# Quantum Scalar i6000 & SafeNet KeySecure Quick Start Guide

SafeNet's KeySecure k460 servers work with Quantum's Scalar i6000 appliance server to create a KMIP-compliant encryption system. The Key Management Interoperability Protocol (KMIP®) is a specification developed by OASIS®. Its function is to standardize communication between enterprise key management systems and encryption systems.

Details about the Quantum Scalar i6000/SafeNet k460 KMIP-compliant implementation include:

- A minimum of two SafeNet KeySecure servers are required for failover purposes. A total of 10 SafeNet encryption servers are allowed, for increased failover capability.
- Data encryption keys are generated one at a time, as needed, upon request.

This document summarizes the information available in the quick start and user guides that accompany your Quantum Scalar i6000 library and SafeNet KeySecure appliances and provides step-by-step instruction for configuring the devices for combined use. For detailed information about each individual product, such as feature configuration instructions and hardware specifics, consult the following documents:

- *Scalar i6000 User's Guide*
- *Scalar i6000 User's Guide Addendum*
- *KeySecure v6.0.0 Installation Guide*
- *KeySecure v6.0.0 User Guide*

## Step 1: Install and Configure the SafeNet KeySecure

You will need the following equipment for each KeySecure:

- Null modem cable.
- Ethernet cable.
- KeySecure power cable.
- Console terminal or PC.
- Phillips Screwdriver.
- SafeNet Pin Entry Device (PED).
- 9-pin Micro-D data cable (included with the PED).
- 3 SafeNet iKeys. Apply the labels so that there is one blue, one red, and one black iKey.

During the initialization process, you must have the following information:

- An IP address for the KeySecure.
- An IP address for the SSKM. This must be on the same subnet as the KeySecure IP.
- The subnet mask for the network.
- The gateway for the network.
- A hostname for the KeySecure.
- A port on the KeySecure on which the web administration occurs. The default port is 9443.
- A port on the KeySecure on which KMIP communication occurs. We recommend port 5696, as this is the standard created by IANA.

**Secure the KeySecure** in a standard 19-inch rack that provides sufficient space at the front and rear for cabling, airflow, and maintenance.

To mount the KeySecure:

1. **Open the bezel**.
2. **Position the rack mount brackets** to align with holes in the rack posts.
3. Use a screwdriver to **start the screws** into the mounting brackets. **Do not tighten**.
4. Properly **align the device** in the rack.
5. Use a screwdriver to **tighten the screws**. This should securely attach the mounting brackets to the rack posts.
6. **Connect the null modem cable to the serial port** on the back panel of the KeySecure. Plug the other end of the null modem cable into the serial port of your console terminal or PC.
7. **Connect the ethernet cable to the ethernet interface** on the back panel of the KeySecure. Plug the other end of the ethernet cable to your network.
8. **Connect the 9-pin Micro-D data cable to the PED port** on the back of the KeySecure. Plug the other end of the data cable to the top of the PED.
9. **Connect the power cable from the power supply** on the back panel of the KeySecure to an AC power source. Unscrew the front plate to access the front panel components. Press the power switch on the front panel. Reattach the front plate. The initial boot sequence and internal configuration can take several minutes.
10. While the KeySecure performs the initial boot sequence, **start a terminal emulation session** using an application such as HyperTerminal or Minicom. Use the following port settings:
    - VT100/ANSI
    - 19200 bps
    - 8 data bits
    - No parity

- 1 stop bit
- Hardware flow control

11 The initialization process begins after you power up the KeySecure.

```
System starting up...
Release 6.0.0

Are you ready to begin setup? (y/halt): y
```

Enter `y` to continue or `halt` to abort the process. Entering `halt` shuts down the machine.

12 **Create the admin account.** You use this account to log in to the Management Console and the CLI. You can modify this account and create additional users later.

```
For further administrative access to this device you will
need an administrative account. An account called 'admin' will
be created and will be the primary administrative account.

Please enter a password for the admin account:
Please enter password again:

User 'admin' has been created.
```

Enter and confirm the password. The system creates the user if the password entries are successful.

WARNING: Remember the admin password. An administrator password can only be reset by another administrator with the appropriate access privileges. This is a fundamental security precaution. *If all administrator passwords are lost, you cannot re-configure the KeySecure. All keys and configuration data will be unrecoverable and you must return the device to have the software reinstalled.*

13 **Set the system time zone, date, and time.**

```
Please select your time zone:
1: Samoa Time Zone
2: Hawaii Time Zone
...
  Enter time zone [5]:

  Enter the local date (MM/DD/YYYY) [03/02/2011]:
  Enter the local time (HH:MM:SS) [15:40:23]:
  The time and date have now been set.
```

You can view the full list of time zones on the console. The script displays default values for the time zone, date, and time in brackets. You can accept those defaults by pressing Enter, or you can enter specific values.

14 **Set the network addresses** for the KeySecure.

```
To support network based configuration, a single IP address
is needed to bind to. Once an IP address is provided all further
configuration can be done remotely using SSH or using the Web
administration site.

Note that this will configure Ethernet #1 on your device.

Please enter the following information:
```

```
IP address:
Subnet mask [255.255.255.0]:
Default gateway [10.20.30.1]:
Hostname:

You have entered the following configuration:

    IP address: 192.168.15.25
    Subnet mask: 255.255.255.0
    Default gateway: 192.168.15.1
    Hostname: box1.company.com

Is this correct? (y/n): y

Network settings have been successfully configured.
```

Enter and confirm the IP address, Subnet mask, Default gateway, and Hostname of your KeySecure.

The script displays default values for the Subnet mask, and Default gateway in brackets. You can accept those defaults by pressing Enter, or you can enter specific values.

Note: This procedure configures ethernet port 1.

15 **Set the port number** for the Management Console.

```
Further administration of this device can be done remotely.
Please enter the port number you wish the Web administration tool
to run from. The default value is recommended.

Enter the port number [9443]:
```

Enter the port number. The script displays the default port of 9443. You can accept this default by pressing Enter, or you can enter another value.

16 **Initialize the hsm.** This requires physical access to the PED and the 3 iKeys.

```
Do you want to initialize the HSM now? (y/n): y

Luna PED operation required to initialize HSM - use Security Officer (blue)
PED key.
```

Important! When prompted to insert iKeys, there is a limited time (approx. 3 minutes) in which to insert the token. After this time period, the operation times out and the HSM initialization must occur separately from the KeySecure installation.

Note: The instructions below assume that you are using new iKeys. If overwriting or reusing existing keys, the installation options will differ, slightly, from those listed below.

