Configuring HSM Devices on Expressway

Important: Read this First

HSM failure. If an Expressway is configured to use HSM and the HSM subsequently fails, **all services that require encryption will become unavailable**. This includes MRA, calls, web access, and so on.

Factory reset. If the HSM is permanently unavailable for any reason, **you will need to do a factory reset** for the Expressway and then configure a new HSM on the Expressway. A factory reset **reinstalls the software image and resets the Expressway configuration** to the default, functional minimum (see the *Expressway Administrator Guide* for instructions about doing a reset.)

How to Enable and Manage HSM

Use the **HSM configuration** page (**Maintenance** > **Security** > **HSM configuration**) to configure the information needed for Expressway.

Settings are replicated across a cluster.

The **HSM configuration** page settings replicate across all peers in an Expressway cluster. So if you add or remove any settings on one peer, the change replicates to all other peers.

Task 1: Configure Prerequisites

Do the following before you enable Hardware Security Module (HSM) functionality on Expressway:

a.	Add an HSM option key.	**i.** Go to **Maintenance** > **Option keys**. **ii.** In the **Software option** section, enter the option key. **iii.** Click **Add option**. The key appears in the list at the top of the page.

b.	Install the HSM TLP package. You can get this from the same download site as the Expressway software image. The HSM TLP is an archive of HSM provider-specific binaries that are needed for the Expressway to use the HSM.	**i.** Go to **Maintenance** > **Upgrade**. **ii.** In the **Upgrade component** section, click **Choose File** to select the TLP file from your local machine. **iii.** Click **Upgrade**. A message, `Component installation succeeded`, appears at the top of the page and the HSM TLP also appears at the top of the page. You can check the list of all installed modules in the drop-down. **Note** You must add the option key and install the TLP on each peer in the cluster. You cannot enable HSM Mode on a cluster unless all peers have the option key and the TLP.
c.	Deploy an HSM box on the Expressway	To configure an nShield Connect XC HSM: **i.** Set up a Security World and Remote File System (RFS) according to the *nShield Connect User Guide*. **ii.** Configure RFS to an nShield Connect that contains master copies of all the files that the HSM needs. RFS normally resides on a client computer, but it can be located on any computer that is accessible on the network. **iii.** After you deploy RFS and the nShield Connect box, run the following command on RFS: `/opt/nfast/bin/rfs-setup --gang-client --write-noauth <Expressway_ip_address>` HSM certificate management will not work properly on the Expressway if this command is not run.
d.	Have access to a certificate signing authority.	-
e.	Create an HSM-compatible certificate.	See the *Expressway Administrator Guide*, *Security* chapter for instructions.

Task 2: Enable HSM on Expressway

This is the recommended procedure to enable HSM use on Expressway:

Step 1 Go to **Maintenance** > **Security** > **HSM configuration**.

Step 2 In **HSM Settings**, choose the HSM provider from the **HSM Mode** drop-down list.

Step 3 Configure the nShield settings:

a. Enter the RFS IP address and RFS Port. The default port is 9004.

b. Click **Save Configuration**.

The following message is displayed at the top of the page.

```
An HSM Settings updated
```

c. In the **Add Module** section, enter the IP address, Port, ESN (Electronic Serial Number), and KNETI (Network Integrity Key) of the device.

d. Click **Add Module**.

   The following message is displayed at the top of the page.

```
An HSM Module successfully added
```

e. The device is now displayed in a table below the **HSM Mode** tab.

f. Repeat the Add Module steps to add more devices.

Step 4 Set the **HSM Mode** to *On* and click **Set Mode**.

The following message is displayed at the top of the page.

```
An HSM Mode successfully updated
```

Note Toggling the HSM Mode to *On/Off* may cause the web to become unavailable. If this happens, reload the browser page.

Results: HSM use is now enabled on the Expressway.

What to do next

To check the HSM operating status see the next section Task 3: Monitor HSM Status Check.

Task 3: Monitor HSM Status Check

After you enable HSM mode, an **HSM Status check** section displays on the **HSM configuration** page. This section displays information about the HSM server and HSM certificate for all Expressway cluster peers, and for all modules on each peer:

HSM server running

1. **TRUE**, after HSM mode is enabled on Expressway, if processes responsible for communicating with the HSM boxes are running on the Expressway.
2. **FALSE**, if processes are not running on the Expressway and an HSM failure alarm is raised.

HSM certificate in use

1. TRUE, when an HSM certificate and private key are in use by Expressway.
2. FALSE, when an HSM certificate and private key are not being used by Expressway. Default state is FALSE. An alarm, `HSM certificate is not used`, is raised on the Expressway - to warn that you are not using an HSM certificate and private key.

After the HSM certificate and private key are deployed to the Expressway, this alarm is lowered and the displayed status changes to TRUE.

The ESN section lists HSM modules that are added during the HSM configuration and are distinguished by their ESN. The other columns define **Connection Status** and **Hardware Status**.

Connection Status

1. OK, if no network issues exist between the Expressway and HSM module.
2. Failed, if network or HSM server connectivity issues exist and an alarm is raised.

Hardware Status

1. OK, if no hardware issues are detected on the HSM box itself.
2. Failed, if there are any hardware or an HSM box configuration issue and an alarm is raised.

Task 4: Next Steps - Generate and Install the HSM Private Key

When HSM is enabled and operating properly, you need to generate and install the HSM private key and certificate on Expressway. For details, see *Managing the Expressway Server Certificate with HSM*, in the *Expressway Administrator Guide*.

How to Delete Modules

Note You cannot remove the last device while HSM mode is enabled. You first need to disable HSM mode.

To optionally delete devices (modules) from the Expressway HSM configuration:

Step 1 Go to **Maintenance** > **Security** > > **HSM configuration**.

Step 2 Choose the required device from the list and click **Delete**.

How to Disable HSM

If you decide to disable HSM for any reason, the recommended procedure is:

Step 1 Go to **Maintenance** > **Security** > **HSM configuration**.

Step 2 Set **HSM Mode** to *Off* and click **Set Mode**. This disables HSM usage on the Expressway.

Step 3 Check an individual device or click **Select all** to choose all the modules in the table to delete. (Click **Unselect all** to de-select all devices in the table.)

Step 4 Click **Delete** and then **OK** in the confirmation dialog.