Configuring Secure Erase Using Cisco Fabric Manager

The Fabric Manager provides a user interface to configure Secure Erase jobs and operations on the switch by using a job creation wizard. This chapter describes how to configure Cisco MDS Secure Erase using Cisco Fabric Manager, and includes the following sections:

- Provisioning Secure Erase on the MSM-18/4 Module, page 3-1
- Using the Secure Erase Pre-Configuration Wizard, page 3-3
- Creating a Secure Erase Workflow Using Fabric Manager, page 3-13
- Displaying Secure Erase Job Status, page 3-18

Secure Erase is supported on the MSM-18/4 module and the MDS 9222i switch. The MSM-18/4 module and the MDS 9222i switch are referred to as a Secure Erase node.

Note
This feature will not be supported on switches running releases prior to NX-OS Release 5.0(1a).

Provisioning Secure Erase on the MSM-18/4 Module

You need to enable the Secure Erase feature on the Secure Erase nodes for them to participate in the Secure Erase operation.

To enable Secure Erase on the MSM-18/4, follow these steps:

Step 1
Expand End Devices in the Physical Attributes pane and click the MSM/SSN tab in the information pane to obtain the module information. (See Figure 3-1.)
Step 2  From the feature drop-down list, select SE to provision the MSM-18/4 with Secure Erase. (See Figure 3-2.)

Once the MSM-18/4 is provisioned, the entry is displayed in the table. (See Figure 3-3.)
**Using the Secure Erase Pre-Configuration Wizard**

The Secure Erase Pre-configuration wizard performs the following steps so that the Secure Erase capable module is ready to run the Secure Erase jobs:

1. Configures SSH by doing the following:
   - Enables SSH.
   - Creates keys.
2. Configures IP connectivity.
   - Creates the VSAN 1 interface and configures IP.
   - Create the CPP IPFC interface and configures IP.
4. Configures the IP default gateway for the MSM-18/4 module or the MDS 9222i switch.
5. Configures a zone to include the pWWN of MSM-18/4 module or the MDS 9222i switch and the supervisor module.

In the Secure Erase Pre-configuration wizard, when you click **Next** at each step, the configuration listed for that step will be preformed. For most steps, the **Back** button is disabled in the wizard. However, if an error occurs at any step, you are prevented from moving to the next step until you modify the data and click **Next** again successfully.

Also, if you click **Cancel**, the wizard exits at the step without undoing any of the settings performed by the previous steps. The **Back** option will not be available for the steps in this wizard.

To use the Secure Erase Pre-configuration wizard, launch the Fabric Manager GUI after selecting the required fabric (See Figure 3-4).

**Note**

Before you use the Secure Erase Pre-configuration wizard, install the Secure Erase package with the SSI image in the switch. SSH is enabled by the Secure Erase pre-configuration setup.
To display the Secure Erase Pre-Configuration wizard, from the Fabric Manager menu, choose **Tools > Secure Erase > Pre-configuration**.

You see the Secure Erase Pre-Configuration Wizard screen. (See **Figure 3-5**.)

**Figure 3-4 Secure Erase Pre-Configuration**
Configuring MDS Modules for Secure Erase

To configure MDS modules for Secure Erase, follow these steps:

**Step 1**
Select the Secure Erase capable modules that you want to configure and click **Next**.

The Modules for Set Up screen (see Figure 3-5) displays only the switch and modules that do not have the Secure Erase feature enabled. The switch must be running Cisco NX-OS Release 5.0 or later. This wizard cannot be used to edit existing configurations.

**Step 2**
The Enable Secure Shell (SSH) screen (see Figure 3-6) displays a list of Secure Erase switches.

The table indicates if SSH is enabled and if the key already exists.

a. Click **Next**.

A SSH key is created if the key does not already exist. SSH is enabled. The SSH key is created for protocol RSA with a numbits value of 1024.

**Note**
If SSH is already enabled on all switches, then the “No action necessary” message is displayed. Click **Next** to continue.
Figure 3-6 Enable Secure Shell (SSH)

Step 3
Select a switch from the drop-down list to configure the IP address and mask for the VSAN 1 interface.

a. Click Add (See Figure 3-7)
   The switch moves from the drop-down list to the table. One entry can be added for each switch.

b. Click Next.
   The IP address is created and the IPv4 routing is enabled for all the switches that are selected.