17 **Insert the SO/HSM Admin (blue) iKey into the PED.** The PED displays and the corresponding actions are shown below.

```
SETTING SO PIN...
Would you like to reuse an existing keyset? (Y/N)
```

a Press No.

```
SETTING SO PIN...
M value? (1-16)
>01
```

**b** Press 1 and press Enter.

```
SETTING SO PIN...
N value? (M-16)
>01
```

**c** Press 1 and press Enter.

```
SETTING SO PIN...
Insert a SO / HSM Admin PED Key. Press ENTER.
```

**d** **Insert the SO/HSM Admin (blue) iKey** and press Enter.

```
SETTING SO PIN...
Enter new PED PIN:
```

**e** Enter a PIN value.

```
SETTING SO PIN...
Confirm new PED PIN:
```

**f** Confirm the same PIN value.

```
SETTING SO PIN...
Are you duplicating this keyset? (Y/N)
```

**g** Press No.

The KeySecure CLI displays the following message:

```
Luna PED operation required to login as HSM Administrator - use Security
Officer (blue) PED key.
```

The PED displays the following text:

```
SO LOGIN
Insert a SO / HSM Admin PED Key. Press ENTER.
```

**h** **Keep the blue iKey inserted in the PED** and press Enter.

```
SO LOGIN
Enter PED PIN:
```

**i** Enter the PIN for the SO/HSM Admin (blue) iKey and press Enter.

The KeySecure CLI displays the following message:

```
Luna PED operation required to generate cloning domain - use Domain (red)
key.
```

The PED displays the following text:

```
SETTING DOMAIN...
Would you like to reuse an existing keyset? (Y/N)
```

j Press No.

```
SETTING DOMAIN...
M value? (1-16)
>00
```

k Press 1 and press Enter.

```
SETTING DOMAIN...
N value? (M-16)
>01
```

l Press 1 and press Enter.

```
SETTING DOMAIN...
Insert a DOMAIN PED Key. Press ENTER.
```

m **Insert the Domain (red) iKey** and press Enter.

```
SETTING DOMAIN...
Enter new PED PIN:
```

n Enter a PIN value.

```
SETTING DOMAIN...
Confirm new PED PIN:
```

o Confirm the same PIN value.

```
SETTING DOMAIN...
Are you duplicating this keyset? (Y/N)
```

p Press No.

The KeySecure CLI displays the following message:

```
Luna PED operation required to create a partition - use User or
Partition Owner (black) PED key.
```

The PED displays the following text:

```
SETTING USER PIN...
Would you like to reuse an existing keyset? (Y/N)
```

q Press No.

```
SETTING USER PIN...
M value? (1-16)
>00
```

r Press 1 and press Enter.

```
SETTING USER PIN...
N value? (M-16)...
>00
```

s Press 1 and press Enter.

```
SETTING USER PIN...
Insert a USER / Partition Owner PED Key. Press ENTER.
```

t **Insert the User/Partition (black) iKey** and press Enter.

```
SETTING USER PIN...
Enter new PED PIN:
```

u Enter a PIN value.

```
SETTING USER PIN...
Confirm new PED PIN:
```

v Confirm the same PIN value.

```
SETTING USER PIN...
Are you duplicating this keyset? (Y/N)
```

w Press No.

```
USER LOGIN...
Insert a USER / Partition Owner PED Key. Press ENTER.
```

x Keep the User/Partition (black) iKey inserted in the PED and press Enter.

```
USER LOGIN...
Enter PED PIN:
```

y Enter the PIN for the User/Partition (black) iKey and press Enter.

The KeySecure CLI displays the following message:

```
Luna PED operation required to generate cloning domain on the
partition - use Domain (red) PED key.
```

The PED displays the following text:

```
SETTING DOMAIN...
Would you like to reuse an existing keyset? (Y/N)
```

z Press **Yes**. You will reuse the Domain (red) iKey you created above.

```
READING DOMAIN...
Insert a Domain PED Key. Press ENTER.
```

**aa** **Insert the Domain (red) iKey** and press Enter.

```
READING DOMAIN...
Enter PED PIN:
```

**ab** Enter the PIN for the Domain (red) iKey and press Enter.

```
READING DOMAIN...
Are you duplicating this keyset? (Y/N)
```

**ac** Press No

```
LOGIN SECRET VALUE...
MxCT-c7F9-HHX5-YtH3
Please write it down. Press Enter.
```

**ad** Write down the password displayed on the PED.

The KeySecure CLI displays the following message:

```
Do you want to set the HSM password now? (y/n): y
```

The KeySecure CLI displays the following message:

```
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.
```

**ae** **Insert the User/Partition (black) iKey** and press Enter.

```
USER LOGIN...
Enter PED PIN.
```

**af** Enter the PIN for the User/Partition Owner (black) iKey and press Enter.

The KeySecure CLI displays the following message:

```
Crypto user successful logged into the HSM
```

**18** **Configure the SSKM network interface.** Alternatively, you can configure the SSKM network interface later, using the CLI or the management console. For information about configuring the SSKM network interface after installing the KeySecure, see Chapter 3, “SSKM Interface Configuration”.

```
Do you want to configure the SSKM Network Interface now (y/n): y
IP Address (in same subnet as IP of physical interface): 192.168.15.125
Netmask: 255.255.255.0

You have entered the following configuration:
    IP address: 192.168.15.125
    Subnet mask: 255.255.255.0

Is this correct? (y/n): y
Network Templates generated OK
IP address 192.168.15.125 scheduled for assignment to SSKM
```

```
Warning: If SSKM is not started soon, IP 192.168.15.125 may become stale
SUCCESS: Configured network interface with ip=192.168.15.125,
netmask=255.255.255.0 and interface=eth0
Start SSKM now? (y/n): y

SUCCESS: SSKM Started OK
```

Note: The SSKM can only be started when the HSM is initialized. If you defer the HSM initialization, you can configure the SSKM interface, but you must start the SSKM after initializing the HSM. To start the SSKM use the you cannot start the SSKM, though you can configure it.

