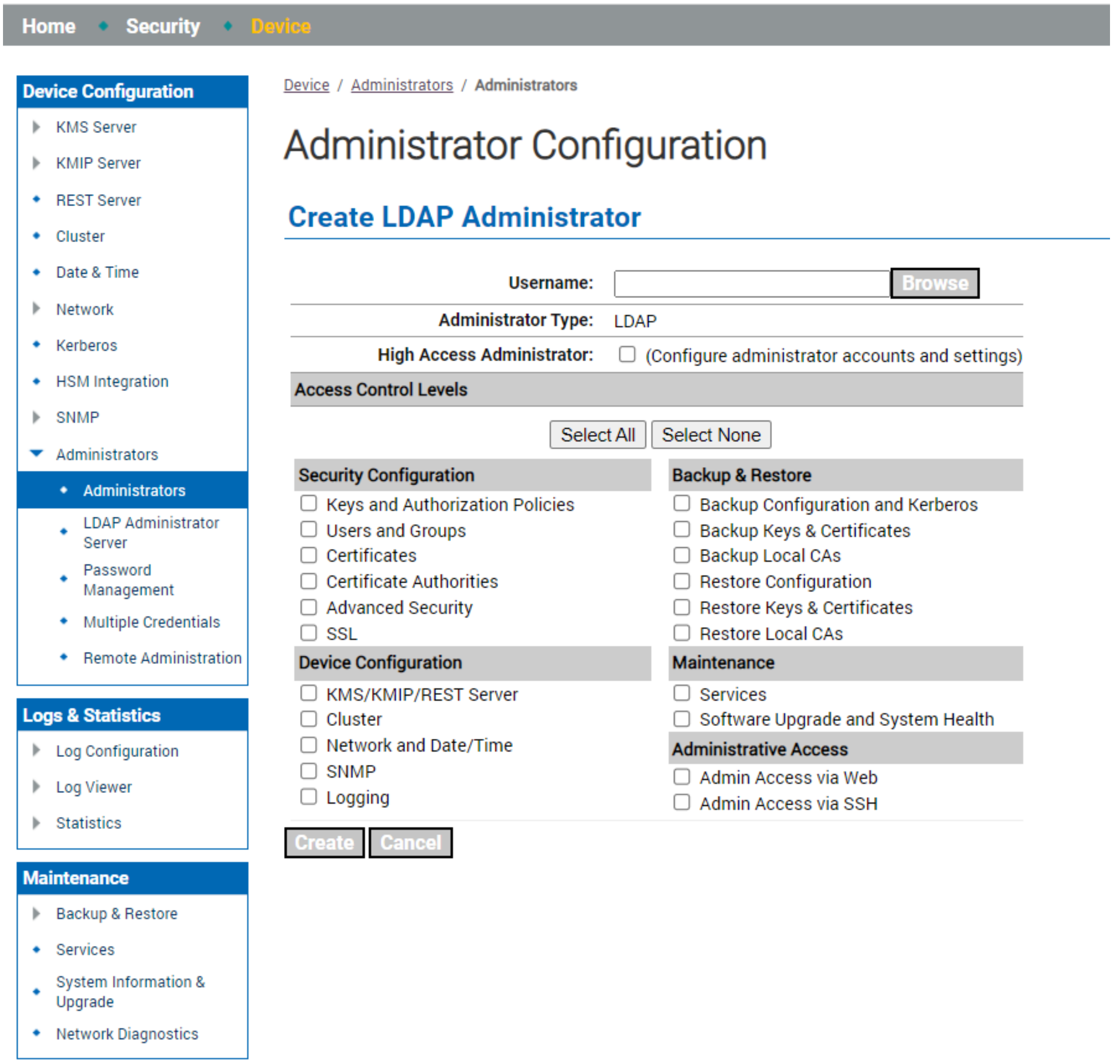
Device Configuration
- □ KMS/KMIP/REST Server
- □ Cluster
- □ Network and Date/Time
- □ SNMP
- □ Logging

Backup & Restore
- □ Backup Configuration and Kerberos
- □ Backup Keys & Certificates
- □ Backup Local CAs
- □ Restore Configuration
- □ Restore Keys & Certificates
- □ Restore Local CAs

Maintenance
- □ Services
- □ Software Upgrade and System Health

Administrative Access
- □ Admin Access via Web
- □ Admin Access via SSH

Figure 21 : Create Local Administrator



Administrator Configuration

Create LDAP Administrator

Username:

Administrator Type: LDAP

High Access Administrator: □ (Configure administrator accounts and settings)

Access Control Levels

Security Configuration	Backup & Restore
□ Keys and Authorization Policies	□ Backup Configuration and Kerberos
□ Users and Groups	□ Backup Keys & Certificates
□ Certificates	□ Backup Local CAs
□ Certificate Authorities	□ Restore Configuration
□ Advanced Security	□ Restore Keys & Certificates
□ SSL	□ Restore Local CAs
Device Configuration	**Maintenance**
□ KMS/KMIP/REST Server	□ Services
□ Cluster	□ Software Upgrade and System Health
□ Network and Date/Time	**Administrative Access**
□ SNMP	□ Admin Access via Web
□ Logging	□ Admin Access via SSH

Figure 22 : Create LDAP Administrator

5. Click **Create.**

4.16.2 Deleting an administrator

To delete an administrator account:

1. Log in to the Management Console as an administrator with Administrators access control.

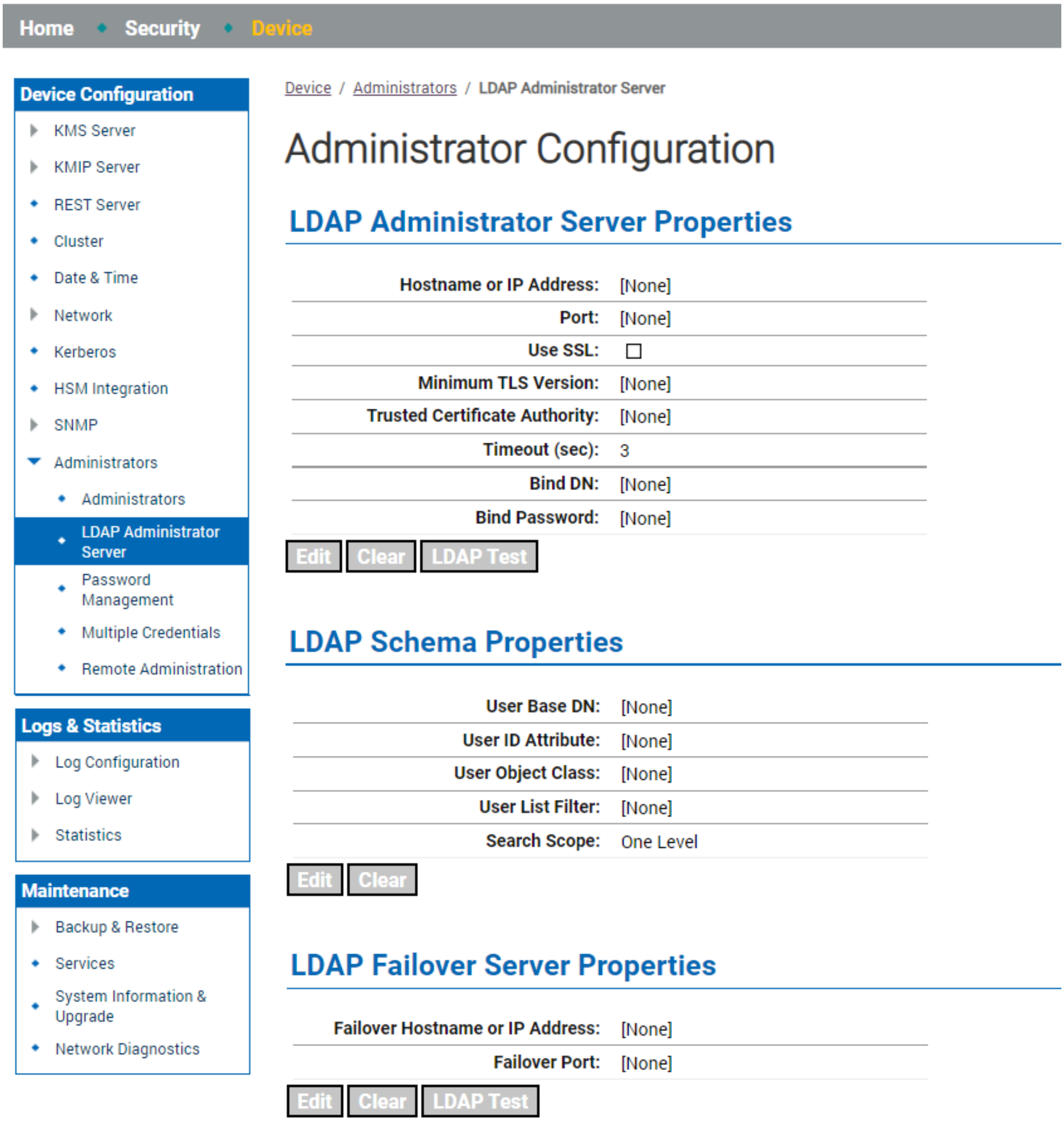
2. Navigate to the Administrator List section on the Administrator Configuration page (**Device** > **Device Configuration** > **Administrators** > **Administrators**).

3. Select the administrator, and then click **Delete**.

4. Confirm the action on the Secondary Approval section.

4.17 LDAP Administrator server procedures

This section describes the procedures for managing LDAP administrator servers.



Administrator Configuration

LDAP Administrator Server Properties

Hostname or IP Address:	[None]
Port:	[None]
Use SSL:	□
Minimum TLS Version:	[None]
Trusted Certificate Authority:	[None]
Timeout (sec):	3
Bind DN:	[None]
Bind Password:	[None]

LDAP Schema Properties

User Base DN:	[None]
User ID Attribute:	[None]
User Object Class:	[None]
User List Filter:	[None]
Search Scope:	One Level

LDAP Failover Server Properties

Failover Hostname or IP Address:	[None]
Failover Port:	[None]

Figure 23 : LDAP Administrator Server Configuration

This section explains the following procedures:

- Setting up the LDAP administrator server (p. 133)
- Testing the LDAP administrator server connection (p. 134)
- Setting up the LDAP schema (p. 134)

- Setting up the LDAP failover server (p. 77)
- Testing the LDAP failover server connection (p. 135)

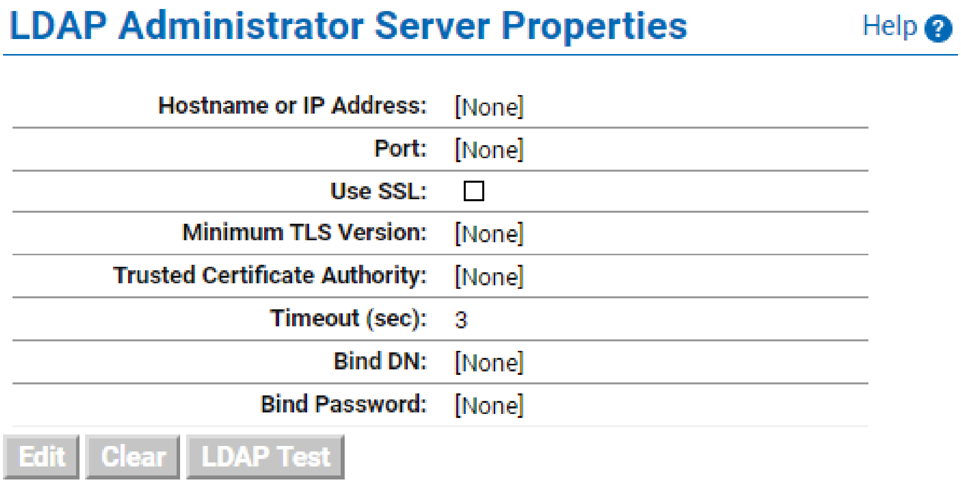
⚠ The KMIP server does not support LDAP.

4.17.1 Setting up the LDAP administrator server

To set up the LDAP Administrator Server:

1. Log in to the ESKM appliance as a Local administrator with High Access Administrator access control.

2. Navigate to the LDAP Administrator Server Properties section of the Administrator Configuration page (**Device** > **Device Configuration** > **Administrators** > **LDAP Administrator Server**).



LDAP Administrator Server Properties

Hostname or IP Address:	[None]
Port:	[None]
Use SSL:	□
Minimum TLS Version:	[None]
Trusted Certificate Authority:	[None]
Timeout (sec):	3
Bind DN:	[None]
Bind Password:	[None]

Figure 24 : LDAP Administrator Server Properties

3. Under LDAP Administrator Server Properties, click **Edit.**

4. Enter the **Hostname or IP Address** and **Port**.

5. If you are using SSL/TLS, check **Use SSL**, enter the **Minimum TLS Version**, and **Trusted Certificate Authority**.

6. Enter the number of seconds to wait for the LDAP server during connections in the **Timeout** field.

7. Enter the **Bind DN** (distinguished name) and **Bind Password**.

8. Click **Save**.

> ⚠ On a FIPS-compliant appliance, selecting a **Minimum TLS version** earlier than TLS 1.2, will make the appliance non-FIPS-compliant.

4.17.2 Testing the LDAP administrator server connection

To test the LDAP administrator server connection:

1. Log in to the ESKM appliance as a Local administrator with High Access Administrator access control.

2. Navigate to the LDAP Administrator Server Properties section of the Administrator Configuration page (**Device** > **Device Configuration** > **Administrators** > **LDAP Administrator Server**).

3. Click **LDAP Test**.

4.17.3 Setting up the LDAP schema

To set up the LDAP Schema:

1. Log in to the ESKM appliance as a Local administrator with High Access Administrator access control.

2. Navigate to the LDAP Schema Properties section of the Administrator Configuration page (**Device** > **Device Configuration** > **Administrators** > **LDAP Administrator Server**).

3. Click **Edit**.

4. Enter the values for your LDAP schema. All fields are required except **User List Filter**.

5. Click **Save**.

4.17.4 Setting up the LDAP failover server

To set up the LDAP Failover Server:

1. Log in to the ESKM appliance as a Local administrator with High Access Administrator access control.

2. Navigate to the LDAP Failover Server section of the LDAP Administrator Configuration page (**Device** > **Device Configuration** > **Administrators** > **LDAP Administrator Server**).

3. Under **LDAP Failover Server Properties**, click **Edit**.

4. Enter the **Failover Hostname or IP Address** and **Failover Port**.

5. Click **Save**.

4.17.5 Testing the LDAP failover server connection

To test the LDAP Failover Server Connection:

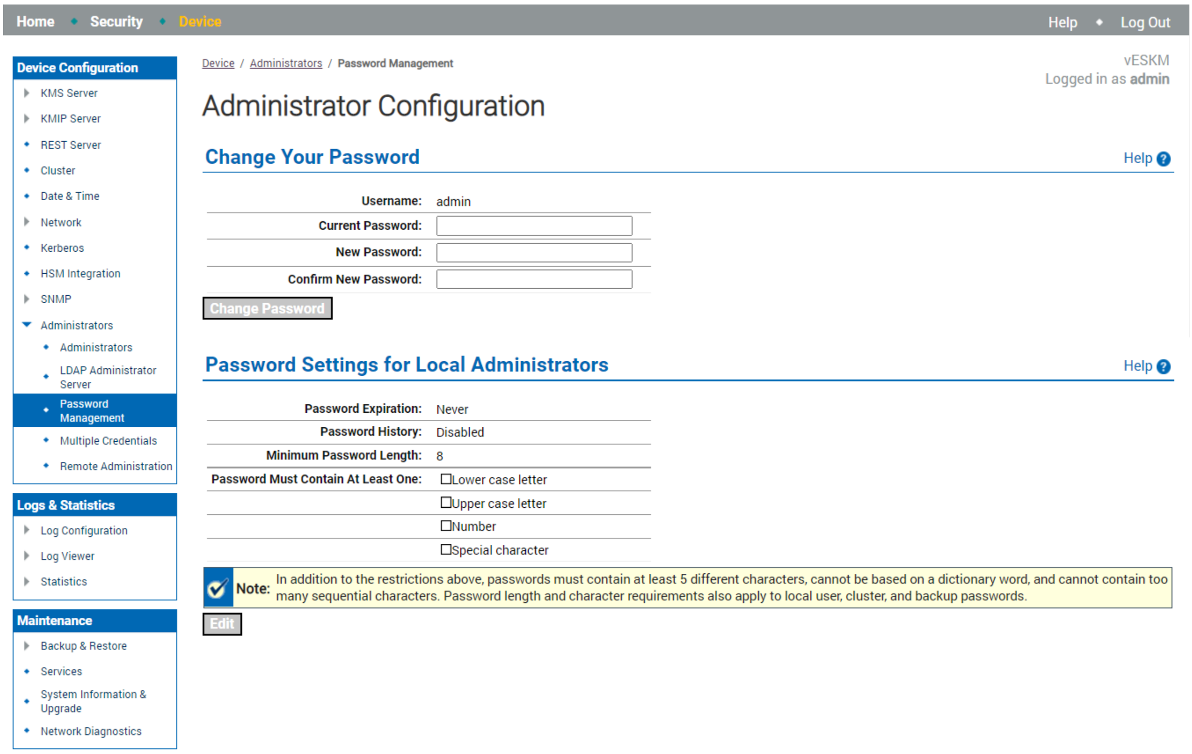
1. Log in to the ESKM appliance as a Local administrator with High Access Administrator access control.

2. Navigate to the LDAP Failover Server section of the LDAP Administrator Configuration page (**Device** > **Device Configuration** > **Administrators** > **LDAP Administrator Server**).

3. Click **LDAP Test**.

4.18 Password management procedures

This section describes the procedures you will follow when changing passwords or configuring password settings, located on **Device Configuration** > **Administrators** > **Password Management**.



Administrator Configuration

Change Your Password

Username:	admin
Current Password:	
New Password:	
Confirm New Password:	

Password Settings for Local Administrators

Password Expiration:	Never
Password History:	Disabled
Minimum Password Length:	8
Password Must Contain At Least One:	□Lower case letter
	□Upper case letter
	□Number
	□Special character

Note: In addition to the restrictions above, passwords must contain at least 5 different characters, cannot be based on a dictionary word, and cannot contain too many sequential characters. Password length and character requirements also apply to local user, cluster, and backup passwords.

Figure 25 : Password Management

This section explains the following processes:

- Changing your password (p. 136)
- Configuring password settings for local administrators (p. 137)
- Changing passwords when a security officer leaves (p. 138)

4.18.1 Changing your password

To change your administrator account password:

1. Log in to the Management Console using your administrator account.

2. Navigate to the Change Your Password section of the Administrator Configuration page (**Device Configuration** > **Administrators** > **Password Management**).

3. Enter your current password in the **Current Password** field.

4. Enter a new password in the **New Password** and **Confirm New Password** fields.

5. Click **Change Password**.

4.18.2 Configuring password settings for local administrators

To configure password settings for local administrators:

1. Log in to the Management Console as an administrator with High Access Administrators access control.

2. Navigate to the Password Settings for Local Administrators section of the Administrator Configuration page (**Device Configuration** > **Administrators** > **Password Management**).

3. Click **Edit**.

4. To enable password expiration, enter the Maximum Password Age in the **Password Expiration** field. When an administrator's password reaches this age, the administrator will be forced to create a new password.

5. To enable password history, enter the **Num Passwords to Remember** in the **Password History** field. When creating a new password, an administrator cannot use a value that exists in their password history.
   The password history is only consulted when administrators attempt to change their own passwords. It is not checked when one administrator changes another's password.

6. Enter the Minimum Password Length.

7. Specify if the password must contain at least one lower case letter, upper case letter, number, or special character, or some combination of these values.

8. Click Save.

4.18.3 Changing passwords when a security officer leaves

In the event of a security officer personnel change, immediately change the passwords for administrator accounts, user accounts, and backups in order to protect the integrity of the system and the data protected by the encryption keys. This procedure should be handled quickly but deliberately, so that access to the ESKM configuration is secured but not performed haphazardly. Plan ahead to have a documented procedure in place to handle such a situation. One possible procedure is the following:

1. Delete the former security officer's administrator account immediately.

2. Create a new administrator account with the same permissions but a different account name. Have the replacement security officer use the new account.
   The account must be deleted because It is not possible for administrators to change another administrator's password on the ESKM appliance.

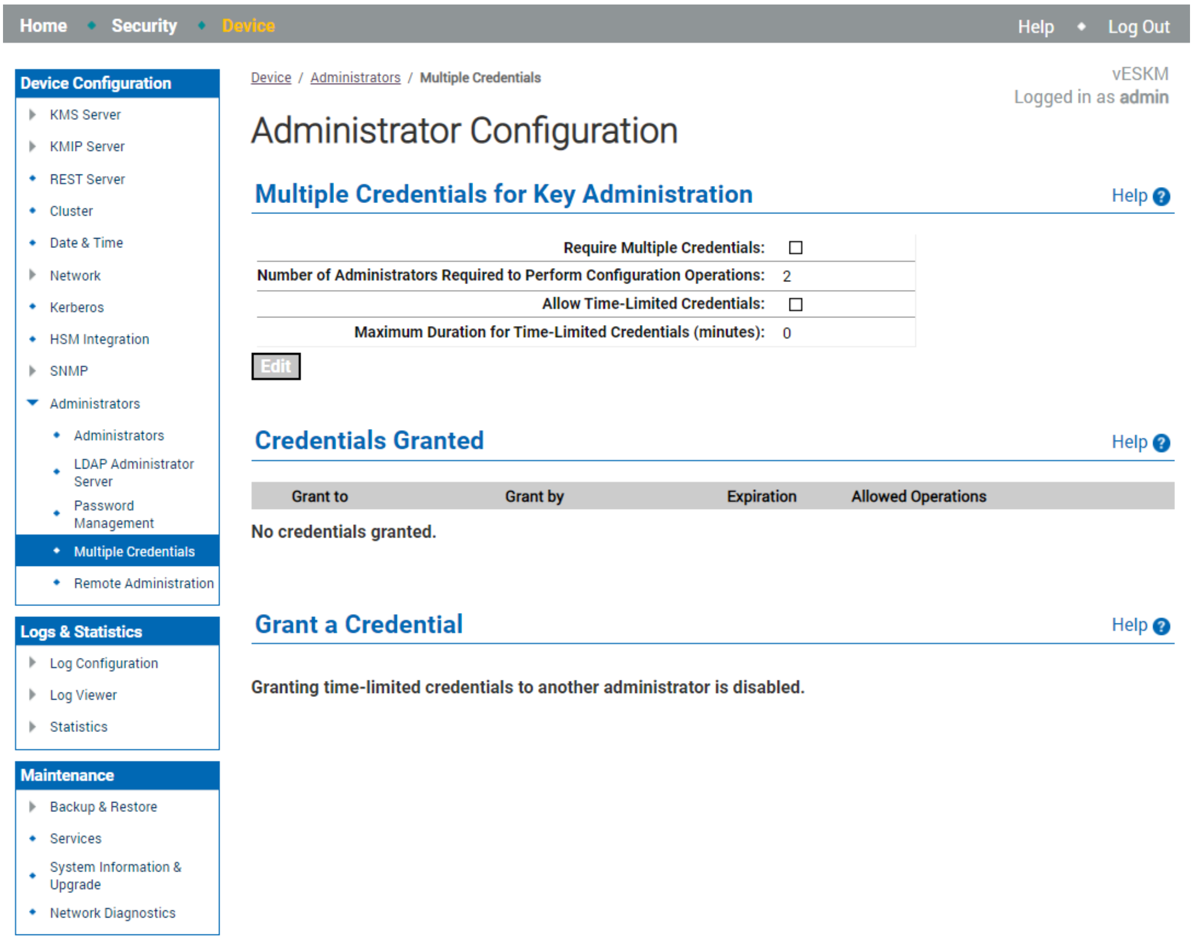
3. Have each remaining security officer change their administrator account password, preferably with at least one other security officer present to witness the password change.

4. Change the user account passwords, on both the ESKM appliance and the enrolled clients, again with at least one other security officer present. Because this may interrupt the ability of the client to retrieve keys during the change and verification, this should be done outside the backup window at the earliest convenience. Refer to the *vESKM Deployment Guide* for instructions on how to do this.

5. Change the backup job passwords for each ESKM appliance in the configuration. Remember that if an automated script is being used to run the backup jobs, the password information will have to be changed in the script, as well.

4.19 Multiple credentials procedures

This section describes the procedures you will follow when configuring the multiple credentials feature and granting credentials.



Device / Administrators / Multiple Credentials

Administrator Configuration

Multiple Credentials for Key Administration

Require Multiple Credentials:	□
Number of Administrators Required to Perform Configuration Operations:	2
Allow Time-Limited Credentials:	□
Maximum Duration for Time-Limited Credentials (minutes):	0

Credentials Granted

Grant to	Grant by	Expiration	Allowed Operations

No credentials granted.

Grant a Credential

Granting time-limited credentials to another administrator is disabled.

Figure 26 : Multiple Credentials

This section explains the following processes:

- Configuring the multiple credentials feature (p. 140)
- Granting credentials (p. 140)
- Revoking a credential grant (p. 141)

The multiple credential feature does not apply to KMIP-managed objects

4.19.1 Configuring the multiple credentials feature

To configure the multiple credentials feature:

1. Log in to the Management Console as an administrator with High Access Administrators access control.

2. Navigate to the Multiple Credentials for Key Administration section on the Administrator Configuration page (**Device** > **Administrators** > **Multiple Credentials**).

3. Click **Edit**.

4. Select **Require Multiple Credentials**.

5. Specify the number of administrators required to perform configuration operations. There must be at least as many administrators with High Access Administrator access control as are required by this field.

6. To allow administrators to grant their credentials to other administrators for a limited time period select **Allow Time-Limited Credentials**, and then enter the time period in the **Maximum Duration for Time-Limited Credentials** field.

7. Click **Save**.

4.19.2 Granting credentials

Prior to granting credentials, you must select **Require Multiple Credentials** and **Allow Time-Limited Credentials** on the Multiple Credentials for Key Administration section.

To grant credentials:

1. Log in to the Management Console as an administrator with High Access Administrator access control. This administrator will grant credentials to another administrator.

2. Navigate to the Grant a Credential section on the Administrator Configuration page (**Device** > **Administrators** > **Multiple Credentials**).

3. Select the administrator, who will receive the credentials, in the **Grant to** field.

4. Enter the duration for which the credentials will be granted. This value must be less that the **Maximum Duration for Time-Limited Credentials** value in the Multiple Credentials for Key Administration section.

5. Select the operations for which you are granting credentials.

6. Click **Grant**. You can now view the granted credentials in the Credentials Granted section.

4.19.3 Revoking a credential grant

Prior to revoking a credential grant, you must have granted credentials.

To revoke a credential grant:

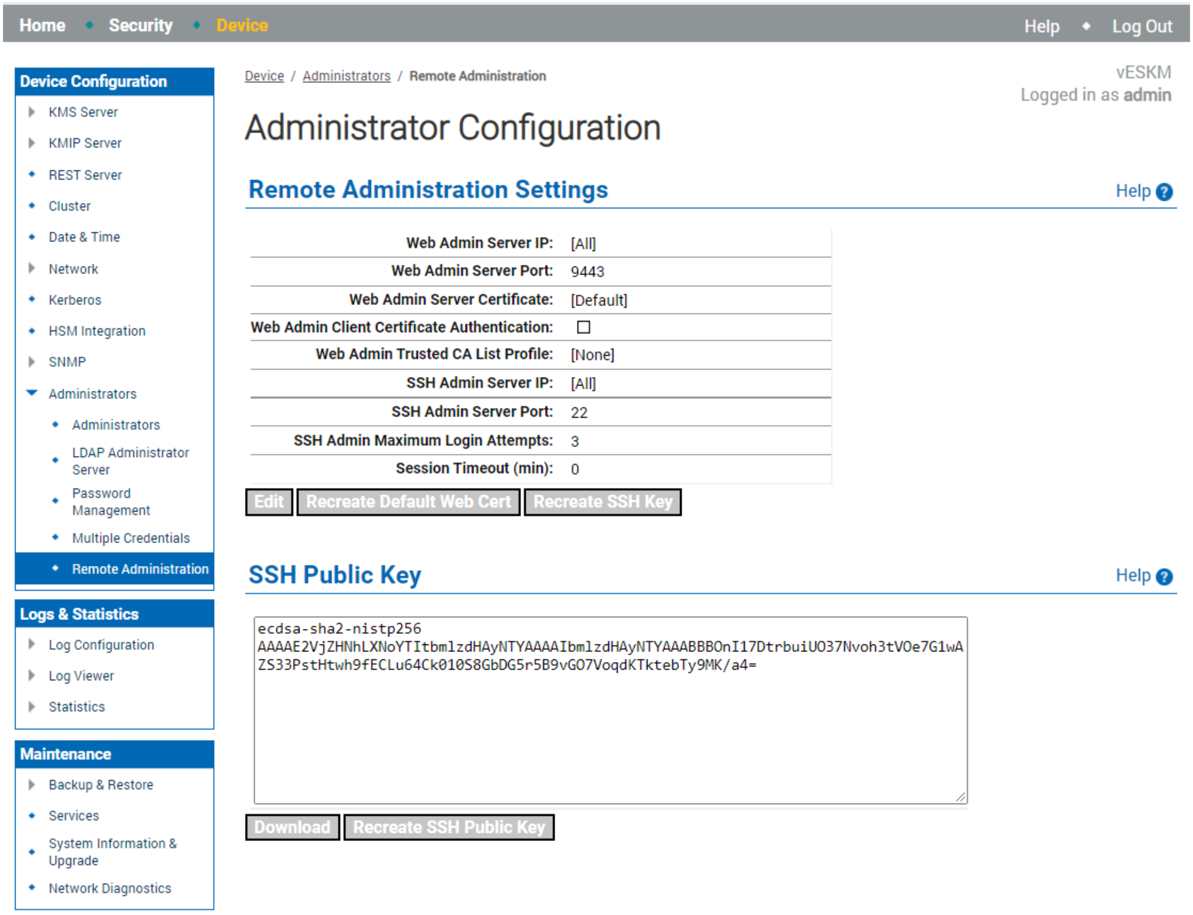
1. Log in to the Management Console as an administrator who has previously granted credentials.

2. Navigate to the Credentials Granted section on the Administrator Configuration page (**Device** > **Device Configuration** > **Administrators** > **Multiple Credentials**).

3. Click **Delete/Revoke**. The credential grant will be removed from the ESKM appliance.

4.20 Remote administration procedures

This section describes the procedures you will follow when configuring remote administration.



Administrator Configuration

Remote Administration Settings

Web Admin Server IP:	[All]
Web Admin Server Port:	9443
Web Admin Server Certificate:	[Default]
Web Admin Client Certificate Authentication:	□
Web Admin Trusted CA List Profile:	[None]
SSH Admin Server IP:	[All]
SSH Admin Server Port:	22
SSH Admin Maximum Login Attempts:	3
Session Timeout (min):	0

SSH Public Key

```
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOnI17DtrbuiUO37Nvoh3tVOe7G1wA
ZS33PstHtwh9fECLu64Ck010S8GbDG5r5B9vGO7VoqdKTktebTy9MK/a4=
```

Figure 27 : Remote Administration

This section explains the following processes:

- Configuring the web admin server certificate (p. 142)
- Signing a certificate request and downloading the certificate (p. 143)
- Converting a certificate from PEM to PKCS12 format (p. 144)
- Enabling web admin client certificate authentication (p. 145)

4.20.1 Configuring the web admin server certificate

By default, the ESKM appliance creates a self-signed web admin server certificate. You can install and specify a different server certificate for remote web administration.

⚠ This procedure assumes that you have already installed the certificate on the ESKM appliance; for more information, see Certificate procedures (p. 78).

⚠ If your ESKM appliances are in a cluster and you are selecting a new web admin server certificate, you must first make sure that all of the appliances in the cluster already have a web admin server certificate installed with this same name.

⚠ Utimaco recommends to set the **Subject Alternative Name** for the Web Admin Server Certificate as modern browsers use **Subject Alternative Name** instead of **Common Name** for host validation.

To configure the ESKM appliance to use a different server certificate for remote web administration:

1. Log in to the Management Console.
2. Navigate to the Remote Administration Settings section (**Device** > **Administrators** > **Remote Administration**).
3. Click **Edit**.
4. Click the **Web Admin Server Certificate** drop-down list and choose the server certificate.
5. Click **Save**.

4.20.2 Signing a certificate request and downloading the certificate

This section describes how to sign a certificate request with a local CA and download the certificate.

⚠ You must download the certificate immediately after it is signed by the CA.

To sign a certificate request with a local CA:

1. Open the certificate request in a text editor.

2. Copy the text of the certificate request. The copied text must include the header (`-----BEGIN CERTIFICATE REQUEST...`) and the footer (`...END CERTIFICATE REQUEST-----`).

3. Log in to the Management Console as an administrator with Certificates access control.

4. Navigate to the Local Certificate Authority List (**Security** > **Certificates & CAs** > **Local CAs**).

5. Select the local CA, and then click **Sign Request** to access the Sign Certificate Request section.

6. Modify the fields as shown:
   - Sign with Certificate Authority—Select the CA that signs the request.
   - Certificate Purpose—Select Client.
   - Certificate Duration (days)—Enter the life span of the certificate.
   - Certificate Request—Paste the entire text from the certificate request, including the header and footer.

7. Click **Sign Request**. This will take you to the CA Certificate Information section where the certificate is displayed in PEM format.

8. Click the **Download** button to save the certificate to your workstation. Provide the certificate to the client.

4.20.3 Converting a certificate from PEM to PKCS12 format

The ESKM appliance can provide you with a certificate in PEM format. You must convert that certificate to PKCS12 before importing it to your web browser.

To convert a certificate from PEM to PKCS12 format:

- Execute the following command if you are using openssl:

```
openssl pkcs12 -export -inkey <key filename> -in <cert filename>
-out <pkcs12 filename>
```

4.20.4 Enabling web admin client certificate authentication

The web admin client certificate authentication feature requires a client certificate signed by the local CA on the ESKM appliance.

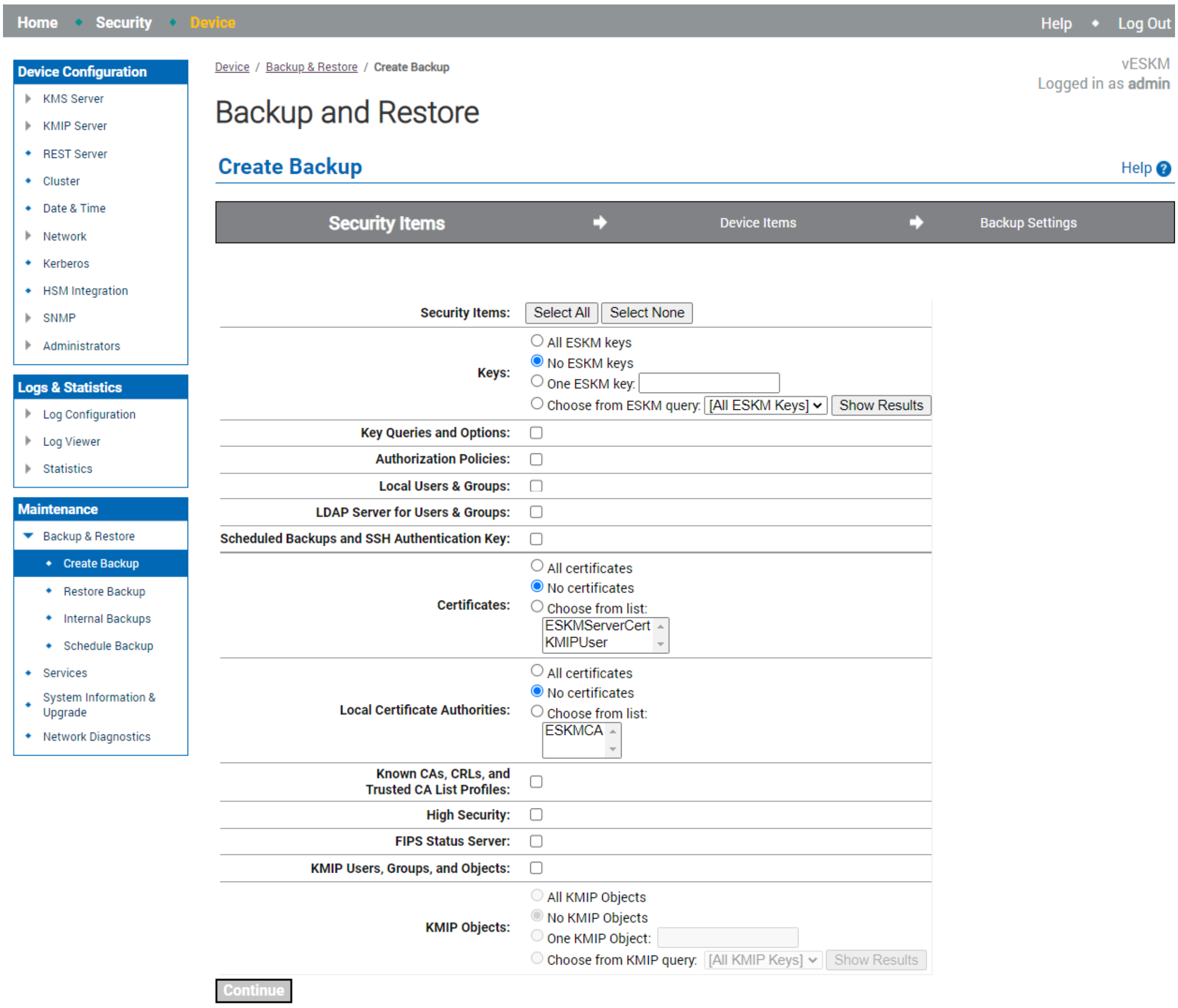
To enable web admin client certificate authentication on the ESKM appliance:

1. Log in to the Management Console.
2. Navigate to the Remote Administration Settings section (**Device** > **Administrators** > **Remote Administration**).
3. Click **Edit**.
4. Select **Web Admin Client Certificate Authentication**.
5. Click **Save**.

⚠ This feature is immediately enabled when you select **Web Admin Client Certificate Authentication**. You will be logged out of the Management Console and will need a valid client certificate to return. If needed, you can use the edit ras settings (p. 740)command from the CLI to disable this feature without presenting a certificate.

4.21 Backup procedures for keys, configurations, and certificates

This section covers the items found under **Device** > **Maintenance** > **Backup & Restore**.



Backup and Restore

Create Backup

Security Items:	Select All Select None
Keys:	○ All ESKM keys ● No ESKM keys ○ One ESKM key: ○ Choose from ESKM query: [All ESKM Keys] Show Results
Key Queries and Options:	□
Authorization Policies:	□
Local Users & Groups:	□
LDAP Server for Users & Groups:	□
Scheduled Backups and SSH Authentication Key:	□
Certificates:	○ All certificates ● No certificates ○ Choose from list: ESKMServerCert KMIPUser
Local Certificate Authorities:	○ All certificates ● No certificates ○ Choose from list: ESKMCA
Known CAs, CRLs, and Trusted CA List Profiles:	□
High Security:	□
FIPS Status Server:	□
KMIP Users, Groups, and Objects:	□
KMIP Objects:	○ All KMIP Objects ● No KMIP Objects ○ One KMIP Object: ○ Choose from KMIP query: [All KMIP Keys] Show Results

Figure 28 : Backup and Restore: Security Items

This section describes the following procedures:

- Importing and exporting KMS keys between clusters (p. 147)
- Backing up configurations and certificates to an external location (p. 153)
- Backing up keys to an external server (p. 154)

4.21.1 Importing and exporting KMS keys between clusters

> ⚠ This section applies only to KMS keys, not KMIP keys. To move KMIP keys to another cluster you must create a backup of the KMIP Users, Groups and Objects, and then restore that backup to an ESKM appliance in the other cluster.

Use the ESKM backup/restore feature to export one KMS key at a time from Cluster #1, and import it to Cluster #2. When a KMS key is exported, the corresponding usage permissions are also exported.

To use the imported key, you must set permissions on Cluster #2’s clients.

When a KMS key is imported (restored) to a cluster, it must be manually replicated to other ESKM appliances in that cluster. For more information, see Force replication of the key across Cluster #2 (p. 151).

> ⚠ The exported KMS key remains accessible to Cluster #1; the key has been copied, not moved.

4.21.1.1 Determine the key name to be exported

> ⚠ The following is one example of how to filter for a specific key. Other filters are available, and may work better in different situations.

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2. Navigate to the Keys section of the Key and Policy Configuration page (**Security** > **Keys**).

3. Select **Query Keys**.

4. Click **Add**, and then click **Next**.

5. From the Create Query section, use the field **Choose Keys Where** to query for the needed key. For example, select **Key Name** on the first box, select **Equals** from the second box, and enter the key name to be exported in the third box.

6. 6. Click **Run Query without Saving**.

4.21.1.2 Determine the Key Sharing Group

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2. Navigate to the Keys section of the Key and Policy Configuration page (**Security** > **Keys**).

3. Select **Keys**.

4. From the list of keys, choose the one with the most recent timestamp, and then click **Properties**.

5. Select the **Permissions** tab to display the name of the Group, listed in the Group Permissions panel, and then note the name of the Group.

4.21.1.3 Export (back up) the key

1. Log in to the Management Console as an administrator with Backup and Restore access control.

2. Navigate to the Backup and Restore page (**Device** > **Maintenance** > **Backup & Restore**).

3. Select **Create Backup**.

4. In the Security Items field, click **Select None**.

5. If the key to be exported has group permission, select **Local Users & Groups**.

6. In the **Keys** field, select **One key**, then enter or copy/paste the key name.

7. Click **Continue**.

8. From **Device Items**, click **Select None**.

9. Click **Continue**.

10. In the **Backup Summary** section of the panel, verify that no settings, certificates, or local CAs are included. In the **Keys** field, verify that the desired key is listed.

11. Enter the Backup Name, Backup Description, and Backup Password, and then select the Destination.

12. Click **Backup**. A message displays when the backup is complete. The backup operation should take a few seconds.

⚠ From Step 5 through 8, ensure the backup file contains only the single key.

4.21.1.4 Import the key on Cluster #2

Send the Destination (backup) file to the Cluster #2 admin. Also transmit the Group name and the backup password.

⚠ For security reasons, Utimaco recommends these communications occur separately, via different communication paths.

1. Log in to the Management Console as an administrator with Backup and Restore access control.

2. Navigate to the Backup and Restore page (**Device** > **Maintenance** > **Backup & Restore**).

3. Select **Restore Backup**.

4. Specify the source of the file and the backup password.

5. In the All Items field of the Backup Restore Information section, select **Select None**.

6. In the Security Items panel, in the Keys field, select **All keys**. Alternatively, you may enter the key name, and **restore 1 key***.

7. Select **Local Users & Groups** if needed.

8. In the Backup Password field, enter the backup password.

9. Click **Restore**. A message displays when the restore is complete.

*Although the backup file should only contain one key, it is a best practice to deselect everything except keys. If anything else is selected, restoring configurations would overwrite existing configurations for that ESKM appliance, and would very likely cause a fatal error.

Restoring keys is additive. New keys are added to the existing list, and no existing keys are replaced.

4.21.1.5 Restart the ESKM appliance

Following a restore, the ESKM appliance must be restarted.

1. Log in to the Management Console as an administrator with Maintenance access control.

2. Navigate to the Backup and Restore page (**Device** > **Maintenance** > **Backup & Restore**).

3. Select **Services**.

4. In the Restart/Halt pane, in the Restart/Halt field, select **Restart**.

5. Click **Commit**.

6. Select **Confirm** to initiate the restart request. The restart will take approximately five minutes.

7. When the restart is complete, login to the ESKM appliance again.

4.21.1.6 Force replication of the key across Cluster #2

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2. Navigate to the Keys section of the Key and Policy Configuration page (**Security** > **Keys**).

3. Select **Query Keys**.

4. Use Query Keys from the **Keys** section of the panel to find the key.

5. Select the Key Name, then click **Properties**.

6. From the Key and Policy Configuration screen, select the **Properties** tab.

7. Click **Edit**.

8. Toggle the **Deletable** property, and then click **Save**.

9. Again, click **Edit**.

10. Again, toggle the Deletable property, and then click **Save**.

> This step changed the imported key's "Deletable" property, then changed it back. A property change forces replication of the key to the other ESKM appliances in the cluster. This method is simpler than restoring the file to, and rebooting, each ESKM appliance.

4.21.1.7 Ensure that the key sharing group has been added

1. Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2. Navigate to the Keys section of the Key and Policy Configuration page (**Security** > **Users & Groups**).

3. Select **Local Groups**.

4. Verify that the Group name from Cluster #1 is listed in the Local Groups section under Group.

5. If the Group name from Cluster #1 is not listed, add it now.
   a. Under Local Groups section, click **Add**.
   b. Enter the Group name, provided from Cluster #1. The names must match exactly.
   c. Click **Save**.
   d. Click the name of the new group.
   e. In the User List section, click **Add**.
   f. Add the name of each client that must access the key, and then click **Save**.

> Permission configuration should only be necessary once. After the key sharing group exists, other keys imported from that group will automatically be shared.

4.21.2 Backing up configurations and certificates to an external location

ESKM configurations and certificates may be backed up to a file on an external appliance or workstation. Because each server’s network configuration is unique, you should repeat the process for each appliance in the cluster.

> KMS keys and KMIP users, groups and objects are not backed up by this process. Key backup is described in Backing up keys to an external server (p. 154).

To back up all configurations and certificates:

1. Log in to the Management Console as an administrator with Backup and Restore access control.
2. Navigate to the Backup and Restore page (**Device** > **Maintenance** > **Backup & Restore**).
3. Select **Create Backup**.
4. In the Create Backup pane, Security Items field, click **Select All**.
5. In the Keys field, select **No ESKM keys**.
6. Click to deselect **KMIP Users, Groups and Objects**.
7. Click **Continue**.
8. In the **Device Items** field, click **Select All**.
9. Click **Continue**.
10. In the Backup Summary section of the panel, verify that all of the settings, certificates, and local certificate authorities are included in the backup, and that KMIP users, groups and objects are not included in the backup. Also verify that **[None]** is selected in the ESKM Keys field.

11. Enter the **Backup Name**, **Backup Description**, and **Backup Password**, and then select the **Destination**. The destination can be the browser or a location on an SCP server.

12. Click **Backup**. A message displays when the backup is complete.

Be sure to save the backup password in a secure place so it is available when the backup is restored.

4.21.3 Backing up keys to an external server

KMS keys and KMIP users, groups, and objects can be backed up to a file on an external server. Utimaco recommends backing up each ESKM appliance individually.

This process backs up ESKM keys, and KMIP users, groups and objects, not configurations and certificates. Certificate and configuration backup is described in Backing up configurations and certificates to an external location (p. 153).

To back up keys only to an external server:

1. Log in to the Management Console as an administrator with Backup and Restore access control.

2. Navigate to the Backup and Restore page (**Device** > **Maintenance** > **Backup & Restore**).

3. Select **Create Backup**.

4. In the Create Backup pane, in the Security Items field, click **Select None**.

5. In the Keys field, select **All ESKM keys**.

6. Click **KMIP Users, Groups and Objects**.

7. Click **Continue**.

8. In the **Device Items** field, click **Select None**.

9. Click **Continue**.

10. In the Backup Summary section of the panel, review the backup summary to ensure only ESKM keys, and KMIP users, groups, and objects are being backed up.

11. Enter the **Backup Name**, **Backup Description**, and **Backup Password**, and then select the Destination. For key backup, Utimaco recommends using an SCP server with at least 10GB of free disk space.

12. Click **Backup**. The Management Console displays a message when complete.

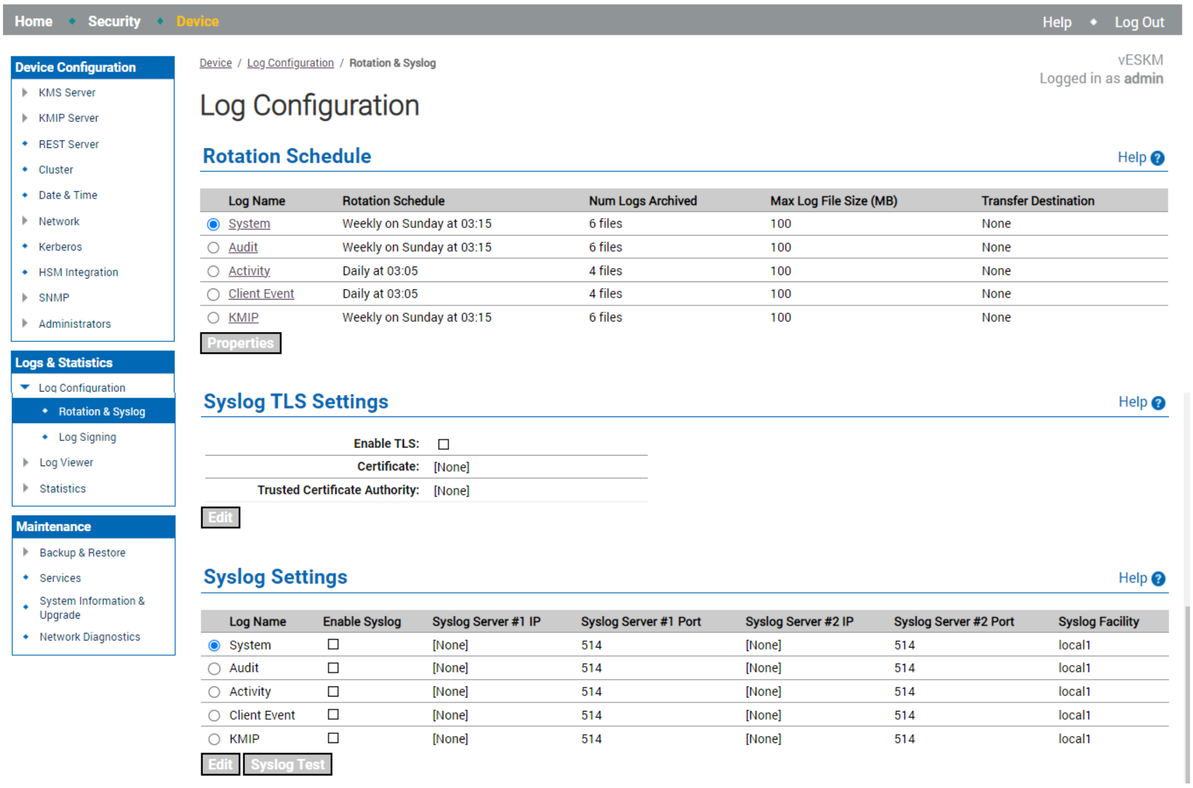
> ⚠ Although the backup file is compressed, the key database could be up to 4 GB.

The backup will consist of multiple files if the size exceeds about 1.5 GB. For 100,000 keys; a single backup file, typically about 1.4 GB, is normal.

> ⚠ Be sure to save the backup password in a secure place, so it is available when the backup is restored.

4.22 Log configuration procedures

This section describes the procedures you will follow when configuring the ESKM appliance logging feature. The configuration settings are located on **Device** > **Logs & Statistics** > **Log Configuration**.



Log Configuration

Rotation Schedule

	Log Name	Rotation Schedule	Num Logs Archived	Max Log File Size (MB)	Transfer Destination
●	System	Weekly on Sunday at 03:15	6 files	100	None
○	Audit	Weekly on Sunday at 03:15	6 files	100	None
○	Activity	Daily at 03:05	4 files	100	None
○	Client Event	Daily at 03:05	4 files	100	None
○	KMIP	Weekly on Sunday at 03:15	6 files	100	None

Syslog TLS Settings

Enable TLS:	□
Certificate:	[None]
Trusted Certificate Authority:	[None]

Syslog Settings

	Log Name	Enable Syslog	Syslog Server #1 IP	Syslog Server #1 Port	Syslog Server #2 IP	Syslog Server #2 Port	Syslog Facility
●	System	□	[None]	514	[None]	514	local1
○	Audit	□	[None]	514	[None]	514	local1
○	Activity	□	[None]	514	[None]	514	local1
○	Client Event	□	[None]	514	[None]	514	local1
○	KMIP	□	[None]	514	[None]	514	local1

Figure 29 : Log Configuration

This section explains the following processes:

- Configuring log rotation (p. 156)
- Enabling syslog (p. 157)
- Enabling signed logs (p. 158)
- Verifying a secure log using Microsoft Outlook (p. 158)
- Verifying a secure log using OpenSSL (p. 159)
- Recreating the log signing certificate (p. 160)

4.22.1 Configuring log rotation

To configure log rotation:

1. Log in to the Management Console as an administrator with Logging access control.

2. Navigate to the Log Configuration page (**Device** > **Log Configuration**), and then click the **Rotation & Syslog** tab.

3. Select a log in the Rotation Schedule section, and then click **Properties** to access the Log Rotation Properties section.

4. Click **Edit**.

5. Use the **Rotation Schedule** and **Rotation Time** fields to specify when the log will be rotated.

6. Specify the number of logs that will be maintained in the log archive using the **Num Logs Archived** field.

7. Enter a value in the **Max Log File Size** field. When a log file reaches this size it is automatically rotated, regardless of the **Rotation Schedule** and **Rotation Time settings**.

8. Enter a transfer destination if you would like the rotated log moved off of the ESKM appliance.

9. Click **Save**.

4.22.2 Enabling syslog

To enable syslog:

1. Log in to the Management Console as an administrator with Logging access control.

2. Navigate to the Log Configuration page (**Device** > **Log Configuration**), and then click the **Rotation & Syslog** tab.

3. Select a log in the Syslog Settings section, and then click **Edit**.

4. Select **Enable Syslog**, and then enter the server IPs, ports, and syslog facility.

5. Click **Save**.

6. Repeat steps 3, 4 and 5 as necessary to enable syslog for other types of logs.

4.22.3 Enabling signed logs

To enable signed logs:

1. Log in to the Management Console as an administrator with Logging access control.

2. Navigate to the Log Configuration page (**Device** > **Log Configuration**), and then click the **Log Signing** tab.

3. Click **Edit** in the Log Settings section.

4. Select **Sign Log** for the log(s) you would like to be signed.

5. Click **Save**. The ESKM appliance signs the selected logs with the log-signing certificate created when the appliance was initialized.

4.22.4 Verifying a secure log using Microsoft Outlook

To verify a secure log using Microsoft Outlook:

1. Move the log file off of the ESKM appliance or download it to a Windows machine.

2. Change the file extension on the log file to **.eml**. The file is now recognized by Windows as an Email file.

3. Double-click the file. Outlook opens and displays a help screen with a security header that reads: “Digitally signed - signing digital ID is not trusted.”

4. Click **Continue**. A security warning appears.

5. Click **View Digital ID**. The Signing Digital ID Properties dialog appears.

6. Click the **Details** tab and scroll down to the **Thumbprint** field.

7. Download the Log Signing Certificate used to sign the log file from the ESKM appliance.

8. Double-click the **Log Signing Certificate**. The Certificate dialog appears.

9. Select the **Details** tab.

10. Scroll down to the **Thumbprint** field.

11. Compare the thumbprints of the Signing Digital ID Properties dialog and the Log Signing Certificate dialog. If the text strings are identical, the integrity of the log file is secure.

4.22.5 Verifying a secure log using OpenSSL

Prior to verifying a secure log, you must have installed OpenSSL on the machine that will verify the log file. You can use this procedure in both Windows and UNIX/Linux environments.

To verify a secure log:

1. Log in to the Management Console as an administrator.

2. Navigate to the Log Configuration page (**Device** > **Log Configuration**), and then click the **Log Levels & Signing** tab.

3. Click **View Log Signing Cert**.

4. Click **Download Log Signing Cert**, and then save the Log Signer certificate to your local workstation.

5. Navigate to the Audit Log page (**Device** > **Logs & Statistics** > **Log Viewer** > <select the log page>), and then click **Download Entire Log**. Save the log file in the same directory as the log signer certificate. (You can save both the log file and the certificate anywhere you like; for the sake of simplicity, these procedures assume that the two files are in the same directory.)

6. From the command prompt, enter the following command:
   ```
   openssl smime -verify -in <signed log file> -nointern -certfile <log cert file> -text -noverify
   ```

   After issuing the command, the text from the log file is displayed. If the text of the log file has not been modified, the system displays “Verification successful” below the log text, as shown here:
   ```
   2016-02-06 11:17:30 [admin]: Logged in from 192.168.1.170 via web
   2016-02-06 11:24:26 [admin]: Downloaded Cert logsigner
   2016-02-06 12:30:17 [admin]: User admin login has expired.
   Verification successful
   ```
   You can test this process by modifying the text in the log file and running the command again. When you issue the command, the system again displays the text of the log file, but this time, it displays “Verification failure” after the text of the log file.

4.22.6 Recreating the log signing certificate

The log signing certificate is valid for one year. It should be recreated on a yearly basis. Prior to creating a new log signing certificate, backup the old certificate so you can verify previously signed logs.

To recreate the log signing certificate:

1. Log in to the Management Console as an administrator with Logging access control.

2. Navigate to the Log Configuration page (**Device** > **Log Configuration**), and then click the **Rotation & Syslog** tab.

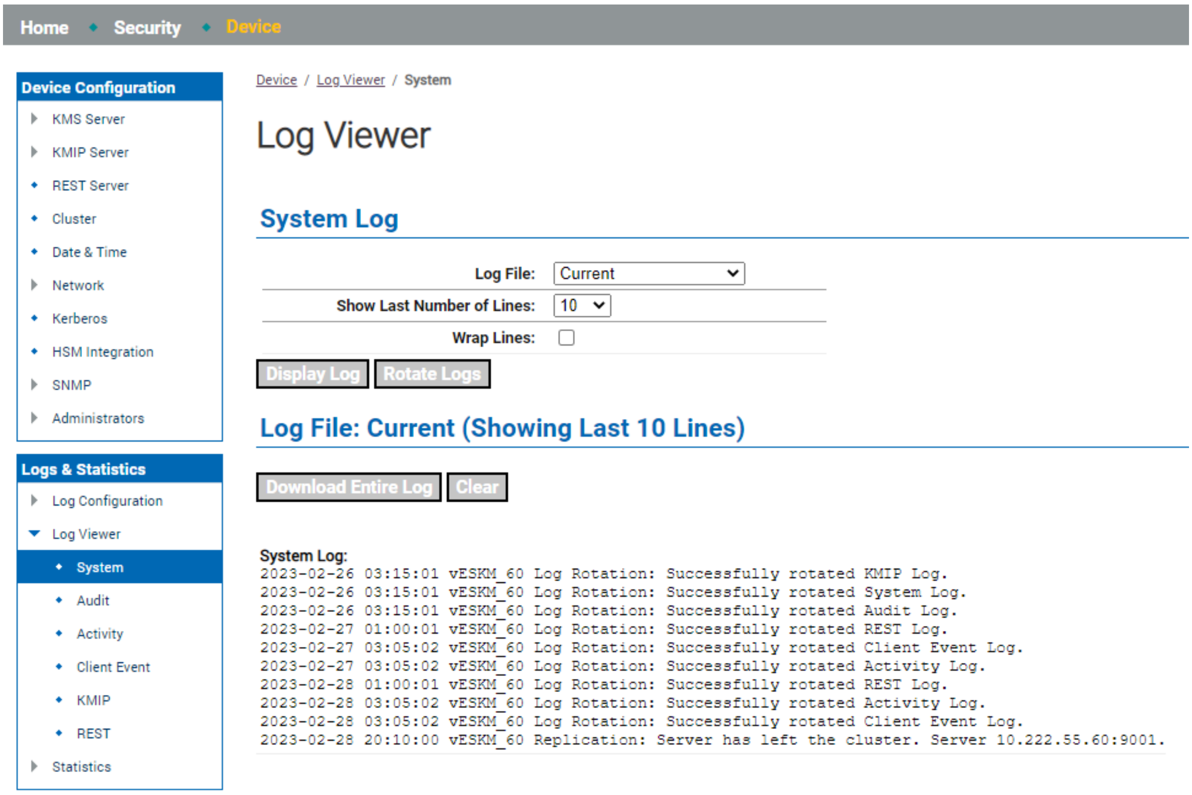
3. Click **Recreate Log Signing Cert** in the Audit Log Settings section.

4. Enter a **Certificate Duration**.

5. Click **Create** and confirm the action.

4.23 Log view procedures

This section describes the procedures you will follow when viewing, rotating, and downloading logs.



Log File: Current

Show Last Number of Lines: 10

Wrap Lines: □

```
System Log:
2023-02-26 03:15:01 vESKM_60 Log Rotation: Successfully rotated KMIP Log.
2023-02-26 03:15:01 vESKM_60 Log Rotation: Successfully rotated System Log.
2023-02-26 03:15:01 vESKM_60 Log Rotation: Successfully rotated Audit Log.
2023-02-27 01:00:01 vESKM_60 Log Rotation: Successfully rotated REST Log.
2023-02-27 03:05:02 vESKM_60 Log Rotation: Successfully rotated Client Event Log.
2023-02-27 03:05:02 vESKM_60 Log Rotation: Successfully rotated Activity Log.
2023-02-28 01:00:01 vESKM_60 Log Rotation: Successfully rotated REST Log.
2023-02-28 03:05:02 vESKM_60 Log Rotation: Successfully rotated Activity Log.
2023-02-28 03:05:02 vESKM_60 Log Rotation: Successfully rotated Client Event Log.
2023-02-28 20:10:00 vESKM_60 Replication: Server has left the cluster. Server 10.222.55.60:9001.
```

Figure 30 : Log View

This section explains the following processes:

- Viewing an archived log (p. 162)
- Manually rotating a log (p. 162)
- Downloading a log (p. 162)

- Clearing a log (p. 163)

4.23.1 Viewing an archived log

To view an archived log:

1. Log in to the Management Console as an administrator with Logging access control.
2. Navigate to the Log Viewer page (**Device** > **Log Viewer**), and then click the tab for the log you would like to view.
3. Choose a log in the **Log File** field. Specify the number of lines to view and select **Wrap Lines** to wrap the lines of text in your browser window.
4. Click **Display Log** to view the log in the Log File section.

4.23.2 Manually rotating a log

To manually rotate a log:

1. Log in to the Management Console as an administrator with Logging access control.
2. Navigate to the Log Viewer page (**Device** > **Log Viewer**), and then click the tab for the log you would like to rotate.
3. Click **Rotate Logs**.

4.23.3 Downloading a log

To download a log:

1. Log in to the Management Console as an administrator with Logging access control.

2. Navigate to the Log Viewer page (**Device** > **Log Viewer**), and then click the tab for the log you would like to download.
3. Choose a log in the **Log File** field.
4. Click **Display Log**.
5. Click **Download Entire Log**.

4.23.4 Clearing a log

To clear a log:

1. Log in to the Management Console as an administrator with Logging access control.
2. Navigate to the Log Viewer page (**Device** > **Log Viewer**), and then click the tab for the log you would like to download.
3. Choose a log in the **Log File** field.
4. Click **Display Log**.
5. Click **Clear**.

5 Maintaining the ESKM appliance

Routine maintenance on the ESKM appliance can be performed from the Management Console and the Command Line Interface. This section contains the following information:

5.1 Backup and restore overview

Clustering ESKM appliances is an effective way of exchanging keys and configuration data to allow for failover, but it is not the complete solution for protecting the overall ESKM environment. Perform regular backups of the appliances to ensure that your encryption solution is protected in a disaster recovery
scenario. In addition, if connectivity between appliances is lost even for a brief time, they can become out-of-sync; for example, one appliance might contain keys from a client that were not replicated across the cluster. In this event, using the backup utility is critical to being able to distribute the unreplicated keys to the other appliances in the cluster. Because of this out-of-sync possibility, it is necessary to back up each ESKM appliance, even in a clustered environment. As this could affect several appliances, some of which might be in off-site locations, develop a method to automate those backups to make administering the system easier.

The ESKM appliance provides different ways of backing up the keys and configuration. There are advantages and disadvantages to each method.

- Backing up internally to the ESKM appliance is the quickest and most secure way of running a backup, but provides no disaster-recovery protection.
- Backup by downloading the data via browser (this encrypts and saves the data to the local computer via the browser interface) provides disaster-recovery protection, since the data is stored outside the ESKM appliance and is operating system independent (because the browser handles the transfer).

- Backup to an external appliance using SCP (secure file transfer) to copy the backup file, provides both disaster-recovery protection and the ability to be automated. However, SCP is an older secure protocol and requires additional software (to send the data to a Windows server) as SCP is not a recognized protocol on Windows. SCP secures the backup data, therefore this method is the preferred solution for backing up the ESKM appliance.
- Backup to an external appliance using Windows Share (Kerberos) to copy the backup file, provides disaster-recovery protection. Kerberos is a network authentication protocol which uses symmetric-key cryptography to authenticate users to network services, which means passwords are never actually sent over the network.

Backups can be initiated in one of four ways:

- Interactively, via the ESKM Management Console interface, see Backup and restore page (p. 166)
- Interactively, via the Command Line Interface, see Backup and restore commands (p. 607)
- Automatically, via a command script provided to the Command Line Interface from an external program
- Automatically, see Schedule backup (p. 184)

The ESKM appliance's backup mechanism allows you to achieve two important objectives:

- Back up information on the ESKM appliance to be restored in case of a failure
- Copy configuration information between ESKM appliances

When an ESKM appliance is fully configured with networking information, certificates, and user accounts, Utimaco recommends that the entire configuration be backed up. Likewise, when you make changes to your configuration, update your backup files.

When restoring a backup, you can select which components of the backup file to restore. In general, once you select which items to restore, the current settings for those items are cleared from the ESKM appliance before the settings from the backup file are restored in their place.

Restoring keys, certificates, or local CAs, in contrast, is an additive process. The ESKM appliance adds the keys, certificates, and local CAs from the backup file to the existing set of keys, certificates, and CAs. This is because keys, certificates, and local CAs are unique cryptographic objects that cannot be recreated.

If one of these objects is being restored on an appliance where there is already a similar object with the same name, the key, certificate, or local CA from the backup file overwrites the existing object. Every backup file is protected with a key on the ESKM appliance and a password provided by the administrator. Because a backup file may contain sensitive information, such as user accounts and certificates, Utimaco recommends a reasonably long backup password.

5.2 Backup and restore page

The **Backup and Restore** page enables you to create and restore backups. The **Backup and Restore** page includes:

- Create backup (p. 166)
- Restore backup (p. 176)
- Backup and restore information (p. 181)
- Internal backup list (p. 183)
- Schedule backup (p. 184)

5.2.1 Create backup

Use the **Create Backup** section of the Backup and Restore page to create a backup configuration. When creating a backup, you can choose which components to back up.

⚠ Do not attempt to perform multiple concurrent backups. Ensure that any previous backup operation has completed successfully, i.e. check the audit log for a created backup record before starting a new backup.

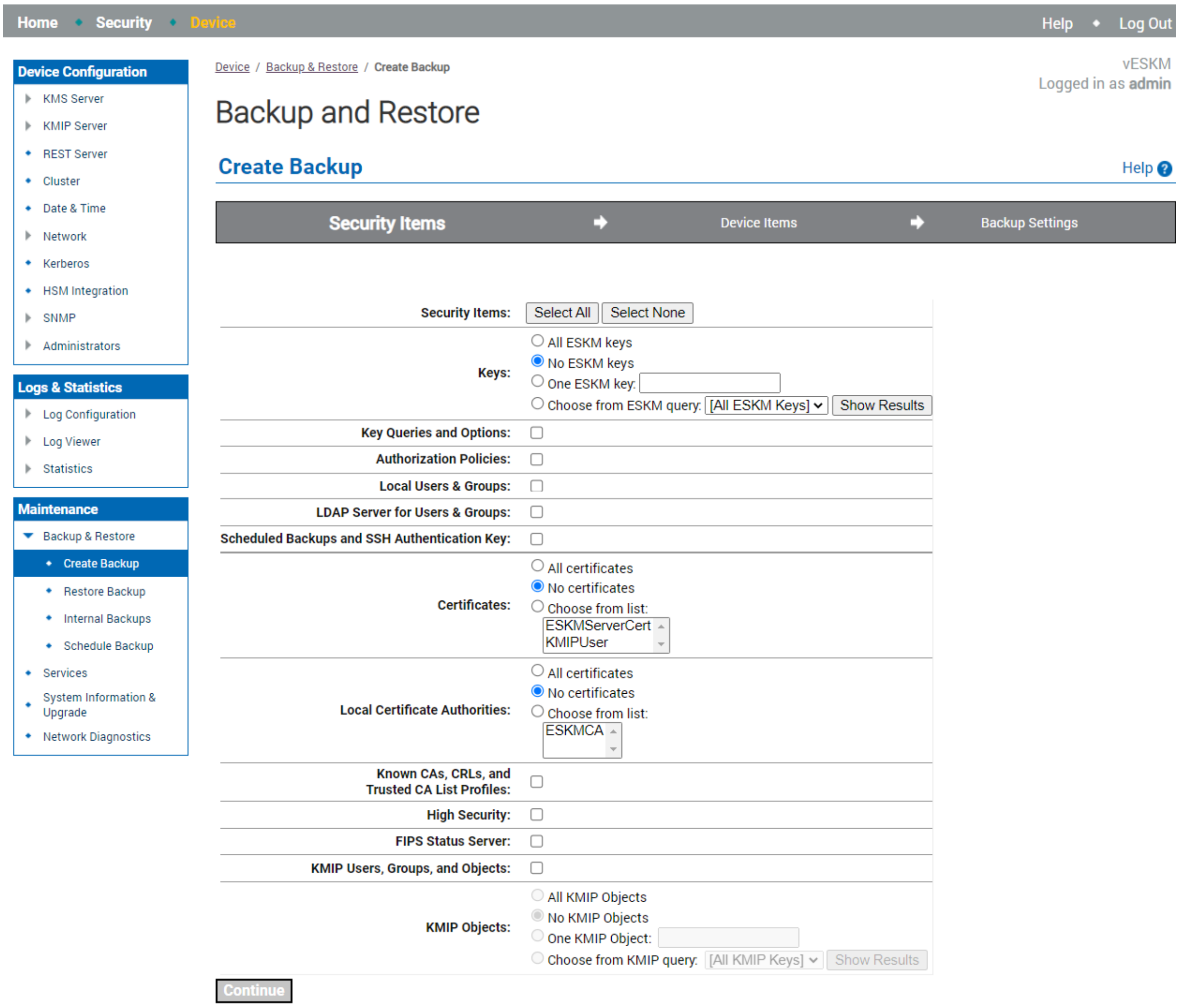
Restoring Local Users & Groups is also an additive process. If there are users in ESKM with the same name as users in the backup, those users will not be restored.

⚠ Since ESKM supports SSH Public Key authentication with SCP selected as backup option for creating the backup, the backup will be created even without a password, provided the SSH Public Key that is displayed in the Remote

Administration section (**Device** > **Device Configuration** > **Administrators** > **Remote Administration**), is installed in the remote device where you intend to take the backup.

5.2.1.1 Create backup: security items

Use this section to select the security items to include in your backup.



Security Items:	Select All Select None
Keys:	○ All ESKM keys ● No ESKM keys ○ One ESKM key: ○ Choose from ESKM query: [All ESKM Keys] Show Results
Key Queries and Options:	□
Authorization Policies:	□
Local Users & Groups:	□
LDAP Server for Users & Groups:	□
Scheduled Backups and SSH Authentication Key:	□
Certificates:	○ All certificates ● No certificates ○ Choose from list: ESKMServerCert KMIPUser
Local Certificate Authorities:	○ All certificates ● No certificates ○ Choose from list: ESKMCA
Known CAs, CRLs, and Trusted CA List Profiles:	□
High Security:	□
FIPS Status Server:	□
KMIP Users, Groups, and Objects:	□
KMIP Objects:	○ All KMIP Objects ● No KMIP Objects ○ One KMIP Object: ○ Choose from KMIP query: [All KMIP Keys] Show Results

Figure 31 : Create Backup-Security Items

The following table describes the components of Create Backup: Security Items.

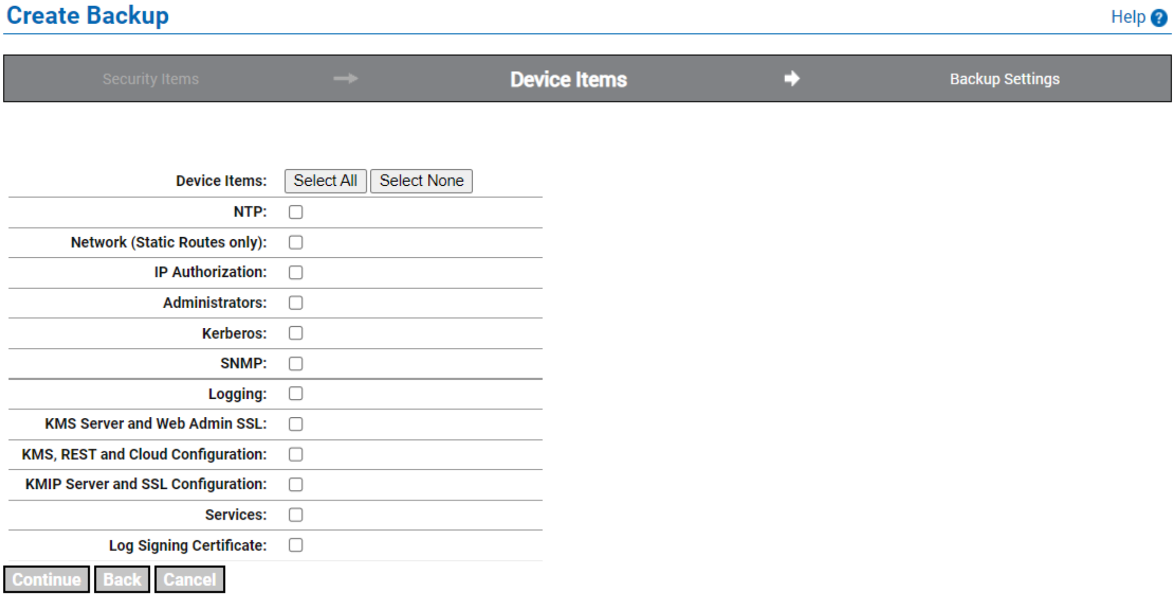
Table 4: Create Backup: Security Items components

Components	***Description***
Security Items	Click **Select All** to include all of the key management items in your backup. Click **Select None** to deselect all key management items.
Keys	Select the method for backing up KMS keys. Select to backup all, none, or a specific key. KMIP keys are backed up when the **KMIP Users, Groups, and Objects** field is checked. ⚠ Only ESKM keys can be backed up in this section.
Show Results	Click **Show Results** to view the results of the selected ESKM key query. You can use this button to learn which keys will be saved in your backup if you select keys based on query.
Key Queries and Options	Select to backup all key queries and options on the appliance.
Authorization Policies	Select to backup all authorization policies on the appliance.
Local Users & Groups	Select to back up all local KMS users and KMS groups on the appliance. If you select this component without selecting the **KMIP Users, Groups and Objects** component, then only the KMS user and group properties will be backed up. If you want to backup and restore all users (both KMS-only users and KMIP users) and all groups (both KMS and KMIP), select both **Local Users & Groups** and **KMIP Users, Groups and Objects**.
LDAP Server for Users & Groups	Select to backup the LDAP server configuration.

Components	***Description***
Scheduled Backups and SSH Authentication Key	Select to backup the scheduled backup backups configuration and SSH Authentication Key.
Certificates	Select the method for backing up certificates. Select to either backup all, none, or specific certificates.
Local Certificate Authorities	Select the method for backing up local certificate authorities. Select to either backup all, none, or specific certificates.
Known CAs, CRLs, and Trusted CA List Profiles	Select to backup all known CAs, CRLs, and trusted CA list profiles.
High Security	Select to backup the device's high security settings.
FIPS Status Server	Select to backup the FIPS status server configuration.
KMIP Users, Groups, and Objects	Select to backup KMIP components. This includes KMIP-enabled users and KMIP groups. This will also include KMIP-managed objects based on the configuration of "KMIP Objects". ⚠ If you select the **KMIP Users, Groups, and Objects** without selecting **Local Users & Groups**, the backup will contain only KMIP-enabled users and KMIP groups. It will not contain the KMS-only (non-KMIP-enabled) users or KMS user groups.
KMIP Objects	Select to backup KMIP objects. After selecting this option, you can specify whether you want to backup all KMIP objects, no KMIP objects, a specific KMIP object (by specifying the UUID), or run a KMIP query to backup the results.
Continue	Click **Continue** to configure the next group of items..

5.2.1.2 Create backup: device items

Use this section to select the device items to include in your backup.



Device Items:	
NTP:	□
Network (Static Routes only):	□
IP Authorization:	□
Administrators:	□
Kerberos:	□
SNMP:	□
Logging:	□
KMS Server and Web Admin SSL:	□
KMS, REST and Cloud Configuration:	□
KMIP Server and SSL Configuration:	□
Services:	□
Log Signing Certificate:	□

Figure 32 : Create Backup: Device Items

The following table describes the components of Create Backup: Device Items.

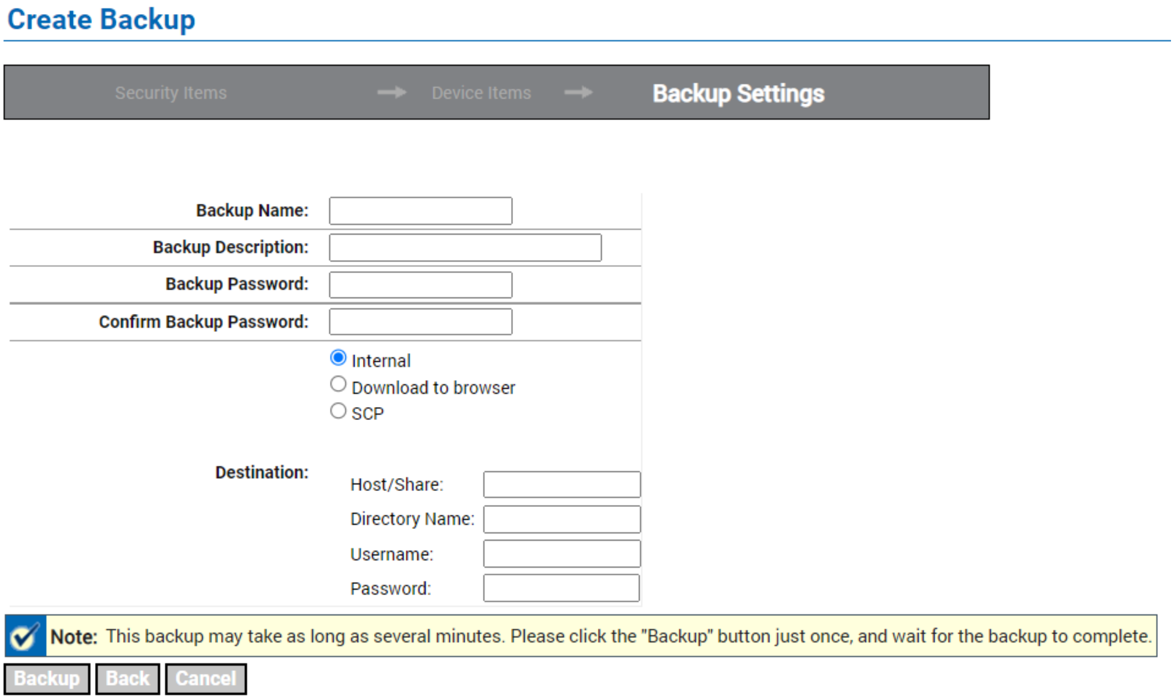
Table 5: Create Backup: Device Items components

Components	***Descriptiom***
Device Items	Click **Select All** to include all of the device configuration items in your backup. Click **Select None** to deselect all device configuration items.
NTP, Network (Static Routes Only), IP Authorization, Administrators, Kerberos, SNMP, Logging, KMS Server and Web Admin SSL, KMS Server Configuration, KMIP Server and SSL Configuration, Services, Log Signing Certificate	Select the corresponding check box to include this configuration information in the backup.
Continue	Click **Continue** to configure the next group of items.

Components	***Descriptiom***
Back	Click **Back** to return to the previous section.
Cancel	Click **Cancel** to abort the backup and return to the **Create Backup: Security Items** section.

5.2.1.3 Create backup: backup settings

Use this section to specify the name, password, and location of the backup and review its contents.



Create Backup

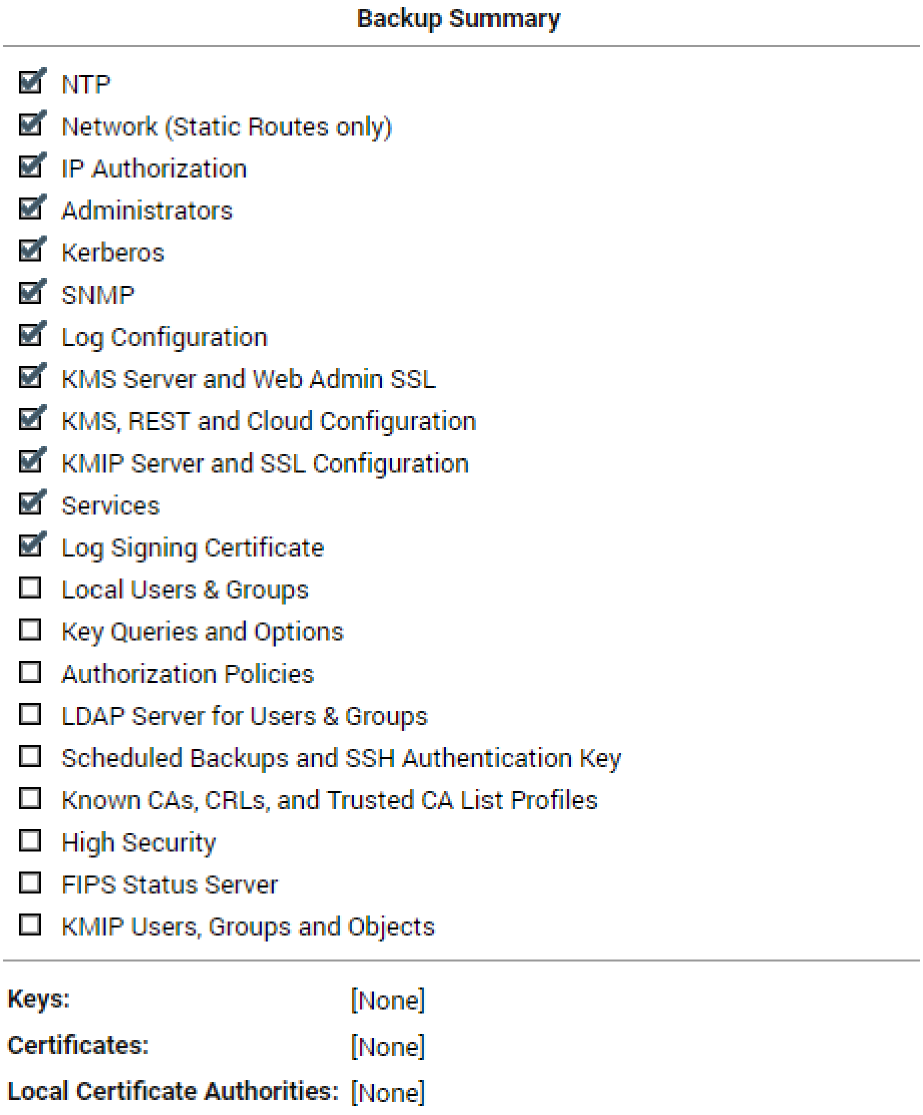
Security Items → Device Items → **Backup Settings**

Backup Name:	
Backup Description:	
Backup Password:	
Confirm Backup Password:	
Destination:	● Internal ○ Download to browser ○ SCP Host/Share: Directory Name: Username: Password:

✓ **Note:** This backup may take as long as several minutes. Please click the "Backup" button just once, and wait for the backup to complete.

Figure 33 : Create Backup: Backup Settings

The Backup Summary shows which items will be included in the backup.



Backup Summary

- ☑ NTP
- ☑ Network (Static Routes only)
- ☑ IP Authorization
- ☑ Administrators
- ☑ Kerberos
- ☑ SNMP
- ☑ Log Configuration
- ☑ KMS Server and Web Admin SSL
- ☑ KMS, REST and Cloud Configuration
- ☑ KMIP Server and SSL Configuration
- ☑ Services
- ☑ Log Signing Certificate
- □ Local Users & Groups
- □ Key Queries and Options
- □ Authorization Policies
- □ LDAP Server for Users & Groups
- □ Scheduled Backups and SSH Authentication Key
- □ Known CAs, CRLs, and Trusted CA List Profiles
- □ High Security
- □ FIPS Status Server
- □ KMIP Users, Groups and Objects

Keys:	[None]
Certificates:	[None]
Local Certificate Authorities:	[None]

Figure 34 : Backup Summary

The following table describes the components of Create Backup: Backup Settings.

Table 6: Create Backup: Backup Settings components

Components	***Description***
Backup Name	Enter a name for the backup file. The maximum length for the name is 25 characters. The system appends the date and time of the backup file creation, to the name. For backups stored externally, the backup filename is created by appending **_0_bkp** to the backup name. For large backups, the zero is incremented by 1 for each additional file. For example, the backup named "prod" could consist of two files: **prod_0_bkp** and **prod_1_bkp**.
Backup Description	Enter a short description for the backup. The maximum length for the description is 256 characters.
Backup Password	Enter a password for your backup configuration. ❗ The backup configuration cannot be restored without this password.
Confirm Backup Password	Confirm the password for your backup configuration.

<table>
<tr><th><em>Components</em></th><th><em>Description</em></th></tr>
<tr><td>Destination</td><td>
<p>Specify the destination information. The backup configuration can be stored internally on the Enterprise Secure Key Manager, downloaded to a browser, or copied to another machine via SCP with password or SCP with SSH Public Key Authentication. It can also be copied to a Windows share (supporting SMB version 3.0 or higher) when the device is in FIPS or Non FIPS compliant mode. You can find the behavior of windows share in the below table.</p>
<table>
<tr><th><em>FIPS Mode</em></th><th><em>Kerberos Configured</em></th><th><em>Manual backup/restore</em></th></tr>
<tr><td>Yes</td><td>Yes</td><td>Windows share (Kerberos)</td></tr>
<tr><td>Yes</td><td>No</td><td>No option for windows share</td></tr>
<tr><td>No</td><td>Yes</td><td>Windows share (Kerberos)</td></tr>
<tr><td>No</td><td>No</td><td>Windows Share</td></tr>
</table>
<ul><li>If you are creating this backup in anticipation of doing a software upgrade immediately, Utimaco recommends that you store the backup file externally.</li></ul>
<p>If you download the backup configuration to a browser, the backup configuration is encrypted and downloaded to your local machine. You must specify a name for the file; however, it is not necessary to specify an extension for the file. If you select SCP or Windows share or Windows share (Kerberos) to copy the backup configuration to another machine, you must provide the following information:</p>
</td></tr>
</table>

Components	*Description*
	- **Destination host:** If the destination is SCP, IPv4 or IPv6 addresses can be specified. If the destination is Windows Share or Windows Share (Kerberos), you need to provide the network path of share in '\\fqdn\share' format. (eg. \\myhost.example.com\myshare). When the Kerberos authentication is not used, network path can also be specified in '\\ip-address\share' format (eg. \\10.222.178.24\myshare). - **Directory name:** Name of the directory on the destination host; the file name can contain path information (You must have write permission for this directory). - **Username:** In case of Windows share (Kerberos), username should be logon name (eg. labuser). But in case of Windows share, username should be in UPN format (eg. labuser@eskmlab.com). - **Password:** The password for the user account on the destination host. ⚠ The ESKM appliance can back up files to a remote host that has an IPv6 address, when IPv6 is enabled on it (see ipv6 enable (p. 693)) and SCP is used to send the files.
Backup	Click **Backup** to create the backup.
Back	Click **Back** to return to the previous section.
Cancel	Click **Cancel** to abort the backup and return to the Create Backup: Security Items section.
Backup Summary	Displays all of the items that could possibly be backed up and indicates the items to be included in your backup configuration.

5.2.2 Restore backup

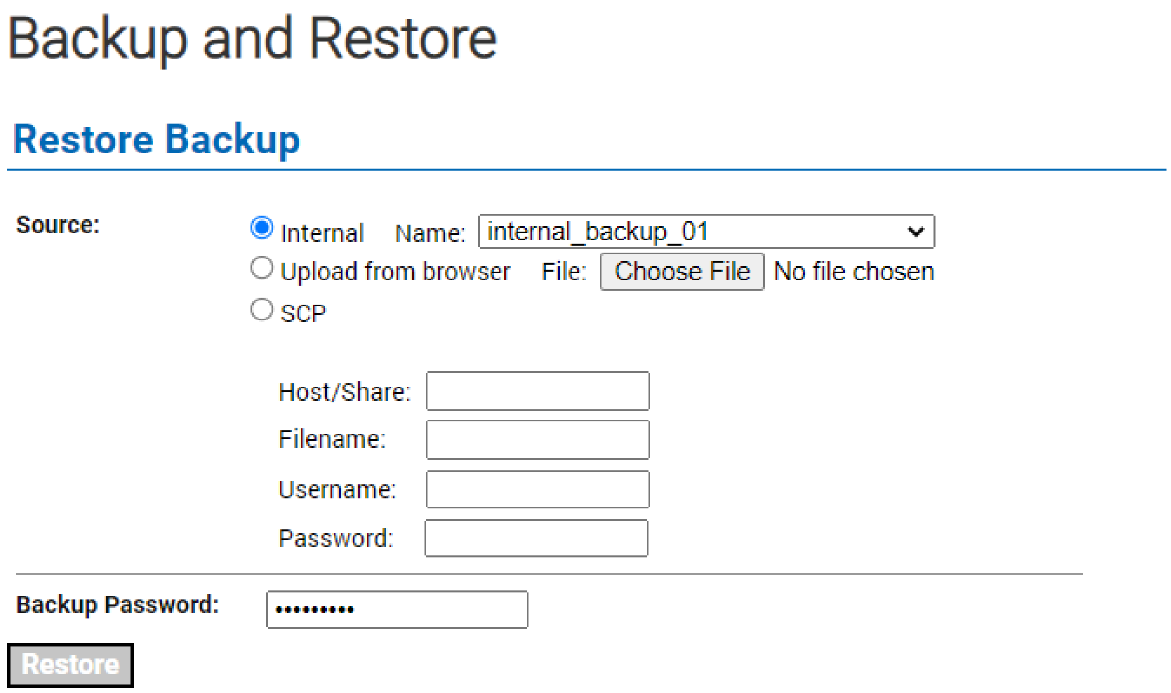
Use the Restore Backup section of the Backup and Restore page to restore data from a backup file.

Restoring a backup that contains KMIP users, groups and objects overwrites all existing KMIP users, groups and objects.

Do not attempt to perform a restore while a backup is in progress. Make sure that any previous backup has completed successfully, i.e. check the audit log for a created backup record, prior to performing a restore.

When the ESKM appliances are clustered, you should only perform a restore on one appliance at a time. After you restore a backup configuration, you must restart the appliance for the changes to take effect. Clicking the Continue button does not restart the ESKM appliance.

If the device is in cluster, all the cluster members should be active to restore a backup. When a backup is restored, the security items will be replicated to all other cluster nodes.



Backup and Restore

Restore Backup

Source:
● Internal Name: internal_backup_01
○ Upload from browser File: Choose File No file chosen
○ SCP

Host/Share:
Filename:
Username:
Password:

Backup Password: •••••••••

Figure 35 : Restore Backup

The following table describes the components of Restore Backup.

Table 7: Restore Backup components

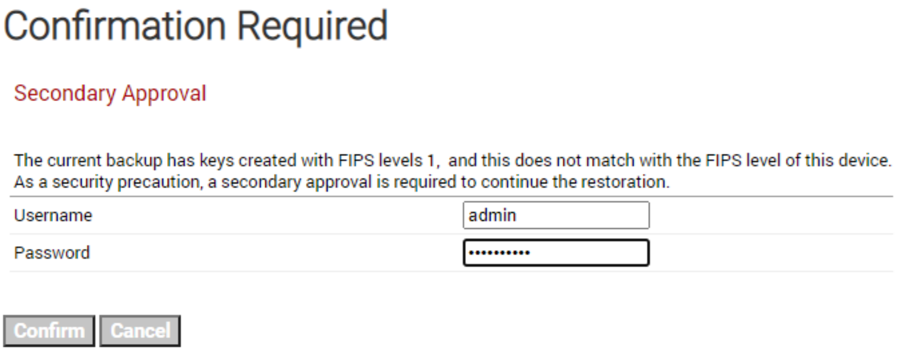
<table>
<tr><th><em>Components</em></th><th><em>Description</em></th></tr>
<tr><td>Source</td><td>
<p>Specify the source of the backup configuration. When restoring a backup that spans multiple files, specify the zero-th file here (for example, internal _0_bkp). Specifying the zero-th file indicates to the ESKM appliance that the backup contains multiple files. The ESKM appliance will then automatically transfers all of the backup files.</p>
<p>The backup configuration might be stored internally or on another machine. If the backup configuration is stored locally, you can select it from the drop-down under the Internal option. If the backup configuration is stored on another machine, you can either upload the file through the browser or you can copy the file to the ESKM appliance via SCP. When the device is operating in either non-FIPS compliant mode or FIPS compliant mode, it is also possible to upload the backup from a Windows share or Windows share (Kerberos) supporting SMB version 3.0 or higher.</p>
<p>You can find the behavior of windows share in the below table.</p>
<table>
<tr><th><em>FIPS Mode</em></th><th><em>Kerberos</em></th><th><em>ConfiguredManual backup/restore</em></th></tr>
<tr><td>Yes</td><td>Yes</td><td>Windows share (Kerberos)</td></tr>
<tr><td>Yes</td><td>No</td><td>No option for windows share</td></tr>
<tr><td>No</td><td>Yes</td><td>Windows share (Kerberos)</td></tr>
<tr><td>No</td><td>No</td><td>Windows Share</td></tr>
</table>
<p>If you are copying the backup configuration to your ESKM appliance via SCP or Windows share, you must provide the following information:</p>
</td></tr>
</table>

Components	***Description***
	▪ **Source host:** If the Source is SCP, IPv4 or IPv6 addresses can be specified. If the Source is Windows Share or Windows Share (Kerberos), you need to provide the network path of share in '\\fqdn\share' format. (eg. \\myhost.example.com\myshare). When the Kerberos authentication is not used, network path can also be specified in '\\ip-address\share' format (eg. \\10.222.178.24\myshare). ▪ **Filename:** The name of the file on the source host. For backups that span multiple files, enter the <backupname>_0_bkp file here. The system will then upload all of the <backupname> files in that directory. ▪ **Username:** In case of Windows share (Kerberos), username should be logon name (eg. labuser). But in case of Windows share, username should be in UPN format (eg. labuser@eskmlab.com). ▪ **Password:** The password for the user account on the source host. ⚠ Backup files larger than 100 MB cannot be transferred through the browser. You can use SCP or Windows share to upload these files. ⚠ The ESKM appliance can restore backup files from a remote host that has an IPv6 address, when IPv6 is enabled on it (see **ipv6 enable** (p. 693)) and SCP is used to receive the backup files.
Backup Password	Enter the backup configuration password.
Restore	Click **Restore** to restore the backup configuration. After the restore completes, you must manually restart the appliance for the restore to take effect, see **Restart/halt** (p. 195).

When the user clicks the the **Restore** button after entering the backup password, the Backup Restore Information section (p. 181) appears.

When the user clicks the **Restore** button after entering the backup password in the **Backup Restore Information** section, the backup file is restored. If one or more keys in the backup file are created on an ESKM appliance that complies to a different FIPS level compared to the device on which it is restored, a new screen will appear to obtain secondary approval from a user with high access.

- If the current user is not a high access user, then the credentials of a user with high access are requested, as shown in the screen below.



Confirmation Required

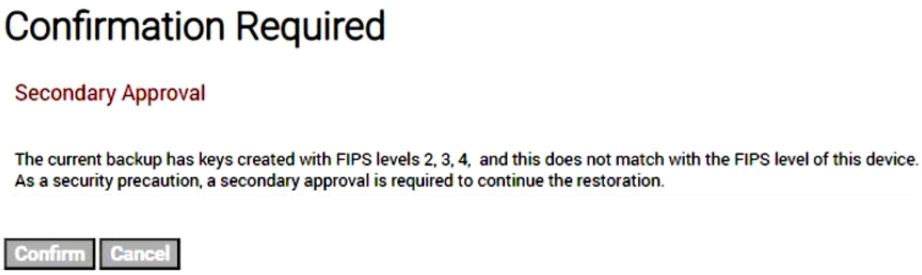
Secondary Approval

The current backup has keys created with FIPS levels 1, and this does not match with the FIPS level of this device.
As a security precaution, a secondary approval is required to continue the restoration.

Username	admin
Password	••••••••••

Figure 36 : Confirmation with credential

- If the current user is already an high access user, then the user only needs to click on **Confirm** button as shown in screen below.



Confirmation Required

Secondary Approval

The current backup has keys created with FIPS levels 2, 3, 4, and this does not match with the FIPS level of this device.
As a security precaution, a secondary approval is required to continue the restoration.

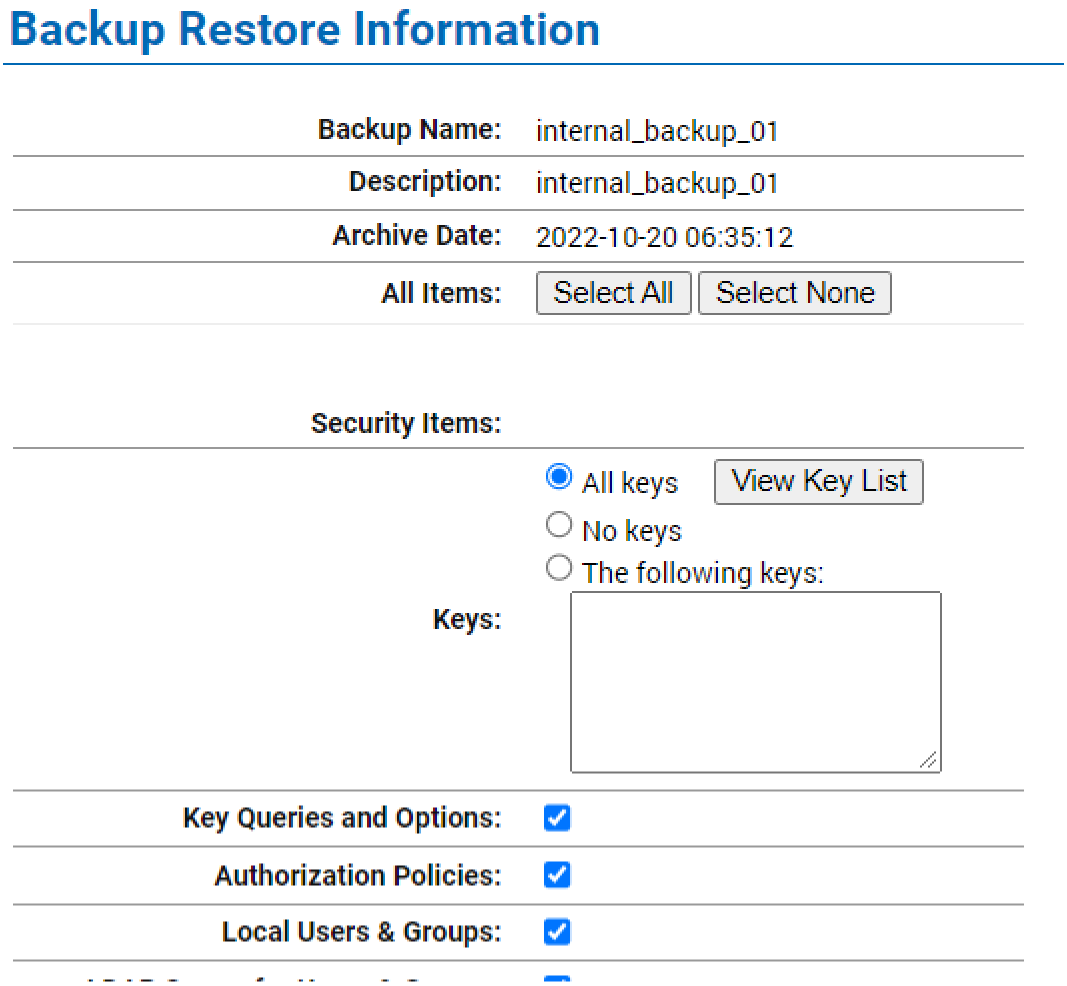
In case the user does not want to have keys with a different tag, the user can use the **back** button to navigate back, uncheck the keys and continue with restoration.

While restoring a key to the ESKM appliance, the key must conform to the appliance's current **Number of Active Versions Allowed for a Key** setting field located on the Key and Policy Configuration page. If the key has more active versions than permitted by that setting, the key restore will fail.

To restore a key with more active versions than the system allows, you must change the **Number of Active Versions Allowed** for a Key setting before restoring the backup. You can then reduce the key's active versions and return the Number of Active Versions Allowed for a Key to its original value.

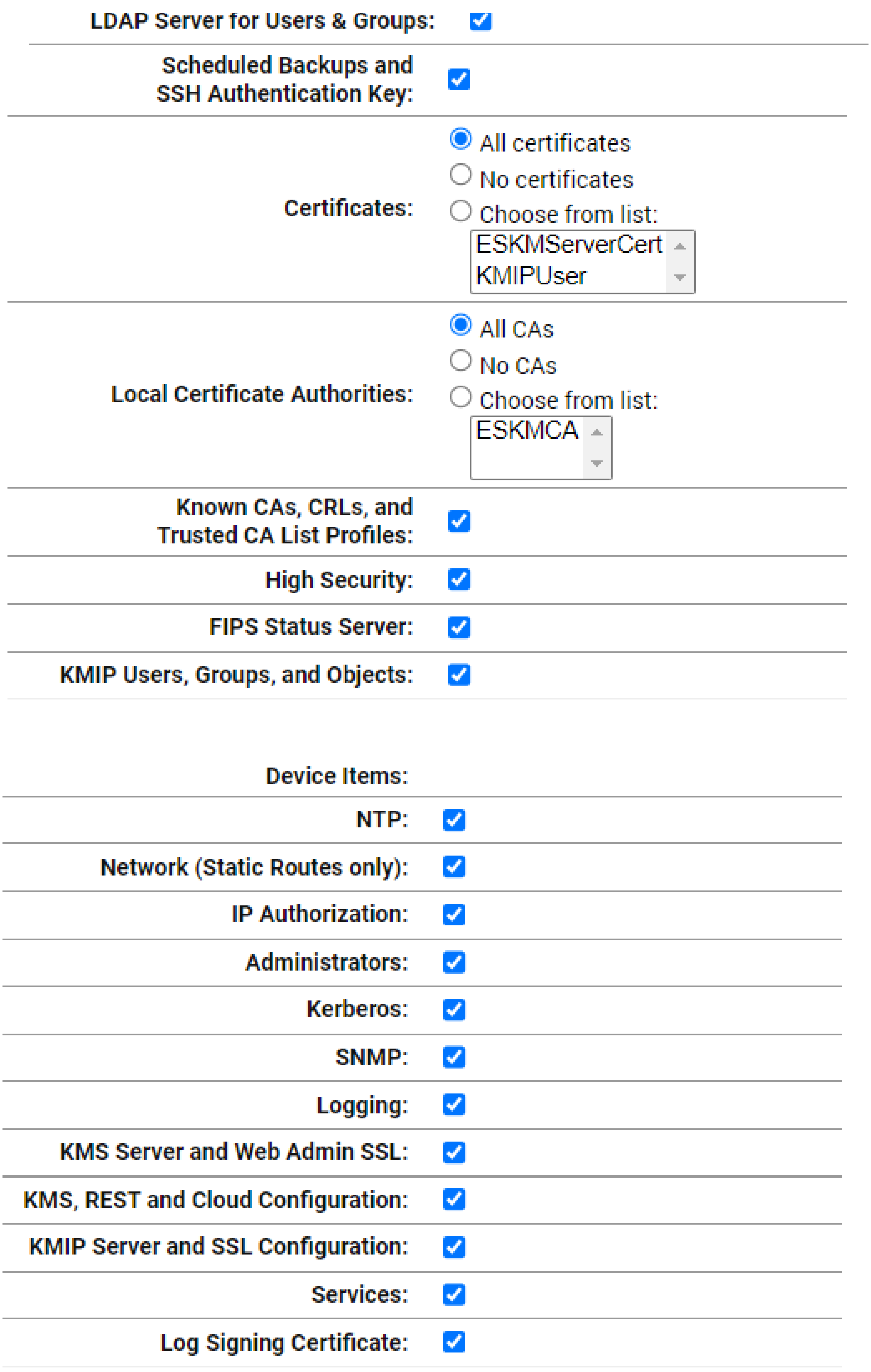
5.2.3 Backup and restore information

The **Backup Restore Information** of the Backup and Restore page provides a list of contents in a given backup file. You can select the individual items to include in the backup.



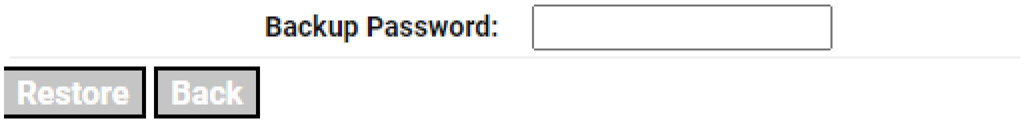
Backup Restore Information

Backup Name:	internal_backup_01
Description:	internal_backup_01
Archive Date:	2022-10-20 06:35:12
All Items:	Select All / Select None
Security Items:	
Keys:	● All keys ○ No keys ○ The following keys:
Key Queries and Options:	☑
Authorization Policies:	☑
Local Users & Groups:	☑



LDAP Server for Users & Groups:	☑
Scheduled Backups and SSH Authentication Key:	☑
Certificates:	● All certificates ○ No certificates ○ Choose from list: ESKMServerCert KMIPUser
Local Certificate Authorities:	● All CAs ○ No CAs ○ Choose from list: ESKMCA
Known CAs, CRLs, and Trusted CA List Profiles:	☑
High Security:	☑
FIPS Status Server:	☑
KMIP Users, Groups, and Objects:	☑

Device Items:	
NTP:	☑
Network (Static Routes only):	☑
IP Authorization:	☑
Administrators:	☑
Kerberos:	☑
SNMP:	☑
Logging:	☑
KMS Server and Web Admin SSL:	☑
KMS, REST and Cloud Configuration:	☑
KMIP Server and SSL Configuration:	☑
Services:	☑
Log Signing Certificate:	☑



Backup Password:

Figure 37 : Backup and Restore Information

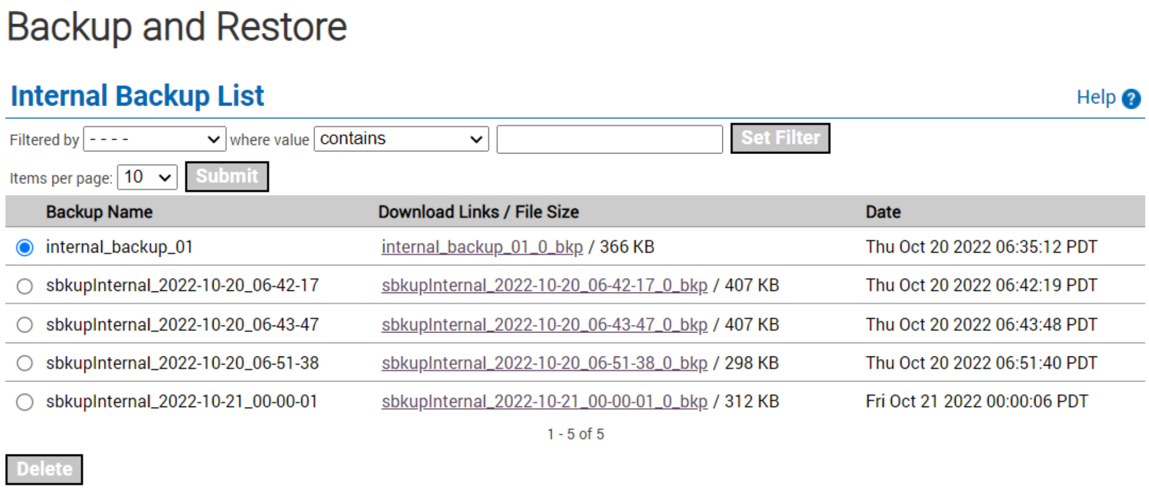
The following table describes the components of the Internal Backup List.

Table 8: Internal Backup List components

Components	***Description***
Backup Name	Displays the backup name.
Description	Displays a description of the backup file.
Archive Date	Displays the date on which the backup was created.
All Items	Click **Select All** to select all of the items included in the backup. Click **Select None** to deselect all of the items. You can then select specific security and device items.
Backup Password	Enter the backup password.
Restore	Click **Restore** to restore all of the selected items.
Back	Click **Back** to return to the Restore Backup section.

5.2.4 Internal backup list

The Internal Backup List of the Backup and Restore page provides a list of internal backup files.



Backup and Restore

Internal Backup List

Filtered by - - - - where value contains

Items per page: 10

	Backup Name	Download Links / File Size	Date
●	internal_backup_01	internal_backup_01_0_bkp / 366 KB	Thu Oct 20 2022 06:35:12 PDT
○	sbkupInternal_2022-10-20_06-42-17	sbkupInternal_2022-10-20_06-42-17_0_bkp / 407 KB	Thu Oct 20 2022 06:42:19 PDT
○	sbkupInternal_2022-10-20_06-43-47	sbkupInternal_2022-10-20_06-43-47_0_bkp / 407 KB	Thu Oct 20 2022 06:43:48 PDT
○	sbkupInternal_2022-10-20_06-51-38	sbkupInternal_2022-10-20_06-51-38_0_bkp / 298 KB	Thu Oct 20 2022 06:51:40 PDT
○	sbkupInternal_2022-10-21_00-00-01	sbkupInternal_2022-10-21_00-00-01_0_bkp / 312 KB	Fri Oct 21 2022 00:00:06 PDT

1 - 5 of 5

Figure 38 : Internal Backup List

The following table describes the components of the Internal Backup List.

Table 9: Internal Backup List components

Components	***Description***
Backup Name	Displays the backup name.
Download Links	Click to download an internal backup file to your browser. This feature enables you to move a previously created internal backup file to a secondary system.
File Size	Displays the size of the backup file.
Date	Displays the date on which the backup was created.
Delete	Click to remove the backup from the ESKM appliance.

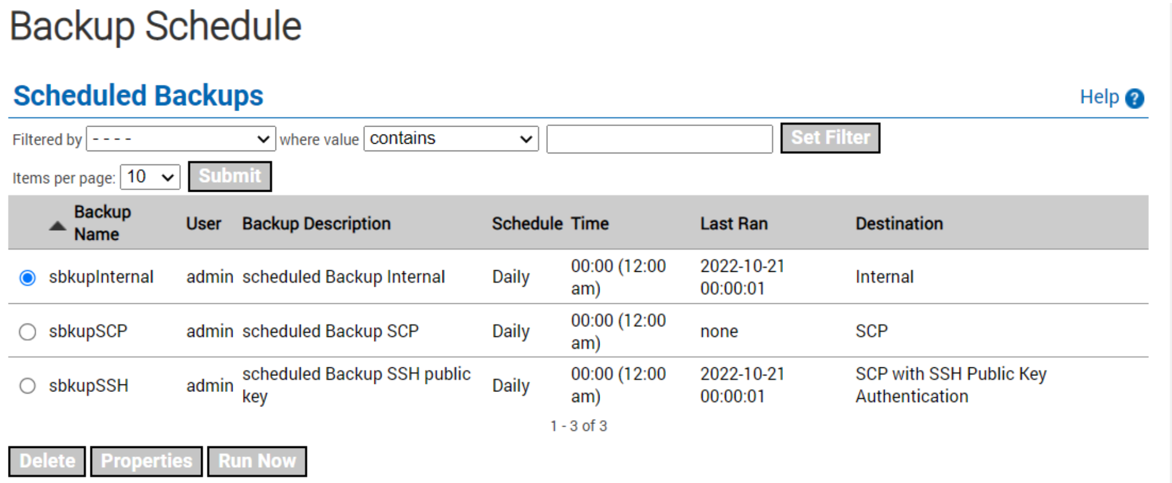
5.2.5 Schedule backup

Use the Schedule Backup page to create a new automated backup schedule, or to modify an existing backup schedule.

To view or change the properties of an existing scheduled backup file, click the radio button to the left of the scheduled backup file, and then click the **Properties** button.

To delete an existing scheduled backup file, click the radio button to the left of the scheduled backup file, and then click the **Delete** button.

- Users with backup restore permission, can edit the Scheduled backup.
- User cannot edit or delete the scheduled backup if the users have only the ACL permission for Administrative access, user must have permission on Backup & Restore ACL.



Backup Schedule

Scheduled Backups

	Backup Name	User	Backup Description	Schedule	Time	Last Ran	Destination
●	sbkupInternal	admin	scheduled Backup Internal	Daily	00:00 (12:00 am)	2022-10-21 00:00:01	Internal
○	sbkupSCP	admin	scheduled Backup SCP	Daily	00:00 (12:00 am)	none	SCP
○	sbkupSSH	admin	scheduled Backup SSH public key	Daily	00:00 (12:00 am)	2022-10-21 00:00:01	SCP with SSH Public Key Authentication

1 - 3 of 3

Figure 39 : Scheduled Backups

The following table describes the components of the Schedule Backup List.

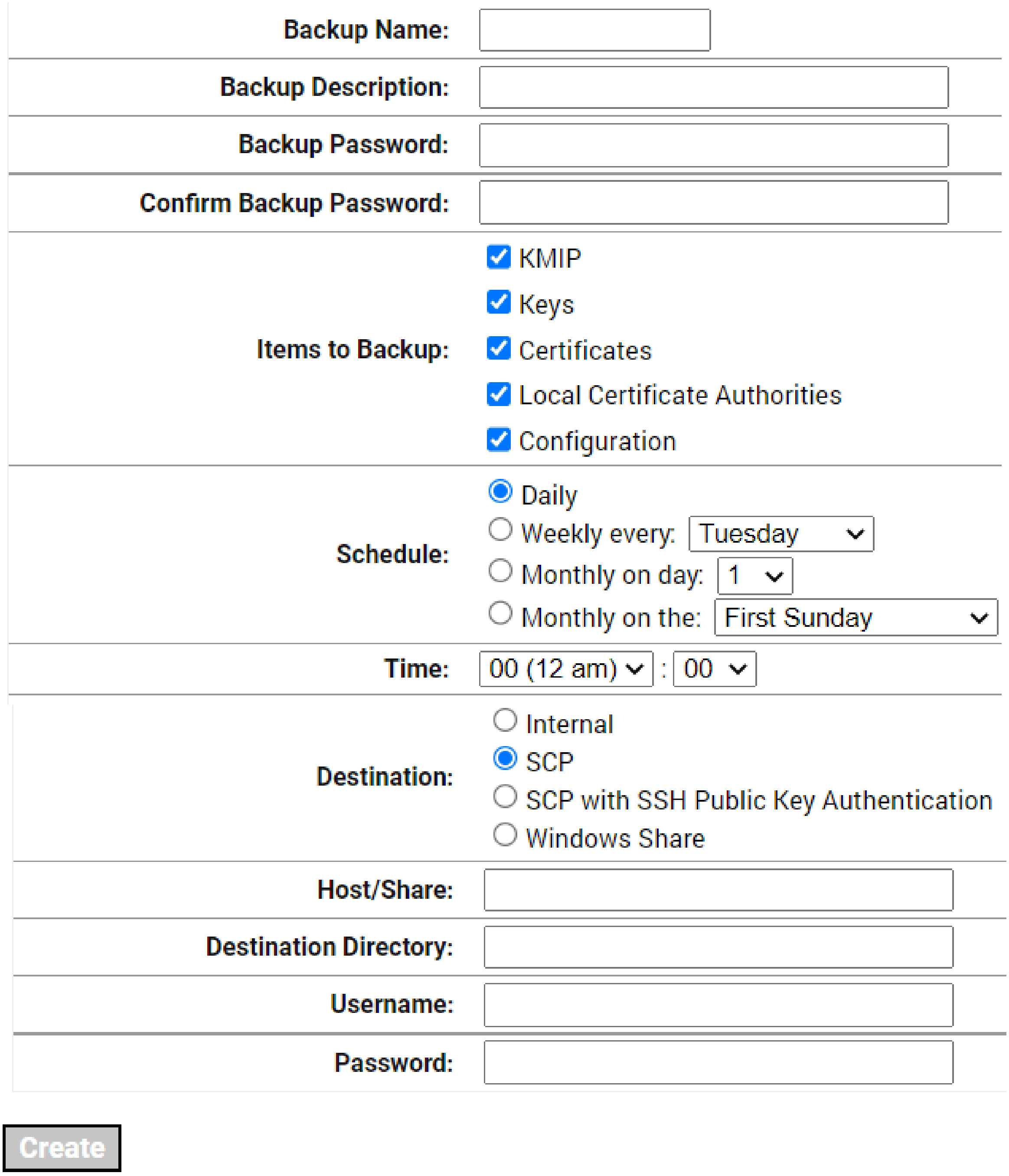
Table 10: Scheduled Backup List components

Components	***Description***
Backup Name	Displays the backup name.
User	Displays the username of the user who created the backup schedule.
Backup Description	Displays the description of the scheduled backup file.

Components	***Description***
Schedule	Displays when the backup will be performed.
Time	Displays the time when the backup will be performed.
Last Ran	Displays the date and time when the scheduled backup was last performed.
Destination	Displays where the backup is stored.
Delete	Click to delete the scheduled backup.
Properties	Click to view the properties of the scheduled backup.
Run Now	Click to initiate a backup at that instance. On successful initiation, the below note is displayed. ⚠ Backup initiated for <*Backup name*>. Please check audit log for more details.

Use the Schedule Backup feature to define what items will be backed up, when the backup will be performed, and where the backup file should be stored. After defining the backup schedule, click the **Create** button to save the backup schedule.

Schedule a Backup



Backup Name:	
Backup Description:	
Backup Password:	
Confirm Backup Password:	
Items to Backup:	☑ KMIP ☑ Keys ☑ Certificates ☑ Local Certificate Authorities ☑ Configuration
Schedule:	● Daily ○ Weekly every: Tuesday ○ Monthly on day: 1 ○ Monthly on the: First Sunday
Time:	00 (12 am) : 00
Destination:	○ Internal ● SCP ○ SCP with SSH Public Key Authentication ○ Windows Share
Host/Share:	
Destination Directory:	
Username:	
Password:	

Figure 40 : Schedule a Backup

The following table describes the components of Scheduling a Backup.

Table 11: Schedule a Backup-components

Components	***Description***
Backup Name	Enter a name for the backup file. The maximum length for the name is 25 characters. The system appends the date and time of the backup file creation, to the name. For backups stored externally, the backup filename is created by appending _0_bkp to the backup name. For large backups, the zero is incremented by 1 for each additional file. For example, a backup named "daily" could consist of two files: daily_0_bkp and daily_1_bkp.
Backup Description	Enter a short description for the backup. The maximum length for the description is 256 characters.
Backup Password	Enter a password for your backup configuration. ❗ The backup cannot be restored without this password.
Confirm Backup Password	Enter the password again.

Components	***Description***
Items to Back Up	KMIP, Keys, Certificates, Local Certificate Authorities and Configuration information. **Keys** includes only the KMS keys. **KMIP** includes KMIP-enabled users, KMIP groups, KMIP-managed objects and attributes, and associated privileges. Selecting KMIP without selecting Configuration will result in backing up only KMIP-enabled users and KMIP groups, but not the KMS-only (non KMIP-enabled) users or KMS groups. To back up all local users, select both **KMIP** and **Configuration**. **Configuration** items include the following: ▪ Local Users & Groups ▪ Key Queries and Options ▪ Authorization Policies ▪ LDAP Server for Users & Groups ▪ Scheduled Backups ▪ SCP with SSH Public Key Authentication ▪ High Security ▪ FIPS Status Server ▪ NTP ▪ Network ▪ IP Authorization ▪ Administrators ▪ Kerberos ▪ SNMP ▪ Log Configuration ▪ KMS Server and Web Admin SSL ▪ KMS and REST Server Configuration ▪ KMIP Server and SSL Configuration ▪ Services ▪ Log Signing Certificate

Components	***Description***
	⚠ The scheduled backup will not be created if the admin does not have the privilege to back up all the items that are defined in the scheduled backup. ⚠ The scheduled backup will not be performed if the admin no longer has the privilege to back up all the items that are scheduled to be backed up.
Schedule	When the backup will be performed. ⚠ If the "Month on Day" value does not exist in a specific month (for example February, 30 or 31), the backup will be performed on the last day of the month.
Time	The time of day (local ESKM appliance time) when the backup will be performed.

<table>
<tr><th><em>Components</em></th><th><em>Description</em></th></tr>
<tr><td>Destination</td><td>
<p>Specify the destination information. The backup configuration can be stored internally on the Enterprise Secure Key Manager, or copied to another machine via SCP with password or SCP with SSH Public Key Authentication. It can also be copied to a Windows share (supporting SMB version 3.0 or higher) when the device is operating in non-FIPS compliant mode.</p>
<p>You can find the behavior of windows share in the below table.</p>
<table>
<tr><th><em>FIPS Mode</em></th><th><em>Kerberos Configured</em></th><th><em>Manual backup/restore</em></th></tr>
<tr><td>Yes</td><td>Yes</td><td>Windows share (Kerberos)</td></tr>
<tr><td>Yes</td><td>No</td><td>No option for windows share</td></tr>
<tr><td>No</td><td>Yes</td><td>Windows share (Kerberos)</td></tr>
<tr><td>No</td><td>No</td><td>Windows Share</td></tr>
</table>
<p>⚠ Windows Share Backups can be scheduled irrespective of FIPS compliance and Kerberos configuration. However, the behavior of the backup at the scheduled time will be as per the table.</p>
<p>⚠ If you are creating this backup in anticipation of doing a software upgrade immediately, Utimaco recommends that you store the backup file externally.</p>
<p>If you select <strong>SCP</strong> or <strong>Windows Share</strong> to copy the backup configuration to another machine, you must provide the following:</p>
</td></tr>
</table>

Components	***Description***
	▪ **Destination host:** If the destination is SCP, IPv4 or IPv6 addresses can be specified. If the destination is Windows Share or Windows Share (Kerberos), you need to provide the network path of share in '\\fqdn\share' format. (eg. \\myhost.example.com\myshare) . When the Kerberos authentication is not used, network path can also be specified in '\\ip-address\share' format (eg. \\10.222.178.24\myshare). ▪ **Directory name:** The name of the directory on the destination host. (You must have write permission for this directory). ▪ **Username:** In case of Windows share (Kerberos), username should be logon name (eg. labuser). But in case of Windows share, username should be in UPN format (eg. labuser@eskmlab.com). ▪ **Password:** The password for the user account on the destination host. If you select **SCP with SSH Public Key Authentication**, to copy the backup configuration to another machine, it is enough to fill in the **Destination host**, **Directory name** and **Username**. Make sure that the another machine has the private key. For information on SSH Public Key, refer SSH Public Key (p. 505). ❗ If the device is FIPS compliant and Kerberos is not configured, "Scheduled Backups" with 'Windows Share' as destination will not work. ⚠ The ESKM appliance can back up files to a remote host which has an IPv6 address, when IPv6 is enabled on it (see ipv6 enable (p. 693)) and SCP is used to send the files.

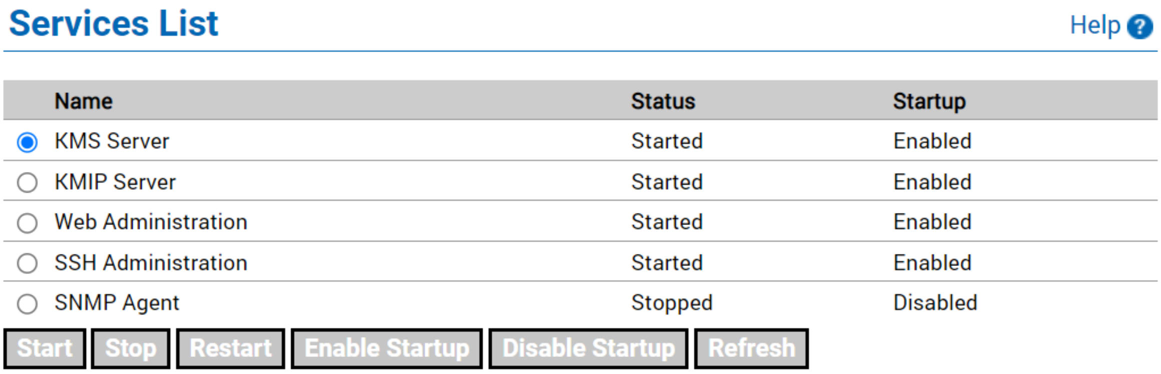
5.3 Services configuration page

Use the Services Configuration page to manage the types of services you want to activate or deactivate during the current session or when the ESKM appliance next boots up. This page contains the following sections:

- Services list (p. 193)
- Restart/halt (p. 195)

5.3.1 Services list

Use the Services List to view current configurations for the services on the ESKM appliance.



Services List

	Name	Status	Startup
●	KMS Server	Started	Enabled
○	KMIP Server	Started	Enabled
○	Web Administration	Started	Enabled
○	SSH Administration	Started	Enabled
○	SNMP Agent	Stopped	Disabled

Figure 41 : Services List

The following table describes the components of the Services List.

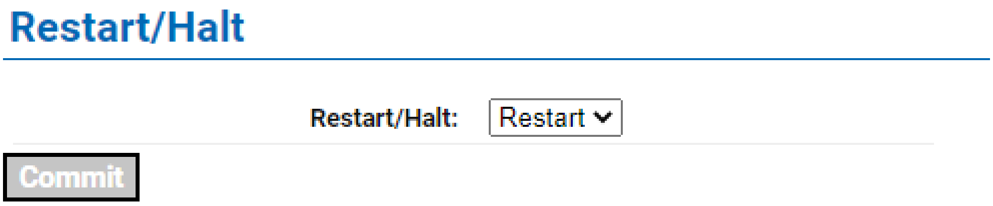
Table 12: Services List components

Components	***Description***
Name	- **KMS Server**: one of the two "brains" of the ESKM appliance, which manages all incoming and outgoing connections (both secure and clear text) using the XML protocol. When disabled, the server cannot be used to fulfill client requests over the XML protocol. - **KMIP Server**: the other "brain" of the ESKM appliance, which manages all incoming and outgoing connections over TLS using the Key Management Interoperability Protocol (KMIP). When disabled, the server cannot be used to fulfill client requests over the KMIP protocol. - **Web Administration**: When enabled, the ESKM appliance can be configured through a web browser. - **SSH Administration**: the remote Command Line Interface (CLI) administration tool. When enabled, the ESKM appliance can be configured using the remote CLI using SSH. - **SNMP Agent**: When enabled, the ESKM appliance sends alerts over the network to monitor the system activity.
Status	Current activity status of the service type, either started or stopped. You control the status by clicking **Start** or **Stop**.
Startup	The state of each of the services after the ESKM appliance boots up.
Start	Click **Start** to start a service. The status column of the Services List displays "Started" for the affected service type.
Stop	Click **Stop** to stop a service. The status column of the Services List displays "Stopped" for the affected service type.
Enable Startup	Click **Enable Startup** to specify that a service should be enabled on startup.

Components	*Description*
Disable Startup	Click **Disable Startup** to specify that a service should be disabled on startup.
Refresh	Click **Refresh** to refresh the values in this section.

5.3.2 Restart/halt

Use Restart/Halt to either shut down or re-start the ESKM appliance.



Restart/Halt

Restart/Halt: Restart

Figure 42 : Restart/Halt

The following table describes the components of Restart/Halt.

Table 13: Restart/Halt components

Components	*Description*
Restart/Halt	Select Restart to restart, or Halt to shutdown. ⚠ Using the restart and halt functions terminate all active connections to the ESKM appliance.
Commit	Click to perform the function selected in the Restart/Halt field.

Remove any peripheral devices connected to the keyboard, mouse, and video ports on the ESKM appliance before restarting. Use of these ports during the restart process can prevent the ESKM appliance from starting successfully.