Note
The valid mask values are 8, 16, 24, or 32.

If the VSAN 1 IP address is already configured for the switch, then the switch does not appear in the drop-down list.

If all the switches already have the VSAN 1 IP address configured, then a message is displayed. Once you click Next, the IPv4 routing is configured.

If you do not add a VSAN 1 IP address for all the switches in the list and click Next, an error message is displayed. (See Figure 3-8.)
Step 4

Select a switch module from the drop-down list and specify the CPP IP address/mask. (See Figure 3-9)

a. Click **Add** to move the switch module from the drop-down list to the table.

   The CPP IP address must be in the same subnet as the VSAN 1 IP address or an error message is displayed. Only one entry can be added for each switch module.

b. Click **View necessary gateways**.

   The Necessary Default Gateways screen is displayed. (See Figure 3-10).

c. Click **Next**.

   The IP address is created and the gateway is configured.

The Configure Module IP Connectivity screen (see Figure 3-9) sets the IP address for CPP and configures the default gateway for the CPP interface to point to the VSAN 1 IP address. All IP traffic from the CPP interface is routed to the management interface.
The Necessary Default Gateways screen (see Figure 3-10) shows the VSAN 1 IP address that will be used to configure the default gateway for each of the switch modules. It also shows if a default gateway already exists.
Chapter 3 Configuring Secure Erase Using Cisco Fabric Manager

Configuring MDS Modules for Secure Erase

Figure 3-10 Necessary Default Gateways

<table>
<thead>
<tr>
<th>Necessary Default Gateways</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following is a list of necessary default gateways, each module needs a default gateway to the switch VSAN 1 IP Address. The “Already Exists?” column indicates if the default gateway exists, only those that don’t exist will be created:</td>
</tr>
<tr>
<td>Switch/Module</td>
</tr>
<tr>
<td>172.16.113.224, Module 2 (DS-91904-01)</td>
</tr>
</tbody>
</table>

**Note**

The valid mask values are 8, 16, 24, or 32.

If the CPP IP address is already configured for the switch module, then the module does not appear in the drop-down list.

The 9222i switch is not displayed in the drop-down list because it is not required to set a separate CPP IP address or default gateway for this module.

If all of the switch modules already have their CPP IP addresses configured, then a message is displayed. Click **Next**. The necessary default gateways are configured.

**Step 5**

Click **Create/Activate Zones**.

The wizard goes through the fabrics to create the zones. (See Figure 3-11)

Before creating the zones, the wizard checks if the active and local zone databases of the principle switch match. If there is a mismatch, an input dialog box is displayed. You will be prompted to copy the active zone database to the local zone database. If you click **Yes**, the zones are created on the principal switch for the fabric. If you click **No**, the zone creation is skipped for the zone mismatched fabric. After the zone creation is complete, a popup dialog box is displayed that specifies if the zone creation process was successful or if it failed.

If there is an error during the zone creation, the **Create/Activate Zones** button is enabled. Click **Create/Activate Zones** again to create the zones that failed previously. Only the zones that failed previously will be created to avoid any duplicate entries in the zones database.

Once all the zones are created successfully on all the fabrics, the **Create/Activate Zones** button is disabled and the **Status** button is enabled. (See Figure 3-12.)
(Optional) If you wish to do the zoning yourself, follow these steps:

a. Click Next without clicking Create/Activate Zones.

A warning message is displayed stating that the zones are not created and asking if you wish to continue to the next step without creating zones.

b. Click Yes to continue.

The Status button allows the user to verify that the zones were added to the active zone database.

Note

Zoning is not required for the MDS 9222i switch because this module type is also a supervisor and does not need to be zoned with the supervisor’s VSAN 1 WWN to allow communication.

The Zoning screen (see Figure 3-11) creates a zone to include the VSAN 1 WWN and the module WWN for each of the selected module.

Figure 3-11  Zoning
The Zone Creation Status screen (see Figure 3-12) shows all the zones in the active zone database.