*At this point, you've given the installation program everything it needs.*

The KeySecure creates a DSA key, an RSA key, and a Web Admin certificate. These keys are used to authenticate the KeySecure to users making SSH and Web Admin connections to the KeySecure. Because the actual key is fairly large, the KeySecure displays the key fingerprint on the console.

```
Creating certificate for Web administration server...
Creating certificate for signing logs...
Creating SSH host keys...

SSH RSA key fingerprint:
2048 41:63:d3:ca:c9:ea:1f:f7:a1:84:8b:05:b4:a6:3b:64
SSH DSA key fingerprint:
2048 1d:04:d7:02:60:d5:f2:11:30:12:0a:d9:bb:19:c2:fe
Webadmin certificate fingerprint (SHA-256):
1024 ad:8b:9f:79:5f:de:88:a0:89:36:d6:51:cd:0a:7f:ff:
d3:88:cd:7a:4a:f0:95:b8:21:b7:19:21:3c:71:39:c1

Initializing the key store. This could take several minutes.
waiting for the server to shut down.... done
server stopped

Starting services...

The Web-based Management Console will now be available at this URL:
<https://192.168.15.25:9443>

This device has now been configured.
Press Enter to continue.
```

Tip: To prevent a "man in the middle" attack when connecting to the KeySecure, we recommend that you write down these fingerprints and compare them with what is presented when you connect to the KeySecure via SSH or HTTPS.

19 At the end of this configuration process, **setup is complete** and you can log into the KeySecure via the Management Console or the CLI.

```
YourDevice login: admin
Password: ******
YourDevice#
```

Use your admin username and password to log in to the system.

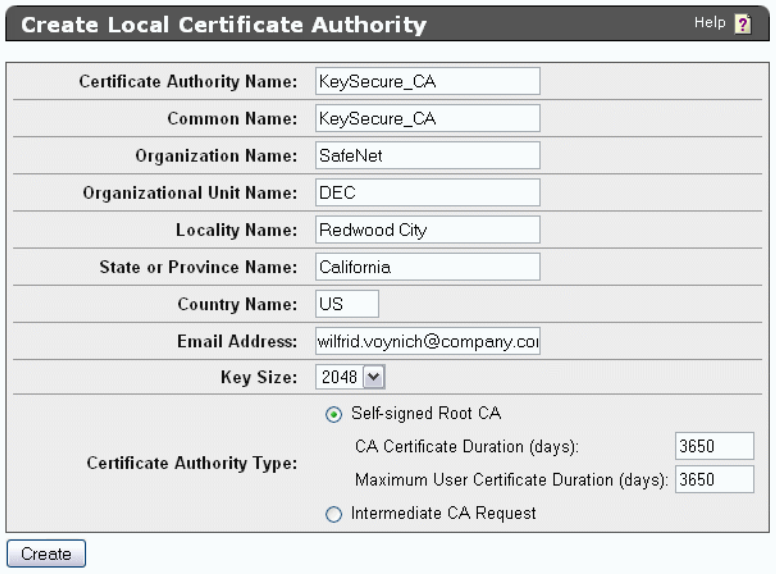
# Step 2: Create a Local CA on the KeySecure

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.

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: | KeySecure_CA |
| Common Name: | KeySecure_CA |
| Organization Name: | SafeNet |
| Organizational Unit Name: | DEC |
| Locality Name: | Redwood City |
| State or Province Name: | California |
| Country Name: | US |
| Email Address: | wilfrid.voynich@company.co |
| Key Size: | 2048 |
| Certificate Authority Type: | ● Self-signed Root CA<br>CA Certificate Duration (days): 3650<br>Maximum User Certificate Duration (days): 3650<br>○ 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**.

Note: To integrate with the Quantum Scalar i6000, the CA's **Key Size** must be 2048.

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.

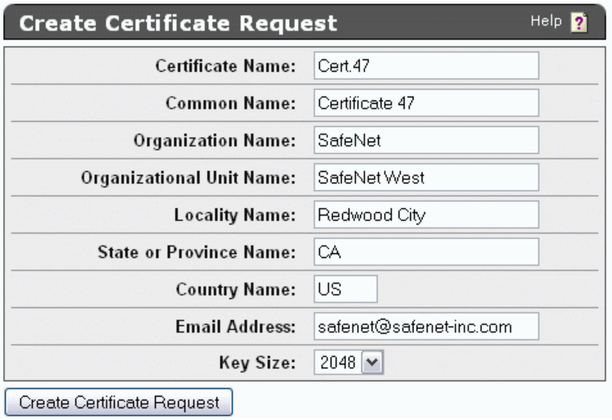
When creating an intermediate CA request, you must also specify a Maximum User Certificate Duration *when installing the certificate response*. This duration cannot be longer than the signing CA's duration.

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

# Step 3: Create a Server Certificate on the KeySecure

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).

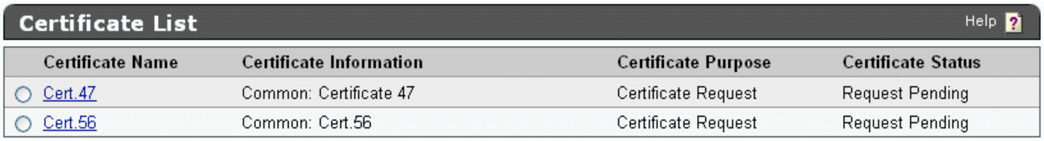


**Create Certificate Request**

| | |
|---|---|
| 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.

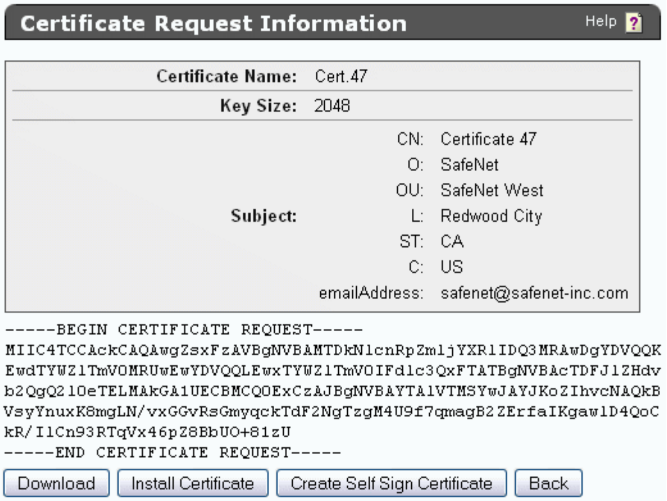
3 Click **Create Certificate Request**. The request appears in the list with a status of *Request Pending*.



