KeySecure
User Guide

Software Version:	6.5.0
Documentation Version:	20131014
Part Number:	007-012356-001 (Rev A)

Preface

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of SafeNet.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person of organization of any such revisions or changes.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.

4690 Millennium Drive
Belcamp, Maryland 21017
USA

Disclaimers

The foregoing integration was performed and tested only with specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

This product contains software that is subject to various public licenses. The source code form of such software and all derivative forms thereof can be copied from the following website: https://serviceportal.safenet-inc.com

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support.

SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:

Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com

Table of Contents

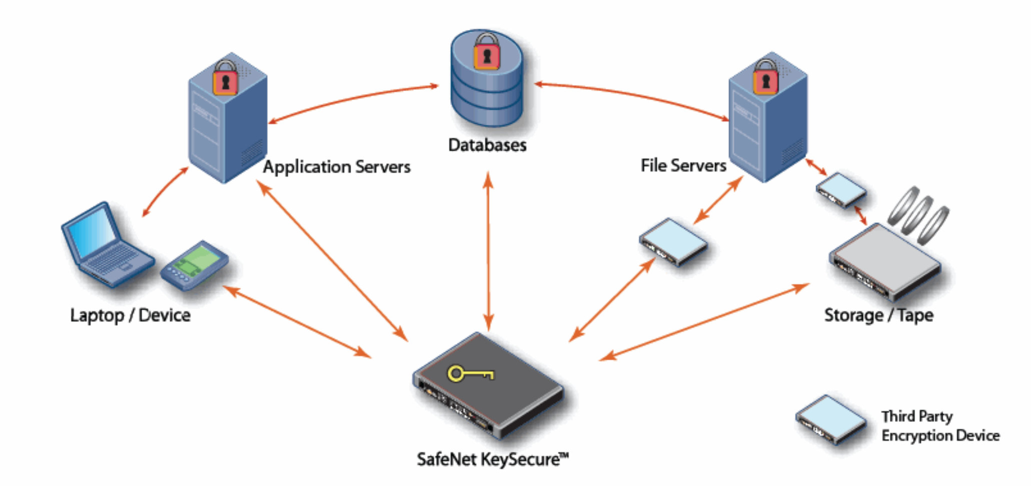
Chapter 1

Overview

Overview of the KeySecure

The SafeNet KeySecure appliance enables organizations to leverage a range of disparate software and hardware-based encryption products, while gaining the efficiency and security benefits of having all keys stored on a centralized, hardened security appliance.

KeySecure offers robust capabilities for managing cryptographic keys across their entire lifecycle, including key generation, key import and export, key rotation, and much more. KeySecure can be integrated through open APIs with virtually any off-the-shelf encryption product, including database encryption, laptop and device encryption, file and storage level encryption, and more.



Robust Security

KeySecure centrally manages keys using a hardened appliance, which maximizes overall security. KeySecure offers a range of robust security features:

- Capabilities for segregating administrative duties between different administrators.
- Granular authorization capabilities that enable constraints to be placed on user operations based on specific key permissions.
- Active alerting capabilities that inform administrators if attempts to breach protected data occur.
- Secure key distribution through support of SSL.
- Secure storage of key encryption keys on a Luna HSM card.

High Performance

KeySecure centralizes all key management on a highly specialized appliance that delivers robust performance. Even for large distributed enterprises that use multiple, disparate encryption solutions, keys can be centrally managed - without making any perceptible impact on system performance.

Broad Flexibility

KeySecure offers key management capabilities that can be integrated with virtually any commercial encryption product. Supported technologies include:

- Luna SA HSM partitions and Luna PCI HSMs.
- Application encryption, either software or hardware based.
- Database encryption, including native database encryption.
- Laptop and device encryption.
- z/OS mainframe encryption.
- File and storage level encryption solutions.

SafeNet supports a wide range of open cryptographic standard interfaces, including PKCS #11, JCE, MSCAPI, and .NET. KeySecure also supports the Key Management Interoperability Protocol (KMIP). Further, customers and partners can take advantage of SafeNet's XML interface to develop their own custom software utilizing the enterprise key management functionality of KeySecure.

Continuous Availability

SafeNet customers can deploy multiple KeySecure appliances in a clustered configuration with real-time replication of keys, policies, and configuration information across multiple appliances - enabling complete disaster recovery and business continuity.

Supported Platforms

Version 6.5.0 of the KeySecure server is supported on the 450 and 460 platforms. For the latest information about this release, please see the Customer Release Notes for version 6.5.0.

The HSM Card

The KeySecure now provides enhanced security by placing an HSM (Hardware Security Module) card at root of trust for the device.

KeySecure

With the K6 HSM card (and required configuration and administrative diligence), the KeySecure k460 key vaulting functionality complies with the FIPS 140-2 Level 3 standard.

The PED and iKeys are the only means of authenticating and permitting access to the administrative interface of the HSM. Accessing the keys on the HSM, required for the KeySecure to have any key management functionality, can only occur when an administrator has physical access to the black Crypto

User iKey, knows the iKey PED PIN, and has access to a PED connected (either remotely or locally) to the HSM in the KeySecure.

As delivered, the HSM card has no partitions. The HSM is initialized as part of the KeySecure initialization. During this process, the Security Officer and Crypto User roles are defined and their corresponding iKeys are created. These roles and iKeys are explained below. At the conclusion of the initialization, the HSM card is activated and ready to create and manage keys at the end of that process.

In the event of a power outage, the HSM card is deactivated. To reactivate the HSM, a KeySecure administrator must run the `hsm login crypto user`. If the power outage lasted longer than 2 hours, running that command will require that the Crypto User login. This means that the black Crypto User iKey must be inserted into the PED.

PED

The Pin Entry Device (PED) is the appliance used to read and manage iKeys, and to connect directly to the HSM card housed within the KeySecure appliance.

PEDs can be set to operate either in **local mode**, where they are connected directly to the HSM, or in **remote mode**, where they are connected to a properly configured client.

When running in local mode, the PED is powered by its connection to the HSM card. This is why no power cord is needed in this mode. The connection to the HSM card is direct: it bypasses other administrative controls, providing a very secure connection to the HSM. This connection cannot be monitored by any software on the KeySecure or any KeySecure client.

When running in remote mode, the PED must be plugged in to a power source. Rather than connecting directly to the HSM, remote mode enables this PED to connect to a client, which in turn connects to the HSM. This allows for remote administration of the HSM, which may be desirable for large deployments.

PEDs do not contain any authentication information and because of this, they are interchangeable.

Using the PED

As soon as it receives power from a connection to a powered appliance (or from a connection to a power supply), the PED performs its startup and self-test routines and then goes to local mode. The PED display shows “Awaiting command...” and the device is ready for use.

There are two things that you can do with the PED at this point:

- Wait for a prompt. This occurs during initialization, and when a program has caused the HSM to request authentication. Prompts typically direct you to enter an iKey, enter a PED PIN, or press the Yes, No, or Enter buttons on the keypad.
- Perform stand-alone PED operations. These operations include entering local or remote mode, and duplicating keys, updating PED software (very rare), and performing the PED self test. The PED self test checks the PED’s keypad, USB port, and display screen.

The PED does not hold the HSM authentication secrets. The PED facilitates the communication of those secrets. The secrets are generated by the HSM during the initialization process. The secrets themselves reside, encrypted, on the portable iKeys. This means that an imprinted iKey can be used only with HSMs that share the particular secret, but PEDs are interchangeable.

There is no need for the PED to be constantly attached to the KeySecure. It must be attached only when the HSM requires authentication, such as HSM initialization and to log in after a prolonged power outage.

For large or geographically disperse deployments, we recommend using the PED in remote mode. To operate in remote mode, you must configure the orange Remote PED iKey, and have purchased the remote PED package, which includes the necessary cabling and software. The PED can be used in remote mode for all actions except HSM initialization.

iKeys

An iKey is a small authentication device with a USB interface, electronically imprinted with identifying information generated by the HSM during initialization. This data is encrypted and stored on the iKey and recalled via the PED when the KeySecure administrator performs some action that requires HSM authentication; for example, when logging in as the crypto user to access keys.

The HSM initialization process creates three types of iKeys, each with distinct roles: the blue Security Officer iKey, the red Domain iKey, and the black Crypto User iKey. Each role is described below:

- The **Security Officer** is responsible for administration of the HSM: initializing the HSM, creating partitions. The blue Security Officer iKey (sometimes referred to as the HSM Admin iKey) is needed to log in the Security Officer during the initialization process and will be required in the event of a firmware upgrade. An HSM can have only one Security Officer.
- The **Domain** is the shared identifier for a group of HSMs. An HSM can be a member of only one domain. There can be one or more HSMs in a domain. The red Domain iKey is needed to initialize the HSM and to create a partition, which both occur during the HSM initialization.
- The **Crypto User** owns the HSM partition that stores the keys used by the KeySecure. The black Crypto User iKey is needed to log in the Crypto User. Login is required to create and manage keys and certificates. If the Crypto User is not logged in, access to this information is denied and the KeySecure cannot perform its crucial functions. Typically, you will log in the Crypto User once, at the end of the initialization process. The Crypto User will remain logged in until explicitly logged out, or may be logged out in the event of a power outage.

  Note: When the Crypto User is logged out, all cluster operations will become disabled. The Device>Cluster>Cluster Configuration page will not indicate that cluster settings exist; it will appear empty. After the Crypto User is logged in again, it can take up to a minute to resume cluster activity. The following warning text should remain on the page until the Crypto User logs back in, and you have refreshed the page:

  > "Crypto User is currently not logged in. All cluster operations are disabled. DO NOT attempt to recreate cluster. Please use CLI to log in the Crypto User."

  After the Crypto User logs back in, reloading the page will make this warning message go away.

  The Crypto User has a password, in the form of `MxCT-c7F9-HHX5-YtH3`, which is generated by the HSM and entered into the KeySecure CLI during initialization. Normally, you will not need to enter the password again unless you re-initialize the HSM or you reset the password using the `hsm set password` command.

All three of the iKeys are created and used during the HSM initialization. Afterwards, the black Crypto User key will be the most used.

The orange **Remote PED iKey** is required to use the PED in remote mode, which is available to customers who have purchased the remote PED package. The iKey is needed to initialize the remote PED (at the KeySecure) and then to use the PED remotely (at the client machine). The orange iKey is configured after completing the initialization.

Using the iKeys

The set of iKeys included with the KeySecure contains ten USB-token PED keys along with colored peel-and-stick labels used for identification. The iKeys are completely interchangeable before they are imprinted and labeled by you.

At a minimum you would have one each of:

- blue HSM Admin iKey
- red Domain iKey
- black User iKey

How you choose to use the iKeys can be straight-forward (one of each listed above, plus one set of backups) or complex (one red Domain iKey shared by multiple HSMs, employing M of N for the black User iKey, etc.). Plan ahead, keeping in mind your organization’s own security policies.

For purposes of backup redundancy, you would normally have at least one other full set of imprinted iKeys for keeping in safe storage. You can create duplicates during the initialization process, or at anytime afterwards using the PED. We recommend creating duplicates as a separate process, done after initializing the HSM. This reduces the number of keys you’ll have to handle during the initialization and lessens the chance that you will accidentally overwrite an iKey.

Each iKey has its own PIN that is needed to access the secret encrypted on the iKey. A PED PIN is a sequence of 4 to 48 digits that you enter at the PED keypad. The PIN is combined with the secret on the iKey and the combined blob is sent to the HSM.

If, for example, you are initializing an HSM and not re-using any existing secret on the iKey that you present (or it’s a blank a key), then during the process, the PED prompts:

```
Enter new PED PIN
```

To impose a PED PIN, enter the PIN when prompted during the iKey configuration process. Thereafter, whenever you present that iKey, you will be prompted to enter the PED PIN. The PED uses the PIN to “unlock” the actual authentication secret, which is then sent to the HSM. Entering the wrong PIN is equivalent to presenting the wrong iKey - it is counted as a “bad password” attempt on the HSM.

Summary of iKey Use

Function	Blue HSM Admin iKey	Black User iKey	Red Domain iKey	Orange Remote iKey
Initialize the HSM `hsm initialize` command			Required	
Create the HSM partition `hsm create partition` command	Required		Required	
Log in the Security Officer `hsm login security officer` command	Required			
Log in the Crypto User `hsm login crypto user` command		Required		
Initialize the remote PED (at the KeySecure) `hsm remote ped init` command				Required
Connect to the remote PED (at the client) `hsm remote ped connect` command				Required

The first four functions, initialize HSM, create partition, log in Security Officer and log in Crypto User are all performed as part of the KeySecure initialization. Once the device is initialized, you may occasionally need to log in the Crypto User, and you have the option of initializing and connecting the remote PED.

Device Configuration Overview

After you have unpacked, installed, and initialized the KeySecure as described in the *KeySecure Quick Start Guide,* you can configure the device.

The following chapters describe how to configure the features of the KeySecure:

- **Chapter 3, "Cryptographic Key Servers"** - create cryptographic key servers that accept client requests from clients using the NAE-XML protocol. You can set the IP, port, and authentication process (e.g., use of SSL) for each server you configure.
- **Chapter 4, "Health Check"** - enables client applications to check the availability of the key server by sending the key server an HTTP request.
- **Chapter 28, "HSM Configuration"** - enables a SafeNet hardware security module (HSM) to store the encryption keys used to create keys and certificates on the KeySecure. You must initialize the HSM card as part of the KeySecure installation process.
- **Chapter 5, "KeySecure Clustering"** - enables multiple KeySecures 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 Key Servers, and improves the failover capabilities of a high availability configuration.
- **Chapter 6, "Date, Time and NTP"** - set the system date and time, and configure NTP servers.
- **Chapter 7, "Network Interfaces"** - enables you to configure the KeySecure network interface list and create VLAN tagged interfaces.

- **Chapter 8, “Gateways & Routing”** - enables you to configure the default gateway list, select the interface to use for outgoing connections, and configure a static route list.
- **Chapter 9, “Hostname & DNS”** - set the KeySecure hostname and connect to any DNS servers in your network.
- **Chapter 10, “Network Interface Port Speed & Duplex”** - enables you to configure the port speed and duplex for the KeySecure network interfaces.
- **Chapter 11, “High Availability”** - enable and configure the high availability feature.
- **Chapter 12, “IP Authorization”** - specify which IP addresses are permitted to connect to the KeySecure and which services those IP addresses may access.
- **Chapter 13, “SNMP”** - enable monitoring of the KeySecure via SNMP.
- **Chapter 14, “Administrator Configuration”** - create and manage local administrator accounts.
- **Chapter 15, “LDAP Administrator”** - enable and configure LDAP administrator accounts.
- **Chapter 16, “Password Management”** - create password policies for all passwords used by the KeySecure: local administrators, local users, KeySecure clusters, and backups.
- **Chapter 17, “Multiple Credentials”** - stipulate that some administrative and key management operations require authorization from more than one administrator.
- **Chapter 18, “Remote Administrator”** - determine the IP addresses, ports, and certificates used for remote KeySecure administration via the Management Console and Command Line Interface.

The KeySecure provides logs and statistics that enable you to monitor system health and performance. The following chapters describe how to configure system logs and view system and server statistics.

- **Chapter 19, “Logging”** - schedule log rotations, configure archiving details, transfer logs to an external device, and configure syslog.
- **Chapter 20, “Log Viewer”** - view log files stored on the KeySecure.
- **Chapter 21, “Statistics”** - view system and server statistics.

Regular maintenance of the KeySecure involves creating backups of the device configuration. You can also stop and restart services, upgrade software, install licenses, monitor system health, and diagnose network connectivity issues.

The following chapters describe how to perform regular device maintenance.

- **Chapter 22, “Backups”** - create and restore backups of system configuration.
- **Chapter 23, “Services”** - start and stop the key servers, web administration service, ssh administration service, and snmp agent, restart those services, enable those services to launch at system startup, restart the KeySecure, and halt the KeySecure.
- **Chapter 24, “Upgrade”** - upgrade software, upload licenses, and examine information about the KeySecure device, including Box ID and current software version.
- **Chapter 25, “System Health”** - view the status of the KeySecure power supply, cooling fan and disks, and prepare for the removal of disk from the RAID.

- **Chapter 26, “Network Diagnostics”** - test the KeySecure network connectivity by running ping, traceroute, host, or netstat commands

The following chapters explain how to manage keys, users, certificates, and the KeySecure advanced security features:

- **Chapter 27, “Keys”** - create keys, create and manage versioned keys, import keys, download the public portion of RSA keys, delete keys, create key queries, and clone keys.
- **Chapter 29, “Authorization Policies”** - create and delete authorization policies.
- **Chapter 30, “Local Users and Groups”** - create a local user, create a local group, remove a user from a group, delete a user, and delete a group.
- **Chapter 31, “LDAP Server”** - set up the LDAP user server.
- **Chapter 32, “LDAP User & Groups”** - view LDAP users and groups.
- **Chapter 33, “Certificates”** - create a server certificate for the KeySecure, create a client certificate, download a certificate, and import a certificate.
- **Chapter 34, “Certificate Authorities”** - manage the trusted CA list, view and download a local CA, create a local certificate authority, create an intermediate CA request, and install a CA certificate.
- **Chapter 35, “Certificate Revocation Lists”** - download and update certificate revocation lists.
- **Chapter 36, “Certificate Management over KMIP”** - manage certificates for KMIP operations.
- **Chapter 37, “High Security Features”** - configure the device for FIPS compliance, configure high security settings for the device, including disabling the use of FTP (for non-FIPS compliant hardware), and configure the device for Common Criteria compliance.
- **Chapter 38, “FIPS Status Server”** - enable the FIPS status server and view the FIPS status report.
- **Chapter 39, “SSL”** - enable ssl protocols and the session key timeout, and manage the ssl cipher priority.

Chapter 2

The KeySecure Management Interfaces

Once you have completed the initial configuration of the KeySecure, described in the *KeySecure Quick Start Guide*, log in to either of the following management interfaces using a valid administrator account.

- **Management Console** - The management console is a graphic user interface that enables you to perform remote administration using a web browser.

  The web browser used to connect to the Management Console must be capable of high-grade 128-bit encryption. To access all functionality of the Management Console, enable javascript on the browser.

- **Command Line Interface** - The command line interface (CLI) enables you to perform administrative functions either at the KeySecure serial console or remotely using SSH.

  The serial console must use a terminal emulation program, such as HyperTerminal. Remote CLI administration requires a terminal emulation program that supports SSH (PuTTY, for example). The SSH client should connect to the IP address defined in the first-time initialization process.

  For more information about the command line interface, see the *KeySecure CLI User Guide.*

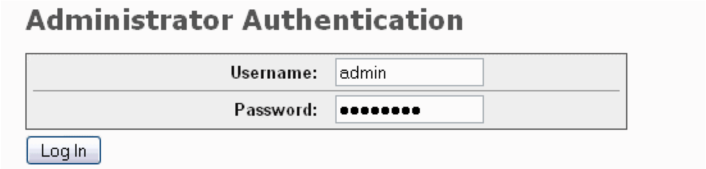
If you attempt unsuccessfully to log in to a user account five consecutive times, that account is locked out immediately for a period of one minute. If SNMP traps are enabled and the SNMP service is running, a trap is sent to the appropriate SNMP Management Station.

Using the Management Console

To log in to the management console:

1 Type the following URL, using the IP address and port you set during the initialization process: `https://IP-address:9443` (assuming that 9443 is the port you set up).

When connecting to the Management Console for the first time, your browser might display a certificate error notice. To avoid this message in the future, instruct the browser to accept the certificate for all sessions.



Administrator Authentication

Username: admin

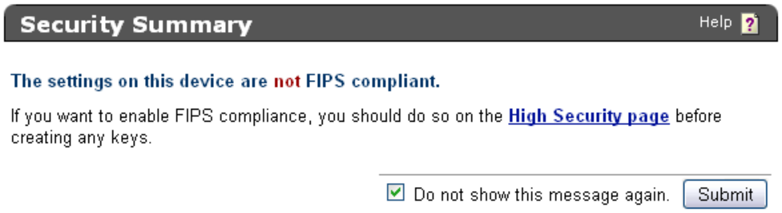
Password: ●●●●●●●●●

2 Enter a **Username**. When logging in for the first time, use the default username *admin*. You can create other administrator accounts using the Administrator Configuration page. This is described in Chapter 14, “Administrator Configuration”.

3 Enter the **Password**. When logging in for the first time, this is the password you created during initialization. Don’t lose this password.

4 Click **Log In**. The Management Console displays the Home page, which includes the following parts:

- **Security Summary** - This section displays security-related information about your KeySecure.



Security Summary

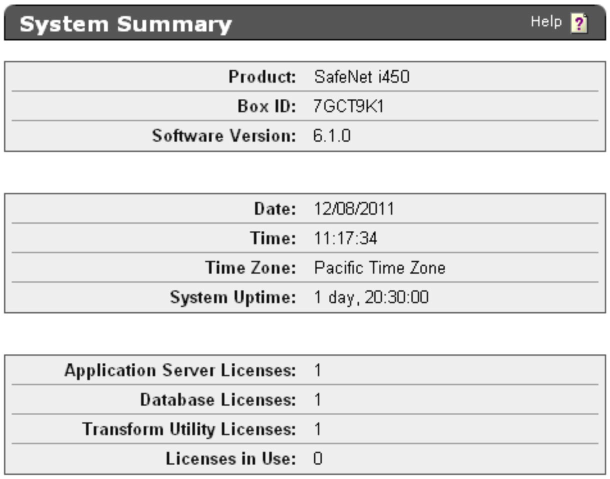
The settings on this device are not FIPS compliant.

If you want to enable FIPS compliance, you should do so on the High Security page before creating any keys.

☑ Do not show this message again. Submit

Click the High Security page link to access the High Security page. You can enable FIPS compliance from there. You can select the **Do not show this message again** checkbox and click **Submit** to remove the Security Summary section from the Home page. Once you remove the Security Summary section from the Home page, you cannot restore that section.

- **System Summary** - This section displays system information about the KeySecure.



System Summary

Product:	SafeNet i450
Box ID:	7GCT9K1
Software Version:	6.1.0

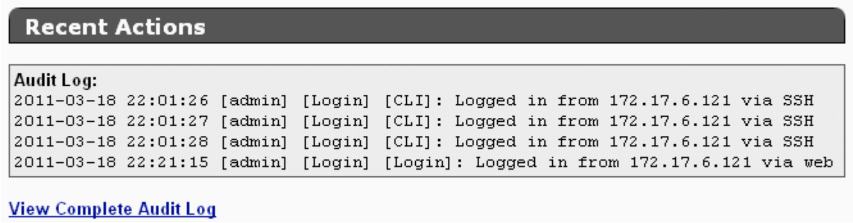
Date:	12/08/2011
Time:	11:17:34
Time Zone:	Pacific Time Zone
System Uptime:	1 day, 20:30:00

Application Server Licenses:	1
Database Licenses:	1
Transform Utility Licenses:	1
Licenses in Use:	0

This section contains the following fields:

- **Product** - the product’s model name (e.g., SafeNet k460).
- **Box ID** - the device’s identification code. You will need this ID if you ever contact our customer support department.
- **Software Version** - version of the software currently running on the device.
- **Date** - current system date.
- **Time** - current system time.
- **Time Zone** -current system time zone.
- **System Uptime** - length of time that the system has been running since the last boot.
- **Application Server Licenses** - number of application server licenses currently in use.
- **Database Server Licenses** - number of database server licenses currently in use.
- **Transform Utility Licenses** - number of transform utility licenses currently in use.
- **Licenses in Use** - total number of licenses in use.

- **Recent Actions** - This section displays the most recent entries in the KeySecure audit log. The audit log contains a record of all configuration changes and user input errors made to the KeySecure, whether through the Management Console or the CLI. Click **View Complete Audit Log** to view the entire log file.



```
Audit Log:
2011-03-18 22:01:26 [admin] [Login] [CLI]: Logged in from 172.17.6.121 via SSH
2011-03-18 22:01:27 [admin] [Login] [CLI]: Logged in from 172.17.6.121 via SSH
2011-03-18 22:01:28 [admin] [Login] [CLI]: Logged in from 172.17.6.121 via SSH
2011-03-18 22:21:15 [admin] [Login] [Login]: Logged in from 172.17.6.121 via web
```

Security Lockouts

If you enter the password incorrectly five consecutive times when logging in to a user account over an ethernet connection, web access and ssh access for that account are locked out immediately.

Important! Once access has been locked, the lock remains in place for 30 minutes from the last attempt during the lockout period.

This means that even if you attempt to login with the correct account name and password during the lockout period, the lock is extended. Any login attempt during the lockout period resets the lockout period and extends it for another 30 minutes.

The other features of security lockouts are listed below.

- A lockout originating on a Web Admin session also applies to ssh access to the CLI.
- A lockout originating over ssh access to the CLI also applies to web access.
- A lockout originating on the Web Admin interface (https) or ssh interface does not apply to direct serial console access. A user who is locked out on the web or ssh could still log in to the console with the correct password.
- A lockout originating on the serial console has an independent start from ethernet logins, but follows a scheme similar to the web logins allowing four consecutive bad entries and locking the session on the fifth. A lockout originating on the serial console affects neither the ability to login through the web admin interface nor the SSH, but remains in place for 30 minutes on the admin console only.
- If SNMP traps are enabled and the SNMP service is running, a trap is sent to the appropriate SNMP Management Station.

Chapter 3

Cryptographic Key Servers

On the KeySecure, you can create Cryptographic Key Servers that accept key management requests from KMIP clients. You can set the IP, port, and authentication process (e.g., use of SSL) for each server you configure. One such server is included by default, you can edit this configuration or make additional servers as needed.

NAE-XML Protocol

The Network-Attached Encryption - XML (NAE-XML) protocol is used to off-load cryptographic operations from clients to the KeySecure. KeySecure clients, such as application servers running Protect-App and databases running Protect-DB, send cryptographic requests via the NAE-XML protocol. The KeySecure is capable of performing asymmetric and symmetric encryption and decryption, MAC and MAC verification, keyed hashes, digital signatures and verifications, and random number generation.

For more information about connecting to the KeySecure using this interface, see the *XML Interface User Guide.* For information about specific client software, see the appropriate ProtectDB or ProtectApp user guide for your product.

KMIP

The Key Management Interoperability Protocol (KMIP) is used to transmit key management requests from clients to the KeySecure. Clients are able to submit the following requests.

- Activate
- AddAttribute
- Create
- CreateKeyPair
- DeleteAttribute
- Destroy
- Get
- GetAttributes
- GetAttributeList
- Locate
- ModifyAttribute
- Query
- Register

- Revoke

The KeySecure currently supports the following managed objects: certificates, private keys, public keys, templates, secret data, and symmetric keys. For more information about the KeySecure implementation of KMIP, see Appendix F, “OASIS KMIP Support.”

Authentication Overview

The communication between the key server and the client varies slightly, depending on whether your protocol configuration requires users to authenticate. If you decide not to authenticate, then users have access only to global keys. Global keys are keys that 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 that 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 a certain number of operations per hour.

Authentication Options

The key server provides many options with respect to security and authentication, for each protocol. You can:

- **mandate SSL** by selecting **Use SSL** – You can choose between SSL connections and standard TCP connections; SSL connections are more secure since all data exchanged between client and server is encrypted.
- **allow global sessions** by disabling **Password Authentication** – You can allow clients to access and create global keys without providing a valid username and password to the key server; this obviously does not offer a high level of security.
- **disable global sessions** by enabling **Password Authentication** and/or enabling **Client Certificate Authentication** – You can 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 key server.
- **require client certificates** by enabling **Client Certificate Authentication** – You can require that clients present a client certificate in order to establish SSL connections. This client certificate can be the sole means of authenticating to the key server, or it can be used in tandem with a username and password combination.
- **enforce strong, two-factor authentication** by enabling **Client Certificate Authentication** and configuring the **Username Field in Client Certificate** field – You can take the require client certificates option one step further by having the key server 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, then the user is authenticated. This may be combined with the IP address requirement.

- **require the client IP address in the certificate** by enabling **Require Client Certificate to Contain Source IP** – You can require that the client certificate contain the client's IP address in the certificate's subjectAltName field. The key server compares that value with the source IP address of the authentication request. If the IPs match, then the user is authenticated. This may be combined with the two-factor authentication option described above.

We recommend that you enforce the most stringent security policy supported by the key server. Such a security policy would mandate SSL, disallow global sessions, and enforce strong, two-factor authentication and require that the client certificate contain the client IP address.

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 that group can use that particular key (after authenticating to the server).

When the client requests that the server 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 server. Once 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 server. Once a key is generated as deletable, only the owner of the key can delete the key.

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

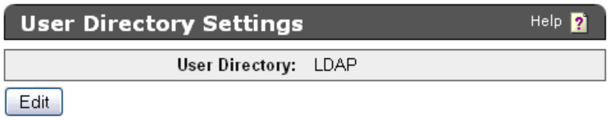
Clients that do not authenticate can only see global keys, which are accessible to all users. Likewise, any keys that the client generates during an unauthenticated connection are global keys. If a global key is marked as exportable or deletable during generation, then all users have permission to export or delete that key.

Configure the User Directory Settings

The User Directory Settings section determines if the KeySecure will employ a local or LDAP user directory when authenticating client requests. To use an LDAP directory, you must select LDAP here, and also configure the LDAP settings on the LDAP Server Configuration page (Security >> LDAP >> LDAP Server)

To configure the user directory settings:

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



User Directory Settings

User Directory: LDAP

3 Click **Edit**.

4 Select *Local* or *LDAP* in the **User Directory** field. You can only choose one user directory at a time.

Important! Selecting LDAP on a FIPS compliant device will take the device out of FIPS compliance - possibly in a manner that does not comply with FIPS standards. For information on disabling FIPS compliance, see Chapter 37, “High Security Features”.

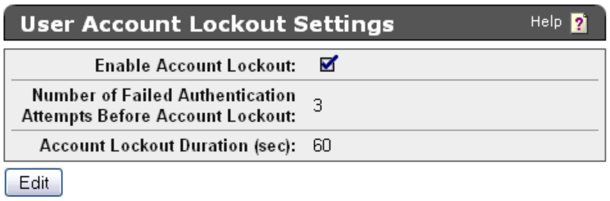
5 Click **Save**. This change applies to all key servers.

Configure the User Account Lockout Settings

To configure the user account lockout settings:

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

2 Navigate to the User Account Lockout Settings section of the Cryptographic Key Server Configuration page (Device >> Key Server >> Key Server).



User Account Lockout Settings

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

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. When not enabled, users can make unlimited attempts to log in to an account.

5 Enter a value in the **Number of Failed Authentication Attempts Before Account Lockout** field. After this number of failed attempts, 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, at which time the counter is reset.

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**.

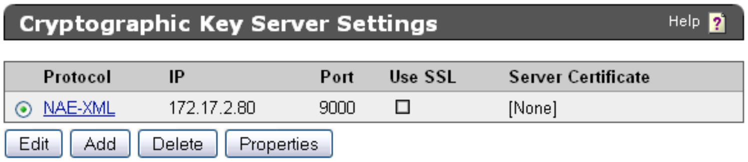
Manage the NAE-XML Server

By default, the key server is pre-configured for the NAE-XML protocol, though you will need to change some settings to enable SSL, enable clients to create, delete, and import keys, manage users, and export keys.

To manage the NAE-XML server:

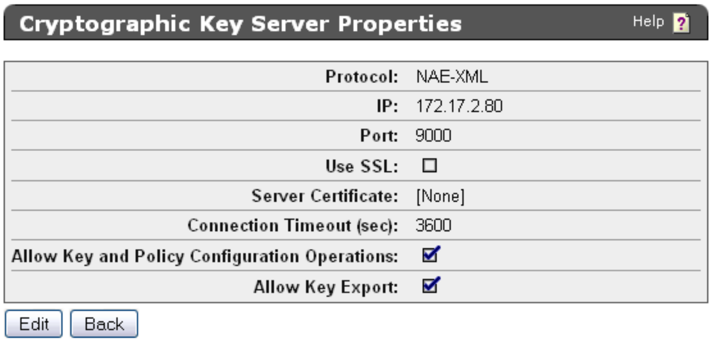
1 Log in to the Management Console.

2 Navigate to the Cryptographic Key Server page (Security >> Key Server).



	Protocol	IP	Port	Use SSL	Server Certificate
●	NAE-XML	172.17.2.80	9000	□	[None]

3 Select NAE-XML and click Properties, or click **Add** to create a new entry.



Protocol:	NAE-XML
IP:	172.17.2.80
Port:	9000
Use SSL:	□
Server Certificate:	[None]
Connection Timeout (sec):	3600
Allow Key and Policy Configuration Operations:	☑
Allow Key Export:	☑

4 View the Cryptographic Key Server Properties. Click **Edit** to alter any values.

WARNING: Regarding Editing in a production environment – Depending on cluster replication settings, changing (editing) a Key Server setting in a production environment can compromise services from clustered servers, and is not recommended. If you are considering such a change, contact SafeNet technical support for advice.

The available fields are:

- **IP** - IP address(es) on which the key server is enabled on the KeySecure. We strongly recommend that you select a *specific* IP address rather than using *[All]*. If you have multiple IP addresses available, using a single address here enables the key server to listen for traffic on only one IP address. This can greatly reduce system vulnerability to outside attacks.
- **Port** - port on which the server is listening for client requests. The default port assignment is 9000 for NAE-XML.
- **Use SSL** - specify whether you want to require that clients connect to the key server using an SSL connection. If SSL is not enabled, the key server will not accept SSL connections.
- **Server Certificate** - required only when using SSL. must point to a server certificate signed by a local CA. This certificate will be used to authenticate the key server to clients.

- **Connection Timeout (sec)** - specifies how long a client connect can remain idle before the key server begins closing them. The default value is 3600, which is also the maximum.
- **Allow Key and Policy Configuration Operations** - when enabled, the key 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 XML interface).

  When this feature is disabled, only authentication, cryptographic, and random number generation requests are available.

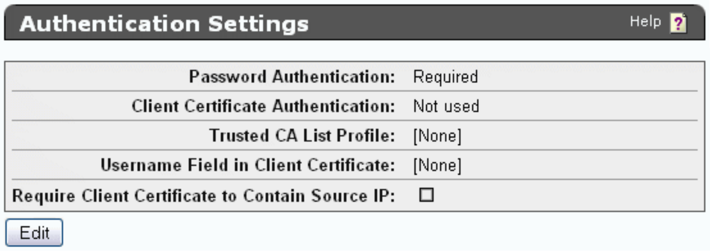
  Note: When using the multiple credentials feature, enabling this option allows users (and unauthenticated sessions) to perform the actions listed without being subjected to the multiple credentials rules. This may pose a security loophole. You might allow this access for automated scripts, or you might disallow it to tighten security.

  Important! Enabling this feature on a FIPS compliant device will take the device out of FIPS compliance - possibly in a manner that does not comply with FIPS standards. For information on disabling FIPS compliance, see Chapter 37, “High Security Features”.

  -**Allow Key Export** - when enabled, the key server allows key export.

  Important! Enabling this feature on a FIPS compliant device will take the device out of FIPS compliance - possibly in a manner that does not comply with FIPS standards. For information on disabling FIPS compliance, see Chapter 37, “High Security Features”.

5 View the Authentication Settings. Click **Edit** to alter any values.



Authentication Settings

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:	□

The available fields are:

- **Password Authentication** - determines whether you require users to provide a username and password to access the key server. There are three options:
  - *Not used* - (default) password authentication is not allowed; non-global sessions are not allowed.
  - *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.

- **Client Certificate Authentication** - there are three options
  - *Not used* - (default) clients do not have to provide a client certificate to authenticate to the key server.
  - *Used for SSL session only* - clients must provide a certificate signed by a CA trusted by the KeySecure in order to establish an SSL 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 KeySecure in order to establish an SSL connection; 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 does provide a username, the key server compares the username derived from the certificate against the username in the authentication request. If the usernames match 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** - select a profile to use to verify that client certificates are signed by a CA trusted by the KeySecure. This field is only used if you select *Used for SSL session only* or *Used for SSL session and username* above. 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 is with at least one trusted CA before the key server can authenticate client certificates.
- **Username Field in Client Certificate** - specify the field from which to derive the username. This field is only used if you select *Used for SSL session and username* above. The username can come from the *UID* (user ID), *CN* (Common Name), *SN* (Surname), *E* (Email address), *E_ND* (Email without domain), or *OU* (Organizational Unit) field.

  If you select *E_ND*, the key 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 key server matches against User1.
- **Require Client Certificate to Contain Source IP** - determines if the key server expects that the client certificate presented by the client application has an IP address in the subjectAltName field. The key server obtains the IP address from the subjectAltName and compares that the source IP address of the client application; if the two IP addresses match, the key server authenticates the user. If the two IP addresses do not match, the key server closes the connection with the client.

Add a KMIP Server

Because the KMIP Interface operates over SSL, KMIP server configuration is done in three parts. First, you must configure a local CA on the KeySecure. Second, you must create a server certificate signed by that local CA. Third, you must configure the KMIP server settings.

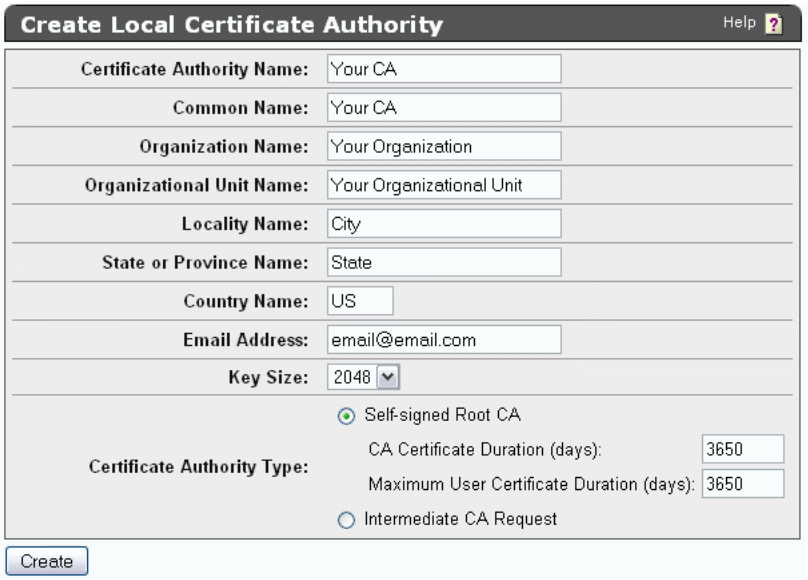
If there is already a local certificate authority on the KeySecure, you can skip to the second set of instructions. If there is already a server certificate, you can skip to the third set of instructions.

KMIP clients must provide certificates to connect to the KeySecure, which means the KeySecure must have access to signing CA to verify the certificate.

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).



Create Local Certificate Authority

Certificate Authority Name:	Your CA
Common Name:	Your CA
Organization Name:	Your Organization
Organizational Unit Name:	Your Organizational Unit
Locality Name:	City
State or Province Name:	State
Country Name:	US
Email Address:	email@email.com
Key Size:	2048
Certificate Authority Type:	● Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 ○ Intermediate CA Request

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

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

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**. Once you create a self-signed root CA, you must add it to the trusted CA list for it to be recognized by the Key Server.

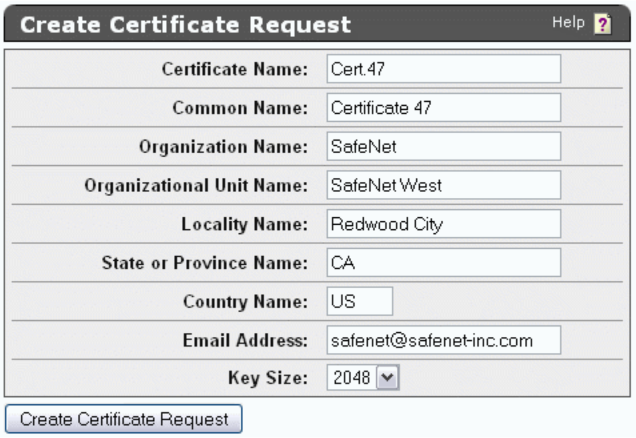
When you create an intermediate CA request, you must sign it with either an existing intermediate CA or your organization’s root CA. Certificates signed by the intermediate CA can be verified by that same intermediate CA, by the root itself, or by any intermediate CAs that link the signing CA with the root. This enables you to de-centralize 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.

5 Click **Create** to create the KeySecure local CA.

To create a server certificate, you must create a certificate request and sign it with the local CA:

1 Navigate to the Create Certificate Request section of the Certificate and CA Configuration page (Security >> SSL Certificates).

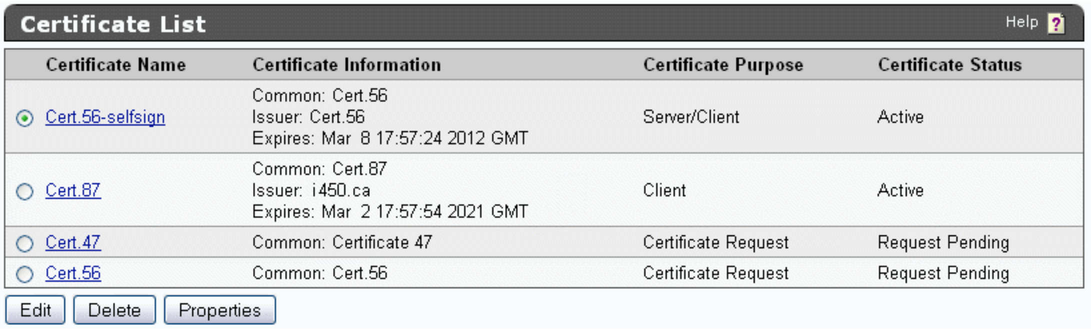


Create Certificate Request

Certificate Name:	Cert.47
Common Name:	Certificate 47
Organization Name:	SafeNet
Organizational Unit Name:	SafeNet West
Locality Name:	Redwood City
State or Province Name:	CA
Country Name:	US
Email Address:	safenet@safenet-inc.com
Key Size:	2048

2 Enter the **Certificate Name**, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, and **Key Size** for the certificate. The KeySecure supports 768-bit, 1024-bit, and 2048-bit key sizes.

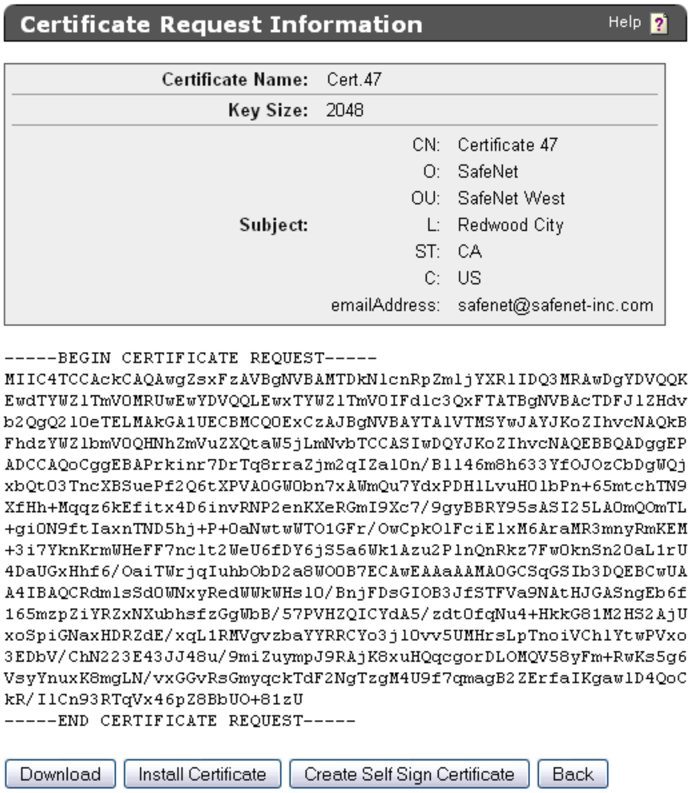
3 Click **Create Certificate Request**. The list shows the new request with a status of *Request Pending*.



Certificate List

	Certificate Name	Certificate Information	Certificate Purpose	Certificate Status
●	Cert.56-selfsign	Common: Cert.56 Issuer: Cert.56 Expires: Mar 8 17:57:24 2012 GMT	Server/Client	Active
○	Cert.87	Common: Cert.87 Issuer: i450.ca Expires: Mar 2 17:57:54 2021 GMT	Client	Active
○	Cert.47	Common: Certificate 47	Certificate Request	Request Pending
○	Cert.56	Common: Cert.56	Certificate Request	Request Pending

4 Select the certificate request and click **Properties** to access the Certificate Request Information section.



Certificate Name:		Cert.47
Key Size:		2048
Subject:	CN:	Certificate 47
	O:	SafeNet
	OU:	SafeNet West
	L:	Redwood City
	ST:	CA
	C:	US
	emailAddress:	safenet@safenet-inc.com

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC4TCCAckCAQAwgZsxFzAVBgNVBAMTDkNlcnRpZmljYXRlIDQ3MRAwDgYDVQQK
EwdTYWZlTmV0MRUwEwYDVQQLEwxTYWZlTmV0IFdlc3QxFTATBgNVBAcTDFJlZHdv
b2QgQ2l0eTELMAkGA1UECBMCQ0ExCzAJBgNVBAYTAlVTMSYwJAYJKoZIhvcNAQkB
FhdzYWZlbmV0QHNhZmVuZXQtaW5jLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAPrkinr7DrTq8rraZjm2qIZalOn/Bll46m8h633YfOJOzCbDgWQj
xbQtO3TncXBSuePf2Q6tXPVAOGWObn7xAWmQu7YdxPDHlLvuHOlbPn+65mtchTN9
XfHh+Mqqz6kEfitx4D6invRNP2enKXeRGmI9Xc7/9gyBBRY95sASI25LAOmQOmTL
+giON9ftIaxnTND5hj+P+OaNwtwWTO1GFr/OwCpkOlFciElxM6AraMR3mnyRmKEM
+3i7YknKrmWHeFF7nclt2WeU6fDY6jS5a6Wk1Azu2PlnQnRkz7FwOknSn2OaL1rU
4DaUGxHhf6/OaiTWrjqIuhbObD2a8WOOB7ECAwEAAaAAMA0GCSqGSIb3DQEBCwUA
A4IBAQCRdmlsSdOWNxyRedWWkWHslO/BnjFDsGIOB3JfSTFVa9NAtHJGASngEb6f
165mzpZiYRZxNXubhsfzGgWbB/57PVHZQICYdA5/zdtOfqNu4+HkkG81M2HS2AjU
xoSpiGNaxHDRZdE/xqL1RMVgvzbaYYRRCYo3jlOvv5UMHrsLpTnoiVChlYtwPVxo
3EDbV/ChN223E43JJ48u/9miZuympJ9RAjK8xuHQqcgorDLOMQV58yFm+RwKs5g6
VsyYnuxK8mgLN/vxGGvRsGmyqckTdF2NgTzgM4U9f7qmagB2ZErfaIKgawlD4QoC
kR/IlCn93RTqVx46pZ8BbUO+81zU
-----END CERTIFICATE REQUEST-----
```

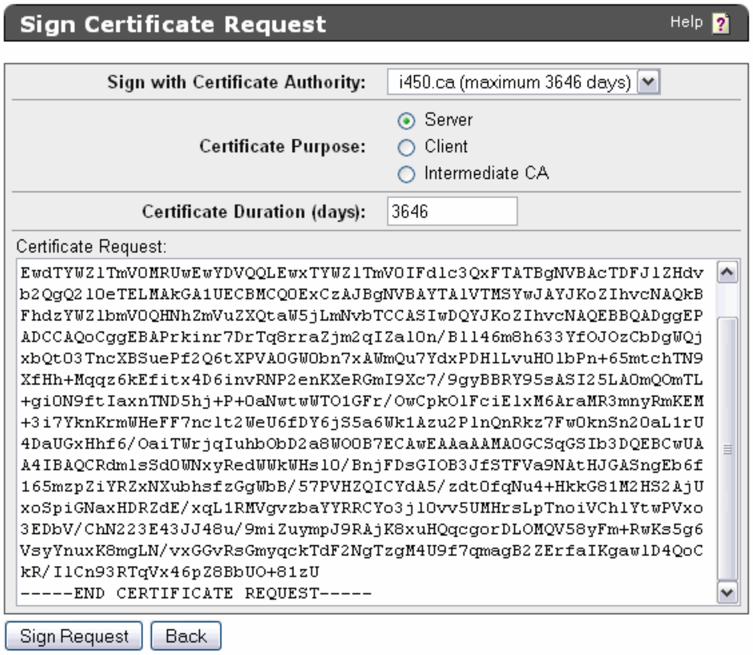
5 Copy the certificate request text. The certificate text looks similar to, but is NOT identical to, the following text.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBmzCCAQQCAQAwWzEPMA0GA1UEAxMGZmxldGNoMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEJM
AcGA1UEBxMAMQkwBwYDVQQIEwAxCzAJBgNVBAYTAlVTMQ8wDQYJKoZIhvcNAQkBFgAwgZ8wDQ
YJKoZIhvcAYBABTUxxgY0AMIGJAoGBAMUqA1t4m&Nm0sCcUqnt5Yug+qTSbgEFnvnYWUApHKD
lx5keC1lguQDU1ol2Xcc3YGrUviGCe4y0JIMK2giQ5b+ABQDemRiD11vInQqkhV6ngWBRD0lp
KCjU6QXDEE9KGCKBRh5uqL70rr2LErqxUuYwOu50Tfn4T3tKb1HGgfdzAgMBAAGgADANBgkqh
kiG9w0BAQQFAAOBgQCuYnv8vBzXEZpgLD71FfeDK2Zqh0FnfTHXAkHrj4JP3MCMF5nKHgOSRV
mImNHHy0cYKTDP+hor68R76XhLVapKMqNuUHUYf7CTB5JNHHy0cYKTNHHy0cYKTuV1Ce8nvvU
G+yp2Eh8aJ7thaua41xDFXPmIEXTqzXi1++DCWAdWaysojPCZugY7jNWXmg==
-----END CERTIFICATE REQUEST-----
```

Important! Be sure to include the first and last lines (-----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----), and enter only the text in the certificate. Do not copy any extra white space.

6 Navigate to the Local Certificate Authority List section (Security >> Local CAs).

7 Select a CA and click **Sign Request**.



Sign with Certificate Authority: i450.ca (maximum 3646 days)

Certificate Purpose: ● Server ○ Client ○ Intermediate CA

Certificate Duration (days): 3646

Certificate Request:

```
EwdTYWZlTmVOMRUwEwYDVQQLEwxTYWZlTmVOIFdlc3QxFTATBgNVBAcTDFJlZHdv
b2QgQ2l0eTELMAkGA1UECBMCQ0ExCzAJBgNVBAYTAlVTMSYwJAYJKoZIhvcNAQkB
FhdzYWZlbmVOQHNhZmVuZXQtaW5jLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAPrkinr7DrTq8rraZjm2qIZa1On/Bl146m8h633YfOJOzCbDgWQj
xbQtO3TncXBSuePf2Q6tXPVAOGWObn7xAWmQu7YdxPDHlLvuHOlbPn+65mtchTN9
XfHh+Mqqz6kEfitx4D6invRNP2enKXeRGmI9Xc7/9gyBBRY95sASI25LAOmQOmTL
+giON9ftIaxnTND5hj+P+OaNwtwWTO1GFr/OwCpkOlFciElxM6AraMR3mnyRmKEM
+3i7YknKrmWHeFF7nclt2WeU6fDY6jS5a6Wk1Azu2PlnQnRkz7FwOknSn2OaL1rU
4DaUGxHhf6/OaiTWrjqIuhbObD2a8WOOB7ECAwEAAaAAMAOGCSqGSIb3DQEBCwUA
A4IBAQCRdmlsSdOWNxyRedWWkWHslO/BnjFDsGIOB3JfSTFVa9NAtHJGASngEb6f
165mzpZiYRZxNXubhsfzGgWbB/57PVHZQICYdA5/zdtOfqNu4+HkkG81M2HS2AjU
xoSpiGNaxHDRZdE/xqL1RMVgvzbaYYRRCYo3jlOvv5UMHrsLpTnoiVChlYtwPVxo
3EDbV/ChN223E43JJ48u/9miZuympJ9RAjK8xuHQqcgorDLOMQV58yFm+RwKs5g6
VsyYnuxK8mgLN/vxGGvRsGmyqckTdF2NgTzgM4U9f7qmagB2ZErfaIKgawlD4QoC
kR/IlCn93RTqVx46pZ8BbUO+81zU
-----END CERTIFICATE REQUEST-----
```

8 Paste the certificate request into the **Certificate Request** field.

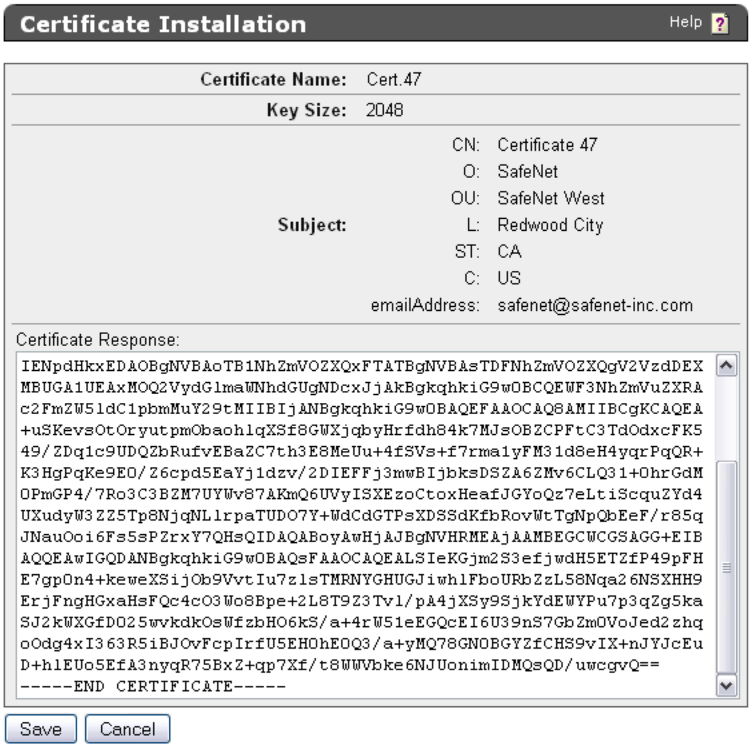
9 Select *Server* as the **Certificate Purpose**, specify a **Certificate Duration** and click **Sign Request**. The newly-activated certificate displays on a new page.

10 Copy the certificate text.

11 Navigate back to the Certificate List section. (Security >> SSL Certificates)

12 Select the certificate request and click **Properties** to access the Certificate Request Information section.

13 Click **Install Certificate**.



Certificate Name:	Cert.47
Key Size:	2048
Subject:	CN: Certificate 47 O: SafeNet OU: SafeNet West L: Redwood City ST: CA C: US emailAddress: safenet@safenet-inc.com

Certificate Response:

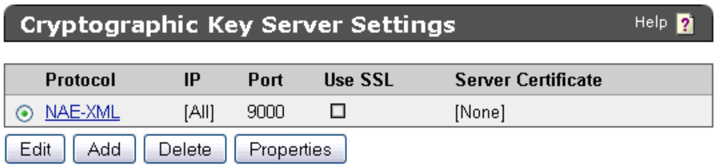
```
IENpdHkxEDAOBgNVBAoTB1NhZmVOZXQxFTATBgNVBAsTDFNhZmVOZXQgV2VzdDEX
MBUGA1UEAxMOQ2VydGlmaWNhdGUgNDcxJjAkBgkqhkiG9w0BCQEWF3NhZmVuZXRA
c2FmZW5ldC1pbmMuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+uSKevsOtOryutpmObaohlqXSf8GWXjqbyHrfdh84k7MJsOBZCPFtC3TdOdxcFK5
49/ZDq1c9UDQZbRufvEBaZC7th3E8MeUu+4fSVs+f7rma1yFM31d8eH4yqrPqQR+
K3HgPqKe9EO/Z6cpd5EaYj1dzv/2DIEFFj3mwBIjbksDSZA6ZMv6CLQ31+OhrGdM
OPmGP4/7Ro3C3BZM7UYWv87AKmQ6UVyISXEzoCtoxHeafJGYoQz7eLtiScquZYd4
UXudyW3ZZ5Tp8NjqNLlrpaTUDO7Y+WdCdGTPsXDSSdKfbRovWtTgNpQbEeF/r85q
JNauOoi6Fs5sPZrxY7QHsQIDAQABoyAwHjAJBgNVHRMEAjAAMBEGCWCGSAGG+EIB
AQQEAwIGQDANBgkqhkiG9w0BAQsFAAOCAQEALSIeKGjm2S3efjwdH5ETZfP49pFH
E7gpOn4+keweXSijOb9VvtIu7zlsTMRNYGHUGJiwhlFboURbZzL58Nqa26NSXHH9
ErjFngHGxaHsFQc4cO3Wo8Bpe+2L8T9Z3Tvl/pA4jXSy9SjkYdEWYPu7p3qZg5ka
SJ2kWXGfDO25wvkdkOsWfzbHO6kS/a+4rW51eEGQcEI6U39nS7GbZmOVoJed2zhq
oOdg4xI363R5iBJOvFcpIrfU5EHOhEOQ3/a+yMQ78GNOBGYZfCHS9vIX+nJYJcEu
D+hlEUo5EfA3nyqR75BxZ+qp7Xf/t8WWVbke6NJUonimIDMQsQD/uwcgvQ==
-----END CERTIFICATE-----
```

14 Paste the text of the signed certificate into the **Certificate Response** field.

15 Click **Save**. When you return to the main Certificate Configuration page, the certificate request is now an active certificate. It can be used in to establish SSL connections with client applications.

To configure the KMIP server settings:

1 Navigate to the Cryptographic Key Server Configuration page (Device >> Key Server).



	Protocol	IP	Port	Use SSL	Server Certificate
●	NAE-XML	[All]	9000	□	[None]

2 Click **Add** in the Cryptographic Key Server Settings section.

3 Select *KMIP* for **Protocol**.

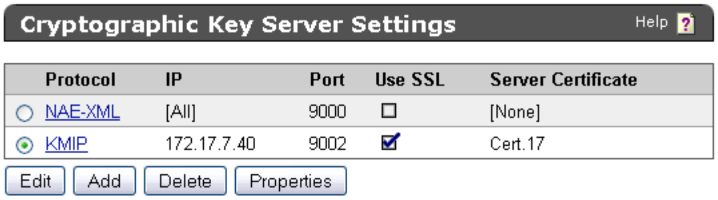
4 Select either *[All]* or a specific IP address for **IP**.

5 Select the **Port**. We recommend *9002*.

6 Select **Use SSL**. SSL is required for KMIP.

7 Select a **Server Certificate** from the drop-down list. The certificate you just created should be available for selection.

8 Click **Save**.

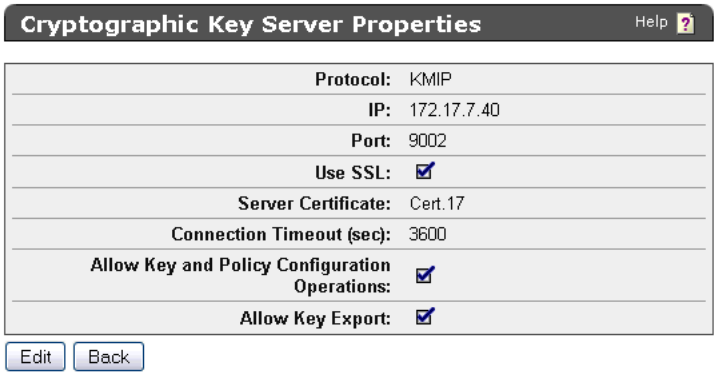


Cryptographic Key Server Settings

	Protocol	IP	Port	Use SSL	Server Certificate
○	NAE-XML	[All]	9000	□	[None]
●	KMIP	172.17.7.40	9002	☑	Cert.17

9 Select the KMIP link.

10 View the Cryptographic Key Server Properties. Click **Edit** to alter any values.



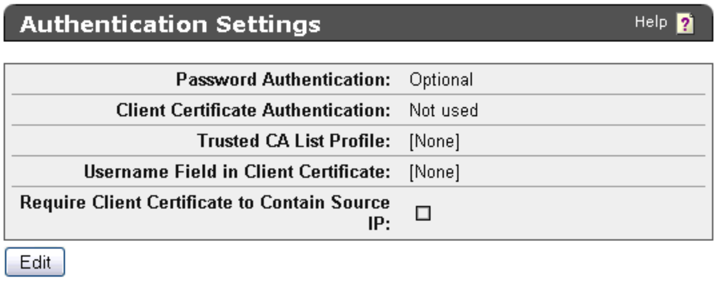
Cryptographic Key Server Properties

Protocol:	KMIP
IP:	172.17.7.40
Port:	9002
Use SSL:	☑
Server Certificate:	Cert.17
Connection Timeout (sec):	3600
Allow Key and Policy Configuration Operations:	☑
Allow Key Export:	☑

The available fields are:

- **IP** - IP address(es) on which the key server is enabled on the KeySecure. We strongly recommend that you select a *specific* IP address rather than using *[All]*. If you have multiple IP addresses available, using a single address here enables the key server to listen for traffic on only one IP address. This can greatly reduce system vulnerability to outside attacks.
- **Port** - port on which the key server is listening for client requests. We recommend 9002 for KMIP.
- **Use SSL** - required for KMIP.
- **Server Certificate** - must point to a server certificate signed by a local CA.
- **Connection Timeout (sec)** - specifies how long a client connect can remain idle before the key server begins closing them. The default value is 3600, which is also the maximum.
- **Allow Key and Policy Configuration Operations** - when enabled, the key server allows the following actions:
  - key creation and deletion
  - key import
- **Allow Key Export** - when enabled, the key server allows key export.

11 View the Authentication Settings. Click **Edit** to alter any values.



Authentication Settings

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

The available fields are:

- **Password Authentication** - determines whether you require users to provide a username and password to access the key server when using KMIP. There are three options:
  - *Not used* - (default) password authentication is not allowed; non-global sessions are not allowed.
  - *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.
- **Client Certificate Authentication** - You must enable this feature to comply with the KMIP standard. There are three options
  - *Not used* - (default) client certificate authentication is not allowed.
  - *Used for SSL session only* - clients must provide a certificate signed by a CA trusted by the KeySecure in order to establish an SSL 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 KeySecure in order to establish an SSL connection; 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 does provide a username, the key server compares the username derived from the certificate against the username in the authentication request. If the usernames match 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** - select a profile to use to verify that client certificates are signed by a CA trusted by the KeySecure. This field is only used if you select *Used for SSL session only* or *Used for SSL session and username* above. 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 is with at least one trusted CA before the key server can authenticate client certificates.
- **Username Field in Client Certificate** - specify the field from which to derive the username. This field is only used if you select *Used for SSL session and username* above. The username can come from the *UID* (user ID), *CN* (Common Name), *SN* (Surname), *E* (Email address), *E_ND* (Email without domain), or *OU* (Organizational Unit) field.

If you select *E_ND*, the key 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 key server matches against User1.

Require Client Certificate to Contain Source IP - determines if the key server expects that the client certificate presented by the client application has an IP address in the subjectAltName field. The key server obtains the IP address from the subjectAltName and compares that the source IP address of the client application; if the two IP addresses match, the key server authenticates the user. If the two IP addresses do not match, the key server closes the connection with the client.

Creating a Certificate Request for an Asymmetric Key Pair

Creating a certificate request for an asymmetric key pair is very similar to creating a server certificate. Navigate directly to the certificate creation page by selecting *Security* >> *Certificate Request*.

- Fill in all the fields and click *Generate Certificate Request*.

To edit the certificate, click on the certificate name in the list that is displayed above the certificate creation form.

Upon creation of a Certificate Request, an asymmetric key pair is generated and stored in KeySecure server. The private key is protected by the Certificate Request Password entered from the UI. When the correct Certificate Request Password is provided, the key pair and Certificate Request can be downloaded as .gz file with the private key encrypted by the Certificate Request Password in PKCS8 format. The certificate requests can be deleted from the Management Console UI.

Chapter 4

Health Check

The Health Check feature enables client applications to check the availability of the KeySecure by sending the server an HTTP request. The Health Check feature listens for requests on a port that you specify in the Health Check section of the Cryptographic Key Server Configuration page. When a request is made to the KeySecure on the port that the Health Check feature is monitoring, the server responds with one of two HTTP response codes:

- 200 OK – the KeySecure is accepting html requests
- 500 Internal Server Error – the KeySecure is unavailable

Note: The Health Check feature really only indicates that the KeySecure is running and responsive to http requests. In fact, if the KMIP server and NAE-XML servers were unavailable, after having been deleted on the Key Server page, Health Check would not reflect this fact and you might still be informed that Health Check Succeeded.

In addition to being able to configure client applications to check the availability of the KeySecure, you can also check the status of the server 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, we recommend that you send a small request. The recommended URL for accessing the Health Check feature is:

```
http://192.168.1.10:9080/
```

where 192.168.1.10 refers to the IP address and 9080 is the port on which the Health Check feature is listening for requests. If the client is unable to connect to the KeySecure or if the KeySecure is unable to respond to a request, the client should assume the server is down. Notice that the protocol is http and not https.

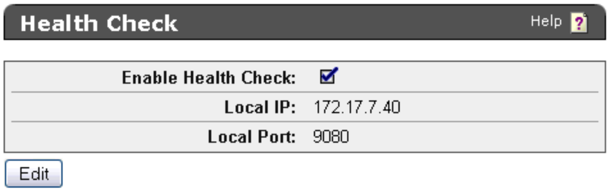
Enable Health Check

Use the Health Check section to enable the health check feature, and set the port and IP address.