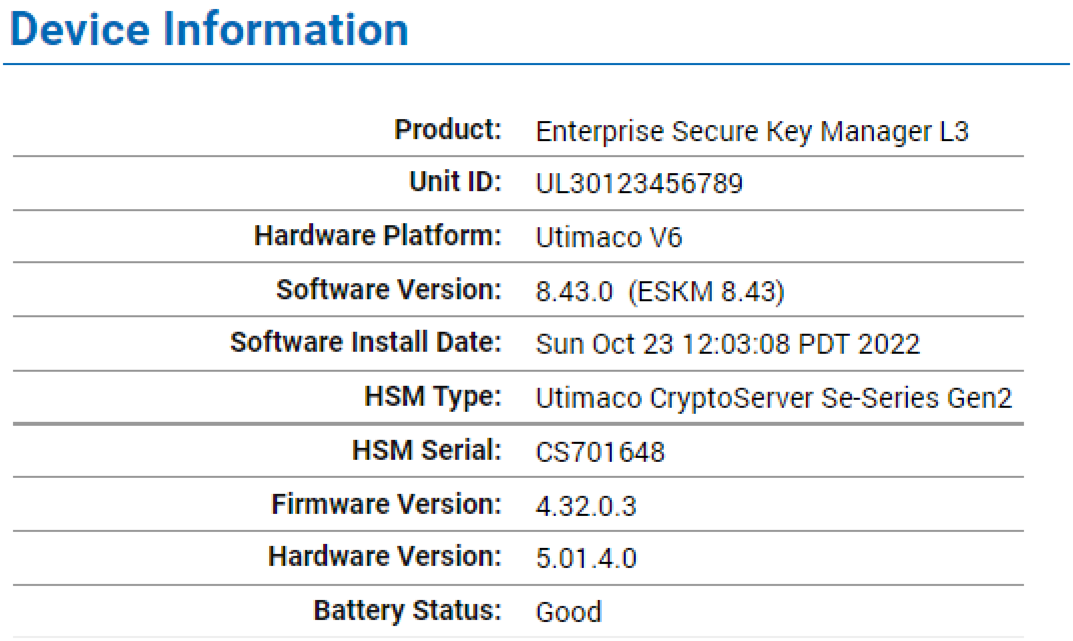
5.4 System information page

Use the System Information page to perform software upgrades and examine information about the system and software currently installed. This page contains the following sections:

- Appliance information (p. 196)
- Software upgrade/install (p. 203)

5.4.1 Device information

The **Device Information** section of the page shows the Unit ID, model of ESKM appliance, software version and software installation date.



Device Information

Product:	Enterprise Secure Key Manager L3
Unit ID:	UL30123456789
Hardware Platform:	Utimaco V6
Software Version:	8.43.0 (ESKM 8.43)
Software Install Date:	Sun Oct 23 12:03:08 PDT 2022
HSM Type:	Utimaco CryptoServer Se-Series Gen2
HSM Serial:	CS701648
Firmware Version:	4.32.0.3
Hardware Version:	5.01.4.0
Battery Status:	Good

Figure 43 : Device Information

The following table describes the components of Appliance Information.

Table 14: Appliance Information components

Components	***Description***
Product	The product name.
Unit ID	The Unit ID is composed of letters and numbers. The Unit ID is ten characters. You will be required to provide your Unit ID if you ever need to contact Utimaco Technical Support (p. 798).
Hardware Platform	Displays the model of the appliance that is running the ESKM software. ⚠ The term "hardware" also refers to the "virtual appliance".
Software Version	Displays the version of the ESKM software.
Software Install Date	Displays the date the ESKM software was installed.

⚠ The following table is applicable only for the ESKM L3 and L4 devices which have embedded HSM.

The following table describes the components of the **Appliance Information (HSM)**.

Table 15: Appliance Information components (HSM)

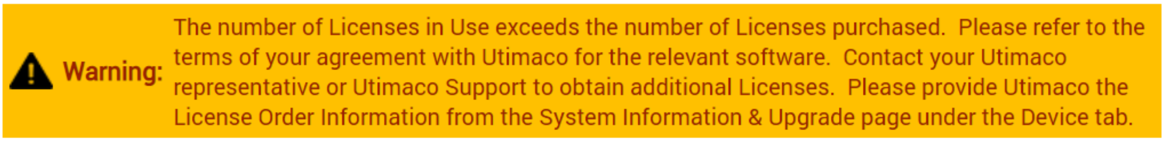
Component	***Description***
HSM Type	Displays the type of the embedded HSM.
HSM Serial	Displays the serial number of the embedded HSM.
Firmware Version	Displays the firmware version of the embedded HSM.

<table>
<tr><th>Component</th><th>Description</th></tr>
<tr><td>Hardware Version</td><td>Displays the hardware version of the embedded HSM.</td></tr>
<tr><td>Battery Status</td><td>Displays the battery status of the embedded HSM.
<table>
<tr><th>Battery status</th><th>Carrier battery</th><th>External battery</th></tr>
<tr><td>Good</td><td>OK</td><td>OK</td></tr>
<tr><td>Carrier Battery Low</td><td>Low</td><td>OK</td></tr>
<tr><td>External Battery Low/ Absent</td><td>OK</td><td>Low or Absent</td></tr>
<tr><td>Carrier and External Battery</td><td>Low</td><td>Low</td></tr>
</table>
</td></tr>
</table>

5.4.2 License information

A client license is required for each client or user enrolled in the ESKM cluster. Each ESKM appliance, by default, includes one client license. When the appliances are clustered, the number of appliances in the cluster establishes and aggregates the number of clients that can be enrolled.

If the number of clients to be enrolled exceeds the number of ESKM appliances you have purchased, a warning message appears.



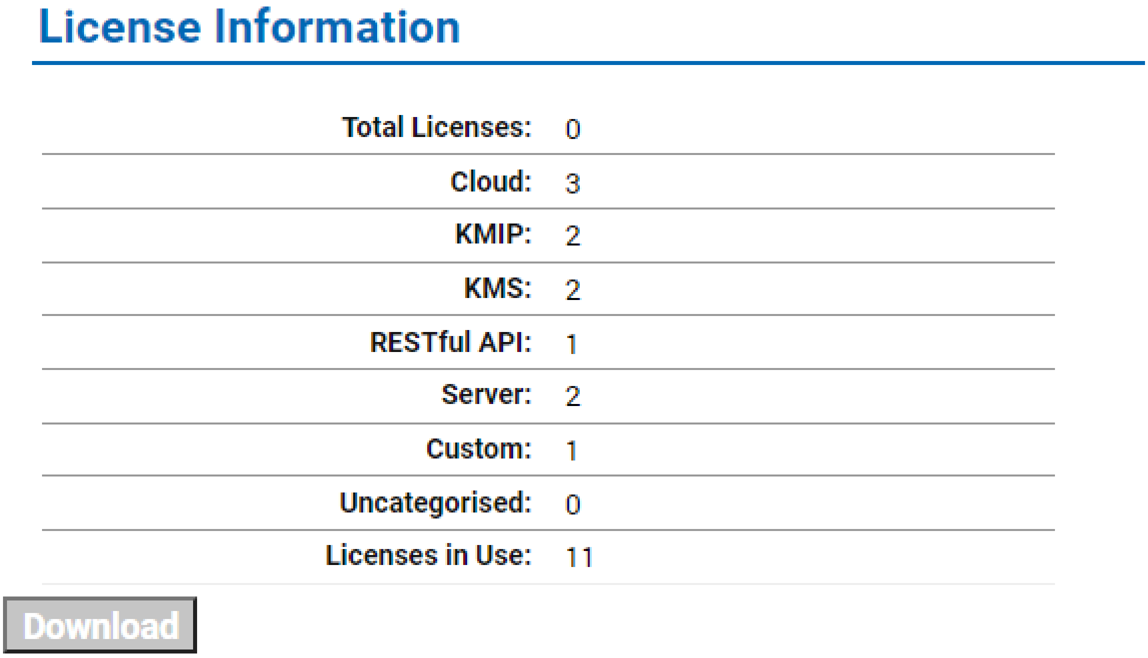
⚠ Warning: The number of Licenses in Use exceeds the number of Licenses purchased. Please refer to the terms of your agreement with Utimaco for the relevant software. Contact your Utimaco representative or Utimaco Support to obtain additional Licenses. Please provide Utimaco the License Order Information from the System Information & Upgrade page under the Device tab.

You must purchase and install a client license pack to allow these additional clients to be enrolled in the cluster. To order a license pack, contact Utimaco Sales or your reseller and provide the License order information (p. 200) from the ESKM appliance.

License packs are used to add additional cluster based licenses using the Management Console Software Upgrade/Install mechanism. When a license pack is installed, it replaces any previously installed license pack, and is automatically replicated to all current cluster members. Similarly, when an ESKM appliance is added to a cluster and synchronization is performed, if there is a license pack installed in the cluster, it is
replicated to the new appliance. When an ESKM appliance is removed from the cluster (using the Management Console), any existing license pack is removed from that ESKM appliance and it reverts to having one individual license.

Backup and Restore do not back up or restore license packs. As long as the cluster exists, any installed license pack will remain. If the entire cluster is lost, then the license pack for the cluster must be re-installed. License pack installation requires that the Unit ID of the ESKM appliance on which the license pack is installed must have been included in the generated license pack. When generating license packs, Utimaco
recommends specifying the Unit IDs of all ESKM appliances that will be in the cluster.

The License Information section displays the number of users that can be enrolled, and the number of users currently enrolled.



License Information

Total Licenses:	0
Cloud:	3
KMIP:	2
KMS:	2
RESTful API:	1
Server:	2
Custom:	1
Uncategorised:	0
Licenses in Use:	11

Figure 44 : License Information

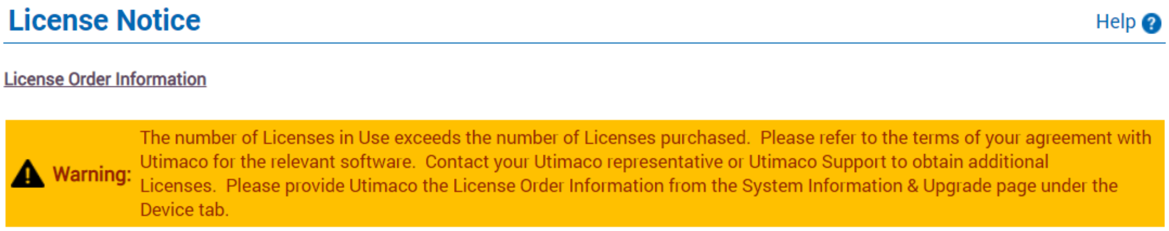
The following table describes the components of License Information.

Table 16: License Information components

Components	***Description***
Total Licenses	Displays the number of users who can be enrolled in the ESKM appliance.
Server	Displays the number of users under server license category.
KMIP	Displays the number of users under KMIP license category.
KMS	Displays the number of users under KMS license category.
Custom	Displays the number of users under custom license category.
Uncategorised	Displays the number of users who are not under any of the above license categories.
Licenses in Use	Displays the number of users currently enrolled in the ESKM appliance. ⚠ A warning message is generated when the number of enrolled users, exceeds the license value.
Download	Click **Download** to download the license information. ⚠ The downloaded license information .eml file can only be opened in Outlook.

5.4.3 License Order Information

To order additional licenses, you must provide Utimaco with information about your ESKM appliance. Click **License Order Information**.



License Notice

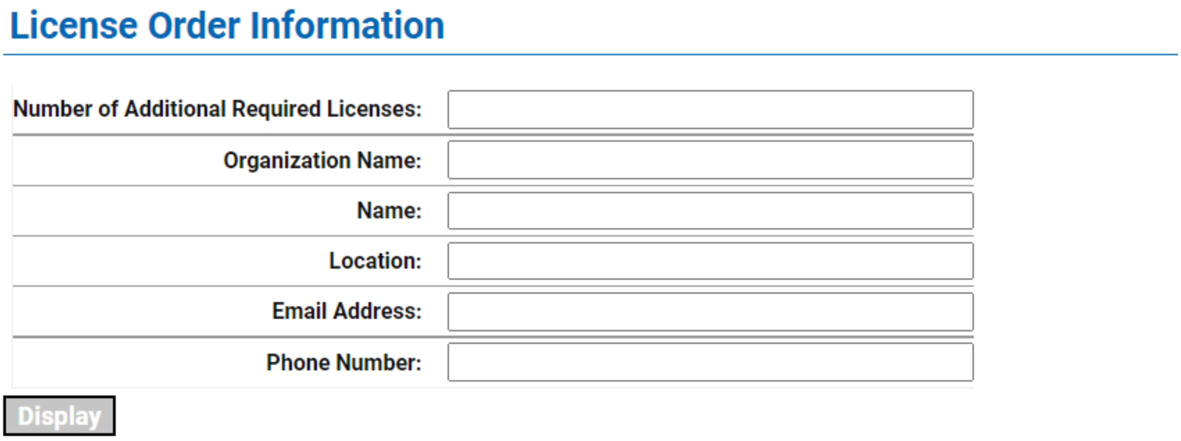
Help ?

License Order Information

⚠ Warning: The number of Licenses in Use exceeds the number of Licenses purchased. Please refer to the terms of your agreement with Utimaco for the relevant software. Contact your Utimaco representative or Utimaco Support to obtain additional Licenses. Please provide Utimaco the License Order Information from the System Information & Upgrade page under the Device tab.

Figure 45 : License Notice

Use the License Order Information to input your contact information.



License Order Information

Number of Additional Required Licenses:	
Organization Name:	
Name:	
Location:	
Email Address:	
Phone Number:	

Figure 46 : License Order Information

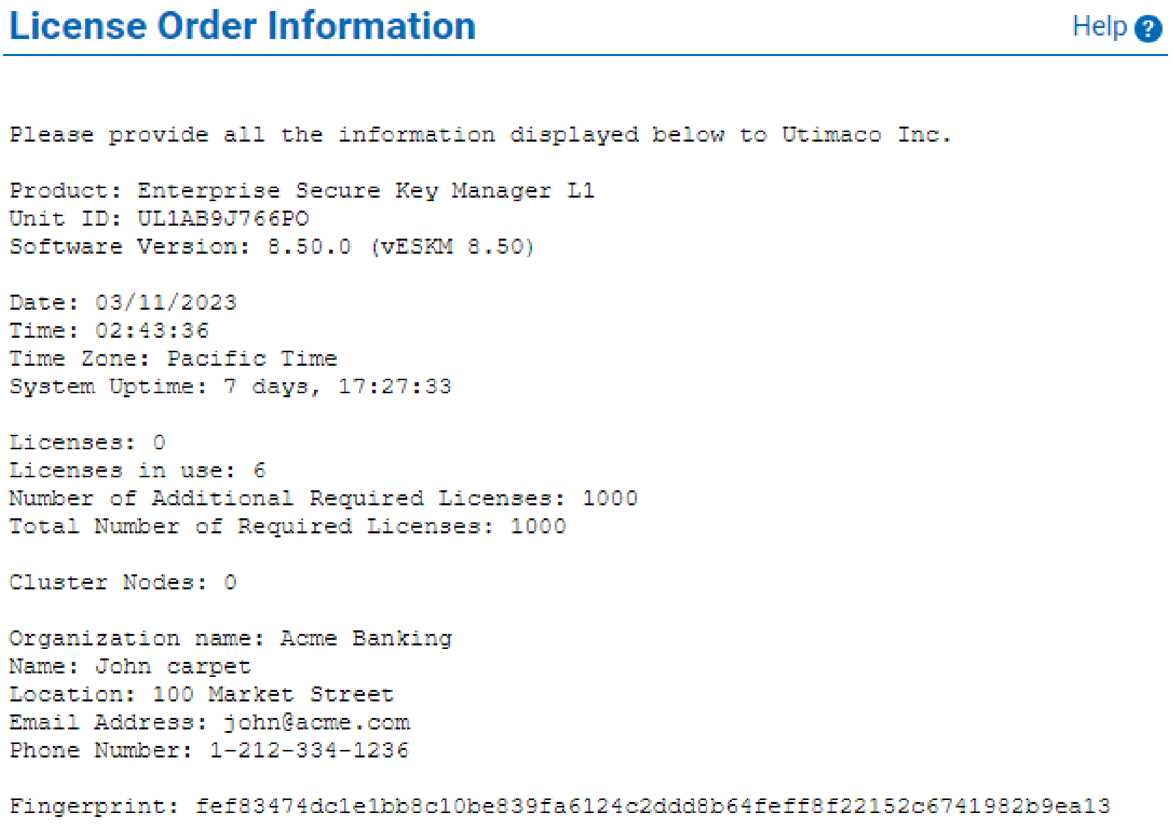
The following table describes the components of **License Order Information**.

Table 17: License Order Information components

Component	***Description***
Number of Additional Required Licenses	Input the number of additional users who will be enrolled in the ESKM appliance. You can also order additional licenses for future use.
Organization Name	Input the name of your organization or company.
Name	Input the name of the person who is purchasing additional licenses.

Component	***Description***
Location	Input the city, state, and country where the ESKM appliance is located.
Email Address	Input the email address of the person who is purchasing additional licenses.
Phone Number	Input the phone number of the person who is purchasing additional licenses.
Display	Click to obtain information on the ESKM appliance.

The following figure is an example of the information obtained from the ESKM system.



```
Please provide all the information displayed below to Utimaco Inc.

Product: Enterprise Secure Key Manager L1
Unit ID: UL1AB9J766PO
Software Version: 8.50.0 (vESKM 8.50)

Date: 03/11/2023
Time: 02:43:36
Time Zone: Pacific Time
System Uptime: 7 days, 17:27:33

Licenses: 0
Licenses in use: 6
Number of Additional Required Licenses: 1000
Total Number of Required Licenses: 1000

Cluster Nodes: 0

Organization name: Acme Banking
Name: John carpet
Location: 100 Market Street
Email Address: john@acme.com
Phone Number: 1-212-334-1236

Fingerprint: fef83474dc1e1bb8c10be839fa6124c2ddd8b64feff8f22152c6741982b9ea13
```

Figure 47 : License Order Information

Click **Download** and a .txt file is downloaded on your workstation. Alternately, you can copy and paste the license order information directly from the Management Console interface. If you do, be sure to include the **Fingerprint**. You must provide all of the license order information to Utimaco during the order for additional licenses.

> ⚠ The license order information data contains the Unit IDs of all ESKM appliances in the cluster.

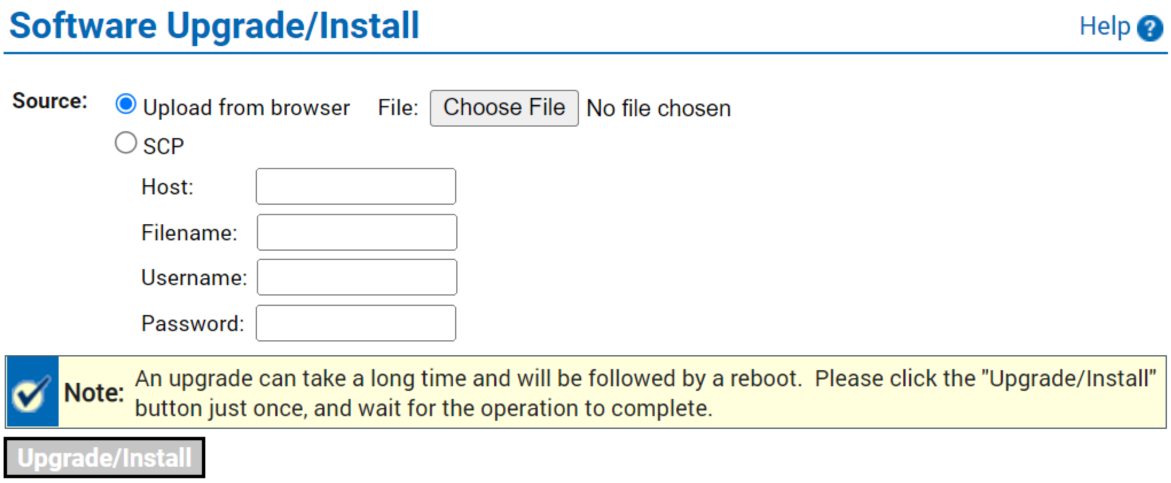
5.4.4 Software upgrade/install

The software upgrade and installation mechanism can be used to install new features, upgrade core software, apply security patches, and install license packs. You can upgrade or install software from both the Management Console and the Command Line Interface. If you are interested in monitoring the status of the upgrade, perform the upgrade from the Command Line Interface, see software install (p. 744).

Software upgrades must be applied individually to all ESKM appliances in a cluster. Software upgrades are not replicated to other appliances in the cluster.

Only software signed by Utimaco can be installed on the ESKM appliance. Changes to multiple components of the software are bundled together in an encrypted software upgrade file.

> ❗ Do not refresh the Management Console page when the upgrade is in progress.



Software Upgrade/Install

Source: ● Upload from browser File: Choose File No file chosen

○ SCP

Host:

Filename:

Username:

Password:

✓ **Note:** An upgrade can take a long time and will be followed by a reboot. Please click the "Upgrade/Install" button just once, and wait for the operation to complete.

Figure 48 : Software Upgrade/Install

The following table describes the components of Software Upgrade/Install.

Table 18: Software Upgrade/Install components

Components	***Description***
Source	Specify the method for copying the software file to the ESKM appliance. If you are uploading the file or a license pack through the browser, select **Upload from browser**, and then click **Browse** and locate the file on the local drive or network. If you are using SCP to copy the file to the ESKM appliance, select the appropriate option and enter the following information: ▪ **Host**: the source host ▪ **Filename**: the name of the file on the source host ▪ **Username**: the username of the account on the source host ▪ **Password**: the password for the user account on the source host ⚠ The ESKM appliance can receive software files from a remote host which has an IPv6 address when IPv6 is enabled on it (see ipv6 enable (p. 693)), and SCP is used to receive the files.
Upgrade/ Install	Click **Upgrade/Install** to copy the software or license pack to the ESKM appliance, verify the signature, and update the system. When these tasks are completed, the system automatically restarts. Because the ESKM appliance is unavailable while it is restarting, your browser might display an error. If this situation should occur, refresh the browser. ⚠ After the upgrade/install process completes, Utimaco recommends that you go to the Cluster Members section (**Device > Cluster**), and then click **Refresh List** to update the remote unit ID list in all ESKM appliances in the cluster.

5.4.4.1 Upgrading to a patch release

To apply a patch, follow the procedure in Software upgrade/install (p. 203), or use the CLI command software install (p. 744).

⚠ You must be running the base release upon which the patch is built before upgrading to the patch release. You cannot upgrade directly from a previous base release to a patch. If you receive a software patch from Utimaco, follow the installation instructions that come with it.

5.4.4.2 Rolling back software

Occasionally it is necessary to roll back software to a previous version. The ESKM appliance allows you to roll back one version of the software. As such, Utimaco recommends that you avoid doing multiple patch upgrades on the same base release.
Instead, roll back from the patch release to the base release before doing the upgrade to the patch release.

⚠ The software rollback process can only be performed from the CLI, see software rollback (p. 745).

ℹ Before performing a software rollback, it is very important that you create a backup of your existing configuration. In most cases, you can restore a backup after you have done the software rollback. If some features are supported in the more recent version of the software and not in the base version you are rolling back to, those features will not be available after the software rollback.

If your ESKM appliances are clustered, you must perform a rollback on each appliance in the cluster.

⚠ A backup taken from ESKM cannot be restored on earlier versions.

5.5 System health page

⚠ This section is not relevant to the “virtual Enterprise Secure Key Manager”.

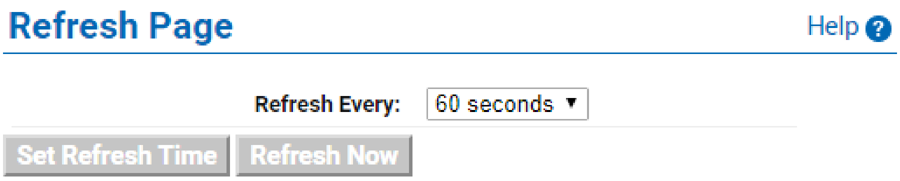
The System Health feature provides information about the ESKM appliance’s RAID disks, power supplies and cooling fans. When the appliance detects a change in the status of a RAID disk, power supply unit or cooling fan, the System Health page reflects the change and displays a warning message if appropriate. In addition, if your system is configured for SNMP, the ESKM appliance sends an SNMP trap to the SNMP Management Station indicating the change in status.

This page contains the following sections:

- Refresh page (p. 206)
- RAID status (p. 207)
- Power supply status (p. 210)
- Cooling fan status (p. 211)

5.5.1 Refresh page

Refresh Page controls how frequently the System Health page is refreshed. When the page is refreshed, the values displayed on the page are updated. The refresh interval you specify on the System Health page does not affect the refresh interval on the CLI.



Refresh Page

Refresh Every: 60 seconds

Figure 49 : Refresh Page

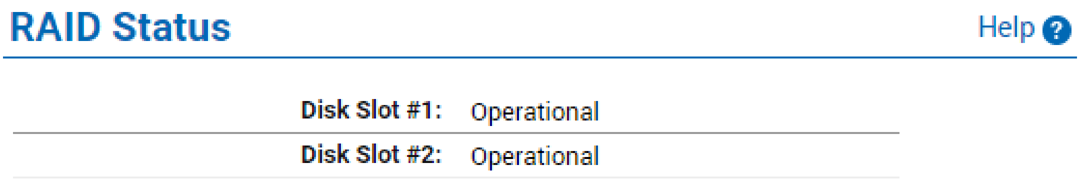
The following table describes the components of Refresh Page.

Table 19: Refresh Page components

Component	***Description***
Refresh Every	Specify the refresh rate of the System Statistics page. Available refresh intervals are: ▪ Never (default value) ▪ 5 seconds ▪ 15 seconds ▪ 30 seconds ▪ 60 seconds ▪ 2 minutes ▪ 5 minutes ⚠ This value is only valid while you are viewing the System Statistics page. If you access another page on the Management Console and return to the System Statistics page, the value returns to Never.
Set Refresh Time	Click **Set Refresh Time** to apply the new value.
Refresh Now	Click **Refresh Now** to refresh the System Statistics page on demand.

5.5.2 RAID status

RAID, or Redundant Array of Inexpensive (or Independent) Disks, refers to the practice of combining multiple disk drives into an array for improved performance or reliability. ESKM appliance supports RAID level 1, or mirroring, a technique in which data written to disk is copied to all members of the array.



RAID Status

Disk Slot #1:	Operational
Disk Slot #2:	Operational

Figure 50 : RAID Status

The following table describes the elements of the RAID Status section of the System Health page.

Table 20: RAID Status Components

Component	***Description***
Array Member	This refers to the slot of the physical hard disk.
Status	▪ **Operational**: indicates that the disk is mirrored and in use. ▪ **Failed**: indicates that a disk has failed. In this case, a warning message is displayed, and, if configured, an SNMP trap is sent. Additionally, the event is noted in the System Log. ▪ **Removed**: indicates that a disk has been removed. In this case, a warning message is displayed, and, if configured, an SNMP trap is sent. Additionally, the event is noted in the System Log. ▪ **Recovery**: indicates that a failed disk has been replaced and data from the Operational disk is being copied to the new disk. In this case, a warning message is displayed, and, if configured, an SNMP trap is sent. Additionally, the event is noted in the System Log. ▪ **Unknown**: indicates that the disk status could not be determined. In this case, a warning message is displayed, and, if configured, an SNMP trap is sent. Additionally, the event is noted in the System Log.

ESKM appliance is available with two SCSI hard disks. The status of each disk is always available from the Management Console and the CLI. If one of the disks fails or is removed, the system immediately begins writing to and reading from the remaining operational disk without any loss of data or service.

5.5.3 Recovery

You can replace a disk, provided there is at least one other operational disk, while the system is up and running; this feature is called hot-swap. When you replace a disk, the status of the newly added disk is “Recovery,” which indicates that data from the operational disk is being copied to the new disk. The ESKM appliance is fully operational while the newly added disk is in the “Recovery” state. The recovery process can take 15 to 30 minutes, depending on the amount of data on the disk and the number of requests the ESKM v8 appliance must fulfill while the recovery is in progress.

5.5.4 SNMP Traps associated with RAID

The following list describes the traps that are sent as a result of a change in the RAID status of an ESKM appliance.

1. Disk operational - This trap is sent when the status of a disk in RAID changes to “Operational.” This can happen if:
   - A new disk that was added to RAID has completed synchronizing with the active member in the array, and its status has changed from “Recovering” to “Operational.”
   - The disk has been having hardware errors causing its previous status to be “Failed,” and the RAID hardware does not detect such errors anymore.
   - The status of a disk changed from “Unknown” to “Operational.”

2. Disk failed - This trap is sent when the status of a disk in RAID changes to “Failed”. This can happen if the disk experiences a hardware failure. Note that the failure may have been determined based on just a few transient errors, and the status of the disk may change to “Operational” later. In any event, if a disk failure is observed, contact Utimaco Technical Support (p. 798).

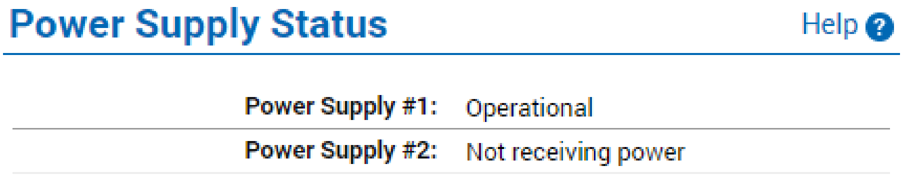
3. Disk recovering - This trap is sent when a new disk is added to RAID and data from the operational disk is being copied to the new disk.

4. **Disk status unknown** - This trap is sent when the status of a disk in RAID changes to “Unknown.” This usually indicates an unexpected hardware or software error.

5. **Disk removed** - This trap is sent when a disk is removed from RAID. The removal can be a physical removal of the disk from the array.

5.5.5 Power supply status

Power Supply Status provides information about the status of the power supplies in the ESKM appliance.



Power Supply Status

Power Supply #1:	Operational
Power Supply #2:	Not receiving power

Figure 51 : Power Supply Status

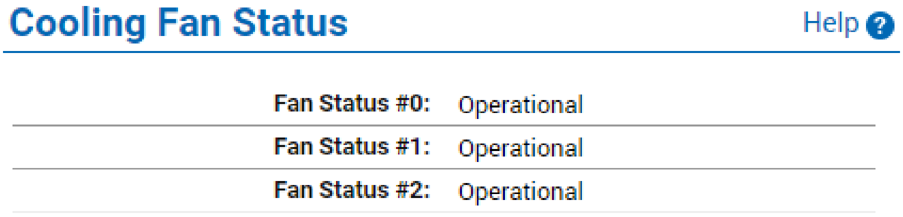
The following table describes the components of Power Supply Status.

Table 21: Power Supply Status components

Component	***Description***
Power Supply	The status of each power supply is represented on a different line. The following states apply: ▪ **Operational**: The power supply unit is operational. ▪ **Not receiving power**: No power is supplied to the power supply unit. The ESKM appliance issues the following warning: “A power supply is not plugged in or is malfunctioning.” ▪ **Removed or damaged**: The power supply unit has been removed from the ESKM appliance. The appliance issues the following warning: “A power supply has been removed or damaged.”

5.5.6 Cooling fan status

The Cooling Fan Status provides information on the status all of the ESKM appliance's cooling fans. The following table describes the different states that are represented in the Cooling Fan Status section.



Cooling Fan Status

Fan Status #0:	Operational
Fan Status #1:	Operational
Fan Status #2:	Operational

Figure 52 : Cooling Fan Status

The number of fans in an ESKM appliance depends upon the Utimaco V6 chassis. The V6 chassis has 3 fan modules.

The following table describes the different states of Cooling Fan.

Table 22: Cooling Fan Status

Component	***Description***
Fan Status	Displays the status of the cooling fan. The following states apply: ▪ **Operational**: The individual fan is operational. ▪ **Failure (Reason)**: A fan has stopped, been removed, or is in an unknown state (malfunctioning). The ESKM appliance displays a warning message until the problem is resolved. The warning reads "Fan failure; please contact Utimaco Technical Support (p. 798) immediately."

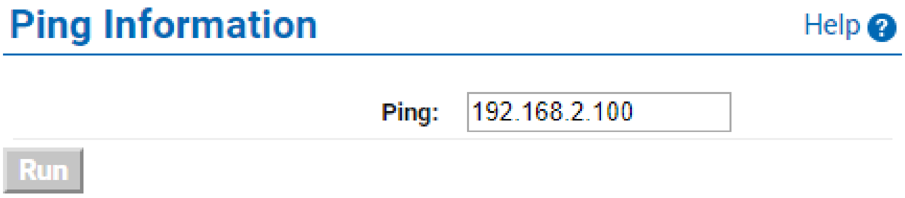
5.6 Network diagnostics page

The Network Diagnostics page allows you to test network connectivity by running any of the following: ping, traceroute, host, or netstat. This page contains the following sections:

- Ping information (p. 212)
- Traceroute information (p. 213)
- Host information (p. 213)
- Netstat information (p. 214)

5.6.1 Ping information

Use Ping Information to test connectivity.



Ping: 192.168.2.100

Figure 53 : Ping Information

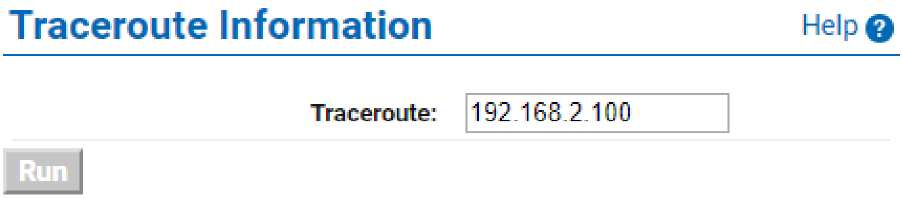
The following table describes the components of Ping Information.

Table 23: Ping Information components

Component	***Description***
Ping	Specify the host name or IP Address of the system to ping. This tool helps to test connectivity. ⚠ The ESKM appliance can ping a remote host which has an IPv6 address, when IPv6 is enabled on it (see ipv6 enable (p. 693)).
Run	Click **Run** to run the process.

5.6.2 Traceroute information

Use the Traceroute Information to examine the path between the ESKM appliance and a destination.



Traceroute Information

Traceroute: 192.168.2.100

Figure 54 : Traceroute Information

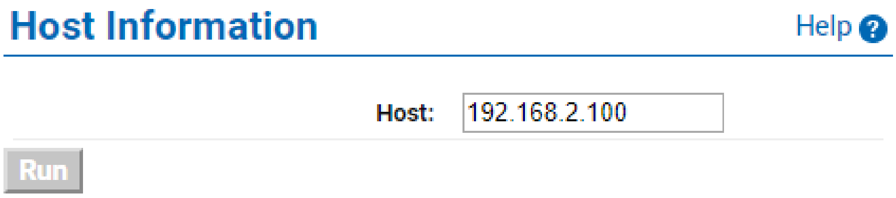
The following table describes the components of Traceroute Information.

Table 24: Traceroute Information components

Component	***Description***
Traceroute	Specify the host name or IPv4/IPv6 address of the destination system for performing a traceroute. This tool helps you examine the path, packets take from the ESKM appliance to the destination.
Run	Click **Run** to run the process.

5.6.3 Host information

Use the Host Information to test DNS.



Host Information

Host: 192.168.2.100

Figure 55 : Host Information

The following table describes the components of Host Information.

Table 25: Host Information components

Component	***Description***
Host	Specify the host name or IP Address to look up with DNS. This tool helps test whether DNS is operational on the appliance.
Run	Click **Run** to run the process.

5.6.4 Netstat information

Use the Netstat Information to list all active network connections to the ESKM appliance.

The ESKM appliance supports IPv6 network connections when IPv6 is enabled on it (see ipv6 enable (p. 693)).

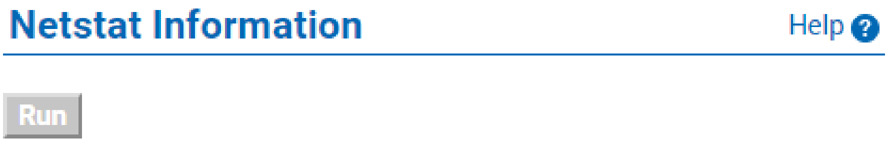


Figure 56 : Netstat Information

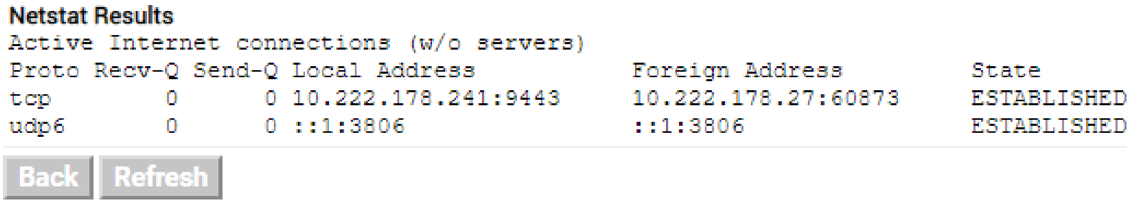
The following table describes the components of Netstat Information.

Table 26: Netstat Information components

Component	***Description***
Run	Click **Run** to see a list of all active network connections on the ESKM appliance.

5.6.4.1 Reading netstat results

The Netstat diagnostic feature provides information about the active network connections on the ESKM appliance in the form of a columnar report, which looks like the following:



Netstat Results

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.222.178.241:9443     10.222.178.27:60873     ESTABLISHED
udp6       0      0 ::1:3806                ::1:3806                ESTABLISHED
```

Figure 57 : Netstat Results

The following table describes the headings that appear in the Netstat report.

Table 27: Netstat Headings

Heading	***Description***
Proto	The protocol used by the connection. Either TCP, UDP, or RAW.
Recv-Q	The number of bytes received from the remote host waiting to be read.
Send-Q	The number of bytes awaiting acknowledgment by the remote host.
Local Address	The local address or hostname and port number of the connection.
Foreign Address	The remote address or hostname and port number of the connection.
State	The state of the connection.

6 Using the Management Console

This section guides you through the Management Console's fundamental elements. It contains the following sections:

6.1 Logging in and out

Use the Administrator Authentication screen to log into the Management Console.

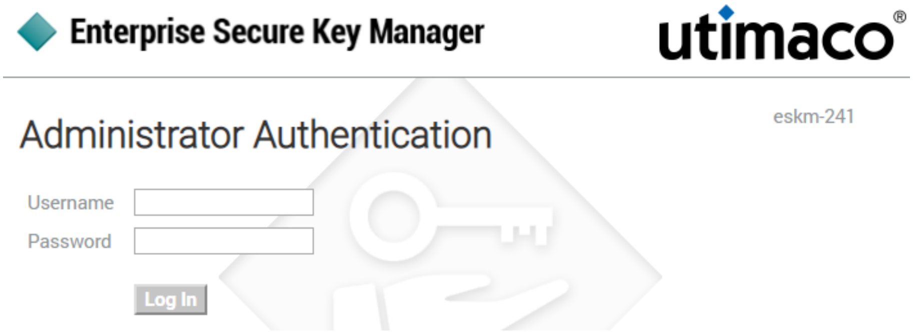


Figure 58 : Administrator Authentication screen

The following table describes the components of the Administrator Authentication page.

Table 28: Administrator Authentication screen components

Components	***Description***
Username	When logging in for the first time, type the default username admin. Thereafter, type the name assigned by the system administrator.
Password	Type the password associated with the username. When logging in for the first time, this is the password created during the firstrun installation.
Log In	Click **Log In** to login and access the Management Console.

Log out of the Management Console at any time using the **Log Out** link on the upper right corner.

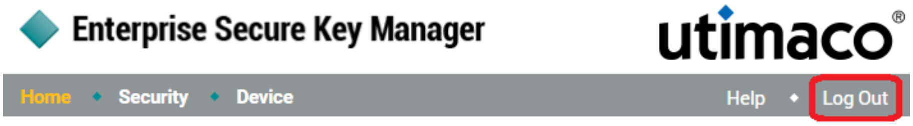
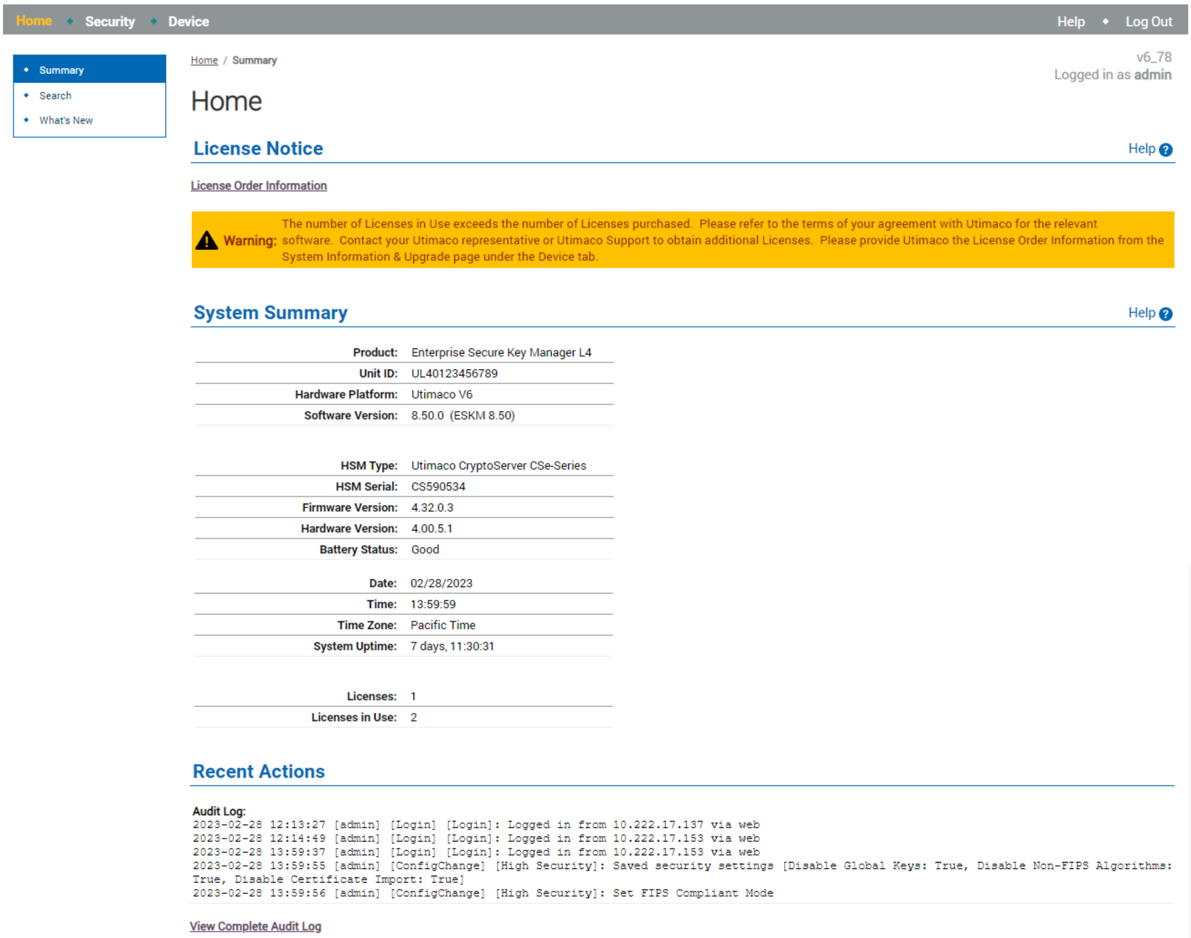


Figure 59 : Logout window

6.2 Using the home tab

After you log in, the following screen appears.



License Notice

Warning: The number of Licenses in Use exceeds the number of Licenses purchased. Please refer to the terms of your agreement with Utimaco for the relevant software. Contact your Utimaco representative or Utimaco Support to obtain additional Licenses. Please provide Utimaco the License Order Information from the System Information & Upgrade page under the Device tab.

System Summary

Product:	Enterprise Secure Key Manager L4
Unit ID:	UL40123456789
Hardware Platform:	Utimaco V6
Software Version:	8.50.0 (ESKM 8.50)
HSM Type:	Utimaco CryptoServer CSe-Series
HSM Serial:	CS590534
Firmware Version:	4.32.0.3
Hardware Version:	4.00.5.1
Battery Status:	Good
Date:	02/28/2023
Time:	13:59:59
Time Zone:	Pacific Time
System Uptime:	7 days, 11:30:31
Licenses:	1
Licenses in Use:	2

Recent Actions

Audit Log:

```
2023-02-28 12:13:27 [admin] [Login] [Login]: Logged in from 10.222.17.137 via web
2023-02-28 12:14:49 [admin] [Login] [Login]: Logged in from 10.222.17.153 via web
2023-02-28 13:59:37 [admin] [Login] [Login]: Logged in from 10.222.17.153 via web
2023-02-28 13:59:55 [admin] [ConfigChange] [High Security]: Saved security settings [Disable Global Keys: True, Disable Non-FIPS Algorithms:
True, Disable Certificate Import: True]
2023-02-28 13:59:56 [admin] [ConfigChange] [High Security]: Set FIPS Compliant Mode
```

Figure 60 : ESKM Management Console

The Home tab contains the Summary screen and the Search screen.

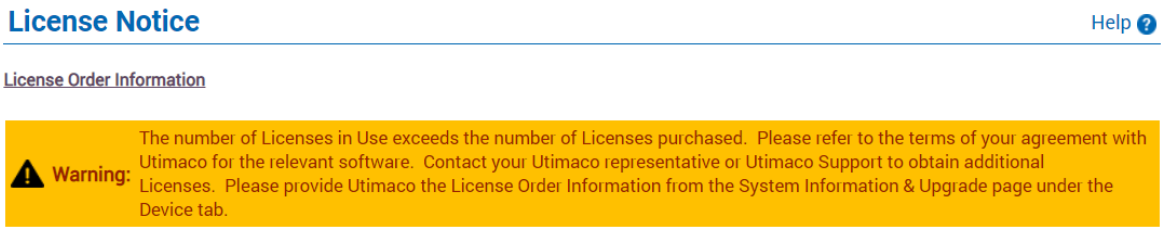
6.2.1 Summary screen

The first page you see in the Management Console is the Summary screen, which displays fundamental information about the ESKM appliance. The Summary screen may contain the following sections:

- License notice (p. 219)
- System summary (p. 219)
- Recent actions (p. 222)

6.2.1.1 License notice

The following warning appears if the number of licenses in use exceeds the number of licenses purchased.



License Notice

Help ?

License Order Information

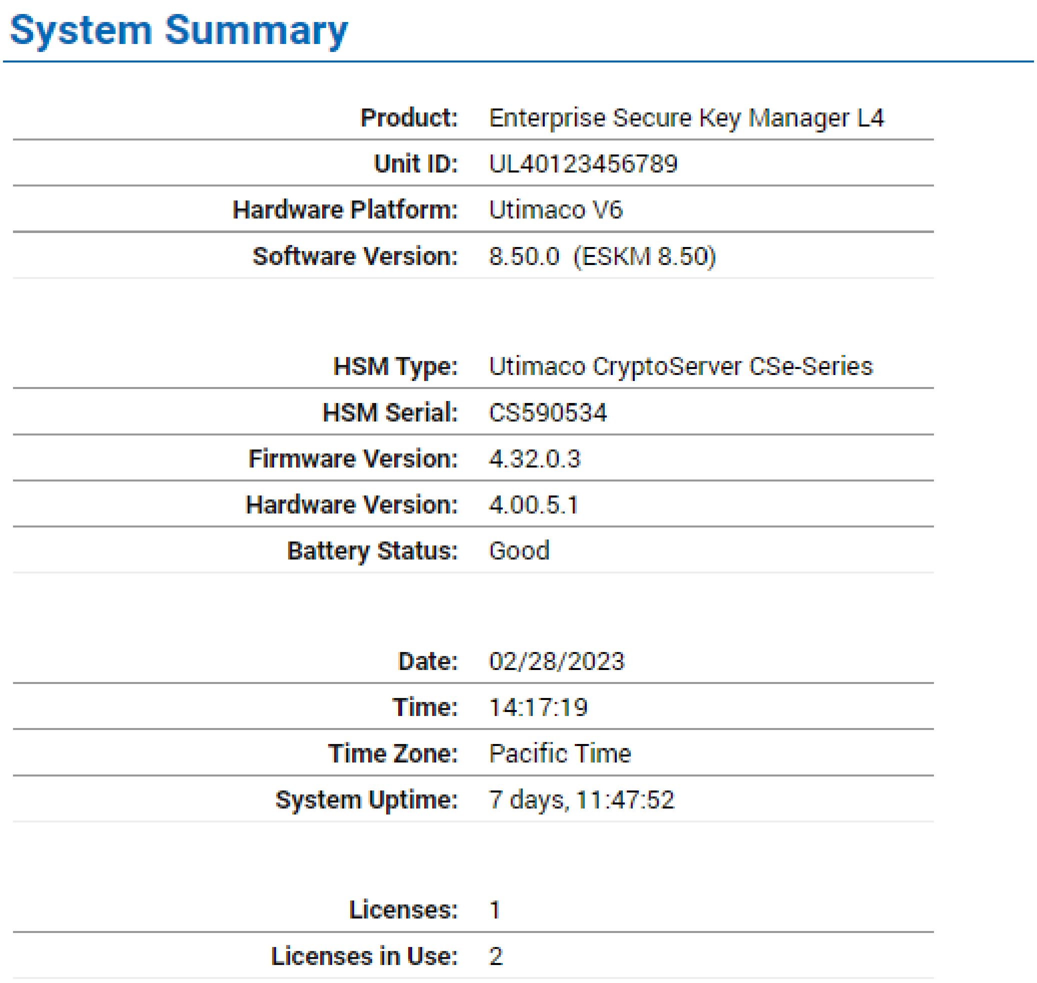
⚠ Warning: The number of Licenses in Use exceeds the number of Licenses purchased. Please refer to the terms of your agreement with Utimaco for the relevant software. Contact your Utimaco representative or Utimaco Support to obtain additional Licenses. Please provide Utimaco the License Order Information from the System Information & Upgrade page under the Device tab.

Figure 61 : License Notice

Click the **License Order Information** link to access the License order information (p. 200).

6.2.1.2 System summary

Use this section to view system summary information for the ESKM appliance.



System Summary

Product:	Enterprise Secure Key Manager L4
Unit ID:	UL40123456789
Hardware Platform:	Utimaco V6
Software Version:	8.50.0 (ESKM 8.50)
HSM Type:	Utimaco CryptoServer CSe-Series
HSM Serial:	CS590534
Firmware Version:	4.32.0.3
Hardware Version:	4.00.5.1
Battery Status:	Good
Date:	02/28/2023
Time:	14:17:19
Time Zone:	Pacific Time
System Uptime:	7 days, 11:47:52
Licenses:	1
Licenses in Use:	2

Figure 62 : System Summary

The following table describes the components of the System Summary.

Table 29: System Summary components

Component	***Description***
Product	Displays the product name.
Unit ID	Displays the ESKM appliance Unit ID.

Component	***Description***
Hardware Platform	Displays the model of the appliance which is running the ESKM software. The term "hardware" also refers to the "virtual machine".
Software Version	Displays the version of the software currently running on the ESKM appliance.
Date	Displays the current date in mm/dd/yyyy format.
Time	Displays the current time.
Time Zone	Displays the current time zone setting.
System Uptime	Shows the length of time that the ESKM appliance has been running.
Licenses	Shows the number of licenses available.
Licenses in Use	Shows the number of licenses currently being used to connect to the ESKM Level 3 appliance.
License Order Information	Click **License Order Information** to input and obtain client license order information.

The following table is applicable only for the ESKM L3 and L4 devices which have embedded HSM.

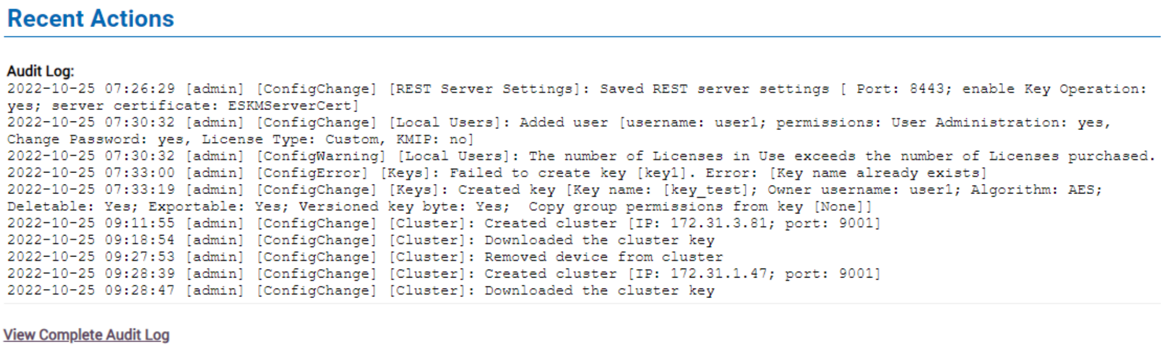
The following table describes the components of the **System Summary (HSM)**.

Table 30: System Summary components (HSM)

<table>
<tr><th><i>Component</i></th><th><i>Description</i></th></tr>
<tr><td>HSM Type</td><td>Displays the type of the embedded HSM.</td></tr>
<tr><td>HSM Serial</td><td>Displays the serial number of the embedded HSM.</td></tr>
<tr><td>Firmware Version</td><td>Displays the firmware version of the embedded HSM.</td></tr>
<tr><td>Hardware Version</td><td>Displays the hardware version of the embedded HSM.</td></tr>
<tr><td>Battery Status</td><td>Displays the battery status of the embedded HSM.
<table>
<tr><th><i>Battery status</i></th><th><i>Carrier battery</i></th><th><i>External battery</i></th></tr>
<tr><td>Good</td><td>OK</td><td>OK</td></tr>
<tr><td>Carrier Battery Low</td><td>Low</td><td>OK</td></tr>
<tr><td>External Battery Low/ Absent</td><td>OK</td><td>Low or Absent</td></tr>
<tr><td>Carrier and External Battery</td><td>Low</td><td>Low</td></tr>
</table>
</td></tr>
</table>

6.2.1.3 Recent actions

Use this section to view the latest entries of the ESKM appliance’s audit log.



Recent Actions

Audit Log:

```
2022-10-25 07:26:29 [admin] [ConfigChange] [REST Server Settings]: Saved REST server settings [ Port: 8443; enable Key Operation:
yes; server certificate: ESKMServerCert]
2022-10-25 07:30:32 [admin] [ConfigChange] [Local Users]: Added user [username: user1; permissions: User Administration: yes,
Change Password: yes, License Type: Custom, KMIP: no]
2022-10-25 07:30:32 [admin] [ConfigWarning] [Local Users]: The number of Licenses in Use exceeds the number of Licenses purchased.
2022-10-25 07:33:00 [admin] [ConfigError] [Keys]: Failed to create key [key1]. Error: [Key name already exists]
2022-10-25 07:33:19 [admin] [ConfigChange] [Keys]: Created key [Key name: [key_test]; Owner username: user1; Algorithm: AES;
Deletable: Yes; Exportable: Yes; Versioned key byte: Yes;  Copy group permissions from key [None]]
2022-10-25 09:11:55 [admin] [ConfigChange] [Cluster]: Created cluster [IP: 172.31.3.81; port: 9001]
2022-10-25 09:18:54 [admin] [ConfigChange] [Cluster]: Downloaded the cluster key
2022-10-25 09:27:53 [admin] [ConfigChange] [Cluster]: Removed device from cluster
2022-10-25 09:28:39 [admin] [ConfigChange] [Cluster]: Created cluster [IP: 172.31.1.47; port: 9001]
2022-10-25 09:28:47 [admin] [ConfigChange] [Cluster]: Downloaded the cluster key
```

Figure 63 : Recent Actions

The following table describes the components of **Recent Actions**.

Table 31: Recent Actions components

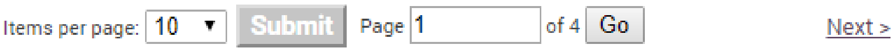
Component	***Description***
Audit Log	The ESKM appliance displays the last ten lines of the latest audit log.
View Complete Audit Log	Click **View Complete Audit Log** to access the Log Viewer page that displays the current audit log.

6.3 Using features common to the security and device tabs

The following sections describe how to set display parameters for Management Console viewing. These parameters are used in some sections of screens on the Security tab and the Device tab.

6.3.1 Setting the number of items per page

Where available, specify the number of items to view in a section.



Items per page: 10 Page 1 of 4

Figure 64 : Number of items per page fields

The following table describes the section search fields.

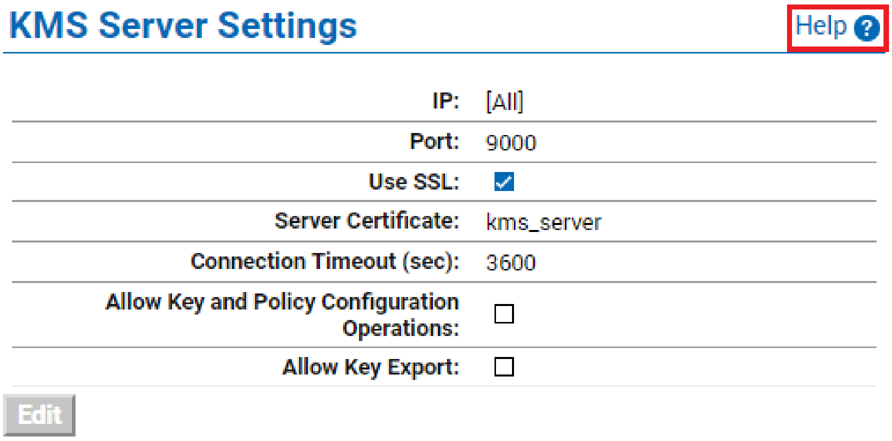
Table 32: Items Per Page fields components

Component	***Description***
Items per page	Select the number of rows displayed on each page.
Submit	Click **Submit** to run the search query or apply the value in the Items per page field.
Go	Enter a page number, and then click **Go** to access that page.
Previous	Click **Previous** to view the previous set of rows for the section.
Next	Click **Next** to view the next set of rows for the section.

6.3.2 Accessing the help system

The Management Console provides you with two ways to access product documentation: context-sensitive help, and help. Both methods access the same files which are stored on the ESKM appliance.

Context-sensitive help is available for each section by clicking the **Help** icon on the top right side of the section header.

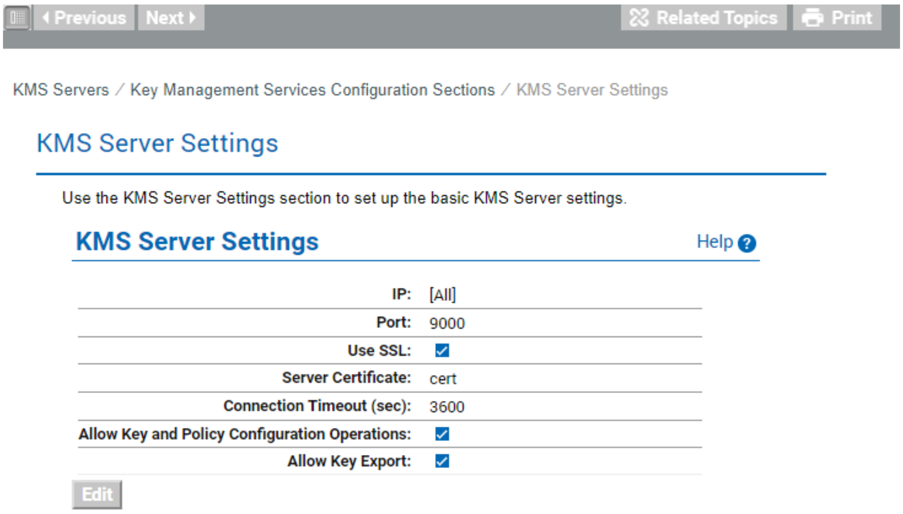


KMS Server Settings

IP:	[All]
Port:	9000
Use SSL:	☑
Server Certificate:	kms_server
Connection Timeout (sec):	3600
Allow Key and Policy Configuration Operations:	□
Allow Key Export:	□

Figure 65 : Locating button to launch context-sensitive help

Clicking this icon opens the documentation for the specific section in a new window. (Subsequent clicks open additional windows.)



KMS Servers / Key Management Services Configuration Sections / KMS Server Settings

KMS Server Settings

Use the KMS Server Settings section to set up the basic KMS Server settings.

KMS Server Settings Help ?

IP:	[All]
Port:	9000
Use SSL:	☑
Server Certificate:	cert
Connection Timeout (sec):	3600
Allow Key and Policy Configuration Operations:	☑
Allow Key Export:	☑

Edit

Figure 66 : Context-sensitive help window

The Help link on the top right side of the Management Console header launches the help system on the ESKM appliance.

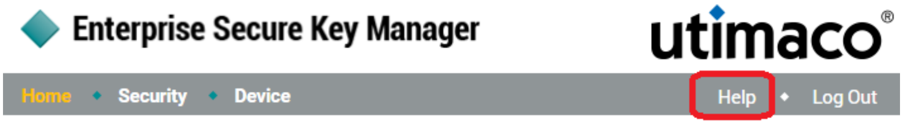


Figure 67 : Finding the Help link

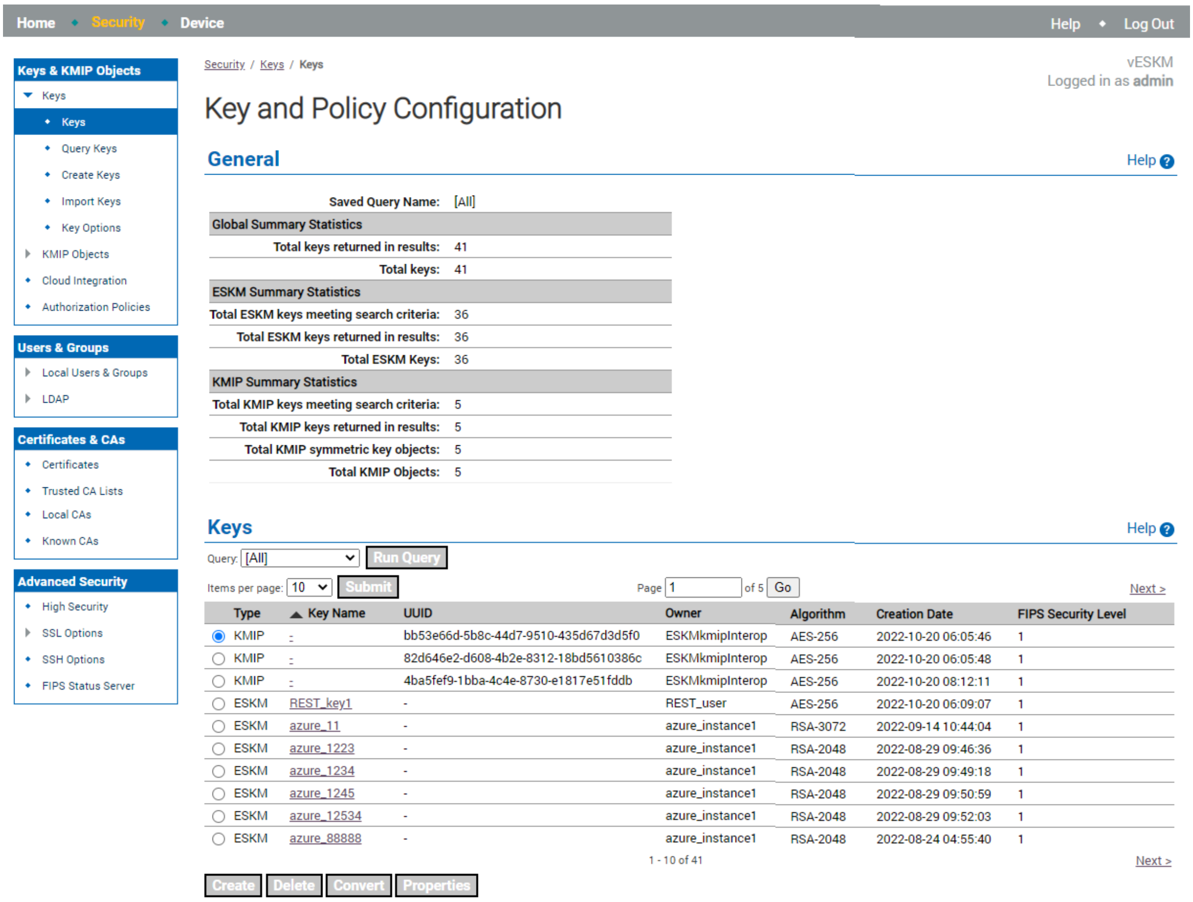
Clicking this link opens the Help system in a new web browser. The default page shows the table of contents.

6.4 Key and Policy Configuration

Keys are used to perform cryptographic operations such as encryption and decryption. Use authorization policies to restrict the use of a key to certain numbers of operations per hour or certain times during the week.

The **Key and Policy Configuration** page allows you to create, import, and manage keys, as well as create and view key queries.

The ESKM appliance can create and store cryptographic keys (DES, AES, RSA, and so on) as well as other KMIP objects such as certificates and opaque objects.



Key and Policy Configuration

General

Saved Query Name:	[All]
Global Summary Statistics	
Total keys returned in results:	41
Total keys:	41
ESKM Summary Statistics	
Total ESKM keys meeting search criteria:	36
Total ESKM keys returned in results:	36
Total ESKM Keys:	36
KMIP Summary Statistics	
Total KMIP keys meeting search criteria:	5
Total KMIP keys returned in results:	5
Total KMIP symmetric key objects:	5
Total KMIP Objects:	5

Keys

Query: [All]

Items per page: 10

Page 1 of 5

	Type	Key Name	UUID	Owner	Algorithm	Creation Date	FIPS Security Level
●	KMIP	-	bb53e66d-5b8c-44d7-9510-435d67d3d5f0	ESKMkmipInterop	AES-256	2022-10-20 06:05:46	1
○	KMIP	-	82d646e2-d608-4b2e-8312-18bd5610386c	ESKMkmipInterop	AES-256	2022-10-20 06:05:48	1
○	KMIP	-	4ba5fef9-1bba-4c4e-8730-e1817e51fddb	ESKMkmipInterop	AES-256	2022-10-20 08:12:11	1
○	ESKM	REST_key1	-	REST_user	AES-256	2022-10-20 06:09:07	1
○	ESKM	azure_11	-	azure_instance1	RSA-3072	2022-09-14 10:44:04	1
○	ESKM	azure_1223	-	azure_instance1	RSA-2048	2022-08-29 09:46:36	1
○	ESKM	azure_1234	-	azure_instance1	RSA-2048	2022-08-29 09:49:18	1
○	ESKM	azure_1245	-	azure_instance1	RSA-2048	2022-08-29 09:50:59	1
○	ESKM	azure_12534	-	azure_instance1	RSA-2048	2022-08-29 09:52:03	1
○	ESKM	azure_88888	-	azure_instance1	RSA-2048	2022-08-24 04:55:40	1

1 - 10 of 41

Figure 68 : Keys

ESKM appliances support two types of cryptographic keys:

- KMS keys (p. 226) are created and managed using the ESKM XML protocol.
- KMIP objects (p. 228) are keys and other cryptographic objects created and managed using the KMIP protocol.

In addition, the ESKM appliance supports key conversion, see Convert keys (p. 266).

6.4.1 KMS keys

KMS keys are created and managed using the ESKM XML protocol. A KMS key is composed of two main parts: key bytes and key metadata.

- **Key bytes** are used by the cryptographic algorithm (together with data) to produce either plaintext or ciphertext.

- **Key metadata** contains information about the key, such as key name, owner username, algorithm, key size, creation date, group permissions, and any custom attributes that you create. The metadata also indicates if the key is a versioned key, deletable, or exportable.

Cryptographic keys can be global or owned by a particular user. Global keys are keys that are available to everyone, with no authentication required. Additionally, group permissions can be assigned to a key. For example, you might give permission to export at any time to members of Group1 and, to export only during a specific time period to members of Group2. Using authorization policies, you can set usage limitations for keys.

As the administrator of the ESKM appliance, you can define how your clients authenticate to the ESKM appliance.

There are two kinds of client sessions:

- Authenticated
- Unauthenticated (global).

When a client authenticates, it authenticates either as a local user or as a user in the LDAP user directory that the ESKM appliance is configured to use. An authenticated client has access to all global keys, all the keys owned by the user, and all keys accessible to groups to which that user belongs. If a client does not authenticate to the ESKM appliance, then that client has access only to global keys.

On the ESKM appliance, keys can be:

- Generated on the Management Console by an administrator
- Imported through the Management Console
- Marked as exportable, deletable, neither or both. An exportable key can be exported from the ESKM appliance. Similarly, a deletable key can be deleted from the ESKM appliance.

❗ Do not delete keys that might be needed to decrypt data at some point in the future. After you delete a key, there is no way to decrypt data that was encrypted with that key. As such, you should be extremely cautious when making decisions about deleting keys.

6.4.2 KMIP objects

KMIP objects are created and managed using the KMIP protocol. The ESKM appliance supports versions 1.0, 1.1, 1.2, 1.3, 1.4, 2.0 and 2.1 of the KMIP protocol. For more information about the KMIP standard, see https://www.oasis-open.org/ standards.

The KMIP specification refers to the objects managed by key management systems, such as the ESKM appliance, as managed objects. Managed objects include symmetric and asymmetric cryptographic keys, digital certificates, and templates used to simplify object creation and use.

Unlike KMS keys created using the ESKM XML protocol where client sessions can either be authenticated or unauthenticated, KMIP keys can only be created by authenticated clients over SSL/TLS sessions. Therefore, all KMIP keys have owners. The KMIP key owner is usually the username of the client which created the key over an authenticated SSL/TLS session; however the key may also be modified by the administrator using the Management Console. Unlike owned KMS keys, which can be accessed only by the owner or by groups to which that user belongs, the privilege to access KMIP keys is determined by the user group. Hence, KMIP keys can be accessed by all users who belong to the user groups, with access rights to the object group containing the key.

The ESKM appliance supports KMIP-managed objects in the **Security** > **Keys & KMIP Objects** of the Management Console in the following manner:

- Viewing of symmetric keys and other KMIP-managed objects in the Management Console.
- Conversion of KMS symmetric keys to KMIP-managed objects.
- Conversion of symmetric key KMIP-managed objects to KMS keys.
- Changing the owner of the KMIP-managed object. This is especially useful for transferring the key ownership prior to deleting a KMIP-enabled user, since users who are owners of KMS keys or KMIP-managed objects cannot be deleted.
- Purging of destroyed KMIP-managed objects.

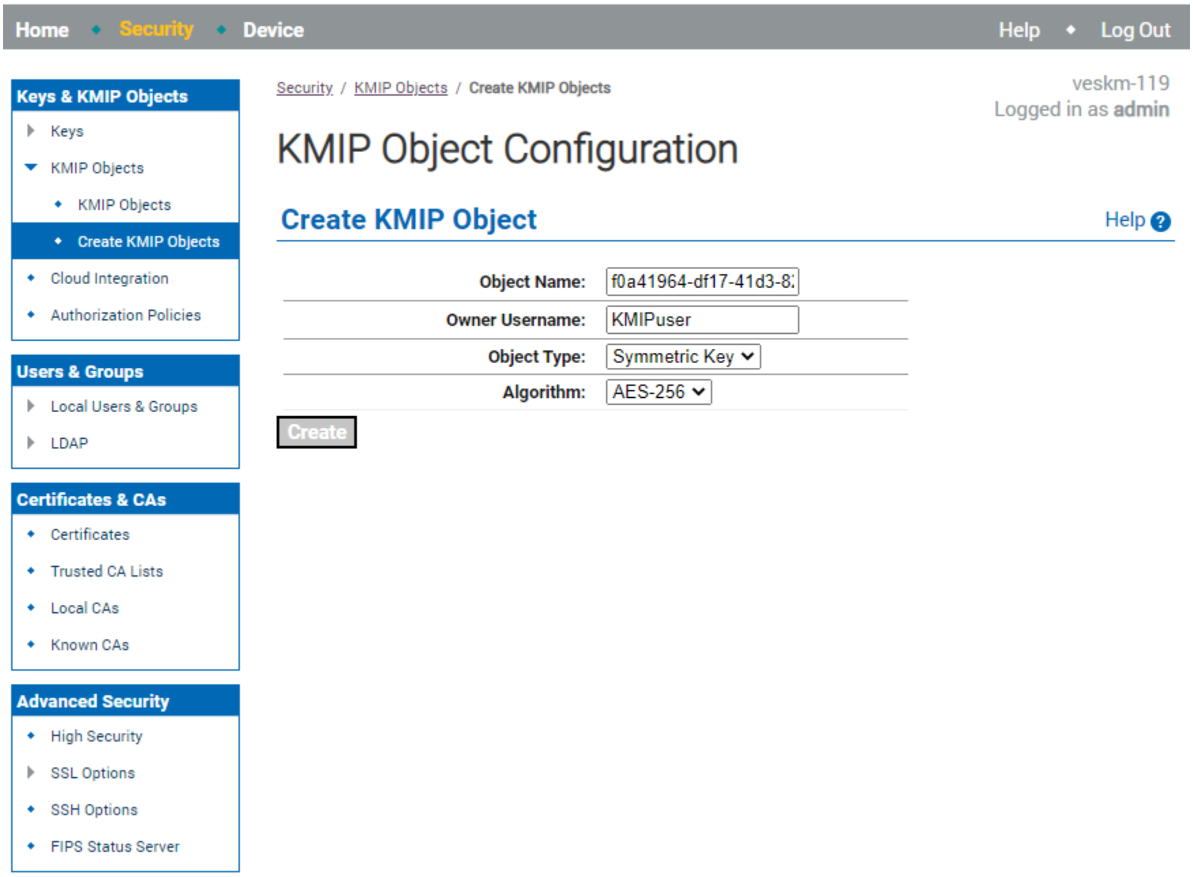
6.4.2.1 Create KMIP object

ESKM allows user to create KMIP object from the UI.

To create KMIP objects

- Navigate to **Security** > **KMIP Objects** > **Create KMIP Objects**.

- Enter the **Object Name**.
- Enter the **KMIP username**.
- Select the **Object Type** from the drop down.
- Select the **Algorithm** from the drop down.
- Click **Create**.



KMIP Object Configuration

Create KMIP Object

Object Name:	f0a41964-df17-41d3-8:
Owner Username:	KMIPuser
Object Type:	Symmetric Key
Algorithm:	AES-256

Figure 69 : KMIP Object Configuration

The following table describes the components of the Create KMIP Object section.

Component	***Description***	
Object Name	This is the name that the server uses to refer to the object. The object name must begin with a letter, must be between 1 and 64 characters (inclusive), and can consist of only letters, numbers, underscores, periods, and hyphens.	

Component	***Description***	
Owner Username	Assign an owner for the object, you can specify any valid KMIP user. Only the assigned user is allowed to access the key (unless the key is given additional group permissions later).	
Object Type	The KMIP object type includes Symmetric-Keys used for algorithms like AES.	
Algorithm	Depending on the Object Type the algorithm might be any of the following: ▪ AES-256 ▪ AES-192 ▪ AES-128	
Create	Click **Create** to create the object.	

⚠ If you try to create a KMIP object with a KMIP user without a certificate, '*User certificate not found'* error message is displayed.

6.4.3 Viewing keys on the Management Console

The **Keys** section allows you to view all the keys on the ESKM appliance. You can click a field name (**Key Name**, **Owner**) to sort the keys by that value; toggle to alternate between ascending and descending order. You can use the Query field to select a query that will filter this page by the key metadata. Click **Run Query** to run the query. The type of query you apply to this page determines which columns are shown:

- For a query of type **All**, summary statistics are shown together with KMS and KMIP keys satisfying the search criteria.

- For a query of type **ESKM**, all KMS keys satisfying the search criteria are returned in the search results.
- For query of type **KMIP**, all KMIP keys satisfying the search criteria are returned in the search results.

6.4.3.1 Displaying search results for All-type queries

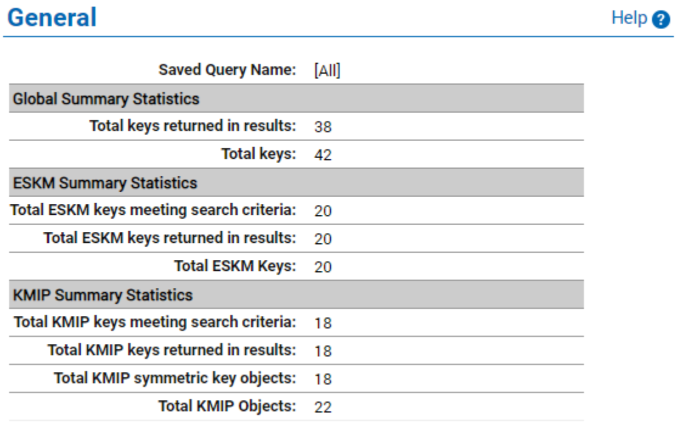
An All-type query is one which returns both KMS and KMIP keys matching the common search criteria. Because KMS and KMIP keys have different properties, the only supported common search criteria are **Key Name** and **Owner**. The criteria is mutually exclusive. Therefore, an All-type query would be one of the following:

- A query returning all KMS keys and KMIP symmetric keys stored in the ESKM appliance.
- A query returning a KMS key and KMIP symmetric key matching a specified key name. Since KMS and KMIP do not share the same namespace, and key names are unique within KMS and KMIP, at most one KMS key and one KMIP key will be returned.
- A query returning all KMS and KMIP keys belonging to the same owner. KMIP-enabled users can either create KMS keys using the ESKM XML protocol or KMIP-managed objects using the KMIP protocol. Therefore, the same user may own KMS keys and KMIP-managed objects.

KMIP-managed objects satisfying the search criteria can include objects other than KMIP symmetric keys, but only KMIP symmetric keys matching the search criteria are returned in the **Keys** listing page. To view search results for other types of KMIP managed objects, go to the **Security** > **Keys & KMIP Objects** > **KMIP Objects** page.

KMS and KMIP keys do not share the same storage space, and hence filtering and sorting of the combined results of All-type queries are done in memory. To prevent resource exhaustion, a maximum of 3,000 KMS keys and 3,000 KMIP symmetric keys are returned in the search results. To bypass this limitation, use a KMS- or KMIP-type query instead of an All-type query. KMS- and KMIP-type queries have no limitations on the number of results returned.

Because the returned results may only be a subset of all keys matching the search criteria, a **General** section is displayed for All-type queries to show summary statistics:



General

Saved Query Name:	[All]
Global Summary Statistics	
Total keys returned in results:	38
Total keys:	42
ESKM Summary Statistics	
Total ESKM keys meeting search criteria:	20
Total ESKM keys returned in results:	20
Total ESKM Keys:	20
KMIP Summary Statistics	
Total KMIP keys meeting search criteria:	18
Total KMIP keys returned in results:	18
Total KMIP symmetric key objects:	18
Total KMIP Objects:	22

Figure 70 : General summary

The following table describes the components of the **General** section.

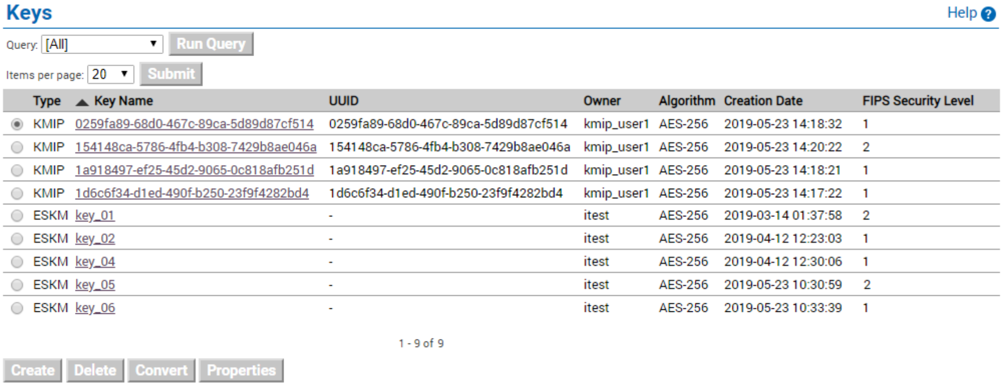
Table 33: General components

Component	***Description***
Saved Query Name	The name of the saved query that is executed to return the search results.
Global Summary Statistics	The global summary statistics that apply to both KMS keys and KMIP-managed objects. These are as follows: ▪ **Total keys returned in results**: These are the keys matching the search criteria that are returned in the results. As at most 3,000 KMS keys and 3,000 KMIP symmetric keys are returned, there may be more keys matching the search criteria that are not returned in the results. ▪ **Total keys**: These are the total number of KMS keys and KMIP-managed objects in the ESKM appliance persistent store. The combined value of Total KMS keys in ESKM Summary Statistics and Total KMIP Objects in the KMIP Summary Statistics should be equal to this number.

Component	***Description***
ESKM server Summary Statistics	These are the statistics specific to KMS keys. These are as follows: ▪ **Total KMS keys meeting search criteria**: This is the total number of KMS keys matching the search criteria for the query given in Saved Query Name. There may be more KMS keys matching the search criteria than what is returned in the results. ▪ **Total KMS keys returned in results**: This is the total number of KMS keys returned in the key listing results. If the value of Total KMS keys meeting search criteria is less than 3,000, then the values of Total KMS keys meeting search criteria and Total KMS keys returned in results will be the same. ▪ **Total KMS keys**: This is the total number of KMS keys in the persistent store, including those that do not match the search criteria.

Component	***Description***
KMIP Summary Statistics	These are the statistics specific to KMIP-managed objects. These are as follows: ▪ **Total KMIP keys meeting search criteria**: This is the total number of KMIP symmetric keys matching the search criteria for the query given in Saved Query Name. The Key Listing page displays the results for KMIP symmetric keys only. Other KMIP-managed objects that are not symmetric keys will not be returned even if they meet the search criteria. There may be more KMIP keys matching the search criteria than what is returned in the results. ▪ **Total KMIP keys returned in results**: This is the total number of KMIP symmetric key objects returned in the key listing results. If the value of Total KMIP keys meeting search criteria is less than 3,000, then the values of Total KMIP keys meeting search criteria and Total KMIP keys returned in results will be the same. Other KMIP-managed objects that are not symmetric keys will not be returned in the results even if they meet the search criteria. ▪ **Total KMIP symmetric key objects**: This is the total number of KMIP symmetric key objects in the persistent store, including those that do not match the search criteria. ▪ **Total KMIP Objects**: This is the total number of KMIP-managed objects, including those that are not symmetric keys. This includes digital certificates, asymmetric keys, opaque objects, templates and other KMIP-managed objects.

The following figure shows the key listing for **All-type Queries**.



Query: [All]

Items per page: 20

	Type	▲ Key Name	UUID	Owner	Algorithm	Creation Date	FIPS Security Level
●	KMIP	0259fa89-68d0-467c-89ca-5d89d87cf514	0259fa89-68d0-467c-89ca-5d89d87cf514	kmip_user1	AES-256	2019-05-23 14:18:32	1
○	KMIP	154148ca-5786-4fb4-b308-7429b8ae046a	154148ca-5786-4fb4-b308-7429b8ae046a	kmip_user1	AES-256	2019-05-23 14:20:22	2
○	KMIP	1a918497-ef25-45d2-9065-0c818afb251d	1a918497-ef25-45d2-9065-0c818afb251d	kmip_user1	AES-256	2019-05-23 14:18:21	1
○	KMIP	1d6c6f34-d1ed-490f-b250-23f9f4282bd4	1d6c6f34-d1ed-490f-b250-23f9f4282bd4	kmip_user1	AES-256	2019-05-23 14:17:22	1
○	ESKM	key_01	-	itest	AES-256	2019-03-14 01:37:58	2
○	ESKM	key_02	-	itest	AES-256	2019-04-12 12:23:03	1
○	ESKM	key_04	-	itest	AES-256	2019-04-12 12:30:06	1
○	ESKM	key_05	-	itest	AES-256	2019-05-23 10:30:59	2
○	ESKM	key_06	-	itest	AES-256	2019-05-23 10:33:39	1

1 - 9 of 9

Figure 71 : Key Listing for All-type Queries

The following table describes the components of the **Keys** section that are common across all query types — All, ESKM, and KMIP.

Table 34: Components of the results of an All-type query

Component	***Description***
Query	Select the query to apply to the page.
Run Query	Select this button to run a query. This Management Console displays a subset of the available keys and their corresponding columns.
Create	Click to create a KMS key. ⚠ Only KMS keys can be created from the Management Console. To create KMIP keys, use the KMIP client and request operations.
Delete	Click to delete a key. ❗ Exercise extreme caution when deleting keys. Unless you have a backup of the key, you will not be able to decrypt any ciphertext created by that key.

Component	***Description***
Convert	Converts a symmetric key. If you click the **Convert** button with a KMS key selected, the KMS key is converted to KMIP format while retaining the key data. If you click the **Convert** button with a KMIP key selected, the KMIP key is converted to KMS format retaining the custom attributes, owner username, cryptographic algorithm and cryptographic length; all other KMIP attributes are not converted. Only KMIP keys in the Pre-Active and Active state can be converted to KMS format. KMIP keys in the Deactivated, Compromised, or Destroyed states cannot be converted.
Properties	Click **Properties** to view the properties of a key.

The following table describes the columns of the results of **All-type** queries.

Table 35: Columns of the results of an All-type query

Component	***Description***
Type	The key type. This is either ESKM for KMS keys or KMIP for KMIP symmetric keys.
Key Name	This is the name that the ESKM appliance uses to refer to the key. KMS keys are identified by their key names, so there is a unique key name for each KMS key. Naming KMIP keys is optional. Therefore, KMIP symmetric keys may have no name, a single name, or multiple key names. KMIP keys with no name will have a hyphen (-) in this column. KMIP keys with multiple names will have each key name separated by a comma.
UUID	The unique identifier for the KMIP key. KMIP-managed objects are identified by UUIDs. For KMS keys, this value is a hyphen (-), because KMS keys do not have UUIDs.

Component	***Description***
Owner	The owner is typically the user who created the key. The implications of key ownership differ depending on whether this is an KMS or KMIP key. For KMS keys: ▪ If an owner is listed for the key, then that user is the only user who can access the key (unless additional group permissions have been granted for the key). ▪ If the key was created in an unauthenticated ESKM XML session, or if no owner was specified when the key was created on the Management Console, then the key is global, in which case the Owner Username would be **[None]**. Global keys can be accessed by all users. For KMIP keys: ▪ All users who are in the same user group as the owner are able to access the key. To ensure that no other user, except the key owner can access the key, configure a user group with only that key owner in it, with privileges to access the target object group.

Component	***Description***
Algorithm	The cryptographic algorithm used to create the key. The set of cryptographic algorithms available for key creation differs depending on whether this is an KMS or KMIP key. For KMS keys, the algorithm may be any of the following: ▪ AES-256 ▪ AES-192 ▪ AES-128 ▪ DES-EDE-168 (three key triple DES) ▪ DES-EDE-112 (two key triple DES) ▪ DES ▪ RC4-128 ▪ RC4-40 ▪ Hmac-SHA1 ▪ RSA-2048 ▪ RSA-1024 ▪ RSA-512 ⚠ Some of these algorithms are not available when the appliance is running in FIPS-compliant mode. A more extensive set of cryptographic algorithms are available for KMIP keys. See the OASIS website at https://www.oasis-open.org/standards for more information on the KMIP protocol specification which documents the full list of supported cryptographic algorithms.
Creation Date	This is the date when the key was created.

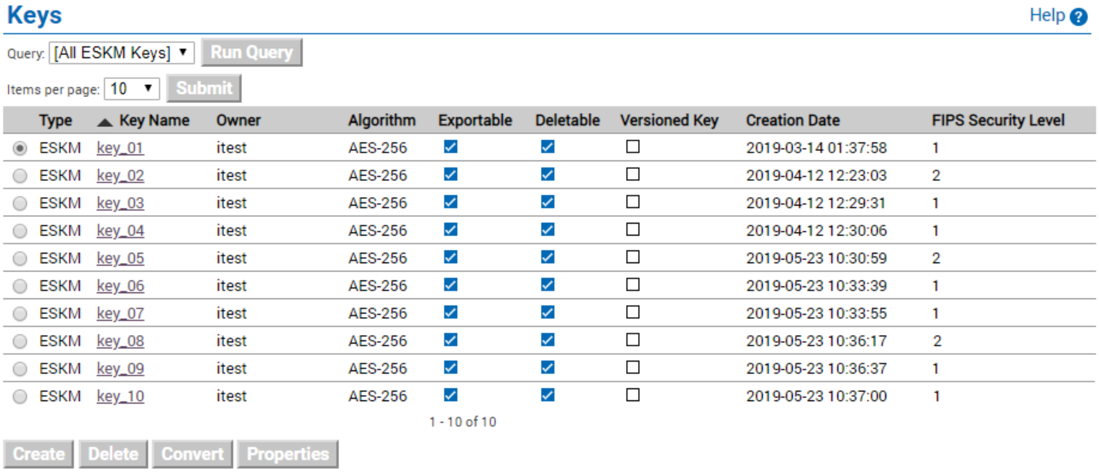
Component	*Description*
FIPS Security Level	The security level of the device where the key was created.

6.4.3.2 Displaying search results for KMS-type queries

A KMS-type query is one which returns only KMS keys matching the search criteria. Since this type of query returns only KMS keys, the number of available search criteria is more extensive than that available for All-type queries.

In contrast to All-type queries, where there is a limit to the number of search results returned, all search results matching the query criteria are returned for KMS-type queries.

The following figure provides a listing for the built-in KMS-type query [All ESKM keys].



Query: [All ESKM Keys]

Items per page: 10

	Type	▲ Key Name	Owner	Algorithm	Exportable	Deletable	Versioned Key	Creation Date	FIPS Security Level
●	ESKM	key_01	itest	AES-256	☑	☑	□	2019-03-14 01:37:58	1
○	ESKM	key_02	itest	AES-256	☑	☑	□	2019-04-12 12:23:03	2
○	ESKM	key_03	itest	AES-256	☑	☑	□	2019-04-12 12:29:31	1
○	ESKM	key_04	itest	AES-256	☑	☑	□	2019-04-12 12:30:06	1
○	ESKM	key_05	itest	AES-256	☑	☑	□	2019-05-23 10:30:59	2
○	ESKM	key_06	itest	AES-256	☑	☑	□	2019-05-23 10:33:39	1
○	ESKM	key_07	itest	AES-256	☑	☑	□	2019-05-23 10:33:55	1
○	ESKM	key_08	itest	AES-256	☑	☑	□	2019-05-23 10:36:17	2
○	ESKM	key_09	itest	AES-256	☑	☑	□	2019-05-23 10:36:37	1
○	ESKM	key_10	itest	AES-256	☑	☑	□	2019-05-23 10:37:00	1

1 - 10 of 10

Figure 72 : Key Listing for KMS-type Queries

The following table describes the columns of the results for KMS-type queries.

Table 36: Columns of the results of KMS-type Queries

Component	*Description*
Type	The key type. Since this is a KMS-type query, this is always ESKM.

Component	***Description***
Key Name	This is the name that the ESKM appliance uses to refer to the key. KMS keys are identified by their key names, so there is a unique key name for each key.
Owner	The owner is typically the user who created the key. If an owner is listed for the key, then that user is the only user who can access the key (unless additional group permissions have been granted for the key). If the key was created in an unauthenticated ESKM XML session, or if no owner was specified when the key was created on the Management Console, then the key is global, in which case the Owner Username would be **[None]**. Global keys can be accessed by all users.

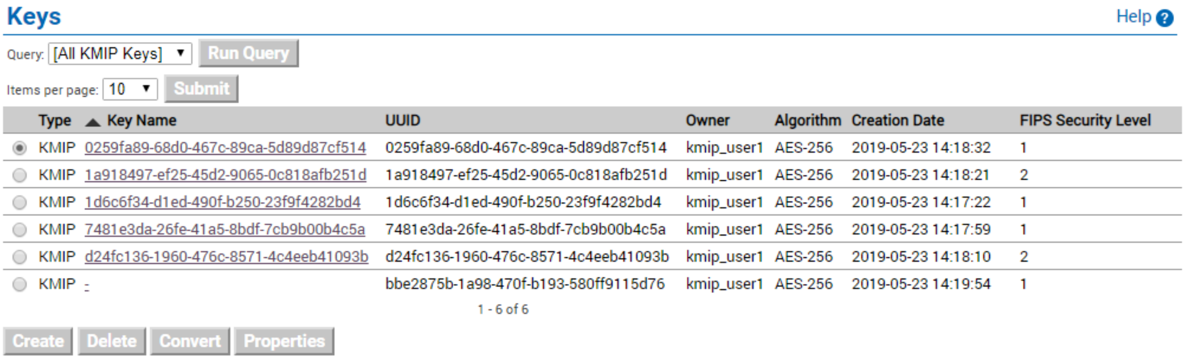
Component	***Description***
Algorithm	The cryptographic algorithm used to create the key. As this is a KMS key, the algorithm may be any of the following: ▪ AES-256 ▪ AES-192 ▪ AES-128 ▪ DES-EDE-168 (three key triple DES) ▪ DES-EDE-112 (two key triple DES) ▪ DES ▪ RC4-128 ▪ RC4-40 ▪ Hmac-SHA1 ▪ RSA-2048 ▪ RSA-1024 ▪ RSA-512 ⚠ Some of these algorithms are not available when the ESKM appliance is running in FIPS-compliant mode.
Exportable	An exportable key can be exported by its owner and by members of a group with "Export" permission for the key. Global keys marked exportable can be exported by any user.
Deletable	A check mark in the box indicates that the key is deletable via an ESKM XML request. If a key is marked deletable, only the owner can delete it. Global keys marked deletable can be deleted by any user.
Versioned Key	Indicates if this is a versioned key.

Component	*Description*
Creation Date	This is the date when the key was created.
FIPS Security Level	The security level of the device where the key was created.

6.4.3.3 Displaying search results for KMIP-type queries

A KMIP-type query is one which returns only KMIP symmetric keys matching the search criteria. If you need to search for KMIP objects of type other than symmetric key, go to **Security** > **Keys & KMIP Objects** > **KMIP Objects**. Since this type of query returns only KMIP keys, the available search criteria is more extensive than that available for All-type queries. KMIP-managed objects also contain more metadata than KMS keys, so the available search criteria is also more extensive than that available for KMS-type queries.

In contrast to All-type queries, where there is a limit to the number of search results returned, all search results matching the query criteria are returned for KMIP-type queries.



Query: [All KMIP Keys] ▼

Items per page: 10 ▼

	Type	▲ Key Name	UUID	Owner	Algorithm	Creation Date	FIPS Security Level
●	KMIP	0259fa89-68d0-467c-89ca-5d89d87cf514	0259fa89-68d0-467c-89ca-5d89d87cf514	kmip_user1	AES-256	2019-05-23 14:18:32	1
○	KMIP	1a918497-ef25-45d2-9065-0c818afb251d	1a918497-ef25-45d2-9065-0c818afb251d	kmip_user1	AES-256	2019-05-23 14:18:21	2
○	KMIP	1d6c6f34-d1ed-490f-b250-23f9f4282bd4	1d6c6f34-d1ed-490f-b250-23f9f4282bd4	kmip_user1	AES-256	2019-05-23 14:17:22	1
○	KMIP	7481e3da-26fe-41a5-8bdf-7cb9b00b4c5a	7481e3da-26fe-41a5-8bdf-7cb9b00b4c5a	kmip_user1	AES-256	2019-05-23 14:17:59	1
○	KMIP	d24fc136-1960-476c-8571-4c4eeb41093b	d24fc136-1960-476c-8571-4c4eeb41093b	kmip_user1	AES-256	2019-05-23 14:18:10	2
○	KMIP	-	bbe2875b-1a98-470f-b193-580ff9115d76	kmip_user1	AES-256	2019-05-23 14:19:54	1

1 - 6 of 6

Figure 73 : Key Listing for KMIP-type Queries

The following table describes the columns of the results of KMIP-type queries.

Table 37: Columns of the results of KMIP-type queries

Component	*Description*
Type	The key type. Because this is a KMIP-type query, this is always KMIP.

Component	***Description***
Key Name	This is the name that the ESKM appliance uses to refer to the key. Naming KMIP keys is optional. Therefore, KMIP symmetric keys may have no name, a single name, or multiple key names. KMIP keys with no name will have a hyphen (-) in this column. KMIP keys with multiple names will have each key name separated by commas.
UUID	The unique identifier for KMIP keys. KMIP-managed objects are identified by UUIDs.
Owner	The owner is typically the user who created the key. All users who are in the same user group as the owner will be able to access the key. To ensure that no other user besides the key owner can access the key, configure a user group with only that key owner in it, with privileges to access the target object group.

Component	***Description***
Algorithm	The cryptographic algorithm used to create the key, with the key length if applicable. See the OASIS website at https://www.oasis-open.org/standards for more information about the KMIP protocol specification, which documents the full list of supported cryptographic algorithms. ▪ DES ▪ 3DES ▪ AES ▪ RSA ▪ DSA ▪ ECDSA ▪ HMAC-SHA1 ▪ HMAC-SHA224 ▪ HMAC-SHA256 ▪ HMAC-SHA384 ▪ HMAC-SHA512 ▪ HMAC-MD5 ▪ DH ▪ ECDH ▪ ECMQV ▪ Blowfish ▪ Camellia ▪ CAST5 ▪ IDEA

Component	***Description***
	▪ MARS ▪ RC2 ▪ RC4 ▪ RC5 ▪ SKIPJACK ▪ Twofish ▪ ChaCha20 ▪ Poly1305 ▪ Chacha20Poly1305 ⚠ Some of these algorithms are not available when the appliance is running in FIPS-compliant mode.
Creation Date	This is the date when the key was created.
FIPS Security Level	The security level of the device where the key was created.

6.4.4 Key properties

Key Properties allow you to view the properties of the selected key. KMS keys do not have the same properties as KMIP keys. For more information on key properties, see KMS key properties (p. 245) and KMIP key general properties (p. 255).

6.4.5 KMS key properties

Clicking the KMS key name (hypertext link) or selecting the KMS key, and then clicking the Properties button displays these tabs:

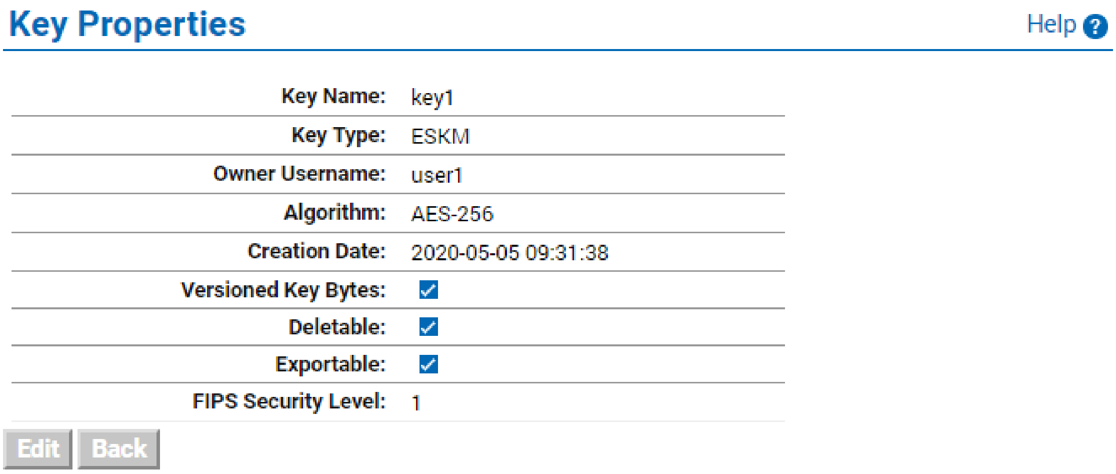
- KMS key properties

- KMS key group permissions (p. 249)
- KMS custom attributes (p. 252)
- KMS versioned keys (p. 253)

Key Properties allow you to view the general properties of the KMS key. You can only edit Key Name, Owner Username, whether it's deletable, and whether it's exportable. The Audit Log captures any changes to these fields.

If you change the Key Name or Owner, you must update your applications accordingly. Changing the Key Name does not create an additional key. Instead, it gives a new name to the existing metadata and key bytes. To create a copy of an existing key, use Clone Key.

The following figure shows an example of **Key Properties**.



Key Properties

Key Name:	key1
Key Type:	ESKM
Owner Username:	user1
Algorithm:	AES-256
Creation Date:	2020-05-05 09:31:38
Versioned Key Bytes:	☑
Deletable:	☑
Exportable:	☑
FIPS Security Level:	1

Figure 74 : Key Properties

The following table describes the components of **Key Properties**.

Table 38: Key Properties components

Component	***Description***
Key Name	Name of key described in the current row.
Key Type	The key type. For KMS keys, the key type is ESKM.

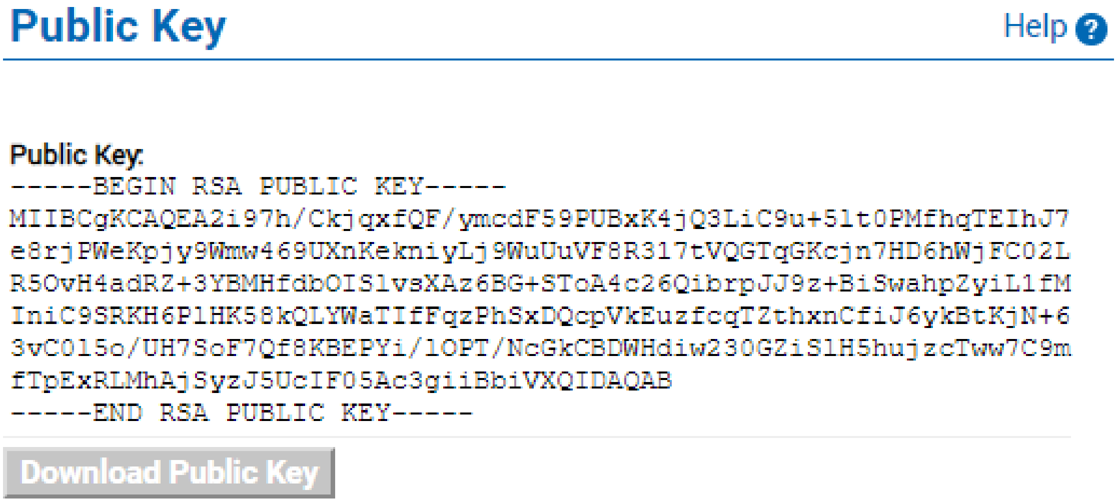
Component	***Description***
Owner Username	Name of the user who owns the key. If blank, the key is a global key and therefore accessible to all users. ⚠ Once a key has an owner, it is no longer a global key. You cannot change it into a global key by removing the owner. This is true even if the key was originally created as a global key.
Algorithm	The algorithm this key uses.
Creation Date	The date and time of the key's creation.
Default IV	Displays the default Initialization Vector (IV) generated by the ESKM appliance when this AES or 3DES key was created or imported. RSA and HMAC keys do not have IVs. ⚠ You cannot specify a default initialization vector for a KMS key via the web administration interface.
Versioned Key Bytes	Indicates if this is a versioned key.
Deletable	If selected, this key is deletable via an ESKM XML request by the key owner. A deletable key may be deleted by its owner and by members of a group with "Full" permission for the key. A global key marked deletable can be deleted by any user. This value may be changed.
Exportable	If selected, this key is exportable via an ESKM XML request. An exportable key can be exported by its owner and by members of a group with "Export" permission for the key. A global key marked exportable can be exported by any user. This value may be changed.
FIPS Security Level	The security level of the device where the key was created.

Component	***Description***
Edit	Click **Edit** to edit the Key Name, Owner Username, Exportable, and Deletable settings.
Back	Click **Back** to return to the Key and Policy Configuration page.

KMS RSA public key

When the KMS key is an RSA key, the Key and Policy Configuration page will also include the Public Key section, which allows you to view and download the public portion of the RSA key.

The following figure shows an example of the **Public Key** section.



Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEA2i97h/CkjqxfQF/ymcdF59PUBxK4jQ3LiC9u+5lt0PMfhqTEIhJ7
e8rjPWeKpjy9Wmw469UXnKekniyLj9WuUuVF8R317tVQGTqGKcjn7HD6hWjFC02L
R5OvH4adRZ+3YBMHfdbOIS1vsXAz6BG+SToA4c26QibrpJJ9z+BiSwahpZyiL1fM
IniC9SRKH6PlHK58kQLYWaTIfFqzPhSxDQcpVkEuzfcqTZthxnCfiJ6ykBtKjN+6
3vC015o/UH7SoF7Qf8KBEPYi/1OPT/NcGkCBDWHdiw230GZiSlH5hujzcTww7C9m
fTpExRLMhAjSyzJ5UcIF05Ac3giiBbiVXQIDAQAB
-----END RSA PUBLIC KEY-----
```

Figure 75 : Public Key

The following table describes the components of the **Public Key** section.

Table 39: Public Key components

Component	***Description***
Public Key	Displays the public key.
Download Public Key	Click **Download Public Key** to download the RSA public key.

6.4.5.1 KMS key group permissions

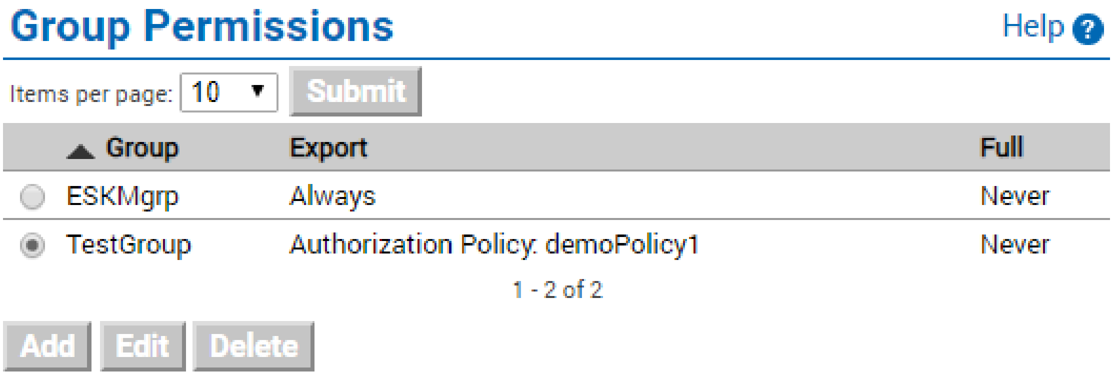
Use Group Permissions to modify the permissions for a KMS key. KMS key permissions are granted at the group level. To assign permissions to a specific user, you must include that user in a group and then assign permissions to the group. To assign an authorization policy to a key, you must first define the policy. The owner of a key implicitly has permissions to perform all applicable operations using the key, even if that user belongs to a group for which permissions are restricted.

> You cannot set group permissions for global keys; all users can access global keys for any applicable operation. For non-global keys, if a user is not the owner and is not a member of a group with permissions to use the key, the user cannot access the key.

For example, in the below figure, members of **group1** have the same permissions as key's owner. Members of **group2** can only export a key. A user who is a member of group1 and group2 always has permission to export a key.

When a user is a member of multiple groups, the user inherits the union of the group permissions.

The following figure shows an example of **Group Permissions**.



Group Permissions

Items per page: 10

	▲ Group	Export	Full
○	ESKMgrp	Always	Never
●	TestGroup	Authorization Policy: demoPolicy1	Never

1 - 2 of 2

Figure 76 : Group Permissions

The following table describes the components of **Group Permissions**.

Table 40: Group Permissions components

Component	***Description***
Group	Displays the groups that have permission to use the key. These groups are defined on either the Local Users and Groups page (when using a local user directory) or on the LDAP server (when using an LDAP user directory). If you are assigning an authorization policy to this key, you must first define the policy.
Export	The operation available to the user group for this key. You can assign this operation using the following options: ▪ **Always**: members of the group can always perform the operation with the key. ▪ **Never**: members of the group cannot perform the operation with the key. ▪ **Authorization Policy**: members of the group can always perform the operation with the key according to the terms of the authorization policy. ⚠ Export permission is only applicable if the key is exportable.

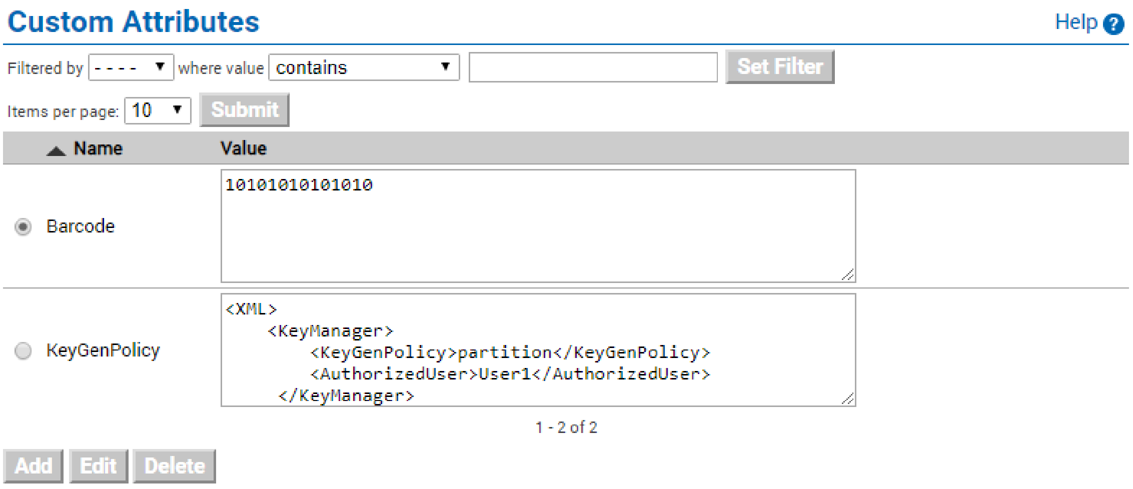
Component	***Description***
Full	Full permission allows users to perform the same key operations available to key owners. Key export is only allowed if the key is exportable. Key deletion is only allowed if the key is deletable. You can assign Full permission using the following options: ▪ **Always**: members of the group can always perform the key operations available under Full permission for that key. There will be no restrictions. ▪ **Never**: allows the administrator to remove the previously set Full permission for a group without deleting the group from the Group Permissions table. ⚠ Full permission will not provide the option to set the Authorization Policy. If the Always option for the Full permission is set after the Authorization Policy for the Export permission was set, the ESKM appliance will ignore the Export Authorization Policy and automatically select the Always option for Export.
Edit	Click **Edit** to modify existing permissions for a group.
Add	Click **Add** to give permissions to a group that uses the key. ⚠ You cannot add group permissions to global keys or certificates.
Delete	Click **Delete** to remove the permissions for a group. Once the group is deleted, the group permission is also removed from key(s) and the group permission will not be restored if group is re-added.

⚠ It is not possible to specify a value of Never for both the Export and Full permissions in a user group.

6.4.5.2 KMS custom attributes

Use Custom Attributes to assign custom attributes to the key. You can assign a maximum of 200 custom attributes. Before assigning custom attributes, you must first create them using **Custom Attributes**.

The following figure shows an example of **Custom Attributes**.



Name	Value
● Barcode	10101010101010

○ KeyGenPolicy	`<XML>`
	`<KeyManager>`
	`<KeyGenPolicy>partition</KeyGenPolicy>`
	`<AuthorizedUser>User1</AuthorizedUser>`
	`</KeyManager>`

Figure 77 : Custom Attributes

The following table describes the components of **Custom Attributes**.

Table 41: Custom Attributes components

Component	***Description***
Name	Enter a unique attribute name. Attribute names can contain alphanumeric characters, hyphens, underscores, and periods. Do exclude whitespaces in the name. In addition, the first character of the name must be a letter. Maximum length is 64 characters.
Value	Enter the value of the attribute. This can contain any printable ASCII characters and spaces, tab,**\n** and **\r**. Maximum length is 4096 characters.

Component	Description
Edit	Click **Edit** to alter the selected attribute.
Add	Click **Add** to add an attribute.
Delete	Click **Delete** to remove the selected attribute.

6.4.5.3 KMS versioned keys

A KMS versioned key maintains the same key metadata, but has a unique set of bytes for each version. Thus, each version is different enough for encryption purposes, but similar enough to allow for easy management. Each key version has its own key bytes, default IV, state, and creation date. The state determines which key operations are available for a key version. Possible states are: active, restricted, and retired.

- **Active**—all key management options are allowed.
- **Restricted**—only key information operations are allowed.
- **Retired**—no operations or access to key management is allowed.

The state, combined with the key type and group permissions determine how the key version can be used. Ultimately, a key version can only be used when:

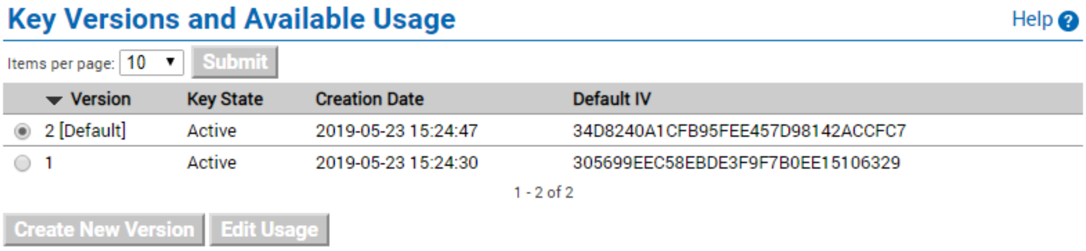
- The key’s group permissions permit the operation
- The key version’s state permits the operation
- The request comes from a member of the permitted group

A key can have a maximum of 4,000 versions. The size of the key blob limits the number of versions (per key) that can be replicated in a cluster. To ensure successful replication to all nodes in a cluster, Utimaco recommends limiting the number of versions (per key) to 30. ESKM clients that issue key version generate requests (i.e. **KeyVersionGenRequest**) on a versioned key should wait five seconds between key version generation requests.

Key versions and available usage

A **Key Versions** tab appears in the **Properties** page for versioned keys. Use this to create new key versions and manage how those versions are used. All versions of a KMS key have the same metadata (found on the Key Properties, Permissions, and Custom Attributes). The version number, key state, creation date, default IV, and key bytes differ for each key version. The latest key version is automatically the default version.

The following figure shows an example of **Key Versions and Available Usage**.



Items per page: 10 ▼

	Version	Key State	Creation Date	Default IV
●	2 [Default]	Active	2019-05-23 15:24:47	34D8240A1CFB95FEE457D98142ACCFC7
○	1	Active	2019-05-23 15:24:30	305699EEC58EBDE3F9F7B0EE15106329

1 - 2 of 2

Figure 78 : Key Versions and Available Usage

Table 42: Key Versions and Available Usage components

Component	***Description***
Version	Displays the version of the key. This number is automatically assigned. You can have a maximum of 4,000 versions of a key. The latest version is automatically the default version - this will be the key used when cryptographic and information requests do not specify a version number.
Key State	Describes how the key can be used. A key version can be in one of three states: ▪ Active - All key management options are allowed. The number of active key versions must be less than the Number of active versions allowed for a key field on Active Versions. ▪ Restricted - Only decryption (MAC Verify for HmacSHA1 keys, Sign Verify for RSA keys) and key-info operations are allowed. ▪ Retired - No access is allowed.
Creation Date	The date and time of the version’s creation.

Component	***Description***
Default IV	The IV only appears for AES and DES keys.
Create New Version	Click **Create New Version** to create a new key version.
Edit Usage	Select a version, and then click **Edit Usage** to change the Key State.

6.4.6 KMIP key properties

The KMIP key properties can be displayed in two ways:

- click the link for the KMIP key name
- select the KMIP key, and then click the **Properties** button

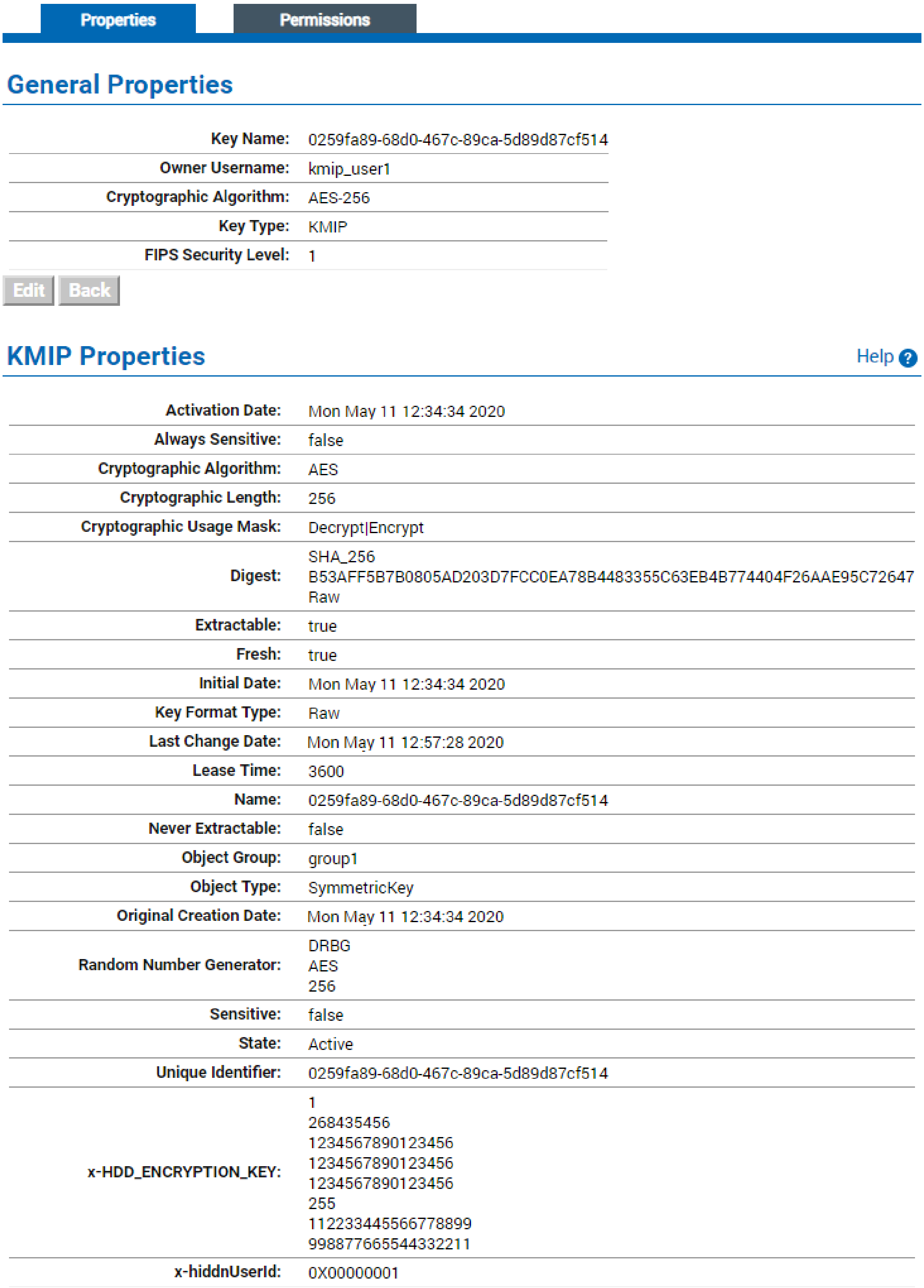
Because KMIP keys contain different metadata than KMS keys, they also have different properties. These properties can be categorized as follows:

- KMIP key general properties (p. 255)
- KMIP group permissions (p. 263)

6.4.6.1 KMIP key general properties

The KMIP key general properties refer to KMIP attributes. These attributes may be either set by the client during a **Create or Register** request operation, or set by the KMIP server, and are displayed in the **Properties** tab. The KMIP attributes displayed at the Management Console are similar to what is returned when the KMIP client issues a **Get Attributes** request operation.

The following figure shows an example of **General Properties** and **KMIP Properties**.



General Properties

Key Name:	0259fa89-68d0-467c-89ca-5d89d87cf514
Owner Username:	kmip_user1
Cryptographic Algorithm:	AES-256
Key Type:	KMIP
FIPS Security Level:	1

KMIP Properties

Activation Date:	Mon May 11 12:34:34 2020
Always Sensitive:	false
Cryptographic Algorithm:	AES
Cryptographic Length:	256
Cryptographic Usage Mask:	Decrypt|Encrypt
Digest:	SHA_256 B53AFF5B7B0805AD203D7FCC0EA78B4483355C63EB4B774404F26AAE95C72647 Raw
Extractable:	true
Fresh:	true
Initial Date:	Mon May 11 12:34:34 2020
Key Format Type:	Raw
Last Change Date:	Mon May 11 12:57:28 2020
Lease Time:	3600
Name:	0259fa89-68d0-467c-89ca-5d89d87cf514
Never Extractable:	false
Object Group:	group1
Object Type:	SymmetricKey
Original Creation Date:	Mon May 11 12:34:34 2020
Random Number Generator:	DRBG AES 256
Sensitive:	false
State:	Active
Unique Identifier:	0259fa89-68d0-467c-89ca-5d89d87cf514
x-HDD_ENCRYPTION_KEY:	1 268435456 1234567890123456 1234567890123456 1234567890123456 255 112233445566778899 998877665544332211
x-hiddnUserId:	0X00000001

Figure 79 : General and KMIP properties

All KMIP attributes in **KMIP Properties** are read-only, and cannot be modified via the Management Console. The number and type of attributes may differ across KMIP-managed objects, and multiple instances of an attribute may exist where allowed by the KMIP specification. To make changes to these attributes, use the KMIP client **Add Attribute**, **Modify Attribute,** and **Delete Attribute** request operations to add, modify and delete KMIP attributes for the given KMIP-managed object.

A summary of available KMIP attributes and their descriptions are provided in the following table. If the value of the Type field is Mandatory, the attribute must always exist for a given KMIP object type. See the KMIP version 1.0, 1.1 and 1.2 specification for more information on each attribute.

Table 43: KMIP Attributes

Attribute Name	***Type***	***Description***
Unique Identifier	Mandatory	The unique identifier is generated by the ESKM appliance to uniquely identify the KMIP object.
Name	Optional	The name attribute is used to identify and locate the object.
Object Type	Mandatory	The Object Type of a managed object (public key, private key, symmetric key, etc) is set by the ESKM appliance, when the object is created or registered.
Cryptographic Algorithm	Mandatory	The cryptographic algorithm of an object, e.g. RSA, DSA, AES.
Cryptographic Length	Mandatory	For keys, this is the length in bits of the clear-text cryptographic key material of the managed object. For certificates, this is the length in bits of the public key contained within the certificate.
Cryptographic Parameters	Optional	Contains a set of optional fields that describe certain cryptographic parameters to be used when performing cryptographic operations using the object.

Attribute Name	***Type***	***Description***
Cryptographic Domain Parameters	Optional	Contains a set of optional fields that may need to be specified in the Create Key Pair request payload.
Certificate Type	Mandatory	The certificate type is set by the ESKM appliance when the certificate is created or registered.
Certificate Length	Mandatory	The length in bytes of the Certificate object.
X.509 Certificate Identifier	Mandatory	The X.509 Certificate Identifier attribute is used to provide identification of an X.509 public key certificate. This contains the Issuer Distinguished Name and Certificate Serial Number.
X.509 Certificate subject	Mandatory	The X.509 Certificate Subject attribute is a structure used to identify the subject of a X.509 certificate. This contains the Subject Distinguished Name and optionally one or more Subject Alternate Names.
X.509 Certificate Issuer	Mandatory	The X.509 Certificate Issuer is a structure used to identify the issuer of a X.509 certificate, containing the Issuer Distinguished Name.
Certificate Identifier	Mandatory	The Certificate Issuer attribute is used to provide the identification of a certificate. This attribute is deprecated as of KMIP version 1.1.
Certificate Subject	Mandatory	The Certificate Subject is used to identify the subject of a certificate. This attribute is deprecated as of KMIP version 1.1.
Certificate Issuer	Mandatory	The Certificate Issuer is used to identify the issuer of a certificate. This attribute is deprecated as of KMIP version 1.1.

Attribute Name	***Type***	***Description***
Digital Signature Algorithm	Mandatory	This identifies the digital signature algorithm associated with a digitally signed object, such as a certificate.
Digest	Mandatory	The Digest attribute contains the digest value of the key or secret data, certificate, or opaque object.
Operation Policy Name	Optional	The operation policy controls what entities may perform which key management operations on the object. This attribute is not interpreted by the ESKM appliance; it is simply stored and displayed.
Cryptographic Usage Mask	Mandatory	The Cryptographic Usage Mask defines the cryptographic usage of a key. This is a bit mask that indicates which cryptographic functions may be performed using the key, and which may not be performed. Examples of cryptographic operations include Sign, Verify, Encrypt, Decrypt, Export, Wrap Key, and Unwrap Key.
Lease Time	Optional	The Lease Time attribute defines a time interval for a managed cryptographic object beyond which the client shall not use the object without obtaining another lease.
Usage Limits	Optional	The Usage Limits attribute is a mechanism for limiting the usage of a managed cryptographic object.
State	Mandatory	This is the State of an object as known to the ESKM appliance. Valid object states are Pre-Active, Active, Deactivated, Compromised, Destroyed, and Destroyed Compromised.
Initial Date	Mandatory	The Initial Date is the date and time when the Managed Object was first created or registered at the ESKM appliance.
Activation Date	Optional	This is the date and time when the managed cryptographic object may begin to be used.

Attribute Name	***Type***	***Description***
Process Start Date	Optional	This is the date and time when a managed symmetric key object may begin to be used to process cryptographically protected information such as decryption or unwrapping, depending on the value of its cryptographic mask attribute.
Protect Stop Date	Optional	This is the date and time when a managed symmetric key object shall not be used for applying cryptographic protection, encryption or wrapping, depending on the value of its cryptographic mask attribute.
Deactivation Date	Optional	This is the date and time when the managed cryptographic object shall not be used for any purpose, except for decryption, signature verification, or unwrapping.
Destroy Date	Optional	This is the date and time when the managed object is destroyed.
Compromise Occurrence Date	Optional	This is the date and time when the managed cryptographic object was first believed to be compromised.
Compromise Date	Optional	This is the date and time when the managed cryptographic object entered into the compromised state.
Revocation Reason	Optional	The Revocation Reason indicates why the managed cryptographic object was revoked.
Archive Date	Optional	The Archive Date is the date and time when the managed object was placed in archival storage.
Object Group	Optional	An object always belongs to the default object group configured by the KMIP user upon creation, if the Object Group attribute is not specified. If the Object Group attribute is specified, the object belongs to that object group.

Attribute Name	***Type***	***Description***
Fresh	Optional	This boolean attribute indicates if the object has not yet been served to a client.
Link	Optional	The Link attribute is used to create a link from one managed cryptographic object to another closely related target managed cryptographic object.
Application Specific Information	Optional	The Application Specific Information attribute is used to store the data specific to the application using the managed object. It consists of the Application Namespace and Application Data fields.
Contact Information	Optional	The content of the Contact Information attribute is used for contact purposes only and not for policy enforcement.
Last Change Date	Mandator y	This is the date and time of the last change to the contents or attributes of the managed object.
Custom Attribute	Optional	This is a client or ESKM appliance defined attribute intended for vendor-specific purposes. It is created by the client and not interpreted by the ESKM appliance.
Alternative Name	Optional	The Alternative Name attribute is used to identify and locate the object. This attribute is assigned by the client, and is intended to be in a form that humans are able to interpret.
Key Value Present	Optional	This is a managed object attribute created by the ESKM appliance. It shall not be specified by the client in a register request.
Key Value Location	Optional	This is a managed object attribute. It may be specified by the client when the Key Value is omitted from the Key Block in a register request.

Attribute Name	***Type***	***Description***
Original Creation Date	Optional	This attribute contains the date and time when the object was created originally. This can be different from when the object is registered with a ESKM appliance.
Random Number Generator	Optional	The Random Number Generator attribute contains the details of the random number generator used during the creation of the managed cryptographic object.
PKCS#12 Friendly Name	Optional	This attribute if supplied on a Register Private Key with Key Format Type PKCS#12, it informs the ESKM appliance of the alias or friendly name under which the private key and its associated certificate chain shall be found in the Key Material.
Description	Optional	The Description attribute and its content is used for informational purposes only. It is not used for policy enforcement.
Comment	Optional	The Comment attribute and its content are used for informational purposes only. It is not used for policy enforcement. The attribute is set by the client or the ESKM appliance.
Sensitive	Mandatory	If the value is set to True, then the ESKM appliance shall prevent the object value from being retrieved via the Get operation unless it is wrapped by another key.
Always Sensitive	Mandatory	The ESKM appliance shall set the value to: ▪ True, if the Sensitive attribute has always been True ▪ False, if the Sensitive attribute has ever been set to False

Attribute Name	***Type***	***Description***
Extractable	Mandatory	If set as False, then the ESKM appliance shall prevent the object value from being retrieved via the Get operation. If no value is provided by the client, then the same shall be set to True.
Never Extractable	Mandatory	The ESKM appliance shall set the value to: ▪ True, if the Extractable attribute has always been False ▪ False, if the Extractable attribute has ever been set to True.