**Certificate List**

| Certificate Name | Certificate Information | Certificate Purpose | Certificate Status |
|---|---|---|---|
| ○ Cert.47 | Common: Certificate 47 | Certificate Request | Request Pending |
| ○ Cert.56 | Common: Cert.56 | Certificate Request | Request Pending |

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



**Certificate Request Information**

| | | |
|---|---|---|
| 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
VsyYnuxK8mgLN/vxGGvRsGmyqckTdF2NgTzgM4U9f7qmagB2ZErfaIKgawlD4QoC
kR/IlCn93RTqVx46pZ8BbUO+81zU
-----END CERTIFICATE REQUEST-----
```

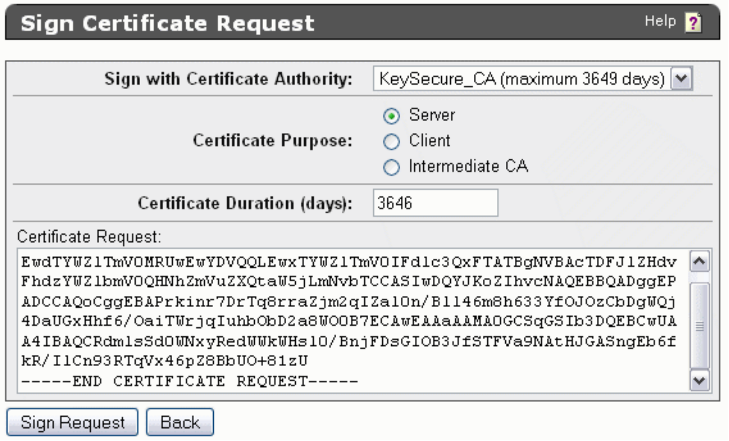
5 Copy the certificate request text. The certificate text looks similar, but not identical, to the following text.

```
-----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 CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----), and copy 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 Certificate Request**

Sign with Certificate Authority: KeySecure_CA (maximum 3649 days)

Certificate Purpose: ● Server ○ Client ○ Intermediate CA

Certificate Duration (days): 3646

Certificate Request:

```
EwdTYWZlTmVOMRUwEwYDVQQLEwxTYWZlTmVOIFdlc3QxFTATBgNVBAcTDFJlZHdv
FhdzYWZlbmVOQHNhZmVuZXQtaW5jLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAPrkinr7DrTq8rraZjm2qIZalOn/Bl146m8h633YfOJOzCbDgWQj
4DaUGxHhf6/OaiTWrjqIuhbObD2a8WOOB7ECAwEAAaAAMAOGCSqGSIb3DQEBCwUA
A4IBAQCRdmlsSdOWNxyRedWWkWHslO/BnjFDsGIOB3JfSTFVa9NAtHJGASngEb6f
kR/IlCn93RTqVx46pZ8BbUO+81zU
-----END CERTIFICATE REQUEST-----
```

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

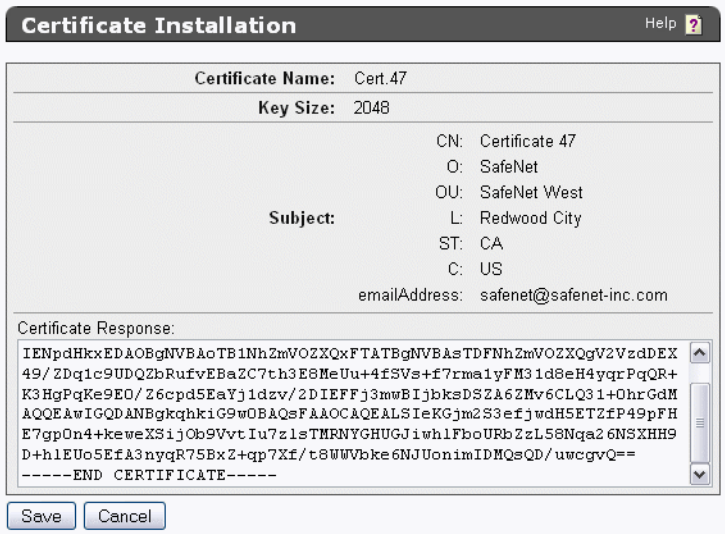
9 Select *Server* as the **Certificate Purpose**, specify a **Certificate Duration** and click **Sign Request**. The newly-activated certificate displays on a new page.

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<br>O: SafeNet<br>OU: SafeNet West<br>L: Redwood City<br>ST: CA<br>C: US<br>emailAddress: safenet@safenet-inc.com |

Certificate Response:

```
IENpdHkxEDAOBgNVBAoTB1NhZmVOZXQxFTATBgNVBAsTDFNhZmVOZXQgV2VzdDEX
49/ZDq1c9UDQZbRufvEBaZC7th3E8MeUu+4fSVs+f7rma1yFM31d8eH4yqrPqQR+
K3HgPqKe9EO/Z6cpd5EaYj1dzv/2DIEFFj3mwBIjbksDSZA6ZMv6CLQ31+OhrGdM
AQQEAwIGQDANBgkqhkiG9w0BAQsFAAOCAQEALSIeKGjm2S3efjwdH5ETZfP49pFH
E7gpOn4+keweXSijOb9VvtIu7zlsTMRNYGHUGJiwhlFboURbZzL58Nqa26NSXHH9
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.

# Step 4: Create a Client Certificate for the i6000

Note: The i6000's client certificate must be a RSA-1024 certificate for which the i6000 must have the private key. Because the client must have the private key, the certificate request can't be created on the KeySecure. Below are the instructions for creating the certificate request in OpenSSL, though you may use another certificate creation tool if desired. The certificate request must be signed by the KeySecure's CA, as described in the steps below.

To create a client certificate for the i6000 using OpenSSL:

1 In OpenSSL, execute the following command:

```
openssl req -newkey rsa:1024 -keyout qtmkey.pem -out qtmkey.csr -outform PEM
```

2 Respond to the prompts to complete the certificate request.

```
Generating a 1024 bit RSA private key
..++++++
.............................++++++
writing new private key to 'ClientKey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:Redwood City
Organization Name (eg, company) [My Company Ltd]:SafeNet
Organizational Unit Name (eg, section) []:DEC
Common Name (eg, your name or your server's hostname) []:Tycho Brahe
Email Address []:tycho.brahe@safenet-inc.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:asdf1234
An optional company name []:
```

3 Open the certificate request in a text editor. Copy the text.

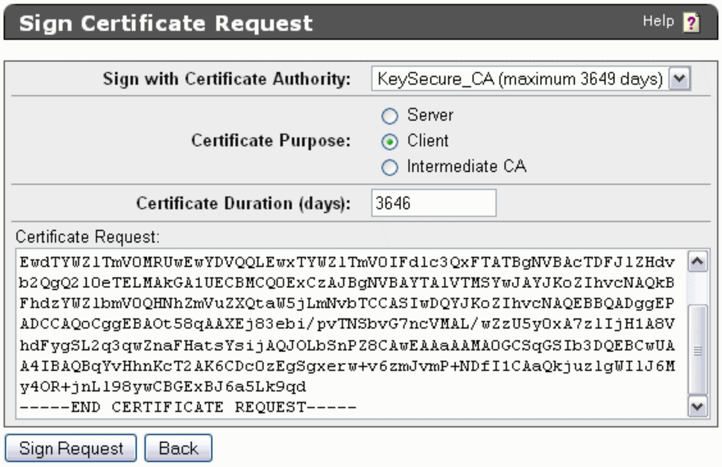
4 Copy the certificate request text. The certificate text looks similar, but not identical, to the following text.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBmzCCAQQCAQAwWzEPMA0GA1UEAxMGZmxldGNoMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEJM
AcGA1UEBxMAMQkwBwYDVQQIEwAxCzAJBgNVBAYTAlVTMQ8wDQYJKoZIhvcNAQkBFgAwgZ8wDQ
YJKoZIhvcAYBABTUxxgY0AMIGJAoGBAMUqA1t4m&Nm0sCcUqnt5Yug+qTSbgEFnvnYWUApHKD
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.

5 Navigate to the Local Certificate Authority List section in the KeySecure's Management Console (Security >> Local CAs).

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



**Sign Certificate Request**

Sign with Certificate Authority: KeySecure_CA (maximum 3649 days)

Certificate Purpose:
○ Server
● Client
○ Intermediate CA

Certificate Duration (days): 3646

Certificate Request:

```
EwdTYWZlTmVOMRUwEwYDVQQLEwxTYWZlTmVOIFdlc3QxFTATBgNVBAcTDFJlZHdv
b2QgQ2l0eTELMAkGA1UECBMCQ0ExCzAJBgNVBAYTAlVTMSYwJAYJKoZIhvcNAQkB
FhdzYWZlbmVOQHNhZmVuZXQtaW5jLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAOt58qAAXEj83ebi/pvTNSbvG7ncVMAL/wZzU5y0xA7zlIjH1A8V
hdFygSL2q3qwZnaFHatsYsijAQJOLbSnPZ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUA
A4IBAQBqYvHhnKcT2AK6CDcOzEgSgxerw+v6zmJvmP+NDfI1CAaQkjuzlgWIlJ6M
y4OR+jnLl98ywCBGExBJ6a5Lk9qd
-----END CERTIFICATE REQUEST-----
```

7 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.

8 Click **Download** to download the certificate to your client. The file will be named signed.crt.

9 Click **Back** to return to the Local Certificate Authority List, select the CA and click **Download** to download a copy of the CA certificate to your client. In this example, the file will be named KeySecure_CA.crt.

10 Bundle the client certificate in PKCS12 format using the following openssl command:

```
openssl pkcs12 -export -in signed.crt -inkey qtmkey.pem -out qtmbundle.p12
```

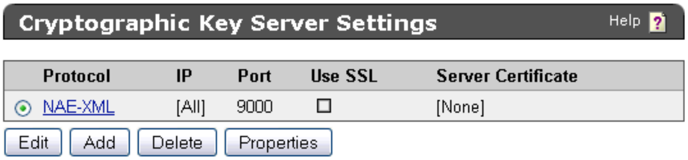
```
Enter pass phrase for qtmkey.pem:
Enter Export Password:
Verifying - Enter Export Password:
```

The client certificate and the Local CA certificate will be imported to the Scalar i6000 library in step 8.

## Step 5: Configure the KMIP Server on the KeySecure

To configure the KMIP server settings:

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



Cryptographic Key Server Settings

| | 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**.

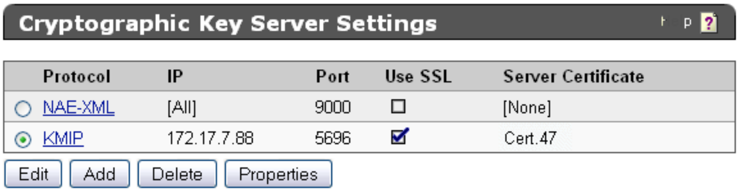
4 Select either *[All]* or a specific IP address for **IP**.

5 Select the **Port**. We recommend *5696*.

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**.

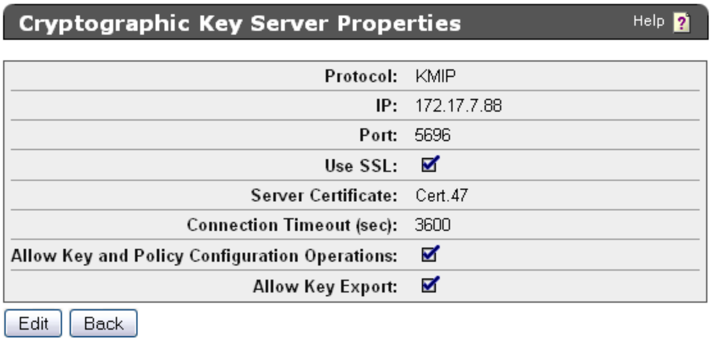


Cryptographic Key Server Settings

| | Protocol | IP | Port | Use SSL | Server Certificate |
|---|---|---|---|---|---|
| ○ | NAE-XML | [All] | 9000 | □ | [None] |
| ● | KMIP | 172.17.7.88 | 5696 | ☑ | Cert.47 |

9 Select the KMIP link.

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



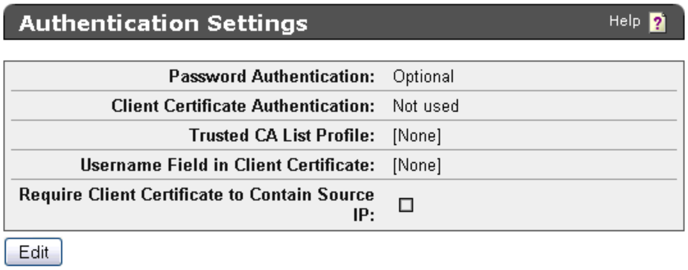
Cryptographic Key Server Properties

| | |
|---|---|
| Protocol: | KMIP |
| IP: | 172.17.7.88 |
| Port: | 5696 |
| Use SSL: | ☑ |
| Server Certificate: | Cert.47 |
| 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 5696 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. KMIP clients must provide certificates to connect to the KeySecure, which means the KeySecure must have access to signing CA to verify the certificate.



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 two options:
  - *Optional* - (default) 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 two options.
  - *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.

The KeySecure is now ready to manage keys and can handle requests that come through the KMIP Interface.

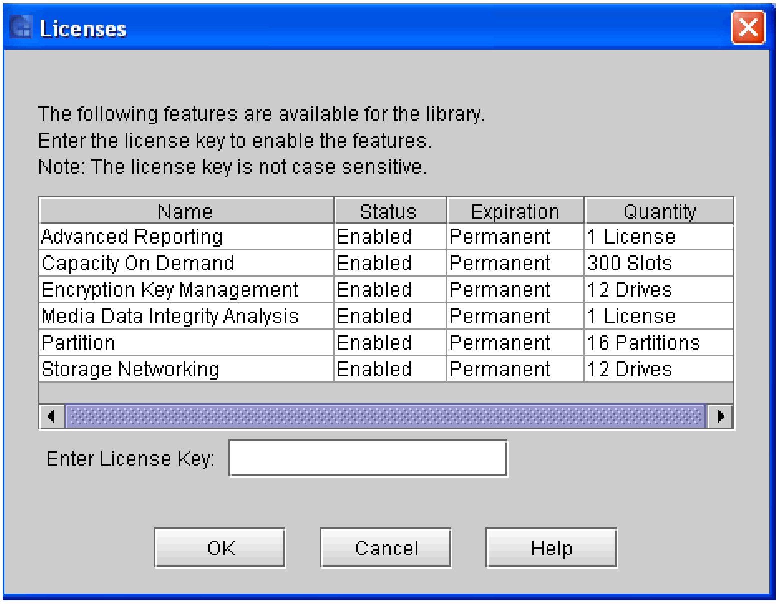
# Step 6: Install the Encryption Key Management License

To install the encryption key management license:

1 Log on to the Scalar i6000 library as an administrator, if you are not currently viewing the physical library.

2 Click **Setup > Licenses**.

The Licenses dialog box appears.



Licenses

The following features are available for the library.
Enter the license key to enable the features.
Note: The license key is not case sensitive.

| Name | Status | Expiration | Quantity |
|---|---|---|---|
| Advanced Reporting | Enabled | Permanent | 1 License |
| Capacity On Demand | Enabled | Permanent | 300 Slots |
| Encryption Key Management | Enabled | Permanent | 12 Drives |
| Media Data Integrity Analysis | Enabled | Permanent | 1 License |
| Partition | Enabled | Permanent | 16 Partitions |
| Storage Networking | Enabled | Permanent | 12 Drives |

Enter License Key:

This dialog box lists the licensed features for your library, plus Status, Expiration, and Quantity. **Quantity** refers to the number drives licensed to use this feature.

3 In the **Enter License Key** box, type the appropriate license key.

- License keys are not case sensitive and are all-inclusive. For example, J2BGL-22622-52C22 can be entered as j2bgl-22622-52c22.
- If you are using the library's touch screen, enter the library key from the lowercase keyboard, which gives you access to the dash (-) character.
