KMIP installation Guide

DataSecure and KeySecure
Version 6.1.2

© 2012 SafeNet, Inc.
007-012120-001

Introduction

This guide provides you with the information necessary to configure the KMIP server on the KeySecure or DataSecure, including guidance about setting up SSL communication between the KMIP server and your KMIP clients.

This guide is intended primarily for network administrators who will be responsible for the installation and maintenance of the KeySecure or DataSecure. It is assumes that the KeySecure or DataSecure has already been physically installed, and that the device has already been initialized as described in the Quick Start Guide.

This document provides some examples and illustrations referring to the KeySecure and its Management Console; however, the fundamental information and instructions apply to the DataSecure environment as well.

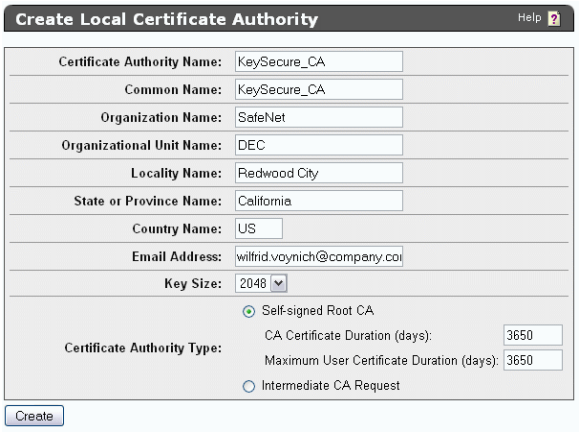
Configure the KMIP server

The KMIP interface operates over SSL, so configuration involves creating a local Certificate Authority (CA) on the KeySecure or DataSecure, creating server and client certificates, and configuring the KMIP server settings.

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).



3. Enter the issuer information (**Certificate Authority Name**, **Common Name**, etc.) and the **Key Size**. The KeySecure or DataSecure supports 2048-, 3072-, and 4096-bit keys.

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**. You must then add the root CA to the trusted CA list for it to be recognized by the KMIP 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 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 local CA on the KeySecure or DataSecure.

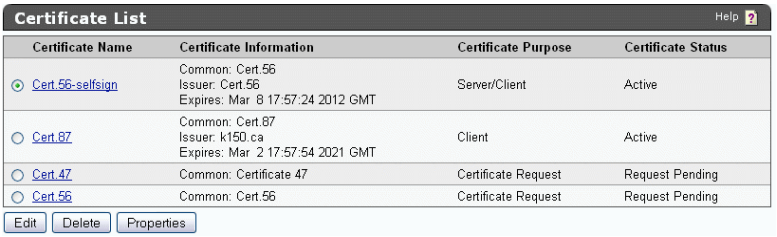
Create a server certificate

To create a server certificate:

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

2. Enter the issuer information (**Certificate Name**, **Common Name**, etc.) and the **Key Size**. The KeySecure supports 728-, 1024-, 2048-, 3072-, and 4096-bit keys.

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



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

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

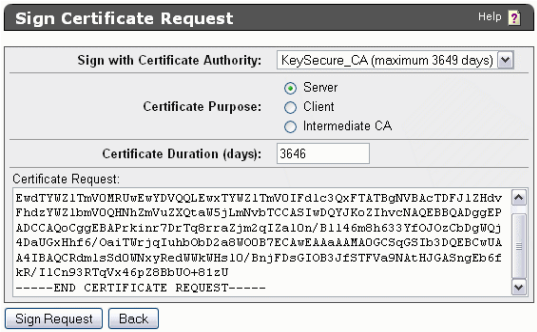
   ```
   -----BEGIN CERTIFICATE REQUEST-----
   MIIBmzCCAQQCAQAwWzEPMA0GA1UEAxMGZmxldGNoMQkwBwYDVQQKEwAx
   CTAHBgNVBAsTADEJMAcGA1UEBxMAMQkwBwYDVQQIEwAxFfeDK2Zqh0Fn
   fTHXAkHrj4JP3MCMF5nKHgOSRVmImNHHy0cYKTDP+hor68R76XhLVapK
   MqjNWXmg==
   -----END CERTIFICATE REQUEST-----
   ```

   IMPORTANT! Be sure to include the first and last lines `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----`.