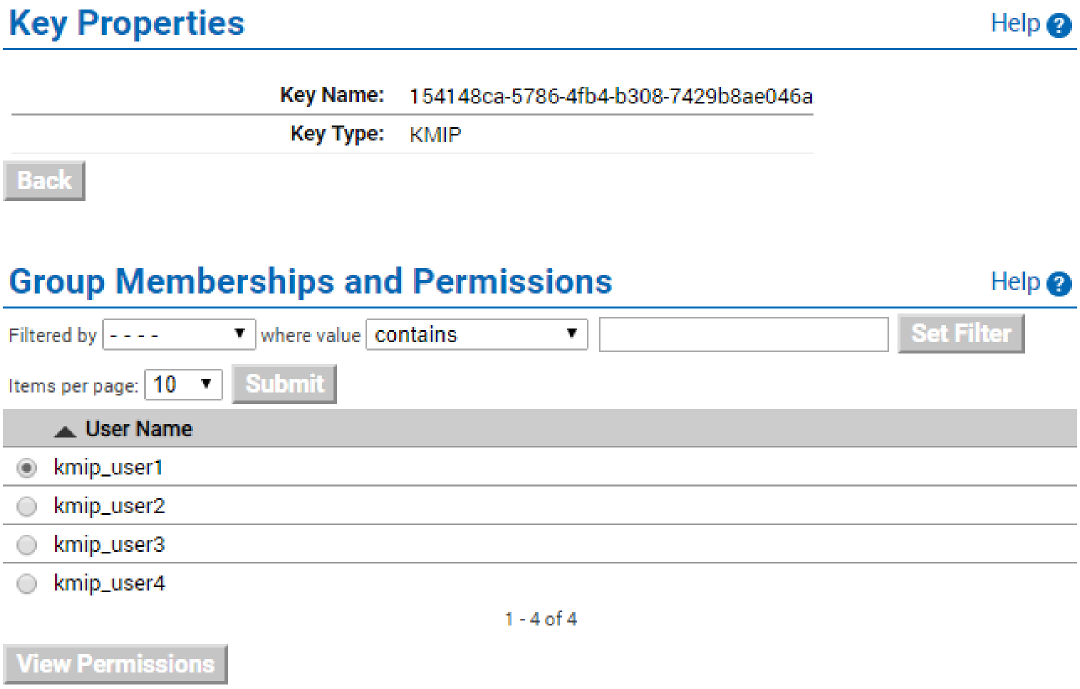
6.4.6.2 KMIP group permissions

The **Group Permissions** tab shows which users have permissions to perform operations on the KMIP-managed object.
Users listed in the **Group Memberships and Permissions** tab have at least one privilege to perform KMIP operations on this object. The permissions listed in this section is the union of all the permissions that this user has, depending on his group memberships.

For example, suppose this user is a member of the KMIP group, **EngineeringUsers,** with **Create** and **Get Attributes** permission but not **Destroy** permission. This user is also a member of the KMIP group, **ProductionUsers,** with **Destroy** permission. This user has **Create**, **Get Attributes,** and **Destroy** permission because of the membership in the two KMIP groups.

User permissions cannot be modified from here. Configured permissions are on a group basis, and apply to all members of the user group. To modify group permissions, go to the **Local Users & Groups** > **Local Groups**, select the group to modify, and then click **Properties**. The group permissions can then be viewed and modified in the **Permissions** tab.

The following sample KMIP group permissions page shows that KMIP-enabled users, “kmip_user1” and “kmip_user2”, have at least one type of permission to perform operations on this KMIP object.



Key Properties

Help

Key Name:	154148ca-5786-4fb4-b308-7429b8ae046a
Key Type:	KMIP

Group Memberships and Permissions

Help

Filtered by - - - - where value contains

Items per page: 10

	User Name
●	kmip_user1
○	kmip_user2
○	kmip_user3
○	kmip_user4

1 - 4 of 4

Figure 80 : KMIP group permissions

Per-user permission detail

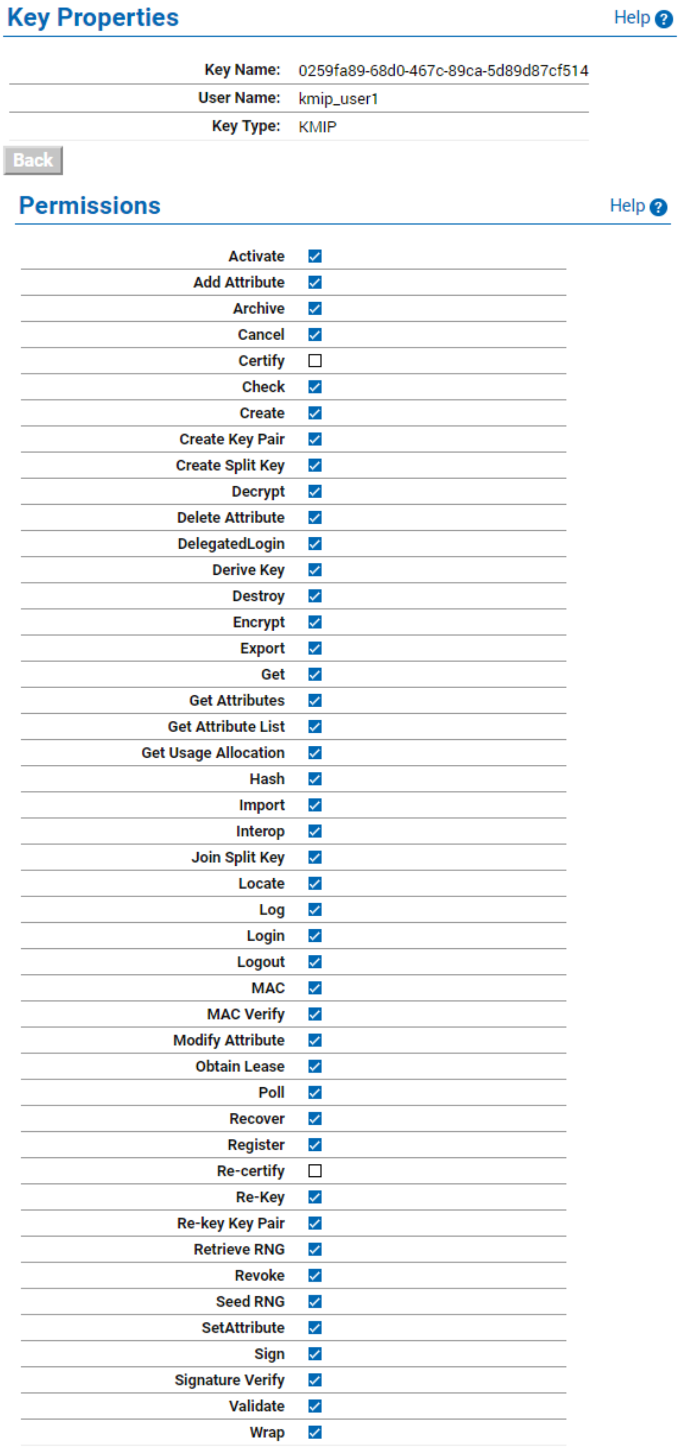
To view the details of what privileges a user has, select the user from the list, and then click **View Permissions**. The below figure shows the permissions that user “kmip_user1” has on the selected KMIP object. Each permission corresponds to a KMIP operation.

For example, the **Get Attributes** permission means that the user is allowed to issue the **Get Attributes** request operation over the KMIP protocol, while the **Destroy** permission means that the user is allowed to destroy this object by issuing the **Destroy** request operation over the KMIP protocol.

These permissions do not apply to the administrator who is logged on to the Management Console. Administrators always have permissions to perform operations on objects supported by the Management Console, such as changing the KMIP object owner and deleting the KMIP object.

> ⚠ The Certify and Re-certify permissions are disabled by default. They must be explicitly enabled.

The following figure shows **KMIP Key Properties** and **Permissions**.



Key Properties

Help ?

Key Name:	0259fa89-68d0-467c-89ca-5d89d87cf514
User Name:	kmip_user1
Key Type:	KMIP

Permissions

Help ?

Activate	☑
Add Attribute	☑
Archive	☑
Cancel	☑
Certify	□
Check	☑
Create	☑
Create Key Pair	☑
Create Split Key	☑
Decrypt	☑
Delete Attribute	☑
DelegatedLogin	☑
Derive Key	☑
Destroy	☑
Encrypt	☑
Export	☑
Get	☑
Get Attributes	☑
Get Attribute List	☑
Get Usage Allocation	☑
Hash	☑
Import	☑
Interop	☑
Join Split Key	☑
Locate	☑
Log	☑
Login	☑
Logout	☑
MAC	☑
MAC Verify	☑
Modify Attribute	☑
Obtain Lease	☑
Poll	☑
Recover	☑
Register	☑
Re-certify	□
Re-Key	☑
Re-key Key Pair	☑
Retrieve RNG	☑
Revoke	☑
Seed RNG	☑
SetAttribute	☑
Sign	☑
Signature Verify	☑
Validate	☑
Wrap	☑

Figure 81 : KMIP permissions detail

6.4.7 Convert keys

KMS and KMIP keys are used in different protocols and have different metadata. A KMS key cannot be used over the KMIP protocol in its original format, neither can a KMIP key be used over the ESKM XML protocol.

It is sometimes useful to convert a key from one protocol to another. For example, when upgrading from a previous ESKM appliance version which only supports the ESKM XML protocol, you may want to use the same key instead of creating a new one, but upgrade to use the KMIP protocol. You will then need to convert the KMS key to KMIP format.

> ⚠ Only AES keys can be converted.

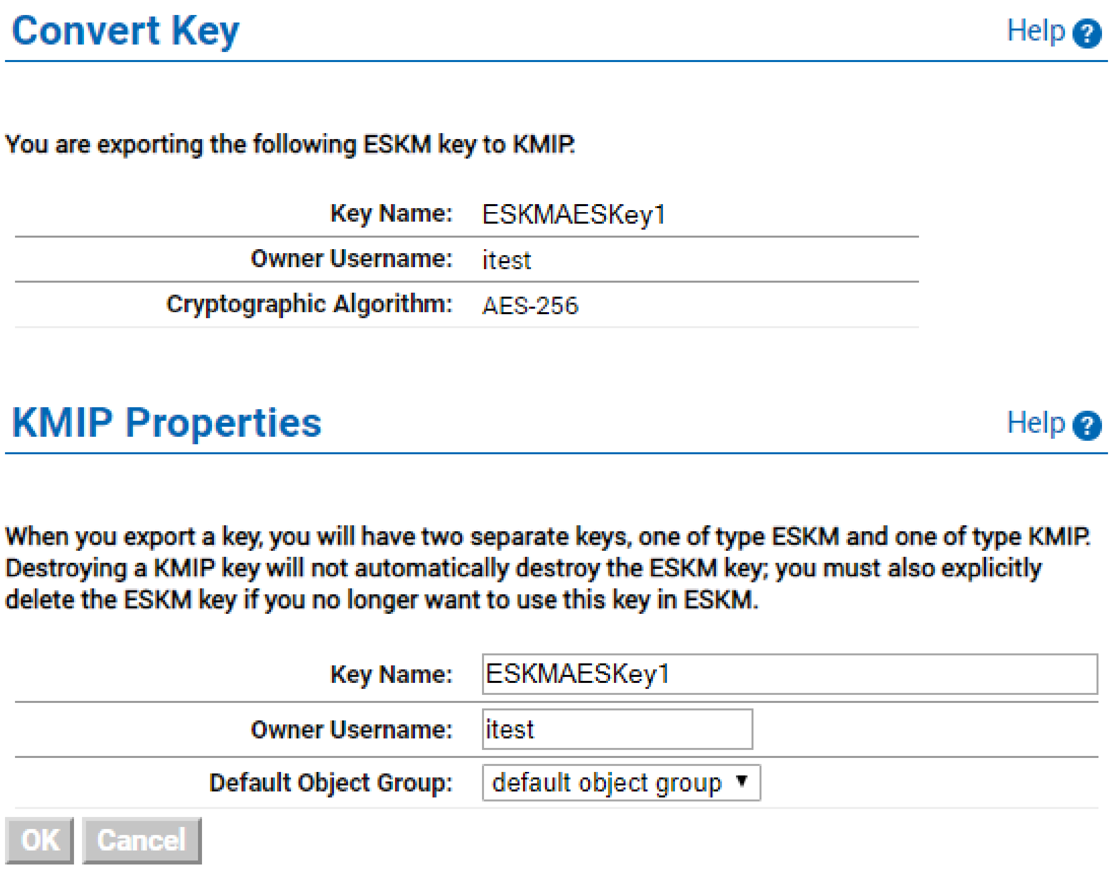
Converting a key from one protocol to another will result in two separate keys, one of type KMS and one of type KMIP. Destroying a KMIP key does not automatically destroy the KMS key. You must also explicitly delete the KMS key if you no longer wish to use this key in the ESKM appliance. The same applies to deleting KMIP keys if you no longer wish to use this key in KMIP.

6.4.7.1 Converting KMS keys to KMIP format

To convert a KMS key to KMIP format, select the KMS key, and then click the **Convert** button. This will convert the KMS key to KMIP format while retaining the key data.

By default, the KMIP key name will be set to the same key name as the existing KMS key; the key name can be changed if necessary. The owner username for the KMIP key will be set to the same as the KMS key; the owner username can be changed if necessary. KMIP keys must be placed into an object group, as such, you will be prompted to select an object group. Ensure that the user you enter in the **Owner Username** field has sufficient privileges to create a key in the selected object group.

The following figure shows the **Convert Key** and **KMIP Properties**.



Convert Key

You are exporting the following ESKM key to KMIP.

Key Name:	ESKMAESKey1
Owner Username:	itest
Cryptographic Algorithm:	AES-256

KMIP Properties

When you export a key, you will have two separate keys, one of type ESKM and one of type KMIP. Destroying a KMIP key will not automatically destroy the ESKM key; you must also explicitly delete the ESKM key if you no longer want to use this key in ESKM.

Key Name:	ESKMAESKey1
Owner Username:	itest
Default Object Group:	default object group ▼

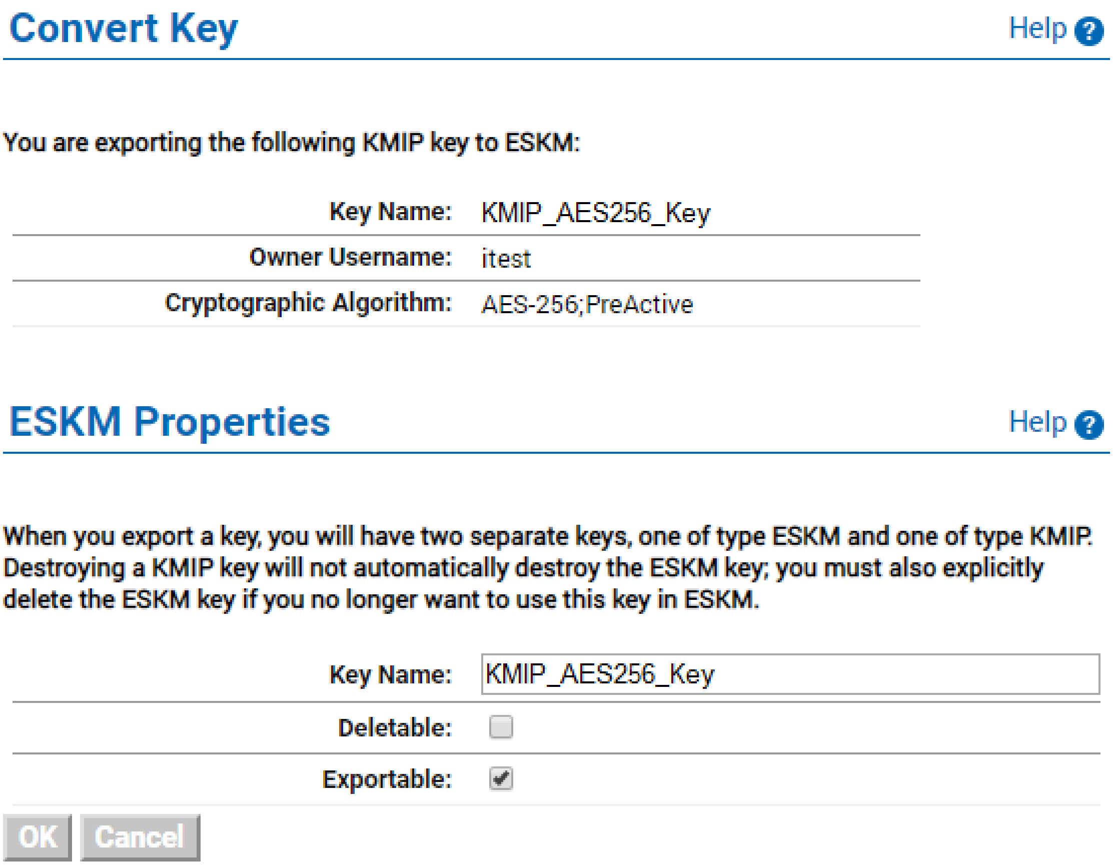
Figure 82 : Converting an ESKM key to KMIP format

KMIP keys have different metadata from KMS keys; the KMS attributes of deletable, exportable, and versioned will be lost on conversion. Click **OK** to proceed, or **Cancel** to abort.

6.4.7.2 Converting KMIP keys to KMS format

In some cases, you may also want to convert a KMIP key to KMS format. When you click the **Convert** button with a KMIP symmetric key selected, the KMIP key is converted to KMS format while retaining the key data.

The following figure shows the **Convert Key** and **ESKM Properties**.



You are exporting the following KMIP key to ESKM:

Key Name:	KMIP_AES256_Key
Owner Username:	itest
Cryptographic Algorithm:	AES-256;PreActive

When you export a key, you will have two separate keys, one of type ESKM and one of type KMIP. Destroying a KMIP key will not automatically destroy the ESKM key; you must also explicitly delete the ESKM key if you no longer want to use this key in ESKM.

Key Name:	KMIP_AES256_Key
Deletable:	□
Exportable:	☑

Figure 83 : Converting a KMIP key to KMS format

When converting a KMIP key to KMS format, you must specify the **Deletable** and **Exportable** attribute. Click **OK** to proceed, or **Cancel** to abort.

6.4.8 Query keys

Use this section to display the saved queries and create key queries. A key query allows you to view a subset of the keys that exist on the ESKM appliance.

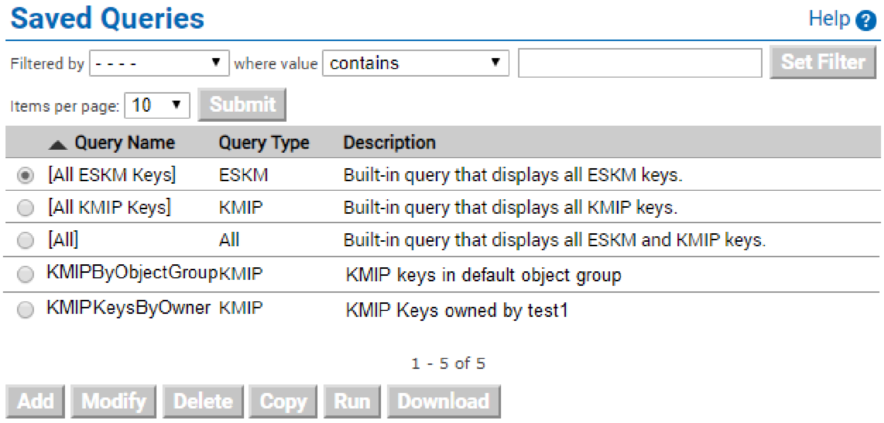
The following operations are supported for key queries:

- Displaying the list of queries (p. 269)
- Creating a new query (p. 271)
- Modify query (p. 278)

- Deleting an existing query (p. 279)
- Copying a query (p. 279)
- Running a query (p. 280)

6.4.8.1 Displaying the list of queries

Go to **Security** > **Keys & KMIP Objects** > **Keys** > **Query Keys** to view the list of saved queries.



Saved Queries

Filtered by - - - - where value contains

Items per page: 10

	▲ Query Name	Query Type	Description
●	[All ESKM Keys]	ESKM	Built-in query that displays all ESKM keys.
○	[All KMIP Keys]	KMIP	Built-in query that displays all KMIP keys.
○	[All]	All	Built-in query that displays all ESKM and KMIP keys.
○	KMIPByObjectGroup	KMIP	KMIP keys in default object group
○	KMIPKeysByOwner	KMIP	KMIP Keys owned by test1

1 - 5 of 5

Figure 84 : Viewing saved queries

The Management Console provides these built-in queries, which cannot be modified:

- **[All]** - This query returns all KMS and KMIP keys in the persistent store.
- **[All ESKM keys]** - This query returns all KMS keys in the persistent store. There is no limit to the number of KMS keys that can be returned.
- **[All KMIP Keys]** - This query returns all the KMIP keys in the persistent store. There is no limit to the number of KMIP keys that can be returned.

The Management Console displays a maximum of 3000 ESKM and 3000 KMIP keys, when **Query type [All]** is selected. Click the appropriate query name, to display all the keys of a particular type. For example: Select **[All ESKM Keys]** or **[All KMIP Keys]**.

Table 44: Saved Queries components

Component	***Description***
Query Name	Displays the name of the query.
Query Type	Displays the query type. This can be one of the following: ▪ All - a general query returning both KMS and KMIP keys. ▪ ESKM - a query returning only KMS keys. ▪ KMIP - a query returning only KMIP-managed objects.
Description	Displays a description of the query.
Modify	Click **Modify** to access Modify Query and alter the saved query. Once you have made your changes, you can save and run the query, save the query, or run the query without saving. The built-in queries [All], [All ESKM keys] and [All KMIP Keys] cannot be modified.
Delete	Click **Delete** to remove the query from the ESKM appliance. The built-in queries [All], [All ESKM keys] and [All KMIP Keys] queries cannot be deleted.
Copy	To make a copy of a selected query, select the query you want to copy and click the **Copy** button. This is an easy way to create a new query that is similar to an existing query. The built-in queries [All], [All ESKM keys] and [All KMIP Keys] queries cannot be copied.
Run	Click **Run** to execute the query.

Filtering the list of saved queries

Use the **Filtered by** function to limit the number of saved queries returned in the list.

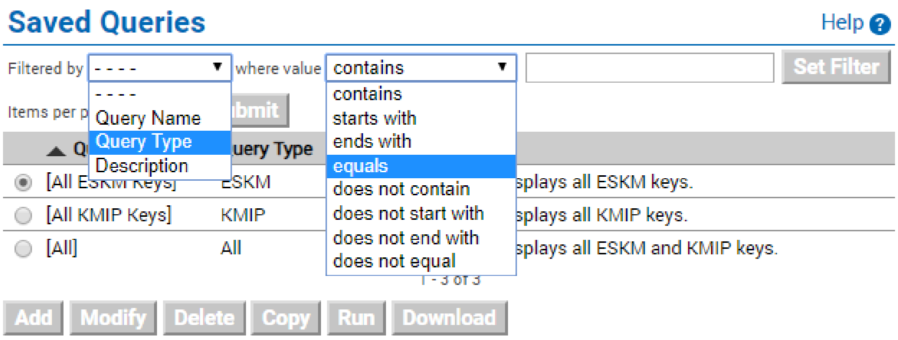


Figure 85 : Saved Queries - Filter by function

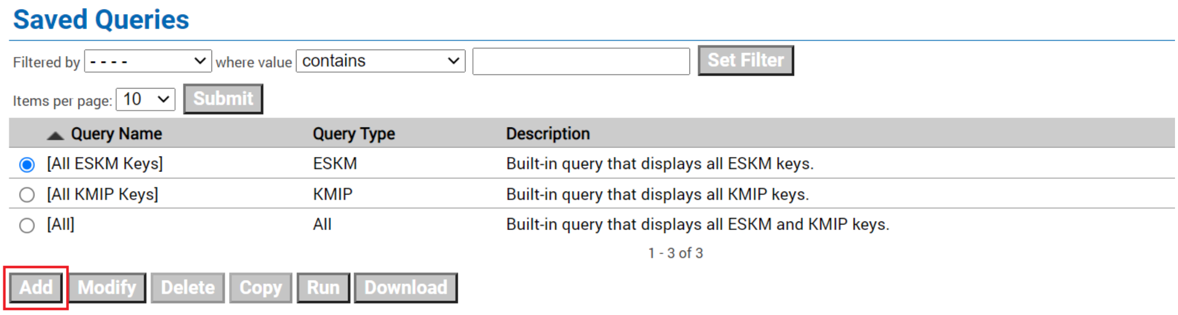
Specify the **Query Type**, **where value**, and then input the filter value.

Table 45: Saved Queries Filtered by components

Component	***Description***
Filtered by	Click in the drop-down list box and choose one of these query types: Query Name, Query Type, or Description.
where value	Click in the drop-down list box and choose one of these: contains, starts with, ends with, equals, does not contain, does not start with, does not end with, or does not equal.
	Click in the empty field, located to the right of the where value, and Input the value to filter.
Set Filter	Click **Set Filter** to execute the query.
Remove Filter	Click **Remove Filter** to remove the filter criteria; all saved queries will be displayed.

6.4.8.2 Creating a new query

Since KMIP queries differ from KMS queries, the administrator needs to specify the query type before the query can be created. When you click the **Add** button in the **Saved Queries** screen, you will be placed in Add mode. Type in the query name, query type, and query description, and then click **Next** to proceed to the next step to enter the query criteria, or click **Cancel** to abort.



Saved Queries

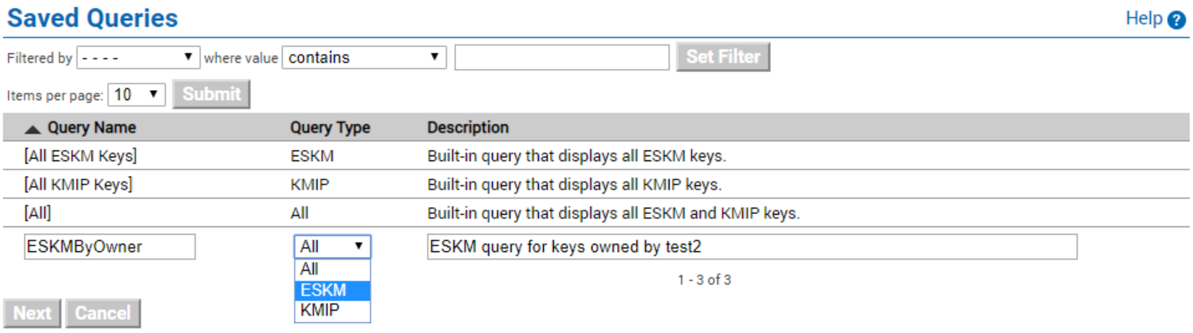
Filtered by - - - - where value contains

Items per page: 10

Query Name	Query Type	Description
● [All ESKM Keys]	ESKM	Built-in query that displays all ESKM keys.
○ [All KMIP Keys]	KMIP	Built-in query that displays all KMIP keys.
○ [All]	All	Built-in query that displays all ESKM and KMIP keys.

1 - 3 of 3

Figure 86 : Add button to create a query



Saved Queries

Filtered by - - - - where value contains

Items per page: 10

Query Name	Query Type	Description
[All ESKM Keys]	ESKM	Built-in query that displays all ESKM keys.
[All KMIP Keys]	KMIP	Built-in query that displays all KMIP keys.
[All]	All	Built-in query that displays all ESKM and KMIP keys.
ESKMByOwner	All	ESKM query for keys owned by test2

1 - 3 of 3

Figure 87 : Create new query

Some of the components listed in the following table are common across all query types.

Table 46: Create query common components

Component	***Description***
Query Name	Displays the name of the query. The name may be changed if necessary.
Query Type	Displays the query type. The query type is determined during the Create Query process and cannot be changed in this screen. This can be one of the following: ▪ All - a general query returning both KMS and KMIP keys. ▪ ESKM - a query returning only KMS keys. ▪ KMIP - a query returning only KMIP-managed objects.
Description	Displays a description of the query.

Component	***Description***
Save and Run Query	Save the query first, and then run it. Saved queries must have a name and will appear in the Saved Queries listing. Running the query will return a key listing of the keys that match the query criteria.
Save Query	Save the query without running it. You will be returned to the Saved Queries listing, where you will see your new query added to the list of saved queries.
Run Query without Saving	Run the query without saving it. This will create a temporary unnamed query. Only one temporary query can exist at one time. This query will be replaced the next time a temporary query is created. Running the query will return a key listing of the keys that match the query criteria.

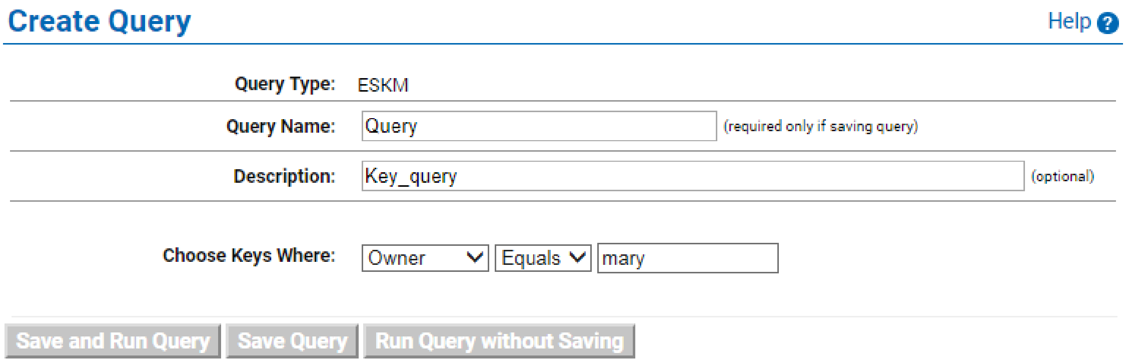
The process to create each of the 3 query types is explained below.

Creating a new general query

Select the **All** option for the Query Type to create a new general query. Since this is a general query, only attributes common to both KMS and KMIP keys can be included.

These are:

- Key Name
- Owner



Create Query

Query Type: ESKM

Query Name: Query (required only if saving query)

Description: Key_query (optional)

Choose Keys Where: Owner Equals mary

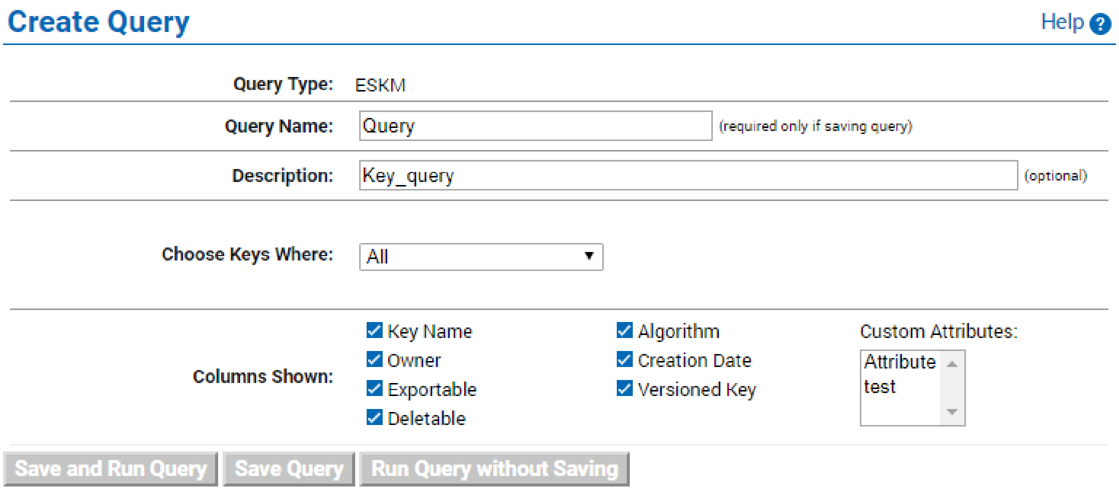
Figure 88 : Create new All-type query

If you select either Save and Run Query, or Run Query without Saving, the key listing returned will be in the format discussed in Displaying search results for All-type queries (p. 231).

Creating a new KMS query

Select ESKM as the **Query Type** to create a new KMS query. The **Query Name** and **Description** fields can be entered. The search criteria can be specified in the **Choose Keys Where** list. Combinations of AND and OR operators are permitted.

Columns Shown is retained for backwards compatibility and is used for informational purposes only. **Columns Shown** cannot be modified.



Create Query

Query Type: ESKM

Query Name: Query (required only if saving query)

Description: Key_query (optional)

Choose Keys Where: All

Columns Shown: ☑ Key Name ☑ Owner ☑ Exportable ☑ Deletable ☑ Algorithm ☑ Creation Date ☑ Versioned Key

Custom Attributes: Attribute test

Figure 89 : Create new KMS query

The following query criteria may be specified for KMS queries.

Table 47: ESKM query criteria

Component	***Description***
Key Name	The key name.
Owner	The owner username.
Group Name	The group name.

Component	*Description*
Algorithm	The cryptographic algorithm. The list of available cryptographic algorithms are: ▪ AES-128 ▪ AES-192 ▪ AES-256 ▪ DES-EDE-168 ▪ DES-EDE-112 ▪ HmacSHA1 ▪ HmacSHA1-256 ▪ HmacSHA1-160 ▪ HmacSHA1-128 ▪ RSA-2048 ▪ RSA-1024
Creation Date	Creation date in the format yyyy-mm-dd. You can also specify a date range using the Ranges or Not Ranges condition.
Latest Key Version Date	The date when the latest key version was created. Applies only to versioned keys.
Any Key Version Date	The date when any of the key versions were created. Applies only to versioned keys.
Versioned Key	This criteria matches versioned keys.
Not Versioned Key	This criteria matches keys that are not versioned.

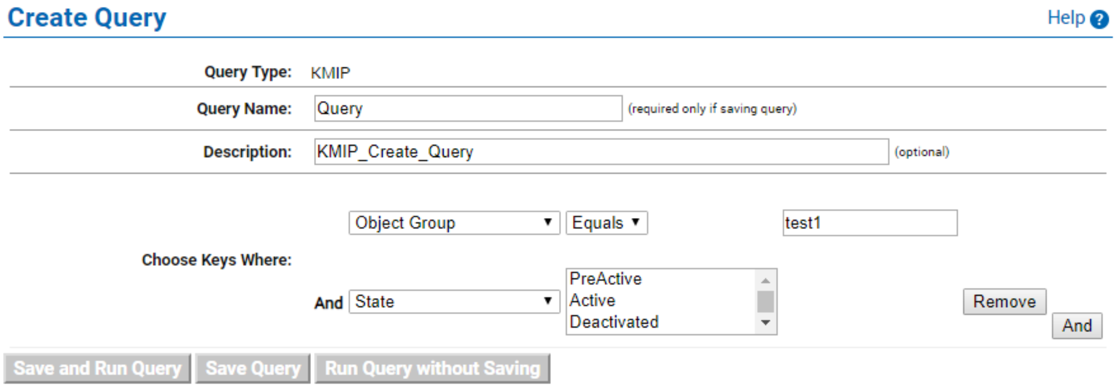
Component	***Description***
Exportable	This criteria matches keys with the Exportable attribute set, that is, keys that can be exported.
Not Exportable	This criteria matches keys with the Exportable attribute cleared, that is, keys that cannot be exported.
Deletable	This criteria matches keys with the Deletable attribute set, that is, keys that can be deleted over the ESKM XML protocol.
Not Deletable	This criteria matches keys with the Deletable attribute cleared, that is, keys that cannot be deleted over the ESKM XML protocol.

Creating a new KMIP query

Select KMIP as the **Query Type** to create a new KMIP query. The **Query Name** and **Description** fields can be entered.

The **Choose Keys Where** list the query criteria items. The following query criteria items require the user to select from a list: Cryptographic Algorithm, State, Object Type, and Revocation Reason. The following query criteria items require the user to enter a specific query value: Unique Identifier, Name, Username, Cryptographic Length, and Object Group.

Click the **And** button to add additional query criteria. This query type does not support the OR operator.



Create Query

Query Type: KMIP

Query Name: Query (required only if saving query)

Description: KMIP_Create_Query (optional)

Choose Keys Where: Object Group Equals test1

And State PreActive / Active / Deactivated

Figure 90 : Create new KMIP query

Other than the Username, the criteria that may be specified for KMIP queries are a subset of the KMIP attributes that are specified in a client Locate request operation. This subset is deemed to be the most common criteria used to search for symmetric keys.

The following criteria may be specified for KMIP queries.

Table 48: KMIP query criteria

Component	***Description***
Unique Identifier	The unique identifier (UUID) for the key. Note that since the UUID is unique within the ESKM appliance, at most one result will be returned. Therefore, there is no need to specify other query criteria if this criteria is present.
Name	The key name. For KMIP objects with multiple names, this query criteria will only match the first Name attribute.
Username	The owner username.
Cryptographic Algorithm	The KMIP cryptographic algorithm. For a full list of supported cryptographic algorithms, see Algorithm(see table 36).
Cryptographic Length	The length of the key.
State	The object state. Valid object states are Pre-Active, Active, Deactivated, Compromised, Destroyed, and Destroyed Compromised.
Initial Date	The date, in yyyy-mm-dd format, when the object was first created or registered at the ESKM appliance.
Revocation Reason	The reason why the object was revoked.

Component	***Description***
Object Group	The name of the object group. This is the value of the Object Group attribute for this object. It does not necessarily mean that the object is currently a member of this object group. The KMIP object is initially placed in this object group when it is first created. Subsequently, the administrator may add the KMIP object to more groups or delete it from its existing group from the Management Console. The Object Group is the value when first created or registered. It does not reflect the administrator actions to change the object group.
Object Type	The type of KMIP object.

6.4.8.3 Modify query

Use **Modify Query** to change an existing query. You can alter the **Query Name, Description** and selection criteria. However you cannot change the **Query Type**. You may then Save and Run Query, Save Query, or Run Query without Saving.

> ⚠ You cannot modify the built-in queries [All], [All ESKM keys], and [All KMIP Keys]. You can only view these queries.

Table 49: Modify Query components

Component	***Description***
Query Name	The name of the query. This field is only required when saving the query. You can run a query without saving; you can only save a query without running it.
Description	A description of the query.
Choose Keys Where	Use this field, in combination with the AND and OR buttons to create your query. You can query on key metadata, combine query strings, and use the results of previously saved queries.

Component	***Description***
Columns Shown	Select the columns to be included in the query results. The Columns Shown feature is only available for KMS key queries.
Save and Run Query	Click **Save and Run Query** to save and then execute the query.
Save Query	Click **Save Query** to save the query without executing it.
Run Query without Saving	Click **Run Query without Saving** to execute the query. The query name will appear on the results page as Unnamed Query. You can navigate away from Keys and still re-apply the Unnamed Query, however, the Management Console will only store one Unnamed Query at a time. Previous unnamed queries are not stored.
Cancel	Click **Cancel** to ignore your changes and return to Saved Queries.

6.4.8.4 Deleting an existing query

To delete an existing query, navigate to **Security** > **Keys & KMIP Objects** > **Keys** > **Query Keys**, select the query you wish to delete, and then click the **Delete** button. You can delete any custom query that you have created.

> ⚠ You cannot delete the 3 built-in queries [All], [All ESKM keys], and [All KMIP Keys].

6.4.8.5 Copying a query

To copy an existing query to another new query, navigate to **Security > Keys & KMIP Objects > Keys > Query Keys**, and select the query you want to copy, and then click the **Copy** button. The existing query will be copied to a new query with the same name as the current query, with ' _copy' appended to the end of the query name. For example, if you copy a query named IT_KMIP, the new query will be named IT_KMIP_copy. All query criteria for the new query will be the same as the existing query. Copying queries is a useful way to create a new query which differs only slightly from the existing query. Modifying the criteria for the copied query may be faster than creating a new query from scratch.

⚠ You cannot copy the 3 built-in queries [All], [All ESKM keys], and [All KMIP Keys].

6.4.8.6 Running a query

There are multiple ways to run a query:

- Navigate to **Security > Keys & KMIP Objects > Keys > Query Keys**, select the query, and then click the **Run** button. The query results will be displayed in the Key Listing.
- Navigate to **Security > Keys & KMIP Objects > Keys > Query Keys**. To run a new query, click **Add** to add a new query, specify the criteria as needed, click **Save**, and then click **Run Query** to save the new query and run it. If you simply want to run the new query without saving it, click **Run Query without Saving**.
- Navigate to **Security > Keys & KMIP Objects > Keys > Query Keys**. To run a modified version of an existing query, select the query you wish to modify, and then click the **Modify** button. Modify the query criteria as needed, and then click **Save and Run Query** to save the modified query and run it. If you simply want to run the modified query without saving it, click **Run Query without Saving**.
- Navigate to **Security > Keys & KMIP Objects > Keys > Keys**. Select the query from the drop-down list box named **Query** at the top of the page, and then click **Run Query**. This is equivalent to navigating to **Security > Keys & KMIP Objects > Keys,** Query Keys, selecting the query, and then clicking the **Run** button.

These queries will return only KMIP symmetric keys in the Key Listing page. To return other types of KMIP-managed objects in addition to KMIP symmetric keys, navigate to **Security > Keys & KMIP Objects > KMIP Objects**. Only KMIP queries will appear in the **Query** drop-down list box. If you select a query from the drop-down list box on this page, all KMIP-managed objects matching the query criteria will be returned. This may include other KMIP-managed objects in addition to symmetric key objects.

6.4.8.7 Download ESKM query

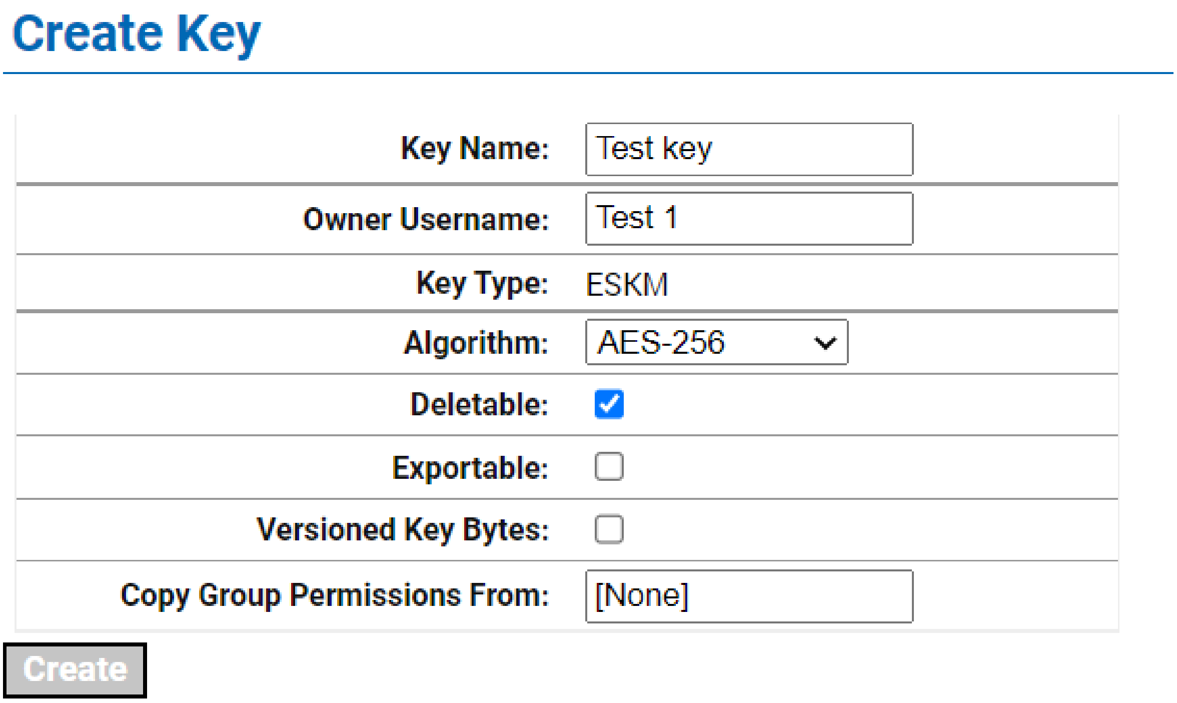
To download an ESKM key query, navigate to **Security > Keys & KMIP Objects > Keys > Query Keys**, select **[All ESKM Keys]**, and click **Download**. This downloads the ESKM key query in an Excel file format. The Excel file contains the following key attributes for all the KMS keys in the query.

- Type
- Key Name
- Owner
- Algorithm
- Exportable
- Deletable
- Versioned Key
- Creation Date
- Default IV

⚠ The Download option is only available for the built-in query **[All ESKM Keys]**.

6.4.9 Create keys

Create Key allows you to create KMS keys on the ESKM appliance. This only supports KMS keys, not KMIP keys. KMIP keys can only be created via clients using the KMIP protocol. You can change the name or owner of the KMS key, modify the values for the **Deletable** and **Exportable** fields, specify if multiple key versions can be created, and also to copy the group permissions from an existing KMS key. You cannot change the key type. You can convert a KMIP key to a KMS key, see Converting KMIP keys to KMS format (p. 267).



Create Key

Key Name:	Test key
Owner Username:	Test 1
Key Type:	ESKM
Algorithm:	AES-256
Deletable:	☑
Exportable:	☐
Versioned Key Bytes:	☐
Copy Group Permissions From:	[None]

Figure 91 : Create Keys

The following table describes the components of **Create Key**.

Table 50: Create Key components

Component	***Description***
Key Name	This is the name the ESKM appliance uses to refer to the key. The key name must begin with a letter, must be between 1 and 64 characters (inclusive), and can consist of only letters, numbers, underscores (_), periods (.), and hyphens (-).
Owner Username	You do not have to specify an owner for the key; if you leave that field blank, the created key is a global key and therefore accessible to all users. If you want to assign an owner for the key, you can specify any valid user in the Owner Username field. If you assign an owner, then that user is the only user who can access the key (unless the key is given additional group permissions later).

Component	***Description***
Algorithm	The algorithm might be any one of the following: ▪ AES-256 ▪ AES-192 ▪ AES-128 ▪ DES-EDE-168 (three key triple DES) ▪ DES-EDE-112 (two key triple DES)* ▪ DES* ▪ RC4-128* ▪ RC4-40* ▪ HmacSHA1 ▪ RSA-2048 ▪ RSA-3072 ▪ RSA-4096 ▪ RSA-1024* ▪ RSA-512* ⚠ *These algorithms are not available when the ESKM appliance is running in FIPS-compliant mode.
Deletable	A check mark in the box indicates that the key is deletable via an ESKM XML request by the key owner (or any user for global keys). After a key is created, this value may be changed.

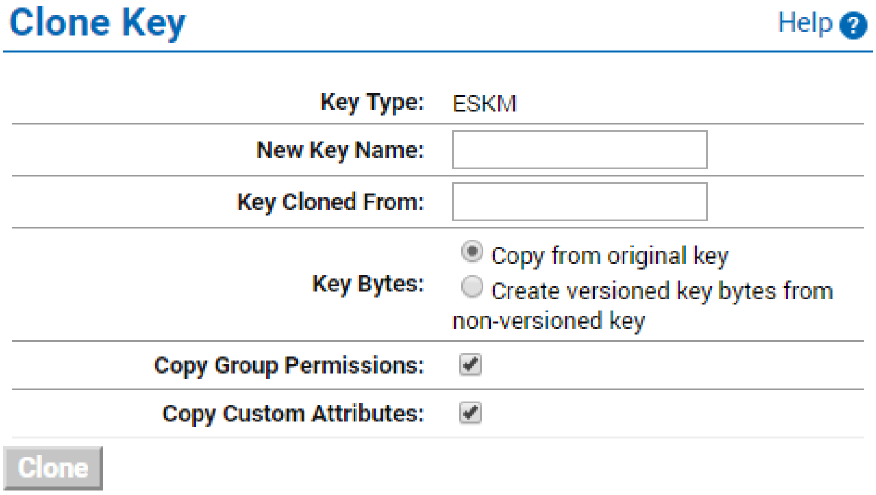
Component	***Description***
Exportable	A check mark in the box indicates that the key is exportable via an ESKM XML request. An exportable key can be exported by its owner and by members of a group with “Export” permission for the key. (A global key marked exportable can be exported by any user.) After a key is created, this value may be changed.
Versioned Key Bytes	When selected, the KMS key contains multiple versions, up to a maximum of 4,000. Each key version has unique key bytes, but shared key metadata (key name, algorithm, permissions, and so on. The first key version is created when the key is created. Additional key versions may be created later using the Key Versions.
Copy Group Permissions From	Select an existing key to copy its group permissions. The new key and the existing key must be of compatible types; specifically, they must both use RSA, both use HmacSHA1, or they may use either AES, DES, or RC4.
Create	Click **Create** to create the key.

6.4.10 Clone key

Use **Clone Key** to assign the key bytes and key metadata from an existing KMS key to a new key. You can choose to copy or ignore the existing group permissions and custom attributes. You can also use this to create a versioned key from a non-versioned key.

A versioned key cannot be cloned.

Only KMS keys can be cloned. Cloning of KMIP keys is not supported. To perform the equivalent key clone operation for KMIP keys, perform a KMIP client **Get** and **Get Attributes** operation, followed by a **Register** operation.



Clone Key

Key Type: ESKM

New Key Name:

Key Cloned From:

Key Bytes:
● Copy from original key
○ Create versioned key bytes from non-versioned key

Copy Group Permissions: ☑

Copy Custom Attributes: ☑

Figure 92 : Clone Key

The following table describes the components of **Clone Key**.

Table 51: Clone Key components

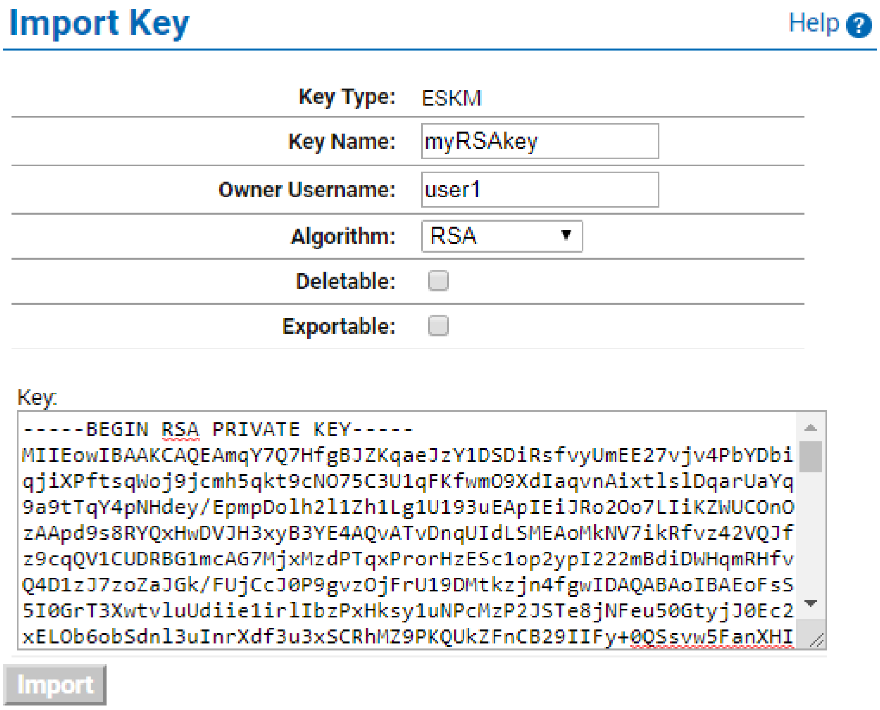
Component	***Description***
Key Type	The type of key to be cloned. Only KMS keys can be cloned. Therefore, the value for this field is always ESKM.
New Key Name	This is the name the ESKM appliance uses to refer to the new key. The key name must begin with a letter, it must be between 1 and 64 characters (inclusive), and it can consist of letters, numbers, underscores (_), periods (.), and hyphens (-).
Key Cloned From	This is the key that will be copied.
Key Bytes	▪ Select **Copy from original key** to create a duplicate of the non-versioned key under a new name ▪ Select **Create versioned key bytes from non-versioned key** to create a new versioned key and copy the non-versioned key to version 1.

Component	***Description***
Copy Group Permissions	Select this option to copy the group permissions from the existing key.
Copy Custom Attributes	Select this option to copy the custom attributes from the existing key.
Clone	Click **Clone** to create a copy of the key.

6.4.11 Import keys

Import Key allows you to import clear text keys into the ESKM appliance. Asymmetric keys must be imported in PEM-encoded ASN.1 DER-encoded PKCS #1 format, and both the public and private keys must be imported. Symmetric keys must be in Base 16 format, and in the case of DES keys, parity bits must be properly set.

ℹ The ESKM appliance will not import keys that are known to be weak, such as 64 bit DES. In addition, the parity bits must be set properly; otherwise, the appliance returns an error.



Key Type:	ESKM
Key Name:	myRSAkey
Owner Username:	user1
Algorithm:	RSA ▾
Deletable:	□
Exportable:	□

Key:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAmqY7Q7HfgBJZKqaeJzY1DSDiRsfvyUmEE27vjv4PbYDbi
qjiXPftsqWoj9jcmh5qkt9cNO75C3U1qFKfwmO9XdIaqvnAixtlslDqarUaYq
9a9tTqY4pNHdey/EpmpDolh2l1Zh1Lg1U193uEApIEiJRo2Oo7LIiKZWUCOnO
zAApd9s8RYQxHwDVJH3xyB3YE4AQvATvDnqUIdLSMEAoMkNV7ikRfvz42VQJf
z9cqQV1CUDRBG1mcAG7MjxMzdPTqxProrHzESc1op2ypI222mBdiDWHqmRHfv
Q4D1zJ7zoZaJGk/FUjCcJ0P9gvzOjFrU19DMtkzjn4fgwIDAQABAoIBAEoFsS
5I0GrT3XwtvluUdiie1irlIbzPxHksy1uNPcMzP2JSTe8jNFeu50GtyjJ0Ec2
xELOb6obSdnl3uInrXdf3u3xSCRhMZ9PKQUkZFnCB29IIFy+0QSsvw5FanXHI
```

Figure 93 : Import Key

The following table describes the components of **Import Key**.

Table 52: Import Key components

Component	***Description***
Key Name	This is the name the ESKM appliance uses to refer to the key. The key name must begin with a letter, it must be between 1 and 64 characters (inclusive), and it can consist of letters, numbers, underscores (_), periods (.), and hyphens (-).
Owner Username	When you import and export keys, metadata such as key ownership is not retained. As such, any previous owner assigned to a key must be re-assigned once the key is imported. You do not have to specify an owner for the key; if you leave that field blank, the imported key is a global key and therefore accessible to all users. If you want to assign an owner for the key, you can specify any valid user in the Owner Username field. If you assign an owner, then that user is the only user who can access the key (unless the key is given additional group permissions later).

Component	***Description***
Algorithm	The algorithm is any one of the following: - AES - 3DES-EDE - HMAC SHA1 - RSA ⚠ Some of these algorithms will not be available when the ESKM appliance is running in FIPS-compliant mode.
Deletable	A check mark in the box indicates that the key is deletable via an ESKM XML request by the key owner (or any user for global keys). After a key is created, this value may be changed.
Exportable	A check mark in the box indicates that the key is exportable via an ESKM XML request. An exportable key can be exported by its owner and by members of a group with "Export" permission for the key. A global key marked exportable can be exported by any user. After a key is created, this value may be changed.
Key	To import a key to the ESKM appliance, you must enter the properly encoded bytes of the key in the Key field.
Import	Click **Import** to import the key.

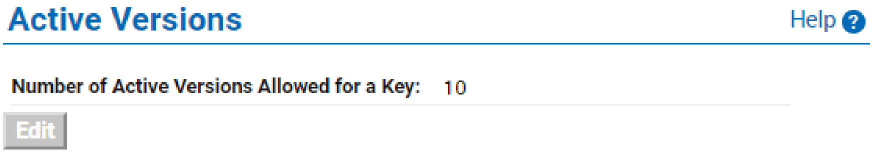
6.4.12 Key options

The **Key and Policy Configuration** allows you to configure global settings for KMS keys.

⚠ This option relates to KMS keys only. To configure KMIP key options, go to **Device > KMIP Server** and modify the settings in either **KMIP Server** or the **KMIP Interoperability Settings**.

6.4.12.1 Active versions

Use **Active Versions** to configure the number of active versions allowed for a versioned key. Active versions of a key can be used for both encryption and decryption (or Sign/SignVerify, or MAC/MACVerify depending on the algorithm).



Number of Active Versions Allowed for a Key: 10

Figure 94 : Active Versions

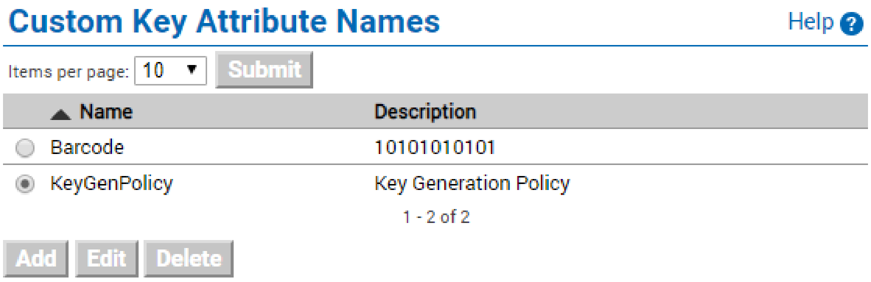
Table 53: Active Versions components

Component	***Description***
Number of Active Versions Allowed for a Key	Displays the number of active versions allowed for a versioned key.
Edit	Click **Edit** to change the number of active versions allowed.

When restoring a key to the ESKM appliance, the key must conform to the KMS' current **Number of Active Versions Allowed for a Key** setting on the **Key and Policy Configuration** page. If the key has more active versions than permitted by that setting, the key restore will fail. To restore a key with more active versions than the system allows, you must change the **Number of Active Versions Allowed for a Key** setting before restoring the backup. You can then reduce the key's active versions and return the **Number of Active Versions Allowed for a Key** to its original value.

6.4.12.2 Custom key attributes

Use **Custom Key Attribute Names** to create the custom attributes that you assign to your keys. Once you have created the attribute, you can assign it to a key using Custom Attributes.



Custom Key Attribute Names

Help ?

Items per page: 10 ▼ Submit

	▲ Name	Description
○	Barcode	10101010101
●	KeyGenPolicy	Key Generation Policy

1 - 2 of 2

Figure 95 : Custom Key Attributes

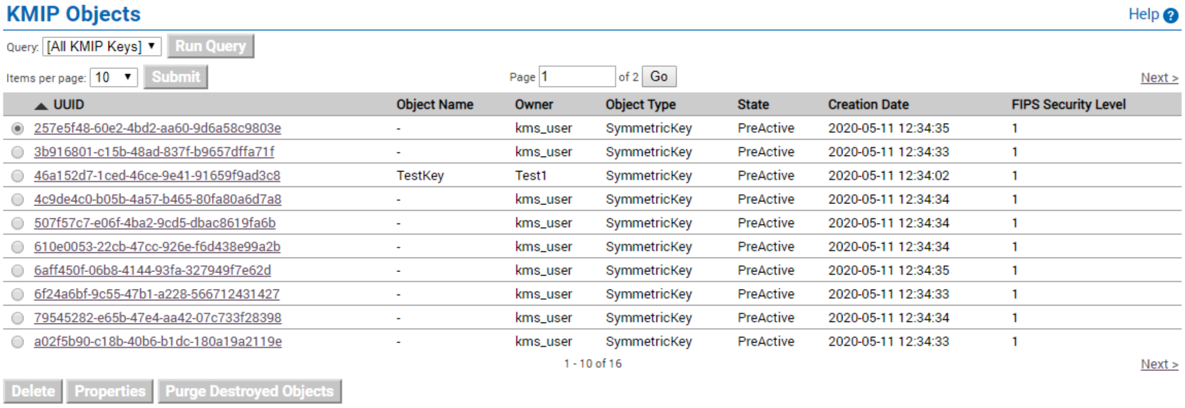
Table 54: Custom Key Attributions components

Components	***Description***
Attribute Name	Enter a unique attribute name. Attribute names can contain alphanumeric characters, hyphens, underscores, and periods. You cannot include whitespaces in the name. Maximum length is 256 characters.
Attribute Value	Enter the value of the attribute. This can contain any printable ASCII characters and spaces, tab, \n, and \r. Maximum length is 4,096 characters.
Edit	Click **Edit** to alter the selected attribute.
Add	Click **Add** to add an attribute.
Delete	Click **Delete** to remove the selected attribute.

6.5 KMIP objects

The KMIP Object Configuration page (**Security > Keys & KMIP Objects > KMIP Objects**) allows you to view a list of KMIP-managed objects, view the attributes of a KMIP-managed object, and delete a KMIP-managed object. You can also use it to purge KMIP-managed objects that are in the destroyed state.

You can click a field name (UUID, Object Name, Owner, etc) to sort the KMIP-managed objects by that value; toggle to alternate between the ascending and descending order. You can click **Next** to go to the next page, **Previous** to go to the previous page, or enter a page number at the Page box and then click **Go** to jump to a specific page. You can use the Query field to select a query that will filter this page by the key metadata. To run a query, click the **Run Query** button. The query you apply to this page determines which columns are shown. The default query is **[All KMIP Objects]**; it displays all KMIP-managed objects.



Query: [All KMIP Keys]

Items per page: 10

Page 1 of 2

	▲ UUID	Object Name	Owner	Object Type	State	Creation Date	FIPS Security Level
●	257e5f48-60e2-4bd2-aa60-9d6a58c9803e	-	kms_user	SymmetricKey	PreActive	2020-05-11 12:34:35	1
○	3b916801-c15b-48ad-837f-b9657dffa71f	-	kms_user	SymmetricKey	PreActive	2020-05-11 12:34:33	1
○	46a152d7-1ced-46ce-9e41-91659f9ad3c8	TestKey	Test1	SymmetricKey	PreActive	2020-05-11 12:34:02	1
○	4c9de4c0-b05b-4a57-b465-80fa80a6d7a8	-	kms_user	SymmetricKey	PreActive	2020-05-11 12:34:34	1
○	507f57c7-e06f-4ba2-9cd5-dbac8619fa6b	-	kms_user	SymmetricKey	PreActive	2020-05-11 12:34:34	1
○	610e0053-22cb-47cc-926e-f6d438e99a2b	-	kms_user	SymmetricKey	PreActive	2020-05-11 12:34:34	1
○	6aff450f-06b8-4144-93fa-327949f7e62d	-	kms_user	SymmetricKey	PreActive	2020-05-11 12:34:35	1
○	6f24a6bf-9c55-47b1-a228-566712431427	-	kms_user	SymmetricKey	PreActive	2020-05-11 12:34:33	1
○	79545282-e65b-47e4-aa42-07c733f28398	-	kms_user	SymmetricKey	PreActive	2020-05-11 12:34:34	1
○	a02f5b90-c18b-40b6-b1dc-180a19a2119e	-	kms_user	SymmetricKey	PreActive	2020-05-11 12:34:33	1

1 - 10 of 16

Figure 96 : KMIP Objects

The following table describes the components of **KMIP Objects**.

Table 55: KMIP Objects components

Component	***Description***
Query	Select the query to apply to the page.
Run Query	Click **Run Query** to run a query. A subset of the available KMIP objects and their corresponding columns will be displayed. ⚠ The built-in query [All KMIP keys] will return all KMIP-managed objects on this page. The same query will only return all KMIP-managed objects of type symmetric key in the Keys listing page.
UUID	The UUID for the KMIP-managed object.

Component	***Description***
Object Name	This is the name that the ESKM appliance uses to refer to the KMIP-managed object. Names are optional for KMIP-managed objects, therefore this field may be blank. If the KMIP-managed object has multiple names, each name will be displayed, separated by a space.
Owner	The owner is typically the user who created the KMIP-managed object.
Object Type	The KMIP object type, for example a SymmetricKey.
State	The object state.
Creation Date	The date and time the KMIP-managed object was created.
FIPS Security Level	The security level of the device where the key was created.
Delete	Click **Delete** to delete a key. ! Exercise extreme caution when deleting keys. If you erroneously delete a key, you cannot recreate the key. Unless you have a backup of the key, you will not be able to decrypt any ciphertext created by the key.
Properties	Click **Properties** to view the attributes of the KMIP object.
Purge Destroyed Objects	Click **Purge Destroyed Objects** to purge all KMIP-managed objects that are in the Destroyed state.

6.6 Authorization policy

An authorization policy allows you to limit how a group may use a KMS key; it does not apply to KMIP groups and objects. You implement an authorization policy when establishing a key's group permissions. The policies are applied to a key separately for each group; groups that share a key do not necessarily share the same authorization policy.

> ⚠ The key owner is never limited by the key's policy restrictions.

Authorization policies define two types of limits:

- **Rate Limits**: The number of export operations (per hour) that members of the group can perform. The default is unlimited operations. If a user attempts to perform an operation and has exceeded the rate limit, an error is returned and the connection is closed.

> ⚠ Rate limiting is done on a per-user basis, not on a per-group basis. If the limit is 500 operations, each user in the group can perform 500 operations with the key.

- **Time Limits**: The hours or days when the members of the group can perform operations. The default is unlimited access. If a member of a restricted group attempts to use the key outside of the designated time, an error is returned and the connection is closed.

Once an authorization policy is defined, it is associated with a key and a group through Group Permissions in the Management Console. Individual keys can be associated with multiple groups, which may in turn have differing or conflicting authorization policies. In this case, the ESKM appliance chooses the least restrictive authorization policy available (the most operations per hour for the current time of day).

By default, no authorization policies are assigned to any group.

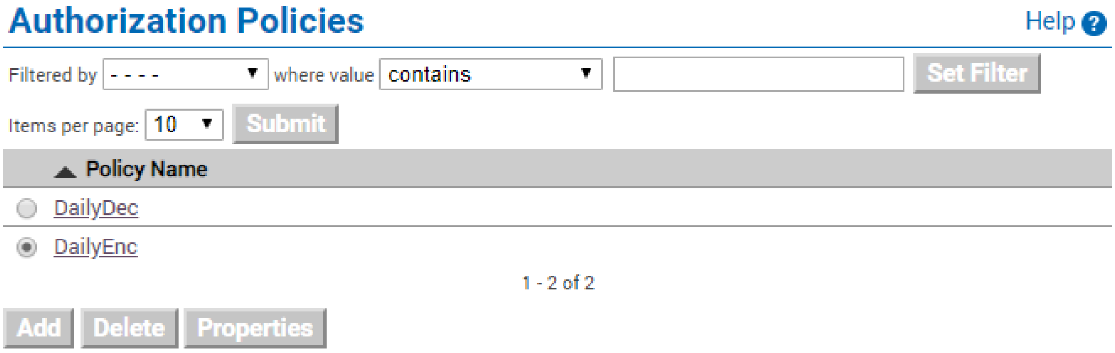
> ⚠ Authorization policies cannot be applied to global keys or to certificates. Key owners are not subject to policy restrictions.

The Authorization Policy Configuration page (**Security > Keys & KMIP Objects > Authorization Policies**) allows you to create and manage authorization policies. This section discusses the following topics:

- Authorization policies (p. 294)
- Authorization policy properties (p. 295)
- Authorized usage periods (p. 296)

6.6.1 Authorization policies

Use Authorization Policies to create and manage the authorization policies for the ESKM appliance.



Authorization Policies

Filtered by: - - - - where value: contains

Items per page: 10

Policy Name
○ DailyDec
● DailyEnc

1 - 2 of 2

Figure 97 : Authorization Policies

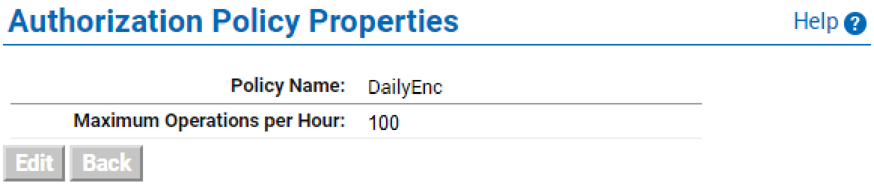
The following table describes the components of the **Authorization Policies**.

Table 56: Authorization Policies components

Component	***Description***
Policy Name	Click the name to view the details of a policy.
Add	Click **Add** to add a new policy.
Delete	Click **Delete** to delete a policy.
Properties	Click **Properties** to view the details of a policy.

6.6.1.1 Authorization policy properties

Authorization Policy Properties shows the name of the policy and the maximum operations per hour that users with that policy can perform.



Policy Name: DailyEnc

Maximum Operations per Hour: 100

Figure 98 : Authorization Policy Properties

The following table describes **Authorization Policy Properties**.

Table 57: Authorization Policy Properties components

Component	***Description***
Policy Name	Click the name to view the details of a policy.
Maximum Operations per Hour	By default, policies can perform unlimited operations. The valid range of operations is 1 to 500,000,000.
Edit	Click **Edit** to modify the policy properties.
Back	Click **Back** to return to the Authorization Policy Configuration page.

The ESKM appliance starts keeping track of the number of operations performed by a user as soon as that user makes a request to it. When the clock is running, the user has a one-hour window to perform no more than the number of operations specified in the **Maximum Operations per Hour** field. The changes made by the user, to the limit for a particular policy, are recognized immediately.

The following example illustrates the point: The rate limit for Key1 is 100 operations per hour.

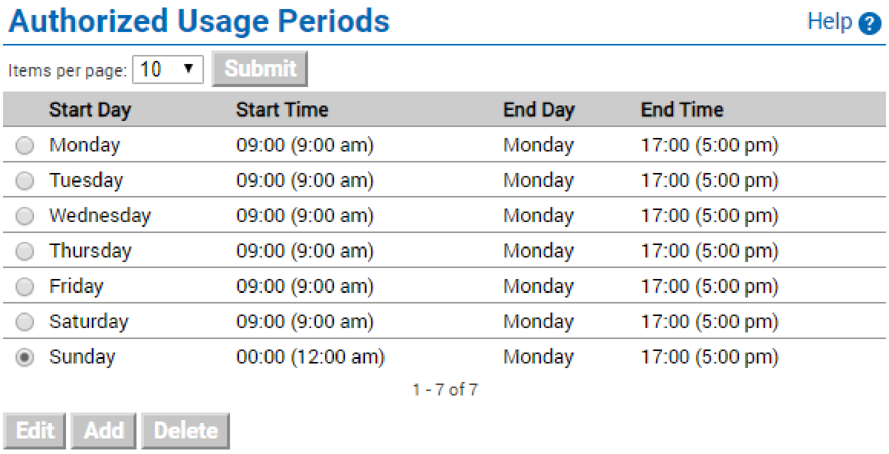
- At 11:00 AM, User1 logs in and begins making requests using the Key1.
- At 11:30 AM, User1 has used 50 operations with Key1.

- At 11:31 AM, the administrator changes the rate limit for Key1 to 150 operations per hour.
- User1 can make only 100 more requests between 11:31 AM and 11:59 AM.

> ⚠ Had the limit been lowered to 75, User1 would only be allowed to make 25 more requests.

6.6.1.2 Authorized usage periods

Use the **Authorize Usage Periods** to define, view, change or delete usage periods in which users within a group can use a key. A usage period can span up to 7 days of the week or any portion of those days.



Authorized Usage Periods

Items per page: 10

	Start Day	Start Time	End Day	End Time
○	Monday	09:00 (9:00 am)	Monday	17:00 (5:00 pm)
○	Tuesday	09:00 (9:00 am)	Monday	17:00 (5:00 pm)
○	Wednesday	09:00 (9:00 am)	Monday	17:00 (5:00 pm)
○	Thursday	09:00 (9:00 am)	Monday	17:00 (5:00 pm)
○	Friday	09:00 (9:00 am)	Monday	17:00 (5:00 pm)
○	Saturday	09:00 (9:00 am)	Monday	17:00 (5:00 pm)
●	Sunday	00:00 (12:00 am)	Monday	17:00 (5:00 pm)

1 - 7 of 7

Figure 99 : Authorized Usage Periods

The following table describes **Authorization Usage Periods**.

Table 58: Authorization Usage Periods components

Component	***Description***
Start Day	Displays the day on which the usage period begins.
Start Time	Displays the time at which the usage period begins.
End Day	Displays the day on which the usage period ends.

Component	***Description***
End Time	Displays the time at which the usage period ends.
Edit	Click **Edit** to modify a usage period.
Add	Click **Add** to add a new usage period, then use the menu to choose a day and time for each start and end time.
Delete	Click **Delete** to remove a usage period.

A usage period can span multiple days with a maximum of 7 days (e.g. from Monday 12:00 AM to Sunday 11:59 PM). A usage period can have only one start day and time, and one end day and time. To establish a daily usage period of 9 AM to 5 PM, you must define a usage period for each day of the week.

If the start day and the end day are the same, and the end time precedes the start time, the authorization policy applies at all times except those between the end time and the start time on that day.

For example, if the start day and time are Monday 13:00 (1 PM) and the end day and time are Monday 08:00 (8 AM), then operations are allowed from 1 PM Monday until 8 AM the following Monday.

6.7 Configuring users and groups

A user directory contains a list of users who may access the keys on your ESKM appliance, and a list of groups to which those users belong. The appliance can use one of the two user directories:

- A local user directory, where users and groups are defined only on the local ESKM appliance and are not available to any other appliance.
- A central server running the Lightweight Directory Access Protocol (LDAP), which enables all ESKM appliances to access the same set of users and groups. If you have several servers in use, LDAP can greatly simplify user and group administration.

6.7.1 KMS Users and Groups

The KMS server can either use local user and group authentication or LDAP authentication; it cannot use both at the same time. You can define which authentication method your ESKM appliance uses on the KMS Configuration page. See KMS server authentication settings (p. 404) for more details.

When you configure the ESKM appliance to use an LDAP user directory instead of the local user directory (or vice versa), or change the LDAP server settings to point to a different user directory, existing key permissions become invalid if the user and group names no longer exist in the new user directory. However, if a user or group name appears in both the old and new directories, the new user or group inherits the key permissions and database user mappings from the old user or group.

6.7.2 KMIP Users and Groups

The KMIP server only uses local user and group authentication, LDAP authentication is not supported for KMIP.
All users configured in the ESKM appliance can use the ESKM XML protocol via the KMS server. KMIP requires an additional set of user properties. Therefore, to use the KMIP protocol, these users must be KMIP-enabled, and the KMIP-specific properties must be correctly configured.

6.8 User and Group Configuration

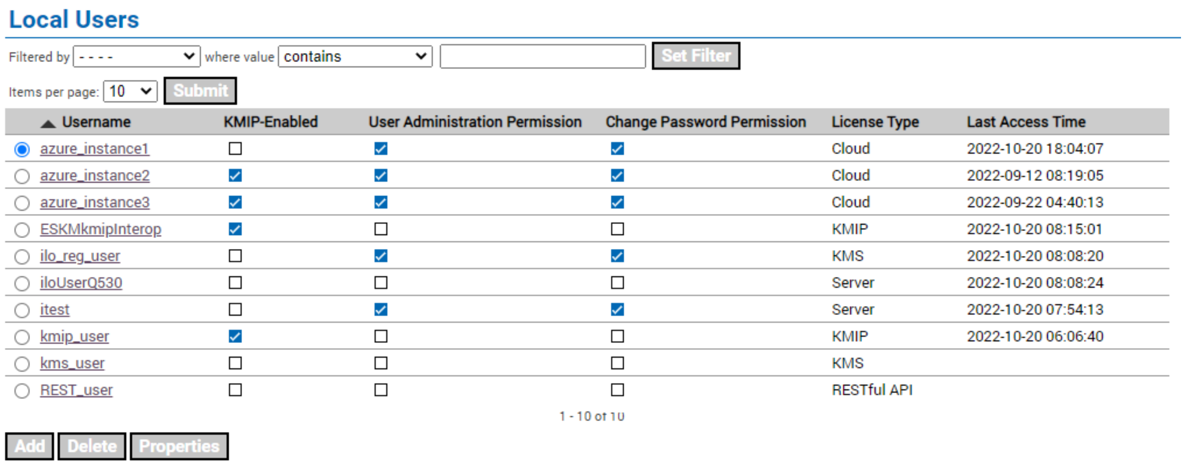
The User and Group Configuration page (**Security > Users & Groups > Local Users & Groups**) allows you to view, create, and modify the local user and group directory on the ESKM appliance. This section discusses the following topics:

- Local users (p. 299)
- Selected local user (p. 301)
- Local groups (p. 310)
- Local group administration (p. 311)
- LDAP server configuration (p. 326)
- LDAP user and group configuration (p. 331)

6.8.1 Local users

Use **Local Users** to add or modify local users. Once a user has been created, you can change the password but you cannot change the username.

A license is required for every user added to the ESKM appliance.



Local Users

Filtered by - - - - where value contains Set Filter

Items per page: 10 Submit

	▲ Username	KMIP-Enabled	User Administration Permission	Change Password Permission	License Type	Last Access Time
●	azure_instance1	□	☑	☑	Cloud	2022-10-20 18:04:07
○	azure_instance2	☑	☑	☑	Cloud	2022-09-12 08:19:05
○	azure_instance3	☑	☑	☑	Cloud	2022-09-22 04:40:13
○	ESKMkmipInterop	☑	□	□	KMIP	2022-10-20 08:15:01
○	ilo_reg_user	□	☑	☑	KMS	2022-10-20 08:08:20
○	iloUserQ530	□	□	□	Server	2022-10-20 08:08:24
○	itest	□	☑	☑	Server	2022-10-20 07:54:13
○	kmip_user	☑	□	□	KMIP	2022-10-20 06:06:40
○	kms_user	□	□	□	KMS	
○	REST_user	□	□	□	RESTful API	

1 - 10 of 10

Figure 100 : Local Users

The following table describes the components of **Local Users**.

Table 59: Local Users components

Component	***Description***

Username	This is the name of the user. The username must begin with a letter, it must be between 1 and 64 characters (inclusive), and it can consist of letters, numbers, underscores (_), periods (.), and hyphens (-).
	KMIP-enabled users using device authentication have a special username format.
	`device-serial-number:device-identifier:`
	`network-identifier:machine-identifier:media-identifier`
	For example, if the device serial number is *serial123*, device identifier is *devid456*, and machine identifier is *machine1*, and the network identifier and media identifier are blank, then the username should be configured as *serial123:devid456::machine1:*.
	The password field in the credential structure should match the password configured for this KMIP-enabled user. For more information, see Device credential authentication (p. 51).

KMIP Enabled	Specifies whether or not this user is KMIP-enabled. All users, whether or not they are KMIP-enabled, can communicate with the KMS server over the ESKM XML protocol. Only KMIP-enabled users can communicate using the KMIP protocol. ⚠ You can select KMIP-Enabled in the **Filtered by** drop-down box and enter "1" in the text box before the **Set Filter** button to select only the KMIP-enabled users. It is not possible to select only non KMIP-enabled users.
User Administration Permission	When selected, this user can create, modify, and delete users and groups via the ESKM XML interface. This permission also allows a user to modify his or her own user permissions. Users with the User Administration Permission value selected, automatically have the Change Password Permission.
Change Password Permission	When selected, this user can change the password via the ESKM XML interface. Users with User Administration Permission selected, automatically have the Change Password Permission.

Component	***Description***
License Type	This is the category of license, to which the user belongs.
Last Access Time	This shows the last time when user accessed the ESKM.
Add	Click **Add** to add a user.
Delete	Click **Delete** to delete a user.
Properties	Click **Properties** to access the **Selected Local User** page, which provides access to the Memberships, Interoperability, and Customer Attributes tabs. You can also click on the hypertext at the user name to access the user properties.

6.8.1.1 User administration permission

❗ You should be extremely cautious in assigning the User Administration Permission. Its use should be reserved for situations where you want to perform user administration programmatically using the ESKM XML interface (as opposed to the Management Console). In such deployments, the User Administration Permission should be given to a limited number of users. Most users should not be given this permission.

⚠ The User Administration Permission and Change Password Permission apply only to local users. LDAP users cannot be managed through the ESKM appliance; they must be managed through the LDAP server.

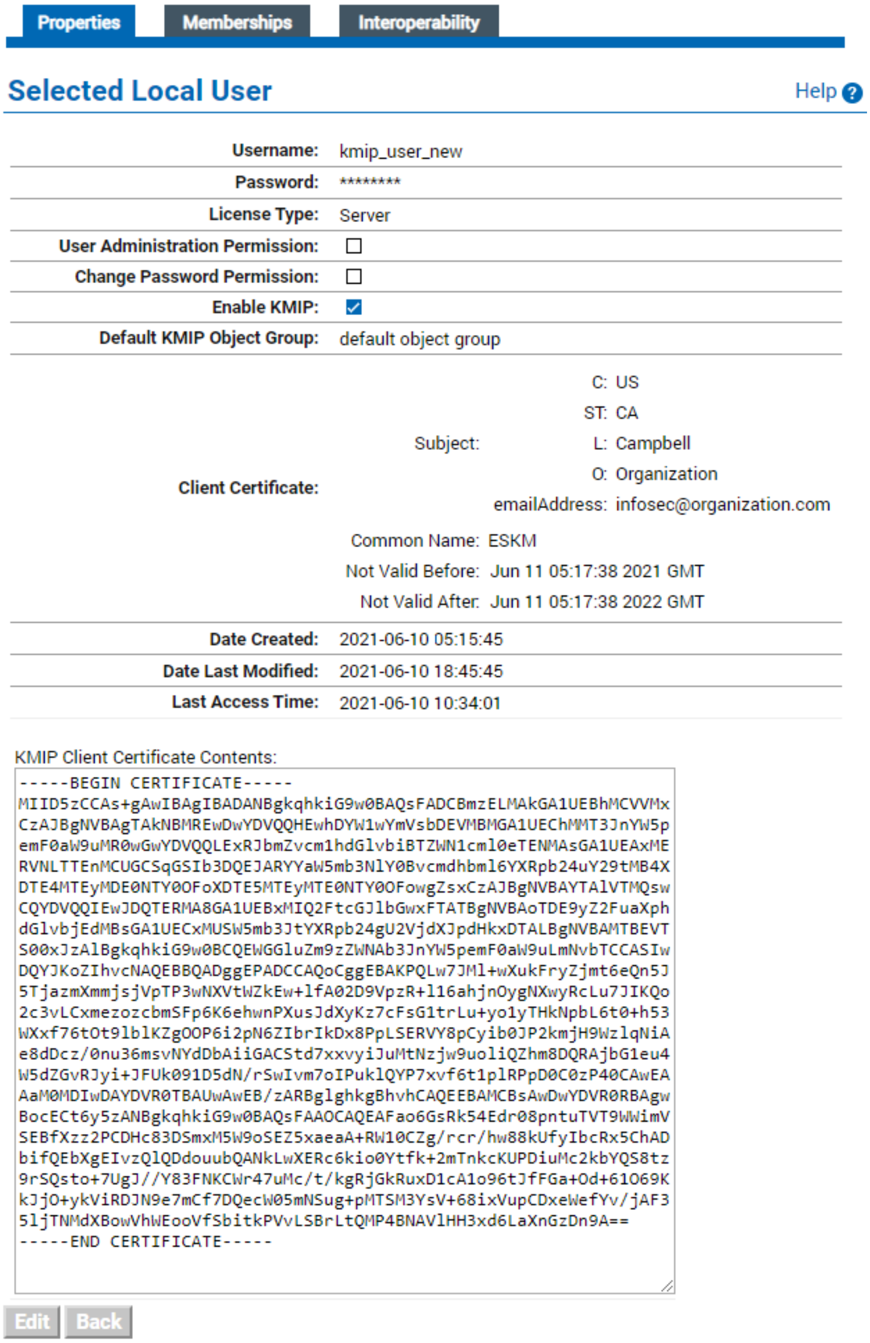
6.8.2 Selected local user

Use Selected Local User to view information about an individual user. Specific user information is provided in these three tabs:

- Properties (p. 302)
- Memberships (p. 305)
- Interoperability (p. 307)
- Custom Attributes (p. 308)

6.8.2.1 Properties

Use the **Properties** tab to display general user information.



Selected Local User

Username:	kmip_user_new
Password:	********
License Type:	Server
User Administration Permission:	□
Change Password Permission:	□
Enable KMIP:	☑
Default KMIP Object Group:	default object group
Client Certificate:	Subject: C: US ST: CA L: Campbell O: Organization emailAddress: infosec@organization.com Common Name: ESKM Not Valid Before: Jun 11 05:17:38 2021 GMT Not Valid After: Jun 11 05:17:38 2022 GMT
Date Created:	2021-06-10 05:15:45
Date Last Modified:	2021-06-10 18:45:45
Last Access Time:	2021-06-10 10:34:01

KMIP Client Certificate Contents:

```
-----BEGIN CERTIFICATE-----
MIID5zCCAs+gAwIBAgIBADANBgkqhkiG9w0BAQsFADCBmzELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcm1hdGlvbiBTZWN1cml0eTENMAsGA1UEAxME
RVNLTTEnMCUGCSqGSIb3DQEJARYYaW5mb3NlY0Bvcmdhbml6YXRpb24uY29tMB4X
DTE4MTEyMDE0NTY0OFoXDTE5MTEyMTE0NTY0OFowgZsxCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJDQTERMA8GA1UEBxMIQ2FtcGJlbGwxFTATBgNVBAoTDE9yZ2FuaXph
dGlvbjEdMBsGA1UECxMUSW5mb3JtYXRpb24gU2VjdXJpdHkxDTALBgNVBAMTBEVT
S00xJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9uLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPQLw7JMl+wXukFryZjmt6eQn5J
5TjazmXmmjsjVpTP3wNXVtWZkEw+lfA02D9VpzR+l16ahjnOygNXwyRcLu7JIKQo
2c3vLCxmezozcbmSFp6K6ehwnPXusJdXyKz7cFsG1trLu+yo1yTHkNpbL6t0+h53
WXxf76tOt9lblKZgOOP6i2pN6ZIbrIkDx8PpLSERVY8pCyib0JP2kmjH9WzlqNiA
e8dDcz/0nu36msvNYdDbAiiGACStd7xxvyiJuMtNzjw9uoliQZhm8DQRAjbG1eu4
W5dZGvRJyi+JFUk091D5dN/rSwIvm7oIPuklQYP7xvf6t1plRPpD0C0zP40CAwEA
AaM0MDIwDAYDVR0TBAUwAwEB/zARBglghkgBhvhCAQEEBAMCBsAwDwYDVR0RBAgw
BocECt6y5zANBgkqhkiG9w0BAQsFAAOCAQEAFao6GsRk54Edr08pntuTVT9WWimV
SEBfXzz2PCDHc83DSmxM5W9oSEZ5xaeaA+RW10CZg/rcr/hw88kUfyIbcRx5ChAD
bifQEbXgEIvzQlQDdouubQANkLwXERc6kio0Ytfk+2mTnkcKUPDiuMc2kbYQS8tz
9rSQsto+7UgJ//Y83FNKCWr47uMc/t/kgRjGkRuxD1cA1o96tJfFGa+Od+61O69K
kJjO+ykViRDJN9e7mCf7DQecW05mNSug+pMTSM3YsV+68ixVupCDxeWefYv/jAF3
5ljTNMdXBowVhWEooVfSbitkPVvLSBrLtQMP4BNAVlHH3xd6LaXnGzDn9A==
-----END CERTIFICATE-----
```

Figure 101 : Selected local KMIP-enabled user with certificate

The following table describes the components of the **Selected Local User**.

Table 60: Selected Local User components

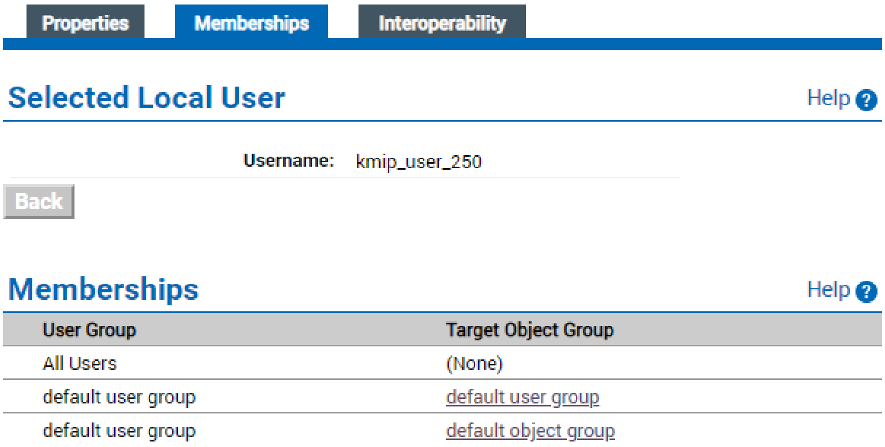
Component	***Description***
Username	This is the name of the user. The username must begin with a letter, it must be between 1 and 64 characters (inclusive), and it can consist of letters, numbers, underscores (_), periods (.), and hyphens (-).
Password	The password for the local user. The requirements for the local user password depend on your Password Management Settings. For information on password requirements, see Password constraints (p. 491). The maximum password length is 256 characters. The passwords displayed on Local Users are masked with eight asterisks (*). When changing the password, you should clear this field before entering the new password. If you do not clear this field, the asterisks become a part of the new password. ⚠ This password is used for both ESKM and KMIP authentication.
License Type	This is the category of license, to which the user belongs.
Last Access Time	This shows the last time when user accessed the ESKM.
User Administration Permission	When selected, this user can create, modify, and delete users and groups via the ESKM XML interface. This permission also allows a user to modify his or her own user permissions. Users with the User Administration Permission value selected, automatically have the Change Password Permission.
Change Password Permission	When selected, this user can change the password via the ESKM XML interface. Users with User Administration Permission selected, automatically have the Change Password Permission.
Enable KMIP	When checked, this user is KMIP-enabled. All users can send requests to the KMS using the ESKM XML protocol, but only KMIP-enabled users can send requests to the ESKM appliance using the KMIP protocol via port 5696 (default).

Component	***Description***
Default KMIP Object Group *	The default KMIP object group for this user. This is the object group that KMIP-managed objects, created by this user, will be placed in, if no Object Group attribute is specified in the KMIP client request. Ensure that you specify an object group that this KMIP-enabled user has privileges to write to; otherwise, all KMIP client requests without an Object Group attribute will fail.
Client Certificate *	The KMIP client certificate is used for KMIP authentication using certificates. For more information on certificate-based authentication, see Certificate-based authentication (p. 50).
Date Created*	The date this user was created.
Date Last Modified *	The date this user was last modified.
Client Certificate Contents *	The contents of the certificate uploaded by the client. This is displayed only for KMIP-enabled users who can use certificate authentication.
Edit	Click **Edit** to modify the properties for this user.
Back	Click **Back** to return to the Local Users section.
⚠ *These components are displayed only for KMIP-enabled users.	

6.8.2.2 Memberships

Use the **Memberships** tab to view information about an individual KMIP-enabled user. Since the KMIP permission model is based on groups, all users who are members of the same user group share the same privileges. For more information, see KMIP permission model (p. 38).

This section is read-only. To modify user memberships, go to the **Local Groups** menu and select the group name.



Selected Local User

Username: kmip_user_250

Memberships

User Group	Target Object Group
All Users	(None)
default user group	default user group
default user group	default object group

Figure 102 : Selected local user - KMIP-enabled user group memberships

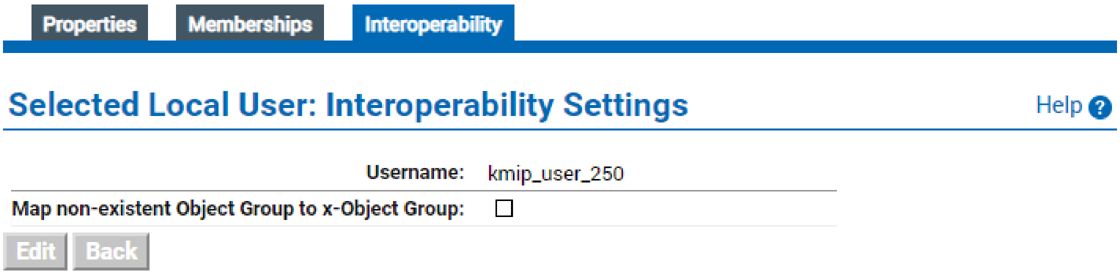
The following section describes **Memberships**. It shows the user groups that the user is a member of, and the privileges the members of this user group have, to perform various KMIP operations on the target object groups.

- The first entry - All Users, indicates that this user is a member of the system-defined All Users group. This is a special group that all KMIP-enabled users belong to; it is used for internal purposes only. Therefore, the Target Object Group is (None), indicating that there are no target object groups that the members are allowed to access.
- The second entry indicates that this user is a member of the group named default user group, and that members of this user group have at least one privilege to manipulate objects in the default object group. For details on the privileges are available, click on to the default object group hypertext. For more information on the relationship between source user groups and target object groups, see KMIP permission model (p. 38).
- The last entry indicates that the user group, default user group, also has privileges to manipulate itself. As discussed in Source groups and target groups (p. 40), a target group is typically an object group; it may also be a user group. Privileges for target user groups are useful for KMIP operations like Cancel and Poll.

6.8.2.3 Interoperability

Interoperability settings are sometimes required in order for KMIP clients from certain vendors to operate correctly with the KMIP server on the ESKM appliance. Configuring interoperability settings may result in non-compliant KMIP behavior. Use these settings only when necessary.

Use the **Interoperability** tab to view and configure interoperability settings for this KMIP-enabled user. Global interoperability settings may also be configured in **Device > KMIP Server > Interoperability.**



Selected Local User: Interoperability Settings

Username: kmip_user_250

Map non-existent Object Group to x-Object Group: □

Figure 103 : Interoperability

The following table describes the components of **Interoperability**.

Table 61: Interoperability components

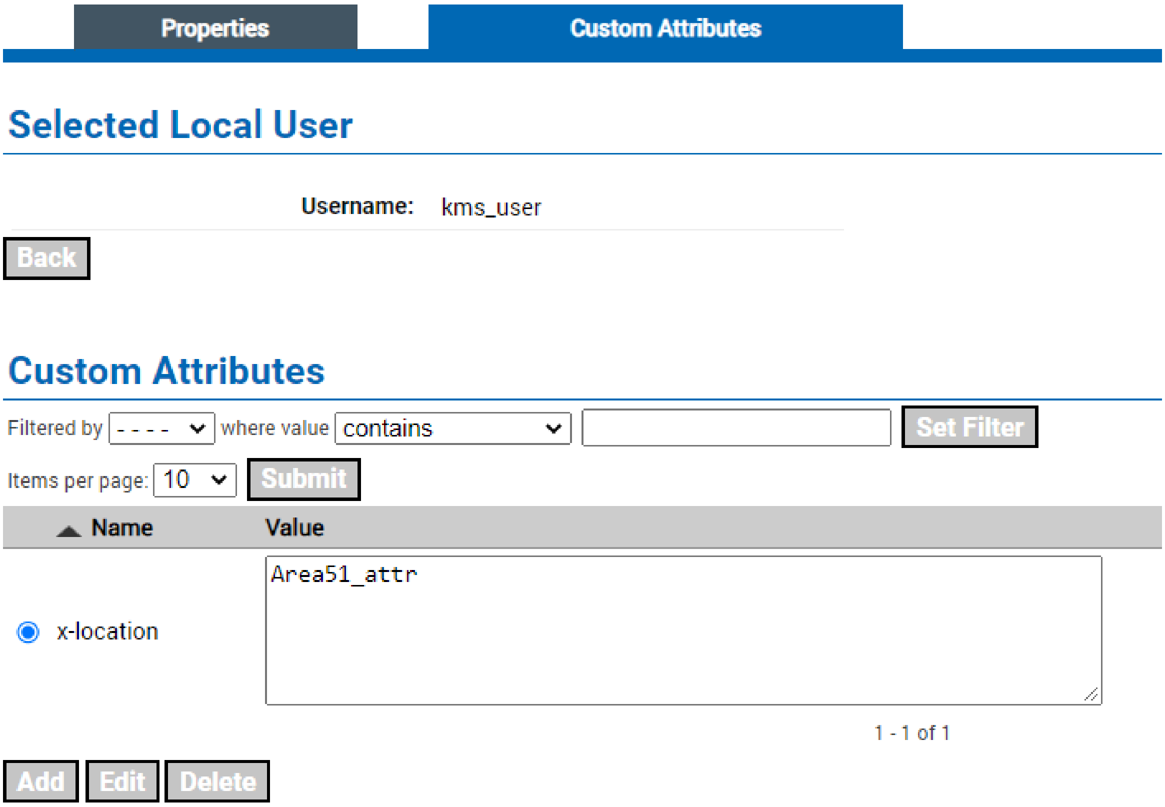
Component	***Description***
Username	The name of the selected local user.

Component	***Description***
Map non-existent Object Group to x-Object Group	This setting enables support for clients which assume that any value can be provided in an Object Group attribute without requiring pre-configuration. If checked, the KMIP requests specifying an Object Group attribute value that does not exist on the ESKM appliance, will have this attribute mapped to a custom attribute named x-Object Group. If unchecked, the KMIP server performs the normal handling, which is to fail the request. ⚠ Enabling this interoperability option will result in non-standard KMIP behavior. This option should be enabled only for KMIP clients which will not work without this setting enabled.
Edit	Click **Edit** to alter the interoperability settings.
Back	Click **Back** to return to the Local User listing.

6.8.2.4 Custom Attributes

⚠ No custom attributes are supported for KMIP users.

Use Custom Attributes to view and assign your own attributes to a local user.



Selected Local User

Username: kms_user

Custom Attributes

Filtered by - - - - where value contains

Items per page: 10

Name	Value
● x-location	Area51_attr

1 - 1 of 1

Figure 104 : Custom Attributes

The following table describes the components of Custom Attributes.

Component	***Description***
Attribute Name	Enter the name of the attribute. Attribute names must contain alphanumeric characters only. You cannot include special characters or whitespaces in the name.
Attribute Value	Enter the value of the attribute. It can contain any printable ASCII characters and spaces, tab, \n, and \r. Maximum length is 1024 characters.

Component	***Description***
Edit	Click Edit to alter the selected attribute.
Add	Click Add to add an attribute.
Delete	Click Delete to remove the selected attribute.

6.8.3 Local groups

Local Groups lists the users in a group and allows you to modify group membership.

To access the local group administration screens, go to Security > Local Users & Groups > Local Groups. These group types are supported:

- KMS groups (p. 310)
- KMIP groups (p. 310)

The purpose of these groups are discussed in this section.

6.8.3.1 KMS groups

KMS groups are used to determine group permissions for KMS keys used by the KMS server in the ESKM XML protocol. All users can be members of KMS groups.

6.8.3.2 KMIP groups

KMIP groups are used to determine the permissions for various KMIP operations used by the KMIP server. KMIP groups are further subdivided into two subtypes:

- User groups: Only KMIP-enabled users can be members of KMIP user groups.
- Object groups: Only KMIP-managed objects can be members of KMIP object groups.

The KMIP permission model governs the permissions for users to perform various operations on either user groups or object groups. See KMIP permission model (p. 38) for a discussion on how group membership governs access to various KMIP operations.

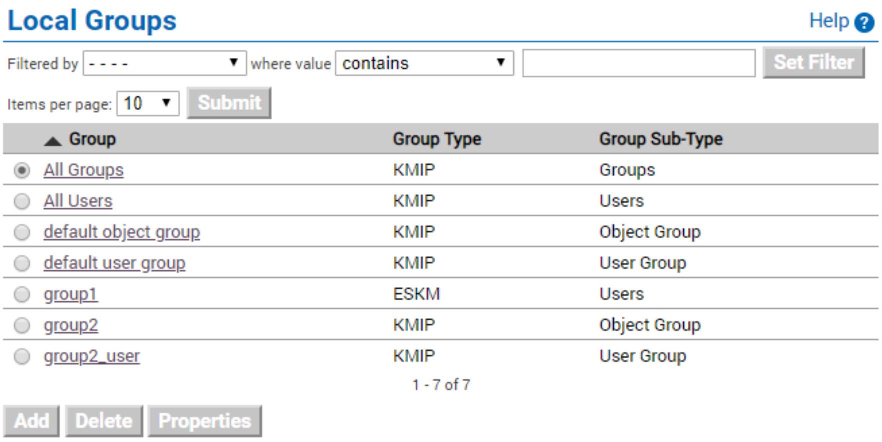
6.8.4 Local group administration

The **Local Group administration** screens can be divided into the following categories:

- Displaying the list of queries (p. 269)
- Displaying and modifying local group properties (p. 314)
- Adding a new group (p. 320)
- Deleting an existing group (p. 325)

6.8.4.1 Displaying the list of groups

Local Groups lists the groups and allows you to modify group membership and permissions.



Local Groups

Filtered by: - - - - where value: contains

Items per page: 10

	Group	Group Type	Group Sub-Type
●	All Groups	KMIP	Groups
○	All Users	KMIP	Users
○	default object group	KMIP	Object Group
○	default user group	KMIP	User Group
○	group1	ESKM	Users
○	group2	KMIP	Object Group
○	group2_user	KMIP	User Group

1 - 7 of 7

Figure 105 : Local Groups

The following table describes the components of **Local Groups**.

Table 62: Local Groups components

Component	***Description***
Group	Displays the local groups on the ESKM appliance.
Group Type	The group type: either KMS or KMIP.

Component	***Description***
Group Sub-Type	The group sub-type. The sub-type for KMS groups is always Users. For KMIP groups, there are four possible sub-types: ▪ **Groups**: This is only used for the system-defined group All Groups. ▪ **Users**: This is only used for the system-defined group All Users. ▪ **User Group**: This is used for user groups, which may contain either users or groups of users. A user group can only contain users. ▪ **Object Group**: This is used for object groups, which may contain either KMIP-managed objects or other object groups. An object group only supports objects.
Add	Click **Add** to add a group to the group list.
Delete	Click **Delete** to delete a group from the group list.
Properties	Click **Properties** to access the group properties. For KMS groups, properties include the User List, where you can view and configure the users in the selected group. KMIP group properties include additional details of group memberships and permission.

Predefined KMIP groups

There are four pre-defined KMIP groups that are created automatically during the ESKM appliance installation process. These groups are either used for internal administrative purposes by the KMIP server or as part of the KMIP permission model.

The following table describes the predefined KMIP groups.

Table 63: Predefined KMIP groups

Group Name	***Group Subtype***	***Description***
All Groups	Groups	The group that contains all KMIP groups. Every KMIP group, including the All Groups group, is a member of this group. This group is maintained by the ESKM appliance and cannot be modified or deleted by the user.
All Users	Users	The group that contains all KMIP users. Every KMIP user is a member of this group, in addition to the group that is specified in the KMIP user creation or modification request. This group is maintained by the ESKM appliance and cannot be modified or deleted by the user.
default object group	Object Group	The name of a predefined object group. When creating or modifying a KMIP-enabled user, you can either choose this object group in the user's Default KMIP Object Group property or create custom groups. A default object group is one where objects created by a KMIP-enabled user will be placed, if no Object Group attribute is specified in the KMIP client request. If no custom groups are created, this will be the only object group displayed in the drop-down list box of the **Default KMIP Object Group** field when creating or modifying a KMIP-enabled user.

Group Name	***Group Subtype***	***Description***
default user group	User Group	The name of a predefined user group. When creating a KMIP-enabled user, you can either choose this user group in the user's KMIP User Group property or create custom groups. In order for a KMIP-enabled user to perform any KMIP client operations, it must belong to at least one user group. If no custom groups are created, this will be the only user group displayed in the drop-down list box of the **KMIP User Group** field when creating a KMIP-enabled user.

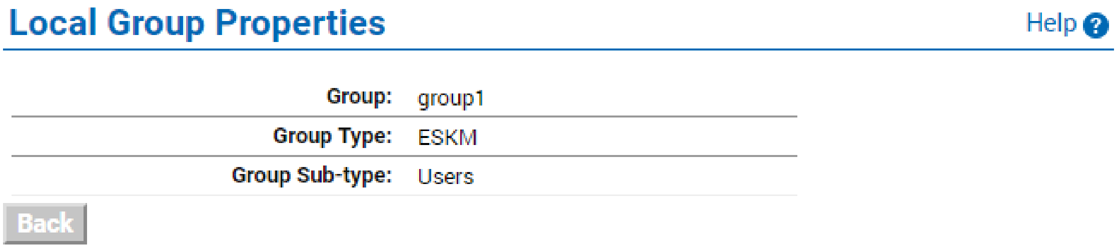
6.8.4.2 Displaying and modifying local group properties

Local Group Properties displays general properties of the group. The contents of the **Properties** tab depend on whether this is a KMS or KMIP group.

6.8.4.2.1 KMS group properties

For KMS groups, **Local Group Properties** displays the group name. The **Group Type** and **Group Sub-Type** fields are always set to ESKM and Users respectively. KMS group names cannot be modified.

The following figure shows **Local Group Properties**.



Local Group Properties

Group:	group1
Group Type:	ESKM
Group Sub-type:	Users

Figure 106 : Local Group Properties

The following table describes the components of **Local Group Properties**.

Table 64: Local Group Properties components

Component	*Description*
Group	Displays the name of the selected group.
Group Type	The group type of the selected group. This can be either ESKM or KMIP.
Group Sub-Type	The sub-type of the selected group.
Back	Click **Back** to return to Local Groups.

The following figure shows the **User List** of **Local Group Properties**. It lists the users in a group and allows you to view and modify KMS group membership.

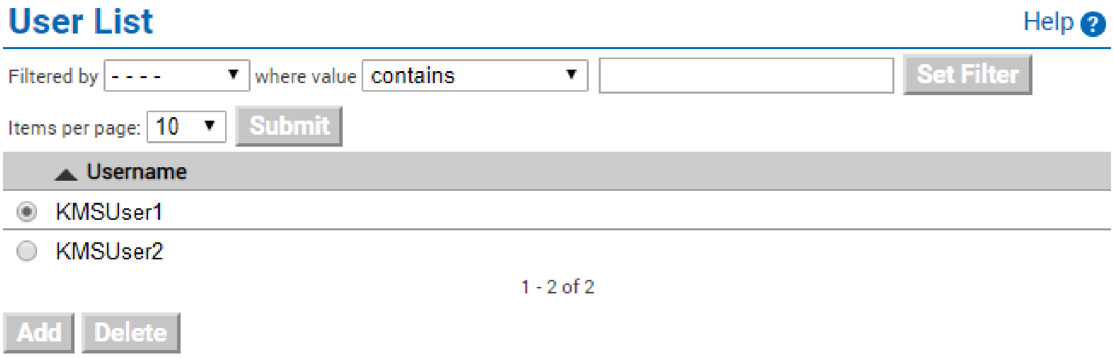


Figure 107 : User List

The following table describes the components of the **User List**.

Table 65: User List components

Component	*Description*
Username	Displays the users in the group.
Add	Click **Add** to add a user to the user list.

Component	***Description***
Delete	Click **Delete** to delete a user from the user list.

6.8.4.2.2 KMIP group properties

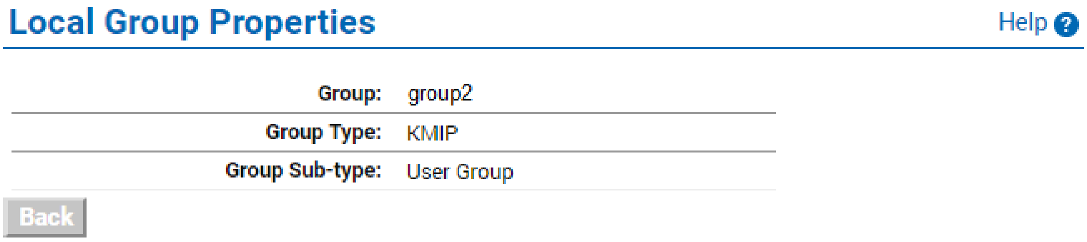
KMIP groups contain two types of properties, each of which has its own tab:

- Group Membership List (p. 316)
- Target Group Permissions (p. 316)

Group Membership List

For KMIP groups, **Local Group Properties** displays the **Group name**. The **Group Type** is always set to KMIP. **Group Sub-Type** field displays the group sub-type.

The following figure shows **Local Group Properties**.



Local Group Properties

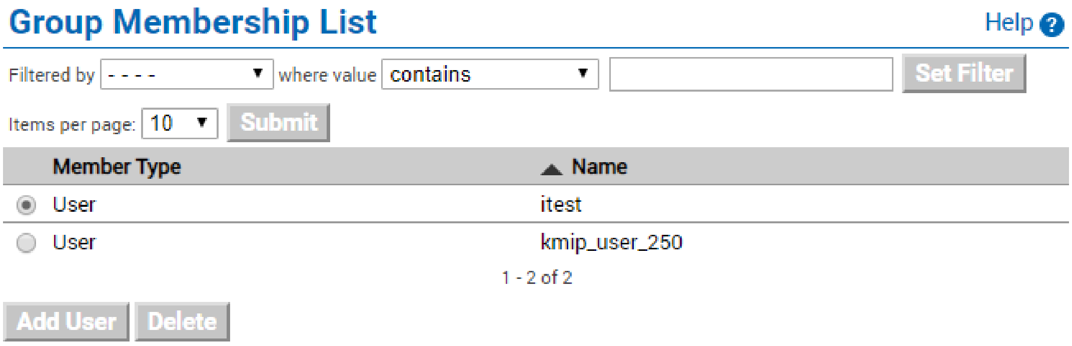
Group:	group2
Group Type:	KMIP
Group Sub-type:	User Group

Figure 108 : Local Group Properties for a KMIP group

The **Group Membership List** lists the group members and enables the administrator to modify group membership. The group membership depends on the Group Sub-type:

- **User groups** contain only users.
- **Object groups** contain only KMIP-managed objects.

The following figure provides an example of the **Group Membership List** for a KMIP user group.



Group Membership List

	Member Type	▲ Name
●	User	itest
○	User	kmip_user_250

1 - 2 of 2

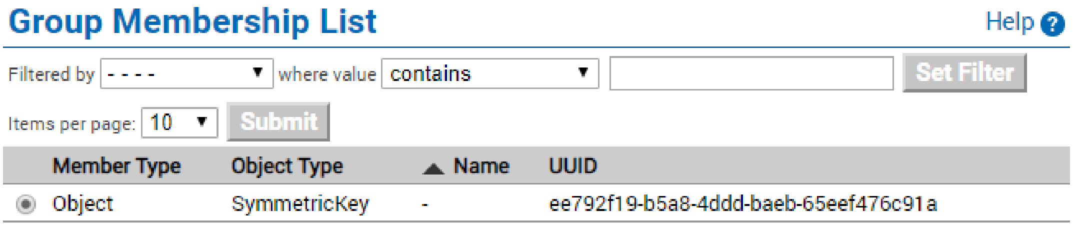
Figure 109 : Group Membership for a KMIP group

The following table describes the components of the **Group Membership List** for KMIP user groups.

Table 66: Group Membership List components

Component	***Description***
Member Type	Displays the member type. This will always be User, since only users can be members of KMIP user groups.
Name	The name of the KMIP-enabled user.
Add User	Click **Add User** to add another user to the KMIP user group.
Delete	Click **Delete** to delete the user from the KMIP user group. Since group memberships determine the objects which the user can access, care should be taken to ensure that the user is a member of at least one user group which has access rights to the target object group.

The following figure provides an example of the **Group Membership List** for object groups.



Group Membership List

	Member Type	Object Type	▲ Name	UUID
●	Object	SymmetricKey	-	ee792f19-b5a8-4ddd-baeb-65eef476c91a

Figure 110 : Group Membership for KMIP object groups

The following table describes the components of the **Local Group Properties**.

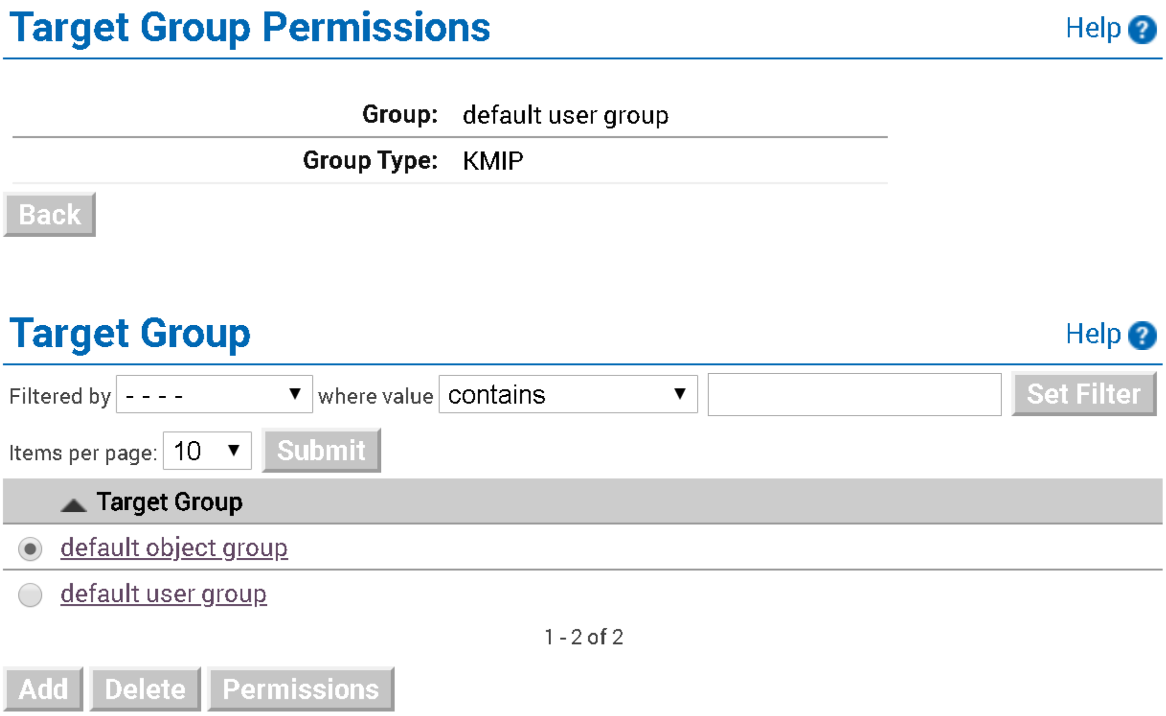
Table 67: Group Membership List components

Component	***Description***
Member Type	Displays the member type. This will always be Object, since only KMIP-managed objects can be members of KMIP object groups.
Object Type	The object type, such as SymmetricKey. A full list of KMIP object types can be found in the KMIP Specification.
Name	The object name, if available.
UUID	The object UUID which uniquely identifies the object.

KMIP object group membership cannot be modified from the Management Console. To modify KMIP object group membership, use the KMIP client interface with operations such as **Create**, **Create Key Pair**, **Add Attribute**, **Delete Attribute**, or **Modify Attribute**, specifying the Object Group property. For example, to create a symmetric key in the Encryption object group, use the KMIP Create operation and specify the Object Group property with the value Encryption. You can also add a single object to multiple object groups by specifying multiple instances of the Object Group property or by using the **Add Attribute** operation.

Target Group Permissions

A target group is one on which the current source group can operate.



Group:	default user group
Group Type:	KMIP

Target Group
● default object group
○ default user group

1 - 2 of 2

Figure 111 : Target Group Permissions

The following table describes the components of **Target Group Permissions**.

Table 68: Target Group components

Component	***Description***
Back	Click the **Back** button to return to the Local Groups list.
Target Group	Displays the name of the target group.
Add	Click the **Add** button to add a target group to this source group.
Delete	Click the **Delete** button to delete a target group. Deleting a target group also deletes all permissions between the selected source group and the target group. That is, members of the source user group can no longer perform any KMIP operation on the target group.
Permissions	Click **Permissions** to view details on the permissions between the source group and the target group.

6.8.4.3 Adding a new group

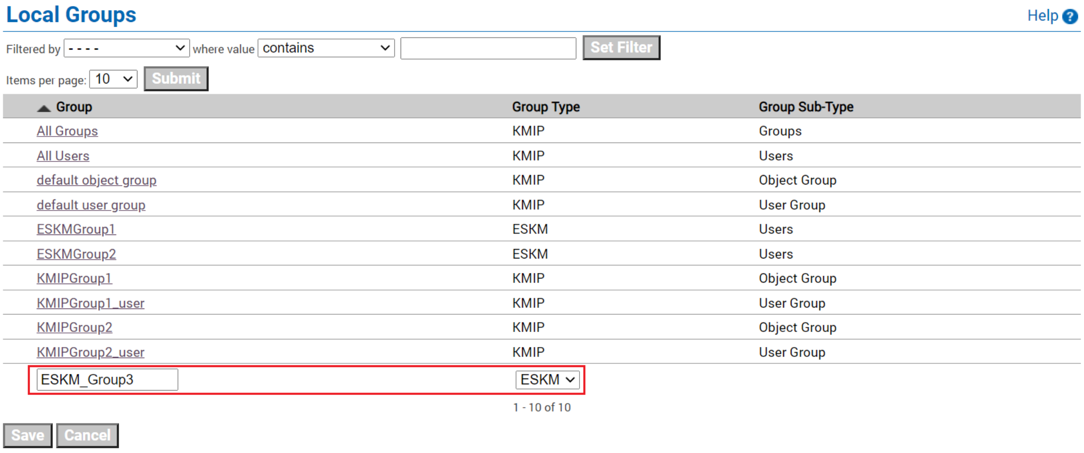
The ESKM appliance supports two types of groups: KMS group and KMIP group. Click the **Add** button in the Local Groups listing to add a new group.

To add a new KMS group

1. Navigate to **Security** > **Users & Groups** > **Local Users & Groups** > **Local Groups**.

2. Click the **Add** button under the Local Groups list.

3. Enter the **Group** name, select **ESKM** from the **Group Type** drop-down list box.



Group	Group Type	Group Sub-Type
All Groups	KMIP	Groups
All Users	KMIP	Users
default object group	KMIP	Object Group
default user group	KMIP	User Group
ESKMGroup1	ESKM	Users
ESKMGroup2	ESKM	Users
KMIPGroup1	KMIP	Object Group
KMIPGroup1_user	KMIP	User Group
KMIPGroup2	KMIP	Object Group
KMIPGroup2_user	KMIP	User Group
ESKM_Group3	ESKM	

Figure 112 : Add KMS Group

4. Click **Save**.

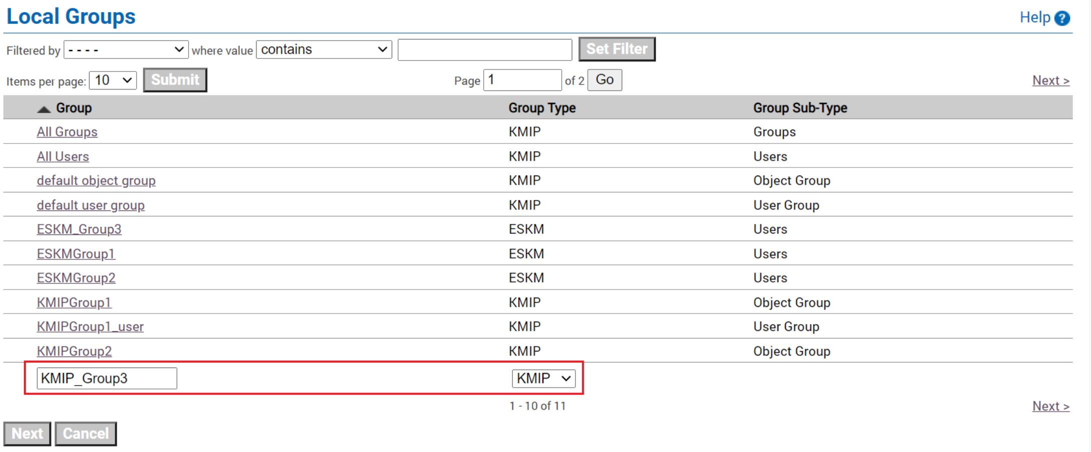
KMS group names can only contain letters, numbers, hyphens, underscores, and periods.

To add a new KMIP group

1. Navigate to **Security** > **Users & Groups** > **Local Users & Groups** > **Local Groups**.

2. Click the **Add** button under the Local Groups list.

3. Enter the **Group** name, select **KMIP** from the **Group Type** drop-down list box.



Local Groups

Filtered by - - - - where value contains

Items per page: 10 Page 1 of 2

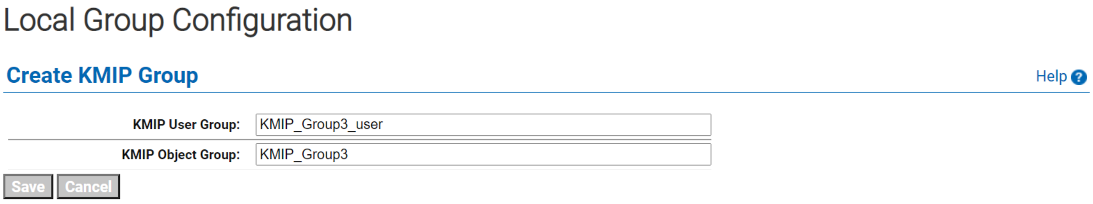
Group	Group Type	Group Sub-Type
All Groups	KMIP	Groups
All Users	KMIP	Users
default object group	KMIP	Object Group
default user group	KMIP	User Group
ESKM_Group3	ESKM	Users
ESKMGroup1	ESKM	Users
ESKMGroup2	ESKM	Users
KMIPGroup1	KMIP	Object Group
KMIPGroup1_user	KMIP	User Group
KMIPGroup2	KMIP	Object Group
KMIP_Group3	KMIP	

1 - 10 of 11

Figure 113 : Add KMIP Group

4. Click **Next.**

   The ESKM appliance automatically creates a corresponding KMIP user group, with "_user" appended to the name.



Local Group Configuration

Create KMIP Group

KMIP User Group: KMIP_Group3_user

KMIP Object Group: KMIP_Group3

Figure 114 : KMIP Group

5. At the **Create KMIP Group** screen, you can change the name of KMIP user and/or object group. Click **Save.**

> ⚠ The maximum length of a KMIP group name is 255 characters.

All permissions from the source user group to the target object group will be enabled. KMIP clients will be able to perform any operation if they are members of the user group and the objects they create or manipulate are members of the target group. See KMIP permission model (p. 38) for a discussion on the relationship between users, groups, and permissions, and a more specific discussion on permissions in the section Operation-based permissions (p. 45).

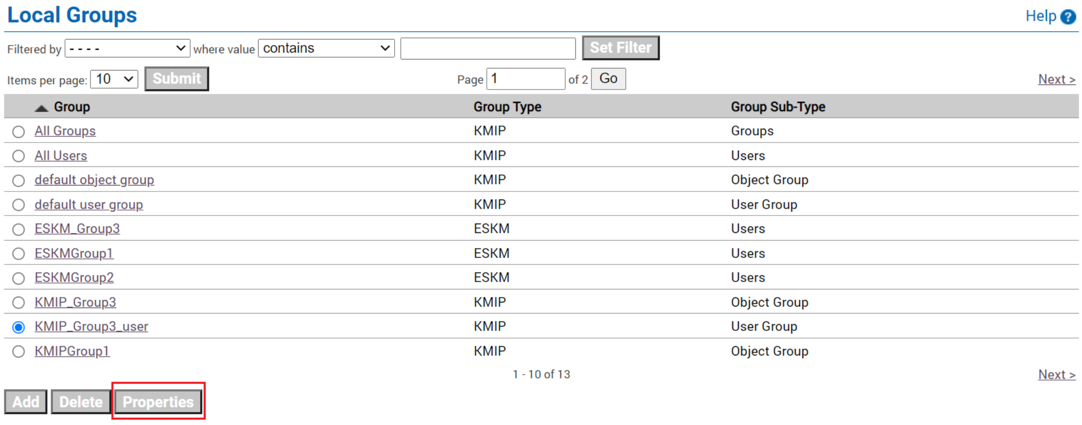
For example, a user belonging to the source group2 user group would need **Create** permission to create a symmetric key in the group2_objects object group, and **Create Key Pai**r permission to create an asymmetric key pair.

As discussed in KMIP permission model (p. 38), although the target group is normally an object group, it may also be a user group in some cases. Permissions such as **Hash** and **Poll** apply to target user groups, as such, a user belonging to the group2 source user group would need **Poll** permission in order to perform the KMIP Poll operation on the group2 target user group.

To change permissions

1. Select the group at the **Local Groups** screen.

2. Click **Properties**.



Local Groups

Help

Filtered by ---- where value contains [Set Filter]

Items per page: 10 [Submit] Page 1 of 2 [Go] Next >

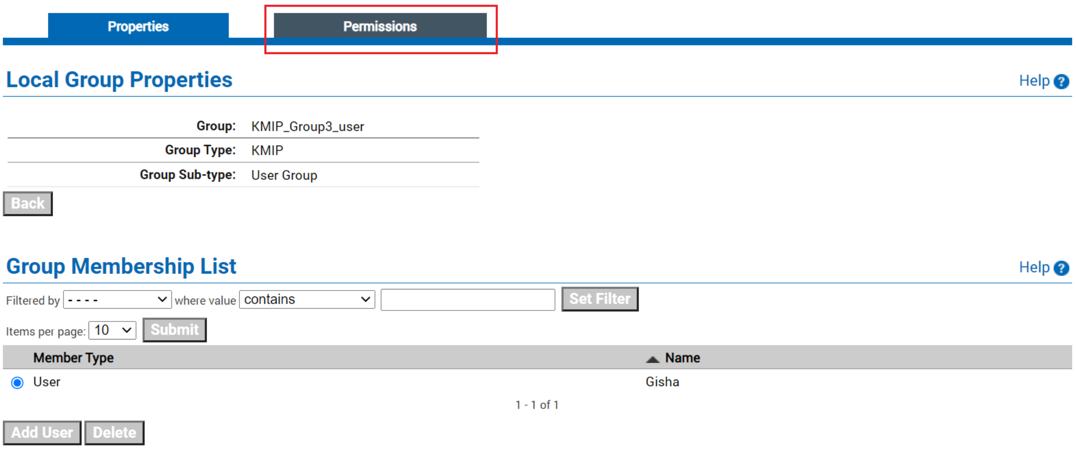
	▲ Group	Group Type	Group Sub-Type
○	All Groups	KMIP	Groups
○	All Users	KMIP	Users
○	default object group	KMIP	Object Group
○	default user group	KMIP	User Group
○	ESKM_Group3	ESKM	Users
○	ESKMGroup1	ESKM	Users
○	ESKMGroup2	ESKM	Users
○	KMIP_Group3	KMIP	Object Group
●	KMIP_Group3_user	KMIP	User Group
○	KMIPGroup1	KMIP	Object Group

1 - 10 of 13 Next >

[Add] [Delete] [Properties]

Figure 115 : Local Groups-Properties tab

3. At the next screen, click the **Permissions** tab.



Local Group Properties

Group:	KMIP_Group3_user
Group Type:	KMIP
Group Sub-type:	User Group

Group Membership List

Filtered by - - - - where value contains

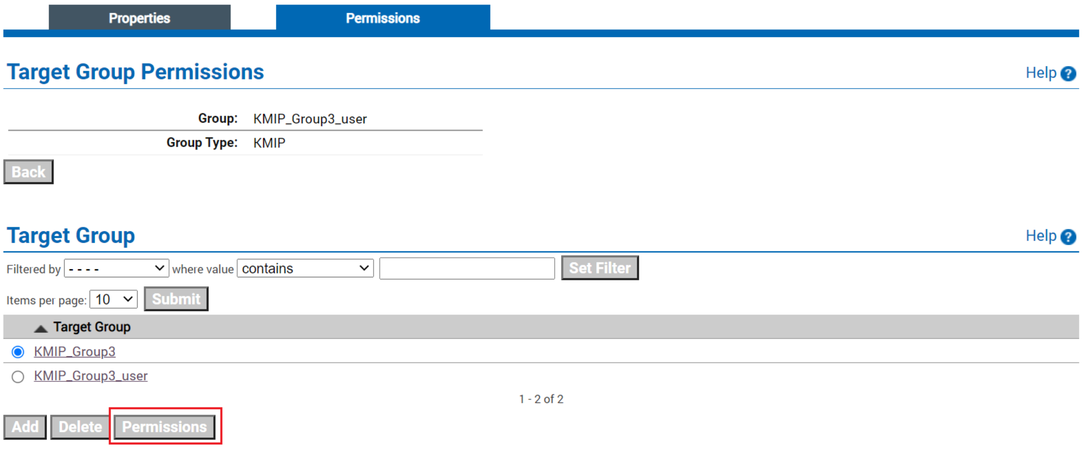
Items per page: 10

	Member Type	Name
●	User	Gisha

1 - 1 of 1

Figure 116 : Permissions tab

4. In Target Group, select the group, and then click the **Permissions** button.



Target Group Permissions

Group:	KMIP_Group3_user
Group Type:	KMIP

Target Group

Filtered by - - - - where value contains

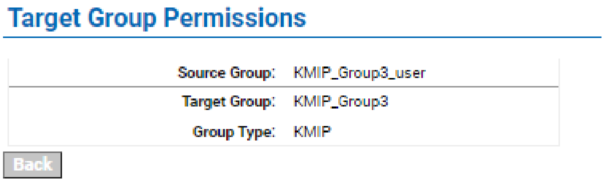
Items per page: 10

	Target Group
●	KMIP_Group3
○	KMIP_Group3_user

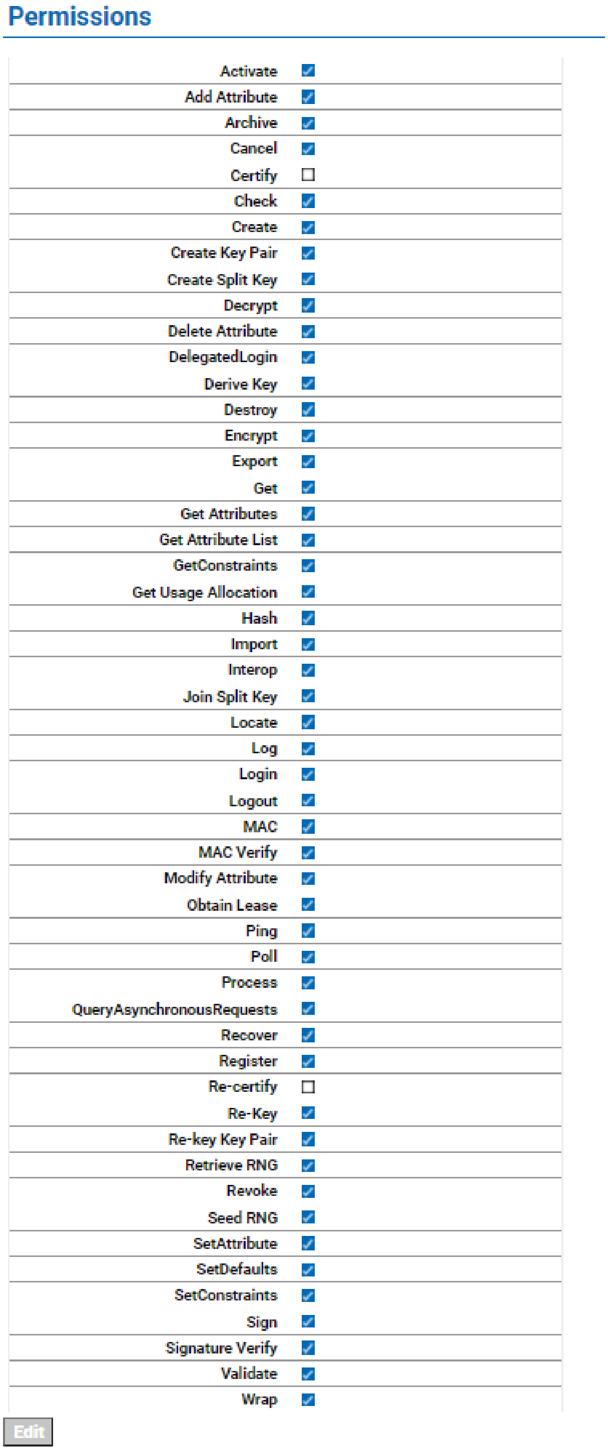
1 - 2 of 2

Figure 117 : Target Group-Permissions

5. Click the **Edit** button to change permissions.


Target Group Permissions

Source Group:	KMIP_Group3_user
Target Group:	KMIP_Group3
Group Type:	KMIP



Permissions

Activate	☑
Add Attribute	☑
Archive	☑
Cancel	☑
Certify	□
Check	☑
Create	☑
Create Key Pair	☑
Create Split Key	☑
Decrypt	☑
Delete Attribute	☑
DelegatedLogin	☑
Derive Key	☑
Destroy	☑
Encrypt	☑
Export	☑
Get	☑
Get Attributes	☑
Get Attribute List	☑
GetConstraints	☑
Get Usage Allocation	☑
Hash	☑
Import	☑
Interop	☑
Join Split Key	☑
Locate	☑
Log	☑
Login	☑
Logout	☑
MAC	☑
MAC Verify	☑
Modify Attribute	☑
Obtain Lease	☑
Ping	☑
Poll	☑
Process	☑
QueryAsynchronousRequests	☑
Recover	☑
Register	☑
Re-certify	□
Re-Key	☑
Re-key Key Pair	☑
Retrieve RNG	☑
Revoke	☑
Seed RNG	☑
SetAttribute	☑
SetDefaults	☑
SetConstraints	☑
Sign	☑
Signature Verify	☑
Validate	☑
Wrap	☑

Figure 118 : KMIP Permissions

6. Click the **Save** button to save the permissions, or click the **Cancel** button to return without saving the permissions.

7. Click the **Back** button to return to the previous page.

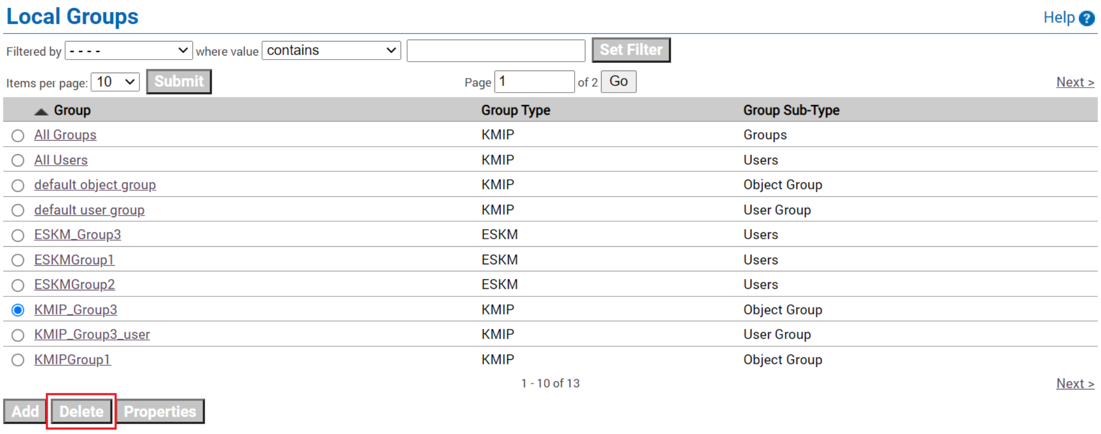
6.8.4.4 Deleting an existing group

To delete an existing group

1. Navigate to the **Local Groups** page (**Security > Users & Groups > Local Users & Groups > Local Groups**).

2. Select the group you wish to delete.

3. Click the **Delete** button.



Filtered by - - - - where value contains

Items per page: 10

Page 1 of 2

	Group	Group Type	Group Sub-Type
○	All Groups	KMIP	Groups
○	All Users	KMIP	Users
○	default object group	KMIP	Object Group
○	default user group	KMIP	User Group
○	ESKM_Group3	ESKM	Users
○	ESKMGroup1	ESKM	Users
○	ESKMGroup2	ESKM	Users
●	KMIP_Group3	KMIP	Object Group
○	KMIP_Group3_user	KMIP	User Group
○	KMIPGroup1	KMIP	Object Group

1 - 10 of 13

Figure 119 : Delete an existing Group

The following restrictions apply:

- You cannot delete the built-in KMIP groups, **All Groups** and **All Users.** The **Delete** button is disabled for these groups.
- You can only delete a KMIP group if it does not have any members.

6.8.5 LDAP server configuration

Lightweight Directory Access Protocol (LDAP) is a protocol that allows you to enable authentication of your ESKM appliance based on a central directory of users, rather than the local users and groups defined on each server. To use LDAP with the ESKM appliance, you need an LDAP server available such as MS Active Directory, Netscape Directory Server or OpenLDAP. You should also be familiar with the schema defined by that server.

> If you set up the ESKM appliance to use LDAP for users and groups, those users and groups are case-insensitive. For example, user ID of JohnSmith can also be used throughout the system as johnsmith. This is different from most other parts of the system where upper and lower cases are treated differently.

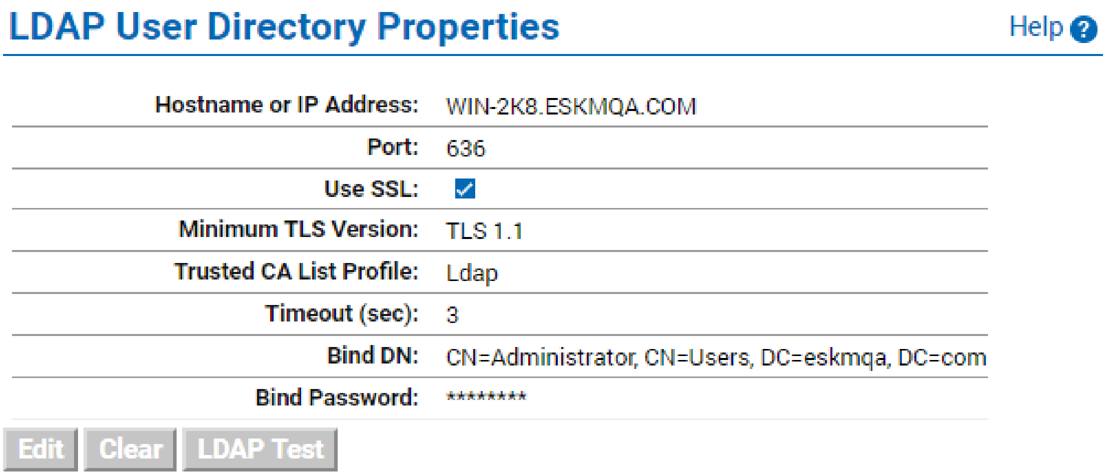
Passwords for both local users and LDAP users must not contain the less than character (<).

The LDAP Server Configuration page of the Management Console (**Security > Users & Groups > LDAP**) describes the configuration of the LDAP server and its schema. This page contains the following sections:

- LDAP user directory properties (p. 326)
- LDAP schema properties (p. 328)
- LDAP failover server properties (p. 330)

6.8.5.1 LDAP user directory properties

Use **LDAP User Directory Properties** to define the basic properties of the LDAP server.



LDAP User Directory Properties

Hostname or IP Address:	WIN-2K8.ESKMQA.COM
Port:	636
Use SSL:	☑
Minimum TLS Version:	TLS 1.1
Trusted CA List Profile:	Ldap
Timeout (sec):	3
Bind DN:	CN=Administrator, CN=Users, DC=eskmqa, DC=com
Bind Password:	********

Figure 120 : LDAP User Directory Properties

The following table describes the components of LDAP User Directory Properties.

Table 69: LDAP User Directory Properties components

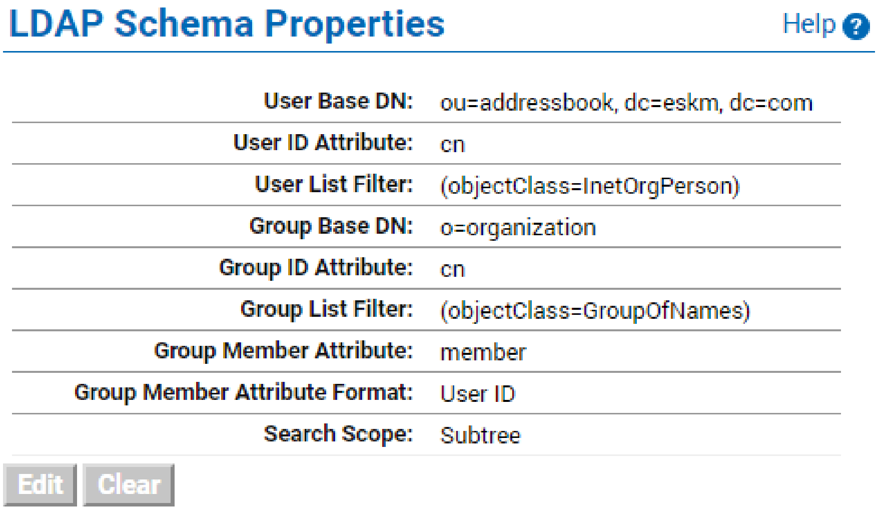
Component	***Description***
Server IP or Hostname	The IPv4/IPv6 address or hostname of the primary LDAP server[a].
Server Port	The port on which the LDAP server is listening. LDAP servers typically use port 389. For SSL connections, LDAP servers typically use port 636.
Use SSL	By default, the ESKM appliance connects directly to the LDAP server over TCP. Check this box to use SSL between the ESKM appliance and the LDAP server.
Minimum TLS Version	This field allows you to select minimum TLS version that will be negotiated. If the server does not support at least that version, the SSL handshake will fail. Available options are TLS 1.0, TLS 1.1 and TLS 1.2. This option is only valid if you are using SSL to communicate with the LDAP server.
Trusted CA List Profile	This field allows you to select a Trusted CA List profile. It is used to verify that server certificates presented by the LDAP server are signed by a CA trusted by the ESKM appliance. This option is only valid if you are using SSL to communicate with the LDAP server.
Timeout (sec)	The number of seconds to wait for the LDAP server during connections and searches before timing out. If the connection times out, the authorization fails.
Bind DN	The distinguished name (DN) to be used to bind to the server. The ESKM appliance will use these credentials to bind with the LDAP server when performing searches for users and groups. If your LDAP server supports anonymous searches, you may leave this field and the Bind Password field empty.

Component	***Description***
Bind Password	The password to be used to bind to the LDAP server.
Edit	Click **Edit** to modify the properties.
Clear	Click **Clear** to remove the current properties.
LDAP Test	Click **LDAP Test** to test the LDAP connection after you have defined an LDAP server.

[a]For SSL connections the LDAP server **hostname** should match the **common name** of the **LDAP server certificate**. When the hostname is specified in **LDAP configuration**, the DNS server IP needs to be added in **Device > Device Configuration > Hostname & DNS >DNS Server List** to resolve the hostname.

6.8.5.2 LDAP schema properties

LDAP Schema Properties describe the schema for your LDAP user directory.



LDAP Schema Properties

User Base DN:	ou=addressbook, dc=eskm, dc=com
User ID Attribute:	cn
User List Filter:	(objectClass=InetOrgPerson)
Group Base DN:	o=organization
Group ID Attribute:	cn
Group List Filter:	(objectClass=GroupOfNames)
Group Member Attribute:	member
Group Member Attribute Format:	User ID
Search Scope:	Subtree

Figure 121 : LDAP Schema Properties

The following table describes the components of **LDAP Schema Properties**.

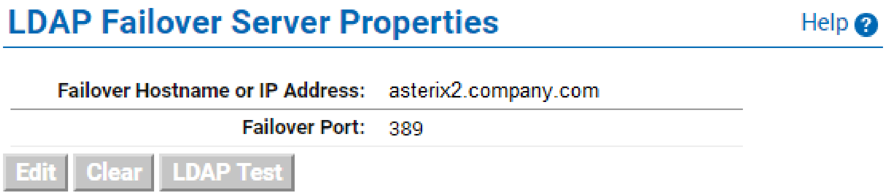
Table 70: LDAP Schema Properties components

Component	***Description***
User Base DN	The base distinguished name (DN) from which to begin the search for usernames.
User ID Attribute	The attribute type for the user. The attribute type you choose must result in globally unique users.
User List Filter	The search filter for users, for example: `(& (objectClass=user) (objectCategory=person))` To specify all, use `(objectClass=*)`
Group Base DN	The base DN from which to begin the search for groups.
Group ID Attribute	The attribute type for the group on which to search.
Group List Filter	The search filter for groups, for example: (objectClass=group)
Group Member Attribute	The Group Member Attribute is the attribute used to search for a user within a group, for example, member. The format of the Group Member attribute may be a user ID or a DN, and is determined by the Group Member Attribute Format.
Group Member Attribute Format	The Group Member attribute can take one of two formats: ▪ User ID ▪ User DN

Component	***Description***
Search Scope	The Search Scope determines how deep within the LDAP user directory the ESKM appliance searches for a user or group. ▪ One Level: search only the children of the base node. ▪ Subtree: search all the descendants of the base node. Depending on the size of your LDAP directory, this can be very inefficient. ⚠ The LDAP protocol supports four search scopes: base, one level, subtree and children. The ESKM appliance allows you to specify only one level and subtree. Subtree includes base and children, so by specifying subtree, the search scope includes subtree, base, and children.
Edit	Click **Edit** to modify the properties.
Clear	Click **Clear** to remove the current properties.

6.8.5.3 LDAP failover server properties

Use the **LDAP Failover Server Properties** to define a backup LDAP server to use in case the main LDAP server becomes inaccessible due to a non-timeout error. When the primary LDAP server is down, the ESKM appliance shifts to the failover LDAP server and periodically retries the primary LDAP server to see if it has become accessible again.



Failover Hostname or IP Address: asterix2.company.com

Failover Port: 389

Figure 122 : LDAP Failover Server Properties

The following table describes the components of the **LDAP Failover Server Properties**.

Table 71: LDAP Failover Server Properties components

Component	***Description***
Failover Server IP or Hostname	The IPv4/IPv6 address or hostname of the LDAP server to use as the failover.
Failover Server Port	The port on which the LDAP server is listening.
Edit	Click **Edit** to modify the properties.
Clear	Click **Clear** to remove the current properties.
LDAP Test	Click **LDAP Test** to test the LDAP connection after you have defined an LDAP server.

ⓘ The CLI commands ldap test administrators primary (p. 597) and ldap server administrators failover (p. 593) are basically equivalent to the **LDAP Test** buttons in the Management Console. However, they display connection information as well, and thus can be more helpful in debugging connection problems.

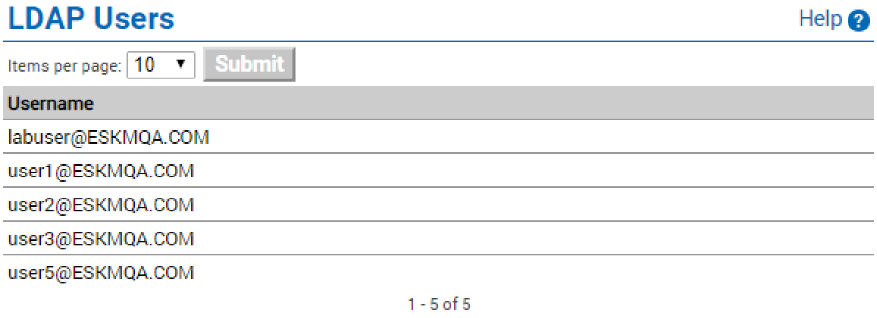
6.8.6 LDAP user and group configuration

The LDAP Users & Groups Configuration page (**Security > Users & Groups > LDAP > LDAP Users & Groups**) allows you to view the users and groups for the ESKM appliance as defined by the LDAP directory. You can only view the users and groups on this page; users and groups are created, modified, and removed on the LDAP server itself. This page contains the following sections:

- LDAP users (p. 332)
- LDAP groups (p. 332)
- User list (p. 333)

6.8.6.1 LDAP users

LDAP Users displays the users available in the LDAP user directory.



Username
labuser@ESKMQA.COM
user1@ESKMQA.COM
user2@ESKMQA.COM
user3@ESKMQA.COM
user5@ESKMQA.COM

1 - 5 of 5

Figure 123 : LDAP Users

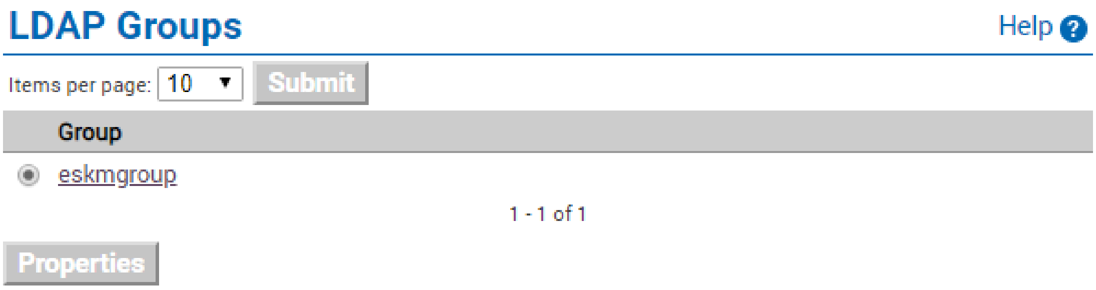
The following table describes the components of **LDAP Users**.

Table 72: LDAP Users components

Component	***Description***
Username	Displays the users who can access the ESKM appliance from the LDAP server.
Edit	Click **Edit** to edit a user.
Add	Click **Add** to add a user.
Delete	Click **Delete** to delete a user.
Properties	Click **Properties** to access the User List page and view the users within a specific group.

6.8.6.2 LDAP groups

LDAP Groups displays the groups available in the LDAP user directory.



Items per page: 10

Figure 124 : LDAP Groups

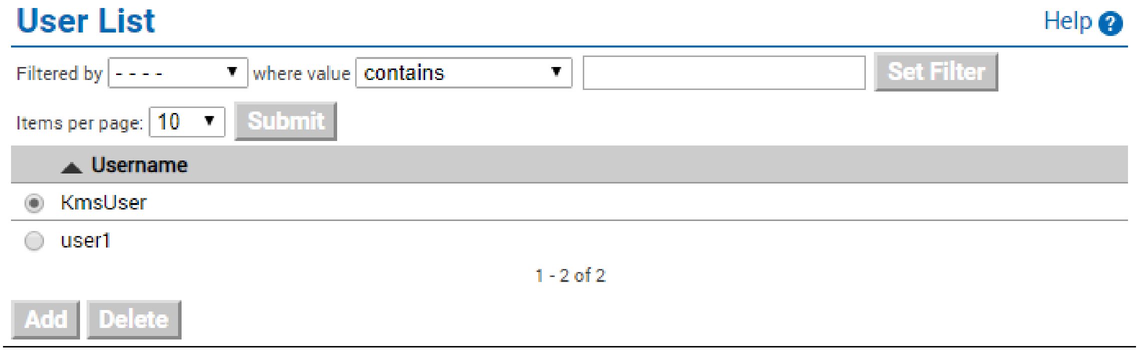
The following table describes the components of **LDAP Groups**.

Table 73: LDAP Groups components

Component	***Description***
Group	Displays the groups that can access the ESKM appliance from the LDAP server. Click the group name to access the User List page and view the members of that group.
Add	Click **Add** to add a group.
Delete	Click **Delete** to delete a group.
Properties	Click **Properties** to access the User List page and view the users within a specific group.

6.8.6.3 User list

The **User List** displays the members of a specific group.



● KmsUser

○ user1

Figure 125 : User List

The following table describes the components of the **User List**.

Table 74: LDAP User List components

Component	***Description***
Username	Displays the users who can access the ESKM appliance from the LDAP.
Add	Click **Add** to add a user.
Delete	Click **Delete** to delete a user.

6.9 Certificate and CA configuration

The ESKM appliance allows you to manage a trusted CA list, manage local CAs, sign certificate requests, create local CAs, and install CAs.

This section discusses the following Certificate and CA configuration topics:

- Certificates (p. 335)
- Trusted CA lists (p. 349)
- Local CAs (p. 353)
- Known CAs (p. 364)

6.9.1 Certificates

Certificates identify one entity to another. In this case, when making SSL/TLS connections between a client application and the ESKM appliance, the ESKM appliance must provide its server certificate to the client application. Likewise, if you require client applications to validate themselves to the ESKM appliance via client certificates, then the client application must provide its client certificate to the ESKM appliance during the SSL/TLS handshake.

The ESKM appliance uses the following two kinds of certificates:

- Server certificates on the ESKM appliance allow it to authenticate itself to a client application during an SSL/TLS handshake.
- Client certificates allow client applications to authenticate themselves to the ESKM appliance during an SSL/TLS handshake. Where the certificate resides varies from application to application.

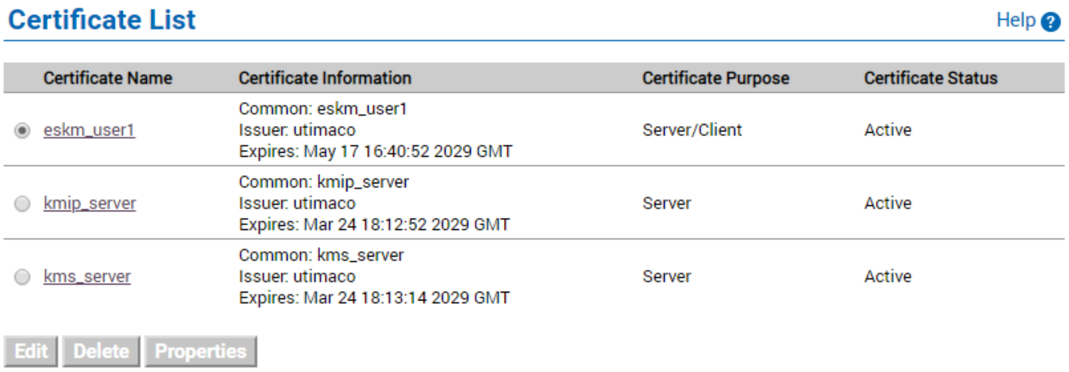
For more information on creating a local CA, see Create local CA (p. 361).

The Certificate and CA Configuration page (**Security > Certificates & CAs > Certificates**) allows you to view existing certificates and certificate requests, create certificates, create certificate requests, and import certificates. This section discusses the following topics:

- Certificate list (p. 335)
- Certificate information (p. 337)
- Certificate installation (p. 340)
- Self-signed certificate (p. 342)
- Create certificate (p. 344)
- Importing a certificate (p. 347)

6.9.1.1 Certificate list

The Certificate List displays the list of certificates and certificate requests on the ESKM appliance. Use the **Certificate List** to view all certificates on the appliance.



Certificate List

	Certificate Name	Certificate Information	Certificate Purpose	Certificate Status
●	eskm_user1	Common: eskm_user1 Issuer: utimaco Expires: May 17 16:40:52 2029 GMT	Server/Client	Active
○	kmip_server	Common: kmip_server Issuer: utimaco Expires: Mar 24 18:12:52 2029 GMT	Server	Active
○	kms_server	Common: kms_server Issuer: utimaco Expires: Mar 24 18:13:14 2029 GMT	Server	Active

Figure 126 : Certificate List

The following table describes the components of the **Certificate List**.

Table 75: Certificate List components

Component	***Description***
Certificate Name	The name of the certificate; this name is used internally by the ESKM appliance. Click the certificate name to view properties and access the certificate information.
Certificate Information	A certificate summary containing the following information: ▪ **Common Name**: Name of entity to which the certificate is issued. This is typically the name of the application. ▪ **Issuer Name**: Name of CA that issued the certificate. This information is not displayed for certificate requests. ▪ **Expiration Date**: The final date on which this certificate is valid. Following this date, the certificate can only be renewed by obtaining a new certificate from the CA. This information is not displayed for certificate requests.
Certificate Purpose	A certificate installed on the ESKM appliance can be a either a client certificate, a server certificate, or in the case of a dual-use certificate it can be both a server and client certificate.

Component	***Description***
Certificate Status	The certificate status is one of the following: ▪ **Request Pending** — Certificate request has been generated but has not yet been signed by the local CA. ▪ **Certificate Active** — Certificate is ready to be used. ▪ **Certificate Expires in [x] days** — Expires in x days. This state appears when a certificate expires in less than 30 days. ▪ **Certificate Expired** — Certificate expiration date is earlier than current date. ▪ **Certificate Not Yet Active** — Certificate activation date is after the current date. ▪ **Invalid Certificate** — Certificate is improperly signed by CA. ▪ **Error in Certificate** — Malformed certificate.
Edit	Click **Edit** to modify the CA name.
Delete	Click **Delete** to remove the specified certificate.
Properties	Click **Properties** to access the Certificate Information and view information about download, and install certificates.

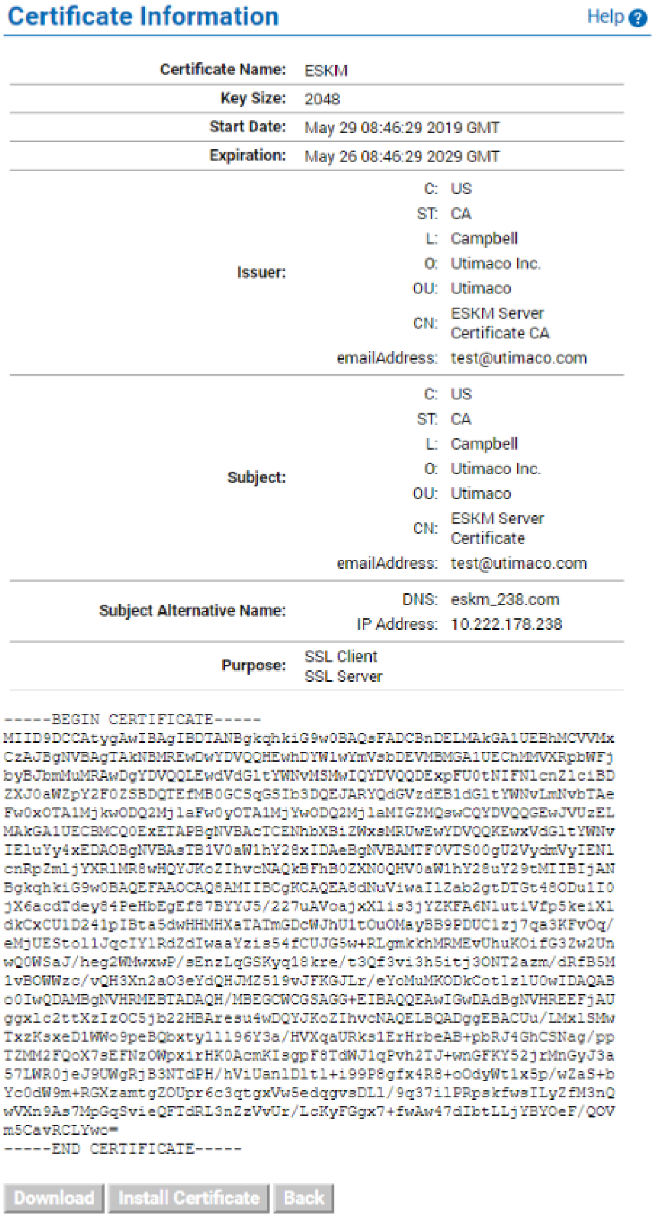
6.9.1.2 Certificate information

Use the **Certificate Information** to view information about, download, and install certificates. The top portion of the **Certificate Information** page contains the configured elements of the certificate. The lower portion of this page contains the PEM-encoded X.509 certificate data.

When you are viewing the properties of a certificate request, the **Certificate Information** page presents only the Certificate Name, Key Size, and Subject fields above the X.509 certificate request data. An active certificate presents Certificate Name, Key Size, Start Date, Expiration, Issuer, Subject above the X.509 certificate data.

Additionally, you have the option to create a self-signed certificate.

If you are copying the certificate text into an application such as Microsoft Word, it is important to ensure that no carriage returns/line feeds are lost. Such a loss would corrupt the certificate and prevent you from getting the certificate signed by a CA.



Certificate Information

Certificate Name:	ESKM
Key Size:	2048
Start Date:	May 29 08:46:29 2019 GMT
Expiration:	May 26 08:46:29 2029 GMT
Issuer:	C: US ST: CA L: Campbell O: Utimaco Inc. OU: Utimaco CN: ESKM Server Certificate CA emailAddress: test@utimaco.com
Subject:	C: US ST: CA L: Campbell O: Utimaco Inc. OU: Utimaco CN: ESKM Server Certificate emailAddress: test@utimaco.com
Subject Alternative Name:	DNS: eskm_238.com IP Address: 10.222.178.238
Purpose:	SSL Client SSL Server