To enable health check:

1 Log in to the Management Console.

2 Navigate to the Health Check section (Device >> Device Configuration >> Key Server >> Health Check).



Enable Health Check: ☑
Local IP: 172.17.7.40
Local Port: 9080

3 Select **Edit**.

4 Select **Enable Health Check**.

5 Enter the **Local IP**. This is the IP address on which you want to listen for health check requests. You can specify an individual IP address bound to the KeySecure, or you can specify *All*.

Tip: We strongly recommend that you limit the Health Check feature to a specific IP address. If you have four IP addresses bound to the KeySecure, and you enable the Health Check feature for all IP addresses, then the KeySecure listens for health check requests on four different IP addresses; whereas, if you specify a single IP address, the KeySecure listens for health check requests on only one IP address. This can greatly reduce system vulnerability to outside attacks.

6 Enter the **Local Port**. This is the port on which you want the KeySecure to listen for health check requests. The default value for this setting is 9080.

Chapter 5

KeySecure Clustering

Clustering enables multiple KeySecures to share configuration settings. With some exceptions, such as specific IP addresses for key servers or SNMP agents, 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 KeySecure and improves the failover capabilities of a high availability configuration.

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 KeySecure immediately sends a similar operation request to every other member using the cluster port.

If the replication succeeds for a device, the operation is recorded in the System Log. If the replication fails, the server waits 30 seconds and tries again. If three consecutive replications fail, the server records the failure in the System Log and sends an SNMP trap indicating that the cluster is out of sync. Once a device is out of sync, an administrator must synchronize it manually.

The following configuration settings *can* be replicated within a cluster. Items in **bold** must be replicated. You may opt not to replicate the other settings depending on your deployment strategy.

- Administrators
- **Authorization Policies**
- DNS
- IP Authorization
- Key Server
- **Keys**
- Known CAs, CRLs, and Trusted CA List Profiles
- **LDAP Server**
- Local Certificate Authorities (CAs)
- **Local Users & Groups**
- Log Signing Certificate
- Logging
- NTP
- Service Startup
- SNMP
- SSL

The following configuration settings *cannot* be replicated within a cluster:

- Network settings
- Certificates (other than the Log Signing Certificate)

Additionally, the following settings may be available depending on which features have been activated for the KeySecure:

- ProtectDB Manager
- ProtectFile Manager
- Tokenization Manager

Note: Items not replicated by the clustering feature can be replicated manually using the Backup and Restore mechanism described in Chapter 22, “Backups”.

The 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 devices from the cluster (this will effectively delete the cluster). You can then create a new cluster and add members using the new key.

The 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 devices 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 section of the Cluster Configuration page *for every member of the cluster*. You can do this if you forget the original password, for example. 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 that password.

Clusters and High Availability

If you are using both clustering and the High Availability feature, you should ensure that the master and slave devices belong to the same cluster. As part of the same cluster, the master and slave will automatically synchronize. This ensures that when the slave comes online, its configuration is current.

Multi-keys

Regardless of your cluster settings, multi-keys will not be replicated to KeySecures that are running software version 4.3 and older. This is because the multi-key functionality is not enabled on those devices.

Local Certificate Authority Replication

The cluster feature enables 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, a KeySecure inherits a new list of local CAs from the cluster. The device'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.

Note: When upgrading from a previous release, local CA replication is disabled by default.

Automatic Synchronization Backups

Prior to each synchronization, and when a KeySecure joins a cluster, the Key Server 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, and HHMMSS is the time.

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.

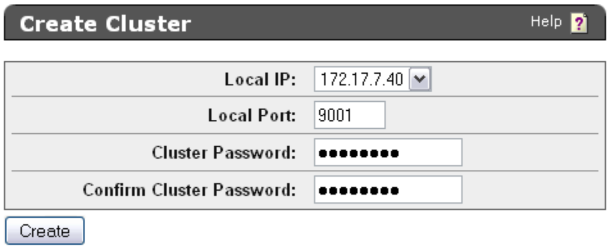
Creating a Cluster

You create a cluster on one KeySecure and then join other members to that cluster. To create a cluster:

1 Select a KeySecure to be the first cluster member. This device cannot currently be a member of a cluster.

2 Log in to the Management Console as an administrator with Cluster access control.

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



Local IP:	172.17.7.40
Local Port:	9001
Cluster Password:	●●●●●●●●●
Confirm Cluster Password:	●●●●●●●●●

4 Enter the **Local IP**. If the device has multiple network interfaces, the pull-down menu lists all available interfaces.

5 **Enter the Local Port**. The cluster port (typically 9001) must be different from the key server port (typically 9000).

6 Enter the **Cluster Password**. The requirements for the cluster password depend on your Password Management Settings. For information on password requirements, refer to Chapter 16, “Password Management”.

7 Click **Create Cluster**. A new cluster key is internally created, and this device appears in the Cluster Members list.

8 By default, the cluster replication settings will be compatible with KeySecure version 4.4 and above.

9 Click **Edit** to view or edit the entire list of replicated settings.

Configuring the Replication Settings

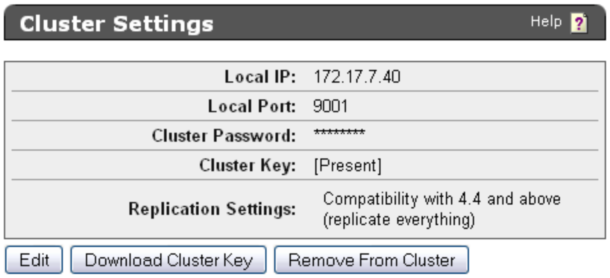
The Replication Settings determine which configuration settings are shared by the cluster members. Upon saving these settings on one device, that Key Server will push the new configuration out to the other cluster members. *No automatic synchronization backup will occur.* You should edit the replication settings only on a device that has a configuration you want to replicate.

To configure the replication settings for a cluster:

1 Select a KeySecure with configuration settings that you can push out to other cluster members.

2 Log in to the Management Console as an administrator with Cluster access control.

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



Local IP:	172.17.7.40
Local Port:	9001
Cluster Password:	********
Cluster Key:	[Present]
Replication Settings:	Compatibility with 4.4 and above (replicate everything)

4 Click **Edit**.

5 Select an option for the **Replication Settings** field. Once you set the **Replication Settings** field and return to the edit mode of the Cluster Settings section, the items checked under Advanced Settings will reflect your current configuration. Available values are:

- Compatibility with 4.4 and above - replicates all configuration settings.
- Compatibility with 4.2 & 4.3 - replicates keys, Authorization Policies, Local users & Groups, and LDAP Server, and ProtectDB settings.
- Compatibility with 4.0 & 4.1 - replicates keys, Authorization Policies, Local users & Groups, and LDAP Server settings.
- Advanced Settings - You can select individual configuration settings to replicate.

Note: Certificates, with the exception of the Log Signing Certificate, cannot be replicated within a cluster. However, if you are replicating Key Server settings, and those settings include the use of a specific server certificate, you must create a certificate with that name on each cluster member.

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

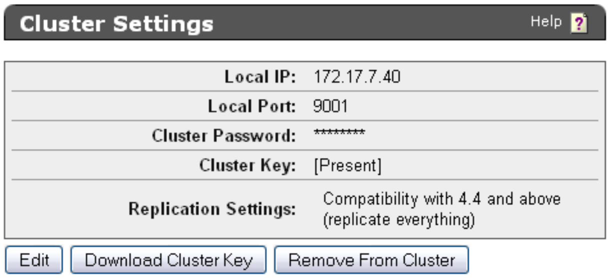
Joining a Cluster

You must know the IP and port number of another member of the cluster, and you need a local copy of the cluster key and the cluster password. A device can be a member of only one 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 Navigate to the Cluster Settings section of the Cluster Configuration page (Device >> Cluster).



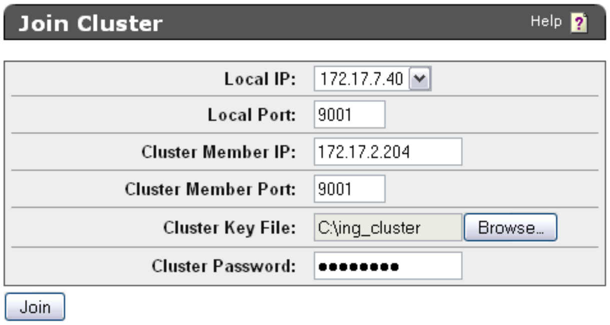
Cluster Settings

Local IP:	172.17.7.40
Local Port:	9001
Cluster Password:	********
Cluster Key:	[Present]
Replication Settings:	Compatibility with 4.4 and above (replicate everything)

3 Click **Download Cluster Key** to save the key on your local file system. The cluster key contains authentication information used when passing information between cluster members.

4 Write down the **Local IP** and **Local Port** values.

5 Log in to the KeySecure that you want to add to the cluster and navigate to Join Cluster section on the Cluster Configuration page.



Local IP:	172.17.7.40
Local Port:	9001
Cluster Member IP:	172.17.2.204
Cluster Member Port:	9001
Cluster Key File:	C:\ing_cluster
Cluster Password:	●●●●●●●●●

6 Enter the **Local IP**. If the device has multiple network interfaces, the pull-down menu lists all available interfaces.

7 Enter the **Local Port**. The cluster port (typically 9001) must be different from the key server port (typically 9000).

8 Enter the IP and port values from step 4 in the **Cluster Member IP** and **Cluster Member Port** fields.

9 Enter the **Cluster Password**.

10 Enter the location of the cluster key in the **Cluster Key** field. Click **Browse** to locate the downloaded cluster key file in your file system.

11 Click **Join Cluster**. After clicking this button you are asked to synchronize with the specified cluster member. Click **Confirm** to synchronize now, or **Cancel** if you want to synchronize manually later on. In either case, the local device becomes a member of the cluster.

WARNING: Synchronizing the local device 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 device, you can use the backup and restore features to copy them to another KeySecure before synchronizing the local device.

Important! When adding a device running a higher software version than the existing cluster members, you will have to edit the cluster settings to ensure that the replication settings are correct. For more information, see “Configuring the Replication Settings” on page 37.

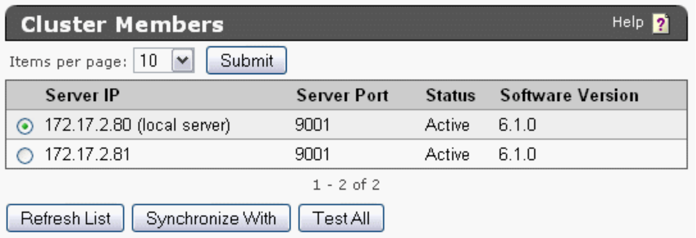
12 Delete the cluster key from the local file system on your workstation.

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).



	Server IP	Server Port	Status	Software Version
●	172.17.2.80 (local server)	9001	Active	6.1.0
○	172.17.2.81	9001	Active	6.1.0

3 Click **Refresh List** to update the list of server IPs that are members of this cluster. This will not update the **Status** of each cluster member.

4 Click **Test All** to verify the device's connection to all the members of this cluster. This will update the **Status** for each cluster member.

5 View the server **Status**. Valid values are:

- *Active* - connected to the cluster.
- *Inactive* - not connected to the cluster
- *Pending Refresh* - the exact status of the device is unknown either because the device is currently synchronizing with the cluster or because there was no direct communication with that server. View the system log for information about synchronizations.

6 Select the server from which you will copy configuration settings.

7 Click **Synchronize With** and confirm this action. As part of the synchronization, the Key Server will create an automatic synchronization backup before installing the new configuration.

WARNING: Synchronizing the local device 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 device, you can use the backup and restore features to copy them to another KeySecure before synchronizing the local device.

Setting up SSL in a Cluster

When using SSL in a cluster, the replication settings must include Key Server settings and all cluster members must use a server certificate with the same name, as indicated on the Key Server Settings section. The contents of those server certificates, however should be unique.

To configure SSL for a cluster:

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

2 Navigate to the Create Certificate Request section on the Certificate and CA Configuration page (Device >> Cluster).

3 Create a certificate request.

4 Repeat steps 1, 2, and 3 for each device in the cluster. *Use the same name for each certificate request.*

5 Sign all of the certificate requests with the same CA. You can use a local CA on one of your devices, or another CA within your organization's PKI.

6 Install each signed certificate on the appropriate device.

7 Select a KeySecure with configuration settings that you can push out to other cluster members.

8 Log in to that device's Management Console as an administrator with Key Server access control.

9 Navigate to the Key Server Settings section on the Key Server Configuration page.

10 Select **Use SSL** and set **Server Certificate** to the newly created certificate.

11 Navigate to the Cluster Settings section on the Cluster Configuration page.

12 Set the **Replication Settings** field so that Key Server settings are replicated across the cluster by selecting Compatibility with 4.4 and above, or using Advanced Settings. The new SSL configuration will be replicated along with the other Key Server settings.

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

Removing a Device from a Cluster

To remove a device from a cluster:

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

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

3 Click **Remove From Cluster**. The device is removed from the cluster. The cluster key is also removed from the device.

To delete an entire cluster, you must remove each device individually. If this is the last device 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 device, a new cluster key is generated.

Removing an Invalid Device from a Cluster

If a member of a cluster is bad, the usual method described above to remove a device from a cluster does not work. To make changes with a dead node, use the following command to remove the node.

```
cluster remove device <ip> <port>
```

Issue the command from any cluster member node. For example, the following command removes 172.17.17.210:9001 from a cluster.

```
(config)# cluster remove device 172.17.17.210 9001
```

Upgrading a Cluster

A cluster must be upgraded ***by updating the release on one device at a time***. Once all of the devices are running the new software, you can configure the replication settings as needed.

Create a backup before upgrading.

Tip: Do not make other configuration changes while upgrading a cluster.

To upgrade a cluster to the new release, perform the following steps:

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

2 Remove one node from the cluster.

3 Upgrade the software on that device to the newer release.

4 Rejoin that node to the cluster.

You will need to repeat steps 1 through 4 for each member of the cluster.

After all nodes are updated, you can configure the replication settings by working with one member of the cluster. For more information, see “Configuring the Replication Settings” on page 37.

Deleting a Cluster

A cluster is deleted when the last member is removed from the cluster.

To delete a cluster:

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

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

3 Click **Remove From Cluster**.

4 Repeat these steps for each member of the cluster.

Retry Key Replication across a Cluster

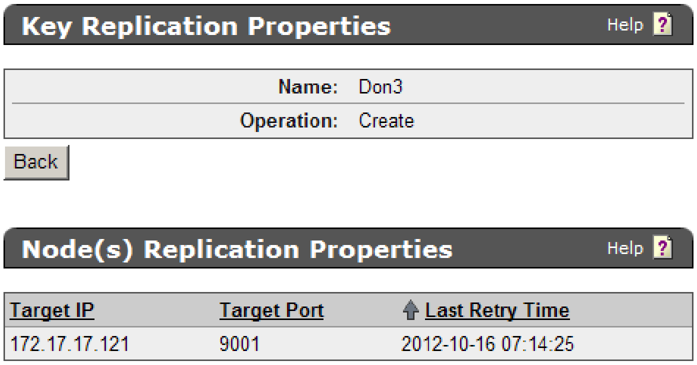
When your attempt to replicate key information across a cluster fails (for example, when synchronization or resynchronization fail to replicate a key), you may have the option to re-try the replication. Information about the most recent key replication operation you wanted to perform is stored for you. You can see in a single page which key replication operations failed, and use this information to retry the replication.

You can replicate attempts to create a key, modify a key, or delete a key.

To attempt the key replication operation again, use Retry Replication.

To retry replication:

1. Log in the Management Console of the device from which the key replication was attempted as an administrator with Cluster access control.
2. Navigate to the Keys to Replicate Again section of the Cluster Retry Replication page (Device >> Cluster >> Retry Replication).
3. Click a radio button to select the key you want to replicate, then click Retry. If you first want to see the details of the Retry key operation before you commit, click Properties. The Retry Replication Properties page appears. This shows the Key Replication item name and the operation you can replicate. Click the Back button to return to the Cluster Retry Replication page.



Key Replication Properties

Name: Don3

Operation: Create

Node(s) Replication Properties

Target IP	Target Port	Last Retry Time
172.17.17.121	9001	2012-10-16 07:14:25

4. Repeat the step above for each key replication operation you want to perform.

Be aware that each retry is an attempt; successful attempts will be confirmed.

Chapter 6

Date, Time and NTP

This feature enables you to set the system date and time, and configure NTP servers. The Network Time Protocol (NTP) is a protocol by which computers on a network synchronize their clocks against an NTP server. The KeySecure allows you to synchronize a clock manually or at regular intervals.

When the KeySecure attempts to synchronize its clock against the NTP server(s), one of three outcomes is possible:

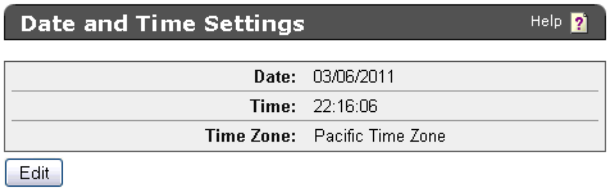
- If the clock on the KeySecure is successfully synchronized, and the difference between the time on the KeySecure and the NTP server(s) is less than 0.5 seconds, the time on the KeySecure is gradually *slewed* to the real time.
- If the clock on the KeySecure is successfully synchronized, and the difference between the time on the KeySecure and the NTP server(s) is greater than 0.5 seconds, the time on the KeySecure is immediately *stepped* to the real time. This event is recorded in the System Log.
- If an error prevented the KeySecure from synchronizing its clock, an error message is recorded in the System Log.

Note: Synchronizing the time causes the Key Server to restart if the time change is greater than one minute. While restarting, the Key Server is unavailable for up to 60 seconds.

Setting the Date and Time on the KeySecure

To set the date and time on the KeySecure:

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 & Time Configuration page (Device >> Date & Time).



Date: 03/06/2011
Time: 22:16:06
Time Zone: Pacific Time Zone

3. Click **Edit**. You cannot edit the KeySecure **Date** and **Time** fields when NTP is enabled.
4. Modify the **Date**, **Time**, and **Time Zone** fields as follows:
   - **Date** - Use the drop-down lists to set the month, day, and year.
   - **Time** - Use the drop-down lists to define the current hour, minutes, and seconds.
   - **Time Zone** - Use the drop down list to select a time zone.
5. Click **Save**.

If you adjust the date and time settings forward, any log rotations and automated backups scheduled for a time that is skipped will not occur. You can rotate such logs manually using the Log Viewer page.

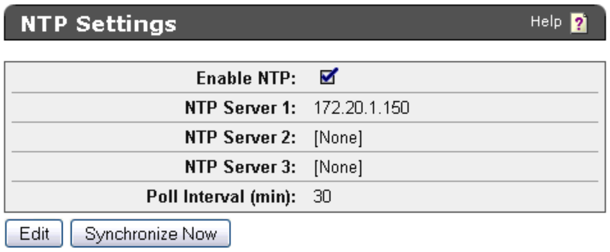
If you adjust the date and time settings backwards, any log rotations scheduled for the repeated time period will occur again.

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 & Time Configuration page (Device >> Date & Time).


NTP Settings

Enable NTP:	☑
NTP Server 1:	172.20.1.150
NTP Server 2:	[None]
NTP Server 3:	[None]
Poll Interval (min):	30

3 Click **Edit**.

4 Select **Enable NTP** to enable the feature. Once enabled, you cannot manually set the time or date on the KeySecure. You can still modify the timezone.

5 Enter the IP addresses or hostnames of the servers in the **NTP Server** fields. You can list as many as three NTP servers. When clocks are synchronized, the KeySecure polls the list of servers, in order, and uses the first valid NTP response returned to determine the correct time.

6 Enter the **Poll Interval**, in minutes. This is the length of time between consecutive pools. 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 KeySecure rounds down to the nearest multiple of 5.

7 Click **Save**.

Manually Synchronizing with an NTP Server

The KeySecure will automatically synchronize 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 & Time Configuration page (Device >> Date & Time).

3 Click **Synchronize Now** to synchronize the clock on the KeySecure immediately. The **Synchronize Now** button can be used even when automatic NTP synchronization is not enabled.

Chapter 7

Network Interfaces

The Network Configuration page enables you to configure the KeySecure network interface list and create VLAN tagged interfaces.

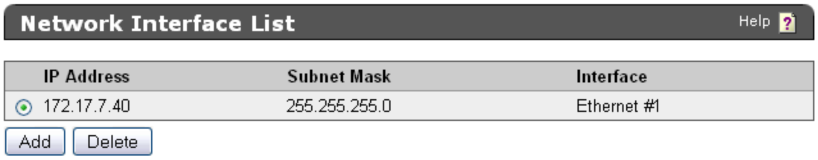
Configure Network Interfaces

Note: The first network interface (Ethernet #1) was configured as part of the installation process. Use the Network Interface List section to configure additional interfaces, or to reconfigure Ethernet #1.

To configure a network interface:

1 Log in to the Management Console.

2 Navigate to the Network Interface List section of the Network Configuration page (Device >> Network).



	IP Address	Subnet Mask	Interface
◉	172.17.7.40	255.255.255.0	Ethernet #1

3 Click **Add**.

4 Enter the **IP Address**.

5 Enter the **Subnet Mask**.

6 Enter the **Interface**. The number of interfaces on the KeySecure depends on the model. Network interfaces are located on the back of the device.

There can be an option for a **Virtual Interface**. Virtual interface IPs are not bound to any physical interfaces. On a KeySecure with multiple NICs, clients can ensure better connectivity with the NAE server by using a virtual IP, such as

```
eth0: 172.17.17.120
eth1: 172.17.17.121
vip1: 172.17.17.130
```

If eth0 is having some issues and the client uses x.x.17.120, it cannot reach the server. It has to change the server IP to 17.121 to connect. But if the client is configured with the virtual 17.130 interface, the connection goes through if eth1 is working.

Better security can be achieved using virtual interfaces. Applications (clients) can be given different VIPs. If one is compromised, the others can still be used safely on the NAE server and Web server Management Console.

7. Click **Save**.

Changing an Existing IP Address

To change an IP address, there are two steps.

1. Add the new IP address, as described in the preceding section.
2. Delete the existing IP address by selecting it in the Network Interface List shown above and then clicking **Delete**.

   Note: If the existing IP address is referenced by a server function like clustering or a key server (KMIP or NAE-XML), remove or change those references before deleting the old IP address.

Changing the IP Address on an Existing SSKM VM

On the KeySecure, use the command line interface (CLI) to change the IP address of an existing SSkm VM with the two commands shown below. Specify the new IP address and the existing interface in the interface command. For more information on these commands, see chapter 19, *SSKM Interface*, in the *KeySecure Command Line Interface Reference Guide*.

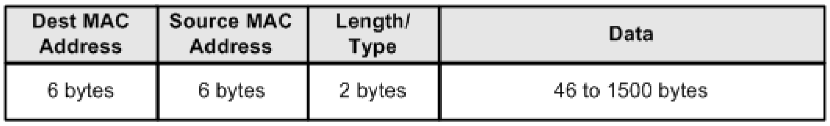
```
sskm halt
```

```
sskm interface <ip address> <interface>
```

Important! After issuing these two commands, **reboot** the machine that holds the SSKM VM. Restarting the SSKM VM is not sufficient after changing the IP address; a reboot is required. After rebooting, the VM restarts automatically.

Configure VLAN Tagged Interfaces

The KeySecure can accept standard 802.3 Ethernet frames and 802.1Q Ethernet frames. In a typical Ethernet network, frames are no larger than 1514 bytes (excluding the checksum and preamble). The format of a frame in such a network is shown here:

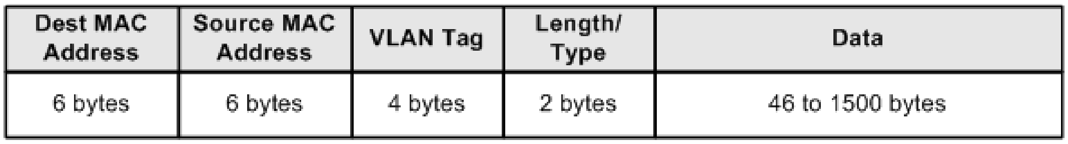


Dest MAC Address	Source MAC Address	Length/ Type	Data
6 bytes	6 bytes	2 bytes	46 to 1500 bytes

Field	Description
Dest MAC Address	Identifies the station or stations that should receive the frame.
Source MAC Address	Identifies the station where the frame originated.

Field	Description
Length/Type	If this field is less than or equal to 1500, then it indicates the number of bytes in the subsequent Data field. If the value of this field is greater than or equal to 1536, then the it indicates protocol type.
Data	Contains the data transferred from the source station to the destination station or stations. The maximum size of this field is 1500 bytes.

The 802.1Q specification established a standard method for inserting Virtual LAN (VLAN) membership information into Ethernet frames. An extra field with a size of 4 bytes is inserted into VLAN Tagged ethernet frames immediately after the Source MAC Address. The format of a frame in such a VLAN Tagged Ethernet network is shown here:



Dest MAC Address	Source MAC Address	VLAN Tag	Length/ Type	Data
6 bytes	6 bytes	4 bytes	2 bytes	46 to 1500 bytes

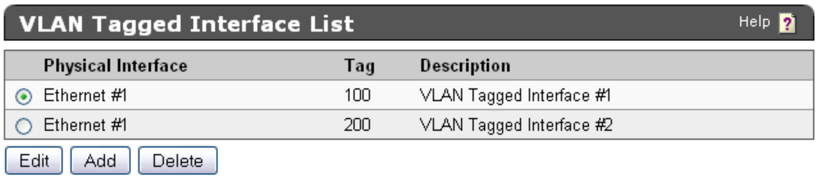
The VLAN Tag field uniquely identifies the VLAN to which the Ethernet frame belongs.

VLAN tagged interfaces behave in exactly the same way as non–VLAN tagged interfaces. You can assign a unique IP address to a VLAN tagged interface, just as you can to a non–VLAN tagged interface, and you can use that IP address wherever you have to supply a local IP address.

To configure a VLAN tagged interface:

1 Log in to the Management Console.

2 Navigate to the Network Configuration page (Device >> Network).



VLAN Tagged Interface List

Physical Interface	Tag	Description
● Ethernet #1	100	VLAN Tagged Interface #1
○ Ethernet #1	200	VLAN Tagged Interface #2

3 Click **Add** to create a VLAN tagged interface. You must then enter the following values:

- **Physical Interface** - select the physical interface on which you want to create the VLAN tagged interface
- **Tag** - supply a VLAN group number between 2 and 4094.
- **Description** - enter an optional description of no more than 256 characters.

You can have a maximum of 16 VLAN tagged interfaces on a KeySecure.

4 Click **Delete** to remove a VLAN tagged interface. You cannot delete a VLAN tagged interface if it is being used elsewhere in the environment. For example, you cannot delete a VLAN tagged interface if an IP address is bound to the VLAN tagged interface.

Chapter 8

Gateways & Routing

The Network Configuration page enables you to configure the default gateway list, select the interface to use for outgoing connections, and configure a static route list.

Configure the Default Gateway

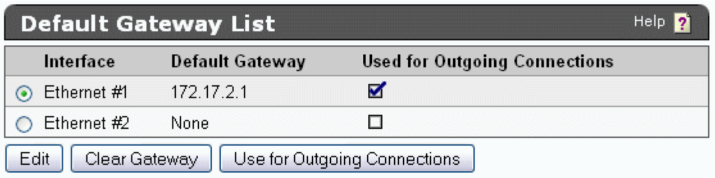
The Default Gateway List section of the Network Configuration page provides a view of the default gateways used by the KeySecure for routing. A default gateway is used to identify the IP address to which all packets destined for a remote network are routed. One default gateway can be associated with each physical interface. Most network configurations require only a single default gateway. Multiple default gateways might be necessary for network configurations where multiple interfaces of the KeySecure are connected to the network.

Note: The **Default Gateway** was created during the KeySecure installation.

To configure the default gateway:

1 Log in to the Management Console.

2 Navigate to the Default Gateway List section of the Network Configuration page (Device >> Network >> Gateways & Routing). The number of interfaces displayed depends on the device hardware itself. All available interfaces are listed - even if they are not used or configured.



	Interface	Default Gateway	Used for Outgoing Connections
●	Ethernet #1	172.17.2.1	☑
○	Ethernet #2	None	□

3 Select **Edit**.

4 Edit the Default Gateway field, if necessary. A blank Default Gateway indicates that no default gateway exists. The Default Gateway address cannot be a broadcast of network address as determined by the IP addresses on the system.

5 Select **Save.**

6 Select Clear Gateway to remove a default gateway.

7 Select **Used for Outgoing Connections** to use the selected interface for outgoing connections initiated by the KeySecure. If this gateway fails, all outgoing connections initiated by the KeySecure will fail. When using multiple interfaces, you must indicate which interface will handle outgoing connections. For devices with one gateway, that interface is automatically used for outgoing connections.

Examples of Default Gateway Configuration

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 #1             172.17.7.1        yes
Ethernet #2             none              no
```

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 Ethernet #2 interface.

All connections initiated by the KeySecure leave from 172.17.7.1.

Example 2

```
Interface               Default Gateway   Used for Outgoing Connections
---------------------------------------------------------------------------
Ethernet #1             none              no
Ethernet #2             10.20.41.1        yes
```

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 KeySecure leave from 10.20.41.1.

Example 3

```
Interface               Default Gateway   Used for Outgoing Connections
---------------------------------------------------------------------------
Ethernet #1             172.17.7.1        yes
Ethernet #2             10.20.41.1        no
```

All responses to incoming packets destined for IPs bound to Ethernet #1 leave from 172.17.7.1. All responses to incoming packets destined for IPs bound to Ethernet #2 leave from 10.20.41.1.

If packets destined for Ethernet #1 are received by the Ethernet #2 interface, the response packets will still leave from 172.17.7.1. Likewise, any packets destined for Ethernet #2 that are received by the Ethernet #1 interface will still leave from 10.20.41.1.

If one of the default gateways should fail, the other interface is not affected. For example, if 172.17.7.1 fails, IPs bound to Ethernet #1 will be unreachable - but the Ethernet #2 interface will operate normally.

All connections initiated by the KeySecure (regardless of destination) leave from 172.17.7.1, because 'Used for Outgoing Connections' is configured for that gateway. If this gateway fails, all outgoing connections fail.

Example 4

```
Interface                Default Gateway   Used for Outgoing Connections
---------------------------------------------------------------------------
Ethernet #1              172.17.7.1        yes
Ethernet #2              10.20.41.1        no
```

This configuration is the same as example 3, but in this scenario there are some hosts and networks that are not reachable through 172.17.7.1. Most often these would be private or secure sub-networks. In such a case you would add a static route out of 10.20.41.1 so that the KeySecure can reach the additional hosts or networks. The static route is shown below:

```
IP Address               Subnet Mask       Gateway            Interface
------------------------------------------------------------------------
66.230.200.0             255.255.255.0     10.20.41.1         Ethernet #2
```

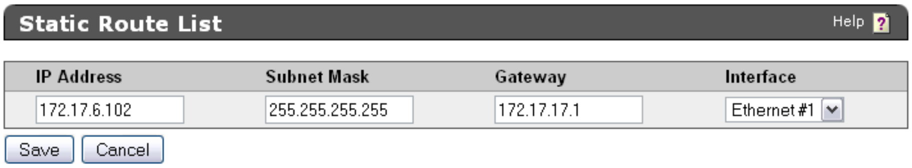
Configure a Static Route

The Static Route features allows you to explicitly specify a route from the KeySecure to another network device. Such a route is stored in the routing table on the KeySecure.

To configure the default gateway:

1 Log in to the Management Console.

2 Navigate to the Static Route List section (Device >> Network >> Gateways & Routing).



Static Route List

IP Address	Subnet Mask	Gateway	Interface
172.17.6.102	255.255.255.255	172.17.17.1	Ethernet #1

3 Click Add.

4 Enter an IP Address. This is the address you a trying to reach with this route. Valid values are IP or network addresses matching the specific Subnet Mask.

5 Enter the Subnet Mask associated with the IP Address/Network needed to identify the destination. Valid values are any subnet mask address.

6 Enter the Gateway used to reach the destination. A static route that does not include 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 IP address.
- The gateway must be reachable based on the network routes created by the addition of an IP address to the system.
- The gateway address cannot be a broadcast or network address as determined by the IP 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.

7 Click **Save**.

Chapter 9

Hostname & DNS

The Network Configuration page enables you to set the KeySecure hostname and connect to any DNS servers in your network.

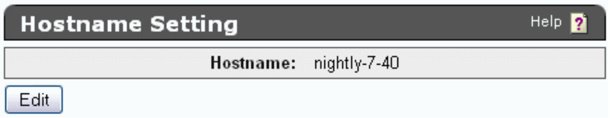
Set the Hostname

The hostname, which identifies each KeySecure in a network, is the unique name assigned to a KeySecure. It is initially assigned during installation.

To set the hostname:

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

2 Navigate to the Hostname Setting section of the Network Configuration page (Device >> Network >> Hostname & DNS).



Hostname Setting

Hostname: nightly-7-40

3 Click **Edit**.

4 Enter the **Hostname**. This string cannot be longer than 64 characters.

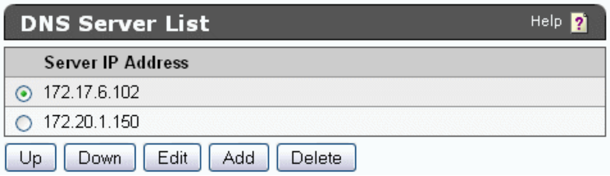
5 Click **Save**.

Configure DNS Server

Domain Name Service (DNS) settings are viewed and modified on the DNS Server List section on the DNS tab of the Network Configuration page. From this section, the user can opt to review the server list or use the buttons to prioritize, add, modify, or remove a DNS server.

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

2 Navigate to the Hostname Setting section of the Network Configuration page (Device >> Network >> Hostname & DNS).



DNS Server List

	Server IP Address
●	172.17.6.102
○	172.20.1.150

3 Click Edit or Add.

4 Enter a **Server IP Address** and select **Save**.

5 Use the **Up** and **Down** buttons to set the order in which the servers will be queried by the KeySecure.

Chapter 10

Network Interface Port Speed & Duplex

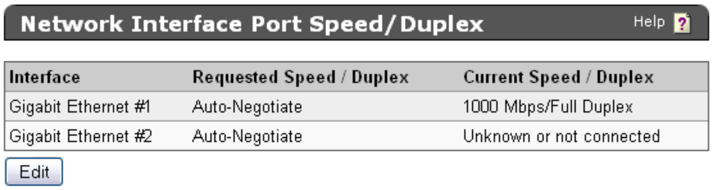
The Network Configuration page enables you to configure the port speed and duplex for the KeySecure network interfaces.

Configure Network Interface Port Speed/Duplex

The KeySecure 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 KeySecure 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.

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

2 Navigate to the Network Interface Port Speed/Duplex section of the Network Configuration page (Device >> Network >> Port Speed).



Interface	Requested Speed / Duplex	Current Speed / Duplex
Gigabit Ethernet #1	Auto-Negotiate	1000 Mbps/Full Duplex
Gigabit Ethernet #2	Auto-Negotiate	Unknown or not connected

3 Click **Edit**.

4 Select one of the following options for each interface:

- Auto-Negotiate
- 10 Mbps/Half Duplex
- 10 Mbps/Full Duplex
- 100 Mbps/Half Duplex
- 100 Mbps/Full Duplex
- 1000 Mbps/Full Duplex

5 Click **Save**.

WARNING! 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 KeySecure. Potential performance degradation can result if these settings do not match. We recommend that you leave the port speed and duplex setting on the KeySecure at Auto-Negotiate unless you know the settings of the network device it is communicating with.

Note: When a switch forces a port speed and the KeySecure is set to Auto-Negotiate, the KeySecure defaults to Half Duplex. Thus, when you force Full Duplex on the switch and leave the KeySecure set to Auto-Negotiate, the KeySecure may be unable to negotiate a connection with other network devices.

Chapter 11

High Availability

The High Availability feature provides failover functionality between two KeySecures. This mechanism is based on the failover protocol VRRP defined in RFC 2338, which you can find here: http://www.ietf.org/rfc/rfc2338.txt.

The high availability feature enables you to configure two KeySecures such that if one device goes offline for some reason, all future traffic to the offline device is automatically sent to the second device. The first device, the master, is normally the active device and receives the network traffic. The other device, the slave, is normally the passive device. It receives no traffic except for the VRRP messages sent by the master every minute.

Failover occurs when the master is unable to send VRRP messages. When this occurs, the slave assumes the role of the active device and receives all of its network traffic. This is a *total* failover. If the master has multiple network interfaces, all interfaces fail over to the slave.

As soon as the master is able to fulfill client traffic, failback occurs: control of network traffic shifts back from the slave to the master.

Failover and failback are mostly invisible to the client. When this feature is enabled, KeySecure clients should communicate with the high availability interface, a virtual IP created on the Network Configuration page and shared by the master and slave. The failover is not totally invisible. The slave does not replicate user connections, so all connections that were active on the master when the device went offline must be re-established on the slave. Your client application must be capable of handling this scenario.

The master and slave are members of a virtual group. They share the same Group IDs for each available network interface. The VRRP documentation refers to these values as virtual router identifiers (VRIDs). Both members of the virtual group also share the same virtual IP address, defined in the KeySecure Management Console as a High Availability Interface.

The KeySecure supports single arm configurations and dual–home configurations. The KeySecure does not support hybrid single–arm/dual home configurations.

Note: High Availability is not supported on the k150.

Configure High Availability

Configuring the high availability feature requires that you configure a high availability interface on two KeySecures: the master and the slave. Then, for both devices, you must also enable and configure the high available settings. The full set of instructions are below, you need to perform these steps on both the master and the slave.

Note: The master and slave must be on the same LAN segment because VRRP messages are not routable. High availability is not available for devices on different LAN segments.

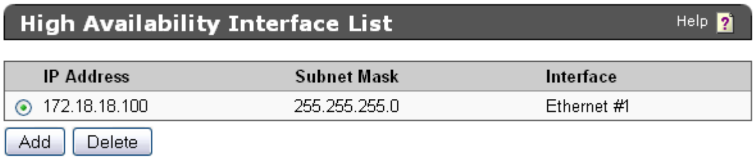
Prerequisites:

- The master and slave must have identical configurations. You accomplish this by clustering the two devices. For more information on clustering, please see Chapter 5, “KeySecure Clustering”.
- Configure the related switch for IP multicast support in order to eliminate unnecessary packet proliferation. Most switches have this disabled by default and simply broadcast multicast packets on all ports, thus eliminating the cost-effectiveness of multicasting.
- High Availability is not supported on the k150.

To configure a high availability interface:

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

2 Navigate to the High Availability Interface List on the Network Configuration page (Device >> Network).


High Availability Interface List

	IP Address	Subnet Mask	Interface
●	172.18.18.100	255.255.255.0	Ethernet #1

3 Click **Add**.

4 Enter the IP address. This is the virtual IP that clients must use to communicate with the KeySecure in order to benefit from the high availability feature. This value must be the same for both the master and the slave. Be sure to use an IP that otherwise does not exist in your network.

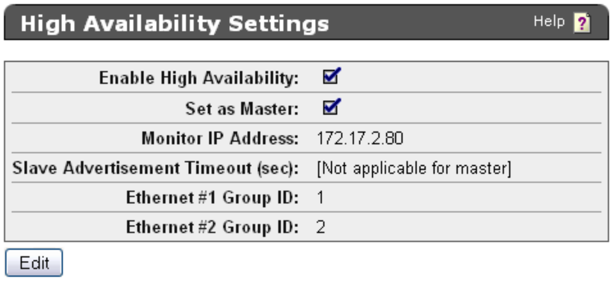
5 Enter the **Subnet Mask**.

6 Enter the **Interface**. The number of available interfaces depends on the KeySecure model. Network interfaces are located on the back of the device.

7 Click **Save**.

To configure the high availability settings:

1 Navigate to the High Availability Interface Settings section (Device >> Network >> High Availability).


High Availability Settings

Enable High Availability:	☑
Set as Master:	☑
Monitor IP Address:	172.17.2.80
Slave Advertisement Timeout (sec):	[Not applicable for master]
Ethernet #1 Group ID:	1
Ethernet #2 Group ID:	2

2 Click **Edit**.

3 Select **Enable High Availability**.

4 Select **Set as Master** to set one device as the master. On the slave device, leave this field unselected.

5 Select a value in **Monitor IP Address**. This is the KeySecure IP address used to create a connection to the other device in the high availability group. This connection is used to monitor device status.

6 Enter a value in the **Slave Advertisement Timeout (sec)** field. This is the time that must elapse before the slave assumes the master is inactive and thus takes over control and become the active device. The default value for this field is 3 seconds and the field is only set on the slave.

7 Enter a value for the **Ethernet Group ID**. KeySecures that share these values are part of the same virtual group, which is required for the master-slave association. This field allows you to specify the VRIDs for each interface. The values must be different for each interface, but these entries must be identical on the master and the slave. The default group id matches the interface number. You can change from the default value, but the ID must be a number between 1 and 255.

If you are using the VRRP protocol for other devices that share the LAN with the KeySecure, it is necessary to carefully manage the VRIDs in order to avoid collisions.

8 Click **Save**.

Chapter 12

IP Authorization

The IP Authorization feature enables you to specify which IP addresses are permitted to connect to the KeySecure and which services those IP addresses may access.

Once enabled, the KeySecure 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.

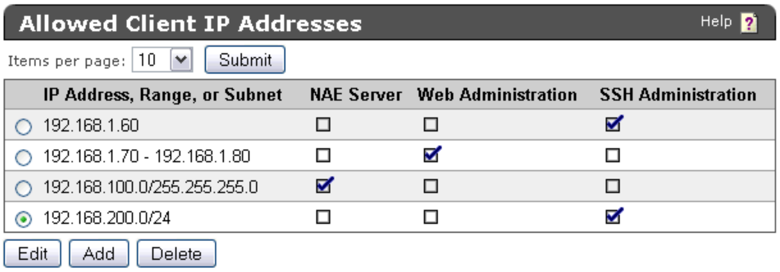
Configure the IP Authorization Feature

IP Authorization settings are viewed and modified from the IP Authorization tab on the Network Configuration page. Use the IP Authorization Settings section to view and set these settings for your KeySecure.

To configure the IP Authorization feature:

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).



Allowed Client IP Addresses

Items per page: 10

	IP Address, Range, or Subnet	NAE Server	Web Administration	SSH Administration
○	192.168.1.60	□	□	☑
○	192.168.1.70 - 192.168.1.80	□	☑	□
○	192.168.100.0/255.255.255.0	☑	□	□
●	192.168.200.0/24	□	□	☑

3 Click **Add**.

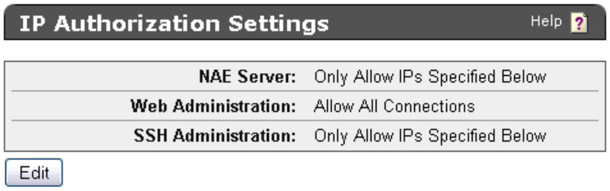
4 Enter a single IP address (e.g., 192.168.1.60), a range of addresses (e.g., 192,168.1.70 - 192.168.1.80), or a subnet (e.g., 192.168.100.0/255.255.255.0, or 192.168.200.0/24) in the **IP Address, Range, or Subnet** field.

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.

5 Select the services that will be available to this client using the **Key Server**, **Web Administration**, and **SSH Administration** fields.

Note: 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. Use the **Add** and **Delete** buttons when needed.
8. Click **Edit** on the IP Authorization Settings section.



NAE Server:	Only Allow IPs Specified Below
Web Administration:	Allow All Connections
SSH Administration:	Only Allow IPs Specified Below

9. For each service select either *Allow All Connections* to grant access to all clients or *Only Allow IPs Specified Below* to grant access to only the clients listed in the Allowed Client IP Addresses section *with that service selected.*
10. Click **Save**.

Note: When updating this feature from the Management Console, the system ensures that the current administrator IP address maintains its web administration permissions. When updating this feature from the CLI, the system ensures that the active SSH administration permissions remain intact.

Chapter 13

SNMP

The Simple Network Management Protocol (SNMP) 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; and the MIB defines what kind of information 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 KeySecure supports all three versions of SNMP.

Note: There are many different versions of SNMPv2. The KeySecure 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 a SafeNet 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 KeySecure 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 User–based Security Model (USM), which consists of two important services: authentication and privacy. Additionally, SNMPv3 enhanced the existing View Access Control Model (VACM).

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.

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 with the DES algorithm. The sender encrypts all messages with the DES algorithm and its secret key, and sends the message to the receiver, who decrypts it using the DES algorithm and the same secret key.

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.

Configuring SNMPv1/v2 on the KeySecure

The KeySecure supports all three versions of SNMP. From a configuration standpoint, SNMPv1/v2 are treated as a unit, and SNMPv3 is treated separately. SNMP requires an agent, a community, and a management station.

Please note that SafeNet SNMP agent is capable of providing the following SNMP functionality:

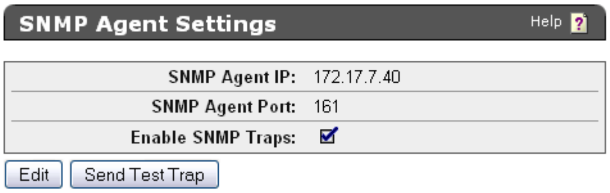
- it enables the NMS to access the MIBs on the KeySecure.
- it initiates trap messages to the NMS.

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

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

1 Log in to the KeySecure

2 Navigate to the SNMP Configuration page (Device >> SNMP).



SNMP Agent Settings

SNMP Agent IP:	172.17.7.40
SNMP Agent Port:	161
Enable SNMP Traps:	☑

3 Click **Edit** in the SNMP Agent Settings section.

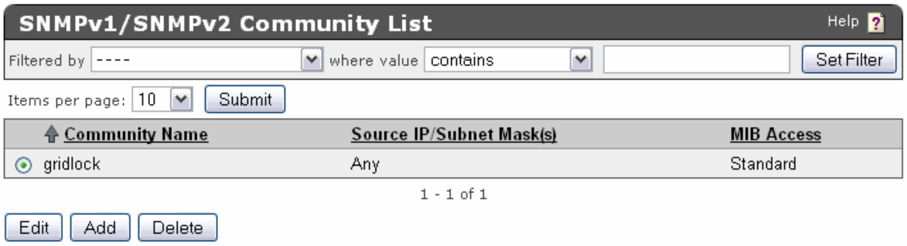
4 Select the **SNMP Agent IP**. You can select *All* or an individual IP address. We recommend that you specify an individual IP address.

5 Select the **SNMP Agent Port**. The default value is 161.

6 Select **Enable SNMP Traps**. By default, the KeySecure does not send SNMP traps.

Note: You can send a trap with the Send Test Trap button. If the receiving management station is setup correctly, you can check the management station server to which it is sent to verify the trap.

7. Navigate to the SNMPv1/SNMPv2 Community List section (Device >> SNMP >> Communities & Usernames). The community list is used to configure the agent to communicate with an NMS running either SNMPv1 or SNMPv2 software. The community list is where you define from which SNMPv1/v2 management stations the KeySecure receives SNMP MIB requests.



SNMPv1/SNMPv2 Community List

Community Name	Source IP/Subnet Mask(s)	MIB Access
○ gridlock	Any	Standard

1 - 1 of 1

When creating a community on the KeySecure, 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.

Note: For security purposes, the SNMP community name is read–only. The `set` command is not allowed on the SNMP agent.

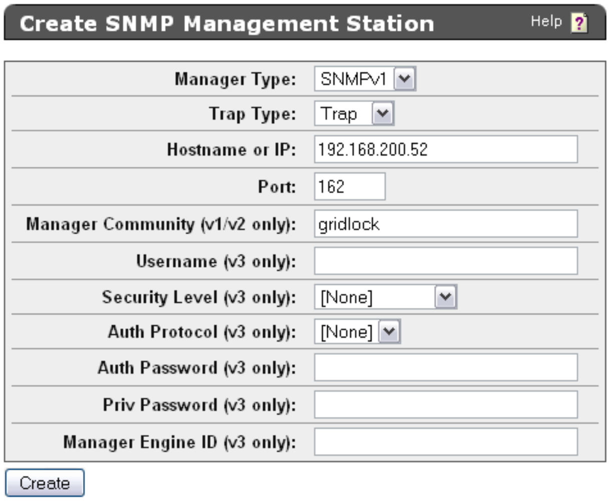
8. Click **Edit** or **Add**.

9. Enter a **Community Name**. This value can contain only alphanumeric characters and punctuation marks, and they cannot contain non-printing characters and whitespaces. Community names cannot exceed 64 characters. Avoid using the names “public” and “private” as these names are very commonly used.

10. Enter a **Source IP/Subnet Mask**. These are the IP address(es) allowed to access the agent. You can enter a specific IP address range, or you can enter a value of *Any*. If you are listing a specific IP address, you must also include the **Subnet Mask**. Separate the **Source IP** and **Subnet Mask** with a slash (/). If you are entering multiple **Source IP/Subnet Mask** pairs, you must separate each pair with a comma. We recommend that you limit access to the agent to particular IP addresses.

11. Select the community’s **MIB Access**. Can be either or both of the following:
    - *Enterprise* - Contains information on caching, SSL, CPU utilization, and operational statistics.
    - *Standard* - also known as MIB-II. contains information on network interface utilization, system health, and statistics for IP, TCP, ICMP, UDP, and SNMP.

12. Navigate to the Create SNMP Management Station section (Device >> SNMP >> Management Stations).



Manager Type:	SNMPv1
Trap Type:	Trap
Hostname or IP:	192.168.200.52
Port:	162
Manager Community (v1/v2 only):	gridlock
Username (v3 only):	
Security Level (v3 only):	[None]
Auth Protocol (v3 only):	[None]
Auth Password (v3 only):	
Priv Password (v3 only):	
Manager Engine ID (v3 only):	

13 Enter the **Manager Type**. Select either *SNMPv1* or *SNMPv2*.

14 Enter the **Trap Type**. Select either *Trap* or *Inform*. We recommend that you always use Inform.

15 Enter the **Hostname or IP** of the NMS.

16 Enter the **Port**. The default value is 162.

17 Enter the **Manager Community**. This is the name used to send SNMP data to SNMPv1/v2 management station. 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.

18 Click **Create** to create the SNMP management station.

Configuring SNMPv3 on the KeySecure

The KeySecure 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 SafeNet SNMP agent is capable of providing the following SNMP functionality:

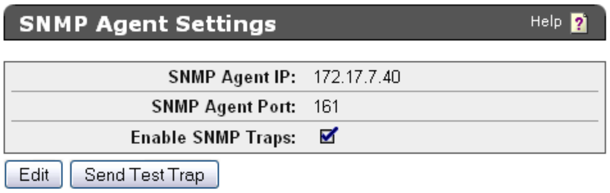
- it enables the NMS to access the MIBs on the KeySecure.
- it initiates trap messages to the NMS.

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

To configure a SafeNet agent to communicate with an NMS running SNMPv3 software:

1 Log in to the KeySecure

2 Navigate to the SNMP Configuration page (Device >> SNMP).



SNMP Agent IP:	172.17.7.40
SNMP Agent Port:	161
Enable SNMP Traps:	☑

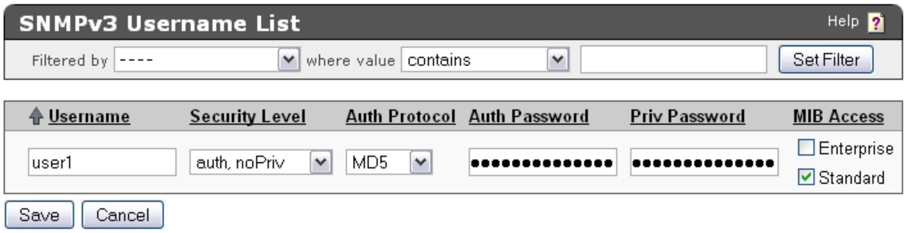
3 Click **Edit** in the SNMP Agent Settings section.

4 Select the **SNMP Agent IP**. You can select *All* or an individual IP address. We recommend that you specify an individual IP address.

5 Select the **SNMP Agent Port**. The default value is 161.

6 Select **Enable SNMP Traps**. By default, the KeySecure does not send SNMP traps.

7 Navigate to the SNMPv3 Username List section (Device >> SNMP >> Communities & Usernames). The username list is used to configure the agent to communicate with an NMS running SNMPv3 software. The username list is where you define from which SNMPv3 management stations the KeySecure receives SNMP MIB requests.



Username	Security Level	Auth Protocol	Auth Password	Priv Password	MIB Access
user1	auth, noPriv	MD5	●●●●●●●●●●●●●●	●●●●●●●●●●●●●●	☐ Enterprise ☑ Standard

8 Click **Add** or **Edit**.

9 Enter a **Username**. The **username** defines from whom the KeySecure accepts SNMP messages, and it is one of many elements used to create a key that is shared between the NMS and the agent. Usernames can contain only alphanumeric characters and punctuation marks and they cannot contain non-printing characters and white spaces.

10 Select the **Security Level**. There are three options:

- auth, priv – authorization and privacy. This option takes full advantage of the enhanced security features in SNMPv3. This option means that the KeySecure authenticates the sender of the SNMP message; in addition, all data exchanged between the SafeNet 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 KeySecure 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.

11 Select the **Auth Protocol**. Choose either *MD5, SHA*, or *None*.

12 Enter the **Auth Password**. This password is used to create the secret key that performs the MAC operation on the data shared between the SafeNet agent and the management station. The **Auth Password** must be between 8 and 256 characters.

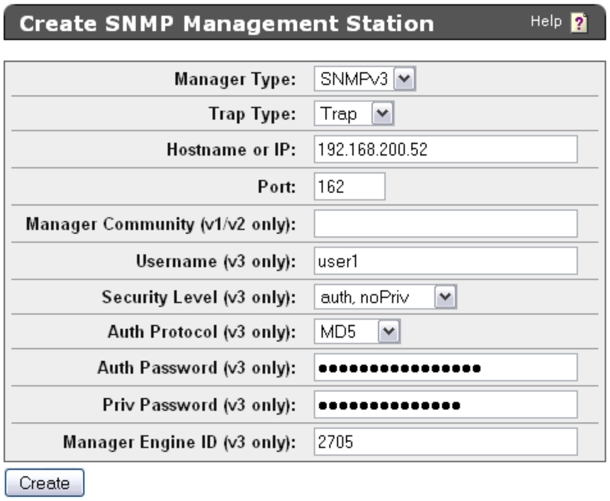
13 Enter the **Priv Password**. This password is used to create the secret key that performs the encrypt and decrypt operations on the data shared between the agent and the NMS. The **Priv Password** must be between 8 and 256 characters.

Note: If you select *auth, priv* for **Security Level**, enter a valid value in the **Auth Password** field, and then leave the **Priv Password** field blank, the **Auth Password** will also be used as the **Priv Password**.

14 Select the username's **MIB Access**. Can be either or both of the following:

- *Enterprise* - Contains information on caching, SSL, CPU utilization, and operational statistics.
- *Standard* - also known as MIB-II. contains information on network interface utilization, system health, and statistics for IP, TCP, ICMP, UDP, and SNMP.

15 Navigate to the Create SNMP Management Station section (Device >> SNMP >> Management Stations).



Create SNMP Management Station

Manager Type:	SNMPv3
Trap Type:	Trap
Hostname or IP:	192.168.200.52
Port:	162
Manager Community (v1/v2 only):	
Username (v3 only):	user1
Security Level (v3 only):	auth, noPriv
Auth Protocol (v3 only):	MD5
Auth Password (v3 only):	••••••••••••••••
Priv Password (v3 only):	••••••••••••••
Manager Engine ID (v3 only):	2705

16 Enter the **Manager Type**. Select either *SNMPv1* or *SNMPv2*.

17 Enter the **Trap Type**. Select either *Trap* or *Inform*. We recommend that you always use Inform.

18 Enter the **Hostname or IP** of the NMS.

19 Enter the **Port**. The default value is 162.

20 Enter the **Username**. This is the name 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

21 Enter the **Security Level**. There are three options:

- auth, priv – authorization and privacy. This option takes full advantage of the enhanced security features in SNMPv3. This option means that the KeySecure is authenticated by the NMS when the KeySecure sends a trap; in addition, all data exchanged between the SafeNet 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 KeySecure 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.

22 Select the **Auth Protocol**. Choose either *MD5, SHA*, or *None*.

23 Enter the **Auth Password**. 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 256 characters.

24 Enter the **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 256 characters.

Note: If you select *auth, priv* for **Security Level**, enter a valid value in the **Auth Password** field, and then leave the **Priv Password** field blank, the **Auth Password** will also be used as the **Priv Password**.

25 Enter the **Manager Engine**, do not exceed 128 characters. This 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

26 Click **Create** to create the SNMP management station.

Enterprise MIB Overview

We distribute MIBs in SMIv2 format; if you want SMIv1, you can derive it from the SMIv2 MIB distributed by SafeNet. You can obtain the Enterprise MIBs at the Web Support Center. You must have a Web Support Center account before you can download the MIBs.

The Enterprise MIBs are broken out into the following functional groups:

- **System Statistics**. The System Statistics provide 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, please see Chapter 21, “Statistics”.
- **NAE Server Statistics**. NAE 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 administrative 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.
  - DB Tools – data migration operation completed, key rotation operation completed, column unencryption operation completed.
  - 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.
  - License Notification Objects – No licenses available.

- **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.
  - High Availability Notification – System set as master, HA service is non-functional.
  - Accelerator Notification Object – Accelerator self test failed.
  - RAID Disk Notification – disk operational, disk failed, disk recovering, disk status unknown, disk removed, disk added.

Chapter 14

Administrator Configuration

An administrator is a user who can configure and manage the KeySecure. 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.

Important! Administrators are *not* users. Users use KeySecure client software to access the Key Server in order to perform some cryptographic function.

Using Multiple Administrator Accounts

Most likely, you will want to create multiple administrators. When doing so, 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'll want to create unique administrators for each of those roles.

When creating an administrator, you should assign the *minimum* amount of access controls needed. For example, a backup administrator will only need the Backup & Restore access controls. (You'll probably also want to assign an Administrative Access access control to most of your administrators.)

Note: We strongly discourage the sharing of administrator accounts. Each administrator should have their own administrator account.

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, therefore, have *full* control over the configuration of the KeySecure: they can create and delete administrator accounts, change administrator passwords, and assign and revoke access controls. When you select this option, you'll notice that the system will automatically enable *all* of the access controls for that administrator.

Important! 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.

The Default Administrator

The KeySecure ships with a default administrator (`admin`). `admin` is a local High Access Administrator. Once the initial configuration is complete, you must log in as the `admin` administrator; thereafter, you can create different administrators and log in with a different username.

Local and LDAP Administrators

The KeySecure 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.

Local Administrators

Local administrators are created within the SafeNet environment, either on the local device, or on a member of a cluster. They are managed entirely on the KeySecure.

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 KeySecure's password policies. These are discussed in Chapter 16, "Password Management".

Important! 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 KeySecure as a High Access Administrator. *If you lose or forget the passwords for all administrator accounts, you cannot configure the* KeySecure*, and you must ship it back to have the software reinstalled. All keys and configuration data will be unrecoverable.*

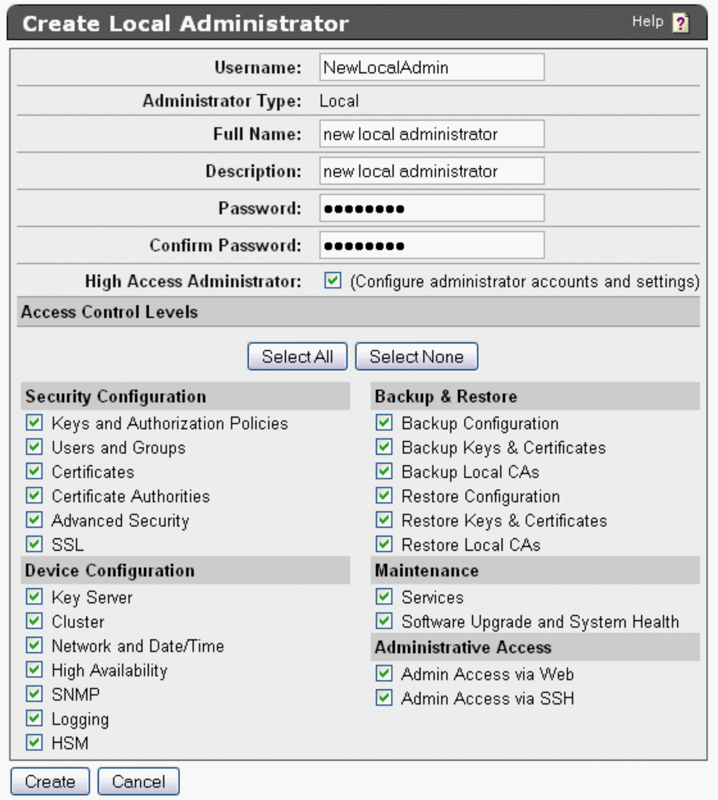
When a local administrator logs in to the CLI or the Management Console, the KeySecure authenticates the username and password with the values stored securely on the KeySecure. If the authentication succeeds, the administrator will be logged in to the KeySecure.

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 local administrator, the administrator whose password changed is prompted to change his or her password immediately after logging in (with the new password) to the KeySecure. After changing the password, the administrator continues to the Management Console or the command prompt as usual.

Creating a Local Administrator

To create a local administrator account:

1. Log in the KeySecure as an administrator with High Access Administrator access control.
2. Navigate to the Administrator Configuration page (Device >> Administrators >> Administrators).
3. Click **Create Local Administrator**.



Create Local Administrator Help ?

Username:	NewLocalAdmin
Administrator Type:	Local
Full Name:	new local administrator
Description:	new local administrator
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
- ☑ Key Server
- ☑ Cluster
- ☑ Network and Date/Time
- ☑ High Availability
- ☑ SNMP
- ☑ Logging
- ☑ HSM

Backup & Restore
- ☑ Backup Configuration
- ☑ 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

4 Enter a **Username**. **Usernames** must contain alphanumeric characters only and cannot be longer than 30 characters. You cannot include special characters or whitespace in the username. In addition, the first character must be a letter.

5 Enter values in the **Full Name** and **Description** fields.

6 Enter the **Password**. Immediately after logging in for the first time, the administrator must change the password. The requirements for the password depend on your Password Management settings. The value shown here is masked.

Important! When changing the password, be sure to clear the field first. If you do not clear the field first, the asterisks used to mask the value will become part of the new password.

7 Confirm the password in the **Confirm Password** field.

8 Select **High Access Administrator**, if you want to grant the administrator the ability to create, modify, and delete other administrator accounts, assign and modify access privileges for other administrators, and configure all administrator settings (administrators, LDAP administrator server, password management, multiple credentials, and remote administration).

Important! If you enable this checkbox, all other Access Control settings will automatically be checked. Any of the other Access Control settings can be disabled before creating the administrator account. However, since High Access Administrators can edit these settings, the new administrator will be able to re-enable any of the Access Control settings that were initially disabled.

WARNING: It is very important that you take great caution in granting the High Access Administrator access control option, which allows an administrator full control over the configuration of the KeySecure. Some of the privileges available to such an administrator are as follows: can change the passwords of other administrators, can assign him or herself additional permissions, and can create additional administrators.

9 Select the access controls for the administrator account. Use the **Select All** and **Select None** buttons as appropriate. Select from the following values:

- 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 server settings.
- Certificates: Create and import certificates.
- Certificate Authorities: Manage certificate authorities on the KeySecure.
- Advanced Security: Manage advanced security settings, including FIPS and Common Criteria configuration.
- SSL: Modify SSL configuration.
- Key Server: Enable and configure the Key Server.
- Cluster: create a cluster, join or remove this device from an existing cluster.
- Network and Date/Time: Configure network and date/time settings.
- High Availability: Configure high availability settings.
- SNMP: Manage SNMP community names and management stations.
- Logging: Modify logging settings.
- Backup Configuration: Create system backups that include everything but keys, certificates and local CAs.
- Backup Keys & 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.
- Services: Modify startup service setting.
- Software Upgrade and System Health: Upgrade to a new version of the KeySecure.
- Admin Access via Web: Administrate the KeySecure through the web interface.
- Admin Access via SSH: Administrate the KeySecure through SSH.

Note: The Admin Access access control options specify whether an administrator can configure the KeySecure 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 KeySecure from a serial console connection, which would preclude that administrator from modifying almost all security configuration settings and some device configuration settings (e.g. Key Server, Keys, Users & Groups).

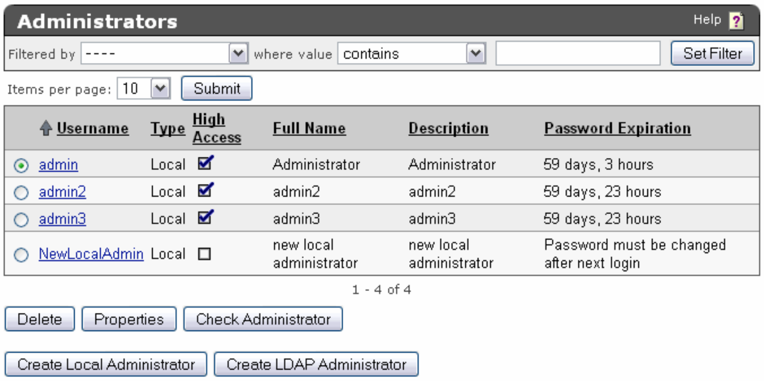
10 Click **Create.**

Deleting a Local Administrator

To delete a local administrator account:

1 Log in the KeySecure as an administrator with High Access Administrator access control.

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



Filtered by ---- where value contains

Items per page: 10

	Username	Type	High Access	Full Name	Description	Password Expiration
●	admin	Local	☑	Administrator	Administrator	59 days, 3 hours
○	admin2	Local	☑	admin2	admin2	59 days, 23 hours
○	admin3	Local	☑	admin3	admin3	59 days, 23 hours
○	NewLocalAdmin	Local	□	new local administrator	new local administrator	Password must be changed after next login

1 - 4 of 4

3 Select the administrator in the Administrators section.

4 Click **Delete**.

5 Confirm the action on the Secondary Approval section.

Note: For disaster recoverability purposes, the last local administrator account on a KeySecure *cannot* be deleted.

Chapter 15

LDAP Administrator

The KeySecure 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. Local administrators are detailed in Chapter 14, “Administrator Configuration”.

LDAP Administrators

LDAP administrators are based on user accounts managed on an external LDAP server. The KeySecure 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 KeySecure. You use the LDAP server to configure your policies and store the passwords. LDAP administrators cannot change their passwords using the KeySecure. The configurable password settings, password history, and password expiration features on the KeySecure do not apply to LDAP administrators.

Important! 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 device. 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 KeySecure connects to the LDAP server to authenticate the username and password. If the authentication succeeds, the administrator will be logged in to the KeySecure.

LDAP Administrator Server and FIPS Compliance

For more information about FIPS mode and other High Security settings, see Chapter 37, “High Security Features”.

If an LDAP Administrator Server is configured, the KeySecure cannot be in FIPS compliance. On a FIPS-compliant KeySecure, configuring the LDAP Administrator Server will take the KeySecure out of FIPS compliance. When you try to edit the LDAP Administrator Server on a FIPS-compliant KeySecure, the Management Console displays a warning that configuring the LDAP Administrator Server will take the KeySecure out of FIPS compliance.

If the device is not in FIPS compliance because an LDAP Administrator Server is currently configured, clicking “Set FIPS Compliant” on the High Security Configuration page will result in an error. The LDAP Administrator Server settings must be cleared manually before the device can become FIPS-compliant.

Setting up the LDAP Administrator 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 that can be designated as LDAP administrators. When creating an LDAP administrator on the KeySecure, 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, we recommend that you enable SSL in the LDAP Administrator Server settings. This ensures that the connection between the KeySecure and the LDAP server is secure. If you do not use SSL, 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.

Likewise, 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.

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.

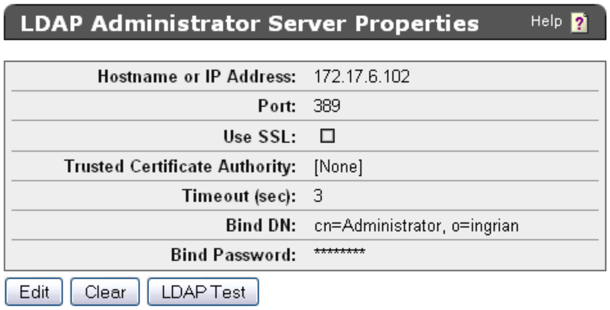
An LDAP account cannot be designated as an administrator if there is already a local administrator account with the same username. Likewise, a local account cannot be created or renamed with the same username as an LDAP account which has been designated as an administrator.

Note: LDAP administrators cannot modify LDAP administrator server settings.

To set up the LDAP administrator server:

1 Log in to the KeySecure 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 >> Administrators >> LDAP Administrator Server).



LDAP Administrator Server Properties

Hostname or IP Address:	172.17.6.102
Port:	389
Use SSL:	□
Trusted Certificate Authority:	[None]
Timeout (sec):	3
Bind DN:	cn=Administrator, o=ingrian
Bind Password:	********

3 Click **Edit**.

4 Enter the **Hostname or IP Address and Port** of the primary LDAP server. The port is typically 389.

5 Select **Use SSL** to enable SSL. By default, the KeySecure connects to the LDAP server over TCP.

6 If using SSL, enter the **Trusted Certificate Authority**. The CA will verify that the server certificate presented by LDAP servers are signed by a CA trusted by the KeySecure.

7 Enter a value in the **Timeout** field. This is the number of seconds to wait for the LDAP server during connections and searches. If the connection times out, the authorization fails.

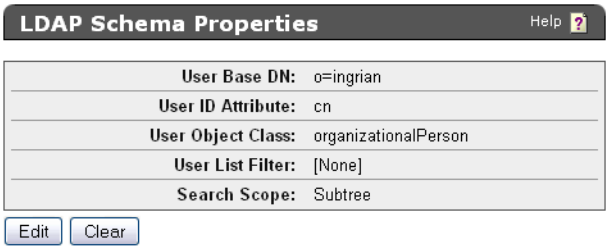
8 Enter the **Bind DN** (distinguished name) used to bind to the server. The device will bind using these credentials to perform searches for users and groups. If your LDAP server supports anonymous searches, you may leave this field and the **Blind Password** field empty.

9 Enter the **Bind Password**. This is password used to bind to the LDAP server.

10 Click **Save**.

11 Click **LDAP Test** to test the connection.

12 Set up the LDAP schema using the LDAP Schema Properties section (Device >> Administrators >> LDAP Administrator Server).



LDAP Schema Properties

User Base DN:	o=ingrian
User ID Attribute:	cn
User Object Class:	organizationalPerson
User List Filter:	[None]
Search Scope:	Subtree

13 Click **Edit**.

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

- 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 that can be used for authentication.
- User List Filter - used for narrowing the search within the object class.

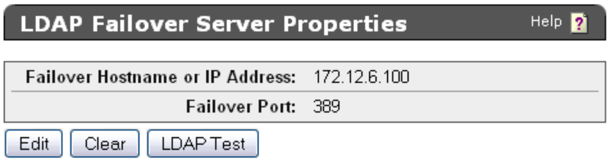
15 Choose the **Search Scope** to determine how deep with the LDAP user directory the system searches for a user. Can be either *One Level* **or *Subtree*.**

- One Level - search only the children of the base node.
- Subtree - search all the descendents of the base node. Depending on size of your LDAP directory, this can be very inefficient.

Note: The LDAP protocol supports four search scopes: base, onelevel, subtree and children. You can specify only onelevel and subtree at this time. Note that subtree includes base and children, so by specifying subtree, the search scope includes subtree, base, and children.

16 Click **Save**.

17 Set up the LDAP failover server using the LDAP Failover Server section (Device >> Administrators >> LDAP Administrator Server). When the primary LDAP server is down, the KeySecure shifts to the failover server and periodically retries the main server to see if it have become accessible again.



LDAP Failover Server Properties

Failover Hostname or IP Address: 172.12.6.100
Failover Port: 389

18 Click **Edit**.

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

20 Click **Save**.

21 Click **LDAP Test** to test the connection.

Creating an LDAP Administrator

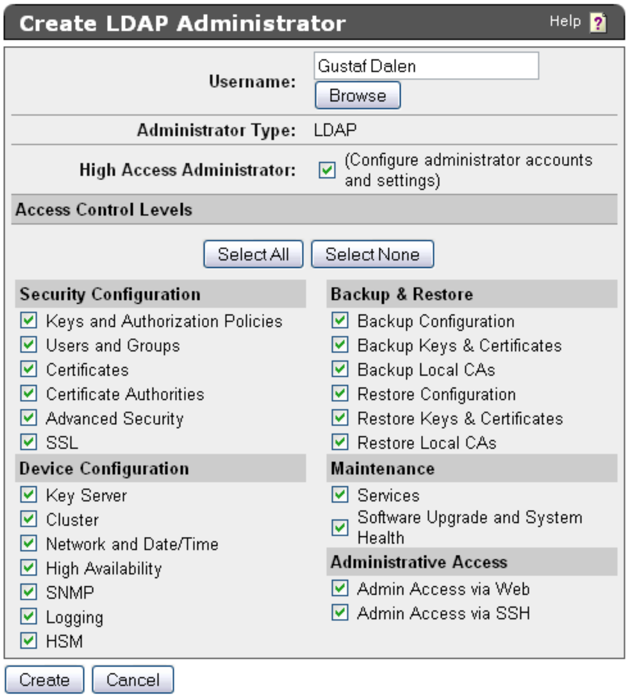
Note: You must configure the LDAP Administrator Server settings before you can create an LDAP administrator.

To create an administrator account:

1 Log in the KeySecure 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 LDAP Administrator**.



Create LDAP Administrator

Username: Gustaf Dalen

Administrator Type: LDAP

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
- ☑ Key Server
- ☑ Cluster
- ☑ Network and Date/Time
- ☑ High Availability
- ☑ SNMP
- ☑ Logging
- ☑ HSM

Backup & Restore
- ☑ Backup Configuration
- ☑ 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

4 Select **High Access Administrator**, if you want to grant the administrator the ability to create, modify, and delete other administrator accounts, assign and modify access privileges for other administrators, and configure all administrator settings (administrators, LDAP administrator server, password management, multiple credentials, and remote administration).

Important! If you enable this checkbox, all other Access Control settings will automatically be checked. Any of the other Access Control settings can be disabled before creating the administrator account. However, since High Access Administrators can edit these settings, the new administrator will be able to re-enable any of the Access Control settings that were disabled.

WARNING: It is very important that you take great caution in granting the High Access Administrator access control option, which allows an administrator full control over the configuration of the KeySecure. Some of the privileges available to such an administrator are as follows: can change the passwords of other administrators, can assign him or herself additional permissions, and can create additional administrators.

5 Select the access controls for the administrator account. Use the **Select All** and **Select None** buttons as appropriate. Select from the following values:

- 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 server settings.
- Certificates: Create and import certificates.
- Certificate Authorities: Manage certificate authorities on the KeySecure.
- Advanced Security: Manage advanced security settings, including FIPS and Common Criteria configuration.

- SSL: Modify SSL configuration.
- Key Server: Enable and configure the Key Server.
- Cluster: create a cluster, join or remove this device from an existing cluster.
- Network and Date/Time: Configure network and date/time settings.
- High Availability: Configure high availability settings.
- SNMP: Manage SNMP community names and management stations.
- Logging: Modify logging settings.
- Backup Configuration: Create system backups that include everything but keys, certificates and local CAs.
- Backup Keys & 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.
- Services: Modify startup service setting.
- Software Upgrade and System Health: Upgrade to a new version of the KeySecure.
- Admin Access via Web: Administrate the KeySecure through the web interface.
- Admin Access via SSH: Administrate the KeySecure through SSH.

Note: The Admin Access access control options specify whether an administrator can configure the KeySecure 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 KeySecure from a serial console connection, which would preclude that administrator from modifying almost all security configuration settings and some device configuration settings (e.g. Key Server, Keys, Users & Groups).

6 Click **Create.**

Deleting an LDAP Administrator

To delete an administrator account:

1 Log in the KeySecure as an administrator with High Access Administrator access control.

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

3 Select the administrator in the Administrators section.

4 Click **Delete**.

5 Confirm the action on the Secondary Approval section.

Note: For disaster recoverability purposes, the last local administrator account on a KeySecure *cannot* be deleted.

Chapter 16

Password Management

All passwords on the KeySecure (local administrator, local user, KeySecure clusters, and backups) are subject to the same basic constraints. Passwords must contain at least five different characters. Passwords *must not*:

- contain only whitespace.
- resemble a phone number, dictionary word, or reversed dictionary word.
- be based on the username associated with the password.

In addition to these rules, an administrator may set up more constraints on the Password Settings for Local Administrators section.

Note: LDAP administrators cannot change their passwords on the KeySecure. LDAP passwords must be changed on the LDAP server.

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: (1) an administrator cannot turn back the system time to prevent a password from expiring; (2) it avoids a scenario where many or all passwords expire simultaneously due to a large jump forward in the system time.

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: (1) administrators cannot determine the passwords of other administrators, and (2) 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.

Changing Your Password

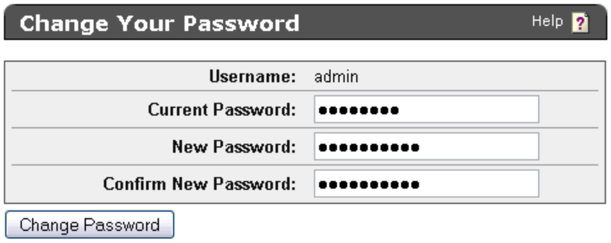
This section allows administrators to change their own password. Administrators can change their own passwords regardless of their access control settings. To change your own password simply enter your current password, and then enter a new password and confirm the new password.

Note: LDAP administrators cannot change their passwords on the KeySecure. 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 KeySecure.

To change your administrator account password:

1 Log in to the KeySecure using your administrator account.

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



Change Your Password

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

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

4 Enter a new password in the **New Password** and **Confirm New Password** fields. The new password must adhere to all of the rules established in the Password Settings for Local Administrators section.

5 Click **Change Password**.

Configuring Password Settings for Local Administrators

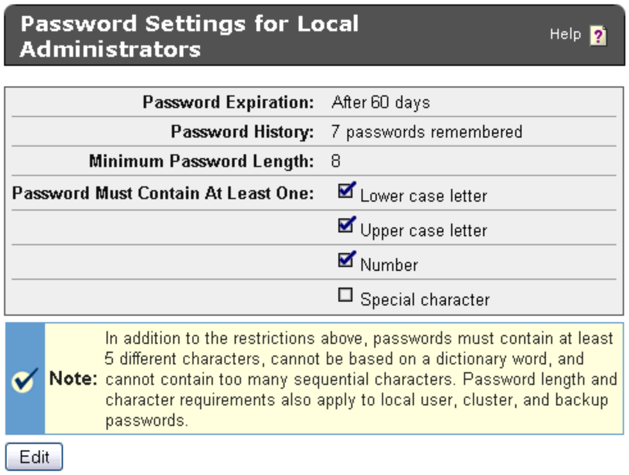
The Password Settings for Local Administrators section allows you to specify additional password constraints for local administrator passwords. Some of these constraints (password length and character restrictions) also apply to local users, clusters, and backups. The password expiration and password history features apply only to administrators.You must have High Access Administrator access control to make changes to this section.

Note: 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 KeySecure.

To configure password settings for local administrators:

1 Log in to the KeySecure as an administrator with High Access Administrator access control.

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



Password Settings for Local Administrators

Password Expiration:	After 60 days
Password History:	7 passwords remembered
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.

3 Click **Edit**.

4 To enable password expiration, enter the *Maximum Password Age* in the **Password Expiration** field. The maximum is 365 days. Once enabled, this feature applies to all current administrator passwords - all current administrator passwords have the same duration period, regardless of when they may have been created initially. When an administrator’s password reaches this age, the administrator will be forced to create a new password. You can view the status of an administrator’s password by navigating to the Administrator Configuration page (Device >> Administrators >> Administrators). Select *Never* to disable the password expiration feature.

5 To enable password history, enter the *Num Passwords to Remember* in the **Password History** field. The acceptable range is from 1 to 25. When creating a new password, an administrator cannot use a value that exists in their password history. Select *Disabled* to disable the password history feature. Once disabled, the system deletes the existing password histories. This feature applies only to administrator passwords.

Note: 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, special character, or some combination of these values.

8 Click **Save**.

Note: 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.

Chapter 17

Multiple Credentials

If the KeySecure has 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.

You can predetermine the number of administrators required to confirm certain operations, let administrators give their credentials to one another for a set period of time, and enable multiple credentials functionality within a clustered environment.

Operations Requiring Multiple Authentication

When the feature is enabled, the following operations require multiple authentication:

- Disable Multiple Credentials
- Create/Edit/Delete/Import Keys
- Edit a key’s 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
- Rollback 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.

Multiple Credentials in Clusters

To implement multiple credentials on KeySecures within a cluster, you must adhere to the following guidelines:

- All devices within the cluster must have the multiple credentials feature enabled. The feature can be enabled on one device and replicated to the others.
- For each device 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 device to a cluster with multiple credentials enabled:

1. Make sure that the new device 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 device within the cluster. This action requires confirmation from multiple administrators.
3. Add the new device to the cluster. For information on adding a KeySecure to a cluster, refer to Chapter 5, “KeySecure Clustering”.
4. Enable the multiple credentials feature for the cluster by enabling the feature for one member.

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 having to enter 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 lets an administrator grant credentials from a different computer.

Note: 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
- Affect authorization policies
- Modify LDAP settings for users and groups

Administrators that are not normally permitted to execute any of these operations cannot grant credentials for them; those options are unavailable. Credentials cannot be granted for those operations not listed.

Note: 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, she will never be able to create a key, even if another administrator grants credentials to her.

Important! If an administrator changes the KeySecure system time or reboots it, all temporary administrator credentials immediately expire.

WARNING! If your KeySecure is configured to use NTP, modifications to the NTP system time can extend the life span of a granted credential.

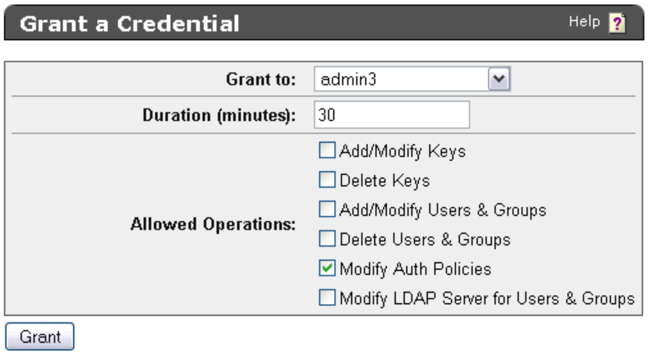
Note: Granted credentials are not included in backups.

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 KeySecure as an administrator that will grant credentials to another.

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



Grant a Credential

Grant to:	admin3
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

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

4 Enter the **Duration** that the credentials will be granted. This value must be less than 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 in the **Allowed Operations** field.

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

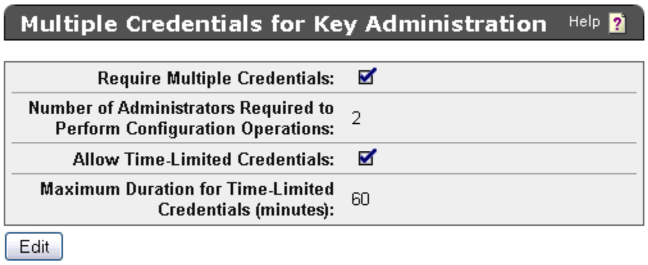
Configuring the Multiple Credentials Feature

Use the Multiple Credentials for Key Administration section 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.

To configure the multiple credentials feature:

1 Log in to the KeySecure as an administrator with High Access Administrator access control.

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



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):	60

3 Click **Edit**.

4 Select **Require Multiple Credentials**. This enables the multiple credentials feature. You must have High Access Administrator access control to enable this feature. Uncheck this field to disable the 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 disabling of the feature.

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**. Enter the time period in the **Maximum Duration for Time-Limited Credentials** field.

7 Click **Save**.

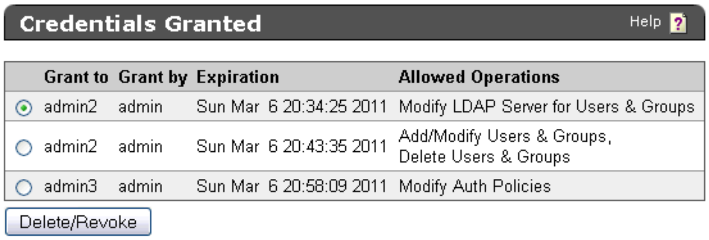
View and Revoke Granted Credentials

Once the multiple credentials feature is enabled, you'll want to track who is granting what to whom. The Credentials Granted section shows the credentials granted to or by the current administrator. Any credential grants that do not involve the current administrator are not displayed.

To view granted credentials:

1 Log in to the Management Console.

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



Credentials Granted

	Grant to	Grant by	Expiration	Allowed Operations
●	admin2	admin	Sun Mar 6 20:34:25 2011	Modify LDAP Server for Users & Groups
○	admin2	admin	Sun Mar 6 20:43:35 2011	Add/Modify Users & Groups, Delete Users & Groups
○	admin3	admin	Sun Mar 6 20:58:09 2011	Modify Auth Policies

3 View the following fields:

- **Grant to** - the administrator receiving the credentials.
- **Grant by** - the administrator granting the credentials.
- **Expiration** - the date and time upon which the credential grant expires. Credential grants expire automatically if the KeySecure is rebooting or the system time is altered.
- **Allowed Operations** - lists the specific operations for which the credentials have been granted.

4 Click **Delete/Revoke** to cancel the grant. The credential grant will be removed from the system.

Chapter 18

Remote Administrator

You can administer the KeySecure locally and remotely. **Local administration** involves logging into the KeySecure from a machine that is physically connected to the device via a null modem cable. **Remote administration** involves logging into the KeySecure 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 KeySecure.

The Web Admin User Authentication feature provides an additional security safeguard against unauthorized configuration of the KeySecure. When this feature is enabled, administrators are asked for a Client Certificate when they attempt to log in to the KeySecure. After presenting a client certificate, administrators can only log in to the KeySecure 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 administrators 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 KeySecure. The Remote Admin Certificate is a self–signed certificate created during initial configuration that can be used to verify that the hostname in the certificate matches the hostname of the machine 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.

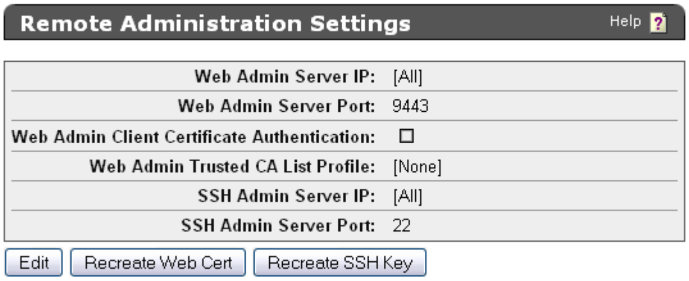
The SSH Key is used to generate a session key that is used for encryption and decryption operations while you are logged into the KeySecure.

Managing the Remote Administration Settings

To view and edit the remote administration settings:

1 Log on to the Management Console.

2 Navigate to the Remote Administration section (Device >> Administrators >> Remote Administrators).



Remote Administration Settings

Web Admin Server IP:	[All]
Web Admin Server Port:	9443
Web Admin Client Certificate Authentication:	□
Web Admin Trusted CA List Profile:	[None]
SSH Admin Server IP:	[All]
SSH Admin Server Port:	22

3 View the section. Click **Edit** to change the values. Remember that changing some values may immediately sever your connection with the KeySecure. The section contains the following fields:

- **Web Admin Server IP** - The Web Admin Server IP address is the local IP address used to configure the KeySecure via the Management Console. You can select one specific IP address or you can select all of the IP addresses bound to the KeySecure. The URL used to connect to the Management Console is: https://IP-address:port.

  Tip: We strongly recommend that you limit the Web Admin Server IP to a specific IP address. If you have four IP addresses bound to the KeySecure, and you select All instead of a specific IP address, then the KeySecure listens for Web Administration requests on four different IP addresses; whereas, if you specify a single IP address, the KeySecure listens for Web Administration requests on only one 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.
- **Web Admin Client Certificate Authentication** - activates the Management Console Client Authentication feature, which requires that users present a client certificate when logging into the Management Console.

  WARNING: 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 command from the CLI to disable this feature without presenting a certificate.
- **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 KeySecure. This option is only valid if you require clients to provide a certificate to authenticate to the Key Server. For more information, see Chapter 34, “Certificate Authorities”.

  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 Key Server can authenticate client certificates.
- **SSH Admin Server IP** - The SSH Admin Server IP address is the IP address used to configure the KeySecure from the CLI. You can select one specific IP address or all of the IP addresses bound to the KeySecure.

  Tip: We strongly recommend that you limit the SSH Admin Server IP to a specific IP address. If you have four IP addresses bound to the KeySecure, and you select All instead of a specific IP address, then the KeySecure listens for SSH Administration requests on four different IP addresses; whereas, if you specify a single IP address, the KeySecure 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.

Enabling the Web Admin User Authentication Feature

The Web Admin User Authentication feature requires a client certificate signed by a local CA on the KeySecure. The following instructions explain how to use the req.exe application to create the client certificate. Though we deliver the req.exe application with most of our client software, you can create the client certificate however you’d like.

Instructions for configuring Web Admin User Authentication are divided into the following sections:

- Generating a Client Certificate Request with req.exe
- Signing a Certificate Request and Downloading the Certificate
- Converting a Certificate from PEM to PKCS12 Format
- Importing a Certificate to a Web Browser
- Enabling the Web Admin User Authentication Feature

Generating a Client Certificate Request with req.exe

To generate a client certificate request:

1 Open a prompt window and navigate to the directory where the SafeNet Certificate Request Generator utility (req.exe) is installed.

2 Generate an RSA key and a client certificate request using the following command:

```
req -out clientreq -newkey rsa:1024 -keyout clientkey
```

where clientreq is the name of the certificate request being created, and clientkey is the name of the private key associated with the certificate request.

If you are using OpenSSL, use the following command:

```
openssl req -out clientreq -newkey rsa:1024 -keyout clientkey
```

Note: The certificate request and private key will both be created in the working directory by default. You can generate them in another directory by including a location in the request and key names. For example, to create them in the C:\client_certs folder, use the following command:

```
openssl req -out C:\client_certs\clientreq -newkey rsa:1024
-keyout C:\client_certs\clientkey
```

The key generation process will then request the following data:

- A PEM passphrase to encode the private key. The passphrase that encodes the private key is the first passphrase you provide after issuing the command above. You must specify this value in the Client Private Key Passphrase section of the IngrianNAE.properties file.
- The distinguished name. The distinguished name is a series of fields whose values are incorporated into the certificate request. These fields include country name, state or province name, locality name, organization name, organizational unit name, common name, email address, surname, user ID, and IP address.

  Important! The **common name** field *must* be the username of a valid administrator account. When using this certificate, only that administrator account will be usable.
- A challenge password. This challenge password is NOT used in the SafeNet environment.
- An optional company name.

Signing a Certificate Request and Downloading the Certificate

This section describes how to sign a certificate request with a local CA and then 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 KeySecure as an administrator with Certificates access control.

4 Navigate to the Local Certificate Authority List (Security >> CAs & SSL Certificates >> Local CAs). Select the local CA and click **Sign Request** to access the Sign Certificate Request section.

5 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 all text from the certificate request, including the header and footer.

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

7 Click the **Download** button to save the certificate to your client.

Converting a Certificate from PEM to PKCS12 Format

The KeySecure 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:

1 Execute the following command if you are using openssl:

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

Importing a Certificate to a Web Browser

To import a certificate into Mozilla Firefox:

1 From the menu, go to Tools > Options.

2 Click **Advanced**.

3 Click the Security tab.

4 Click **View Certificates**.

5 Click the **Import a Certificate** button.

6 Click **Import** on the Your Certificates tab.

7 Enter the passwords when prompted.

To import a certificate into Microsoft Internet Explorer:

1 From the menu, go to Tools > Internet Options.

2 Click the Content tab.

3 Click **Certificates**.

4 Click **Import**.

The Import Certificate Wizard guides you through the rest of the certificate import process.

Enabling Web Admin User Authentication on the KeySecure

To enable Web Admin User Authentication on the KeySecure:

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 User Authentication**.

5 Click **Save**.

Note: This feature is *immediately* enabled when you select **Web Admin User 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` command from the CLI to disable this feature without presenting a certificate.

Recreating the Web Cert

To recreate the web certificate:

1 Log in to the Management Console.

2 Navigate to the Remote Administration Settings section (Device >> Administrators >> Remote Administration).

3 Click **Recreate Web Cert** to generate a new certificate for the remote administration Management Console. After you click **Recreate Web Cert**, you are presented with an intermediate page that allows you to specify the duration of the Web Admin 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.

Recreating the SSH Key

To enable Web Admin User Authentication on the KeySecure:

1 Log in to the Management Console.

2 Navigate to the Remote Administration Settings section (Device >> Administrators >> Remote Administration).

3 Click **Recreate SSH Key** to generate a new key for remote administration use via SSH. Recreating the key closes all active SSH connections.

Chapter 19

Logging

The KeySecure 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 KeySecure, stipulate the maximum log file size, and transfer logs to a log server.

The following logs are created:

- **Activity Log** – Contains a record of each request received by the Key Server.
- **Audit Log** – Contains a record of all configuration changes and user input errors made to the KeySecure, whether through the Management Console or the CLI.
- **Client Event Log** – Contains a record of all client requests that have the <RecordEventRequest> element.
- **Database Encryption Log** – Contains a record of the data migration, unencryption, and key rotation operations performed by the KeySecure. This log is only produced when the Databases are set on the Management Console.
- **ProtectFile Client Log** – Contains a record of all operations performed by the ProtectFile clients. This log is available only when ProtectFile client is installed and configured in the Management Console.
- **ProtectFile Manager Log** – Contains a record of all operations performed by the ProtectFile Manager. This log is available only when the ProtectFile Manager feature is enabled and the ProtectFile client is installed and configured in the Management Console.
- **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.
- **SQL Log** – Contains a record of all SQL statements that are run against a database for schema migration, data migration, and key rotation. This log is only produced when the Databases are set on the Management Console.

For each type of log, the current log entries are kept in a file named ‘Current’.

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 KeySecure, 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.

Log Archives

If you do not configure the log transfer feature, old log files are stored on the KeySecure. 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 KeySecure 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.

Important! The KeySecure should not be a permanent storage place for log files. You should transfer those files to another location.

Log Transfer

The KeySecure acts as a temporary repository for logs; *it is not meant to store log files permanently*. We recommend 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 a KeySecure: SCP, FTP, browser download, and syslog. Because syslog and FTP are not secure protocols, we recommend that you use SCP to transfer your log files.

When a log is rotated, if you have configured a transfer destination for that log, the KeySecure 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 the KeySecure attempts to transfer the file every two hours until it is successfully transferred. If the KeySecure rotates the log before that file is successfully transferred, the KeySecure 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 KeySecure, the following naming convention is applied:

<log type>.<archive number>.<datetime stamp>.<hostname>

Value	Description
log type	type of log (e.g., System Log, Audit Log.)
archive number	indicates the file's place in the log archive. 1 indicates the most recent log file.
datetime stamp	The date and time when the log file was created.
hostname	The hostname of the KeySecure.

For example, the filename audit.log.1.2011-04-04_160146.demo would identify this file as:

- An Audit Log.
- The first log file in the log index.
- A file created on 2011-04-04 at 16:01:46.
- A log from the KeySecure with the hostname 'demo'.

This naming convention allows you to transfer log files from multiple KeySecures 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.

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 external servers. When you configure two servers, the KeySecure sends syslog messages to both.

You should be aware of the following before configuring syslog on your KeySecure.

- By default, the KeySecure transmits messages using syslog facility "local1;" however, this is configurable on a per–log–basis. Refer to RFC 3164, *"The BSD syslog Protocol,"* for details about syslog.
- The KeySecure can send syslog messages over either UDP (for syslog servers) or TCP (for syslog-ng servers). You can configure this for each message type and for each external syslog server.
- 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 KeySecure.
- 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 KeySecure, 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. With regard to the Audit Log, all existing CLI sessions continue to abide by the syslog settings that were in effect when the CLI session began. Once a user ends a CLI session and logs back in, the new syslog settings take effect for that session.

Syslog Message Format

When messages on the KeySecure are syslogged, they appear at the remote syslog server with an additional prefix of `<timestamp> <origin_host_or_ip> <LogName>`

where `LogName` might be "System," "Audit," or "Activity," depending on which log the message is from. The format of the timestamp and origin host/IP are determined by the remote syslog server software. Sometimes, the origin host/IP will be repeated twice in the message prefix. The message body (the elements after `LogName`) is the same as the entry in the local log file.

An example from the System Log is shown here:

original log message:

```
---------------------
2005-09-12 10:23:47 irwin.company.com NAE Server: Starting NAE Server
```

log message at syslog server (displays on one line):

```
-------------------------------------------------------
Sep 12 10:23:48 you.com demo System: 2005-09-12 10:23:47 you.com NAE Server:
Starting NAE Server
```

Secure Logs

The KeySecure allows you to sign your log files before moving them to another machine or downloading them, which makes them more secure than unsigned log files.

A Log Signing Certificate is created the first time the KeySecure is run and when the machine 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 KeySecure. The signed log file is then sent to the specified host in multipart 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 plaintext when downloaded.

Note: Signed logs files are significantly larger than unsigned logs. Specifically, the size of a signed log file is *approximately* equal to 2098 bytes plus 1.3864 times the size of the unsigned file. This means that logs securely transferred off of the KeySecure will be larger than the **Max Log File Size** value shown in the Rotation Schedule section.

Important! If you decide to recreate a Log Signing Certificate, it is very important to make a backup of the existing certificate so that old log files signed with the existing certificate can still be properly verified.

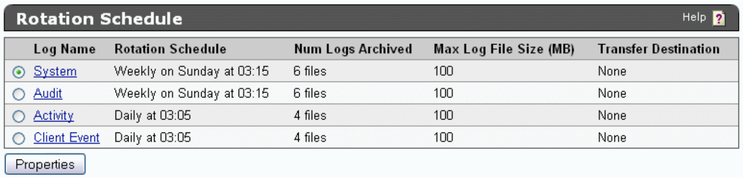
Tip: You should store your Log Signing Certificate separately from the signed logs files.

Configure Log Rotation

To configure log rotation:

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

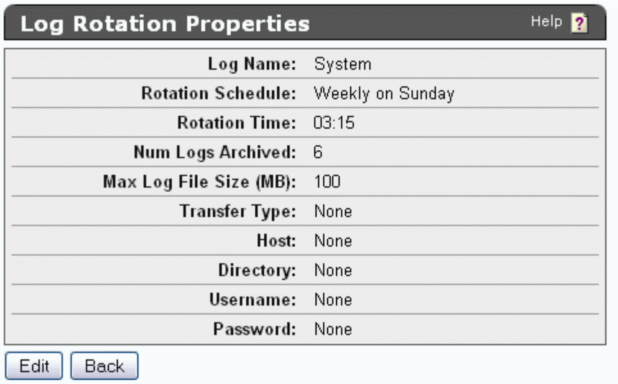
2 Navigate to the Log Configuration page (Device >> Log Configuration >> Rotation & Syslog).



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

3 Select a log in the Rotation Schedule section and click **Properties**.



Log Rotation Properties

Log Name:	System
Rotation Schedule:	Weekly on Sunday
Rotation Time:	03:15
Num Logs Archived:	6
Max Log File Size (MB):	100
Transfer Type:	None
Host:	None
Directory:	None
Username:	None
Password:	None

4 Click **Edit** on the Log Rotation Properties section. Enter values for the following fields:

- **Rotation Schedule** - specifies the frequency of log rotation. When a log is rotated, the current log 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.
- **Rotation Time** - specifies the time of day when the log rotation occurs.
- **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 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 file size limit, the system rotates the current file and begins writing to a new file. This is the maximum size of the unsigned log file as it is stored on the KeySecure. Signed logs are considerably larger.
- **Transfer Destination** - destination the log files are sent to, as defined by the Host and Directory fields. The Username must have write access to the Host and Directory. Selecting *None* implies that log files will be stored internally on the KeySecure. Selecting *FTP* or *SCP* implies that the log file will be sent via FTP or SCP to the specified hostname.

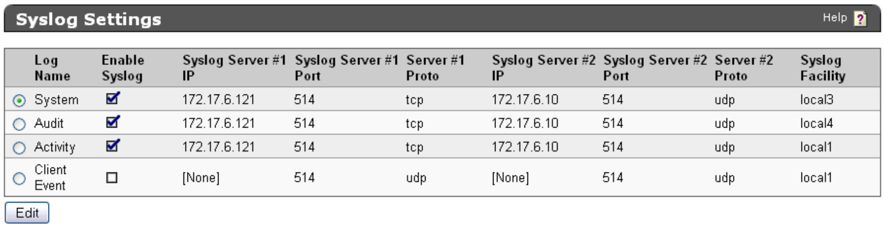
5 Click **Save**.

Enable 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 >> Rotation & Syslog).



	Log Name	Enable Syslog	Syslog Server #1 IP	Syslog Server #1 Port	Server #1 Proto	Syslog Server #2 IP	Syslog Server #2 Port	Server #2 Proto	Syslog Facility
●	System	☑	172.17.6.121	514	tcp	172.17.6.10	514	udp	local3
○	Audit	☑	172.17.6.121	514	tcp	172.17.6.10	514	udp	local4
○	Activity	☑	172.17.6.121	514	tcp	172.17.6.10	514	udp	local1
○	Client Event	□	[None]	514	udp	[None]	514	udp	local1

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

4 Select **Enable Syslog**.

5 Specify a hostname or IP address of the primary log server (Syslog Server #1), the port that this log server is listening on, and the protocol used to send the syslog message, either *udp* for syslog servers or *tcp* for syslog-ng servers. You can optionally enter an IP address, port, and protocol for a second server. When two servers are configured on this page, the KeySecure sends messages to both.

6 Enter the Syslog Facility. The default is local1. You can choose from local0 to local7.

7 Click **Save**.

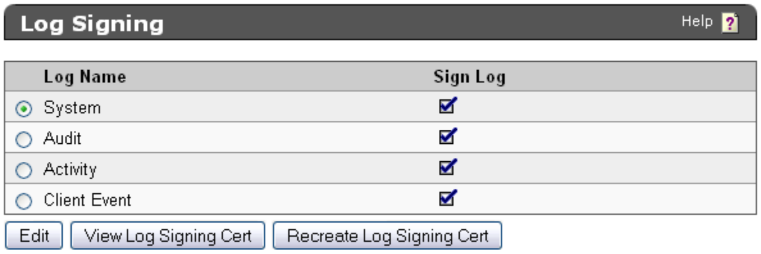
8 Repeat steps 3, 4 and 5 to enable syslog for multiple logs.

Enable 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).



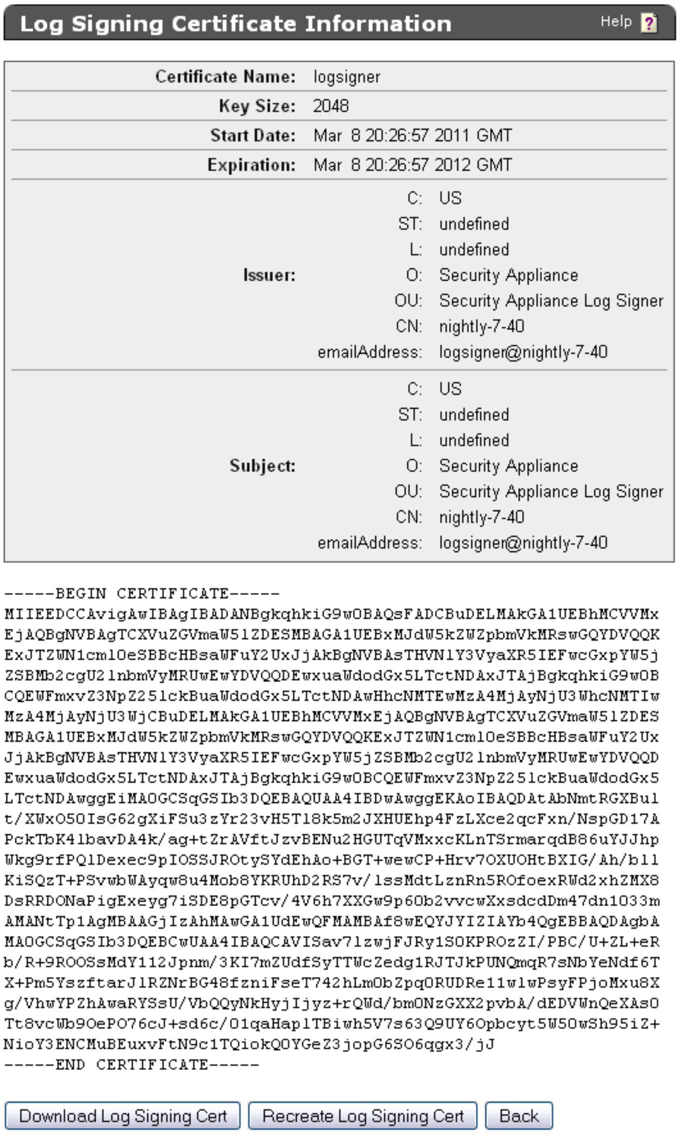
	Log Name	Sign Log
●	System	☑
○	Audit	☑
○	Activity	☑
○	Client Event	☑

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**. From now on, the system will sign the selected logs with the log signing certificate created when the KeySecure was initialized.

6 Click **View Log Signing Cert** to view the certificate used to sign the logs.



Certificate Name:	logsigner	
Key Size:	2048	
Start Date:	Mar 8 20:26:57 2011 GMT	
Expiration:	Mar 8 20:26:57 2012 GMT	
Issuer:	C:	US
	ST:	undefined
	L:	undefined
	O:	Security Appliance
	OU:	Security Appliance Log Signer
	CN:	nightly-7-40
	emailAddress:	logsigner@nightly-7-40
Subject:	C:	US
	ST:	undefined
	L:	undefined
	O:	Security Appliance
	OU:	Security Appliance Log Signer
	CN:	nightly-7-40
	emailAddress:	logsigner@nightly-7-40

```
-----BEGIN CERTIFICATE-----
MIIEEDCCAvigAwIBAgIBADANBgkqhkiG9w0BAQsFADCBuDELMAkGA1UEBhMCVVMx
EjAQBgNVBAgTCXVuZGVmaW5lZDESMBAGA1UEBxMJdW5kZWZpbmVkMRswGQYDVQQK
ExJTZWN1cml0eSBBcHBsaWFuY2UxJjAkBgNVBAsTHVNlY3VyaXR5IEFwcGxpYW5j
ZSBMb2cgU2lnbmVyMRUwEwYDVQQDEwxuaWdodGx5LTctNDAxJTAjBgkqhkiG9w0B
CQEWFmxvZ3NpZ25lckBuaWdodGx5LTctNDAwHhcNMTEwMzA4MjAyNjU3WhcNMTIw
MzA4MjAyNjU3WjCBuDELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCXVuZGVmaW5lZDES
MBAGA1UEBxMJdW5kZWZpbmVkMRswGQYDVQQKExJTZWN1cml0eSBBcHBsaWFuY2Ux
JjAkBgNVBAsTHVNlY3VyaXR5IEFwcGxpYW5jZSBMb2cgU2lnbmVyMRUwEwYDVQQD
EwxuaWdodGx5LTctNDAxJTAjBgkqhkiG9w0BCQEWFmxvZ3NpZ25lckBuaWdodGx5
LTctNDAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAtAbNmtRGXBul
t/XWxO5OIsG62gXiFSu3zYr23vH5Tl8k5m2JXHUEhp4FzLXce2qcFxn/NspGD17A
PckTbK4lbavDA4k/ag+tZrAVftJzvBENu2HGUTqVMxxcKLnTSrmarqdB86uYJJhp
Wkg9rfPQlDexec9pIOSSJROtySYdEhAo+BGT+wewCP+Hrv7OXUOHtBXIG/Ah/bll
KiSQzT+PSvwbWAyqw8u4Mob8YKRUhD2RS7v/lssMdtLznRn5ROfoexRWd2xhZMX8
DsRRDONaPigExeyg7iSDE8pGTcv/4V6h7XXGw9p6Ob2vvcwXxsdcdDm47dn1O33m
AMANtTp1AgMBAAGjIzAhMAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4QgEBBAQDAgbA
MA0GCSqGSIb3DQEBCwUAA4IBAQCAVISav7lzwjFJRy1SOKPROzZI/PBC/U+ZL+eR
b/R+9ROOSsMdY112Jpnm/3KI7mZUdfSyTTWcZedg1RJTJkPUNQmqR7sNbYeNdf6T
X+Pm5YszftarJlRZNrBG48fzniFseT742hLmObZpqORUDRe11wlwPsyFPjoMxu8X
g/VhwYPZhAwaRYSsU/VbQQyNkHyjIjyz+rQWd/bmONzGXX2pvbA/dEDVWnQeXAsO
Tt8vcWb9OePO76cJ+sd6c/O1qaHaplTBiwh5V7s63Q9UY6Opbcyt5W5OwSh95iZ+
NioY3ENCMuBEuxvFtN9c1TQiokQOYGeZ3jopG6SO6qgx3/jJ
-----END CERTIFICATE-----
```

7 Click **Download Log Signing Cert** to download the certificate through the web browser.

8 Click **Recreate Log Signing Cert** to generate a new log signing certificate.

Verify a Secure Log Using Microsoft Outlook

To verify a secure log using Microsoft Outlook:

1. Move the log file off of the KeySecure or download it to a Windows machine.
2. Change the file extension on the log file to .eml. The file will now be recognized by Windows as an email file.
3. Double-click on the file. Outlook Express will open and display a help screen with a security header that reads “Digitally signed - signing digital ID is not trusted”.
4. Click **Continue**. A security warning will appear.
5. Click **View Digital ID**. The Signing Digital ID Properties dialog will appear.
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 KeySecure.
8. Double-click on the Log Signing Certificate. The Certificate dialog will appear.
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.

Verify 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 the procedure in both Windows and UNIX/Linux environments. If OpenSSL has not been installed on your Windows machine, you can find a Windows distribution here:

http://www.slproweb.com/products/Win32OpenSSL.html

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).
3. Click **View Log Signing Cert**.
4. Click **Download Log Signing Cert** and save the Log Signer certificate to your local machine.
5. Navigate to the log page (Device >> Logs & Statistics >> Log Viewer >> <select the log page>) and click **Download Entire Log**. Save the log file in the same directory as the log signer cert. (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
```

where <signed log file> is the log you downloaded in step 5, and <log cert file> is the log signer cert you downloaded in step 4.

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:

```
2006-07-06 09:15:02 [admin]: Logged in from 192.168.1.170 via web
2006-07-06 11:17:30 [admin]: Logged in from 192.168.1.170 via web
2006-07-06 11:24:26 [admin]: Downloaded Cert logsigner
2006-07-06 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 from step 6 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.

Chapter 20

Log Viewer

The KeySecure maintains logs and statistics you can use to monitor your system'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.

System Logs

The **System Log** contains a record of all system events, such as:

- Failed log transfers.
- Hardware failures.
- License errors.
- Service starts, stops, and restarts.
- SNMP traps.
- Successful or failed cluster replication and synchronization.

Audit Logs

The **Audit Log** contains a record of all configuration changes and user input errors made to the KeySecure, whether through the Management Console or the CLI. The audit log cannot be cleared or manually rotated.

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.

Activity Logs

The **Activity Log** contains a record of each request received by the Key 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 Key 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>
```

Field	Description
date	enclosed in brackets, the date field shows the date and time that the KeySecure 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
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 table below.
error code	numerical error code returned to the client
message	enclosed in brackets, the message field displays either “Success” if the server 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.

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
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)

Client Event Logs

The **Client Event Log** contains a record of each message sent by clients using the `<RecordMessageRequest>` 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>
```

Field	Description
date	enclosed in brackets, the date field shows the date and time that the KeySecure 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.

Database Encryption Logs

The Database Encryption Log contains a record of the data migration, unencryption, and key rotation operations performed by the KeySecure. This log is only produced when the ProtectDB Manager feature is enabled.

An entry is made to this log whenever a column is encrypted or decrypted, or a key rotation operation is executed on a column. Log entries include the database column information, the number of rows encrypted or decrypted, the new key name (for key rotations), and a timestamp.

The format of the Database Encryption Log is as follows:

```
<date> <time> <operation> <database information: alias, hostname or IP, database
user, database name> <table information: table name,  table owner> <column name>
<operation information: key name>
```

A sample entry is shown here:

```
2005-10-27 04:49:21 SetEncryption database: [alias=master, host=192.168.1.129,
user=app_user, dbname=master] table: [name=ingtst1, owner=dbo] column: [name=
ssn] encryption: [key=yourkey]
```

SQL Logs

The SQL Log contains a record of all SQL statements that are run against a database for schema migration, data migration, and key rotation. The log entries include information necessary to identify each SQL operation, such as the database connection information, the user that executed the operation, the purpose of the operation, and a timestamp. Some entries are abbreviated if they would be repetitive or if they would contain cleartext information. The format of the SQL Log is as follows:

```
<date> <time> <database type> <database server IP> <database user> <database
name> <log level> <operation>
```

A sample entry is shown here:

```
2004-10-20 20:23:27 [SQLServer 192.168.1.129 SA CUSTOMER][INFO]:  INSERT INTO
[CUST_TEMP] SELECT ING_ROW_ID,[CC_NUM] FROM [CUST]
```

ProtectFile Client Logs

For more information about configuring the ProtectFile client log, see the *SafeNet ProtectFile User Guide.*

The ProtectFile Client Log contains a record of the operations performed by ProtectFile clients on file servers. This log is produced only when ProtectFile is installed on a file server and configured in the Management Console.

Logs written by ProtectFile are stored on the file server and can be configured to uploaded to the KeySecure. After uploading to the KeySecure, the logs are validated, after which the logs are viewable either on the KeySecure under **ProtectFile Client** or from a syslog server, if configured.

Note: Log rotation can significantly impact performance on an i110™.

The ProtectFile client logs messages for the following file server events:

- File opens
- Data migration start and end
- Key rotation start and end
- Application errors and warnings

Each log message includes the following information:

- Time stamp
- Hostname/IP address
- User name
- File name
- Operation attempted

The format for log entries is:

```
<C> <timestamp> <file server user> <file server name> <file name> <operation>
```

Where C is:	**Denoting:**
• -	Log line has successfully validated.
• F	Log line did not validate.
• 0	No verification occurred for this line.

A sample entry is shown here:

```
- Tue Jan 02 14:11:37 2007 User: [jsmith] File server [hr-475], file [d:\hr-
stop\optionsq206.xls] File open
```

ProtectFile Manager Logs

The ProtectFile Manager Log contains a record of the cryptographic and key rotation operations performed by the ProtectFile Manager through the ProtectFile client. This log is only produced when the ProtectFile Manager feature is enabled and the ProtectFile client is installed.

An entry is made to this log whenever a directory or file is encrypted or decrypted, or a key rotation operation is executed on a directory or file. Log entries include the file server and directory, the previous state and the new state (including the key, recursive encryption on directories, and extensions to which the operation applied), and a timestamp.

The format of the ProtectFile Manager Log is as follows:

```
<date> <time> <log message> File server [file server], directory [directory or
file path], old state [key name: <blank=none or key name before operation>; re-
cursive: <blank=false, 1=true>; extensions: <blank=all or extensions list>], new
state [key name: <blank=none or key name after operation>; recursive: <blank=
false, 1=true>; extensions: <blank=all or extensions list>]
```

A sample entry is shown here:

```
2007-01-27 12:34:56 Operation completed successfully. File server [hr-475], di-
rectory [d:\hrstop], old state [key name: ; recursive: ; extensions: ], new state
[key name: hr55; recursive: 1; extensions: ]
```

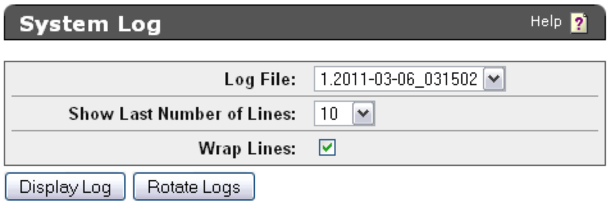
View Logs

To view the system log:

1 Log on to the Management Console.

2 Navigate to the Log Viewer page (Device >> Log Viewer).

3 Select the type of log to view in the left-hand navigation, either System, Audit, Activity, or Client Event.



System Log

Log File: 1.2011-03-06_031502

Show Last Number of Lines: 10

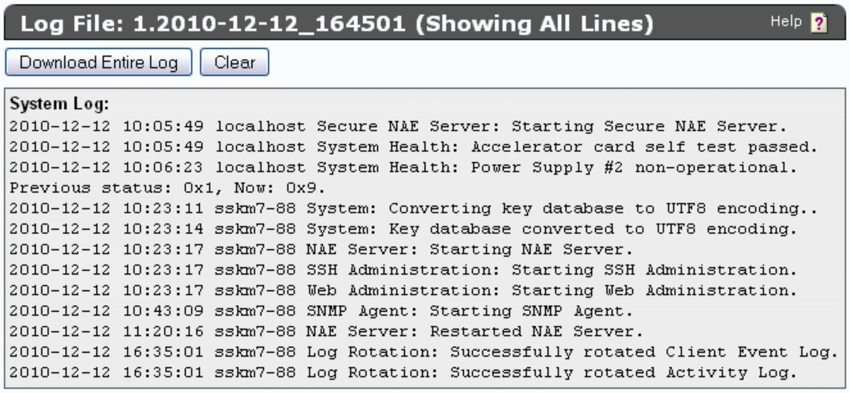
Wrap Lines: ☑

4 Select the file from the **Log File** list.

5 Select the number of lines to display in the **Show Last Number of Lines** field.

6 Select **Wrap Lines** to wrap long log entries in the display area.

7 Select **Display Log**. The log is now viewable in the display area:



```
System Log:
2010-12-12 10:05:49 localhost Secure NAE Server: Starting Secure NAE Server.
2010-12-12 10:05:49 localhost System Health: Accelerator card self test passed.
2010-12-12 10:06:23 localhost System Health: Power Supply #2 non-operational.
Previous status: 0x1, Now: 0x9.
2010-12-12 10:23:11 sskm7-88 System: Converting key database to UTF8 encoding..
2010-12-12 10:23:14 sskm7-88 System: Key database converted to UTF8 encoding.
2010-12-12 10:23:17 sskm7-88 NAE Server: Starting NAE Server.
2010-12-12 10:23:17 sskm7-88 SSH Administration: Starting SSH Administration.
2010-12-12 10:23:17 sskm7-88 Web Administration: Starting Web Administration.
2010-12-12 10:43:09 sskm7-88 SNMP Agent: Starting SNMP Agent.
2010-12-12 11:20:16 sskm7-88 NAE Server: Restarted NAE Server.
2010-12-12 16:35:01 sskm7-88 Log Rotation: Successfully rotated Client Event Log.
2010-12-12 16:35:01 sskm7-88 Log Rotation: Successfully rotated Activity Log.
```

Rotate Logs

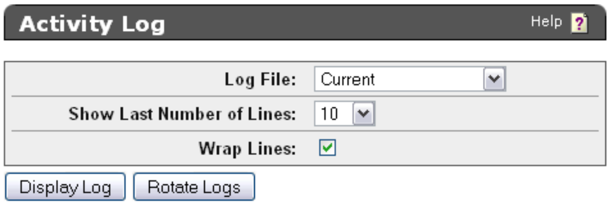
You can only rotate the system, activity, and client event logs. You cannot manually rotate the audit log.

To view the system log:

1 Log on to the Management Console.

2 Navigate to the Log Viewer page (Device >> Log Viewer).

3 Select the type of log to view in the left-hand navigation, either System, Activity, or Client Event. The current log file is displayed by default.



Log File:	Current
Show Last Number of Lines:	10
Wrap Lines:	☑

4 Select **Rotate Logs**. What was the current log will now be a log file with the current timestamp. You can view this by selecting the **Log File** drop-down list. The new current log will have the following entry "`Log Rotation: Successfully rotated x Log.`"

Clear Logs

You cannot clear an audit log.

To clear a log:

1 Log on to the Management Console.

2 Navigate to the Log Viewer page (Device >> Log Viewer).

3 Select the type of log to view in the left-hand navigation, either System, Activity, or Client Event. The current log file is displayed by default.

4 Choose a log in the **Log File** field.

5 Click **Display Log**.

6 Click **Clear**.

Download Logs

To download a log:

1 Log on to the Management Console.

2 Navigate to the Log Viewer page (Device >> Log Viewer).

3 Select the type of log to view in the left-hand navigation, either System, Audit, Activity, or Client Event. The current log file is displayed by default.

4 Choose a log in the **Log File** field.

5 Click **Display Log**.

6 Click **Download Entire Log** to download the log to your browser.

Chapter 21

Statistics

The Statistics page enables you to view real-time system statistics about client connections, network throughput, and cache, CPU, and memory utilization. The page displays information about the cryptographic requests made to the NAE-XML server.

Notes on the data provided in the Statistics page:

- The Refresh Period drop-down list is used to configure the refresh time on this page. The default setting is No Refresh.

  Note: Active Scripting must be enabled for proper functioning of the UI.

- A Reset Statistics button has been introduced to the page. This button basically resets all the cumulative statistics of the tables (averages and maximums) and restarts the sampling.
- In the statistical tables provided on this page, the Average and Maximum values are based on data collected since the last reboot or since the last Statistic Reset.
- The Maximum column shows the maximum value within all of the samples seen since the last reboot or Statistic Reset.
- CPU utilization data (always expressed as a percentage) is based on sample data gathered by queries performed approximately every 3 seconds.
- Incoming and Outgoing values for Key Server and Ethernet Interfaces are based on the sum of bytes being received or sent, respectively.
- Changes in data between current and previous queries are processed, as is the delay time between two queries. Throughput is derived from these deltas as follows: delta_mbytes/delta_sec = throughput.
- Averages are computed by dividing the sum of samples by the count of samples (Average= Sum_of_sample_values/count).

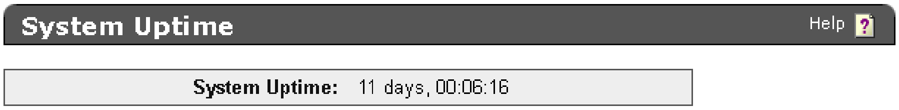
View System Statistics

The System Statistics section provides general system statistics, such as how much the CPUs are utilized and how long since the system was rebooted.

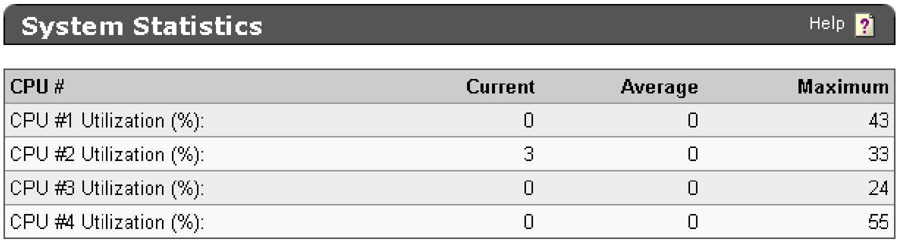
To view system statistics:

1. Log on the Management Console.
2. Navigate to the Statistics page (Device >> Statistics).
3. View the data in the System Uptime section.
   - System Uptime - the duration of time elapsed since the last reboot.
4. View the data in the System Statistics section.

- **CPU Utilization** - the percentage of CPU time that in use for each CPU.



System Uptime: 11 days, 00:06:16



CPU #	Current	Average	Maximum
CPU #1 Utilization (%):	0	0	43
CPU #2 Utilization (%):	3	0	33
CPU #3 Utilization (%):	0	0	24
CPU #4 Utilization (%):	0	0	55

View Connection Statistics

The Connection Statistics section provides information on the total number of connections since the KeySecure was rebooted.

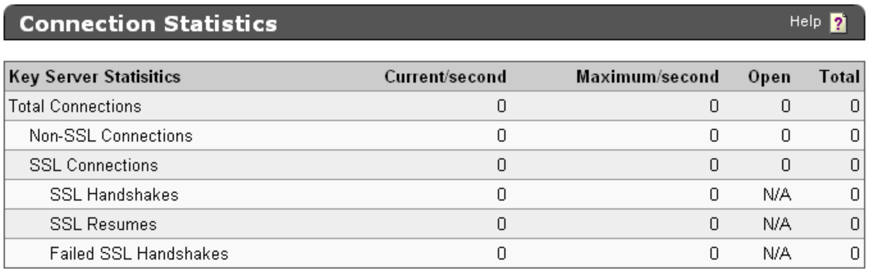
To view connection statistics:

1 Log on to the Management Console.

2 Navigate to the Statistics page (Device >> Statistics).

3 View the data in the Connection Statistics section. The section presents data for the following types of connections:

- Total Connections
- Non-SSL Connections
- SSL Connections
- SSL Handshakes
- SSL Resumes
- Failed SSL Handshakes



Key Server Statisitics	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

For each connection type, the section shows the current connections per second (**Current/second**), the maximum connection number for each type (**Maximum/second**), the number of open connections

(**Open**), and the total number of all connections (**Total**). Note that **Open** is not applicable to SSL Handshakes, SSL Resumes, and Failed SSL Handshakes, since those events do not remain open.

View Throughput Statistics

The Throughput section shows statistics for data traffic on each physical interface on the KeySecure.

Understanding Throughput Data

Notes:

The standard unit of measure for throughput statistics is megabytes per second. The data are based on measurements precise to the millisecond.

Incoming and Outgoing values for Key Server and Ethernet Interfaces are based on the sum of bytes being received or sent, respectively.

Averages are computed by dividing the sum of samples by the count of samples (Average= Sum_of_sample_values/count).

The Maximum column shows the maximum value within all of the samples seen since the last reboot or Statistic Reset.

To obtain throughput, changes in the rate of Mbits per second between current and previous queries are processed, as is the exact delay time between two queries. Throughput is derived from these deltas as follows: delta_mbytes/delta_sec = throughput.

To view Throughput Statistics:

1 Log on to the Management Console.

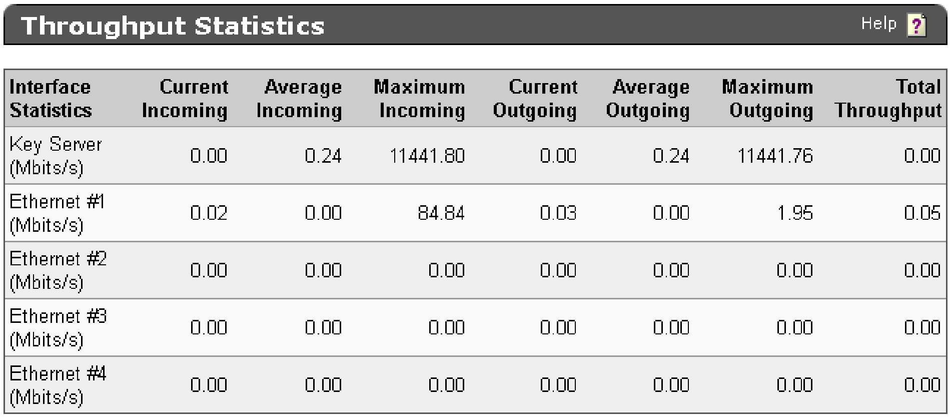
2 Navigate to the Statistics page (Device >> Statistics) and scroll down.

3 View the data in the Throughput Statistics section. The section presents data for each interface: Key Server and Ethernet.

  - **Key Server Interface Statistics** - This row expresses in megabits per second the amount of data passing through the Key Server. This traffic is generated when the KeySecure processes client requests. This does not include any overhead from the SSL, TCP, or IP protocols. Furthermore, this does not include traffic to the Management Console or the SSH administration tool.
    - **Current Incoming** - result of most recent query for bytes flowing into the Key Server as a result of client requests.
    - **Average Incoming** - average of queries for bytes flowing into the Key Server as a result of client requests.
    - **Maximum Incoming** - maximum bytes flowing into the Key Server as a result of client requests.
    - **Current Outgoing** - result of most recent query for bytes flowing out of the Key Server as a result of responses to client requests.
    - **Average Outgoing** - average of bytes flowing out of the Key Server as a result of responses to client requests.

- **Maximum Outgoing** - maximum bytes flowing out of the Key Server as a result of responses to client requests.
- **Total Throughput** - the rate at which bytes are flowing into and out of the KeySecure for client traffic.

- **Ethernet Interface Statistics** - This row expresses in megabits per second the amount of data passing through each interface on the KeySecure. The Interface Statistics measure all traffic flowing through the box, including data generated from client requests, SSH connections, SNMP traps, log rotation, etc.
  - Columns for Ethernet Interface Statistics are as for Key Server Statistics. See the column definitions above, under the Key Server heading.



Throughput Statistics

Interface Statistics	Current Incoming	Average Incoming	Maximum Incoming	Current Outgoing	Average Outgoing	Maximum Outgoing	Total Throughput
Key Server (Mbits/s)	0.00	0.24	11441.80	0.00	0.24	11441.76	0.00
Ethernet #1 (Mbits/s)	0.02	0.00	84.84	0.03	0.00	1.95	0.05
Ethernet #2 (Mbits/s)	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Ethernet #3 (Mbits/s)	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Ethernet #4 (Mbits/s)	0.00	0.00	0.00	0.00	0.00	0.00	0.00

View License Usage

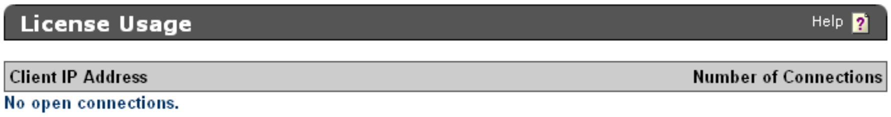
The License Usage section shows how many clients are connected to a KeySecure at any given time.

To view throughput statistics:

1 Log on to the Management Console.

2 Navigate to the Statistics page (Device >> Statistics).

3 View the data in the License Usage section. The section lists the **Client IP Address**es for each device connected to the KeySecure and displays the **Number of Connections** for each IP. Only client connections established on the Key Server Port (defined on the Key Server Configuration page) are counted. Administrative connections are not counted.



License Usage

Client IP Address	Number of Connections

No open connections.

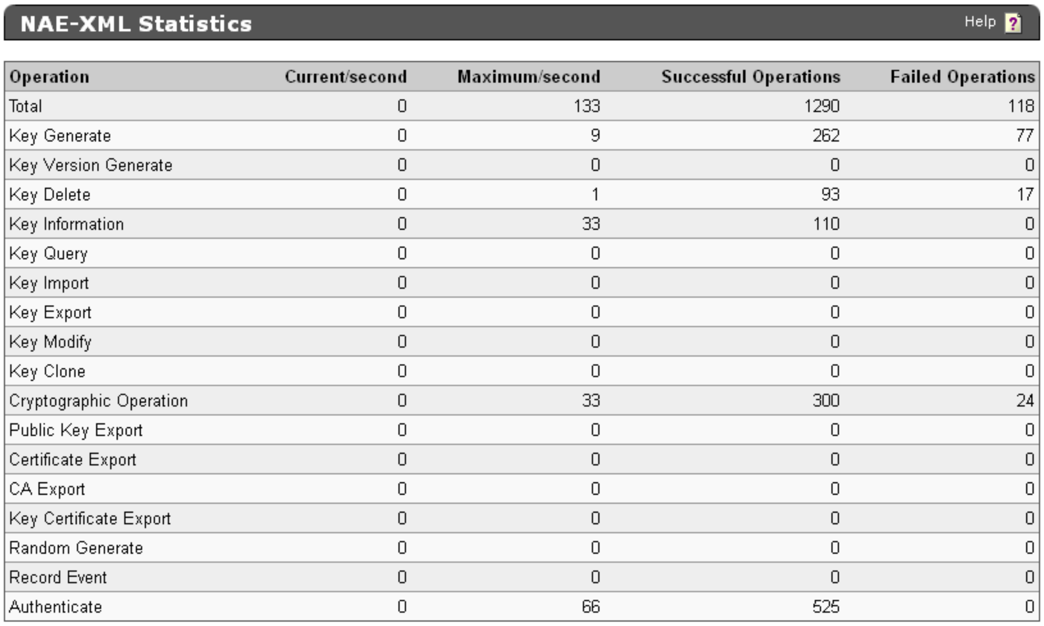
View NAE-XML Statistics

The NAE-XML Statistics section shows statistics for client usage of the Key Server via the NAE-XML protocol. Statistics are broken out by operation.

To view NAE-XML statistics:

1. Log on to the Management Console.
2. Navigate to the NAE-XML Statistics page (Device >> Statistics>> NAE-XML Statistics).
3. View the data in the NAE-XML Statistics section. The section displays the following fields:
   - **Operations**
     - *Total* - total number of NAE-XML client requests since the KeySecure was last rebooted.
     - *Key Generate* - request to generate a cryptographic key.
     - *Key Version Generate* - request to generate a new version of a key.
     - *Key Delete* - request to delete a key.
     - *Key Information* - requests for information about a particular 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.
     - *Cryptographic Operation* - request to perform a cryptographic operation.
     - *Public Key Export* - request to export a public key.
     - *Certificate Export* - request to export a certificate.
     - *CA Export* - request to export a CA.
     - *Key Certificate Export* - request to export a key certificate.
     - *Random Generate* - request to generate a random byte sequence.
     - *Record Event* - request to record an event from a client
     - *Authenticate* - request to authenticate.

- **Current/second** - shows how many of a given statistic were counted on the KeySecure in the second the NAE-XML Statistics were refreshed.
- **Maximum/second** - shows the maximum number of a given statistic that were counted by the KeySecure during any one second.
- **Successful Operations** - displays the number of successful operations.
- **Failed Operations** - displays the number of failed operations.



Operation	Current/second	Maximum/second	Successful Operations	Failed Operations
Total	0	133	1290	118
Key Generate	0	9	262	77
Key Version Generate	0	0	0	0
Key Delete	0	1	93	17
Key Information	0	33	110	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 Clone	0	0	0	0
Cryptographic Operation	0	33	300	24
Public Key Export	0	0	0	0
Certificate Export	0	0	0	0
CA Export	0	0	0	0
Key Certificate Export	0	0	0	0
Random Generate	0	0	0	0
Record Event	0	0	0	0
Authenticate	0	66	525	0

Important! This page tracks client requests to the Key Server only. It does *not* include operations initiated directly by this device, such as operations performed through the Management Console.

View KMIP Statistics

The KMIP Statistics section shows statistics for client usage of the Key Server via the KMIP protocol. Statistics are broken out by operation.

Note: In the list below, the KMIP operations performed on “objects” refer to operations performed on KMIP managed objects (e.g., keys, certificates).

To view KMIP statistics:

1 Log on to the Management Console.

2 Navigate to the KMIP Statistics page (Device >> Statistics>> KMIP Statistics).

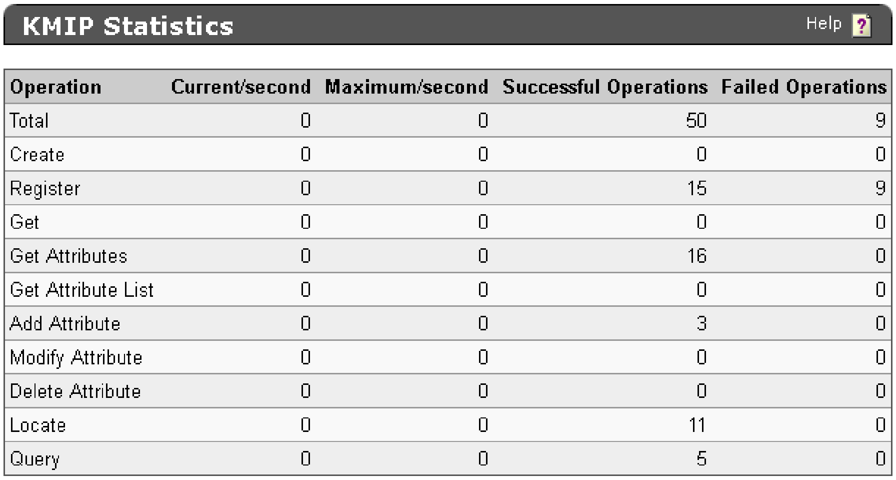
3 View the data in the KMIP Statistics section. The table lists data for the following **Operations**:

- *Total* - total number of KMIP client requests since the last reboot.
- *Create* - request to create an object through KMIP.
- *Register* - request to register (import) an object through KMIP.

- *Get* - request to get (fetch) an object through KMIP.
- *Get Attributes* - request to get (fetch) an object attribute through KMIP.
- *Get Attribute List* - request to get (fetch) a list of object attributes through KMIP.
- *Add Attribute* - request to add an object attribute through KMIP.
- *Modify Attribute* - request to modify an object attribute through KMIP.
- *Delete Attribute* - request to delete an attribute through KMIP.
- *Locate* - request to locate an object through KMIP.
- *Query* - request to search for an object through KMIP.

The columns display information as follows:

- **Current/second** - shows how many of a given statistic were counted on the KeySecure in the second the KMIP Statistics were refreshed.
- **Maximum/second** - shows the maximum number of a given statistic that were counted by the KeySecure during any one second.
- **Successful Operations** - displays the number of successful operations.
- **Failed Operations** - displays the number of failed operations.



Operation	Current/second	Maximum/second	Successful Operations	Failed Operations
Total	0	0	50	9
Create	0	0	0	0
Register	0	0	15	9
Get	0	0	0	0
Get Attributes	0	0	16	0
Get Attribute List	0	0	0	0
Add Attribute	0	0	3	0
Modify Attribute	0	0	0	0
Delete Attribute	0	0	0	0
Locate	0	0	11	0
Query	0	0	5	0

Important! This page tracks client requests to the Key Server only. It does not include operations initiated directly by this device, such as operations performed through the Management Console.

Chapter 22

Backups

Use the Backup and Restore page to create and restore backups of system configuration. You can also view backup files stored on the KeySecure.

Permission Requirements

On the KeySecure k460 platform with an imbedded Luna HSM card, permission from the security officer is required before performing a backup or restore operation. This permission is granted with a HSM PED key USB device, known as an iKey. The permission procedure contains the following three steps.

1. The security officer logs in. If the security officer is already logged, it is not necessary to log out and log in again.
2. Plug the iKey into the USB port.
3. Enter the passcode when prompted on the pad.

   WARNING: If the security officer does not enter the correct code within three tried, all keys are deleted. Be sure to know the code before plugging in the iKey.

After this procedure, the security officer can perform any backup or restore operations.

Creating a Backup

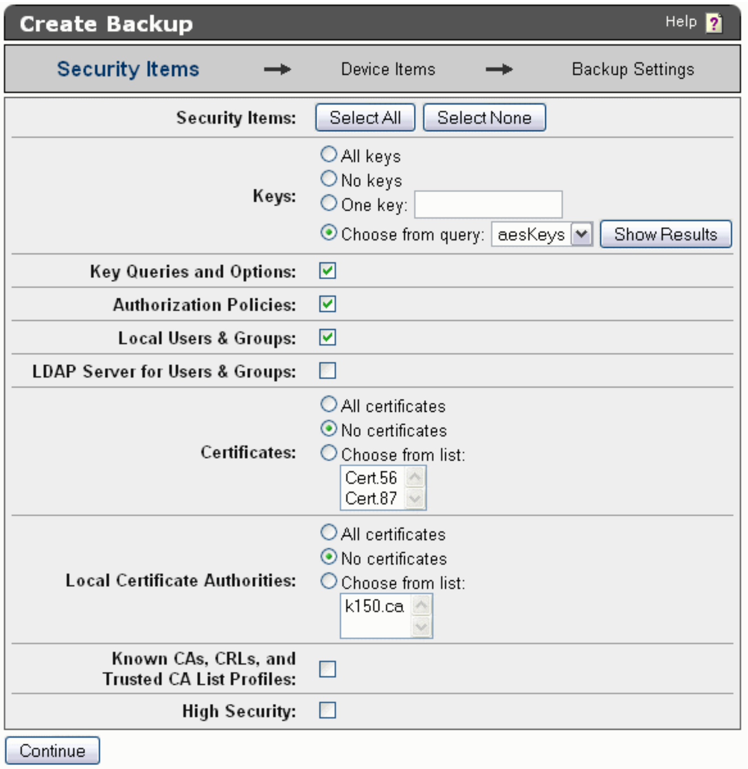
The KeySecure backup mechanism allows you to back up information on the device or externally, to be restored in case of a failure. Once a device is fully configured, we recommend that the entire configuration be backed up. After making any changes to your configuration (e.g., adding keys), create additional backups.

- See “Restoring a Backup” on page 123 to learn more about what backups can do and how to get optimal results from the restoration process.
- “Backup and Restore in a Clustered Environment” on page 126 for information and best practices for backup and restoral in a clustered environment.

Note: To set up an automatic scheduled remote backup, you must start by creating a backup, using the instructions provided here.

To create a backup:

1. Log on to the Management Console as an administrator with the appropriate backup access control. There are specific access controls for backing up configuration, keys & certificates, and local CAs.
2. Navigate to the Backup and Restore page (Device >> Maintenance >> Backup & Restore).



Create Backup

Security Items → Device Items → Backup Settings

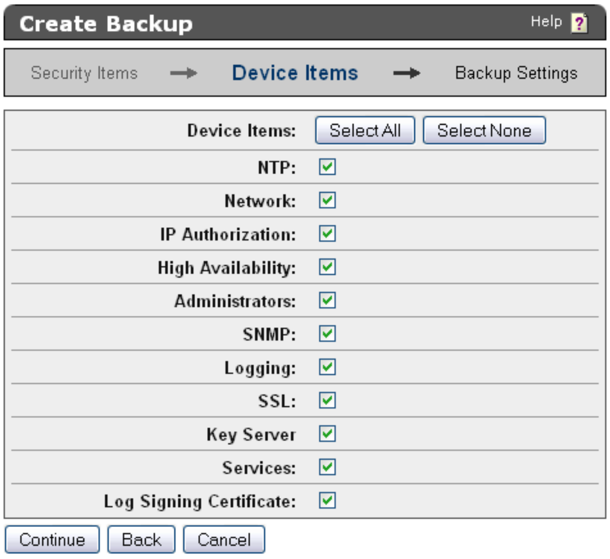
Security Items:	Select All Select None
Keys:	○ All keys ○ No keys ○ One key: ● Choose from query: aesKeys Show Results
Key Queries and Options:	☑
Authorization Policies:	☑
Local Users & Groups:	☑
LDAP Server for Users & Groups:	□
Certificates:	○ All certificates ● No certificates ○ Choose from list: Cert.56 Cert.87
Local Certificate Authorities:	○ All certificates ● No certificates ○ Choose from list: k150.ca
Known CAs, CRLs, and Trusted CA List Profiles:	□
High Security:	□

Continue

3 Select the configuration items to include in the backup file. Use **Select All** to select all items on the page. When selecting **Keys**, you have the option of selecting all keys, no keys, specific keys, or backing up the results of a query. You can view the query results using the **Show Results** button. When selecting **Certificates** and **Local Certificate Authorities**, you can select all, none, or select items from a list.

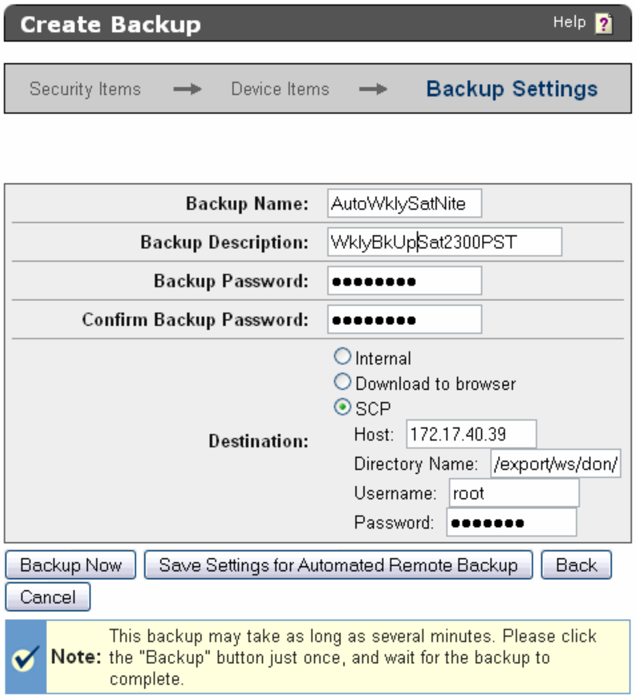
Note: The Log Signing Certificate is not included with the other certificates on the device. To backup the log signing certificate, you must specifically select it on the next page.

4 Select **Continue** to access the next group of configuration items.



Device Items:	
NTP:	☑
Network:	☑
IP Authorization:	☑
High Availability:	☑
Administrators:	☑
SNMP:	☑
Logging:	☑
SSL:	☑
Key Server	☑
Services:	☑
Log Signing Certificate:	☑

5 Use **Select All**, **Select None**, and **Back** to perfect your list. Select **Continue** to access the Backup Settings page.


Create Backup
Help
Security Items → Device Items → Backup Settings
Backup Now
Save Settings for Automated Remote Backup
Back
Cancel

Backup Name:	AutoWklySatNite
Backup Description:	WklyBkUpSat2300PST
Backup Password:	●●●●●●●●
Confirm Backup Password:	●●●●●●●●
Destination:	○ Internal ○ Download to browser ● SCP Host: 172.17.40.39 Directory Name: /export/ws/don/ Username: root 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.

6 Configure the details of the backup file itself: name, description, and password:

- **Backup Name** - Enter a name for the backup. Special characters and whitespace are not allowed in backup names; use only alphanumeric characters. For backups stored externally, the backup filename is created by appending _0_bkp to this name. For large backups, the zero is incremented by 1 for each additional file. For example, backup *foo* could consist of two files: foo_0_bkp and foo_1_bkp.
- **Backup Description** - Enter a short description for the backup.
- **Backup Password** - Enter a password for your backup file. Remember, this file contains very valuable information and will likely have a long life span. Use an appropriately complex password. The password can have a maximum of 30 characters.

WARNING: The backup file cannot be restored without this password.

7 Enter the **Destination** of the file. The backup configuration can be stored internally on the KeySecure, downloaded to a browser, or copied to another machine via FTP or SCP.

If you intend to schedule this backup using the Automated Remote Backup Schedule option, then you must select SCP. This will enable the button labeled Save Settings for Automated Remote Backup.

Note: If you are creating this backup in anticipation of doing a software upgrade immediately after, we recommend that you store the backup file *externally*.

Note: FTP will not be available if the device is FIPS compliant.

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 FTP or SCP to copy the backup configuration to another machine, you must provide the following:

- the destination host.
- the name of the directory on the destination host. (You must have write permission for this directory.)
- the username of the account on the destination host.
- the password for the user account on the destination host.

8 Before proceeding, review the Backup Summary listing. If you need to make changes, use the Back button to return to appropriate page and make the necessary edits. After making changes, you may have to re-enter data in the last page, Backup Settings.

9 If you need to complete a one-time backup immediately, select **Backup Now** to create and store the backup file, then click Save. Confirm your save when requested to do so.

Note: The backup you have defined is started immediately when you click Backup Now. The detailed settings used by Backup Now processing are not preserved, so you may wish to keep a record of these settings yourself. To see a summary of the contents of the backup file (without restoring any part of it), use the initial steps of the Restore Backup process.

10To set up a schedule that automatically runs the backup you have just configured, click **Save Settings for Automated Remote Backup**. See “Schedule an Automated Remote Backup”, below, for instructions.

- If you have already saved settings for an automated remote backup, you will be allowed to cancel or to confirm your new backup definition as the replacement. Be aware that *you can only have one scheduled backup definition set up at a time*; if you save a new set, it will overwrite any existing one.

11 Confirm your save when requested to do so.

Schedule an Automated Remote Backup

To set up an automated remote backup, you must use an extension of the Create Backup workflow. Start the process of creating a scheduled automated remote backup by following the instructions for Creating a Backup, above.

Tip: Do not click **Automated Remote Backup Schedule** unless you want to edit an existing scheduled backup.

Setting up a scheduled automated remote backup is a two-part process. First you must define the backup by using the Create Backup option (see above). Then you can use the Automated Remote Backup options described below to schedule the backup. The resulting remote backup process is repeated automatically according to the schedule you define.

Note that you can only have one scheduled automated remote backup definition set up at a time; if you save a new automatic backup, it will overwrite any existing one.

Prerequisite: In order to set up the automated remote backup so that scheduling is enabled, *you must specify and save an SCP Host and Directory Name in the final stage of the* Create Backup *Process.*

To set up the schedule for an automatic remote backup – immediately after you have defined the SCP Host data using step 8 of the Create Backup process:

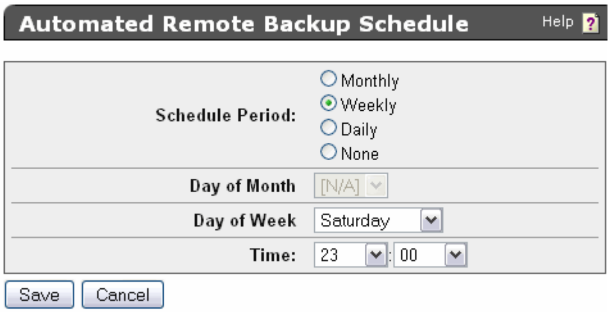
1 Click **Save Settings for Automated Remote Backup** to set up a schedule that automatically runs the backup you have just configured.

A message appears, informing you that your backup settings will not take effect until an Automate Backup Schedule is setup and enabled.

2 Click Continue**.**

The Automated Remote Backup Schedule page appears, allowing you to set up the schedule.

3 Click Edit.



Automated Remote Backup Schedule

Schedule Period:	○ Monthly ● Weekly ○ Daily ○ None
Day of Month	[N/A]
Day of Week	Saturday
Time:	23 : 00

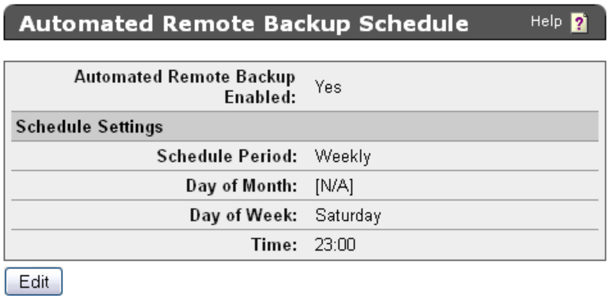
WARNING: If you edit an existing schedule, the new schedule overwrites and replaces the old one.

4 Select a monthly, weekly, or daily backup schedule and click **Save.**

This completes the scheduling of the automatic remote backup. The page does not close. Confirmation is provided when real data populates the “Last Automated Remote Backup Status” table (see sample in the illustration below).

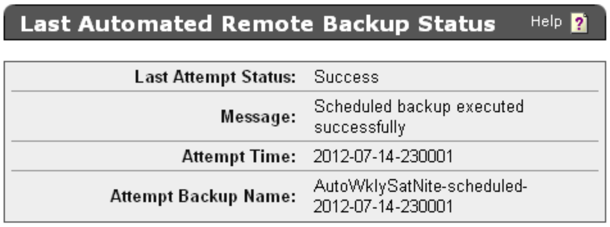
Note: To end scheduled backups and delete an automated remote backup schedule, select **None** and **Save** instead of setting a schedule. All associated backup and scheduling data will be permamently deleted.

At the scheduled time, the defined backup will run, and the information on the page will be updated to show the “Last Automated Remote Backup Status” data.



Automated Remote Backup Schedule

Automated Remote Backup Enabled:	Yes
Schedule Settings	
Schedule Period:	Weekly
Day of Month:	[N/A]
Day of Week:	Saturday
Time:	23:00



Last Automated Remote Backup Status

Last Attempt Status:	Success
Message:	Scheduled backup executed successfully
Attempt Time:	2012-07-14-230001
Attempt Backup Name:	AutoWklySatNite-scheduled-2012-07-14-230001

5 To check information about your most recent automatic backup at any time, navigate to the Backup and Restore page (Device >> Maintenance >> Backup & Restore) and click Automated Remote Backup Schedule.

Note: The automated backup, when triggered per schedule, generates a file named according to this convention: <user_defined_backup_name>-scheduled-<yyyy-mm-dd-hhmmss>_<0/1 (file_size_indicator_digit)>_bkp. No extension/specific file type is associated with a backup file; it is an encrypted binary file that only SafeNet appliances can read.

Restoring a Backup

When restoring a backup, you can select which components of the backup file to restore - you do not have to restore all items in the file. When doing so, unselected items in the backup are ignored. If you choose to restore only NTP settings from a backup, no other configuration items would be affected by this restore.

In general, once you select which items to restore, the current settings for those items are cleared from the KeySecure before the settings from the backup file are restored in their place. So when you restore NTP settings, expect that the current KeySecure NTP settings will be overwritten by the data in the backup.

Restoring keys, certificates, or local CAs, in contrast, is an **additive** process. The KeySecure 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 your KeySecure has Key1 and Key2, restoring Key3 from the backup file will result in the KeySecure having Key1, Key2, and Key3.

If one of these objects is being restored on a device where there is already a similar object with the same name (for example, both are symmetric keys with the same name), the backup file *overwrites* the existing object. For example, your KeySecure has Key1, a global key, but the backup file has Key1, owned by user1. Restoring that backup file will remove the global Key1 and replace it with Key1 owned by user1.

If one key is symmetric and the other is asymmetric, the restored key will *not overwrite* the old key. However, since there will then be two keys in the system with the same name, neither will be available for use, and there is no way to delete or rename the key.

Important! For versioned keys, this means that if your backup file contains a versioned key, the backup will overwrite the existing object *even if the existing object has newer versions*. Those newer versions will be *deleted*. You should backup each new key version upon creation.

To restore a backup

1 Log on to the Management Console as an administrator with the appropriate Restore access control. There are specific access controls for restoring configuration, keys & certificates, and local CAs.

2 Navigate to the Restore Backup section (Device >> Maintenance >> Backup & Restore >> Restore Backup).

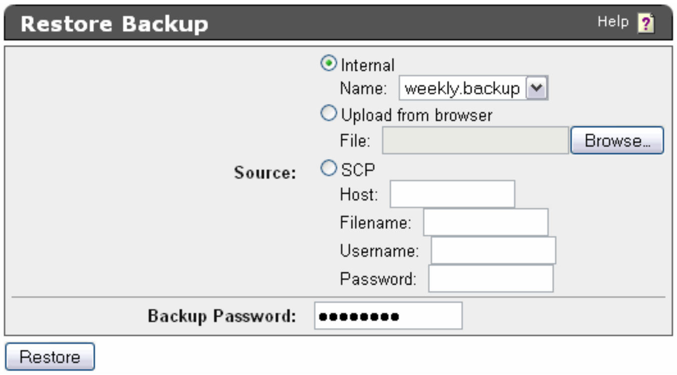
3 Enter the **Source** of the backup. When restoring a backup that spans multiple files, specify the zeroth file here (for example, WeeklyBackup_0_bkp). Specifying the zeroth file indicates to the KeySecure that the backup contains multiple files; the KeySecure will then automatically transfer all of the backup files.

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 KeySecure via FTP or SCP.

If you are copying the backup configuration to your KeySecure via FTP or SCP, you must provide the following:

- the source host.
- the name of the file on the source host. For backups that span multiple files, enter the <name>_0_bkp file here. The system will then upload all of the <name> files in that directory.
- the username of the account on the source host.
- the password for the user account on the source host.

Backup files larger than 100 MB, and backups that span multiple files cannot be transferred through the browser. You must use SCP or FTP to upload these files.



Restore Backup

Source:
● Internal
Name: weekly.backup
○ Upload from browser
File: [Browse...]
○ SCP
Host:
Filename:
Username:
Password:

Backup Password: ●●●●●●●●●

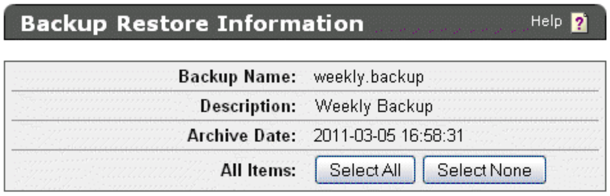
4 Enter the **Backup Password**.

5 Select **Restore**.

Important! When restoring a key to the KeySecure, the key must conform to the appliance's 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. 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 View the Backup Restore Information. Select the specific items to restore.



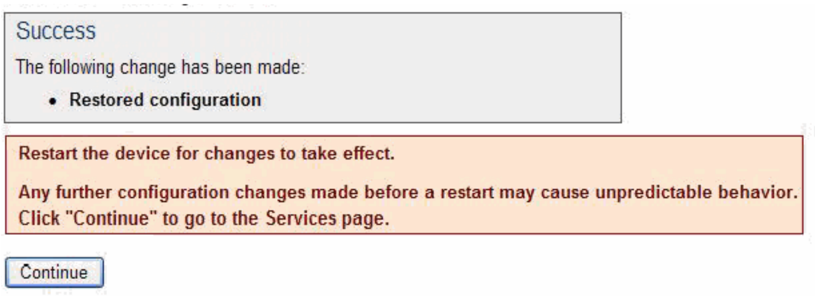
Backup Restore Information

Backup Name:	weekly.backup
Description:	Weekly Backup
Archive Date:	2011-03-05 16:58:31
All Items:	Select All Select None

7 Enter the **Backup Password**, again.

8 Click **Restore**.

A confirmation page appears, titled “Action Completed”. Be aware that, for changes to take effect, you will need to restart the device.



Success

The following change has been made:

- **Restored configuration**

Restart the device for changes to take effect.

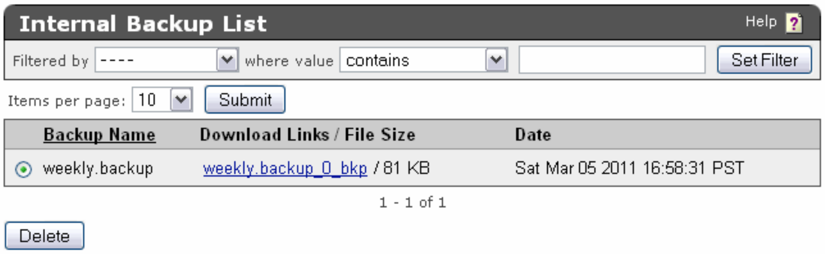
Any further configuration changes made before a restart may cause unpredictable behavior.
Click "Continue" to go to the Services page.

View the List of Internal Backups

To view the list of internal backups:

1 Log on to the Management Console.

2 Navigate to the Internal Backups section (Device >> Maintenance >> Backup & Restore >> Internal Backups).



Internal Backup List

Filtered by: ---- where value: contains

Items per page: 10

Backup Name	Download Links / File Size	Date
● weekly.backup	weekly.backup_0_bkp / 81 KB	Sat Mar 05 2011 16:58:31 PST

1 - 1 of 1

3 View the list of backup files stored on the device. Click the download link to download the files to the browser. Large backups will contain multiple files. Click **Delete** if confident enough to lose the backup information forever.

Backup/Restore Compatibility

- Backups from virtual appliance and physical appliance are not compatible. The backup from virtual appliance cannot be restored on a physical appliance, or vice versa.
- For physical appliance backups, backups taken on a higher KeySecure version cannot be restored on a lower version KeySecure. For example, backups taken on KeySecure version 6.5.0 cannot be restored on KeySecure version 6.4.0.
- For physical appliance, a backup taken on one k460 appliance can be restored on any other k460 appliance.

- For physical appliance backups, backup and restore between versions 6.4.1 and 7.0.1, and 6.5.0 and 7.1.0 are supported.

Backup and Restore in a Clustered Environment

The following two items are not transferred across clustering. You must use a device backup to transfer or otherwise keep this information.

- Device SSL Certificates
- Device Network Settings (IP settings, etc.)

Best Practice: Backup each device in a cluster individually. Restart the appliance after restoring a backup.

Restoring a key does not trigger automatic updates to other cluster nodes. If you restore many keys there are two options: (1) manually sync all cluster nodes to updated correct node, or (2) restore backups to all nodes.

Manual syncing performs the following three operations.

- Creates a copy of all clustered information on the appliance with which you are syncing.
- Transfers that copy to the initiating device.
- Restores that copy in the initiating device.

Manual syncing includes all clustered information and cannot be restricted in any fashion. Devices performing a manual sync cannot service requests properly until the sync is completed and services are restarted.

Chapter 23

Services

Use the Services Configuration page to start and stop the key servers, web administration service, ssh administration service, and snmp agent, restart those services, enable a service to launch at system startup, disable launch at system startup, restart the KeySecure, and halt the KeySecure.

The following services are available on the KeySecure:

- **NAE Server** - manages all incoming and outgoing connections, both secure and clear text.
- **SNMP Agent** - the KeySecure's SNMP service that enables it to send alerts over the network to monitor system activity.
- **SSH Administration** - the Command Line Interface (CLI) tool that enables administrators to configure the KeySecure over a remote ssh connection.
- **Web Administration** - the Management Console, that enables administrators to configure the KeySecure through a web browser.

Start, Stop, or Restart Services

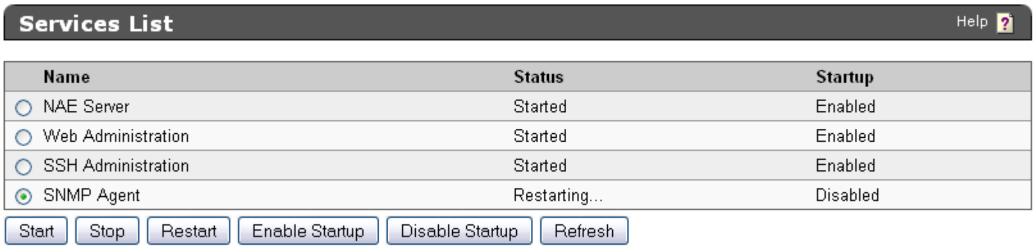
To start or stop a service:

1 Log on to the Management Console.

2 Navigate to the Services Configuration page (Device >> Maintenance >> Services).

3 Select the service.

4 Select either **Start**, **Stop**, or **Restart**. The service's **Status** will change to *Starting...*, *Stopping...*, or *Restarting....*



Services List

	Name	Status	Startup
○	NAE Server	Started	Enabled
○	Web Administration	Started	Enabled
○	SSH Administration	Started	Enabled
●	SNMP Agent	Restarting...	Disabled

5 Select **Refresh** to refresh the page and see the service's new status.

Launch a Service at System Startup

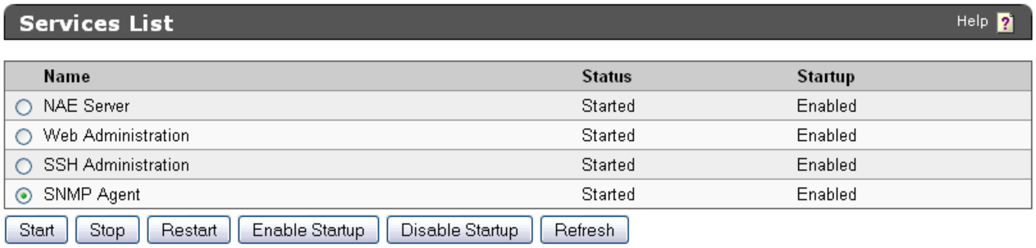
To configure that a service start when the KeySecure starts up:

1 Log on to the Management Console.

2 Navigate to the Services Configuration page (Device >> Maintenance >> Services).

3 Select the service

4 Click **Enable Startup**.



Services List

	Name	Status	Startup
○	NAE Server	Started	Enabled
○	Web Administration	Started	Enabled
○	SSH Administration	Started	Enabled
●	SNMP Agent	Started	Enabled

You can likewise disable a service at startup by selecting **Disable Startup**.

Restart the KeySecure

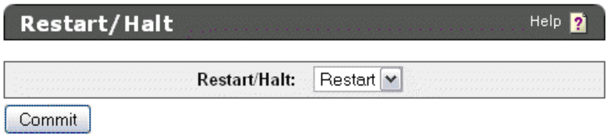
Important! Remove any peripheral devices connected to the keyboard, mouse, and video ports on the KeySecure before restarting. Use of these ports during the restart process can cause the process to hang.

To restart the KeySecure:

1 Log on to the Management Console.

2 Navigate to the Restart/Halt page (Device >> Maintenance >> Services).

3 Select *Restart* in the **Restart/Halt** field.



Restart/Halt

Restart/Halt: Restart

4 Click **Commit**. This will terminate all active connections to the KeySecure.

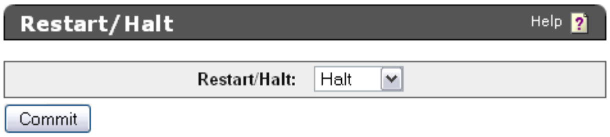
Halt the KeySecure

To restart the KeySecure:

1 Log on to the Management Console.

2 Navigate to the Restart/Halt page (Device >> Maintenance >> Services).

3 Select *Halt* in the **Restart/Halt** field.



Restart/Halt

Restart/Halt: Halt

4 Click **Commit**. This will terminate all active connections to the KeySecure.

Chapter 24

Upgrade

Use the System Information page to perform software upgrades, upload licenses, and examine information about the system, including Box ID and current software version.

View Device Information

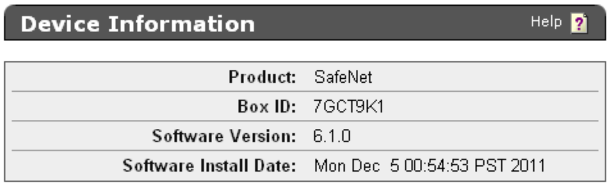
Device information is the product's model name (e.g., SafeNet k460), **Box ID**, **Software Version**, and **Software Install Date**. You will need to the **Box ID** should you ever contact our Customer Support Department. The software referred to is the software running on the KeySecure.

To view device information:

1 Log on to the Management Console.

2 Navigate to the Device Information page (Device >> Maintenance >> System Information & Upgrade).

3 View the information. The fields are not editable.



Product:	SafeNet
Box ID:	7GCT9K1
Software Version:	6.1.0
Software Install Date:	Mon Dec 5 00:54:53 PST 2011

View License Information

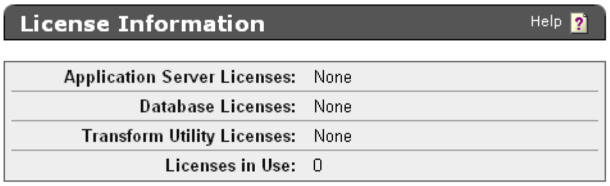
Licenses allow a set number of client devices to connect to the KeySecure at any particular time; once the set number of clients has been reached, subsequent connection requests are refused until another connection has been terminated. Before any clients can connect to the KeySecure, you must install a valid license. Licenses can be obtained from Customer Support.

To view license information:

1 Log on to the Management Console

2 Navigate to the License Information page (Device >> Maintenance >> System Information & Upgrade).

3 View the information. The fields are not editable.



Application Server Licenses:	None
Database Licenses:	None
Transform Utility Licenses:	None
Licenses in Use:	0

View the Feature Activation List

The Feature Activation List displays the complete list of additional features running on the KeySecure, including their names, activation and expiration dates, and current status.

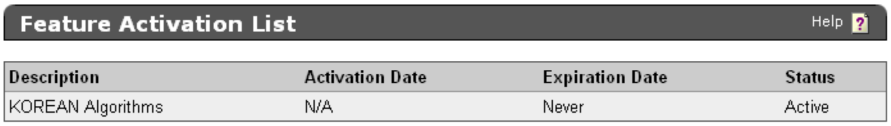
Installing and activating software on the KeySecure are separate processes. Software must be installed and activated on the KeySecure before it can be used. A software component might be installed but not active. Once activated, a component cannot be specifically de-activated. You would have to rollback the server software to a point before the software was activated.

To view the feature activation list:

1 Log on to the Management Console

2 Navigate to the Network Diagnostics page (Device >> Maintenance >> System Information & Upgrade).

3 View the information. The fields are not editable.



Description	Activation Date	Expiration Date	Status
KOREAN Algorithms	N/A	Never	Active

Install Software Licenses

The software upgrade and installation mechanism can be used to install licenses.

License file installation must be applied to all KeySecures individually in a cluster - the file upload is not replicated across members of a cluster. If you have an existing license, and you have purchased additional licenses, you can simply install the new license file you receive from KeySecure.

To safeguard KeySecures, only license files signed by SafeNet, Inc. can be installed on the KeySecure.

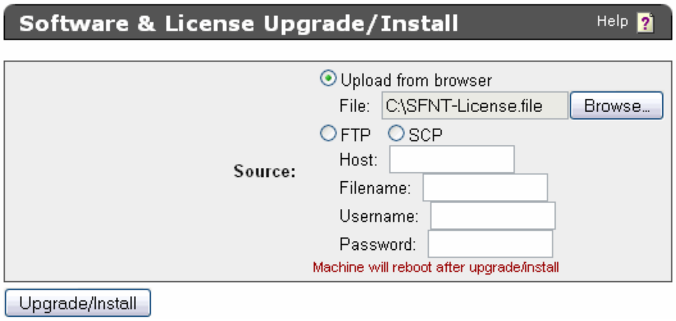
To install a software license:

1 Obtain the license

2 Log on the Management Console.

3 Navigate to the Software & License Upgrade/Install page (Device >> Maintenance >> System Information & Upgrade).

4 Select the method of uploading the license file. Either by selecting Upload from browser and clicking **Browse** to locate the file on the local drive or network. Or by selecting FTP or SCP and then specifying the Host (source host), Filename (the name of the file on the source host), Username (the username of the account on the source host), and password (the username password) needed to locate and access the file.



Software & License Upgrade/Install

Source:

● Upload from browser

File: C:\SFNT-License.file

○ FTP ○ SCP

Host:

Filename:

Username:

Password:

Machine will reboot after upgrade/install

5 Click **Upgrade/Install** to upload the license file. The system will reboot when the file is uploaded.

Upgrade Software

The software upgrade and installation mechanism can be used to install new features, upgrade core software, and apply security patches. 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, you should perform the upgrade from the Command Line Interface.

Software upgrades must be applied to all KeySecures individually in a cluster - the file upload is not replicated across members of a cluster.

To safeguard KeySecures, only software files signed by SafeNet, Inc. can be installed on the KeySecure. Changes to multiple components of the system are bundled together in an encrypted software file provided by the Customer Service organization at SafeNet, Inc.

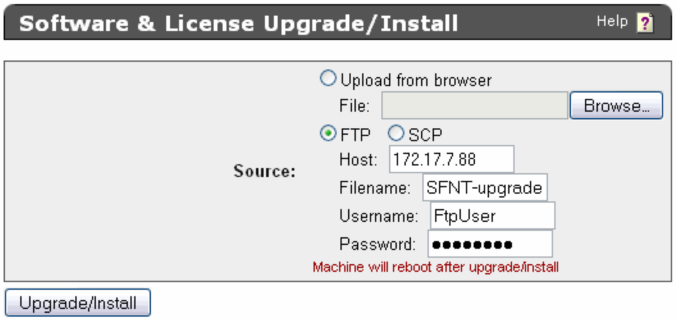
To install a software license:

1 Obtain the license

2 Log on the Management Console.

3 Navigate to the Software & License Upgrade/Install page (Device >> Maintenance >> System Information & Upgrade).

4 Select the method of uploading the software file. Either by selecting Upload from browser and clicking **Browse** to locate the file on the local drive or network. Or by selecting FTP or SCP and then specifying the Host (source host), Filename (the name of the file on the source host), Username (the username of the account on the source host), and password (the username password) needed to locate and access the file.



Source:
○ Upload from browser
File: Browse...
● FTP ○ SCP
Host: 172.17.7.88
Filename: SFNT-upgrade
Username: FtpUser
Password: ●●●●●●●●●
Machine will reboot after upgrade/install

5 Click **Upgrade/Install** to upload the software file. The system will reboot when the file is uploaded.

Upgrade to a Patch Release

Patch releases are lightweight, which means that customers do not have to re-qualify an entire release. All patches are cumulative, which means that the functionality in patch one exists in patch two, and so on. Because patches are cumulative, we recommend that you always install the most recent patch. We use the following nomenclature for patch releases:

KeySecure Version 5.3.1p1

where KeySecure Version 5.3.1 refers to the “base release” upon which the patch is built, and “p1” refers to the number of the patch. In this case, “p1” implies that this is the first patch release for KeySecure Version 5.3.1 and there are no other patches for this release. If this were patch 4, that would imply that there are three previous patches for the particular base release.

Roll Back Software

Occasionally it is necessary to roll back KeySecure software to a previous version. The KeySecure allows you to roll back one version of the software. For example, if you were originally running KeySecure Version 5.3.0, upgraded to KeySecure Version 5.3.0p1, and finally upgraded to KeySecure Version 5.4.0, you would only be able to do a software rollback to KeySecure Version 5.3.0p1. As such, we recommend that you avoid doing multiple patch upgrades on the same base release. What you should do instead is roll back from the patch release to the base release before doing the upgrade to the patch release.

Using the preceding example, the order of operations would be:

- upgrade from KeySecure Version 5.3.0 to KeySecure Version 5.3.0p1
- do a software rollback to KeySecure Version 5.3.0
- upgrade from KeySecure Version 5.3.0 to KeySecure Version 5.4.0.

Note: The software rollback process can be performed from the CLI only; it cannot be performed from the Management Console.

Important! Before performing a software rollback, **it is very important that you create a secured external 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 the base version you are rolling back to, those features will not be available after the software rollback.

Important! Rolling back the software returns your admin accounts to the settings they had before the last upgrade. If you cannot recall the old admin passwords you will not be able to log in to the KeySecure after the rollback. If you do not know the earlier admin passwords, you should backup your current configuration, and contact SafeNet support. (For contact information, see the inside front cover, page 2 of this document.) With the guidance of SafeNet support, you should be able to reset factory settings, upgrade to the desired software version and then restore the backup.

Chapter 25

System Health

The System Health page enables you to view the status of the KeySecure power supply and cooling fan.

When the KeySecure detects a change in the status of a power supply unit, the System Health page reflects the change and displays a warning message if appropriate. In addition, if your system is configured for SNMP, the KeySecure sends an SNMP trap to the SNMP Management Station indicating the change in status.

Set Refresh Page Time

The time period to refresh the System Health page can be configured. The refresh time interval can be set in the Refresh Every drop-down list available under the Refresh Page section. The default setting is Never.

After selecting a value in the **Refresh Every** drop-down list, click **Set Refresh Time**. To refresh the page immediately, click **Refresh Now**.

Note: Active Scripting must be enabled for proper functioning of the UI.

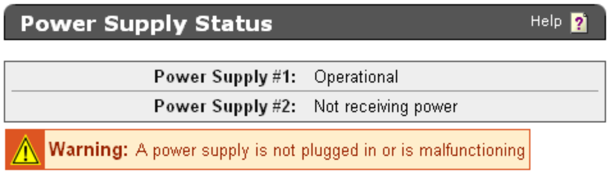
View Power Supply Status

The System Health page provides information on the status of the KeySecure power supply. For KeySecure models with multiple power supplies, this page can inform administrators when one power supply is not receiving power, has been removed, or is damaged. For KeySecures with one power supply, this page will only inform administrators when the power supply is operational, since you won’t be able to access the management console when that power supply is not functioning.

To view power supply status:

1. Log on to the Management Console.
2. Navigate to the System Health page (Device >> System Health).
3. View the **Power Supply** field. The following values are possible:

- Operational - The power supply unit is operational.
- Not receiving power - No power is supplied to the power supply unit. The system issues a warning stating that “A power supply is not plugged in or is malfunctioning.”
- Removed or damaged - The power supply unit has been removed from the KeySecure. The system issues a warning stating that “A power supply has been removed or damaged.”



Power Supply Status

Power Supply #1:	Operational
Power Supply #2:	Not receiving power

Warning: A power supply is not plugged in or is malfunctioning

View Cooling Fan Status

The Cooling Fan Status section provides information on the status all of the KeySecure cooling fans.

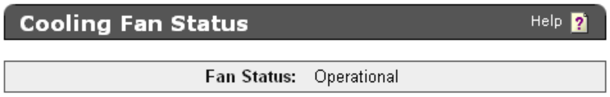
To view the status of a cooling fan:

1 Log on to the Management Console.

2 Navigate to the System Health page (Device >> System Health).

3 View the **Fan Status** field. The following values are possible:

- Operational - All fans are operational.
- Failure: One or more fans have stopped, lost power, or are broken. The system displays a warning message until the problem is resolved and power to the KeySecure is removed. The warning reads "Fan failure; please contact support immediately."



Fan Status: Operational

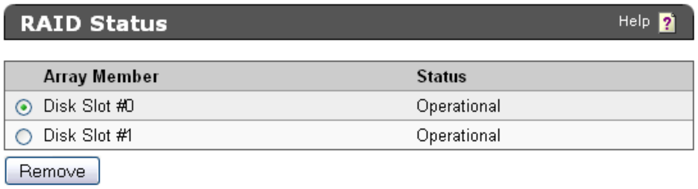
View RAID Status

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.

To view RAID status:

1 Log on to the Management Console.

2 Navigate to the RAID Status section of the System Health page (Device >> System Health).



Array Member	Status
● Disk Slot #0	Operational
○ Disk Slot #1	Operational

3 View the **Status** field for each Array Member. An **Array Member** refers to the physical disk slot of the hard disk. The **Status** can be one of the following:

- Operational – the disk is mirrored and in use.
- Failed – 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.
- Recovery – 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 – 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.

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 KeySecure 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 NAE Server must fulfill while the recovery is in progress.

WARNING! It is extremely important that you not reboot the system when a disk is in the recovery state. Such an action could render the system unstable or unusable. If the system experiences a power outage while a disk is recovering, we recommend that the recovering disk be physically unplugged before powering the system up. Once the system is powered up, you should physically insert the disk, then add the disk via the RAID interface provided in the Management Console or CLI.

SNMP Traps Associated with RAID

The following list describes the traps that might be sent as a result of a change in the RAID status.

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 software 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, we recommend that a disk whose status is reported as “Failed” be replaced as soon as possible to prevent the loss of redundancy resulting from operating with unreliable hardware.
3. Disk recovering – This trap is sent when the status of a disk in RAID changes to “Recovering.” This trap will normally not be sent because the initial status of a newly added disk is “Recovering,” and a “Disk added” trap is sent instead. Sometimes, there may be a small window after a disk has been added to RAID where its status is “Unknown,” and then changes to “Recovering,” causing this trap to be sent.
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 an event requested by the administrator through the user interface, or a physical removal of the disk without removing it from the array through the user interface first.
6. Disk added – This trap is sent when a disk is added to RAID by inserting a new disk in one of the disk slots and then adding it to the array through the user interface.

Adding a Disk

To add a disk through the Management Console:

1. Insert the disk into any of the available disk slots on the KeySecure, and take note of the slot you insert the disk into.
2. Log on to the Management Console.
3. Navigate to the RAID Status section of the System Health page (Device >> System Health).
4. The **Add** button is enabled when there is only one operational disk. If there are two operational disks, the **Add** button is not shown.
5. Click **Add**. You are prompted to select the slot number of the newly–added disk.
6. Confirm that you want to add the disk at the confirmation page.

To add a disk through the CLI:

1. Insert the disk into any of the available disk slots on the KeySecure, and take note of the slot you insert the disk into.
2. Log in to the CLI and enter config mode (type **`config`**).
3. Issue the following command: raid add <disk_slot_number>
4. Confirm that you want to add the disk.

Immediately after confirming that you want to add a disk (when executed from either the CLI or the Management Console), if SNMP is enabled, two traps are sent to the appropriate management station, and the event is noted in the System Log. The add disk operation should take between 10 and 15 seconds to complete. Once the operation is complete, you are returned to the System Health page or the command prompt, depending on where you are performing the add disk operation. When the system is again responsive, you will notice that the newly added disk is in the recovery state, during which time the data from the operational disk is copied to the newly added disk. To verify that the disk is in the recovery state from the CLI, issue the `show system health` command. Once recovery is completed (typically after 15 to 30 minutes), the status of the newly added disk changes to operational, traps are sent (if SNMP is enabled), and the event is noted in the System Log.

WARNING! Never boot the KeySecure with a disk that has not been added to the array through the Management Console or the CLI.

Removing a Disk

There are two scenarios in which you might remove a disk:

- RAID detects that there is a problem with the disk and changes the status of the disk to “Failed.”
- RAID is unable to detect the state of the disk and changes the status to “Unknown.”

Note: We recommend that you not physically unplug a disk that is part of a RAID configuration without first removing it through the Management Console or the CLI. If a disk is unplugged in this manner, SNMP traps are sent (if SNMP is enabled) and the event is noted in the System Log.

To remove a disk through the Management Console:

1 Log on to the Management Console.

2 Navigate to the RAID Status section of the System Health page (Device >> System Health).

3 If there is only one operational disk, the **Remove** button is disabled. You should also note that if a disk is in the recovery state, the other (only operational) disk cannot be removed.

4 Select the disk you want to remove.

5 Click **Remove**.

6 Confirm that you want to remove the disk at the confirmation page.

Important! The system will be unresponsive for about 15 seconds. It is imperative that you not unplug the disk until the system says that it has been removed in RAID software.

7 Unplug the disk from the KeySecure.

To remove a disk through the CLI:

1 Log in to the CLI and enter config mode (type **`config`**).

2 Issue the following command: `raid remove <disk_slot_number>`

3 Confirm that you want to remove the disk.

Important! The system will be unresponsive for about 15 seconds. It is imperative that you not unplug the disk until the system says that it has been removed in RAID software.

4 Unplug the disk from the KeySecure.

Important! Always unplug a disk that has been removed through the RAID interface provided in the Management Console or CLI. It the disk remains plugged in, it is possible that the KeySecure will attempt to boot from the disk during subsequent reboots. This can lead to system instability.

If SNMP is enabled, two traps are sent immediately after confirmation, and the event is noted in the System Log. The remove disk operation should take between 10 and 15 seconds to complete. Once the operation is complete, you are returned to the System Health page or the command prompt (depending on where you are performing the remove disk operation). When the system is again responsive, you will notice that the newly–removed disk is no longer displayed in the RAID Status section of the System Health page or the show system health command.

Chapter 26

Network Diagnostics

You can test the KeySecure’s network connectivity by running ping, traceroute, host, or netstat commands.

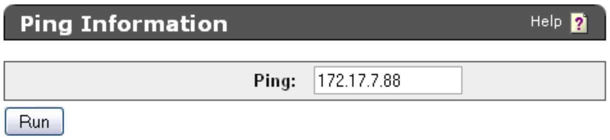
Ping a Hostname or IP

To ping a hostname or IP:

1 Log on to the Management Console.

2 Navigate to the Network Diagnostics page (Device >> Maintenance >> Network Diagnostics).

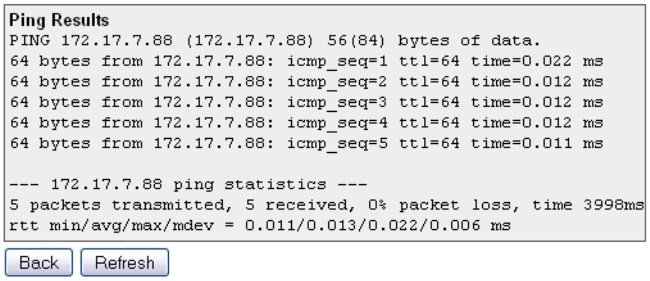
3 Enter the hostname or ip of the target system in the **Ping** field.



Ping Information

Ping: 172.17.7.88

4 Click **Run**. View the Ping Results.



Ping Results

```
PING 172.17.7.88 (172.17.7.88) 56(84) bytes of data.
64 bytes from 172.17.7.88: icmp_seq=1 ttl=64 time=0.022 ms
64 bytes from 172.17.7.88: icmp_seq=2 ttl=64 time=0.012 ms
64 bytes from 172.17.7.88: icmp_seq=3 ttl=64 time=0.012 ms
64 bytes from 172.17.7.88: icmp_seq=4 ttl=64 time=0.012 ms
64 bytes from 172.17.7.88: icmp_seq=5 ttl=64 time=0.011 ms

--- 172.17.7.88 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.011/0.013/0.022/0.006 ms
```

Run Traceroute

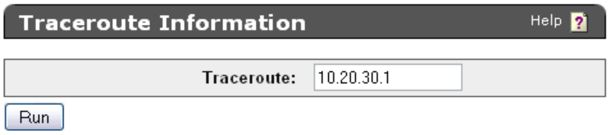
The traceroute command examines the path that packets take between the KeySecure and the target destination.

To run a traceroute:

1 Log on to the Management Console.

2 Navigate to the Network Diagnostics page (Device >> Maintenance >> Network Diagnostics).

3 Enter the hostname or ip of the target system in the **Traceroute** field.



Traceroute: 10.20.30.1

4 Click **Run**.

Check DNS for a Hostname or IP

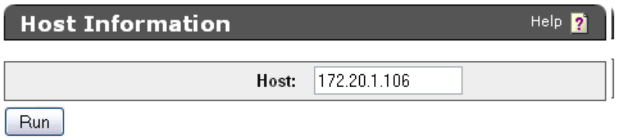
The host must be registered with the DNS configured on the KeySecure. Be sure to add the DNS server to the KeySecure DNS server list before using this feature (Device >> Network >> Hostname & DNS).

To run the host command:

1 Log on to the Management Console.

2 Navigate to the Network Diagnostics page (Device >> Maintenance >> Network Diagnostics).

3 Enter the hostname or ip of the target system in the **Host** field.



Host: 172.20.1.106

4 Click **Run**.

Run Netstat

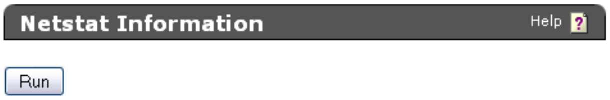
The netstat command returns a list of all active network connections to the KeySecure.

To run netstat:

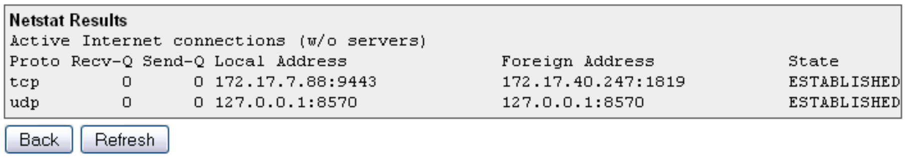
1 Log on to the Management Console.

2 Navigate to the Network Diagnostics page (Device >> Maintenance >> Network Diagnostics).

3 Click **Run** in the Netstat Information section.



The results will be similar to the following:



Netstat Results

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address            Foreign Address          State
tcp        0      0 172.17.7.88:9443         172.17.40.247:1819       ESTABLISHED
udp        0      0 127.0.0.1:8570           127.0.0.1:8570           ESTABLISHED
```

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 acknowledgement 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.

Chapter 27

Keys

The KeySecure can create and store keys. A key is composed of two main parts: the key bytes and the key metadata. The key bytes are the bytes used by the cryptographic algorithm (together with the input data) to produce either plaintext or ciphertext.

The key metadata contains information about the key bytes: key name, ownership information, algorithm, key size, creation date, group permissions, life cycle management state, and any custom attributes that you create. The metadata also indicates whether a key is deletable or exportable.

At key creation time, you can choose to make your key into a template or a versioned key. A template is a metadata-only pattern for other keys. A versioned key is one key with multiple bytestrings.

- After you set a key to be a template and click create, it no longer contains any key bytes at all. The Key Properties page for a template does not show a Life Cycle tab. The entry in the key list for a template does not show any value for State (the Life Cycle State). For more information on templates, see “Create a Key Template” on page 151.
- A versioned key is similar to a template. The Key Properties page for a versioned key also does not show a Life Cycle tab. The entry in the key list for a versioned key does not show any value for State (the Life Cycle State).

Important! Life Cycle State does not apply to versioned and standard keys used by the NAE-XML protocol. The procedures described in “Manage Key and Certificate Life Cycle States” on page 155 apply to standard keys used by the KMIP protocol only. Although Life Cycle States are shown in the Management Console, they do not have any effect on NAE-XML keys. For more information on state support for versioned keys, see “Versioned Keys” on page 145.

Key Ownership

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 members of Group1 permission to encrypt and members of Group2 permission to decrypt. Using authorization policies, you can set usage limitations for keys.

For more information, see Chapter 29, “Authorization Policies”.

Accessing Keys During Authenticated and Global Sessions

As the administrator of the KeySecure, you can define how your clients authenticate to the server. A client might be an application or a database, for example. There are two kinds of client sessions: authenticated and unauthenticated (global). When a client authenticates, it authenticates either as a local user or as a user in the LDAP user directory that the server 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 server, then that client has access only to global keys. On the NAE server, keys can be:

- Generated on the Management Console by an administrator.
- Generated by an NAE client, such as the SafeNet JCE Provider.
- Imported through the Management Console or through one of the NAE clients.
- Marked as exportable, deletable, neither or both. An exportable key is a key that a client can export from the server. Similarly, a deletable key is a key that the client can delete from the server.

WARNING! Do not delete keys that might be needed to decrypt data at some point in the future. Once 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.

Versioned Keys

A versioned key maintains a single set of key metadata but contains multiple byte strings. Each version contains a unique key byte string. In the Key Properties view, versioned keys have a unique tab, named Key Versions.

Versioned keys are an alternative to keys managed as KMIP cryptographic managed objects. After a key is set as versioned, the Life Cycle tab in the Key Properties page is not visible. The entry in the key list for a versioned key does not show any value for State (the Life Cycle State).

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: encryption and decryption and all key management options are allowed.
- Restricted: only key information operations are allowed.
- Retired: no operations or access to key management is allowed.
- Wiped: the version is deleted.

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, and the request comes from a member of the permitted group.

A key can have a maximum of 4000 versions. Wiped versions display in ~~strikeout~~ type.

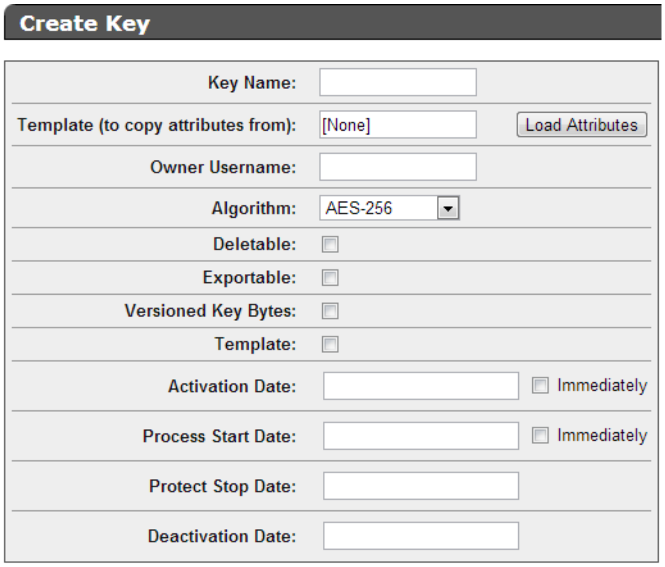
Note: To wipe a versioned key, first retire it, then, wipe it. The Wiped state is not available for an active or restricted versioned key.

Create a Key

To create a 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).



Create Key

Key Name:		
Template (to copy attributes from):	[None]	Load Attributes
Owner Username:		
Algorithm:	AES-256	
Deletable:	□	
Exportable:	□	
Versioned Key Bytes:	□	
Template:	□	
Activation Date:		□ Immediately
Process Start Date:		□ Immediately
Protect Stop Date:		
Deactivation Date:		

3 Enter a unique key name in the **Key Name** field. This is the name that the server 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. This value may be changed after the key is created.

4 Enter a **Template** and click **Load Attributes**. (Optional) A template is a collection of attributes that can be assigned only when the key is created. You must first create a template before it can be used to create keys. For more information, see "Create a Key Template".

5 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, then that is the only user who can access the key, unless you set group permissions. Global keys can be accessed by all users. This value may be changed after the key is created.

6 Select an **Algorithm**. The available algorithms depend on your device configuration. The complete list of possible configurations and available algorithms is in Appendix B, "Supported Key Algorithms."

Note: Some of the algorithms listed above will not be available on FIPS-compliant devices.

7 To make the key deletable by the owner, select **Deletable**. Deletable global keys are deletable by all users. This value may be changed after the key is created.

8 To make the key exportable (on non-FIPS-compliant KeySecure), select **Exportable**. An exportable key can be exported by its owner and by members of a group with “Export” permission for the key. An exportable global key is exportable by all users. This value may be changed after the key is created.

9 Select **Versioned Key Bytes** to create a versioned key. A versioned key can have up to 4000 versions, each with its own unique set of key bytes, but with shared key metadata (key name, algorithms, permissions, etc.). The first key version is created when the key is created. Additional key versions may be created later using the Key Versions section. For more information on key versions, see “Versioned Keys” on page 145.

10 Enter the optional Activation, Process, Protect, and Deactivation dates as desired.

Note: These dates do not apply to versioned keys and are specific to KMIP.

11 Click **Create**.

- Creating large remote foundry keys and making them available across a widely distributed network may require more processing time than expected. If you receive a time out message or an error message, be aware that the process has not necessarily aborted. Wait one or two minutes, refresh the Key List, and check for your new key. If you are creating several such keys for a global network, the best practice is to wait one minute or more between the creation of each key.

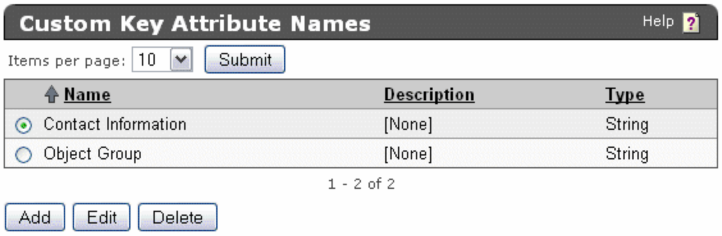
When the key appears in the Key List, the fundamental key creation process is done.

Note: You may want to assign key attributes and group permissions to the key. These optional instructions are included below.

Note: Once the key is created you can add additional key names by editing the **Other Key Names** field in the key’s properties. To access this field, go to the Keys section (Security >> Keys), select the key name and click **Properties**.

12 Assign an attribute to the key.

- To assign a predefined attribute, navigate to the Custom Key Attribute Names section of the Key and Policy Configuration page (Security >> Keys >> Key Options). The KeySecure includes the *Contact Information* and *Object Group* attributes., which are used by KMIP. These attributes cannot be deleted or modified.



Items per page: 10

	Name	Description	Type
●	Contact Information	[None]	String
○	Object Group	[None]	String

1 - 2 of 2

13 Click **Add** to create your own key attribute names.

14 Enter the attribute’s **Name**. Attribute names can contain alphanumeric characters, hyphens, underscores, and periods. You cannot include whitespaces in the name. In addition, the first character of the name must be a letter. Maximum length is 255 characters.

15 Enter a **Description**. This field can contain any printable ASCII characters and spaces, tab, \n and \r. Maximum length is 4095 characters.

16 Select the **Type**. Once selected, the type cannot change. Key attributes can be any of the following data type:

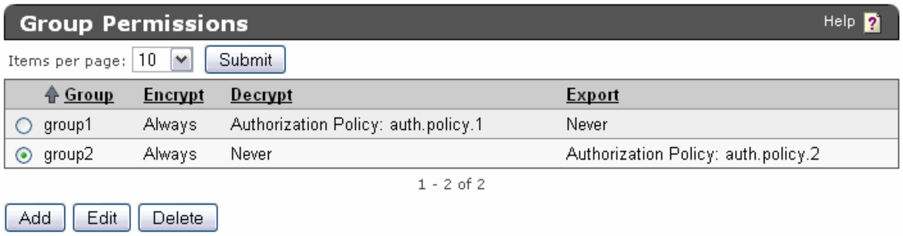
- String
- Integer
- Long Integer
- Big Integer
- Enumeration
- Boolean
- Byte String
- Data/Time
- Interval

Note: Any attribute created through the XML interface is automatically a String.

