KeySecure
Version 6.1.0

www.safenet-inc.com
4690 Millennium Drive, Belcamp, Maryland 21017 USA
Telephone: +1 410 931 7500 or 1 800 533 3958

007-011889-001, Rev. A

Quick Start Guide

Introduction

This guide describes the steps that the KeySecure administrator must perform to install this appliance in the network, initialize the HSM, configure the optional SSKM network interface, and make the appliance available to SafeNet's KeySecure Management Console.

Items required for installation

Installing the appliance requires items included in the shipping package and from the environment where the appliance will be installed.

- Null modem cable (included).
- Ethernet cable (not included). You must have the correct number and length of network cables.
- KeySecure power cable (included).
- Console terminal or PC (not included).
- Phillips screwdriver (not included).
- PIN Entry Device (included).
- 9-pin Micro-D data cable (included).
- 3 iKeys, minimum (included).

Network information required for installation

Collect this information before initializing the KeySecure:

- An IP address for the KeySecure.
- An IP address for the SSKM (optional). The IP must be on the same subnet as the KeySecure.
- The subnet mask for the network.
- The gateway for the network.
- A hostname for the network.
- A port on the KeySecure for Web administration (the default is 9443).

11. Execute the `hsm generate certificates` command. These certificates are used by the KeySecure when communicating with the HSM.

    ```
    DemoBox (config)# hsm generate certificates
    ```

12. **Log in as the Crypto User**. Use the `hsm login crypto user` command to log in as the Crypto User.

    ```
    DemoBox (config)# hsm login crypto user

    Luna PED operation required for crypto user login on HSM – use User or Partition Owner (black) PED key.
    ```

    Insert the black iKey and press Enter. Enter the PIN.

    The KeySecure CLI displays the following message:

    ```
    Crypto user successfully logged into the HSM.
    ```

The HSM is now available and the KeySecure can be used to manage keys.

7. Execute the `hsm create partition` command to create a partition on the HSM and to create the Crypto User, the user with access to that partition.

   ```
   DemoBox (config)# hsm create partition
   ```

   The KeySecure CLI displays the following message:

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

8. **Create the black Crypto User iKey**. Decline the option of reusing an existing keyset. The PED asks you to set the M of N feature. Enter the number of M and the number of N. If not using this feature, enter **1** for both. Insert the black Crypto User iKey. Set and confirm the PIN. Decline duplicating the keyset. If using M of N, enter the necessary amount of black iKeys (N).

9. **Generate the Crypto User password**. Keep the black iKey inserted into the PED. Enter the PIN. The PED will now use the red Domain iKey from step 6, above, to create the Crypto User password. 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)
   ```

   Press **Yes**. Insert your red Domain iKey. Enter the PIN. Decline duplicating the keyset.

   The PED displays the Crypto User password.

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

   Write down the password.

   The KeySecure CLI displays the following message:

   ```
   'partition create ' successful
   ```

10. Execute the `hsm set password` command. Use the password created in the previous step.

    ```
    DemoBox (config)# hsm set password MxCT-c7F9-HHX5-
    YtH3
    ```


Install the KeySecure appliance

Rack mount the appliance

The KeySecure should be mounted at the bottom of the rack if it is the only unit in the rack. When mounting the appliance in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. Install any provided rack stabilizers before mounting or servicing the appliance in the rack.

1. **Secure the KeySecure on a standard 19-inch rack** that provides sufficient space for cabling, airflow, and maintenance.
2. **Open the bezel**.
3. **Position the rack mount brackets** to align with holes in the rack posts.
4. **Start the screws** into the brackets. **Do not tighten**.
5. Properly **align the device** in the rack.
6. Use a screwdriver to **tighten the screws**. This should securely attach the mounting brackets to the rack posts.

Connect the null modem cable

Connect the null modem cable to the serial port on the back panel of the KeySecure. Plug the other end of the cable into the serial port of your console terminal or PC.

Connect the ethernet cable

Connect the ethernet cable to ethernet interface #1 on the back panel of the KeySecure. Plug the other end of the cable to your network.

Apply power

Connect the power cable from the power supply on the back panel of the KeySecure to an AC power source. Unscrew the bezel. Press the power switch on the front panel to start the boot sequence. Reattach the bezel.

Configure the KeySecure appliance

Start the terminal emulation session

While the KeySecure performs the initial boot sequence, start a terminal emulation session on the console terminal or PC. Use an application such as HyperTerminal or Minicom. Specify the following communication settings:

- VT100/ANSI
- 8 data bits
- 1 stop bit
- 19200 bps
- no parity
- hardware flow control

Start the initialization process

The initialization process begins when the boot sequence completes. The terminal or PC displays the following:

```
System starting up...
Release 6.1.0

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

1. Enter **y** to begin setup.
2. **Create the admin account**. You use this account to log into the Management Console and the CLI. You can modify this account and create additional administrators later.
3. **Enter and confirm the admin password**. The KeySecure enforces strong password checking. Use a complex password.

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

You must also have at least 3 iKeys: one blue, one red, and one black. You will need additional iKeys if using the M of N feature.

The instructions below assume that you will not use a pre-existing keyset until step 9, when you **must** reuse the red Domain iKey from step 6. If you plan to reuse pre-existing iKeys in steps 4, 6, or 8, adjust those instructions accordingly.

To initialize the HSM:

1. Log in to the KeySecure CLI as admin.
2. Execute the config command to enter configure mode.

   ```
   DemoBox# config

   DemoBox (config)#
   ```

3. Execute the hsm initialize command.

   ```
   DemoBox# hsm initialize

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

4. **Create the blue Security Officer iKey**. At the PED, decline the option of reusing an existing keyset. The PED asks you to set the M of N feature. Enter the number of M and the number of N. If not using this feature, enter **1** for both. Insert the blue Security Officer iKey. Set and confirm the PIN. Decline duplicating the keyset. If using M of N, enter the necessary amount of blue iKeys (N).
5. **Log in as the Security Officer**. Enter the blue Security Officer iKey, and enter M of N, if configured. Enter the PED PIN. The Security Officer is now logged in, which allows for further configuration of the HSM.
6. **Create the red Domain iKey**. Decline the option of reusing an existing keyset. The PED asks you to set the M of N feature. Enter the number of M and the number of N. If not using this feature, enter **1** for both. Insert the red Domain iKey. Set and confirm the PIN. Decline duplicating the keyset. If using M of N, enter the necessary amount of red iKeys (N).

   The KeySecure CLI displays the following message:

   ```
   'hsm init ' successful.
   ```

Configuring port speed

The Port Speed/Duplex setting is an advanced feature you can use to ensure that the KeySecure negotiates a usable connection with other network devices. In most networks, the default value (Auto-Negotiate) should suffice; however, if you force a particular setting on a network device, you must configure the KeySecure to use the same settings. For more information, please refer to the *KeySecure User Guide*.

Configuring the KMIP server

The *KeySecure Installation Guide* contains the detailed instructions needed to configure the KeySecure's KMIP server, including the steps required to configure SSL.

Additional configuration

The KeySecure's device management features are easily configurable using either the Management Console or the CLI. Refer to the *KeySecure User Guide* for information on:

- Clustering multiple KeySecures.
- Managing the system clock with NTP servers.
- Managing domain names with DNS servers.
- Monitoring system health via SNMP v1, v2, and v3.
- Rotating and transferring signed, secure logs.
- Using LDAP servers to manage users and administrators.

Initializing the HSM as a separate process

Normally, you will initialize the HSM as part of the KeySecure initialization described above. If, for some reason, you choose to delay the HSM initialization, you must perform the steps shown below. Until the HSM initialized, the KeySecure will not be able to perform its key management functions.

To initialize the HSM, you must have access to the KeySecure's Command Line Interface (CLI) and the PED, which must be connected to the HSM port on the back panel of the KeySecure.

4. **Set the system time zone, date, and time**. The system displays default values in brackets. You can accept those defaults by pressing Enter or you can enter specific values. The system offers a long list of time zones. If your time zone is not provided, select GMT.
5. **Set the network address**, **subnet mask**, **default gateway**, and **hostname** for the KeySecure. This step configures ethernet port 1. Accept the default values by pressing Enter or enter specific values.
6. **Enter the port number** for the Management Console. The system displays the default port, 9443. Accept this default by pressing Enter or enter another value.

Initialize the HSM