```
-----BEGIN CERTIFICATE-----
MIID9DCCAtygAwIBAgIBDTANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMVXRpbWFj
byBJbmMuMRAwDgYDVQQLEwdVdGltYWNvMSMwIQYDVQQDExpFU0tNIFNlcnZlciBD
ZXJ0aWZpY2F0ZSBDQTEfMB0GCSqGSIb3DQEJARYQdGVzdEB1dGltYWNvLmNvbTAe
Fw0xOTA1MjkwODQ2MjlaFw0yOTA1MjYwODQ2MjlaMIGZMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCQ0ExETAPBgNVBAcTCENhbXBiZWxsMRUwEwYDVQQKEwxVdGltYWNv
IEluYy4xEDAOBgNVBAsTB1V0aW1hY28xIDAeBgNVBAMTF0VTS00gU2VydmVyIENl
cnRpZmljYXRlMR8wHQYJKoZIhvcNAQkBFhB0ZXN0QHV0aW1hY28uY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8dNuViwaIlZab2gtDTGt48ODu1I0
jX6acdTdey84PeHbEgEf87BYYJ5/227uAVoajxXlis3jYZKFA6NlutiVfp5keiXl
dkCxCU1D241pIBta5dwHHMHXaTAImGDcWJhU1tOuOMayBB9PDUC1zj7qa3KFvOq/
eMjUEStol1JqcIY1RdZdIwaaYzis54fCUJG5w+RLgmkkhMRMEvUhuKOifG3Zw2Un
wQ0WSaJ/heg2WMwxwP/sEnzLqGSKyq18kre/t3Qf3vi3h5itj3ONT2azm/dRfB5M
1vBOWWzc/vQH3Xn2aO3eYdQHJMZ519vJFKGJLr/eYoMuMKODkCotlz1U0wIDAQAB
o0IwQDAMBgNVHRMEBTADAQH/MBEGCWCGSAGG+EIBAQQEAwIGwDAdBgNVHREEFjAU
ggxlc2ttXzIzOC5jb22HBAresu4wDQYJKoZIhvcNAQELBQADggEBACUu/LMx1SMw
TxzKsxeD1WWo9peBQbxty11196Y3a/HVXqaURks1ErHrbeAB+pbRJ4GhCSNag/pp
TZMM2FQoX7sEFNzOWpxirHK0AcmKIsgpF8TdWJ1qPvh2TJ+wnGFKY52jrMnGyJ3a
57LWR0jeJ9UWgRjB3NTdPH/hViUanlDltl+i99P8gfx4R8+oOdyWt1x5p/wZaS+b
Yc0dW9m+RGXzamtgZOUpr6c3qtgxVw5edqgvsDLl/9q37ilPRpskfwsILyZfM3nQ
wVXn9As7MpGqSvieQFTdRL3nZzVvUr/LcKyFGgx7+fwAw47dIbtLLjYBYOeF/QOV
m5CavRCLYwo=
-----END CERTIFICATE-----
```

Figure 127 : Certificate Information

The following table describes the components of **Certificate Information**.

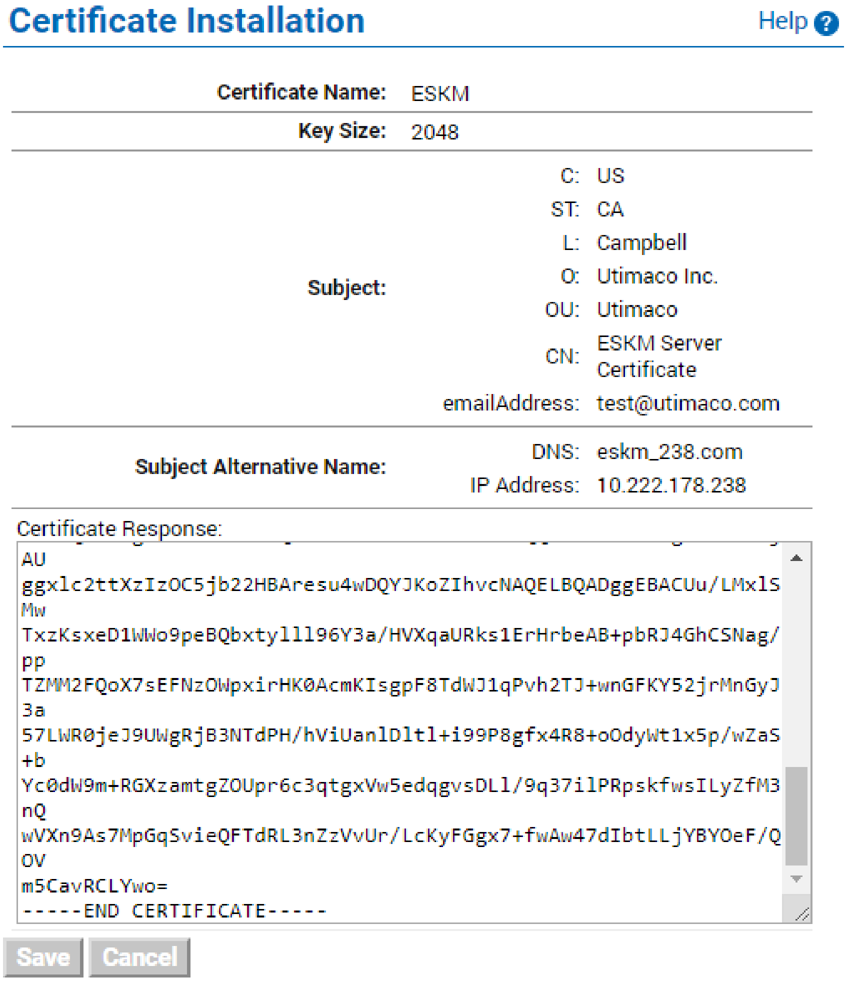
Table 76: Certificate Information components

Component	***Description***
Certificate Name	Name of the certificate. This name is only used internally by the ESKM appliance.
Key Size	Size of the key associated with this certificate.
Start Date	The activation date for the certificate. The certificate cannot be used before the activation date.
Expiration	The expiration date for the certificate. The certificate cannot be used after the expiration date.
Issuer	Full information about the CA who issued the certificate.
Subject	Full information about the entity to whom the certificate is issued.
Subject Alternative Name	Additional identities to whom the certificate is issued.
Purpose	A certificate installed on the ESKM appliance can be a client, server, or both client and server certificate.
Download	Click **Download** to download the certificate request data or the certificate data onto your web browser.

Component	***Description***
Install Certificate	Click **Install Certificate** to go to the Certificate Installation page. The **Install Certificate** button can be applied to either certificate requests or active certificates. ▪ When applied to a certificate request, the button is intended for transforming the certificate request into an active certificate. ▪ When applied to an existing certificate, the button is intended for reinstalling a certificate. Applying the Install Certificate button to a certificate should not be used under normal circumstances. ⚠ For more information on installing a certificate, see Certificate installation (p. 340).
Create Self Sign Certificate	Click **Create Self Sign Certificate** to create a self-signed certificate. The **Create Self Sign Certificate** button is only enabled for certificate requests. For more information on installing a certificate, see Certificate installation (p. 340).
Back	Click **Back** to return to the Certificate Configuration page.

6.9.1.3 Certificate installation

Use **Certificate Installation** to install a certificate for a certificate request that was generated on the ESKM appliance, or to reinstall a certificate for an active certificate. Supported certificate types include PEM-encoded PKCS #7, PEM-encoded PKCS #12, and PEM-encoded X.509.



Certificate Name:	ESKM
Key Size:	2048
Subject:	C: US ST: CA L: Campbell O: Utimaco Inc. OU: Utimaco CN: ESKM Server Certificate emailAddress: test@utimaco.com
Subject Alternative Name:	DNS: eskm_238.com IP Address: 10.222.178.238

Certificate Response:

```
AU
ggxlc2ttXzIzOC5jb22HBAresu4wDQYJKoZIhvcNAQELBQADggEBACUu/LMxlS
Mw
TxzKsxeD1WWo9peBQbxtyll196Y3a/HVXqaURks1ErHrbeAB+pbRJ4GhCSNag/
pp
TZMM2FQoX7sEFNzOWpxirHK0AcmKIsgpF8TdWJ1qPvh2TJ+wnGFKY52jrMnGyJ
3a
57LWR0jeJ9UWgRjB3NTdPH/hViUanlDltl+i99P8gfx4R8+oOdyWt1x5p/wZaS
+b
Yc0dW9m+RGXzamtgZOUpr6c3qtgxVw5edqgvsDLl/9q37ilPRpskfwsILyZfM3
nQ
wVXn9As7MpGqSvieQFTdRL3nZzVvUr/LcKyFGgx7+fwAw47dIbtLLjYBYOeF/Q
OV
m5CavRCLYwo=
-----END CERTIFICATE-----
```

Figure 128 : Certificate Installation

When multiple certificates are nested in one certificate, the certificate is installed as a certificate chain.

The following table describes the components of **Certificate Installation**.

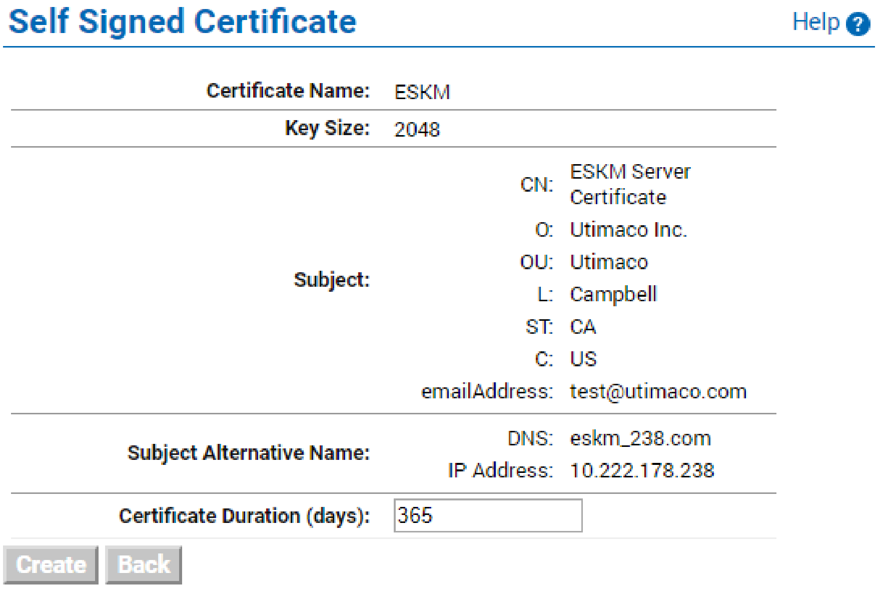
Table 77: Certificate Installation components

Component	***Description***
Certificate Name	Displays the name assigned to this certificate.
Key Size	Displays the key size associated with this certificate.

Component	***Description***
Subject	Displays the identity to which the certificate is issued using the following parameters: ▪ CN = Common Name ▪ O = Organization ▪ OU = Organizational unit ▪ L = Locality ▪ ST = State ▪ C = Country
Subject Alternative Name	Displays the identities to which the certificate is issued.
Certificate Response	The certificate response from the Certificate Authority.
Save	Click **Save** to save the certificate.
Cancel	Click **Cancel** to abort the process and return to the **Certificate Information**.

6.9.1.4 Self-signed certificate

Use the **Self Signed Certificate** to sign certificates created on the ESKM appliance.



Certificate Name:	ESKM
Key Size:	2048
Subject:	CN: ESKM Server Certificate O: Utimaco Inc. OU: Utimaco L: Campbell ST: CA C: US emailAddress: test@utimaco.com
Subject Alternative Name:	DNS: eskm_238.com IP Address: 10.222.178.238
Certificate Duration (days):	365

Figure 129 : Self Signed Certificate

The following table describes the components of the **Self Signed Certificate**.

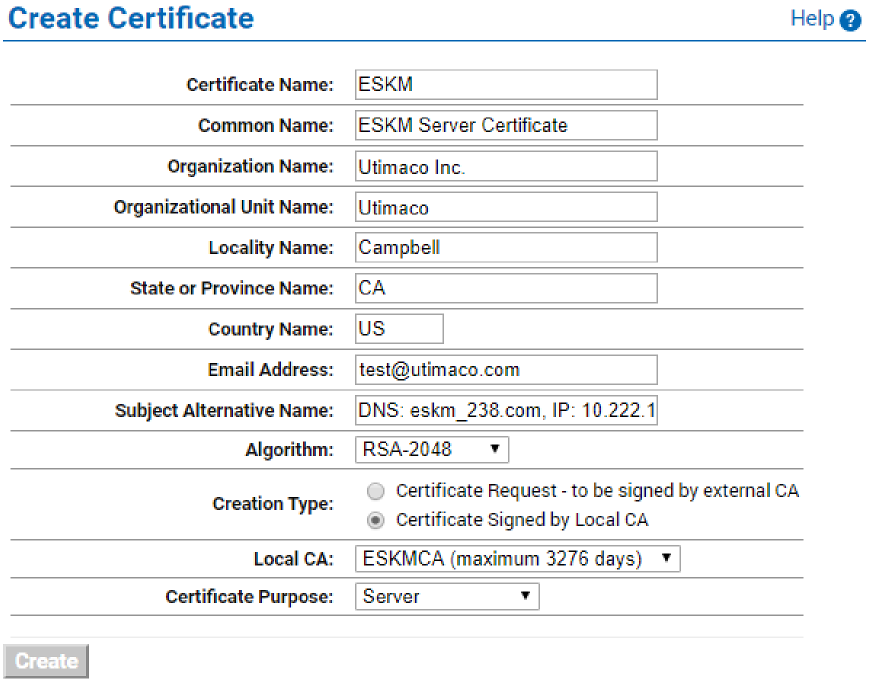
Table 78: Self Signed Certificate components

Component	***Description***
Certificate Name	The name of the certificate; this name is used internally by the ESKM appliance.
Key Size	The size of the key that will be generated.
Subject	Displays the values that will be used to create the certificate.
Subject Alternative Name	Displays the identities that will be used to create the certificate.
Certificate Duration (days)	The duration during which the certificate is valid.
Create	Click **Create** to create the certificate.

Component	***Description***
Back	Click **Back** to return to **Certificate Request Information**.

6.9.1.5 Create certificate

Create Certificate is used to create certificates that are signed by a local CA, and certificate requests that can be signed by a local or an external CA. Once created, the requests and certificates appear in the Certificate List. The certificate request is displayed in PEM-encoded PKCS #10 format.



Certificate Name:	ESKM
Common Name:	ESKM Server Certificate
Organization Name:	Utimaco Inc.
Organizational Unit Name:	Utimaco
Locality Name:	Campbell
State or Province Name:	CA
Country Name:	US
Email Address:	test@utimaco.com
Subject Alternative Name:	DNS: eskm_238.com, IP: 10.222.1
Algorithm:	RSA-2048 ▾
Creation Type:	○ Certificate Request - to be signed by external CA ● Certificate Signed by Local CA
Local CA:	ESKMCA (maximum 3276 days) ▾
Certificate Purpose:	Server ▾

Figure 130 : Create Certificate

The following table describes the components of **Create Certificate**.

Table 79: Create Certificate components

Component	***Description***
Certificate Name	Name of the certificate request. This name will be used when referring to this certificate request in other parts of the ESKM administrative interface. This field is required.

Component	***Description***
Common Name	Name of the application using this certificate. This field is required.
Organization Name	Name of the organization that owns this certificate. This field is optional.
Organizational Unit Name	Name of the unit within the organization requesting the certificate. This field is optional.
Locality Name	Name of city to which the certificate is being issued. This field is optional.
State or Province Name	Name of state where request is issued. This field is optional.
Country Name	Two-character ISO 3166 code of country where request is issued. This field is optional.
Email Address	E-mail address of person requesting the certificate. This field is optional.
Subject Alternative Name	Identities to be bound to the subject of the certificate. This field is optional. The **Subject Alternative Name** extension allows various literal values to be used. These include email (an email address), DNS (a DNS domain name) and IP (an IP address). Multiple name forms and multiple instances of each name form may be included. These name forms should be separated by a comma (,). The IP address used in the IP options can be in IPv4 /IPv6 format. Examples: ▪ DNS: eskm238.utimaco.com ▪ IP: 192.168.2.238, IP: 2000::238 ▪ email: test@utimaco.com, IP: 192.168.2.238, DNS: eskm238.utimaco.com

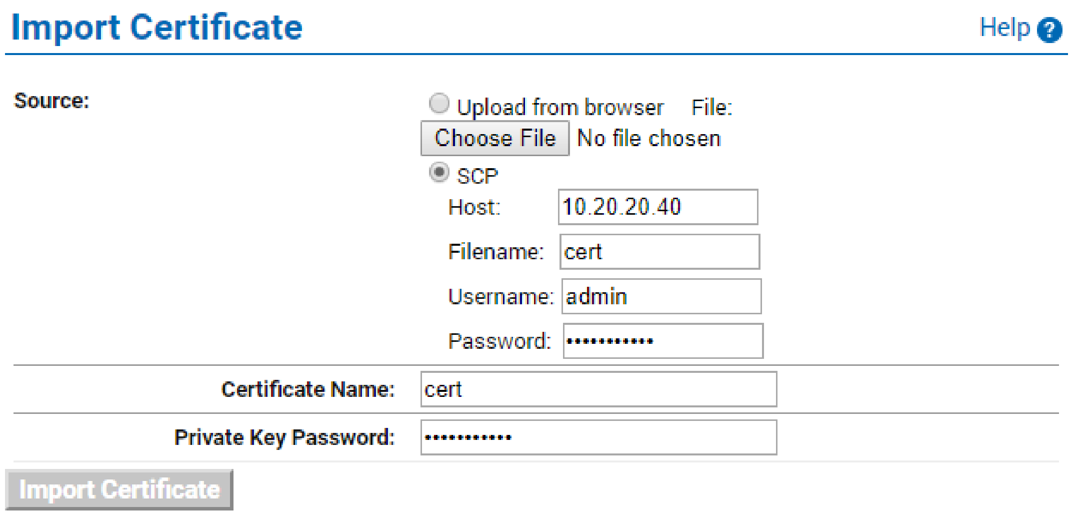
Component	***Description***
Algorithm	The **Algorithm** is used to create the certificate request. The ESKM appliance supports the following algorithms: ▪ RSA-768 ▪ RSA-1024 ▪ RSA-2048 ▪ RSA-3072 ▪ RSA-4096 ▪ ECDSA-P256 ▪ ECDSA-P384 ▪ ECDSA-P521 This field is required. ⚠ Some of the algorithms listed above will not be available when the ESKM is operating in FIPS mode.
Creation Type	Select the appropriate option based on whether you want to create a certificate (signed by a Local CA) or a certificate request (to be signed by local or external CA). ⚠ Please ensure that, at least one active Local CA is present before proceeding with the option "Certificate Signed by Local CA".
Local CA	Select the CA who will sign the certificate request. ⚠ This component will be enabled only if **Creation Type** is "Certificate Signed by Local CA".

Component	*Description*
Certificate Purpose	Select the purpose of the certificate, depending on where it will be used. It can be used either on client or server or both. ⚠ This component will be enabled only if **Creation Type** is "Certificate Signed by Local CA".
Create	Click **Create** to create the certificate request or a certificate depending on the option selected in **Creation Type**. Once created, the request and the certificates appears in the Certificate List. Certificate requests will appear with a status of **Request Pending**.

6.9.1.6 Importing a certificate

The ESKM appliance can import certificates in PEM-encoded PKCS #7, PEMencoded PKCS #12, and PEM-encoded X.509, as long as the private key is included with the certificate.

> ⚠ You can either import an RSA or the EC certificates.



Source: ○ Upload from browser File: No file chosen

● SCP

Host: 10.20.20.40

Filename: cert

Username: admin

Password: ••••••••••

Certificate Name: cert

Private Key Password: ••••••••••

Figure 131 : Import Certificate

The following table describes the components of **Import Certificate**.

Table 80: Import Certificate components

Component	***Description***
Source	Specify the method for importing the certificate to the ESKM appliance. If you are uploading the certificate through the browser, select **Upload from browser**, click Browse, and then locate the file on the local drive or network. If you are using SCP to copy the file to the ESKM appliance, select the appropriate option and enter the following information: ▪ **Host**: the source host. ▪ **Filename**: the name of the file on the source host. ▪ **Username**: the username of the account on the source host. ▪ **Password**: the password for the user account on the source host. ⚠ The ESKM appliance can import a certificate from a remote host which has an IPv6 address, when IPv6 is enabled (see ipv6 enable (p. 693)) and SCP is used to transfer the certificate file.
Certificate Name	The name of the certificate; this name is used internally by the ESKM appliance.
Private Key Password	The password used to access the key.
Import Certificate	Click **Import Certificate** to import the certificate to the ESKM appliance.

6.9.1.7 Exporting a certificate with a private key

The client certificates created in the ESKM can be exported in PKCS#12 format, which can be used in client applications. Use the **Export Certificate** section to export a client certificate along with private key in PKCS#12 format.

⚠ Only “client certificate” can be exported.

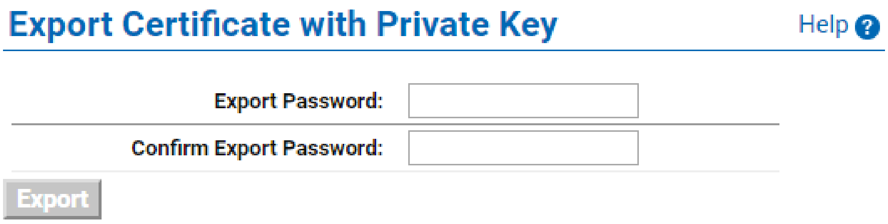


Figure 132 : Export Certificate with Private Key

The following table describes the components of **Export Certificate with Private Key**.

Table 81: Export Certificate with Private Key components

Component	***Description***
Export Password	Export Password for new PKCS12 file. ❗ The certificate cannot be imported anywhere else without this password.
Confirm Export Password	Confirm the password for the new PKCS12 file.
Export	Click **Export** to export the certificate and download to your local machine.

6.9.2 Trusted CA lists

The ESKM appliance is capable of functioning as a Certificate Authority (CA). Local CAs are managed on the Certificate Authority Configuration page (**Security > Certificates & CAs**) and are used to issue certificates to clients that might be making requests to the ESKM appliance. You can also use the Certificate and CA Configuration page to configure the list of

Certificate Authorities recognized by the
ESKM appliance.

The Certificate and CA Configuration page allows you to manage a trusted CA list, manage local CAs, sign certificate requests, create local CAs, and install CAs.

This section discusses the following topics:

- Trusted certificate authority list profiles (p. 350)
- Trusted certificate authority list (p. 351)

6.9.2.1 Trusted certificate authority list profiles

Trusted Certificate Authority List Profiles allow you to create lists of Trusted CAs that can be used to verify certificates for your client applications. When the Client Certificate Authentication option is enabled on the ESKM appliance, it verifies that the CA that signed the client certificate is in the list of Trusted CAs for the Trusted CA profile specified on the KMS Server Authentication Settings (**Device > Device Configuration > KMS Server**), KMIP Server Authentication Settings (**Device > Device Configuration > KMIP Server**), and Remote Administration Settings (**Device > Administrators > Remote Administration Settings**) pages.

The following figure shows **Trusted Certificate Authority List Profiles**.

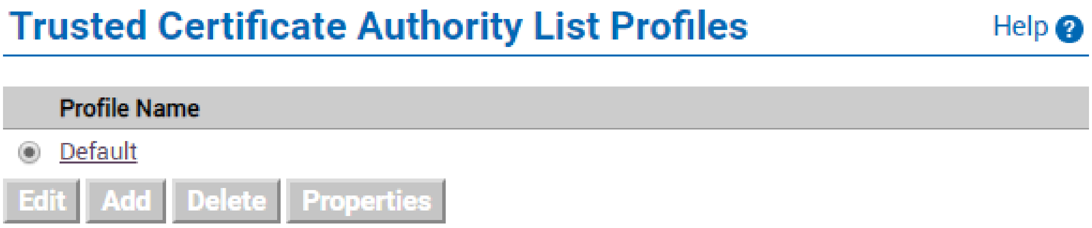


Figure 133 : Trusted Certificate Authority List Profiles

The following table describes the components of **Trusted Certificate Authority List Profiles**.

Table 82: Trusted Certificate Authority List Profiles components

Component	***Description***
Profile Name	Displays the profiles available on the ESKM appliance.
Edit	Click **Edit** to change the name of a profile. You cannot change the name of the Default profile.

Component	***Description***
Add	Click **Add** to create a profile. A newly created profile is initially empty. You must add CAs to the list of Trusted CAs for that profile.
Delete	Click **Delete** to remove a profile. You cannot delete the Default profile. You cannot delete a profile if it is specified on either the KMS Server Authentication Settings of the KMS Configuration page, the KMIP Settings of the KMIP Server Configuration page, or the Remote Administration Settings page.
Properties	Click **Properties** to access the Trusted CA List for the profile.

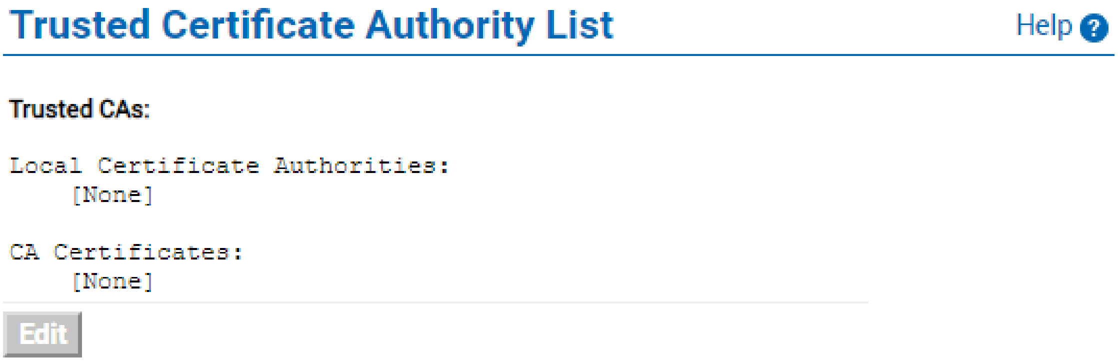
6.9.2.2 Default profile

The Default profile is empty by default. When you import a CA Certificate onto the ESKM appliance, it appears in the master list of CA Certificates, but it is not “trusted” until it is added to a Trusted CA list. The same is true for local CAs you generate on the ESKM appliance. You can change the list of Trusted CAs for the Default profile.

6.9.2.3 Trusted certificate authority list

Trusted Certificate Authority List allows you to view and modify the set of Trusted CAs for a profile. The Default profile contains no CAs; you must manually add CAs.

The following figure shows the **Trusted Certificate Authority List**.



Trusted Certificate Authority List

Trusted CAs:

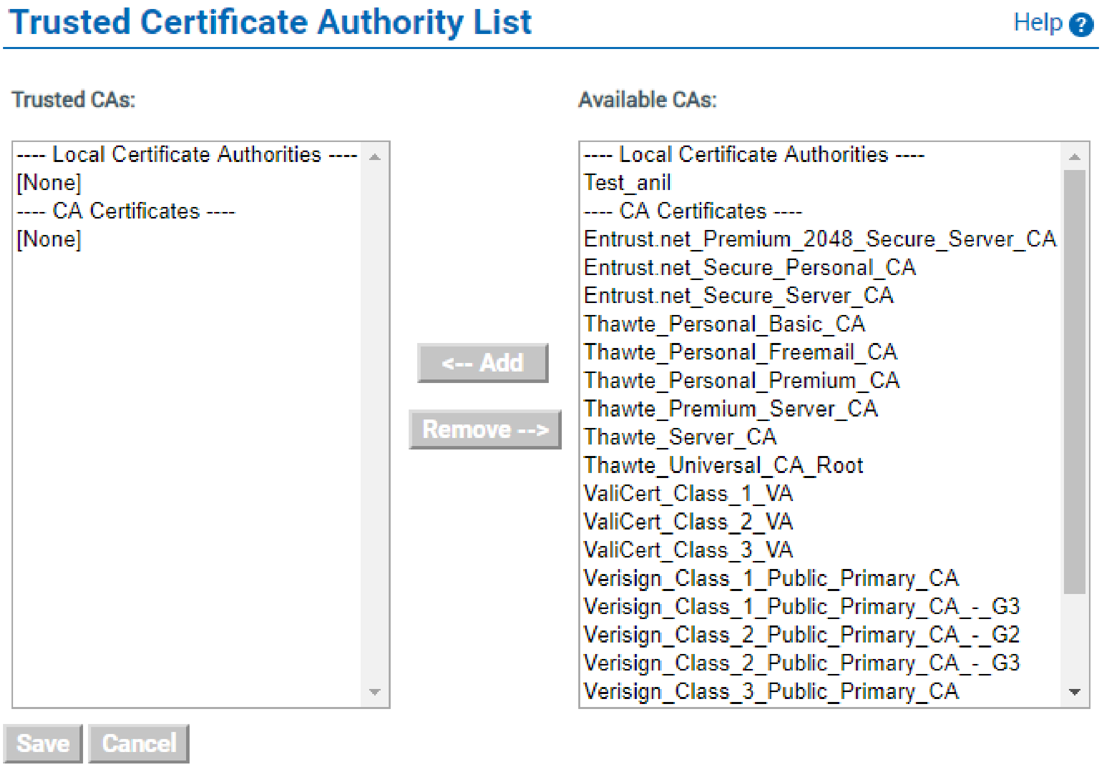
```
Local Certificate Authorities:
    [None]

CA Certificates:
    [None]
```

Figure 134 : Trusted Certificate Authority List

The following table describes the components of the **Trusted Certificate Authority List**.

Table 83: Trusted Certificate Authority List components

Component	***Description***
Trusted CAs	Displays the list of trusted CAs for this profile.
Edit	Click **Edit** to modify the list of Trusted CAs. This allows you to populate a trusted CA list.



Trusted CAs:

---- Local Certificate Authorities ----
[None]
---- CA Certificates ----
[None]

Available CAs:

---- Local Certificate Authorities ----
Test_anil
---- CA Certificates ----
Entrust.net_Premium_2048_Secure_Server_CA
Entrust.net_Secure_Personal_CA
Entrust.net_Secure_Server_CA
Thawte_Personal_Basic_CA
Thawte_Personal_Freemail_CA
Thawte_Personal_Premium_CA
Thawte_Premium_Server_CA
Thawte_Server_CA
Thawte_Universal_CA_Root
ValiCert_Class_1_VA
ValiCert_Class_2_VA
ValiCert_Class_3_VA
Verisign_Class_1_Public_Primary_CA
Verisign_Class_1_Public_Primary_CA_-_G3
Verisign_Class_2_Public_Primary_CA_-_G2
Verisign_Class_2_Public_Primary_CA_-_G3
Verisign_Class_3_Public_Primary_CA

Figure 135 : Trusted Certificate Authority List (Edit Mode)

The following table describes the components of the **Trusted Certificate Authority List**.

Table 84: Trusted Certificate Authority List (Edit Mode) Components

Component	***Description***
Trusted CAs	The Trusted CAs window displays the list of CAs that are trusted. You can remove a CA from the list of Trusted CAs by selecting it in the Trusted CAs window and clicking **Remove**. You can select multiple CAs by holding down the Shift key while selecting.
Available CAs	The Available CAs window displays CAs, both local and external, that can be added to the list of Trusted CAs. To add a CA, select it in the **Available CAs** window, and then click **Add**. You can select multiple CAs by holding down the Shift key while selecting.
Add / Remove	Click **Add** and **Remove** to add and remove available CAs to the list of trusted CAs.
Save	Click **Save** when you finish editing the list of Trusted CAs. Once your Trusted CA List has one or more CAs, it can be used by either the KMS or KMIP servers to verify client certificates, or the Web Administration server.
Cancel	Click Cancel to abort the changes made on this page.

6.9.3 Local CAs

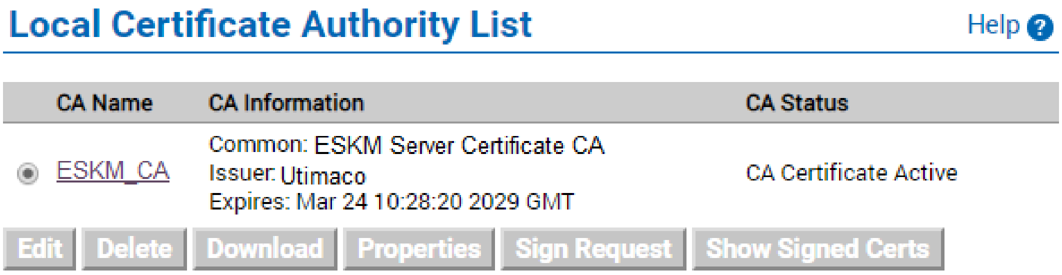
The **Certificate and CA Configuration** page allows you to manage a trusted CA list, manage local CAs, sign certificate requests, create local CAs, and install CAs. This section discusses the following topics:

- Local certificate authority list (p. 354)
- CA certificate properties (p. 355)
- Sign certificate request (p. 357)
- Signed certificates (p. 359)
- Signed certificate information (p. 360)

- Create local CA (p. 361)

6.9.3.1 Local certificate authority list

The **Certificate and CA Configuration** page contains a list of local Certificate Authorities managed on the ESKM appliance.



Local Certificate Authority List

	CA Name	CA Information	CA Status
●	ESKM_CA	Common: ESKM Server Certificate CA Issuer: Utimaco Expires: Mar 24 10:28:20 2029 GMT	CA Certificate Active

Figure 136 : Local Certificate Authority List

The following table describes the components of the **Local Certificate Authority List**.

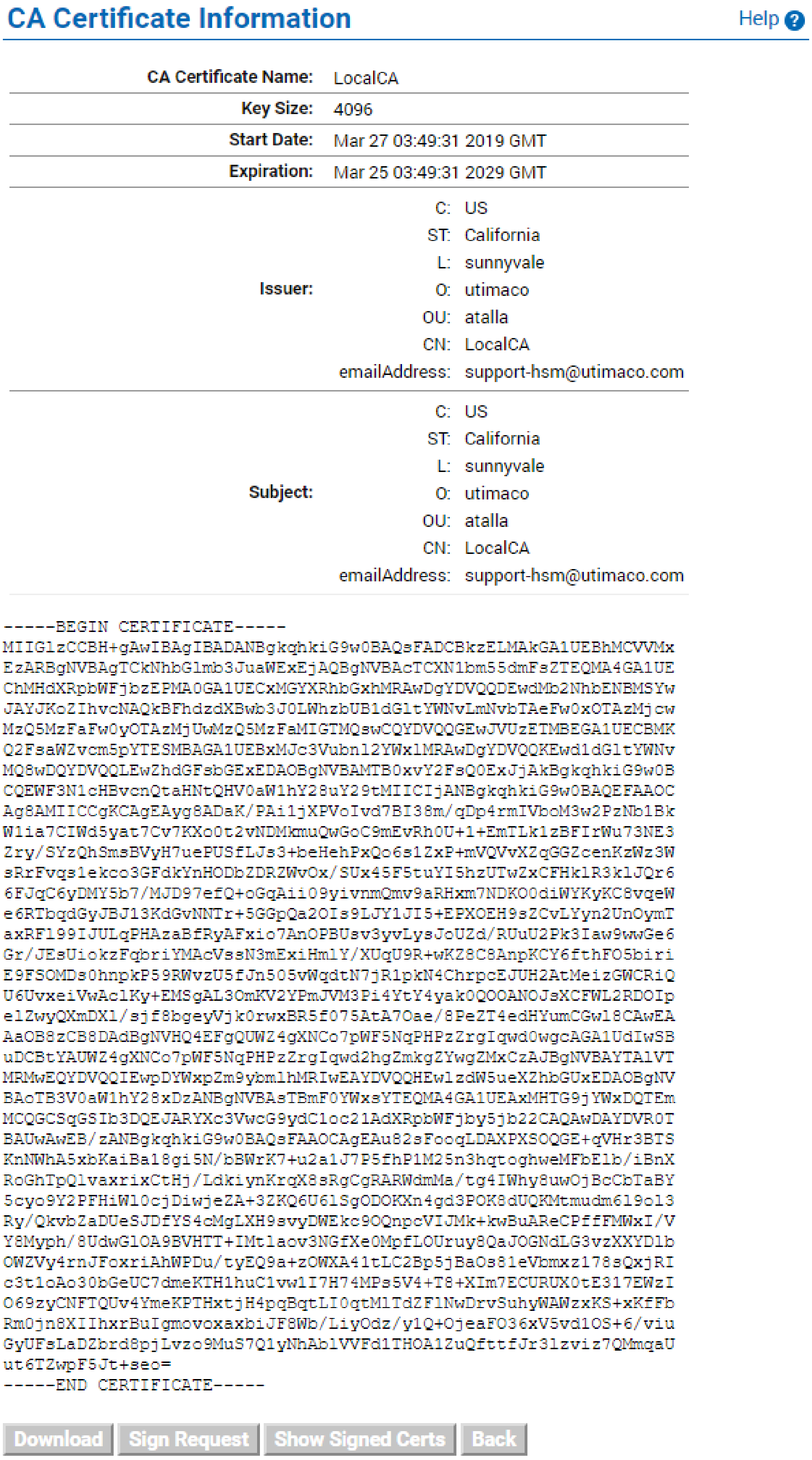
Table 85: Local Certificate Authority List components

Component	***Description***
CA Name	Displays the name of a certificate authority; this name is used internally by the ESKM appliance.
CA Information	Displays the common name, issuer, and expiration date of a CA.
CA Status	Displays the status of the CA.
Edit	Click **Edit** to edit the values of a CA.
Delete	Click **Delete** to remove a CA certificate from the list.

Component	***Description***
Download	Click **Download** to download the CA certificate onto your local machine. ⚠ Downloading a CA certificate could be very important when you are attempting to establish SSL/TLS connections between the ESKM appliance and client applications. To establish trust between the ESKM appliance and the client application, it might be necessary to install a CA certificate on the client application.
Properties	Click **Properties** to view the properties of a CA.
Sign Request	Click **Sign Request** to sign a certificate request.
Show Signed Certs	Click **Show Signed Certs** to show the certificates that have been signed by this CA.

6.9.3.2 CA certificate properties

Use **CA Certificate Information** to view information associated with a specific CA certificate. The top portion of the **CA Certificate Information** page displays several of the X.509 fields in the CA certificate. The lower portion of the page displays the X.509 certificate encoded in PEM format. Since this is a CA certificate, the issuer and subject are identical. You may wish to download a CA certificate so that you can add it to the trusted CA on a client device.



CA Certificate Name:	LocalCA
Key Size:	4096
Start Date:	Mar 27 03:49:31 2019 GMT
Expiration:	Mar 25 03:49:31 2029 GMT
Issuer:	C: US ST: California L: sunnyvale O: utimaco OU: atalla CN: LocalCA emailAddress: support-hsm@utimaco.com
Subject:	C: US ST: California L: sunnyvale O: utimaco OU: atalla CN: LocalCA emailAddress: support-hsm@utimaco.com

```
-----BEGIN CERTIFICATE-----
MIIGlzCCBH+gAwIBAgIBADANBgkqhkiG9w0BAQsFADCBkzELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExEjAQBgNVBAcTCXN1bm55dmFsZTEQMA4GA1UE
ChMHdXRpbWFjbzEPMA0GA1UECxMGYXRhbGxhMRAwDgYDVQQDEwdMb2NhbENBMSYw
JAYJKoZIhvcNAQkBFhdzdXBwb3J0LWhzbUB1dGltYWNvLmNvbTAeFw0xOTAzMjcw
MzQ5MzFaFw0yOTAzMjUwMzQ5MzFaMIGTMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
Q2FsaWZvcm5pYTESMBAGA1UEBxMJc3Vubnl2YWxlMRAwDgYDVQQKEwd1dGltYWNv
MQ8wDQYDVQQLEwZhdGFsbGExEDAOBgNVBAMTB0xvY2FsQ0ExJjAkBgkqhkiG9w0B
CQEWF3N1cHBvcnQtaHNtQHV0aW1hY28uY29tMIICIjANBgkqhkiG9w0BAQEFAAOC
Ag8AMIICCgKCAgEAyg8ADaK/PAi1jXPVoIvd7BI38m/qDp4rmIVboM3w2PzNb1Bk
W1ia7CIWd5yat7Cv7KXo0t2vNDMkmuQwGoC9mEvRh0U+1+EmTLk1zBFIrWu73NE3
Zry/SYzQhSmsBVyH7uePUSfLJs3+beHehPxQo6s1ZxP+mVQVvXZqGGZcenKzWz3W
sRrFvqs1ekco3GFdkYnHODbZDRZWvOx/SUx45F5tuYI5hzUTwZxCFHk1R3k1JQr6
6FJqC6yDMY5b7/MJD97efQ+oGqAii09yivnmQmv9aRHxm7NDKO0diWYKyKC8vqeW
e6RTbqdGyJBJ13KdGvNNTr+5GGpQa2OIs9LJY1JI5+EPXOEH9sZCvLYyn2UnOymT
axRF199IJULqPHAzaBfRyAFxio7AnOPBUsv3yvLysJoUZd/RUuU2Pk3Iaw9wwGe6
Gr/JEsUiokzFqbriYMAcVssN3mExiHmlY/XUqU9R+wKZ8C8AnpKCY6fthFO5biri
E9FSOMDs0hnpkP59RWvzU5fJn505vWqdtN7jR1pkN4ChrpcEJUH2AtMeizGWCRiQ
U6UvxeiVwAclKy+EMSgAL3OmKV2YPmJVM3Pi4YtY4yak0QOOANOJsXCFWL2RDOIp
elZwyQXmDXl/sjf8bgeyVjk0rwxBR5f075AtA7Oae/8PeZT4edHYumCGwl8CAwEA
AaOB8zCB8DAdBgNVHQ4EFgQUWZ4gXNCo7pWF5NqPHPzZrgIqwd0wgcAGA1UdIwSB
uDCBtYAUWZ4gXNCo7pWF5NqPHPzZrgIqwd2hgZmkgZYwgZMxCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQHEwlzdW5ueXZhbGUxEDAOBgNV
BAoTB3V0aW1hY28xDzANBgNVBAsTBmF0YWxsYTEQMA4GA1UEAxMHTG9jYWxDQTEm
MCQGCSqGSIb3DQEJARYXc3VwcG9ydC1oc21AdXRpbWFjby5jb22CAQAwDAYDVR0T
BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAu82sFooqLDAXPXSOQGE+qVHr3BTS
KnNWhA5xbKaiBa18gi5N/bBWrK7+u2a1J7P5fhP1M25n3hqtoghweMFbE1b/iBnX
RoGhTpQ1vaxrixCtHj/LdkiynKrqX8sRgCgRARWdmMa/tg4IWhy8uwOjBcCbTaBY
5cyo9Y2PFHiW10cjDiwjeZA+3ZKQ6U61SgODOKXn4gd3POK8dUQKMtmudm619o13
Ry/QkvbZaDUeSJDfYS4cMgLXH9svyDWEkc9OQnpcVIJMk+kwBuAReCPffFMWxI/V
Y8Myph/8UdwG1OA9BVHTT+IMtlaov3NGfXe0MpfLOUruy8QaJOGNdLG3vzXXYD1b
OWZVy4rnJFoxriAhWPDu/tyEQ9a+zOWXA41tLC2Bp5jBaOs81eVbmxz178sQxjRI
c3t1oAo30bGeUC7dmeKTH1huC1vw1I7H74MPs5V4+T8+XIm7ECURUX0tE317EWzI
O69zyCNFTQUv4YmeKPTHxtjH4pqBqtLI0qtM1TdZF1NwDrvSuhyWAWzxKS+xKfFb
Rm0jn8XIIhxrBuIgmovoxaxbiJF8Wb/LiyOdz/y1Q+OjeaFO36xV5vd1OS+6/viu
GyUFsLaDZbrd8pjLvzo9MuS7Q1yNhAblVVFd1THOA1ZuQfttfJr3lzviz7QMmqaU
ut6TZwpF5Jt+seo=
-----END CERTIFICATE-----
```

Figure 137 : CA Certificate Information

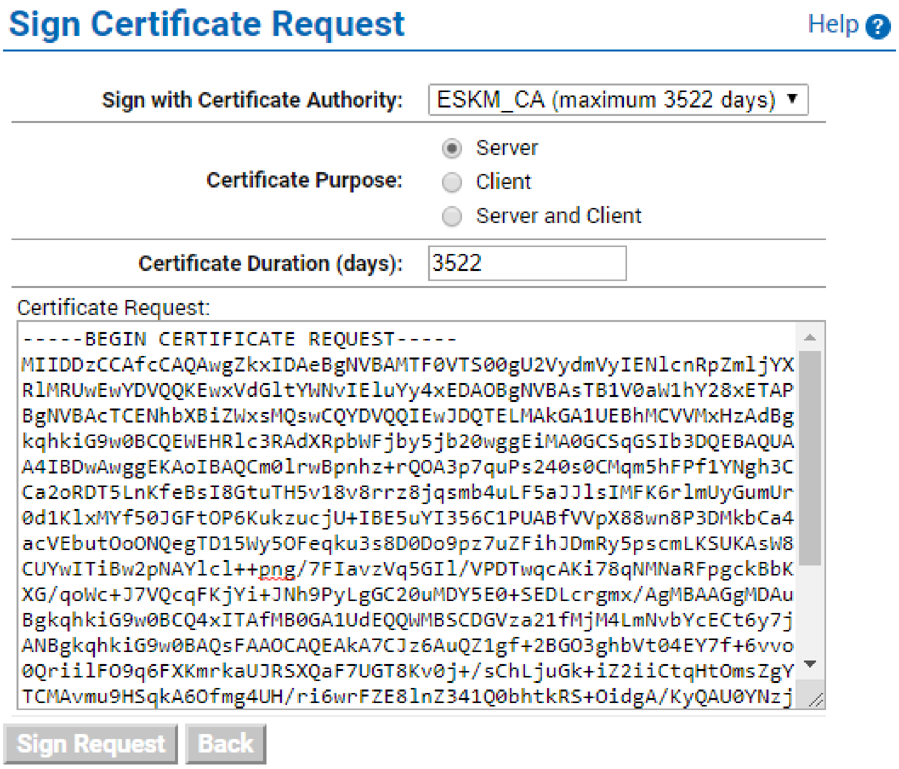
The following table describes the components of CA Certificate Information.

Table 86: CA Certificate Information components

Component	***Description***
Certificate Name	Name of the certificate; this name is used internally by the ESKM appliance.
Key Size	Size of the key associated with this certificate.
Start Date	The activation date for the certificate. The certificate cannot be used before the activation date.
Expiration	The expiration date for the certificate. The certificate cannot be used after the expiration date.
Issuer	Full information about the CA who issued the certificate.
Subject	Full information about the entity to whom the certificate is issued.
Download	Click **Download** to download the certificate request data or the certificate data onto your web browser.
Sign Request	Click **Sign Request** to sign a certificate request.
Show Signed Certs	Click **Show Signed Cert** to show the certificates that have been signed by this CA.
Back	Click **Back** to return to the Local CAs tab.

6.9.3.3 Sign certificate request

Use the **Sign Certificate Request** to sign certificate requests.



Sign with Certificate Authority: ESKM_CA (maximum 3522 days) ▼

Certificate Purpose: ● Server ○ Client ○ Server and Client

Certificate Duration (days): 3522

Certificate Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDzCCAfcCAQAwgZkxIDAeBgNVBAMTF0VTS00gU2VydmVyIENlcnRpZmljYX
RlMRUwEwYDVQQKEwxVdGltYWNvIEluYy4xEDAOBgNVBAsTB1V0aW1hY28xETAP
BgNVBAcTCENhbXBiZWxsMQswCQYDVQQIEwJDQTELMAkGA1UEBhMCVVMxHzAdBg
kqhkiG9w0BCQEWEHRlc3RAdXRpbWFjby5jb20wggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCm0lrwBpnhz+rQOA3p7quPs240s0CMqm5hFPf1YNgh3C
Ca2oRDT5LnKfeBsI8GtuTH5v18v8rrz8jqsmb4uLF5aJJlsIMFK6rlmUyGumUr
0d1KlxMYf50JGFtOP6KukzucjU+IBE5uYI356C1PUABfVVpX88wn8P3DMkbCa4
acVEbutOoONQegTD15Wy5OFeqku3s8D0Do9pz7uZFihJDmRy5pscmLKSUKAsW8
CUYwITiBw2pNAYlcl++png/7FIavzVq5GIl/VPDTwqcAKi78qNMNaRFpgckBbK
XG/qoWc+J7VQcqFKjYi+JNh9PyLgGC20uMDY5E0+SEDLcrgmx/AgMBAAGgMDAu
BgkqhkiG9w0BCQ4xITAfMB0GA1UdEQQWMBSCDGVza21fMjM4LmNvbYcECt6y7j
ANBgkqhkiG9w0BAQsFAAOCAQEAkA7CJz6AuQZ1gf+2BGO3ghbVt04EY7f+6vvo
0QriilFO9q6FXKmrkaUJRSXQaF7UGT8Kv0j+/sChLjuGk+iZ2iiCtqHtOmsZgY
TCMAvmu9HSqkA6Ofmg4UH/ri6wrFZE8lnZ341Q0bhtkRS+OidgA/KyQAU0YNzj
```

Figure 138 : Sign Certificate Request

The following table describes the components of the **Sign Certificate Request**.

Table 87: Sign Certificate Request components

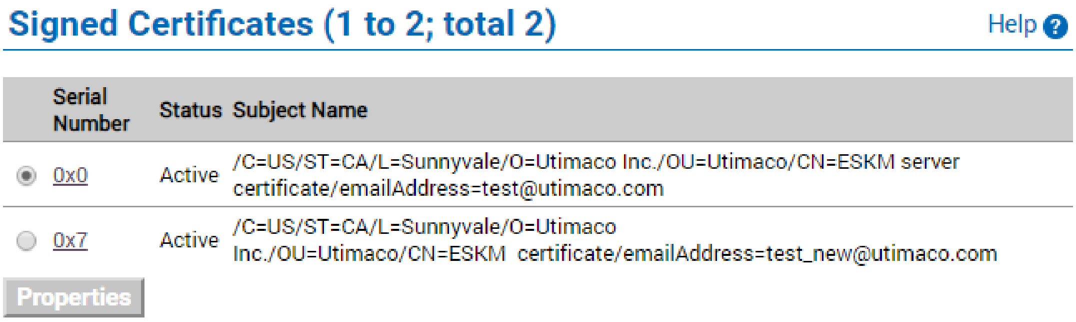
Component	***Description***
Sign with Certificate Authority	Select the CA that will sign the certificate request.
Certificate Purpose	Select where the certificate will be used, either on the client or the server, or in the case of a dual-use certificate select the third choice, Server and Client.
Certificate Duration (days)	Specify the period during which the certificate is valid. The default value for this field is 3649, this value may not be larger than the maximum duration allowed for the selected CA.
Certificate Request	The certificate request text to be signed.

Component	*Description*
Sign Request	Click **Sign Request** to sign the request.
Back	Click **Back** to return to the Local CAs tab.

6.9.3.4 Signed certificates

Use the **Show Signed Certs** button to display all certificates signed by a local CA. Displaying signed certificates helps you to track and maintain certificates on the ESKM appliance.

The following figure shows **Signed Certificates**.



Signed Certificates (1 to 2; total 2)

	Serial Number	Status	Subject Name
●	0x0	Active	/C=US/ST=CA/L=Sunnyvale/O=Utimaco Inc./OU=Utimaco/CN=ESKM server certificate/emailAddress=test@utimaco.com
○	0x7	Active	/C=US/ST=CA/L=Sunnyvale/O=Utimaco Inc./OU=Utimaco/CN=ESKM certificate/emailAddress=test_new@utimaco.com

Figure 139 : Signed Certificates

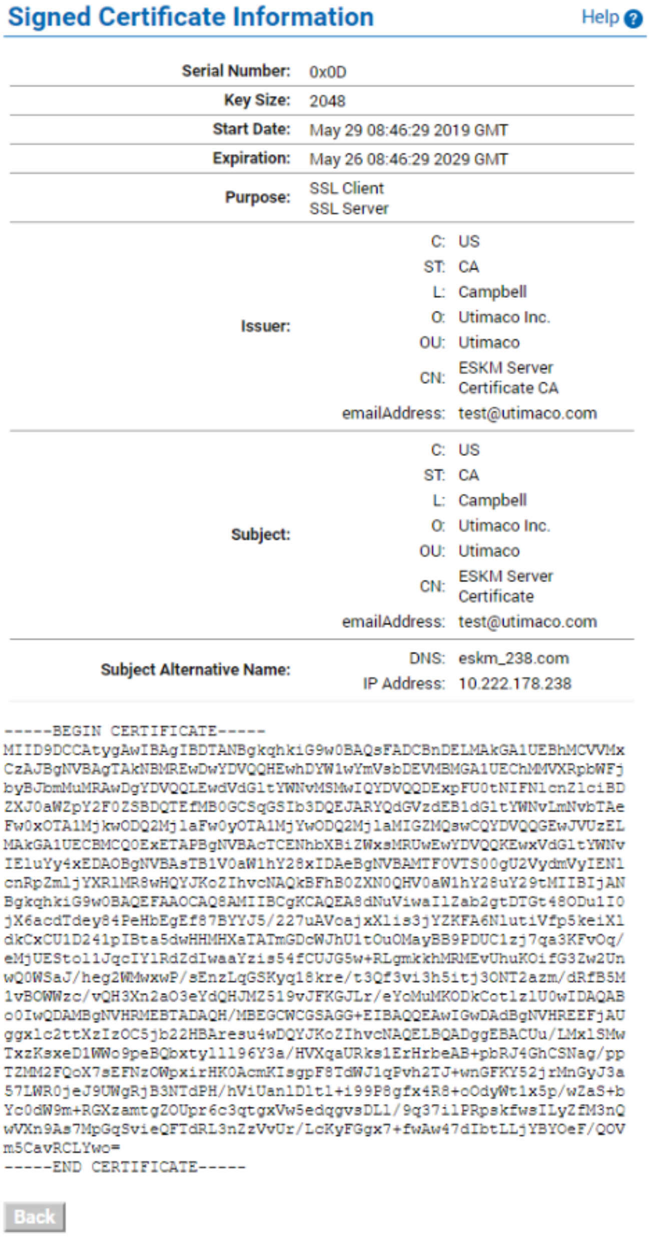
Table 88: Signed Certificates components

Component	*Description*
Serial Number	The Serial Number, which is expressed in Base 16 notation, is assigned by the ESKM appliance and used internally to refer to a certificate signed by a local CA. There is only one counter on the ESKM appliance, which means that all serial numbers for certificates signed by local CAs will be in numerical order regardless of which local CA signed the certificate. For example, a certificate signed by one local CA might get the serial number 0x7. The next certificate signed by a local CA on the ESKM appliance would get the serial number 0x8, regardless of which local CA signed it. The first certificate in the list of signed certificates is always the local CA itself, which always has a serial number of 0x0.

Component	***Description***
Status	Status of the certificate.
Subject Name	This field shows the concatenated subject information for the signed certificate.
Properties	Click **Properties** to access **Signed Certificate Information** and view the properties of the selected certificate.

6.9.3.5 Signed certificate information

You can view the information of a certificate by selecting the certificate and clicking **Properties**.
The information includes the serial number, key size, start date, expiration date, purpose, issuer, subject, and Subject Alternative Names(s). In addition, the PEM encoded X.509 certificate can be used to install the certificate if necessary.



Serial Number:	0x0D	
Key Size:	2048	
Start Date:	May 29 08:46:29 2019 GMT	
Expiration:	May 26 08:46:29 2029 GMT	
Purpose:	SSL Client SSL Server	
Issuer:	C:	US
	ST:	CA
	L:	Campbell
	O:	Utimaco Inc.
	OU:	Utimaco
	CN:	ESKM Server Certificate CA
	emailAddress:	test@utimaco.com
Subject:	C:	US
	ST:	CA
	L:	Campbell
	O:	Utimaco Inc.
	OU:	Utimaco
	CN:	ESKM Server Certificate
	emailAddress:	test@utimaco.com
Subject Alternative Name:	DNS:	eskm_238.com
	IP Address:	10.222.178.238

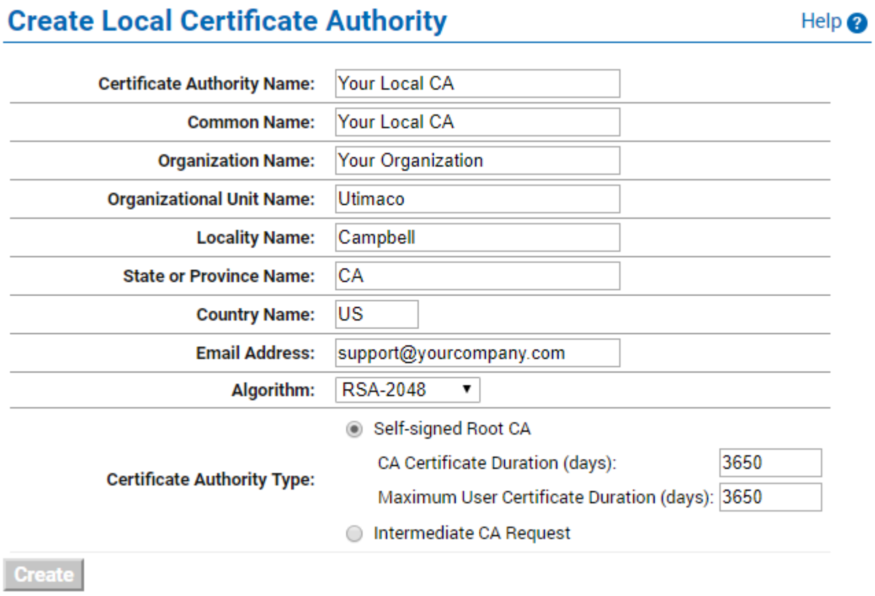
```
-----BEGIN CERTIFICATE-----
MIID9DCCAtygAwIBAgIBDTANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMVXRpbWFj
byBJbmMuMRAwDgYDVQQLEwdVdGltYWNvMSMwIQYDVQQDExpFU0tNIFNlcnZlciBD
ZXJ0aWZpY2F0ZSBDQTEfMB0GCSqGSIb3DQEJARYQdGVzdEB1dGltYWNvLmNvbTAe
Fw0xOTA1MjkwODQ2MjlaFw0yOTA1MjYwODQ2MjlaMIGZMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCQ0ExETAPBgNVBAcTCENhbXBiZWxsMRUwEwYDVQQKEwxVdGltYWNv
IEluYy4xEDAOBgNVBAsTB1V0aW1hY28xIDAeBgNVBAMTF0VTS00gU2VydmVyIENl
cnRpZmljYXRlMR8wHQYJKoZIhvcNAQkBFhB0ZXN0QHV0aW1hY28uY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8dNuViwaIlZab2gtDTGt48ODu1I0
jX6acdTdey84PeHbEgEf87BYYJ5/227uAVoajxXlis3jYZKFA6NlutiVfp5keiXl
dkCxCU1D241pIBta5dwHHMHXaTATmGDcWJhU1tOuOMayBB9PDUC1zj7qa3KFvOq/
eMjUEStol1JqcIY1RdZdIwaaYzis54fCUJG5w+RLgmkkhMRMEvUhuKOifG3Zw2Un
wQ0WSaJ/heg2WMwxwP/sEnzLqGSKyq18kre/t3Qf3vi3h5itj3ONT2azm/dRfB5M
1vBOWWzc/vQH3Xn2aO3eYdQHJMZ519vJFKGJLr/eYoMuMKODkCotlzlU0wIDAQAB
o0IwQDAMBgNVHRMEBTADAQH/MBEGCWCGSAGG+EIBAQQEAwIGwDAdBgNVHREEFjAU
ggxlc2ttXzIzOC5jb22HBAresu4wDQYJKoZIhvcNAQELBQADggEBACUu/LMxlSMw
TxzKsxeD1WWo9peBQbxtyl1l96Y3a/HVXqaURks1ErHrbeAB+pbRJ4GhCSNag/pp
TZMM2FQoX7sEFNzOWpxirHK0AcmKIsgpF8TdWJ1qPvh2TJ+wnGFKY52jrMnGyJ3a
57LWR0jeJ9UWgRjB3NTdPH/hViUanlDltl+i99P8gfx4R8+oOdyWt1x5p/wZaS+b
Yc0dW9m+RGXzamtgZOUpr6c3qtgxVw5edqgvsDLl/9q37ilPRpskfwsILyZfM3nQ
wVXn9As7MpGqSvieQFTdRL3nZzVvUr/LcKyFGgx7+fwAw47dIbtLLjYBYOeF/QOV
m5CavRCLYwo=
-----END CERTIFICATE-----
```

Figure 140 : Signed Certificate Information

The components of **Signed Certificate Information** are view-only.

6.9.3.6 Create local CA

Create Local CA allows you to create a new local CA on the ESKM appliance. The fields are similar to those used to create a certificate on the Certificates page. When creating a local CA, you must provide a value for each field, except the email address.



Create Local Certificate Authority

Certificate Authority Name:	Your Local CA
Common Name:	Your Local CA
Organization Name:	Your Organization
Organizational Unit Name:	Utimaco
Locality Name:	Campbell
State or Province Name:	CA
Country Name:	US
Email Address:	support@yourcompany.com
Algorithm:	RSA-2048 ▼
Certificate Authority Type:	● Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 ○ Intermediate CA Request

Figure 141 : Create Local Certificate Authority

The following table describes the components of the **Create Local Certificate Authority**.

Table 89: Create Local Certificate Authority components

Component	***Description***
Certificate Authority Name	The name of the newly generated certificate authority. This name will be used when referring to this CA in other parts of the ESKM administrative interface.
Common Name	Common name of the new CA.
Organization Name	Name of the organization that owns this CA.
Organizational Unit Name	Name of unit within the organization generating the CA.
Locality Name	Name of city where CA is created.
State or Province Name	Name of state where CA is created.

Component	***Description***
Country Name	Two-letter name of country where request is issued.
Email Address	E-mail address of person creating the CA.
Algorithm	Used to create the certificate request. The ESKM appliance supports the following algorithms: ▪ RSA-768 ▪ RSA-1024 ▪ RSA-2048 ▪ RSA-3072 ▪ RSA-4096 ▪ ECDSA-P256 ▪ ECDSA-P384 ▪ ECDSA-P521 This field is required. ⚠ Some of the algorithms listed above will not be available when the ESKM is operating in FIPS mode.

Component	***Description***
Certificate Authority Type	Local CAs can be one of two types: **Self-signed root CA**, or **Intermediate CA Request**. When you create a **self-signed root CA**, you must also specify a **CA Certificate Duration** and a **Maximum User Certificate Duration**, which become valid once you click Create. After you create a self-signed root CA, you must add it to the trusted CA list for it to be recognized by the ESKM appliance. When you create an **intermediate CA request**, you must sign it with either an existing intermediate CA or your organization's root CA. Certificates signed by the intermediate CA can be verified by that same intermediate CA, by the root itself, or by any intermediate CAs that link the signing CA with the root. This allows you to decentralize certificate signing and verification. When creating an intermediate CA request, you must also specify a **Maximum User Certificate Duration** when installing the certificate response. This duration cannot be longer than the signing CA's duration.
CA Certificate Duration	Period of time for which the local CA is valid. Specify a value in days. This value must be more than the **Maximum User Certificate Duration**.
Maximum User Certificate Duration	Period of time for which certificates signed by the local CA are valid. Specify a value in days. This value must be less than or equal to the **CA Certificate Duration**.
Create	Click **Create** to create the CA. Once created, the new CA appears as CA certificate active. A newly generated CA remains active for five years.

6.9.4 Known CAs

- CA certificate list (p. 365)

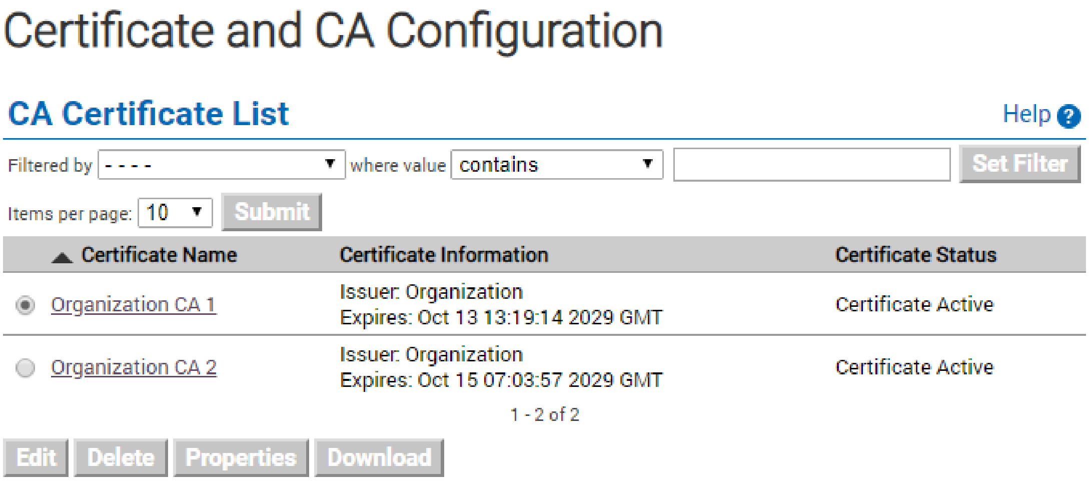
- Install CA certificate (p. 366)

6.9.4.1 CA certificate list

This portion of the Known CAs tab presents the list of CAs that are recognized by the ESKM appliance.

> ⚠ Known CAs which have expired, are removed periodically if they are not set as a trusted CA for KMS, KMIP, Web Admin or LDAP authentication. A warning is issued on installation of a well known CA expiring in 30 days.

The following figure shows the **CA Certificate List**.



Certificate and CA Configuration

CA Certificate List

	Certificate Name	Certificate Information	Certificate Status
●	Organization CA 1	Issuer: Organization Expires: Oct 13 13:19:14 2029 GMT	Certificate Active
○	Organization CA 2	Issuer: Organization Expires: Oct 15 07:03:57 2029 GMT	Certificate Active

1 - 2 of 2

Figure 142 : CA Certificate List

The following table describes the components of the **CA Certificate List**.

Table 90: CA Certificate List components

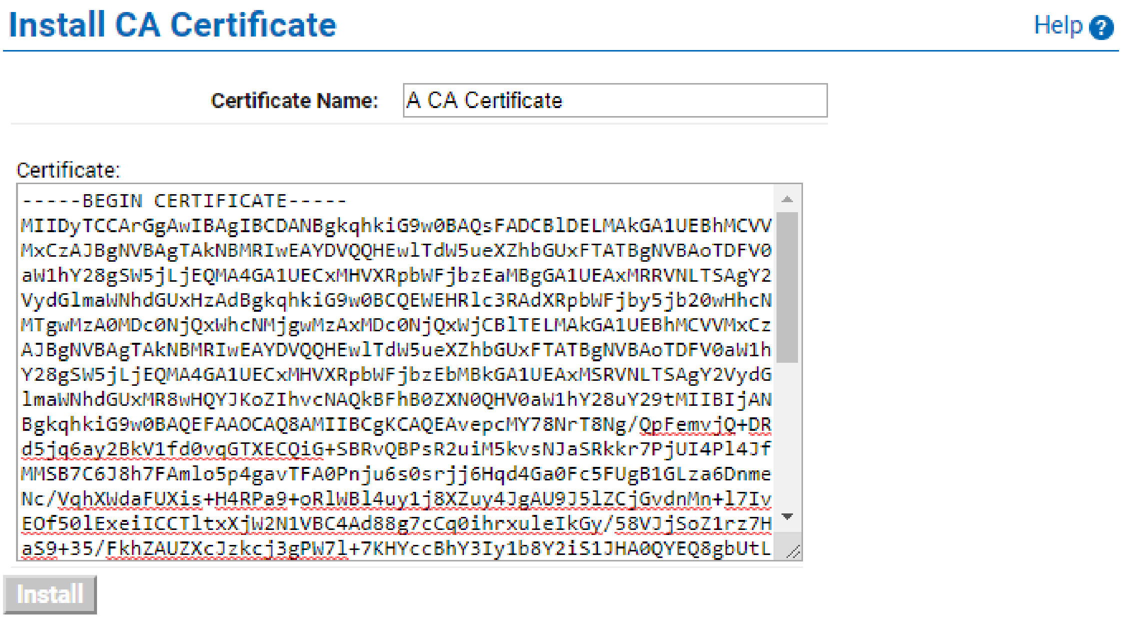
Component	***Description***
Certificate Name	Displays the certificate name. Click this link to view the CA certificate information.
Certificate Information	Displays the certificate issuer and expiration date.

Component	***Description***
Certificate Status	Displays one of three values: ▪ Certificate Active—The CA can be used to issue certificates and sign certificate requests. ▪ Certificate Expires: X Days—The CA certificate expires in X days. This status first appears 30 days before the certificate expires. ▪ Certificate Expired—The CA has expired. For an external CA, such as VeriSign, contact the CA to obtain a new certificate.
Edit	Click **Edit** to change the name of a CA certificate.
Delete	Click **Delete** to remove a CA certificate.
Properties	Click **Properties** to view additional information about a CA certificate.
Download	Click **Download** to download a CA certificate to your web browser.

6.9.4.2 Install CA certificate

Use **Install CA Certificate** of the Known CAs tab to add CA certificates to the CA Certificate List.

The following figure shows **Install CA Certificate**.