17 Click **Save**. The key attribute can now be associated with a key.

18 Navigate to the key's Key Properties section. Go to the Keys section (Security >> Keys), select the key name and click **Properties**.

19 Click the Permissions tab. Key permissions are granted at the group level. To assign permissions, there must be local groups defined on the KeySecure. 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, because all users can access global keys for any applicable operation.



Group Permissions

Items per page: 10

	Group	Encrypt	Decrypt	Export
○	group1	Always	Authorization Policy: auth.policy.1	Never
●	group2	Always	Never	Authorization Policy: auth.policy.2

1 - 2 of 2

Note: To include authorization policies when assigning permissions, you must first create the policies you need. For instructions on creating authorization policies, see Chapter 29, "Authorization Policies".

20 Click **Add**.

21 Enter a **Group**. These can be local or LDAP groups, if an LDAP user directory is configured for your KeySecure.

22 Assign permissions for the available operations, which vary by algorithm:

- RSA: Encrypt, Decrypt, Sign, Sign Verify, Export
- HmacSHA1: MAC, MAC Verify, Export

- ARIA: Encrypt, Decrypt, Export (Available by Feature Enablement)
- SEED: Encrypt, Decrypt, Export (Available by Feature Enablement)

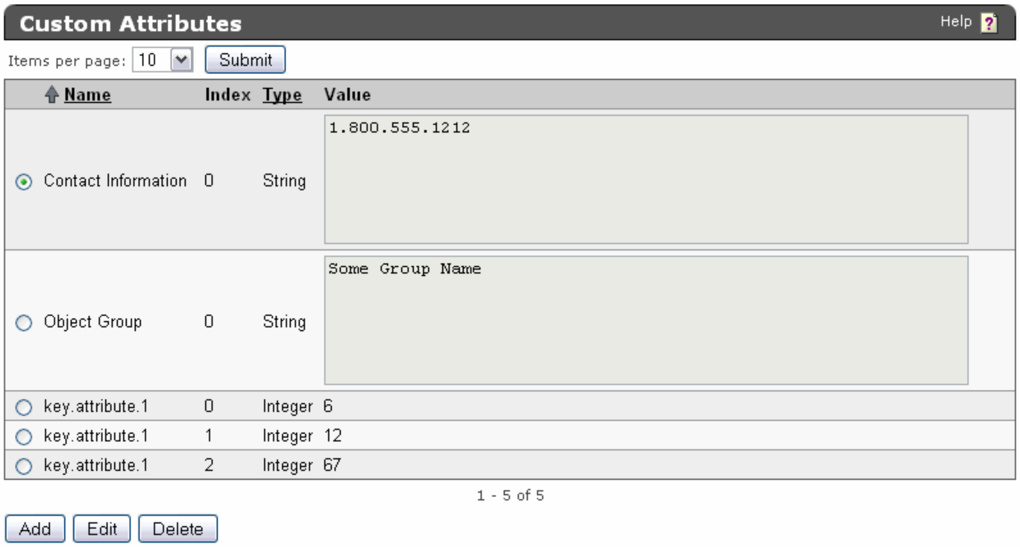
You can assign these operations using the following options:

- *Never* - Members of the group can never perform the operation with the key.
- *Always* - Members of the group can always perform the operation with the key.
- *Authorization Policy* - Members of the group can perform the operation with the key according to the terms of the authorization policy.

Note: Export permissions are only applicable if the key is exportable.

23 Click **Save**.

24 Click the Custom Attributes tab.



	Name	Index	Type	Value
●	Contact Information	0	String	1.800.555.1212
○	Object Group	0	String	Some Group Name
○	key.attribute.1	0	Integer	6
○	key.attribute.1	1	Integer	12
○	key.attribute.1	2	Integer	67

25 Click **Add**. You can assign a maximum of 100 custom attributes. Only one instance of *Contact Information* is allowed per key. Each attribute is given an **Index**. The **Index** is per attribute, per key. The first instance of an attribute is given **Index** 0. The second instance is given **Index** 1, and so on. Thus, since there can only be one instance of *Contact Information*, it will always be **Index** 0.

26 Select the **Name**. Only attributes that already exist on the Custom Key Attributes Names section are available here.

27 Enter a **Value**. This can be any printable ASCII characters and spaces, tab, \n and \r. Maximum length is 4096 characters.

28 Click **Save**.

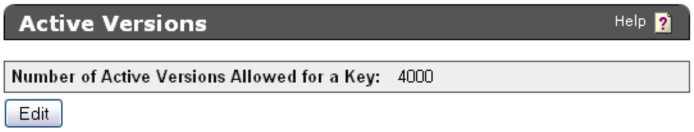
Important! You should create a backup immediately after creating a key. There is no way to recover a key that has not been backed up.

Set the Maximum Number of Key Versions

To set the maximum number of versions allowed for a key:

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

2 Navigate to the Active Versions section on the Key and Policy Configuration page (Security >> Keys >> Key Options).



Number of Active Versions Allowed for a Key: 4000

3 Click **Edit**.

4 Enter a value for the **Number of Active Versions Allowed for a Key**. Active versions of a key can be used for both encryption and decryption (or Sign/SignVerify, or MAC/MACVerify depending on the algorithm).

5 Click **Save**.

Important! When restoring a key to the KeySecure, the key must conform to the appliance's 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, 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.

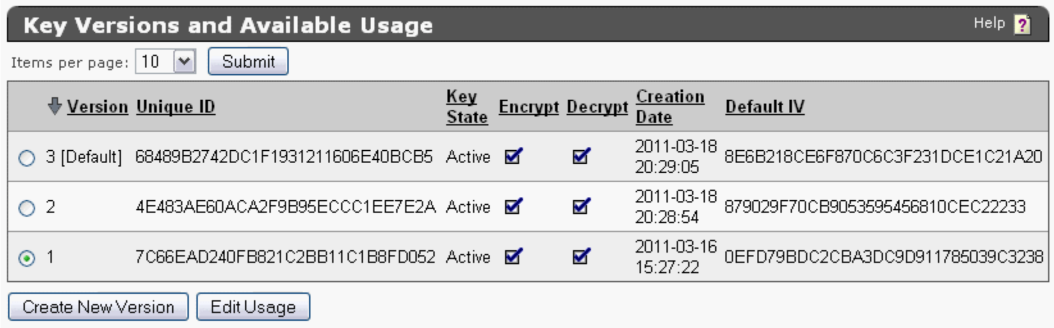
Create and Manage Key Versions

The first version of a versioned key is created when the key is created. To create and manage key versions use the Key Versions tab on the Key Properties page.

To create and manage key versions:

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

2 Navigate to the Key Versions and Available Usage section. Go to the Keys section on the Key and Policy Configuration page (Security >> Keys), select the **Key Name**, and click the Key Versions tab.



	Version	Unique ID	Key State	Encrypt	Decrypt	Creation Date	Default IV
○	3 [Default]	68489B2742DC1F1931211606E40BCB5	Active	☑	☑	2011-03-18 20:29:05	8E6B218CE6F870C6C3F231DCE1C21A20
○	2	4E483AE60ACA2F9B95ECCC1EE7E2A	Active	☑	☑	2011-03-18 20:28:54	879029F70CB9053595456810CEC22233
●	1	7C66EAD240FB821C2BB11C1B8FD052	Active	☑	☑	2011-03-16 15:27:22	0EFD79BDC2CBA3DC9D911785039C3238

3 Click **Create New Version** to create a new key version. The new version is now the default version. This will be the version used when cryptographic and information requests do not specify a version number. The maximum amount of versions is set on the Active Versions (Security >> Keys >> Key Options).

All versions of a key have the same metadata (found on the Key Properties, Permissions, and Custom Attributes sections). But, the **Version**, **Unique ID**, **Key State**, **Creation Date**, **Default IV**, and key bytes differ for each version.

4 Click **Edit Usage**.

5 Alter the **Key State** for any or all version. You can edit all but the Default key version. The following options are available:

- 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 the Active Versions section.
- Restricted - Only decrypt (MAC Verify for HmacSHA1 keys, Sign Verify for RSA keys) and key info operations are allowed.
- Retired - No access is allowed.
- Wiped - The key is deleted.

Note: To wipe a versioned key, first retire it, then, wipe it. The Wiped state is not available for an active or restricted versioned key.

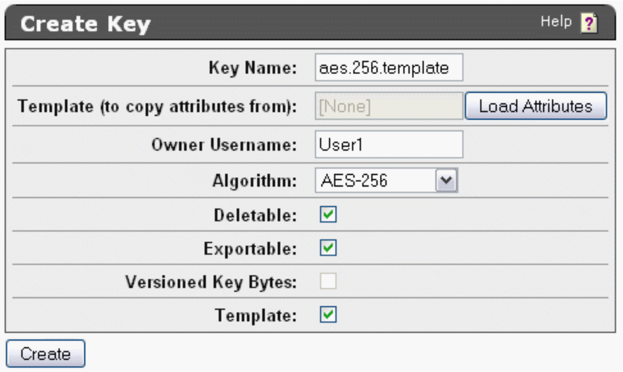
6 Click **Save**.

Create a Key Template

To create a key template:

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).



Create Key

Key Name:	aes.256.template
Template (to copy attributes from):	[None] Load Attributes
Owner Username:	User1
Algorithm:	AES-256
Deletable:	☑
Exportable:	☑
Versioned Key Bytes:	☐
Template:	☑

3 Enter a unique key name in the **Key Name** field. This is the name that the server 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. This value may be changed after the key is created.

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, then that is the only user who can access the key, unless you set group permissions. Global keys can be accessed by all users. This value may be changed after the key is created.

5 Select an Algorithm. For a list of supported algorithms, refer to Appendix B, “Supported Key Algorithms.”

Note: Some of the algorithms listed above will not be available on FIPS-compliant devices.

6 To make the key deletable by the owner, select **Deletable**. Deletable global keys are deletable by all users. This value may be changed after the key is created.

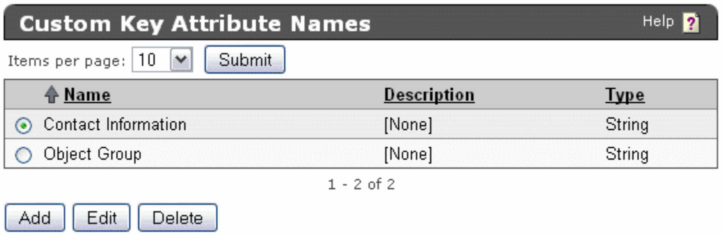
7 To make the key exportable select **Exportable**. An exportable key can be exported by its owner and by members of a group with “Export” permission for the key. An exportable global key is exportable by all users. This value may be changed after the key is created.

Note: You cannot select **Versioned Key Bytes** when creating a template. To create versioned keys from a template, you must select this option for each key individually after loading the key properties.

8 Select **Template** to create a key template based on the values set above.

9 Click **Create**.

10 Navigate to the Custom Key Attribute Names section of the Key and Policy Configuration page (Security >> Keys >> Key Options). The KeySecure includes the *Contact Information* and *Object Group* attributes used by KMIP. These attributes cannot be deleted or modified.



Custom Key Attribute Names

Items per page: 10

Name	Description	Type
● Contact Information	[None]	String
○ Object Group	[None]	String

1 - 2 of 2

11 Click **Add** to create your own key attribute names.

12 Enter the attribute's **Name**. Attribute names can contain alphanumeric characters, hyphens, underscores, and periods. You cannot include whitespaces in the name. In addition, the first character of the name must be a letter. Maximum length is 255 characters.

13 Enter a **Description**. This field can contain any printable ASCII characters and spaces, tab, \n and \r. Maximum length is 4095 characters.

14 Select the **Type**. Once selected, the type cannot change. Key attributes can be any of the following data type:

- String
- Integer
- Long Integer
- Big Integer
- Enumeration
- Boolean
- Byte String
- Data/Time
- Interval

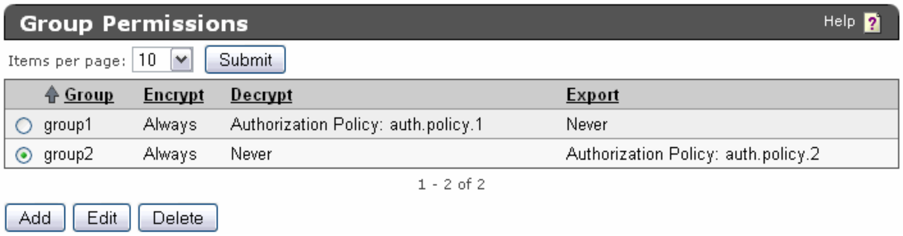
Note: Any attribute created through the XML interface is automatically a String.

Note: Each attribute is assigned an index. The index is only visible when queried by a KMIP client. This index cannot be changed.

15 Click **Save**. The key attribute can now be associated with a key.

16 Navigate to the template's Key Properties section. Go to the Keys section (Security >> Keys), select the template name and click **Properties**.

17 Click the Permissions tab. Key permissions are granted at the group level. To assign permissions, there must be local groups defined on the KeySecure. 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, because all users can access global keys for any applicable operation.



	Group	Encrypt	Decrypt	Export
○	group1	Always	Authorization Policy: auth.policy.1	Never
●	group2	Always	Never	Authorization Policy: auth.policy.2

1 - 2 of 2

Note: To include authorization policies when assigning permissions, you must first create the policies you need. For instructions on creating authorization policies, see Chapter 29, “Authorization Policies”.

18 Click **Add**.

19 Enter a **Group**. These can be local or LDAP groups, if an LDAP user directory is configured for your KeySecure.

20 Assign permissions for the available operations, which vary by algorithm:

- AES: Encrypt, Decrypt, Export
- DES: Encrypt, Decrypt, Export
- RC4: Encrypt, Decrypt, Export
- HmacSHA: MAC, MAC Verify, Export
- RSA: Encrypt, Decrypt, Sign, Sign Verify, Export
- SEED: Encrypt, Decrypt, Export

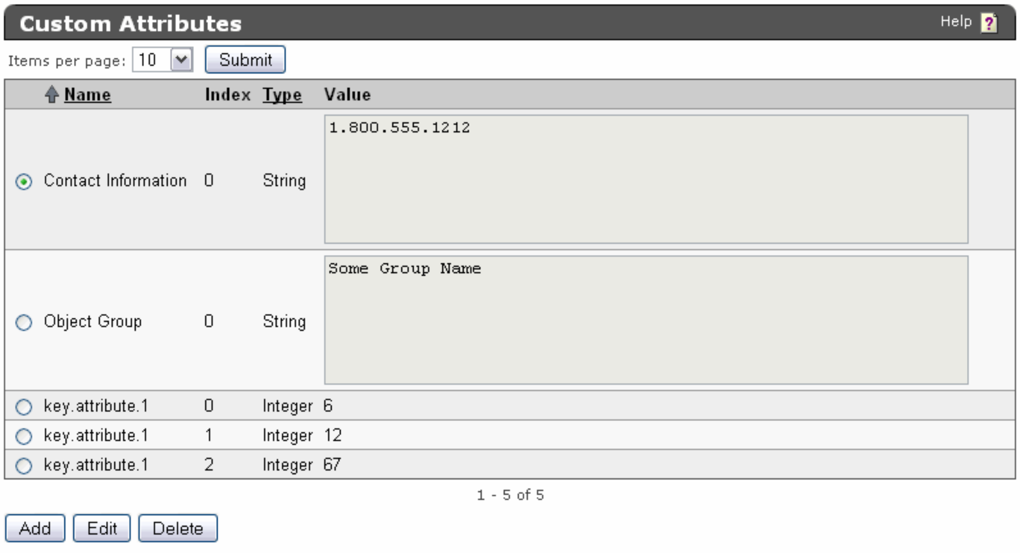
You can assign these operations using the following options:

- *Never* - Members of the group can never perform the operation with the key.
- *Always* - Members of the group can always perform the operation with the key.
- *Authorization Policy* - Members of the group can perform the operation with the key according to the terms of the authorization policy.

Note: Export permissions are only applicable if the key is exportable.

21 Click **Save**.

22 Click the Custom Attributes tab.



Custom Attributes

Items per page: 10 Submit

	Name	Index	Type	Value
●	Contact Information	0	String	1.800.555.1212
○	Object Group	0	String	Some Group Name
○	key.attribute.1	0	Integer	6
○	key.attribute.1	1	Integer	12
○	key.attribute.1	2	Integer	67

1 - 5 of 5

23 Click **Add**. You can assign a maximum of 100 custom attributes. Only one instance of *Contact Information* is allowed per key. Each attribute is given an **Index**. The **Index** is per attribute, per key. The first instance of an attribute is given **Index** 0. The second instance is given **Index** 1, and so on. Thus, since there can only be one instance of *Contact Information*, it will always be **Index** 0.

24 Select the **Name**. Only attributes that already exist on the Custom Key Attributes Names section are available here.

25 Enter a **Value**. This can be any printable ASCII characters and spaces, tab, \n and \r. Maximum length is 4096 characters.

26 Click **Save**.

Now all keys created with this template will share these properties.

Manage Key and Certificate Life Cycle States

There are three supported states for standard keys and certificates, pre-active, active, and deactivated. For each of these states, there is an associated date of when the key moved into the state.

There is one-way movement through the states. Once a key is activated, it cannot move back to a pre-active state. Once a key is deactivated, it cannot be activated again.

You can manage standard key states and dates through the Management Console or with KMIP. Use KMIP to modify certificate states and dates.

Important! Life Cycle State does not apply to versioned and standard keys used by the NAE-XML protocol. The procedures described in this section apply to standard keys used by the KMIP protocol only. Although Life Cycle States are shown in the Management Console, they do not have any effect on NAE-XML keys. For more information on state support for versioned keys, see “Versioned Keys” on page 145.

Edit the State and Associated Dates for a Key or Certificate

Use the following procedures to modify the state and the dates associated with that state for a standard key on the Management Console.

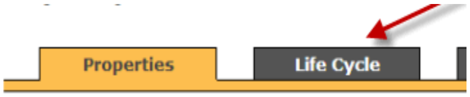
1 Log in to the Management Console as an administrator with Keys and Authorization Policies access control.

2 Navigate to the Keys or Certificates section of the Key and Policy Configuration page.

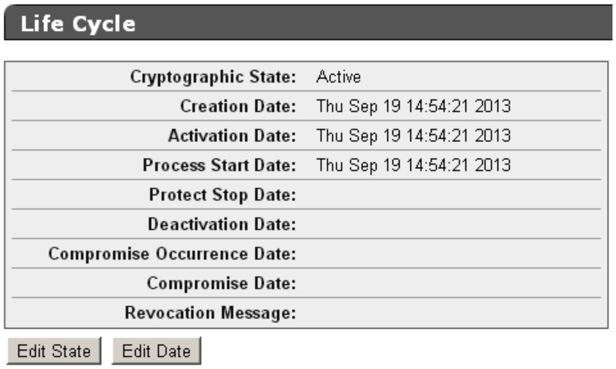
- To edit states and dates for a key, select Security, and then select Keys.
- To edit states and dates for a certificate, select Security, and then select Certificates.

3 Select a key or certificate and click **Properties**.

4 Click the **Life Cycle** tab, as shown below.



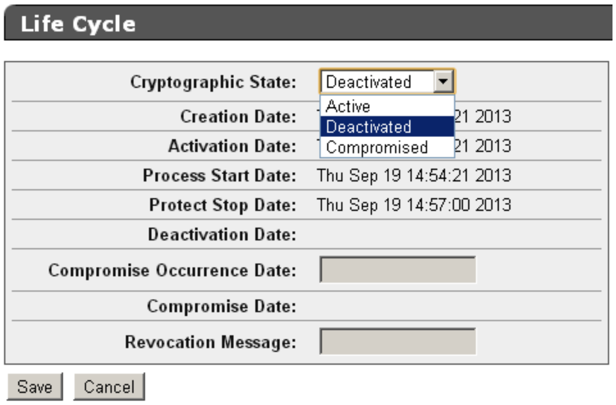
5 In the lower portion of the screen the Life Cycle box appears and shows all the state and date information for a key. Click either edit button to make modification. After certain options, the edit buttons might be replaced by save and cancel buttons. If the edit buttons are not visible, click the **Life Cycle** tab shown above a second time.



Life Cycle

Cryptographic State:	Active
Creation Date:	Thu Sep 19 14:54:21 2013
Activation Date:	Thu Sep 19 14:54:21 2013
Process Start Date:	Thu Sep 19 14:54:21 2013
Protect Stop Date:	
Deactivation Date:	
Compromise Occurrence Date:	
Compromise Date:	
Revocation Message:	

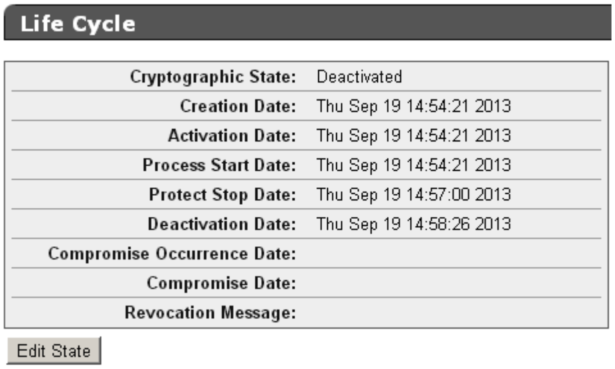
6 If you edit the state, a drop-down box displays all options for that key or certificate. The example shown below is an active key; the only option is to deactivate it.



Life Cycle

Cryptographic State:	Deactivated
Creation Date:	21 2013
Activation Date:	21 2013
Process Start Date:	Thu Sep 19 14:54:21 2013
Protect Stop Date:	Thu Sep 19 14:57:00 2013
Deactivation Date:	
Compromise Occurrence Date:	
Compromise Date:	
Revocation Message:	

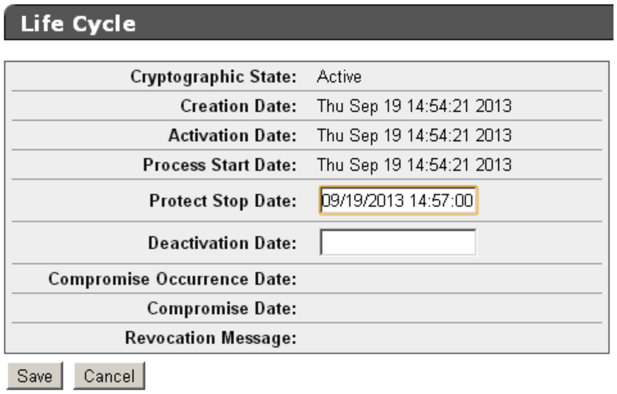
If you change the state to deactivated, the system fills in the deactivation date, as shown below.



Life Cycle

Cryptographic State:	Deactivated
Creation Date:	Thu Sep 19 14:54:21 2013
Activation Date:	Thu Sep 19 14:54:21 2013
Process Start Date:	Thu Sep 19 14:54:21 2013
Protect Stop Date:	Thu Sep 19 14:57:00 2013
Deactivation Date:	Thu Sep 19 14:58:26 2013
Compromise Occurrence Date:	
Compromise Date:	
Revocation Message:	

7 If you edit the date, all editable text boxes appear for all dates that you can change. Enter all new dates in the format **mm/dd/yyyy hh:mm:ss**. Be sure to enter the complete time and date. The example below shows a key with an editable Protect Stop Date and Deactivation Date. A new Protect Stop Date has been entered. Note that the entry format is different from the display format.



Life Cycle

Cryptographic State:	Active
Creation Date:	Thu Sep 19 14:54:21 2013
Activation Date:	Thu Sep 19 14:54:21 2013
Process Start Date:	Thu Sep 19 14:54:21 2013
Protect Stop Date:	09/19/2013 14:57:00
Deactivation Date:	
Compromise Occurrence Date:	
Compromise Date:	
Revocation Message:	

Note: If you add a Deactivation Date, the system changes the state to deactivated. Once a key or certificate is deactivated, you cannot reactivate it again.

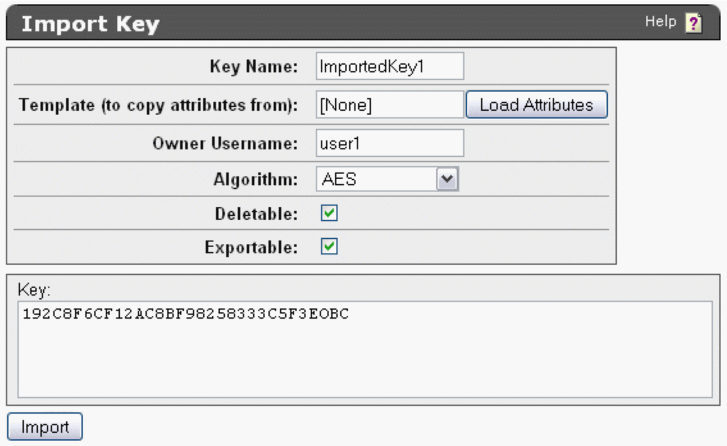
Importing a Key

The Import Key section allows you to import clear text keys on KeySecures. 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.

To import a key:

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

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



Key Name:	ImportedKey1
Template (to copy attributes from):	[None]
Owner Username:	user1
Algorithm:	AES
Deletable:	☑
Exportable:	☑

Key:

```
192C8F6CF12AC8BF98258333C5F3E0BC
```

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

4 Enter a value in the **Owner Username** field to assign a specific owner or leave this value blank to create a global key. When you import a key through the management console, the existing key ownership data is not maintained, so any previous ownership must be re-established. If an owner is listed for the key, then that is the only user who can access the key, unless you set group permissions. Global keys can be accessed by all users.

5 Select the **Algorithm**.

6 To make the key deletable (from a non-FIPS-Compliant KeySecure), select **Deletable**. Deletable global keys are deletable by all users. This value may be changed later.

7 To make the key exportable, select **Exportable**. An exportable key can be exported by its owner and by members of a group with “Export” permission for the key. An exportable global key is exportable by all users. This value may be changed later.

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.

Important! The server 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 server returns an error.

9 Click **Import**.

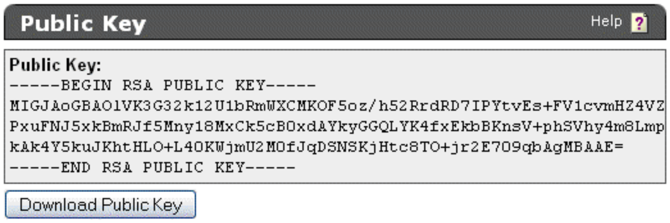
Downloading an RSA Key

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 Navigate to the Public Key section.



Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAO1VK3G32k12U1bRmWXCMKOF5oz/h52RrdRD7IPYtvEs+FV1cvmHZ4VZ
PxuFNJ5xkBmRJf5Mny18MxCk5cB0xdAYkyGGQLYK4fxEkbBKnsV+phSVhy4m8Lmp
kAk4Y5kuJKhtHLO+L40KWjmU2M0fJqDSNSKjHtc8TO+jr2E709qbAgMBAAE=
-----END RSA PUBLIC KEY-----
```

4 Click **Download Public Key** to download the public portion of the RSA key.

Deleting a Key

WARNING! Exercise extreme caution when deleting keys. *If you erroneously delete a key, you cannot recreate that key.* As a result, unless you have a backup of that key, you will not be able to decrypt any ciphertext created by that 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 click **Delete**.

Delete Multiple Keys

The ability to delete multiple keys at a time is a convenience, but it also introduces risk. To minimize the risk of unintentionally deleting keys, the multiple key deletion feature allows you to delete no more than 50 keys at once, and then only the keys that are listed on one page: the current Key List page.

Important! To make sure that ONLY the keys you want to delete appear on one page, you will need to perform a query. The query must return a list that contains ONLY keys that you want to delete. Before attempting to delete multiple keys, make sure you can define the query or queries required to identify exactly the keys that you want to delete. Refer to the instructions for “Create a Key Query”, below.

WARNING! Exercise extreme caution when deleting keys. *If you erroneously delete a key, you cannot recreate that key.* As a result, unless you have a backup of that key, you will not be able to decrypt any ciphertext created by that key. Before deleting keys, creating a backup is strongly recommended.

To delete multiple keys:

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 Change the "Items-per-page" setting to a number greater than the number of Keys you would like to delete, but not more than 50.

- The Delete Multiple Keys function currently supports the deletion of up to 50 keys at once. Larger numbers must be deleted in batches.

4 Run a query, as necessary, to list in the current page only the keys you need to delete. (Refer to the instructions for “Create a Key Query”, below.)

- As a general rule, use the “Save and Run a Query” option. When deleting keys, you want to record all details pertaining to the procedure.
- The keys displayed on the Key List returned by the query will all be deleted, and only these keys. If your query returns more keys than fit on a page because of items-per-page constraint, the keys that don’t appear in the current list are not deleted.
- If you list more keys on a page than you can see on your screen, be sure to scroll through all the keys in the list to prevent accidental deletions.

5 Click **Delete All Keys On Current Page** to delete ALL keys currently rendered on the page.

WARNING: Radio button selections are not considered as keys are deleted. ALL listed keys on the page are deleted, whether selected or not.

- After you click the **Delete All Keys...** button, a “Confirmation Required” page appears.

6 Click **Confirm**.

- Deletion of the keys is proven by the appearance of a new, empty Key List corresponding to the query you just performed, and also a note saying, “Keys deleted.”

7 Clear the query list by selecting “All” from the drop-down Query list and clicking Run Query.

- The current list of keys (not deleted) appears.

To delete many keys, you may need to repeat the process of querying and deleting.

Note: In the extremely unlikely event that an error were to occur during key deletion (due to failure of a local program, for example), the deletions completed prior to the failure would remain deleted. (No rollback occurs.) The error log can confirm details and assist in troubleshooting.

Note: Be aware that deleting many keys stresses the network and may slow traffic, especially during replication in a clustered environment. Traffic may slow more if the nodes in the cluster are widely distributed in a global network. In such scenarios, you can avoid the situation by performing a manual synchronization instead. In the Console, see Device >> Cluster, refer to the topic titled “Synchronize with a Cluster Member”. Use the **Synchronize With** button to perform a manual synchronization.

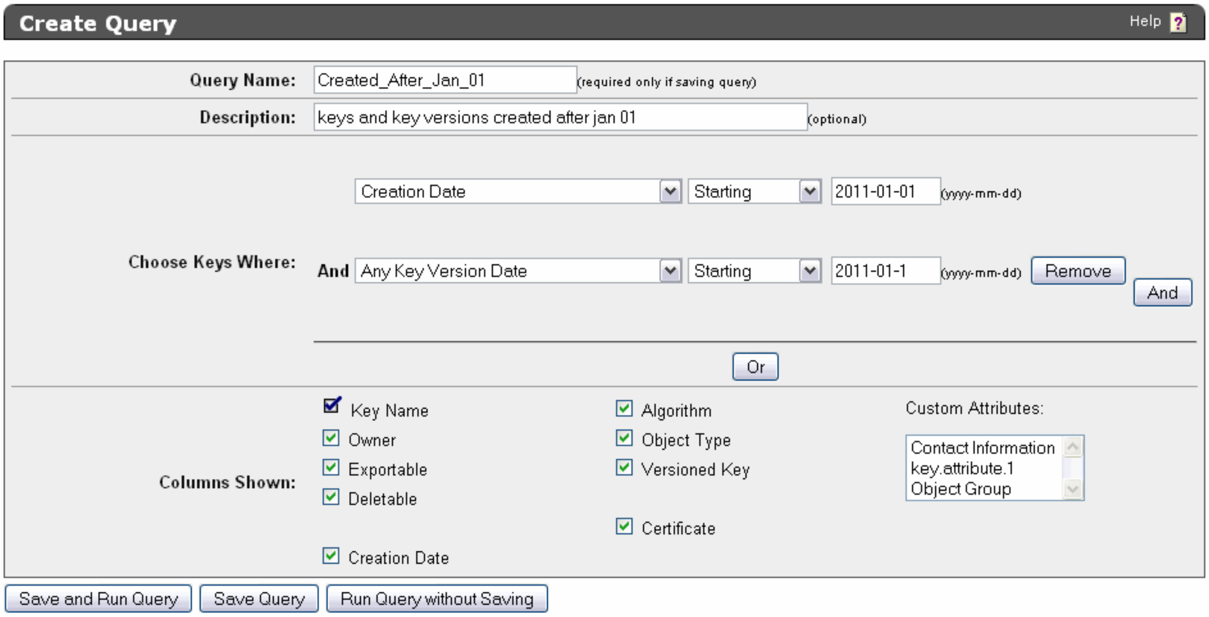
Create a Key Query

A key query enables you to view a subset of the keys that exist on the KeySecure. You can create new queries, run saved queries, and modify queries.

To create a query:

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

2 Navigate to the Queries section of the Key and Policy Configuration page (Security >> Keys >> Query Keys). This section enables you to create very specific queries using multiple and/or statements and using the results of other saved queries. You can also tailor your query to show specific columns.



Create Query

Query Name: Created_After_Jan_01 (required only if saving query)

Description: keys and key versions created after jan 01 (optional)

Choose Keys Where:

Creation Date | Starting | 2011-01-01 (yyyy-mm-dd)

And Any Key Version Date | Starting | 2011-01-1 (yyyy-mm-dd)

Columns Shown:

☑ Key Name
☑ Owner
☑ Exportable
☑ Deletable
☑ Creation Date
☑ Algorithm
☑ Object Type
☑ Versioned Key
☑ Certificate

Custom Attributes:
Contact Information
key.attribute.1
Object Group

3 Enter the **Query Name**. This field is only required if you will save the query. You can run a query without saving, but *you can only save a query before running it*.

4 Enter a **Description** of the query.

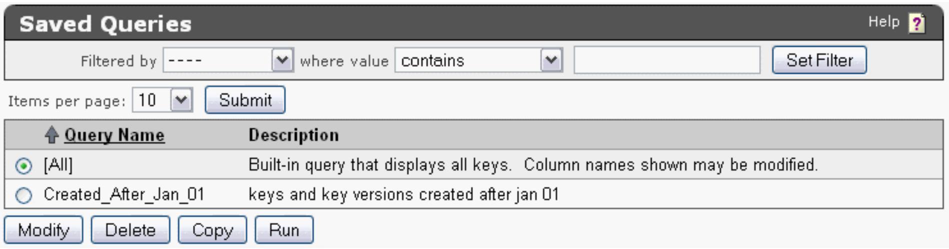
5 Use the **Choose Keys Where** field in combination with the **AND** and **OR** buttons to create your own query. You can query on key metadata, combine query strings, and use the results of previously saved queries.

6 Select the **Columns Shown** in the query results.

7 Select one of the following:

- **Save and Run Query** - save and execute the query.
- **Save Query** - save the query without executing.
- **Run Query without Saving** - execute the query without saving. The results will show the **Query Name** as *Unnamed Query*. You can navigate away from the Keys sections and still reapply the *Unnamed Query*, however, the Management Console will only store one *Unnamed Query* at a time. Old unnamed queries are forgotten.

Saved queries appear in the Saved Queries section. They can be run, copied, deleted, and modified. Click the **Modify** button in the Saved Queries section and then alter the Query Name, **Description**, **Selection Criteria**, and the **Columns Shown** fields.



Saved Queries

Filtered by ---- where value contains

Items per page: 10

	Query Name	Description
●	[All]	Built-in query that displays all keys. Column names shown may be modified.
○	Created_After_Jan_01	keys and key versions created after jan 01

Note: You cannot greatly modify the built-in query [All]. The KeySecure will only permit you to change the **Columns Shown** values.

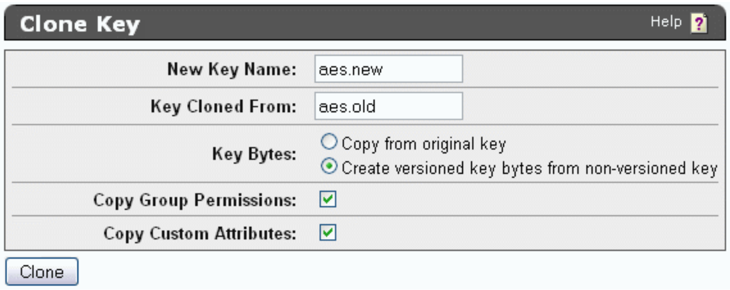
Clone a Key

Cloning a key involves assigning the key bytes and key metadata from an existing key to a new key. You can choose to copy or ignore the existing group permissions and custom attributes. You can use this feature to create a versioned key from a non-versioned key.

To clone a key:

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

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



Clone Key

New Key Name:	aes.new
Key Cloned From:	aes.old
Key Bytes:	○ Copy from original key ● Create versioned key bytes from non-versioned key
Copy Group Permissions:	☑
Copy Custom Attributes:	☑

3 Enter the **New Key Name**. The name must begin with a letter, is must be between 1 and 64 characters (inclusive), and it can consist of letters, numbers, underscores, periods, and hyphens.

4 Enter the old key name in the **Key Cloned From** field. This is the key that will be copied.

5 Choose an option for the **Key Bytes** field:

- *Copy from original key* - clones a standard key
- *Create versioned key bytes from non-versioned key* - creates a new versioned key based on a standard key.

In both cases, the new key will have the same metadata and key bytes as the cloned key.

6 Select **Copy Group Permissions** to copy the group permissions from the existing key.

7 Select **Copy Custom Attributes** to copy the custom attributes from the existing key.

8 Click **Clone** to create a new copy of the key.

Application Specific Information

The Application Specific Information attribute is used to store data which is specific to the applications using the key. The attribute is stored as a pair containing an Application Name Space and the Application Data. The following examples of Application Name Space and Application Data pairs are given in the KMIP Usage Guide.

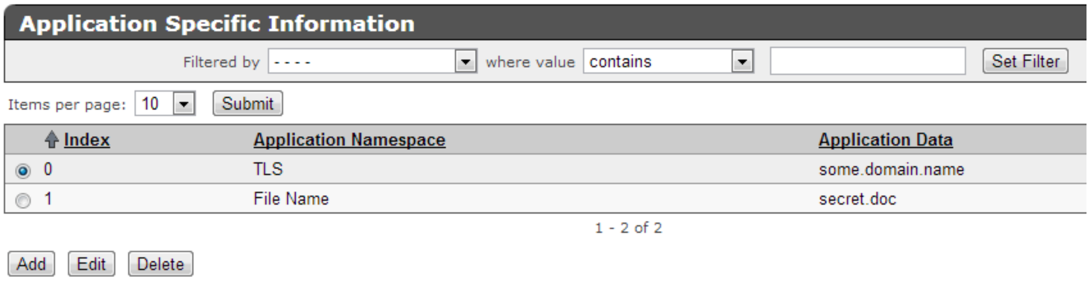
Application Namespace	Application Data
SMIME	someuser@company.com
TLS	some.domain.name
Volume Identification	123343434
File Name	secret.doc

To view or edit Application Specific Information

1 Click **Keys** and then, click the name of an existing key.

2 Click the **Attributes** tab.

The Application Specific Information displays near the top of the window in the format shown below.



Application Specific Information

Filtered by ---- ▾ where value contains ▾

Items per page: 10 ▾

	Index	Application Namespace	Application Data
●	0	TLS	some.domain.name
○	1	File Name	secret.doc

1 - 2 of 2

If there is existing Application Specific Information, it is listed. You can modify the information or the view as follows.

- To limit the information displayed, enter any desired filter information and click **Set Filter**.
- To change the information, use the **Add**, **Edit**, or **Delete** buttons, as needed.

Chapter 28

HSM Configuration

HSM configuration information applies only to the KeySecure k460 hardware appliances. These appliances utilize the FIPS 140-2 Level 3 capabilities of the embedded SafeNet Luna HSM card.

You initialize the HSM as part of the KeySecure setup. This is documented in the *KeySecure Quick Start Guide*.

The KeySecure uses a SafeNet HSM card to store the key encryption keys used to create keys and certificates on the KeySecure. You must initialize the HSM card as part of the KeySecure initialization or you will not be in FIPS mode and therefore not in FIPS compliance.

The management console offers you the option of viewing the HSM status.

The HSM card requires the Pin Entry Device (PED) and at least three iKeys (USB tokens). If you initialize the HSM as part of the KeySecure setup (documented in the *KeySecure Quick Start Guide*) you can configure the remote PED after the set up is completed; remote PED configuration is documented in this chapter.

The HSM **auto-activation** feature governs the behavior of the HSM in the event of a reboot. If the KeySecure was powered off for less than 2 hours, the KeySecure remembers if the HSM was activated. Upon reboot, the HSM will be restored to activation status. If the KeySecure was powered off for more than 2 hours, the black Crypto User iKey must be used to reactivate the HSM.

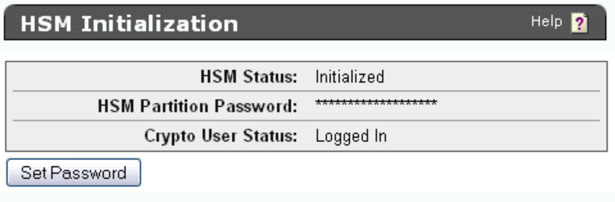
Check HSM Status

Use the HSM Initialization section to check the status of the HSM.

To view the HSM status:

1 Log in to the Management Console.

2 Navigate to the HSM Configuration page (Device >> Device Configuration >> HSM).



HSM Status: Initialized

HSM Partition Password: ********************

Crypto User Status: Logged In

3 View the **HSM Status** field.

4 View the **Crypto User Status** field. (This field is only visible after HSM initialization is complete.) If the KeySecure has been without electrical power for more than 2 hours, the crypto user is automatically logged out. The Crypto User must be logged in for the KeySecure to be able to perform its key management duties.

To log in the crypto user, enter the `hsm login crypto user` command at the Command Line Interface.

```
DemoBox (config)# hsm login crypto user
Luna PED operation required for crypto user login on HSM - use User or
Partition Owner (black) PED key.
```

The PED displays the following text:

```
USER LOGIN...
Insert a USER / Partition Owner PED Key. Press ENTER.
```

a **Insert the black Crypto User iKey** and press Enter.

```
USER LOGIN...
Enter PED PIN.
```

b Enter the PIN for the black Crypto User iKey and press Enter.

The KeySecure CLI displays the following message:

```
Crypto user successful logged into the HSM
```

Configure the Remote PED

The PED can be configured for either local or remote mode. Local mode is used when the PED is connected directly to the KeySecure. Remote mode is used when the PED is connected to the KeySecure by way of a Windows PC running the PED server software. Remote mode is **not** available for the KeySecure installation. It is only available after the HSM has been initialized.

The instructions below use the terms Local PED and Remote PED. The Remote PED Kit, which is ordered separately from the KeySecure, includes the additional cabling and a software CD needed to setup and configure the remote device. The Local PED is local to the KeySecure, and is needed to configure the orange Remote iKey.

Use the Remote PED Configuration section of the Management Console to configure the remote PED.

You will also need to configure a Windows XP client (either 32- or 64-bit) on which the Remote PED can run. This involves installing the device driver and the PED Server executable file on either a Windows 7 or Windows XP client - the driver installation differs for each client.

Note: The remote PED software is **not** supported on Windows Vista.

To install the Remote PED device driver and software on **Windows 7**:

1 Insert the SafeNet Remote PED CD into the Windows PC CD-ROM drive.

2 Configure the power cable for your environment and connect the power cable to the Remote PED and the power supply.

3 Connect the Remote PED to the Windows 7 device. The Windows “Found New Hardware Wizard” will start, but fail to install the device driver.

4 Run Device Manager (Computer > Properties).

5 Select Luna PED under the System devices heading.

6 Right click, select **Properties** and select **Update Driver**.

7 Guide the wizard to the CD’s USB Driver folder (D:\USBDriver). Select the LunaPED_/inf file and click **Open**.

8 Click **OK**.

9 Click **Next**. The wizard installs the software.

10 Click **Finish**.

11 Copy D:\Windows\PedServer.exe to the Windows PC. You need this file to start the PED server.

To install the Remote PED device driver and software on **Windows XP**:

1 Insert the SafeNet Remote PED CD into the Windows PC CD-ROM drive.

2 Configure the power cable for your environment and connect the power cable to the Remote PED and the power supply.

3 Connect the Remote PED to the Windows XP device. The Windows “Found New Hardware Wizard” will start.

4 Click **Yes, this time only** in the Welcome Menu. Click **Next**.

5 Select **Install from a list or specific location (Advanced)**. Click **Next**.

6 Select **Don’t search, I will choose the driver to install**. Click **Next**.

7 Click **Have Disk...**.

8 Guide the wizard to the CD’s USB Driver folder (D:\USBDriver). Select the LunaPED_/inf file and click **Open**.

9 Click **OK**.

10 Click **Next**. The wizard installs the software.

11 Click **Finish**.

12 Copy D:\Windows\PedServer.exe to the Windows PC. You need this file to start the PED server.

To configure remote mode:

1 Be sure that the Local PED is connected to the KeySecure, as was needed during the installation.

2 Login to the KeySecure CLI as an administrator (e.g., `admin`).

3 Type `config` to enter configuration mode.

4 Execute the `hsm remote ped init` command. The Security Officer must be logged in to execute this command. Use the blue Security Officer iKey to log in the Security Officer.

```
DemoBox (config)# hsm remote ped init
Luna PED operation required to initialize remote PED key vector - use orange
PED key(s).
```

5 Insert the RPK/Remote (orange) iKey into the Local PED. The Local PED display and the corresponding actions are shown below:

```
SETTING RPV...
Would you like to reuse an existing keyset? (Y/N)
```

a Press No.

```
SETTING RPV...
M value? (1-16)
>01
```

b Press 1 and press Enter.

```
SETTING RPV...
N value? (M-16)
>01
```

c Press 1 and press Enter.

```
SETTING RPV...
Insert a RPK / Remote PED Key. Press ENTER.
```

d **Insert the RPK/Remote (orange) iKey** and press Enter.

```
SETTING RPV...
Enter new PED PIN:
```

e Enter a PIN value.

```
SETTING RPV...
Confirm new PED PIN:
```

f Confirm the same PIN value.

```
SETTING RPV...
Are you duplicating this keyset? (Y/N)
```

g Press No.

```
Ped Client Version 1.0.5 (10005)
Ped Client launched in shutdown mode.
```

```
Shutdown passed.
```

6. Take out the RPK/Remote (orange) iKey.

7. Configure the PED server:

```
C:>PedServer.exe -m config -create

Ped Server Version 1.0.5 (10005)
Ped Server launched in configuration mode.
Configuration command passed.
```

8. Start the remote PED server:

```
C:>PedServer.exe -m start

Ped Server Version 1.0.5 (10005)
Ped Server launched in startup mode.
Starting background process
Background process started
Ped Server Process created, exiting this process.
```

9. View the server status:

```
C:>PedServer.exe -m show

Ped Server Version 1.0.5 (10005)
Ped Server launched in status mode.

   Server Information:
      Hostname:                           DemoClient
      IP:                                 172.17.66.233
      Firmware Version:                   0.0.0-0
      PedII Protocol Version:             0.0.0-0
      Software Version:                   1.0.5 (10005)

      Ped2 Connection Status:             Disconnected
      Ped2 RPK Count                      0
      Ped2 RPK Serial Numbers             (none)

   Client Information:                    Not Available

   Operating Information:
      Server Port:                        1503
      External Server Interface:          Yes
      Admin Port:                         1502
      External Admin Interface:           No

      Server Up Time:                     91 (secs)
      Server Idle Time:                   91 (secs) (100%)
      Idle Timeout Value:                 1800 (secs)

      Current Connection Time:            0 (secs)
```

```
          Current Connection Idle Time:        0 (secs)
          Current Connection Total Idle Time: 0 (secs) (100%)
          Total Connection Time:               0 (secs)
          Total Connection Idle Time:          0 (secs) (100%)

    Show command passed.
```

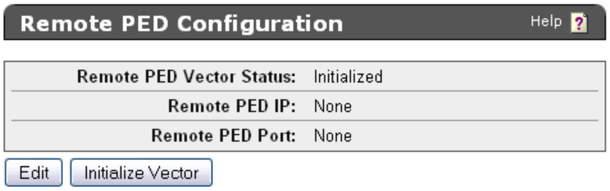
10 Record the Server **IP** and **Server Port** values.

11 Press **<** on the Remote PED to access the mode selection screen.

12 Press **7** for Remote PED mode.

13 Log in to the Management Console.

14 Navigate to the HSM Configuration page (Device >> Device Configuration >> HSM).



Remote PED Vector Status:	Initialized
Remote PED IP:	None
Remote PED Port:	None

15 Click **Edit**.

16 Enter the **Remote PED IP** and the **Remote PED Port**.

17 Click **Save**.

18 Click **Connect**. To connect to the Remote PED.

19 Insert the RPK/Remote (orange) iKey into the Remote PED. The Remote PED display and the corresponding actions are shown below:

```
COMPUTE SESSION KEY...
Insert a RPK / Remote PED Key. Press ENTER.
```

a **Insert the RPK/Remote (orange) iKey** and press Enter.

```
COMPUTE SESSION KEY...
Enter PED PIN.
```

b Enter the PIN for the RPK/Remote (orange) iKey and press Enter.

The Management Console will show that you have successfully connected to the Remote PED. You can now use the Remote PED.

Note: You have 480 seconds in which to insert the orange Remote PED iKey and enter the PED PIN. If this is not completed in time, the connection will fail and you must repeat steps 21 and 22.

Note: In the event of a power outage or system reboot, you must reconnect the remote PED by either repeating steps 16 through 22 above, or by running the `hsm remote ped connect` command from the KeySecure CLI.

To test the Remote PED, you will need the black Crypto User iKey.

1 From the KeySecure CLI, deactivate and reactivate the HSM.

```
DemoBox (config)# hsm deactivate

'partition deactivate' successful.


DemoBox (config)# hsm activate

Luna PED operation required to activate partition on HSM - use User
or Partition Owner (black) PED key.
```

At this point, the Remote PED will prompt for the black Crypto User iKey - also referred to as the Partition Owner PED key. Insert the key and enter the PED PIN. This should successfully reactivate the HSM card.

Activating the HSM Card

To activate the HSM Card, you must log in as the Crypto User. This is requested (and required) as part of the HSM initialization process, but there are other scenarios in which this will be needed.

- HSM card deactivated for less than 2 hours:

  This can happen because of a power outage, scheduled system downtime, or because an admin ran the “hsm deactivate” command from the CLI. To reactivate the HSM, simply run the “hsm login crypto user” command from the CLI.

- HSM card deactivated for more than 2 hours:

  Again, this can happen because of a power outage, scheduled system downtime, or because an admin ran the “hsm deactivate” command from the CLI. In this case, running the “hsm login crypto user” command will require that the crypto user iKey (black) be inserted in a PED; a Remote PED can be used if available and already configured, or a Local PED can be used.

  Note: After a power outage, you will need to run the `hsm remote ped connect` command to re-establish the Remote PED’s connection with the HSM.

Secure Key Caching

Secure key caching improves performance by providing faster access to the key, while maintaining data security. In SafeNet test environments, some key management operations ran 2 -3 times faster when key caching was enabled.

You can **enable** and **disable** secure key caching by using CLI commands as described below.

Note: Secure key caching is available on KeySecure 460 with K6. The two related CLI commands, `hsm enable secure-key-cache` and `hsm disable secure-key-cache`, can be used with the KeySecure 460 platform.

Secure key caching stores the HSM master keys in the process memory of internal servers. To ensure security, these keys are obfuscated, and they are never swapped to disk. On a KeySecure, only the HSM keys that are specific to KeySecure VM are cached; SSKM VM keys are not.

You do not violate FIPS requirements by enabling secure-key-caching.

Note: The secure key caching settings are not replicated across a cluster; you must enable or disable secure key caching by using the CLI command for each node in the cluster, as needed.

Note the following characteristics regarding secure-key-caching:

- For this command to work, the crypto user must be logged in.
- Even though the master keys are cached, the master keys are not available for use when the crypto user is logged out. So, the system behavior is the same as without secure key caching.
- When a box is freshly imaged, it will start with secure-key-caching disabled by default.
- The secure-key-caching configuration is not maintained by Backup or Restore capabilities.

You can discover the current state of the secure-key-cache by using `show hsm status`. For example:

```
DemoBox# show hsm status
   HSM Status:    Initialized
   Crypto-user logged in: yes
   HSM secure-key-cache: Enabled
```

Secure Key Caching CLI Commands

There are two secure key caching commands, enable and disable, which are explained below, For general information about secure key caching, see the introduction above.

hsm enable secure-key-cache – start applying the key-caching functions

When you run the this command, the response tells you if it failed or succeeded, or if it is already in the state requested by the command. For example:

Here is confirmation of a successful use of `enable secure-key-cache`:

```
DemoBox#  hsm enable secure-key-cache

Successfully enabled HSM secure-key-cache.
```

Here is the result when secure-key-caching is already enabled:

```
DemoBox#  hsm enable secure-key-cache

HSM secure-key-cache is already enabled.
```

hsm disable secure-key-cache – stop the key-caching functions

When you run the this command, the response tells you if it failed or succeeded, or if it is already in the state requested by the command. For example:

Here is confirmation of a successful use of `disable secure-key-cache`:

```
DemoBox#  hsm disable secure-key-cache
Successfully disabled HSM secure-key-cache.
```

Here is the result when secure-key-caching is already disabled:

```
DemoBox#  hsm disable secure-key-cache
HSM secure-key-cache is already disabled.
```

Duplicating iKeys

At some time you may want to duplicate iKeys. The PED display avails this opportunity when you configure the iKeys during the HSM initialization, but we recommend duplicating iKeys **after** the initialization process is complete and its success has been confirmed.

Duplicating iKeys requires:

- **The iKey** - the original key that will be duplicated. You should demarcate this original key so that its uniqueness is obvious. ***Do not overwrite the original!*** Overwriting the original iKey would be very unfortunate; to recover, you need to repeat whichever process was required to create the iKey. For the orange Remote PED iKey, this process is relatively simple. For the black User iKey, blue SO/HSM Admin iKey, and the red Domain iKey, however, you must re-initialize the HSM, which requires you to restore the KeySecure to its initial factory settings. This requires the guidance of SafeNet Technical Support. So, be cautious.
- **The PED** - configured to operate in either local or remote mode
- **Extra iKeys -** the iKeys that will become duplicates of the original.

To duplicate an iKey:

1. Insert the working iKey into the PED.
2. Press **<** to exit the current mode.
3. Press **4** to enter Admin mode.
4. Press **1** to enter PED Key mode.
5. Insert the **original** iKey - the iKey that will be duplicated.
6. Press **1** to Login.
7. Press **7** to Duplicate.
8. Insert the **target** iKey and Press **Enter**.
9. Follow the PED prompts. Make additional duplicates if desired.

For example, to make one duplicate of the black User iKey while using the remote PED:

1 Remove any iKey from the PED.

2 Select **<** to exit Remote PED mode. The PED will warn you that exiting will invalidate the orange Remote PED iKey. As long as you have physical access to this orange iKey, there is no need to be alarmed. You'll reinsert that iKey later to return to Remote mode. Press **Yes**.

3 Press **4** to enter Admin mode.

4 Press **1** to enter PED Key mode.

5 Insert the **original** iKey you want to duplicate. In this example, it's the **black** User iKey.

6 Press **1** to Login.

7 Press **7** to Duplicate.

8 Insert the **target** iKey. This is a **blank** black User iKey - or at least an iKey you want to overwrite.

9 Press **Enter**.

Note: If you are overwriting an existing iKey, the PED will warn you before doing so.

The duplicate is now created. Remove it an press **Enter**. For this example, decline the offer to make another duplicate.

10 Return to Remote PED Mode. (Press **<** twice and then **7**).

To test the new black User iKey, you will deactivate and then activate the HSM.

11 Log on to the KeySecure Command Line Interface as an administrator.

12 Type `config` to enter configuration mode.

13 Run `hsm deactivate` to deactivate the HSM card.

14 Run `hsm activate` to activate the HSM card. Activating the card requires the black User iKey.

15 Since this example uses the Remote PED, you must validate the orange Remote PED iKey. **Insert** the orange iKey and press **Enter**.

16 Enter the PED PIN.

17 Once the orange iKey is validated, you must enter the black User iKey to activate the HSM. Insert the **new** black iKey and press **Enter**.

18 Enter the PED PIN.

The KeySecure Command Line Interface should now indicate that the hsm activation was successful.

To test a duplicate orange Remote PED iKey, follow the procedure above, but insert the **original** orange iKey in step 5 and the **target** orange iKey in step 8. Use the new orange iKey in steps 11 through 18 to check that it works correctly.

To test a duplicate blue SO/HSM Admin iKey, substitute the `hsm logout security officer` and `hsm login security officer` commands instead of the `hsm deactivate` and `hsm activate` commands shown in steps 13 and 14.

Chapter 29

Authorization Policies

An authorization policy enables you to limit how a user group may use a key. On the KeySecure 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.

Important! Authorization Policies are an alternative to management by key Life Cycle. Do not use Authorization Policies in conjunction with Life Cycle Management.

Authorization policies define two kinds of limits:

- **Rate Limits:** The number of 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.

  Note: 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.

  The Key Server starts keeping track of the number of operations performed by a user as soon as that user makes a request to the server. Once the clock is running, the user has a one hour time period in which to perform no more than the number of operations specified in the Maximum Operations per Hour field. Should you change the limit for a particular policy, those changes 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

  Likewise, if the limit was lowered to 75, User1 would only be allowed to make 25 more requests.

- **Time Limits:** The hours or days in which 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.

  A usage period is an uninterrupted time span, during which the authorization policy applies. 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.

Once an authorization policy is defined it is associated with a key and a group through the Group Permissions section 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 server 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.

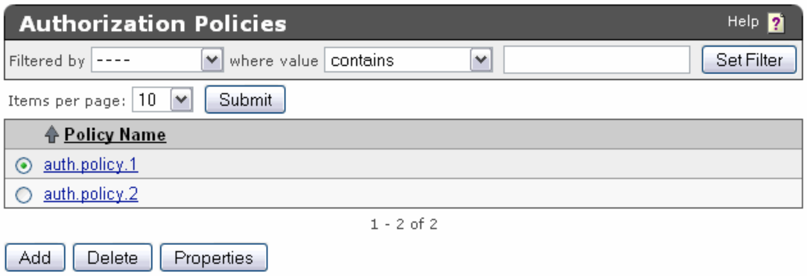
Note: Authorization policies cannot be applied to global keys or to certificates. Key owners are not subject to policy restrictions.

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).



Authorization Policies

Filtered by ---- where value contains

Items per page: 10

Policy Name
● auth.policy.1
○ auth.policy.2

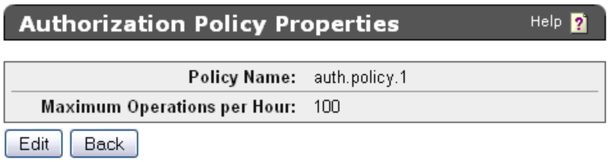
1 - 2 of 2

3 Click **Add**.

4 Enter a **Policy Name**.

5 Click **Save**.

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



Authorization Policy Properties

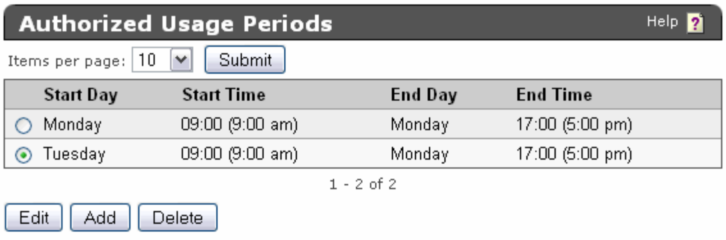
Policy Name: auth.policy.1

Maximum Operations per Hour: 100

7 Click **Edit** to establish a rate limit using the **Maximum Operations per Hour** field. By default, policies can perform unlimited operations. The valid range of operations is 1 to 500,000,000.

8 Click **Save**.

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

1 - 2 of 2

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

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 and click **Delete**.

Chapter 30

Local Users and Groups

A user directory contains a list of users that may access the keys on your Key Server, and a list of groups to which those users belong. The Key Server can use one of two user directories:

- A local user directory, where users and groups are defined only on the local device and are not available to any other KeySecure.
- A central server running the Lightweight Directory Access Protocol (LDAP), which enables all devices to access the same set of users and groups. If you have several KeySecures in use, LDAP can greatly simplify user and group administration.

The Key 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 Key Server uses on the Network-Attached Encryption Server Configuration page in the section Key Server Authentication Settings. See “Configure the User Directory Settings” on page 19 for more details.

When you configure the Key Server to use an LDAP user directory instead of the local user directory (or vice versa), or if you change the LDAP server settings to point to a different user directory, existing key permissions and database user mappings 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.

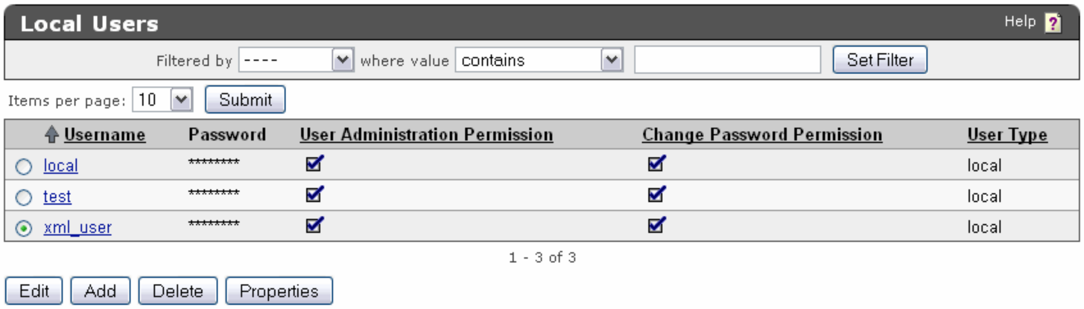
For more information about LDAP users, see Chapter 32, “LDAP User & Groups”.

Create a Local User

To create a local 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 & Group Configuration page (Security >> Local Users & Groups).



Filtered by ---- where value contains

Items per page: 10

	Username	Password	User Administration Permission	Change Password Permission	User Type
○	local	*********	☑	☑	local
○	test	*********	☑	☑	local
●	xml_user	*********	☑	☑	local

1 - 3 of 3

3 Click **Add**.

4 Enter a **Username**. 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. Once saved, you cannot change the **Username**.

5 Enter a **Password**. The requirements for the local user password depend on your Password Management Settings. For information on password requirements, refer to Chapter 16, “Password Management”. The maximum password length is 256 characters and it cannot contain the less than character (<).

The passwords displayed on the Local Users section are masked with eight asterisks (*). When changing the password, clear this field before entering the new password. If you do not clear this field, the asterisks become a part of the new password.

6 Select **User Administration Permission** to give this user the ability to create, modify, and delete users and groups via the XML interface. Users with this feature enabled automatically have the **Change Password Permission**.

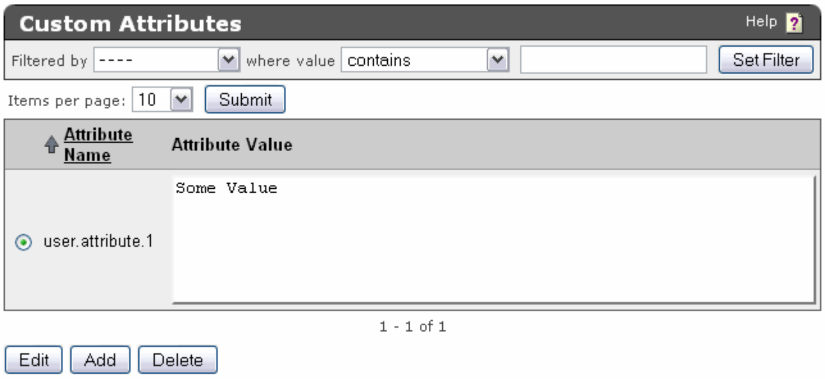
Important! You should be extremely cautious in assigning the User Administration Permission. Its use should be reserved for situations where you want to perform user administration programmatically using the XML interface of the Key Server (as opposed to the Management Console). In such deployments, the User Administration Permission should be given to a very small number of users. Most users should not be given this permission.

7 Select **Change Password Permission** to give this user the ability to change his or her own password via the XML interface.

8 Click **Save**. The **User Type** field will automatically populate with the value *local*. The remainder of these instructions describe how to create custom attributes, which are not required.

9 Select the **Username** and click **Properties**.

10 Select the Custom Attributes tab.



Filtered by ---- where value contains

Items per page: 10

Attribute Name	Attribute Value
● user.attribute.1	Some Value

1 - 1 of 1

11 Click **Add**.

12 Enter an **Attribute Name**. The name can contain alphanumeric characters, hyphens, underscores, and periods. You cannot include whitespace in the name. In addition, the first character of the name must be a letter. The maximum length is 64 characters.

13 Enter an **Attribute Value**. Enter the value of the attribute. This can contain any printable ASCII characters and spaces, tabs, \n and \r. The maximum length is 1000 characters.

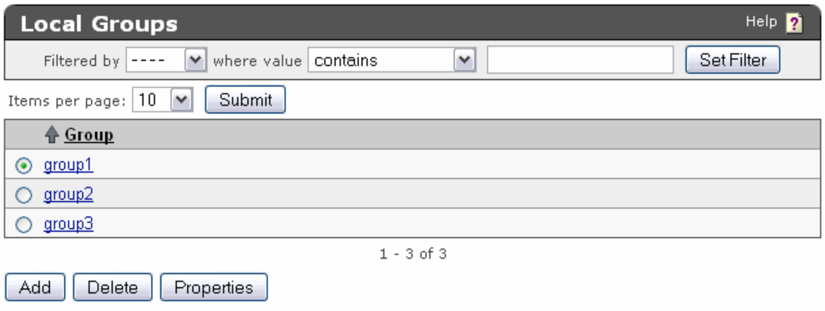
14 Click **Save**.

Creating a Local Group

To create a local 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 & Group Configuration page (Security >> Local Users & Groups).



	Group
●	group1
○	group2
○	group3

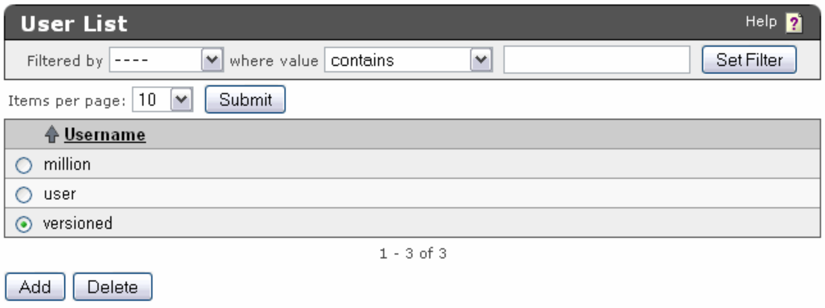
1 - 3 of 3

3 Click **Add**.

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

5 Click **Save**. You can now add users to the group.

6 Select the **Group** on the Local Groups section to access the User List.



	Username
○	million
○	user
●	versioned

1 - 3 of 3

7 Click **Add** and enter a local user in the **Username** field. Click ALT-[down arrow] to see a list of available local users.

8 Click **Save**.

Removing a User from a Group

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 & Group Configuration page (Security >> Local Users & Groups).
3. Select a Group and click **Properties** or click the group name to access the User List section.
4. Select the **Username** and click **Delete**.

Deleting a User

When deleting users, the system does not check to see if that user has been mapped to a database user. All database users mapped to the user being deleted lose all privileges associated with that user. In such a scenario, the database users lose access to the keys, which means that those users cannot encrypt or decrypt data.

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

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 & Group Configuration page (Security >> Local Users & Groups).
3. Select the **Username** and click **Delete**.

Note: You cannot delete a user if it is a key owner.

Deleting a 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 & Group Configuration page (Security >> Local Users & Groups).
3. Select the **Group** and click **Delete**.

Chapter 31

LDAP Server

Lightweight Directory Access Protocol (LDAP) is a protocol that allows you to enable authentication of your Key Server based on a central directory of users, rather than the local users and groups defined on each device. To use LDAP with the Key Server, 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.

Note: If you set up the Key Server to use LDAP for users and groups, those users and groups are case-*in*sensitive. For example, a 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 case are treated differently.

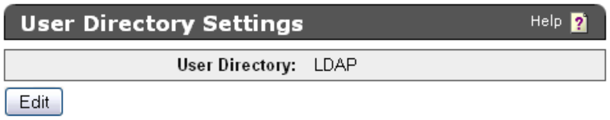
Passwords for both local users and LDAP users must not contain the less than character (<).

Setting up the LDAP User Server

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 User Directory Settings section of the Cryptographic Key Server Configuration page (Device >> Key Server).

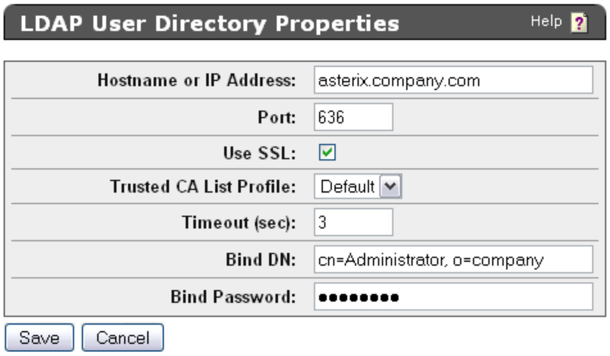


User Directory Settings

User Directory: LDAP

3 Click **Edit**. Select *LDAP* and click **Save**.

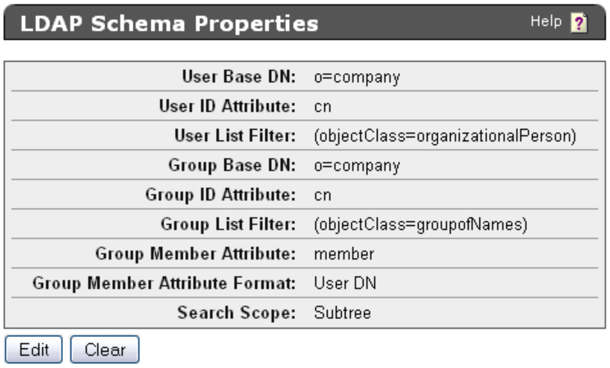
4 Navigate to the LDAP User Directory Properties section of the LDAP Server Configuration page (Security >> LDAP >> LDAP Server).



LDAP User Directory Properties

Hostname or IP Address:	asterix.company.com
Port:	636
Use SSL:	☑
Trusted CA List Profile:	Default
Timeout (sec):	3
Bind DN:	cn=Administrator, o=company
Bind Password:	●●●●●●●●

5. Click **Edit**.
6. Enter the **Hostname or** IP **Address** and **Port** of the primary LDAP server. LDAP servers typically use port 389. For SSL connections, LDAP servers typically use port 636.
7. Select **Use SSL** to enable SSL. By default, the KeySecure connects directly to the LDAP server over TCP.
8. If using SSL, enter the **Trusted Certificate Authority**. The CA will verify that the server certificate presented by LDAP servers are signed by a CA trusted by the KeySecure.
9. Enter a value in the **Timeout** field. This is the number of seconds to wait for the LDAP server during connections and searches. If the connection times out, the authorization fails.
10. Enter the **Bind DN** (distinguished name) used to bind to the server. The device 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 **Blind Password** field empty.
11. Click **Save**.
12. Click **LDAP Test** to test the connection.
13. Set up the LDAP Schema using the LDAP Schema Properties section (Security >> LDAP >> LDAP Server).



LDAP Schema Properties

User Base DN:	o=company
User ID Attribute:	cn
User List Filter:	(objectClass=organizationalPerson)
Group Base DN:	o=company
Group ID Attribute:	cn
Group List Filter:	(objectClass=groupofNames)
Group Member Attribute:	member
Group Member Attribute Format:	User DN
Search Scope:	Subtree

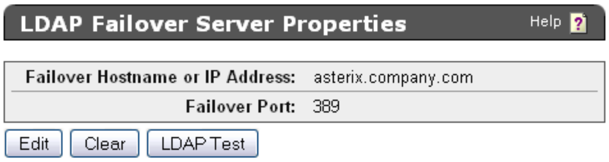
14. Click **Edit**.
15. Enter the values for your LDAP schema.
    - **User Base DN** - the base distinguished name (DN) from which to begin the search for usernames.
    - **User ID Attribute** - the attribute type for the user on which to search. The attribute type you choose must result in globally unique users.
    - **User List Filter** - used for narrowing the search within the object class. 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 attribute that is 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 next setting.
- **Group Member Attribute Format** - either *Used ID* or *User DN.*
- **Search Scope** - determines how deep within the LDAP user directory the Key Server searches for a user or group.
  - *One Level*: search only the children of the base node
  - *Subtree*: search all the descendents 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, onelevel, subtree and children. The Key Server allows you to specify only onelevel and subtree at this time. You should note that subtree includes base and children, so by specifying subtree, the search scope includes subtree, base, and children.

16 Click **Save**.

17 Set up the LDAP failover server using the LDAP Failover Server Properties section of the LDAP Server Configuration page (Security >> LDAP >> LDAP Server). When the primary LDAP server is down, the KeySecure shifts to the failover server and periodically retries the main server to see if it have become accessible again.



Failover Hostname or IP Address:	asterix.company.com
Failover Port:	389

18 Click **Edit**.

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

20 Click **Save**.

21 Click **LDAP Test** to test the connection.

When the LDAP server is configured, the available users and groups will be visible on the LDAP Users and LDAP Groups sections (Security >> LDAP >> LDAP Users & Groups)

Chapter 32

LDAP User & Groups

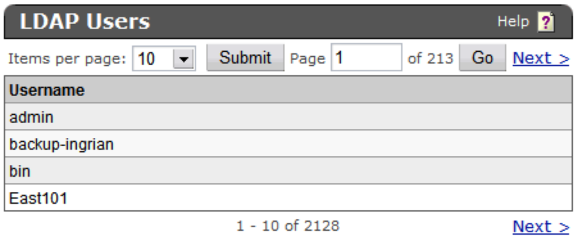
The LDAP User & Group Configuration page enables you to view the users and groups for the server as defined by the LDAP directory. You can only view the users and groups on this page; users and groups are created, modified, and removed on the LDAP server itself.

View LDAP Users

To view LDAP users:

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

2 Navigate to the LDAP User & Group Configuration page (Security >> LDAP >> LDAP Users & Groups).



Username
admin
backup-ingrian
bin
East101

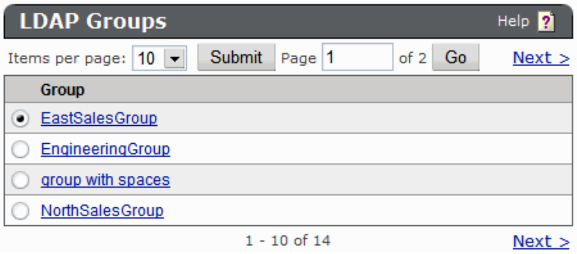
3 View the list of users. These users are created, modified, and removed on your LDAP server.

View LDAP Groups

To view LDAP groups:

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

2 Navigate to the LDAP User & Group Configuration page (Security >> LDAP >> LDAP Users & Groups).



	Group
●	EastSalesGroup
○	EngineeringGroup
○	group with spaces
○	NorthSalesGroup

3 View the list of groups. These groups are created, modified, and removed on your LDAP server.

4 Click the group name to access the User List section and view the group members.

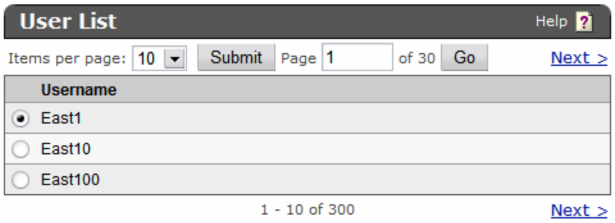
View LDAP Group Members

To view LDAP groups:

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

2 Navigate to the LDAP User & Group Configuration page (Security >> LDAP >> LDAP Users & Groups).

3 Select a group name.



Items per page: 10 Page 1 of 30

	Username
●	East1
○	East10
○	East100

1 - 10 of 300

4 View the group membership list. Groups and users are managed on the LDAP server.

Chapter 33

Certificates

Certificates identify one entity to another. In this case, when making SSL connections between a client application and the Key Server, the server must provide its server certificate to the client application. Likewise, if you require client applications to validate themselves to the Key Server via client certificates, then the client application must provide its client certificate to the server during the SSL handshake.

The Key Server uses the following two kinds of certificates:

- *Server* certificates on the KeySecure allow a KeySecure to authenticate itself to a client application during an SSL handshake.
- *Client* certificates allow client applications to authenticate themselves to the KeySecure during an SSL handshake. Where the certificate resides varies from application to application and database to database.

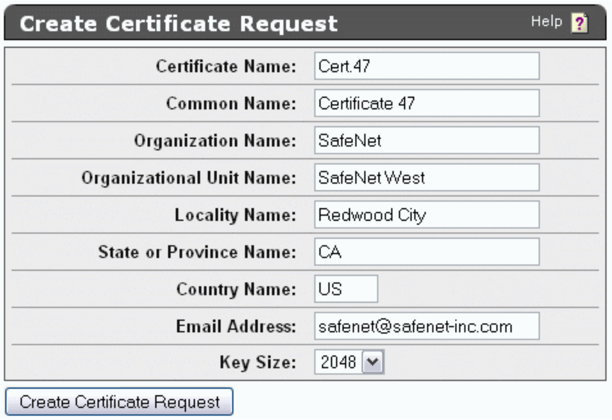
Creating a Server Certificate for the KeySecure

Before the KeySecure can respond to SSL requests from a client application, the KeySecure must be configured with at least one server certificate.

Note: To generate a valid certificate, you must have a certificate authority sign a certificate request. You can create local CAs on the KeySecure, and use those CAs to sign certificate requests. Otherwise, you must use an external CA to sign certificate requests. The following steps assume that you have already created a local CA.

To create a server certificate for the KeySecure:

1. Log in to the Management Console as an administrator with Certificates access control.
2. Navigate to the Create Certificate Request section of the Certificate and CA Configuration page (Security >> SSL Certificates).

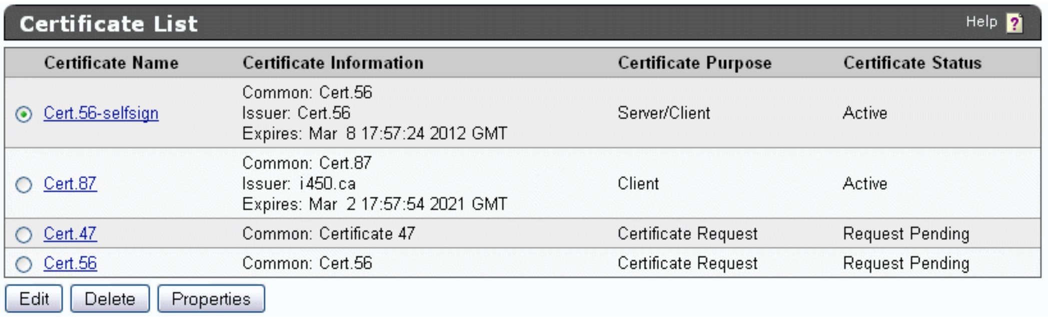


Create Certificate Request

Certificate Name:	Cert.47
Common Name:	Certificate 47
Organization Name:	SafeNet
Organizational Unit Name:	SafeNet West
Locality Name:	Redwood City
State or Province Name:	CA
Country Name:	US
Email Address:	safenet@safenet-inc.com
Key Size:	2048

3 Enter the **Certificate Name**, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, and **Key Size** for the certificate. The KeySecure supports 768-bit, 1024-bit, and 2048-bit key sizes.

4 Click **Create Certificate Request**. The new request appears in the Certificate List with a status of *Request Pending*.

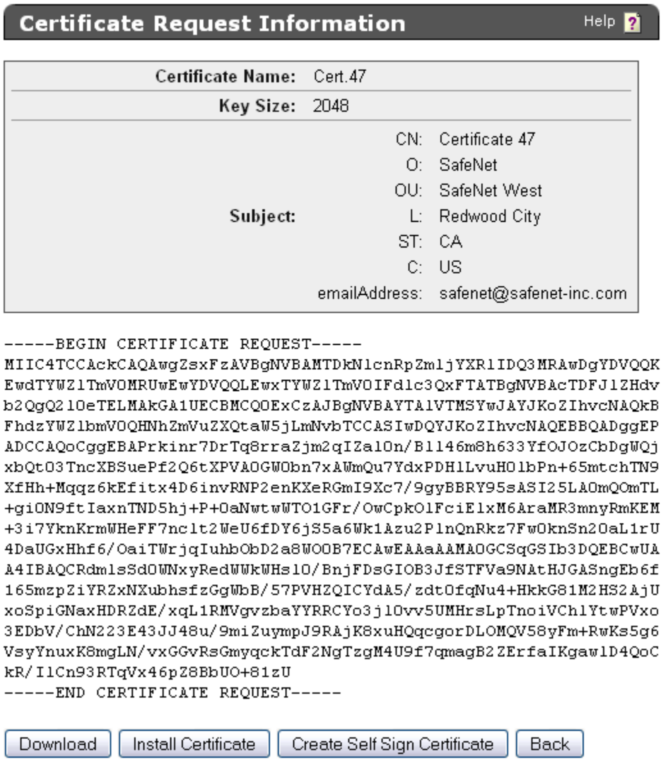


Certificate List

Certificate Name	Certificate Information	Certificate Purpose	Certificate Status
● Cert.56-selfsign	Common: Cert.56 Issuer: Cert.56 Expires: Mar 8 17:57:24 2012 GMT	Server/Client	Active
○ Cert.87	Common: Cert.87 Issuer: i450.ca Expires: Mar 2 17:57:54 2021 GMT	Client	Active
○ Cert.47	Common: Certificate 47	Certificate Request	Request Pending
○ Cert.56	Common: Cert.56	Certificate Request	Request Pending

5 Select the certificate request and click **Properties** to access the Certificate Request Information section.

Note: At this point you can select **Create Self Sign Certificate** to create a self-signed certificate. This enables you to avoid getting a certificate request signed by a local CA, or a CA on another KeySecure. Self-signed certificates can be presented to client applications just like any other certificate. We recommend that self-signed certificates be used for testing purposes only. Any attempt to connect to a KeySecure using a self-signed certificate sends a warning to the client browser. The remainder of these instructions explain how to sign a certificate request with a CA.



Certificate Name:	Cert.47	
Key Size:	2048	
Subject:	CN:	Certificate 47
	O:	SafeNet
	OU:	SafeNet West
	L:	Redwood City
	ST:	CA
	C:	US
	emailAddress:	safenet@safenet-inc.com

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC4TCCAckCAQAwgZsxFzAVBgNVBAMTDkNlcnRpZmljYXRlIDQ3MRAwDgYDVQQK
EwdTYWZlTmV0MRUwEwYDVQQLEwxTYWZlTmV0IFdlc3QxFTATBgNVBAcTDFJlZHdv
b2QgQ2l0eTELMAkGA1UECBMCQ0ExCzAJBgNVBAYTAlVTMSYwJAYJKoZIhvcNAQkB
FhdzYWZlbmV0QHNhZmVuZXQtaW5jLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAPrkinr7DrTq8rraZjm2qIZalOn/Bll46m8h633YfOJOzCbDgWQj
xbQtO3TncXBSuePf2Q6tXPVAOGWObn7xAWmQu7YdxPDHlLvuHOlbPn+65mtchTN9
XfHh+Mqqz6kEfitx4D6invRNP2enKXeRGmI9Xc7/9gyBBRY95sASI25LAOmQOmTL
+giON9ftIaxnTND5hj+P+0aNwtwWTO1GFr/OwCpkOlFciElxM6AraMR3mnyRmKEM
+3i7YknKrmWHeFF7nclt2WeU6fDY6jS5a6Wk1Azu2PlnQnRkz7FwOknSn2OaL1rU
4DaUGxHhf6/OaiTWrjqIuhbObD2a8WOOB7ECAwEAAaAAMA0GCSqGSIb3DQEBCwUA
A4IBAQCRdmlsSdOWNxyRedWWkWHslO/BnjFDsGIOB3JfSTFVa9NAtHJGASngEb6f
165mzpZiYRZxNXubhsfzGgWbB/57PVHZQICYdA5/zdtOfqNu4+HkkG81M2HS2AjU
xoSpiGNaxHDRZdE/xqL1RMVgvzbaYYRRCYo3jlOvv5UMHrsLpTnoiVChlYtwPVxo
3EDbV/ChN223E43JJ48u/9miZuympJ9RAjK8xuHQqcgorDLOMQV58yFm+RwKs5g6
VsyYnuxK8mgLN/vxGGvRsGmyqckTdF2NgTzgM4U9f7qmagB2ZErfaIKgawlD4QoC
kR/IlCn93RTqVx46pZ8BbUO+81zU
-----END CERTIFICATE REQUEST-----
```

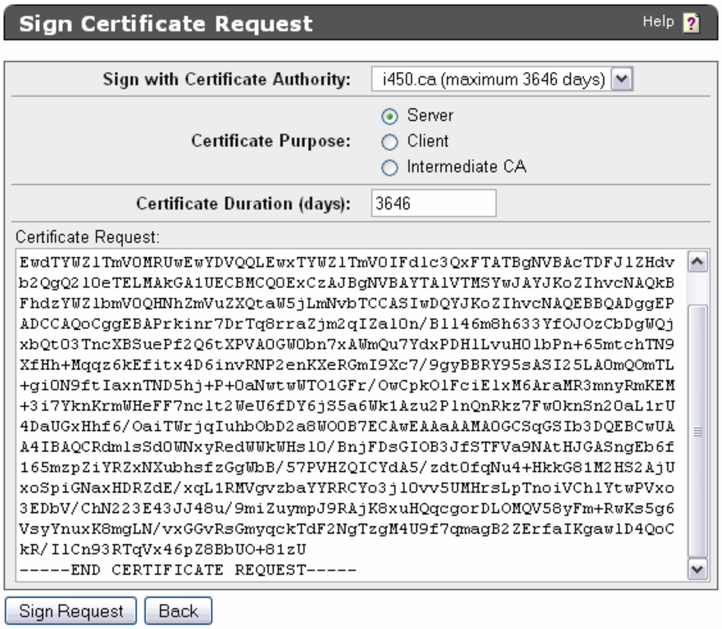
6 Copy the certificate request text. The certificate text looks similar, but not identical, to the following text.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBmzCCAQQCAQAwWzEPMA0GA1UEAxMGZmxldGNoMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEJM
AcGA1UEBxMAMQkwBwYDVQQIEwAxCzAJBgNVBAYTAlVTMQ8wDQYJKoZIhvcNAQkBFgAwgZ8wDQ
YJKoZIhvcAYBABTUxxgY0AMIGJAoGBAMUqA1t4m&Nm0sCcUqnt5Yug+qTSbgEFnvnYWUApHKD
lx5keC1lguQDU1ol2Xcc3YGrUviGCe4y0JIMK2giQ5b+ABQDemRiD11vInQqkhV6ngWBRD0lp
KCjU6QXDEE9KGCKBRh5uqL70rr2LErqxUuYwOu50Tfn4T3tKb1HGgfdzAgMBAAGgADANBgkqh
kiG9w0BAQQFAAOBgQCuYnv8vBzXEZpgLD71FfeDK2Zqh0FnfTHXAkHrj4JP3MCMF5nKHgOSRV
mImNHHy0cYKTDP+hor68R76XhLVapKMqNuUHUYf7CTB5JNHHy0cYKTNHHy0cYKTuV1Ce8nvvU
G+yp2Eh8aJ7thaua41xDFXPmIEXTqzXi1++DCWAdWaysojPCZugY7jNWXmg==
-----END CERTIFICATE REQUEST-----
```

Important! Be sure to include the first and last lines (-----BEGIN CERT... and -----END CERT...), and copy only the text in the certificate. Do not copy any extra white space.

7 Navigate to the Local Certificate Authority List section (Security >> Local CAs).

8 Select a CA and click **Sign Request**.



Sign with Certificate Authority: i450.ca (maximum 3646 days)

Certificate Purpose: ● Server ○ Client ○ Intermediate CA

Certificate Duration (days): 3646

Certificate Request:

```
EwdTYWZlTmVOMRUwEwYDVQQLEwxTYWZlTmVOIFdlc3QxFTATBgNVBAcTDFJlZHdv
b2QgQ2l0eTELMAkGA1UECBMCQ0ExCzAJBgNVBAYTAlVTMSYwJAYJKoZIhvcNAQkB
FhdzYWZlbmV0QHNhZmVuZXQtaW5jLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAPrkinr7DrTq8rraZjm2qIZal0n/Bl146m8h633YfOJOzCbDgWQj
xbQtO3TncXBSuePf2Q6tXPVAOGWObn7xAWmQu7YdxPDHlLvuHOlbPn+65mtchTN9
XfHh+Mqqz6kEfitx4D6invRNP2enKXeRGmI9Xc7/9gyBBRY95sASI25LAOmQOmTL
+giON9ftIaxnTND5hj+P+OaNwtwWTO1GFr/OwCpkOlFciElxM6AraMR3mnyRmKEM
+3i7YknKrmWHeFF7nclt2WeU6fDY6jS5a6Wk1Azu2PlnQnRkz7FwOknSn2OaL1rU
4DaUGxHhf6/OaiTWrjqIuhbObD2a8WOOB7ECAwEAAaAAMAOGCSqGSIb3DQEBCwUA
A4IBAQCRdmlsSdOWNxyRedWWkWHs1O/BnjFDsGIOB3JfSTFVa9NAtHJGASngEb6f
165mzpZiYRZxNXubhsfzGgWbB/57PVHZQICYdA5/zdtOfqNu4+HkkG81M2HS2AjU
xoSpiGNaxHDRZdE/xqL1RMVgvzbaYYRRCYo3jlOvv5UMHrsLpTnoiVChlYtwPVxo
3EDbV/ChN223E43JJ48u/9miZuympJ9RAjK8xuHQqcgorDLOMQV58yFm+RwKs5g6
VsyYnuxK8mgLN/vxGGvRsGmyqckTdF2NgTzgM4U9f7qmagB2ZErfaIKgawlD4QoC
kR/IlCn93RTqVx46pZ8BbUO+81zU
-----END CERTIFICATE REQUEST-----
```

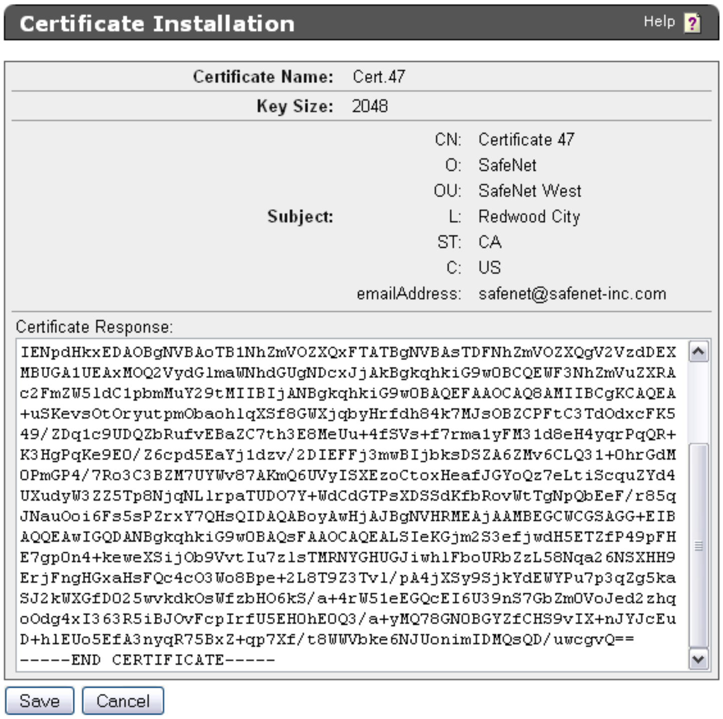
9 Paste the certificate request into the **Certificate Request** field. Select Server as the **Certificate Purpose**, specify a **Certificate Duration** and click **Sign Request**. The newly-activated certificate displays on a new page.

10 Copy the certificate text.

11 Navigate back to the Certificate List section.

12 Select the certificate request and click **Properties** to access the Certificate Request Information section.

13 Click **Install Certificate**.



Certificate Name:	Cert.47
Key Size:	2048
Subject:	CN: Certificate 47 O: SafeNet OU: SafeNet West L: Redwood City ST: CA C: US emailAddress: safenet@safenet-inc.com

Certificate Response:

```
IENpdHkxEDAOBgNVBAoTB1NhZmVOZXQxFTATBgNVBAsTDFNhZmVOZXQgV2VzdDEX
MBUGA1UEAxMOQ2VydGlmaWNhdGUgNDcxJjAkBgkqhkiG9w0BCQEWF3NhZmVuZXRA
c2FmZW5ldC1pbmMuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+uSKevsOtOryutpmObaohlqXSf8GWXjqbyHrfdh84k7MJsOBZCPFtC3TdOdxcFK5
49/ZDq1c9UDQZbRufvEBaZC7th3E8MeUu+4fSVs+f7rma1yFM31d8eH4yqrPqQR+
K3HgPqKe9EO/Z6cpd5EaYj1dzv/2DIEFFj3mwBIjbksDSZA6ZMv6CLQ31+OhrGdM
OPmGP4/7Ro3C3BZM7UYWv87AKmQ6UVyISXEzoCtoxHeafJGYoQz7eLtiScquZYd4
UXudyW3ZZ5Tp8NjqNLlrpaTUDO7Y+WdCdGTPsXDSSdKfbRovWtTgNpQbEeF/r85q
JNauOoi6Fs5sPZrxY7QHsQIDAQABoyAwHjAJBgNVHRMEAjAAMBEGCWCGSAGG+EIB
AQQEAwIGQDANBgkqhkiG9w0BAQsFAAOCAQEALSIeKGjm2S3efjwdH5ETZfP49pFH
E7gpOn4+keweXSijOb9VvtIu7zlsTMRNYGHUGJiwhlFboURbZzL58Nqa26NSXHH9
ErjFngHGxaHsFQc4cO3Wo8Bpe+2L8T9Z3Tvl/pA4jXSy9SjkYdEWYPu7p3qZg5ka
SJ2kWXGfDO25wvkdkOsWfzbHO6kS/a+4rW51eEGQcEI6U39nS7GbZmOVoJed2zhq
oOdg4xI363R5iBJOvFcpIrfU5EHOhEOQ3/a+yMQ78GNOBGYZfCHS9vIX+nJYJcEu
D+hlEUo5EfA3nyqR75BxZ+qp7Xf/t8WWVbke6NJUonimIDMQsQD/uwcgvQ==
-----END CERTIFICATE-----
```

14 Paste the text of the signed certificate into the **Certificate Response** field.

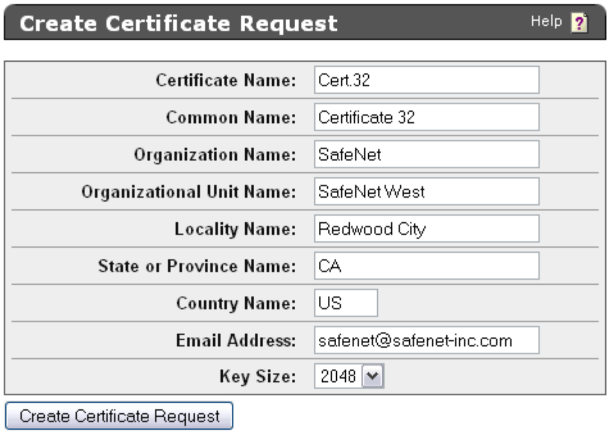
15 Click **Save**. When you return to the main Certificate Configuration page, the certificate request is now an active certificate. It can be used in to establish SSL connections with client applications.

Creating a Client Certificate

To create a client certificate for the KeySecure:

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

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

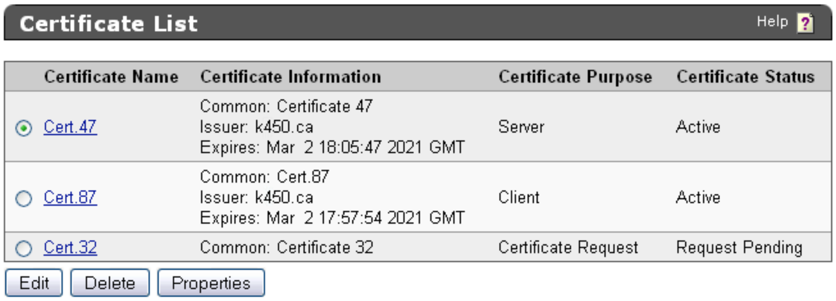


Create Certificate Request

Certificate Name:	Cert.32
Common Name:	Certificate 32
Organization Name:	SafeNet
Organizational Unit Name:	SafeNet West
Locality Name:	Redwood City
State or Province Name:	CA
Country Name:	US
Email Address:	safenet@safenet-inc.com
Key Size:	2048

3 Enter the **Certificate Name**, **Common Name**, **Organization Name**, **Organizational Unit Name**, **Locality Name**, **State or Province Name**, **Country Name**, **Email Address**, and **Key Size** for the certificate.

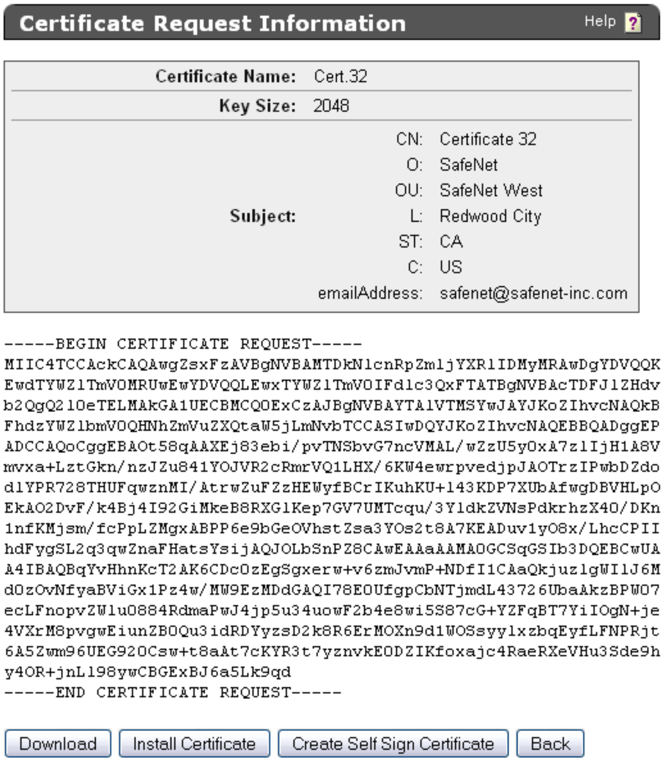
4 Click **Create Certificate Request**. The new request appears in the Certificate List with a status of *Request Pending*.



Certificate List

Certificate Name	Certificate Information	Certificate Purpose	Certificate Status
● Cert.47	Common: Certificate 47 Issuer: k450.ca Expires: Mar 2 18:05:47 2021 GMT	Server	Active
○ Cert.87	Common: Cert.87 Issuer: k450.ca Expires: Mar 2 17:57:54 2021 GMT	Client	Active
○ Cert.32	Common: Certificate 32	Certificate Request	Request Pending

5 Select the certificate request and click **Properties** to access the Certificate Request Information section.



Certificate Request Information

Certificate Name:	Cert.32	
Key Size:	2048	
Subject:	CN:	Certificate 32
	O:	SafeNet
	OU:	SafeNet West
	L:	Redwood City
	ST:	CA
	C:	US
	emailAddress:	safenet@safenet-inc.com

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC4TCCAckCAQAwgZsxFzAVBgNVBAMTDkNlcnRpZmljYXRlIDMyMRAwDgYDVQQK
EwdTYWZlTmV0MRUwEwYDVQQLEwxTYWZlTmV0IFdlc3QxFTATBgNVBAcTDFJlZHdv
b2QgQ2l0eTELMAkGA1UECBMCQ0ExCzAJBgNVBAYTAlVTMSYwJAYJKoZIhvcNAQkB
FhdzYWZlbmV0QHNhZmVuZXQtaW5jLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAOt58qAAXEj83ebi/pvTNSbvG7ncVMAL/wZzU5y0xA7zlIjH1A8V
mvxa+LztGkn/nzJZu841YOJVR2cRmrVQ1LHX/6KW4ewrpvedjpJAOTrzIPwbDZdo
dlYPR728THUFqwznMI/AtrwZuFZzHEWyfBCrIKuhKU+l43KDP7XUbAfwgDBVHLpO
EkAO2DvF/k4Bj4I92GiMkeB8RXGlKep7GV7UMTcqu/3YldkZVNsPdkrhzX4O/DKn
1nfKMjsm/fcPpLZMgxABPP6e9bGeOVhstZsa3YOs2t8A7KEADuv1yO8x/LhcCPII
hdFygSL2q3qwZnaFHatsYsijAQJOLbSnPZ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUA
A4IBAQBqYvHhnKcT2AK6CDcOzEgSgxerw+v6zmJvmP+NDfI1CAaQkjuzlgWIlJ6M
d0zOvNfyaBViGx1Pz4w/MW9EzMDdGAQI78EOUfgpCbNTjmdL43726UbaAkzBPWO7
ecLFnopvZWlu0884RdmaPwJ4jp5u34uowF2b4e8wi5S87cG+YZFqBT7YiIOgN+je
4VXrM8pvgwEiunZBOQu3idRDYyzsD2k8R6ErMOXn9d1WOSsyylxzbqEyfLFNPRjt
6A5Zwm96UEG92OCsw+t8aAt7cKYR3t7yznvkEODZIKfoxajc4RaeRXeVHu3Sde9h
y4OR+jnLl98ywCBGExBJ6a5Lk9qd
-----END CERTIFICATE REQUEST-----
```

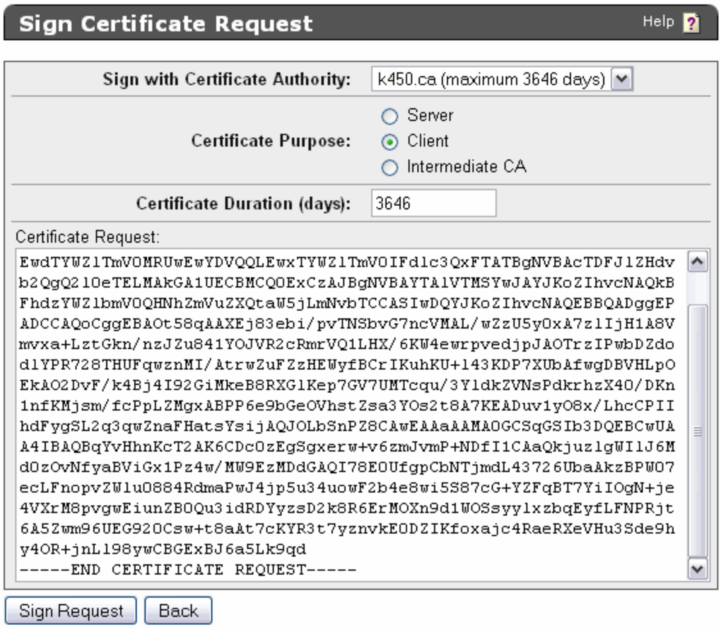
6 Copy the certificate request text. The certificate text looks similar, but not identical, to the following text.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBmzCCAQQCAQAwWzEPMA0GA1UEAxMGZmxldGNoMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEJM
AcGA1UEBxMAMQkwBwYDVQQIEwAxCzAJBgNVBAYTAlVTMQ8wDQYJKoZIhvcNAQkBFgAwgZ8wDQ
YJKoZIhvcAYBABTUxxgY0AMIGJAoGBAMUqA1t4m&Nm0sCcUqnt5Yug+qTSbgEFnvnYWUApHKD
lx5keC1lguQDU1ol2Xcc3YGrUviGCe4y0JIMK2giQ5b+ABQDemRiD11vInQqkhV6ngWBRD0lp
KCjU6QXDEE9KGCKBRh5uqL70rr2LErqxUuYwOu50Tfn4T3tKb1HGgfdzAgMBAAGgADANBgkqh
kiG9w0BAQQFAAOBgQCuYnv8vBzXEZpgLD71FfeDK2Zqh0FnfTHXAkHrj4JP3MCMF5nKHgOSRV
mImNHHy0cYKTDP+hor68R76XhLVapKMqNuUHUYf7CTB5JNHHy0cYKTNHHy0cYKTuV1Ce8nvvU
G+yp2Eh8aJ7thaua41xDFXPmIEXTqzXi1++DCWAdWaysojPCZugY7jNWXmg==
-----END CERTIFICATE REQUEST-----
```

Important! Be sure to include the first and last lines (-----BEGIN CERT... and -----END CERT...), and copy only the text in the certificate. Do not copy any extra white space.

7 Navigate to the Local Certificate Authority List section.

8 Select a CA and click **Sign Request**.



Sign with Certificate Authority: k450.ca (maximum 3646 days)

Certificate Purpose: ○ Server ● Client ○ Intermediate CA

Certificate Duration (days): 3646

Certificate Request:

```
EwdTYWZlTmVOMRUwEwYDVQQLEwxTYWZlTmVOIFdlc3QxFTATBgNVBAcTDFJlZHdv
b2QgQ2lOeTELMAkGA1UECBMCQOExCzAJBgNVBAYTAlVTMSYwJAYJKoZIhvcNAQkB
FhdzYWZlbmVOQHNhZmVuZXQtaW5jLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAOt58qAAXEj83ebi/pvTNSbvG7ncVMAL/wZzU5yOxA7zlIjH1A8V
mvxa+LztGkn/nzJZu841YOJVR2cRmrVQ1LHX/6KW4ewrpvedjpJAOTrzIPwbDZdo
dlYPR728THUFqwznMI/AtrwZuFZzHEWyfBCrIKuhKU+l43KDP7XUbAfwgDBVHLpO
EkAO2DvF/k4Bj4I92GiMkeB8RXGlKep7GV7UMTcqu/3YldkZVNsPdkrhzX4O/DKn
1nfKMjsm/fcPpLZMgxABPP6e9bGeOVhstZsa3YOs2t8A7KEADuv1yO8x/LhcCPII
hdFygSL2q3qwZnaFHatsYsijAQJOLbSnPZ8CAwEAAaAAMAOGCSqGSIb3DQEBCwUA
A4IBAQBqYvHhnKcT2AK6CDcOzEgSgxerw+v6zmJvmP+NDfI1CAaQkjuzlgWIlJ6M
dOzOvNfyaBViGx1Pz4w/MW9EzMDdGAQI78EOUfgpCbNTjmdL43726UbaAkzBPWO7
ecLFnopvZWlu0884RdmaPwJ4jp5u34uowF2b4e8wi5S87cG+YZFqBT7YiIOgN+je
4VXrM8pvgwEiunZBOQu3idRDYyzsD2k8R6ErMOXn9d1WOSsyylxzbqEyfLFNPRjt
6A5Zwm96UEG92OCsw+t8aAt7cKYR3t7yznvkEODZIKfoxajc4RaeRXeVHu3Sde9h
y4OR+jnLl98ywCBGExBJ6a5Lk9qd
-----END CERTIFICATE REQUEST-----
```

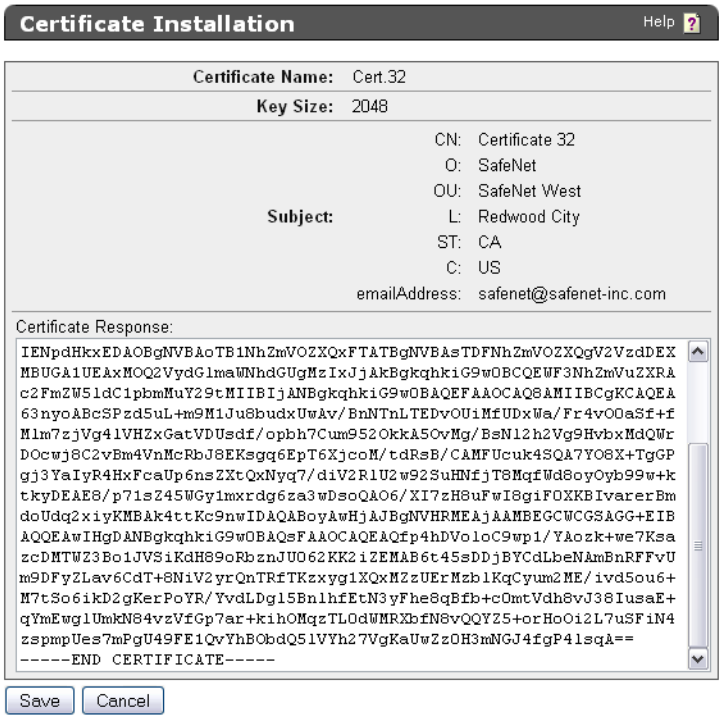
9 Paste the certificate request into the **Certificate Request** field. Select *Client* as the **Certificate Purpose**, specify a **Certificate Duration** and click **Sign Request**. The newly-activated certificate displays on a new page.

10 Copy the certificate text.

11 Navigate back to the Certificate List section.

12 Select the certificate request and click **Properties** to access the Certificate Request Information section.

13 Click **Install Certificate**.



Certificate Name:	Cert.32
Key Size:	2048
Subject:	CN: Certificate 32 O: SafeNet OU: SafeNet West L: Redwood City ST: CA C: US emailAddress: safenet@safenet-inc.com

Certificate Response:

```
IENpdHkxEDAOBgNVBAoTB1NhZmVOZXQxFTATBgNVBAsTDFNhZmVOZXQgV2VzdDEX
MBUGA1UEAxMOQ2VydGlmaWNhdGUgMzIxJjAkBgkqhkiG9w0BCQEWF3NhZmVuZXRA
c2FmZW5ldC1pbmMuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
63nyoABcSPzd5uL+m9M1Ju8budxUwAv/BnNTnLTEDvOUiMfUDxWa/Fr4vO0aSf+f
Mlm7zjVg4lVHZxGatVDUsdf/opbh7Cum952OkkA5OvMg/BsNl2h2Vg9HvbxMdQWr
DOcwj8C2vBm4VnMcRbJ8EKsgq6EpT6XjcoM/tdRsB/CAMFUcuk4SQA7YO8X+TgGP
gj3YaIyR4HxFcaUp6nsZXtQxNyq7/diV2RlU2w92SuHNfjT8MqfWd8oyOyb99w+k
tkyDEAE8/p71sZ45WGy1mxrdg6za3wDsoQAO6/XI7zH8uFwI8giFOXKBIvarerBm
doUdq2xiyKMBAk4ttKc9nwIDAQABoyAwHjAJBgNVHRMEAjAAMBEGCWCGSAGG+EIB
AQQEAwIHgDANBgkqhkiG9w0BAQsFAAOCAQEAQfp4hDVoloC9wp1/YAozk+we7Ksa
zcDMTWZ3Bo1JVSiKdH89oRbznJU062KK2iZEMAB6t45sDDjBYCdLbeNAmBnRFFvU
m9DFyZLav6CdT+8NiV2yrQnTRfTKzxyg1XQxMZzUErMzblKqCyum2ME/ivd5ou6+
M7tSo6ikD2gKerPoYR/YvdLDgl5BnlhfEtN3yFhe8qBfb+cOmtVdh8vJ38IusaE+
qYmEwglUmkN84vzVfGp7ar+kihOMqzTL0dWMRXbfN8vQQYZ5+orHoOi2L7uSFiN4
zspmpUes7mPgU49FE1QvYhBObdQ5lVYh27VgKaUwZzOH3mNGJ4fgP4lsqA==
-----END CERTIFICATE-----
```

14 Paste the text of the signed certificate into the **Certificate Response** field.

15 Click **Save**. When you return to the main Certificate Configuration page, the certificate request is now an active certificate. If the certificate is for a client application, please see the appropriate developer guide for instructions on installing the client certificate.

Installing a Certificate Chain

When CAs sign server certificates with an intermediate CA, it might be necessary for a KeySecure to send multiple certificates to a client 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 on the chain.

Certificate chains can be installed on the KeySecure through the Certificate Installation page.

To install a certificate chain:

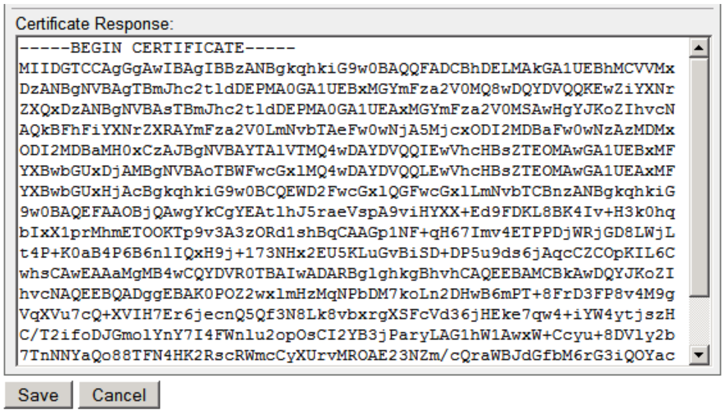
1 Log in to the Management Console as an administrator with Certificates access control.

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

3 Select the certificate and 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, as shown here:



Certificate Response:

```
-----BEGIN CERTIFICATE-----
MIIDGTCCAgGgAwIBAgIBBzANBgkqhkiG9w0BAQQFADCBhDELMAkGA1UEBhMCVVMx
DzANBgNVBAgTBmJhc2tldDEPMA0GA1UEBxMGYmFza2V0MQ8wDQYDVQQKEwZiYXNr
ZXQxDzANBgNVBAsTBmJhc2tldDEPMA0GA1UEAxMGYmFza2V0MSAwHgYJKoZIhvcN
AQkBFhFiYXNrZXRAYmFza2V0LmNvbTAeFw0wNjA5MjcxODI2MDBaFw0wNzAzMDMx
ODI2MDBaMH0xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIEwVhcHBsZTEOMAwGA1UEBxMF
YXBwbGUxDjAMBgNVBAoTBWFwcGxlMQ4wDAYDVQQLEwVhcHBsZTEOMAwGA1UEAxMF
YXBwbGUxHjAcBgkqhkiG9w0BCQEWD2FwcGxlQGFwcGxlLmNvbTCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAtlhJ5raeVspA9viHYXX+Ed9FDKL8BK4Iv+H3k0hq
bIxX1prMhmETOOKTp9v3A3zORd1shBqCAAGp1NF+qH67Imv4ETPPDjWRjGD8LWjL
t4P+K0aB4P6B6nlIQxH9j+173NHx2EU5KLuGvBiSD+DP5u9ds6jAqcCZCOpKIL6C
whsCAwEAAaMgMB4wCQYDVR0TBAIwADARBglghkgBhvhCAQEEBAMCBkAwDQYJKoZI
hvcNAQEEBQADggEBAK0POZ2wxlmHzMqNPbDM7koLn2DHwB6mPT+8FrD3FP8v4M9g
VqXVu7cQ+XVIH7Er6jecnQ5Qf3N8Lk8vbxrgXSFcVd36jHEke7qw4+iYW4ytjszH
C/T2ifoDJGmolYnY7I4FWnlu2opOsCI2YB3jParyLAG1hW1AwxW+Ccyu+8DVly2b
7TnNNYaQo88TFN4HK2RscRWmcCyXUrvMROAE23NZm/cQraWBJdGfbM6rG3iQOYac
```

6 Click **Save**.

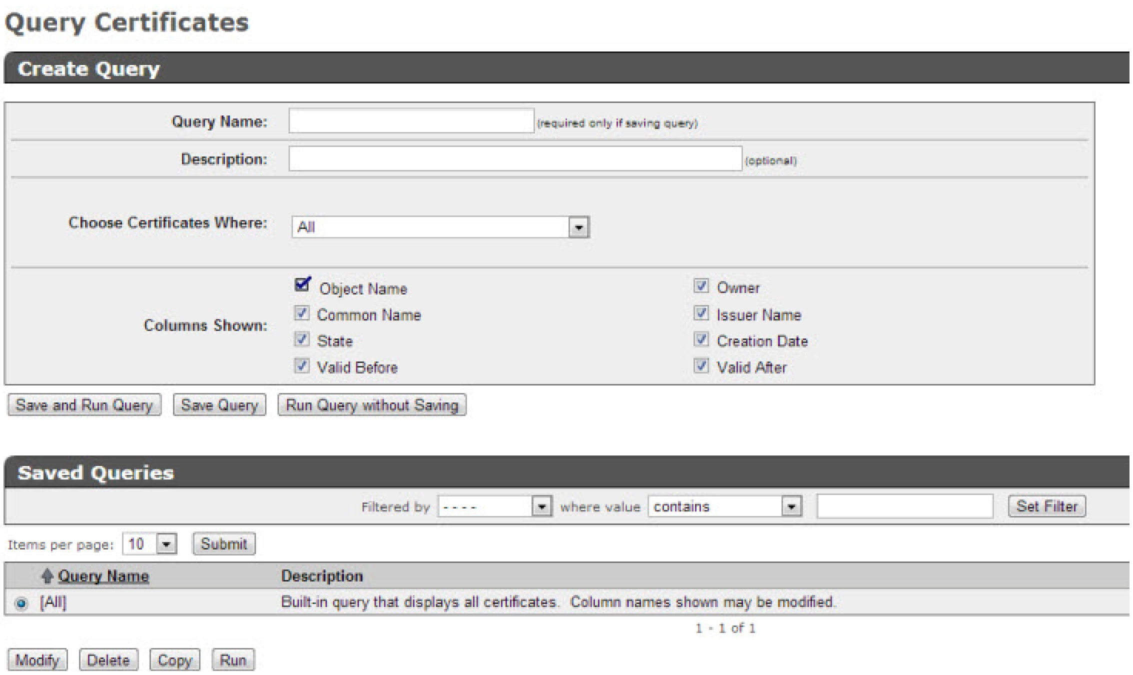
Create a Certificate Query

A certificate query enables you to view a subset of the certificates that exist on the KeySecure. You can create new queries, run saved queries, and modify queries.

To create a query:

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

2 Navigate to the Queries section (Security >> Certificates >> Query Certificates). This section enables you to create very specific queries using multiple and/or statements and using the results of other saved queries. You can also tailor your query to show specific columns.



Query Certificates

Create Query

Query Name:	(required only if saving query)
Description:	(optional)
Choose Certificates Where:	All
Columns Shown:	☑ Object Name ☑ Owner ☑ Common Name ☑ Issuer Name ☑ State ☑ Creation Date ☑ Valid Before ☑ Valid After

Saved Queries

Filtered by - - - - where value contains

Items per page: 10

	Query Name	Description
●	[All]	Built-in query that displays all certificates. Column names shown may be modified.

1 - 1 of 1

3 Enter the **Query Name**. This field is only required if you will save the query. You can run a query without saving, but *you can only save a query before running it*.

4 Enter a **Description** of the query.

5 Use the **Choose Certificates Where** field in combination with the **AND** and **OR** buttons to create your own query. You can query on key metadata, combine query strings, and use the results of previously saved queries.

6 Select the **Columns Shown** in the query results.

7 Select one of the following:

- **Save and Run Query** - save and execute the query.
- **Save Query** - save the query without executing.
- **Run Query without Saving** - execute the query without saving. The results will show the **Query Name** as *Unnamed Query*. You can navigate away from the Keys sections and still reapply the *Unnamed Query*, however, the Management Console will only store one *Unnamed Query* at a time. Old unnamed queries are forgotten.

Saved queries appear in the Saved Queries section. They can be run, copied, deleted, and modified. Click the **Modify** button in the Saved Queries section and then alter the Query Name, **Description**, **Selection Criteria**, and the **Columns Shown** fields.

Note: You cannot greatly modify the built-in query [All]. The KeySecure will only permit you to change the **Columns Shown** values.

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 >> SSL Certificates).

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

4 Click **Download**.

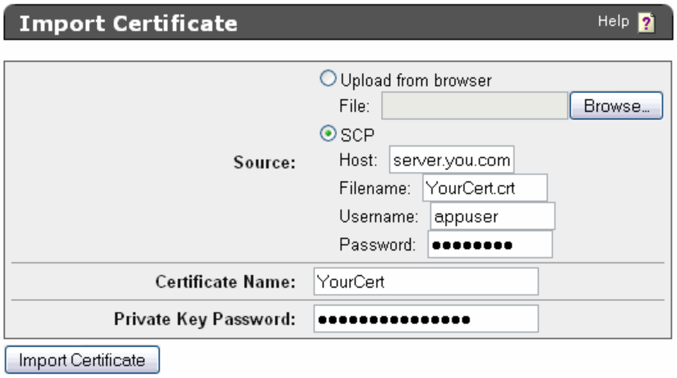
Import a Certificate

The KeySecure can import certificates in PEM-encoded PKCS #12, and PEM-encoded X.509, as long as the private key is included with the certificate.

To import a certificate:

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

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



Import Certificate

Source:
○ Upload from browser
File:
● SCP
Host: server.you.com
Filename: YourCert.crt
Username: appuser
Password: ●●●●●●●●

Certificate Name: YourCert

Private Key Password: ●●●●●●●●●●●●●●●

3 Select the **Source** of the import. You can select one of three options:

- Choose *Upload from browser* to upload the certificate through the browser and click **Browse** to locate the file on the local drive or network.
- Choose *SCP* and enter values for the *Host*, *Filename*, *Username*, and *Password* to copy the file via SCP. *Username* refers to the account on the source host that has access to the file.
- Choose *FTP* and enter values for the *Host*, *Filename*, *Username*, and *Password* to copy the file via SCP. *Username* refers to the account on the source host that has access to the file.

4 Enter the **Certificate Name**.

5 Enter the **Private Key Password**.

6 Select **Import Certificate** to import the certificate to your KeySecure.

Note: You can import certificates with a key size of 2048-bit or smaller.

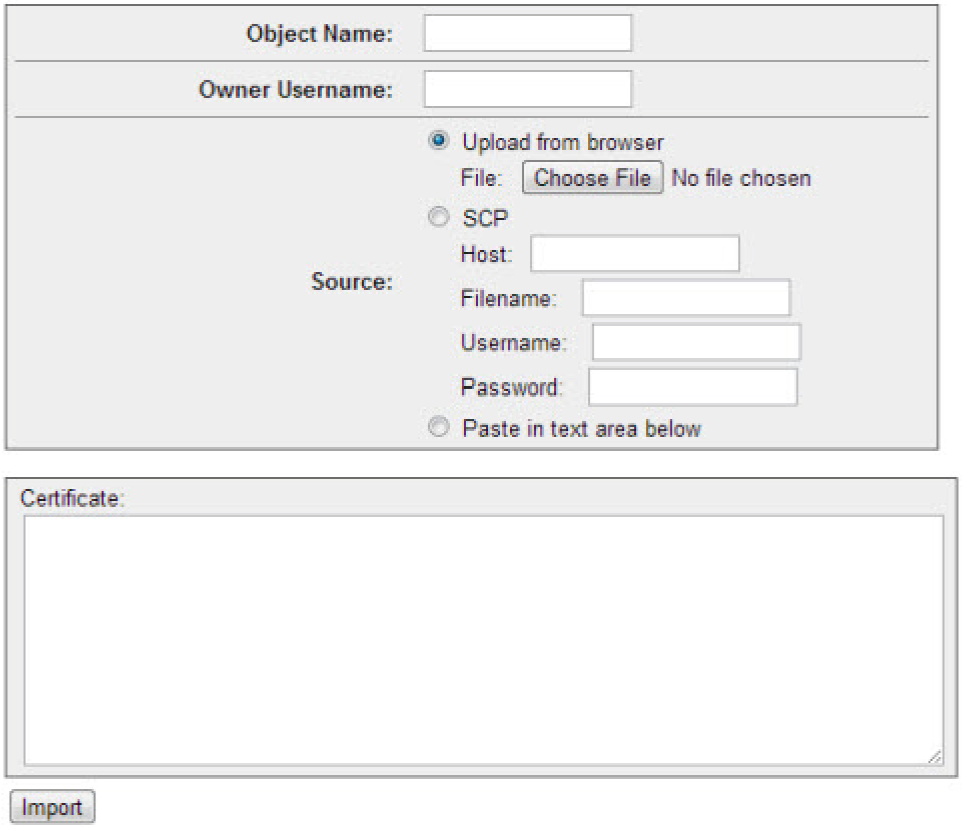
Import a Certificate as a Managed Object

The Import Certificate section allows you to import certificates in PEM-encoded PKCS #7, PEM-encoded PKCS #12, and PEM-encoded X509, as long as the private key is included with the certificate. Certificates imported using this section are managed as keys and can be used for encryption.

To import a certificate as a managed object:

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

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



Object Name:

Owner Username:

Source:

● Upload from browser

File: Choose File No file chosen

○ SCP

Host:

Filename:

Username:

Password:

○ Paste in text area below

Certificate:

3 Enter a unique certificate name in the **Object Name** field. The 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.

4 Enter a value in the **Owner Username** field to assign a specific owner or leave this value blank to create a global key. When you import a key through the management console, the existing key ownership data is not maintained, so any previous ownership must be re-established. If an owner is listed for the key, then that is the only user who can access the key, unless you set group permissions. Global keys can be accessed by all users.

5 Select the **Source** of the certificate import. You can select one of three options:

- Choose *Upload from browser* to upload the certificate through the browser and click **Browse** to locate the file on the local drive or network.
- Choose *SCP* and enter values for the *Host*, *Filename*, *Username*, and *Password* to copy the file via SCP. *Username* refers to the account on the source host that has access to the file.
- Choose *Paste in text area below* and paste the certificate in the **Certificate** field.

6 Click **Import**.

Chapter 34

Certificate Authorities

The KeySecure is capable of functioning as a certificate authority (CA). Local CAs are managed on the Certificate Authority Configuration page and are used to issue certificates to clients that might be making requests to the Key Server. These might include applications and databases. You can also use the Certificate and CA Configuration page to configure the list of Certificate Authorities recognized by the KeySecure.

When the Client Certificate Authentication option is enabled on the Key Server, the KeySecure verifies that the CA that signed the client certificate is in the list of Trusted CAs for the Trusted CA profile specified on the Key Server page.

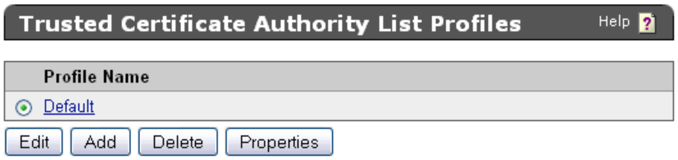
The Default Trusted List CA List profile is empty by default. When you import a CA Certificate onto the KeySecure, it appears in the master list of CA Certificates, but it is not "trusted" until it is added to a Trusted CA list. The same is true for local CAs you generate on the KeySecure. You cannot change the name of the Default profile; however, you can change the list of Trusted CAs for the Default profile.

Manage the Trusted CA List

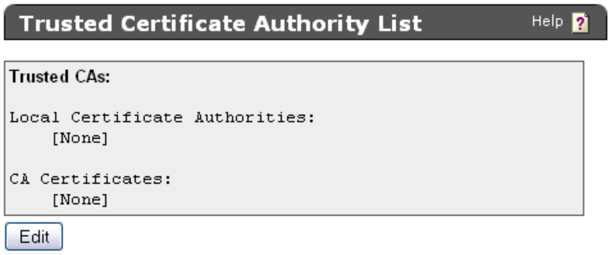
To add or remove a CA certificate to the trusted CA list:

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 click **Properties** to access the Trusted Certificate Authority List section. To create a new CA List profile, click **Add**. Use the **Delete** button to remove unwanted/unused CA List profiles - but note that the Default list cannot be deleted.

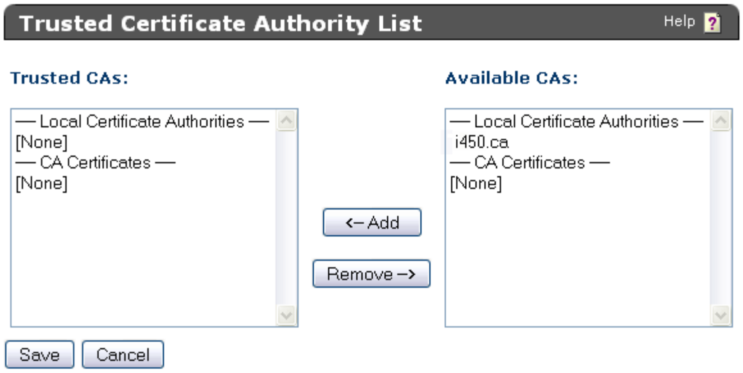


Trusted CAs:

```
Local Certificate Authorities:
    [None]

CA Certificates:
    [None]
```

4 Click **Edit**. The management console displays the **Trusted CAs** and the **Available CAs** and enables you to add **Available CAs** to the trusted list. The list of **Available CAs** includes both local and external CAs.



Trusted Certificate Authority List

Trusted CAs:

— Local Certificate Authorities —
[None]
— CA Certificates —
[None]

Available CAs:

— Local Certificate Authorities —
i450.ca
— CA Certificates —
[None]

5 Use the **Add** and **Remove** buttons as needed.

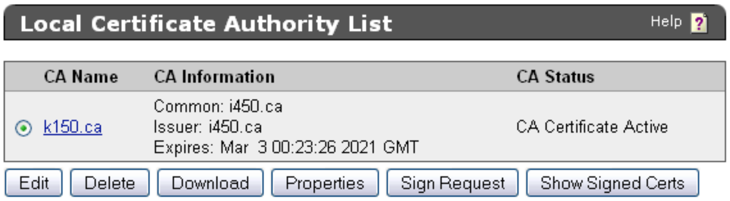
6 Click **Save**.

View and Download 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.

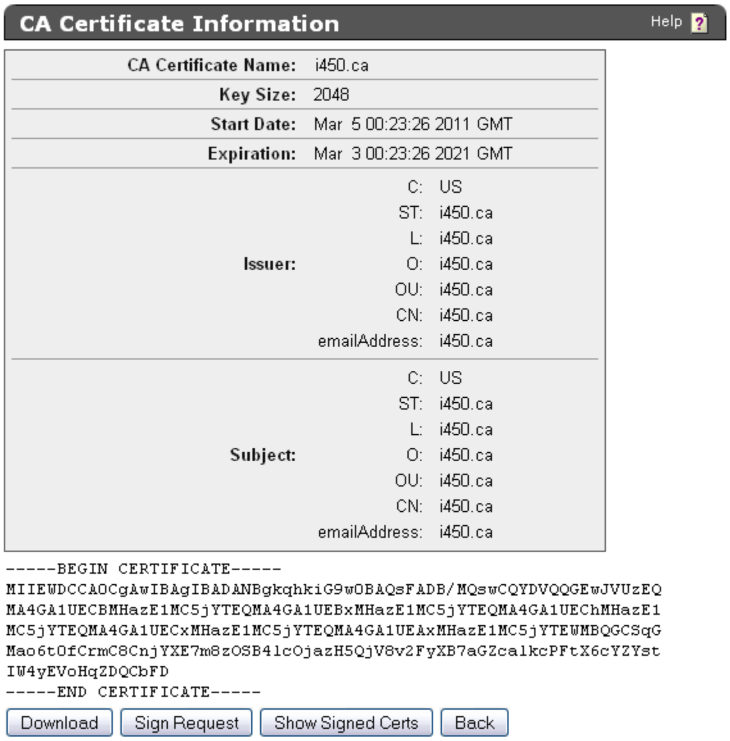
2 Navigate to the Local Certificate Authority List section of the Certificate and CA Configuration page (Security >> Local CAs).



Local Certificate Authority List

	CA Name	CA Information	CA Status
●	k150.ca	Common: i450.ca Issuer: i450.ca Expires: Mar 3 00:23:26 2021 GMT	CA Certificate Active

3 Select a certificate authority and click **Properties** to view information associated with a specific CA Certificate. The top portion of the CA Certificate Information page displays several of the X509 fields in the CA certificate. The lower portion of this page displays the X509 certificate encoded in PEM format. Since this is a CA certificate, the issuer and subject are identical.



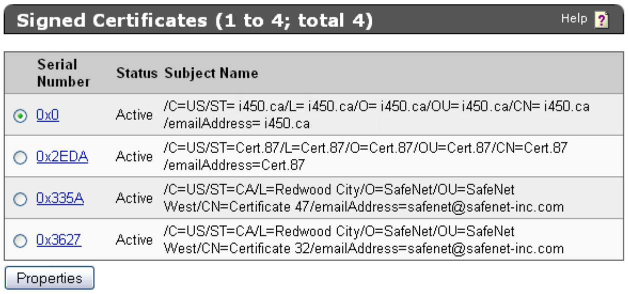
CA Certificate Name:	i450.ca	
Key Size:	2048	
Start Date:	Mar 5 00:23:26 2011 GMT	
Expiration:	Mar 3 00:23:26 2021 GMT	
Issuer:	C:	US
	ST:	i450.ca
	L:	i450.ca
	O:	i450.ca
	OU:	i450.ca
	CN:	i450.ca
	emailAddress:	i450.ca
Subject:	C:	US
	ST:	i450.ca
	L:	i450.ca
	O:	i450.ca
	OU:	i450.ca
	CN:	i450.ca
	emailAddress:	i450.ca

