HSM Switch Configuration Guide

(Safenet)

Copyright

Contents

1 SafeNet: Switching HSM Modules

This section provides information about switching between Soft HSM and SafeNet HSM.

Note:

- The switching of HSM modules is disabled for release v7.1.
- The procedure provided in this section is for SafeNet Network HSM 7000 device and Luna 7
- For installation of Safenet libraries and client tools, refer to the Safenet documentation. You must convert the standard RPM and DEB installer packages to *.tgz* files for installations on ESA.

1.1 Switching from Soft HSM to SafeNet HSM

In this release, an internal Soft HSM generates the Master key and ERK. If an organization uses a SafeNet HSM as part of their IT infrastructure, then Protegrity Key Management functionality can be configured to use the SafeNet HSM.

Note: It is recommended that careful analysis is performed for any data that might be linked to an older key before switching to a SafeNet HSM. Consult IT security professionals, such as Protegrity support or Professional Services, to understand how you can switch HSM with minimal impact to business processes involved.

Before you Begin:

- Login to ESA as System Administrator.
- Ensure that the library files (`libCryptoki2_64.so`), certificates and the configuration file (`Chrystoki.conf`) are available for upload in ESA.
- Edit the `Chrystoki.conf` file as per the following table.

Table 1: Configuration File Values

File Name	Parameter in .conf file	Value
Openssl config file	SSLConfigFile	`/usr/lib/ssl/openssl.cnf`
HSM Client Certificate	ClientCertFile	`/opt/protegrity/hubcontroller/data/cert/client/<client_cert_file.pem>`
HSM Client Key	ClientPrivKeyFile	`/opt/protegrity/hubcontroller/data/cert/client/<client_priv_key_file.pem>`
HSM Server Certificate	ServerCAFile	`/opt/protegrity/hubcontroller/data/cert/server/<server_ca_file.pem>`

Ensure that the *libCryptoki2_64.so*, *Chrystoki.conf*, HSM Client Certificate, HSM Client Key and the HSM Server Certificate files are compressed in a *.tgz* file before uploading in ESA.

➢ To configure SafeNet HSM with ESA:

1. On the ESA Web UI, click **Settings➢ System➢ File Upload**.
2. Click **Choose File**.
3. Select the *.tgz* file containing the library and the configuration file, and then click **Open**.
4. Click **Upload**.
   Note: For more information about configuration file parameters and values, refer to Editing Configuration File.
5. In the ESA CLI manager, navigate to **Administration➢ OS Console**.

6. Enter the *root* password.
7. Navigate to the */products/uploads* directory.
8. Extract the *.tgz* file using the following command.

```
tar -xvz <filename>.tgz
```

9. Copy the extracted files from the */product/uploads* directory to the */opt/protegrity/hubcontroller/data* directory.

   Note: The file permissions for the library file and configuration file must be changed to *744*. Also, ensure that the file owner is *service_admin*.

10. Copy the *Chrystoki.conf* file to the default */etc* directory. You can also copy this file to non-default directory for e.g. */opt/protegrity/hubcontroller/data*. If file is copied to non-default directory, then you must set *ChrystokiConfigurationPath* variable in the */opt/protegrity/hubcontroller/bin/hubcontroller.env* file.

    In the following sample command, the path */opt/protegrity/hubcontroller/data/* is set to *ChrystokiConfigurationPath* variable.

```
export ChrystokiConfigurationPath=/opt/protegrity/hubcontroller/data/
```

11. In the ESA CLI manager, navigate to **Tools➢ Data Protection System Tools➢ Switch HSM Module**.
12. Enter the *root* password.
13. Enter the details as per the following figure.