Certificate Name: A CA Certificate

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDyTCCArGgAwIBAgIBCDANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCVV
MxCzAJBgNVBAgTAkNBMRIwEAYDVQQHEwlTdW5ueXZhbGUxFTATBgNVBAoTDFV0
aW1hY28gSW5jLjEQMA4GA1UECxMHVXRpbWFjbzEaMBgGA1UEAxMRRVNLTSAgY2
VydGlmaWNhdGUxHzAdBgkqhkiG9w0BCQEWEHRlc3RAdXRpbWFjby5jb20wHhcN
MTgwMzA0MDc0NjQxWhcNMjgwMzAxMDc0NjQxWjCBlTELMAkGA1UEBhMCVVMxCz
AJBgNVBAgTAkNBMRIwEAYDVQQHEwlTdW5ueXZhbGUxFTATBgNVBAoTDFV0aW1h
Y28gSW5jLjEQMA4GA1UECxMHVXRpbWFjbzEbMBkGA1UEAxMSRVNLTSAgY2VydG
lmaWNhdGUxMR8wHQYJKoZIhvcNAQkBFhB0ZXN0QHV0aW1hY28uY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvepcMY78NrT8Ng/QpFemvjQ+DR
d5jq6ay2BkV1fd0vqGTXECQiG+SBRvQBPsR2uiM5kvsNJaSRkkr7PjUI4Pl4Jf
MMSB7C6J8h7FAmlo5p4gavTFA0Pnju6s0srjj6Hqd4Ga0Fc5FUgB1GLza6Dnme
Nc/VqhXWdaFUXis+H4RPa9+oRlWBl4uy1j8XZuy4JgAU9J5lZCjGvdnMn+l7Iv
EOf50lExeiICCTltxXjW2N1VBC4Ad88g7cCq0ihrxuleIkGy/58VJjSoZ1rz7H
aS9+35/FkhZAUZXcJzkcj3gPW7l+7KHYccBhY3Iy1b8Y2iS1JHA0QYEQ8gbUtL
```

Figure 143 : Install CA Certificate

The following table describes the components of **Install CA Certificate**.

Table 91: Install CA Certificate components

Component	*Description*
Certificate Name	Enter the certificate name.
Certificate	Paste the contents of the certificate into this field.
Install	Click **Install** to install the CA.

6.10 Support for certificate revocation list

Configuration of the ESKM appliance to work with a Certificate Revocation List (CRL) is done exclusively from the Command Line Interface, see CRL commands (p. 631).

6.11 Advanced security features

Advanced security features provide the highest level of secure operation on the ESKM appliance. This section discusses the following topics:

6.11.1 Advanced security overview

Use the Advanced Security settings on the ESKM appliance to set the highest level of security for administrative and cryptographic operations. Advanced security features are divided into these major sections: High security settings (p. 374), Security settings configured elsewhere (p. 377), SSL/TLS (p. 388), and FIPS status server (p. 381). Use the following table as a quick reference to determine which security features apply to the KMS and KMIP servers.

Table 92: Advanced security features

Advanced security feature	***KMS server***	***KMIP server***
High Security Settings		
Key Security	Yes	No
Device Security	Yes	No
Disable Certificate Import through Serial Console Paste	Yes	Yes
Security Settings Configured Elsewhere		

Advanced security feature	***KMS server***	***KMIP server***
Allow Key and Policy Configuration Operations	Yes	No
Allow Key Export	Yes	No
User Directory	Yes	Yes
LDAP Administrator Server Configured	Yes	Yes
Allowed SSL Protocol	Yes	No
Enabled SSL Cipher	Yes	No
SSL	Yes	Yes
FIPS Status Server	Yes	Yes

6.11.2 Advanced security access control

Altering the security settings on the High security configuration (p. 371) can have a profound effect on the security of your ESKM appliance and alter your compliance with FIPS standards. For this reason, administrators must have the Advanced Security Access Control permission to modify these settings.

The FIPS standards describe hardware and software parameters that must be met for full compliance. Utimaco provides both FIPS-compliant hardware and software security settings to enable the ESKM appliance to operate with the highest software security settings described in the FIPS standards.

6.11.2.1 ESKM appliance settings required for FIPS compliance

In order to comply with FIPS 140-2 standards, the following functionality must be disabled on the ESKM appliance:

- LDAP authentication without SSL or Minimum TLS Version less than 1.2.

- LDAP administrator server without SSL or Minimum TLS Version less than 1.2.
- Use of the following algorithms: RC4, DES, DES-EDE-112, RSA-512, and RSA-1024; these algorithms are not available when FIPS compliance is enabled.
- Utimaco recommends running TLS 1.2 over the ESKM XML interface; this requires that you generate a certificate and enable it.
- Hot-swappable drive capability.
- RSA encrypt/decrypt operations—RSA encrypt/decrypt associated with TLS handshakes, and Sign and SignVerify operations are permitted.

These settings are adjusted automatically when you use the Management Console's High Security Configuration page to enable FIPS compliance on the ESKM appliance.

6.11.2.2 FIPS compliance and clustering

The ESKM appliance being added to a cluster assumes the mode of the server nodes already in the cluster. For example, adding a non-FIPS-compliant ESKM appliance to a cluster, in which all nodes are operating in FIPS-compliant mode, causes the appliance being added to enter FIPS-compliant mode.

Conversely, adding a FIPS-compliant ESKM appliance to a cluster, in which all of the other appliances are operating in non-FIPS-compliant mode, causes the appliance being added to enter non-FIPS-compliant mode.

For more information about clustering, see Clustering procedures (p. 114).

6.11.2.3 Backups

FIPS and non-FIPS ESKM appliances cannot share backups.

6.11.2.4 FIPS self-test

To run a FIPS self-test, restart the ESKM appliance, see Restart/halt (p. 195).

6.11.2.5 Software patches and upgrades

Utimaco will indicate which software versions and configurations are FIPS validated. Utimaco recommends using FIPS validated configurations whenever possible.

6.11.2.6 Enabling and disabling FIPS compliance

According to FIPS requirements, you cannot enable or disable FIPS compliance when there are keys on the ESKM appliance. You must manually delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion.

Utimaco strongly recommends that you back up your keys before deleting them.

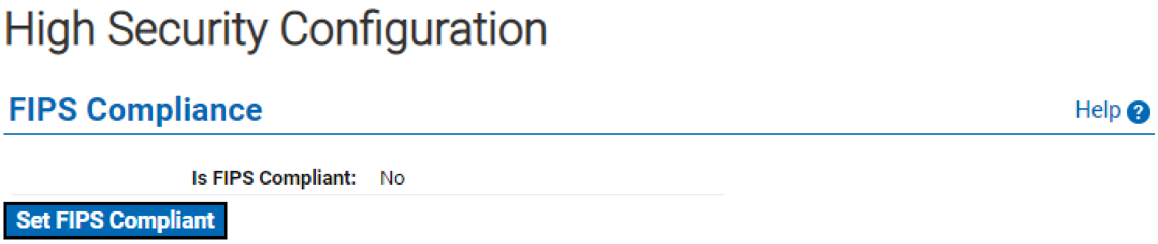
6.11.3 High security configuration

The High Security Configuration page allows you to manage the high security settings for the ESKM appliance. This page contains the following sections:

- FIPS compliance (p. 371)
- High security settings (p. 374)
- Security settings configured elsewhere (p. 377)

6.11.3.1 FIPS compliance

Use this section to determine if the ESKM appliance is FIPS-compliant, and also to enable FIPS compliance.



High Security Configuration

FIPS Compliance

Is FIPS Compliant: No

Figure 144 : Set FIPS Compliance

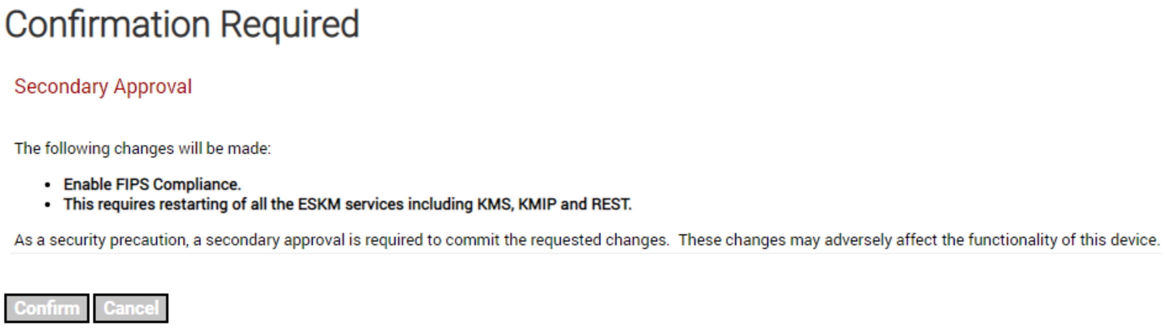
Before making **ESKM FIPS Compliant**, please make sure that all the TLS connections with ESKM (KMS, KMIP & LDAP) work with TLS 1.2 and the certificates configured for LDAP server and KMS/KMIP clients are with FIPS approved algorithms. In order to make ESKM FIPS compliant, click **Set FIPS Compliant** button in the high security page. For more information, see SSL Options (p. 389).

The following table describes the components of **FIPS Compliance**.

Table 93: FIPS Compliance components

Component	***Description***
Is FIPS Compliant	Indicates if the ESKM appliance's overall security configuration is consistent with FIPS 140-2 requirements. You cannot edit this field. If this value is Yes, the **Set FIPS Compliant** button is not enabled.
Set FIPS Compliant	Click **Set FIPS Compliant** to automatically comply with FIPS 140-2 standards and alter the settings shown in the **High Security Settings** and **Security Settings Configured Elsewhere**. ℹ Modifying any of the settings in the **High Security Settings** and **Security Settings Configured Elsewhere** takes the ESKM appliance out of FIPS 140-2 compliance. ❗ According to FIPS requirements, you cannot enable or disable FIPS compliance while there are keys on the ESKM appliance. You must manually delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion. Utimaco strongly recommends that you back up your keys before deleting them. This button is available in ESKM appliances that are not configured for FIPS compliance.

Clicking the FIPS Compliant button, the user is prompted to click the Confirm button in order to enable FIPS Compliance.



Confirmation Required

Secondary Approval

The following changes will be made:

- **Enable FIPS Compliance.**
- **This requires restarting of all the ESKM services including KMS, KMIP and REST.**

As a security precaution, a secondary approval is required to commit the requested changes. These changes may adversely affect the functionality of this device.

Figure 145 : Confirmation - Enable FIPS Compliance

This confirmation is required only if Disable Non-FIPS Algorithms and Key Sizes disabled.

6.11.3.1.1 FIPS Mode changes

Following security settings are not allowed when ESKM is FIPS compliant,

1. TLS 1.0 or TLS 1.1 in KMS and KMIP SSL options
2. TLS ciphers with RSA key exchange in KMS and KMIP SSL options
3. TLS 1.0 or TLS 1.1 as Minimum TLS version LDAP server settings
4. Import of certificates created with non-FIPS approved algorithms (SHA1, 3DES etc..)
5. Client certificates created with non-FIPS approved algorithms (SHA1, 3DES etc..) for client side authentication

On upgrading to 8.50 release, ESKM will go to FIPS non-compliance if TLS 1.0 or TLS 1.1 or any TLS cipher with RSA key exchange is enabled prior upgrade. User has to go to high security page and check the section(v8.50.0) 2021-0046 Security settings configured elsewhere*Security Settings Configured Elsewhere* (p. 377) to see the reason for FIPS non-compliance.

ESKM will go to FIPS non-compliance, if TLS 1.0 or TLS 1.1 or TLS cipher with RSA key exchange is enabled.

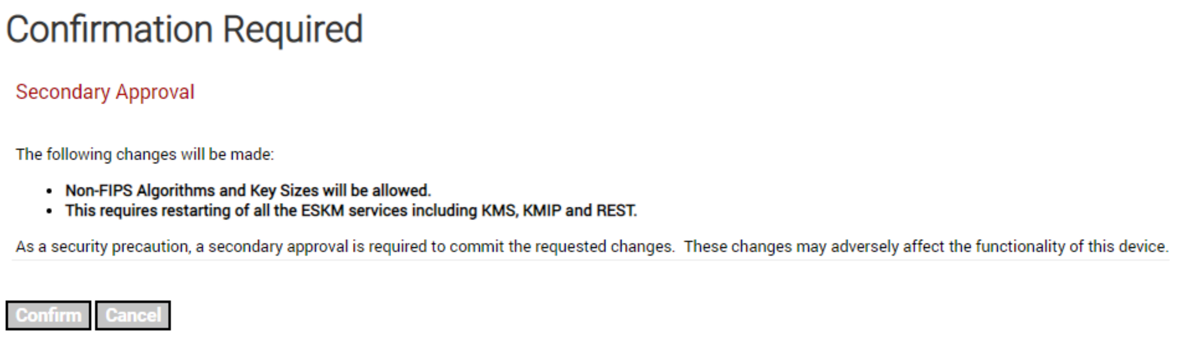
The parameter *Disable Non-FIPS Algorithms and Key Sizes* (in Security->High Security Page) must be disabled for the proper working of TLS 1.0 or TLS 1.1. This parameter change requires restarting of all the ESKM services including KMS, KMIP and REST.

6.11.3.2 High security settings

Use **High Security Settings** to view the status of security-related functionality on the ESKM appliance. This functionality must be disabled for FIPS compliance. These settings are automatically configured when you select **Set FIPS Compliance** in FIPS Compliance.

When you enable FIPS compliance on the ESKM appliance, the functionality displayed here is disabled. Modifying any of the items in the High Security Settings requires the user to click the Confirm button, which immediately takes the appliance out of FIPS compliance.

This should be used to review the key and device security functionality that has been disabled for full FIPS compliance. When the ESKM appliance is FIPS-compliant, you should not alter these settings.



Confirmation Required

Secondary Approval

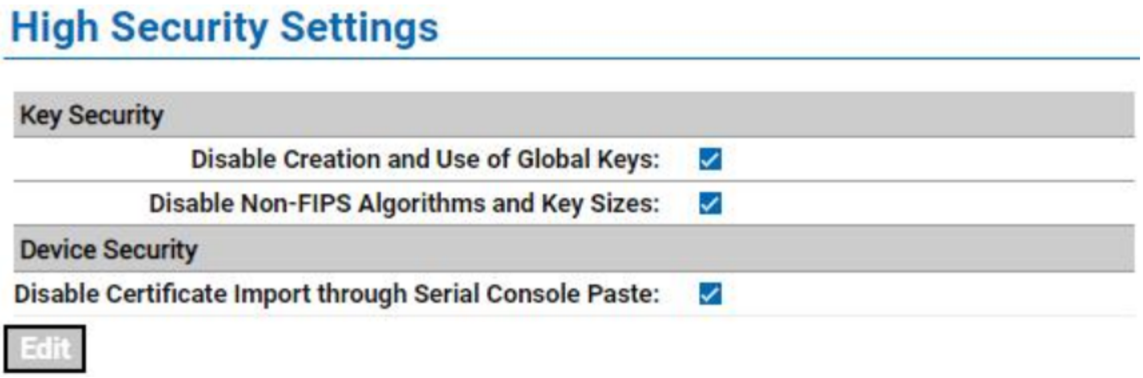
The following changes will be made:

- **Non-FIPS Algorithms and Key Sizes will be allowed.**
- **This requires restarting of all the ESKM services including KMS, KMIP and REST.**

As a security precaution, a secondary approval is required to commit the requested changes. These changes may adversely affect the functionality of this device.

Figure 146 : Confirmation

According to FIPS requirements, you cannot enable or disable FIPS compliance while there are keys on the ESKM appliance. You must manually delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion. Utimaco strongly recommends that you back up your keys before deleting them.



High Security Settings

Key Security

Disable Creation and Use of Global Keys: ☑

Disable Non-FIPS Algorithms and Key Sizes: ☑

Device Security

Disable Certificate Import through Serial Console Paste: ☑

Figure 147 : High Security Settings

The following table describes the components of **High Security Settings**.

Table 94: High Security Settings components

Component	***Description***
Disable Creation and Use of Global Keys	Disables the ability to create and use global keys. Once this option is selected, global keys cannot be created on the ESKM appliance. Any existing global keys will not be usable by the ESKM appliance for any purpose. While the ESKM appliance is FIPS-compliant, you may assign an owner to an existing global key.

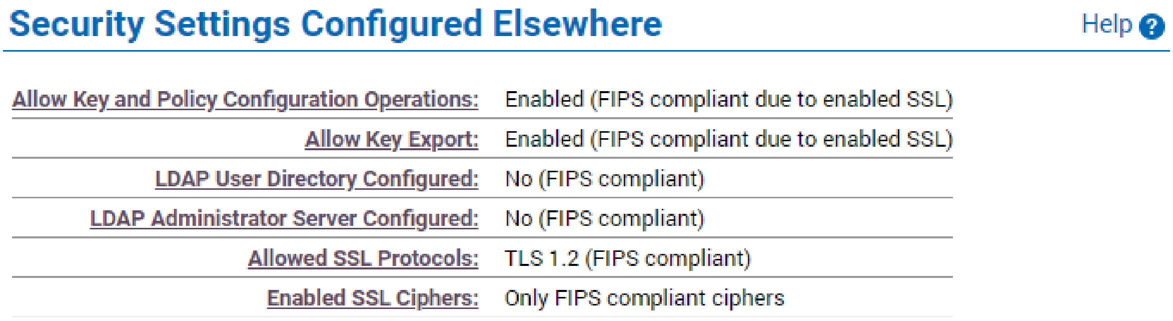
Component	***Description***
Disable Non-FIPS Algorithms and Key Sizes	Prevents the creation or use of algorithms and key sizes that are not FIPS-compliant. The following algorithms and key size combinations will be disallowed: ▪ RC4 ▪ DES ▪ DES-EDE-112 ▪ RSA-768 and RSA-1024** ⚠ **If your server currently uses a 768-bit or 1024-bit certificate, this option cannot be selected. You must select, and possibly create, a different server certificate. ⚠ Clients with 768-bit certificates will be rejected when they try to connect to a FIPS-compliant ESKM appliance. Any existing keys and certificates based on these algorithms and key sizes will not be usable by the ESKM appliance for any purpose. The following algorithms and keys sizes will continue to be available on the ESKM appliance: ▪ AES-128, AES-192, AES-256 ▪ DES-EDE-168 ▪ HMAC SHA-1 ▪ RSA-2048 ▪ RSA-3072 ▪ RSA-4096

Component	***Description***
	⚠ This parameter change requires restarting of all the ESKM services including KMS, KMIP and REST. ⚠ The setting Disable Non-FIPS Algorithms and Key Size is local to the node. Modifications made to this parameter will not be replicated to other nodes in the cluster.
Disable Certificate Import through Serial Console Paste	Prevents administrators from importing certificates through the serial console using cut and paste.
Edit	Click to change the settings. ⚠ Deselecting any of these fields takes the ESKM appliance out of FIPS compliance.

6.11.3.3 Security settings configured elsewhere

Use Security Settings Configured Elsewhere to monitor the status of security settings that are configured on other pages of the Management Console.

> ℹ Modifying any of the items in Security Settings Configured Elsewhere immediately takes the ESKM appliance out of FIPS 140-2 compliance.



Security Settings Configured Elsewhere

Allow Key and Policy Configuration Operations:	Enabled (FIPS compliant due to enabled SSL)
Allow Key Export:	Enabled (FIPS compliant due to enabled SSL)
LDAP User Directory Configured:	No (FIPS compliant)
LDAP Administrator Server Configured:	No (FIPS compliant)
Allowed SSL Protocols:	TLS 1.2 (FIPS compliant)
Enabled SSL Ciphers:	Only FIPS compliant ciphers

Figure 148 : Security Settings Configured Elsewhere

The following table describes the components of **Security Settings Configured Elsewhere**.

Table 95: Security Settings Configured Elsewhere components

Component	***Description***
Allow Key and Policy Configuration Operations	Displays the value of the **Allow Key and Policy Configuration Operations** field in KMS Server Settings. When enabled, users can configure keys and authorization policies through the ESKM XML Interface. Click the link to access KMS Server Settings. For FIPS compliance, this functionality must be disabled, or SSL/TLS must be enabled.
Allow Key Export	Displays the value of the **Allow Key Export** field in KMS Server Settings. When enabled, users can export keys from the ESKM appliance through the ESKM XML Interface. Click the link to access KMS Server Settings. For FIPS 140-2 compliance, this functionality must be disabled, or SSL/TLS must be enabled.
LDAP User Directory Configured	Displays the value of the **LDAP User Directory.** Click the link to access LDAP User Directory Properties. For FIPS 140-2 compliance, an LDAP User Directory must have SSL enabled with minimum TLS version TLS 1.2 configured.
LDAP Administrator Server Configured	Displays the value of **LDAP Administrator Server**. Click the link to access LDAP Administrator Server Properties. For FIPS 140-2 compliance, an LDAP Administrator Server must have SSL enabled with minimum TLS version TLS 1.2 configured.

Component	***Description***
Allowed SSL Protocols	Displays the SSL Protocols enabled in SSL Options. Click the link to access SSL Options. FIPS compliance requires TLS 1.2 or later.
Enabled SSL Ciphers	Indicates the security strength of the SSL/TLS cipher suites enabled in the **SSL Cipher Order**. Click the link to access **SSL Cipher Order**. All SSL/TLS ciphers with ECDHE key exchange are FIPS compliant.

6.11.4 High security procedures

This section describes the procedures for managing the high security features of the ESKM appliance.

It explains the following processes:

- Configuring for overall FIPS compliance (p. 379)
- Configuring the high security settings (p. 380)

6.11.4.1 Configuring for overall FIPS compliance

The ESKM appliance can be configured to comply with FIPS 140-2 standards.

To configure the ESKM appliance for FIPS compliance

1. View the Security Protocols enabled on your Internet Browser. You must enable TLS, version 1.0 or higher, to access the Management Console for FIPS compliance.

2. Log in to the Management Console as an administrator with SSL/TLS, Advanced Security, and KMS/KMIP Server access controls.

3. Navigate to the High Security Configuration page (**Security > High Security**).

4. Confirm that the **Is FIPS Compliant** value is “No” in **FIPS Compliance**.
If the **Is FIPS Compliant** value is “Yes,” the ESKM appliance is currently FIPS 140-2-compliant and settings should not be modified.

5. Click **Set FIPS Compliant** in **FIPS Compliance**.

> The KMS and KMIP servers restart automatically and your browser might display an error. If this situation should occur, refresh the browser.

> Review the settings in **High Security Settings** and **Security Settings Configured Elsewhere** to confirm all settings have been adjusted for FIPS 140-2 compliance.

6.11.4.2 Configuring the high security settings

> When you enable FIPS compliance on the ESKM appliance, the functionality displayed here is disabled. Modifying any of the items in the **High Security Settings** immediately takes the ESKM appliance out of FIPS compliance. This section should be used to review the key and device
> security functionality that has been disabled for full FIPS compliance. When the ESKM appliance is FIPS-compliant, you should not alter these settings.

To configure the High Security settings on a non-FIPS-compliant ESKM appliance

1. Log in to the Management Console as an administrator with SSL/TLS, Advanced Security, and KMS server access controls.

2. Navigate to the High Security Configuration page (**Security > High Security**).

3. Alter the fields in **High Security Settings** as needed.

4. Navigate to **Security Settings Configured Elsewhere** (located below High Security Settings).

5. Review the settings in this section. To alter these settings, click the fields to access the appropriate sections.

6.11.5 FIPS status server

The FIPS Status Server is an http server that provides system status, in the form of FIPS status report (p. 381), whenever the ESKM appliance is running. The report indicates:

- The latest results of all system self-tests
- The ESKM appliance's state (either error or normal)
- The status of FIPS 140-2 level 2 compliance (either yes or no)

If any of these tests fail, the FIPS Status Report indicates which test failed and when the failure occurred. The appliance then enters an error state: access to the Management Console, the Command Line Interface, and the ESKM XML Interface is denied. Limited access to the appliance via the serial console is supported.

To restore functionality, restart the ESKM appliance. If the problem persists, contact Utimaco Technical Support (p. 798).

6.11.5.1 FIPS status report

Use the FIPS Status Report to view information about the ESKM appliance, including server status, FIPS compliance, and self-test results. You can view the FIPS Status Report by accessing the following address in your browser:

<http://<Local> IPv4>:<Local Port>/status.html
<http://[<Local> IPv6>]:<Local Port>/status.html

See Viewing the FIPS status report (p. 96).

The following table describes the components of **FIPS Status Server Settings**.

Table 96: FIPS Status report components

Component	***Description***
Product	Displays the product name.
Unit ID	The Unit ID is composed of alphanumeric characters.
Hostname	The hostname is the name used to identify the ESKM appliance on the network.

Component	***Description***
IP Address(es)	This field specifies the IPv4/IPv6 address(es) on which the KMS and KMIP servers are enabled on the ESKM appliance.
Device State	Indicates the current state of the ESKM appliance, either normal or error. When in an error state, functionality is dramatically limited: you will not be able to communicate with the appliance using the CLI, the Management Console, or the ESKM XML Interface. Limited access to the appliance via the serial console will be supported. Reboot the appliance to restore functionality. If the problem persists, contact Utimaco Technical Support (p. 798).
FIPS Compliant	Indicates whether the ESKM appliance is FIPS-compliant.

Component	***Description***
Test Results	Displays the result and timestamp for each of the following self-tests:

Component	***Description***
	▪ KMS AES Known Answer Test ▪ AES Known Answer Test ▪ KMS AES CCM Known Answer Test ▪ AES CCM Known Answer Test ▪ KMS AES GCM Known Answer Test ▪ AES GCM Known Answer Test ▪ KMS AES XTS Known Answer Test ▪ AES XTS Known Answer Test ▪ AES Key Wrap Known Answer Test ▪ KMS TDES Known Answer Test ▪ TDES Known Answer Test ▪ DSA POST Pairwise Consistency Test ▪ KMS HMAC SHA-1 Known Answer Test ▪ KMS HMAC SHA-224 Known Answer Test ▪ KMS HMAC SHA-256 Known Answer Test ▪ RSA Decryption Primitive Known Answer Test ▪ RSA Known Answer Test ▪ Diffie-Hellman Known Answer Test ▪ SSH Key Derivation Known Answer Test ▪ SNMP Key Derivation Known Answer Test ▪ TLS Key Derivation Known Answer Test ▪ ECDSA POST Pairwise Consistency Test ▪ ECDH Known Answer Test ▪ ECDSA Pairwise Consistency Test ▪ KMS ECDH Known Answer Test ▪ KMS ECDH Primitive Test ▪ ECDH Primitive Test ▪ KMS ECDH Pairwise Test ▪ ECDH Pairwise Test ▪ KMS DRBG Known Answer Test ▪ DRBG Known Answer Test

Component	***Description***
	▪ KMS HMAC SHA-384 Known Answer Test ▪ KMS HMAC SHA-512 Known Answer Test ▪ HMAC Known Answer Test ▪ CMAC Known Answer Test ▪ KMS RSA Known Answer Test ▪ Continuous Random Number Generation Test ▪ RSA Pairwise Consistency Test ▪ DSA Pairwise Consistency Test ▪ DH Pairwise Consistency Test ▪ Software Integrity

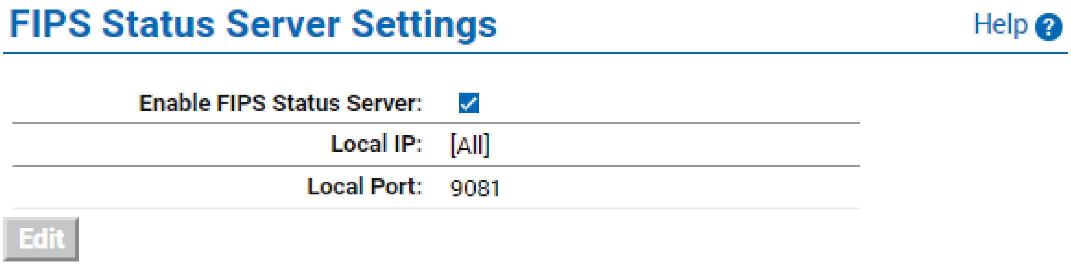
If the ESKM appliance enters an error state, restart it. If the error persists, contact Utimaco Technical Support (p. 798).

6.11.6 FIPS status server page

The FIPS Status Server page allows you to manage the FIPS status server. The FIPS status server monitors for FIPS-related status and error messages. If the ESKM appliance self-test fails upon start-up, all other services on the appliance shut down, including the Management Console. Only the FIPS status server continues to run in this state.

6.11.6.1 FIPS status server settings

Use FIPS Status Server Settings to enable the FIPS Status Server, and then select the IPv4/ IPv6 address and port used to access the status report.



FIPS Status Server Settings

Enable FIPS Status Server:	☑
Local IP:	[All]
Local Port:	9081

Figure 149 : FIPS Status Server Settings

The following table describes the components of **FIPS Status Server Settings**.

Table 97: FIPS Status Server Settings components

Component	***Description***
Enable FIPS Status Server	Select this option to enable the FIPS Status Server on the ESKM appliance. Only administrators with Advanced Security access control permission can enable the FIPS Status Server, see Modifying administrator properties (p. 481).
Local IP	Select the IPv4/IPv6 addresses on which the FIPS Status Server is enabled on the ESKM appliance.
Local Port	Select the port on which the server status report is available. Default is 9081.

6.11.7 SSL/TLS overview

The ESKM appliance is designed to be able to establish Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections with all client applications that make requests to the ESKM appliance. KMIP clients must use TLS. SSL and TLS are the most widely deployed security protocols in network security. The following section provides a brief overview of the SSL/TLS protocol so that you might better understand how to configure the ESKM appliance.

SSL/TLS is used to establish secure connections between two entities, such as a client application and an ESKM appliance. In addition to securing connections, SSL/TLS is commonly used to authenticate a server to a client and vice versa. The SSL/TLS protocol is composed of two phases: (1) establishing a secure connection using the SSL/TLS handshake protocol, and (2) exchanging data over the secure connection.

6.11.7.1 SSL/TLS handshake

The following steps describe a typical SSL/TLS handshake:

1. The protocol is initiated by the requesting client application using a client hello message. This message includes a list of all the cipher suites supported by the client application. The application also sends a session ID that may refer to previously established sessions.

2. The ESKM appliance responds with a server hello message, which includes the KMS certificate and the cipher suite chosen by the ESKM appliance. Once the session is established, it is secured using the chosen cipher suite. The message also contains a session ID.

3. The client application and the ESKM appliance then engage in a key exchange protocol. The result is a session key that is used for encrypting the entire session.

Once the SSL/TLS handshake is completed, the two sides begin exchanging application data, such as cryptographic operations, data migration operations, and so on. All data is encrypted using the negotiated session key.

6.11.7.2 SSL/TLS session resume

Because the SSL/TLS key exchange protocol is based on public key cryptography, it consumes significant computing resources. To minimize the number of SSL/TLS handshakes, SSL/TLS provides a shortcut to a full key exchange.

Consider a client application that has previously established a secure session with the ESKM appliance. Both the client application and the ESKM appliance already share a session-key. When the client application reconnects to the ESKM appliance, there is no need to create a new session key. During the reconnection process, the two sides execute the SSL/TLS resume protocol, which bypasses the key exchange part of the SSL/TLS handshake. The resumed session is encrypted using the previously negotiated session-key. Establishing a secure connection using SSL/TLS resume is much faster than a full SSL/TLS handshake.

In this scenario, the client application indicates that it is willing to perform an SSL/TLS resume (rather than a full handshake) by sending a previously negotiated session-id in the CLIENT-HELLO message. The ESKM appliance checks that it has the session key for the given session-id. If so, it acknowledges that it is willing to resume the session by using the same session-id in the SERVER-HELLO message. Otherwise, the ESKM appliance responds with a new session-id.

6.11.7.3 SSL/TLS session timeout

All SSL/TLS sessions stored in the ESKM appliance's session cache have an expiration period, typically two hours. This means the ESKM appliance accepts a session resume request for at most two hours after the session is first established.

Consequently, every client application must reconnect a session key at least once every two hours. This limits the amount of information encrypted with a particular session key. Hence, an attacker who is able to deduce a session key would only obtain the exchanged information during a two hour window. The SSL/TLS session timeout on the ESKM appliance is configured using the SSL options (p. 389).

6.11.7.4 SSL/TLS certificate management

Certificates are used to authenticate one entity to another. This authentication takes place during the SSL/TLS handshake protocol. Certificates are issued by Certification Authorities (CAs) such as VeriSign, Entrust, Thawte, and others. The ESKM appliance is equipped with CA capabilities, and can issue certificates for all client applications.

When establishing an SSL/TLS connection with a client application, you can mandate that the client application authenticate itself to the ESKM appliance by presenting a certificate. Because the ESKM appliance can issue certificates to client applications, there is no need for you to use a public CA such as VeriSign to issue these certificates. You can generate these certificates on the ESKM appliance.

The ESKM appliance CA is managed on the CA Certificates page. To issue certificates for your client applications, you must first create a local CA on the ESKM appliance. This local CA is then used to issue certificates for all your client applications. Local certificates issued by the ESKM appliance CA are valid only for authenticating to the ESKM appliance.

6.11.8 SSL/TLS

The **SSL Configuration** page allows you to manage your SSL/TLS settings for both the KMS and KMIP servers. This section contains information on the following SSL-related topics:

- SSL options (p. 389)
- SSL/TLS cipher order (p. 390)

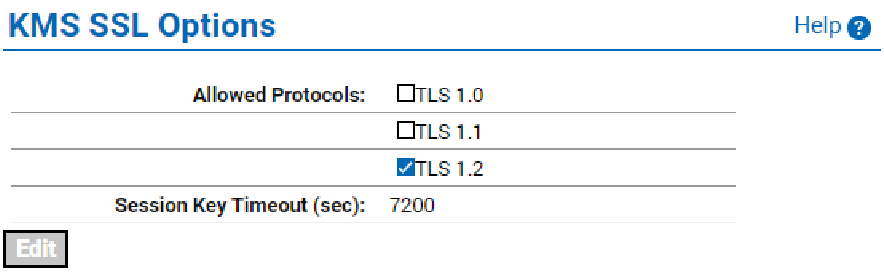
6.11.8.1 SSL options

Use **SSL Options** to view and modify SSL/TLS settings. These settings affect the ESKM appliance's communication with client applications when SSL/TLS is enabled. These settings also affect all connections to the web-based Management Console.

TLS 1.0 and TLS 1.1 are not allowed when operating in FIPS mode. You must enable TLS 1.2 and disable TLS 1.0 and 1.1.

Please make sure that TLS 1.2 is enabled in the web browser and KMS/KMIP client application.

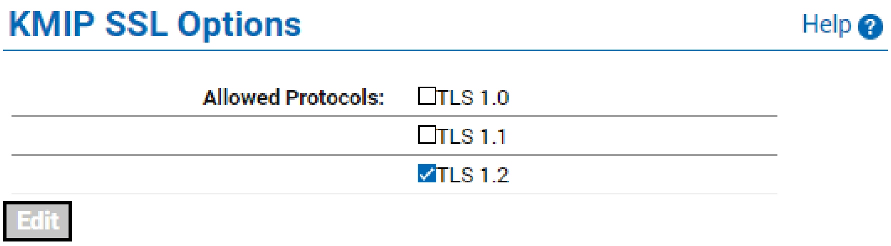
Utimaco recommends that you always enable at least one of the TLS protocols on the ESKM appliance.



KMS SSL Options

Allowed Protocols:	☐TLS 1.0
	☐TLS 1.1
	☑TLS 1.2
Session Key Timeout (sec):	7200

Figure 150 : KMS SSL Options



KMIP SSL Options

Allowed Protocols:	☐TLS 1.0
	☐TLS 1.1
	☑TLS 1.2

Figure 151 : KMIP SSL Options

Changing ESKM or KMIP SSL/TLS Options causes the ESKM or KMIP server to restart, which takes it offline for a few seconds.

The following table describes the components of **SSL Options**.

Table 98: SSL/TLS Options components

Component	***Description***
Allowed Protocols	The Allowed Protocols field allows you to specify which versions of SSL and TLS are enabled on the ESKM appliance. The supported protocols are: ▪ TLS 1.0 (Transport Layer Security version 1.0), TLS 1.1, and TLS 1.2. ⚠ If your internet browser is not configured to use the protocol selected here, you will be denied access to the Management Console. Consult and alter your browser settings before changing these values. ⚠ Enabling TLS 1.0 or TLS 1.1 on a FIPS-compliant ESKM appliance takes the appliance out of FIPS compliance — possibly in a manner that does not comply with FIPS standards. For information about disabling FIPS compliance, see FIPS compliance (p. 371). ⚠ The parameter Disable Non-FIPS Algorithms and Key Sizes in high security settings must be disabled for the proper working of TLS 1.0 or TLS 1.1.
Session Key Timeout (sec)	The Session Key Timeout option specifies the number of seconds that a previously negotiated session key is reused for incoming SSL/TLS client connections to the ESKM appliance. The default value is 7200 seconds (2 hours). Setting this value to 0 disables the timeout.
Edit	Click **Edit** to modify the SSL/TLS options.

6.11.8.2 (v8.50.0) 2021-0046 SSL/TLS cipher order

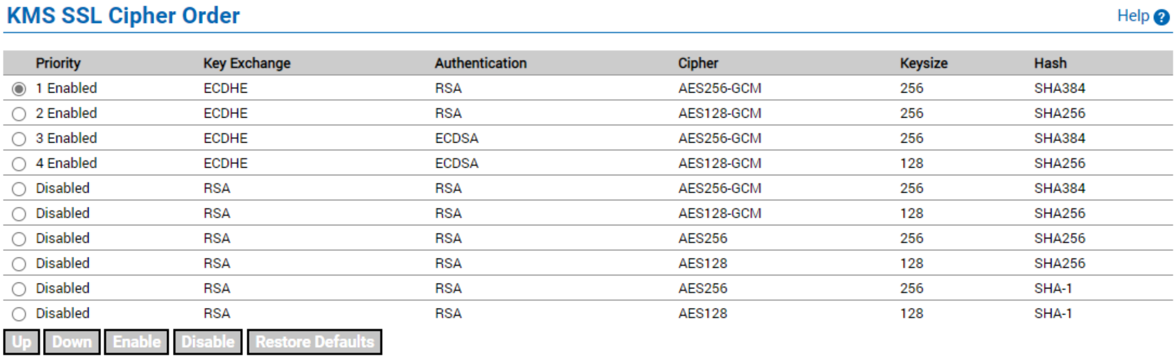
Use **SSL Cipher Order** to enable, disable, and order the priority of SSL/TLS cipher suites.

Different client applications support different encryption algorithms for securing SSL/TLS sessions. The ESKM appliance supports many SSL/TLS cipher suites and consequently can communicate securely using many common cipher suites.

SSL Cipher Order pertains to the communication channel between the client application and the ESKM appliance. When a client application presents the ESKM appliance with a list of supported cipher suites, the appliance “chooses” the supported cipher suite that is highest on its priority list.

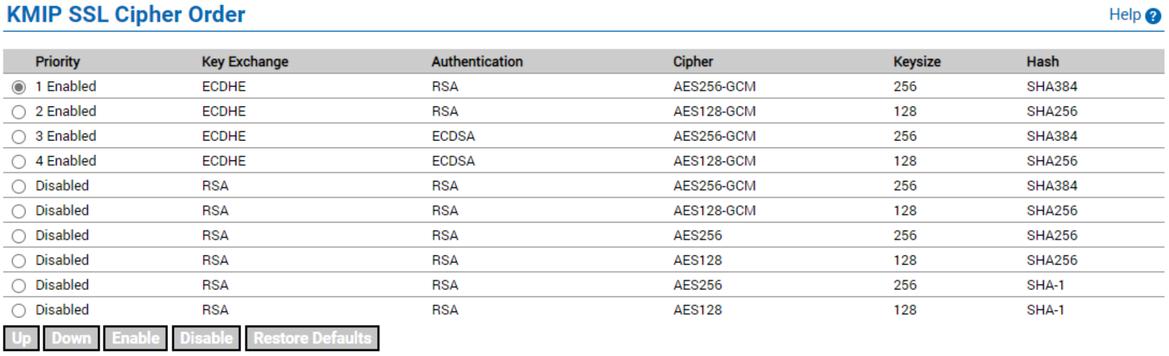
Exercise caution when modifying the **SSL/TLS cipher orde**r. Unless you are familiar with SSL/TLS cipher suites, you should not rearrange the **Cipher Order** list. Changes to the list may affect both performance and security. Click **Restore Defaults** to reset the list to the original settings.

Enabling or disabling a TLS cipher suite or changing the cipher order will cause the KMS or KMIP server service to restart and may result in client connections to be dropped.



Priority	Key Exchange	Authentication	Cipher	Keysize	Hash
● 1 Enabled	ECDHE	RSA	AES256-GCM	256	SHA384
○ 2 Enabled	ECDHE	RSA	AES128-GCM	256	SHA256
○ 3 Enabled	ECDHE	ECDSA	AES256-GCM	256	SHA384
○ 4 Enabled	ECDHE	ECDSA	AES128-GCM	128	SHA256
○ Disabled	RSA	RSA	AES256-GCM	256	SHA384
○ Disabled	RSA	RSA	AES128-GCM	128	SHA256
○ Disabled	RSA	RSA	AES256	256	SHA256
○ Disabled	RSA	RSA	AES128	128	SHA256
○ Disabled	RSA	RSA	AES256	256	SHA-1
○ Disabled	RSA	RSA	AES128	128	SHA-1

Figure 152 : KMS SSL Cipher Order



KMIP SSL Cipher Order

Priority	Key Exchange	Authentication	Cipher	Keysize	Hash
● 1 Enabled	ECDHE	RSA	AES256-GCM	256	SHA384
○ 2 Enabled	ECDHE	RSA	AES128-GCM	128	SHA256
○ 3 Enabled	ECDHE	ECDSA	AES256-GCM	256	SHA384
○ 4 Enabled	ECDHE	ECDSA	AES128-GCM	128	SHA256
○ Disabled	RSA	RSA	AES256-GCM	256	SHA384
○ Disabled	RSA	RSA	AES128-GCM	128	SHA256
○ Disabled	RSA	RSA	AES256	256	SHA256
○ Disabled	RSA	RSA	AES128	128	SHA256
○ Disabled	RSA	RSA	AES256	256	SHA-1
○ Disabled	RSA	RSA	AES128	128	SHA-1

Figure 153 : KMIP SSL Cipher Order

The following table describes the components of **SSL Cipher Order**.

Table 99: SSL Cipher Order components

Component	***Description***
Priority	You can arrange the SSL/TLS cipher suite order using the Up and Down buttons. One (1) is the highest priority, and ten (10) is a low priority.
Key Exchange	This field specifies the algorithm to use for key establishment. Supported key exchanges: ECDHE and RSA.
Authentication	This field specifies the authentication algorithm. Supported algorithms: ECDSA and RSA.

Component	***Description***
Cipher	This field specifies the cipher to use to encrypt TLS sessions. Supported ciphers are the following: FIPS Compliant Ciphers ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 FIPS Non-Compliant Ciphers RSA-RSA-AES256-GCM-SHA384 RSA-RSA-AES128-GCM-SHA256 RSA-RSA-AES256-SHA256 RSA-RSA-AES128-SHA256 RSA-RSA-AES256-SHA1 RSA-RSA-AES128-SHA1 Ciphers supported for TLS 1.0 & TLS 1.1 RSA-RSA-AES256-SHA1 RSA-RSA-AES128-SHA1
Keysize	This field specifies the number of bits of the session key size. Supported key sizes vary for each cipher suite.
Hash	This field specifies the keyed-hash message authentication code (HMAC) to use to authenticate TLS sessions. Supported HMACs: HMAC SHA-1, HMAC SHA-256 and HMAC SHA-384.
Up / Down	Click **Up** and **Down** to arrange the SSL/TLS cipher order. You cannot change the order of a disabled cipher suite.

Component	***Description***
Enable or Disable	Click **Enable** and **Disable** to enable and disable the selected cipher suite. Enabling TLS cipher suites with RSA key exchange on a FIPS-compliant ESKM appliance takes the appliance out of FIPS compliance.
Restore Defaults	Click **Restore Defaults** to restore the original SSL/TLS cipher order.

6.11.9 SSH Configuration

The **SSH Configuration** page enables you to manage your SSH cryptographic algorithms.

ESKM allows the user to configure the Ciphers, MACs and KeyExchange algorithms used to protect an SSH connection.

6.11.9.1 SSH Cipher Order

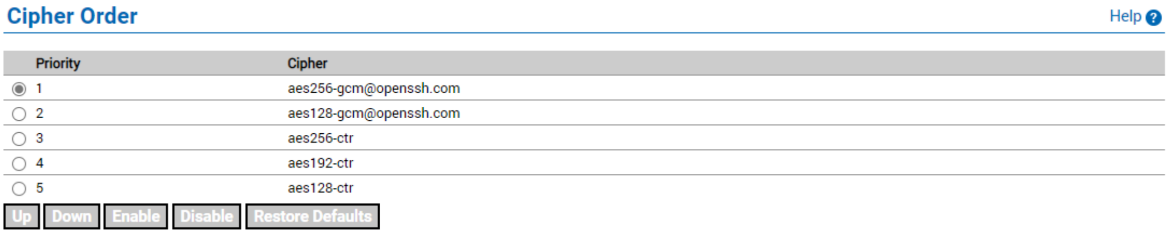
Use this section to enable, disable, and order the priority of SSH ciphers.

Different client applications support different encryption algorithms for securing SSH sessions. The Enterprise Secure Key Manager supports many SSH ciphers and consequently can communicate securely using all common ciphers.

The SSH cipher selected for securing connection is based on the first common cipher present in the priority list of both the server as well as the client.

Exercise caution when modifying the **SSH Cipher Order**. Unless you are familiar with SSH Ciphers, you should not rearrange the **Cipher Order** list. Changes to the list may affect both performance and security. Click **Restore Defaults** to reset the list to the original settings.

The SSH service will restart every time when the Cipher order is changed, a cipher is enabled or disabled.


Cipher Order

	Priority	Cipher
●	1	aes256-gcm@openssh.com
○	2	aes128-gcm@openssh.com
○	3	aes256-ctr
○	4	aes192-ctr
○	5	aes128-ctr

Figure 154 : Cipher Order

The following table describes the components of the SSH Cipher Order section:

Table 100: SSH Cipher Order components

Component	***Description***
Priority	You can arrange the SSH Cipher order using the **Up** and **Down** buttons. One (1) is the highest priority, and six (6) is the lowest priority.
Cipher	This field specifies the symmetric cipher to use to encrypt SSH sessions. Supported ciphers are aes256-ctr, aes128-ctr, aes192-ctr, aes256-gcm@openssh.com, and aes128-gcm@openssh.com.
Up / Down	Click **Up** and **Down** to arrange the SSH Cipher order.
Enable/Disable	Click **Enable** and **Disable** to enable and disable the selected cipher.
Restore Defaults	Click **Restore Defaults** to restore the original SSH cipher order.

6.11.9.2 SSH MAC Order

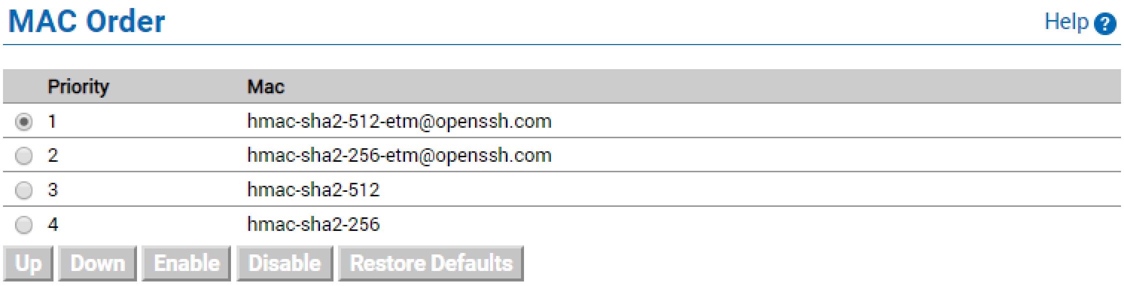
Use this section to enable, disable, and order the priority of SSH MACs.

Different client applications support different algorithms for securing SSH sessions. The Enterprise Secure Key Manager supports many SSH MACs and consequently can communicate securely using all common MACs.

The SSH MAC selected for securing connection is based on the first common MAC present in the priority list of both the server as well as the client.

Exercise caution when modifying the **SSH MAC Order**. Unless you are familiar with SSH MACs, you should not rearrange the MAC Order list. Changes to the list may affect both performance and security. Click **Restore Defaults** to reset the list to the original settings.

The SSH service will restart when the MAC order is changed or a MAC is enabled or disabled.



	Priority	Mac
●	1	hmac-sha2-512-etm@openssh.com
○	2	hmac-sha2-256-etm@openssh.com
○	3	hmac-sha2-512
○	4	hmac-sha2-256

Figure 155 : MAC Order

The following table describes the components of the SSH MAC Order section.

Table 101: SSH MAC Order components

Component	***Description***
Priority	You can arrange the SSH MAC order using the Up and Down buttons. One (1) is the highest priority, and four (4) is the lowest priority.
MAC	This field specifies the MAC to use to authenticate SSH sessions. Supported MACs are hmac-sha2-256-etm@openssh.com, hmac-sha2-512, hmac-sha2-512-etm@openssh.com, and hmac-sha2-256.
Up / Down	Click **Up** and **Down** to arrange the SSH MAC order.
Enable/Disable	Click **Enable** and **Disable** to enable and disable the selected MAC.
Restore Defaults	Click **Restore Defaults** to restore the original SSH MAC order.

6.11.9.3 SSH KEXAlgorithm Order

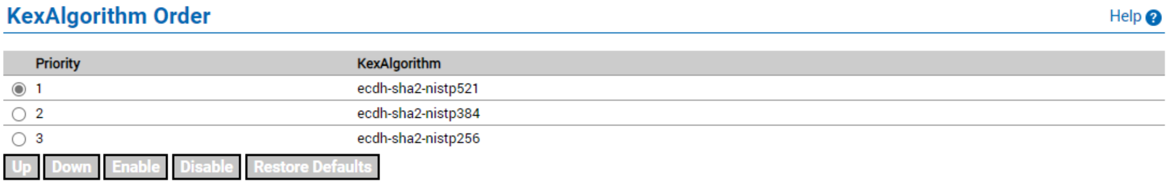
Use this section to enable, disable, and order the priority of SSH KEXAlgorithm.

Different client applications support different algorithms for securing SSH sessions. The Enterprise Secure Key Manager supports many SSH KEXAlgorithms and consequently can communicate securely using all common KEXAlgorithms.

The SSH KEXAlgorithm selected for securing connection is based on the first common KEXAlgorithm present in the priority list of both the server as well as the client.

> Exercise caution when modifying the **SSH KEXAlgorithm Order**. Unless you are familiar with SSH KEXAlgorithms, you should not rearrange the KEXAlgorithm Order list. Changes to the list may affect both performance and security. Click **Restore Defaults** to reset the list to the original settings.

The SSH service will restart once we change the KEXAlgorithm Order or enable/disable a KEXAlgorithm.



KexAlgorithm Order

	Priority	KexAlgorithm
●	1	ecdh-sha2-nistp521
○	2	ecdh-sha2-nistp384
○	3	ecdh-sha2-nistp256

Figure 156 : SSH KEXAlgorithm Order

The following table describes the components of the SSH KEXAlgorithm Order section.

Table 102: SSH KEXAlgorithm Order

Component	***Description***
Priority	You can arrange the SSH KEXAlgorithm order using the Up and Down buttons. One (1) is the highest priority, and nine (9) is the lowest priority.
KEXAlgorithm	This field specifies the KEXAlgorithms to use to establish SSH session keys. Supported KEXAlgorithms are ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521.
Up / Down	Click **Up** and **Down** to arrange the SSH KEXAlgorithm order.

Component	***Description***
Enable/Disable	Click **Enable** and **Disable** to enable and disable the selected SSH KEXAlgorithm.
Restore Defaults	Click **Restore Defaults** to restore the original SSH KEXAlgorithm order.

6.12 KMS server configuration

The ESKM appliance allows you to off-load cryptographic operations from client applications to the appliance. This section contains the following topics:

- Authentication overview (p. 398)
- Key management services configuration (p. 400)
- Health check overview (p. 408)
- Health check (p. 409)

6.12.1 Authentication overview

The communication between the client and the ESKM appliance varies slightly, depending on whether your appliance configuration requires users to authenticate. If you decide not to authenticate, then users have access only to global keys. Global keys are available to everyone, with no authentication required.

If you want to require authentication, then you must create keys for each user or group of users.

An authenticated user has access to all global keys, all the keys owned by the user, and all keys accessible to groups to which the user belongs. In addition, a group of users can have an authorization policy assigned to it, which restricts the use of the keys accessible by the group to certain time periods or certain operations per hour.

The ESKM appliance can define a local users and groups list or you can use an LDAP server to centrally manage your users and groups.

6.12.1.1 Authentication options

The ESKM appliance provides many options with respect to security and authentication. You can:

- Mandate SSL/TLS—Choose between SSL/TLS connections and standard TCP connections; SSL/TLS connections are more secure, because the data exchanged between client and server is encrypted.
- Allow global sessions—Allow clients to access and create global keys without providing a valid username and password to the ESKM appliance; this obviously does not offer a high level of security.
- Disable global sessions—Disable global sessions altogether, which requires all users to provide either a valid username and password combination, or a client certificate signed by a CA trusted by the ESKM appliance.
- Require client certificates—Mandate that clients present a client certificate in order to establish SSL/TLS connections. This client certificate can be the sole means of authenticating to the ESKM appliance, or it can be used in tandem with a username and password combination.
- Enforce strong, two-factor authentication—Take the required client certificates option one step further whereby the ESKM appliance will derive the username from the certificate; that username is then compared against the username provided in the authentication request. If the usernames match and the password provided is correct, the user is authenticated.

> ⚠ Utimaco recommends that you enforce the most stringent security policy supported by the ESKM appliance. Such a security policy would mandate SSL/TLS, disallow global sessions, and enforce strong, two-factor authentication.

6.12.1.2 Key access and ownership

Keys can be created as global or owned by a particular user (keys are not owned by administrators). When you give group access permission for a key, all the users in the group can use that particular key (after authenticating to the server).

When the client requests the server to generate a new key, it can specify that the key should be exportable and/or deletable. An exportable key is a key that a client can export from the

ESKM appliance. After a key is generated as exportable, it can be exported only by the owner and any members of a group with the “Export” permission for that key.

A deletable key is a key that the client can delete from the appliance. When a key is generated as deletable, only the owner of the key can delete the key.

> Administrators with Keys and Authorization Policies access control can delete any key, regardless of whether it is marked as deletable.

Clients that do not authenticate can only see global keys, which are accessible to all users. Likewise, any keys that the client generates during an unauthenticated connection are global keys. If a global key is marked as exportable or deletable during generation, then all users have permission to export or delete that key.

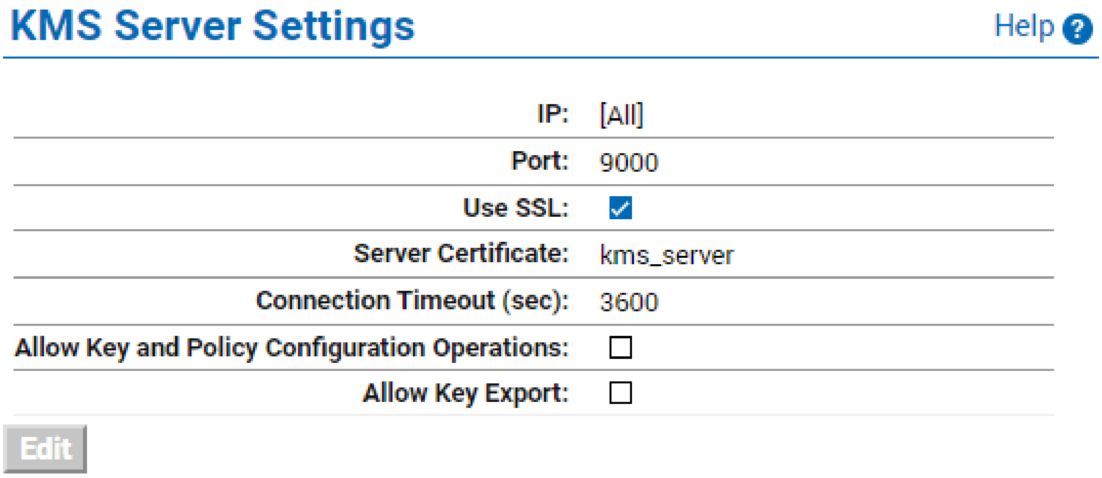
6.12.2 Key management services configuration

The KMS Configuration page (**Device > KMS Server > Key Management Services Configuration**) allows you to configure the KMS server, KMS server authentication settings, and the user account lockout settings. This page contains the following KMS server-related sections:

- KMS server settings (p. 400)
- KMS server authentication settings (p. 404)
- User account lockout settings (p. 407)

6.12.2.1 KMS server settings

Use **KMS Server Settings** to set up the basic KMS server settings.



KMS Server Settings

Help ?

IP:	[All]
Port:	9000
Use SSL:	☑
Server Certificate:	kms_server
Connection Timeout (sec):	3600
Allow Key and Policy Configuration Operations:	□
Allow Key Export:	□

Figure 157 : KMS Server Settings

The following table describes the components of **KMS Server Settings**.

Table 103: KMS Server Settings components

Component	***Description***
IP	This field specifies the IP address(es) which the KMS server will use to listen for client requests. The drop-down list box consists of all IPv4 and IPv6 addresses bound to the ESKM appliance. Utimaco strongly recommends that you select a specific IP address instead of specifying [All]. If you have four IP addresses bound to the ESKM appliance, then the KMS server "listens" for traffic on four different IP addresses; whereas, if you specify a single IP address, the KMS server "listens" for traffic on only one IP address. This can greatly reduce system vulnerability to outside attacks.
Port	Port on which the KMS server is listening for client requests. The default port is 9000; however, you can use any available port.

Component	***Description***
Use SSL	Specify whether you want to mandate that clients connect to the KMS server using an SSL connection. A check mark in the box indicates that the KMS server only accepts traffic on an SSL connection. If the Use SSL option is not enabled, the KMS server will not accept SSL connections.
Server Certificate	If you are requiring SSL/TLS, you must provide the certificate that will be used to authenticate the KMS server to clients.
Connection Timeout (sec)	The Connection Timeout value specifies, in seconds, how long client connections can remain idle before the KMS server begins closing them. The default value is 3600 (1 hour); the maximum value is 7200 (2 hours). Specifying a value of 0 means that the KMS server will not close client connections due to inactivity.

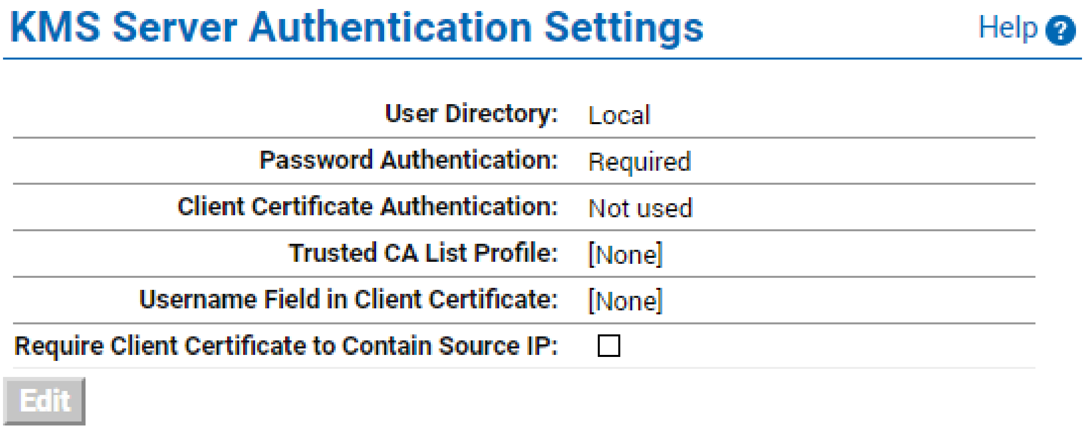
Component	***Description***
Allow Key and Policy Configuration Operations	When this feature is enabled, the KMS server allows the following actions: ▪ Key creation and deletion ▪ Key import ▪ Users with User Administration Permission can create, delete, and modify users and groups (available only through the ESKM XML interface.) When this feature is disabled, only authentication, cryptographic, and random number generation requests are available. By default, this feature is disabled. When using the multiple credentials feature, enabling this option allows users (and unauthenticated sessions) to perform the actions listed, without being subjected to the multiple credentials rule. ! This feature may pose a security loophole. You might allow this access for automated scripts, or you might disallow it to tighten security. ℹ Enabling this feature on a FIPS-compliant ESKM appliance takes it out of FIPS compliance — possibly in a manner that does not comply with FIPS standards. For information about disabling FIPS compliance, see FIPS compliance (p. 371).

Component	***Description***
Allow Key Export	When this feature is enabled, the KMS server allows key export. Enabling this feature on a FIPS-compliant ESKM appliance takes it out of FIPS compliance — possibly in a manner that does not comply with FIPS standards. For information about disabling FIPS compliance, see FIPS compliance (p. 371).
Edit	Click **Edit** to modify the KMS server settings.

6.12.2.2 KMS server authentication settings

KMS Server Authentication Settings allow you to specify whether and how clients authenticate to the KMS server.

The following figure shows KMS Server Authentication Settings.



KMS Server Authentication Settings

Help ?

User Directory:	Local
Password Authentication:	Required
Client Certificate Authentication:	Not used
Trusted CA List Profile:	[None]
Username Field in Client Certificate:	[None]
Require Client Certificate to Contain Source IP:	□

Figure 158 : KMS Server Authentication Settings

The following table describes the elements of KMS Server Authentication Settings.

Table 104: KMS Server Authentication Settings components

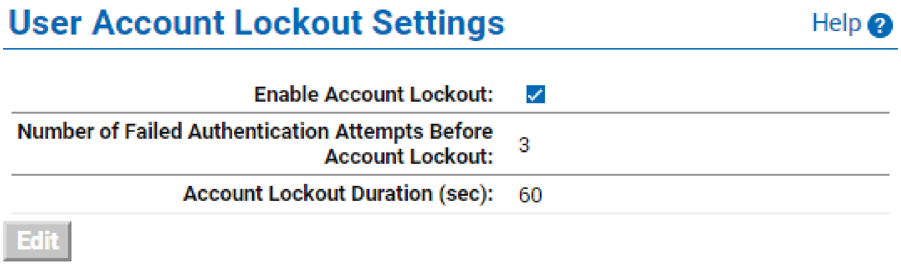
Component	***Description***
User Directory	This field determines whether the KMS server uses a local user and groups directory for the ESKM appliance or a central LDAP server. You can only choose one user directory at a time; if you choose LDAP, any local users or groups you define will be unavailable. ⚠ Selecting LDAP on a FIPS-compliant ESKM appliance takes it out of FIPS compliance — possibly in a manner that does not comply with FIPS standards. For information about disabling FIPS compliance, see FIPS compliance (p. 371).
Password Authentication	This field determines whether you require users to provide a username and password to access the KMS server. Doing so effectively disables global sessions. You have two choices for this field: ▪ Optional — no password authentication is required; global sessions are allowed; unauthenticated users can create global keys; all users can access global keys; only authenticated users can create and access non-global keys. ▪ Required — password authentication is required; global sessions are not allowed; only non-global keys can be created; authenticated users can access global and non-global keys.

Component	***Description***
Client Certificate Authentication	You have three options for client certificate authentication: ▪ Not used — clients do not have to provide a client certificate to authenticate to the KMS server. ▪ Used for SSL session only — clients must provide a certificate signed by a CA trusted by the ESKM appliance in order to establish an SSL/TLS connection. When you select this option, you must also select a Trusted CA List Profile. ▪ Used for SSL session and username — clients must provide a certificate signed by a CA trusted by the ESKM appliance in order to establish an SSL/TLS session with the KMS server; additionally, a username is derived from the client certificate. That username is the sole means of authentication if password authentication is optional and the client does not provide a username and password. If the client provides a username, the KMS server compares the username derived from the certificate against the username in the authentication request. If the usernames are the same and the password is valid, the user is authenticated. If the usernames are not the same, the connection is closed immediately. When you select this option, you must also select a Trusted CA List Profile, and you must choose the field from which the username is derived.
Trusted CA List Profile	This field allows you to select a profile to use to verify that client certificates are signed by a CA trusted by the ESKM appliance. This option is only valid if you require clients to provide a certificate to authenticate to the KMS server. For more information, see Trusted certificate authority list profiles (p. 350). The default Trusted CA List profile contains no CAs. You must either add CAs to the default profile or create a new profile and populate it with at least one trusted CA before the KMS server can authenticate client certificates.

Component	*Description*
Username Field in Client Certificate	This option allows you to specify the certificate field from which the username is derived. The username can be derived from the (user ID), (Common Name), (Surname), (Email address), (Email without domain), or (Organizational Unit) field. When you select the E_ND option, the KMS server matches against the data to the left of the @ symbol in the Email address in the certificate request. For example, if the certificate request contains the Email address User1@company.com, then the KMS server matches against User1.
Require Client Certificate to Contain Source IP	When this option is enabled, the KMS server expects that the client certificate presented by the client application has an IPv4 address in the subjectAltName field. The KMS server obtains the IPv4 address from the subjectAltName and compares that to the source IPv4 address of the client application. If the two IP addresses match, the KMS server authenticates the user. If the two IP addresses do not match, the KMS server closes the connection with the client.
Edit	Click **Edit** to modify the KMS server authentication settings.

6.12.2.3 User account lockout settings

User Account Lockout Settings manage an account lockout policy.



User Account Lockout Settings

Enable Account Lockout:	☑
Number of Failed Authentication Attempts Before Account Lockout:	3
Account Lockout Duration (sec):	60

Figure 159 : User Account Lockout Settings

The following table describes the components of **User Account Lockout Settings**.

Table 105: User Account Lockout Settings components

Component	***Description***
Enable Account Lockout	Indicates if the feature is enabled. When not enabled, users can make unlimited attempts to log in to an account.
Number of Failed Authentication Attempts Before Account Lockout	The number of failed login attempts permitted before the system temporarily forbids access to the account. After the last failed authentication attempt, the system ignores any subsequent login requests until the end of the account lockout duration, after which the counter is reset.
Account Lockout Duration (sec)	The period of time during which the account is not available.
Edit	Click **Edit** to modify the account lockout settings.

6.12.3 Health check overview

The Health Check feature allows you to configure client applications to check the availability of the ESKM appliance by sending it an HTTP request. The Health Check feature “listens” for requests on a port that you specify in **Health Check** of the **Key Management Services Configuration** page and **KMIP Health Check** of the **KMIP Server Configuration** page. When a request is made to the ESKM appliance on the port that the Health Check feature is monitoring, it responds with one of two HTTP response codes:

- 200 OK — ESKM Server is available
- 500 Internal Server Error — ESKM Server is unavailable

In addition to being able to configure client applications to check the availability of the ESKM appliance, you can also check the status by making an HTTP request from a web browser.

The Health Check feature responds to GET, POST, and HEAD requests, and it processes the entire request before responding. As such, Utimaco recommends that you send a small request.

- The recommended URL for accessing the KMS Health Check feature is:

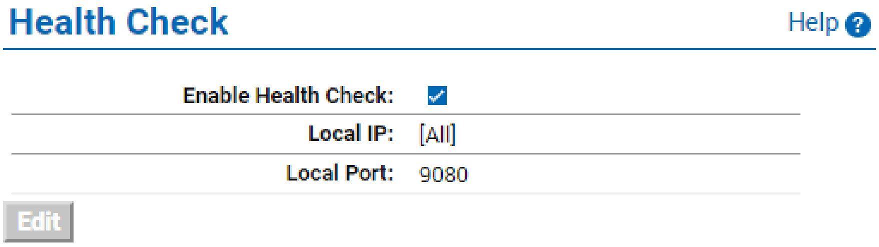
http://IPv4 address:9080/
...where IPv4 address refers to the IPv4 address of the ESKM appliance and 9080 is the port on which the Health Check feature is “listening” for requests.

- The recommended IPv6 URL for accessing the KMS Health Check feature is:
  http://[IPv6 address]:9080
  ...where [IPv6 address] refers to the IPv6 address of the ESKM appliance and 9080 is the port on which the KMS Health Check feature is “listening” for requests.
- The recommended URL for accessing the KMIP Health Check feature is:
  http://IPv4 address:9082/
  ...where IPv4 address refers to the IPv4 address of the ESKM appliance to check, and 9082 is the port on which the Health Check feature is listening for requests.
- The recommended IPv6 URL for accessing the KMIP Health Check feature is:
  http://[IPv6 address]:9082
  ...where [IPv6 address] refers to the IPv6 address of the ESKM appliance, and 9082 is the port on which the KMIP Health Check feature is listening for requests.

If the client is unable to connect to the ESKM appliance or if it is unable to respond to a request, you should assume that the ESKM appliance is down.

6.12.3.1 Health check

The **Health Check** option enables the KMS server health check feature, and sets the port and IP address.


Health Check

Enable Health Check:	☑
Local IP:	[All]
Local Port:	9080

Figure 160 : Health Check

The following table describes the components of **Health Check**.

Table 106: Health Check components

Component	***Description***
Enable Health Check	A check mark in this box indicates that the Health Check feature is enabled.
Local IP	In this field you specify the IPv4/IPv6 address on which the ESKM appliance will listen for health check requests. You can specify an individual IP address bound to the ESKM appliance or you can specify All. The drop-down list box consists of all IPv4 and IPv6 addresses bound to the ESKM appliance. ℹ Utimaco strongly recommends that you limit the Health Check feature to a specific IP address. If you have four IP addresses bound to the ESKM appliance, and you enable the Health Check feature for all IP addresses, then the ESKM "listens" for health check requests on four different IP addresses; whereas, if you specify a single IP address, the ESKM appliance "listens" for health check requests on only one IP address. This can greatly reduce system vulnerability to outside attacks.
Local Port	In this field you specify the port on which the ESKM appliance will listen for health check requests. The default value for this setting is 9080.
Edit	Click **Edit** to modify the health check settings.

6.13 KMIP server configuration

The **KMIP Server Configuration** page allows you to configure KMIP server settings, KMIP server authentication settings, client interoperability options, and the KMIP health check settings. This page contains the following KMIP server-related sections:

- KMIP server settings (p. 411)

- KMIP server authentication settings (p. 413)
- Interoperability (p. 414)
- KMIP health check (p. 418)

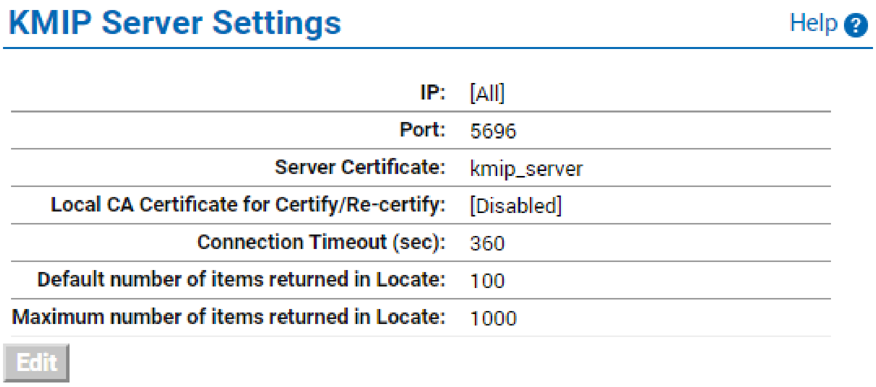
6.13.1 KMIP server settings

Use the **KMIP Server Settings** to set up the basic KMIP server settings.

⚠ The KMIP server requires the use of TLS.

⚠ Changing the KMIP server configuration causes the KMIP server service to restart, which takes it offline for a few seconds.

⚠ If the ESKM appliance is operating in FIPS-compliant mode, you must use a KMIP server certificate that complies with the FIPS requirements.



KMIP Server Settings

IP:	[All]
Port:	5696
Server Certificate:	kmip_server
Local CA Certificate for Certify/Re-certify:	[Disabled]
Connection Timeout (sec):	360
Default number of items returned in Locate:	100
Maximum number of items returned in Locate:	1000

Figure 161 : KMIP Server Settings

The following table describes the components of the **KMIP Server Settings**.

Table 107: KMIP Server Settings components

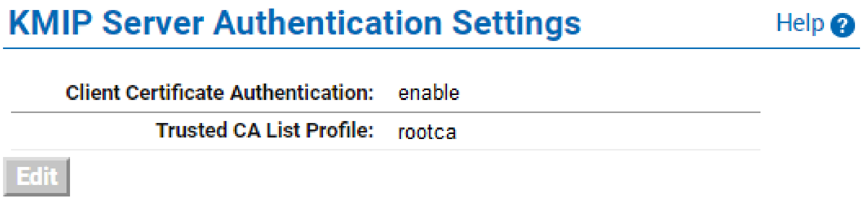
Component	***Description***
IP	This field specifies the IP address(es) which the KMIP server will use to listen for client requests. The drop-down list box consists of all IPv4 and IPv6 addresses bound to the ESKM appliance. ℹ Utimaco strongly recommends that you select a specific IP address instead of specifying [All]. If you have four IP addresses bound to the ESKM appliance, then the KMIP server "listens" for traffic on four different IP addresses; whereas, if you specify a single IP address, the KMIP server "listens" for traffic on only one IP address. This can greatly reduce system vulnerability to outside attacks.
Port	The port on which the KMIP server is listening for client requests. The default port is 5696; however, you can use any available port.
Server Certificate	The KMIP server requires the use of TLS. You must provide the certificate that will be used to authenticate the KMIP server to clients. For initial setup and demonstration purposes, you can use the default system-generated server certificate. ℹ It is strongly recommended that you create your own KMIP server certificate using the Web Administration Console and replace the default certificate with this certificate before production use.

Component	***Description***
Local CA Certificate for Certify/Re-certify	The KMIP CERTIFY and RE-CERTIFY operations allow certificate requests to be signed by a Local CA. Select the Local CA that you have previously created for this purpose. The default is disabled, which means the KMIP server will not allow CERTIFY or RE-CERTIFY operations. In addition, the CERTIFY and RE-CERTIFY permissions must be explicitly enabled for the group, see Per-user permission detail (p. 264).
Connection Timeout (sec)	The Connection Timeout value specifies in seconds how long client connections can remain idle before the KMIP server begins closing them. The default value is 360 (6 minutes); the maximum value is 7200 (2 hours). Specifying a value of 0 means that the KMIP server will not close client connections due to inactivity.
Default number of items returned in Locate	The default number of items returned in a LOCATE operation, if the number is not specified by the user. The default value is 100. The minimum value is 10 and the maximum value is 1,000.
Maximum number of items returned in Locate	The maximum number of items returned in a LOCATE operation. The default value is 1,000. Only this number of items will be returned, even if the user specifies a number greater than this limit. The minimum value is 1,000 and the maximum value is 10,000.
Edit	Click **Edit** to modify the KMIP server settings.

6.13.2 KMIP server authentication settings

KMIP Server Authentication Settings allow you to specify how clients authenticate to the KMIP server.

The following figure shows the **KMIP Server Authentication Settings**.



KMIP Server Authentication Settings

Client Certificate Authentication: enable

Trusted CA List Profile: rootca

Figure 162 : KMIP Server Authentication Settings

The following table describes the components of the **KMIP Server Authentication Settings**.

Table 108: KMIP Server Authentication Settings components

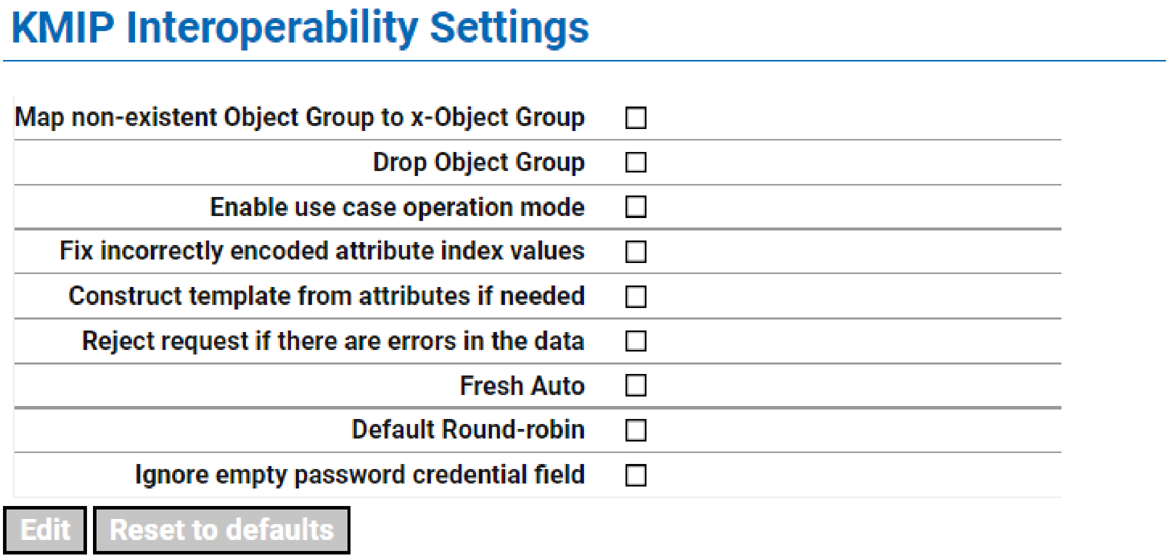
Component	***Description***
Client Certificate Authentication	You have two choices for this field: **Disable** — clients do not have to provide a client certificate to authenticate to the KMIP server. **Enable** — clients must provide a certificate signed by a CA trusted by the ESKM appliance to establish a TLS connection. When you select this option, you must also select a Trusted CA List Profile.
Trusted CA List Profile	This field allows you to select a profile that the ESKM appliance uses to verify that client certificates are signed by a CA trusted by the server. This option is only valid if you require clients to provide a certificate to authenticate to the KMIP server.
Edit	Click **Edit** to modify the KMIP Server Authentication Settings.

Changing the KMIP server authentication settings causes the KMIP server service to restart, which takes it offline for a few seconds.

6.13.3 Interoperability

Use **KMIP Interoperability Settings** to configure the KMIP server to be compatible with specific client options.

Changing the KMIP interoperability settings causes the KMIP server service to restart, which takes it offline for a few seconds.



KMIP Interoperability Settings

Map non-existent Object Group to x-Object Group	□
Drop Object Group	□
Enable use case operation mode	□
Fix incorrectly encoded attribute index values	□
Construct template from attributes if needed	□
Reject request if there are errors in the data	□
Fresh Auto	□
Default Round-robin	□
Ignore empty password credential field	□

Figure 163 : KMIP Interoperability Settings

The following table describes the components of the **KMIP Interoperability Settings**.

Table 109: KMIP Interoperability Settings components

Component	***Description***
Map non-existent Object Group to x-Object Group	Renames the incoming "Object Group" attribute to the "x-Object Group" custom attribute as a client-side attribute. The KMIP privilege model states that the KMIP client issuing the request must belong to a user group that has appropriate permissions to perform operations on the object group specified in the Object Group attribute of the incoming request. If the user does not have permission to create objects in the specified object group, or the object group does not exist, the standard KMIP behavior is to return an error. Enabling this option overrides the standard behavior. This setting enables support for clients which assume that any value can be provided in an Object Group attribute without requiring pre-configuration.

Component	***Description***
Drop Object Group	Drop (remove) any incoming "Object Group" attribute.
Enable use case operation mode	This option applies only to KMIP version 1.0 clients. It enables the handling of the Use-case: Register / Create / Get attributes / Destroy which is documented in http://docs.oasis-open.org/kmip/usecases/v1.0/kmip-usecases-1.0.pdf. When enabled, KMIP v1.0 client requests which insert the template name into the template will be re-written by the KMIP server, such that, the template name will be extracted from the template and inserted into a template-attribute.
Fix incorrectly encoded attribute index values	Correct an incorrectly encoded attribute index value. This option is required for interoperability with KMIP clients where the order of fields within the attribute structure is encoded incorrectly.
Construct template from attributes if needed	When performing a Register request and the managed object is a template and a template value has not been provided, the KMIP server will construct the template from the provided set of attributes. ⚠ In KMIP version1.2, all managed objects provided in the register request are explicitly required to provide a value structure.
Reject request if there are errors in the data	Reject the incoming KMIP request if there are errors in the data.

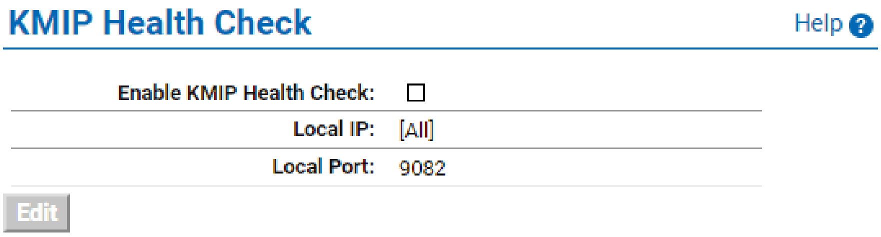
Component	*Description*
Fresh Auto	When performing a Locate operation and the result set returned is empty, and the client has provided the Object Group Member flag in the request, and the value specified for Object Group Member is "Group Member Fresh", the KMIP server will automatically create an AES256-bit key with Cryptographic Usage Mask set to "Encrypt | Decrypt". Certain contexts for usage proposed for KMIP, depend on either a pre-configured set of managed objects being allocated in a "pool" available to be added automatically or the creation of managed objects "on-the-fly" during a locate operation.
Default Round-robin	When performing a Locate operation and the result set returned is empty, and the client has provided the Object Group Member flag in the request, and the value specified for Object Group Member is "Group Member Default", the KMIP server will automatically create an AES256-bit key with Cryptographic Usage Mask set to "Encrypt | Decrypt". Certain contexts for usage proposed for KMIP, depend on cycling through a pre-configured set of managed objects. The KMIP server does not perform round-robin allocation and as an alternative it operates as though "Group Member Fresh" had been provided in the client request.
Ignore empty password credential field	Ignore the empty password credential field in the KMIP authentication request, if the certificate authentication is successful.
Edit	Click **Edit** to modify the KMIP Interoperability Settings.

Component	*Description*
Reset to defaults	Click **Reset to defaults** to return the KMIP Interoperability Settings to their factory default values.

6.13.4 KMIP health check

Use the **KMIP Health Check** to enable the health check feature, and set the port and IP address.

> Changing the KMIP health check configuration causes the KMIP server service to restart, which takes it offline for a few seconds.



KMIP Health Check

Enable KMIP Health Check: □

Local IP: [All]

Local Port: 9082

Figure 164 : KMIP Health Check

The following table describes the components of the **KMIP Health Check**.

Table 110: KMIP Health Check components

Component	*Description*
Enable KMIP Health Check	A check mark in this box indicates that the KMIP Health Check feature is enabled.

Component	*Description*
Local IP	In this field you specify the IPv4/IPv6 address on which you want to listen for health check requests. You can specify an individual IP address bound to the ESKM appliance or you can specify All. The drop-down list box consists of all IPv4 and IPv6 addresses bound to the ESKM appliance. Utimaco strongly recommends that you limit the KMIP Health Check feature to a specific IP address. If you have four IP addresses bound to the ESKM appliance, and you enable the KMIP Health Check feature for all IP addresses, then the ESKM appliance "listens" for health check requests on four different IP addresses; whereas, if you specify a single IP address, the ESKM appliance "listens" for health check requests on only one IP address. This can greatly reduce system vulnerability to outside attacks.
Local Port	In this field you specify the port on which you want the ESKM appliance to "listen" for health check requests. The default value for this setting is 9082.
Edit	Click **Edit** to modify the health check settings.

6.14 REST server configuration

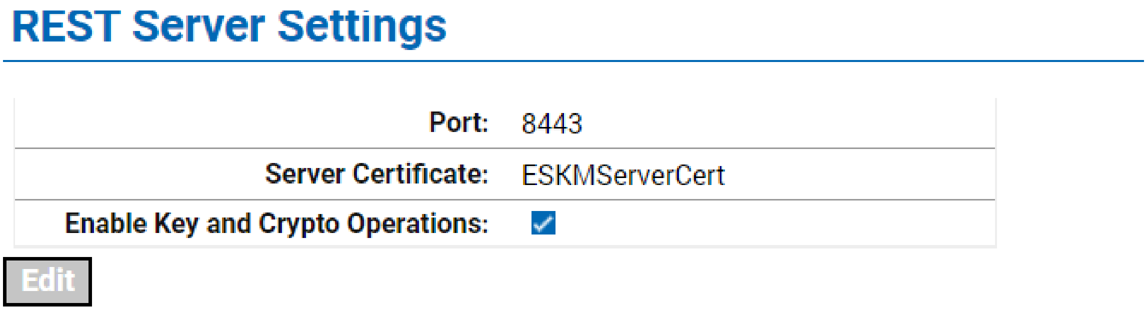
REST Server Settings

Use the **REST Server Settings** section in the **REST Configuration page** to configure the Rest Server.

> The REST server requires TLS.

Changing the REST server configuration causes the REST server service to restart, which takes it offline for a few seconds.

If the ESKM appliance is operating in FIPS-compliant mode, you must use a REST server certificate that complies with the FIPS requirements.



REST Server Settings

Port: 8443

Server Certificate: ESKMServerCert

Enable Key and Crypto Operations: ☑

Figure 165 : REST Configuration

The following table describes the components of the **REST Server Settings**.

Component	***Description***
Port	The Port used for communicating with the clients. The default port is 8443; however, you can use any available port.

Component	***Description***
Server Certificate	The REST server requires TLS. Select the **Server Certificate**, that will be used to protect the communication between the client and the REST interface, from the drop-down list. This will replace the default system-generated server certificate. ⚠ Once replaced, the user will not be able to change the Server Certificate back to the default system-generated certificate. ℹ Utimaco strongly recommends replacing the default system-generated certificate.
Enable Key and Crypto Operations	Check the **Enable Key and Crypto Operations** box to allow the client applications to do cryptographic key management using REST commands.
Edit	Click **Edit** to modify the REST server settings. ❗ Changing the configuration restarts the REST service which may take a while. Key and Crypto operations will not be available while the service restarts. Also, this configuration applies to the HSM Configuration UI.

6.15 Cluster configuration

Clustering enables multiple ESKM appliances in a distributed environment to synchronize and replicate configuration information, thus reducing administration overhead. This section contains the following information:

6.15.1 Clustering overview

A cluster enables multiple ESKM appliances to share configuration settings. Any changes made to these values on one cluster member are replicated to all members within the same cluster. This enables you to immediately share configuration changes with other ESKM appliances.

When a configuration operation is performed on one cluster member, the cluster feature determines if the operation should be replicated throughout the cluster. If so, the ESKM appliance immediately sends a similar operation request to every other member using the cluster port.

Utimaco recommends that ESKM appliances be configured in a cluster, for high availability and for disaster recovery scenarios. If an unclustered appliance fails, all data from the last backup to the point of failure is lost. Utimaco strongly recommends performing frequent backups.

All ESKM appliances in a cluster must be running the same major version of software. For example, it is not possible to cluster ESKM appliances with ESKM v4, ESKM v4.1, ESKM v4.2, and ESKM v4.1.0 appliances.

Adding multiple ESKM appliances to a cluster is a sequential process, make sure the first appliance is successfully added to the cluster before attempting to add the next one to the cluster

When a configuration operation is performed on one cluster member, the cluster feature determines if the operation should be replicated throughout the cluster. If so, the ESKM appliance immediately sends a similar operation request to every other member using the cluster port.

If the replication succeeds for an ESKM appliance, the operation is recorded in the System Log. If the replication fails, the appliance waits 60 seconds and tries again. If 1440 consecutive replications fail, the appliance records the failure in the System Log, and then sends an SNMP trap indicating that the cluster is out of sync. When an ESKM appliance is out of sync, an administrator must synchronize it manually.

The following configuration settings are replicated within a cluster:

- Keys
- Local Users and Groups
- KMS server
- KMIP server
- REST server
- NTP
- DNS
- SNMP
- Log Signing Certificate
- Local Certificate Authorities (CAs)
- Authorization Policies
- LDAP server
- SSL/TLS
- Administrators and Remote Administration
- IP Authorization
- Logging
- Service Startup
- Known CAs, CRLs, and Trusted CA List Profiles
- SSH Cryptographic Parameters

The following configuration settings can not be automatically replicated within a cluster:

- Network settings
- Date and Time
- Certificates (other than the Log Signing Certificate)
- SSH Public Key

Items not replicated by the clustering feature can be replicated manually using the Backup and Restore mechanism described in Backup and restore overview (p. 164).

6.15.1.1 Cluster key

A cluster uses a cluster key to authenticate members during replication and synchronization. When a cluster is created, this key is created automatically.

If a cluster member is stolen or the key is otherwise compromised, remove all ESKM appliances from the cluster (this will effectively delete the cluster). You can then create a new cluster and add members using the new key.

6.15.1.2 Cluster password

A cluster key is protected by a cluster password, which is provided by the administrator when creating the cluster. This password must be provided when ESKM appliances attempt to join a cluster, or when an administrator attempts to restore a cluster backup.

You can change the password by editing **Cluster Password** and **Confirm Cluster Password** on the Cluster Settings of the **Cluster Configuration** page for every ESKM appliance in the cluster. For example, you can do this if you forget the original password. However, to restore an automatic synchronization backup, you will need the cluster password used when the backup was created. Therefore, if you forget a cluster password, you can still maintain the cluster, but you will lose the backups that use the forgotten password.

6.15.1.3 Local certificate authority replication

The cluster feature allows you to replicate local certificate authorities (CAs) within a cluster. This includes the CA’s public and private keys, the list of signed certificates, and the list of revoked certificates.

During synchronization, an ESKM appliance will inherit a new list of local CAs from the cluster. The ESKM appliance’s old list of local CAs will be deleted. Should you need to access a deleted local CA, you can restore the automatic synchronization backup.

⚠ When upgrading from a previous version, local CA replication is disabled by default.

6.15.1.4 Automatic synchronization backups

Prior to each synchronization, and when an ESKM appliance joins a cluster, the ESKM appliance creates an automatic backup of the full list of items that can be replicated. Your synchronization backup may contain some configuration settings that you normally do not replicate.

These internal backups adhere to the following naming convention: `sync_autobackup_YYYYMMDD_HHMMSS` ...where YYYYMMDD is the year, month and day; HHMMSS is the hour, minute and second.

Synchronization backups can be viewed and restored on the **Backup and Restore** page. To restore a backup, you must provide the cluster password used, when the backup was created, in the **Backup Password** field.

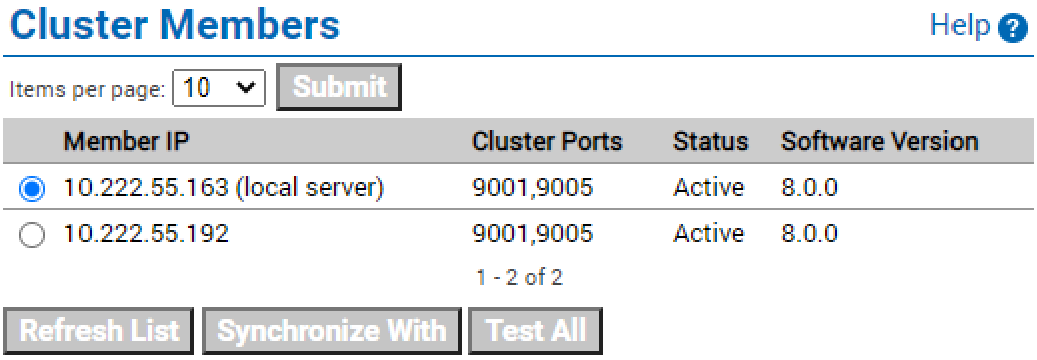
6.15.2 Cluster configuration page

The Cluster Configuration page allows you to create and manage clusters and cluster keys. This page contains the following sections:

- Cluster members (p. 425)
- Cluster settings (p. 427)
- Create cluster (p. 429)
- Join cluster (p. 431)

6.15.2.1 Cluster members

If the ESKM appliance is part of a cluster, **Cluster Members** displays all of the appliances that are members of that cluster, including the local ESKM appliance, and their status. If it is not part of a cluster, this section displays no information.



Cluster Members

Items per page: 10

	Member IP	Cluster Ports	Status	Software Version
●	10.222.55.163 (local server)	9001,9005	Active	8.0.0
○	10.222.55.192	9001,9005	Active	8.0.0

1 - 2 of 2

Figure 166 : Cluster Member

The following table describes the components of **Cluster Members**.

Table 111: Cluster Members components

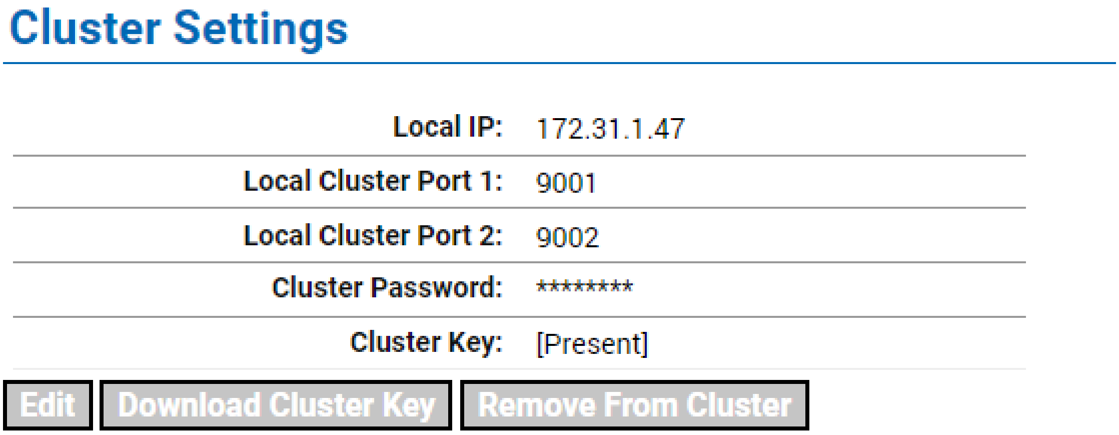
Component	***Description***
Member IP	The IPv4/IPv6 address of the member ESKM appliance.

Component	***Description***
Cluster Ports	The ports on which the ESKM appliance "listens" for cluster administration requests. ❗ The cluster port (default 9001) must be different from the KMS server port (default 9000) and the KMIP server port (default 5696).
Status	The appliance's current status. Valid values are: ▪ **Active**—The ESKM appliance is currently connected to the cluster. ▪ **Inactive**—The ESKM appliance is currently not connected to the cluster. ▪ **Pending Refresh**—The exact status of the ESKM appliance is unknown either because it is currently synchronizing with the cluster or because there was no direct communication with that ESKM appliance. View the system log for information about synchronizations. Click **Test All** to update the status of each cluster member.
Software Version	Displays the version of the software running on the ESKM appliance.
Refresh List	Click to update the list of ESKM appliance IP addresses that are members of this cluster. The local ESKM appliance will communicate with the IP address selected in the Server IP field. In addition, it will also update the remote unit ID list. This action does not update the status of each cluster member.

Component	***Description***
Synchronize With	Click **Synchronize With** to manually synchronize the local ESKM appliance with the selected cluster member. You must synchronize the local ESKM appliance with the cluster, if the ESKM appliance was unavailable during a replication process. ! Synchronizing the local ESKM appliance with the cluster overwrites the existing configuration, which may include keys. You can access the overwritten information using the synchronization backup. If you have any keys that only exist on the local ESKM appliance, you can use the backup and restore features to copy them to another appliance before synchronizing the local ESKM appliance.
Test All	Click **Test All** to verify the local ESKM appliance's connection to all the members of this cluster. This will update the Status for each cluster member.

6.15.2.2 Cluster settings

If this ESKM appliance is part of a cluster, **Cluster Settings** displays the IPv4/IPv6 address and port on which this appliance “listens” for cluster updates, and the status of the cluster key. If this appliance is not part of a cluster, this section displays no information.



Cluster Settings

Local IP:	172.31.1.47
Local Cluster Port 1:	9001
Local Cluster Port 2:	9002
Cluster Password:	********
Cluster Key:	[Present]

Figure 167 : Cluster Settings

The following table describes the components of **Cluster Settings**.

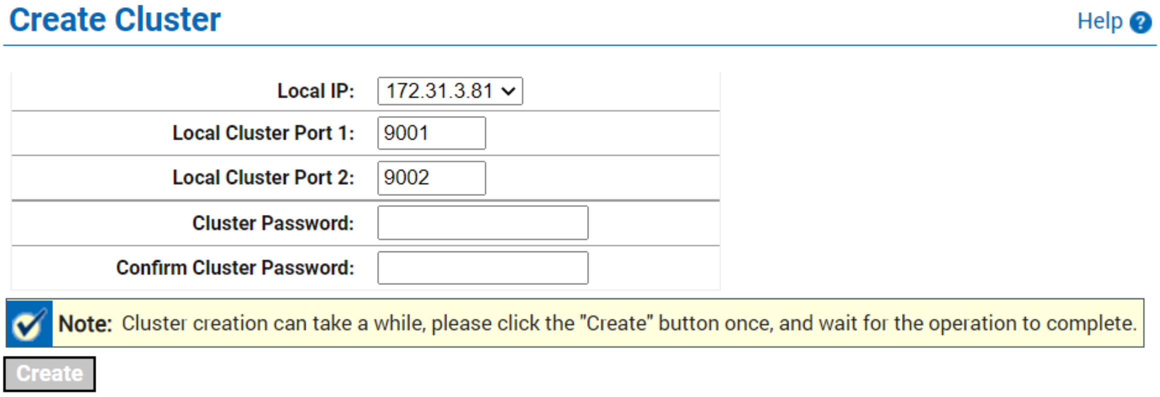
Table 112: Cluster Settings components

Component	***Description***
Local IP	The IPv4/IPv6 address of the current ESKM appliance. If the ESKM appliance has multiple network interfaces, the pull-down list shows all available interfaces.
Local Cluster Port 1	The port on which the ESKM appliance "listens" for cluster administration requests. ❗ The cluster port (default 9001) must be different from the KMS server port (default 9000) and the KMIP server port (default 5696).
Local Cluster Port 2	The port on which the ESKM appliance "listens" for key modifications. ❗ The cluster port (default 9002) must be different from the Local Cluster Port1 (default 9001), KMS server port (default 9000) and the KMIP server port (default 5696).
Cluster Password	The password for the cluster. You can change the cluster password by entering a new password while in edit mode.
Cluster Key	Click **Browse** to choose the downloaded cluster key file from your file system. This file must have been previously exported from a cluster member using **Download Cluster Key**.

Component	***Description***
Edit	Click **Edit** to edit the cluster settings. You can only change the local IP if your ESKM appliance has multiple interfaces. Click **Save** to save the changes.
Download Cluster Key	Click **Download Cluster Key** to save the key to your local file system. To join a cluster, an ESKM appliance must have a local copy of the cluster key. ⚠ It is recommended to download the cluster key to a new file instead of overwriting an existing file.
Remove From Cluster	Click **Remove From Cluster** to remove this ESKM appliance from the cluster. The ESKM appliance is removed from the list of cluster members. The cluster key is also removed from the local ESKM appliance. To delete an entire cluster, you must remove each ESKM appliance individually. If this is the last ESKM appliance in the cluster, the final cluster key is removed and all other downloaded cluster keys from this cluster become invalid. If you later create a new cluster with this ESKM appliance, a new cluster key is generated.

6.15.2.3 Create cluster

Use this to create a new cluster with the local ESKM appliance as its member. Local IP indicates the IPv4/IPv6 address for the current appliance. You can create only one cluster per appliance.



Local IP:	172.31.3.81
Local Cluster Port 1:	9001
Local Cluster Port 2:	9002
Cluster Password:	
Confirm Cluster Password:	

✓ **Note:** Cluster creation can take a while, please click the "Create" button once, and wait for the operation to complete.

Figure 168 : Create Cluster

The following table describes the components of **Create Cluster**.

Table 113: Create Cluster components

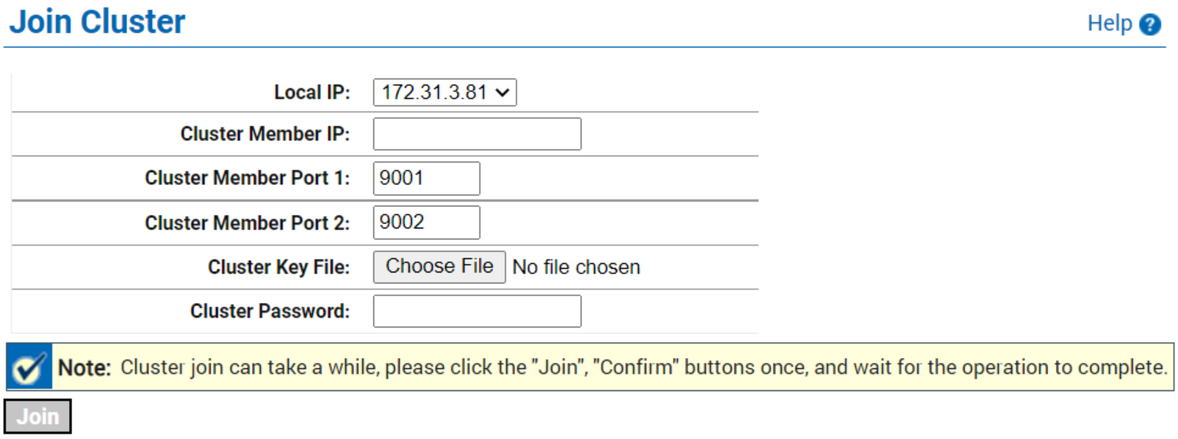
Component	***Description***
Local IP	The IPv4/IPv6 address of the current ESKM appliance. If it has multiple network interfaces, the pull-down list shows all available interfaces.
Local Cluster Port 1	The port on which the ESKM appliance "listens" for cluster administration requests. ❗ The cluster port (default 9001) must be different from the KMS server port (default 9000) and the KMIP server port (default 5696).

Component	***Description***
Local Cluster Port 2	The port on which the ESKM appliance "listens" for "database" based cluster administration requests. The cluster port (default 9002) must be different from the Local Cluster Port1 (default 9001), KMS server port (default 9000) and the KMIP server port (default 5696).
Cluster Password	The password for the cluster. The requirements for the cluster password depend on your Password Management Settings. For information about password requirements, see Password constraints (p. 491).
Confirm Cluster Password	Re-enter the cluster password.
Create	Click **Create** to create the cluster. A new cluster key is internally created, and this ESKM appliance appears in the Cluster Members list.

6.15.2.4 Join cluster

Use **Join Cluster** to add the ESKM appliance to an existing cluster. You must know the IPv4/IPv6 address and port number of another ESKM appliance in the cluster, and you need a local copy of the cluster key and the cluster password.

An ESKM appliance can be a member of only one cluster.



Join Cluster

Local IP:	172.31.3.81
Cluster Member IP:	
Cluster Member Port 1:	9001
Cluster Member Port 2:	9002
Cluster Key File:	Choose File No file chosen
Cluster Password:	

Note: Cluster join can take a while, please click the "Join", "Confirm" buttons once, and wait for the operation to complete.

Figure 169 : Join Cluster

The following table describes the components of **Join Cluster**.

Table 114: Join Cluster components

Component	***Description***
Local IP	The IPv4/IPv6 address of the current ESKM appliance. If the appliance has multiple network interfaces, the pull-down list shows all available interfaces.
Cluster Member IP	The IPv4/IPv6 address of another ESKM appliance in the cluster. ⚠ Cluster Member IP and Local IP should belong to the same IP address family.
Cluster Member Port 1	The port number of the ESKM appliance defined in the Cluster Member IP field.
Cluster Member Port 2	The port number used by the ESKM appliance defined in the existing Cluster Member IP field for replication of data.
Cluster Key File	Click **Browse** to locate the downloaded cluster key file in your file system. This file must have been previously exported from a cluster member using Cluster Settings.

Component	***Description***
Cluster Password	The password for the cluster.
Join	Click **Join** to join a cluster. ℹ You can only join a cluster of ESKM appliances that are running the same version of software and hardware. For example, you cannot join an ESKM appliance to a cluster of ESKM v4.2 appliances. After clicking this button you are asked to synchronize with the specified cluster member. Click **Confirm** to synchronize now, or if you want to synchronize manually later on. In either case, the local appliance becomes a member of the cluster. ❗ Synchronizing a local appliance with the cluster overwrites the existing configuration, which may include keys. You can access overwritten information using the synchronization backup. If you have any keys that only exist on the local appliance, you can use the backup and restore features to copy them to another appliance before synchronizing the local one. ⚠ If the cluster configuration specifies a KMIP server certificate that does not exist on the server joining the cluster, a warning message displays indicating that the KMIP server cannot start. To resolve this issue, create a KMIP server certificate with the same name as the KMIP server certificate specified in the cluster configuration.

6.16 Date and time configuration

The **Date and Time Configuration** page allows you to edit the date and time for the ESKM appliance, and configure the network time protocol settings. For more information, see also Date and time procedures (p. 122). This section contains the following information:

- Network time protocol overview (p. 434)
- Date and time configuration (p. 434)

6.16.1 Network time protocol overview

The Network Time Protocol (NTP) is a protocol by which computers on a network synchronize their clocks against an NTP server. The NTP implementation on the ESKM appliance allows you to synchronize a clock manually or at regular intervals.

When the ESKM appliance attempts to synchronize its clock against the NTP server (s), three outcomes are possible:

- If the clock on the ESKM appliance is successfully synchronized, and the difference between the time on the appliance and the NTP server (s) is less than 0.5 seconds, the time on the ESKM appliance is gradually slewed to the real time.
- If the clock on the ESKM appliance is successfully synchronized, and the difference between the time on the ESKM appliance and the NTP server (s) is greater than 0.5 seconds, the time on the ESKM appliance is immediately stepped to the real time. This event is recorded in the System Log.
- If an error prevented the ESKM appliance from synchronizing its clock, an error message is recorded in the System Log.

⚠ Synchronizing the time causes the KMS and KMIP servers to restart if the time change is greater than one minute. While restarting, the KMS and KMIP servers are unavailable for a brief time ranging from a few seconds to half a minute.

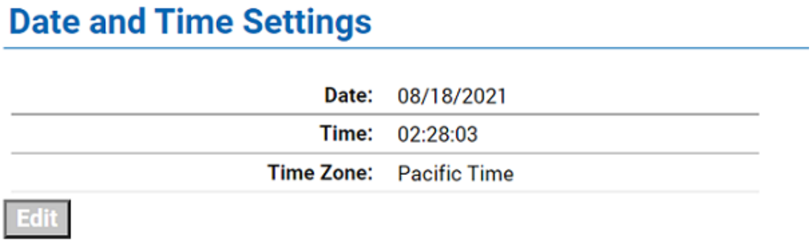
6.16.2 Date and time configuration

The **Date and Time Configuration** page allows you to view and edit the date and time settings on the ESKM appliance and manage NTP communications. This page contains the following sections:

- Date and time settings (p. 435)
- NTP settings (p. 436)

6.16.2.1 Date and time settings

Use the **Date and Time Settings** to view and edit the date, time, and time zone settings.



Date and Time Settings

Date:	08/18/2021
Time:	02:28:03
Time Zone:	Pacific Time

Figure 170 : Date and Time

The following table describes the components of **Date and Time Settings**.

Table 115: Date and Time Settings components

Component	***Description***
Date	Use the drop-down lists in this field to set the month, day, and year. ▪ **Month**: select a value in the range 1 – 12. ▪ **Date**: select a value in the range 1 – 31. ▪ **Year**: select a value in the range 2000 – 2035

Component	***Description***
Time	Use the drop-down lists in this field to define the current hour, minutes, and seconds. ▪ **Hour**: select a value in the range 0 – 23. ▪ **Minutes**: select a value in the range 0 – 59. ▪ **Seconds**: select a value in the range 0 – 59.
Time Zone	Use the drop-down list in this field to select a time zone.
Edit	Click **Edit** to modify the date and time settings. When the NTP feature is enabled, you cannot manually set the time or date on the ESKM appliance.

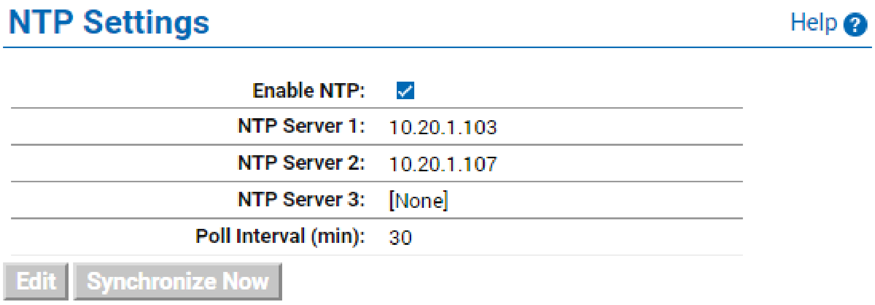
If you adjust the date and time settings forward, any log rotations scheduled for the skipped time period will not occur. You can rotate those logs manually using the Viewing logs (p. 531).

If you adjust the date and time settings backwards, any log rotations scheduled for the repeated time period will occur again.

Any change to Date and Time Settings causes the KMS and KMIP servers to restart, which takes the KMS and KMIP servers offline for a few seconds.

6.16.2.2 NTP settings

Use **NTP Settings** to enable NTP, establish the NTP servers, set a polling interval, and synchronize the ESKM appliance on demand.



NTP Settings

Enable NTP:	☑
NTP Server 1:	10.20.1.103
NTP Server 2:	10.20.1.107
NTP Server 3:	[None]
Poll Interval (min):	30

Figure 171 : NTP Settings

The following table describes the components of **NTP Settings**.

Table 116: NTP Settings components

Component	***Description***
Enable NTP	Click inside the box to enable automatic NTP synchronization on the ESKM appliance. A check mark inside the box denotes that the feature is enabled. When the NTP feature is enabled, the ESKM appliance synchronizes its time with the time on the NTP servers at the interval specified in the Poll Interval field. ⚠ When this feature is enabled, you cannot manually set the time or date on the ESKM appliance.
NTP Server	Specify the IPv4 address of the NTP server on the network. You can list as many as three NTP servers. When clocks are synchronized, the ESKM appliance polls all the NTP servers listed to determine the correct time.
Poll Interval (min)	The poll interval, expressed in minutes, is the length of time between consecutive polls. The minimum value for this field is 5; the maximum value is 10080 (one week). This value must be a multiple of 5. If you attempt to set a value that is not a multiple of 5, the ESKM appliance rounds down to the nearest multiple of 5.
Edit	Click **Edit** to modify the NTP settings.

Component	***Description***
Synchronize Now	Click **Synchronize Now** to synchronize the clock on the ESKM appliance immediately. ⚠ The **Synchronize Now** button synchronizes the clock on the ESKM appliance even when automatic NTP synchronization is not enabled.

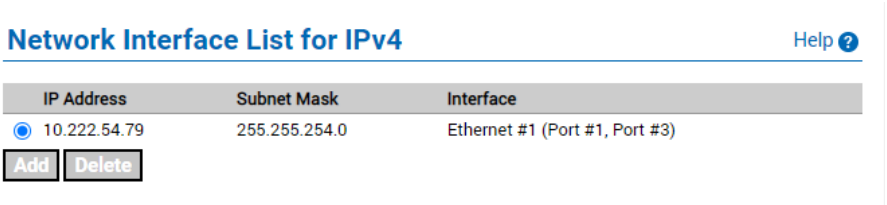
6.17 Network configuration

The Network Configuration page allows you to edit the network information for an ESKM appliance. This section contains the following information:

- Network interface list (p. 438)
- Gateways and routing configuration (p. 440)
- Hostname and DNS configuration (p. 444)
- Port speed configuration (p. 445)
- IP authorization configuration (p. 447)

6.17.1 Network interface list

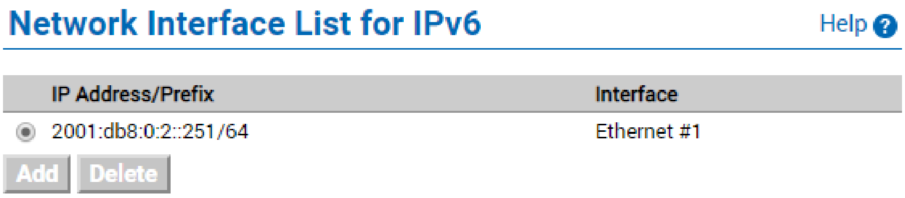
Network Interface settings are viewed and modified from the **Network Interfaces** tab on the **Network Configuration** page. Use the **Network Interface List** to view and set network interfaces for the ESKM appliance. Lists for both IPv4 and IPv6 are provided.



Network Interface List for IPv4

	IP Address	Subnet Mask	Interface
●	10.222.54.79	255.255.254.0	Ethernet #1 (Port #1, Port #3)

Figure 172 : IPv4 Network Interface List



Network Interface List for IPv6

IP Address/Prefix	Interface
● 2001:db8:0:2::251/64	Ethernet #1

Figure 173 : IPv6 Network Interface List

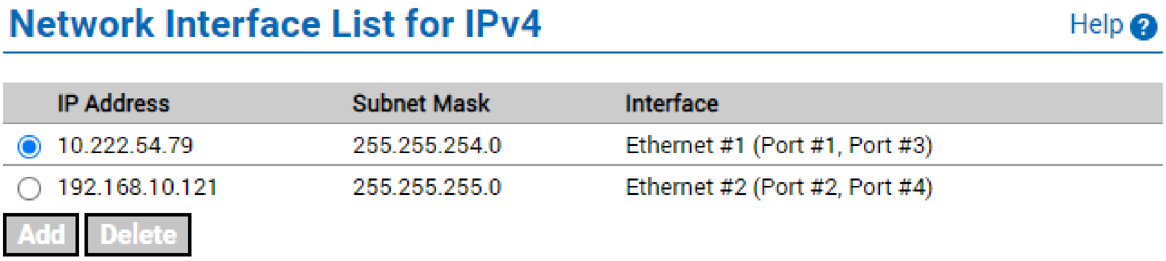
The following table describes the components of the **Network Interface List**.

Table 117: Network Interface List components

Component	***Description***
IP Address	Enter the IP Address to bind to the ESKM appliance. For IPv6, the default prefix is 64.
Subnet Mask	Enter the subnet mask associated with the IP address. This parameter only applies to IPv4.
Interface	The network interface to which the IP address is bound. Network Interfaces are located on the back of the ESKM appliance.
Add	Click **Add** to configure a new network interface.
Delete	Click **Delete** to remove a network interface configuration.

6.17.2 NIC Teaming

NIC teaming allows to combine physical NICs to a single logical interface. In ESKM, the teaming works in active-backup mode which avoids the single point of failure. The teaming feature is supported in all ESKM appliances (L2, L3 & L4). ESKMs are pre-configured with network Port #1, Port #3 teamed together and Port #2 and Port #4 teamed together. There is no provision provided to modify this configuration.



	IP Address	Subnet Mask	Interface
●	10.222.54.79	255.255.254.0	Ethernet #1 (Port #1, Port #3)
○	192.168.10.121	255.255.255.0	Ethernet #2 (Port #2, Port #4)

Figure 174 : NIC teaming IPv4

6.17.3 Gateways and routing configuration

The Network Configuration page contains the following gateway and routing-related sections:

- Default gateway list (p. 440)
- Static route list (p. 442)

6.17.3.1 Default gateway list

The **Default Gateway List** of the **Network Configuration** page provides a view of the default gateway which is used by the ESKM appliance for routing. A default gateway is used to identify the IPv4/IPv6 address to which all packets destined for a remote network are routed.

> IPv6 must be enabled before an IPv6 default gateway can be configured. To enable IPv6, see ipv6 enable (p. 693).

When the ESKM appliance is configured to support multiple interfaces, the interface that has been configured with the default gateway will handle outgoing connections.

> The same IP address cannot be configured as the default gateway for two different interfaces.

The following table describes the components of the **Default Gateway List**.

Table 118: Default Gateway List components

Component	***Description***
Interface	The network interface to which the default gateway is associated.
Default Gateway	The IPv4/IPv6 address associated with the appliance that routes all packets destined for a remote host. A blank Default Gateway indicates that no default gateway exists. ⚠ The Default Gateway address cannot be a broadcast or network address as determined by the IP addresses on the system.
Used for Outgoing Connections	Displays if the interface is used for outgoing connections initiated by the ESKM appliance. You can select one interface only. If this gateway fails for any reason, all outgoing connections initiated by the ESKM appliance also fail.
Edit	Click **Edit** to modify the default gateway settings.
Clear Gateway	Click **Clear Gateway** to remove a default gateway.
Use for Outgoing Connections	Click **Use for Outgoing Connections** to send outgoing packets through the selected interface.

6.17.3.2 Examples of default gateway configurations

The following examples illustrate the possible configurations. In each example, Ethernet #1 is bound to 172.17.7.16 and Ethernet #2 is bound to 10.20.41.16.

Example 1

```
Interface Default Gateway    Used for Outgoing Connections
------------------------------------------------------------------_
Ethernet 172.17.7.1          yes
#1
```

```
Ethernet none               no
#2
```

All responses to incoming packets leave from 172.17.7.1 — except the responses to incoming packets from the 10.20.41.0 addresses (the local subnet of Ethernet #2). Those responses leave from the Ethernet #2 interface. All connections initiated by the ESKM appliance leave from 172.17.7.1.

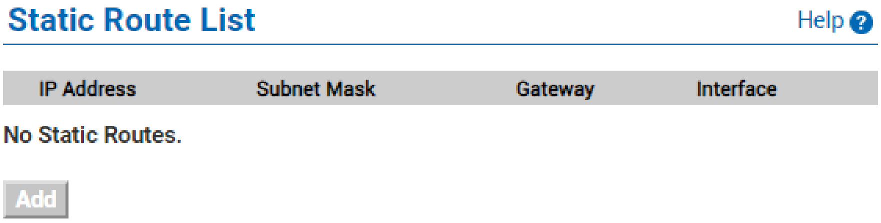
Example 2

```
Interface Default Gateway  Used for Outgoing Connections
-----------------------------------------------------------------_
Ethernet none             no
#1
Ethernet 10.20.41.1       yes
#2
```

All responses to incoming packets leave from 10.20.41.1 - except the responses to incoming packets from the 172.17.7.0 addresses (the local subnet of Ethernet #1). Those responses leave from the Ethernet #1 interface. All connections initiated by the ESKM appliance leave from 10.20.41.1.

6.17.3.3 Static route list

The Static Route features allows you to explicitly specify a route from the ESKM appliance to another network device. This route is stored in the routing table on the ESKM appliance.



Static Route List

IP Address	Subnet Mask	Gateway	Interface

No Static Routes.

Figure 175 : Static Route List

The following table describes the components of the **Static Route List**.

Table 119: Static Route List components

Component	***Description***
IP Address	The address that you are trying to reach with this route. Valid values are IPv4/IPv6 or network addresses "matching" the specified Subnet Mask.
Subnet Mask	The network mask associated with the IP Address/Network needed to identify the destination. Valid values are any subnet mask address.
Gateway	The gateway used to reach the destination. A static route that does exclude a gateway indicates that the destination address can be reached on the local subnet for the specified physical interface. Values for the Gateway field are constrained by the following: ▪ If you specify a value for the Gateway field, you must specify an IPv4/IPv6 address. ▪ The gateway must be reachable based on the network routes created by the addition of an IPv4/IPv6 address to the system. ▪ The gateway address cannot be a broadcast or network address as determined by the IPv4/IPv6 addresses on the system or the static route being added. ▪ The gateway must not be used by any other route on a different physical interface.
Interface	The physical interface on the ESKM appliance used to reach the destination.
Edit	Click **Edit** to modify the static route list.
Add	Click **Add** to add a new static route.
Delete	Click **Delete** to remove a static route.

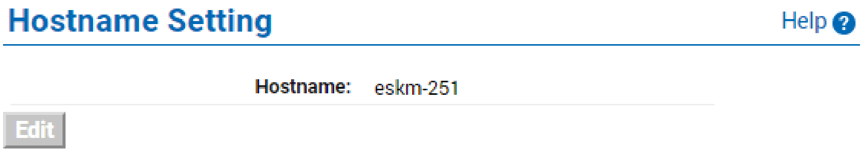
6.17.4 Hostname and DNS configuration

The Network Configuration page contains the following hostname and DNS-related sections:

- Hostname setting (p. 444)
- DNS server list (p. 444)

6.17.4.1 Hostname setting

The hostname, which identifies each ESKM appliance in a network, is the unique name assigned to an ESKM appliance.



Hostname: eskm-251

Figure 176 : Hostname Setting

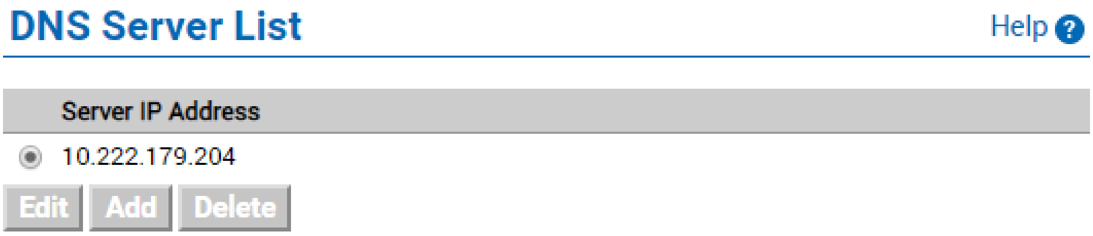
The following table describes the components of the **Hostname Setting**.

Table 120: Hostname Setting components

Component	***Description***
Hostname	The hostname is the name used to identify the ESKM appliance on the network. It is originally assigned during initial configuration. This string cannot be longer than 64 characters.
Edit	Click **Edit** to modify the Hostname field.

6.17.4.2 DNS server list

Domain Name Service (DNS) settings are viewed and modified on the **DNS Server List** on the **Hostname & DNS** tab of the **Network Configuration** page (**Device > Network > Hostname & DNS**). From the **DNS Server List**, the user can opt to review the server list or use the buttons to prioritize, add, modify, or remove a DNS server.



DNS Server List

Server IP Address

● 10.222.179.204

Figure 177 : DNS Server List

Changes to the DNS Server List causes the ESKM appliance to restart, which takes the ESKM appliance offline for a few minutes.

The following table describes the components of the **DNS Server List**.

Table 121: DNS Server List components

Components	***Description***
Up, Down	Use the **Up** and **Down** buttons to specify the order in which the DNS servers are to be queried by the ESKM appliance.
Edit	Click **Edit** to modify an existing domain name server.
Add	Click **Add** to add a domain name server.
Delete	Click **Delete** to remove a domain name server.

6.17.5 Port speed configuration

The **Network Configuration** page contains the following Network interface port speed/duplex information.

The ESKM appliance can auto-negotiate a port speed and duplex setting when communicating with other network devices. In some network configurations, however, you might want to force the ESKM appliance to use a particular port speed and duplex setting. The **Port Speed** tab on the **Network Configuration** page allows you to choose between Auto-Negotiate and a variety of port speed and duplex settings.

The **Edit** option is not available in the “virtual Enterprise Secure Key Manager”

The Port Speed/Duplex setting is an advanced feature that should only be used when you are certain of the port speed and duplex settings of the network device communicating with the ESKM appliance. Potential performance degrade can result if these settings do not match. Utimaco recommends that you leave the port speed and duplex setting on the ESKM appliance at Auto-Negotiate unless you know the settings of the network device it is communicating with.

When a switch forces a port speed and the ESKM appliance is set to Auto-Negotiate, the ESKM appliance defaults to Half Duplex. As such, when you force Full Duplex on the switch and leave it set to Auto-Negotiate, you might notice that the ESKM appliance is unable to negotiate a usable connection with other network devices.

The following table describes the components of **Network Interface Port Speed/Duplex**.

Table 122: Network Interface Port Speed/Duplex components

Components	***Description***
Ethernet Port #1/ Ethernet Port #2/ Ethernet Port #3/ Ethernet Port #4	Select from the following options: ▪ Auto-Negotiate ▪ 100 Mbps/Full Duplex ▪ 1 Gbps/Full Duplex ▪ 10 Gbps/Full Duplex
Edit	Click **Edit** to modify the Network Interface Port Speed/Duplex settings

To avoid single point of failure, Port #1 and Port #3 are teamed together and Port #2 and Port #4 are teamed together.

6.17.6 IP authorization configuration

The IP Authorization feature allows you to specify which IP addresses are permitted to connect to the ESKM appliance and which services those IP addresses may access. Once enabled, it examines each network packet sent to the protected TCP ports. Authorized packets are processed; unauthorized packets are dropped and logged. You can view the unauthorized packets in the system log.

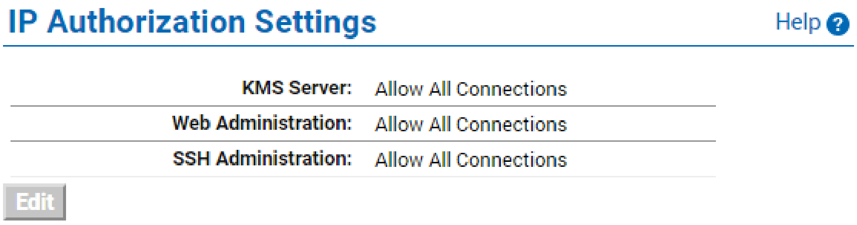
The REST server and KMIP server does not support the IP Authorization feature.

The **Network Configuration** page contains the following IP Authorization-related sections:

- IP authorization settings (p. 447)
- Allowed client IP addresses (p. 448)

6.17.6.1 IP authorization settings

IP Authorization settings are viewed and modified from the **IP Authorization** tab on the **Network Configuration** page. Use **IP Authorization Settings** to view and set these settings for the ESKM appliance.



IP Authorization Settings

KMS Server:	Allow All Connections
Web Administration:	Allow All Connections
SSH Administration:	Allow All Connections

Figure 178 : IP Authorization Settings

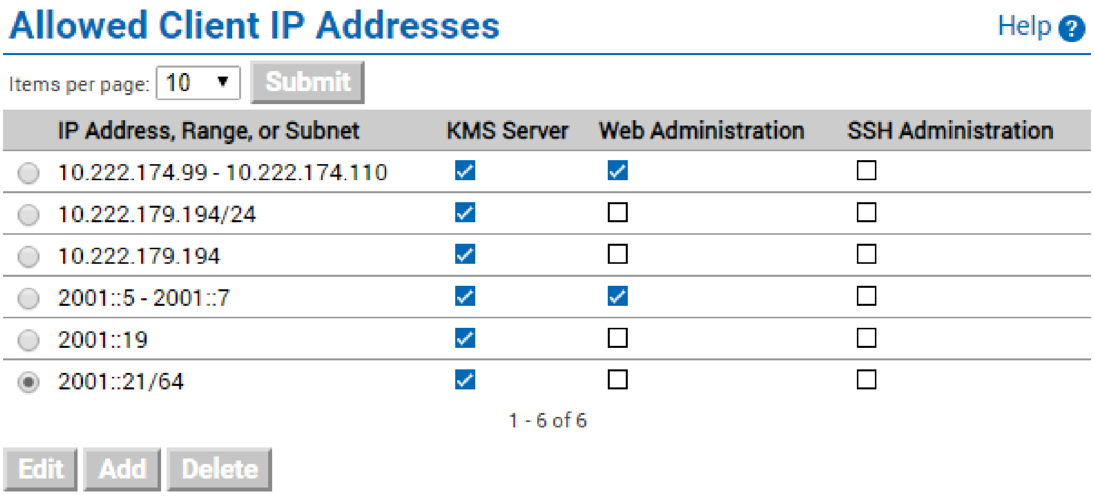
The following table describes the components of **IP Authorization Settings**.

Table 123: IP Authorization Settings components

Components	***Description***
KMS Server	You can grant all IPs access to the server, or you can grant access to the IPs listed in **Allowed Client IP Addresses**. Only IPv4 addresses are supported.
Web Administration	You can grant all IPs access to the Management Console, or you can grant access to the IPs listed in **Allowed Client IP Addresses.** Both IPv4 and IPv6 addresses are supported.
SSH Administration	You can grant all IPs access to the CLI, or you can grant access to the IPs listed in **Allowed Client IP Addresses**.
Edit	Click **Edit** to modify the IP authorization settings.

6.17.6.2 Allowed client IP addresses

Allowed client IP addresses are viewed and modified from the **IP Authorization** tab on the **Network Configuration** page. Use the **Allowed Client IP Addresses** to assign access permissions to individual IP addresses, ranges of IPs, or subnets. You can grant access to various features but you cannot explicitly deny access to a specific client. In the event that a specific IP is listed individually and as part of a group, that IP address acquires the sum of listed permissions.



Allowed Client IP Addresses

Items per page: 10 ▼

	IP Address, Range, or Subnet	KMS Server	Web Administration	SSH Administration
○	10.222.174.99 - 10.222.174.110	☑	☑	□
○	10.222.179.194/24	☑	□	□
○	10.222.179.194	☑	□	□
○	2001::5 - 2001::7	☑	☑	□
○	2001::19	☑	□	□
●	2001::21/64	☑	□	□

1 - 6 of 6

Figure 179 : Allowed Client IP Addresses

Utimaco recommends that you configure IPv4/IPv6 address on all the ESKM nodes in a cluster, before enabling the corresponding IP authorization entries.

The following table describes the components of **Allowed Client IP Addresses**.

Table 124: Allowed Client IP Addresses components

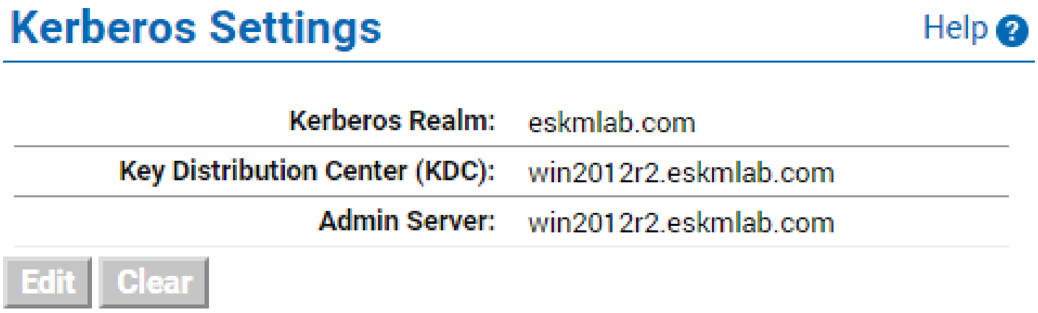
Components	***Description***
IP Address, Range or Subnet	Enter IP addresses in the following formats: ▪ Single IP address (192.168.1.60 or 2001::21) ▪ A range of IPs (192.168.1.70 - 192.168.1.80 or 2001::21-2001::31) ▪ An IP and subnet (192.168.100.0/255.255.255.0) ▪ An IP and subnet in CIDR format (192.168.200.0/24 or 2001::21/64)
KMS Server	Select to grant access to the KMS Server.
Web Administration	Select to grant access to the Management Console.

Components	***Description***
SSH Administration	Select to grant access to the CLI.
Edit	Click **Edit** to modify an existing IPv4/IPv6 address entry.
Add	Click **Add** to add a new IPv4/IPv6 address.
Delete	Click **Delete** to remove an IPv4/IPv6 address.

⚠ When updating this feature from the Management Console, the ESKM appliance ensures that the current administrator IP address maintains its web administration permissions. When updating this feature from the CLI, the active SSH administration permissions remain intact.

6.18 Kerberos configuration

Kerberos is a network authentication protocol which uses symmetric-key cryptography to authenticate users to network services, which means passwords are never actually sent over the network. Instead of authenticating each user to each network service, Kerberos uses symmetric encryption and a trusted third party, to authenticate users to a suite of network services. When a user authenticates to the KDC, the KDC sends a ticket specific to that session back to the user's machine, and services look for the ticket on the user's machine rather than requiring the user to authenticate using a password.



Kerberos Settings

Kerberos Realm:	eskmlab.com
Key Distribution Center (KDC):	win2012r2.eskmlab.com
Admin Server:	win2012r2.eskmlab.com

Figure 180 : Kerberos Settings

The following table describes the components of **Kerberos Settings**.

Table 125: Allowed Client IP Addresses components

Components	***Description***
Kerberos Realm	This is the domain, over which a Kerberos authentication server has the authority to authenticate an user. Realm names can consist of any ASCII string. Usually, the realm name is the same as your DNS domain name. Example:eskmlab.com
Key Distribution Center (KDC)	Key Distribution Centre is the service, that is responsible for issuing the kerberos ticket. KDC name can consist of any ASCII string. Usually KDC is same as your hostname of the server. Example:win2012r2.eskmlab.com.
Admin Server	Identifies the host, where the administrator service is running. Admin Server name can consist of any ASCII string. Usually, admin server is the same as your hostname of the server. Example:win2012r2.eskmlab.com.
Edit	Click **Edit** to modify the Kerberos configuration settings.
Clear	Click **Clear** to clear the Kerberos configuration settings.

You must add DNS server, when Kerberos is configured to use Windows share for Backup/Restore files.

6.19 HSM window

This section is relevant only to the vESKM and ESKM L2 appliance.

Login to Management Console as an administrator and navigate to **Device > Device Configuration > HSM** to get the new HSM window.

6.20 SNMP

The Simple Network Management Protocol (SNMP) allows you to manage network performance, and also find and solve network problems as they arise. You can configure an ESKM appliance to provide SNMP data from the **SNMP Configuration** page. You can access the **SNMP Configuration** page from the navigation bar by selecting **SNMP** in the **Device Configuration** tab. This section contains the following topics:

6.20.1 SNMP overview

The SNMP protocol enables network and system administrators to remotely monitor devices on the network, such as switches, routers, proxies, and hubs. This protocol relies on three main concepts: network management station (NMS), agent, and Management Information Base (MIB).

- The **NMS** is configured on a network node and runs SNMP management software.
- **Agents** run on network devices that are being monitored by the NMS.
- The **MIB** defines the kind of information that can be exchanged between the agent and the NMS.

SNMP is a request-response protocol used to communicate management information between an NMS and an agent. SNMP trap messages, sent from agents to managers, might indicate a warning or error condition or otherwise notify the manager about the agent's state. There are three versions of SNMP: SNMPv1, SNMPv2, and SNMPv3. The ESKM appliance supports all three versions of SNMP.

> There are many different versions of SNMPv2. The ESKM appliance supports SNMPv2c. For the sake of simplicity, throughout the rest of this document SNMPv2c is referred to simply as SNMPv2.

SNMPv1/v2 rely on the concept of a community to provide a low level of security for communications between the NMS and agent. In an ESKM SNMPv1/v2 deployment, each SNMP request packet includes a community name, which is similar to a password and is associated with a certain MIB access level. When the ESKM appliance receives a request, the agent looks for the community name in its table. If the name is found and the source IP of the sender is in the access list for the community, the request is accepted and the MIB information is sent. If the name is not found or the source IP address is not in the access list, the request is denied.

Because SNMPv1/v2 cannot authenticate the source of a management message or provide encryption, it is possible for unauthorized users to perform SNMP network management functions. Likewise, it is also possible for unauthorized users to eavesdrop on management information as it passes from agents to the NMS.

SNMPv3 incorporated all the capabilities of SNMPv1/v2, and introduced the concept of a Userbased Security Model (USM), which consists of two important services: authentication and privacy. Additionally, SNMPv3 enhanced the existing View Access Control Model (VACM).

6.20.1.1 Authentication

The authentication piece of the USM ensures that a message was sent by the agent or NMS whose identifier appears as the source in the message header. Authentication also ensures that the message was not altered, artificially delayed, or replayed.

In SNMPv3, the agent and NMS share a key that is based on the username and password supplied when the username is created. The sender provides a means for authentication to the receiver by including a MAC with the SNMPv3 message it is sending. When the receiver gets the message, it uses the same secret key to recompute the MAC. If the receiver’s version of the code matches the value appended to the incoming message, then the receiver knows that the message originated from an authorized sender, and that the message was not altered in transit.

6.20.1.2 Privacy

The privacy piece of the USM allows managers and agents to encrypt messages to prevent eavesdropping. As is the case with authentication in SNMPv3, both the NMS and the agent must share a secret key. When an NMS and agent are configured for privacy, all traffic between them is encrypted. Both the AES and DES algorithms are supported. The sender encrypts all messages with the specified algorithm and its secret key, and sends the message to the receiver, who decrypts it using the same algorithm and the same secret key.

6.20.1.3 Access control

Access control in SNMP makes it possible for agents to provide different levels of MIB access to different managers. You can restrict access by allowing one NMS to view only standard MIBs and another NMS to view both standard MIBs and Enterprise MIBs.

6.20.1.4 SNMP concepts

Before discussing how SNMP is configured on the ESKM appliance, it is important that a few terms are understood.

Management Station: A network management station (NMS) is a node on the network that runs SNMP manager software. The NMS monitors network devices by polling agents, sending responses to inform notifications sent by agents, and listening for unsolicited, asynchronous (UDP) messages from the agents.

Agent: An agent is a device on the network that is running the SNMP agent software. The agent is able to communicate with the NMS to provide information about security, performance, system health, statistics, and so on.

Entity: An SNMP entity simply refers to an agent or an NMS. Both the agent and the NMS consist of a variety of applications and services; however, for the sake of simplicity, this documentation does not attempt to describe all the component parts.

Engine: Core SNMP software around which you can build an agent or NMS. For the sake of simplicity, Engine and Entity are used interchangeably.

Engine ID: Unique identifier for an SNMP entity.

Community: A community, also referred to as a community string, is used by the agent when it is communicating with an NMS running SNMPv1/v2. A community functions more like a password than what its name suggests. In combination with the IP address/ subnet mask specified for a community, the community name determines from where the ESKM appliance accepts a request for information. A community should be defined on both the agent and the NMS.

Username: In combination with the security and authentication pieces of the Userbased Security Model (USM), the username determines from where the agent accepts SNMP requests. Also called a security name, the username is used by the agent when communicating with an NMS running SNMPv3. A username always has an associated security level and access level. Additionally, you can specify an authorization password. Like a community name, a username should also be defined on the agent and the NMS.

Notification: Notification is a generic term that refers to Traps and Informs — messages that an agent might send to an NMS. Traps are simply data packets sent out by the agent that require no acknowledgment from the NMS. Informs are similar to traps, but they require acknowledgment from the NMS.

MIB: MIB is the acronym for Management Information Base. MIBs define what kind of information can be exchanged between the agent and the NMS. MIBs can be either Standard or Enterprise. Standard MIBs are common to all SNMP systems, whereas Enterprise MIBs are particular to the ESKM appliance hardware/virtual appliance and software.

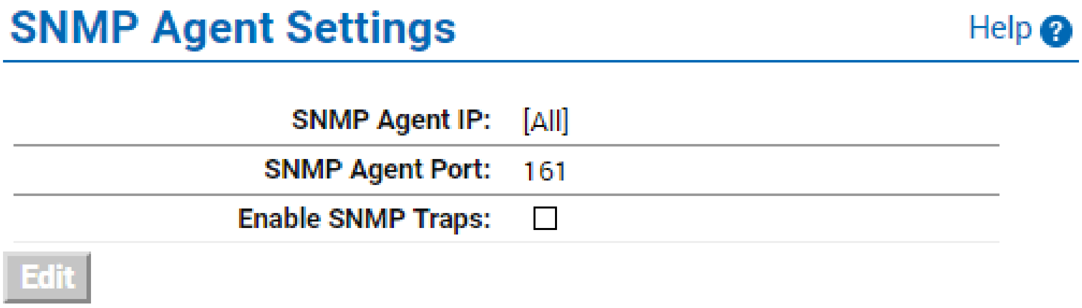
6.20.2 SNMP configuration

The SNMP Configuration page allows you to configure the ESKM appliance's SNMP agent, which is capable of communicating with management stations that run SNMPv1, SNMPv2, and SNMPv3. There is only one ESKM SNMP agent, whereas there might be multiple management stations. This page contains the following sections:

- SNMP agent settings (p. 455) — Changes to SNMP Agent Settings apply to all management stations, usernames and communities defined on the ESKM appliance.
- SNMPv1/SNMPv2 community list (p. 456) — This section of the SNMP configuration page is where you define from which SNMPv1/v2 management stations the ESKM appliance receives SNMP MIB requests.
- SNMPv3 username list (p. 459)— The SNMPv3 Username List defines from which SNMPv3 management stations the ESKM appliance receives SNMP MIB requests. Because SNMPv3 offers authentication and privacy, there is more to configure when creating an SNMPv3 Username as opposed to a community.
- SNMP management station list (p. 462) — This section lists the management stations defined on the ESKM appliance.
- Create SNMP management station (p. 467) — This is where you configure outbound SNMP traffic on the ESKM appliance. Whereas creating usernames and communities is particular to a specific version of SNMP, management stations are common to all three version of SNMP. This section is where you define the management stations that the agent sends traps to.

6.20.2.1 SNMP agent settings

SNMP Agent Settings controls whether SNMP traps are enabled on the ESKM appliance, the IP address on which SNMP in enabled, and the port on which the ESKM appliance "listens" for requests from the NMS. Changes to **SNMP Agent Settings** apply to all other SNMP settings defined on the ESKM appliance.



SNMP Agent Settings

SNMP Agent IP: [All]

SNMP Agent Port: 161

Enable SNMP Traps: □

Figure 181 : SNMP Agent Settings

The following table describes the components of the **SNMP Agent Settings**.

Table 126: SNMP Agent Settings components

Component	***Description***
SNMP Agent IP	This field specifies the IPv4/IPv6 address on which SNMP is enabled. You can select "All" or an individual IP address. Utimaco recommends that you specify an individual IP address.
SNMP Agent Port	This value specifies the port on which the ESKM appliance "listens" to requests from the NMS. The default is 161.
Enable SNMP Traps	By default, the ESKM appliance does not send SNMP traps. To enable the sending of SNMP traps, check the Enable SNMP Traps box. The SNMP service must be started for traps to be sent.
Edit	Click Edit to modify the SNMP agent settings.

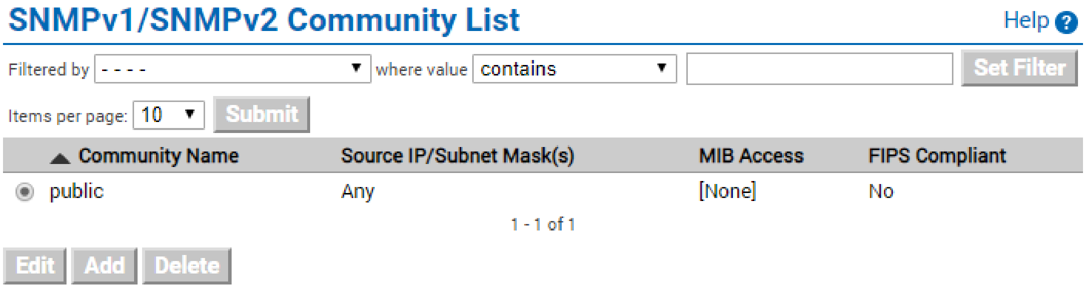
6.20.2.2 SNMPv1/SNMPv2 community list

As the name suggests, the SNMPv1/SNMPv2 Community list is used to configure the agent to communicate with an NMS running either SNMPv1 or SNMPv2 software. You can think of this section of the Communities and Usernames tab as the place where you define from which SNMPv1/v2 management stations the ESKM appliance receives SNMP MIB requests. Use this section to add, edit, or delete a community on the ESKM appliance.

> ⚠ If you are configuring the agent to communicate with an NMS running SNMPv3 software, you can disregard this section.

When creating a community on the ESKM appliance, it is a good security practice to secure agents by filtering all SNMP requests by community name and source IP address. This filtering restricts where SNMP requests are allowed to come from, and greatly reduces system vulnerability to outside attacks. In addition, it is a good idea to use community names other than “public” and “private,” as these names are very commonly used.

> ⚠ For security purposes, the SNMP community name is read-only. The set command is not allowed on the SNMP agent.



SNMPv1/SNMPv2 Community List

Filtered by: - - - - where value: contains

Items per page: 10

	Community Name	Source IP/Subnet Mask(s)	MIB Access	FIPS Compliant
○	public	Any	[None]	No

1 - 1 of 1

Figure 182 : SNMPv1/SNMPv2 Community List

The following table describes the components of the **SNMPv1/SNMPv2 Community List.**

Table 127: SNMPv1/SNMPv2 Community List components

Component	***Description***
Community Name	Community names can contain only alphanumeric characters and punctuation marks and they cannot contain non-printing characters and whitespaces. Community names cannot exceed 64 characters.

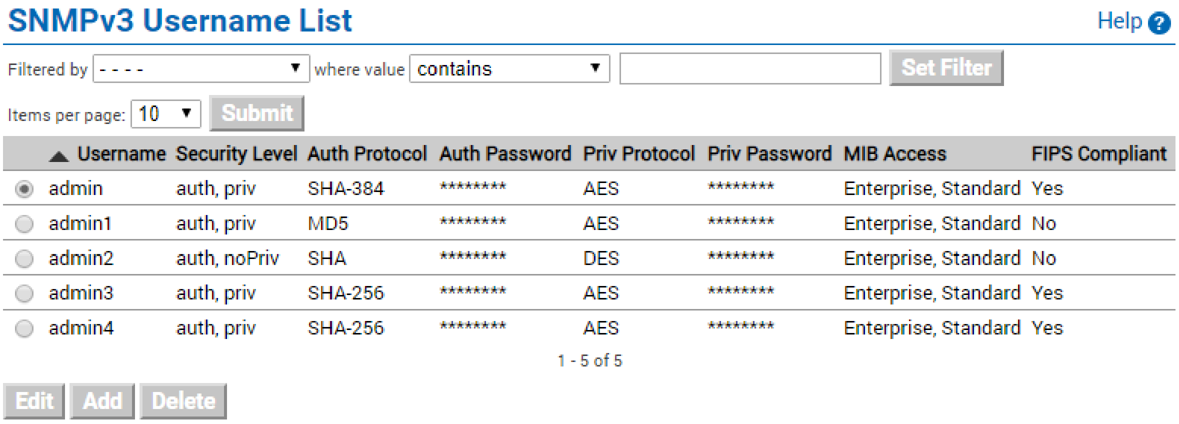
Component	***Description***
Source IP/Subnet Mask(s)	IPv4/IPv6 address(es) allowed to access the agent. You can enter a specific IP address range, or you can enter the value of "any". If you are listing a specific IP address, you must also include the Subnet Mask. Separate the IP address and Subnet Mask with a slash (/). If you are entering multiple IP address/Subnet Mask pairs, you must separate each IP address/Subnet Mask pair with a comma (,). ℹ Utimaco recommends that you limit access to the agent to particular IP addresses.
MIB Access	▪ **Enterprise**: Contains caching, SSL/TLS, CPU utilization, and operational statistics. ▪ **Standard**: Also known as MIB-II, the standard MIB contains information on network interface utilization, system health, and statistics for IP, TCP, ICMP, UDP, and SNMP.
FIPS Compliant	Displays if the configuration is FIPS compliant or not.
Edit	Click **Edit** to change the community name, source IP/subnet mask, or the MIB access for the community.
Add	Click **Add** to add a community to the ESKM appliance.
Delete	Click **Delete** to remove a selected community from the ESKM appliance.

⚠ SNMPv1 and SNMPv2 are not allowed when operating in FIPS mode.

6.20.2.3 SNMPv3 username list

As the name suggests, the SNMPv3 Username list is used to configure the agent to communicate with an NMS running SNMPv3 software. You can think of this section much in the same way as the SNMPv1/SNMPv2 Community list. The SNMPv3 Username list defines from which management stations the ESKM appliance receives SNMP MIB requests. The main difference is that usernames are specific to SNMPv3. Because SNMPv3 offers authentication and privacy, there is more to configure when creating an SNMPv3 Username as opposed to a community.

> If you are configuring the agent to communicate with an NMS running SNMPv1/v2 software, you can disregard this section.



SNMPv3 Username List

Filtered by - - - - where value contains

Items per page: 10

	Username	Security Level	Auth Protocol	Auth Password	Priv Protocol	Priv Password	MIB Access	FIPS Compliant
●	admin	auth, priv	SHA-384	********	AES	********	Enterprise, Standard	Yes
○	admin1	auth, priv	MD5	********	AES	********	Enterprise, Standard	No
○	admin2	auth, noPriv	SHA	********	DES	********	Enterprise, Standard	No
○	admin3	auth, priv	SHA-256	********	AES	********	Enterprise, Standard	Yes
○	admin4	auth, priv	SHA-256	********	AES	********	Enterprise, Standard	Yes

1 - 5 of 5

Figure 183 : SNMPv3 Username List

The following table describes the components of the **SNMPv3 Username List**.

Table 128: SNMPv3 Username List components

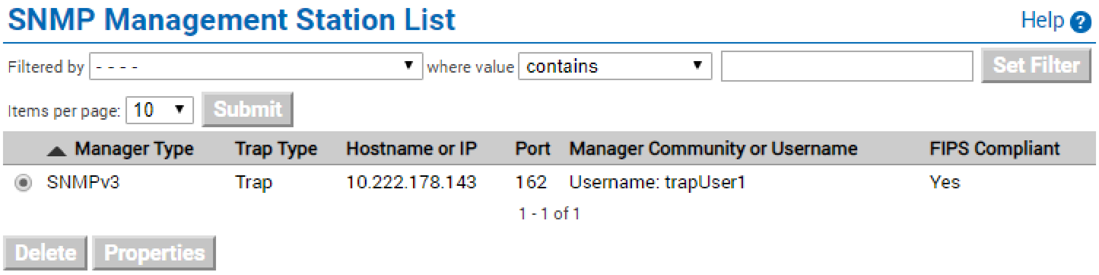
Component	***Description***
Username	The username defines from whom the ESKM appliance accepts SNMP messages, and it is one of the many elements used to create a key that is shared between the NMS and agent. Usernames can contain only alphanumeric characters and punctuation marks and they cannot contain non-printing characters and white spaces.

Component	***Description***
Security Level	You have three choices for the security level ▪ **auth, priv** — authorization and privacy. This option takes full advantage of the enhanced security features in SNMPv3. This option means that the ESKM appliance authenticates the sender of the SNMP message; in addition, all data exchanged between the ESKM appliance's SNMP agent and the NMS is encrypted using the DES algorithm and a secret key. ▪ **auth, no priv** — authorization, no privacy. This option allows you to guarantee that the ESKM appliance only accepts SNMP messages from trusted sources, but the data is not encrypted. ▪ **no auth, no priv** — no authorization, no privacy. This option is similar to the security offered in SNMPv1/v2. No encryption is performed, and the authenticity of the sender of the SNMP message is not guaranteed. ⚠ Only **auth, priv** will be allowed when operating in FIPS mode.
Auth Protocol	You can choose from MD5, SHA, **SHA-256**, **SHA-384**, and **SHA 512.** ⚠ Only FIPS approved algorithms (in bold) will be allowed when operating in FIPS mode.
Auth Password	This password is used to create the secret key that performs the MAC operation on the data that is shared between the ESKM appliance's SNMP agent and the management station. The auth password must be between 8 and 64 characters.

Component	***Description***
Priv Protocol	You can choose from AES or DES. (128-bit AES is supported.) ⚠ Only "AES" will be allowed when operating in FIPS mode.
Priv Password	This password is used to create the secret key that performs the encrypt and decrypt operations on the data shared between the agent and the NMS. The priv password must be between 8 and 64 characters. ⚠ If you select the auth, priv security option and you enter a valid value in the Auth Password field, and leave the Priv Password field blank, the value you entered in the Auth Password field is used for the Priv Password as well.
MIB Access	▪ **Enterprise**: Contains caching, SSL/TLS, CPU utilization, and operational statistics and defines traps. ▪ **Standard**: Also known as MIB-II, the standard MIB contains information on network interface utilization, system health, and statistics for IP, TCP, ICMP, UDP, and SNMP.
FIPS Compliant	Displays if the configuration is FIPS compliant or not.
Edit	Click **Edit** to change any of the values associated with a username, such as the security level, the authorization protocol, the passwords, or the MIB access for the username.
Add	Click **Add** to add a username to the ESKM appliance.
Delete	Click **Delete** to remove a username from the ESKM appliance.

6.20.2.4 SNMP management station list

The SNMP Management Station List provides a view of all the management stations configured on the ESKM appliance. You can think of the SNMP Management Station list as the place where you specify the management stations where traps should be sent from the ESKM SNMP agent.



SNMP Management Station List

Filtered by - - - - where value contains

Items per page: 10

Manager Type	Trap Type	Hostname or IP	Port	Manager Community or Username	FIPS Compliant
● SNMPv3	Trap	10.222.178.143	162	Username: trapUser1	Yes

1 - 1 of 1

Figure 184 : SNMP Management Station List

The following table describes the components of the **SNMP Management Station List**.

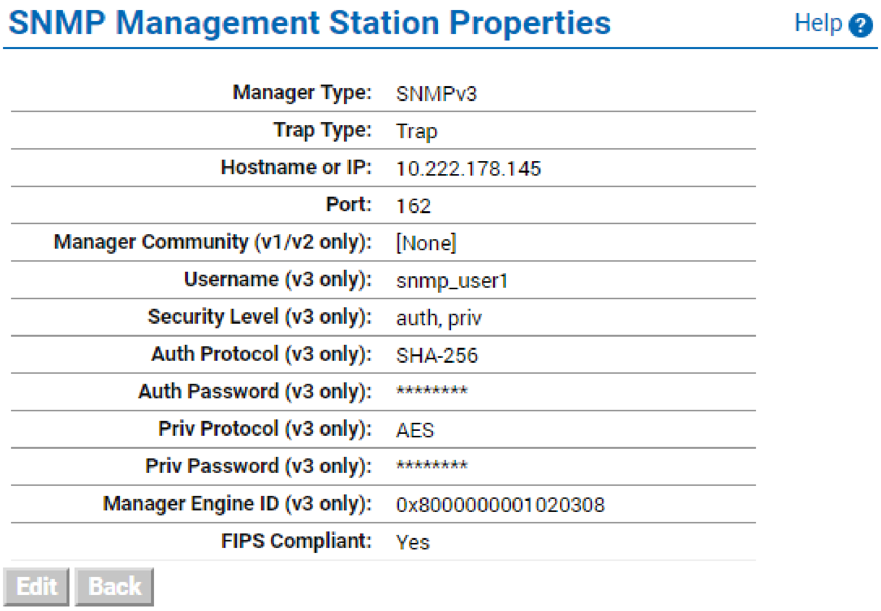
Table 129: SNMP Management Station List components

Component	***Description***
Manager Type	The SNMP version used on the NMS. All three versions of SNMP are supported on the ESKM appliance.
Trap Type	Specifies whether this NMS is configured to receive Trap of Information messages. ⚠ Utimaco recommends that you always use Inform messages.
Hostname or IP	The hostname or IPv4/IPv6 address of the NMS.
Port	Port on which the NMS is listening for SNMP traffic. The default is 162.

Component	*Description*
Management Community or Username	Displays either the management community or username. The management community is used to send SNMP data to the SNMPv1/v2 management stations. The manager community is used by SNMPv1/v2 management stations to filter SNMP traps and is not related to the agent community name. The Manager Community name cannot exceed 64 characters. The username is used to send SNMP data to SNMPv3 management stations. The username is used to create a key that is shared by the agent and the NMS.
FIPS Compliant	Displays if the configuration is FIPS compliant or not.
Delete	Click **Delete** to remove a selected NMS from the ESKM appliance.
Properties	Click **Properties** to view the extended properties of an NMS. From the properties page, you can edit any of the values associated with the NMS.

6.20.2.5 SNMP management station properties

The SNMP Management Station Properties page allows you to view and modify the extended properties of an NMS defined on the ESKM appliance.



SNMP Management Station Properties

Manager Type:	SNMPv3
Trap Type:	Trap
Hostname or IP:	10.222.178.145
Port:	162
Manager Community (v1/v2 only):	[None]
Username (v3 only):	snmp_user1
Security Level (v3 only):	auth, priv
Auth Protocol (v3 only):	SHA-256
Auth Password (v3 only):	********
Priv Protocol (v3 only):	AES
Priv Password (v3 only):	********
Manager Engine ID (v3 only):	0x8000000001020308
FIPS Compliant:	Yes

Figure 185 : SNMP Management Station Properties

The following table describes the components of **SNMP Management Station Properties**.

Table 130: SNMP Management Station Properties components

Component	***Description***
Manager Type	The SNMP version used on the NMS. All three versions of SNMP are supported on the ESKM appliance. ⚠ Only SNMPv3 will be allowed when operating in FIPS mode.
Trap Type	Specifies whether this NMS is configured to receive Trap of Information messages. ⚠ Utimaco recommends that you always use Inform messages.
Hostname or IP	The hostname or IPv4/IPv6 address of the NMS.

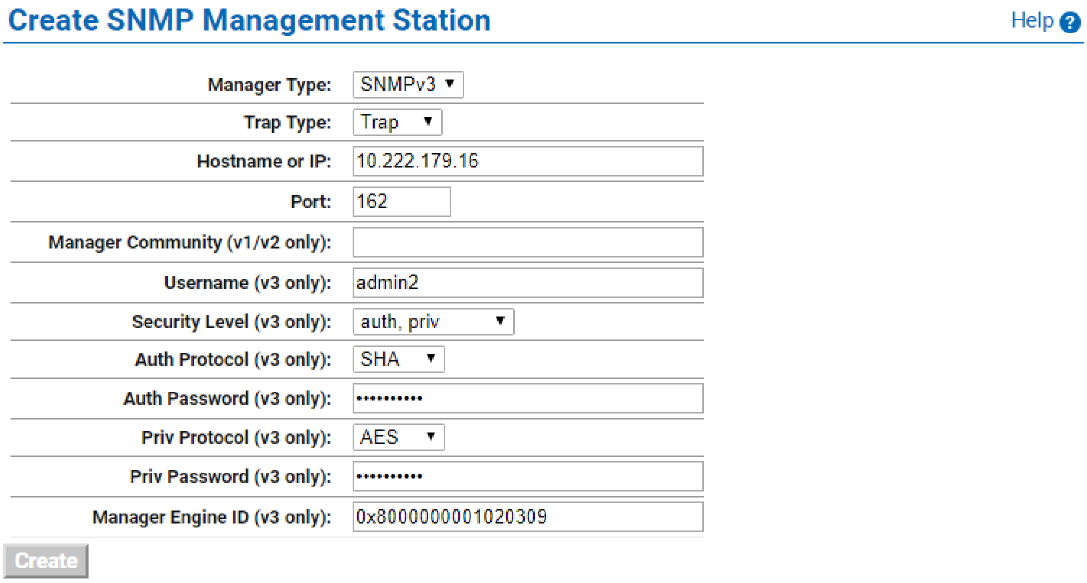
Component	***Description***
Port	Port on which the NMS is listening for SNMP traffic. The default is 162.
Management Community (v1/v2 only)	Name that is used to send SNMP data to the SNMPv1/v2 management stations. The manager community is used by SNMPv1/v2 management stations to filter SNMP traps and is not related to the agent community name. The Manager Community name cannot exceed 64 characters.
Username (v3 only)	Name that is used to send SNMP data to SNMPv3 management stations. The username is used to create a key that is shared by the agent and the NMS.
Security Level (v3 only)	You have three choices for the security level ▪ **auth, priv** — authorization and privacy. This option takes full advantage of the enhanced security features in SNMPv3. This option means that the ESKM appliance is authenticated by the NMS when the ESKM appliance sends a trap; in addition, all data exchanged between the agent and the NMS is encrypted using the DES algorithm and a secret key. ▪ **auth, no priv** — authorization, no privacy. This option allows you to specify that the ESKM appliance is authenticated by the NMS, but data that is exchanged between the agent and NMS is unencrypted. ▪ **no auth, no priv** — no authorization, no privacy. This option is similar to the security offered in SNMPv1/v2. No encryption is performed, and the authenticity of the sender of the SNMP message is not be guaranteed. ⚠ Only **auth, priv** will be allowed when operating in FIPS mode.

Component	***Description***
Auth Protocol (v3 only)	You can choose from MD5, SHA, **SHA-256**, **SHA-384**, and **SHA 512**. ⚠ Only FIPS approved algorithms (in bold) will be allowed when operating in FIPS mode.
Auth Password (v3 only)	This password is used to create the secret key that is used to authenticate the sender of SNMP messages. The auth password must be between 8 and 64 characters.
Priv Protocol (v3 only)	You can choose either AES or DES. (128-bit AES is supported.) ⚠ Only "AES" will be allowed when operating in FIPS mode.
Priv Password (v3 only)	This password is used to create the secret key that is used to encrypt data that is shared between the ESKM appliance's SNMP agent and the NMS. The auth password must be between 8 and 64 characters. ⚠ If you select the auth, priv security option and you enter a valid value in the Auth Password field, and leave the Priv Password field blank, the value you entered in the Auth Password field is used to create the Priv Password.
Manager Engine ID (v3 only)	The Manager Engine ID is a unique identifier for the manager entity that is used for authentication. The Manager Engine ID is not used when sending inform messages. The Manager Engine ID cannot exceed 128 characters.
FIPS Compliant	Displays if the configuration is FIPS compliant or not.

Component	***Description***
Edit	Click **Edit** to modify any of the values associated with the NMS.
Back	Click **Back** to return to the Management Stations tab of the SNMP Configuration page.

6.20.2.6 Create SNMP management station

You can use **Create SNMP Management Station** to add a new management station on the ESKM appliance.



Create SNMP Management Station

Manager Type:	SNMPv3 ▾
Trap Type:	Trap ▾
Hostname or IP:	10.222.179.16
Port:	162
Manager Community (v1/v2 only):	
Username (v3 only):	admin2
Security Level (v3 only):	auth, priv ▾
Auth Protocol (v3 only):	SHA ▾
Auth Password (v3 only):	••••••••••
Priv Protocol (v3 only):	AES ▾
Priv Password (v3 only):	••••••••••
Manager Engine ID (v3 only):	0x8000000001020309

Figure 186 : Create SNMP Management Station

The following table describes the components of the **Create SNMP Management Station**.

Table 131: Create SNMP Management Station components

Component	***Description***
Manager Type	The SNMP version used on the NMS. All three versions of SNMP are supported on the ESKM. ⚠ Only SNMPv3 will be allowed when operating in FIPS mode.
Trap Type	Specifies whether this NMS is configured to receive Trap or Inform messages. ⚠ Utimaco recommends that you always use Inform messages.
Hostname or IP	The hostname or IPv4/IPv6 address of the NMS.
Port	Port on which the NMS is listening for SNMP traffic. The default is 162.
Manager Community (v1/v2)	Name that is used to send SNMP data to SNMPv1/v2 management stations. The manager community is used by SNMPv1/v2 management stations to filter SNMP traps and is not related to the agent community name. The Manager Community name cannot exceed 64 characters.
Username (v3 only)	Name that is used to send SNMP data to SNMPv3 management stations. The username is used to create a key that is shared by the agent and the NMS.

Component	***Description***
Security Level (v3 only)	You have three choices for the security level ▪ **auth, priv** — authorization and privacy. This option takes full advantage of the enhanced security features in SNMPv3. This option means that the ESKM appliance is authenticated by the NMS, when the ESKM appliance sends a trap; in addition, all data exchanged between the ESKM appliance's SNMP agent and the NMS is encrypted using the DES algorithm and a secret key. ▪ **auth, no priv** — authorization, no privacy. This option allows you to specify that the ESKM appliance is authenticated by the NMS, but data that is exchanged between the agent and NMS is unencrypted. ▪ **no auth, no priv** — no authorization, no privacy. This option is similar to the security offered in SNMPv1/v2. No encryption is performed, and the authenticity of the sender of the SNMP message is not be guaranteed. ⚠ Only **auth, priv** will be allowed when operating in FIPS mode.
Auth Protocol (v3 only)	You can choose from MD5, SHA, **SHA-256**, **SHA-384**, and **SHA 512.** ⚠ Only FIPS approved algorithms (in bold) will be allowed when operating in FIPS mode.
Auth Password (v3 only)	This password is used to create the secret key that is used to authenticate the sender of SNMP messages. The auth password must be between 8 and 64 characters.

Component	***Description***
Priv Protocol (v3 only)	You can choose either AES or DES. (128-bit AES is supported.) ⚠ Only "AES" will be allowed when operating in FIPS mode.
Priv Password (v3 only)	This password is used to create the secret key that is used to encrypt data that is shared between the ESKM appliance’s SNMP agent and the NMS. The auth password must be between 8 and 64 characters. ⚠ If you select the auth, priv security option and you enter a valid value in the Auth Password field, and leave the Priv Password field blank, the value you entered in the Auth Password field is used to create the Priv Password.
Manager Engine ID (v3 only)	The Manager Engine ID is a unique identifier for the manager entity that is used for authentication. The Manager Engine ID is not used when sending inform messages. The Manager Engine ID cannot exceed 128 characters.
Create	Click **Create** to create the SNMP management station.

6.20.3 Enterprise MIB overview

MIBs, in SMIv2 format, are provided in a file which is located on the user documentation CD-ROM that ships with each ESKM appliance. If you need MIBs in SMIv1 format, you can derive them from the SMIv2 MIBs. The Enterprise MIBs are broken out into the following functional groups:

- **System Statistics**: The System Statistics provides basic system information like system uptime, CPU utilization, Number of CPUs in the system, and Memory utilization. For a more thorough description of the System Statistics, see Refresh statistics (p. 556).

- KMS Server Statistics: KMS server statistics are available through the MIBs; for each statistic set, you can view the following: current requests per second, maximum requests per second, successful operations, and failed operations. The following statistics are available:
  - Total Requests
  - Key operations
  - Key Generate Requests
  - Key Information Requests
  - Key Delete Requests
  - Key Query Requests
  - Key Import Requests
  - Key Export Requests
  - Random Generate Requests
  - Cryptographic Requests
  - Authenticate Requests
- Software Objects/Traps: Software objects are broken out into the following groups:
  - Services — Traps are sent for any of the following events: service started or stopped, the system restarted a down service, a certificate expired, a certificate will expire soon, failed to transfer log, a client application attempts to use a certificate that has been revoked, multiple unsuccessful attempts to restart a service.
  - Security Warnings — An administrator experienced multiple password failures while attempting to log in, the system was reset to factory settings, the system was restored to default settings, configuration data was corrupted or modified.
  - Generic Security Objects — Content detected as defaced, invalid client certificate, multiple username/password failures from a user, wrong key in use, operation not permitted, other security warning.
  - Cluster Objects — Server joined/left cluster, success or failure notification for the following: key replication, key deletion, user or group replication, LDAP configuration replication, authorization policy replication, cluster synchronization.

    - **LDAP Notification Objects** — LDAP server connection succeeded, LDAP server connection failed, switching to alternate LDAP server.

- Hardware Objects/Traps.
    - **System Notification Objects** — System starting up/shutting down, system preparing to restart/halt.
    - **Power Supply Notification Objects** — Power supply operational/non-operational.
    - **Fan Notification** — Fault detected.
    - **Disk Utilization** — Disk usage exceeded.
    - **RAID Disk Notification** — Disk operational, disk failed, disk recovering, disk status unknown, disk removed.

6.21 Administrator accounts configuration

The **Administrator Configuration page** allows you to create administrator accounts, specify access control options, manage passwords and password settings, require that multiple administrators authorize certain operations, and configure remote administration settings. This section contains the following information:

- Administrator overview (p. 473)
- LDAP administrators (p. 478)
- LDAP administrative server (p. 478)
- Administrator procedure (p. 479)
- Password management overview (p. 490)
- Password management (p. 494)
- Multiple credentials overview (p. 497)
- Multiple credentials (p. 501)
- Remote administration settings overview (p. 504)
- Remote administration settings (p. 505)

For more information see also:

- Administrator procedures (p. 128)
- Password management procedures (p. 136)
- Multiple credentials procedures (p. 139)
- Remote administration procedures (p. 141)

6.21.1 Administrator overview

An administrator is a user who can configure and manage the ESKM appliance. This is done using the Management Console and the Command Line Interface (CLI). An administrator's access control settings determine which features can be configured and which operations can be performed.

For more information about administrator procedures, see Administrator procedures (p. 128).

6.21.1.1 Access controls

An access control is the permission to configure a feature or perform an operation. To create a certificate, the administrator must have the Certificates access control. Access Controls are managed and stored on the ESKM appliance. The available access controls are grouped into categories and described here.

Security Configuration Access Controls enable the administrator to:

- Create, modify, and delete keys and establish authorization policies (Keys and Authorization Policies)
- Create and modify users and groups and maintain LDAP server settings (Users and Groups)
- Create and import certificates (Certificates)
- Manage certificate authorities on the ESKM appliance (Certificate Authorities)
- Manage advanced security settings, including FIPS (Advanced Security)
- Modify SSL/TLS configuration

Device Configuration Access Controls enable the administrator to:

- Configure KMS, KMIP, and REST server settings.

- Create a cluster, join or remove an ESKM appliance from an existing cluster (Cluster)
- Configure network and date/time settings (Network and Date/Time)
- Enable and configure high availability settings (High Availability)
- Manage SNMP community names and management stations (SNMP)
- Modify logging settings (Logging)

Backup and Restore Access Controls enable the administrator to:

- Create backups excluding backup of keys, certificates and local certificate authorities and configure kerberos settings (Backup Configuration and Kerberos)
- Create backups of keys and certificates (Backup Keys and Certificates)
- Create backups of local certificate authorities and associated private keys (Backup Local CAs)
- Restore backups excluding backup of keys, certificates, and local certificate authorities (Restore Configuration)
- Restore backups of keys and certificates (Restore Keys and Certificates)
- Restore backups of local certificate authorities and associated private keys (Restore Local CAs)

Maintenance access controls enable the administrator to:

- Modify the startup service setting (Services)
- Upgrade to a new software version and add and remove disks (Software Upgrade and System Health)

Administrative Access access controls enable the administrator to:

- Access the Management Console (Admin Access via Web)
- Access the Command Line Interface over an SSH connection (Admin Access via SSH)

Regardless of the Administrative Access settings, all administrators can access the ESKM appliance directly using the serial console. Using the serial console connection precludes the administrator from modifying almost all security configuration settings and some device configuration settings (for example, Keys, Users and Groups, and others).

6.21.1.2 Using multiple administrator accounts

When setting up your system, you will likely need multiple administrators. When creating those officers, you should assign access controls that mirror your organization’s procedures. For example, if you separate the tasks of key management, system backup, and device configuration, you will want to create unique administrators for each of those roles.

When creating an administrator, you should assign the minimum number of access controls needed. For example, a backup administrator will only need the Backup and Restore access controls. (You will probably also want to assign an Administrative Access access control to most of your administrators.)

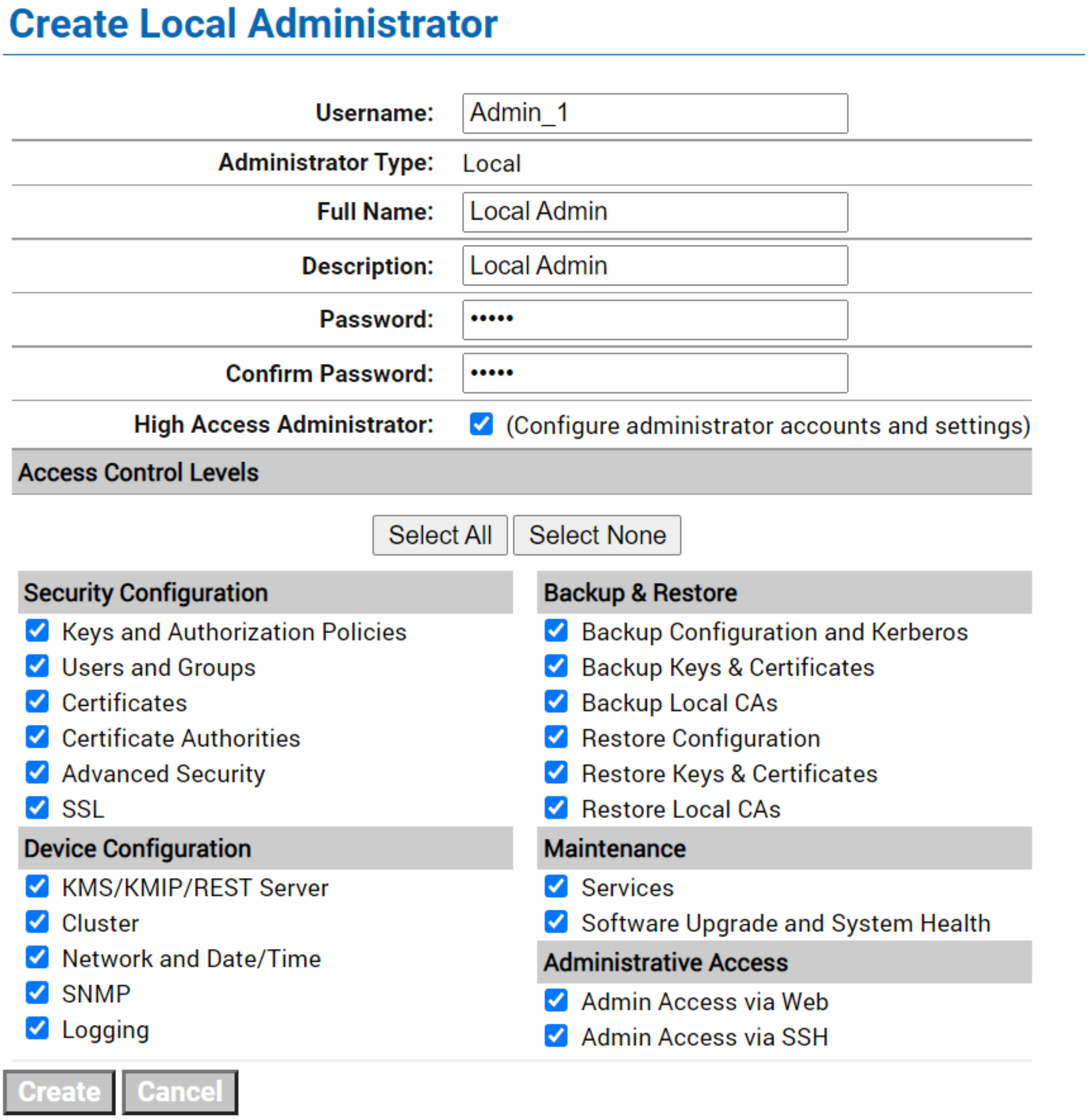
> Utimaco strongly discourages the sharing of administrator accounts. Each administrator should have their own administrator account.

6.21.1.3 High-access administrators

When creating or modifying an administrator, you can select the High Access Administrator field. High Access administrators have all access controls. They have full control over the configuration of the appliance. They can:

- Create and delete administrator accounts
- Change administrator passwords
- Assign and revoke access controls

When you select this option, the system automatically enables all access controls for that administrator.



Create Local Administrator

Username:	Admin_1
Administrator Type:	Local
Full Name:	Local Admin
Description:	Local Admin
Password:	•••••
Confirm Password:	•••••
High Access Administrator:	☑ (Configure administrator accounts and settings)

Access Control Levels

Security Configuration

- ☑ Keys and Authorization Policies
- ☑ Users and Groups
- ☑ Certificates
- ☑ Certificate Authorities
- ☑ Advanced Security
- ☑ SSL

Device Configuration

- ☑ KMS/KMIP/REST Server
- ☑ Cluster
- ☑ Network and Date/Time
- ☑ SNMP
- ☑ Logging

Backup & Restore

- ☑ Backup Configuration and Kerberos
- ☑ Backup Keys & Certificates
- ☑ Backup Local CAs
- ☑ Restore Configuration
- ☑ Restore Keys & Certificates
- ☑ Restore Local CAs

Maintenance

- ☑ Services
- ☑ Software Upgrade and System Health

Administrative Access

- ☑ Admin Access via Web
- ☑ Admin Access via SSH

Figure 187 : High Access Administrator

Take great caution when creating High Access administrators. It might be helpful to think of such administrators as “super users”, who can change the passwords of local administrators, assign and revoke permissions, and create and delete administrators.

Both local and LDAP administrators can be High Access administrators. The admin account created during first-time initialization is a local High Access administrator.

6.21.1.4 Default administrator

The ESKM appliance comes with a default administrator (admin), a local High Access Administrator. Once the initial configuration is complete, you must log in as admin; thereafter, you can create different administrators and log in with a different username.

6.21.1.5 Local and LDAP administrators

The ESKM appliance supports two types of administrators: local and LDAP. Functionally, local and LDAP administrators have the same capabilities. For example, both local and LDAP administrators can be High Access administrators. You can have multiple local and LDAP administrators at the same time.

6.21.1.6 Administrator passwords

Local administrators are created within the ESKM appliance environment, either on the local server, or on an appliance that is a member of a cluster. They are managed entirely on the ESKM appliance. Local administrator usernames are restricted to letters and numbers only, must start with a letter, and can be up to 30 characters long. Local administrator passwords must adhere to the ESKM appliance's password policies, which are discussed in Password management overview (p. 490).

> ❗ It is absolutely crucial that you remember the passwords for all of your local administrators. For security reasons, there is no way to reset a local administrator's password without logging into the ESKM appliance as a High Access Administrator. If you lose or forget the passwords for all administrator accounts, you cannot configure the ESKM appliance, and you must ship it back to have the software reinstalled. All keys and configuration data will be unrecoverable.

When a local administrator logs in to the CLI or the Management Console, the ESKM appliance authenticates the username and password with the values stored securely on it. If the authentication succeeds, the administrator will be logged in to the ESKM appliance.

High Access Administrators can change the password of any local administrator. (Such an event is recorded in the Audit Log.) If one administrator changes the password of another administrator, the administrator whose password is changed, is prompted to change the password immediately after logging in to the ESKM appliance. After changing the password, the administrator continues to the Management Console or the command prompt as usual.

6.21.2 LDAP administrators

LDAP administrators are based on user accounts managed on an LDAP server. The LDAP server is external to the ESKM appliance environment; the ESKM appliance does not store any information on the LDAP server. One of the main benefits of using LDAP administrators is that you can centralize your administrator account management. If you already have an LDAP server set up, you do not have to configure local administrators. LDAP administrator usernames can contain letters, numbers, spaces, and punctuation characters, and they can be up to 64 characters long.

Password management is controlled by the LDAP server, not the ESKM appliance. You use the LDAP server to configure your policies and store the passwords. LDAP administrators cannot change their passwords using the ESKM appliance. The configurable password settings, password history, and password expiration features on the ESKM appliance do not apply to LDAP administrators.

> Resetting forgotten passwords may be possible on your LDAP server. This can be both a benefit and a security risk. If all of your administrator passwords are forgotten, you may be able to use your LDAP server to reset an LDAP administrator password. Otherwise, it will be impossible to log into the ESKM appliance. However, this ability could also be used to hijack an LDAP administrator account.

When an LDAP administrator logs in to the CLI or the Management Console, the ESKM appliance connects to the LDAP server to authenticate the username and password. If the authentication succeeds, the administrator will be logged in to the ESKM appliance.

6.21.3 LDAP administrative server

In order to create an LDAP administrator, you must first configure the LDAP Administrator Server settings. These settings define an external LDAP server containing the list of users who can be designated as LDAP administrators. When creating an LDAP administrator on the ESKM appliance, you will choose the LDAP administrator from this list of users.

Configuration of the LDAP Administrator Server and the first LDAP administrator must be performed by a local administrator. Thereafter, you can use the LDAP administrator.

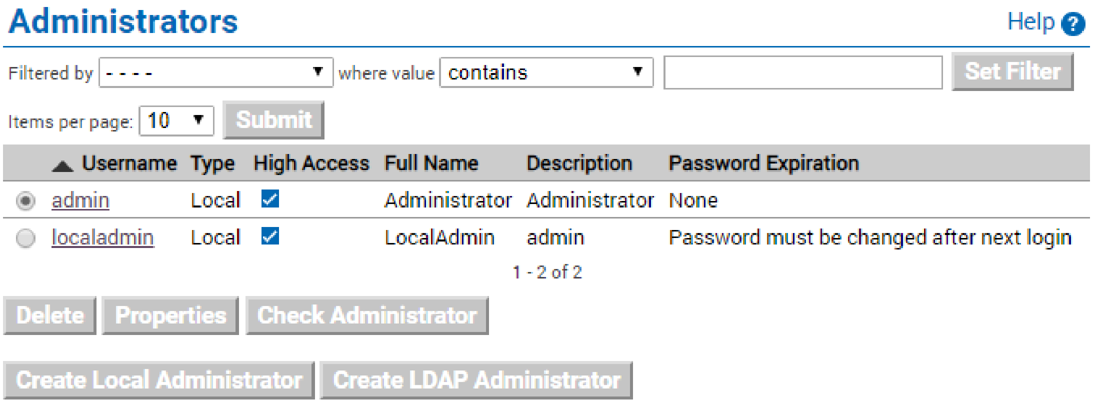
If you are using LDAP administrators, Utimaco recommends that you enable SSL/TLS in the LDAP Administrator Server settings. This ensures that the connection between the ESKM appliance and the LDAP server is secure. If you do not use SSL/TLS, then it is possible that the LDAP administrator passwords will travel in the clear during authentication, depending on the LDAP server's configuration (such as if the server is set to use "simple" authentication).

If you use LDAP administrators predominantly, at least one local administrator account must always exist, and that local administrator must be a High Access Administrator. This local High Access Administrator is needed in the event that connectivity to the LDAP server is lost, or if all administrator accounts on the LDAP server are removed or renamed.

If you use the Multiple Credentials feature, there must exist at least as many local High Access Administrators as are needed to perform configuration operations. LDAP administrators are otherwise fully compatible with the Multiple Credentials feature.

6.21.4 Administrator procedure

The **Administrator Configuration** page allows you to create and manage administrator accounts.



Filtered by - - - - where value contains

Items per page: 10

	▲ Username	Type	High Access	Full Name	Description	Password Expiration
●	admin	Local	☑	Administrator	Administrator	None
○	localadmin	Local	☑	LocalAdmin	admin	Password must be changed after next login

1 - 2 of 2

Figure 188 : Administrator Configuration

6.21.4.1 Creating an administrator

To create an administrator account:

1. Log in the ESKM appliance as an administrator with High Access Administrator access control.

2. Navigate to the Administrators section on the Administrator Configuration page (**Device > Administrators > Administrators**).

3. Click **Create Local Administrator** or **Create LDAP Administrator**.
   You must configure the LDAP Administrator Server settings before you can create an LDAP administrator.

4. Enter values in the **Username**, **Full Name**, **Description**, and **Password** fields for Local administrators or enter the Username for LDAP administrators.
   Use the **Browse** button to access **Select LDAP Username** and select a Username from the list.

5. Confirm the password in the **Confirm Password field** for Local administrators.

6. Select the access controls for the administrator account.

7. Click **Create**.

6.21.4.2 Deleting an administrator

To delete an administrator account:

1. Log in to the Management Console as an administrator with High Access Administrator access control.

2. Navigate to the Administrator section on the Administrator Configuration page (**Device > Administrators > Administrators**).

3. Select the administrator in the **Administrator** section.

4. Click **Delete**.

5. Confirm the action in the **Secondary Approval** section.

⚠ For disaster recovery purposes, the last local administrator account on an ESKM appliance cannot be deleted.

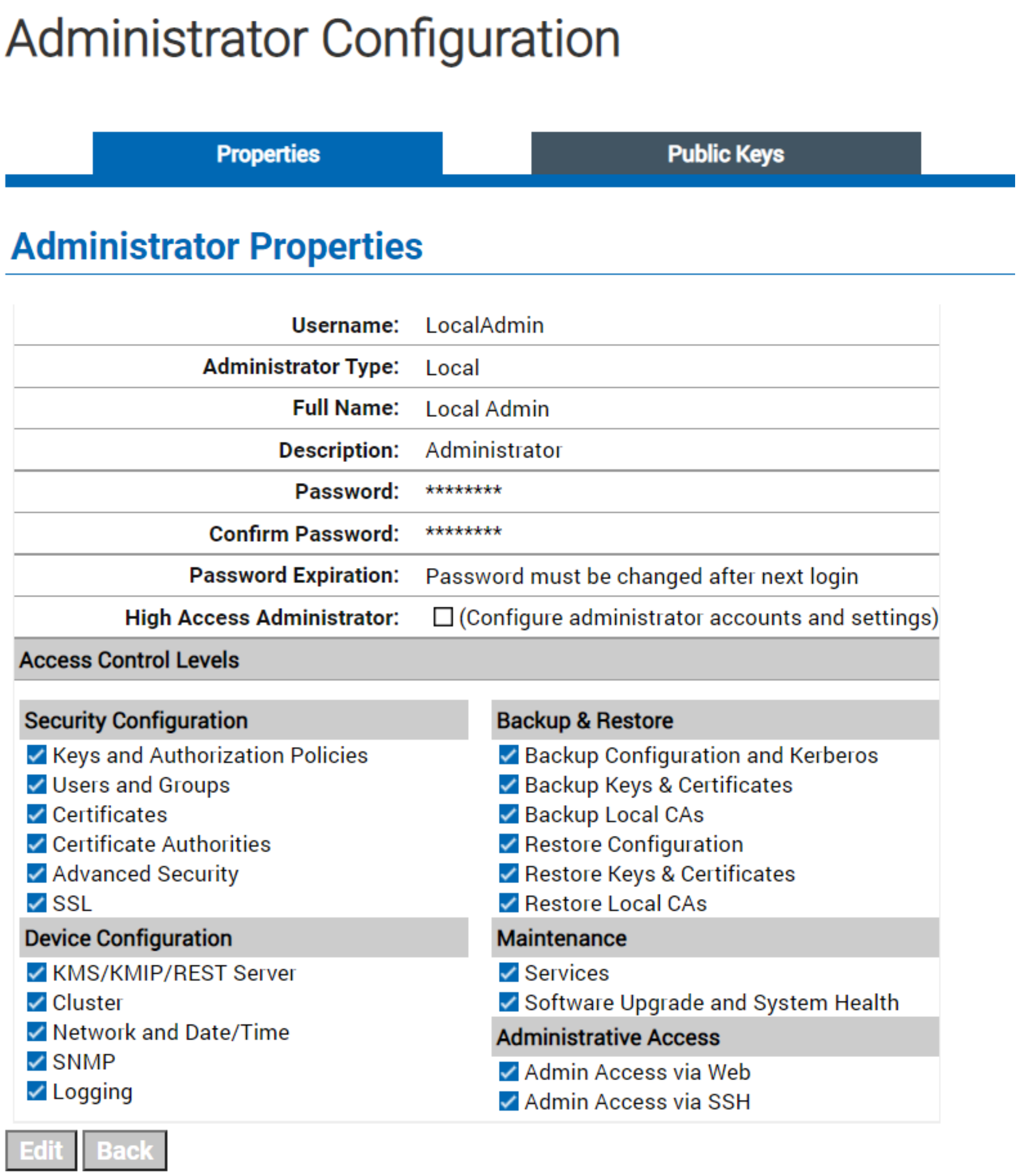
6.21.4.3 Modifying administrator properties

To modify administrator properties:

1. Log in the ESKM appliance as an administrator with High Access Administrator access control.

2. Navigate to the Administrators section on the Administrator Configuration page (**Device > Administrators > Administrators**).

3. Click on the username, or click the radio button to the left of the administrator, and then click **Properties**.



Administrator Properties

Username:	LocalAdmin
Administrator Type:	Local
Full Name:	Local Admin
Description:	Administrator
Password:	********
Confirm Password:	********
Password Expiration:	Password must be changed after next login
High Access Administrator:	□ (Configure administrator accounts and settings)

Access Control Levels

Security Configuration

☑ Keys and Authorization Policies
☑ Users and Groups
☑ Certificates
☑ Certificate Authorities
☑ Advanced Security
☑ SSL

Device Configuration

☑ KMS/KMIP/REST Server
☑ Cluster
☑ Network and Date/Time
☑ SNMP
☑ Logging

Backup & Restore

☑ Backup Configuration and Kerberos
☑ Backup Keys & Certificates
☑ Backup Local CAs
☑ Restore Configuration
☑ Restore Keys & Certificates
☑ Restore Local CAs

Maintenance

☑ Services
☑ Software Upgrade and System Health

Administrative Access

☑ Admin Access via Web
☑ Admin Access via SSH

Figure 189 : Administrator Properties

4. Click **Edit** to modify the administrator properties.

5. When finished, click **Save**.

6.21.4.4 SSH Public key authentication

ESKM supports the ability to authenticate an administrator using SSH protocol version 2. To authenticate an administrator a 2048, 3072, or 4096-bit RSA public key must be associated with each administrator.

> If you are using a Linux system to administer the ESKM appliance, you can use the following command to create the 2048-bit RSA key pair.
>
> ```
> ssh-keygen -t rsa
> ```
>
> You can use the `-b <key size>` parameter to specify a larger key size. For example,
>
> ```
> ssh-keygen -t rsa -b 3072
> ssh-keygen -t rsa -b 4096
> ```

The following ESKM operations support the ability to authenticate the administrator.

Table 132: Administrator functions that support public key authentication

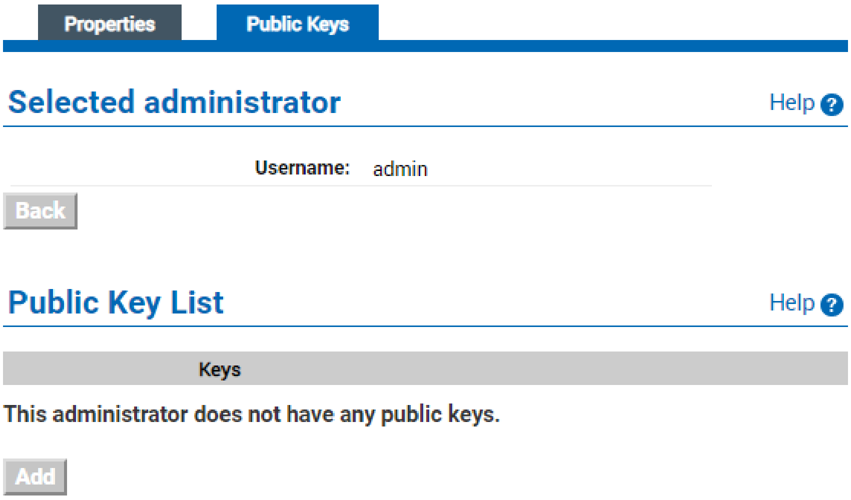
Server operation	***Management Console***	***Command Line Interface***
Remote Management	No	Yes
Transferring on-demand as well as scheduled backups via SCP to a remote machine.	Yes	Yes
Restoring backups from a remote machine via SCP.	Yes	Yes
Transferring logs via SCP to a remote machine.	No	Yes
Performing a software upgrade via SCP.	Yes	Yes
Importing a certificate via SCP.	Yes	Yes

To associate a public key with an administrator:

1. Log in the ESKM appliance as an administrator with High Access Administrator access control.

2. Navigate to the Administrators section on the Administrator Configuration page (**Device > Administrators > Administrators**).

3. Click the radio button to the left of the administrator, click on the **Properties** button, and then click the **Public Keys** tab.



Selected administrator

Username: admin

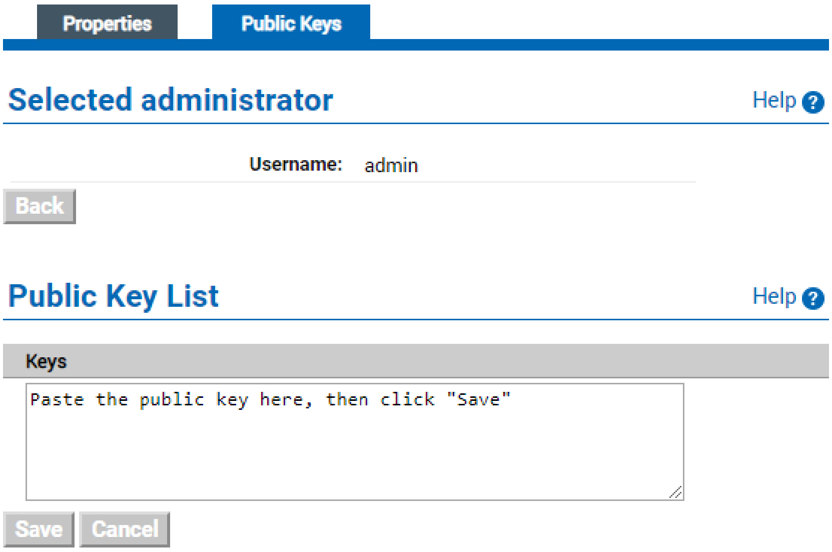
Public Key List

Keys

This administrator does not have any public keys.

Figure 190 : Administrator Public Keys

4. Click **Add**.



Selected administrator

Username: admin

Public Key List

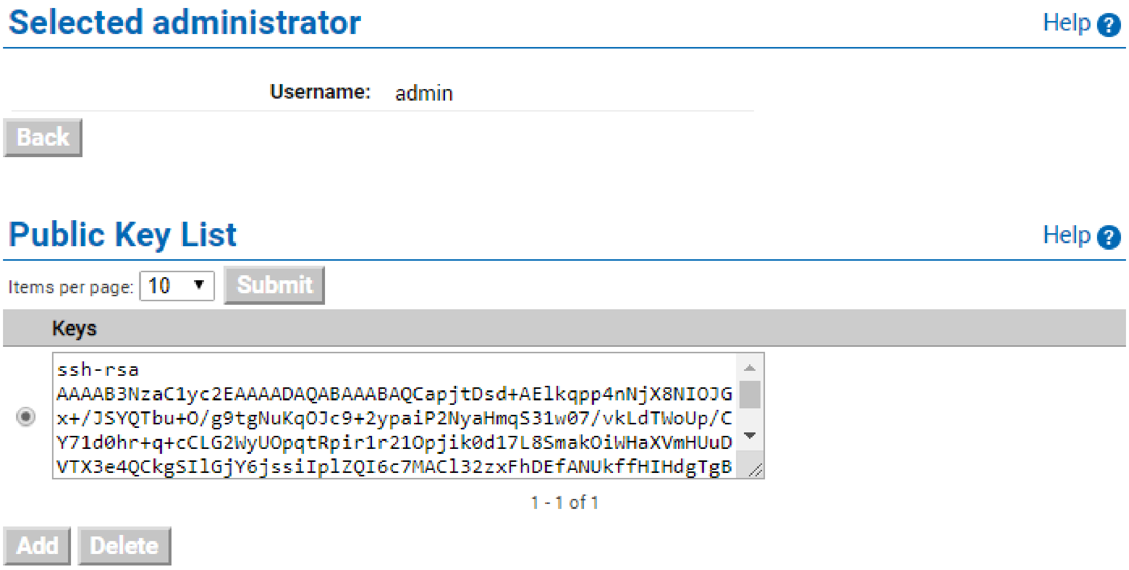
Keys