- If you cannot locate the license keys shipped with the library, you can obtain them by contacting technical support or, if you are an end user, by contacting your inside sales representative.

4 Click **OK**.

# Step 7: Install Required Drives and Drive Firmware

To install the required drive firmware:

1. If not already installed, install HP LTO-4 and/or LTO-5 Fibre Channel tape drives in the partition(s) you will be using for library-managed encryption.
2. Unload all tape cartridges from these tape drives.
3. On the tape drives, install the latest version of firmware that is qualified for the library firmware installed on your library. Refer to the *Scalar i6000 Release Notes* for the correct version of tape drive firmware.

# Step 8: Install the Root and Client Certificates in the Library

Transport Layer Security (TLS) communication certificates are unique certificates that must be installed on the library in order for the library to communicate securely with attached SafeNet KeySecures. TLS certificates (the client and CA certificates) will be provided by your SafeNet server administrator.

Your server administrator should provide the following certificates:

- Root Certificate, also called the CA certificate, or Certificate Authority Certificate (KeySecure_CA.crt from the example above)
- Client Certificate (qtmbundle.p12 from the example above)

These files must be in the proper format, as follows. If any of the following requirements is not met, neither of the certificates will be imported.

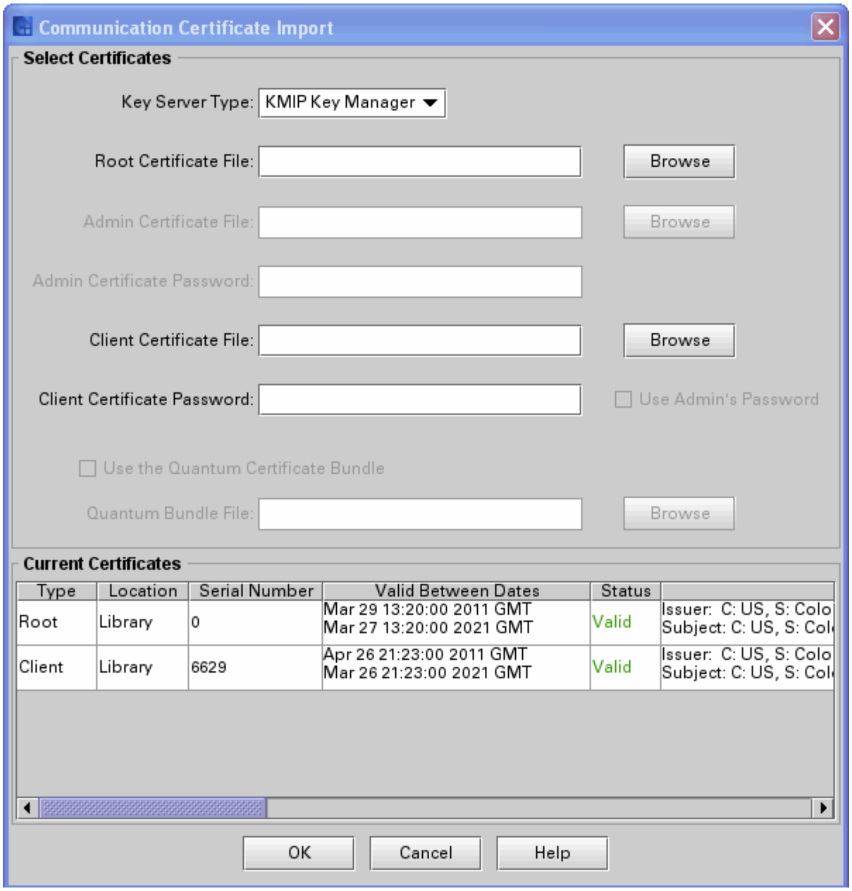
- The Root Certificate must be 2048 bits and be in PEM format.
- The Client certificate must be 1024 bits and be in pkcs12 (.p12) format.

  Note: The .p12 format combines the public/private key pair files in .pem file format and password protects access to such .pem certificate files.
- The Client certificate must be signed by the Root Certificate.
- Certificates must have the Organization name (O) set in their Issuer and Subject info.
- The same Root Certificate must be installed on the encryption key servers and the library.
- All the certificates must have a valid validity period according to the date and time settings on the encryption key server.

Follow the steps below to install the certificates.

1. Place the certificate files in an accessible location on your computer.
2. From the library **Tools** menu, select **EKM Management > Import Communication Certificates.**

   The **Communication Certificate Import** dialog box appears. If no certificates are installed, then nothing will be listed under **Current Certificates**. If certificates are already installed, then any certificates you install will overwrite the currently installed certificates.



Communication Certificate Import

Select Certificates

Key Server Type: KMIP Key Manager

Root Certificate File: Browse

Admin Certificate File: Browse

Admin Certificate Password:

Client Certificate File: Browse

Client Certificate Password: □ Use Admin's Password

□ Use the Quantum Certificate Bundle

Quantum Bundle File: Browse

Current Certificates

| Type | Location | Serial Number | Valid Between Dates | Status | |
|---|---|---|---|---|---|
| Root | Library | 0 | Mar 29 13:20:00 2011 GMT<br>Mar 27 13:20:00 2021 GMT | Valid | Issuer: C: US, S: Colo<br>Subject: C: US, S: Col |
| Client | Library | 6629 | Apr 26 21:23:00 2011 GMT<br>Mar 26 21:23:00 2021 GMT | Valid | Issuer: C: US, S: Colo<br>Subject: C: US, S: Col |

OK Cancel Help

3 From the Key Server Type drop-down list, select **KMIP Key Manager**.

Note: Some of the fields will be disabled.

4 Click **Browse** to retrieve the **Root Certificate File**.

5 Click **Browse** to retrieve the **Client Certificate File**.

6 In the **Client Certificate Password** field, type the password used when generating the certificate files (your server administrator should provide this).

7 Click **OK**.

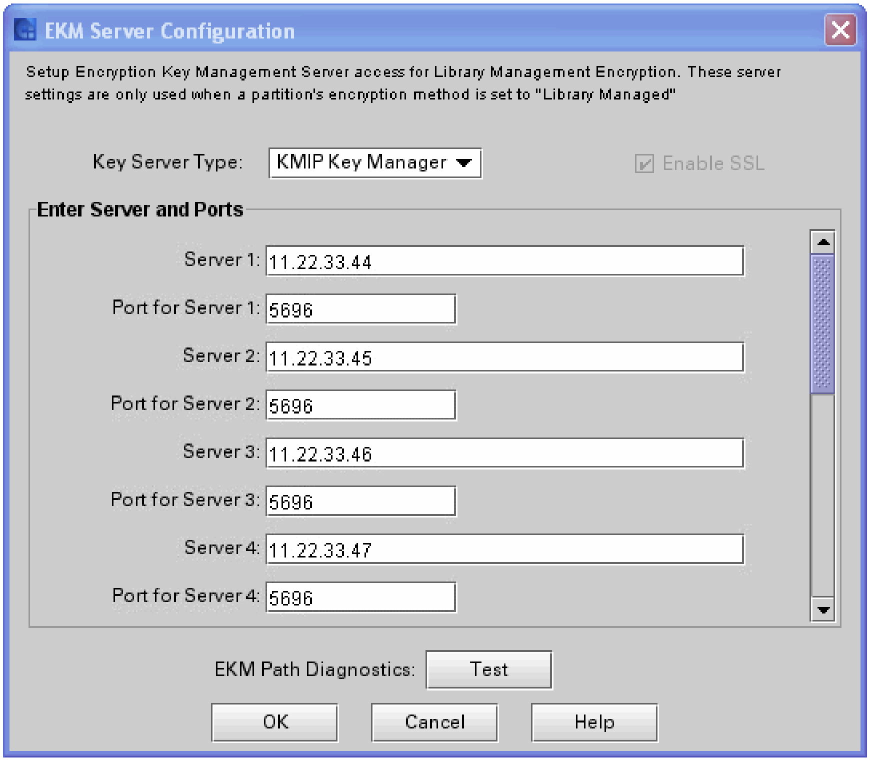
8 Verify that the certificates are installed. They will be listed in the table under **Current Certificates**. (You may need to go back to the screen by selecting **Tools** > **EKM Management > Import Communication Certificates**).

# Step 9: Configure Library Access to the SafeNet KeySecure

To configure the library access to the SafeNet KeySecure:

1 From the menu bar, click **Setup** > **Encryption** > **Server Configuration**.

The **EKM Server Configuration** dialog box appears.



EKM Server Configuration

Setup Encryption Key Management Server access for Library Management Encryption. These server settings are only used when a partition's encryption method is set to "Library Managed"

Key Server Type: KMIP Key Manager

☑ Enable SSL

Enter Server and Ports

Server 1: 11.22.33.44

Port for Server 1: 5696

Server 2: 11.22.33.45

Port for Server 2: 5696

Server 3: 11.22.33.46

Port for Server 3: 5696

Server 4: 11.22.33.47

Port for Server 4: 5696

EKM Path Diagnostics: Test

2 From the **Key Server Type** drop-down list, select **KMIP Key Manager**.

3 Fill in the rest of the fields as follows:

For the server IP address, you can enter the following:

- IPv4 address
- IPv6 address—if IPv6 is configured
- Domain name—if DNS is configured

Note: Assign your SafeNet KeySecures on this screen in the order in which you want failover to occur. Server 1 is the primary server; Server 2 is the secondary server; and so on. For an initial key request, the library tries Server 1 (the primary server) first. If Server 1 is not available to perform a key request, the library tries Server 2. If server 2 is not available, the library will try Server 3, and so on, in order, until it finds a server that can perform the request. Once found, this server remains the active server until it fails a key request or the library is rebooted. At that point, the library starts over and uses Server 1 for key requests. If Server 1 is not available, it will try Server 2, and so on.

a **Enable SSL** - The check box is checked automatically and the field is disabled.

b **Server 1** - Type the IP address or domain name of the primary SafeNet KeySecure.

c **Port for Server 1** - Accept the default or type the applicable port. The default port number is 443.

Note: The port number must match the port number on the primary SafeNet KeySecure.

d **Server 2** - Type the IP address or domain name of the secondary SafeNet KeySecure.

e **Port for Server 2** - Accept the default or type the applicable port number. The port number must match the port number on the secondary SafeNet KeySecure.

WARNING: **Do not use port 443**. Port 443 will not allow keys to be served. If port 443 is configured on the SafeNet KeySecure, you must change it.

f Repeat Step d and Step e for up to eight additional SafeNet KeySecures, in the order in which you would like failover to occur. The port number listed in each **Port** field must match the port number used on that SafeNet KeySecures.

g **Key Class** - This field is not applicable.

4 Test the settings by clicking the EKM Path Diagnostics **Test** button.

The **Path Diagnostic Results** dialog box appears. If all the tests do not pass, troubleshoot until they all pass. For more information on EKM Path Diagnostics, see *Scalar i6000 User's Guide.*

5 Click **Close**.

6 Click **OK**.

An **Operation in Progress** dialog box appears, indicating the settings are being modified. Upon successful completion, the system returns to the main console.

7 Ensure all ports corresponding to the SafeNet KeySecures are open on your firewall to allow the library to connect to the servers.

## Step 10: Configure Partitions for Library-Managed Encryption

In order to use the library to manage encryption on your SafeNet KeySecures, you must configure the partitions for library-managed encryption. Encryption on the Scalar i6000 library is enabled by partition only. You cannot select individual drives for encryption; you must select an entire partition for encryption.

There are two encryption methods available on the library:

- **Allow Application Managed** — Allows your host application to provide encryption support on all encryption-capable tape drives and media within the partition. This is the default setting if the partition contains encryption-capable tape drives. If you select this option, the library will not communicate with the key server on this partition. If you want an application to manage encryption, you must specifically configure the application to do so. The library will not participate in performing encryption. See your host documentation for further details.