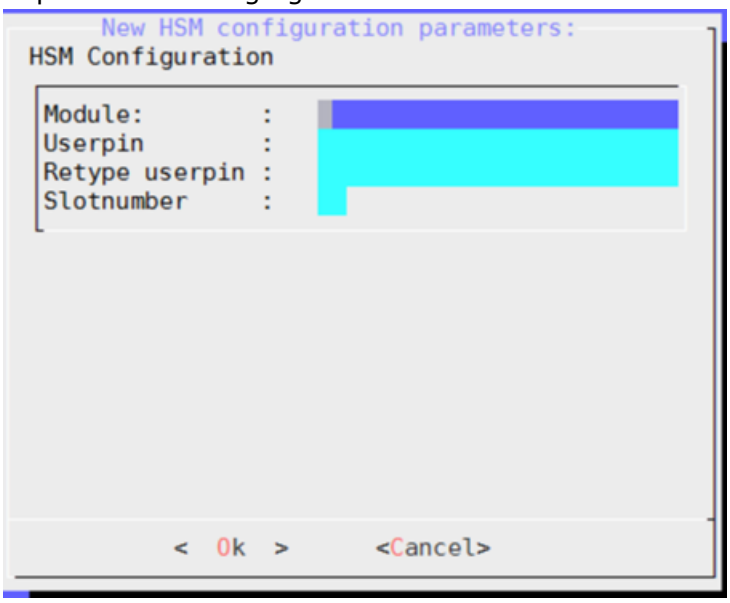

Figure 1: SafeNet HSM Details

Table 2: The following table provides information about the fields.

Field	Description	Value
Module	Name of the library file.	libCryptoki2_64.so
Userpin	Userpin for the slot number where the keys will be stored in the HSM.	n/a*
Retype userpin	Re-enter the userpin for confirmation.	n/a*
Slotnumber	Slot in an HSM hardware that is used to store keys and is protected by the userpin.	Can be any value as defined for the HSM between 0-99.

n/a* - Not applicable

14. Press **OK**.
    The following message appears.

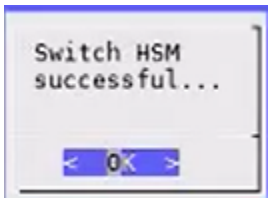

Figure 2: HSM switched successfully

Note: For more information about switching HSM logging, refer to the *dpsswitchhsm.log* file in the */opt/protegrity/hubcontroller/data* folder.

If you are exporting and importing Policy Management of ESA with HSM, ensure that the HSM related files are present in the */opt/protegrity/hubcontroller/data* folder.

If the HSM related files are present in some other directory, then you must perform following steps prior to configuring HSM with ESA.

➢ Steps to perform after importing policy management on ESA:

1. Copy the HSM related files to the correct location in ESA. The correct location for these files must be same as the one in ESA, from where the data was exported.
```
/opt/protegrity/hubcontroller/data/cert/client/<client_cert_file.pem>
/opt/protegrity/hubcontroller/data/cert/client/<client_priv_key_file.pem>
/opt/protegrity/hubcontroller/data/cert/server/<server_ca_file.pem>
/etc/Chrystoki.conf
/opt/protegrity/hubcontroller/data/libCryptoki2_64.so
```
2. Ensure that the owner and rights of user for these files is same as before.
3. Link the *pkcs11.plm* file to the client library file.
```
cd /opt/protegrity/hubcontroller/data/
ln -s /opt/protegrity/hubcontroller/data/libCryptoki2_64.so pkcs11.plm
```
4. If the *Chrystoki.conf* file is copied in a non-default directory for e.g. */opt/protegrity/hubcontroller/data*, then you must set the *ChrystokiConfigurationPath* variable in the */opt/protegrity/hubcontroller/bin/hubcontroller.env* file.
   In the following sample command, the path */opt/protegrity/hubcontroller/data/* is set to *ChrystokiConfigurationPath* variable.
```
export ChrystokiConfigurationPath=/opt/protegrity/hubcontroller/data/
```
5. Restart **Hubcontroller** and **Admin Server** services from **ESA Web UI ➢ System ➢ Services** or **ESA CLI ➢ Administration ➢ Services**.

1.2 Switching from SafeNet HSM to Soft HSM

You can switch to ESA Soft HSM, if required, using the procedure provided in this section.