```
Paste the public key here, then click "Save"
```

5. Paste the public key into the Keys field, and then click **Save**.

Each public key must have a unique user name. The same public key value can be added to multiple administrators.

When a public key has been saved, the public keys window include a **Delete** button, which can be used to delete a public key.



Selected administrator

Username: admin

Public Key List

Items per page: 10 ▼

Keys

●

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCapjtDsd+AElkqpp4nNjX8NIOJG
x+/JSYQTbu+O/g9tgNuKqOJc9+2ypaiP2NyaHmqS31w07/vkLdTWoUp/C
Y71d0hr+q+cCLG2WyUOpqtRpir1r21Opjik0d17L8SmakOiWHaXVmHUuD
VTX3e4QCkgSIlGjY6jssiIplZQI6c7MACl32zxFhDEfANUkffHIHdgTgB
```

1 - 1 of 1

Figure 191 : Deleting a public key

There is no confirmation prompt for the delete operation. When you click **Delete**, the public key is deleted.

6.21.4.5 Check administrator

To validate a selected LDAP administrator account (particularly if the LDAP settings have been modified or updated):

1. Log in the ESKM appliance as an administrator with High Access Administrator access control.

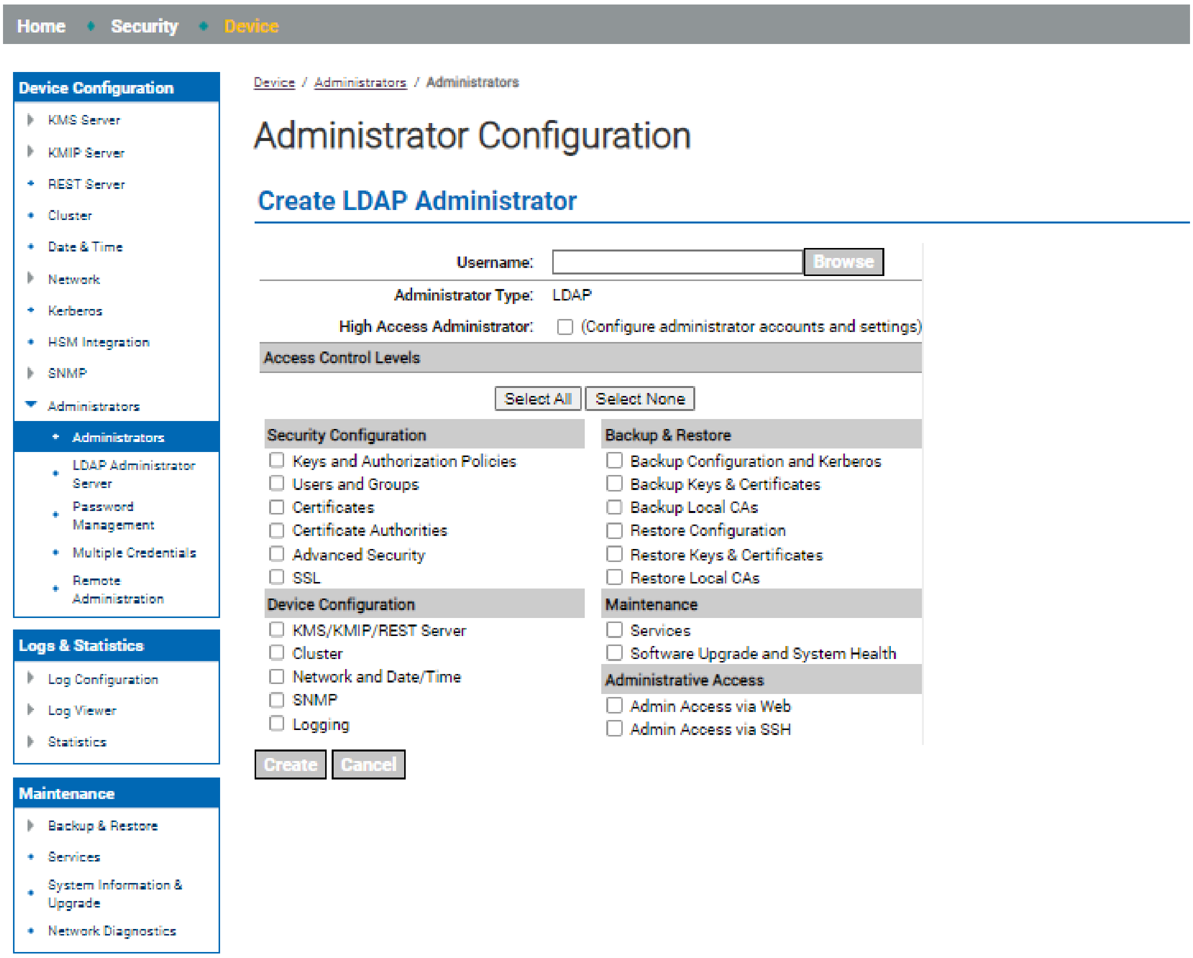
2. Navigate to the Administrators section on the Administrator Configuration page (**Device > Administrators > Administrators**).

3. Click the radio button to the left of the administrator, and then click **Check Administrator**.

6.21.4.6 Create LDAP administrator

The **Create Local Administrator** and **Create LDAP Administrator** sections are the same, except that Create LDAP Administrator requires only a Username—passwords are administered on the LDAP server—and provides a **Browse** button to browse for specific users in the LDAP directory.

> The ESKM appliance must have a connection to the LDAP server. To configure it to connect to a LDAP server, see LDAP server configuration (p. 326).



Administrator Configuration

Create LDAP Administrator

Username:

Administrator Type: LDAP

High Access Administrator: □ (Configure administrator accounts and settings)

Access Control Levels

Security Configuration	Backup & Restore
□ Keys and Authorization Policies	□ Backup Configuration and Kerberos
□ Users and Groups	□ Backup Keys & Certificates
□ Certificates	□ Backup Local CAs
□ Certificate Authorities	□ Restore Configuration
□ Advanced Security	□ Restore Keys & Certificates
□ SSL	□ Restore Local CAs
Device Configuration	**Maintenance**
□ KMS/KMIP/REST Server	□ Services
□ Cluster	□ Software Upgrade and System Health
□ Network and Date/Time	**Administrative Access**
□ SNMP	□ Admin Access via Web
□ Logging	□ Admin Access via SSH

Figure 192 : Create LDAP Administrator

The following table describes the components of **Create Administrator**.

Table 133: Create LDAP Administrator components

Component	***Description***
Username	Enter the login name the administrator uses to access the ESKM appliance.
Browse	Click to access Select LDAP Username.
Access Control — Security Configuration	Access control options related to the ESKM appliance security configuration. ▪ **Keys and Authorization Policies**: Create, modify and delete keys and establish authorization policies. ▪ **Users and Groups**: create and modify local users and groups and maintain LDAP user server settings. ▪ **Certificates**: Create and import certificates. ▪ **Certificate Authorities**: Manage certificate authorities on the ESKM Level 3 appliance. ▪ **Advanced Security**: Manage advanced security settings, including FIPS configuration. ▪ **SSL/TLS**: Modify SSL/TLS configuration.

Component	***Description***
Access Control — Device Configuration	Access controls relating to general ESKM appliance configuration. - **KMS/KMIP/REST Server**: Configure the KMS, KMIP, and REST server settings. - **Cluster**: Create a cluster, join or remove this ESKM appliance from an existing cluster. - **Network and Date/Time**: Configure network and date/time settings. - **High Availability**: Enable and configure high availability settings. - **SNMP**: Manage SNMP community names and management stations. - **Logging**: Modify logging settings.
Access Control — Backup and Restore	Access controls relating to backing up and restoring ESKM appliance and cryptographic configurations. - **Backup Configuration and Kerberos**: Create system backups that include everything but keys, certificates and local CAs, and configure Kerberos settings. - **Backup Keys and Certificates**: Create backups of keys and certificates - **Backup Local CAs**: Create backups of local CAs. - **Restore Configuration**: Restore system backups that include everything but keys, certificates and local CAs. - **Restore Keys and Certificates**: Restore backups of keys and certificates. - **Restore Local CAs**: Restore backups of local CAs.

Component	***Description***
Access Control — Maintenance	Access control options relating to the ESKM appliance maintenance. - **Services**: Modify startup service setting. - **Software Upgrade**: Upgrade to a new version of the software.
Access Control — Administrative Access	Access control options relating to remotely administering the ESKM appliance. - **Admin Access via Web**: Administer the ESKM appliance through the web interface. - **Admin Access via SSH**: Administer the ESKM appliance through SSH. These access control options specify whether an administrator can configure the ESKM appliance from the Management Console and the CLI. You should note that administrators who cannot log in via either of these interfaces can only manage the ESKM appliance from a serial console connection, which would preclude the administrator from modifying almost all security configuration settings and some ESKM appliance configuration settings (for example: Server, Keys, and Users and Groups).

6.21.4.7 Select LDAP username

Select LDAP Username allows you to browse and select an LDAP user when creating an LDAP administrator account.

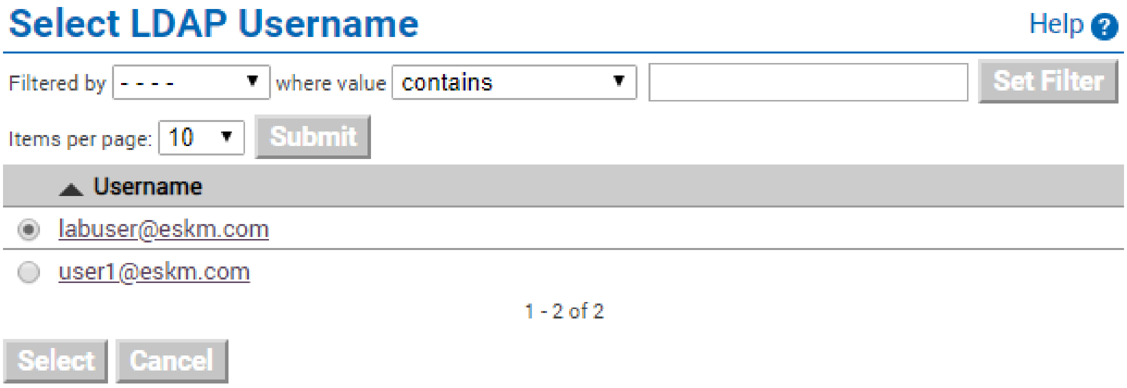


Figure 193 : Select LDAP Username

Table 134: Select LDAP Username components

Component	***Description***
Username	Select a username from the list to create the LDAP administrator. Click on a username to select the user and return to Create LDAP Administrator.
Select	Click to add the selected user to Create LDAP Administrator. The Management Console returns to Create LDAP Administrator of the Administrator Configuration page after a user has been selected.
Cancel	Click to exit the page without selecting a user. The Management Console returns to Create LDAP Administrator of the Administrator Configuration page.

6.21.5 Password management overview

This section contains overview information about password constraints, and the password expiration and history features. All passwords must be stored in a safe place.

A "safe place" means under lock and key. Utimaco recommends that you treat this, along with the bezel keys and other passwords, as highly confidential material, and as such, should be guarded with the level of security that you treat the data stored in the ESKM appliance.

The following topics are covered in this section:

6.21.5.1 Password constraints

All passwords on the ESKM appliance are subject to the same basic constraints. Passwords must contain at least five different characters. Passwords have the following constraints:

- They cannot contain only whitespace
- They cannot resemble a phone number, dictionary word, or reversed dictionary word
- They cannot be based on the username associated with the password

If you enter a password that doesn't conform to these constraints, an error message appears, indicating why the password failed.

In addition to these rules, an administrator may set up more constraints on the **Password Settings for Local Administrators.**

For information on additional constraints, see Password settings for local administrators (p. 495).

LDAP administrators cannot change their passwords on the ESKM appliance. LDAP passwords must be changed on the LDAP server.

6.21.5.2 Password expiration

The password expiration feature allows you to specify a duration for administrator passwords. By default, this feature is disabled. When an administrator password expires, the system forces that administrator to create a new password after logging in with the expired password. (If the administrator is currently logged in when the password expires, that session continues as normal).

The duration of passwords is unaffected by changes to the system time (either manual changes or changes due to NTP synchronization). This accomplishes two objectives:

- An administrator cannot turn back the system time to prevent a password from expiring
- It avoids a scenario where many or all passwords expire simultaneously due to a large jump forward in the system time

6.21.5.3 Password history

The password history feature enables the system to maintain a list of previously-used administrator passwords for each administrator. When an administrator creates a new password, the system checks that the entry does not exist on the password list. Once created, the new password is added to the administrator's password history.

The password history is only consulted when an administrator attempts to change his or her own password. It is not checked when one administrator changes another's password. This accomplishes two objectives:

- Administrators cannot determine the passwords of other administrators
- It allows you to reset an administrator's password to a standardized temporary password

By default, the password history feature is disabled. The system populates the password history with passwords created after the feature is enabled. Passwords currently in use when the feature is selected are not included in the password history. Likewise, passwords assigned during the administrator creation process are not retained by this feature. All password histories are cleared when the feature is disabled.

6.21.5.4 Recommendations for managing passwords

Password protection is a high priority. If passwords are not managed properly, they can become a security risk. Some key actions to properly manage passwords are presented here.

Each of the four types of passwords on the ESKM appliance should be changed on a regular basis.

- Administrator account passwords should be scheduled to change frequently, and in the event of a security officer personnel change.
- User account passwords should be scheduled to change regularly, but less frequently than the administrator account passwords, and in the event of a security officer personnel change.
- Backup passwords should be scheduled to change regularly, but less frequently than the administrator or user account passwords, and in the event of a security officer personnel change.
- Cluster passwords should be changed rarely, if at all.

The cluster password is not replicated to other ESKM appliances in the cluster. If the cluster password is changed, be sure to record the ESKM appliance which was used to change the password. You must also keep track of the password related to each cluster key. Care must be taken to ensure that no information is overwritten during the recreation of the cluster, following the password change.

Choose the intervals between scheduled password changes to be short enough so that security is assured, yet long enough so that the changes do not negatively impact business operations. Time schedule password changes, so that at least one full-access administrator account is unchanged during the process.

In addition to all scheduled password changes, immediately change all administrator, user account, and backup passwords any time a security officer takes a new position or leaves the company. See Changing passwords when a security officer leaves (p. 138).

Document the password policy and communicate it to all appropriate parties including security officers and other corporate personnel.

6.21.6 Password management

Password Management on the **Administrator Configuration** page allows administrators change their own password, manage administrator password features, and set additional constraints for all passwords on the ESKM appliance. This section discusses the following topics:

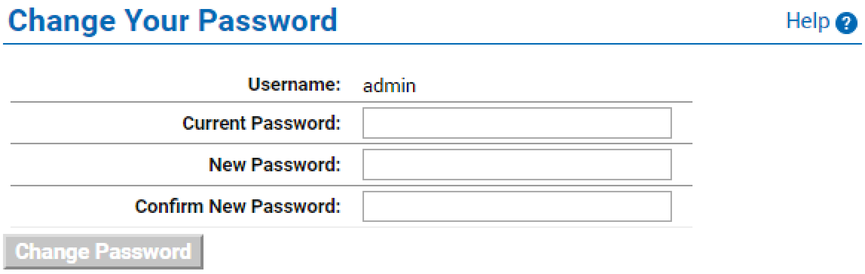
- Change your password (p. 494)
- Password settings for local administrators (p. 495)

6.21.6.1 Change your password

This section allows administrators to change their own password. Administrators can change their own passwords regardless of their access control settings. To change your own password, simply enter your current password, and then enter a new password and confirm the new password.

⚠ Utimaco recommends the local administrators to change their login passwords at regular intervals for security reasons

⚠ LDAP administrators cannot change their passwords on the ESKM appliance. LDAP administrator passwords must be changed on the LDAP server. LDAP administrator passwords are not subject to any of the constraints that apply to other passwords on the ESKM appliance.



Change Your Password

Username:	admin
Current Password:	
New Password:	
Confirm New Password:	

Figure 194 : Change Your Password

The following table describes the components of **Change Your Password**.

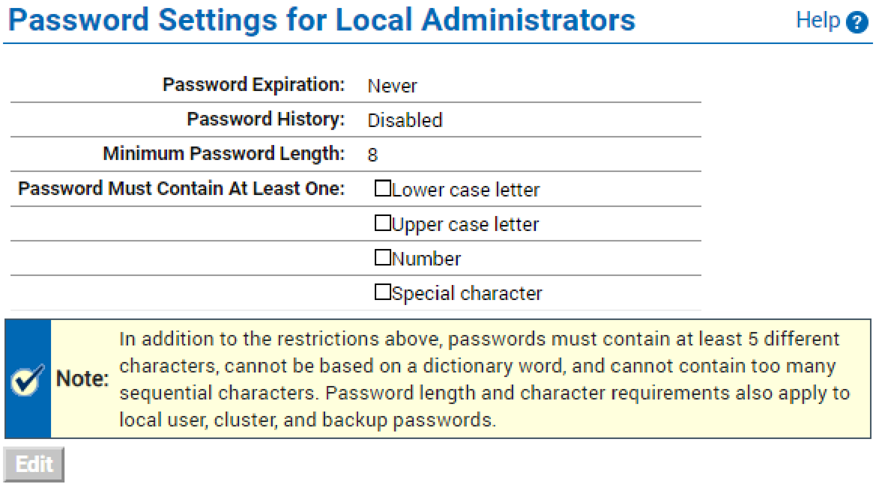
Table 135: Change Your Password components

Component	***Description***
Username	This column displays the login name of the administrator.
Current Password	Enter the current password.
New Password	Enter the new password. The new password must adhere to all of the rules established in **Password Settings for Local Administrators**.
Confirm New Password	Re-enter the new password.
Change Password	Click **Change Password** to implement the changes.

6.21.6.2 Password settings for local administrators

Password Settings for Local Administrators allows you to specify additional password constraints for local administrator passwords. Some of these constraints (password length and character restrictions) also apply to local users, clusters, and backups. The password expiration and password history features apply only to administrators. You must have High Access Administrator access control to make changes to this section.

> ⚠ These settings do not apply to LDAP administrator passwords. LDAP administrator passwords are not subject to any of the constraints that apply to other passwords on the ESKM appliance.



Password Settings for Local Administrators

Password Expiration:	Never
Password History:	Disabled
Minimum Password Length:	8
Password Must Contain At Least One:	□Lower case letter
	□Upper case letter
	□Number
	□Special character

✓ Note: In addition to the restrictions above, passwords must contain at least 5 different characters, cannot be based on a dictionary word, and cannot contain too many sequential characters. Password length and character requirements also apply to local user, cluster, and backup passwords.

Figure 195 : Password Settings for Local Administrators

The following table describes the components of **Password Settings for Local Administrators**.

Table 136: Password Settings for Local Administrators components

Component	***Description***
Password Expiration	Select **Never** to disable the password expiration feature. To enable the feature, enter the maximum number of days for which a password is valid. The maximum is 365 days. Once enabled, this feature applies to all current administrator passwords—all current administrator passwords have the same duration, regardless of when they may have been created initially.
Password History	Select **Disabled** to disable the password history feature. Once disabled, the system deletes the existing password histories. To enable the feature, enter the number of passwords to remember. The acceptable range is from 1 to 25. This feature applies only to administrator passwords.
Minimum Password Length	Enter the minimum password length. The default length is 8. This value applies to all passwords on the ESKM appliance (local administrator, user, backup, tamper resistance, and cluster).

Component	***Description***
Password Must Contain At Least One	Select one or more additional password constraints. You can mandate that the password contains at least one: ▪ Lower case letter ▪ Upper case letter ▪ Number (a numeral between 0 and 9) ▪ Special character (e.g., ! @ # $ % ^ & *) These values apply to all passwords on the ESKM appliance (local administrator, user, backup, and cluster).

> ⚠ Changes made to this section (with the exception of the Password Expiration feature) apply to passwords created after the changes are saved. For example, if all administrator passwords are 8 characters long, and you change the minimum password length to 12 characters, the administrators do not have to immediately change their passwords. Rather, the next time your administrators change their passwords, they must comply with the new rules.

6.21.7 Multiple credentials overview

If your configuration of the ESKM appliance includes multiple administrators, you can stipulate that some administrative and key management operations require authorization from more than one administrator. The multiple credentials feature provides an additional layer of security by protecting your high-level functions.

> ⚠ The multiple credentials feature does not apply to KMIP users, groups or objects.

You can predetermine the number of administrators required to confirm certain operations, let administrators give their credentials to one another for a period of time, and enable multiple credentials functionality within a clustered environment.

6.21.7.1 Operations requiring multiple authentication

When the feature is enabled, the following operations require multiple authentication:

- Disable multiple authorization
- Create/edit/delete/import keys
- Edit a key's owner, delete, and export properties
- Add/edit/delete key group permissions
- Create/edit/delete users
- Create/edit/delete groups
- Add/remove users from a group
- Create/edit/delete authorization policies
- Modify LDAP server settings
- Create/edit/delete administrators
- Restore backups
- Roll back system

Any request for these operations, from either the Management Console or the CLI, results in a request for additional administrator accounts and passwords. The operation only continues when those credentials are supplied. Otherwise, an error message appears.

6.21.7.2 Granting credentials

Administrators can grant their credentials to another administrator for a specific period of time. This allows one administrator to execute several operations without entering multiple credentials for each request. The granting administrator can specify:

- The grantee
- The length of the grant
- The permitted operations

Credentials are granted for a particular administrator account, not a session. This allows an administrator to grant credentials from a different workstation.

> Credential grants cannot be inherited. One administrator can grant only their credentials to one other administrator.

An administrator can grant credentials for the following operations:

- Add/modify keys
- Delete keys
- Add/modify users and groups
- Delete users and groups
- Modify authorization policies
- Modify LDAP settings for users and groups

Administrators who are not normally permitted to execute any of these operations cannot grant credentials for them; those options are unavailable.

Granting a credential does not affect that administrator’s access control privileges. For example, if an administrator does not have the access control for **Keys and Authorization Policies** configuration, that administrator will never be able to create a key, even if another administrator grants credentials to the first administrator.

If an administrator changes the ESKM appliance’s system time or reboots it, all temporary administrator credentials immediately expire.

If the ESKM appliance is configured to use NTP, modifications to the NTP system time can extend the life span of a granted credential.

Granted credentials are not included in backups.

6.21.7.3 Multiple credentials in clusters

To implement multiple credentials on ESKM appliances within a cluster, you must adhere to the following guidelines:

- All ESKM appliances within the cluster must have the multiple credentials feature enabled. The feature can be enabled on one server and replicated to the others.

- For each ESKM appliance within the cluster, the number of administrators with High Access Administrator access control must be greater than or equal to the number of administrators required to authorize an operation. If not, the feature is not be enabled.

To add a new ESKM appliance to a cluster with multiple credentials enabled

1. Ensure that the new ESKM appliance has the correct number of administrators with High Access Administrator access control.

2. Disable the multiple credentials feature for the cluster by disabling the feature for one ESKM appliance within the cluster. This action requires confirmation from multiple administrators.

3. Add the new ESKM appliance to the cluster. For information about adding a new appliance to a cluster, see Join cluster (p. 431).

4. Enable the multiple credentials feature for the cluster by enabling the feature for one ESKM appliance within the cluster.

6.21.7.4 System backup

The following information contained in the Multiple Credentials section of the Management Console is backed up during system backups:

- Status of the Multiple Credentials feature (enabled, disabled)
- Number of administrators required
- Credential timeout limit
- Status of administration via provider (enabled, disabled)

Information about temporarily granted credentials is not backed up.

⚠ Restoring the administration configuration is not possible if the Multiple Credentials feature is enabled but the config file is not included in the backup.

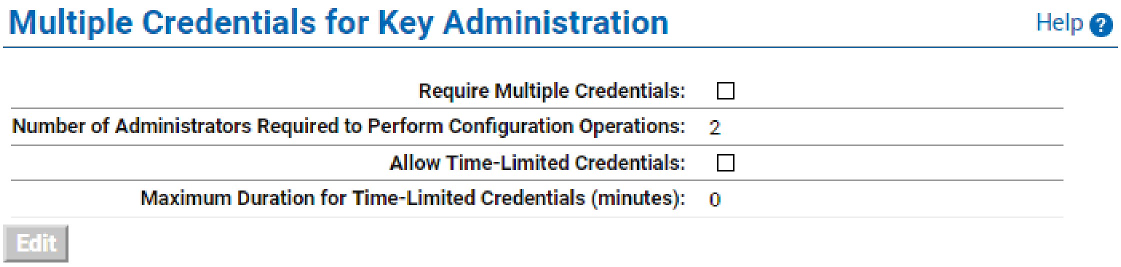
6.21.8 Multiple credentials

Multiple Credentials on the **Administrator Configuration** page lets you enable the multiple credentials feature, grant credentials, and view granted credentials. This page contains the following multiple credentials-related sections:

- Multiple credentials for key administration (p. 501)
- Credentials granted (p. 502)
- Grant a credential (p. 503)

6.21.8.1 Multiple credentials for key administration

Use **Multiple Credentials for Key Administration** to enable the multiple credentials feature, specify the number of administrators required for sensitive operations, enable the granting of credentials, and set the time period for credential grants.



Multiple Credentials for Key Administration

Require Multiple Credentials:	□
Number of Administrators Required to Perform Configuration Operations:	2
Allow Time-Limited Credentials:	□
Maximum Duration for Time-Limited Credentials (minutes):	0

Figure 196 : Multiple Credentials for Key Administration

The following table describes the components of **Multiple Credentials for Key Administration**.

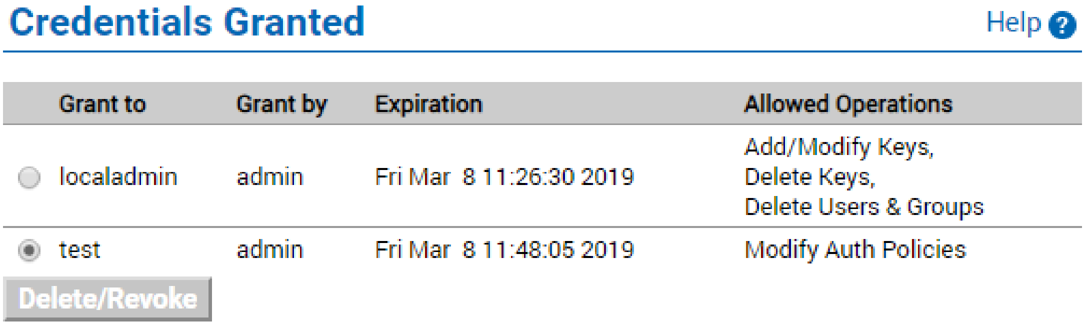
Table 137: Multiple Credentials for Key Administration components

Component	***Description***
Require Multiple Credentials	Select this check box to enable the multiple credentials feature. You must have High Access Administrator access control to enable this feature. De-select this check box to disable the multiple credentials feature. Disabling multiple credentials is governed by the same rules as the operations that require multiple credentials. The specified number of administrators must authorize the action.

Component	***Description***
Number of Administrators Required to Perform Configuration Operations	Select the number of administrators who must authorize the configuration operations. There must be at least as many High Access Administrators as are required by this field.
Allow Time-Limited Credentials	Select this check box to allow administrators to grant their credentials to other administrators for a limited time period.
Maximum Duration for Time-Limited Credentials	Select the maximum length of time that credentials can be granted to another administrator.
Edit	Click **Edit** to modify the multiple credentials settings.

6.21.8.2 Credentials granted

Use **Credentials Granted** to view the credentials granted to or by the current administrator. Any credential grants that do not involve the current administrator are not displayed.



Credentials Granted

	Grant to	Grant by	Expiration	Allowed Operations
○	localadmin	admin	Fri Mar 8 11:26:30 2019	Add/Modify Keys, Delete Keys, Delete Users & Groups
●	test	admin	Fri Mar 8 11:48:05 2019	Modify Auth Policies

Figure 197 : Credentials Granted

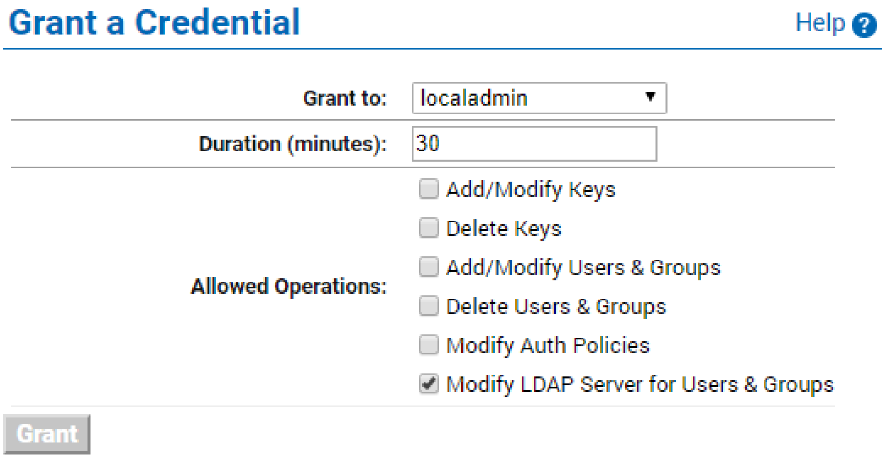
The following table describes the components of **Credentials Granted**.

Table 138: Credentials Granted components

Component	***Description***
Grant to	Displays the administrator receiving the credentials.
Grant by	Displays the administrator granting the credentials.
Expiration	Displays the date and time when the credential grant expires. Credential grants expire automatically if the ESKM appliance is rebooted or the system time is altered.
Allowed Operations	Lists the specific operations for which the credentials have been granted.
Delete/Revoke	Click **Delete/Revoke** to cancel the grant.

6.21.8.3 Grant a credential

Use **Grant a Credential** to grant credentials to another administrator for a specific period of time.



Grant a Credential

Grant to:	localadmin
Duration (minutes):	30
Allowed Operations:	□ Add/Modify Keys □ Delete Keys □ Add/Modify Users & Groups □ Delete Users & Groups □ Modify Auth Policies ☑ Modify LDAP Server for Users & Groups

Figure 198 : Grant a Credential

The following table describes the components of **Grant a Credential**.

Table 139: Grant a Credential components

Component	***Description***
Grant to	Enter the name of the administrator to whom you grant your credentials.
Duration (in minutes)	Enter the duration. This duration cannot be longer than the Maximum Duration for Time-Limited Credentials established in Multiple Credentials for Key Administration.
Allowed Operations	Select the specific operations for which you are granting your credentials. You may only grant credentials for those operations listed here.
Grant	Click **Grant** to execute the credential grant.

6.21.9 Remote administration settings overview

On the remote server side, the public key is saved in a file that contains a list of all authorized public keys. On the user’s side, the public key is stored in SSH key management software or in a file on their computer. The private key remains only on the system being used to access the remote server and is used to decrypt messages.You can administer the ESKM appliance locally and remotely. Local administration involves logging into the ESKM appliance from a workstation that is physically connected to the appliance via a null modem cable. Remote administration involves logging into the appliance from the Management Console or an SSH session. The **Remote Administration Settings**, which are first specified during initial configuration, determine the IP addresses and ports that are used to administer the ESKM appliance.

The Web Admin User Authentication feature provides an additional security safeguard against unauthorized configuration of the ESKM appliance. When this feature is enabled, administrators are asked for a Client Certificate when they attempt to log in to the ESKM appliance. After presenting a client certificate, administrators can only log in to the ESKM appliance with a username that matches the common name field on the client certificate. For example, if the common name of the client certificate is admin, then the administrator can only log in as admin.

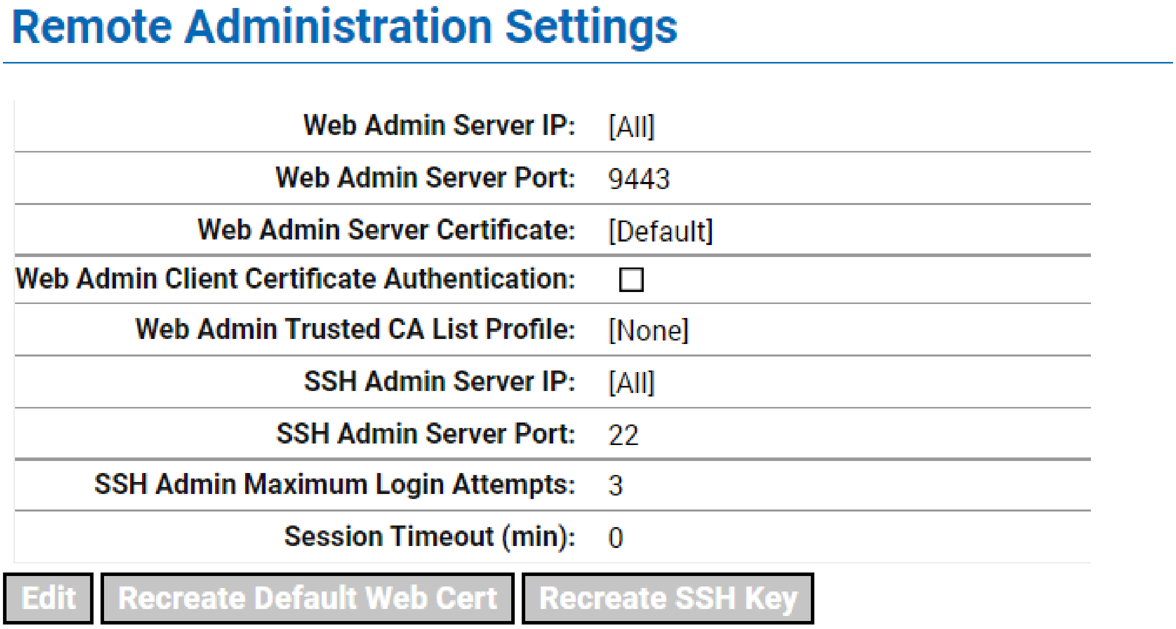
From the **Remote Administrations Settings** page, you can also recreate the Web Administration Certificate and the SSH Key used by the ESKM appliance. The Remote Admin

Certificate is a self-signed certificate created during initial configuration that can be used to verify if the hostname in the certificate matches the hostname of the ESKM appliance being logged into. Because the certificate is only presented to people logging into the Management Console, there is no reason to have the certificate signed by a Certificate Authority. The SSH Key is used to generate a session key that is used for encryption and decryption operations while you are logged into the ESKM appliance.

The SSH public key helps the user to securely transfer backup files to a remote server instead of password based authentication. On the remote server side, the public key is saved in a file that contains a list of all authorized public keys. The private key remains only on ESKM being used to access the remote server while transferring the backups.

6.21.10 Remote administration settings

The **Administrator Configuration** page allows you to configure remote administration.



Remote Administration Settings

Web Admin Server IP:	[All]
Web Admin Server Port:	9443
Web Admin Server Certificate:	[Default]
Web Admin Client Certificate Authentication:	□
Web Admin Trusted CA List Profile:	[None]
SSH Admin Server IP:	[All]
SSH Admin Server Port:	22
SSH Admin Maximum Login Attempts:	3
Session Timeout (min):	0

Figure 199 : Remote Administration Settings

The following table describes the components of the **Remote Administration Settings**.

Table 140: Remote Administration Settings components

Component	***Description***

Web Admin Server IP	The Web Admin Server IP address is the local IP address used to configure the ESKM appliance via the Management Console. You can select one specific IP address or you can select all of the IP addresses bound to the ESKM appliance.
	The IPv4 URI used to connect to the Management Console is:
	`https://IPv4-address:port`
	The IPv6 URI used to connect to the Management Console is:
	`https//[IPv6-address]:port`
	ℹ Utimaco strongly recommends that you limit the Web Admin Server IP to a specific IP address. If you have four IP addresses bound to the ESKM appliance, and you select **All** instead of a specific IP address, then the ESKM appliance "listens" for Web Administration requests on four different IP addresses.
	If you specify a single IP address, the ESKM appliance "listens" for Web Administration requests on only IP address. This can greatly reduce system vulnerability to outside attacks.

Web Admin Server Port	The Web Admin Server Port specifies the port on which the server "listens" for requests. The default port is 9443.

Component	***Description***
Web Admin Server Certificate	The Web Admin Server Certificate specifies the server certificate that is sent to Web Admin client during the handshake portion of the SSL/TLS protocol. The default server certificate is a self-signed certificate. ⚠ If your ESKM appliances are in a cluster and you are selecting a new web admin server certificate, you must first make sure that all of the ESKM appliances in the cluster already have a web admin server certificate installed with this same name.
Web Admin Client Certificate Authentication	The Web Admin Client Certificate Authentication setting activates the Management Console Client Authentication feature, which requires that users present a client certificate when logging into the Management Console. ❗ This feature is immediately enabled when you select this checkbox. If you select this option through the Management Console, you will be immediately logged off and will need a valid client certificate to return. If needed, you can use the edit ras settings (p. 740) command from the CLI to disable this feature without presenting a certificate. For more information about this feature, see Remote administration procedures (p. 141).
Web Admin Trusted CA List Profile	This field allows you to select a profile to use to verify that client certificates are signed by a CA trusted by the ESKM appliance. This option is only valid if you require clients to provide a certificate to authenticate to the ESKM appliance. As delivered, the default Trusted CA List profile contains no CAs. You must either add CAs to the default profile or create a new profile and populate it with at least one trusted CA before the ESKM appliance can authenticate client certificates.

Component	***Description***

SSH Admin Server IP	The SSH Admin Server IP address is the IP address used to configure the ESKM appliance from the CLI. You can select one specific IP address or all of the IP addresses bound to the ESKM appliance.
	The IPv4 URI used to connect to the CLI is:
	`https://IPv4-address:port`
	The IPv6 URI used to connect to the CLI is:
	`https//[Ipv6-address]:port`
	❗ Utimaco strongly recommends that you limit the SSH Admin Server IP to a specific IP address. If you have four IP addresses bound to the ESKM appliance, and you select **All** instead of a specific IP address, then the ESKM appliance "listens" for SSH Administration requests on four different IP addresses.If you specify a single IP address, the ESKM appliance "listens" for SSH Administration requests on only one IP address. This can greatly reduce system vulnerability to outside attacks.

SSH Admin Server Port	The SSH Administration Server Port specifies the port on which the server "listens" for requests. The default port is 22.
SSH Admin Maximum Login Attempts	The SSH Administration Maximum Login Attempts specifies the number of authentication attempts permitted per connection. If the number of failed attempts reaches the limit, the connection gets closed. Allowed range for this parameter is 1-6. The default value is 3.
Session Timeout (min)	The Session Timeout specifies the number of minutes, the Management Console and CLI, remains idle prior to logging off the user. Allowed range for this parameter is 0 to 720. Setting **Session Timeout** to 0 will disable timeout. After changing the value, go to any page for the change to take effect. The default value is 10.

Component	***Description***
Edit	Click **Edit** to modify the remote administrator settings.
Recreate Default Web Cert	Click **Recreate Default Web Cert** to generate a new default certificate for the remote administration Management Console. After you click **Recreate Default Web Cert**, you are presented with an intermediate page that allows you to specify the duration of the default web administration certificate. After you specify a value in days, click **Create**. You must close all browser windows and restart the browser to reconnect to the Management Console.
Recreate SSH Key	Click **Recreate SSH Key** to generate a new key for remote administration use via SSH. Recreating the key closes all active SSH connections.

The following table describes the components of the **SSH Public Key** section.

Table 141: SSH Public Key Components

Component	***Description***
SSH Public Key	The SSH Public Key is displayed in the text box. The user can encrypt the data with this public key and can decrypt with the corresponding private key.
Download	To download the SSH Public Key as a .txt file, click **Download**.
Recreate SSH Public Key	Click **Recreate SSH Public Key** to generate a new key for remote administration use via SSH. A secondary approval is required to make this change, click **Confirm** to proceed. This creates both, a public key and a private key.

SSH Public Key

SSH Public Keys provides a more secure authentication method without the need to use a password.

To use the SSH Public Key

- Copy and paste the SSH Public Key to the relevant path of the remote machine, where the backup is to be saved.
  You can either copy the SSH Public Key displayed in the **Device** > **Administrators** > **Remote Administration** > **SSH Public Key** or click **Download** to download as a text file.

⚠ Make sure the remote machine supports the SSH Public Key authentication.

For example: If you are using OpenSSH, add or append the SSH public key to the file, "*<home directory>/.ssh/authorized_keys*". Check if this file has *755* permission.
To provide the *755* permission, use the command "*chmod 755 <home directory>/.ssh/authorized_keys*".
If there is no "*authorized_keys*" file, create the file and give the *755* permission and then add the key to it.

⚠ Follow your SSH user guide if you use a different SSH protocol.

ℹ

- While creating Scheduled backups, if you choose **SCP with SSH Public Key Authentication** method and the host machine has the public key, there is no need to enter the password.
- Click **Create** to create the Scheduled Backup.

6.22 LDAP administrator server configuration

You configure LDAP servers for administrators separately from LDAP servers for users. This allows for greater flexibility, and simplifies cluster replication, since administrators and users are separately replicated.

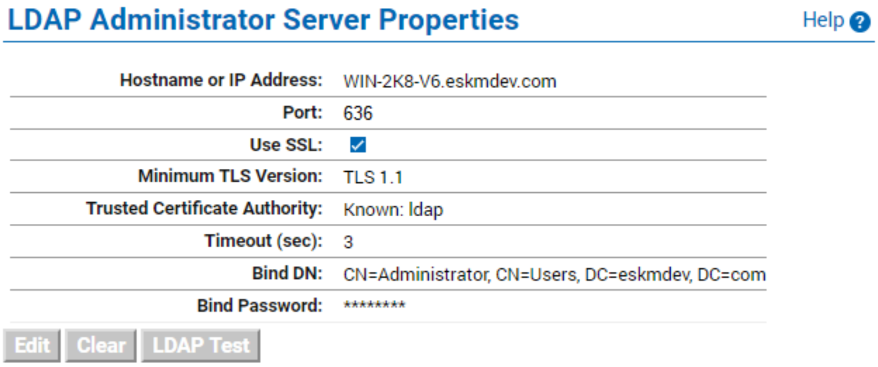
An LDAP account cannot be designated as an administrator if there is already a local administrator account with the same username. Likewise, a local account cannot be created or renamed with the same username as an LDAP account which has been designated as an administrator.

LDAP administrators cannot modify LDAP administrator server settings.

Only IPv4 addresses are supported.

6.22.1 LDAP administrator server properties

Use **LDAP Administrator Server Properties** to define the basic properties of the LDAP administrator directory server.



LDAP Administrator Server Properties

Hostname or IP Address:	WIN-2K8-V6.eskmdev.com
Port:	636
Use SSL:	☑
Minimum TLS Version:	TLS 1.1
Trusted Certificate Authority:	Known: ldap
Timeout (sec):	3
Bind DN:	CN=Administrator, CN=Users, DC=eskmdev, DC=com
Bind Password:	********

Figure 200 : Viewing LDAP Administrator Server Properties

Table 142: LDAP Administrator Server Properties components

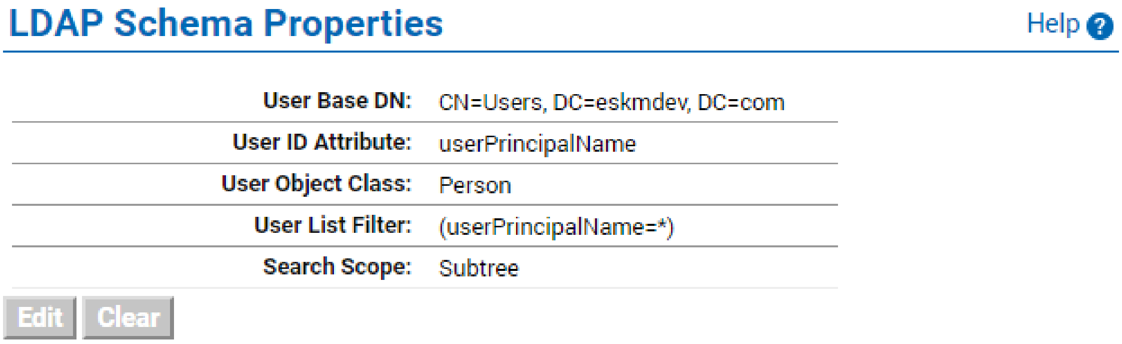
Component	***Description***
Hostname or IP Address	The hostname or IPv4 address of the primary LDAP server.[a]
Port	The port on which the LDAP server is listening. LDAP servers typically use port 389.
Use SSL	By default, the ESKM appliance connects directly to the LDAP server over TCP. Check this box to use SSL between the ESKM appliance and the LDAP server.

Component	***Description***
Minimum TLS Version	Specifies the minimum TLS version.The available versions are TLS 1.0, TLS 1.1, and TLS 1.2. If the server does not support the selected version, the SSL handshake fails. This option is valid only if you use SSL to communicate with the LDAP server.
Trusted Certificate Authority	Select a Trusted Certificate Authority to verify that server certificates presented by LDAP servers are signed by a CA trusted by the ESKM appliance. This option is valid only if you use SSL to communicate with the LDAP server.
Timeout (sec)	The number of seconds to wait for the LDAP server during connections and searches before timing out. If the connection times out, the authorization fails.
Bind DN	The distinguished name (DN) to be used to bind to the server. The ESKM appliance will bind using these credentials to perform searches for users and groups. If your LDAP server supports anonymous searches, you may leave this field and the Bind Password field empty.
Bind Password	The password to be used to bind to the LDAP server.
Edit	Click to modify the properties.
Clear	Click to remove the current properties
LDAP Test	Click to test the LDAP connection after you have defined an LDAP server.

[a] For SSL connections the LDAP server **hostname** should match the **common name** of the **LDAP server certificate**. When hostname is specified in **LDAP configuration**, the DNS server IP needs to be added in **Device >Device Configuration >Hostname & DNS > DNS Server List** to resolve the hostname.

6.22.2 LDAP schema properties

LDAP Schema Properties describes the schema for your LDAP administrator directory.



LDAP Schema Properties

User Base DN:	CN=Users, DC=eskmdev, DC=com
User ID Attribute:	userPrincipalName
User Object Class:	Person
User List Filter:	(userPrincipalName=*)
Search Scope:	Subtree

Figure 201 : Viewing LDAP Schema Properties

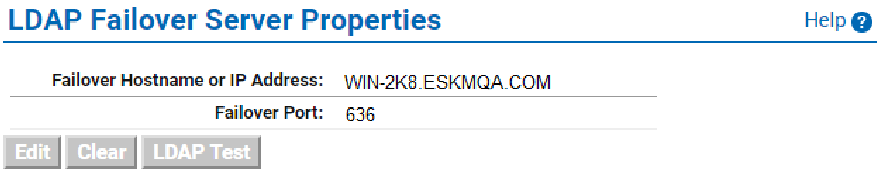
Table 143: LDAP Schema Properties components

Component	***Description***
User Base DN	The base distinguished name (DN) from which to begin the search for usernames.
User ID Attribute	The attribute type for the user on which to search. The attribute type you choose must result in globally unique users.
User Object Class	Used to identify records of users who can be used for authentication.
User List Filter	Used for narrowing the search within the object class.

Component	***Description***
Search Scope	The Search Scope determines how deep within the LDAP user directory the system searches for a user. - **One Level**: search only the children of the base node. - **Sub Tree**: search all the descendants of the base node. Depending on the size of your LDAP directory, this can be very inefficient. ⚠ The LDAP protocol supports four search scopes: Base, One Level, Subtree and Children. You can specify only One Level and Subtree. Note that Subtree includes Base and Children, so by specifying subtree, the search scope includes Subtree, Base, and Children.
Edit	Click to modify the properties.
Clear	Click to remove the current properties.

6.22.3 LDAP schema properties

Use **LDAP Failover Server Properties** to define a backup LDAP server to use in case the main LDAP server becomes inaccessible due to a non-timeout error. When the primary LDAP server is down, the ESKM appliance shifts to the failover LDAP server and periodically retries the primary LDAP server to see if it has become accessible again.



Failover Hostname or IP Address: WIN-2K8.ESKMQA.COM
Failover Port: 636

Figure 202 : LDAP Failover Server Properties

Table 144: LDAP Failover Server Properties components

Component	***Description***
Failover Hostname or IP Address	The hostname or IPv4 address of the LDAP server to use as the failover.
Failover Port	The port on which the LDAP server “listens”.
Edit	Click to modify the properties.
Clear	Click to remove the current properties.
LDAP Test	Click to test the LDAP connection after you have defined an LDAP server.

6.23 Viewing logs and statistics

The ESKM appliance maintains logs and statistics you can use to monitor your ESKM appliance’s performance. The **Log Configuration** and **Log View** pages enable you to configure log rotation schedules, syslog settings, specify log levels, and view and download logs. The Statistics page allows you to view real-time system, connection, and throughput information.

This section contains the following information:

- Logging overview (p. 515)
- Log configuration (p. 521)
- Viewing Statistics (p. 556)

6.23.1 Logging overview

The ESKM appliance maintains a variety of logs to record administrative actions, network activity, cryptography requests, and more. You can schedule log rotations, configure the number of logs archived on the ESKM appliance, stipulate the maximum log file size, and transfer logs to a log server.

The following logs are created:

- System Log — Contains a record of all system events, such as: service starts, stops, and restarts; SNMP traps; hardware failures; successful or failed cluster replication and synchronization; failed log transfers; and license errors.
- Audit Log — Contains a record of all configuration changes and user input errors made to the ESKM appliance, whether through the Management Console or the CLI.
- Activity Log — Contains a record of each request received by the KMS server and the REST server.
- Client Event Log — Contains a record of all client requests containing the `<RecordEventRequest>` element.
- KMIP Log — Contains a record of each request received by the KMIP server.

For each type of log, the current log entries are kept in a file named **Current**.

6.23.2 Log rotation

When a log file is rotated, the Current log file is closed and renamed with a timestamp. This renamed file is then either stored in the log archive or transferred off of the ESKM appliance, depending on your configuration. A new Current log file is then created.

Log rotation occurs according to a configured schedule. Rotation can also occur earlier, if the log file grows to predetermined maximum size. You configure all of these parameters.

Your rotation schedule can be set to automatically rotate logs on a daily, weekly, or monthly basis, at any time of day. The system maintains these settings for each log type; your Activity and Audit logs, for example, can adhere to different schedules.

By specifying a maximum log file size, you can ensure that logs are rotated when they reach a certain size, regardless of their rotation schedule.

For example, you can schedule that system rotate the Audit Log every Sunday morning at 3:15 or when the file size reaches 100 MB, whichever comes first.

6.23.2.1 Log archives

If you do not configure the log transfer feature, old log files are stored on the ESKM appliance. For each type of log, you can select the maximum number of log files that can be archived. When that maximum number is reached, any new addition to the log archive will remove the oldest log file.

For example, suppose you limit the number of archived System Logs to six and do not enable the log transfer feature. After six System Log rotations, the archive is full. The next time you rotate the System log, the oldest System log file on the ESKM appliance will be removed to make room for the latest System log file.

If you limit the number of archived System Logs to six and do enable the log transfer feature, logs that would normally be deleted are instead sent to the transfer destination.

If you set the number of archived logs to zero, no logs will be archived. Rotated logs will either be deleted or sent to the transfer destination, depending on your log transfer settings.

> The ESKM appliance should not be a permanent storage place for log files. You should transfer those files to another location.

6.23.2.2 Log transfer

For more information on streaming Activity and KMIP logs to a remote server, see Syslog settings (p. 525).
The ESKM appliance acts as a temporary repository for logs; *it is not meant to store log files permanently*. Utimaco recommends that you enable the log transfer feature and store your log files on a log server.

There are four different ways you can transfer a log file off of an ESKM appliance:

- SCP
- Browser download
- syslog

The ESKM appliance can transfer log files to a remote host which has an IPv6 address, when IPv6 is enabled on the ESKM appliance (see ipv6 enable (p. 693)) and SCP is used to transfer the files.

When a log is rotated, if you have configured a transfer destination for that log, the appliance attempts to transfer that log file to the location you have specified. If the file transfer fails, the log file sits in a queue as it attempts to transfer the file every two hours until it is successfully transferred. If the ESKM appliance rotates the log before that file is successfully transferred, it attempts to transfer both the current log file and the log file that previously failed to transfer.

Log file naming convention

When a log file is transferred off of the ESKM appliance, the following naming convention is applied:
`<log type>.<archive number>.<datetime stamp>.<hostname>`

Table 145: Log file naming conventions

Value	***Description***
`log type`	The type of log (such as System Log, Audit Log).
`archive number`	This number indicates the file's place in the log archive on the ESKM appliance. "1" indicates the most recent log file.
`datetime stamp`	The date and time when the log file was created.
`hostname`	The hostname of the ESKM appliance.

For example, the filename audit.log.1.2021-08-04_160146.demo would identify this file as:

- An Audit Log
- The first log file in the log index
- A file created on 2021-08-04 at 16:01:46
- A log from the ESKM appliance with the hostname "demo"

This naming convention allows you to transfer log files from multiple servers to the same remote log server while avoiding the problem of overwriting log files due to naming conflicts. These file names are not visible from the CLI or the Management Console.

6.23.3 Syslog

The syslog protocol is used to transmit event notification messages across networks. Messages that are recorded in any of the logs can also be sent to an external server that is configured to receive messages via the syslog protocol.

You can configure one or two syslog servers. When you configure two syslog servers, the ESKM appliance sends syslog messages to both.

You should be aware of the following information before configuring syslog on the ESKM appliance.

- By default, the ESKM appliance transmits messages using syslog facility local1. However, this is configurable on a per-log-basis. See RFC 5424[4], "The Syslog Protocol," for details about syslog.
- Syslog is not a secure protocol. Event notification messages that are sent to an external server are not encrypted or signed. As such, it is not the recommended method for transferring logs from the ESKM appliance.
- Regardless of whether syslog is enabled or disabled for any particular log, all log messages continue to be saved to the normal log files on the ESKM appliance, and all logs still use the traditional rotation/transfer mechanism.
- Changes to the syslog configuration take effect immediately for all logs except the Audit Log. In that case, all existing CLI sessions continue to abide by the syslog settings that were in effect when the CLI session began. After a user ends a CLI session and logs back in, the new syslog settings take effect.

For more information about rotating log files off of the ESKM appliance, see Log rotation (p. 516).

6.23.3.1 Syslog message format

The ESKM appliance will send the syslog messages to the remote syslog server in RFC 5424 format. They appear at the remote syslog server with an additional prefix of: `<TIMESTAMP> < HOSTNAME > <APP-NAME><PROCID>`.
In this case, `<APP-NAME>` might be "KeyManagerSystem," "KeyManagerAudit," "KeyManagerKMIP" or "KeyManagerActivity," depending on the type of the log. `PROCID` is the process ID associated with a syslog system. The message body (the part after < `PROC-`

[4] https://datatracker.ietf.org/doc/html/rfc5424

`ID` >) is the same as the entry in the local log file. An example from the System Log is shown below.

```
original log message:

2019-03-01 11:55:57 eskm_250 KMS Server: Restarted KMS Server.


log message at syslog server (displays on one line):

2019-03-01T11:55:57.388709-07:00 eskm_250 KeyManagerSystem 2195 - -
2019-03-01 11:55:57 eskm_250 KMS Server: Restarted KMS Server.
```

6.23.4 Secure logs

The ESKM appliance allows you to sign your log files before moving them to another machine or downloading them, which makes your log files more secure than unsigned log files.

A Log Signing Certificate is created the first time the ESKM appliance is run and when it is restored to the factory defaults. If the Sign Log option is selected, a log file is signed with the Log Signing Certificate right before it is downloaded or moved off of the appliance. The signed log file is then sent to the specified host in multi-part S/MIME Email format. The first part of the signed log file contains the clear text log; the second part of the signed log file contains the signature in PEM encoded PKCS7 format. The certificate used to verify the signed log file is embedded within the signature, but it is insecure to simply rely on this embedded certificate for verification.

Signed logs do not appear in plain text when downloaded.

> ℹ The log signing certificate is valid for one year. It should be recreated on a yearly basis, see Recreating the log signing certificate (p. 160). Similarly, if a backup which is older than one year and contains the log signing certificate is restored, you must recreate the log signing certificate. It is very important to make a backup of the existing log signing certificate so that old log files signed with the existing certificate can still be properly verified.

You should store your Log Signing Certificate separately from the signed logs files.

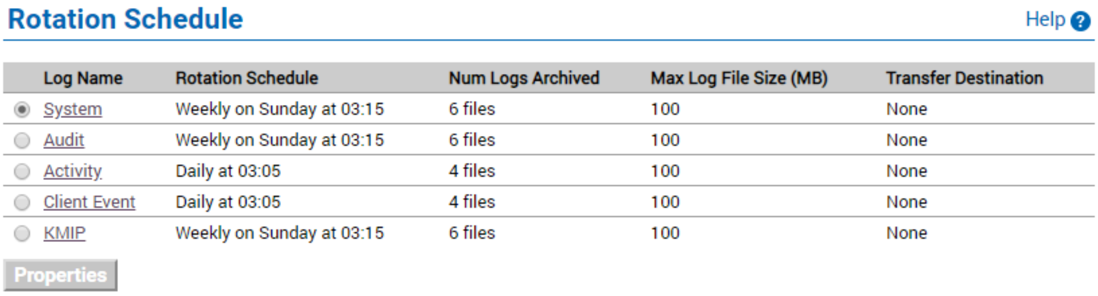
6.23.5 Log configuration

The Log Configuration page allows you to configure rotation schedules, syslog settings, create signed logs, and specify log levels. This page contains the following sections:

- Rotation schedule (p. 521)
- Log rotation properties (p. 523)
- Syslog settings (p. 525)
- Syslog TLS settings (p. 527)
- Log signing (p. 528)
- Log signing certificate information (p. 529)

6.23.5.1 Rotation schedule

The **Rotation Schedule** provides a summary view of the properties of the logs on the ESKM appliance.



Rotation Schedule

	Log Name	Rotation Schedule	Num Logs Archived	Max Log File Size (MB)	Transfer Destination
●	System	Weekly on Sunday at 03:15	6 files	100	None
○	Audit	Weekly on Sunday at 03:15	6 files	100	None
○	Activity	Daily at 03:05	4 files	100	None
○	Client Event	Daily at 03:05	4 files	100	None
○	KMIP	Weekly on Sunday at 03:15	6 files	100	None

Figure 203 : Rotation Schedule

The following table describes the components of the **Rotation Schedule**.

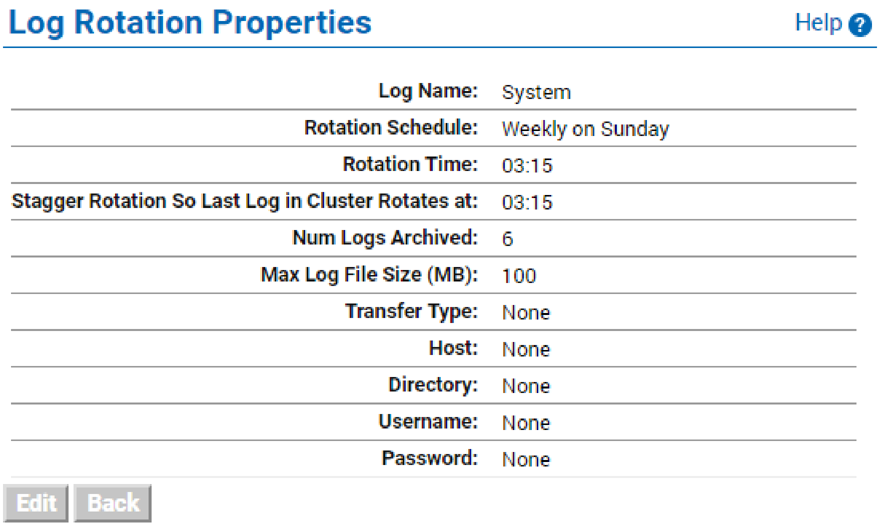
Table 146: Rotation Schedule components

Component	***Description***
Log Name	One of the predefined log names supported by the ESKM appliance. Log types are: System, Audit, Activity, Client Event and KMIP.
Rotation Schedule	Specifies the frequency of log rotation. When a log is rotated, the current log file is closed and a new log file is opened. Supported log rotation frequencies are: ▪ **Daily** — happens at 3:05 AM ▪ **Weekly** — happens at 3:15 AM on Sundays ▪ **Monthly** — happens at 3:25 AM on the first day of the month See Log rotation (p. 516) for more information.
Num Logs Archived	Number of files to retain. Once this limit is reached, a new log file causes the oldest log file to be removed. The maximum number of log files you can retain is 64; the minimum is 0.
Max Log File Size (MB)	Specifies the maximum size log file. When the log file reaches the log file size limit, the system rotates the current file and begins writing to a new file.

Component	***Description***
Transfer Destination	Destination the log files are sent to, as defined by the following entries: ▪ Method for sending the files: select either None, or SCP. None implies that log files will be stored internally on the ESKM appliance. SCP specifies that the log file will be sent via SCP to the specified Hostname. ▪ Host. Name of host to which file will be sent. ▪ Directory. Name of file on host. ▪ Username. Username to use for logging into host. ▪ Password. Password to use for logging into host. The ESKM appliance can transfer log files to a remote host which has an IPv6 address, when IPv6 is enabled on the ESKM appliance (see ipv6 enable (p. 693)) and SCP is used to transfer the files.
Properties	Click **Properties** to access the Log Rotation Properties page and view or edit the properties of a specific log.

6.23.5.2 Log rotation properties

You can view and edit all of the configuration settings for a particular log at **Log Rotation Properties**.



Log Rotation Properties

Log Name:	System
Rotation Schedule:	Weekly on Sunday
Rotation Time:	03:15
Stagger Rotation So Last Log in Cluster Rotates at:	03:15
Num Logs Archived:	6
Max Log File Size (MB):	100
Transfer Type:	None
Host:	None
Directory:	None
Username:	None
Password:	None

Figure 204 : Log Rotation Properties

The following table describes the components of **Log Rotation Properties**.

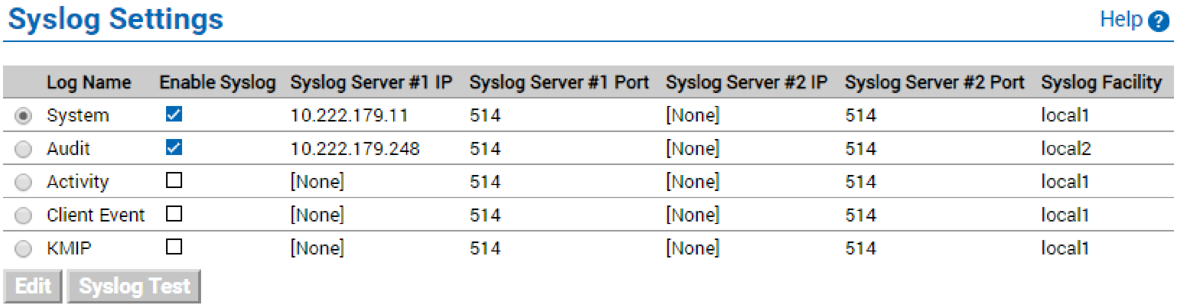
Table 147: Log Rotation Properties components

Component	***Description***
Log Name	One of the predefined log names supported by the ESKM appliance. Log types are: **System**, **Audit**, **Activity**, **Client Event**, and **KMIP**.
Rotation Schedule	Specifies the frequency of log rotation. When a log is rotated, the current log file is closed and a new log file is opened. Supported log rotation frequencies are Daily, Weekly, and Monthly. See Log rotation (p. 516) for more information.
Rotation Time	Specifies the time of day when the log rotation occurs.
Stagger Rotation So Last Log in Cluster Rotates at	Enter the start time for the last log rotation in the cluster. The system calculates the rotation times of all ESKM appliances in the cluster based on this value and the Rotation Time. This field is only available for the ESKM appliances in a cluster that replicates log configuration.

Component	***Description***
Num Logs Archived	Number of files to retain. Once this limit is reached, a new log file causes the oldest log file to be removed. The maximum number of log files you can retain is 64; the minimum is 0.
Max Log File Size (MB)	Specifies the maximum size log file. When the log file reaches the log file size limit, the system rotates the current file and begins writing to a new file.
Transfer Type	Specifies the method for transferring the log file to its destination. SCP indicate that the log file will be sent via SCP to the specified hostname. None implies that the log files will be stored internally on the ESKM appliance.
Host	Specifies the name of the host to which the file will be sent, when the transfer type is SCP.
Directory	Specifies the location of the file on the host.
Username	Specifies the username used for logging into the host.
Password	Specifies the password used for logging into the host.
Edit	Click to alter the log rotation properties.
Back	Click to return to the Log Configuration page.

6.23.5.3 Syslog settings

To enable syslog, select a type of log, and then click **Edit**. Specify a hostname or IPv4/IPv6 address of the primary log server (Syslog Server #1) and the port that the syslog server is listening on. You can optionally specify a backup syslog server by entering an IPv4/IPv6 address and port for the Syslog Server #2 IP and Syslog Server #2 Port fields. Click **Save** when you are done.



Syslog Settings

	Log Name	Enable Syslog	Syslog Server #1 IP	Syslog Server #1 Port	Syslog Server #2 IP	Syslog Server #2 Port	Syslog Facility
●	System	☑	10.222.179.11	514	[None]	514	local1
○	Audit	☑	10.222.179.248	514	[None]	514	local2
○	Activity	□	[None]	514	[None]	514	local1
○	Client Event	□	[None]	514	[None]	514	local1
○	KMIP	□	[None]	514	[None]	514	local1

Figure 205 : Syslog Settings

Changes to the Syslog Settings cause the KMS and KMIP servers to restart, which takes them offline for a few seconds.

Syslog Facility for each log should be unique.

Clicking on **Syslog Test** will test, only the connection on one of the given server IPs (Connection on IP1 will be tested, if IP1 is the given server IP).

The following table describes the components of the **Syslog Settings**.

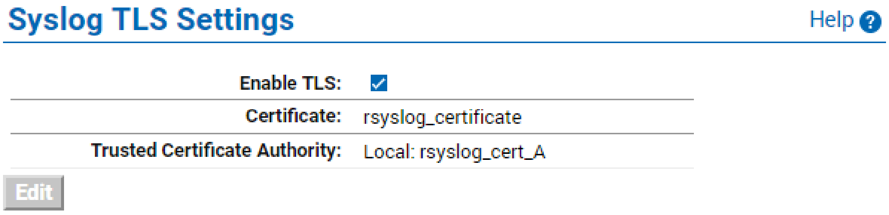
Table 148: Syslog Settings components

Component	***Description***
Log Name	You can enable syslog for the all ESKM appliance logs.
Enable Syslog	If there is a check mark in the box, syslog is enabled. If there is no check mark in the box, syslog is disabled.
Syslog Server#1 IP	Specify a syslog server that should receive event notification messages. You can specify a hostname or an IPv4/IPv6 address.
Syslog Server#1 Port	Specify the port on which the syslog server is “listening”. The default is 514.

Component	***Description***
Syslog Server#2 IP	Specify a syslog server that should receive event notification messages. You can specify a hostname or an IPv4/IPv6 address.
Syslog Server#2 Port	Specify the port on which the syslog server is “listening”. The default is 514.
Syslog Facility	The default is **local1**. You can choose from **local0** to **local7**.
Edit	Click to modify the Syslog settings.
Syslog Test	Click to test the TLS connection after you have defined a syslog server.

6.23.5.4 Syslog TLS settings

To enable TLS for syslog click **Edit**. Select a Trusted Certificate Authority and a certificate in the respective fields. Click **Save** when you are done.



Syslog TLS Settings

Enable TLS:	☑
Certificate:	rsyslog_certificate
Trusted Certificate Authority:	Local: rsyslog_cert_A

Figure 206 : Syslog TLS Settings

The following table describes the components of the **Syslog TLS Settings**.

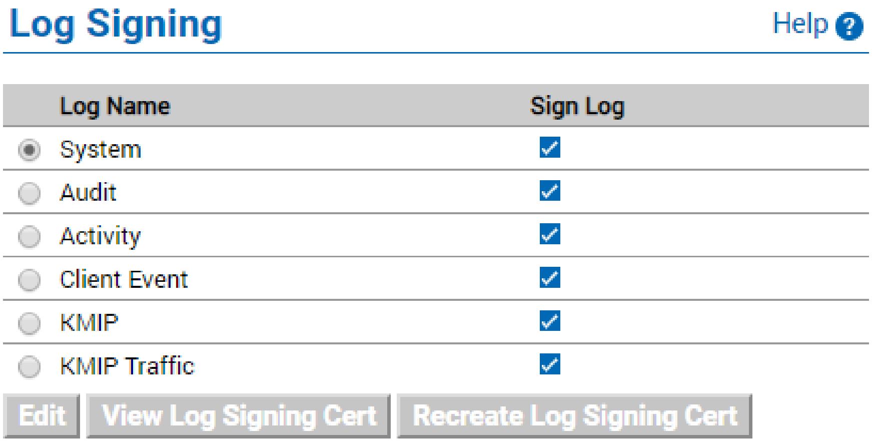
Table 149: Syslog TLS Settings components

Component	***Description***
Enable TLS	You can enable TLS for syslog.

Component	***Description***
Certificate	You must provide the certificate that will be used to authenticate the Syslog Server.
Trusted Certificate Authority	Select to verify the server certificates presented by Syslog server.
Edit	Click to modify the Syslog TLS settings.

6.23.5.5 Log signing

Use this section to select the logs to sign.



	Log Name	Sign Log
●	System	☑
○	Audit	☑
○	Activity	☑
○	Client Event	☑
○	KMIP	☑
○	KMIP Traffic	☑

Figure 207 : Log Signing

The following table describes the components of **Log Signing**.

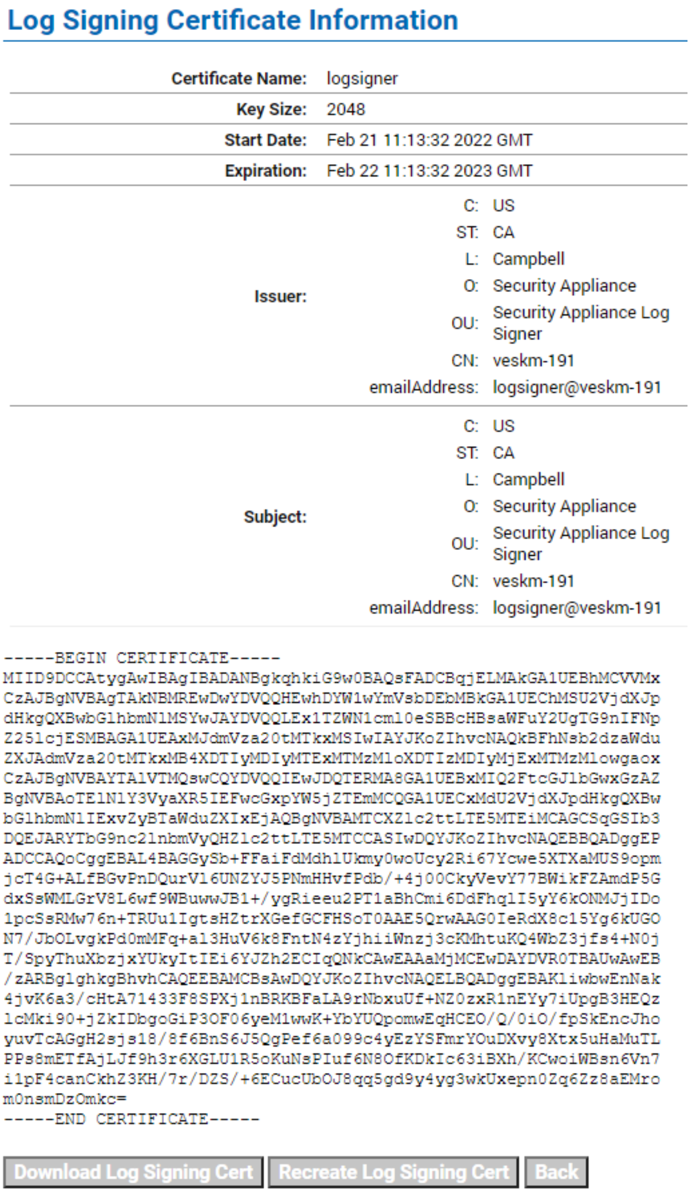
Table 150: Log Signing components

Component	***Description***
Log Name	Displays the logs available on the ESKM appliance.
Sign Log	Select this option to enable Secure Logs. See Secure logs (p. 520) for more information.

Component	*Description*
Edit	Click to edit the log signing settings for the selected log.
View Log Signing Cert	Click to view the Log Signing Certificate information.
Recreate Log Signing Cert	Click to access the Log Signing Certificate to specify the certificate duration and recreate the Log Signing Certificate.

6.23.5.6 Log signing certificate information

Use the Log Signing Certificate Information to view, download, and recreate the log signing certificate.



Log Signing Certificate Information

Certificate Name:	logsigner
Key Size:	2048
Start Date:	Feb 21 11:13:32 2022 GMT
Expiration:	Feb 22 11:13:32 2023 GMT
Issuer:	C: US ST: CA L: Campbell O: Security Appliance OU: Security Appliance Log Signer CN: veskm-191 emailAddress: logsigner@veskm-191
Subject:	C: US ST: CA L: Campbell O: Security Appliance OU: Security Appliance Log Signer CN: veskm-191 emailAddress: logsigner@veskm-191

```
-----BEGIN CERTIFICATE-----
MIID9DCCAtygAwIBAgIBADANBgkqhkiG9w0BAQsFADCBqjELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEbMBkGA1UEChMSU2VjdXJp
dHkgQXBwbGlhbmNlMSYwJAYDVQQLEx1TZWN1cml0eSBBcHBsaWFuY2UgTG9nIFNp
Z25lcjESMBAGA1UEAxMJdmVza20tMTkxMSIwIAYJKoZIhvcNAQkBFhNsb2dzaWdu
ZXJAdmVza20tMTkxMB4XDTIyMDIyMTExMTMzMloXDTIzMDIyMjExMTMzMlowgaox
CzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTERMA8GA1UEBxMIQ2FtcGJlbGwxGzAZ
BgNVBAoTElNlY3VyaXR5IEFwcGxpYW5jZTEmMCQGA1UECxMdU2VjdXJpdHkgQXBw
bGlhbmNlIExvZyBTaWduZXIxEjAQBgNVBAMTCXZlc2ttLTE5MTEiMCAGCSqGSIb3
DQEJARYTbG9nc2lnbmVyQHZlc2ttLTE5MTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAL4BAGGySb+FFaiFdMdhlUkmy0woUcy2Ri67Ycwe5XTXaMUS9opm
jcT4G+ALfBGvPnDQurVl6UNZYJ5PNmHHvfPdb/+4j00CkyVevY77BWikFZAmdP5G
dxSsWMLGrV8L6wf9WBuwwJB1+/ygRieeu2PT1aBhCmi6DdFhqlI5yY6kONMJjIDo
1pcSsRMw76n+TRUu1IgtsHZtrXGefGCFHSoT0AAE5QrwAAG0IeRdX8c15Yg6kUGO
N7/JbOLvgkPd0mMFq+al3HuV6k8FntN4zYjhiiWnzj3cKMhtuKQ4WbZ3jfs4+N0j
T/SpyThuXbzjxYUkyItIEi6YJZh2ECIqQNkCAwEAAaMjMCEwDAYDVR0TBAUwAwEB
/zARBglghkgBhvhCAQEEBAMCBsAwDQYJKoZIhvcNAQELBQADggEBAKliwbwEnNak
4jvK6a3/cHtA71433F8SPXj1nBRKBFaLA9rNbxuUf+NZ0zxR1nEYy7iUpgB3HEQz
lcMki90+jZkIDbgoGiP3OF06yeM1wwK+YbYUQpomwEqHCEO/Q/0iO/fpSkEncJho
yuvTcAGgH2sjs18/8f6BnS6J5QgPef6a099c4yEzYSFmrYOuDXvy8Xtx5uHaMuTL
PPs8mETfAjLJf9h3r6XGLU1R5oKuNsPIuf6N8OfKDkIc63iBXh/KCwoiWBsn6Vn7
i1pF4canCkhZ3KH/7r/DZS/+6ECucUbOJ8qq5gd9y4yg3wkUxepn0Zq6Zz8aEMro
m0nsmDzOmkc=
-----END CERTIFICATE-----
```

Figure 208 : Log Signing Certificate Information

The following table describes the components of the **Log Signing Certificate Information**.

Table 151: Log Signing Certificate Information components

Component	***Description***
Download Log Signing Cert	Click to download the certificate.

Component	***Description***
Recreate Log Signing Cert	Click to access the Log Signing Certificate to specify the certificate duration and recreate the Log Signing Certificate.
Back	Click to return to the Log Configuration page.

6.23.6 Viewing logs

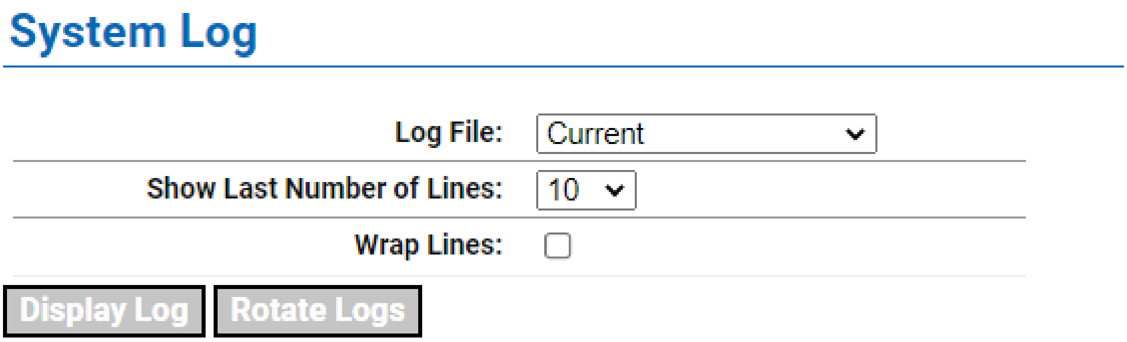
The Log Viewer page allows you to view and download logs. This page contains the following sections:

- System log (p. 531)
- Audit log (p. 533)
- Activity log (p. 535)
- Client event log (p. 542)
- KMIP Log (p. 544)
- REST Log (p. 554)

6.23.6.1 System log

The System Log contains a record of all system events, such as:

- Service starts, stops, and restarts
- REST Server service starts, stops, and restarts
- SNMP traps
- Hardware failures
- Successful or failed cluster replication and synchronization
- Failed log transfers
- License errors



System Log

Log File: Current

Show Last Number of Lines: 10

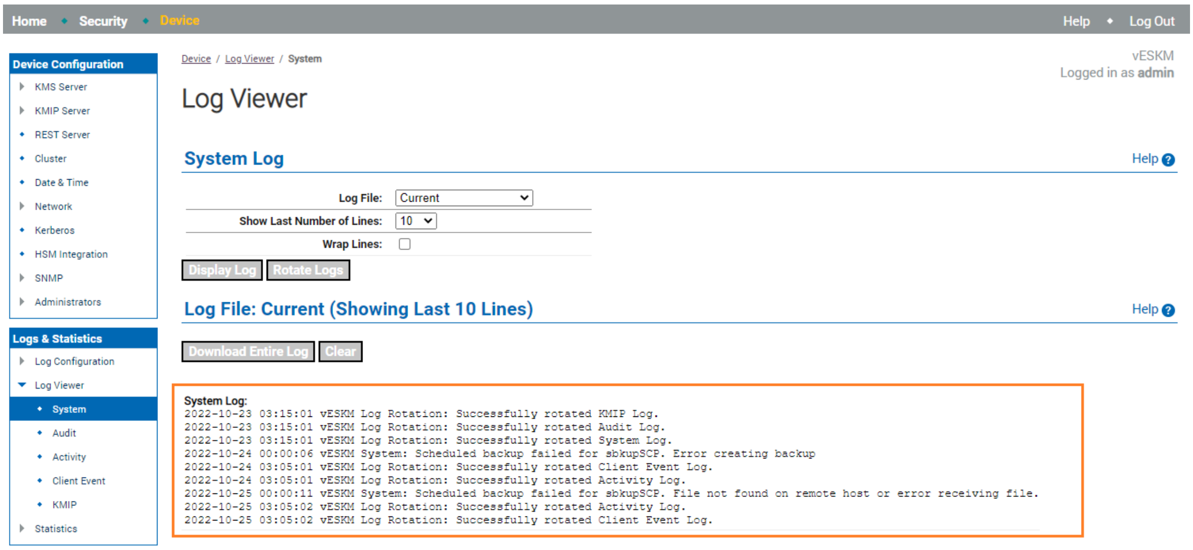
Wrap Lines: □

Figure 209 : System Log

The following table describes the components of the **System Log**.

Table 152: System Log components

Component	***Description***
Log File	Select older logs to display.
Show Last Number of Lines	Select the number of log entries to view.
Wrap Lines	Select to wrap text in the display area.
Display Log	Click to display the last few lines of the log.
Rotate Logs	Click to close the current log and start a new log.



Log File: Current

Show Last Number of Lines: 10

Wrap Lines: ☐

```
System Log:
2022-10-23 03:15:01 vESKM Log Rotation: Successfully rotated KMIP Log.
2022-10-23 03:15:01 vESKM Log Rotation: Successfully rotated Audit Log.
2022-10-23 03:15:01 vESKM Log Rotation: Successfully rotated System Log.
2022-10-24 00:00:06 vESKM System: Scheduled backup failed for sbkupSCP. Error creating backup
2022-10-24 03:05:01 vESKM Log Rotation: Successfully rotated Client Event Log.
2022-10-24 03:05:01 vESKM Log Rotation: Successfully rotated Activity Log.
2022-10-25 00:00:11 vESKM System: Scheduled backup failed for sbkupSCP. File not found on remote host or error receiving file.
2022-10-25 03:05:02 vESKM Log Rotation: Successfully rotated Activity Log.
2022-10-25 03:05:02 vESKM Log Rotation: Successfully rotated Client Event Log.
```

Figure 210 : Current System Log

The following table describes the components of the **Current Log**.

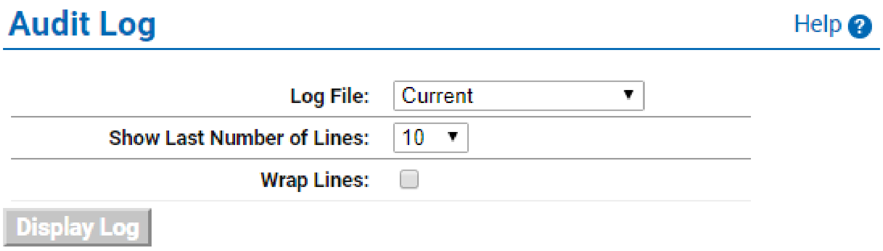
Table 153: Current System Log components

Component	***Description***
Download Entire Log	Click to download the log to your browser.
Clear	Click to delete the select log.

6.23.6.2 Audit log

The Audit Log contains a record of all configuration changes and user input errors made to the ESKM appliance, whether through the Management Console or the CLI. Each line in the audit log corresponds to one configuration change. Lines in the audit log contain the following information in the order shown:

- Date and time change was made.
- Username: the username that made the configuration change.
- Event: a text description of the configuration change.



Log File: Current

Show Last Number of Lines: 10

Wrap Lines: □

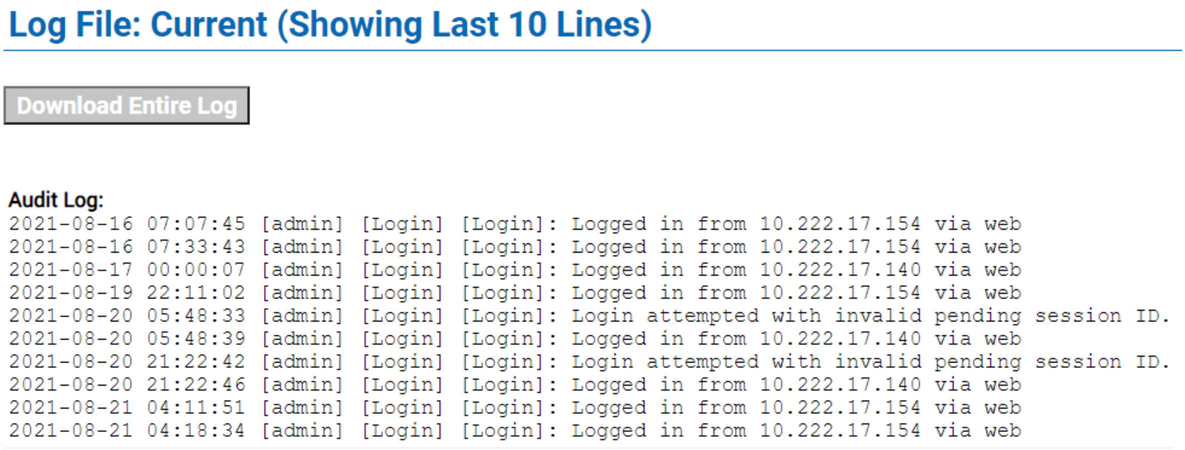
Figure 211 : Audit Log

The following table describes the components of the **Audit Log**.

Table 154: Audit Log components

Component	***Description***
Log File	Select older logs to display.
Show Last Number of Lines	Select the number of log entries to view.
Wrap Lines	Select to wrap text in the display area.
Display Log	Click to display the last few lines of the log.

Current audit log



Log File: Current (Showing Last 10 Lines)

Audit Log:

```
2021-08-16 07:07:45 [admin] [Login] [Login]: Logged in from 10.222.17.154 via web
2021-08-16 07:33:43 [admin] [Login] [Login]: Logged in from 10.222.17.154 via web
2021-08-17 00:00:07 [admin] [Login] [Login]: Logged in from 10.222.17.140 via web
2021-08-19 22:11:02 [admin] [Login] [Login]: Logged in from 10.222.17.154 via web
2021-08-20 05:48:33 [admin] [Login] [Login]: Login attempted with invalid pending session ID.
2021-08-20 05:48:39 [admin] [Login] [Login]: Logged in from 10.222.17.140 via web
2021-08-20 21:22:42 [admin] [Login] [Login]: Login attempted with invalid pending session ID.
2021-08-20 21:22:46 [admin] [Login] [Login]: Logged in from 10.222.17.140 via web
2021-08-21 04:11:51 [admin] [Login] [Login]: Logged in from 10.222.17.154 via web
2021-08-21 04:18:34 [admin] [Login] [Login]: Logged in from 10.222.17.154 via web
```

Figure 212 : Current Audit Log

The following table describes the components of the **Current Audit Log**.

Table 155: Current Audit Log components

Component	***Description***
Download Entire Log	Click to download the log to your browser.

6.23.6.3 Activity log

The Activity Log contains a record of each request received by the KMS server. For client requests that contain multiple cryptographic operations, each operation is logged as a separate entry in the Activity Log. Requests for cryptographic operations are not logged until the KMS server has received all the data from the client or an error has occurred. When there is no data for a particular field, a dash is inserted. The format of the Activity Log is as follows: `<date> <priority> <ip> <common name> <user> <request id> <request type> <key> <detail> <error code>` `<message>`

The following table describes the fields that are present in the **Activity Log**.

Table 156: Fields in the Activity Log

Field	***Description***
`date`	Enclosed in brackets ([ ]), the date field shows the date and time that the ESKM appliance finished processing the request, specified in the local time zone. The date and time are represented as follows: `yyyy-mm-dd hh:mm:ss`.
`priority`	ERROR or INFO, depending on the result of the request.
`ip`	IP address of the client machine.
`common name`	Enclosed in brackets ([ ]), the common name field displays the common name defined in the certificate that was provided by the client. This field only has data when you require client authentication.
`user`	Authenticated user who issued the request.
`request id`	Request ID of the client request.
`request type`	Type of client request; the request type field is the name of the XML request without the suffix “Request.” For example, a KeyGenRequest log entry would have a request type value of “KeyGen.”
`key`	Name of the key specified in the request.
`detail`	Enclosed in brackets ([ ]), the detail field provides different information based on the type of request; the details field is described in the tabe below (p. 537).
`error code`	Numerical error code returned to the client.

Field	Description
`message`	Enclosed in brackets ([ ]), the message field displays either "Success" if the ESKM appliance was able to fulfill the request, or, if there was an error, this field displays the error message that coincides with the appropriate numerical error code.

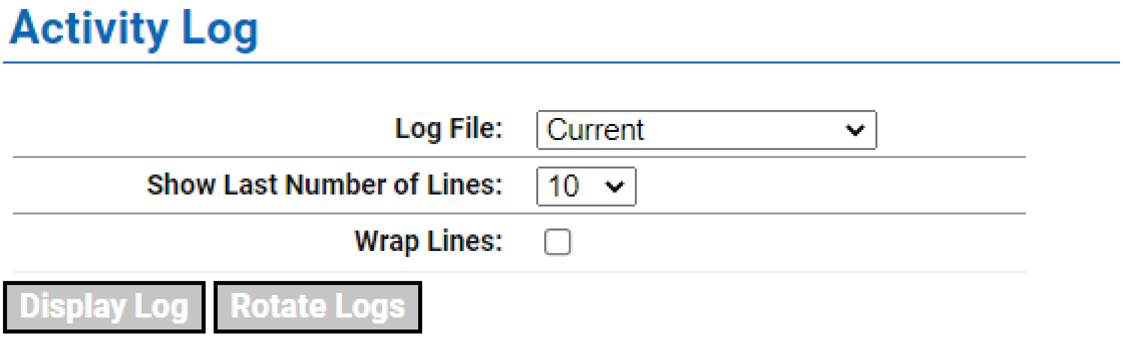
As mentioned, the detail field provides different information depending on what the client requests. The following table lists the different types of requests the client might submit and then describes what information is present in the detail field for each request.

Table 157: Values for the Detail Field in the Activity Log

Request Type	Detail Information
authentication	Username provided by the client.
key generation	Algorithm and key size; the value for the Deletable and Exportable options are listed as well if they are set by the client.
key import	Algorithm and key size specified in the request; the value for the Deletable and Exportable options are listed as well if they are set by the client.
key deletion	Nothing is listed in the detail field.
key export	Nothing is listed in the detail field.
random number generation	Size in bytes of the random number being generated.
replication export	Nothing is listed in the detail field.
replication import	Nothing is listed in the detail field.
key information	Nothing is listed in the detail field.

Request Type	***Detail Information***
key queries	Nothing is listed in the detail field.
cryptographic	Ordinal number of the operation, the name of the operation, and the algorithm (including mode and padding).

The following figure shows an example of the **Activity Log**.