HSM initialization requires physical access to the PIN Entry Device (PED) and at least 3 iKeys. Use the iKey peel-and-stick labels to label one blue, one red, and one black iKey. You will need additional iKeys if using the M of N feature.

When prompted to insert iKeys, there is a limited time (about 3 minutes) in which to insert the iKey. After this time period, the operation times out and the HSM initialization must occur separately from the KeySecure installation. For details, see the *Initializing the HSM as a separate process* section in this guide.

TIP: When creating the iKeys at the PED, the process enables you to create duplicates. We recommend that you defer creating duplicates until immediately after initializing.

Prompts at the KeySecure CLI and the PED guide you through this process. The instructions below assume that you will not use a pre-existing keyset until step 6, when you **must** reuse the red Domain iKey from step 4. If you plan to reuse pre-existing iKeys in steps 2, 4 or 5, adjust those instructions accordingly.

To initialize the HSM:

1. Continue the initialization process at the KeySecure.

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

   Enter **y** and turn to the PED.

2. **Create the blue Security Officer iKey**. At the PED, decline the option of reusing an existing keyset. The PED

asks you to set the M of N feature. Enter the number of M and the number of N. If not using this feature, enter **1** for both. Insert the blue Security Officer iKey. Set and confirm the PIN. Decline duplicating the keyset. If using M of N, enter the necessary amount of blue iKeys (N).

3. **Log in as the Security Officer**. Enter the blue Security Officer iKey, and enter M of N, if configured. Enter the PED PIN. The Security Officer is now logged in, which allows for further configuration of the HSM.
4. **Create the red Domain iKey**. Decline the option of reusing an existing keyset. The PED asks you to set the M of N feature. Enter the number of M and the number of N. If not using this feature, enter **1** for both. Insert the red Domain iKey. Set and confirm the PIN. Decline duplicating the keyset. If using M of N, enter the necessary amount of red iKeys (N).
5. **Create the black Crypto User iKey**. Decline the option of reusing an existing keyset. The PED asks you to set the M of N feature. Enter the number of M and the number of N. If not using this feature, enter **1** for both. Insert the black Crypto User iKey. Set and confirm the PIN. Decline duplicating the keyset. If using M of N, enter the necessary amount of black iKeys (N).
6. **Generate the Crypto User Password**. Keep the black iKey inserted into the PED. Enter the PIN. The PED will now use the red Domain iKey from step 4, above, to create the Crypto User password. 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)
   ```

   Press **Yes**. Insert your red Domain iKey. Decline duplicating the keyset.

   The PED displays the Crypto User password.

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


   The KeySecure CLI displays the following message:

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

   Enter **y** and type the Crypto User password at the KeySecure CLI.

7. **Log in as the Crypto User**. Keep the black iKey inserted into the PED. Enter the PIN and enter M of N, if configured. The KeySecure CLI displays the following message:

   ```
   Crypto user successfully logged into the HSM.
   ```

Configure the SSKM network interface

This step is only required when using SSKM. Enter the IP address and subnet mask. Start the SSKM.

Completing the installation

The KeySecure creates a DSA key, an RSA key, and a Web Admin certificate. These keys authenticate the KeySecure when administrators connect to the Management Console via HTTPs or the Command Line Interface (CLI) via SSH.

At the end of the initialization process, the KeySecure displays the key fingerprints. To prevent a “man in the middle” attack, save these fingerprints and compare them to what is presented when making administrative connections to the KeySecure.

When the setup process is complete, you can log in to the KeySecure.

Logging in

To log in to the KeySecure, use either of these methods:

- The CLI at the serial console or using an SSH session. When using the console for CLI access, you may have to press [Enter] a few times to get the login prompt to appear.
- The Management Console using a web browser that supports 128-bit encryption, at the following URL:

  https://[IP-address]:[admin-port]

  Use the IP address and port specified above. For example, https://192.168.0.1:9443