Note: It is recommended that careful analysis is performed for any data that might be linked to an older key before switching to a SafeNet HSM. Consult IT security professionals, such as Protegrity support, to understand how you can switch HSM with minimal impact to business processes involved.

Before you Begin:

- Login to ESA as System Administrator.
- Verify if the following files are available in ESA as per the following table.
  Note: The files mentioned in the table are created by default when ESA is installed.

Table 3: ESA Soft HSM Files/Folders

File Name/Directory Name	Description	File Path
libsofthsm2.so	ESA Soft HSM library file. **Note:** Ensure that the file has *644* permissions and the owner is *service_admin*.	*/opt/protegrity/hubcontroller/data*
softhsm.conf	ESA Soft HSM configuration file.	*/opt/protegrity/hubcontroller/conf*
Keys folder	ESA keys are stored at this location.	*/opt/protegrity/hubcontroller/keys*

- Ensure that the password for the soft HSM is available. To derive this password, you must send the *userpin.bin.bkup.<timestamp>* backup file in the */opt/protegrity/hubcontroller/data* to Protegrity support. The support team will use this file to generate the userpin for the Soft HSM.

  Note: Ensure that the Userpin backup file that was created when you switched to a SafeNet HSM for the first time is sent to the support team. This file contains the password for the Soft HSM.

➢ To configure Soft HSM with ESA:

1. In the ESA CLI manager, navigate to **Tools➢ Data Protection System Tools➢ Switch HSM Module**.
2. Enter the *root* password.
3. Enter the details as per the following figure.

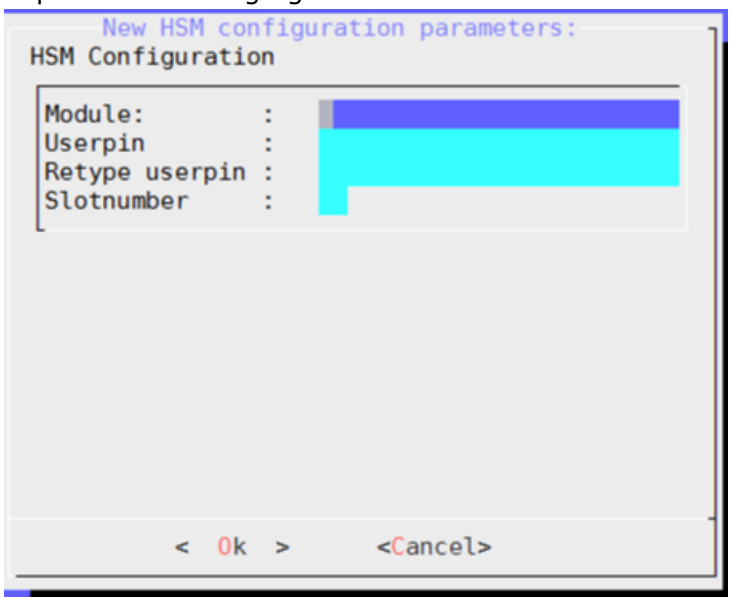

Figure 3: SafeNet HSM Details

Table 4: The following table provides information about the fields.

Field	Description	Value

Module	Name of the library file.	libsofthsm2.so
Userpin	Userpin password for the slot number where the keys will be stored in the HSM. This password is provided by the Protegrity support team. For more information, refer to Generate Soft HSM userpin password.	n/a*
Retype userpin	Re-enter the userpin for confirmation.	n/a*
Slotnumber	Slot in an HSM hardware that is used to store keys and is protected by the userpin.	0

n/a* - Not applicable

4. Press **OK**.
   The following message appears.

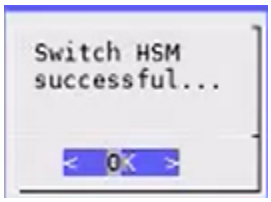

Figure 4: HSM switched successfully

5. Restart **Hubcontroller** and **Admin Server** services from **ESA Web UI ➤ System ➤ Services** or **ESA CLI ➤ Administration ➤ Services**