Activity Log

Log File:	Current
Show Last Number of Lines:	10
Wrap Lines:	□

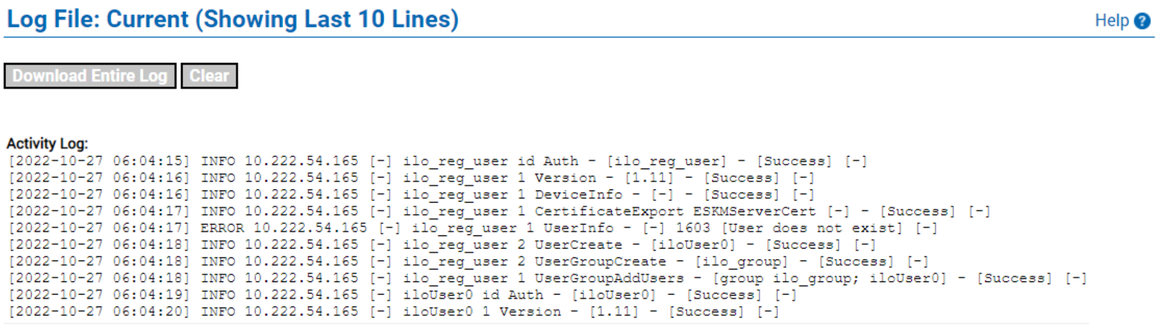
Figure 213 : Activity Log

The following table describes the components of the **Activity Log**.

Table 158: Activity Log components

Component	***Description***
Log File	Select older logs to display.
Show Last Number of Lines	Select the number of log entries to view.
Wrap Lines	Select to wrap text in the display area.
Display Log	Click to display the specified number of lines of the log.
Rotate Logs	Click to close current log and start a new log.

Current activity log



Activity Log:

```
[2022-10-27 06:04:15] INFO 10.222.54.165 [-] ilo_reg_user id Auth - [ilo_reg_user] - [Success] [-]
[2022-10-27 06:04:16] INFO 10.222.54.165 [-] ilo_reg_user 1 Version - [1.11] - [Success] [-]
[2022-10-27 06:04:16] INFO 10.222.54.165 [-] ilo_reg_user 1 DeviceInfo - [-] - [Success] [-]
[2022-10-27 06:04:17] INFO 10.222.54.165 [-] ilo_reg_user 1 CertificateExport ESKMServerCert [-] - [Success] [-]
[2022-10-27 06:04:17] ERROR 10.222.54.165 [-] ilo_reg_user 1 UserInfo - [-] 1603 [User does not exist] [-]
[2022-10-27 06:04:18] INFO 10.222.54.165 [-] ilo_reg_user 2 UserCreate - [iloUser0] - [Success] [-]
[2022-10-27 06:04:18] INFO 10.222.54.165 [-] ilo_reg_user 2 UserGroupCreate - [ilo_group] - [Success] [-]
[2022-10-27 06:04:18] INFO 10.222.54.165 [-] ilo_reg_user 1 UserGroupAddUsers - [group ilo_group; iloUser0] - [Success] [-]
[2022-10-27 06:04:19] INFO 10.222.54.165 [-] iloUser0 id Auth - [iloUser0] - [Success] [-]
[2022-10-27 06:04:20] INFO 10.222.54.165 [-] iloUser0 1 Version - [1.11] - [Success] [-]
```

Figure 214 : Current Activity Log

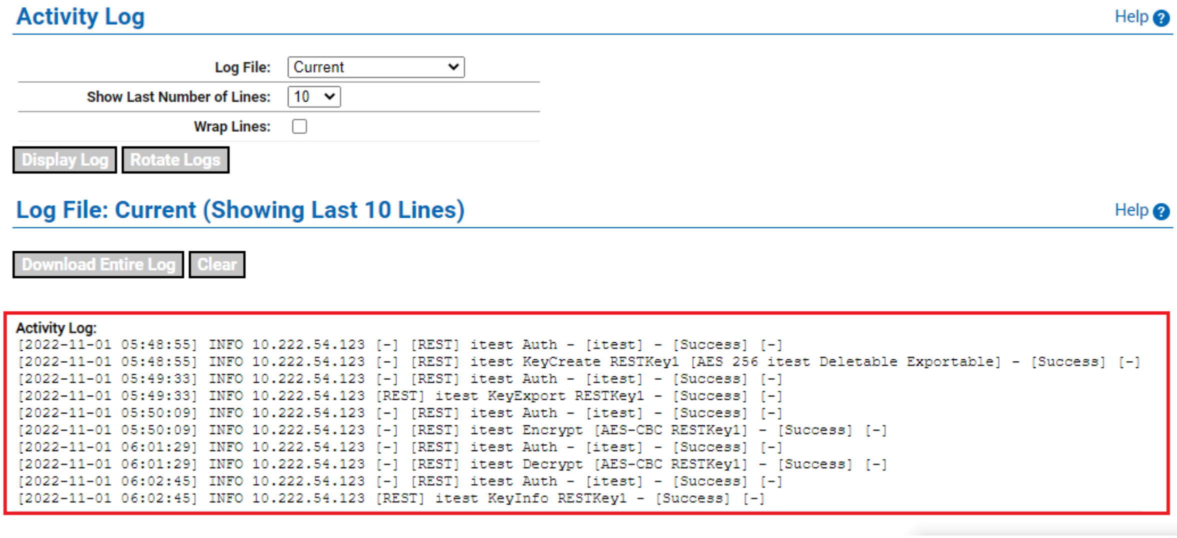
The following table describes the components of the **Current Activity Log**.

Table 159: Current Activity Log components

Component	***Description***
Download Entire Log	Click to download the log to your browser.
Clear	Click to delete the select log.

6.23.6.3.1 Activity log - REST

The Activity Log also contains a record of each cryptographic key management request received by the REST server.



Log File: Current

Show Last Number of Lines: 10

Wrap Lines: □

Activity Log:

```
[2022-11-01 05:48:55] INFO 10.222.54.123 [-] [REST] itest Auth - [itest] - [Success] [-]
[2022-11-01 05:48:55] INFO 10.222.54.123 [-] [REST] itest KeyCreate RESTKey1 [AES 256 itest Deletable Exportable] - [Success] [-]
[2022-11-01 05:49:33] INFO 10.222.54.123 [-] [REST] itest Auth - [itest] - [Success] [-]
[2022-11-01 05:49:33] INFO 10.222.54.123 [REST] itest KeyExport RESTKey1 - [Success] [-]
[2022-11-01 05:50:09] INFO 10.222.54.123 [-] [REST] itest Auth - [itest] - [Success] [-]
[2022-11-01 05:50:09] INFO 10.222.54.123 [-] [REST] itest Encrypt [AES-CBC RESTKey1] - [Success] [-]
[2022-11-01 06:01:29] INFO 10.222.54.123 [-] [REST] itest Auth - [itest] - [Success] [-]
[2022-11-01 06:01:29] INFO 10.222.54.123 [-] [REST] itest Decrypt [AES-CBC RESTKey1] - [Success] [-]
[2022-11-01 06:02:45] INFO 10.222.54.123 [-] [REST] itest Auth - [itest] - [Success] [-]
[2022-11-01 06:02:45] INFO 10.222.54.123 [REST] itest KeyInfo RESTKey1 - [Success] [-]
```

Figure 215 : Activity Log - REST

The format of the Activity Log for the requests received by REST server is as follows: `<date> <priority> <ip> <REST> <user> <request type> <key> <detail> <message>`

The following table describes the fields that are present in the **Activity Log** for REST requests.

Table 160: Activity Log - REST requests

Field	***Description***
`date`	Enclosed in brackets [ ], the date field shows the date and time when the ESKM finished processing the request. The date and time are represented as follows: `yyyy-mm-dd hh:mm:ss` (local time zone).
`priority`	ERROR or INFO, depending on the result of the request.
`ip`	IP address of the client machine.
`REST`	The requests received by the REST server have **REST** in the Activity Log entries.
`user`	Authenticated user who issued the request.

Field	***Description***
`request type`	Type of client request. The request type can take one of the below values. ▪ `KeyInfo` - Request to retrieve key information ▪ `KeyExport` - Request to export key bytes along with the key information ▪ `KeyCreate` - Request to create a key ▪ `KeyModify` - Request to update an existing key ▪ `KeyDelete` - Request to delete a key ▪ `Auth` - Authenticating the user ▪ `Encrypt` - Request to encrypt the data ▪ `Decrypt` - Request to decrypt the data
`key`	The name of the key in the request. `Auth` request types have the authenticating user in [], instead of the key name.
`detail` (only for `KeyCreate`, `Encrypt` and `Decrypt` request types)	This field is enclosed in [] and lists the algorithm, size, and key owner for key operations and algorithm-mode and key used for encryption/decryption. Deletable and Exportable options are listed if set, for the key operations.
`message`	`[Success]` - If the operation is successful `[Error message]` followed by `[Failed]` - If the operation failed

6.23.6.4 Client event log

The Client Event Log contains a record of each message sent by clients using the <RecordEventRequest> element. The client event data must be base64-encoded. When there is no data for a particular field, a dash is inserted. The format of the Client Event Log is as follows:

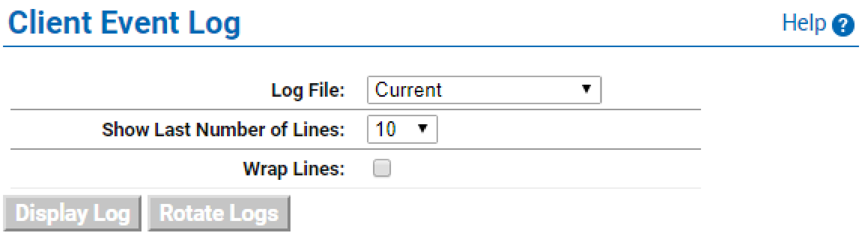
```
<date> <priority> <ip> <common name> <user> <request id> <message>
```

The following table describes the fields that are present in the **Client Event Log**.

Table 161: Fields in the Client Event Log

Field	***Description***
`date`	Enclosed in brackets ([ ]), the date field shows the date and time that the ESKM appliance finished processing the request, specified in the local time zone. The date and time are represented as follows: `yyyy-mm-dd hh:mm:ss` .
`priority`	`ERROR` or `INFO` , depending on the result of the request.
`ip`	IP address of the client machine.
`common name`	Enclosed in brackets ([ ]), the common name field displays the common name defined in the certificate that was provided by the client. This field only has data when you require client authentication.
`user`	Authenticated user that issued the request.
`request id`	Request ID of the client request.
`message`	Enclosed in brackets ([ ]), the message field displays the plaintext that corresponds with the base64 encoded message included in the client event.

The following figure shows an example of the **Client Event Log**.



Client Event Log

Log File: Current

Show Last Number of Lines: 10

Wrap Lines: □

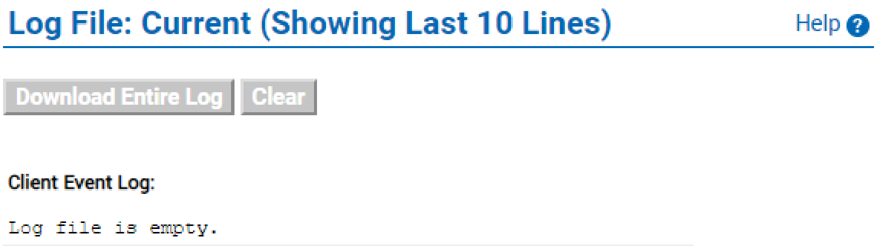
Figure 216 : Client Event Log

The following table describes the components of the **Client Event Log**.

Table 162: Client Event Log components

Component	***Description***
Log File	Select older logs to display.
Show Last Number of Lines	Select the number of log entries to view.
Wrap Lines	Select to wrap text in the display area.
Display Log	Click to display the specified number of lines of the log.
Rotate Logs	Click to close current log and start a new log.

Current Client Event log



Log File: Current (Showing Last 10 Lines)

Client Event Log:

```
Log file is empty.
```

Figure 217 : Current Client Event Log

The following table describes the components of the **Current Client Event Log**.

Table 163: Current Client Event Log components

Component	***Description***
Download Entire Log	Click to download the log to your browser.
Clear	Click to delete the select log.

6.23.6.5 KMIP Log

The KMIP Log contains a record of each request received by the KMIP server.

For client requests that contain multiple KMIP operations, each operation is logged as a separate entry in the KMIP Log.

Requests for KMIP operations do not appear in the log until the KMIP server has received all of the relevant data from the client, or until an error has occurred. When there is no relevant data for a field, a dash is inserted.

The format of the KMIP Log is as follows:

```
<date> <hostname> User:[<username>]UUID:[<uuid>] Operation:[<operation>] Object Type:[<object-type>] Result:[<result>] [Reason:<reason>] Message:[<message>]
```

The following table describes the fields that are present in the **KMIP Log**.

Table 164: Fields in the KMIP Log

Field	***Description***
`date`	The date field shows the date and time that the ESKM appliance finished processing the request, specified in the local time zone. The date and time are represented as follows: `yyyy-mm-dd hh:mm:ss.`

Field	*Description*
`hostname`	The host name of the ESKM appliance.
`operation type`	Enclosed in brackets (**[ ]**),the operation type, for example `[Client Operation]` or `[State Change]` .
`User`	Enclosed in brackets (**[ ]**), the username of the KMIP client that sent this KMIP operation request.
`UUID`	Enclosed in brackets (**[ ]**), the unique identifier for the target KMIP object for which the client request applies. In the event that a single KMIP client request involves more than one KMIP object, only the UUID of the first object is shown.
`Operation`	Enclosed in brackets (**[ ]**), the KMIP operation.
`Object type`	Enclosed in brackets (**[ ]**), the type of object specified in the UUID, if available. This field is not always available, however; for example, a client request specifying an invalid UUID will not have an object type in the log.
`Result`	Enclosed in brackets (**[ ]**), the result of the KMIP operation, including `[SUCCESS]` or a short keyword indicating failure, such as `[OPERATION_FAILED].`
`Reason`	Enclosed in brackets (**[ ]**), the short keyword representing the reason for the reported result; for example: `[ITEM_NOT_FOUND].`
`Message`	Enclosed in brackets (**[ ]**), more information on the failed operation, if available; for example: `[NOT_FOUND]` .

Multiple entries of a log event are suppressed into a single log event with a count for number of times it is repeated.

- The log event repeats every minute. In this case, it is suppressed and displayed with the count after the reset time of the flag, which is 60 minutes. Any further repetition is a new log event.
- The event repeats every minute, for example, 20 minutes, and then does not repeat in the next minute. In this case, it is displayed with the repetition count after 21 minutes in the KMIP Log. Any further repetition is considered a new log event.

The event doesn't repeat in the next minute after it is received for the first time. No additional steps are performed in this case.The following table lists the KMIP operations supported by the ESKM appliance.

Table 165: KMIP Operations

Operation	***Description***
KMIP Version 1.0 Client-to-Server Operations	
Activate	This operation requests the ESKM to activate a Managed Cryptographic Object.
Add Attribute	This operation requests the ESKM to add a new attribute instance to be associated with a Managed Object and set its value.
Archive	This operation is used to specify that a Managed Object may be archived.
Cancel	This operation requests the ESKM to cancel an outstanding asynchronous operation.
Check	This operation requests that the ESKM check for the use of a Managed Object according to values specified in the request.
Certify	This request is used to generate a Certificate object for a public key.

Operation	***Description***
Create	This operation requests the ESKM to generate a new symmetric key as a Managed Cryptographic Object.
Create Key Pair	This operation requests the ESKM to generate a new public/ private key pair and register the two corresponding new Managed Cryptographic Objects.
Delete Attribute	This operation requests the ESKM to delete an attribute associated with a Managed Object.
Destroy	This operation is used to indicate to the ESKM that the key material for the specified Managed Object shall be destroyed.
Get	This operation requests that the ESKM returns the Managed Object specified by its Unique Identifier.
Get Attributes	This operation requests one or more attributes of a Managed Object.
Get Attributes List	This operation requests a list of the attribute names associated with a Managed Object.
Get Usage Allocation	This operation requests the ESKM to obtain an allocation from the current Usage Limits value to allow the client to use the Managed Cryptographic Object for applying cryptographic protection.
Locate	This operation requests that the ESKM search for one or more Managed Objects depending on the attributes specified in the request.
Modify Attribute	This operation requests the ESKM to modify the value of an existing attribute instance associated with a Managed Object.

Operation	***Description***
Obtain Lease	This operation requests the ESKM to obtain a new Lease Time for a specified Managed Object.
Poll	This operation requests the ESKM to cancel an outstanding asynchronous operation.
Query	This operation is used by the client to interrogate the ESKM to determine its capabilities and/or protocol mechanisms.
Recover	This operation is used to obtain access to a Managed Object that has been archived.
Register	This operation requests the ESKM to register a Managed Object that was created by the client or obtained by the client through some other means, allowing the ESKM to manage the object.
Re-key	This request is used to generate a replacement key for an existing symmetric key.
Re-certify	This request is used to renew an existing certificate for the same key pair.
Revoke	This operation requests the ESKM to revoke a Managed Cryptographic Object or an Opaque Object.
Validate	This operation requests that the ESKM validate a certificate chain and return information on its validity.
KMIP Version 1.1 Operations (all above operations plus these additional operations.)	
Discover Versions	This request is used by the client to determine a list of protocol versions that is supported by the ESKM.

Operation	*Description*
Re-key Key Pair	This request is used to generate a replacement key pair for an existing public/private key pair.
KMIP Version 1.2 Operations (all above operations plus these additional operations.)	
Create Split Key	This operation requests the ESKM to generate a new split key and register all the splits as individual new Managed Cryptographic Objects.
Decrypt	This operation requests the ESKM to perform a decryption operation on the provided data using a Managed Cryptographic Object as the key for the decryption operation.
Encrypt	This operation requests the ESKM to perform an encryption operation on the provided data using a Managed Cryptographic Object as the key for the encryption operation.
Hash	This operation requests the ESKM to perform a hash operation on the data provided.
Join Split Key	This operation requests the ESKM to combine a list of Split Keys into a single Managed Cryptographic Object.
MAC	This operation requests the ESKM to perform message authentication code (MAC) operation on the provided data using a Managed Cryptographic Object as the key for the MAC operation.
MAC Verify	This operation requests the ESKM to perform message authentication code (MAC) verify operation on the provided data using a Managed Cryptographic Object as the key for the MAC verify operation.
RNG Retrieve	This operation requests the ESKM to return output from a Random Number Generator (RNG).

Operation	***Description***
RNG Seed	This operation requests the ESKM to seed a Random Number Generator.
Sign	This operation requests the ESKM to perform a signature operation on the provided data using a Managed Cryptographic Object as the key for the signature operation.
Signature Verify	This operation requests the ESKM to perform a signature verify operation on the provided data using a Managed Cryptographic Object as the key for the signature verification operation.
KMIP Version 1.4 Operations (all above operations plus these additional operations.)	
Export	This operation requests that the ESKM returns a Managed Object specified by its Unique Identifier, together with its attributes.
Import	This operation requests the ESKM to Import a Managed Object specified by its Unique Identifier.
KMIP Version 2.1 Operations (all above operations plus these additional operations.)	
Set Defaults	This operation instructs the ESKM to set the default attributes that will be applied to Managed Objects during factory operations if the client does not supply values for mandatory attributes
Set Constraints	This operation instructs the ESKM to set the constraints that will be applied to Managed Objects during operations.
Get Constraints	This operation instructs the ESKM to return the constraints that are being applied to Managed Objects during operations.

Operation	***Description***
Query Asynchronous Requests	This operation requests the ESKM to report on any asynchronous requests that have been made for which results have not yet been obtained via the normal Poll (or less-normal Cancel) operation.
Process	This operation requests the ESKM to modify its processing of a previously-submitted asynchronous request such that the next Poll for that asynchronous request shall not return a "pending" status, effectively changing the processing mode for that batch item to that resembling synchronous processing. ⚠ This may have processing implications for other items in that same batch if Batch Order Option is True, which is the default.
Ping	This operation is used to determine if an ESKM is alive and responding. The ESKM may treat the Ping operation as a non-logged operation.

The following table lists the KMIP Object Types supported by the ESKM appliance.

Table 166: KMIP Object Types

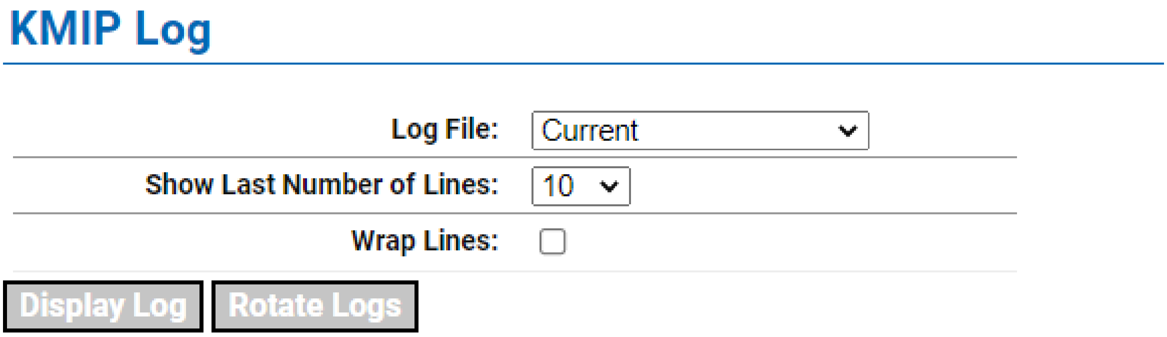
Object Type	***Description***
KMIP Version 1.0 and 1.1 Object Types	
Certificate	A Managed Cryptographic Object that is a digital certificate.
Symmetric Key	A Managed Cryptographic Object that is a symmetric key.
Secret Data	A Managed Cryptographic Object containing a shared secret value that is not a key or certificate (e.g., a password).

Object Type	***Description***
Public Key	A Managed Cryptographic Object that is the public portion of an asymmetric key pair.
Private Key	A Managed Cryptographic Object that is the private portion of an asymmetric key pair.
Template[a]	A Template is a named Managed Object containing the client-settable attributes of a Managed Cryptographic Object (i.e., a stored, named list of attributes).
Opaque Object	A Managed Object that the key management server is possibly not able to interpret.
Split Key	A Managed Cryptographic Object that is a split key.
KMIP Version 1.2 Object Types (all above object types plus these additions.)	
PGP Key[b]	A Managed Cryptographic Object that is a text-based representation of a PGP key.
KMIP Version 1.3[a] Object Types (all above object types from previous versions; no additions.)	
KMIP Version 1.4 Object Types (all above object types from previous versions; no additions.)	
KMIP Version 2.0 Object Types (all above object types except PGP key & Template plus the below additions.)	
Certificate Request	A Managed Cryptographic Object containing the certificate request.

[a]The Template Managed Object is deprecated as of version 1.3 and is removed in version 2.0. Individual Attributes should be used in operations which currently support use of a **Name** within a **Template-Attribute** to reference a **Template**. For more information, see p.30 of the KMIP Specification version 1.3[5], published by OASIS..

[b]The **PGP Key** Managed Object is removed in KMIP version 2.0.

The following figure shows an example of the KMIP Log.



KMIP Log

Log File: Current

Show Last Number of Lines: 10

Wrap Lines: □

Figure 218 : KMIP Log

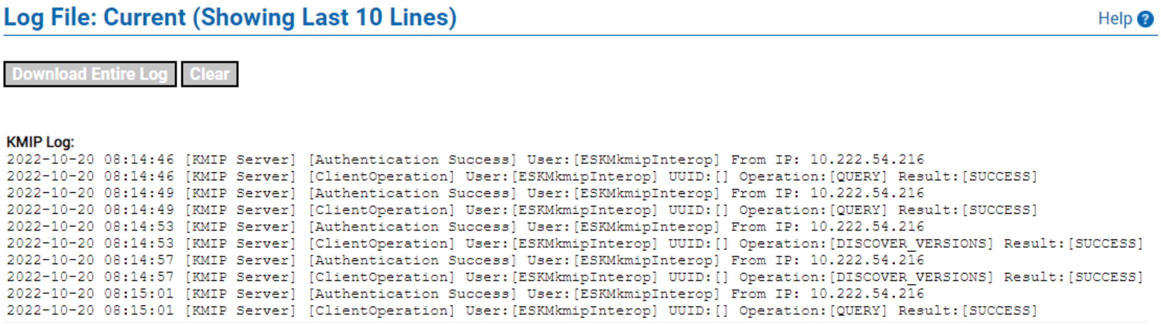
The following table describes the components of the **KMIP Log**.

Table 167: KMIP Log components

Component	***Description***
Log File	Select older logs to display.
Show Last Number of Lines	Select the number of log entries to view.
Wrap Lines	Select to wrap text in the display area.
Display Log	Click to display the specified number of lines of the log.
Rotate Logs	Click to close current log and start a new log.

[5] http://docs.oasis-open.org/kmip/spec/v1.4/kmip-spec-v1.4.pdf

Current KMIP Log



KMIP Log:

```
2022-10-20 08:14:46 [KMIP Server] [Authentication Success] User:[ESKMkmipInterop] From IP: 10.222.54.216
2022-10-20 08:14:46 [KMIP Server] [ClientOperation] User:[ESKMkmipInterop] UUID:[] Operation:[QUERY] Result:[SUCCESS]
2022-10-20 08:14:49 [KMIP Server] [Authentication Success] User:[ESKMkmipInterop] From IP: 10.222.54.216
2022-10-20 08:14:49 [KMIP Server] [ClientOperation] User:[ESKMkmipInterop] UUID:[] Operation:[QUERY] Result:[SUCCESS]
2022-10-20 08:14:53 [KMIP Server] [Authentication Success] User:[ESKMkmipInterop] From IP: 10.222.54.216
2022-10-20 08:14:53 [KMIP Server] [ClientOperation] User:[ESKMkmipInterop] UUID:[] Operation:[DISCOVER_VERSIONS] Result:[SUCCESS]
2022-10-20 08:14:57 [KMIP Server] [Authentication Success] User:[ESKMkmipInterop] From IP: 10.222.54.216
2022-10-20 08:14:57 [KMIP Server] [ClientOperation] User:[ESKMkmipInterop] UUID:[] Operation:[DISCOVER_VERSIONS] Result:[SUCCESS]
2022-10-20 08:15:01 [KMIP Server] [Authentication Success] User:[ESKMkmipInterop] From IP: 10.222.54.216
2022-10-20 08:15:01 [KMIP Server] [ClientOperation] User:[ESKMkmipInterop] UUID:[] Operation:[QUERY] Result:[SUCCESS]
```

Figure 219 : Current KMIP Log

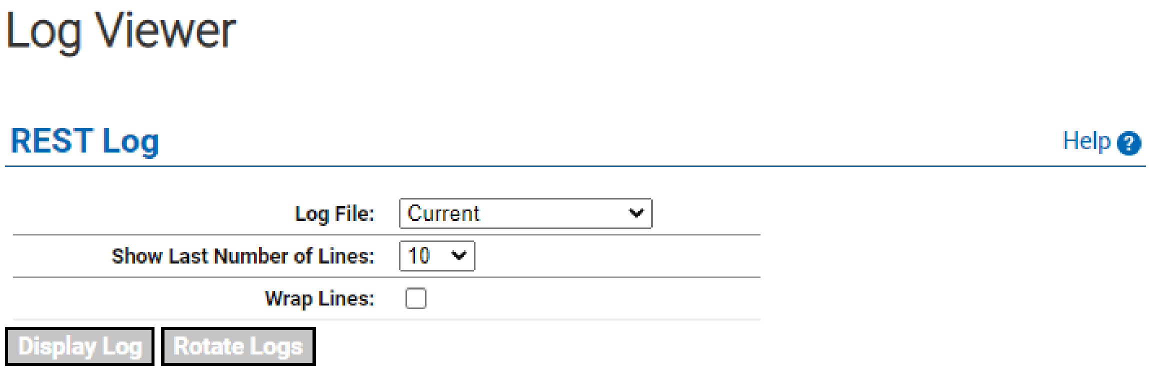
Table 168: Current KMIP Log components

Component	***Description***
Download Entire Log	Click to download the log to your browser.
Clear	Click to delete the select log.

6.23.6.6 REST Log

The REST Log contains a record of all REST server-related activities. Each line of the REST log represents a single activity. The following information is contained in each line of the REST log, in the order shown:

- Date and Time
- Priority: ERROR, WARNING or INFO, depending on the result of the activity.
- Section:The category of service the activity is related to.
- Event:a text description of the activity.



Log Viewer

REST Log

Log File: Current

Show Last Number of Lines: 10

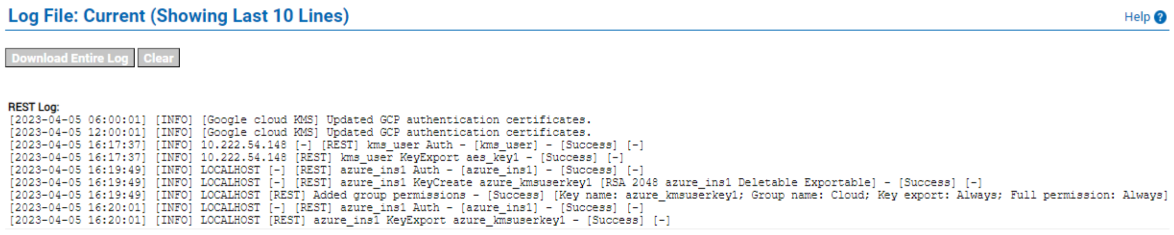
Wrap Lines: □

Figure 220 : Rest Log

The following table describes the components of the REST Log section.

Component	***Description***
Log File	Select older logs to display.
Show Last Number of Lines	Select the number of log entries to view.
Wrap Lines	Select to wrap text in the display area.
Display Log	Click **Display Log** to display the last few lines of the log.

Current Rest Log



Log File: Current (Showing Last 10 Lines)

REST Log:

```
[2023-04-05 06:00:01] [INFO] [Google cloud KMS] Updated GCP authentication certificates.
[2023-04-05 12:00:01] [INFO] [Google cloud KMS] Updated GCP authentication certificates.
[2023-04-05 16:17:37] [INFO] 10.222.54.148 [-] [REST] kms_user Auth - [kms_user] - [Success] [-]
[2023-04-05 16:17:37] [INFO] 10.222.54.148 [REST] kms_user KeyExport aes_key1 - [Success] [-]
[2023-04-05 16:19:49] [INFO] LOCALHOST [-] [REST] azure_ins1 Auth - [azure_ins1] - [Success] [-]
[2023-04-05 16:19:49] [INFO] LOCALHOST [-] [REST] azure_ins1 KeyCreate azure_kmsuserkey1 [RSA 2048 azure_ins1 Deletable Exportable] - [Success] [-]
[2023-04-05 16:19:49] [INFO] LOCALHOST [REST] Added group permissions - [Success] [Key name: azure_kmsuserkey1; Group name: Cloud; Key export: Always; Full permission: Always]
[2023-04-05 16:20:01] [INFO] LOCALHOST [-] [REST] azure_ins1 Auth - [azure_ins1] - [Success] [-]
[2023-04-05 16:20:01] [INFO] LOCALHOST [REST] azure_ins1 KeyExport azure_kmsuserkey1 - [Success] [-]
```

Figure 221 : Current REST Log

The following table describes the components of the Current REST Log section.

Component	***Description***
Download Entire Log	Click **Download Enter Log** to download the log to your browser.

6.23.7 Viewing Statistics

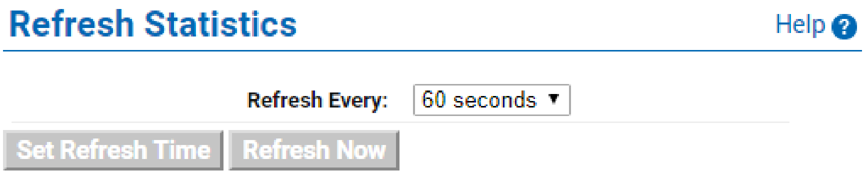
The **Statistics** page allows you to view real-time system statistics about client connections, network throughput, and cache, CPU, and memory utilization. It also displays information about requests made to the KMS and KMIP servers; such requests might include key generation, key deletion, key rotation, and more.

This section contains the following headings:

- Refresh statistics (p. 556)
- System statistics (p. 557)
- Connection statistics (p. 558)
- Throughput (p. 560)
- License usage (p. 562)
- KMS statistics (p. 563)
- KMIP statistics (p. 566)

6.23.7.1 Refresh statistics

Refresh Statistics controls how frequently the **System Statistics** page is refreshed. When the page is refreshed, the values displayed on the page are updated. The refresh interval you specify here does not affect the refresh interval on the CLI. To specify the refresh interval on the CLI see show statistics (p. 738).



Refresh Every: 60 seconds

Figure 222 : Refresh Statistics

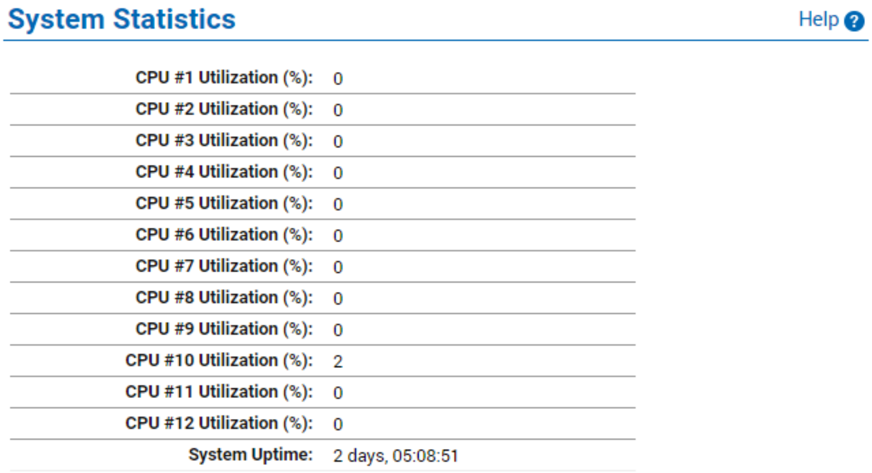
The following table describes the components of Refresh Statistics.

Table 169: Refresh Statistics components

Component	***Description***
Refresh Every	Specify the refresh rate of the System Statistics page. Available refresh intervals are: ▪ Never (default value) ▪ 5 seconds ▪ 15 seconds ▪ 30 seconds ▪ 60 seconds ▪ 2 minutes ▪ 5 minutes This value is only valid while you are viewing the System Statistics page. If you access another page on the Management Console and return to the System Statistics page, the value returns to Never.
Set Refresh Time	Click to apply the new value.
Refresh Now	Click to refresh the System Statistics page on demand.

6.23.7.2 System statistics

System Statistics provides general system statistics, such as how much tis the CPU utilization and how long since the system was restarted.



CPU #1 Utilization (%):	0
CPU #2 Utilization (%):	0
CPU #3 Utilization (%):	0
CPU #4 Utilization (%):	0
CPU #5 Utilization (%):	0
CPU #6 Utilization (%):	0
CPU #7 Utilization (%):	0
CPU #8 Utilization (%):	0
CPU #9 Utilization (%):	0
CPU #10 Utilization (%):	2
CPU #11 Utilization (%):	0
CPU #12 Utilization (%):	0
System Uptime:	2 days, 05:08:51

Figure 223 : System Statistics

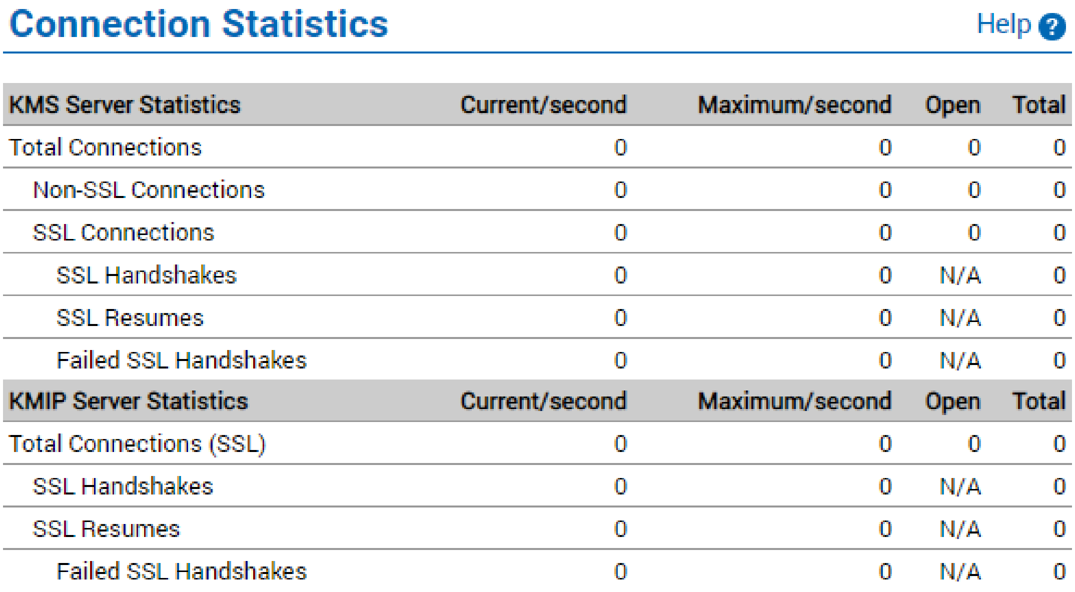
The following table describes the components of **System Statistics**.

Table 170: System Statistics components

Component	***Description***
CPU Utilization (%)	This number represents the percentage of CPU time that was in use for each CPU at the moment the System Statistics page was updated.
System Uptime	This field represents the duration of time that has elapsed since the ESKM appliance was last rebooted.

6.23.7.3 Connection statistics

Connection Statistics provide information on the total number of connections since the ESKM appliance was rebooted.



Connection Statistics

Help ?

KMS Server Statistics	Current/second	Maximum/second	Open	Total
Total Connections	0	0	0	0
Non-SSL Connections	0	0	0	0
SSL Connections	0	0	0	0
SSL Handshakes	0	0	N/A	0
SSL Resumes	0	0	N/A	0
Failed SSL Handshakes	0	0	N/A	0
KMIP Server Statistics	**Current/second**	**Maximum/second**	**Open**	**Total**
Total Connections (SSL)	0	0	0	0
SSL Handshakes	0	0	N/A	0
SSL Resumes	0	0	N/A	0
Failed SSL Handshakes	0	0	N/A	0

Figure 224 : Connection Statistics

The following table describes the components of **Connection Statistics**.

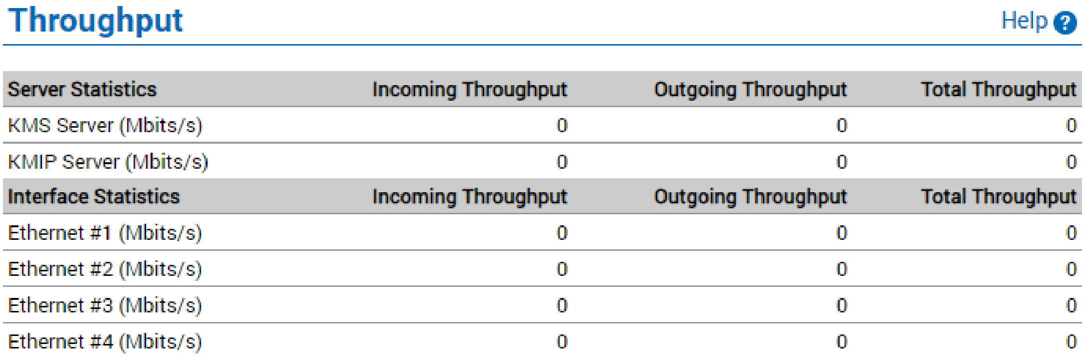
Table 171: Connection Statistics components

Component	***Description***
KMS Server Statistics	Total Connections ▪ Non-SSL Connections ▪ SSL Connections ▪ SSL Handshakes ▪ SSL Resumes ▪ Failed SSL Handshakes

Component	***Description***
KMIP Server Statistics	Total Connections (SSL) ▪ SSL Handshakes ▪ SSL Resumes ▪ Failed SSL Handshakes
Current/second	The Current per second column shows how many of a given statistic were counted on the ESKM appliance in the second the System Statistics were refreshed.
Maximum/second	The Maximum per second column shows the maximum number of a given statistic that were counted by the ESKM appliance during any one second.
Open	The Open column shows the current number of open connections on the ESKM appliance. Note that this column never reflects the number of “open” SSL Handshakes, SSL Resumes, or Failed SSL Handshakes. These are events that happen and therefore cannot be counted as “open.”
Total	The Total column shows the cumulative number of a given statistic on the ESKM appliance since it was rebooted.

6.23.7.4 Throughput

Throughput shows statistics for data traffic on the KMS and KMIP servers and data traffic on each physical interface on the ESKM appliance.



Throughput

Help

Server Statistics	Incoming Throughput	Outgoing Throughput	Total Throughput
KMS Server (Mbits/s)	0	0	0
KMIP Server (Mbits/s)	0	0	0
Interface Statistics	**Incoming Throughput**	**Outgoing Throughput**	**Total Throughput**
Ethernet #1 (Mbits/s)	0	0	0
Ethernet #2 (Mbits/s)	0	0	0
Ethernet #3 (Mbits/s)	0	0	0
Ethernet #4 (Mbits/s)	0	0	0

Figure 225 : Throughput

The following table describes the components of **Throughput**.

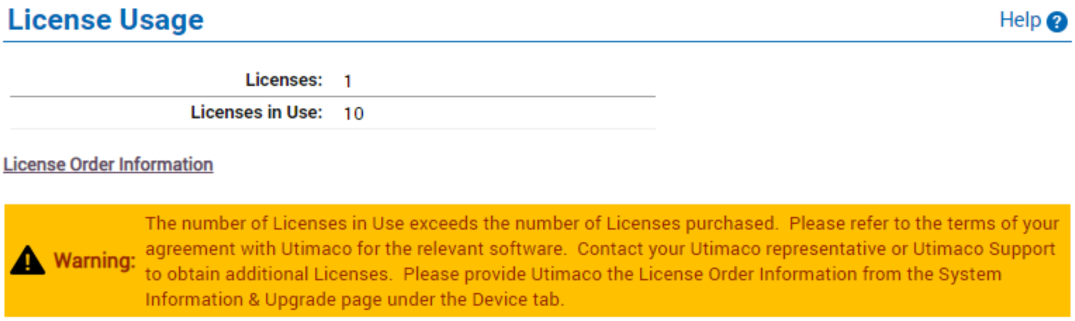
Table 172: Throughput components

Component	***Description***
KMS Server Statistics	This field expresses in megabits per second the amount of data passing through the KMS server. This traffic is generated when the ESKM appliance processes client requests. This does exclude any overhead from the SSL/TLS, TCP, or IP protocols. Furthermore, this does exclude traffic to the Management Console or the SSH administration tool. ▪ **Incoming Throughput** — bytes flowing into the KMS server as a result of client requests. ▪ **Outgoing Throughput** — bytes flowing out of the KMS server as a result of responses to client requests. ▪ **Total Throughput** — the rate at which bytes are flowing into and out of the ESKM appliance for client traffic.

Component	***Description***
KMIP Server Statistics	This field expresses in megabits per second the amount of data passing through the KMIP server. This traffic is generated when the ESKM appliance processes client requests. This does exclude any overhead from the SSL/TLS, TCP, or IP protocols. Furthermore, this does exclude traffic to the Management Console or the SSH administration tool. ▪ **Incoming Throughput** — bytes flowing into the KMIP server as a result of client requests. ▪ **Outgoing Throughput** — bytes flowing out of the KMIP server as a result of responses to client requests. ▪ **Total Throughput** — the rate at which bytes are flowing into and out of the ESKM server for client traffic.
Interface Statistics	This field expresses in megabits per second the amount of data passing through each interface on the ESKM appliance. The Interface Statistics measure all traffic flowing through the box, including data generated from client requests, SSH connections, SNMP traps, log rotation, and so on. ▪ **Incoming Throughput** — bytes flowing into the ESKM appliance. ▪ **Outgoing Throughput** — bytes flowing out of the ESKM appliance. ▪ **Total Throughput** — sum of bytes flowing into and out of the ESKM appliance.

6.23.7.5 License usage

License Usage details the number of users allowed to access the ESKM appliance and the number of users currently enrolled. If the number of clients to be enrolled exceeds the number of ESKM appliances you have purchased, a warning message and a link to the License Order Information section is displayed. To order additional licenses, see License notice.



License Usage

Help

Licenses: 1

Licenses in Use: 10

License Order Information

Warning: The number of Licenses in Use exceeds the number of Licenses purchased. Please refer to the terms of your agreement with Utimaco for the relevant software. Contact your Utimaco representative or Utimaco Support to obtain additional Licenses. Please provide Utimaco the License Order Information from the System Information & Upgrade page under the Device tab.

Figure 226 : License Usage

The following table describes the components of **License Usage**.

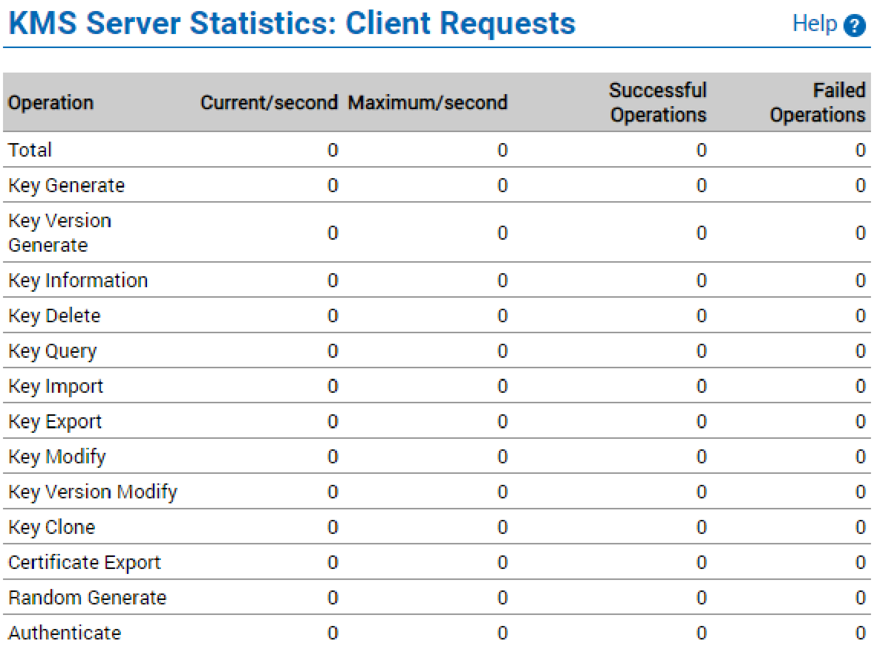
Table 173: License Usage components

Component	***Description***
Licenses	Displays the number of users who are authorized to access the ESKM appliance.
Licenses in Use	Displays the number of users who have been added to the ESKM appliance.
License Order Information	Click on the link to enter and obtain the information required to order additional licenses.

6.23.7.6 KMS statistics

KMS Statistics shows statistics for client usage of the KMS server. Statistics are provided by operation.

This page tracks client requests to the KMS server only. It does not include operations initiated directly by this ESKM appliance, such as operations performed through the Management Console.



KMS Server Statistics: Client Requests

Operation	Current/second	Maximum/second	Successful Operations	Failed Operations
Total	0	0	0	0
Key Generate	0	0	0	0
Key Version Generate	0	0	0	0
Key Information	0	0	0	0
Key Delete	0	0	0	0
Key Query	0	0	0	0
Key Import	0	0	0	0
Key Export	0	0	0	0
Key Modify	0	0	0	0
Key Version Modify	0	0	0	0
Key Clone	0	0	0	0
Certificate Export	0	0	0	0
Random Generate	0	0	0	0
Authenticate	0	0	0	0

Figure 227 : KMS Statistics

The following table describes the components of **KMS Statistics.**

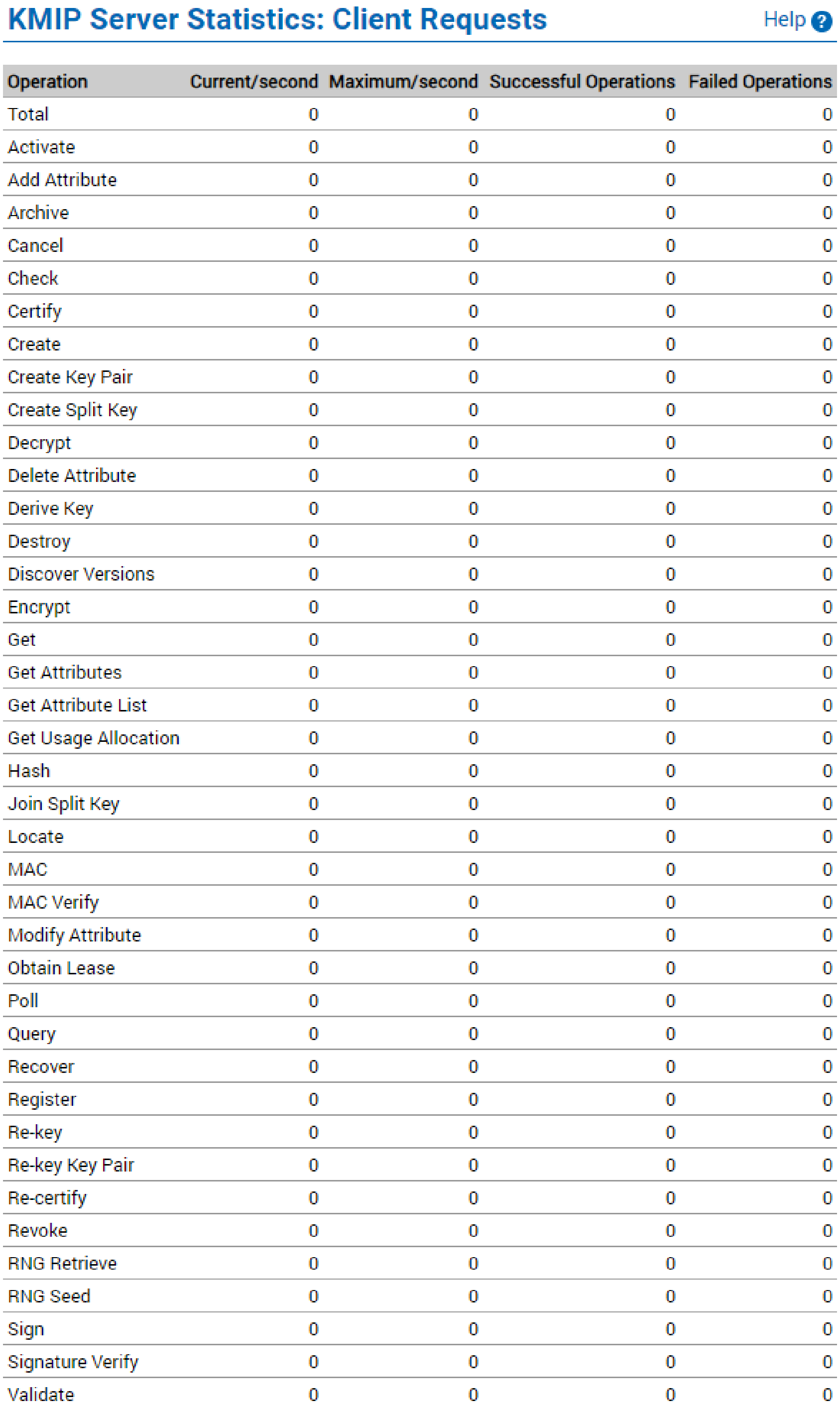
Table 174: KMS Statistics components

Component	***Description***
KMS Operations	▪ **Total** - total number of client requests since the ESKM appliance was last rebooted. ▪ **Key Generate** - request to generate a cryptographic key. ▪ **Key Information** - requests for information about a particular key. ▪ **Key Delete** - request to delete a key. ▪ **Key Query** - request to view all keys available to a client. ▪ **Key Import** - request to import a key. ▪ **Key Export** - request to export a key. ▪ **Key Modify** - request to modify a key. ▪ **Key Clone** - request to clone a key. ▪ **Certificate Export** - request to export a certificate. ▪ **Random Generate** - request to generate a random byte sequence. ▪ **Authenticate** - request to authenticate.
Current/second	The Current per second column shows how many of a given statistic were counted on the ESKM appliance in the second the KMS Statistics were refreshed.
Maximum/second	The Maximum per second column shows the maximum number of a given statistic that were counted by the ESKM appliance during any one second.
Successful Operations	Displays the number of successful operations.
Failed Operations	Displays the number of failed operations.

6.23.7.7 KMIP statistics

KMIP Statistics shows statistics for client usage of the KMIP server. Statistics are provided by operation.

> This page tracks client requests to the KMIP server only. It does not include operations initiated directly by this ESKM appliance, such as operations performed through the Management Console.



KMIP Server Statistics: Client Requests

Operation	Current/second	Maximum/second	Successful Operations	Failed Operations
Total	0	0	0	0
Activate	0	0	0	0
Add Attribute	0	0	0	0
Archive	0	0	0	0
Cancel	0	0	0	0
Check	0	0	0	0
Certify	0	0	0	0
Create	0	0	0	0
Create Key Pair	0	0	0	0
Create Split Key	0	0	0	0
Decrypt	0	0	0	0
Delete Attribute	0	0	0	0
Derive Key	0	0	0	0
Destroy	0	0	0	0
Discover Versions	0	0	0	0
Encrypt	0	0	0	0
Get	0	0	0	0
Get Attributes	0	0	0	0
Get Attribute List	0	0	0	0
Get Usage Allocation	0	0	0	0
Hash	0	0	0	0
Join Split Key	0	0	0	0
Locate	0	0	0	0
MAC	0	0	0	0
MAC Verify	0	0	0	0
Modify Attribute	0	0	0	0
Obtain Lease	0	0	0	0
Poll	0	0	0	0
Query	0	0	0	0
Recover	0	0	0	0
Register	0	0	0	0
Re-key	0	0	0	0
Re-key Key Pair	0	0	0	0
Re-certify	0	0	0	0
Revoke	0	0	0	0
RNG Retrieve	0	0	0	0
RNG Seed	0	0	0	0
Sign	0	0	0	0
Signature Verify	0	0	0	0
Validate	0	0	0	0

Figure 228 : KMIP Statistics

The following table describes the components of **KMIP Statistics**.

Table 175: KMIP Statistics components

Component	***Description***
KMIP Operations	Total - total number of client requests since the ESKM appliance was last rebooted. See KMIP Operations (p. 546) for a list of all KMIP operations.
Current/second	The Current per second column shows how many of a given statistic were counted on the ESKM appliance in the second the KMIP Statistics were refreshed.
Maximum/ second	The Maximum per second column shows the maximum number of a given statistic that were counted by the ESKM appliance during any one second.
Successful Operations	Displays the number of successful operations.
Failed Operations	Displays the number of failed operations.

7 Using the command line interface

This section contains the description and reference of the ESKM Command Line Interface (CLI).

The following sub-sections are covered:

7.1 Shell commands

The CLI supports a few shell commands that allow you to perform various search, cut, and paste operations. The following shell commands are valid:

- Ctrl + c — Clears the prompt
- Ctrl + r — Allows you to search backward through the command history
- Ctrl + k — Deletes the text from the cursor to the end of the line
- Ctrl + u — Erases the entire line
- Ctrl + y — Pastes text erased by Ctrl + k or Ctrl + u
- Ctrl + p — Moves backwards through the history

7.2 Command line interface syntax

In general, the Command Line Interface (CLI) separates input into separate arguments by using spaces as delimiters.

For example, the command `cert request newcertrequest` is treated as three separate arguments:

- `cert`

- `request`
- `newcertrequest`

7.2.1 Quoting arguments

You can include spaces in an argument by quoting the argument. Placing quotes around a string causes it to be treated as one argument.

For example, the command `cert request "new cert request"` is treated as three separate arguments:

- `cert`
- `request`
- `new cert request`

Single quotes (') and double quotes (") are treated identically and can be used interchangeably.

As such, the command `cert request 'new cert request"` is treated as three separate arguments:

- `cert`
- `request`
- `new cert request`

If there are no spaces between segments of quoted and non-quoted text, the two segments are treated as one argument.

For example, the command `new cert "new cert request"` is treated as three separate arguments:

- `new`
- `cert`
- `new cert request`

7.2.1.1 Escaping characters using backslash

You can include a quote character (" or ') within an argument by putting a backslash (\) in front of it.

For example, the command `new cert 'new cert \'request' ` is treated as three separate arguments:

- `new`
- `cert`
- `new cert 'request`

Similarly, the command `new cert newcert\"request` is treated as three separate arguments:

- `new`
- `cert`
- `newcert"request`

The backslash character can also be used to escape itself. Thus, the string “\\” is treated as just a single backslash character. Except for the cases when it appears before a single quote ('), double quote ("), or a backslash (\), the backslash character behaves normally.

For example, the command `new cert "new \\reques\t"` is treated as three separate arguments:

- `new`
- `cert`
- `new \reques\t`

7.2.1.2 Tab completion

The tab completion feature allows you to type part of a command and use the tab key to fill in the remainder. If the command is unambiguous, the CLI will fill in the rest of the command up until the next point of ambiguity. For example, if you type `sh`, the CLI will complete the word `show`, as this is the only possible ending to that word.

Because the majority of commands include multiple words, you will most likely type the beginning of one word, press tab to complete the word, start another word, and press tab again. Tab completion is available as long as the CLI knows you can only be referring to one word or command.

If the text you have entered can refer to multiple commands, tab completion will not work, but you can press the return key to view the possible commands. For example, if you type `show sys` and press the return key, the CLI displays the commands that begin with `show sys`.

7.2.1.3 Command shortcuts

Similar to tab completion, the CLI enables you to execute commands without typing the complete command name. When you do not type the complete command name, the ESKM appliance attempts to match the pattern you typed against all the commands available in the current mode (view, config, or script). If there is only one command that matches, that command is executed.

If multiple commands match the pattern, those commands are displayed on the screen. For example, if you type `sh au lo` on the command line, the ESKM appliance executes the `show audit log` command. However, if you type `sh au l` on the command line, the ESKM appliance displays the commands that match that pattern.

7.2.1.4 Command search

To search for a command without executing it, type the command, or part of the command, and include a question mark (?). The CLI displays the commands that match the pattern you typed.

For example, if you type `sh au l ?` on the command line, the CLI displays the commands that match that pattern. If you type `show audit log ?`, the CLI will indicate that `show audit log` is a unique command.

> Include a space before the question mark. Otherwise, the CLI interprets the punctuation as part of the command, and returns an error.

7.3 Command modes

There are three modes of use:

- “View mode (p. 573)”
- “Configure mode (p. 573)”
- “Script mode (p. 573)”

These modes requires secure shell (SSH) administration privilege.

7.3.1 View mode

This is the default mode. It allows viewing of current configuration and system status; you cannot change any values or settings.

The view mode prompt is the hostname of the ESKM appliance followed by the number sign (#), as follows:

```
hostname#
```

7.3.2 Configure mode

Configure mode allows both viewing and configuration.

The ESKM appliance is in configure mode when the following prompt is available on the screen: `hostname (config)#`

To enter configure mode, type `configure terminal` at the prompt:

```
hostname# configure terminal
```

```
hostname (config)#
```

To exit configure mode and go to view mode, type `exit` at the prompt:

```
hostname (config)# exit
hostname#
```

7.3.3 Script mode

Script mode allows you to create and run scripts containing “ `show` " and/or " `configure` " mode CLI commands.

7.3.3.1 (2021-0046 Entering script mode

To enter script mode, you must first enter configure mode, then type `script` at the command prompt.

The ESKM appliance is in script mode when the following prompt is displayed:

```
hostname (script)#
```

To enter script mode, type `script` at the prompt:

```
hostname (config)# script
```

To exit script mode and go to configure mode, type `exit` at the prompt:

```
hostname (script)# exit
hostname (config)#
```

This section describes how to perform the following actions in scripting mode:

- "Creating scripts (p. 574)"
- "Executing scripts (p. 575)"
- "Displaying and deleting scripts (p. 576)"
- "IInstalling certificates (p. 576)"
- "Entering passwords (p. 576)"

7.3.3.2 Creating scripts

There are essentially two different ways to create CLI scripts: manually or via the Script Recorder.

7.3.3.2.1 Manual creation

This is done using the command `create script <script name>`, as shown here:

```
hostname(script)# create script testscript
```

Perform the following actions to create the script:

- Type or paste the script immediately after the question mark.
- Press **Return** twice when you have finished.

After you type the command, you are presented with the above directions. You can then either enter your script line by line or create it using another editor and just paste it in after the question mark.

When you are manually creating scripts, you must take care to format the script file correctly. For example, when scripting an interactive command (i.e. one that asks for input), the command often prompts the user multiple times to enter input. You must ensure that each response to a prompt for input is entered on a separate line in the script file.

> ⚠ The Script Recorder takes care of all such formatting issues and hence is probably the best way to create scripts initially.

7.3.3.2.2 Script Recorder

The Script Recorder is started by typing in the command `record <script name>`:

```
hostname(script)# record testscript
Recording to script testscript.
```

You can then type in any “show” or “configure” mode CLI commands and they will automatically be written to the script specified in the correct format.

To stop the Script Recorder, type `no record`, as shown here:

```
hostname(script)# no record
Recording successfully stopped.
```

7.3.3.3 Executing scripts

To execute a script, you must first load it using the command `load <script name>` as shown here:

```
hostname(script)# load testscript
Script testscript successfully loaded.
```

Once loaded, a script can either be stepped through (executed one line at a time), or the entire script can be run.

To step through a script, use the command `“step”`, as shown here:

```
hostname(script)# step
```

To run the entire script, use the command `“go”`, as shown here:

```
hostname(script)# go
```

7.3.3.4 Displaying and deleting scripts

To display the current scripts that have been created on the ESKM appliance, use the command `show script`.

To display the contents of a specified script, use the command `show script <script name>`, as shown here:

```
hostname(script)# show script testscript
```

If you want to delete an existing script, use the command `no script <script name>`, as shown here:

```
hostname(script)# no script testscript
```

7.3.3.5 Installing certificates

When you attempt to enter a command in a script that requires a certificate to be pasted in, the actual certificate will not be stored in the script. Instead the script will prompt you when it is run, to paste in the certificate.

7.3.3.6 Entering passwords

Whenever a command that requires a password is executed in a script, the actual password will not be stored in the script. Instead, when the script is run, it will prompt you to enter the password. User passwords must be at least 8 characters long.

7.4 CLI commands

The following table is an alphabetical listing all of the CLI commands by functional groups.

Table 176: List of CLI commands

“Activity log commands”

activity log rotate (p. 665) activity syslog (p. 675) no activity log (p. 661) no activity syslog (p. 680) show activity log (p. 663) show activity syslog (p. 682) transfer activity log (p. 671)	
“Administrator and LDAP commands”	
administrator (p. 587) administrator-keys (p. 589) credential settings (p. 590) edit administrator (p. 591) grant credential (p. 592) ldap server administrators failover (p. 593) ldap server administrators primary (p. 594) ldap server administrators schema (p. 595) ldap test administrators failover (p. 596) ldap test administrators primary (p. 597) ldap test users failover (p. 598) ldap test users primary (p. 599)	no administrator (p. 599) no administrator-keys (p. 589) no granted credential (p. 600) no ldap server administrators failover (p. 600) no ldap server administrators primary (p. 601) no ldap server administrators schema (p. 602) passwd (p. 602) password settings (p. 603) show administrator (p. 603) show administrator-keys (p. 589) show credential settings (p. 604) show granted credential (p. 604) show ldap server administrators (p. 605) show password settings (p. 606)
“Audit log commands”	
audit syslog (p. 676) no audit syslog (p. 680) show audit log (p. 663) show audit syslog (p. 682) transfer audit log (p. 671)	
“Autologout commands”	
autologout (p. 607) show autologout (p. 607)	
“Backup and restore commands”	

“CA certificate commands”

“Certificate commands”

“CRL commands”
crl auto-update (p. 634) crl list send (p. 634) crl list update (p. 635) crl settings (p. 636) no crl auto-update (p. 637) no crl list (p. 637) no crl auto-update (p. 637) show crl entry (p. 638) show crl list (p. 631) show crl settings (p. 638) show crl status (p. 639)
“Client event log commands”
clientevent log rotate (p. 666) clientevent syslog (p. 677) no clientevent log (p. 661) no clientevent syslog (p. 681) show clientevent log (p. 664) show clientevent syslog (p. 683) transfer clientevent log (p. 672)
“Appliance reset and restore commands”
reset factory settings (p. 640) restore default configuration (p. 641) zeroize all keys (p. 642) zeroize all kmip-objects (p. 643)
“Diagnostic commands”
host run (p. 644) ping run (p. 644) netstat run (p. 644) traceroute run (p. 645)

“FIPS commands”
fips compliant (p. 646) fips server (p. 647) security settings (p. 648) show security settings (p. 649) show fips server (p. 650) show fips status (p. 650)
“Group commands”
edit group (p. 651) edit group-permissions (p. 652) group (p. 653) kmip group (p. 654) no group (p. 654) show group (p. 655) show group detail (p. 655) show group-permissions (p. 656)
“Health check configuration commands”
health check (p. 657) show health check (p. 658)
“Help commands”
? (p. 659) help (p. 659)
“History command”
history (p. 660)
“KMIP log commands”

kmip log rotate (p. 666)
kmip syslog (p. 678)
no kmip log (p. 662)
no kmip syslog (p. 681)
show kmip log (p. 664)
show kmip syslog (p. 683)
transfer kmip log (p. 673)

“Log commands”

activity log rotate (p. 665)
activity syslog (p. 675)
audit syslog (p. 676)
clientevent log rotate (p. 666)
clientevent syslog (p. 677)
edit log rotation (p. 668)
kmip log rotate (p. 666)
kmip syslog (p. 678)
log signing (p. 669)
no activity log (p. 661)
no activity syslog (p. 680)
no audit syslog (p. 680)
no clientevent log (p. 661)
no clientevent syslog (p. 681)
no kmip log (p. 662)
no kmip syslog (p. 681)
no syslog tls (p. 684)
no system log (p. 662)
no system syslog (p. 682)
recreate logsigning cert (p. 670)
show activity log (p. 663)
show activity syslog (p. 682)
show audit log (p. 663)
show audit syslog (p. 682)
show clientevent log (p. 664)
show clientevent syslog (p. 683)
show log rotation (p. 668)
show logsigning cert (p. 670)
show log signing (p. 669)
show kmip log (p. 664)
show kmip syslog (p. 683)
show syslog tls (p. 685)
show system log (p. 665)
show system syslog (p. 683)
syslog test (p. 685)
syslog tls (p. 684)
system log rotate (p. 667)
system syslog (p. 679)
transfer activity log (p. 671)
transfer audit log (p. 671)
transfer clientevent log (p. 672)
transfer kmip log (p. 673)
transfer system log (p. 674)

“Mode commands”

configure (p. 686)
configure terminal (p. 686)
exit (p. 687)
script (p. 687)

“Network commands”	
edit ip authorization allowed (p. 688) ethernet port (p. 689) gateway (p. 689) gateway6 (p. 690) ip address (p. 691) ipv6 address (p. 692) ipv6 enable (p. 693) ipv6 status (p. 694) ip authorization (p. 695) ip authorization allowed (p. 696) ip name-server (p. 696) no gateway (p. 697) no gateway6 (p. 697) no ip address (p. 698) no ipv6 address (p. 698) no ip authorization allowed (p. 699) no ip name-server (p. 699) no static route (p. 700) outgoing gateway (p. 690) outgoing gateway6 (p. 691)	show ethernet port (p. 700) show gateway (p. 700) show hosts (p. 701) show interface ethernet (p. 701) show interfaces (p. 702) show ip authorization (p. 703) show ip authorization allowed (p. 704) show static route (p. 705) static route (p. 705)
“Services commands”	
halt (p. 706) kmip-server run (p. 706) kmip-server startup (p. 706) kms-server run (p. 706) kms-server startup (p. 707) no kmip-server run (p. 707) no kmip-server startup (p. 707) no kms-server run (p. 707) no kms-server startup (p. 708) no snmp run (p. 708) no snmp startup (p. 708) no sshadmin run (p. 708) no sshadmin startup (p. 709) no webadmin run (p. 709) no webadmin startup (p. 709)	reboot (p. 709) show services (p. 710) snmp run (p. 711) snmp startup (p. 711) sshadmin run (p. 711) sshadmin startup (p. 711) webadmin run (p. 712) webadmin startup (p. 712) service start restserver (p. 712) service stop restserver (p. 713) service restart restserver (p. 713)

“SNMP commands”

“SSH commands”

“SSL/TLS commands”

cipherspec (p. 728) cipherspec priority (p. 729) kmip cipherspec (p. 730) kmip cipherspec priority (p. 731) kmip ssl protocol (p. 732) no cipherspec (p. 732) no kmip cipherspec (p. 733) no kmip ssl protocol (p. 733) no ssl protocol (p. 733) restore cipherspec (p. 734) restore kmip cipherspec (p. 734) show cipherspec (p. 735) show ssl (p. 735) ssl protocol (p. 736) ssl timeout (p. 736)
“Statistics commands”
show license (p. 751) show license usage (p. 737) show statistics (p. 738)
“System commands”
clock set(see table 176) edit ras settings (p. 740) hostname (p. 741) no ntp server (p. 741) ntp (p. 742) ntp synchronize (p. 742) recreate ssh key (p. 743) reissue webadmin certificate (p. 743) software install (p. 744) software rollback (p. 745) timezone set (p. 745)
“System health commands”
show system health (p. 749)

“System information commands”
display fingerprints (p. 749) show clock (p. 750) show copyright (p. 750) show device (p. 750) show hostname (p. 750) show license order information (p. 751) show ntp (p. 751) show software all (p. 752) show ras settings (p. 752)
“System log commands”
no system log (p. 662) no kmip syslog (p. 681) show system log (p. 665) show system syslog (p. 683) system log rotate (p. 667) system syslog (p. 679) transfer system log (p. 674)
“User commands”
edit user (p. 754) no user (p. 755) kmip edit user (p. 755) kmip user (p. 756) show user (p. 758) show user detail (p. 759) show user-memberships (p. 759) show user-permissions (p. 760) user (p. 761)

7.4.1 Activity log commands

The Activity Log contains a record of each request received by the KMS Server and its result. Use these commands to view and manage the Activity Log. For more information on log commands, see “Log commands (p. 660)”.

- “activity log rotate” (p. 665)
- “activity syslog” (p. 675)
- “no activity log (p. 661)”
- “no activity syslog” (p. 680)
- “show activity log” (p. 663)
- “show activity syslog (p. 682)”
- “transfer activity log” (p. 671)

7.4.2 Administrator and LDAP commands

`administrator` — create a new local administrator on the ESKM appliance.

Syntax

```
hostname (config)# administrator <administrator name>
Administrator Type:

1. Local

2. LDAP
Enter a number (1 - 2) [1]:
Full Name:
Description:
Password:
Confirm Password:
High Access Administrator (y/n) [n]:


Access Control - Security Configuration
    Keys and Authorization Policies (y/n) [n]:
    Users and Groups (y/n) [n]:
    Certificates (y/n) [n]:
    Certificate Authorities (y/n) [n]:
    Advanced Security (y/n) [n]:
    SSL (y/n) [n]:


Access Control - Device Configuration
    KMS/KMIP/REST Server (y/n) [n]:
    Cluster (y/n) [n]:
    Network and Date/Time (y/n) [n]:
    SNMP (y/n) [n]:
    Logging (y/n) [n]:
```

```
Access Control - Backup & Restore
    Backup Configuration and Kerberos (y/n) [n]:
    Backup Keys & Certificates (y/n) [n]:
    Backup Local CAs (y/n) [n]:
    Restore Configuration (y/n) [n]:
    Restore Keys & Certificates (y/n) [n]:
    Restore Local CAs (y/n) [n]:

Access Control - Maintenance
    Services (y/n) [n]:
Software Upgrade and System Health (y/n) [n]:

Access Control - Administrative Access
Admin Access via Web (y/n) [n]:
Admin Access via SSH (y/n) [n]:

Warning: High access administrators may grant themselves other access
rights
Administrator successfully added.
```

Related command(s)

- “edit administrator (p. 591)”
- “show administrator (p. 603)”
- “no administrator (p. 599)”

`administrator-keys` — associate a public key with an administrator. This 2048-bit RSA public key will be used to authenticate the administrator using the SSH protocol version 2.

Syntax

```
hostname (config)# administrator-keys <administrator name>
<"public key">
```

Related command(s)

- "no administrator-keys (p. 589)"
- "show administrator-keys (p. 589)"

`no administrator-keys` — delete a public key that was associated with an administrator.

Syntax

```
hostname (config)# no administrator-keys <administrator name>
<"public key">
```

Related command(s)

- "administrator-keys (p. 589)"
- "show administrator-keys (p. 589)"

`show administrator-keys` — view the list of public keys associated with the administrator.

Syntax

```
hostname# show administrator-keys [administrator username]
```

Related command(s)

- "administrator-keys (p. 589)"
- "no administrator-keys (p. 589)"

`credential settings` — establish the multiple credential settings.

Syntax

```
hostname# credential settings
Require Multiple Credentials [n]:
Num of Admins Required for Operations:
1: 2
2: 3
3: 4
Enter a number (1 - 3) [1]:
Allow Time-Limited Credentials [n]:
Maximum Duration for Credentials (minutes) [0]:
Changed Multiple Credentials settings
```

Related command(s)

- "grant credential (p. 592)"
- "show granted credential (p. 604)"
- "no granted credential (p. 600)"
- "show credential settings (p. 604)"

`edit administrator` - modify settings for a specified administrator.

Syntax

```
hostname (config)# edit administrator <administrator name>
Username [admin]:
Full Name [Administrator One]:
Description [Administrator]:
Password [********]:
High Access Administrator (y/n) [y]:
```

The ESKM appliance prompts for access control configuration information as shown in administrator (p. 587).

Related command(s)

- "administrator (p. 587)"
- "no administrator (p. 599)"
- "show administrator (p. 603)"

`grant credential` — grant credentials to another administrator.

The Require Multiple Credentials features must be enabled before you can grant credentials to another administrator.

Syntax

```
hostname (config)# grant credential

Grant to:

1: [Select Administrator]

Enter a number (1 - 3) [1]:

Duration (minutes):

Allowed Operations:

Add/Modify Keys [n]:

Delete Keys [n]:

Add/Modify Users & Groups [n]:

Delete Users & Groups [n]:

Modify Auth Policies [n]:

Modify LDAP Server [n]:
```

Related command(s)

- "show granted credential (p. 604)"
- "no granted credential (p. 600)"
- "credential settings (p. 590)"
- "show credential settings (p. 604)"

`ldap server administrators failover` — define the hostname or IP address and port number of the LDAP failover server.

Syntax

```
hostname (config)# ldap server administrators failover
```

```
Failover Hostname or IP Address: [None]
```

```
Failover Port: [None]
```

Related command(s)

- "ldap server administrators primary (p. 594)"
- "ldap server administrators schema (p. 595)"
- "ldap test administrators primary (p. 597)"
- "no ldap server administrators failover (p. 600)"
- "no ldap server administrators primary (p. 601)"
- "no ldap server administrators schema (p. 602)"
- "show ldap server administrators (p. 605)"
- "ldap test users failover (p. 598)"
- "ldap test users primary (p. 598)"

`ldap server administrators primary` — define the configuration of the primary LDAP server.

Syntax

```
hostname (config)# ldap server administrators primary

Hostname or IP Address: [None]

Port: [None]

Use SSL: no
Minimum TLS Version:

        1: None

        2: TLS 1.0

        3: TLS 1.1

        4: TLS 1.2

Trusted Certificate Authority: [None]

Timeout (sec): 3

Bind DN: [None]

Bind Password: [None]
```

Related command(s)

- "ldap server administrators schema (p. 595)"
- "ldap server administrators failover" (p. 593)
- "ldap test administrators primary (p. 597)"
- "no ldap server administrators failover (p. 600)"
- "no ldap server administrators primary (p. 601)"
- "no ldap server administrators schema (p. 602)"

- “show ldap server administrators (p. 605)”
- “ldap test users failover (p. 598)”
- “ldap test users primary (p. 598)”

`ldap server administrators schema` — define the schema for the LDAP server administrators.

Syntax

```
hostname (config)# ldap server administrators schema
User Base DN: [None]
User ID Attribute: [None]
User Object Class: [None]
User List Filter: [None]
Search Scope:
Please select from the following options:
1) One Level    2) Subtree
Search Scope [1]:
```

Related command(s)

- “ldap server administrators primary (p. 594)”
- “ldap server administrators failover” (p. 593)
- “ldap test administrators primary (p. 597)”
- “no ldap server administrators failover (p. 600)”
- “no ldap server administrators primary (p. 601)”
- “no ldap server administrators schema (p. 602)”
- “show ldap server administrators (p. 605)”
- “ldap test users failover (p. 598)”
- “ldap test users primary (p. 598)”

`ldap test administrators failover` — connect to the failover LDAP server (if defined) and print connection status.

Syntax

```
hostname (config)# ldap test administrators failover
```

Related command(s)

- “ldap server administrators primary (p. 594)”
- “ldap server administrators failover” (p. 593)
- “ldap test administrators primary (p. 597)”
- “no ldap server administrators failover (p. 600)”
- “no ldap server administrators primary (p. 601)”
- “no ldap server administrators schema (p. 602)”
- “show ldap server administrators (p. 605)”
- “ldap test users failover (p. 598)”
- “ldap test users primary (p. 598)”

`ldap test administrators primary` — connect to the primary LDAP server and print connection status.

Syntax

```
hostname (config)# ldap test administrators primary
```

Related command(s)

- “ldap server administrators primary (p. 594)”
- “ldap server administrators failover” (p. 593)
- “ldap test administrators failover (p. 596)”
- “no ldap server administrators failover (p. 600)”
- “no ldap server administrators primary (p. 601)”
- “no ldap server administrators schema (p. 602)”
- “show ldap server administrators (p. 605)”
- “ldap test users failover (p. 598)”
- “ldap test users primary (p. 598)”

`ldap test users failover` — connect to the failover LDAP server (if defined) and print connection status.

Syntax

```
hostname# ldap test users failover
```

Related command(s)

- “ldap server administrators primary (p. 594)”
- “ldap server administrators failover” (p. 593)
- “ldap test administrators primary (p. 597)”
- “ldap test administrators failover (p. 596)”
- “no ldap server administrators failover (p. 600)”
- “no ldap server administrators primary (p. 601)”
- “no ldap server administrators schema (p. 602)”
- “show ldap server administrators (p. 605)”
- “ldap test users primary (p. 598)”

`ldap test users primary` — connect to the primary LDAP server and print connection status.

Syntax

```
hostname# ldap test users primary
```

Related command(s)

- “ldap server administrators primary (p. 594)”
- “ldap server administrators failover” (p. 593)
- “ldap test administrators primary (p. 597)”
- “ldap test administrators failover (p. 596)”
- “no ldap server administrators failover (p. 600)”
- “no ldap server administrators primary (p. 601)”
- “no ldap server administrators schema (p. 602)”
- “show ldap server administrators (p. 605)”
- “ldap test users failover (p. 598)”

`no administrator` — delete an administrator from the Administrator List.

Syntax

```
hostname (config)# no administrator <administrator name>
```

Related command(s)

- “administrator (p. 587)”
- “edit administrator (p. 591)”
- “show administrator (p. 603)”

`no granted credential` — cancel an existing credential grant.

Syntax

```
hostname# no granted credential <number>
```

Related command(s)

- "grant credential (p. 592)"
- "show granted credential (p. 604)"
- "credential settings (p. 590)"
- "show credential settings (p. 604)"

`no ldap server administrators failover` — delete the failover LDAP server.

Syntax

```
hostname (config)# no ldap server administrators failover
```

Related command(s)

- "ldap server administrators primary (p. 594)"
- "ldap server administrators failover" (p. 593)
- "ldap test administrators primary (p. 597)"
- "ldap test administrators failover (p. 596)"
- "ldap test users primary (p. 598)"
- "no ldap server administrators primary (p. 601)"
- "no ldap server administrators schema (p. 602)"
- "show ldap server administrators (p. 605)"
- "ldap test users failover (p. 598)"

`no ldap server administrators primary` — delete the primary LDAP server.

Syntax

```
hostname (config)# no ldap server administrators primary
```

Related command(s)

- “ldap server administrators primary (p. 594)”
- “ldap server administrators failover” (p. 593)
- “ldap test administrators primary (p. 597)”
- “ldap test administrators failover (p. 596)”
- “ldap test users primary (p. 598)”
- “no ldap server administrators schema (p. 602)”
- “show ldap server administrators (p. 605)”
- “ldap test users failover (p. 598)”
- “ldap test users primary (p. 598)”
- “no ldap server administrators failover (p. 600)”

`no ldap server administrators schema` — delete the LDAP server schema

Syntax

```
hostname (config)# no ldap server administrators schema
```

Related command(s)

- “ldap server administrators primary (p. 594)”
- “ldap server administrators failover” (p. 593)
- “ldap test administrators primary (p. 597)”
- “ldap test administrators failover (p. 596)”
- “ldap test users primary (p. 598)”
- “show ldap server administrators (p. 605)”
- “ldap test users failover (p. 598)”
- “ldap test users primary (p. 598)”
- “no ldap server administrators primary (p. 601)”
- “no ldap server administrators failover (p. 600)”

`passwd` — change your own password.

Syntax

```
hostname (config)# passwd
```

Related command(s)

- “show password settings (p. 606)”
- “password settings (p. 603)”

`password settings` — edit the password settings for all administrators

Syntax

```
hostname config# password settings
Enable Password Expiration (y/n) [n]:
Enable Password History (y/n) [n]:
Minimum Password Length [8]:
Must Passwords Contain At Least One:
Lower Case Letter (y/n) [n]:
Upper Case Letter (y/n) [n]:
Number (y/n) [n]:
Special Character (y/n) [n]:
Password settings successfully saved.
```

Related command(s)

- "passwd (p. 602)"
- "show password settings (p. 606)"

`show administrator` — view specific, or all, administrators currently configured on the ESKM appliance.

Syntax

```
hostname# show administrator [administrator username]
```

Related command(s)

- "administrator (p. 587)"
- "edit administrator (p. 591)"
- "no administrator (p. 599)"

`show credential settings` -display the multiple credential settings.

Syntax

```
hostname# show credential settings
Require Multiple Credentials: yes
Num of Admins Required for Operations: 2
Allow Time-Limited Credentials: yes
Maximum Duration for Credentials (minutes): 10
```

Related command(s)

- "grant credential (p. 592)"
- "show granted credential (p. 604)"
- "credential settings (p. 590)"
- "show credential settings (p. 604)"

`show granted credential` — display the existing credential grants.

Syntax

```
hostname# show granted credential
```

Related command(s)

- "grant credential (p. 592)"
- "show granted credential (p. 604)"
- "credential settings (p. 590)"
- "show credential settings (p. 604)"

`show ldap server administrators` — displays the LDAP Administrator Server, Failover Server, and Schema properties.

Syntax

```
hostname# show ldap server administrators
```

Related command(s)

- "ldap server administrators primary (p. 594)"
- "ldap server administrators failover" (p. 593)
- "ldap test administrators primary (p. 597)"
- "ldap test administrators failover (p. 596)"
- "ldap test users primary (p. 598)"
- "ldap test users failover (p. 598)"
- "no ldap server administrators schema (p. 602)"
- "no ldap server administrators primary (p. 601)"
- "no ldap server administrators failover (p. 600)"

`show password settings` — view the password settings for all administrators.

In addition to the restrictions below, passwords must contain at least 5 different characters, cannot be based on a dictionary word, and cannot contain too many sequential characters. Password length and character requirements also apply to local user, cluster, and backup passwords.

Syntax

```
hostname# show password settings
Password Expiration: After 180 days
Password History: 4 passwords remembered
Minimum Password Length: 8
Passwords Must Contain At Least One:
Lower Case Letter: yes
Upper Case Letter: yes
Number: yes
Special Character: yes
```

Related command(s)

- “passwd (p. 602)”
- “password settings (p. 603)”

7.4.3 Audit log commands

The Audit Log contains a record of all configuration changes and user input errors made to the ESKM appliance, whether through the Management Console or the CLI. Each line in the audit log corresponds to one configuration change. Use the below commands to view and manage the Audit Log. For more information on log commands, see Log commands (p. 660).

- “audit syslog (p. 676)”
- “no audit syslog (p. 680)”
- “show audit log (p. 663)”
- “show audit syslog (p. 682)”
- “transfer audit log (p. 671)”

7.4.4 Autologout commands

Use these commands to manage and view the autologout timer.

`autologout` — set the number of minutes the CLI remains inactive prior to logging off the current user ID, or disable autologout on the ESKM appliance. The Management Console timeout is 60 minutes and is not controlled by this feature.

Syntax

```
hostname (config)# autologout <minutes>
```

The default autologout is 30 minutes. You can disable autologout by specifying a value of 0. You must specify a value in the range of 0 to 720.

Related command(s)

- "show autologout (p. 607)"

`show autologout` — view the currently configured autologout settings.

Syntax

```
hostname# show autologout
```

Related command(s)

- "autologout (p. 607)"

7.4.5 Backup and restore commands

Use these commands to create, delete, list, and schedule backups on the ESKM appliance, and also to restore backups on the ESKM appliance.

`backup` — create a system backup.

⚠ You can specify an IPv6 address for the host when IPv6 is enabled on the ESKM appliance, see ipv6 enable (p. 693), and SCP is used to send the backup file.

Syntax

```
hostname (config)# backup
Enter the backup name:
Enter a backup description:
Please indicate below which Security items are to be backed up:
Which keys would you like to back up?
1:  All ESKM keys
2:  No ESKM keys
3:  One ESKM key
Enter a number (1 - 3): 1
KMIP Users, Groups, Objects (y/n):
Which Objects would you like to back up?
1:  All ESKM keys
2:  No ESKM keys
3:  One ESKM key
Enter a number (1 - 3): 1
Key Query and Options (y/n):
Authorization Policies (y/n):
Local Users & Groups (y/n):
LDAP Server for Users & Groups (y/n):
Scheduled Backups and SSH Authentication Key (y/n):
Would you like to back up all the certificates (y/n):
Would you like to back up all the local certificate authorities (y/n):
Please select the local CAs to be backed up:
Known CAs, CRLs, Trusted CA Lists (y/n):
High Security (y/n):
FIPS Status Server (y/n):
Please indicate below which Device items are to be backed up:
NTP (y/n):
```

```
Network (y/n):
IP Authorization (y/n):
Administrators (y/n):
Kerberos (y/n):
SNMP (y/n):
Logging (y/n):
KMS Server and Web Admin SSL (y/n):
KMIP server and SSL configuration (y/n):
KMS and REST Configuration  (y/n):
Services (y/n):
Log Signing Certificate (y/n):
Enter the backup password:
Please enter the password again:
Please pick one of the following types of backup:
1) Internal      2) SCP       3) Windows share (Kerberos)
Backup Type (1-3):
```

```
This backup may take several minutes...
```

```
Backup successful.
```

Related command(s)

- “no backup (p. 610)”
- ”restore backup (p. 611)”
- “show backup (p. 615)”

`edit scheduled backup` — modify an existing scheduled backup. You can use this command to change the description, password, items to backup, schedule, time, or destination of an existing scheduled backup file.

Syntax

```
hostname (config)# edit scheduled backup <name of scheduled backup>
```

Related command(s)

- “no scheduled backup (p. 611)”
- “scheduled backup (p. 613)”
- “show scheduled backup (p. 615)”

`no backup` — remove a specified system backup file.

Syntax

```
hostname (config)# no backup <name of backup>
```

Related command(s)

- “backup (p. 608)”
- ”restore backup (p. 611)”
- “show backup (p. 615)”

`no scheduled backup` — remove a specified scheduled backup file.

Syntax

```
hostname (config)# no scheduled backup <name of scheduled backup>
```

Related command(s)

- “edit scheduled backup (p. 610)”
- “scheduled backup (p. 613)”
- “show scheduled backup (p. 615)”

`restore backup` — restore a backup file.

> You can specify an IPv6 address for the host when IPv6 is enabled on the ESKM appliance, see ipv6 enable (p. 693), and SCP is used to receive the backup file.

Syntax

```
hostname (config)# restore backup
Please pick the type of backup to restore:
1) Internal    2) SCP      3) Windows share (Kerberos)
Backup Type (1-3):
Enter the source filename:
Enter the backup password:
The following describes the backup you are going to restore:
Backup Name:
Description:
Archive Date: 2014-04-10 14:51:30
Would you like to restore this configuration item? (yes or no):
NTP (y/n):
Network (y/n):
IP Authorization (y/n):
Administrators (y/n):
Kerberos (y/n):
SNMP (y/n):
```

```
Logging (y/n):
KMS Server and Web Admin SSL (y/n):
Known CAs, CRLs, Trusted CA Lists (y/n):
High Security (y/n):
FIPS Status Server (y/n):
KMS and REST Configuration (y/n):
KMIP Server and SSL Configuration (y/n):
Key Query and Options (y/n):
Authorization Policies (y/n):
Local Users & Groups (y/n):
LDAP Server for Users & Groups (y/n):
Scheduled Backups and SSH Authentication Key (y/n):
Services (y/n):
Log Signing Certificate (y/n):
Certificates:
Would you like to restore all the certificates (y/n):
Local Certificate Authorities:
Would you like to restore all the certificate authorities
(y/n):
Would you like to restore the KMIP Users, Groups and Objects? (y/n):
Keys:
Would you like to restore all the keys (y/n):
Enter the backup password again to restore this backup:
Backup successfully restored.
Warning: Restart your system for changes to take effect.
```

Related command(s)

- “backup (p. 608)”
- “no backup (p. 607)”
- “show backup (p. 607)”

`scheduled backup` — create a scheduled backup.

You can specify an IPv6 address for the host when IPv6 is enabled on the ESKM appliance, see ipv6 enable, and SCP is used to send the backup file.

Syntax

```
hostname (config)# scheduled backup

Enter the backup name:

Enter a backup description:

Would you like to back up the keys? [y]:

Would you like to back up the certificates? [y]:

Would you like to back up the local certificate authorities? [y]:

Would you like to back up the system configuration? [y]:

Enter the backup password:

Please enter the password again:

Please pick one of the following types of backup:

1: Internal

2: SCP

3: SCP with SSH Public Key Authentication

4: Windows Share

Enter selection: 2

Enter the destination host:

Enter the destination directory:

Enter the SCP login username:
```

```
Enter the SCP login password:

Please pick one of the following backup schedules:

1: Daily

2: Weekly

3: Monthly

Enter selection:

Select the type of monthly schedule:

1: Fixed Day of Month

2: Fixed Day of Week

Enter selection:

Enter the day of the month (1-31) for backup to occur:

Enter the hour (0-23) for backup to occur [03]:

Enter the minute (0-59) for backup to occur [15]:

Added scheduled backup [name;description]
```

⚠ System Configuration items include the following:
Local Users & Groups, Key Queries and Options, Authorization Policies, LDAP Server for Users & Groups, Scheduled Backups, High Security, FIPS Status Server, NTP, Network, IP Authorization, Administrators, Kerberos, SNMP, Log Configuration, KMS Server and Web Admin SSL, KMS Server Configuration, KMIP Server and SSL Configuration, Services, Log Signing Certificate, and License data

⚠ The term KMIP database refers to the KMIP users, groups, and objects.

Related command(s)

- “edit scheduled backup (p. 607)”
- “no scheduled backup (p. 607)”
- “show scheduled backup (p. 607)”

`show backup` — view a list of the backup files stored on the ESKM appliance.

Syntax

```
hostname# show backup
```

Related command(s)

- “backup (p. 608)”
- “no backup (p. 610)”
- ”restore backup (p. 611)”

`show scheduled backup` — view the properties of a specified scheduled backup or a list of the scheduled backup files on the ESKM appliance.

Syntax

```
hostname# show scheduled backup [name of scheduled backup]
```

> The name of scheduled backup is an optional parameter, when specified the properties of the scheduled backup will be listed. When not specified the names of all existing scheduled backups will be listed.

Related command(s)

- “edit scheduled backup (p. 610)”
- “scheduled backup (p. 613)”
- “no scheduled backup (p. 607)”

7.4.6 CA certificate commands

Use these commands to manage CAs, certificates, and CA profiles.

`ca certificate install` — install a CA certificate.

Syntax

```
hostname (config)# ca certificate install <cert name>
Please perform these 2 steps to install the CA certificate:

1) Paste the CA certificate immediately after the question mark

2) Press return twice when you have finished
?
```

Related command(s)

- "no ca certificate (p. 622)"
- "show ca certificate (p. 624)"

`ca profile` — create an empty Trusted CA List profile.

Syntax

```
hostname (config)# ca profile <profile name>
```

The profile is only useful when you populate it.

Related command(s)

- "ca profile duplicate (p. 617)"
- "ca profile entry (p. 617)"
- "ca profile rename (p. 618)"
- "show ca profile (p. 625)"
- "no ca profile (p. 623)"
- "no ca profile entry (p. 623)"

`ca profile duplicate` — copy the Trusted CA List from one profile and populate the Trusted CA List of another profile.

Syntax

```
hostname (config)# ca profile duplicate <source profile> <target
profile>
```

Related command(s)

- “ca profile entry (p. 617)”
- “ca profile rename (p. 618)”
- “show ca profile (p. 625)”
- “no ca profile (p. 623)”
- “no ca profile entry (p. 623)”
- ”ca profile” (p. 616)

`ca profile entry` — add a CA to a Trusted CA List.

Syntax

```
hostname (config)# ca profile entry <profile name> <ca name>
```

Related command(s)

- “ca profile duplicate (p. 617)”
- “ca profile rename (p. 618)”
- “show ca profile (p. 625)”
- “no ca profile (p. 623)”
- “no ca profile entry (p. 623)”
- ”ca profile” (p. 616)

`ca profile rename` — rename a Trusted CA List profile.

Syntax

```
hostname (config)# ca profile rename <old name> <new name>
```

Related command(s)

- "ca profile" (p. 616)
- “ca profile duplicate (p. 617)”
- “ca profile rename (p. 618)”
- “show ca profile (p. 625)”
- “ca profile entry (p. 617)”
- “no ca profile entry (p. 623)”

`cert install` — install a certificate.

Syntax

```
hostname (config)# cert install <cert name>
Please perform these 2 steps to install the certificate:

1) Paste the certificate immediately after the question mark

2) Press return twice when you have finished
?
```

During the installation session, the ESKM appliance will prompt for the certificate.

Related command(s)

- “cert request (p. 628)”
- “show request (p. 631)”
- “no request (p. 630)”
- “no cert (p. 629)”
- “cert import (p. 627)”
- “show cert (p. 630)”
- “cert selfsign install (p. 629)”

`cert renew` — renew a certificate that has been signed and revoked by a local CA. Use the show signed certificate command to obtain the serial number of the certificate.

Syntax

```
hostname (config)# cert renew <local ca name> <serial number>
```

Related command(s)

- “show signed certificate (p. 626)”

`cert revoke` — revoke a certificate signed by a local CA. Use the show signed certificate command to obtain the serial number of the certificate.

Syntax

```
hostname (config)# cert revoke <local ca name> <serial number>
```

Related command(s)

- "show signed certificate (p. 626)"

`local ca` — generate a local CA certificate.

Syntax

```
hostname (config)# local ca
Enter the certificate name:
Enter the common name:
Enter the organization name:
Enter the organization unit name:
Enter the locality name:
Enter the state name:
Enter the country name [US]:
Enter the email address:
Algorithm (RSA-2048, RSA-3072, RSA-4096, ECDSA-P256, ECDSA-P384, ECDSA-P521) [RSA-2048]:
Please pick the Certificate Authority Type to create:

1) Self-signed Root CA

2) Intermediate CA Request
Certificate Type (1-2) [1]: 1
Enter a number of days for CA certificate duration [3650]:
Enter a number of days for maximum user certificate duration [3650]:
Warning: Local CA certificates must be added to a trusted CA list in order to be recognized by the KMS Server. Local CA certificates should be backed up for protection.
Local CA certificate successfully generated.
```

Related command(s)

- “show local ca (p. 625)”
- “no local ca (p. 624)”
- “sign request (p. 626)”

`local ca install` — install an Intermediate CA Request certificate. Before executing this command, use the local ca (p. 616) command to create the Intermediate CA Request certificate, use the show local ca (p. 616) command to copy the certificate request, and then use the sign request (p. 616) command to sign the Intermediate CA Request certificate.

Syntax

```
hostname (config)# local ca install
Enter the Local CA request that this certificate is for:
Enter a number of days for maximum user certificate duration [3650]:
Please perform these 2 steps to install the certificate:
1) Paste the certificate immediately after the question mark
2) Press return twice when you have finished
Warning: Certificates should be backed up for protection
Certificate has been successfully installed.
```

Related command(s)

- "show local ca (p. 625)"
- "local ca (p. 621)"
- "sign request (p. 626)"

`no ca certificate` — remove a CA certificate.

Syntax

```
hostname (config)# no ca certificate <cert name>
```

Related command(s)

- "ca certificate install (p. 616)"

`no ca profile` — delete a Trusted CA List profile.

Syntax

```
hostname# no ca profile <profile name>
```

⚠ You cannot delete a trusted CA list profile if it used by the Web Administration, KMS or KMIP service. In addition, you cannot delete the default profile.

Related command(s)

- "ca profile" (p. 616)
- “ca profile duplicate (p. 617)”
- “ca profile rename (p. 618)”
- “show ca profile (p. 625)”
- “no ca profile entry (p. 623)”

`no ca profile entry` — delete a CA from a Trusted CA List.

Syntax

```
hostname# no ca profile entry <profile name> <ca name>
```

Related command(s)

- “ca profile (p. 616)”
- “ca profile duplicate (p. 616)”
- “ca profile entry (p. 616)”
- “ca profile rename (p. 616)”
- “show ca profile (p. 616)”
- “no ca profile entry (p. 616)”

`no local ca` — remove a specified local CA certificate.

Syntax

```
hostname (config)# no local ca <ca_name>
```

Related command(s)

- “show local ca (p. 616)”
- “local ca (p. 616)”

`show ca certificate` — view the names of all CA certificates, or to view details about a specified ca certificate.

Syntax

```
hostname# show ca certificate [ca cert name]
```

Related command(s)

- “ca certificate install (p. 616)”
- “no ca certificate (p. 616)”

`show ca profile` — display a list of Trusted Certificate Authority List Profiles, or to view details about a specified ca profile.

Syntax

```
hostname# show ca profile [profile name]
```

Related command(s)

- "ca profile (p. 616)"
- "ca profile duplicate (p. 616)"
- "ca profile entry (p. 616)"
- "ca profile rename (p. 616)"
- "show ca profile (p. 616)"
- "no ca profile entry (p. 616)"

`show local ca` — view the list of all currently configured local CA certificates, or details for a specified local CA certificate.

Syntax

```
hostname# show local ca [ca name]
```

Related command(s)

- "no local ca (p. 624)"

`show signed certificate` — display information about certificates signed by local CAs.

Syntax

```
hostname# show signed certificate <local ca name>
[serial number]
```

If you specify a local CA after the show signed certificate command, the ESKM appliance displays all of the certificates signed by that CA. If you specify a local CA and the serial number of a certificate signed by that CA, the ESKM appliance shows specific certificate information for that signed certificate.

Related command(s)

None

`sign request` — sign a certificate request using a local CA.

Syntax

```
hostname (config)# sign request
Enter the Local CA certificate to sign this request with:
Enter the certificate purpose of this request [Server/Client/Both]:
Enter a number of days for the certificate duration [3649]:
Please perform these 2 steps to sign the request:

1) Paste the request immediately after the question mark

2) Press return twice when you have finished
?
```

Related command(s)

- "show local ca (p. 625)"
- "local ca (p. 621)"

7.4.7 Certificate commands

Use these commands to manage certificates and certificate requests.

`cert import` — import a certificate.
You can specify an IPv6 address for the host when IPv6 is enabled on the ESKM appliance, see ipv6 enable (p. 693), and SCP is used to import the certificate.

Syntax

```
hostname (config)# cert import
Please pick the upload option for uploading your certificate:
1) Console Paste (PEM certs only)
2) SCP
Upload Type (1-2)? :
Enter cert name:
Enter the password protecting the private key:
Please perform these 2 steps to finish importing a PEM encoded
certificate and key:

1) Paste the PEM encoded certificate and private key (in any order)
immediately after the question mark

2) Press return three times when you are done
?
```

⚠ There is a line at the top of all certificates that includes five dashes, the words BEGIN CERTIFICATE, and five more dashes. The line looks like this:

```
-----BEGIN CERTIFICATE-----
```

Likewise, at the end of the certificate, there is a line that includes five dashes, the words END CERTIFICATE, and five more dashes. The line looks like this:

```
-----END CERTIFICATE-----
```

If any of those dashes are missing, the certificate import operation fails. These same issues pertain to the private key as well.

Related command(s)

- “cert request (p. 628)”
- “show request (p. 631)”
- “no request (p. 630)”
- “no cert (p. 629)”

- "cert install (p. 619)l"
- "show cert (p. 630)"
- "cert selfsign install (p. 629)"

`cert request` — create a certificate request.

Syntax

```
hostname (config)# cert request <cert name>
Common Name:
Organization Name:
Organizational Unit Name:
Locality Name:
State or Province Name:
Country Name [US]:
Email Address:
Subject Alternative Name:
Algorithm (RSA-2048, RSA-3072, RSA-4096, ECDSA-P256, ECDSA-P384, ECDSA-
P521) [RSA-2048]:
```

When you have entered all the information, the ESKM appliance displays a backup warning, then displays the new certificate request.

Related command(s)

- "show request (p. 631)"
- "no request (p. 630)"
- "no cert (p. 629)"
- "cert install (p. 619)"
- "show cert (p. 630)"
- "cert selfsign install (p. 629)"
- "cert import (p. 627)"

`cert selfsign install` — install a test certificate. This command allows you to set up a self-signed certificate. The optional duration parameter allows you to specify in days the duration for which the certificate is valid.

Syntax

```
hostname (config)# cert selfsign install <cert name> [duration]
```

Related command(s)

- “cert request (p. 628)”
- “show request (p. 631)”
- “no request (p. 630)”
- “no cert (p. 629)”
- “cert install (p. 619)”
- “show cert (p. 630)”
- “cert import (p. 627)”

`no cert` — delete an installed certificate.

Syntax

```
hostname (config)# no  <cert name>
```

Related command(s)

- “cert request (p. 628)”
- “show request (p. 631)”
- “no request (p. 630)”
- “cert install (p. 619)”
- “show cert (p. 630)”
- “cert import (p. 627)”
- “cert selfsign install (p. 629)”

`no request` — delete a certificate request.

Syntax

```
hostname (config)# no request <cert name>
```

Related command(s)

- "no cert (p. 629)"
- "cert request (p. 628)"
- "show request (p. 631)"
- "cert install (p. 619)"
- "show cert (p. 630)"
- "cert import (p. 627)"
- "cert selfsign install (p. 629)"

`show cert` — view either specific certificate details or all installed certificates.

Syntax

```
hostname# show cert [cert name]
```

Related command(s)

- "no cert (p. 629)"
- "cert request (p. 628)"
- "show request (p. 631)"
- "cert install (p. 619)"
- "cert import (p. 627)"
- "cert selfsign install (p. 629)"
- "no request (p. 630)"

`show request` — view specific, or all, certificate request details.

Syntax

```
hostname# show request [cert name]
```

Related command(s)

- "no cert (p. 629)"
- "cert request (p. 628)"
- "cert install (p. 619)"
- "cert import (p. 627)"
- "cert selfsign install (p. 629)"
- "no request (p. 630)"
- "show cert (p. 630)"

7.4.8 CRL commands

Certificate Authorities (CAs) regularly publish a list of certificates that have been revoked by that CA. Such a list is called a certificate revocation list (CRL). The list of revoked certificates is distributed in X.509 CRL v2 format. Support for CRLs on the ESKM appliance allows you to obtain, query, and maintain CRLs published by CAs supported on the ESKM appliance.

7.4.8.1 Support for certificate revocation lists

The ESKM appliance uses CRLs to verify certificates in two ways.

- Require Client Authentication — When enabled, the ESKM appliance only accepts connections from clients that present a valid client certificate. As certificates are presented to the ESKM appliance, they are checked against the CRL published by the CA who issued the certificate.
- Web Administration User Authentication — When enabled, this option specifies that you cannot log in to the Management Console without presenting a valid client certificate. As certificates are presented to the ESKM appliance, they are checked

against the CRL published by the CA who issued the
certificate.

You can configure the ESKM appliance to fetch the CRL at a regular interval. The CRL is transported to the ESKM appliance via SCP or HTTP. The ESKM appliance can only be configured to retrieve complete CRLs, as opposed to partial, delta, or indirect CRLs. You can also manually download updated CRLs to the ESKM appliance.

The ESKM appliance validates all CRLs that it downloads. For the ESKM appliance to validate a CRL, the CA that signed the CRL must be in the list of Trusted CAs on the ESKM appliance. CRLs published by untrusted CAs are rejected by the ESKM appliance. Once a CRL is installed on the ESKM appliance, it remains in effect on the device until the CRL is successfully updated by a CRL from the same issuing
CA. If a CRL has been signed with a key that does not match the key in the CA certificate on the ESKM appliance, the validation of the CRL fails.

When a certificate on the ESKM appliance appears on a CRL, the event is logged in the System Log. Traps for revoked certificates are sent daily around 5:10 AM local time.

Local CAs

Additionally, you can export a CRL issued by local CAs. CRLs exported from the ESKM appliance contain a list of certificates revoked by local CAs. The format of CRLs exported by the ESKM appliance is in PEM-encoded X.509 format.

Auto-update

Each CA promises to update its CRL at the day and time specified in the Next Update field for that CA. When you enable the Auto-Update feature, at 5:00 AM every day the ESKM appliance inspects the Next Update value for the CRL associated with each CA on the ESKM appliance. For CRLs whose Next Update time is in the past, the ESKM appliance attempts to connect to the CRL distribution point (CDP) for the CA to download the updated CRL. If the download was successful, the Next Update field for that CA is changed to the new update time contained in the newly-downloaded CRL. If the Next Update value for that CRL is in the future, the ESKM appliance waits until that specified time to attempt to connect to the CDP and download the updated CRL.

Example:
There is a CA named XYZ that has a CRL Next Update time of Oct 20 01:00:00 2002 (1:00 AM). The administrator has enabled CRL auto-updates on the ESKM appliance. At 5:00 AM on Oct 20, the ESKM appliance checks the Next Update times for all of the CAs. When it gets to CA XYZ, it will notice that the Next Update time was in the past (4 hours ago), and it will attempt to download an updated CRL from the appropriate CDP.

If the CRL download was successful, the Next Update field for that CA is changed to the new update time contained in the downloaded CRL.

Should the CRL download fail, the ESKM appliance continues using the old CRL, and it tries again each day to download the updated CRL at the normal 5:00 AM autoupdate time.

The Auto-Update feature is a global setting. If you want to disable Auto-Update for a particular CA, you can use the crl settings command to set the Next Update value to a time in the distant future.

⚠ The Auto-Update feature does not apply to local CAs.

Force periodic update

The ESKM appliance performs a daily check of the Next Update field to determine whether it should attempt to update the CRL for a particular CA. If you are not satisfied with a daily check of the Next Update field or if it is possible that the CA incorrectly set the Next Update field in the CRL, you can use the optional Force Periodic Update parameter to instruct the ESKM appliance to download updated CRLs at an interval you specify. It is important to note that when you specify a value for the Force Periodic Update parameter, the ESKM appliance does not stop making daily checks of the Next Update field. For example, if you set the Force Periodic Update parameter to 10800 minutes (one week), the ESKM appliance continues to check the Next Update field on a daily basis to see if it is necessary to download an updated CRL. In addition, the ESKM appliance downloads the CRL from the CDP according to the value you specify in the Force Periodic Update parameter.

The Force Periodic Update parameter supports values between 5 and 525600 minutes (one year). Values must be a multiple of 5; if you enter a number that is not a multiple of 5, the value is rounded down to the closest multiple of 5. For example, if you enter a value of 12, the value will be rounded down to 10.

⚠ The Force Periodic Update parameter is not available for local CAs.

Use the below commands to manage the CRL.

`crl auto-update` — enable the Auto-Update feature.

Syntax

```
hostname (config)# crl auto-update
```

Related command(s)

- "no crl auto-update (p. 637)"
- "show crl auto-update (p. 637)"

`crl list send` — export a CRL.

Syntax

```
hostname (config)# crl list send <ca name>
Transport Method: SCP
Host:
Filename:
Username:
Password:
```

Related command(s)

None

`crl list update` — manually update a CRL. This command cannot be applied to a local CA.

Syntax

```
hostname (config)# crl list update <ca name>
Transport Method:
1) SCP 2) HTTP
Enter a number(1-2):
Host:
Filename:
Username:
Password:
```

Related command(s)

- "crl auto-update (p. 634)"
- "show crl auto-update (p. 637)"

`crl settings` — configure the ESKM appliance to automatically download the CRL for a CA.

Syntax

```
hostname (config)# crl settings <ca name>
Transport Method:
1) SCP 2) HTTP
Enter a number(1-2):
Host:
Filename:
Username:
Password:
Confirm password:
Next Update:
Enter a date as Month Day HH:MM:SS Year TZ
For example, Jan 04 00:00:00 2014 GMT
Force a periodic update of the CRL?[n]:
Force Update Interval (min):
```

The Next Update prompt is used to set the Next Update field in the CRL, not to change the actual update time. The actual update time follows the normal 5:00 AM procedures.

This command is only effective when crl auto-update (p. 634) is enabled. This command cannot be used for local CAs.

Related command(s)

- "show crl settings (p. 638)"

`no crl auto-update` — disable the Auto-Update feature.

Syntax

```
hostname (config)# no crl auto-update
```

Related command(s)

- "crl auto-update (p. 634)"
- "show crl auto-update (p. 637)"

`no crl list` — renew all revoked certificates signed by a local CA or delete the CRL published by a known CA.

Syntax

```
hostname (config)# no crl list <ca name>
```

When you use the no crl list command with a Known CA (as opposed to a local CA), the ESKM appliance deletes the CRL published by that CA. When you use the no crl list command with a local CA, the ESKM appliance renews all revoked certificates signed by that local CA.

Related command(s)

None

`show crl auto-update` — check if the Auto-Update feature is enabled.

Syntax

```
hostname# show crl auto-update
```

Related command(s)

- "crl auto-update (p. 634)"
- "no crl auto-update (p. 637)"

`show crl entry` — check if a certificate is on a CRL.

Syntax

```
hostname# show crl entry <ca name> <serial number>
```

Use the show signed certificate command to obtain the serial number of the certificate.

Related command(s)

- "show signed certificate (p. 626)"

`show crl list` — display the serial number and revocation date of all revoked certificates in the CRL.

Syntax

```
hostname# show crl list <ca name>
```

Related command(s)

None

`show crl settings` — display the CRL settings for a CA.

Syntax

```
hostname# show crl settings <ca name>
CA Name: Thawte_Personal_Freemail_CA
CDP: ftp://crl.company.com/crl_update.crl
Next Update: Nov 20 05:00:00 2013 PST
Username: admin
```

When you execute this command, the information you see should be similar to what is shown above.

Related command(s)

- "crl settings (p. 636)"

`show crl status` — display the general information associated with a CRL.

General information includes:

- complete DN of the Issuer
- last update and next update value for the CRL
- signature algorithm for the CRL

Syntax

```
hostname# show crl status <ca name>
```

Related command(s)

- "show crl list (p. 638)"

7.4.9 Client event log commands

The Client Event Log contains a record of each message sent by ESKM clients to the KMS Server using the <RecordMessageRequest> element. Use these commands to view and manage the Client Event Log. For more information on log commands, see Log commands (p. 660).

- "clientevent log rotate" (p. 666)
- "clientevent syslog" (p. 677)
- "no clientevent log" (p. 661)
- "no clientevent syslog" (p. 681)
- "show clientevent log" (p. 664)
- "show clientevent syslog" (p. 683)
- "transfer clientevent log" (p. 672)

7.4.10 Appliance reset and restore commands

Use these commands to reset, restore or zeroize keys in the ESKM appliance.

`reset factory settings` — delete all information stored in the ESKM appliance and reset it to its original factory setting.

This command deletes all configuration information and any installed patches and upgrades. Utimaco recommends contacting Utimaco Technical Support (p. 798) prior to using this command.

For security purposes, this command can only be run from the CLI at the console. You cannot execute this command remotely via the CLI over SSH or from the Management Console.

Syntax

```
hostname (config)# reset factory settings
```

Related command(s)

- "zeroize all keys (p. 642)"
- "restore default configuration (p. 641)"

`reset factory settings zeroize` — zeroize all keys and passwords on the device.

For security purposes, this command can only be run from the CLI at the console. You cannot execute this command remotely via the CLI over SSH or from the Management Console.

Syntax

```
hostname (config)# reset factory settings zeroize
```

Related command(s)

- "reset factory settings (p. 640)"

`restore default configuration` — return the ESKM appliance to the default configuration.

This command deletes all configuration information, while leaving all installed patches and activated features intact. Utimaco recommends contacting Utimaco Technical Support (p. 798) prior to using this command.

For security purposes, this command can only be run from the CLI at the console. You cannot execute this command remotely via the CLI over SSH or from the Management Console.

Syntax

```
hostname (config)# restore default configuration
```

Related command(s)

- "reset factory settings (p. 640)"
- "zeroize all keys (p. 642)"

`zeroize all keys` — delete all keys from the ESKM appliance.

No KMS key is recoverable after using this command. Appliance configuration remains intact. Utimaco recommends contacting Utimaco Technical Support (p. 798) prior to using this command.

This command removes only KMS keys, not KMIP keys, from the local ESKM appliance. To zeroize KMS keys from an entire cluster, you must run the zeroize all KMS keys command on each ESKM appliance in the cluster.

Syntax

```
hostname (config)# zeroize all keys
Are you sure you want to continue? [n]:y
Are you REALLY sure you want to continue? [n]:y
All keys have been successfully zeroized.
```

Related command(s)

- “reset factory settings (p. 640)”
- “restore default configuration (p. 641)”

`zeroize all kmip-objects` — delete all KMIP objects from ESKM appliance.

No KMIP object is recoverable after using this command. Appliance configuration remains intact. Utimaco recommends contacting Utimaco Technical Support (p. 798) prior to using this command.

This command removes only KMIP objects, not KMS keys, from the local ESKM appliance. To zeroize KMIP objects from an entire cluster, you must run the zeroize all KMIP- objects command on each ESKM appliance in the cluster.

Syntax

```
hostname (config)# zeroize all kmip-objects
This command will delete 100 KMIP objects. Are you sure you want to
continue? [n]:y
Are you REALLY sure you want to continue? [n]:y
All KMIP objects have been successfully zeroized.
```

Related command(s)

- “reset factory settings (p. 640)”
- “zeroize all keys (p. 642)”

7.4.11 Diagnostic commands

Use these commands to perform diagnostics on the ESKM appliance.

`host run` — look up the host specified using the domain server.

Syntax

```
hostname (config)# host run <hostname>
```

Related command(s)

- "traceroute run (p. 645)"
- "netstat run (p. 644)"
- "ping run (p. 644)"

`ping run` — send ICMP ECHO_REQUEST packets to the specified network host.

Syntax

```
hostname (config)# ping run <hostname>
```

Related command(s)

- "host run (p. 644)"
- "traceroute run (p. 645)"
- "netstat run (p. 644)"

`netstat run` — generate a list of all active connections on the ESKM appliance.

Syntax

```
hostname (config)# netstat run
```

Related command(s)

- "host run (p. 644)"
- "traceroute run (p. 645)"
- "ping run (p. 644)"

`traceroute run` — print the route packets take to the specified network host. Only IPv4 addresses are supported.
Syntax

```
hostname (config)# traceroute run <hostname>
```

Related command(s)

- "host run (p. 644)"
- "netstat run (p. 644)"
- "ping run (p. 644)"

7.4.12 FIPS commands

Use these commands to manage the FIPS compliant settings on the ESKM appliance.

`fips compliant` — make the ESKM appliance FIPS-compliant. This will alter various server settings, as documented in Advanced security features (p. 368).

According to FIPS requirements, you cannot enable or disable FIPS when there are keys on the ESKM appliance. You must manually delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion. Utimaco strongly recommends that you back up your keys before deleting them.

Setting the ESKM appliance to be FIPS-compliant forces SSL/TLS connections to the KMS Server and to the Web Administration service to use TLS. Some Web browsers, do not have TLS enabled by default. If your browser is no longer able to make a connection to this Appliance, please check that it has TLS enabled.

Syntax

```
hostname (config)# fips compliant
```

```
Enable FIPS Compliance
This requires restarting of all the ESKM services including KMS, KMIP,
REST and SSH. Do you want to continue? (y/n) [n]: y
This device is now FIPS compliant.
Services are being restarted. This may take a while.
```

Related command(s)

- “show fips status (p. 650)”

`fips server` — enable the FIPS status server and assign it an IP address and a port.

Syntax

```
hostname (config)# fips server
Enable FIPS Status Server [y]:
Available IP addresses:

   1) All

   2) 172.17.3.21
Local IP (1-2)[1]:
Local Port [9081]:
```

⚠ You can view the FIPS Status Report by accessing `<http://<Local> IP>:<Local Port>/status.html`

Related command(s)

- “show fips server (p. 650)”

`security settings` — change the status of security-related functionality on the ESKM appliance. This functionality must be disabled for FIPS compliance. These settings are automatically configured when you select **Set FIPS Compliance** in the FIPS Compliance section.

> When you enable FIPS compliance on the ESKM appliance, the functionality displayed here is disabled. Modifying any of the items in the High Security Settings section immediately takes the Appliance out of FIPS compliance. This section should be used to review the key and device security functionality that has been disabled for full FIPS compliance. When the Appliance is FIPS-compliant, do not alter these settings.

> According to FIPS requirements, you cannot enable or disable FIPS when there are keys on the ESKM appliance. You must manually delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion. Utimaco strongly recommends that you back up your keys before deleting them.

For more information, see Advanced security features (p. 645).

Syntax

```
hostname (config)# security settings
Disable Creation and Use of Global Keys [y]:
Disable Non-FIPS Algorithms and Key Sizes [y]:
Disable Certificate Import through Serial Console Paste [y]:
```

```
Non-FIPS Algorithms and key Sizes are now allowed.
This requires restarting of all the ESKM services including KMS, KMIP,
REST and SSH. Do you want to continue? (y/n):
```

```
Non-FIPS Algorithms and Key sizes are now allowed.
Services are being restarted. This may take a while.
```

Related command(s)

- "show security settings (p. 649)"

`show security settings` — view the status of security-related functionality on the ESKM appliance.

⚠ This functionality must be disabled for FIPS compliance. These settings are automatically configured when you select Set FIPS Compliance in the FIPS Compliance section. For more information, see Advanced security features (p. 368).

Syntax

```
hostname (config)# show security settings
Key Security
Disable Creation and Use of Global Keys: Yes
Disable Non-FIPS Algorithms and Key Sizes: Yes
Device Security
Disable Certificate Import through Serial Console Paste: Yes
Other Security
Allow Key & Policy Configuration Operations: Disabled (FIPS compliant)
Allow Key Export: Disabled (FIPS compliant)
LDAP User Directory Configured:                  Yes (FIPS compliant)
LDAP Administrator Server Configured:          Yes (FIPS compliant)
Allowed SSL Protocols:                         TLS 1.2 (FIPS compliant)
Enabled SSL Ciphers:                         Only FIPS-compliant ciphers
```

Related command(s)

- "security settings (p. 648)"

`show fips server` — view the status of the FIPS Status Server and its IP and port.

Syntax

```
hostname# show fips server
Enable FIPS Status Server: Yes
Local IP: [All]
Local Port: 9081
You can view the FIPS Status Report by accessing:
<http://<Local> IP>:<Local Port>/status.html
```

Related command(s)

- "fips server (p. 647)"

`show fips status` — view to determine whether the ESKM appliance is FIPS 140-2-compliant. Also shows whether the HSM is FIPS 140-2 Level 3-compliant.

Syntax

```
hostname# show fips status
FIPS Compliant: No
```

Related command(s) "

- "fips compliant (p. 646)"

7.4.13 Group commands

Use these commands to manage ESKM and KMIP groups. ESKM groups only contain users. There are several types of KMIP groups: users, groups, and objects. There are four system generated KMIP groups: All Users, default user group, All Groups and default object group.

When you add a KMIP-enabled object group it automatically becomes a member of All Groups, in addition, a user group of the same name plus a suffix of _user is also automatically created. For example, when you add a KMIP-enabled object group named Production, a user group named Production_user is automatically created.

When adding a KMIP-enabled user you can either specify the KMIP user group this user will be a member of, or select the default user group. In addition, you can either specify an existing object group or select the default object group. KMIP-enabled users are automatically added to the All Users group.

For more information see, Users, groups, and permissions (p. 37).

`edit group` — add/remove a user to/from a specified user group. Use the show user detail (p. 759) command to view a list of exiting ESKM and KMIP-enabled users. You can only add or remove ESKM users to or from an ESKM group. Similarly, you can only add or remove KMIP-enabled users to or from a KMIP user group. You cannot edit a KMIP object group. To delete group memberships for KMIP objects, use the Delete Attribute request operation from the KMIP client with the Object Group attribute.

Syntax

```
hostname (config)# edit group <groupname>
Edit Type:
1. Add
2. Remove
Enter a number (1-2)[1]:
User Name:
Group successfully modified.
```

Related command(s)

- “group (p. 653)”
- “show group (p. 655)”
- “no group (p. 654)”
- “show user detail (p. 759)”

`edit group-permissions` — add or remove a permission for an operation that the KMIP source group can perform on the target group. A permission value of true indicates that the source group can perform this operation on the target group. A permission value of false indicates that the source group does not have permission to perform this operation on the target group.

Syntax

```
hostname (config)# edit group-permissions <source-group> <target-group>
Enter Permission Name:
Enter a number (1 - 27) [1]: 1
Permission Value (true/false) [true]:
```

Related command(s)

- "kmip group (p. 654)"
- "show user detail (p. 759)"
- "show group-permissions (p. 656)"

`group` — create a new ESKM user group.

Syntax

```
hostname (config)# group <groupname>
Group Type:
   1. Local
   2. LDAP
Enter a number (1-2) [1]:
Group successfully added.
The LDAP group type is not supported.
A group name of “detail” is not valid.
You can specify an ESKM user group name which has the same name as a
KMIP object group.
```

Related command(s)

- “edit group (p. 651)”
- “show group (p. 655)”
- “no group (p. 654)”

`kmip group` — create a new KMIP user group/object group pair.

Syntax

```
hostname (config)# kmip group <groupname>
KMIP User Group [groupname_user]:
KMIP Object Group [groupname]:
Group successfully added.
A groupname of “detail” is not valid.
You can specify an ESKM user group name which has the same name as a
KMIP object group.
```

Related command(s)

- “show group (p. 655)”
- “no group (p. 654)”
- “show group detail (p. 655)”

`no group` — delete a group from the ESKM appliance. Deleting a KMIP user group does not delete the associated object group.

Syntax

```
hostname (config)# no group <groupname>
```

Related command(s)

- “edit group (p. 651)”
- “show group (p. 655)”
- “group (p. 653)”
- “show group detail (p. 655)”

`show group` — view a list of all groups, or a list of users/objects that are in the specified group.

Syntax

```
hostname# show group [groupname]
```

⚠ The optional parameter, groupname, is used to specify a specific group, when present all users in the specified group will be listed. When not specified, all existing groups will be listed.

⚠ A groupname of “detail” is not valid.

Related command(s)

- “edit group (p. 651)”
- “no group (p. 654)”
- “show group detail (p. 655)”

`show group detail` — view a list of ESKM user groups and KMIP groups and group-subtype.

Syntax

```
hostname# show group detail
```

Related command(s)

- “edit group (p. 651)”
- “no group (p. 654)”
- “show group (p. 655)”

`show group-permissions` — view a list of KMIP target groups where the KMIP source group has permission to perform at least one operation on the listed target groups. When the name of the target group is included in the command a list of all the possible operations and their permission is displayed. A permission value of true indicates that the source group can perform this operation on the target group. A permission value of false indicates that the source group does not have permission to perform this operation on the target group.

Syntax

```
hostname# show group-permissions <source-group>
[target-group]
```

Related command(s)

- "edit group-permissions (p. 652)"
- "no group (p. 654)"
- "show group (p. 655)"

7.4.14 Health check configuration commands

Use the below commands to configure the health check feature in the KMS and KMIP servers.

`health check` — enable and configure the KMS Health Check feature. IPv4 addresses are supported. If IPv6 has been enabled and IPv6 addresses have been configured they are also supported.

Syntax

```
hostname (config)# health check
Enable Health Check [n]: y
Local IP:
1: All
2: 192.168.200.195
Enter a number (1 - 2) [1]:
Local Port [9080]:
Health check settings successfully saved. Health check is enabled.
```

Related command(s)

- "show health check (p. 658)"

`kmip-health check` — enable and configure the KMIP Health Check feature. IPv4 addresses are supported. If IPv6 has been enabled and IPv6 addresses have been configured they are also supported.
Syntax

```
hostname (config)# kmip-health check
Enable KMIP Health Check [n]:
Local IP:
1: All
2: 192.168.200.195
Enter a number (1 - 2) [1]:
Local Port [9082]:
KMIP health check settings successfully saved. KMIP health check is
enabled.
```

Related command(s)

- "show kmip-health check (p. 656)"

`show health check` — view the Health Check settings of the ESKM appliance.

Syntax

```
hostname# show health check
```

Related command(s)

- "health check (p. 657)"

`show kmip-health check` — view the KMIP Health Check settings of the ESKM appliance.

Syntax

```
hostname# show kmip-health check
```

Related command(s)

- "kmip-health check (p. 657)"

7.4.15 Help commands

Use these commands to view a list of help topics, or to view the commands in a category.

`?` — view a list of commands associated with the current command mode.

This command is functionally identical to the help command.

Syntax

```
hostname# ? <category>
```

or

```
hostname (config)# ? <category>
```

Related command(s)

- "help (p. 659)"

`help` — view a list of commands associated with the current command mode.

Syntax

```
hostname# help <category>
```

or

```
hostname (config)# help <category>
```

Related command(s)

"? (p. 659)"

7.4.16 History command

Use this command to view the list of commands that have been executed during the current session.

`history` — view the list of commands executed on the ESKM appliance during the current session.

Syntax

```
hostname# history
```

Related command(s)

None

7.4.17 KMIP log commands

The KMIP Log contains a record of each request received by the KMIP Server and its result. Use these commands to view and manage the KMIP Log. For more information on log commands, see Log commands (p. 660).

- "kmip log rotate" (p. 666)
- "kmip syslog" (p. 678)
- "no kmip log" (p. 662)
- "no kmip syslog" (p. 681)
- "show kmip log" (p. 664)
- "show kmip syslog" (p. 683)
- "transfer kmip log" (p. 673)

7.4.18 Log commands

There are five types of logs: Audit, Activity, Client Event, KMIP, and System. These logs can be:

- cleared - see "Clear log file commands" (p. 661)
- displayed - see "Show log file commands" (p. 662)
- rotated - see "Rotate log file commands" (p. 665)

- signed - see "Sign log file commands" (p. 669)
- transferred - see "Transfer log file commands" (p. 670)
- sent via the syslog protocol to an external machine - see "Syslog commands" (p. 674)

7.4.18.1 Clear log file commands

The "no" command is used to clear the contents of a log. You can clear these logs: activity, clientevent, kmip, and system, you cannot clear the audit log.

`no activity log` — clear the contents of an activity log file.

Syntax

```
hostname (config)# no activity log <log name>
```

Related command(s)

- "activity log rotate (p. 665)"
- "show activity log (p. 663)"

`no clientevent log` — clear the context of a client event log file.

Syntax

```
hostname (config)# no clientevent log <log name>
```

Related command(s)

- "clientevent log rotate (p. 666)"
- "show clientevent log (p. 664)"

`no kmip log` — clear the context of a kmip log file.

Syntax

```
hostname (config)# no kmip log <log name>
```

Related command(s)

- “kmip log rotate (p. 666)”
- “show kmip log (p. 664)”

`no system log` — clear the context of a system log file.

Syntax

```
hostname (config)# no system log <log name>
```

Related command(s)

- “system log rotate (p. 667)”
- “show system log (p. 665)”

7.4.18.2 Show log file commands

The “show” command is used to display a list of logs, or to view a specific log. This command is also used to display log configuration information.The log names are: activity, audit, clientevent, kmip, and system.

`show activity log` — display a list of Activity Logs on the ESKM appliance, or view a specific Activity Log. The optional parameter, number of lines, allows you to specify how many lines to display.

Syntax

```
hostname# show activity log [log name] [number of lines]
```

Related command(s)

- "activity log rotate (p. 665)"
- "no activity log (p. 661)"
- "transfer activity log (p. 671)"

`show audit log` — display a list of the Audit Logs on the ESKM appliance, or view a specific Audit log. The optional parameter, number of lines, allows you to specify how many lines to display.

Syntax

```
hostname# show audit log [name] [number of lines]
```

Related command(s)

- "transfer audit log (p. 671)"

`show clientevent log` — display a list of client event log on the ESKM appliance, or view a specific client event log. The optional parameter, number of lines, allows you to specify how many lines to display.