**Figure 3-12 Zone Creation Status**

![Zone Creation Status](image)

**Step 6** Click **Finish** to complete the Secure Erase Pre-configuration wizard setup (See Figure 3-13).
The Secure Erase Pre-configuration wizard enables the Secure Erase functionality for all the nodes on the modules selected.

A message appears that shows the status of the setup as a success or as a failure. If successful, the Finish button is disabled and the Cancel button changes to Close.
Creating a Secure Erase Workflow Using Fabric Manager

You can create a Secure Erase job using the Secure Erase wizard in Fabric Manager.

To create a workflow using the Secure Erase wizard, from the Fabric Manager menu, choose **Tools > Secure Erase > Secure Erase**.

The job creation screen is displayed. (See **Figure 3-14**.)

![Figure 3-14 Secure Erase Configuration](image)

**Note**

Fabric Manager will internally add the string SE as a prefix to all job names so that they are identified as SE jobs and not as DMM jobs.

The Secure Erase job creation panel is displayed with all the enclosures listed.
Creating a Secure Erase Job Using Fabric Manager

To configure Secure Erase jobs, follow these steps:

**Step 1**
Select an enclosure from the enclosure list.
The port list is populated with the end ports belonging to the selected enclosure. (See Figure 3-15)

a. Select multiple target ports from the list.
b. Click Next.

The wizard will validate that the target ports selected belong to the same fabric and the same VSAN (the target ports cannot span across VSANs).

*Note*
The selected multiple target ports should belong to the same fabric and the same VSAN.

**Figure 3-15 Secure Erase Create Job**

**Step 2**
Select the SE-enabled module in the fabric. (See Figure 3-16.)
a. Click Next.

All DPP Virtual Initiators (VIs) for the selected module are listed.
All of the SE-enabled modules in the VSAN that the target ports belong to are listed. The module with the least number of active jobs should be selected by default. Ensure that the number of active jobs for each module is listed correctly.

Figure 3-16 Secure Erase Enable Module

Step 3 Select a DPP Virtual Initiator (VI) for Secure Erase.

The first DPP VI in the list is selected by default. Verify that the pWWN, nWWN, and the job number are listed correctly for each DPP VI. (See Figure 3-17.)

a. Click Create/Activate Zone.

The Zone Activation Status is displayed. (See Figure 3-18.)

Zones are created for each of the VSANs that the selected targets belong to and the selected DPP VI.

b. Click Status to view the Zone creation or activation status.

c. Click Next.

All of the selected targets with the LUNs are listed.
Figure 3-17  DPP VI Selection

Step 3: DPP VI Selection
Select DPP VIs from the list for Secure erase. Please program them to give access to all LUNs in Storage.
Step 4  Select the LUNs for which the sessions need to be created. (See Figure 3-19.)

Note  Checking the Session check box at target level will check all the LUNs for that target. Unchecking the session check box for any of the LUNs will automatically uncheck the check box at the parent target level.

a. Select the algorithm for each LUN. (See Figure 3-19.)

Note  Selecting an algorithm at target level will select that algorithm for all the LUNs for that target. Selecting a different algorithm for any of the LUNs will automatically mark the algorithm as Mixed at the parent target level.
Creating a Secure Erase Job Using Fabric Manager

Figure 3-19 Create Session

Step 5 Click Finish.

The Secure Erase job is created with specified sessions.

If multiple LUNs were selected and at least one session is created successfully, then the operation is considered to be successful.

Displaying Secure Erase Job Status

To verify the Secure Erase jobs and session information, follow these steps:

Step 1 Expand End Devices in the Physical Attributes pane and select Secure Erase.

The information pane is displayed. (See Figure 3-20.)
Step 2  Select a job status for each Secure Erase job.

The following operations are allowed on each job:

- **Start**—Starts the Secure Erase job. The session progress can be viewed in the session rows.
- **Stop**—Stops the Secure Erase job. The session progress can be viewed in the session rows.
- **Abort**—Aborts the Secure Erase job. The session progress can be viewed in the session rows.
- **Validate**—Validates the Secure Erase job. The session progress can be viewed in the session rows.
- **Delete**—Deletes the selected Secure Erase job.