```
-----BEGIN CERTIFICATE-----
MIIEWDCCA0CgAwIBAgIBADANBgkqhkiG9w0BAQsFADB/MQswCQYDVQQGEwJVUzEQ
MA4GA1UECBMHazE1MC5jYTEQMA4GA1UEBxMHazE1MC5jYTEQMA4GA1UEChMHazE1
MC5jYTEQMA4GA1UECxMHazE1MC5jYTEQMA4GA1UEAxMHazE1MC5jYTEWMBQGCSqG
Mao6t0fCrmC8CnjYXE7m8zOSB4lcOjazH5QjV8v2FyXB7aGZcalkcPFtX6cYZYst
IW4yEVoHqZDQCbFD
-----END CERTIFICATE-----
```

4 Select **Download** to download a CA certificate so that you can add it to the trusted CA on a client device. Downloading a CA certificate could be very important when you are attempting to establish SSL connections between the Key Server and client applications. To establish trust between the Key Server and the client application, it might be necessary to install a CA certificate on the client application.

5 Select **Show Signed Certs** to access the Signed Certificates section. The page displays the following information:

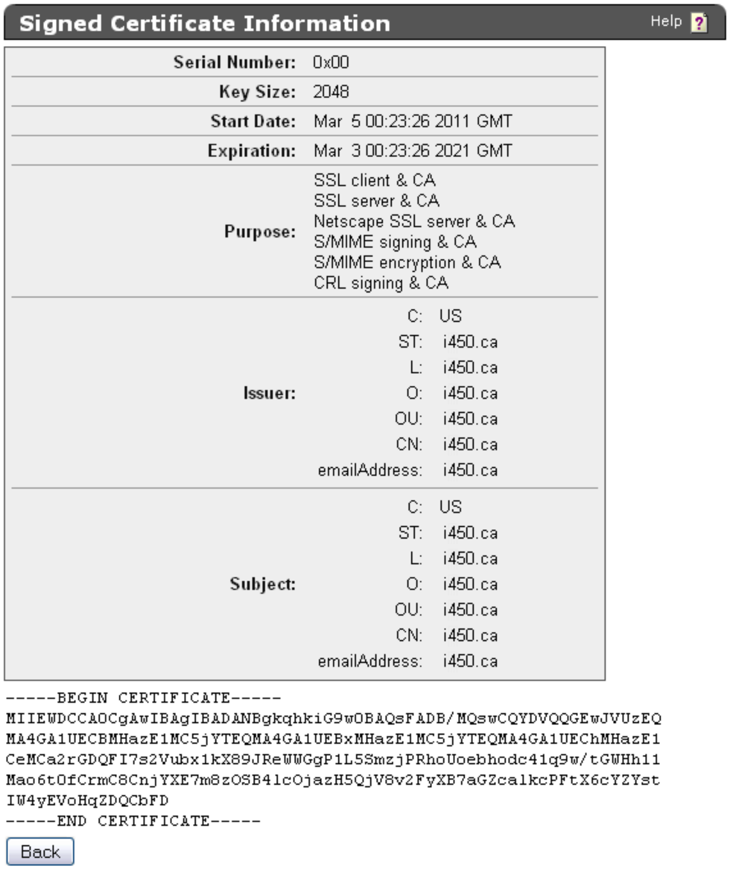
- Serial Number - The Serial Number, expressed in Base 16 notation, is assigned by the KeySecure and used internally to refer to a certificate signed by a local CA. There is only one counter on the KeySecure, which means that all serial numbers for certificates signed by local CAs will be in numerical 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 KeySecure 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.
- Status - status of the certificate.
- Subject Name - the concatenated subject information for the signed certificate.



Signed Certificates (1 to 4; total 4) Help ?

	Serial Number	Status	Subject Name
●	0x0	Active	/C=US/ST= i450.ca/L= i450.ca/O= i450.ca/OU= i450.ca/CN= i450.ca /emailAddress= i450.ca
○	0x2EDA	Active	/C=US/ST=Cert.87/L=Cert.87/O=Cert.87/OU=Cert.87/CN=Cert.87 /emailAddress=Cert.87
○	0x335A	Active	/C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet West/CN=Certificate 47/emailAddress=safenet@safenet-inc.com
○	0x3627	Active	/C=US/ST=CA/L=Redwood City/O=SafeNet/OU=SafeNet West/CN=Certificate 32/emailAddress=safenet@safenet-inc.com

6 Select a certificate and click **Properties** to view the signed certificate. The page displays the serial number, key size, expiration date, issuer, and subject. In addition, the PEM encoded x.509 certificate can be used to install the certificate if necessary. This page is view-only.



Signed Certificate Information Help ?

Serial Number:	0x00
Key Size:	2048
Start Date:	Mar 5 00:23:26 2011 GMT
Expiration:	Mar 3 00:23:26 2021 GMT
Purpose:	SSL client & CA SSL server & CA Netscape SSL server & CA S/MIME signing & CA S/MIME encryption & CA CRL signing & CA
Issuer:	C: US ST: i450.ca L: i450.ca O: i450.ca OU: i450.ca CN: i450.ca emailAddress: i450.ca
Subject:	C: US ST: i450.ca L: i450.ca O: i450.ca OU: i450.ca CN: i450.ca emailAddress: i450.ca

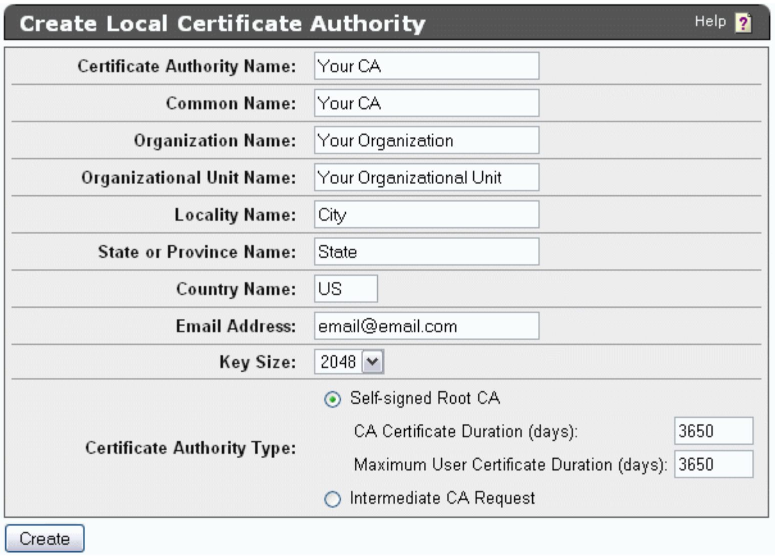
```
-----BEGIN CERTIFICATE-----
MIIEWDCCAOCgAwIBAgIBADANBgkqhkiG9wOBAQsFADB/MQswCQYDVQQGEwJVUzEQ
MA4GA1UECBMHazE1MC5jYTEQMA4GA1UEBxMHazE1MC5jYTEQMA4GA1UEChMHazE1
CeMCa2rGDQFI7s2Vubx1kX89JReWWGgP1L5SmzjPRhoUoebhodc41q9w/tGWHh11
Mao6tOfCrmC8CnjYXE7m8zOSB4lcOjazH5QjV8v2FyXB7aGZcalkcPFtX6cYZYst
IW4yEVoHqZDQCbFD
-----END CERTIFICATE-----
```

Create a Local Certificate Authority

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).



Create Local Certificate Authority

Certificate Authority Name:	Your CA
Common Name:	Your CA
Organization Name:	Your Organization
Organizational Unit Name:	Your Organizational Unit
Locality Name:	City
State or Province Name:	State
Country Name:	US
Email Address:	email@email.com
Key Size:	2048
Certificate Authority Type:	● Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 ○ Intermediate CA Request

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

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

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**. Once you create a self-signed root CA, you must add it to the trusted CA list for it to be recognized by the Key Server.

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 enables you to de-centralize 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.

5 Click **Create**.

Create 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 **Key Size**.
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 a status of *CA Certificate Request Pending.*
6. Navigate to the Local Certificate Authority List section of the Certificate and CA Configuration page (Security >> Local CAs).
7. Select the CA Certificate Request and click **Properties** to access the CA Certificate Information section.
8. Copy the CA certificate request text. The certificate text looks similar, but not identical, to the following text.

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   MIIBmzCCAQQCAQAwWzEPMA0GA1UEAxMGZmxldGNoMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEJM
   AcGA1UEBxMAMQkwBwYDVQQIEwAxCzAJBgNVBAYTAlVTMQ8wDQYJKoZIhvcNAQkBFgAwgZ8wDQ
   YJKoZIhvcAYBABTUxxgY0AMIGJAoGBAMUqA1t4m&Nm0sCcUqnt5Yug+qTSbgEFnvnYWUApHKD
   lx5keC1lguQDU1ol2Xcc3YGrUviGCe4y0JIMK2giQ5b+ABQDemRiD11vInQqkhV6ngWBRD0lp
   KCjU6QXDEE9KGCKBRh5uqL70rr2LErqxUuYwOu50Tfn4T3tKb1HGgfdzAgMBAAGgADANBgkqh
   kiG9w0BAQQFAAOBgQCuYnv8vBzXEZpgLD71FfeDK2Zqh0FnfTHYKTuV1Ce8nvvUG+yp2Eh8aJ
   7thaua41xDFXPmIEXTqzXi1++DCWAdWaysojPCZugY7jNWXmg==
   -----END CERTIFICATE REQUEST-----
   ```

   Important! Be sure to include the first and last lines (-----BEGIN CERT... and -----END CERT...), and copy only the text in the certificate. Do not copy any extra white space.
9. Sign this request with another CA. Copy the signed certificate text.
10. Navigate back to the Local Certificate Authority List section.
11. Select the CA Certificate Request and 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**. When you return to the Local Certificate Authority List section, the CA certificate is now active.

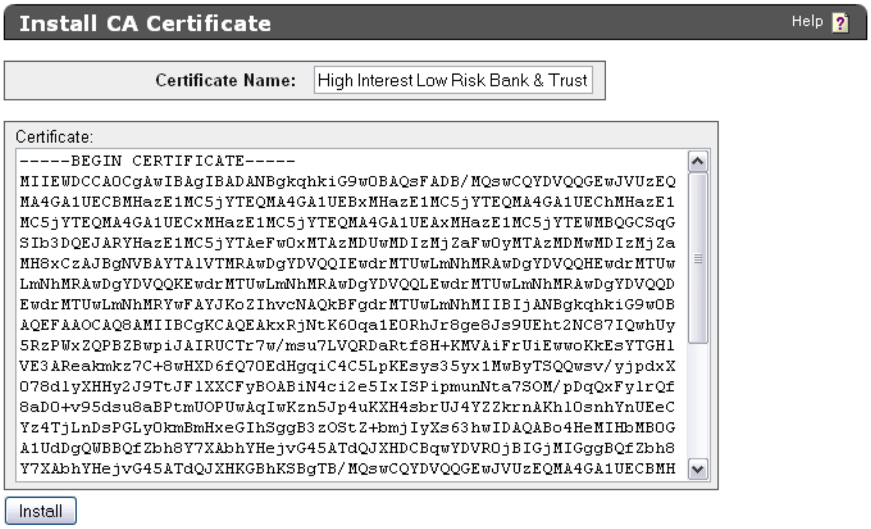
Install a CA Certificate

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

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).



Certificate Name: High Interest Low Risk Bank & Trust

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIEWDCCA0CgAwIBAgIBADANBgkqhkiG9w0BAQsFADB/MQswCQYDVQQGEwJVUzEQ
MA4GA1UECBMHazE1MC5jYTEQMA4GA1UEBxMHazE1MC5jYTEQMA4GA1UEChMHazE1
MC5jYTEQMA4GA1UECxMHazE1MC5jYTEQMA4GA1UEAxMHazE1MC5jYTEWMBQGCSqG
SIb3DQEJARYHazE1MC5jYTAeFw0xMTAzMDUwMDIzMjZaFw0yMTAzMDMwMDIzMjZa
MH8xCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdrMTUwLmNhMRAwDgYDVQQHEwdrMTUw
LmNhMRAwDgYDVQQKEwdrMTUwLmNhMRAwDgYDVQQLEwdrMTUwLmNhMRAwDgYDVQQD
EwdrMTUwLmNhMRYwFAYJKoZIhvcNAQkBFgdrMTUwLmNhMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAkxRjNtK60qa1E0RhJr8ge8Js9UEht2NC87IQwhUy
5RzPWxZQPBZBwpiJAIRUCTr7w/msu7LVQRDaRtf8H+KMVAiFrUiEwwoKkEsYTGHl
VE3AReakmkz7C+8wHXD6fQ70EdHgqiC4C5LpKEsys35yx1MwByTSQQwsv/yjpdxX
078dlyXHHy2J9TtJFlXXCFyBOABiN4ci2e5IxISPipmunNta7SOM/pDqQxFylrQf
8aDO+v95dsu8aBPtmUOPUwAqIwKzn5Jp4uKXH4sbrUJ4YZZkrnAKhl0snhYnUEeC
Yz4TjLnDsPGLy0kmBmHxeGIhSggB3zOStZ+bmjIyXs63hwIDAQABo4HeMIHbMB0G
A1UdDgQWBBQfZbh8Y7XAbhYHejvG45ATdQJXHDCBqwYDVR0jBIGjMIGggBQfZbh8
Y7XAbhYHejvG45ATdQJXHKGBhKSBgTB/MQswCQYDVQQGEwJVUzEQMA4GA1UECBMH
```

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.

Chapter 35

Certificate Revocation Lists

Certificate Authorities 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 KeySecure allows you to obtain, query, and maintain CRLs published by CAs supported on the KeySecure. The KeySecure uses CRLs to verify certificates in two ways.

- Require Client Authentication – when enabled, the KeySecure only accepts connections from clients that present a valid client certificate. As certificates are presented to the KeySecure, they are checked against the CRL published by the CA who issued the certificate.
- Web Administration User Authentication – this option specifies that you must present a valid client certificate to log in to the Management Console. As certificates are presented to the KeySecure, they are checked against the CRL published by the CA who issued the certificate.

You can configure the KeySecure to fetch the CRL at a regular interval. The CRL is transported to the KeySecure via FTP, SCP or HTTP. The KeySecure 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 KeySecure.

The KeySecure validates all CRLs that it downloads. To validate a CRL, the CA that signed the CRL must be in the list of Trusted CAs on the KeySecure. CRLs published by untrusted CAs are rejected by the KeySecure. Once a CRL is installed on the KeySecure, 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 KeySecure, the validation of the CRL fails.

When a certificate on the KeySecure appears on a CRL, the event is logged in System Log. Traps for revoked certificates are sent daily around 5:10 AM local time.

Local CAs

The CRL functionality allows you to revoke and renew certificates that are signed with local CAs. Additionally, you can export a CRL issued by local CAs. CRLs exported from the KeySecure contain a list of certificates revoked by local CAs. The format of CRLs exported by the KeySecure 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 KeySecure inspects the Next Update value for the CRL associated with each CA on the KeySecure. For CRLs whose Next Update time is in the past, the KeySecure 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 KeySecure waits until that specified time to attempt to connect to the CDP and download the updated CRL. For 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 KeySecure. At 5:00 AM on Oct 20, the KeySecure 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 KeySecure continues using the old CRL, and it tries again each day to download the updated CRL at the normal 5:00 AM auto-update 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 in the CLI to set the Next Update value to a time in the distant future.

Note: The Auto-Update feature does not apply to local CAs.

Force Periodic Update

The KeySecure 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 KeySecure 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 KeySecure 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 KeySecure 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 KeySecure 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 it is not, 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.

Note: The Force Periodic Update parameter is not available for local CAs.

Chapter 36

Certificate Management over KMIP

The KeySecure provides additional Certificate Management features using the Key Management Interoperability Protocol (KMIP). These features extend the Certificate Management features that use SafeNet's NAE-XML protocol, allowing clients to manage certificates using a standard protocol.

The following KMIP operations are supported in conjunction with certificates:

- Register
- Get
- Get Attributes
- Add/Modify/Delete Attributes
- Locate

If you use the Management Console for Key management, then Certificate management over KMIP will seem very familiar. The Certificates section (Security » Certificates » Certificate List) provides a similar user interface to import, modify, export and delete Certificates.

There are differences. Certificate Management over KMIP supports the following attributes, which are defined by the KMIP specification:

- Certificate Issuer
- Certificate Type
- Certificate Subject
- Certificate Identifier

The KeySecure contains a separate list of managed certificates called "Certificates." This is placed at the same level as the list of managed objects entitled "Keys."

The features of Certificate Management over KMIP has both similarities and differences when compared to the Certificate Management features over NAE-XML. The differences go beyond just the protocol used to transfer the certificates. The certificates imported over NAE-XML can be used to extract the keys associated with them, and these keys can be used to perform cryptographic operations. In contrast, certificates imported over KMIP are only stored by the server and may not be used to perform cryptographic operations.

At a high level, certificates imported using NAE-XML will work as before, while certificates imported over KMIP function basically as managed objects. Certificates imported over KMIP are not subject to any verification. As a result, certificates that are not trusted or are expired may be imported. These certificates have no connection to the list of Trusted CAs, Known CAs, Local CAs or SSL Certificates, which can be found under "Device CAs & SSL Certificates" section of the Management Console’s Security tab.

As required by KMIP specification, certificates must be expressed as DER-encoded ASN.1 X.509 objects.

Certificate Ownership

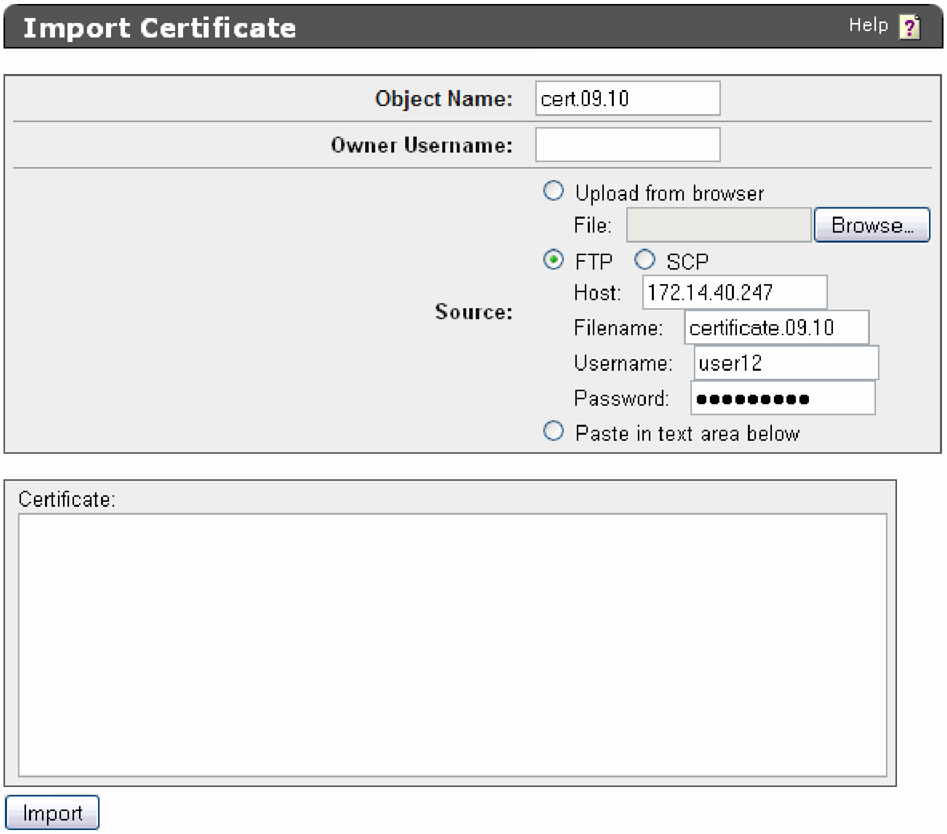
As with the other types of managed objects, Certificate owners are the KeySecure local users that issued an import request (a KMIP Register operation). Unlike key owners, Certificate owner information may not be changed by the server administrator.

Import a Certificate using the Management Console

The Import Certificate section allows you to import certificates in PEM-encoded PKCS #7 and PEM-encoded X509, as long as the private key is included with the certificate. Certificates imported using this section are managed in the same manner as keys and can be used for encryption.

To import a certificate:

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



Import Certificate

Object Name:	cert.09.10
Owner Username:	
Source:	○ Upload from browser File: ● FTP ○ SCP Host: 172.14.40.247 Filename: certificate.09.10 Username: user12 Password: ●●●●●●●●● ○ Paste in text area below

Certificate:

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

3 Enter a unique certificate name in the Name field. The certificate name must begin with a letter, the name must be between 1 and 64 characters (inclusive), and it must consist of letters, numbers, underscores, periods, and hyphens; no spaces or other special characters are allowed.

4 Enter a value in the Owner Username field to assign a specific owner, or leave this value blank to create a global certificate. When you import a certificate through the management console, no ownership data is maintained or created, so ownership must be established as your organization requires it. If an owner is listed for the certificate, then that is the only user who can access the certificate, unless you set group permissions. Global certificate can be accessed by all users.

5 Select the Source of the certificate import. You can select one of three options:

- Choose Upload from browser to upload the certificate through the browser and click Browse to locate the file on the local drive or network.
- Choose SCP and enter values for the Host, Filename, Username, and Password to copy the file via SCP. Username refers to the account on the source host that has access to the file.
- Choose Paste in text area below and paste the certificate in the Certificate field.

6 Click Import.

- To see the attributes of a certificate, click on the object name, or click the Properties button.The Certificate Properties are displayed in a new page. This enables an Administrator to inspect the attributes of a certificate. For example, you can see issued the certificate, check the validity or expiration date of the certificate, discover the subject name of this certificate or see who this certificate is issued to.

To set or Modify Attributes of a Certificate

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

2 Select the Certificate, then navigate to the Certificate's Properties. Click on the Certificate (object) name, or select the object and click the Properties button.

3 When the Managed Object Properties page appears (Security >> Certificates >> Properties), select the Attributes tab. The Attributes tab allows you to save information of three types: **Application Specific Information**, **Object Links**, and **Custom Attributes**. You can apply standard filtering functionality to find and list information of each type.

4 At the bottom of the Application Specific Information section, click **Add** to identify an Application Namespace and Application data to associate with the Certificate.

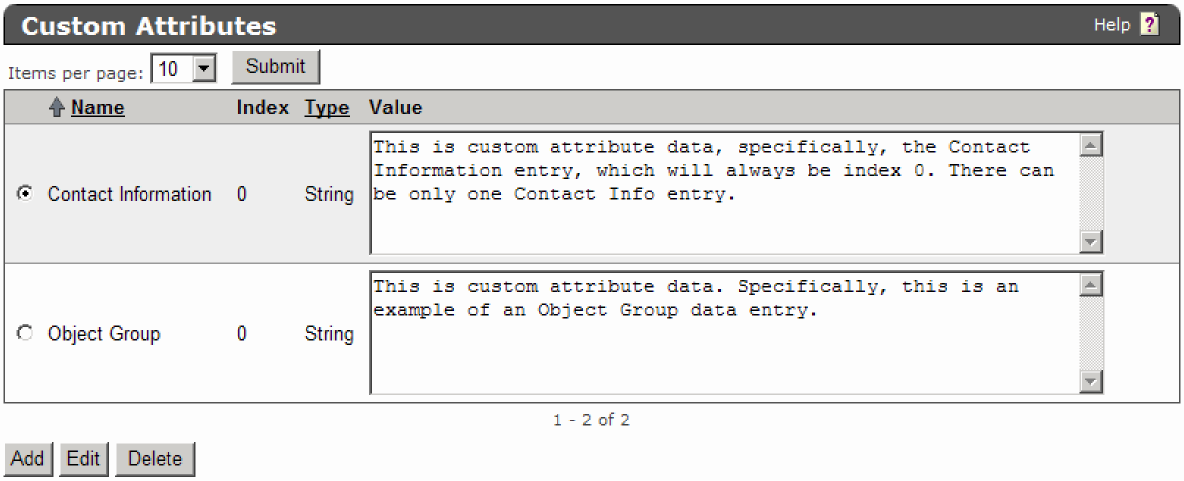
5 At the bottom of the Object Links section, click **Add** to identify an Object Name and Link Type to associate with the Certificate. Click Save when finished.

6 At the bottom of the Custom Attributes section, click **Add** to provide Custom Attributes information for the Certificate.

- You can assign a maximum of 100 custom attributes. There are two types of custom attributes: Contact Information and Object Group. Only one instance of Contact Information is allowed per key. Each attribute is given an Index. The Index is per attribute, per key. The first instance of an attribute is given Index 0. The second instance is given Index 1, and so on. Thus, since there can only be one instance of Contact Information, it will always be Index 0.

7 Enter a **Value**. This can be any printable ASCII characters and spaces, tab, \n and \r. Maximum length is 4096 characters.

8 Click **Save**.



Custom Attributes

Items per page: 10

	Name	Index	Type	Value
●	Contact Information	0	String	This is custom attribute data, specifically, the Contact Information entry, which will always be index 0. There can be only one Contact Info entry.
○	Object Group	0	String	This is custom attribute data. Specifically, this is an example of an Object Group data entry.

1 - 2 of 2

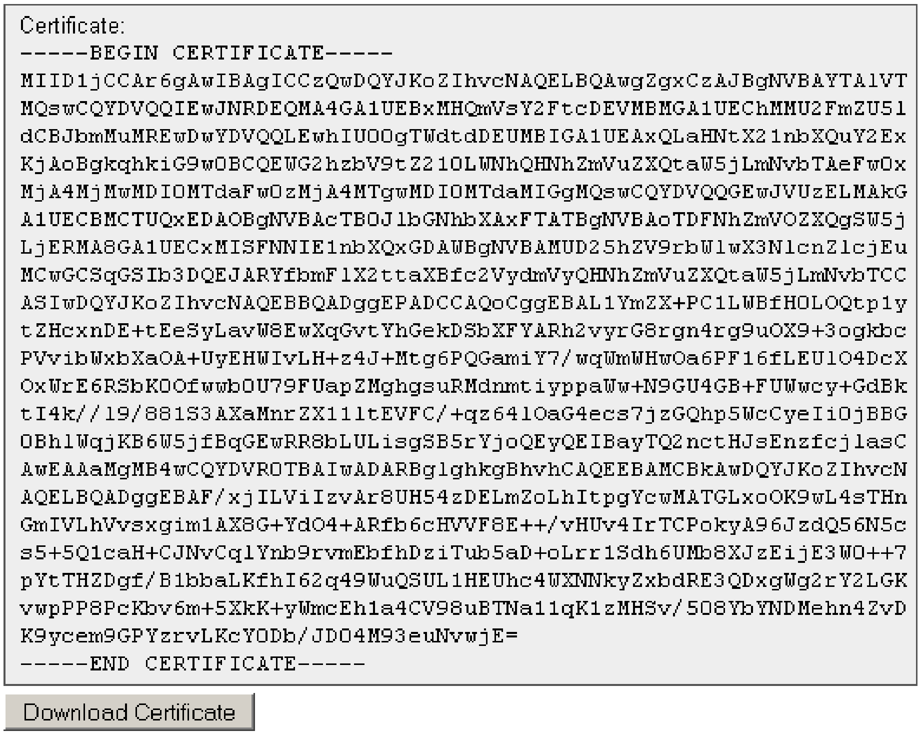
Download a Certificate

To download a Certificate

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

2 Select the Certificate, then navigate to the certificate's Properties. Click on the object name, or select the object and click the Properties button.

3 In the Certificate Properties tab, navigate to bottom of the Certificates section (Security >> Certificates >> Properties).



Certificate:

```
-----BEGIN CERTIFICATE-----
MIID1jCCAr6gAwIBAgICCzQwDQYJKoZIhvcNAQELBQAwgZgxCzAJBgNVBAYTAlVT
MQswCQYDVQQIEwJNRDEQMA4GA1UEBxMHQmVsY2FtcDEVMBMGA1UEChMMU2FmZU5l
dCBJbmMuMREwDwYDVQQLEwhIU00gTWdtdDEUMBIGA1UEAxQLaHNtX21nbXQuY2Ex
KjAoBgkqhkiG9w0BCQEWG2hzbV9tZ210LWNhQHNhZmVuZXQtaW5jLmNvbTAeFw0x
MjA4MjMwMDI0MTdaFw0zMjA4MTgwMDI0MTdaMIGgMQswCQYDVQQGEwJVUzELMAkG
A1UECBMCTUQxEDAOBgNVBAcTB0JlbGNhbXAxFTATBgNVBAoTDFNhZmVOZXQgSW5j
LjERMA8GA1UECxMISFNNIE1nbXQxGDAWBgNVBAMUD25hZV9rbWlwX3NlcnZlcjEu
MCwGCSqGSIb3DQEJARYfbmFlX2ttaXBfc2VydmVyQHNhZmVuZXQtaW5jLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL1YmZX+PC1LWBfHOLOQtp1y
tZHcxnDE+tEeSyLavW8EwXqGvtYhGekDSbXFYARh2vyrG8rgn4rg9uOX9+3ogkbc
PVvibWxbXaOA+UyEHWIvLH+z4J+Mtg6PQGamiY7/wqWmWHwOa6PF16fLEUlO4DcX
OxWrE6RSbKOOfwwbOU79FUapZMghgsuRMdnmtiyppaWw+N9GU4GB+FUWwcy+GdBk
tI4k//l9/881S3AXaMnrZX11ltEVFC/+qz64lOaG4ecs7jzGQhp5WcCyeIi0jBBG
OBhlWqjKB6W5jfBqGEwRR8bLULisgSB5rYjoQEyQEIBayTQ2nctHJsEnzfcjlasC
AwEAAaMgMB4wCQYDVR0TBAIwADARBglghkgBhvhCAQEEBAMCBkAwDQYJKoZIhvcN
AQELBQADggEBAF/xjILViIzvAr8UH54zDELmZoLhItpgYcwMATGLxoOK9wL4sTHn
GmIVLhVvsxgim1AX8G+YdO4+ARfb6cHVVF8E++/vHUv4IrTCPokyA96JzdQ56N5c
s5+5Q1caH+CJNvCqlYnb9rvmEbfhDziTub5aD+oLrr1Sdh6UMb8XJzEijE3WO++7
pYtTHZDgf/B1bbaLKfhI62q49WuQSUL1HEUhc4WXNNkyZxbdRE3QDxgWg2rY2LGK
vwpPP8PcKbv6m+5XkK+yWmcEh1a4CV98uBTNa11qK1zMHSv/508YbYNDMehn4ZvD
K9ycem9GPYzrvLKcYODb/JD04M93euNvwjE=
-----END CERTIFICATE-----
```

4 Click Download to download the Certificate.

Delete a Certificate

WARNING! Exercise caution when deleting a certificate. If you erroneously delete a certificate, all operations that depend on that certificate will fail. Unless you recover, using a backup of that certificate, you will not be able to complete the cryptographic tasks that it supported.

To delete a certificate:

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

2 Navigate to the Certificates section of the Certificate Configuration page (Security >> Certificates).

3 Select the certificate and click Delete.

Delete Multiple Certificates

WARNING! Exercise extreme caution when deleting Certificates. If you erroneously delete a certificate, all operations that depend on that certificate will fail. Unless you recover, using a backup of that certificate, you will not be able to complete the cryptographic tasks that it supported. Creating a backup is highly recommended.

To delete multiple certificates:

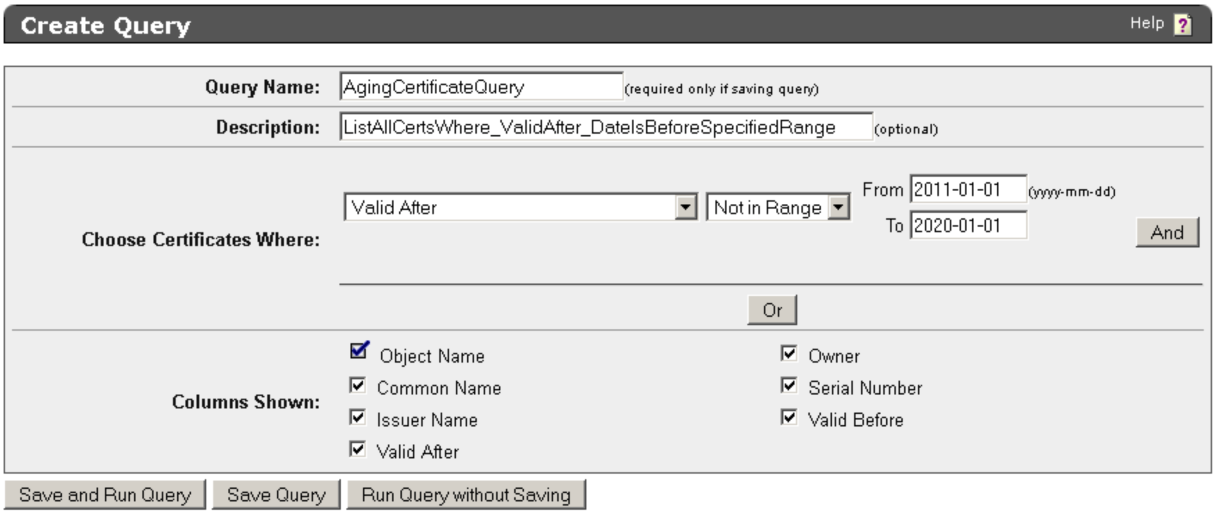
1. Log in to the Management Console as an administrator with Certificates Configuration access control.
2. Navigate to the Certificates section of the Certificates Configuration page (Security >> Certificates).
3. Change the "Items per page" setting to a number greater than the number of certificates you would like to delete, but not more than 50.
   - The Delete Multiple Certificates function currently supports the deletion of up to 50 certificates at once. Larger numbers must be deleted in batches.
   - Run queries as necessary to list in the current page the certificates you need to delete. Only the certificates displayed on the current page will be deleted. When you list more certificates on a page than you can see on your screen, be sure to scroll through and check all certificates.
4. Click **Delete All Certificates On Current Page** to delete all certificates currently rendered on the page.

Create a Certificate Query

A certificate query enables you to view a subset of the certificates that exist on the KeySecure. You can create new queries, run saved queries, and modify queries.

To create a query:

1. Log in to the Management Console as an administrator with Certificates Configuration access control.
2. Navigate to the Query Certificates section of the Certificates Configuration page (Security >> Certificates >> Query Certificates). This section enables you to create very specific queries using multiple and/or statements and using the results of other saved queries. You can also tailor your query to show specific columns.



Create Query

Help ?

Query Name: AgingCertificateQuery (required only if saving query)

Description: ListAllCertsWhere_ValidAfter_DateIsBeforeSpecifiedRange (optional)

Choose Certificates Where: Valid After | Not in Range | From 2011-01-01 (yyyy-mm-dd) To 2020-01-01 | And

Or

Columns Shown:

- ☑ Object Name
- ☑ Common Name
- ☑ Issuer Name
- ☑ Valid After
- ☑ Owner
- ☑ Serial Number
- ☑ Valid Before

Save and Run Query | Save Query | Run Query without Saving

3 Enter the **Query Name**. This field is only required if you will save the query. You can run a query without saving, but you can only save a query before running it.

4 Enter a **Description** of the query.

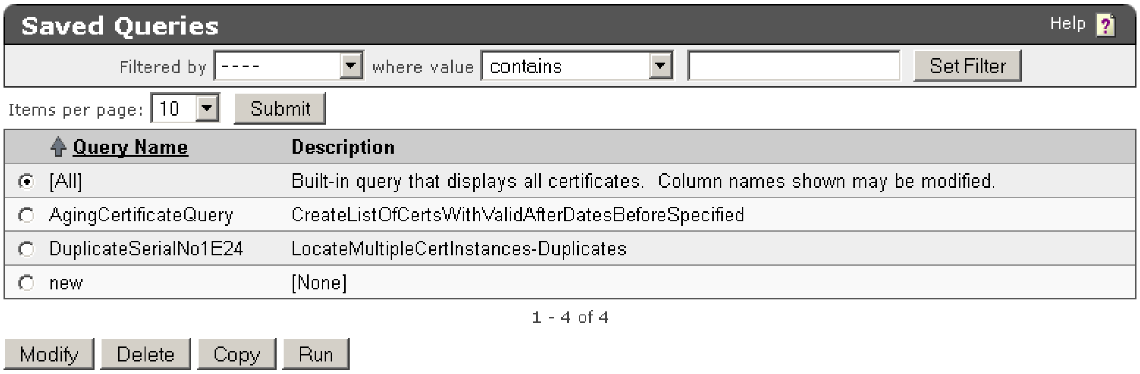
5 Use the **Choose Certificates Where** field in combination with the AND and OR buttons to create your own query. You can query on certificate metadata, combine query strings, and use the results of previously saved queries.

6 Select the **Columns Shown** in the query results.

7 Select one of the following:

- **Save and Run Query** - save and execute the query.
- **Save Query** - save the query without executing.
- **Run Query without Saving** - execute the query without saving. The results will show the Query Name as Unnamed Query. You can navigate away from the Certificates sections and still reapply the Unnamed Query, however, the Management Console will only store one Unnamed Query at a time. Old unnamed queries are forgotten.

Saved queries appear in the Saved Queries section. They can be run, copied, deleted, and modified. Click the Modify button in the Saved Queries section and then alter the Query Name, Description, Selection Criteria, and the Columns Shown fields.



Saved Queries
Help ?
Filtered by ---- ▼ where value contains ▼ Set Filter
Items per page: 10 ▼ Submit

	Query Name	Description
●	[All]	Built-in query that displays all certificates. Column names shown may be modified.
○	AgingCertificateQuery	CreateListOfCertsWithValidAfterDatesBeforeSpecified
○	DuplicateSerialNo1E24	LocateMultipleCertInstances-Duplicates
○	new	[None]

1 - 4 of 4

Note: You cannot greatly modify the built-in query [All]. The KeySecure will only permit you to change the **Columns Shown** values.

Chapter 37

High Security Features

Use the High Security settings on the KeySecure to set the highest level of security for administrative and cryptographic operations on the device. Depending on the KeySecure in use, the advanced security settings may be configurable to comply with the Federal Information Processing Standard (FIPS) 140-2, Level 3 cryptography requirements and/or international Common Criteria (CC) standards. If you use a non-FIPS compliant KeySecure, you can still use high security settings.

The following models are capable of operating in accordance with FIPS and Common Criteria standards:

- KeySecure k450
- KeySecure k460

Note: You also have the option to configure the KeySecure for Korean Crypto Module Validation Program (KCMVP) compliance.To support KCMVP compliance, the KeySecure offers a Korean Algorithm feature that embeds the Korea Library (KLIB) crypto module in the KeySecure. Be aware that the Korean Algorithm feature set is not supported unless a customer specifically requests the KLIB and KCMVP configuration. You may detect references to this configuration, its features and capabilities in some versions of the KeySecure Management Console, but the titles and controls will be grayed out and non-functional.

Advanced Security Access Control

Altering the security settings on the High Security Configuration page can have a profound effect on the security of your SafeNet platform *and* alter your compliance with FIPS and Common Criteria standards. For this reason, administrators must have the Advanced Security Access Control to modify these settings.

FIPS Compliance

FIPS standards describe hardware and software parameters that must be met for full compliance. SafeNet provides both FIPS compliant hardware and software security settings that enable specified KeySecures to operate in compliance with FIPS 140-2, Level 2 certification.

The K-6 HSM card (the cryptographic module) that is included with the KeySecure appliance in this release provides key vaulting capabilities that meet FIPS 140-2 Level 3 requirements.

Be aware that certification of an implementation of a software release can differ from the certification level associated with the embedded cryptographic module.

For more information on FIPS certification of the Luna cryptographic module, see Item#1694 at NIST web site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm

KeySecure Settings Required for FIPS Compliance

In order to apply for FIPS 140-2 certification, the following functionality must be *disabled* on the KeySecure:

- Global Keys
- Administrative options on XML interface
- FTP transport for importing certificates and downloading and restoring backup files
- LDAP authentication
- LDAP administrator server
- Use of the following algorithms: SEED/ARIA, RC4, DES, RSA-512, RSA-768. These algorithms are not available when FIPS compliance is enabled.
- SSL 2.0 and SSL 3.0*
- Hot-swappable drive capability
- RSA encrypt/decrypt operations**

* We recommend running TLS over the XML interface. This requires that you generate a certificate and enable it.

**RSA encrypt/decrypt associated with TLS handshakes and Sign and Sign Verify are permitted.

These settings are adjusted automatically when you use the Management Console's High Security Configuration page to enable FIPS compliance on FIPS capable KeySecures.

WARNING! Logging in and changing passwords through the serial console while not physically present will take the device out of FIPS compliance.

Clustering

Clustering FIPS-compliant devices with non-FIPS compliant devices will disable FIPS certification for all devices in the cluster. For example, clustering a hypothetical FIPS-compliant k460 with a non-FIPS capable k150 would take that k460 out of FIPS compliance. It also means that clustering one or more such FIPS-compliant k460s with even one non-FIPS device would, technically, render the entire cluster non-compliant.

FIPS-capable and non-FIPS-capable KeySecures should not be clustered together.

WARNING! In a FIPS-compliant cluster, taking one device out of FIPS compliance will disable FIPS for the entire cluster.

Backups

FIPS and non-FIPS devices cannot share backups.

FIPS Self-Test

To run a FIPS self-test on the KeySecure, powercycle the device.

Software Patches and Upgrades

SafeNet, Inc. will indicate which software patches and upgrades are FIPS certified. Apply only FIPS certified software to a FIPS compliant device. Doing otherwise takes the device out of FIPS compliance.

Enabling and Disabling FIPS Compliance

According to FIPS requirements, you cannot enable or disable FIPS when there are keys on the KeySecure. You must *manually* delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion. *We strongly recommend that you back up your keys before deleting.*

Common Criteria Compliance

The FIPS configuration settings are a subset of the Common Criteria evaluated configuration settings. Following the FIPS guidelines also makes the KeySecure compliant with Common Criteria standards. As with FIPS, Common Criteria standards also depend on specific hardware requirements met only with the FIPS compliant KeySecures mentioned above.

To meet the requirements for Common Criteria operations, follow the preceding guidelines outlined in this chapter for FIPS 140-2 Level 2. You may run SEED and RC-4 in a Common Criteria configuration by clearing the **Disable Non-FIPS Algorithms and Key Sizes checkbox**.

Note: Support for the SEED algorithm is available only on non–FIPS-compliant KeySecures, and must be feature-activated.

Important! When the **Disable Non-FIPS Algorithms and Key Sizes** checkbox is cleared, the DES, RSA-512, and RSA-768 algorithms can be used on the KeySecure. Note, however that these algorithms are not allowed under the International Common Criteria standards; *using them will take the device out of Common Criteria compliance.*

In addition, you must run TLS over the XML interface. You must generate a certificate and then activate TLS.

Configuring the KeySecure for FIPS Compliance

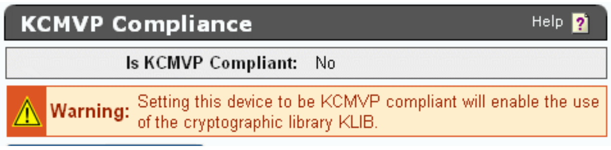
Note: Only devices explicitly identified by SafeNet as configurable for FIPS compliance can be made to comply with FIPS standards. You cannot enable FIPS compliance on other SafeNet devices. You can enact some of the same policies required by the FIPS standards, but the device will not be officially compliant.

To configure the KeySecure for FIPS compliance:

1 View the Security Protocols enabled on your Internet Browser. You must enable TLS 1.0 to access the Management Console while FIPS compliant.

2 Log in to the Management Console as an administrator with SSL, Advanced Security, and Key Server access controls.

3 Navigate to the High Security Configuration page (Security >> High Security).



KCMVP Compliance

Is KCMVP Compliant: No

Warning: Setting this device to be KCMVP compliant will enable the use of the cryptographic library KLIB.

4 Confirm that the **Is FIPS Compliant** value is “No” in the FIPS Compliance section. This field indicates if the KeySecure security configuration is consistent with FIPS requirements.

Note: If the **Is FIPS Compliant** value is “Yes,” then the device is currently FIPS compliant, settings should not be modified, and the **Set FIPS Compliant** button is not available.

5 Click **Set FIPS Compliant** in the FIPS Compliance section. This will alter the settings shown in the High Security Settings and Security Settings Configured Elsewhere sections and enable FIPS compliance. The management console automatically adjusts the settings to comply with FIPS standards.

WARNING: Modifying any of the settings in the High Security Settings and Security Settings Configured Elsewhere sections will take this device out of FIPS compliance.

WARNING: According to FIPS requirements, you cannot enable or disable FIPS when there are keys on the KeySecure. You must manually delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion. We strongly recommend that you back up your keys before deleting.

6 Review the settings in the High Security Settings and Security Settings Configured Elsewhere sections to confirm all settings have been adjusted for FIPS compliance.

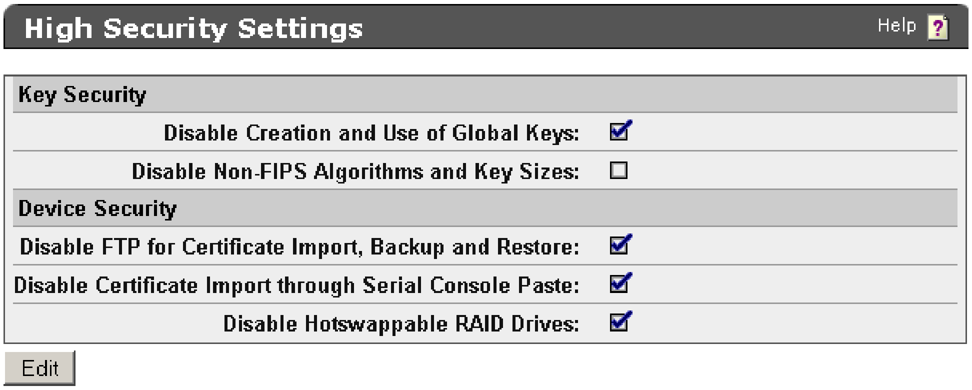
Configuring the High Security Settings on a KeySecure

WARNING! When you enable FIPS compliance on the KeySecure, the functionality displayed here is disabled. Modifying *any* of the items in the High Security Settings section immediately takes the device 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 device is FIPS compliant, you should not alter these settings.

To configure the High Security settings on a non-FIPS compliant KeySecure:

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

2 Navigate to the High Security Configuration page (Security >> High Security). This section lists the functionality that must be disabled for FIPS compliance. These sections are automatically configured when you select **Set FIPS Compliance** in the FIPS Compliance section.



High Security Settings

Key Security

Disable Creation and Use of Global Keys:	☑
Disable Non-FIPS Algorithms and Key Sizes:	☐

Device Security

Disable FTP for Certificate Import, Backup and Restore:	☑
Disable Certificate Import through Serial Console Paste:	☑
Disable Hotswappable RAID Drives:	☑

3 Alter the fields in the High Security Settings section as needed.

WARNING: When you enable FIPS compliance on the KeySecure, the functionality displayed here is disabled. **Modifying *any* of the items in the High Security Settings section immediately takes the device 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 device is FIPS compliant, you should not alter these settings.

Important! According to FIPS requirements, you cannot enable or disable FIPS when there are keys on the KeySecure. You must *manually* delete all keys before enabling and disabling FIPS compliance. Keys are zeroized upon deletion. *We strongly recommend that you back up your keys before deleting.*

- **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 KeySecure. Any existing global keys will not be usable by the KeySecure for any purpose. While the device is FIPS compliance, you may assign an owner to an existing global key.
- **Disable Non-FIPS Algorithms and Key Sizes** - Prevents the creation or use of algorithms and key sizes that are not FIPS compliant. The following algorithm and key size combinations will be disallowed. Any existing keys and certificates based on these algorithms and key sizes will not be usable by the KeySecure for any purpose.
  - SEED (this is feature-activated and may not appear on most devices)
  - RC4
  - DES
  - RSA-512, RSA-768 (If your server currently uses a 768-bit certificate, this option cannot be selected. You must select, and possibly create, a different server certificate. Clients with 512 or 768 bit certificates will be rejected when they try to connect to a FIPS compliant device.)

The following algorithms and keys sizes *will* continue to be available on the KeySecure:

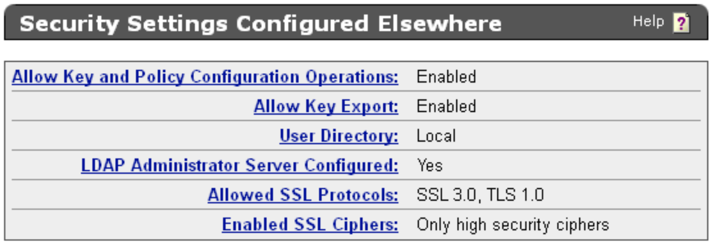
- AES-128, AES-192, AES-256
- DES-EDE-112, DES-EDE-168
- HmacSHA1, HmacSHA256, HmacSHA384, HmacSHA512
- RSA-1024, RSA-2048, RSA-3072, RSA-4096

- **Disable RSA Encryption and Decryption** - As of Release 6.2, KeySecure no longer provides the Disable RSA Encryption and Decryption option. Retiring this option was necessary to allow clients to perform key wrapping and unwrapping (encryption and decryption) using RSA keys. Disabling RSA encryption and decryption altogether was too broad in its effect. To maintain FIPS compliance going forward, do not use RSA encryption and decryption on user data (credit cards, social security numbers, medical records, etc.)
- **Disable FTP for Certificate Import, Backup and Restore** - Disables the use of FTP for importing certificates, downloading backup files, and restoring backup files. Administrators can still download and upload through the browser and via SCP.
- **Disable Certificate Import through Serial Console Paste** - Prevents administrators from importing certificates through the serial console using cut and paste.
- **Disabled Hotswappable RAID Drives** - Prevents administrators from changing RAID drives through the management console. This option will appear on RAID capable devices only.

WARNING: You cannot replace RAID drives and remain FIPS compliant. To change RAID drives you must either disable FIPS or return the device for drive replacement.

4 Click Exit.

5 Navigate to the Security Settings Configured Elsewhere section (located below High Security Settings).



Allow Key and Policy Configuration Operations:	Enabled
Allow Key Export:	Enabled
User Directory:	Local
LDAP Administrator Server Configured:	Yes
Allowed SSL Protocols:	SSL 3.0, TLS 1.0
Enabled SSL Ciphers:	Only high security ciphers

6 Review the settings. To alter these settings, click the fields to access the appropriate sections.

WARNING: Modifying *any* of the items in the Security Settings Configured Elsewhere section immediately takes the KeySecure out of FIPS compliance.

- Allow Key and Policy Configuration Operations - Displays the value of the **Allow Key and Policy Configuration Operations** field in the Key Server Settings section. When enabled, users can configure keys and authorization policies through the XML Interface. Click the link to access the Key Server Settings section. For FIPS compliance, this functionality must be disabled.
- Allow Key Export - Displays the value of the **Allow Key Export** field in the Key Server Settings section. When enabled, users can export keys from the KeySecure through the XML Interface. Click the link to access the Key Server Settings section. For FIPS compliance, this functionality must be disabled, or SSL must be enabled.
- User Directory - Displays the value of the **User Directory** field in the Key Server Authentication Settings section, which determines whether the Key Server uses a local directory or an LDAP server. Click the link to access the Key Server Authentication Settings section. For FIPS compliance, a local user directory must be used.

- Allowed SSL Protocols - Displays the SSL Protocols enabled in the SSL Options section. Click the link to access the SSL Options section. FIPS compliance requires that SSL 2.0 and SSL 3.0 be disabled.
- Enabled SSL Ciphers - Indicates the security strength of the SSL ciphers enabled in the SSL Cipher Order section. Click the link to access the SSL Cipher Order section. On FIPS capable devices, this field indicates if the enabled SSL ciphers permit FIPS compliance and, if not, what is preventing compliance. For FIPS compliance, you must disable ciphers with key sizes smaller than 128-bits and all RC4 ciphers.

Configuring the KeySecure for Common Criteria Compliance

Note: The KeySecure devices can be configured to comply with Common Criteria standards. You cannot enable Common Criteria compliance on other devices. You can enact some of the same policies required by the Common Criteria standards, but the device will not be officially compliant.

To configure the KeySecure for Common Criteria standards:

1 View the Security Protocols enabled on your Internet Browser. You must enable TLS 1.0 to access the Management Console while FIPS compliant.

2 Log in to the Management Console as an administrator with SSL, Advanced Security, and Key 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 the FIPS Compliance section.

   Note: If the **Is FIPS Compliant** value is “Yes,” the device is currently FIPS compliant and settings should not be modified.

5 Click **Set FIPS Compliant** in the FIPS Compliance section.

6 Review the settings in the High Security Settings and Security Settings Configured Elsewhere sections to confirm all settings have been adjusted for FIPS compliance.

This puts the KeySecure in compliance with Common Criteria standards. However, you can also enable the SEED and RC-4 algorithms and still be compliant with Common Criteria standards.

To enable the SEED and RC-4 algorithms and still be compliant with Common Criteria standards:

1 Follow the steps outlined in “Configuring the KeySecure for FIPS Compliance” on page 221.

2 On the High Security Configuration page, High Security Settings section, click **Edit**.

3 Clear the **Disable Non-FIPS Algorithms and Key Sizes** checkbox.

You can now enable SEED and RC-4 algorithms on the device. When the **Disable Non-FIPS Algorithms and Key Sizes** checkbox is cleared, RC-4 is automatically enabled. The SEED algorithm is feature enabled and requires a license to activate.

Important! When the **Disable Non-FIPS Algorithms and Key Sizes** checkbox is cleared, the DES, RSA-512, and RSA-768 algorithms can be used on the KeySecure. These algorithms are not allowed under the International Common Criteria standards; *using them will take the device out of Common Criteria compliance.*

Chapter 38

FIPS Status Server

The FIPS Status Server is an http server that provides system status, in the form of the FIPS Status report, whenever the device is running. The FIPS status server monitors for FIPS-related status and error messages. If the device self-test fails upon start-up, all other services on the device shutdown, including the Management Console. Only the FIPS status server continues to run in this state.

The report indicates:

- the latest results of all system self-tests
- the device state (either *error* or *normal*)
- the status of FIPS compliance (either *yes* or *no*)

The device performs the following tests:

Test	Power -Up	Conditional	Description
AES Encryption	X		Known Algorithm Test for the AES algorithm. This test is performed at power-up.
DES Encryption	X		Known Algorithm Test for the DES algorithm. This test is performed at power-up.
DSA Encryption	X		Known Algorithm Test for the DSA algorithm. This test is performed at power-up.
SHA-1 Algorithm	X		Known Algorithm Test for the SHA-1 algorithm. This test is performed at power-up.
SHA2-256 Algorithm	X		Known Algorithm Test for the SHA2-256 algorithm. This test is performed at power-up
SHA2-384 Algorithm	X		Known Algorithm Test for the SHA2-384 algorithm. This test is performed at power-up
SHA2-512 Algorithm	X		Known Algorithm Test for the SHA2-512 algorithm. This test is performed at power-up
HMAC Algorithm (SHA1, SHA2-256)	X		Known Algorithm Test for the HMAC algorithm, which tests both SHA1 and SHA2-256. This test is performed at power-up.
RSA Encryption	X		Known Algorithm Test for the RSA algorithm. This test is performed at power-up.
X9.31 PRNG	X		Known Algorithm Test for the X9.31 PRNG. This test is performed at power-up.
Continuous Random Number Generation		X	Test of the random number generation. This test is run whenever the system generates a random number.
RSA Pairwise Consistency		X	Pairwise consistency test of RSA key generation. This test is run whenever the system generates a key.

Test	Power -Up	Conditional	Description *(continued)*
DSA Pairwise Consistency		X	Pairwise consistency test of DSA key generation. This test is run whenever the system generates a key.
Software Integrity	X		Checksum test of all software. This test is performed at power-up.

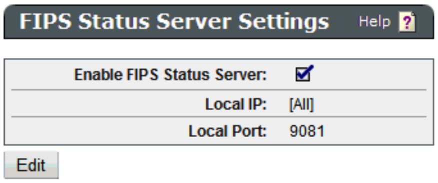
If any of these tests fail, the FIPS Status Report will indicate which test failed and when the failure occurred. The device will enter error state: access to the Management Console, the Command Line Interface, and the XML Interface will be denied. Limited access to the device via the serial console will be supported. To restore functionality, reboot the device. If the problem persists, contact customer support.

Enabling the FIPS Status Server

To enable the FIPS Status Server:

1 Log in to the Management Console as an administrator with SSL, Security, and Key Server access controls.

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



Enable FIPS Status Server: ☑

Local IP: [All]

Local Port: 9081

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** the FIPS Status Server listens on or, accept the default port value of 9081.

7 Click **Save**.

Viewing the FIPS Status Report

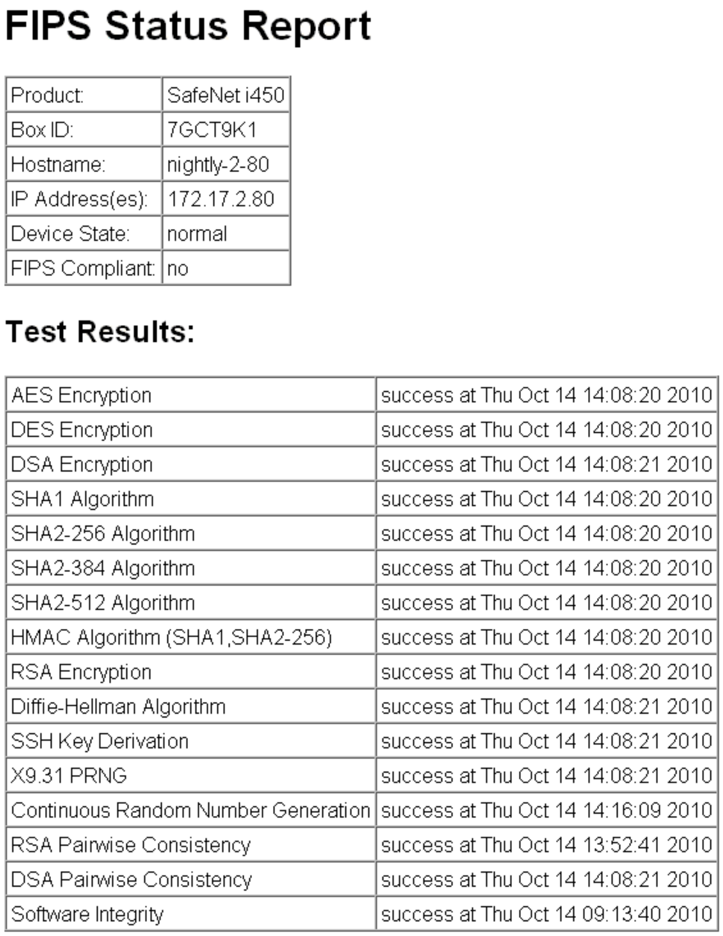
To view the FIPS Status Report:

1 Use either the Management Console or the CLI to locate the IP and port of the status report. By default, the location is <*Management Console IP*>*:9081/status.html*.

a To locate the IP and port 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 To locate the IP and port using the CLI: log in to the CLI and use the `show fips server` command.

2 Open a web browser and navigate to the IP and port using http. For example, *http:192.168.12.20:9081/status.html*.



FIPS Status Report

Product:	SafeNet i450
Box ID:	7GCT9K1
Hostname:	nightly-2-80
IP Address(es):	172.17.2.80
Device State:	normal
FIPS Compliant:	no

Test Results:

AES Encryption	success at Thu Oct 14 14:08:20 2010
DES Encryption	success at Thu Oct 14 14:08:20 2010
DSA Encryption	success at Thu Oct 14 14:08:21 2010
SHA1 Algorithm	success at Thu Oct 14 14:08:20 2010
SHA2-256 Algorithm	success at Thu Oct 14 14:08:20 2010
SHA2-384 Algorithm	success at Thu Oct 14 14:08:20 2010
SHA2-512 Algorithm	success at Thu Oct 14 14:08:20 2010
HMAC Algorithm (SHA1,SHA2-256)	success at Thu Oct 14 14:08:20 2010
RSA Encryption	success at Thu Oct 14 14:08:20 2010
Diffie-Hellman Algorithm	success at Thu Oct 14 14:08:21 2010
SSH Key Derivation	success at Thu Oct 14 14:08:21 2010
X9.31 PRNG	success at Thu Oct 14 14:08:21 2010
Continuous Random Number Generation	success at Thu Oct 14 14:16:09 2010
RSA Pairwise Consistency	success at Thu Oct 14 13:52:41 2010
DSA Pairwise Consistency	success at Thu Oct 14 14:08:21 2010
Software Integrity	success at Thu Oct 14 09:13:40 2010

3 View the following fields:

- Product - the model of the KeySecure.
- Box ID - the unique box ID, composed of alphanumeric characters.
- Hostname - the hostname used to identify the KeySecure on the network.
- IP Address(es) - the IP address(es) on which the key server is enabled on the KeySecure.
- Device State - indicates the current state of the device, either *normal* or *error*. When the device is in error state, functionality is dramatically limited: you will not be able to communicate with the device using the CLI, the Management Console, or the XML or KMIP Interfaces. Limited access to the device via the serial console will be supported. Reboot the device to restore functionality. If the problem persists, contact customer support.
- FIPS Mode Enabled - Indicates if the device is FIPS compliant.

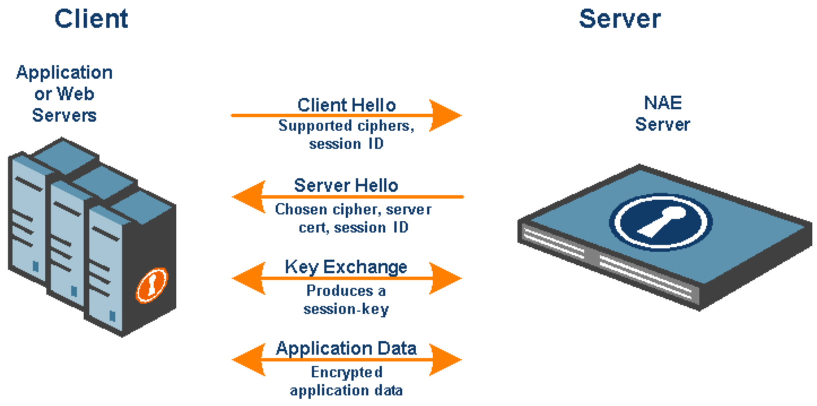
- Test Results - Displays the result and timestamp for each of the following self-tests:
  - AES Encryption
  - DES Encryption
  - DSA Encryption
  - SHA1 Algorithm
  - SHA2-256 Algorithm
  - SHA2-384 Algorithm
  - SHA2-512 Algorithm
  - HMAC Algorithm (SHA1 and SHA2-256)
  - RSA Encryption
  - Diffie-Hellman Algorithm
  - SSH Key Derivation
  - X9.31 PRNG
  - Continuous Random Number Generation
  - RSA Pairwise Consistency
  - DSA Pairwise Consistency
  - Software Integrity

Chapter 39

SSL

The KeySecure is designed to be able to establish Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections with all applications and databases that make requests to the NAE Server. SSL and TLS are the most widely deployed security protocols in network security. The following section provides a brief overview of the SSL protocol so that you might better understand how to configure the KeySecure.

SSL is used to establish secure connections between two entities, such as a client application and an NAE Server. In addition to securing connections, SSL is commonly used to authenticate a server to a client and vice versa. The SSL protocol is composed of two phases: (1) establishing a secure connection using the SSL handshake protocol, and (2) exchanging data over the secure connection. The SSL protocol steps are summarized below.


Client
Server
Application or Web Servers
NAE Server
Client Hello
Supported ciphers, session ID
Server Hello
Chosen cipher, server cert, session ID
Key Exchange
Produces a session-key
Application Data
Encrypted application data

SSL Handshake

The following steps describe a typical SSL handshake:

1 The protocol is initiated by the requesting application using a client hello message. This message includes a list of all the ciphers supported by the client application. The application also sends a session ID that might refer to previously established sessions.

2 The KeySecure responds with a server hello message, which includes the KeySecure certificate and the cipher chosen by the KeySecure. Once the session is established, it is secured using the chosen cipher. The message also contains a session ID.

3 The application and the KeySecure then engage in a key exchange protocol. The result is a session key that is then used for encrypting the entire session.

Once the SSL 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.

SSL Session Resume

Because the SSL key exchange protocol is based on public key cryptography, it consumes significant computing resources. To minimize the number of SSL handshakes, SSL provides a shortcut to a full key exchange. Consider an application that has previously established a secure session with the KeySecure. Both the application and the KeySecure already share a session–key. When the application reconnects to the NAE Server, there is no need to renegotiate a session key. During the reconnection process the two sides execute the SSL resume protocol, which bypasses the key exchange part of the SSL handshake. The resumed session is encrypted using the previously negotiated session–key. Establishing a secure connection using SSL resume is much faster than a full SSL handshake.

In this scenario, the client application indicates that it is willing to perform an SSL resume (rather than a full handshake) by sending a previously negotiated session–id in the CLIENT–HELLO message. The KeySecure 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 KeySecure responds with a new session–id.

SSL Session Timeout

All SSL sessions stored in the KeySecure session cache have an expiration time. A typical session expiration period is two hours. This means the KeySecure accepts a session resume request for at most two hours after the session is first established. The SSL session timeout on the KeySecure is configured on the SSL Configuration page, as described later in this chapter.

SSL Certificate Management on the KeySecure

Certificates are used to authenticate one entity to another. This authentication takes place during the SSL handshake protocol. Certificates are issued by Certification Authorities (CA's) such as VeriSign, Entrust, Thawte, and others. The KeySecure is equipped with CA capabilities, and can issue certificates for all your applications.

When establishing an SSL connection with a client application, you have the option to require the application authenticate itself to the KeySecure by presenting a certificate. Because the KeySecure can issue certificates to applications and databases, 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 KeySecure.

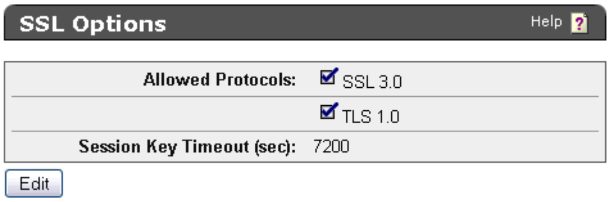
The KeySecure CA is managed on the CA Certificates page. To issue certificates for your applications, you must first create a local CA on the KeySecure. This local CA is then used to issue certificates for all your applications. Local certificates issued by the KeySecure CA are only valid for authenticating to the KeySecure.

Enabling SSL Protocols and Session Key Timeout

Use this section to view and modify SSL settings. These settings affect the Key Server's communication with client applications and databases when SSL is enabled. These settings also affect all connections to the web-based Management Console.

To enable SSL protocols and set the session key timeout:

1. Log in to the KeySecure.
2. Navigate to the SSL Configuration page (Security >> SSL).



SSL Options

Allowed Protocols:	☑ SSL 3.0
	☑ TLS 1.0
Session Key Timeout (sec):	7200

3. Select **Edit**.
4. Enable or disable SSL 3.0 and TLS 1.0 as appropriate for your installation.

   Important! 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.

   Important! Enabling SSL 3.0 on a FIPS compliant device will take the device out of FIPS compliance - possibly in a manner that does not comply with FIPS standards. For information on disabling FIPS compliance, see Chapter 37, “High Security Features”.

5. Enter a value for the **Session Key Timeout**. This field specifies the number of seconds that a previously negotiated session key is reused for incoming SSL client connections to the KeySecure. The default value is 7200 seconds (2 hours). Setting this value to 0 disables the time-out.
6. Click **Save**.

Note: FIPS compliant devices *cannot* use the default SSL configuration. On those devices, you must enable TLS 1.0 and disable SSL 3.0.

Important! Some web browsers, including Internet Explorer 6.0, do not have TLS 1.0 enabled by default. If you disable SSL 3.0, please check first that your browser has TLS 1.0 enabled. (In Internet Explorer, select Internet Options from the Tools menu, click the Advanced tab, scroll down to the Security section, and make sure the "Use TLS 1.0" checkbox is checked.)

Note: Changes to the SSL Options cause the Key Server to restart, which takes the Key Server offline for a few seconds.

Managing the SSL Cipher Order

Different applications and databases support different encryption algorithms for securing SSL sessions. The KeySecure supports many SSL ciphers and consequently can communicate securely using all common ciphers.

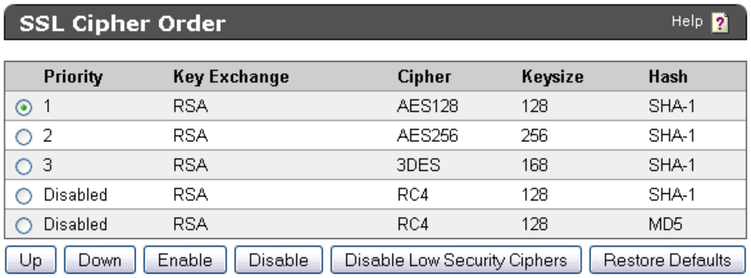
Please note that the SSL Cipher Order pertains to the communication channel between the client (application, database, etc.) and the KeySecure. It does not affect the keys that might be used to encrypt data by the Key Server. When an application or database presents the KeySecure with a list of supported ciphers, the KeySecure chooses the supported cipher that is highest on its priority list.

WARNING! Exercise caution when modifying the SSL Cipher Order. Unless you are familiar with SSL 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.

To manage the SSL cipher order:

1 Log in to the KeySecure.

2 Navigate to the SSL Configuration page (Security >> SSL).



	Priority	Key Exchange	Cipher	Keysize	Hash
●	1	RSA	AES128	128	SHA-1
○	2	RSA	AES256	256	SHA-1
○	3	RSA	3DES	168	SHA-1
○	Disabled	RSA	RC4	128	SHA-1
○	Disabled	RSA	RC4	128	MD5

3 The SSL Cipher Order section shows the following fields.

- **Priority** - 1 is the highest priority.
- **Key Exchange** - the algorithm to use for encryption and authentication. RSA is the only supported algorithm for key exchange.
- **Cipher** - the symmetric cipher to use to encrypt SSL sessions. Supported ciphers are: AES128, AES256, 3DES, and RC4.
- **Keysize** - the number of bits of the session key size. Supported key sizes vary for each cipher. 128 for RC4, 168 for 3DES, and 128 and 256 for AES.
- **Hash** -the hash function to use for SSL session integrity. The supported hash functions are:
  - SHA-1: operates on 64-byte blocks of data and produces a 160-bit authentication value.
  - MD5: operates on 64-byte blocks of data and produces a 128-bit authentication value.

4 Use the **Up**, **Down**, **Enable**, **Disable**, and **Restore Defaults** buttons to organize the list, as appropriate.

5 Use the **Disable Low Security Ciphers** button to mandate that only high security ciphers (those 128-bit and above) be used. This disables 128-bit RC4, both SHA-1 and MD5.

Appendix A

Default Ports for KeySecure Features

This appendix provides information to assist with making firewall configuration decisions for KeySecure deployments.

Inbound and Inbound/Outbound Ports

The **Port** number in the following table is the port on the KeySecure that is open and receives incoming connections.

If the **Config** column contains “yes,” the port value is configurable. For Management Console navigation to the page where ports in the following table can be configured see “Management Console” below.

Port	Feature	Protocol	Config	Required	Session Initiation
	Ping / Traceroute	ICMP	no	Optional	inbound / outbound
22	SSH Administration	TCP	yes	Optional[a]	inbound
161	SNMP Agent	UDP	yes	Optional	inbound
9000	NAE Server[b]	TCP	yes	Required	inbound
9001[c]	Cluster[d]	SSL	yes	Optional	inbound / outbound
9003	ProtectFile Manager Service	SSL	yes	Optional[e]	inbound
9080	Health Check	TCP	yes	Optional	inbound
9443	Web Administration	TCP	yes	Optional[a]	inbound

[a] SafeNet recommends opening ports for remote Web Administration (9443) and/or SSH Administration (22).

[b] Minimum Requirement: The NAE Server must have an open port to process cryptographic and key management operations with TCP or SSL transport. Corresponds to NAE_Port client configuration in IngrianNAE.properties file.

[c] This Port is also the destination port used for connections from one KeySecure to another. The source port for appliance-to-appliance connections may be ephemeral.

[d] The Cluster feature is used for server-side replication of configuration data.

[e] Required when using the ProtectFile.

Outbound Ports

The **Port** number in the following table is the port on an *external device* used for connections from the KeySecure to that external device. The source port used for these connections may be ephemeral.

If the **Config** column contains “yes,” the port value is configurable. For Management Console navigation to the page where ports in the following table can be configured see “Management Console” below.

Port	Feature	Protocol	Config	Required	Session Initiation
20	FTP data[a]	TCP	no	Optional	outbound
21	FTP control[a]	TCP	no	Optional	outbound
22	SCP[a]	TCP	no	Optional	outbound
53	DNS	UDP	no	Optional	outbound
123	NTP	UDP	no	Optional	outbound

Port	Feature	Protocol	Config	Required	Session Initiation
162	SNMP Traps	UDP	yes	Optional	outbound
514	Syslog	UDP	yes	Optional	outbound
1025	ProtectDB-Teradata	TCP	yes	Optional[b]	outbound
1433	ProtectDB-SQL Server	TCP	yes	Optional[b]	outbound
1521	ProtectDB-Oracle	TCP	yes	Optional[b]	outbound
8003	ProtectFile	TCP	yes	Optional[b]	outbound
50000	ProtectDB-DB2	TCP	yes	Optional[b]	outbound
389 636	LDAP Administrator Server[c]	TCP SSL	yes	Optional	outbound
389 636	LDAP User Directory[c]	TCP SSL	yes	Optional	outbound

[a] Log Rotation, Software & License Upgrade/Install, and Backup & Restore operations.

[b] Required when using the corresponding ProtectDB or ProtectFile.

[c] LDAP servers typically use port 389 for TCP and 636 for SSL. Required when using an external LDAP server for login authentication.

Management Console Navigation

The following table provides the Management Console navigation to the page where ports in the preceding tables can be configured.

Feature	Management Console Navigation
Key Server	Device >> Key Server >> Key Server
Web Administration	Device >> Administrators >> Remote Administration
SSH Administration	Device >> Administrators >> Remote Administration
SNMP Agent	Device >> SNMP >> Agent
ProtectFile Manager Service	Security >> ProtectFile Manager >> Service Settings Security >> ProtectFile Manager >> Connector Profiles
Health Check	Device >> Key Server >> Health Check
Cluster	Device >> Cluster
LDAP Administrator Server	Device >> Administrators >> LDAP Administrator Server
LDAP User Directory	Security >> LDAP >> LDAP Server
SNMP Traps	Device >> SNMP >> Management Stations
Syslog	Device >> Log Configuration >> Rotation & Syslog
Oracle Connector	Security >> Databases (in the ProtectDB Manager section)
SQL Server Connector	Security >> Databases (in the ProtectDB Manager section)
DB2 Connector	Security >> Databases (in the ProtectDB Manager section)
Teradata Connector	Security >> Databases (in the ProtectDB Manager section)
ProtectFile	Security >> ProtectFile Manager >> File Servers

Note: ProtectFile must be activated to view the ProtectFileManager links.

Appendix B

Supported Key Algorithms

When people think of cryptography, they often think of encrypting and decrypting information, but cryptography goes beyond encryption and decryption. Using the KeySecure you can encrypt or decrypt data, create a MAC, create a digital signature, and generate random numbers. These topics are described in the following sections:

- Encryption and Decryption with Symmetric Keys
- Encryption and Decryption with Asymmetric Keys
- Message Authentication Codes (MACs)
- Digital Signatures

Encryption and Decryption with Symmetric Keys

Encryption is the process of obscuring information (plaintext data) to make it unreadable (ciphertext) to anyone who does not possess a key, secret, or code. Decryption, then, uses a key, secret, or code to transform ciphertext into something readable. Because you can derive the original plaintext data from the ciphertext (provided, of course, that you have the correct key), encryption is a reversible operation. Encryption and decryption are, by far, the most common cryptographic requests made by NAE clients.

The vast majority of encrypt and decrypt operations performed in the KeySecure environment are with symmetric key algorithms. Symmetric key algorithms can be divided into stream ciphers and block ciphers. Stream ciphers process data bit–by–bit, while block ciphers process fixed–size blocks of data. For a variety of reasons, we discourage the use of stream ciphers. Encryption and decryption with symmetric keys is quite simple. The following example illustrates this exchange:

- Bob wants to send a message to Alice, and Bob wants to be sure that no one else can read that message, so Alice and Bob agree on a shared secret key (let's call it Key1).
- The message Bob wants to send Alice is "This is a super secret message from Bob." Bob encrypts that message using Key1 and sends Alice the ciphertext (`6QNKMgUDJcE....`).
- Alice decrypts the ciphertext with Key1 and is now able to read Bob's message.

In this way, Alice and Bob can continue communicating over a network while preventing potential eavesdroppers from understanding their messages. If Alice wants to indicate to Bob that she received his message, she can encrypt her message with Key1 and send Bob the ciphertext, which Bob can then decrypt with Key1.

Block Ciphers

To encrypt or decrypt with a block algorithm, it must be possible to divide the plaintext value into full blocks of a specific size. (In the case of AES and SEED, the block size is sixteen bytes; in the case of DESede and DES, the block size is eight bytes.) If the plaintext length is not a multiple of the algorithm's block size, padding is used to fill the remainder of the last block. If the length of the plaintext value is a multiple of the block size, padding is used to fill an additional, trailing block. This additional block is used to indicate that padding is not present in the preceding blocks. Whichever algorithm is used to encrypt data, the ciphertext is larger than the original plaintext value. The following table illustrates how this is true for the AES and SEED algorithms.

Plaintext Size in bytes	Ciphertext Size in bytes
15	16
16	32
17	32
127	128
128	144

As mentioned, DESede and DES use a block size of eight bytes. The following table illustrates how padding affects the length of ciphertexts from DES and DESede algorithms.

Plaintext Size in bytes	Ciphertext Size in bytes
7	8
8	16
9	16
95	96
96	104

Modes of Operation

If you are using a block cipher (AES, DESede, or DES), decide whether you want to use the algorithm in electronic codebook (ECB) mode, or cipher-block chaining (CBC) mode.

- In ECB mode, each block is encrypted separately, through the same procedure. Thus, two identical plaintext blocks encrypt to the same ciphertext and any data patterns in the plaintext can be detected in the encrypted data.
- In CBC mode, the first block is XORed with an initialization vector before being encrypted. All subsequent plaintext blocks are XORed with the previous ciphertext block before being encrypted. This dependency makes it more difficult for an attacker to swap blocks, because blocks must be decrypted in the same order in which they were encrypted to produce the original plaintext.

  When the same key and different IVs are used, identical plaintexts are guaranteed to have different ciphertexts.

We recommend that you use CBC mode, unless you have a compelling reason to use ECB mode.

Initialization Vectors

An initialization vector (IV) is a sequence of random bytes appended to the front of the plaintext before encryption. Use of a unique IV eliminates the possibility that the initial ciphertext block is the same for any two encryption operations of the same plaintext that use the same key. In the KeySecure environment, IVs are only used by block ciphers in CBC mode. The size of the IV depends on the algorithm; AES and SEED use a sixteen byte IV, while DESede and DES use an eight byte IV. The KeySecure can generate random IVs for you, or you can supply your own.

When supplying your own IV for data migration, it is important to note that IVs must be specified in hexadecimal (base 16 encoded) characters. As such, an eight byte IV requires sixteen characters; likewise, a sixteen byte IV requires thirty-two characters. Sometimes, the examples in this documentation show impractical IVs for the sake of simplicity, for example 112233445566.... Make sure that your IV is sufficiently complex, and if you are supplying your own IV for anything other than data migration, it is crucial that you remember the IV your supplied.

Note: To ensure a unique ciphertext during data migration, you would have to apply IVs at the field–level and not the column–level.

Supported Algorithms

- AES
- ARIA
- DES
- DESede (triple DES)
- SEED
- RC4

In general, we recommend that you use symmetric one of the following block ciphers to encrypt data in the KeySecure environment: AES, DESede, or SEED (if enabled). Of the symmetric block ciphers, we recommend AES because it performs better and is considered to be more secure than the others.

We recommend that you not use the DES algorithm, because it is known to be a weak algorithm and is supported only for backward compatibility.

Encryption and Decryption with Asymmetric Keys

While symmetric key encryption utilizes a shared secret key, public key cryptography (crypto operations performed with asymmetric keys) typically utilizes a pair of keys: one public, the other private. This allows users to communicate securely without having prior access to a shared secret key. All public keys are published and therefore available to anyone, while all private keys remain with the user. Keys are related mathematically, such that each key allows you to reverse the operations performed with the other key. In other words, you can encrypt with the public key and decrypt with the private key. This method of encryption is extremely slow compared to symmetric ciphers.

The following example illustrates the exchange:

- Bob and Alice each generate public/private key pairs and publish their public keys.
- Alice looks up Bob’s public key, encrypts her message with it, and send Bob her message.
- Bob gets Alice’s message and decrypts it with his private key.
- Bob looks up Alice’s public key, encrypts his reply with it, and sends it to Alice.
- Alice can then decrypt Bob’s message with her private key.

In this way, Alice and Bob can continue communicating over a network while preventing potential eavesdroppers from understanding their messages.

Supported Algorithms

- RSA

Asymmetric algorithms, such as RSA, can be up to an order of magnitude slower than symmetric algorithms.

When using RSA keys to encrypt data, the ciphertext is always the size of the key; if your RSA key is 2048 bits (or 256 bytes), then the ciphertext is also 256 bytes. And because PKCS #1 padding is always used with RSA keys, you can encrypt no more than the key size, less eleven. For example, if you use a 2048-bit RSA key, the maximum data size that you can encrypt with that key is 245 bytes.

The speed and size issues make public key cryptography impractical for encrypting data. Therefore, we recommend that you use symmetric key algorithms to encrypt your data.

Message Authentication Codes (MACs)

A cryptographic hash is a one–way (non–reversible) algorithm that applies a hash function and a secret key to any amount of input and returns a fixed–size output (the MAC). A MAC, short for Message Authentication Code, can be thought of as a keyed hash or checksum. Only if you hold the secret key used to calculate the MAC can you verify the MAC. MACs are used to ensure data integrity and authenticity.

The following example illustrates the exchange:

Bob wants to send a message to Alice, and Bob wants Alice to be able to trust that the message she receives is from Bob and that it has not been modified in any way. So Bob decides to create a MAC of the message that he wants to send Alice. Bob has already given Alice a copy of the HMAC key that Bob uses to compute the MAC.

- Bob composes the following plaintext message: “This is indeed a message from Bob, and it has not been altered.”
- Bob uses his HMAC key to compute the MAC of his message text. The MAC value for this particular key and text is: `k8vifJC1F4sgg6pbeSpp9iMRfQ4r2hMD`.
- Bob sends the plaintext message along with the MAC value he computed to Alice.
- Once she receives the message, Alice uses the HMAC key Bob gave her to compute the MAC value on the plaintext message Bob sent her.

When the MAC value Alice computes matches the MAC value Bob sent her, she can be confident that the message Bob sent her has not been altered (integrity), and Bob is the sender of the message (authenticity).

Supported Algorithms

- HMAC-SHA1
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512

If you have an interest in storing passwords securely, you might think about creating a MAC at the application level (using one of the Cryptographic Providers) on your passwords and storing the MAC values instead of the plaintext passwords. That way you minimize the amount of time that passwords are in plaintext in your network

MACs can be created through the XML interface and all of the Cryptographic Providers except for the MSCAPI Provider.

The same plaintext value, MACed with the same key, always yields the same output.

By unreversible, it is meant that you cannot apply a reverse function to the MAC value to derive the original plaintext message.

Digital Signatures

Digital signatures rely on the use of public key cryptography, which generally allows users to communicate securely without having prior access to a shared secret key. Digital signatures can be used to ensure the authenticity of a sender. For example, Bob can encrypt a message with his private key and send it to Alice. If Alice can successfully decrypt it using the corresponding public key, this provides assurance to Alice that Bob (and no one else) sent it.

Digital signatures can be created through all of the Cryptographic Providers except for the .NET Provider. You can also create MACs through the XML interface.

Supported Algorithm

- RSA

Summary

In summary, you can use the KeySecure to perform a variety of cryptographic operations. The following table lists the cryptographic algorithms supported by the KeySecure. Each algorithm is discussed in “Supported Algorithms” on page 242.

Note: Not all algorithms are supported by all client software.

Algorithm	Supported Operations	Description	Function
AES	• Encrypt • Decrypt	symmetric key block cipher	Highly secure algorithm; recommended for most environments. Discussed in detail in “AES” on page 243.
ARIA	• Encrypt • Decrypt	symmetric key block cipher	National standard encryption algorithm in the Republic of Korea. Discussed in detail in “ARIA” on page 243.
DES	• Encrypt • Decrypt	symmetric key block cipher	Known to be an insecure algorithm; not recommended for any environment. Discussed in detail in “DES” on page 244.
DESede	• Encrypt • Decrypt	symmetric key block cipher	Not as secure as AES; can be used in many environments. Discussed in detail in “DESede” on page 244.
HMAC-SHA1	• MAC • MAC Verify	keyed hash function	Used to protect integrity and authenticity. Strength is determined by key size. Discussed in detail in “HMAC-SHA1” on page 245.
RC4	• Encrypt • Decrypt	symmetric key stream cipher	Extremely slow compared to block ciphers. Discussed in detail in “RC4” on page 246.
RSA	• Encrypt • Decrypt • Sign • Sign Verify	public key algorithm	Used to encrypt data and create digital signatures; not the recommended encryption algorithm. Discussed in detail in “RSA” on page 246.
SEED	• Encrypt • Decrypt	symmetric key block cipher	National standard encryption algorithm in the Republic of Korea. Discussed in detail in “SEED” on page 247.

Supported Algorithms

The KeySecure supports the following public algorithms:

- AES
- ARIA
- DES
- DESede
- HMAC-SHA1
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512
- RC4
- RSA
- SEED

A proprietary format, which utilizes the DES algorithm, is also supported.

Note: PKCS#11 does not support ECB mode with PKCS5Padding.

AES

Block Size	16 bytes
Supported Modes	• ECB (default) • CBC
Padding Schemes	• PKCS5Padding • NoPadding – When using AES is NoPadding mode, you must supply ciphertext in multiples of 16 bytes.
IV	• CBC mode requires a 16 byte IV. • IV is not allowed in ECB mode.
Key Size (in bits)	• 128 (default) • 192 • 256
Identifier Strings	• AES/CBC/NoPadding • AES/CBC/PKCS5Padding • AES/ECB/NoPadding • AES/ECB/PKCS5Padding • AES – This is equivalent to AES/ECB/PKCS5Padding
Additional Notes	When using AES keys with NoPadding, or in ECB mode, you must supply data (both ciphertext for decryption and plaintext for encryption) in multiples of 16 bytes.

ARIA

Block Size	16 bytes
Supported Modes	• ECB (default) • CBC
Padding Schemes	• PKCS5Padding • NoPadding – When using ARIA is NoPadding mode, you must supply ciphertext in multiples of 16 bytes.
IV	• CBC mode requires a 16 byte IV. • IV is not allowed in ECB mode.
Key Size (in bits)	• 128 (default) • 192 • 256
Identifier Strings	• ARIA/CBC/NoPadding • ARIA/CBC/PKCS5Padding • ARIA/ECB/NoPadding • ARIA/ECB/PKCS5Padding • ARIA – This is equivalent to ARIA/ECB/PKCS5Padding
Additional Notes	When using ARIA keys with NoPadding, or in ECB mode, you must supply data (both ciphertext for decryption and plaintext for encryption) in multiples of 16 bytes.

DES

Block Size	8 bytes
Supported Modes	• ECB (default) • CBC
Padding Schemes	• PKCS5Padding (default) • NoPadding
IV	• CBC mode requires an 8 byte IV. • IV is not allowed in ECB mode.
Key Size	Supported key size is 56 bits. The key contains an extra 8 bits of parity, for a total key size to 64 bits.
Identifier Strings	• DES/CBC/NoPadding – Uses outer CBC mode • DES/CBC/PKCS5Padding – Uses outer CBC mode • DES/ECB/NoPadding • DES/ECB/PKCS5Padding • DES – This is equivalent to DES/ECB/PKCS5Padding
Additional Notes	When using DES keys with NoPadding, or in ECB mode, you must supply data (both ciphertext for decryption and plaintext for encryption) in multiples of 8 bytes.

DESede

Block Size	8 bytes
Supported Modes	• ECB (default) • CBC
Padding Schemes	• PKCS5Padding (default) • NoPadding • IngrianPadding
IV	• CBC mode requires an 8 byte IV. • IV is not allowed in ECB mode.
Key Size	Supported key sizes are 168 (default) and 112 bits. Each key contains an extra 8 bits of parity. Thus, when you create a key of 112 bits, the *actual* key size is 128 bits; when you crete a key of 168 bits, the *actual* key size is 192 bits. A key size of 112 bits refers to two–key triple DES. The sequence of operations in two–key triple DES is: • Encrypt with Key1 • Decrypt with Key2 • Encrypt with Key1 A key size of 168 bits refers to three–key triple DES. The sequence of operations in three–key triple DES is: • Encrypt with Key1 • Decrypt with Key2 • Encrypt with Key3

Identifier Strings	• DESede/CBC/NoPadding – Uses outer CBC mode • DESede/CBC/PKCS5Padding – Uses outer CBC mode • DESede/CBC/IngrianPadding • DESede/ECB/NoPadding • DESede/ECB/PKCS5Padding • DESede – This is equivalent to DESede/ECB/PKCS5Padding
Additional Notes	When using DESede keys with NoPadding, or in ECB mode, you must supply data (both ciphertext for decryption and plaintext for encryption) in multiples of 8 bytes.

HMAC-SHA1

Supported Hash Function	SHA-1
Padding Schemes	Uses padding from SHA-1 algorithm. No additional padding.
IV	No IV is required.
Key Size	Keys can be between 128 and 256 bits. We recommend that the key size be at least 160 bits, and sets the default at 160. The HMAC keys you generate should be a multiple of 8 bytes. On some platforms, HMAC keys that are not a multiple of 8 bytes might yield incorrect results when generating MACs.
Identifier String	• HmacSHA1
Additional Notes	HMAC is a stream cipher. HMAC keys are bitstreams of multiples of 8 bits.

HMAC-SHA256

Hash Function	SHA-2
Padding Schemes	Uses padding from SHA-2 algorithm. No additional padding.
IV	No IV is required.
Key Size	Keys can be 128, 192, or 256 bits. The default is 256. The HMAC keys you generate should be a multiple of 8 bytes. On some platforms, HMAC keys that are not a multiple of 8 bytes might yield incorrect results when generating MACs.
Identifier String	• HmacSHA256
Additional Notes	HMAC is a stream cipher. HMAC keys are bitstreams of multiples of 8 bits.

HMAC-SHA384

Hash Function	SHA-2
Padding Schemes	Uses padding from SHA-2 algorithm. No additional padding.
IV	No IV is required.
Key Size	Keys can be 192, 288, or 384 bits. The default is 384. The HMAC keys you generate should be a multiple of 8 bytes. On some platforms, HMAC keys that are not a multiple of 8 bytes might yield incorrect results when generating MACs.

Identifier String	• HmacSHA384
Additional Notes	HMAC is a stream cipher. HMAC keys are bitstreams of multiples of 8 bits.

HMAC-SHA512

Hash Function	SHA-2
Padding Schemes	Uses padding from SHA-2 algorithm. No additional padding.
IV	No IV is required.
Key Size	Keys can be 256, 384, or 512 bits. The default is 512. The HMAC keys you generate should be a multiple of 8 bytes. On some platforms, HMAC keys that are not a multiple of 8 bytes might yield incorrect results when generating MACs.
Identifier String	• HmacSHA512
Additional Notes	HMAC is a stream cipher. HMAC keys are bitstreams of multiples of 8 bits.

RC4

IV	No IV required.
Key Size	Supported key sizes are 40 and 128 bits.
Identifier String	RC4
Additional Notes	RC4 is a stream cipher with byte–oriented operations, which means that RC4 keys are bitstreams of multiples of 8 bits.

RSA

IV	No IV is required.
Key Size	• 512 • 1024 (default) • 2048 • 3072 • 4096 Note: RSA-3072 and RSA-4096 are not supported for cryptographic operations on i300 series KeySecures. Keys using these algorithms can still be created, imported, and exported on those devices. RSA-4096 cannot be created using the XML interface, they can only be created using the Management Console.
Identifier Strings	• SHA1withRSA – for signatures • RSA – for encryption
Additional Notes	• The ciphertext is always the size of the RSA key; if your RSA key is 2048 bits (256 bytes), then the ciphertext is 256 bytes. Because they use PKCS#1 padding, RSA keys can encrypt data up to 11 bytes smaller than the key size. If you use a 2048–bit RSA key, then the maximum data size that you can encrypt with that key is 245 bytes. • RSA keys cannot be used to perform data migration operations.

SEED

Block Size	16 bytes
Supported Modes	• ECB • CBC
Padding Schemes	• PKCS5Padding • NoPadding
IV	• CBC mode requires a 16 byte IV. • IV is not allowed in ECB mode.
Key Size	Supported key size is 128 bits.
Additional Notes	Support for the SEED algorithm is only available on devices that are not FIPS compliant, and must be feature–activated. Both server and client must be running version 4.3 or later.

Appendix C

Hardware Specifications

This appendix contains the hardware descriptions of the KeySecure devices.

KeySecure server platform devices supported in the 6.5.0 release:

- KeySecure k150
- KeySecure k460

Note: HSM and SSKM are supported by the KeySecure k460.

KeySecure k150 Attributes

Processor Details	
Processor	One VIA C3 800MHz processor
Cryptographic Operations per second	11,000 Less than 250 microseconds latency. Scalable to tens of thousands of transactions per second with the addition of more KeySecure platforms.

Interfaces	
Network	1 10/100 Mbps ethernet port

Power Supply Details	
Power Supply	250W; 100 - 240 VAC, auto-ranging, 50-60 Hz, 5 - 3A

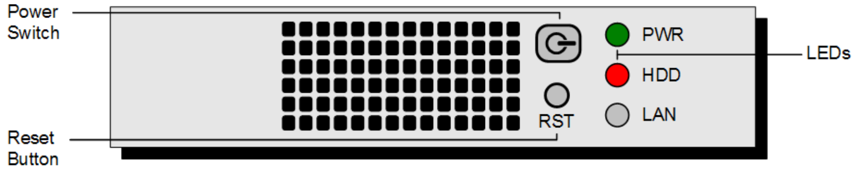
Environmental Requirements	
Operating Temperature	Ambient temperature: 50° to 95°F (10° to 30°C)
Nonoperating Temperature	Ambient temperature: -40° to 149°F (-40° to 65°C)
Operating Humidity	8% to 85% (non-condensing) with a maximum gradation of 10% per hour.
Operating Humidity	5% to 95% (non-condensing)

Acoustic Noise Emissions	
Acoustic Noise	66 decibels

Dimensions	
Height	1.75 in (4.45 cm)
Width	19 in (48.26 cm)
Depth	13 in (33.02 cm)

Front Panel

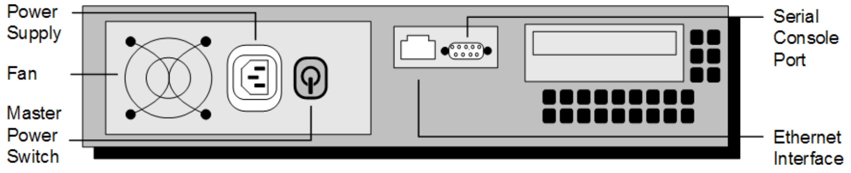
The front of the k150 contains a metal bezel, below which are a power switch, a reset button, and three LEDs. You must remove the front plate with a screwdriver to access the components shown below.



Component	Description
Power Switch	Turns the appliance on for the boot process. Used in combination with the Master Power Switch on the back panel. When booting the appliance for the first time: • Turn on the Master Power Switch on the back panel. • Remove the front bezel. • Press the power switch on the front panel. After completing the initial boot process, you do not need this switch to power the appliance.
Reset Button	Press this button to reboot the appliance.
LEDs	• PWR – shows green when the unit is on. • HDD – shows red when the system is accessing the hard disk. • LAN – disabled.

Back Panel

The back panel of the k150 contains an ethernet interface, a serial console port, a master power switch, a power supply, and a fan.



Component	Description
Ethernet Interface	One 10/100 Mbps Ethernet port for an RJ45 connector.
Serial Console Port	DB9 port used to obtain console access to the device.

Component	Description *(continued)*
Master Power Switch	Use this power switch to turn the KeySecure on or off. *When booting the device for the first time*, you must turn this switch on and then press the power switch on the front panel.
Power Supply	AC power socket.
Fan	Fans used to cool the power supply.

KeySecure k460 Attributes

Specifications	
Processor	Intel XeonE5620 2.4Ghz, 12M Cache, Turbo, HT, 1066MHz Max Mem
Network Interfaces	4 x 10/100/1000 Mbps ethernet ports
Hard Drive	Two 500GB 7.2K RPM SATA 2.5” HotPlug Hard Drives
RAM	8 GB

Power Supply Details	
Power Supply	Two 502W Energy Smart Hot-Plug Power Supplies
Power Supply Output Rating	502 Watts
Power Consumption	Using one power supply: 110 - 125 W Using two power supplies: 120 - 150 W
Input Power Range	100-240 VAC
Maximum Input Current	1.67 A
Maximum Heat Dissipation	1712.9 BTU per hour
Power Supply Efficiency at Specified Loadings	79.9%@10% 88.4%@20% 92.5%@50% 92%@100%
Power Supply Power Factor at Specified Loadings	0.74@10% 0.85@20% 0.95@50% 0.98@100%

Environmental Requirements	
Operating Temperature	Ambient temperature: 50° to 95°F (10° to 35°C) with a maximum temperature gradation of 10°C per hour. For altitudes above 2950 feet, the maximum operating temperature is de-rated 1°F/550 ft.
Non-operating Temperature	Ambient temperature: -40° to 149°F (-40° to 65°C) with a maximum temperature gradation of 20°C per hour.
Operating Humidity	20% to 80% (non-condensing) with a maximum humidity gradation of 10% per hour.
Non-operating Humidity	5% to 95% (non-condensing) with a maximum humidity gradation of 10% per hour.

Acoustic Noise Emissions	
Acoustic Noise	Typically configured 2. 5” chassis in 23 +/- 2 C ambient Idle: LwA-UL = 5.3 bels, LpAm = 35 dBA

Dimensions	
Height	1.7 in (4.32 cm)
Width	19.0 in (48.3 cm) - includes rack ears used to mount the device to a server rack. 16.7 in (42.3 cm) - without rack ears.
Depth	33.0 in (83.7 cm) - includes PSU handles and locking bezel. 31.3 in (79.5 cm) - includes PSU handles, without bezel.
Weight	39 lbs (17.69 kg)

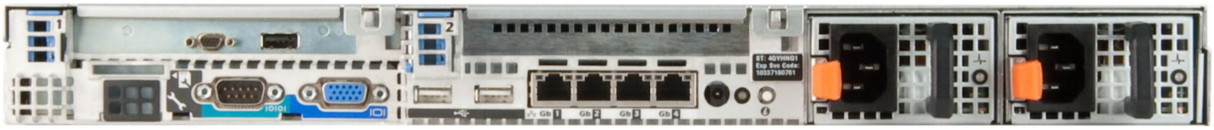
Front Panel

The front panel of the k460 contains a locking bezel, two hard disks, a power button, and a LCD panel.

Component	Description
Locking Bezel	Unlock the protective bezel to access the power button.
Power Button and Power Indicator	This button is used to power up or turn off the appliance. The power-on indicator lights when the system power is on.
LCD Panel	Provides ID, status information, and system error messages.
Hard Disks	The appliance supports two 2.5” SATA hard disks.

Back Panel

The back panel of the k460 contains four ethernet interfaces, a serial port, two power supplies, and PED port.



Component	Description
DB9 Serial Console Port	The DB9 port is used to perform first-time initialization and gain console access to the appliance.
Ethernet Interfaces	The appliance has 4 x 10/100/1000 Mbps ethernet ports
Power Supplies	The appliance has two hot-plug high-efficient 502W Energy Smart PSUs.
PED port	The PED port is used to connect the PIN entry device (PED) to the KeySecure.

Dell iDRAC Interface

KeySecure appliances support the iDRAC interface from Dell. The appliances ship with the default username and password from Dell. The default username is root, and the default password is calvin. For detailed information, see the "iDRAC Configuration Utility" sections in the Dell PowerEge R610 Systems Hardware Owner's Manual that is available at:

http://www.dell.com/support/Manuals/us/en/19/Product/poweredge-r610

Separate and more complete documentation is available as part of the Integrated Dell Remote Access Controller User Guide.

Apple Reboot

Rebooting a KeySecure running on an Apple machine requires action at the physical machine, You must press the F1 key during the reboot process.

Remote PED Firmware Version

When using Luna Remote PED, the PED Server must be running Firmware Version 2.4 or higher. To check the PED firmware version, execute `PedServer.exe -m show`. For example:

```
#PedServer.exe -m show
Ped Server Version 1.0.5 (10005)
Ped Server launched in status mode.
Server Information:
Hostname: RED1-206921
IP: 172.17.36.254
Firmware Version: 2.4.0-3
```

Appendix D

Regulatory and Certification Statements

This appendix contains the regulatory, certification, and compliance statements for the KeySecure k460 appliance.

FCC Class A Declaration of Conformity

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

European Union

Marking by the symbol CE indicates compliance of this SafeNet device to the EMC directives and the Low Voltage Directives of the European Union.

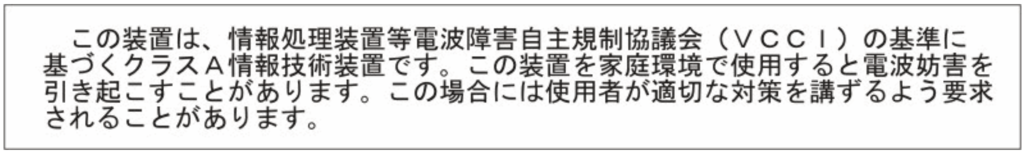
This is a class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take adequate remedial measures.

Canadian ICES-003

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

VCCI Class A Statement



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

CE Statement

The standards compliance label on the appliance contains the CE mark, which indicates that this system conforms to the provisions of all European Council directives, laws, and standards.

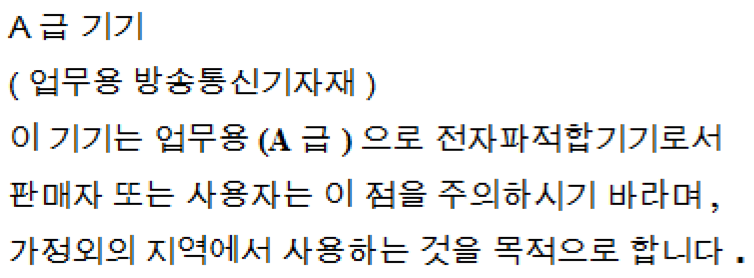
The appliance is in conformity with the provisions of the following EC directives, including all amendments, and national legislation implementing these directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

The following harmonized standards have been applied:

- EN 55022: 2006 + A1: 2007
- EN 61000-3-2: 2006
- EN 61000-3-3: 1995 + A1: 2001 + A2: 2005
- EN 55024: 1998 + A1: 2001 + A2: 2003
- EN 60950-1: 2006 + A11: 2009

KCC Statement



A 급 기기

(업무용 방송통신기자재)

이 기기는 업무용 (A 급) 으로 전자파적합기기로서

판매자 또는 사용자는 이 점을 주의하시기 바라며 ,

가정외의 지역에서 사용하는 것을 목적으로 합니다 .

This equipment is suitable for electromagnetic equipment for office work (Class A) and it can be used outside home.

Appendix E

Notices, Warnings, and Certifications

This appendix contains notices, warnings, and certification statements that apply to the KeySecure k460 appliance.

Notices and Warnings

For appliance related safety notices and warnings, see warnings on the side of the chassis adjacent to the power supplies.

Power Supply Notice

This appliance is suitable for IT power systems. Connect each power supply to a separate power source for failover support.

WARNING! The power supply cord is used as the main disconnect device. Ensure that the socket outlet is located/installed near the equipment and is easily accessible.

WARNING! This product relies on the building’s installation for short circuit (over current) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current carrying conductors).

Dual Power Supply Notice

WARNING! This unit has more than one power supply connection; all connections must be removed to remove all power from the unit.

Lithium Battery Notice for Service Personnel

This product contains lithium batteries. While the internal Hardware Security Module battery is not field-serviceable, the server battery is serviceable. Observe the following warning:

CAUTION! Danger of explosion if battery is replaced with incorrect type. Replace only with the same type recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions.

Perchlorate Information

This product’s coin cell battery may contain perchlorate and may require special handling when recycled or disposed of. See www.dtsc.ca.gov/hazardouswaste/perchlorate.

Rack Mounting

Appropriate hardware is provided with the appliance in order to mount it in an EIA standard 19” rack.

WARNING! To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. These guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

CAUTION! Slide/rail mounted equipment is not to be used as a shelf or a workspace.

Electrostatic Discharge

As with all electronic devices, the operator must guard against Electrostatic Discharge (ESD). Use of proper ESD management techniques (ESD flooring, wrist straps, etc.) will prevent potential damage to the unit. It is strongly recommended to eliminate the potential of ESD during the following procedures:

- installing the unit in a rack
- replacing a power supply module

Hinweise, Warnungen und Zertifizierungen

Informationen über Hardware-Hinweise, Warnungen und Zertifizierungsangaben.

Hinweise und Warnungen

Gerätebezogene Sicherheitshinweise und Warnungen.

Stromversorgungshinweis

Das Gerät eignet sich für IT-Stromanlagen. Verbinden Sie jede Stromzufuhr zur Ausfallsicherung mit einer getrennten Stromquelle.

WARNHINWEIS! Das Stromzufuhrkabel wird als Hauptabschaltvorrichtung verwendet. Stellen Sie sicher, dass sich die Steckdose in der Nähe des Geräts befindet bzw. dort angebracht wird und dass sie leicht zugänglich ist.

WARNHINWEIS! Dieses Produkt vertraut für Kurzschlussschutz (Überstrom) auf die installierten Schutzeinrichtungen des Gebäudes. Stellen Sie sicher, dass für die Phasenleiter (alle stromführenden Leitungen) eine Sicherung oder ein Leistungsschalter von maximal 120 VAC, 15 A (in den USA, 240 VAC und 10 A international) verwendet wird.

Hinweis zur doppelten Stromversorgung

WARNHINWEIS! Dieses Gerät verfügt über mehr als einen Stromanschluss. Alle Verbindungen müssen getrennt werden, um das Gerät vom Stromkreis zu trennen.

Hinweis zur Lithiumbatterie für Servicemitarbeiter

Dieses Produkt enthält Lithiumbatterien. Die interne Batterie des Hardware-Security-Moduls lässt sich zwar nicht vor Ort warten, die Serverbatterie jedoch schon. Beachten Sie bitte den folgenden Warnhinweis:

ACHTUNG! Explosionsgefahr, wenn die Batterie nicht durch eine korrekte Batterieart ausgetauscht wird. Austausch nur mit demselben Typ, der vom Hersteller empfohlen wird. Entsorgen Sie verbrauchte Batterien entsprechend den Anweisungen des Herstellers.

Rack-Montage

Das Gerät wird zusammen mit entsprechenden Zubehörteilen geliefert, um es in einem 19-Zoll-EIA-Standard-Rack zu montieren.

ACHTUNG! Um Körperverletzungen bei der Montage oder Wartung dieses Geräts in einem Rack zu vermeiden, müssen besondere Vorsichtsmaßnahmen ergriffen werden, um sicherzustellen, dass das System stabil bleibt. Diese Richtlinien werden zur Gewährleistung Ihrer Sicherheit bereitgestellt:

- Dieses Gerät sollte im Rack ganz unten montiert werden, wenn es das einzige Gerät im Rack ist.
- Wenn dieses Gerät in einem teilweise gefüllten Rack montiert werden soll, beladen Sie das Rack von unten nach oben, wobei die schwersten Geräte unten anzubringen sind.
- Wenn das Rack gemeinsam mit Stabilisierungskomponenten geliefert wird, installieren Sie die Stabilisierungselemente, bevor Sie das Gerät im Rack montieren oder warten.

ACHTUNG! Auf Laufschienen montierte Geräte dürfen nicht als Regal oder als Arbeitsbereich verwendet werden.

Elektrostatische Entladung

Wie bei allen elektronischen Geräten, muss sich der Bediener auch hier vor elektrostatischen Entladungen (ESD) schützen. Der Einsatz angemessener Verfahren zum Schutz vor elektrostatischer Entladung (ESD-Bodenbeläge, Armbänder, etc.) verhindern mögliche Schäden am Gerät. Es wird nachdrücklich empfohlen, das Risiko von elektrostatische Entladungen anhand der folgenden Verfahren zu eliminieren:

- Installation des Geräts in einem Rack
- Ersatz eines Stromzufuhrmoduls

Notificaciones, advertencias y certificaciones

Información acerca de las notificaciones, advertencias y declaraciones de certificaciones del hardware.

Notificaciones y advertencias

Notificaciones y advertencias de seguridad relativas al equipo.

Notificación sobre la fuente de alimentación

El dispositivo es recomendable para sistemas eléctricos de tipo IT (sin conexión a tierra). Conecte cada fuente de alimentación a una fuente distinta para obtener tolerancia a fallos.

¡ADVERTENCIA! El cable de la fuente de alimentación se utiliza como el principal dispositivo de desconexión. Asegúrese de que el tomacorriente esté ubicado/instalado cerca del equipo y sea de fácil acceso.

¡ADVERTENCIA! Este producto depende de la instalación del edificio para la protección contra cortocircuitos (sobrecarga). Asegúrese de utilizar un fusible o disyuntor que no supere 120 VCA, 15A (EE.UU.) o 240 VCA, 10A (internacional) en los conductores de fase (todos los conductores de corriente).

Notificación sobre la fuente de alimentación dual

¡ADVERTENCIA! Esta unidad cuenta con más de una conexión a la fuente de alimentación; se deben extraer todas las conexiones para desconectar la alimentación de la unidad.

Notificación acerca de la batería de litio para el personal de mantenimiento

Este producto contiene baterías de litio. Si bien la batería interna del Módulo de seguridad de hardware no se puede reparar en el lugar, la batería del servidor sí. Tenga en cuenta la siguiente advertencia:

¡PRECAUCIÓN! Peligro de explosión si la batería se reemplaza por un tipo incorrecto. Reemplace únicamente con el mismo tipo recomendado por el fabricante. Deseche las baterías utilizadas según las indicaciones del fabricante.

Montaje en rack

El dispositivo cuenta con los elementos de sujeción adecuados para montarlo en un rack estándar de 19 pulgadas que cumple con la norma EIA.

¡ADVERTENCIA! Para evitar daños corporales cuando se monta o realiza mantenimiento de esta unidad en un rack, debe asegurarse de que el sistema permanezca estable. Siga las siguientes pautas para su seguridad:

- Esta unidad debe montarse en la parte inferior del rack, si es la única unidad en el mismo.

- Cuando monte esta unidad en un rack que esté parcialmente lleno, cargue el rack desde abajo hacia arriba y coloque el componente más pesado en la parte inferior del mismo.
- Si el rack contiene dispositivos de estabilización, instale los estabilizadores antes de montar o realizar el mantenimiento de la unidad en el rack.

¡PRECAUCIÓN! No deben utilizarse los equipos montados sobre rieles/soportes deslizantes como estantes o espacio de trabajo.

Descarga electrostática

Como con todos los dispositivos eléctricos, el operador debe protegerse contra la descarga electrostática (ESD, por sus siglas en inglés). El uso de las técnicas adecuadas de manejo de ESD (piso especial, correas, etc.) evitará daños potenciales a la unidad. Se recomienda firmemente eliminar toda ESD potencial durante los siguientes procedimientos:

- instalación de la unidad en un rack
- reemplazo del módulo de la fuente de alimentación

Avis, avertissements et certifications

Informations relatives aux avis, avertissements et déclarations de certification du matériel.

Avis et avertissements

Avis et avertissements de sécurité associés à l'équipement.

Avis relatif à l'alimentation

L'équipement est adapté aux systèmes d'alimentation informatiques. Connectez chaque alimentation à une source d'alimentation pour la prise en charge du basculement.

AVERTISSEMENT! Le cordon d'alimentation est utilisé comme équipement principal de déconnexion. Assurez-vous que la prise de courant est située/installée à proximité de l'équipement et qu'elle est accessible facilement.

AVERTISSEMENT! Ce produit dépend de l'installation du bâtiment en matière de protection contre les courts-circuits (surintensité). Assurez-vous qu'un fusible ou un disjoncteur ne dépassant pas 120 V c.a., 15 A aux États-Unis (240 V c.a., 10 A international) est utilisé sur les conducteurs de phase (tous des conducteurs porteurs de courant).

Avis relatif à la double alimentation

AVERTISSEMENT! Cette unité possède plus d'une connexion d'alimentation; toutes les connexions doivent être débranchées pour retirer toute alimentation de l'unité.

Avis relatif à la batterie au lithium pour le personnel de service

Ce produit contient des batteries au lithium. Si la batterie interne du module de sécurité matériel ne peut pas être entretenue sur site, la batterie du serveur peut l'être. Veuillez observer l'avertissement suivant:

ATTENTION! Danger d'explosion si la batterie est remplacée par un type incorrect. Pour le remplacement, n'utilisez que le type de batterie recommandé par le fabricant. Éliminez les batteries usagées en respectant les instructions du fabricant.

Montage en rack

Le matériel approprié est fourni avec l'équipement afin de pouvoir le monter dans un rack EIA 19" standard.

AVERTISSEMENT! Pour éviter toute blessure corporelle lors du montage ou de l'entretien de cette unité en rack, vous devez prendre des précautions spéciales pour vous assurer que le système reste stable. Les instructions suivantes sont destinées à garantir votre sécurité:

- Cette unité doit être montée en bas du rack si elle est la seule.
- Lorsque vous montez cette unité dans un rack partiellement rempli, chargez le rack du bas en haut, en plaçant le composant le plus lourd tout en bas.
- Si le rack est fourni avec des stabilisateurs, installez ces derniers avant de monter ou d'entretenir l'unité dans le rack.

ATTENTION! L'équipement monté sur rail ou glissière ne doit pas être utilisé en tant qu'étagère ou espace de travail.

Décharge électrostatique

Comme avec tous les équipements électroniques, l'opérateur doit veiller à la décharge électrostatique (ESD). L'utilisation des techniques correctes de gestion ESD (revêtements de sol ESD, bracelets antistatiques, etc.) évite les dommages potentiels que pourrait subir l'unité. Il est vivement recommandé d'éliminer les décharges électrostatiques potentielles au cours des procédures suivantes:

- Installation de l'unité dans un rack
- Remplacement d'un module d'alimentation

通知、警告、認定

ハードウェアの通知、警告、および認定に関する情報。

通知と警告

機器の安全に関する通知と警告。

電源装置に関する通知

本機器は IT 電源システムに適しています。フェールオーバーサポートに関しては、各電源装置を別の電源に接続してください。

警告 : 電源コードはメインの切断機器として使用されます。コンセントが機器の近くにあることおよび簡単に手が届くことを確認します。

警告 : 本製品の短絡保護 (過電流) は、建物に設置されている保護に依存しています。120 VAC, 15A 米国 (240 VAC, 10A 海外) 以下のヒューズまたは回路ブレーカーが、位相導体 (すべての電流導体) に使用されていることを確認します。

2 種類の電源に関する通知

警告 : 本製品は 1 種類以上の電源に接続できます。製品の電源を切断するには、すべての接続を外してください。

修理担当者へのリチウム電池に関する通知

本製品にはリチウム電池が使用されています。製品内のハードウェアセキュリティモジュール電池は現場で修理できませんが、サーバー電池は修理可能です。以下の警告に留意してください。

注意 : 正しい種類の電池と交換しないと、電池が破裂する恐れがあります。メーカーが推奨するものと同じ種類の電池のみと交換してください。使用済みの電池は、メーカーの指示に従って廃棄してください。

ラックマウント

EIA 標準の 19 インチラックに機器を取り付けるために、適切なハードウェアが付属しています。

警告 : ラックに製品を取り付けたり、ラックに取り付けられた製品を修理する際に、身体にケガをしないようにするには、システムを安定した状態に保つように特に注意する必要があります。安全を確保するために、以下のガイドラインに従ってください。

- 本製品がラックに取り付ける唯一のコンポーネントの場合、ラックの一番下に取り付ける必要があります。
- コンポーネントが一部搭載された状態のラックに本製品を取り付ける場合には、最も重いコンポーネントを一番下に取り付け、下から上へと取り付けていきます。
- ラックに安定装置が付属している場合、ラックに製品を取り付けたり、製品の修理を行う前に、安定装置を取り付けます。

注意 : スライドまたはレールに取り付けた機器は、棚や作業台として使用しないでください。

静電放電

すべての電子機器と同様に、使用者は静電放電 (ESD) から機器を保護する必要があります。適切な ESD 管理方法 (ESD フロアー、リストストラップなど) を使って、製品の破損の可能性を防ぎます。以下の手順の間に、潜在的な ESD を除去するよう強く推奨します。

- ラックに製品を取り付ける場合

- 電源モジュールを交換する場合

알림 , 경고 및 인증

하드웨어 알림 , 경고 및 인증 설명에 대한 정보

알림 및 경고

장치 관련 안전 알림 및 경고

파워 서플라이 관련 알림

이 장치는 IT 전원 시스템에 적합합니다 . 장애 조치 지원을 위해 각 파워 서플라이를 별도의 전원에 연결하십시오 .

경고 : 파워 서플라이 코드가 주된 전원 차단 장치로 사용됩니다 . 소켓 콘센트가 장비 근처에 있거나 근처에 설치하여 쉽게 접근할 수 있도록 하십시오 .

경고 : 이 제품은 건물에 설치된 단락 (과전류) 보호 기능에 의존합니다 . 상도체 (전류가 흐르는 모든 도체) 에 120VAC, 15A(미국) 또는 240VAC, 10A(미국 외 국제 표준) 이하의 퓨즈나 회로 차단기를 사용하십시오 .

듀얼 파워 서플라이 관련 알림

경고 : 이 장치에는 2 개 이상의 파워 서플라이 연결 단자가 있습니다 . 장치에서 전원을 분리하려면 모든 단자를 분리해야 합니다 .

서비스 담당자를 위한 리튬 배터리 관련 알림

이 제품은 리튬 배터리를 포함하고 있습니다 . 내부의 하드웨어 보안 모듈 배터리는 현장에서 서비스할 수 없으나 , 서버 배터리는 서비스할 수 있습니다 . 다음 경고 사항을 준수하십시오 .

주의 : 잘못된 유형의 배터리로 교체할 경우 폭발의 위험이 있습니다 . 제조사에서 권장하는 같은 유형의 배터리로만 교체하십시오 . 배터리를 폐기할 때는 제조사의 지침을 따르십시오 .

랙 장착

장치를 EIA 표준 19 ? 랙에 장착하기 위해 필요한 하드웨어가 장치와 함께 제공됩니다 .

경고 : 이 장치를 랙에 장착하거나 서비스할 때 부상을 방지하려면 시스템을 안정적으로 유지하기 위한 특별한 주의를 기울여야 합니다 . 다음은 귀하의 안전을 보장하기 위해 제공되는 지침입니다 .

- 이 장치가 랙에서 유일한 장치일 경우 랙의 하단에 장착해야 합니다 .
- 이 장치를 부분적으로 채워진 랙에 장착할 경우 , 가장 무거운 장치부터 랙의 하단부터 장착하십시오 .
- 랙에 안정화 장치가 제공될 경우, 장치를 랙에 장착하거나 서비스하기 전에 안정기를 먼저 설치하십시오.

주의 : 슬라이드 / 레일 장착 장비를 선반이나 작업 공간으로 사용해서는 안 됩니다

정전기 방전

다른 모든 전자 장치와 마찬가지로 사용자는 정전기 방전 (ESD) 에 대한 대비책을 마련해야 합니다 . 적절한 ESD 관리 기법 (바닥 접지 , 정전기 제거용 손목띠 등) 을 사용하면 장치의 잠재적인 손상을 방지할 수 있습니다 . 다음 절차 중 정전기 방전의 위험을 제거하는 것이 강력히 권장됩니다 .

- 장치를 랙에 설치
- 파워 서플라이 모듈 교체

Appendix F

OASIS KMIP Support

The KeySecure offers support for a subset of the features described in version 1.0 of the Key Management Interoperability Protocol (KMIP). To see the details of that standard, visit OASIS at:

http://docs.oasis-open.org/kmip/spec/v1.0/kmip-spec-1.0.html

Our implementation currently offers support for the following KMIP features:

KMIP Managed Object Support

- *Certificate* - A digital certificate. It is a DER-encoded X.509 public key certificate. For PGP certificates, it is a transferable public key in the OpenPGP message format.
- *Private Key* - Contains the private portion of an asymmetric key pair.
- *Public Key* - Contains the public portion of an asymmetric key pair. This is not a certificate.
- *Secret Data* - Contains a shared secret value that is not a key or certificate (e.g. a password). Composed of a secret data type and a key block. Must be in opaque format.
- *Symmetric Key* - This object is composed of a key block. Can be in raw or opaque format.
- *Template* - Contains the client-settable attributes of a managed cryptographic object. Templates are used to specify the attributes of a new managed cryptographic object in various operations and are intended to be used to specify the cryptographic attributes of new objects in a standardized, convenient way. Supported attributes are shown in the section below.

KMIP Attribute Support

- *Application Specific Information* - A structure used to store data specific to the application(s) using the managed object. The maximum length of the ASI namespace is 64 characters. The maximum ASI data length is 256 characters.
- *Certificate Type* - The type of a certificate (e.g., X.509, PGP, etc). The Certificate Type value can be set by the server when the certificate is created or registered. The Certificate Type value cannot be changed or deleted before the object is destroyed.
- *Certificate Identifier* - A structure used to provide the identification of a certificate.
- *Certificate Issuer* - A structure used to identify the issuer of a certificate, containing the Issuer Distinguished Name (i.e., from the Issuer field of the certificate).
- *Certificate Subject* - A structure used to identify the subject of a certificate.
- *Contact Information** - User-defined contact information. This information is not used for policy enforcement.
- *Cryptographic Algorithm* - The algorithm used by the object, e.g., DES, AES.
- *Cryptographic Length* - The length, in bits, of the cleartext cryptographic key material.

- *Custom Attributes* - Client- or server-defined attributes intended for vendor-specific purposes. Custom attribute structures are not supported. The following types are supported: Big Integer, Boolean, Byte String, Date-Time, Enumeration, Integer, Interval, Long Integer, Text String.
- *Digest* - Contains the digest value of the key or secret data. The KeySecure only creates a SHA-256 digest. Digest is composed of a hashing algorithm and a digest value.
- *Initial Date* - The date and time when the managed object was first created or registered by the KeySecure.
- *Activation Date* - The date and time when the Managed Cryptographic Object may begin to be used.
- *Process Start Date* - The date and time when a Managed Symmetric Key Object may begin to be used to process cryptographically-protected information (e.g., decryption or unwrapping).
- *Protect Stop Date* - The date and time when a Managed Symmetric Key Object shall not be used for applying cryptographic protection (e.g., encryption or wrapping).
- *Deactivation Date* - The date and time when the Managed Cryptographic Object shall not be used for any purpose, except for decryption, signature verification, or unwrapping, but only under extraordinary circumstances and only when special permission is granted.
- *Compromise Occurrence Date* - The date and time when the Managed Cryptographic Object was first believed to be compromised.
- *Compromise Date* - The date and time when the Managed Cryptographic Object entered into the compromised state.
- *Revocation Reason* - A structure used to indicate why the Managed Cryptographic Object was revoked (e.g., “compromised”, “expired”, “no longer used”, etc). This attribute is only set by the server as a part of the Revoke operation.
- *Link* - A link from one Managed Cryptographic Object to another, closely related Managed Cryptographic Object, for example a public and private key pair.
- *Name* - Used to identify and locate an object. This attribute is assigned by the client and is composed of a name value and a name type. KeySecure supports name type *string*.
- *Object Group** - A group of objects. An object may belong to more than one group of objects.
- *Object Type* - Describes the type of object. For example, Symmetric Key, Template, or Secret Data etc.
- *State* - The State of an object as known to the key management server. The State cannot be changed by using the Modify Attribute operation on this attribute. The state can only be changed by the server as a part of other operations or other server processes.
- *Unique Identifier* - Generated by the KeySecure to uniquely identify the managed object.

* *Contact Information* and *Object Group* will appear as custom attributes in certain sections of the Management Console.

KMIP Operations Support

- *Activate* - Requests that a managed object be activated. The request does not specify a Template object. The operation can only be performed on an object in the Pre-Active state. The operation changes the object state to Active, and sets the Activation Date to the current date and time.

The request contains the Unique Identifier of the managed object to be activated. If the Unique Identifier is not specified, then the ID Placeholder is used as the Unique Identifier.

- AddAttribute - Adds a new attribute instance or application specific information instance to a managed object and sets its value.
- *Create* - Generate a new symmetric key. Cannot be used to create a template but multiple templates can be included to simplify the key creation. Our implementation of the create operation supports application specific information, custom attributes, key lifecycle attributes, and aliases.
- *CreateKeyPair* - Generate a new asymmetric key pair. Cannot be used to create a template but multiple private key, public key, or common templates can be included to simplify the key pair creation. Our implementation of the create key pair operation supports application specific information, custom attributes, key lifecycle attributes, and aliases. If you create a KMIP Key Pair and click on one of the keys in the Key Properties dialog box, the key is identified as either a public or private key.
- *DeleteAttribute* - Deletes an attribute associated with a managed object. The object is specified by its unique identifier. Attributes are specified by their name. Any attribute that is required cannot be deleted. Our implementation of the DeleteAttribute operation supports application specific information and custom attributes.
- *Destroy* - Requests that the key material for a managed object be destroyed. Our implementation of KMIP does not retain metadata. Once the managed object is destroyed, its metadata is erased, too. KMIP object state is supported, so objects in the Active state, for example, cannot be destroyed through the KMIP interface. They can still be destroyed through the Management Console or NAE-XML protocol.
- *Get* - Requests that the server return the managed object specified by its unique identifier. Only a single object is returned. The response contains the object’s unique identifier and the object itself. Compression and wrapping are not supported.
- *GetAttributes* - Requests one or more attributes of a managed object. The object is specified by its unique identifier. Attributes are specified by their name. If the specified attribute has multiple instances, then all instances are returned. If a specified attribute does not exist, then it is not present in the returned response. If none of the attributes exist, the response consists only of the unique identifier. If no attribute name is specified in the request, the server will act as if all attributes match the request.
- *GetAttributeList* - Requests a list of the attribute names associated with the managed object. The object is specified by its unique identifier. This request supports application specific information, custom attributes, and aliases.
- *Locate* - Requests that the server search for one or more managed objects. We recommend that you use the Maximum Items field to no more than 1000. Otherwise, the response may be delayed, or the server may close the connection. Wild cards are not supported. The server supports only online objects, so if the storage-status mask excludes online object, the search returns empty. All supported attributes are valid. Date matching is supported.
- *ModifyAttribute* - Modifies the value of an existing attribute instance associated with a managed object. The object is specified by its unique identifier. The operation request contains the attribute name to be modified, the attribute index (optional), and the new value. Only existing values may be changed. If an

attribute has multiple instances, only the specified instance of the attribute is modified. If the attribute has multiple instances, and no index is specified, the index is assumed to 0. If the attribute does not support multiple instances, then an index cannot be specified.

- *Query* - Requests information about the server's capabilities and/or protocol mechanisms. The server vendor identification is *SafeNet, Inc*. We do not support any name spaces, so none are returned.
- *Register* - Requests that the server register a managed object that was created by the client or obtained by the client through some other means. Only templates, secret data, and symmetric keys are supported.
- *Revoke* - Requests to revoke a Managed Cryptographic Object or an Opaque Object. The request doesn't specify a Template object. The request contains a reason for the revocation (e.g., "key compromise", "cessation of operation", etc). Special authentication and authorization is enforced to perform this request. Only the object creator or an authorized security officer is allowed to issue this request. The operation has one of two effects. If the revocation reason is "key compromise", then the object is placed into the "compromised" state, and the Compromise Date attribute is set to the current date and time. Otherwise, the object is placed into the "deactivated" state, and the Deactivation Date attribute is set to the current date and time.