Security Module/Engine Management

About FXOS Security Modules/Security Engine

From the Security Modules/Security Engine page of the chassis manager, you can view the status of a security module/engine and can perform various functions on the security module/engine:

The Security Modules/Security Engine page provides the following information:

- Hardware State—Shows the state of the security module/engine hardware.
  - Up—The security module/engine has powered up successfully and is not showing any hardware faults, even if the security module/engine does not have a logical device associated with it.
  - Booting Up—The security module/engine is in the process of powering up.
  - Restart—The security module/engine is in the process of being restarted.
  - Down—The security module/engine is not powered on or a hardware fault is preventing the security module/engine from starting successfully.
  - Mismatch—The security module has been decommissioned or a new security module was installed into the slot. Use the Acknowledge function to return the security module to a functioning state.
  - Empty—A security module is not installed in that slot.
- Service State—Shows the state of the software on the security module/engine:
  - Not-available—The security module has been removed from the chassis slot. Reinstall the security module to return it to its normal operational state.
  - Online—The security module/engine is installed and is in normal operation mode.

- Offline—The security module/engine is installed but has either been decommissioned, turned off, or is currently in the process of powering up.
- Not Responding—The security module/engine is unresponsive.
- Token Mismatch—Indicates that a security module other than the one previously configured has been installed into the chassis slot. This could also be caused by a software installation error. Use the Reinitialize function to return the security module to a functioning state.
- Fault—The security module/engine is in a fault state. Review the system fault listing for more information about what might be causing the fault state. You can also hover over the information icon for a fault to see additional information.

Security Module Faults

- Failsafe Mode—the security module is in failsafe mode. Applications are blocked from starting in this mode. Connect to the security module for troubleshooting or to disable failsafe mode. The app-instance can also be deleted.
- HDD Error—the security module disk drive has errors. Please verify that the disk drive is present and replace the faulty disk drive if the fault does not clear.
- Filesystem Error—disk partitions on the security module are not compatible. Reboot the security module for possible recovery. If the fault persists, please reinitialize the slot after backing up your data on an external device.
- Format Failure—automatic format failed on the security module disk drive. Reinitialize the security module to reformat.

- Power—Shows the power status of the security module/engine:
  - On—Use the Power off/on function to toggle the power status for the security module/engine.
  - Off—Use the Power off/on function to toggle the power status for the security module/engine.
- Application—Shows the logical device type that is installed on the security module/engine.

From the Security Modules/Security Engine page of the chassis manager, you can perform the following functions on a security module/engine:

- Decommission (security modules only)—Decommissioning a security module places the security module into maintenance mode. You can also decommission and then acknowledge a security module in order to correct certain fault states. See Decommissioning a Security Module, on page 3.
- Acknowledge—Brings newly installed security modules online. See Acknowledge a Security Module/Engine, on page 3.
- Power Cycle—Restarts the security module/engine. See Power-Cycling a Security Module/Engine, on page 4.
- Reinitialize—Reformats the security module/engine hard disk, removing all deployed applications and configurations from the security module/engine, and then restarts the system. After reinitialization is complete, if a logical device is configured for the security module/engine, the FXOS will reinstall the application software, redeploy the logical device, and auto start the application. See Reinitializing a Security Module/Engine, on page 4.

Warning All application data on the security module/engine is deleted during reinitialization. Please back up all application data before reinitializing a security module/engine.

- Power off/on—Toggles the power state for the security module/engine. See Power-Cycling a Security Module/Engine, on page 4.

Decommissioning a Security Module

When you decommission a security module, the security module object is deleted from the configuration and the security module becomes unmanaged. Any logical devices or software running on the security module will become inactive.

You can decommission a security module if you want to temporarily discontinue use of the security module.

Procedure

Step 1 Choose **Security Modules** to open the Security Modules page.

Step 2 To decommission a security module, click **Decommission** for that security module.

Step 3 Click **Yes** to verify that you want to decommission the specified security module.

Acknowledge a Security Module/Engine

When a new security module is installed into the chassis, or when an existing module is replaced with one with a different product ID (PID), you must acknowledge the security module before you can begin using it.

If the security module is showing a status of "mismatch" or "token mismatch," this is an indication that the security module installed in the slot has data on it that does not match what was previously installed in the slot. If the security module has existing data on it and you are sure you want to use it in the new slot (in other words, the security module wasn't inadvertently installed into the wrong slot), you must reinitialize the security module before you can deploy a logical device to it.

Procedure

Step 1 Choose **Security Modules/Security Engine** to open the Security Modules/Security Engine page.

Step 2 Click **Acknowledge** for the security module/engine that you want to acknowledge.

Step 3 Click **Yes** to verify that you want to acknowledge the specified security module/engine.

Power-Cycling a Security Module/Engine

Follow these steps to power-cycle a security module/engine.

Procedure

Step 1 Choose **Security Modules/Security Engine** to open the Security Modules/Security Engine page.