   Copy only the text in the certificate. Do not copy extra white space.

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

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



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

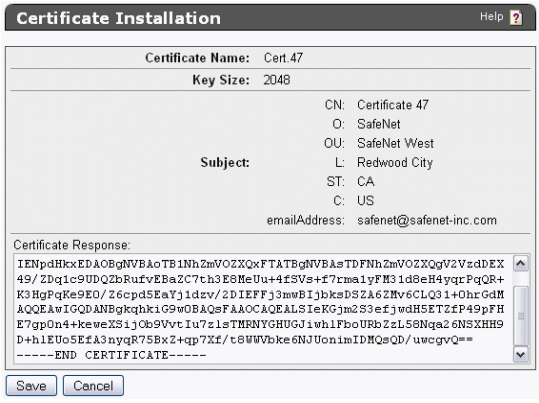
9. Select *Server* as the **Certificate Purpose**, specify a **Certificate Duration** and click **Sign Request**. The newly-activated certificate displays on a new page.

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**.



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 to establish SSL connections with client applications.

Create a client certificate

There are many certificate creation methods available to you for creating your client certificate. Because you cannot create the client certificate on the KeySecure or DataSecure (you won't be able to download the private key), you must create the client certificate elsewhere. The client certificate must be signed by the CA for the KeySecure or DataSecure. The procedure for doing this using the Management Console is described below.

To create a client certificate using OpenSSL:

1. In OpenSSL, execute the following command:

   ```
   openssl req –newkey rsa:1024 –keyout ClientKey.pem –out req.pem –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.

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBmzCCAQQCAQAwWzEPMA0GA1UEAxMGZmxldGNoMQkwBwYDVQQKEwAx
CTAHBgNVBAsTADEJMAcGA1UEBxMAMQkwBwYDVQQIEwAxTNHHy0cYKTuV
1Ce8nvvUG+yp2Eh8aJ7thaua41xDFXPmIEXTqzXi1++DCWAdWaysojPC
ZugY7jNWXmg==
-----END CERTIFICATE REQUEST-----
```

IMPORTANT! Be sure to include the first and last lines `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----.`

Copy only the text in the certificate. Do not copy extra white space.

5. Navigate to the Local Certificate Authority List section in the KeySecure or DataSecure Management Console (Security >> Local CAs).
6. Select a CA and click **Sign 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.

   At this point, adhere to your organization's policy for installing client certificates.

To create a client certificate using Java Keytool:

1. Open a command prompt window on your client and navigate to the Java security directory (<Java_Home>\lib\security).
2. Generate a public/private key paid by issuing the command below. You create an alias for the key pair at this time:

   ```
   keytool –keystore <KeyStoreName> -genkey –alias
   <KeyPairAlias> -keyalg RSA
   ```

   The key generation process will then request the following data:

   - A keystore password.
   - The distinguished name. This is a series of values that are incorporated into the certificate request. These values include country name, state or province name, city or locality name, organization name, organizational unit name, and the user's first and last name.
   - The key password. The certificate password must be the same as the keystore password. You can simply press Return to set the password. You need not retype the keystore password.
3. Create the certificate request by issuing the command below. Reference the Key Pair Alias you created above.

   ```
   keytool –certreq –alias <KeyPairAlias> -file
   <CertReqFileName> -keystore <KeystoreName>
   ```

   The certificate request is in the <CertReqFileName> file.

4. Open the certificate request in a text editor.
5. Copy the certificate request text. The certificate text looks similar, but not identical to the following:

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   MIIBmzCCAQQCAQAwWzEPMA0GA1UEAxMGZmxldGNoMQkwBwYDVQQKEwAx
   CTAHBgNVBAsTADEJMAcGA1UEBxMAMQkwBwYDVQQIEwAxTNHHy0cYKTuV
   1Ce8nvvUG+yp2Eh8aJ7thaua41xDFXPmIEXTqzXi1++DCWAdWaysojPC
   ZugY7jNWXmg==
   -----END CERTIFICATE REQUEST-----
   ```

   IMPORTANT! Be sure to include the first and last lines `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----.`

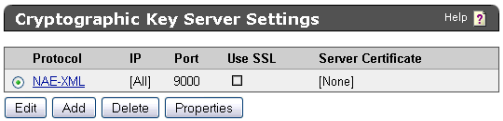
   Copy only the text in the certificate. Do not copy extra white space.
6. Navigate to the Local Certificate Authority List section in the Management Console (Security >> Local CAs).
7. Select a CA and click **Sign Request**.
8. Paste the certificate request into the **Certificate Request** field. Select *Client* as the **Certificate Purpose**, specify a **Certificate Duration** and click **Sign Request**. The newly-activated certificate displays on a new page.
9. Click **Download** to download the certificate to your client.

   At this point, adhere to your organization's policy for installing client certificates.

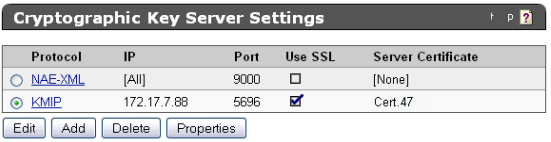
Configure the KMIP server settings

To configure the KMIP server settings:

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

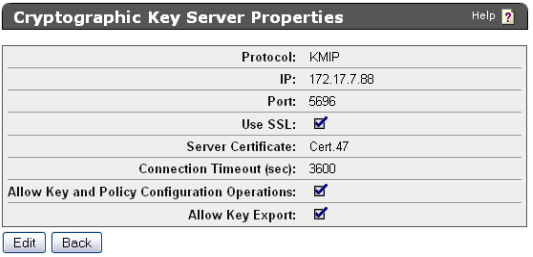


2. Click **Add** in the Cryptographic Key Server Settings section.
3. Select *KMIP* for **Protocol**.
4. Select either *[All]* or a specific IP address for **IP**.
5. Select the **Port**. We recommend 5696.
6. Select **Use SSL**. SSL is required for KMIP.
7. Select a **Server Certificate**. The server certificate you just created should be available for selection.
8. Click **Save**.



9. Select the KMIP link.

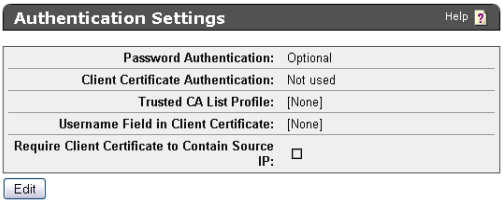
10. View the Cryptographic Key Server Properties. Click **Edit** to alter any values.



The available fields are:

- **IP** – IP address(es) on which the KMIP server is enabled on the KeySecure or DataSecure. We 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 KMIP server to listen for traffic on only one IP address. This can greatly reduce system vulnerability to outside attacks.
- **Port** – port on which the KMIP server is listening for client requests. We recommend 5696.
- **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 connection can remain idle before the KMIP server begins closing them. The default value is 3600, which is also the maximum.
- **Allow Key and Policy Configuration Operations** – when enabled, the KMIP server allows key creation, deletion, and import.
- **Allow Key Export** – when enabled, the KMIP 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 or DataSecure, which means the KeySecure or DataSecure must have access to the signing CA to verify the certificate.



The available fields are:

- **Password Authentication** – this is not used by the KMIP server and should be set to *Optional*.
- **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 or DataSecure in order to establish an SSL connection.
  - *Used for SSL session and username* – clients must provide a certificate signed by a CA trusted by the KeySecure or DataSecure in order to establish an SSL connection; additionally, a username is derived from the client certificate. That username is the sole means of authentication. When you select this option, you must choose the field that contains the username.
- **Trusted CA List Profile** – select a profile to use to verify that client certificates are signed by a CA trusted by the KeySecure or DataSecure. 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 KMIP 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 session and username* above. The username can come from the *UID*, *CN*, *SN*, *E*, *E_ND*, or *OU* fields.

  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 request contains the email address User1@company.com, then the KMIP server matches against User1.
- **Require Client Certificate to Contain Source IP** – determines if the KMIP server expects that the client certificate has an IP address in the subjectAltName field. The KMIP server obtains the IP address from subjectAltName and compares that to the source IP address of the client application; if the two IP addresses match, the KMIP server authenticates the user. If the two IP addresses do not match, the KMIP server closes the connection with the client.

The KeySecure or DataSecure is now ready to manage keys and can handle requests that come through the KMIP interface. To further configure the device, refer to the *KeySecure User Guide* or the *DataSecure User Guide*, as appropriate.

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.