- **Enable Library Managed** — Enables library managed encryption support via a connected key manager server for all tape drives and encryption-capable media assigned to the partition. This is the method you want to use for library communication with SafeNet KeySecures.

  Details and restrictions for using library managed encryption include:

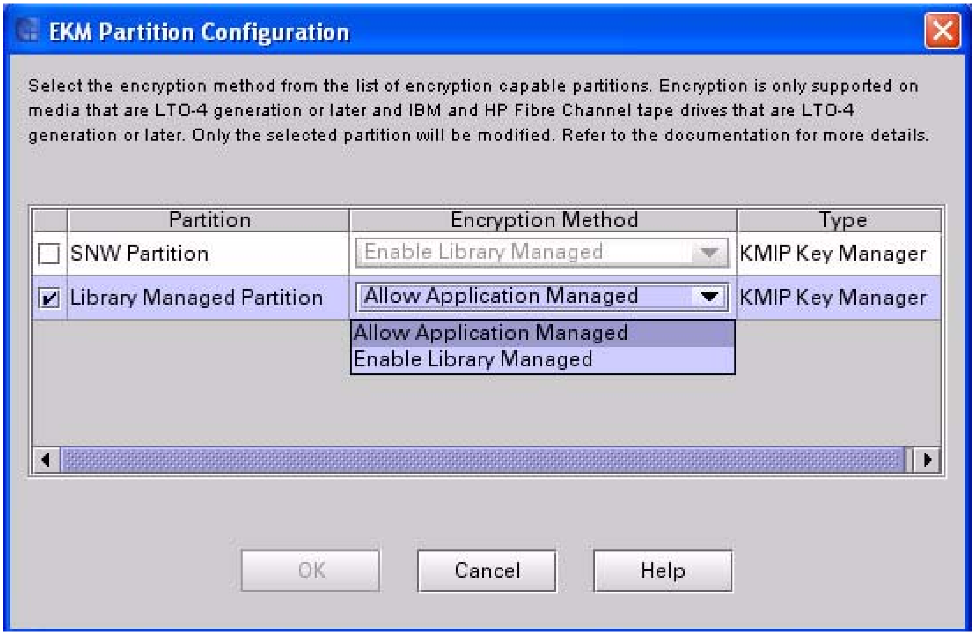
  - Only LTO-4 and LTO-5 tape cartridges will be encrypted in library managed encryption partitions, unless they contain unencrypted data already, and data is appended. The partition may contain LTO-2 and LTO-3 tape cartridges, but they will not be encrypted.
  - Encrypted data will never be appended to unencrypted data on tape, and unencrypted data will never be appended to encrypted data on tape.
  - For data to be encrypted via library managed encryption, the media must be blank or have been written to using library managed encryption at the first write operation at the beginning of tape (BOT). If the media was previously written in a non-encrypted format, all data subsequently written to it will continue to be non-encrypted.
  - Data stored on tape cartridges will not be encrypted with more than one encryption key.

### Changing the Encryption Method

1 If you are not already viewing the physical library, click **View** and select the name of the physical library.

2 Click **Setup > Encryption > Partition Configuration**.

The **EKM Partition Configuration** dialog box appears. Each partition's current encryption method is listed under Encryption Method.



EKM Partition Configuration

Select the encryption method from the list of encryption capable partitions. Encryption is only supported on media that are LTO-4 generation or later and IBM and HP Fibre Channel tape drives that are LTO-4 generation or later. Only the selected partition will be modified. Refer to the documentation for more details.

| | Partition | Encryption Method | Type |
|---|---|---|---|
| □ | SNW Partition | Enable Library Managed | KMIP Key Manager |
| ☑ | Library Managed Partition | Allow Application Managed | KMIP Key Manager |

3 Make sure that the tape drives in the partition do not have cartridges loaded. If there are cartridges in the tape drives, you cannot change the encryption method.

4 Select the check box for the partition whose encryption method you want to change.

5 Change the encryption method by selecting **Enable Library Managed** from the Encryption Method drop-down list:

Note: If you change a partition from Enable Library Managed to Allow Application Managed, any encrypted data that was written to the tapes while the partition was configured for library managed encryption can no longer be read, until you change the partition back to Enable Library Managed.

6 Click **OK**.

The dialog box closes and you are returned to the main console.

If the partition encryption settings were not successfully configured, follow the screen instructions to resolve any issues that occurred during the process.

When you are finished configuring the library, save the library configuration (**Tools > Save/Restore)**.

### Using EKM Path Diagnostics

EKM Path Diagnostics is a series of short tests performed by the library to determine if the EKM servers are connected and operating properly.

You can perform EKM Path Diagnostics tests manually at any time, or automatically in the background at regular intervals:

- **Manual** — You can perform manual EKM Path Diagnostics at any time by clicking the **Test** button on the EKM server setup screen (**Setup > Encryption > Server Configuration**).
- **Background** — The library is configured to automatically perform background EKM Path Diagnostics tests at regularly scheduled intervals and notify you via RAS tickets if any problems arise. To do this, go to **Setup > Physical Library**. Under **EKM Path Diagnostics**, select the **Enable** check box.

  Note: Background EKM Path Diagnostics is always enabled. You cannot disable it.

The tests performed are:

- **Ping** — Verifies the Ethernet communication between the library and the key servers.
- **Path** — Verifies that EKM/RKM/KMIP services are running on the key servers.
- **Config** — Verifies that the key servers are capable of serving encryption keys.