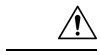
Step 2 Click **Power Cycle** for the security module/engine that you want to reboot.

Step 3 Do one of the following:

- Click **Safe Power Cycle** to have the system wait for up to five minutes for the application running on the security module/engine to shut down before the system power-cycles the specified security module/engine.
- Click **Power Cycle Immediately** to have the system power-cycle the specified security module/engine immediately.

Reinitializing a Security Module/Engine

When a security module/engine is reinitialized, the security module/engine hard disk is formatted and all installed application instances, configurations, and data are removed. After reinitialization has completed, if a logical device is configured for the security module/engine, FXOS will reinstall the application software, redeploy the logical device, and auto start the application.



Caution All application data on the security module/engine is deleted during reinitialization. Back up all application data before reinitializing a security module/engine.

Procedure

Step 1 Choose **Security Modules/Security Engine** to open the Security Modules/Security Engine page.

Step 2 Click **Reinitialize** for the security module/engine that you want to reinitialize.

Step 3 Click **Yes** to verify that you want to reinitialize the specified security module/engine.

The security module/engine is restarted and all data on the security module is deleted. This process can take several minutes.

Acknowledge a Network Module

When a new network module is installed into the chassis, or when an existing module is replaced with one with a different product ID (PID), you must acknowledge the network module before you can begin using it.

Procedure

Step 1 Enter `scope fabric-interconnect` mode:

```
scope fabric-interconnect
```

Step 2 Enter the **acknowledge** command after installing a new module or replacing a network module with another that is not the same type (that is, with a different PID):

```
acknowledge
```

Example:

```
FPR1 /fabric-interconnect # acknowledge
  fault  Fault
  slot   Card Config Slot Id  <======
```

Step 3 Enter the **acknowledge slot** to acknowledge the inserted slot.

```
acknowledge slot
```

Example:

```
FPR1 /fabric-interconnect # acknowledg slot 2
  0-4294967295  Slot Id
```

Step 4 Commit the configuration:

```
commit-buffer
```

Taking a Network Module Offline or Online

Follow these steps to use CLI commands to take a network module offline, or to bring it back online; used for example, when performing module online insertion and removal (OIR).

Note

- If removing and replacing a network module, follow the instructions in the "Maintenance and Upgrades" chapter of the appropriate Install Guide for your device. See https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html.
- If performing a network module online insertion and removal (OIR) on a 8 port 1G Copper FTW Network Module (FPR-NM-8X1G-F FTW), note that the network module LED stays off until you bring the card online using this procedure. The LED first flashes amber, then changes to green once the network module is discovered and the application comes online.

Note If you remove a FTW network module and acknowledge the slot, the network module ports are deleted from the threat defense logical device. In this case, you must delete the hardware bypass inline set configurations using management center before reinserting the network module. After reinserting the network module, you must:

- Configure the network module ports as adminstrative online state using chassis manager or FXOS Command Line Interface (CLI).
- Add the network module ports to the threat defense logical device and reconfigure the ports using management center.

If you remove the network module without acknowledging the slot, the inline set configuration is retained and ports display as down in management center. Once you reinsert the network module, the previous configuration is restored.

For more information about hardware bypass for inline sets, see Hardware Bypass Pairs.

Procedure

Step 1 Use the following commands to enter `/fabric-interconnect` mode and then enter `/card` mode for the module to be taken offline:

```
scope fabric-interconnect a
scope card ID
```

Step 2 You can use the **show detail** command to view information about this card, including its current status.

Step 3 To take the module offline, enter:

```
set adminstate offline
```

Step 4 Enter the **commit-buffer** command to save the configuration change.

You can use the **show detail** command again to confirm that the module is offline.

Step 5 To bring the network module back online, enter:

```
set adminstate online
commit-buffer
```

Example

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope card 2
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
    Id: 2
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD191601DE
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
FP9300-A /fabric-interconnect/card # set adminstate offline
FP9300-A /fabric-interconnect/card* # commit-buffer
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
    Id: 2
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Offline
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD191601DE
    Perf: N/A
    Admin State: Offline
    Power State: Off
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
FP9300-A /fabric-interconnect/card #
```

Blade Health Monitoring

Failsafe is engaged on a security module or engine when a specified number of unexpected application restarts are detected on a blade to prevent an endless boot loop condition, which can cause further side effects in a redundant HA or Cluster deployment.

Blade platform performs health checks periodically and reports it to the MIO. If the blade is in failed state, you will be notified with faults and error messages.

Faults and Error Messages

You can view the faults and error messages in the Overview page of the platform if there are any issues with the blade.

- Overview page—Security Module shows the fault symbol with the operational state as Fault.

- Security Module page—Service State in the blade will show as Fault. The 'i' icon displays the error message when you hover over.
- Logical Devices page—If logical devices are available and the security module goes faulty, the "i" icon displays the error message when you hover over.

Note You can configure and manage failsafe settings from FXOS CLI.