Syntax

```
hostname# show clientevent log [log name] [number of lines]
```

Related command(s)

- "clientevent log rotate (p. 666)"
- "no clientevent log (p. 661)"
- "transfer clientevent log (p. 672)"

`show kmip log` — display a list of the KMIP Logs on the ESKM appliance, or view a specific KMIP log. The optional parameter, number of lines, allows you to specify how many lines to display.

Syntax

```
hostname# show kmip log [log name] [number of lines]
```

Related command(s)

- "kmip log rotate (p. 666)"
- "no kmip log (p. 662)"
- "transfer kmip log (p. 673)"

`show system log` — view a list of the System Log files on the ESKM appliance, or view a specific system log. The optional parameter, number of lines, allows you to specify how many lines to display.

Syntax

```
hostname# show system log [log name] [number of lines]
```

Related command(s)

- “no system log (p. 662)”
- “system log rotate (p. 667)”
- “ransfer system log (p. 674)”

7.4.18.3 Rotate log file commands

The “log rotate” command is used to rotate a log file. The “log rotation” commands are used to configure and display the log rotation schedule. The log names are: activity, audit, clientevent, kmip, and system.

You can specify an IPv6 address for the host when IPv6 is enabled on the ESKM appliance, see ipv6 enable (p. 693), and SCP is used to send the log file.

`activity log rotate` — rotate the Activity Log.

Syntax

```
hostname (config)# activity log rotate
Activity Log successfully rotated.
```

Related command(s)

- “no activity log (p. 661)”
- “show activity log (p. 663)”

`clientevent log rotate` — rotate the Client Event log.

Syntax

```
hostname (config)# clientevent log rotate
Client Event Log successfully rotated.
```

Related command(s)

- "no clientevent log (p. 661)"
- "show clientevent log (p. 664)"
- "transfer clientevent log (p. 672)"

`kmip log rotate` — rotate the KMIP Log.

Syntax

```
hostname (config)# kmip rotate log
KMIP Log successfully rotated.
```

Related command(s)

- "no kmip log (p. 662)"
- "show kmip log (p. 664)"
- "transfer kmip log (p. 673)"

`system log rotate` — rotate the System Log.

Syntax

```
hostname (config)# system log rotate
System Log successfully rotated.
```

Related command(s)

- “no system log (p. 662)”
- “show system log (p. 665)”

`edit log rotation` — edit the log rotation settings for the specified log.

Syntax

```
hostname (config)# edit log rotation <log_name>
Please pick one of the following rotation schedules:
1) Daily         2) Weekly        3) Monthly
Rotation Schedule [2]: 2
Enter the time (HH:MM) for log rotation to occur:
Select the day of week for log rotation to occur:
Day of the Week: 5
Enter the num logs archived: 4
Enter the max log file size (MB): 10
Please pick one of the following types of transfer:
1) None 2) SCP
Transfer Type [1]: 2
Enter the host:
Enter the directory:
Enter the username:
Enter the password:
```

After providing the necessary information, the ESKM appliance displays a message confirming that the log rotation was changed.

Related command(s)

- “show log rotation (p. 665)”

`show log rotation` — show all the current logs and some general information on them, or specify a log name to see the detailed settings for the specified log.

Syntax

```
hostname# show log rotation <log name>
```

Related command(s)

- “edit log rotation (p. 665)”

7.4.18.4 Sign log file commands

The "log signing" commands instructs the ESKM appliance to sign the specified log file. The "logsigning" commands manage the log signing certificate. The log names are: activity, audit, clientevent, kmip, and system.

`log signing` — sign a log file, for more information on log signing, see Secure logs (p. 520).

Syntax

```
hostname (config)# log signing <log-name>
```

Related command(s)

- "recreate logsigning cert (p. 670)"
- "show logsigning cert (p. 670)"
- "show log signing (p. 669)"

`show log signing` — check the status of the Secure Log feature for a specific log.

Syntax

```
hostname# show log signing <log-name>
```

Related command(s)

- "log signing (p. 669)"
- "recreate logsigning cert (p. 670)"
- "show logsigning cert (p. 670)"

`recreate logsigning cert` — recreate the log signing certificate.

Syntax

```
hostname (config)# recreate logsigning cert
```

Related command(s)

- "log signing (p. 669)"
- "show logsigning cert (p. 670)"
- "show log signing (p. 669)"

`show logsigning cert` — show the log signing certificate.

Syntax

```
hostname# show logsigning cert
```

Related command(s)

- "log signing (p. 669)"
- "recreate logsigning cert (p. 670)"
- "show log signing (p. 669)"

7.4.18.5 Transfer log file commands

The "transfer" command is used to manually move a specific log file to a remote host. The log names are: activity, audit, clientevent, kmip, and system.

⚠ The ESKM can transfer log files to a remote host which has an IPv6 address when IPv6 is enabled on the ESKM appliance, see ipv6 enable (p. 693), and SCP is used to send the files.

`transfer activity log` — transfer an activity log file off the ESKM appliance.

Syntax

```
hostname# transfer activity log <log_name>
Please pick one of the following types of transfer:
Transfer Type: SCP
Enter the host:
Enter the directory:
Enter the username:
Enter the password:
Success.
```

Related command(s)

- "activity log rotate (p. 665)"
- "no activity log (p. 661)"
- "show activity log (p. 663)"

`transfer audit log` — transfer an audit log file off the ESKM appliance.

Syntax

```
hostname# transfer audit log <log_name>
Please pick one of the following types of transfer:
Transfer Type: SCP
Enter the host:
Enter the directory:
Enter the username:
Enter the password:
Success.
```

Related command(s)

- "show audit log (p. 663)"

`transfer clientevent log` — transfer a client event log off the ESKM appliance.

Syntax

```
hostname# transfer clientevent log <log_name>
Please pick one of the following types of transfer:
Transfer Type: SCP
Enter the host:
Enter the directory:
Enter the username:
Enter the password:
Success.
```

Related command(s)

- “clientevent log rotate (p. 666)”
- “no clientevent log (p. 661)”
- “show clientevent log (p. 664)”

`transfer kmip log` — transfer a KMIP Log off the ESKM appliance.

Syntax

```
hostname# transfer kmip log <log_name>
Please pick one of the following types of transfer:
Transfer Type: SCP
Enter the host:
Enter the directory:
Enter the username:
Enter the password:
Success.
```

Related command(s)

- “kmip log rotate (p. 666)”
- “no kmip log (p. 662)”
- “show kmip log (p. 664)”

`transfer system log` — transfer a system log off the ESKM appliance.

Syntax

```
hostname# transfer system log <log_name>
Please pick one of the following types of transfer:
Transfer Type: SCP
Enter the host:
Enter the directory:
Enter the username:
Enter the password:
Success.
```

Related command(s)

- "system log rotate (p. 667)"
- "no system log (p. 662)"
- "show system log (p. 665)"

7.4.18.6 Syslog commands

The "syslog" command specifies if the log file messages should be sent to a external machine using the syslog protocol. The log names are: activity, audit, clientevent, kmip, and system.

`activity syslog` — enable the ESKM appliance to use the syslog protocol to send Activity Log messages to an external machine.

Syntax

```
hostname (config)# activity syslog
Enable Syslog [n]:
Syslog Server #1 IP [None]:
Syslog Server #1 Port [514]:
Syslog Server #2 IP [None]:
Syslog Server #2 Port [514]:
Syslog Facility:
1: local0
2: local1
3: local2
4: local3
5: local4
6: local5
7: local6
8: local7
Enter a number (1 - 8) [2]:
Activity Log syslog settings successfully saved. Syslog is enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext.
```

Related command(s)

- "no activity syslog (p. 680)"
- "show activity syslog (p. 682)"

`audit syslog` — enable the ESKM appliance to use the syslog protocol to send Audit Log messages to an external machine.

Syntax

```
hostname (config)# audit syslog
Enable Syslog [n]:
Syslog Server #1 IP [None]:
Syslog Server #1 Port [514]:
Syslog Server #2 IP [None]:
Syslog Server #2 Port [514]:
Syslog Facility:
1: local0
2: local1
3: local2
4: local3
5: local4
6: local5
7: local6
8: local7
Audit Log syslog settings successfully saved. Syslog is enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext.
```

Related command(s)

- “no audit syslog (p. 680)”
- “show audit syslog (p. 682)”

`clientevent syslog` — enable the ESKM appliance to use the syslog protocol to send Client Event Log messages to an external machine.

Syntax

```
hostname (config)# clientevent syslog
Enable Syslog [n]:
Syslog Server #1 IP [None]:
Syslog Server #1 Port [514]:
Syslog Server #2 IP [None]:
Syslog Server #2 Port [514]:
Syslog Facility:
1: local0
2: local1
3: local2
4: local3
5: local4
6: local5
7: local6
8: local7
Enter a number (1 -8) [2]:
Client Event Log syslog settings successfully saved.
Syslog is enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext.
```

Related command(s)

- “no clientevent syslog (p. 681)”
- “show clientevent syslog (p. 683)”

`kmip syslog` — enable the ESKM appliance to use the syslog protocol to send KMIP Log messages to an external machine.

Syntax

```
hostname (config)# kmip syslog
Enable Syslog [n]:
Syslog Server #1 IP [None]:
Syslog Server #1 Port [514]:
Syslog Server #2 IP [None]:
Syslog Server #2 Port [514]:
Syslog Facility:
1: local0
2: local1
3: local2
4: local3
5: local4
6: local5
7: local6
8: local7
KMIP Log syslog settings successfully saved. Syslog is
enabled.
Warning: The syslog protocol insecurely transfers KMIP Logs in
cleartext.
```

Related command(s)

- “no kmip syslog (p. 681)”
- “show kmip syslog (p. 683)”

`system syslog` — enable the ESKM appliance to use the syslog protocol to send System Log messages to an external machine.

Syntax

```
hostname (config)# system syslog
Syslog Server #1 IP [None]:
Syslog Server #1 Port [514]:
Syslog Server #2 IP [None]:
Syslog Server #2 Port [514]:
Syslog Facility:
1: local0
2: local1
3: local2
4: local3
5: local4
6: local5
7: local6
8: local7
System Log syslog settings successfully saved. Syslog is
enabled.
Warning: The syslog protocol insecurely transfers logs in cleartext.
```

Related command(s)

- "no system syslog (p. 682)"
- "show system syslog (p. 683)"

`no activity syslog` — disable the use of the syslog protocol to send Activity Log messages to an external machine.

Syntax

```
hostname (config)# no activity syslog
Activity Log syslog settings cleared. Syslog is disabled.
```

Related command(s)

- "activity syslog (p. 675)"
- "show activity syslog (p. 682)"

The no audit syslog command also clears all values in the Activity Log settings.

`no audit syslog` — disable the use of the syslog protocol to send Audit Log messages to an external machine.

Syntax

```
hostname (config)# no audit syslog
Audit Log syslog settings cleared. Syslog is disabled.
```

Related command(s)

- "show audit syslog (p. 682)"
- "audit syslog (p. 676)"

The no audit syslog command also clears all values in the Audit Log settings.

`no clientevent syslog` — disable the use of the syslog protocol to send Client Event Log messages to an external machine.

Syntax

```
hostname (config)# no clientevent syslog
Client Event Log syslog settings cleared. Syslog is disabled.
```

Related command(s)

- "clientevent syslog (p. 677)"
- "show clientevent syslog (p. 683)"

The no clientevent syslog command also clears all values in the Client Event Log settings.

`no kmip syslog` — disable the use of the syslog protocol to send KMIP Log messages to an external machine.

Syntax

```
hostname (config)# no kmip syslog
KMIP Log syslog settings cleared. Syslog is disabled.
```

Related command(s)

- "kmip syslog (p. 678)"
- "show kmip syslog (p. 683)"

The no kmip syslog command also clears all values in the KMIP Log settings.

`no system syslog` — disable the use of the syslog protocol to send System Log messages to an external machine.

Syntax

```
hostname (config)# no system syslog
```

Related command(s)

- “system syslog (p. 679)”
- “show system syslog (p. 683)”

The no system syslog command also clears all values in the System Log settings.

`show activity syslog` — display the syslog settings for the Activity Log.

Syntax

```
hostname# show activity syslog
```

Related command(s)

- “no activity syslog (p. 680)”
- “activity syslog (p. 675)”

`show audit syslog` — display the syslog settings for the Audit Log.

Syntax

```
hostname# show audit syslog
```

Related command(s)

- “no audit syslog (p. 680)”
- “audit syslog (p. 676)”

`show clientevent syslog` — display the syslog settings for the Client Event Log.

Syntax

```
hostname# show clientevent syslog
```

Related command(s)

- “no clientevent syslog (p. 681)”
- “clientevent syslog (p. 677)”

`show kmip syslog` — display the syslog settings for the KMIP log.

Syntax

```
hostname (config)# show kmip syslog
```

Related command(s)

- “no kmip syslog (p. 681)”
- “kmip syslog (p. 678)”

`show system syslog` — display the syslog settings for the System Log.

Syntax

```
hostname# show system syslog
```

Related command(s)

- “no system syslog (p. 682)”
- “system syslog (p. 679)”

`syslog tls` — define the configuration for TLS settings for syslog.

Syntax

```
hostname (config)# syslog tls
Enable TLS for Syslog [y]:
Certificate:
Enter a number (1 - 3) [3]:
Trusted Certificate Authority:
Enter a number (1 - 24) [24]:
```

Related command(s)

- no syslog tls (p. 684)
- show syslog tls (p. 685)

`no syslog tls` — disable the TLS settings for syslog.

Syntax

```
hostname (config)# no system syslog
TLS for syslog disabled.
```

Related command(s)

- syslog tls (p. 684)
- show syslog tls (p. 685)

`show syslog tls` — display the TLS settings for syslog.

Syntax

```
hostname (config)# show syslog syslog
Enable TLS: no
Certificate: [None]
Certifcate Authority: [None]
```

Related command(s)

- syslog tls (p. 684)
- no syslog tls (p. 684)

`syslog test` — test the TLS connection after you have defined a syslog TLS server.

Syntax

```
hostname (config)# syslog test
Log Name:
1: System
2: Audit
3: Activity
4: Client Event
5: KMIP
Enter a number (1 - 5) [1]:
Successfully connected to syslog server #1.
```

7.4.19 Mode commands

Use these commands to either terminate or change the mode of your current session.

`configure` — enter configuration mode.

Syntax

```
hostname# configure
```

Related command(s)

- “configure terminal (p. 686)”
- “exit (p. 687)”
- “script (p. 687)”

`configure terminal` — enter configuration mode.

Syntax

```
hostname# configure terminal
```

Related command(s)

- “configure (p. 686)”
- “exit (p. 687)”
- “script (p. 687)”

`exit` — exit the current shell mode.

⚠ When in “view” mode, typing exit logs you out of the shell. When in “configure” mode, typing exit returns you to “view” mode.

Syntax

```
hostname# exit
```

or

```
hostname (config)# exit
```

Related command(s)

- “configure (p. 686)”
- “configure terminal (p. 686)”
- “script (p. 687)”

`script` — enter script mode. For more information, see Script mode (p. 573).

Syntax

```
hostname (config)# script
```

Related command(s)

- “configure (p. 686)”
- “configure terminal (p. 686)”
- “exit (p. 687)”

7.4.20 Network commands

Use these commands to view and configure the ESKM appliance network interface connector parameters and IP authorization settings.

⚠ Only these commands support the ability to enter an ipv6 address: ipv6 address (p. 692) and no ipv6 address (p. 698) `edit ip authorization allowed` — edit the IP authorization settings for a particular IP address. The ip authorization allowed command requires that you provide the index number of the IP address you want to edit, rather than the actual IP address itself. You might find it helpful to use the show ip authorization allowed (p. 687) command to find the appropriate index number.

The IP Authorization feature is only supported on the KMS server, it is not supported on the KMIP server.

Syntax

```
hostname (config)# edit ip authorization allowed <index>
IP Address, Range, or Subnet [1.1.1.1]: 1.1.1.2
KMS Server [y]: y
Web Administration [n]:
SSH Administration [n]:
IP successfully saved.
```

Related command(s)

- "ip authorization (p. 695)"
- "ip authorization allowed (p. 696)"
- "no ip authorization allowed (p. 699)"
- "show ip authorization (p. 703)"
- "show ip authorization allowed (p. 704)"

`ethernet port` — change the Network Interface Port Speed/Duplex settings on the ESKM appliance.

Syntax

```
hostname (config)# ethernet port
Enter the port speed and duplex for Gigabit Ethernet Port #1:
1: Auto-Negotiate
2: 100 Mbps/Full Duplex
3: 1 Gbps/Full Duplex
4: 10 Gbps/Full Duplex
```

Related command(s)

- "show ethernet port (p. 700)"

`gateway` — define the default gateway to be used by the ESKM appliance. Only IPv4 addresses are supported.

Syntax

```
hostname (config)# gateway <gateway IP> <interface #>
```

For example, you might enter the following:

```
hostname (config)# gateway 192.10.10.10 1
```

Related command(s)

- "show gateway (p. 700)"
- "no gateway (p. 697)"

`gateway6` — define the default gateway to be used by the ESKM appliance. Only IPv6 addresses are supported.

Syntax

```
hostname (config)# gateway6 <gateway IP> <interface #>
```

For example, you might enter the following:

```
hostname (config)# gateway6 fc00:204:1::5 2
```

Related command(s)

- "outgoing gateway6 (p. 691)"
- "no gateway6 (p. 697)"

`outgoing gateway` — specify the interface to be used as the ESKM appliance's outgoing gateway.

Syntax

```
hostname (config)# outgoing gateway <interface #>
```

For example, you might enter the following:

```
hostname (config)# outgoing gateway 2
```

Related command(s)

- "show gateway (p. 700)"
- "no gateway (p. 697)"

`outgoing gateway6` — specify the interface to be used as the ESKM appliance's outgoing gateway.

Syntax

```
hostname (config)# outgoing gateway6 <interface #>
```

For example, you might enter the following:

```
hostname (config)# outgoing gateway6 1
```

Related command(s)

- "show gateway (p. 700)"
- "no gateway6 (p. 697)"

`ip address` — add an IPv4 address and subnet mask to the specified interface number in the network settings of the ESKM appliance.

Syntax

```
hostname (config)# ip address [<ip address> <submask> <interface #>]
Enter the IP address:
Enter the subnet mask:
Available interfaces:

1. Ethernet #1

2. Ethernet #2
Enter the interface (1-2):
```

Related command(s)

- "no ip address (p. 698)"
- "show interface ethernet (p. 701)"
- "show interfaces (p. 702)"

`ipv6 address` — add an IPv6 address/prefix to the specified interface number in the network settings of the ESKM appliance.

Support for IPv6 must be enabled before you can use this command. If IPv6 support was not enabled during setup you can use ipv6 enable to enable it.

Syntax

```
hostname (config)# ipv6 address <ip address/prefix>
<interface #>
Enter the IPv6 address with prefix [default prefix: /64]:
Available interfaces:

1. Ethernet #1

2. Ethernet #2
Enter the interface (1-2):
```

Related command(s)

- “no ip address (p. 698)”
- “show interface ethernet (p. 701)”
- “show interfaces (p. 702)”
- “ipv6 status (p. 694)”

`ipv6 enable` — enables support for IPv6 on the ESKM appliance.

Only enable IPv6 if you are certain that the ESKM appliance is required to operate on an IPv6 network. Once enabled it cannot be disabled.

The following ESKM features, which use SCP to move files, support IPv6 addresses: backup, restore, scheduled backup, transfer logs, certificate import, and software upgrade/install.

You can remotely administer, and perform network diagnostics (see ping run (p. 644) and netstat run (p. 644)) using a system that has an IPv6 address.

When you execute this command, the SSH and Web servers are automatically stopped and then restarted. Any existing IPv4 connection will be disconnected. Wait at least 1 minute and then re-establish your IPv4 connections again.

Syntax

```
hostname (config)# ipv6 enable
Please confirm that you would like to enable IPv6[y/n]? y
Successfully enabled IPv6.
Restarting SSH and Web Server ...
```

Related command(s)

- "ipv6 address (p. 692)"

`ipv6 status` — provides the state (enabled or disabled) of IPv6 support on the ESKM appliance.

Syntax

```
hostname (config)# ipv6 status
IPv6 is enabled.
```

Related command(s)

- "ipv6 enable (p. 693)"

`ip authorization` — edit the IP authorization settings.

⚠ The IP Authorization feature is only supported on the KMS server, it is not supported on the KMIP server.

Syntax

```
hostname (config)# ip authorization
KMS Server:
Please select from the following options:

1) Allow All Connections 2) Only Allow IPs Specified
KMS Server [2]: 2
Web Administration:
Please select from the following options:

1) Allow All Connections 2) Only Allow IPs Specified
Web Administration [2]: 2
SSH Administration:
Please select from the following options:

1) Allow All Connections 2) Only Allow IPs Specified
SSH Administration [2]: 2
IP Authorization settings successfully saved.
```

Related command(s)

- “ip authorization allowed (p. 696)”
- “edit ip authorization allowed (p. 688)”
- “no ip authorization allowed (p. 699)”
- “show ip authorization (p. 703)”
- “show ip authorization allowed (p. 704)”

`ip authorization allowed` — add a new IP address to the list of authorized IP addresses.

> ⚠ The IP Authorization feature is only supported on the KMS server, it is not supported on the KMIP server.

Syntax

```
hostname (config)# ip authorization allowed
IP Address, Range, or Subnet: 192.168.200.101
KMS Server [n]: y
Web Administration [n]: y
SSH Administration [n]: y
IP successfully saved.
```

Related command(s)

- "no ip address (p. 698)"

`ip name-server` — add a domain name server. You can add multiple DNS servers by executing one command.

Syntax

```
hostname (config)# ip name-server <IP1> <IP2>...<IPn>
```

Related command(s)

- "no ip name-server (p. 699)"
- "show hosts (p. 701)"

`no gateway` — remove a default gateway.

Syntax

```
hostname (config)# no gateway <interface #>
```

For example:

```
hostname (config)# no gateway 2
```

Related command(s)

- “gateway (p. 689)”
- “show gateway (p. 700)”

`no gateway6` — remove a default gateway6.

Syntax

```
hostname (config)# no gateway6 <interface #>
```

For example:

```
hostname (config)# no gateway6 1
```

Related command(s)

- “gateway6 (p. 690)”
- “show gateway (p. 700)”

`no ip address` — delete one or more IPv4 addresses from the network settings of the ESKM appliance.

Syntax

```
hostname (config)# no ip address <IP1> [<IP2>...<IPn>]
```

Related command(s)

- "ip address (p. 691)"
- "show interface ethernet (p. 701)"
- "show interfaces (p. 702)"

`no ipv6 address` — delete one or more IPv6 addresses from the network settings of the ESKM appliance.

Syntax

```
hostname (config)# no ipv6 address <IP1> [<IP2>...<IPn>]
```

Related command(s)

- "ipv6 address (p. 692)"
- "show interface ethernet (p. 701)"
- "show interfaces (p. 702)"

`no ip authorization allowed` — delete an IP address from the list of authorized IP addresses.

The no ip authorization allowed command requires that you provide the index number of the IP address you want to edit, rather than the actual IP address itself. Use the show ip authorization allowed command (p. 687) to find the appropriate index number. The IP Authorization feature is only supported on the KMS server, it is not supported on the KMIP server.

Syntax

```
hostname (config)# no ip authorization allowed <index>
IP successfully removed
```

Related command(s)

- "ip authorization (p. 695)"
- "ip authorization allowed (p. 696)"
- "edit ip authorization allowed (p. 688)"
- "show ip authorization (p. 703)"
- "show ip authorization allowed (p. 704)"

`no ip name-server` — deletes a domain name server from the ESKM appliance.

Syntax

```
hostname (config)# no ip name-server <IP1> <IP2>...<IPn>
```

Related command(s)

- "ip name-server (p. 696)"
- "show hosts (p. 701)"

`no static route` — deletes a static route from the ESKM appliance.

Syntax

```
hostname (config)# no static route
```

Related command(s)

- "static route (p. 705)"
- "show static route (p. 705)"

`show ethernet port` — view the Network Interface Port Speed/Duplex settings on the ESKM appliance.

Syntax

```
hostname# show ethernet port
```

Related command(s)

- "ethernet port (p. 689)"

`show gateway` — show the current gateway.

Syntax

```
hostname# show gateway
```

Related command(s)

- "gateway (p. 689)"
- "gateway6 (p. 690)"
- "no gateway (p. 697)"
- "no gateway6 (p. 697)"

`show hosts` — view currently configured domain name servers.

Syntax

```
hostname# show hosts
```

Related command(s)

- "ip name-server (p. 696)"
- "no ip name-server (p. 699)"

`show interface ethernet` — view the IPv4 address and subnet mask for the specified Ethernet port. If defined the IPv6 address/prefix will be included.

Syntax

```
hostname# show interface ethernet <interface #>
```

Related command(s)

- "ip address (p. 691)"
- "no ip address (p. 687)"
- "no ip name-server (p. 699)"
- "show interfaces (p. 702)"

`show interfaces` — view all network interfaces on the ESKM appliance. The IPv4 address and subnet mask, and IPv6 address/prefix (if defined) will be included

Syntax

```
hostname# show interfaces
```

Related command(s)

- “ip address (p. 687)”
- “no ip address (p. 698)”
- “no ipv6 address (p. 687)”
- “show interface ethernet (p. 687)”

`show mac address` —view the mac addresses of the Ethernet ports.

Syntax

```
hostname# show mac address
```

Related command(s)

- “ip address (p. 687)”
- “show interfaces (p. 702)”

`show ip authorization` — display whether each server grants access to all IPs or only grants access to specific IPs. The IP Authorization feature is only supported on the KMS server, it is not supported on the KMIP server.

Syntax

```
hostname# show ip authorization
KMS Server: Only Allow IPs Specified
Web Administration: Only Allow IPs Specified
SSH Administration: Only Allow IPs Specified
```

Related command(s)

- "ip authorization allowed (p. 696)"
- "edit ip authorization allowed (p. 688)"
- "no ip authorization allowed (p. 699)"
- "ip authorization (p. 695)"
- "show ip authorization allowed (p. 704)"

`show ip authorization allowed` — display the IP authorization settings for all authorized IP addresses. The IP Authorization feature is only supported on the KMS server, it is not supported on the KMIP server.

Syntax

hostname# show ip authorization allowed

```
1. IP Address, Range, or Subnet: 1.1.1.2
KMS Server: yes
Web Administration: no
SSH Administration: no

2. IP Address, Range, or Subnet: 192.168.1.129
KMS Server: yes
Web Administration: yes
SSH Administration: yes
```

⚠ You can view the settings for a particular IP address by passing in the index number of the IP address as a parameter in the show ip authorization allowed command. You might find it helpful to use the show ip authorization allowed command to find the appropriate index number.

Related command(s)

- "ip authorization allowed (p. 696)"
- "edit ip authorization allowed (p. 688)"
- "no ip authorization allowed (p. 699)"
- "ip authorization (p. 695)"
- "show ip authorization (p. 703)"

`show static route` — view the static route settings on the ESKM appliance.

Syntax

```
hostname# show static route
```

Related command(s)

- "static route (p. 705)"
- "no static route (p. 700)"

`static route` — configure a static route on the ESKM appliance.

Syntax

```
hostname (config)# static route
Enter the destination IP address: 10.0.0.0
Enter the subnet mask: 255.0.0.0
Enter the gateway: 192.168.200.2
Available interfaces:

Ethernet #1

Ethernet #2
Enter the interface (1-2):
Static route successfully added
```
.

Related command(s)

- "show static route (p. 705)"
- "no static route (p. 700)"

7.4.21 Services commands

Use these commands to the start and stop the services running on the ESKM appliance and also to halt or reboot the ESKM appliance.

`halt` — halt the ESKM appliance.

Syntax

```
hostname (config)# halt
```

Related command(s)

- “reboot (p. 709)”

`kmip-server startup` — activate KMIP Server when starting up the ESKM appliance.

Syntax

```
hostname (config)# kmip-server startup
```

Related command(s)

- “no kmip-server run (p. 707)”

`kmip-server run` — activate the KMIP Server.

Syntax

```
hostname (config)# kmip-server run
```

Related command(s)

- “no kmip-server run (p. 707)”

`kms-server run` — activate the KMS Server.

Syntax

```
hostname (config)# kms-server run
```

Related command(s)

- “no kms-server run (p. 707)”

`kms-server startup` — activate KMS Server when starting up the ESKM appliance.

Syntax

```
hostname (config)# kms-server startup
```

Related command(s)

- "no kms-server startup (p. 708)"

`no kmip-server run` — halt the KMIP Server.

Syntax

```
hostname (config)# no kmip-server run
```

Related command(s)

- "kmip-server run (p. 706)"

`no kmip-server startup` — disable the KMIP Server when starting up the ESKM appliance.

Syntax

```
hostname (config)# no kmip-server startup
```

Related command(s)

- "kmip-server startup (p. 706)"

`no kms-server run` — halt the KMS Server.

Syntax

```
hostname (config)# no kms-server run
```

Related command(s)

- "kms-server run (p. 706)"

`no kms-server startup` — disable the KMS Server when starting up the ESKM server.

Syntax

```
hostname (config)# no kms-server startup
```

Related command(s)

- “kms-server startup (p. 707)”

`no snmp run` — halt SNMP monitoring.

Syntax

```
hostname (config)# no snmp run
```

Related command(s)

- “snmp run (p. 711)”

`no snmp startup` — disable SNMP when starting up the ESKM server.

Syntax

```
hostname (config)# no snmp startup
```

Related command(s)

- “snmp startup (p. 711)”

`no sshadmin run` — halt SSH administration.

Syntax

```
hostname (config)# no sshadmin run
```

Related command(s)

- “sshadmin run (p. 711)”

`no sshadmin startup` — disable SSH administration when starting up the ESKM server.

Syntax

```
hostname (config)# no sshadmin startup
```

Related command(s)

- "sshadmin startup (p. 711)"

`no webadmin run` — halt web administration.

Syntax

```
hostname (config)# no webadmin run
```

Related command(s)

- "webadmin run (p. 712)"

`no webadmin startup` — disable web administration when starting up the ESKM server.

Syntax

```
hostname (config)# no webadmin startup
```

Related command(s)

- "webadmin startup (p. 712)"

`reboot` — reboot the ESKM appliance.

Syntax

```
hostname (config)# reboot
```

Related command(s)

- "halt (p. 706)"

`show services` — view current and startup service status of the ESKM appliance.

Syntax

```
hostname# show services
Service Group  Service                Status     Startup
kms-server     KMS Server             Started    Enabled
kmip-server    KMIP Server            Started    Enabled
webadmin       Web Administration     Started    Enabled
sshadmin       SSH Administration     Started    Enabled
snmp           SNMP Agent             Stopped    Disabled
```

Related command(s)

- "kmip-server run (p. 706)"
- "kmip-server startup (p. 706)"
- "kms-server run (p. 706)"
- "kms-server startup (p. 707)"
- "no kmip-server run (p. 707)"
- "no kmip-server startup (p. 707)"
- "no kms-server run (p. 707)"
- "no kms-server startup (p. 708)"
- "no snmp startup (p. 708)"
- "no sshadmin run (p. 708)"
- "no webadmin startup (p. 709)"
- "snmp run (p. 711)"
- "snmp startup (p. 711)"
- "sshadmin run (p. 711)"
- "sshadmin startup (p. 711)"
- "webadmin run (p. 712)"

- "webadmin startup (p. 712)"

`snmp run` — activate SNMP.

Syntax

```
hostname (config)# snmp run
```

Related command(s)

- "no snmp run (p. 708)"

`snmp startup` — enable SNMP when starting up the ESKM appliance.

Syntax

```
hostname (config)# snmp startup
```

Related command(s)

- "no snmp startup (p. 708)"

`sshadmin run` — activate SSH administration.

Syntax

```
hostname (config)# sshadmin run
```

Related command(s)

"no sshadmin run (p. 708)"

`sshadmin startup` — enable SSH administration when starting up the ESKM appliance.

Syntax

```
hostname (config)# sshadmin startup
```

Related command(s)

- "no sshadmin startup (p. 709)"

`webadmin run` — activate web administration.

Syntax

```
hostname (config)# webadmin run
```

Related command(s)

- "no webadmin run (p. 709)"

`webadmin startup` — enable web administration when starting up the ESKM appliance.

Syntax

```
hostname (config)# webadmin startup
```

Related command(s)

- "no webadmin startup (p. 709)"

`service start restserver` — start the REST server.

Syntax

```
hostname (config)# service start restserver
```

Related command(s)

- service stop restserver (p. 713)
- service restart restserver (p. 713)

`service stop restserver` — stop the REST server.

Syntax

```
hostname (config)# service stop restserver
```

Related command(s)

- service start restserver (p. 712)
- service restart restserver (p. 713)

`service restart restserver` — restart the REST server.

Syntax

```
hostname (config)# service restart restserver
```

Related command(s)

- service start restserver (p. 712)
- service stop restserver (p. 713)

7.4.22 SNMP commands

Use these commands to configure SNMP on the ESKM appliance.

`community` — add a SNMPv1/v2 community.

Syntax

```
hostname (config)# community
Community Name:
Source IP/subnet mask(s):
Enterprise MIB access [y]:
Standard MIB access [y]:
Successfully added community.
```

Related command(s)

- "show community (p. 719)"
- "no community (p. 718)"
- "edit community (p. 714)"

`edit community` — edit a community.

Syntax

```
hostname (config)# edit community <community name>
Enter your changes to the community public below.
Press enter to keep the current value for a community property.
Community Name [public]:
Community Source IP [192.168.1.40/255.255.255.0,2001::201/64]:
Enterprise MIB Access [y]:
Standard MIB Access [y]:
Successfully modified community.
```

Related command(s)

- "community (p. 714)"
- "show community (p. 719)"
- "no community (p. 718)"

`edit snmp username` — edit an existing SNMPv3 username.

> When you execute the edit snmp username command, the ESKM appliance prompts you to provide the new SNMPv3 username information.

Syntax

```
hostname (config)# edit snmp username <username>
Username [CompanyV3]:
Security Level:
1: noAuth, noPriv
2: auth, noPriv
3: auth, priv
Enter a number (1 - 3) [3]:
Auth Protocol:
1: None
2: MD5
3: SHA
4: SHA-256
5: SHA-384
6: SHA-512
Enter a number (1 - 3) [3]:
Auth Password []:
Priv Protocol:
1: None
2: AES
3: DES
Enter a number (1 - 3) [3]:
Priv Password []:
MIB Access:
Enterprise [y]:
Standard [y]:
```

Related command(s)

- “show snmp username (p. 720)”

- “snmp username (p. 722)”
- “no snmp username (p. 719)”

`edit station` — edit an SNMP management station.

> ⚠ When you execute the edit station command, the ESKM appliance prompts you to provide the new SNMP management station information.

Syntax

```
hostname (config)# edit station <station number>
Manager Type:
1: SNMPv1
2: SNMPv2
3: SNMPv3
Enter a number (1 - 3) [2]:
Trap Type:
1: Trap
2: Inform
Enter a number (1 - 2) [1]:
Hostname or IP [default]:
Port [162]:
Manager Community [company]:
Username [security]:
Security Level:
1: None
2: noAuth, noPriv
3: auth, noPriv
4: auth, priv
Enter a number (1 - 4) [2]:
Auth Protocol:
1: None
2: MD5
3: SHA
4: SHA-256
5: SHA-384
6: SHA-512
Enter a number (1 - 3) [1]:
Auth Password:
```

```
Priv Protocol:
1: None
2: AES
3: DES
Enter a number (1 - 3) [3]:
Priv Password [********]:
Manager Engine ID [4]:
```

Related command(s)

- "show station (p. 720)"
- "station (p. 723)"
- "no station (p. 719)"

`no community` — remove a community from the ESKM appliance's SNMP configuration.

Syntax

```
hostname (config)# no community <community name>
```

Related command(s)

- "community (p. 714)"
- "show community (p. 719)"
- "edit community (p. 714)"

`no snmp username` — delete an existing SNMPv3 username.

Syntax

```
hostname (config)# no snmp username <username>
```

Related command(s)

- “show snmp username (p. 720)”
- “snmp username (p. 722)”
- “edit snmp username (p. 715)”

`no station` — remove an SNMP management station.

Syntax

```
hostname (config)# no station <station number>
```

Related command(s)

- “station (p. 723)”
- “show station (p. 720)”
- “edit station (p. 717)”

`show community` — view either all current communities configured on the ESKM appliance, or detail about a specified community.

Syntax

```
hostname# show community <community name>
```

Related command(s)

- “community (p. 714)”
- “edit community (p. 714)”
- “no community (p. 718)”

`show snmp agent` — display the SNMP agent settings.

Syntax

```
hostname# show snmp agent
```

Related command(s)

- "snmp agent (p. 721)"

`show snmp username` — view the list of existing SNMPv3 usernames.

Syntax

```
hostname# show snmp username <username>
```

Related command(s)

- "snmp username (p. 722)"
- "edit snmp username (p. 715)"
- "no snmp username (p. 719)"

`show station` — view all SNMP management stations.

Syntax

```
hostname# show station <station #>
```

Related command(s)

- "station (p. 723)"
- "no station (p. 719)"
- "edit station (p. 717)"

`snmp agent` — set the SNMP agent settings.

Syntax

```
hostname (config)# snmp agent
Available IP addresses:

All

192.168.200.195

2001:0DB8:AC10:FE01::
SNMP Agent IP [All] (1-2): 1
SNMP Agent port [161]:
Enable SNMP traps [n]:
SNMP agent settings successfully saved.
```

Related command(s)

- "show snmp agent (p. 720)"

`snmp username` — create an SNMPv3 username.

When you execute the snmp username command, the ESKM appliance prompts you to provide the values for the new SNMPv3 username.

Syntax

```
hostname (config)# snmp username
Username:
Security Level:
1: noAuth, noPriv
2: auth, noPriv
3: auth, priv
Enter a number (1 - 3) [3]:
Auth Protocol:
1: None
2: MD5
3: SHA
4: SHA-256
5: SHA-384
6: SHA-512
Enter a number (1 - 3) [2]:
Auth Password []:
Priv Protocol:
1: None
2: AES
3: DES
Enter a number (1 - 3) [2]:
Priv Password []:
MIB Access:
Enterprise [y]:
Standard [y]:
SNMP username successfully saved.
```

Related command(s)

- “edit snmp username (p. 715)”
- “no snmp username (p. 719)”
- “show snmp username (p. 720)”

`station` — add an SNMP management station.

Syntax

```
hostname (config)# station
Manager Type:
1: SNMPv1
2: SNMPv2
3: SNMPv3
Enter a number (1 - 3) [1]:
Trap Type:
1: Trap
2: Inform
Enter a number (1 - 2) [1]:
Hostname or IP:
Port [162]:
Username:
Security Level:
1: None
2: noAuth, noPriv
3: auth, noPriv
4: auth, priv
Enter a number (1 - 4) [1]:
Auth Protocol:
1: None
2: MD5
3: SHA
4: SHA-256
5: SHA-384
6: SHA-512
Enter a number (1 - 3) [1]:
```

```
Auth Password:
Priv Protocol:
1: None
2: AES
3: DES
Enter a number (1 - 3) [2]:
Priv Password:
Manager Engine ID:
SNMP management station successfully saved.
```

Related command(s)

- “no station (p. 719)”
- “edit station (p. 717)”
- “show station (p. 720)”

7.4.23 SSH commands

Use these commands to configure SSH cryptographic parameter.

`no ssh` — < cipher|mac|kex > < priority # of enabled cipher|mac|kex > — disable a cryptographic parameters (cipher/mac/kex).

Syntax

```
hostname (config)# no ssh <crypto param> <enabled crypto param #>
```

For example:

```
no ssh cipher 1
```

Related command(s)

- show ssh <cipher|mac|kex> (p. 725)
- ssh priority <cipher|mac|kex> (p. 726)
- ssh <cipher|mac|kex> <disabled # of cipher|mac|kex> (p. 726)
- ssh restore <cipher|mac|kex> (p. 727)

`show ssh` — .< cipher|mac|kex >— view the priority of all cryptographic parameters (cipher/mac/kex)

Syntax

```
hostname# show ssh <crypto param>
```

For example:

```
show ssh cipher
```

Related command(s)

- ssh <cipher|mac|kex> <disabled # of cipher|mac|kex> (p. 726)
- ssh priority <cipher|mac|kex> (p. 726)
- no ssh <cipher|mac|kex> <priority # of enabled cipher|mac|kex> (p. 725)
- ssh restore <cipher|mac|kex> (p. 727)

`ssh` — < cipher|mac|kex > < disabled # of cipher|mac|kex > — enable a cryptographic parameter (cipher/mac/kex).

Syntax

```
hostname (config)# ssh <disabled crypto param #>
```

For example:

```
ssh cipher 1
```

Related command(s)

- show ssh <cipher|mac|kex> (p. 725)
- ssh priority <cipher|mac|kex> (p. 726)
- no ssh <cipher|mac|kex> <priority # of enabled cipher|mac|kex> (p. 725)
- ssh restore <cipher|mac|kex> (p. 727)

`ssh priority` — < cipher|mac|kex > — prioritize the cryptographic parameter (cipher/mac/kex).

Syntax

```
hostname (config)# ssh priority <crypto param>
```

For example:

```
ssh priority cipher
```

Related command(s)

- show ssh <cipher|mac|kex> (p. 725)
- ssh <cipher|mac|kex> <disabled # cipher|mac|kex> (p. 726)
- no ssh <cipher|mac|kex> <priority # of enabled cipher|mac|kex> (p. 725)
- ssh restore <cipher|mac|kex> (p. 727)

`ssh restore` — < cipher|mac|kex > — restore the cryptographic parameters (cipher/mac/kex) to their default values.

Syntax

```
hostname (config)# ssh restore <crypto param>
```

For example:

```
ssh restore cipher
```

Related command(s)

- show ssh <cipher|mac|kex> (p. 725)
- ssh priority <cipher|mac|kex> (p. 726)
- ssh <cipher|mac|kex> <disabled # of cipher|mac|kex> (p. 726)
- no ssh <cipher|mac|kex> <priority # of enabled cipher|mac|kex> (p. 725)

7.4.24 SSL/TLS commands

Use these commands to configure the SSL/TLS protocol on the KMS and KMIP servers that execute within the ESKM system.

`cipherspec` — enable a cipher suite spec.

The cipher order pertains to the communication channel between the client application and the KMS server. If you do not know the priority of the disabled cipher suite you want to enable, you can use the show cipherspec (p. 727) command to display the cipher suites on the KMS server. For example, show cipherspec kms.

Syntax

```
hostname (config)# cipherspec <disabled cipher #>
```

Related command(s)

- "show cipherspec (p. 735)"
- "cipherspec priority (p. 729)"
- "no cipherspec (p. 732)"
- "restore cipherspec (p. 734)"

`cipherspec priority` — prioritize the cipher suite spec.

> The cipher suite order pertains to the communication channel between the client application and the KMS server.

Syntax

```
hostname (config)# cipherspec priority
CURRENT PRIORITIES
The SSL cipher order is shown below:
Priority   Key Exchange Auth    Cipher     Keysize   Hash
1 Enabled  RSA          RSA     AES256-GCM 256       SHA384
2 Enabled  RSA          RSA     AES128-GCM 128       SHA256
3 Enabled  ECDHE        RSA     AES256-GCM 256       SHA384
4 Enabled  ECDHE        ECDSA   AES256-GCM 256       SHA384
5 Enabled  ECDHE        ECDSA   AES128-GCM 128       SHA256
6 Enabled  RSA          RSA     AES256     256       SHA256
7 Enabled  RSA          RSA     AES128     128       SHA256
8 Enabled  RSA          RSA     AES256     256       SHA-1
9 Enabled  RSA          RSA     AES128     128       SHA-1

NEW PRIORITY CONFIGURATION
Please use the current priority from above to reference each item.
Which item will have priority #1 (1..9):
Which item will have priority #2:
Which item will have priority #3:
Which item will have priority #4:
Which item will have priority #5:
Which item will have priority #6:
Which item will have priority #7:
Which item will have priority #8:
Which item will have priority #9:
KMS SSL cipher order priorities successfully changed.
```

Related command(s)

- "show cipherspec (p. 735)"
- "cipherspec (p. 728)"
- "no cipherspec (p. 732)"
- "restore cipherspec (p. 734)"

`kmip cipherspec` — enable a cipher suite spec.

> ⚠ The cipher order pertains to the communication channel between the client application and the KMIP server.

> ⚠ If you do not know the priority of the disabled cipher suite you want to enable you can use the show cipherspec (p. 727) command to display the cipher suites on the KMIP server. For example: show cipherspec kmip.

Syntax

```
hostname (config)# kmip cipherspec <disabled cipher #>
```

Related command(s)

- "show cipherspec (p. 735)"
- "kmip cipherspec priority (p. 731)"
- "no kmip cipherspec (p. 733)"
- "restore kmip cipherspec (p. 734)"

`kmip cipherspec priority` — prioritize the cipher suite spec.

`The cipher order pertains to the communication channel between the client application and the KMIP server.`

Syntax

```
hostname (config)# kmip cipherspec priority
CURRENT PRIORITIES
The SSL cipher order is shown below:
Priority    Key Exchange Auth    Cipher     Keysize    Hash
1 Enabled   RSA           RSA     AES256-GCM 256        SHA384
2 Enabled   RSA           RSA     AES128-GCM 128        SHA256
3 Enabled   ECDHE         RSA     AES256-GCM 256        SHA384
4 Enabled   ECDHE         ECDSA   AES256-GCM 256        SHA384
5 Enabled   ECDHE         ECDSA   AES128-GCM 128        SHA256
6 Enabled   RSA           RSA     AES256     256        SHA256
7 Enabled   RSA           RSA     AES128     128        SHA256
8 Enabled   RSA           RSA     AES256     256        SHA-1
9 Enabled   RSA           RSA     AES128     128        SHA-1

NEW PRIORITY CONFIGURATION
Please use the current priority from above to reference each item.
Which item will have priority #1 (1..9):
Which item will have priority #2:
Which item will have priority #3:
Which item will have priority #4:
Which item will have priority #5:
Which item will have priority #6:
Which item will have priority #7:
Which item will have priority #8:
Which item will have priority #9:
KMIP SSL cipher order priorities successfully changed.
```

Related command(s)

- "show cipherspec (p. 735)"

- “no kmip cipherspec (p. 733)”
- “restore kmip cipherspec (p. 734)”

`kmip ssl protocol` — enable the use of a particular SSL/TLS protocol on the KMIP server.

Syntax

```
hostname (config)# kmip ssl protocol <protocol>
```

The valid protocols are tls1.0, tls1.1 and tls1.2. For example, you might enter the following command:

```
hostname (config)# kmip ssl protocol tls1.0
```

Related command(s)

“show ssl (p. 735)”
“no kmip ssl protocol (p. 733)”

`no cipherspec` — disable a cipherspec in the KMS server.

> ⚠ If you do not know the priority of the cipher suite you want to disable, you can use the show cipherspec (p. 727) command to display the cipher suites on the KMS server. For example, show cipherspec kms.

Syntax

```
hostname (config)# no cipherspec <priority of enabled cipher>
```

Related command(s)

- “cipherspec priority (p. 729)”
- “cipherspec (p. 728)”
- “restore cipherspec (p. 734)”

`no kmip cipherspec` — disable a cipherspec in the KMIP server.

If you do not know the priority of the cipher suite you want to disable, you can use the show cipherspec (p. 727) command to display the cipher suites on the KMIP server. For example, show cipherspec kmip.

Syntax

```
hostname (config)# kmip cipherspec <priority of enabled cipher>
```

Related command(s)

- “kmip cipherspec (p. 730)”
- “kmip cipherspec priority (p. 731)”
- “restore kmip cipherspec (p. 734)”

`no kmip ssl protocol` — remove the specified protocol from the KMIP server.

Syntax

```
hostname (config)# no kmip ssl protocol <protocol>
```

Related command(s)

- “show ssl (p. 735)”
- “kmip ssl protocol (p. 732)”

`no ssl protocol` — remove the specified protocol from the KMS server.

Syntax

```
hostname (config)# no ssl protocol <protocol>
```

Related command(s)

- “ssl protocol (p. 736)”
- “ssl timeout (p. 736)”
- “show ssl (p. 735)”

`restore cipherspec` — restore the cipherspecs to their default values in the KMS server.

Syntax

```
hostname (config)# restore cipherspec
```

Related command(s)

- "show cipherspec (p. 735)"
- "cipherspec (p. 728)"
- "no cipherspec (p. 732)"
- "cipherspec priority (p. 729)"

`restore kmip cipherspec` — restore the cipherspecs to their default values in the KMIP server.

Syntax

```
hostname (config)# restore kmip cipherspec
```

Related command(s)

- "show cipherspec (p. 735)"
- "kmip cipherspec (p. 730)"
- "kmip cipherspec priority (p. 731)"

`show cipherspec` — view the priority of all ciphers on either the KMS or KMIP server.

Syntax

```
hostname# show cipherspec <server-name>
```

The valid server names are kms and kmip.
For example:
`show cipherspec kms` or `show cipherspec kmip`

Related command(s)

- “cipherspec (p. 728)”
- “no cipherspec (p. 732)”
- “cipherspec priority (p. 729)”
- “restore cipherspec (p. 734)”

`show ssl` — view SSL/TLS settings on either the KMS or KMIP server.

Syntax

```
hostname# show ssl <server-name>
```

The valid server names are kms and kmip.
For example:
`show ssl kms or show ssl kmip`

Related command(s)

- “ssl protocol (p. 727)”
- “kmip ssl protocol (p. 732)”

`ssl protocol` — enable the use of a particular SSL/TLS protocol on the KMS server.

Syntax

```
hostname (config)# ssl protocol <protocol>
```

The valid protocols are ssl3, tls1.0, tls1.1 and tls1.2.

For example, you might enter the following command:

```
hostname (config)# ssl protocol ssl3
```

Related command(s)

- “ssl timeout (p. 736)”
- “no ssl protocol (p. 733)”
- “show ssl (p. 735)”

`ssl timeout` — set the session key timeout for incoming SSL/TLS client connections to the KMS server.

Syntax

```
hostname (config)# ssl timeout <timeout in seconds>
```

⚠ The default value is 7200 seconds (2 hours). Setting this value to zero (0) disables the timeout.

Related command(s)

- “no ssl protocol (p. 733)”
- “show ssl (p. 735)”
- “ssl protocol (p. 727)”

7.4.25 Statistics commands

Use these commands to show license information and also to view connection, throughput, KMS and KMIP server statistics.

`show license usage` — show the number of users currently accessing the ESKM appliance.

Syntax

```
hostname# show license usage
```

```
Server : 1
```

```
KMIP : 2
```

```
KMS : 2
```

```
Custom : 1
```

```
Uncategorized : 1
```

```
Number of Licenses Used : 7
```

Related command(s)

- “show license (p. 751)”

`show statistics` — view statistical information on the operation of the ESKM appliance.

Syntax

```
hostname# show statistics [refresh interval]
```

The refresh interval is an optional parameter to specify how frequently the statistic information should be updated. The default value for the refresh interval is 3 seconds. The value specified from the CLI does not affect the refresh interval on the Management Console. The show statistics command displays the ESKM appliance statistics by default; however, you can also view the Connection Statistics, Throughput Statistics, KMS Server Statistics, and KMIP Server Statistics by pressing 2, 3, 4 or 5 respectively. Press the spacebar to update the statistics immediately. Press the letter “a” to return to the command prompt. Press 1 to return to the System Statistics.

Only the commonly used KMIP operations are displayed.

Related command(s)

None

7.4.26 System commands

Use these commands to manage the ESKM appliance’s system settings.

`clock set` — set the date, time, and time zone for the ESKM appliance.

Syntax

```
hostname (config)# clock set <mm/dd/yy/ hh:mm:ss timezone>
```

See clock set syntax(see table 176) details for further information.

Related command(s)

- "show clock (p. 750)"
- "timezone set (p. 745)"

`edit ras settings` — edit the Remote Administration Settings.

⚠ If you make changes to the remote administration settings via secure shell, you will be logged out of your secure shell client after you have entered all the necessary information.

ℹ IPv6 addresses are supported for Web Admin Server IP and SSH Admin Server IP addresses when IPv6 is enabled on the ESKM appliance, see ipv6 enable (p. 693).

Syntax

```
hostname (config)# edit ras settings
Available IP addresses:
1. All
2. 10.222.178.241
Web Admin Server IP (1-2)[1]:2
Web Admin Server Port [9443]: 9443
Available Server Certificates:
1. [Default]
2. WebCertificate
Web Admin Server Certificate (1-2)[1]:2
Web Admin Client Certificate Authentication (y/n) [n]: n
Available IP addresses:
1. All
2. 10.222.178.241
SSH Admin Server IP (1-2)[1]:2
SSH Admin Server Port [22]:
SSH Admin Maximum Login Attempts [3]: 3
Session Timeout (min) [10]:
```

Related command(s)

- “show ras settings (p. 752)”

`hostname` — define the hostname of the ESKM appliance.

Syntax

```
hostname (config)# hostname <hostname>
```

Related command(s)

- "show hostname (p. 750)"

`no ntp server` — delete an NTP server.

Syntax

```
hostname (config)# no ntp server
```

Related command(s)

- "show ntp (p. 751)"
- "ntp (p. 742)"
- "ntp synchronize (p. 742)"

`ntp` — set the NTP values for the ESKM appliance.

Syntax

```
hostname (config)# ntp
Enable NTP [y]:
NTP Server 1 [None]:
NTP Server 2 [None]:
NTP Server 3 [None]:
Poll Interval (min) [30]:
NTP settings successfully saved
```

Related command(s)

- "show ntp (p. 751)"
- "no ntp server (p. 741)"
- "ntp synchronize (p. 742)"

`ntp synchronize` — immediately synchronize the clock on the ESKM appliance against the NTP server.

Syntax

```
hostname (config)# ntp synchronize
```

Related command(s)

- "show ntp (p. 751)"
- "no ntp server (p. 741)"
- ntp (p. 742)

recreate ssh key — recreate the Secure Shell key.

> ⚠ If you execute the recreate ssh key command from a secure shell client, the ESKM appliance will log you out of your SSH session.

Syntax

```
hostname (config)# recreate ssh key
```

Related command(s)

None

`reissue webadmin certificate` — re-issue the web administration certificate.

> ⚠ This action is performed when initializing the ESKM appliance. The optional duration parameter allows you to specify, in days, the duration that the webadmin certificate is valid.

Syntax

```
hostname (config)# reissue webadmin certificate <duration>
```

Related command(s)

- “show webadmin certificate (p. 752)”

`set webadmin default certificate` — sets the web administration certificate to the default certificate.

Syntax

```
hostname (config)# set webadmin default certificate
```

Related command(s)

- “show webadmin certificate (p. 752)”

`software install` — install new software or a software patch.

⚠ You can specify an IPv6 address for the host when IPv6 is enabled on the ESKM appliance, see ipv6 enable (p. 693), and SCP is used to receive the file.

Syntax

```
hostname (config)# software install
Installation source: SCP
Enter the host:
Enter the filename:
Enter the username:
Enter the password:

Warning: Applying the software upgrade/install may take
a long time and the system will automatically reboot.

Are you sure you want to apply a software upgrade? [n]:
```

Related command(s)

"show software all (p. 752)"
"software rollback (p. 745)"

`software rollback` — roll back one version of the ESKM appliance software.

Syntax

```
hostname (config)# software rollback
```

❗ When this command is executed, key and configuration data are also rolled back; therefore any keys created after the last software update will be deleted. Be sure to backup your keys and configuration data prior to issuing this command.

Related command(s)

- "show software all (p. 752)"
- "software install (p. 744)"

`timezone set` — set the time zone for the ESKM appliance.

Syntax

```
hostname (config)# timezone set <time zone>
```

Related command(s)

"clock set(see table 176)"
show clock (p. 750)

Table 177: clock set syntax details

Parameter	***Description***
mm/dd/yy	*mm*: month: enter value in the range 1 – 12 *dd*: day: enter value in the range 1 – 31 *yy:* year: enter value in 2-digit or 4-digit format

Parameter	***Description***
hh:mm:ss	*hh*: hour: enter value in the range 0 – 23. *mm*: minute: enter value in the range 0 – 59. *ss*: seconds: enter value in the range 0 – 59.

Parameter	***Description***
timezone	▪ SST – Samoa ▪ HST, HDT – Hawaii ▪ HAST, HADT – Aleutian ▪ AKST, AKDT – Alaska ▪ PST, PDT – Pacific ▪ AZST, AZDT – Arizona ▪ MST, MDT – Mountain ▪ CST, CDT – Central ▪ Atlantic – HNA ▪ ISST, ISDT – Indiana Starke ▪ IEST, IEDT – Indiana East ▪ EST, EDT – Eastern ▪ GMT – Greenwich Mean Time ▪ IRISH – Irish (see note below) ▪ BST – British ▪ WET, WEST – Western Europe ▪ CET, CEST – Central Europe ▪ EET, EEST – Eastern Europe ▪ AST – Arabia Standard Time, Saudi Arabia ▪ IST, IDT – Israel ▪ SAST – South Africa ▪ MSK, MSD – Moscow ▪ GST – Gulf Time Zone

Parameter	***Description***
	▪ INDIA – India (see note below) ▪ JAVT, WIB – Western Indonesia ▪ BORT, WITA – Central Indonesia ▪ JAYT, WIT – Eastern Indonesia ▪ JST – Japan ▪ KST – Korea Time Zone ▪ AWST – Australian Western ▪ ACST – Australian Central (Northern Terr.) ▪ ACDT – Australian Central (South Aust.) ▪ AEDT – Australian Eastern (ACT, NSW, Vic.) ▪ AEST – Australian Eastern (Queensland) ▪ NT – Newfoundland Time ▪ BRT, BRST – Brasilia Time, Brasilia Summer Time ▪ AMT, AMST – Amazon Time, Amazon Summer Time, Acre ⚠ The abbreviations for the Irish and India time zones are not standard. Normally, they are IST; however, because IST is also used for the Israel time zone, alternate abbreviations are necessary for the Irish and India time zones to eliminate ambiguity.

7.4.27 System health commands

Use these commands to view the status of the power supply units and cooling fans.

`show system health` — view the status of RAID disks, power supply units and cooling fans on the ESKM appliance.

Syntax

```
hostname (config)# show system health
```

Related command(s)

- "show health check (p. 658)"
- "show kmip-health check (p. 658)"

7.4.28 System information commands

Use these commands to obtain information about the ESKM appliance.

`display fingerprints` — display the fingerprints of SSH host keys and default web administration certificate.

Syntax

```
hostname# display fingerprints
SSH RSA key fingerprint:
2048 SHA256: XxZA5eJaQWZyDpKuTPUW/2LUFEIH/ZzB1Y40IGivonU
SSH ECDSA key fingerprint:
521 SHA256: uAf0tlXh3YY+eEFNaiiaQK9p856Gv6f3X2XMpuVIDCY
SSH ed25519 key fingerprint:
256 SHA256: GvZD+4nCC8htiPMcC6UpM1242GpW19M/3amAhf4/hZk
Webadmin certificate fingerprint (SHA-1):
2048ac:b8:59:ce:99:eb:79:10:4f:3e:d8:96:94:61:75:27:68:d5:e4:fb
```

Related command(s)

- "recreate ssh key (p. 749)"
- "reissue webadmin certificate (p. 749)"

`show clock` — view the current date, time, and time zone reported by the ESKM appliance. The date format is: MM/DD/YYYY. The time format is HH:MM:SS.

Syntax

```
hostname# show clock
```

Related command(s)

- "clock set (p. 749)"

`show copyright` — view the copyright information.

Syntax

```
hostname# show copyright
```

Related command(s)

- "show device (p. 749)"

`show device` — view the Unit ID, hardware platform, software version, HSM information, and software installation date.

Syntax

```
hostname# show device
```

Related command(s)

"show software all (p. 749)"

`show hostname` — view the hostname of the ESKM appliance.

Syntax

```
hostname# show hostname
```

Related command(s)

- "hostname (p. 741)"

`show license` — show the number of users allowed to access the ESKM appliance.

Syntax

```
hostname# show license
Licenses:
```

Related command(s)

- "show license usage (p. 749)"

`show license order information` — order additional client licenses and view cluster information.

Syntax

```
hostname# show license order information
```

Related command(s)

- "show device (p. 749)"

`show ntp` — show the ntp settings for the ESKM appliance.

Syntax

```
hostname# show ntp
Enable NTP:            no
NTP Server 1:          exit
NTP Server 2:          [None]
NTP Server 3:          [None]
Poll Interval (min):   30
```

Related command(s)

- "ntp synchronize (p. 749)"
- "ntp (p. 742)"
- "no ntp server (p. 749)"

`show ras settings` — display the current Remote Administration Settings.

Syntax

```
hostname# show ras settings
Web Admin Server IP: [All]
Web Admin Server Port: 9443
Web Admin Server Certificate: WebCertificate
Web Admin Client Cert Authentication: Disabled
Web Admin Trusted CA List Profile: [None]
SSH Admin Server IP: [All]
SSH Admin Server Port: 22
SSH Admin Server Maximum Login Attempts: 3
Session Timeout (min): 10
```

Related command(s)

"edit ras settings (p. 749)"

`show software all` — view information about the ESKM appliance software.

Syntax

```
hostname# show software all
```

Related command(s)

- "software install (p. 749)"
- "software rollback (p. 749)"

`show webadmin certificate` — view the name of the web administration certificate.

Syntax

```
hostname # show webadmin certificate
```

Related command(s)

- "set webadmin default certificate (p. 749)"

7.4.29 System log commands

The System Log contains a record of all system events, such as: service starts, stops, and restarts; SNMP traps; hardware failures; successful or failed cluster replication and synchronization; failed log transfers; and license errors. Use these commands to view and manage the System Log.

- no system log (p. 662)
- no kmip syslog (p. 681)
- show system log (p. 665)
- show system syslog (p. 683)
- system log rotate (p. 667)
- system syslog (p. 679)
- transfer system log (p. 674)

7.4.30 User commands

Use these commands to view and manage ESKM and KMIP-enabled users.

`edit user` — modify settings for a specified ESKM or a KMIP-enabled user.

Syntax

```
hostname (config)# edit user <user name>
```

```
Password [********]:
```

```
License Type:
```

```
1. Server
```

```
2. KMIP
```

```
3. KMS
```

```
4. Custom
```

```
Enter a number (1-4) [1]:
```

```
User Administration Permission (y/n) [n]:
```

```
Change Password Permission (y/n) [n]:
```

⚠ These additional prompts are present for a KMIP-enabled user.

```
Default KMIP Object Group [default object group]:
Modify Configure Interoperability settings (y/n) [n]:
Map non-existent Object Group to x-Object Group (y/n) [n]:
Modify Client Certificate? (y/n) [n]:
Paste the PEM-encoded client certificate contents here. Do not include
the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines. When
you are done, enter Ctrl-d on a new line:
```

Related command(s)

- “no user (p. 755)”
- “show user (p. 758)”

- “user (p. 761)”

`no user` — delete a user from the user list.

Syntax

```
hostname (config)# no user <username>
```

Related command(s)

- “edit user (p. 754)”
- “show user (p. 758)”
- “user (p. 761)”

`kmip edit user` — convert an ESKM user to a KMIP-enabled user.

Syntax

```
hostname (config)# kmip edit user <username>
Enabling KMIP for user <username>.
KMIP User Group [default user group]:
Default KMIP Object Group [default object group]:
Configure Interoperability settings (y/n) [n]:
Paste the PEM-encoded client certificate contents here. Please include
the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines.
Press return twice when you have finished:
<Enter>
<Enter>
User successfully modified.
```

Related command(s)

- “kmip user (p. 756)”
- “show user detail (p. 759)”

`kmip user` — create a new KMIP-enabled user.

Syntax

```
hostname (config)# kmip user <username>
Password:
Confirm Password:

License Type:

1. Server

2. KMIP

3. KMS

4. Custom

Enter a number (1-4) : 4

User Administration Permission (y/n) [n]:
Change Password Permission (y/n) [n]:
KMIP User Group [default user group]:
Default KMIP Object Group [default object group]:
Configure Interoperability settings (y/n) [n]: y
Paste the PEM-encoded client certificate contents here. Please include
the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines.
Press return twice when you have finished:
```

⚠ Do not paste a client certificate if only password authentication will be used to authenticate the client.

⚠ A username of “detail” is not valid.

Related command(s)

- “edit user (p. 754)”

- “show user (p. 758)”
- “no user (p. 755)”

`show user` — view the properties of an ESKM or KMIP-enabled user, or a list of all users on the ESKM appliance.

Syntax

```
hostname# show user <username>
Username:
User Type:

User Administration Permission:
Change Password Permission:
License Type: Server
Enable KMIP:
Default KMIP Object Group:
Map non-existent Object Group to x-Object Group:
Client Certificate:
Subject:  C=, ST=, L=, O=, CN=
Validity:  Not Before:
Not Valid After:
Date Created:
Date Last Modified:
Last Access Time:
```

> ⚠ The username is an optional parameter, when specified the properties of the specified user are listed. All existing users will be listed if a username is not specified.

> ⚠ Additional properties information is provided for KMIP-enabled users. The interoperability settings appear only if interoperability settings have been configured.

Related command(s)

- "edit user (p. 754)"
- "no user (p. 755)"
- "user (p. 761)"

`show user detail` — view a list of all users on the ESKM appliance. KMIP-enabled users have (KMIP) following their username.

Syntax

```
hostname# show user detail
```

Related command(s)

- "edit user (p. 754)"
- "no user (p. 755)"
- "user (p. 761)"

`show user-memberships` — view the group memberships for a KMIP-enabled user.

Syntax

```
hostname# show user-memberships <username>
Group Memberships for user (<username>):
=====================================
User Group                Target Object Group
=====================================
All Users                 (none)
default user group        default object group
default user group        default user group
```

Related command(s)

- "edit user (p. 754)"
- "no user (p. 755)"
- "user (p. 761)"

`show user-permissions` — view the list of operations that a KMIP-enabled user can perform on the target group. A permission value of true indicates that the KMIP-enabled user can perform this operation on the target group. A permission value of false indicates that the KMIP-enabled user does not have permission to perform this operation on the target group.

Syntax

```
hostname# show user-permissions <username> <targetgroup>
Permissions for user (<username>) for target group
(<targetgroup>):
```

A list of operations and their permission is displayed.

Related command(s)

- "edit user (p. 754)"
- "no user (p. 755)"
- "user (p. 761)"

`user` — create a new ESKM type user.

Syntax

```
hostname (config)# user <user name>

User Type:

1. Local

2. LDAP

Enter a number (1-2) [1]:

Password:

Confirm Password:

License Type:

1. Server

2. KMIP

3. KMS

4. Custom

Enter a number (1-4) :

User Administration Permission (y/n) [n]:

Change Password Permission (y/n) [n]:
```

⚠ The LDAP user type is not currently supported.

⚠ A username of “detail” is not valid.

⚠ A warning message is generated when the number of enrolled users, exceeds the license value.

Related command(s)

- "edit user (p. 754)"
- "no user (p. 755)"
- "show user (p. 758)"

8 Cloud Integration

The ESKM appliance can be integrated with different Cloud Service Providers (CSPs) to use the ESKM keys for various cloud use cases.

Refer *ESKM Cloud Integration User Guide 8.43.0.* for more information.

9 HSM integration

⚠ This section is relevant only to the vESKM and ESKM L2 appliance.

This chapter provides information about:

9.1 HSM features

The vESKM or ESKM L2 appliance can be integrated with the Utimaco CryptoServer LAN Hardware Security Module (HSM) which is a special “trusted” network computer performing a variety of cryptographic operations: key management, key exchange, encryption etc.

- Is built on top of specialized hardware.
- The hardware is well-tested and certified in Utimaco's special laboratories.
- Has a security-focused OS.
- Has limited access via a network interface that is strictly controlled by internal rules.
- Actively hides and protects cryptographic material.

9.2 Using the HSM Web Console

This section guides you through the HSM Web Console’s fundamental elements:

- Global settings (p. 775)
- Refresh tab (p. 777)

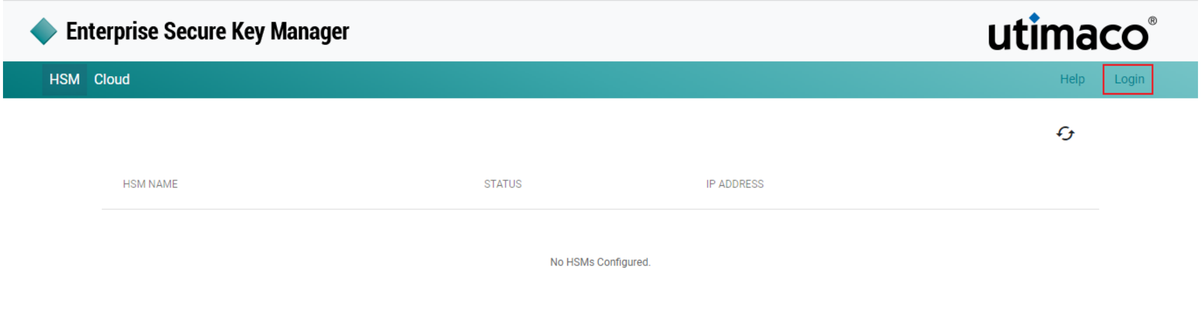
9.2.1 Accessing the HSM Web Console

HSM Web Console can be accessed using the following methods:

- Log in to the ESKM Management Console as an administrator and navigate to **Device > HSM Integration** to access the HSM Web Console.
- Directly access through a web browser: Go to the IP and port using https; for example, https://<ESKM IP>:<port>.

> The port number is the **Port** configured in the **REST Server Settings** section. Default port number is 8443. See REST server procedures (p. 110) and REST server configuration (p. 419).

The following screen appears

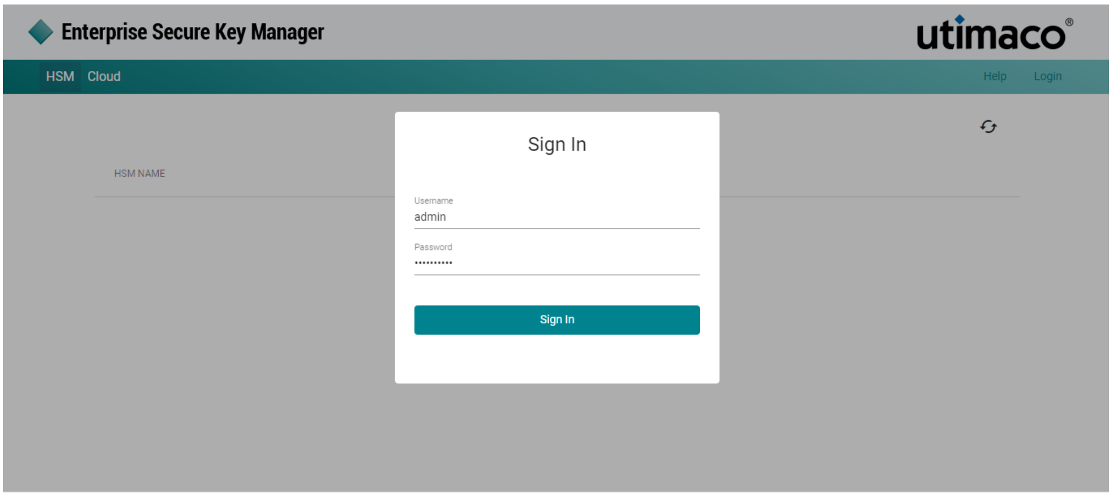


HSM NAME	STATUS	IP ADDRESS

No HSMs Configured.

Figure 229 : HSM Web Console

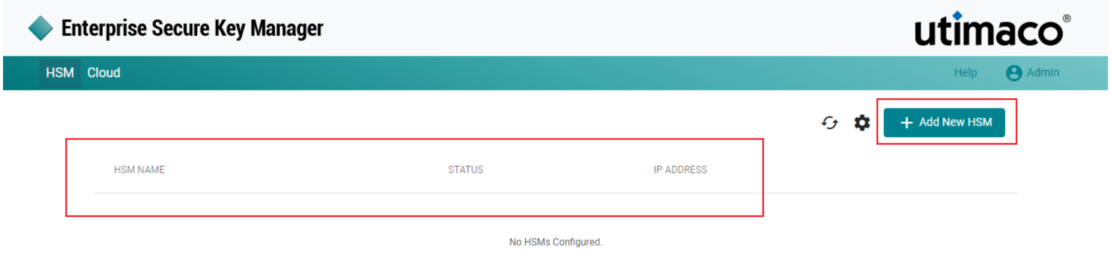
1. Click **Login** at the top right corner of the page.



Username
admin
Password
••••••••••

Figure 230 : Sign In

2. Enter the administrator **Username** and **Password** and click **Sign In**.



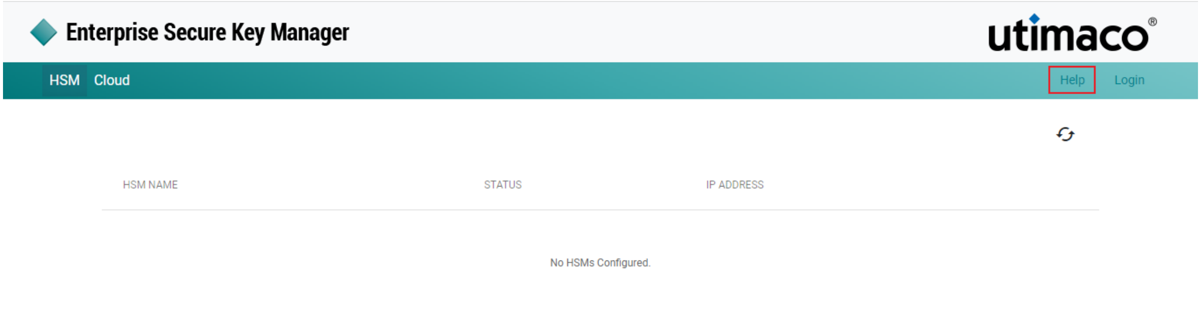
No HSMs Configured.

Figure 231 : HSM Login Status

The HSM Dashboard screen contains **Refresh**, **Global Settings**, and **+ Add New HSM** buttons along with information on the **HSM Name**, **Status**, and **IP Address**.

9.2.2 Accessing the HSM/Cloud Integration help system

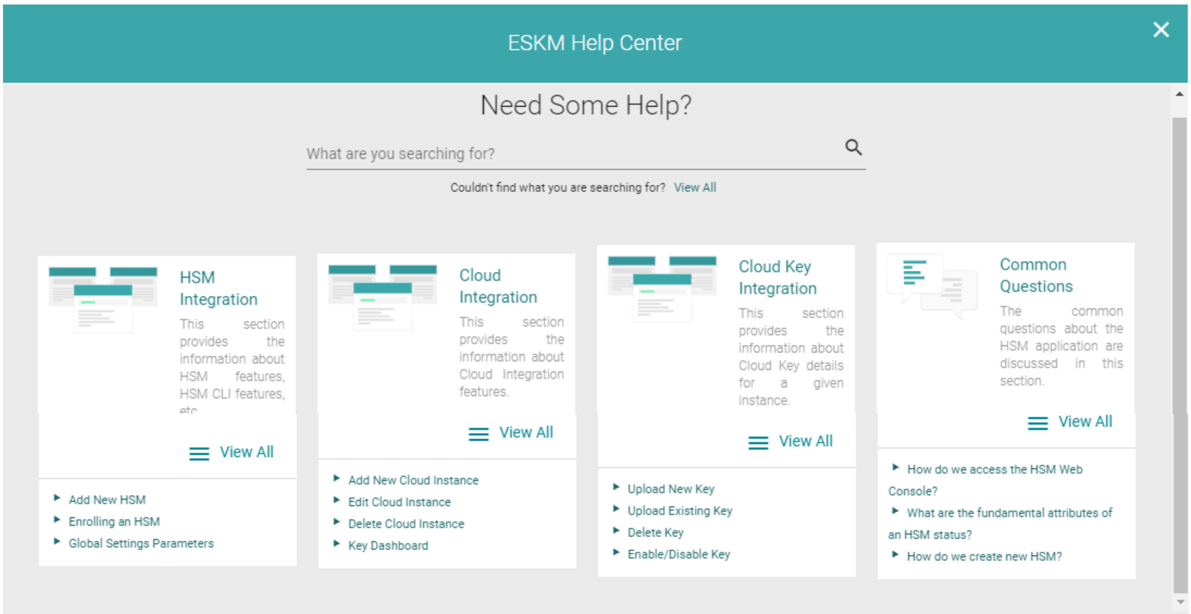
The HSM/Cloud Integration Web Console provides access to product documentation. Clicking the highlighted icon opens the “ESKM Help Center” section in a new window.



HSM NAME	STATUS	IP ADDRESS

No HSMs Configured.

Figure 232 : Locating button to launch HSM help



Need Some Help?

What are you searching for?

Couldn't find what you are searching for? View All

HSM Integration

This section provides the information about HSM features, HSM CLI features, etc.

View All

- Add New HSM
- Enrolling an HSM
- Global Settings Parameters

Cloud Integration

This section provides the information about Cloud Integration features.

View All

- Add New Cloud Instance
- Edit Cloud Instance
- Delete Cloud Instance
- Key Dashboard

Cloud Key Integration

This section provides the information about Cloud Key details for a given instance.

View All

- Upload New Key
- Upload Existing Key
- Delete Key
- Enable/Disable Key

Common Questions

The common questions about the HSM application are discussed in this section.

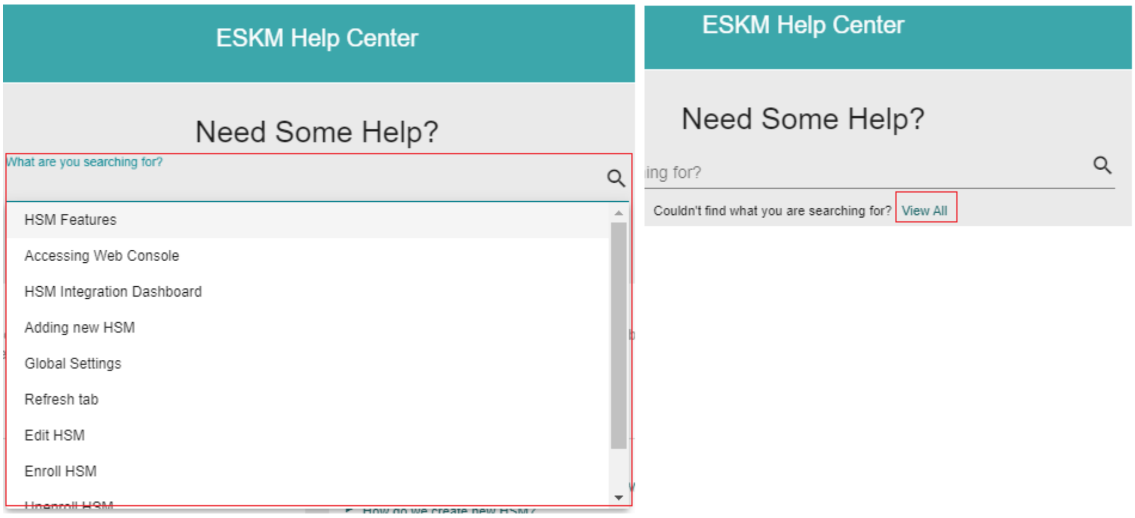
View All

- How do we access the HSM Web Console?
- What are the fundamental attributes of an HSM status?
- How do we create new HSM?

Figure 233 : ESKM Help Center

The "ESKM Help Center" can be utilized in following ways:

- Click on the space under **Need Some Help?** and select the appropriate question from the drop down. Subsequently click on "View All" to view the full list.
- Click on an appropriate question under **HSM Integration/Common Questions**. Subsequently click on "View All" to view the full list.



ESKM Help Center

Need Some Help?

What are you searching for?

- HSM Features
- Accessing Web Console
- HSM Integration Dashboard
- Adding new HSM
- Global Settings
- Refresh tab
- Edit HSM
- Enroll HSM
- Unenroll HSM

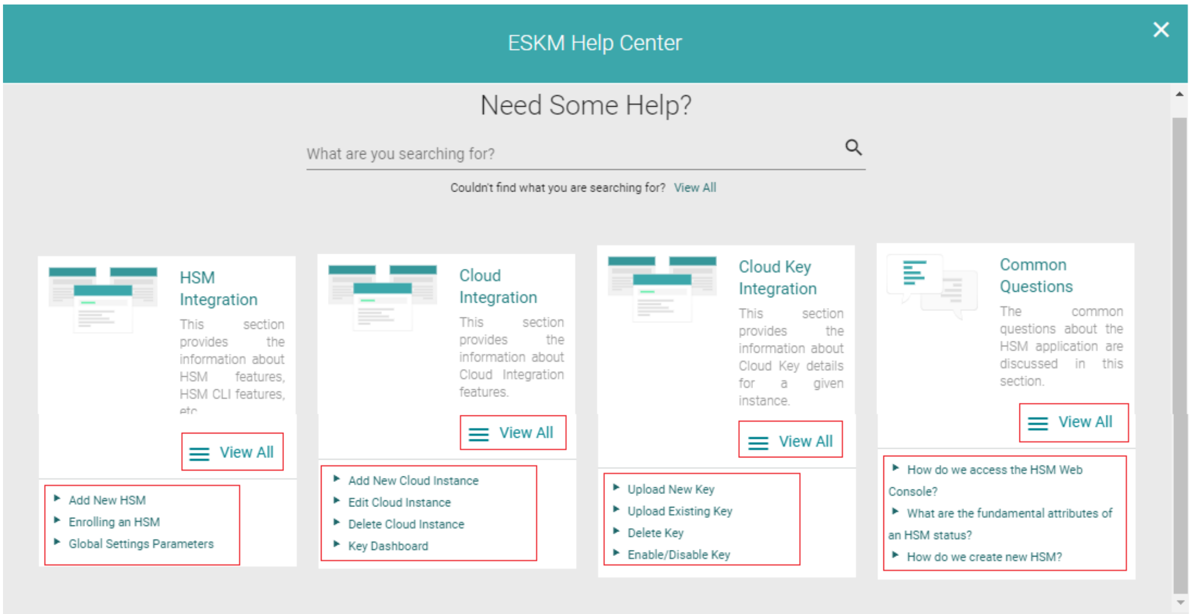
ESKM Help Center

Need Some Help?

ing for?

Couldn't find what you are searching for? View All

Figure 234 : HSM help question list drop down



ESKM Help Center

Need Some Help?

What are you searching for?

Couldn't find what you are searching for? View All

HSM Integration

This section provides the information about HSM features, HSM CLI features, etc

View All

- Add New HSM
- Enrolling an HSM
- Global Settings Parameters

Cloud Integration

This section provides the information about Cloud Integration features.

View All

- Add New Cloud Instance
- Edit Cloud Instance
- Delete Cloud Instance
- Key Dashboard

Cloud Key Integration

This section provides the information about Cloud Key details for a given instance.

View All

- Upload New Key
- Upload Existing Key
- Delete Key
- Enable/Disable Key

Common Questions

The common questions about the HSM application are discussed in this section.

View All

- How do we access the HSM Web Console?
- What are the fundamental attributes of an HSM status?
- How do we create new HSM?

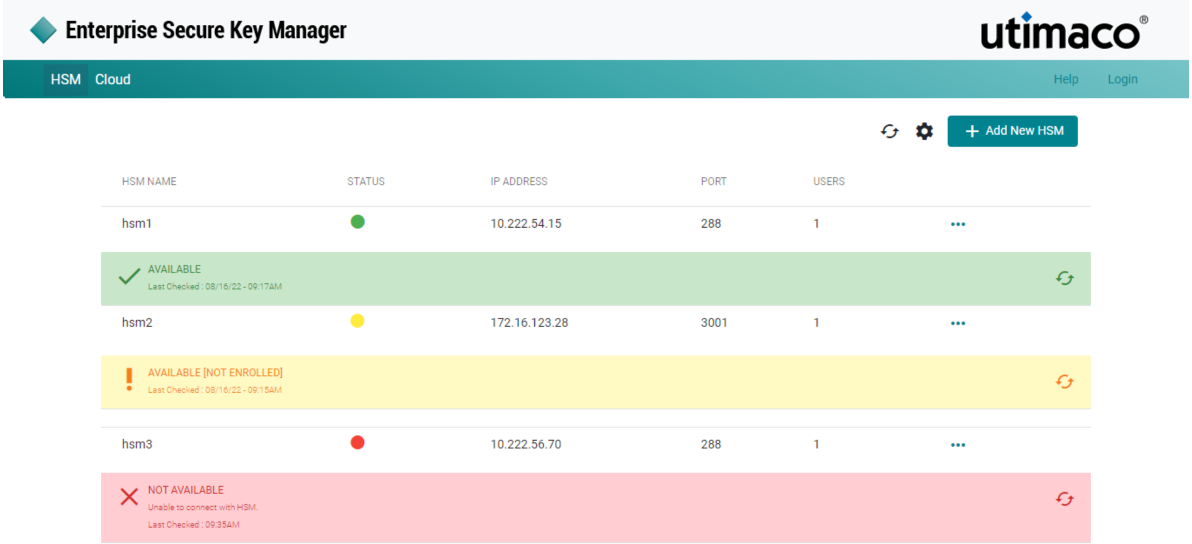
Figure 235 : ESKM Help Center

9.2.3 HSM Status page

After you login, the HSM Status page displays the fundamental information about the HSM. This may contain the following sections:

- HSM name

- Status
- IP Address
- Port
- Users



HSM NAME	STATUS	IP ADDRESS	PORT	USERS
hsm1	●	10.222.54.15	288	1
✓ AVAILABLE Last Checked : 08/16/22 - 09:17AM				
hsm2	●	172.16.123.28	3001	1
! AVAILABLE [NOT ENROLLED] Last Checked : 08/16/22 - 09:15AM				
hsm3	●	10.222.56.70	288	1
✕ NOT AVAILABLE Unable to connect with HSM. Last Checked : 09:35AM				

Figure 236 : HSM Status

The following table describes the components of the **HSM Status** page section.

Table 178: HSM Status page components

Component	***Description***
HSM Name	Displays the name of the new HSM that is added to the list.

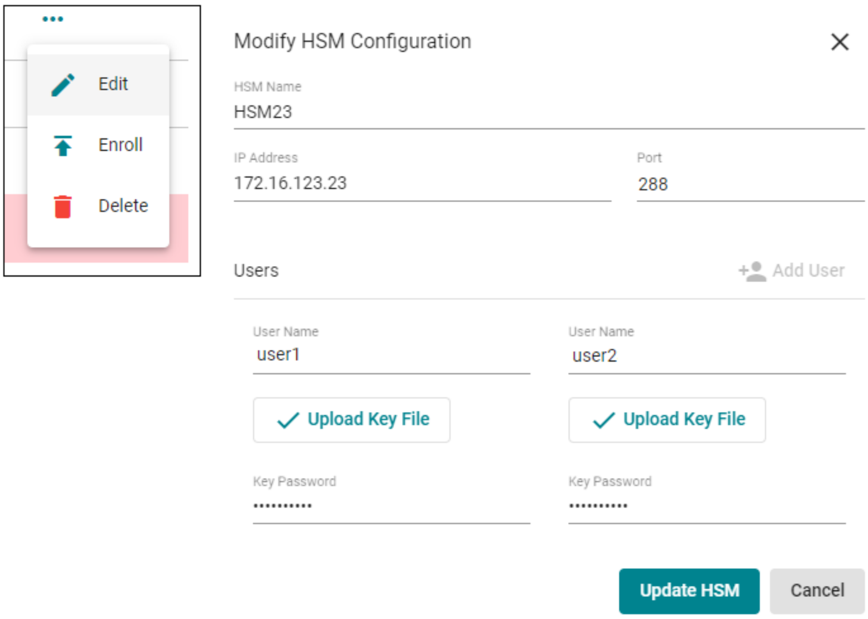
Component	***Description***
Status	Displays the availability of the new HSM configuration. The following color displays their respective status. ▪ **Green**: Available ⚠ An HSM is available and enrolled if it is reachable in the network, and it is possible to login to it using the usernames configured in ESKM. ▪ **Yellow**: Available but not enrolled ⚠ An HSM is available but not enrolled if it is reachable in the network, and it is possible to login to it using the usernames configured in ESKM and is yet to be enrolled. ▪ **Red**: Not available ⚠ An HSM is not available if it is not reachable in the network. ⚠ Click on the refresh icon in the **HSM status message box** to refresh the status of the individual HSM.
IP Address	Displays the IP address of the new HSM configuration.
Port	Displays the port number of the new HSM configuration.
Users	Displays the number of users of the new HSM configuration.

Click on the button "(...)" to get the following options.

- Edit
- Enroll
- Unenroll
- Delete

Edit

Select to get a pop-up window for **Modify HSM Configuration**. Modify the **HSM Name, IP Address, Port,** and **Users** (User Name and Key Password). Click on **Upload Key File** to select the appropriate key file and click on **Update HSM**. Click on **Add User** to add another user by following the same procedure and click on
Update HSM.



HSM Name: HSM23

IP Address: 172.16.123.23

Port: 288

User Name: user1

Key Password: ••••••••••

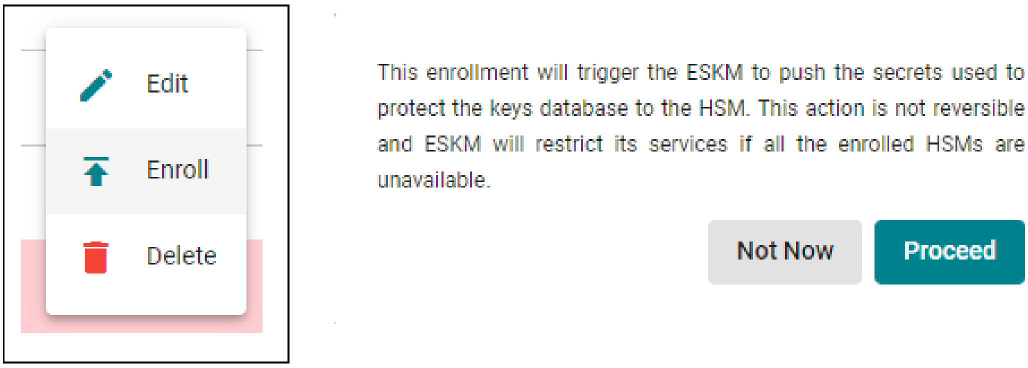
User Name: user2

Key Password: ••••••••••

Figure 237 : Modify HSM Configuration

Enroll

Select to enroll the HSM. A pop-up window will be displayed with a message reading "This enrollment will trigger the ESKM to push the secrets used to protect the keys database to the HSM. This action is not reversible and ESKM will restrict its services if all the enrolled HSMs are unavailable". Click on **Proceed**.



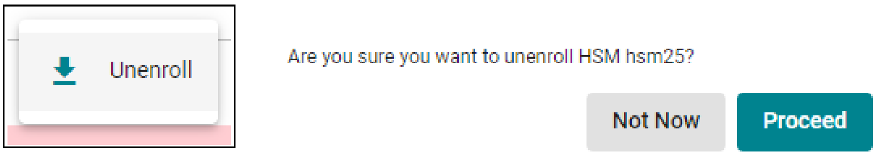
This enrollment will trigger the ESKM to push the secrets used to protect the keys database to the HSM. This action is not reversible and ESKM will restrict its services if all the enrolled HSMs are unavailable.

Figure 238 : Enroll HSM

Post enrollment, ESKM will require HSM to function. If the HSM goes offline for a certain period then the ESKM will stop both KMS and KMIP servers.

Unenroll

Select to unenroll the HSM. A pop-up window will be displayed with a message reading “Are you sure you want to unenroll <hsm name>?”. Click on **Proceed**.

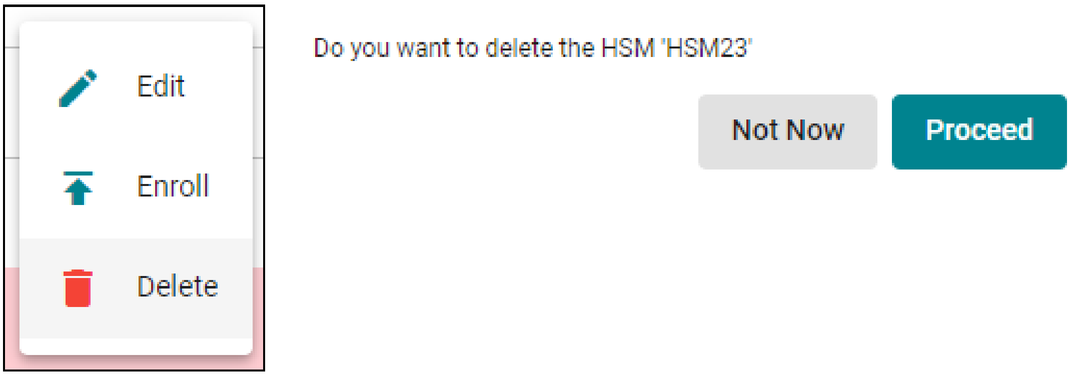


Are you sure you want to unenroll HSM hsm25?

Figure 239 : Unenroll HSM

Delete

Select to delete the HSM configuration from the list. A op-up window will be displayed with a message reading “Do you want to delete the HSM <hsm name>”. Click on **Proceed**.



Do you want to delete the HSM 'HSM23'

Figure 240 : Delete HSM

9.2.4 Adding new HSM

This section desribes the procedure of adding new hsm.

To add new hsm:

1. Login to the HSM Web Console using any one of the methods described in Accessing the HSM Web Console (p. 765).

2. Click on the "+ Add New HSM" icon in the top right corner of the HSM Status page.

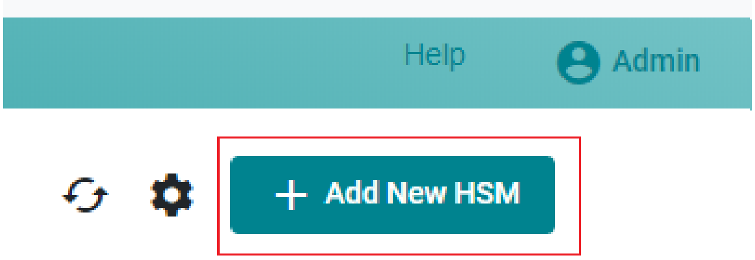
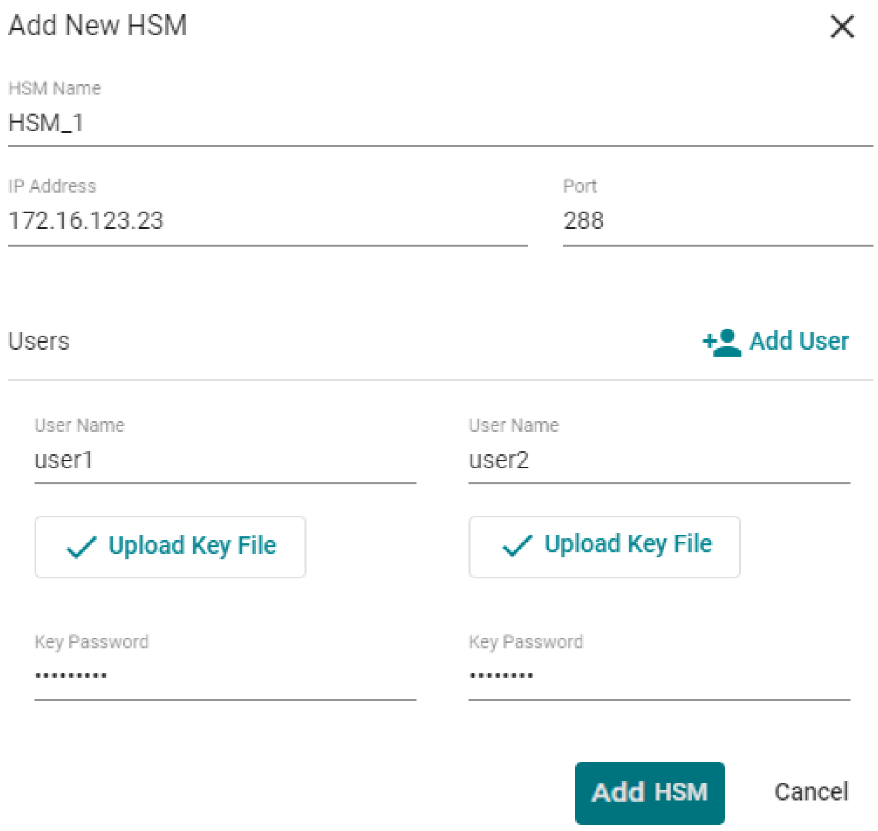


Figure 241 : Add HSM

3. The Add New HSM window will pop up.



Add New HSM

HSM Name
HSM_1

IP Address
172.16.123.23

Port
288

Users

User Name
user1

Key Password
•••••••••

User Name
user2

Key Password
••••••••

Figure 242 : Add New HSM Settings

4. Enter the **HSM Name**, **IP Address**, **Port**, and **Users** (User Name and Key Password). Click on **Upload Key File** to select the appropriate key file and click on **Add HSM**.

5. To add another user, click on **Add User** and enter the User Name and Key Password and select the appropriate key file by clicking on **Upload Key File**. Once done, click on **Add HSM**.

The new HSM is now sucessfully added.

⚠ Please refer to the “CryptoServer” documentation to create the HSM users.

⚠ It is recommended to enroll 2 HSMs for redundancy. An ESKM supports maximum number of 4 HSMs.

⚠ For general purpose HSM, the users added to vESKM for HSM enrollment should have been created with permission **00000002** and for CP5 HSM, with permission **00000022**. If there are two users present, it's sufficient if they have this permission together. Also, the users should be created with attribute "**CXI_GROUP=***"(Access to all groups).

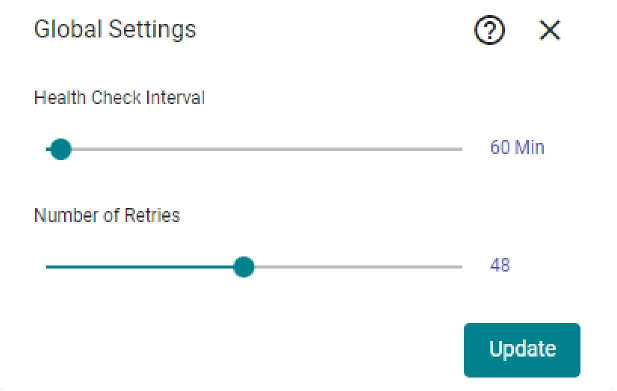
9.2.5 Global settings

This section desribes the procedure of updating the global settings.

To update global settings:

1. Login to the HSM Web Console using any one of the methods described in **Accessing the HSM Web Console** (p. 765).

2. Click on the settings icon in the top right corner of the **HSM Status** page.



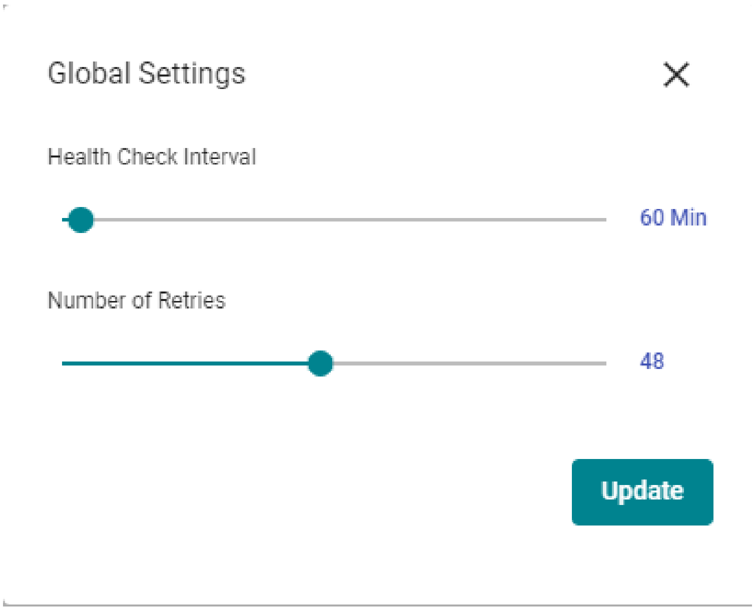
Global Settings

Health Check Interval: 60 Min

Number of Retries: 48

Figure 243 : Global Settings

3. The **Global Settings** window will pop up.



Global Settings

Health Check Interval

60 Min

Number of Retries

48

Figure 244 : Update Global Settings

4. Hold the hand icon on the “green dot” and drag it along the slide bar to set the **Health Check Interval**.
   By selecting the **Health Check Interval** (eg. 60 minutes), the ESKM will check for the HSM availability every 60 minutes.

5. Hold the hand icon on the “green dot” and drag it along the slide bar to set the **Number of Retries**.

   By selecting the **Number of Retries** (eg. 48), the ESKM will continue to try for 48 times to check for the availability of HSM.
   If HSM is still not available, ESKM will stop the key management and web administration services. Post stopping the services, ESKM will continue to check for the availability of HSM once again every 5
   minutes (irrespective of previously selected **Health Check Interval**). Once the HSM is available, ESKM restarts the key management and web administration services.

6. Click **Update**. The latest selections are now updated.

9.2.6 Refresh tab

Click on the refresh icon to refresh the status of the "HSM Integration Dashboard"

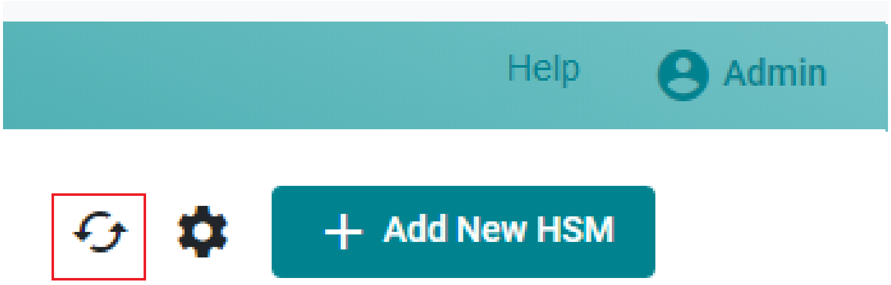


Figure 245 : Refresh tab

9.3 SNMP Traps associated with HSM

The following list describes the scenarios where SNMP traps are being sent.

1. **Unable to connect with HSM:** This trap is sent when the connection to the enrolled HSM is failed. This can happen if:
    - Due to a network issue.
    - HSM connection parameters are changed.
    - HSM is offline.

2. **Failed to authenticate with HSM**: This trap is sent when the login to the enrolled HSM is failed after connecting to the HSM. This can happen if the configured user credentials are changed in the enrolled HSM.

3. **Unable to find the ESKM secrets in the HSM**: This trap is sent when the created ESKM secrets are not found in the enrolled HSM. This can happen if the ESKM secrets are deleted from HSM externally.

4. **Integrity check failed for the ESKM secrets stored in the HSM**: This trap is sent when the created ESKM secrets get changed in the enrolled HSM. This can happen if the ESKM secrets are changed from HSM externally.

5. **HSM health check retry attempts have reached their maximum value**: This trap is sent when HSM health check retry attempts have reached their maximum configured value. Failed to connect with configured HSMs: This trap is sent when all the enrolled HSMs are offline.

6. **Failed to connect with configured HSMs**: This trap is sent when all the enrolled HSMs are offline.

7. **HSM is back online**: This trap is sent when any of the enrolled HSM is back online after all the HSMs have gone offline.

9.4 HSM CLI commands

Below is an alphabetical listing all of the HSM CLI commands.

- show hsm settings (p. 779)
- edit hsm settings (p. 780)
- hsm add (p. 781)
- hsm status (p. 782)
- hsm delete (p. 783)
- hsm enroll (p. 784)
- hsm unenroll (p. 785)
- hsm mode cp5 (p. 786)
- hsm mode gp (p. 787)

`show hsm settings` — view the settings of the hsm

Syntax

```
hostname (config)# show hsm settings
Health Check Interval(min):     60
Number of Retries:              48
```

Related command(s)

- edit hsm settings (p. 780)
- hsm add (p. 781)
- hsm status (p. 782)
- hsm delete (p. 783)
- hsm enroll (p. 784)
- hsm unenroll (p. 785)

`edit hsm settings` — edit the hsm settings

Syntax

```
hostname (config)# edit hsm settings
Enter HSM Health Check Interval(min) [60]: 23
Enter the Number of Retries [48]: 45
Successfully changed Global HSM Settings.
```

Related command(s)

- show hsm settings (p. 779)
- hsm add (p. 781)
- hsm status (p. 782)
- hsm delete (p. 783)
- hsm enroll (p. 784)
- hsm unenroll (p. 785)

`hsm add` — add a new hsm to the list

Syntax

```
hostname (config)# hsm add <name>
Enter HSM IP: 172.16.123.26
Enter HSM port: 3001
Enter Number of HSM Users: 2
User #1: user1
Key #1: (Press Enter key and Ctrl+D to finish)
Key Password #1:
User #2: user2
Key #2: (Press Enter key and Ctrl+D to finish)
Key Password #2:
HSM NewTrial01 added
```

Related command(s)

- show hsm settings (p. 779)
- edit hsm settings (p. 780)
- hsm status (p. 782)
- hsm delete (p. 783)
- hsm enroll (p. 784)
- hsm unenroll (p. 785)

`hsm status` — display the information associated with hsm

Syntax

```
hostname (config)# hsm status <name>
HSM Name:           NewTrial01
IP:                 172.16.123.26
Port:               3001
Number of Users:    2
Enrolled:           Yes
The HSM is Available.
```

```
hostname (config)# hsm status
HSM Name    Enrolled    Available    Last Status Check

hsm1        No          Yes          06/21/2020 06:46:01
hsm2        No          Yes          06/21/2020 06:48:14
```

Related command(s)

- show hsm settings (p. 779)
- edit hsm settings (p. 780)
- hsm add (p. 781)
- hsm delete (p. 783)
- hsm enroll (p. 784)
- hsm unenroll (p. 785)

`hsm delete` — delete the added hsm from the list

Syntax

```
hostname (config)# hsm delete <name>
HSM deleted succcessfully.
```

Related command(s)

- show hsm settings (p. 779)
- edit hsm settings (p. 780)
- hsm add (p. 781)
- hsm status (p. 782)
- hsm enroll (p. 784)
- hsm unenroll (p. 785)

`hsm enroll` — enroll the hsm

Syntax

```
hostname (config)# hsm enroll <name>
Are you sure you want to enroll this HSM? [n]: y
HSM enrollment was successful.
```

```
hostname (config)# hsm enroll <name>
This enrollment will trigger the ESKM to push the secrets used to
protect the keys database to the HSM. This action is not reversible and
ESKM will restrict its services if all the enrolled HSMs are unavailable.
Please type "enroll" to initiate enroll or "q" to quit.
```

```
enroll
HSM enrollment was successful.
```

Related command(s)

- show hsm settings (p. 779)
- edit hsm settings (p. 780)
- hsm add (p. 781)
- hsm status (p. 782)
- hsm delete (p. 783)
- hsm unenroll (p. 785)

`hsm unenroll` — unenroll the hsm

Syntax

```
hostname (config)# hsm unenroll <name>
Are you sure you want to uenroll this HSM? [n]: y
HSM unenrollment was successful.
```

```
hostname (config)# hsm unenroll <name>
Are you sure you want to uenroll this HSM? [n]: y
Error: HSM unenrollment failed: NewTrial01 is not available.
Would you like to delete the HSM? [n]: y
Deleting the HSM without unenrolling will leave the ESKM secrets stored
on the HSM. Are you sure you want to delete the HSM ? [n]: y
HSM deleted successfully.
```

Related command(s)

- show hsm settings (p. 779)
- edit hsm settings (p. 780)
- hsm add (p. 781)
- hsm status (p. 782)
- hsm delete (p. 783)
- hsm enroll (p. 784)

`hsm mode cp5` — switching to cp5 HSM mode

Syntax

```
hostname (config)# hsm mode cp5
Would you like to switch to CP5 mode? [n]: y
Successfully switched HSM mode to CP5.
```

Related command(s)

- show hsm settings (p. 779)
- edit hsm settings (p. 780)
- hsm add (p. 781)
- hsm status (p. 782)
- hsm delete (p. 783)
- hsm enroll (p. 784)
- hsm unenroll (p. 785)
- hsm mode gp (p. 787)

`hsm mode gp` — switching to gp HSM mode

Syntax

```
hostname (config)# hsm mode gp
Would you like to switch to GP mode? [n]: y
Successfully switched HSM mode to GP.
```

Related command(s)

- show hsm settings (p. 779)
- edit hsm settings (p. 780)
- hsm add (p. 781)
- hsm status (p. 782)
- hsm delete (p. 783)
- hsm enroll (p. 784)
- hsm unenroll (p. 785)
- hsm mode cp5 (p. 786)

10 Embedded HSM

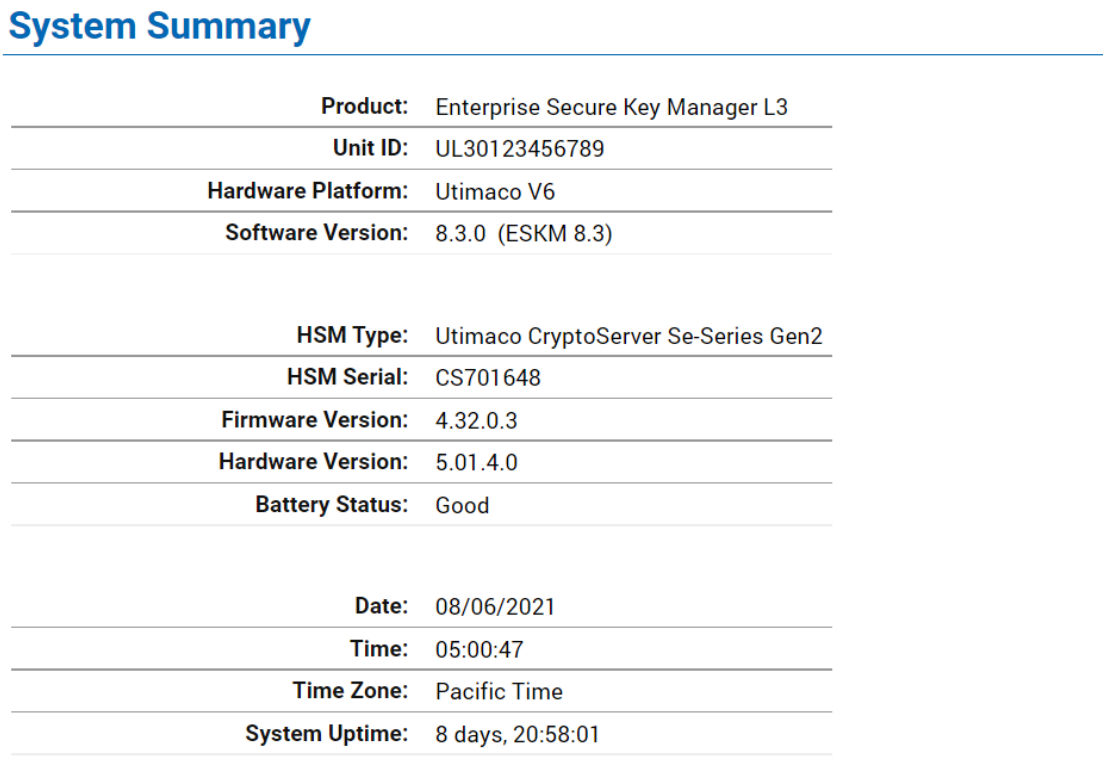
⚠ This section is relevant only to the “Enterprise Secure Key Manager L3 and L4”.

10.1 Embedded HSM features

The ESKM L3 and L4 appliances embed and are integrated with the Utimaco CryptoServer PCIe Hardware Security Module which is capable of resisting both physical and logical attacks and contains special hardware for cryptographic operations and key protection. The Utimaco SecurityServer supports the industry standard interfaces PKCS #11, Microsoft CSP/CNG/SQLEKM and JCE interfaces. It can be used for the most common business applications, such as:

- Public Key Infrastructure (PKI)
- Document Signing
- Code Signing
- Key Injection for securing devices in the IoT
- Database Encryption

The Utimaco's PCIe embedded HSM card is only available on ESKM L3 and L4 appliances.



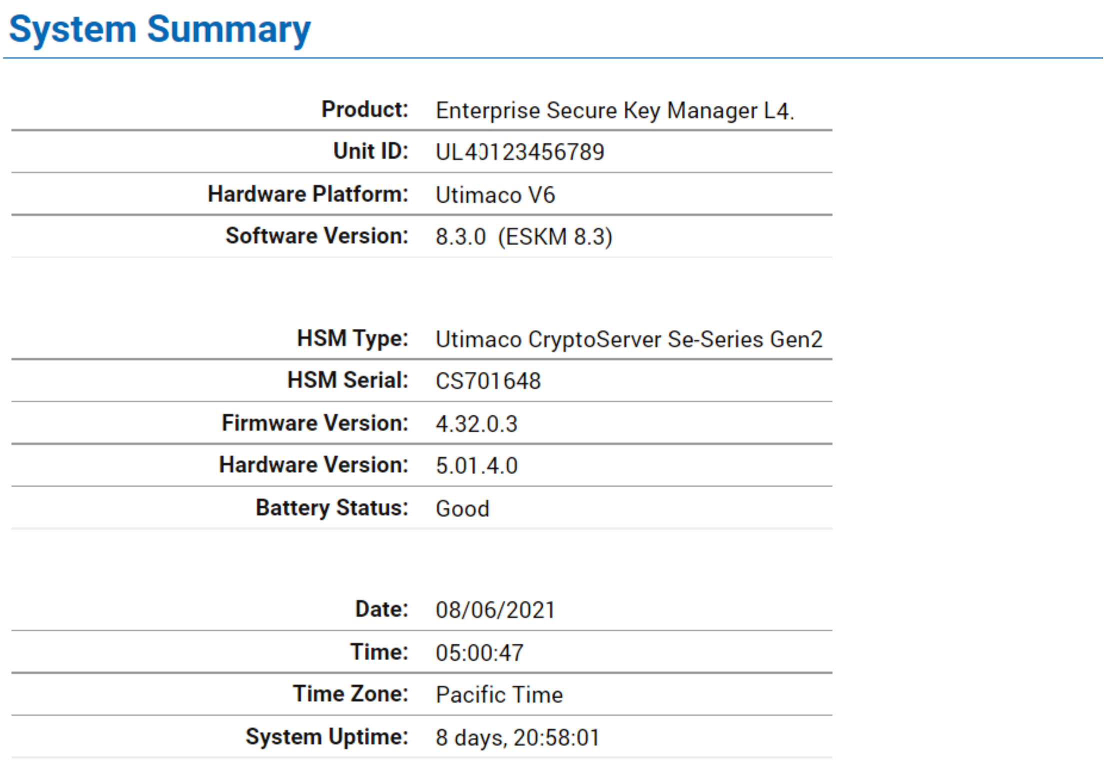
System Summary

Product:	Enterprise Secure Key Manager L3
Unit ID:	UL30123456789
Hardware Platform:	Utimaco V6
Software Version:	8.3.0 (ESKM 8.3)

HSM Type:	Utimaco CryptoServer Se-Series Gen2
HSM Serial:	CS701648
Firmware Version:	4.32.0.3
Hardware Version:	5.01.4.0
Battery Status:	Good

Date:	08/06/2021
Time:	05:00:47
Time Zone:	Pacific Time
System Uptime:	8 days, 20:58:01

Figure 246 : ESKM L3



System Summary

Product:	Enterprise Secure Key Manager L4.
Unit ID:	UL40123456789
Hardware Platform:	Utimaco V6
Software Version:	8.3.0 (ESKM 8.3)
HSM Type:	Utimaco CryptoServer Se-Series Gen2
HSM Serial:	CS701648
Firmware Version:	4.32.0.3
Hardware Version:	5.01.4.0
Battery Status:	Good
Date:	08/06/2021
Time:	05:00:47
Time Zone:	Pacific Time
System Uptime:	8 days, 20:58:01

Figure 247 : ESKM L4

⚠ Every hour, ESKM will perform a health check for the embedded HSM, with a maximum health check time out of 48 hours. In the event of a health check failure, ESKM will send SNMP traps. The ESKM services will be stopped if the HSM card fails after this full timeout or on reboot. As a result, SNMP traps should be configured to detect embedded HSM failure.

10.2 Embedded HSM CLI commands

The following table is an alphabetical listing all of the HSM CLI commands.

- show hsm state (p. 791)
- show hsm mbk (p. 791)
- show hsm firmware (p. 792)

`show hsm state` — view the state of the hsm

Syntax

```
hostname (config)# show hsm state
mode      = Operational Mode
state     = INITIALIZED (0x00140004)
FIPS mode = ON
temp      = 31.6 [C]
alarm     = OFF
bl_ver    = 5.01.0.5 (Model: Se-Series Gen2)
hw_ver    = 5.01.4.0
uid       = 3c00001b b0b6ba01 |<               |
adm1      = 53653132 20202020 43533730 31363438 |Se12    CS701648|
adm2      = 53656375 72697479 53657276 65722020 |SecurityServer|
adm3      = 494e5354 414c4c45 44202020 20202020 |INSTALLED|
```

Related command(s)

- show hsm mbk (p. 791)
- show hsm firmware (p. 792)

`show hsm mbk` — view the mbk of the hsm

Syntax

```
hostname (config)# show hsm mbk
slot name     len algo type   k  generation date     key check value

3    ESKM_MBK 32   AES   XOR    2  2000/06/07 04:30:01
4AD11EFC113303A5:FB715D38B
0D91C02
```

Related command(s)

- show hsm state (p. 791)
- show hsm firmware (p. 792)

`show hsm firmware` — view the firmware of the hsm

Syntax

```
hostname (config)# show hsm firmware
ID name         type version        initialization level

0 SMOS         C64  5.6.3.90       INIT_OK
1 FIPS140      C64  5.1.0.9        INIT_OK
4 POST         C64  1.0.2.0        INIT_OK
a HCE          C64  2.3.0.2        INIT_INACTIVE
d EXAR         C64  2.2.1.2        INIT_INACTIVE
68 CXI          C64  2.4.3.2        INIT_OK
81 VDES         C64  1.0.10.0       INIT_OK
83 CMDS         C64  3.6.5.0        INIT_OK
84 VRSA         C64  1.3.7.0        INIT_OK
86 UTIL         C64  3.0.6.1        INIT_OK
87 ADM          C64  3.0.27.2       INIT_OK
88 DB           C64  1.3.2.5        INIT_OK
89 HASH         C64  1.0.13.0       INIT_OK
8b AES          C64  1.4.2.0        INIT_OK
8d DSA          C64  1.2.5.0        INIT_OK
8e LNA          C64  1.2.4.7        INIT_OK
8f ECA          C64  1.1.14.2       INIT_OK
91 ASN1         C64  1.0.3.9        INIT_OK
96 MBK          C64  2.4.1.0        INIT_OK
9a NTP          C64  1.2.1.1        INIT_OK
9c ECDSA        C64  1.1.22.0       INIT_OK
```

Related command(s)

- show hsm state (p. 791)
- show hsm mbk (p. 791)

11 Appendix A ESKM information sheet

This information is specific to the ESKM appliance to which it is attached. There is one data sheet per ESKM appliance. See figure below for item locations.

Keep this information in a secure location, for access by the Security Officer(s) only. It is needed for the successful installation and management of this ESKM appliance.

Date installed
Completed by (installer)
Product ID number (PID)
Serial Number / Unit ID
Tamper label ID
Key left (tag serial number)
Key right (tag serial number)

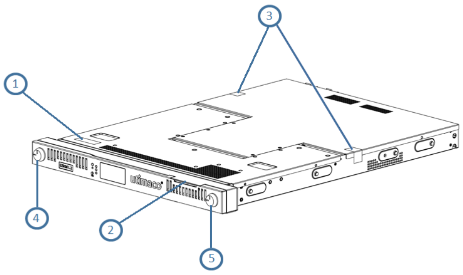


Figure 248 : Front and top of ESKM appliance

Item	***Description***
1	**Model Number** and **Product Number Label** of the ESKM appliance. ⚠ When ordering a replacement appliance, use this information.
2	**Serial Number**/**Unit ID** of the ESKM appliance
3	Tamper-evident labels on the top of the ESKM appliance, **Label ID**
4	Left-most bezel lock as you face front of the ESKM appliance, **Key left**
5	Right-most bezel lock as you face the front of the ESKM appliance, **Key right**

❗ The tamper-evident label has a unique serial number. Upon receipt of the ESKM appliance, customers are advised to visually inspect the tamper label to ensure it has not been tampered with. If the label shows evidence of a tamper, the Security Officer should assume that the ESKM has been compromised and contact Utimaco Technical Support (p. 798).

12 Appendix B Troubleshooting

This appendix addresses some of the typical problems you might face as the administrator of the ESKM appliance.

Table 179: Common problems

Problem	***Possible solution***
Unable to connect to the Management Console	▪ Ensure that the browser version you're using supports TLS 1.1 and above. ▪ Ensure that the URL you are using to connect to the ESKM appliance begins with "HTTPS" (not simply "HTTP") and that the port number is correct. The default web administration port is 9443.
Unable to log into the Management Console	▪ Ensure that cookies are enabled on the browser. ▪ Ensure that the user account was granted the "Web Admin Access" privilege. ▪ Ensure that the "Web Administration" service is running.
Unable to log in via SSH	▪ Ensure that the user account was granted the "SSH Admin Access" privilege. ▪ Ensure that the "SSH Administration" service is running.

Problem	***Possible solution***
Unable to connect to the console	▪ Check the serial terminal emulation application and configure with the following settings: 9600 baud rate, 8N1 (8 data bits, no parity, 1 stop bit), and hardware flow control enabled. ⚠ This solution is not relevant to “virtual appliance”.
Unable to ping the device	▪ Check the network connection on the ESKM appliance. The initial setup procedure configures NIC1.
System reset to the factory settings	▪ The ESKM appliance detected severe disk corruption that could not be repaired. The configuration should be restored from a backup.
Lost the “admin” account password and no other users exist.	Contact Utimaco Technical Support (p. 798).
Unable to create certificate	▪ Ensure that the Country Name is the two letter country code. For example, the country code for the United States is the two letters “US”.

13 Appendix C Technical Support

13.1 Utimaco Technical Support

For technical questions, contact Utimaco Technical Support:

- E-mail: support@utimaco.com[6]
- Telephone: 800-500-7858 (U.S.A.) +1-916-414-0216 (International)
- Website: https://support.utimaco.com/

Before contacting Utimaco with your questions, collect the following information:

- Product model names and numbers
- Technical support registration number or NonStop system number (if applicable)
- Service Agreement ID number (SAID)
- Product serial numbers
- Error messages
- Software version number

13.1.1 24-hour support

24-hour emergency support is available to those customers who have valid service contracts. Use this service for product and system emergencies that occur after normal working hours or on weekends and U.S. holidays. Questions about product installation and setup are supported during normal working hours.

For 24-hour emergency support call: 800-500-7858 (U.S.A.) +1-916-414-0216 (International)

[6] mailto:support@utimaco.com

14 Appendix D Glossary

administrator (admin)	The person or people who configure, use, or manage the Enterprise Secure Key Manager (ESKM) system. The admin may or may not be the SO (see **SO**, below).
authorization policy	The criteria for granting or denying access to a resource, based on the user's identity. This usually follows authentication.
CA	**Certificate Authority**. A trusted third-party organization, company, or other entity that issues digital certificates used to authenticate digital signatures and public-private key pairs. The role of the CA in this process is to assure that the party granted the unique certificate is, in fact, who they claim to be and possess the private key corresponding to the party's public key.
CLI	**Command Line Interface**. Similar to the ESKM Web Management Console, the CLI interface can be used to configure or manage the ESKM system.
client	In this document, a client can also be referred to as a "user" — the machine that communicates with the ESKM to perform key operations. See **user**, below.

cluster	Two or more ESKM appliances may be linked together in a system, or cluster. Clustering enables multiple ESKM appliances in a distributed environment to synchronize and continuously replicate configuration information and new client keys to other ESKM appliances in the cluster, thus providing continuous availability to clients and reducing administration.
DNS	**Domain Name System**. A mnemonic naming system for computers, services, or any resource connected to a network, saving people from having to memorize IP addresses. For example, the DNS name **www.example.com** is much easier to remember than memorizing the IPv4 address 192.0.43.10.
ESKM	**Enterprise Secure Key Manager.** The complete system that provides cryptographic key generation, secure storage, retrieval, and other services to devices and applications performing encryption or digital signatures.
failover	The process in which client users of a service shift from the primary resource to a secondary or alternate resource when the primary is not accessible.
FIPS	**Federal Information Processing Standard**.In this document, "FIPS[7]" often refers to FIPS 140-2 Standard, "Security Requirements for Cryptographic Modules". The ESKM as a whole may be operated in FIPS mode as a cryptographic module. ESKM appliance can be referred to as

[7] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

	having an embedded HSM, which is FIPS 140-2 Level 3 certified.
FIPS Certificate	FIPS 140-2-validated cryptographic modules receive a certificate and certificate number. Validated modules are listed with their certificates and security policies at the NIST[8]website.
group	When organizing the data in an ESKM, establishing groups simplifies management of users (or clients) and their access to their associated objects.
GUI	**Graphical User Interface.** In this document, the GUI is also called the Management Console. This interface is accessible via browser using the following format: `https://<IP address of the ESKM appliance>:<port number of the GUI; the default is 9443>`
HSM	**Hardware Security Module**. A physical computing Appliance that safeguards and manages digital keys for strong authentication and provides crypto processing. The ESKM - Level 3 appliance has an embedded HSM, which meet FIPS 140-2 Level 3 criteria.
key	A string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.
KMIP	**Key Management Interoperability Protocol**. A communication protocol that defines message formats for the manipulation of

[8] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

	cryptographic keys on a key management server. See the OASIS websites for more information on the KMIP specification, usage guides and profile, at https://www.oasis-open.org/standards[9]
KMIP key	The key that is generated or managed by the ESKM using the KMIP protocol.
KMS	**Key Management Service**. The KMS server is the software component of the ESKM appliance that manages communications with client and provides the client key generation, storage, and retrieval using XML protocol.
KMS key	The key that is generated or managed by the ESKM using the ESKM XML protocol.
LDAP	**Lightweight Directory Access Protocol** is an Internet standard for storing, retrieving, and managing directory data. LDAP provides the mechanism for search capabilities and authentication.
Management Console	The GUI for admins to configure, manage, and use the ESKM appliance. Most of the functions required to use the ESKM can be performed using the Management Console.
MIB	**Management Information Base**. A database used for managing the entities in a communication network. The database is hierarchical (tree-structured) and each entry is addressed through an object identifier (OID).

[9] http://www.oasis-open.org/standards

NIST	National Institute of Standards and Technology. Organization that maintains the FIPS security and other standards, the SP 800 series security publications, and the CMVP and CAVP validation programs.
NMS	Network Management System. A set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.
node	In the context of this product, a node is an ESKM appliance in a cluster.
NTP	Network Time Protocol is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
object	An object can refer a key, a CA, or a certificate.
OID	Object Identifier. A term used to name an object (a key, CA, or certificate).
primary device	A designated device that, when up and running, is “preferred”; it is the first device accessed by the user.
RSA	A public-key encryption algorithm first made public by Rivest, Shamir, and Adleman in 1978, now widely used for encryption and digital signatures. “RSA key” may refer to the public key, the corresponding private key, or the combined public-private key pair.

secondary device	A designated device that is passive or not preferred. If the primary device becomes inaccessible, the secondary becomes the active device until the primary is backed up.
SSL	**Secure Socket Layer**. The predecessor to **TLS**.
SO	The person or people who configure, use, or manage the Enterprise Secure Key Manager (ESKM) system. The admin may or may not be the SO (see **SO**, below).
SNMP	**Simple Network Management Protocol**. This protocol is used by network management systems to monitor network-connected devices for conditions that warrant administrator attention.
SP 800	Special Publications, 800-series[10]. NIST's primary mode of publishing computer, cyber, and information security guidelines, recommendations and reference materials.
syslog	A standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them.

[10] http://csrc.nist.gov/publications/PubsSPs.html#SP%20800

TLS	**Transport Layer Security**, the successor version to SSL, is a cryptographic protocol providing privacy and message integrity for secure network communications. TLS also supports the use of digital certificates for one-way or mutual authentication of the communicating parties. By convention, URLs that require an TLS connection start with https: instead of http:.
use model	An organizational scheme used to define encryption and key management operations in an IT storage environment and to configure key management clients for ESKM services.
user	According to FIPS, a user is “an individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.” In this document, a user can also be referred to as a “client” — the machine that communicates with the ESKM to perform cryptographic functions.
VACM	**View-based Access Control Model**. VACM regulates access to MIB objects by providing a fine-grained access control mechanism that associates users with MIB views. VACM gathers user and security model pairs into security groups, which provide a convenient means of identification.