Security Module/Engine Management

About FXOS Security Modules/Security Engine

You can use the FXOS CLI to 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 2.
- Acknowledge—Brings newly installed security modules online. See Acknowledge a Security Module/Engine, on page 2.
- Power Cycle—Restarts the security module/engine. See Power-Cycling a Security Module/Engine, on page 3.
- 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 3.

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.

Note A module must be decommissioned before it can be deleted using the **delete decommissioned** command.

Procedure

Step 1 To decommission a module, enter the **decommission server** command:

decommission server {*ID* | *chassis-id/blade-id*}

Depending on the type of device hosting the module to be decommissioned, identify it using its module ID (4100 series), or the chassis number and the module number (9300 devices).

Example:

```
FP9300-A# decommission server 1/2
FP9300-A* #
```

Step 2 Enter the **commit-buffer** command to commit the change.

You can use the **show server decommissioned** command to view a list of decommissioned modules.

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 Enter `fabric-interconnect` mode:

scope fabric-interconnect

Step 2 Enter the **acknowledge slot** command after decommissioning and physically removing a module that will not be replaced, or after replacing a module with another that is not the same type (that is, with a different PID):

acknowledge slot

Example:

```
FP9300-A# scope fabric-interconnect
FP9300-A /fabric-interconnect # acknowledge slot 2
FP9300-A /fabric-interconnect* #
```

Step 3 Commit the configuration:

commit-buffer

Power-Cycling a Security Module/Engine

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

Procedure

Step 1 Enter /service-profile mode:

scope service-profile server {*chassis_id*>/*blade_id*}

Example:

```
FP9300-A # scope service-profile server 1/1
FP9300-A /org/service-profile #
```

Step 2 Enter one of the **cycle** commands:

- **cycle cycle-immediate**—power-cycles the module immediately.
- **cycle cycle-wait**—the system waits for up to five minutes for the application running on the module to shut down before power-cycling the module.

Example:

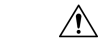
```
FP9300-A /org/service-profile # cycle cycle-wait
FP9300-A /org/service-profile* #
```

Step 3 Commit the buffer to power-cycle the module:

commit-buffer

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 Enter security services mode:

```
scope ssa
```

Step 2 Enter slot mode for the desired module:

```
scope slot {slot_id}
```

Example:

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot #
```

Step 3 Enter the **reinitialize** command:

Example:

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot # reinitialize
Warning: Reinitializing blade takes a few minutes. All the application data on blade will
get lost. Please backup application running config files before commit-buffer.
FP9300-A /ssa/slot* #
```

Step 4 Back up application configuration files as necessary.

Step 5 Commit the buffer to reinitialize the module:

```
commit-buffer
```

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

Step 6 You can use the **show detail** command to check the progress of the reformatting operation, the result of the reformatting (success or failure), and an error code if the operation fails.

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.

To view the status of the slot, use the `show detail` CLI:

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # show detail
Slot:
    Slot ID: 1
```

```
   Log Level: Info
   Admin State: Ok
   Oper State: Fault
   Disk Format State: Ok
   Disk Format Status:
   Clear Log Data: Available
Error Msg: Security Module is in failsafe mode. Applications are blocked from starting in
this mode. Connect to security module for troubleshooting or to disable failsafe mode. The
app-instance can also be deleted. Security Module: 1. Application: cisco-asa.99.1.20.52.
```

Troubleshooting and Debugging

You can monitor, configure, and reset the blade settings from FXOS CLI.

Use `show fault` and `show events` to monitor the security module:

```
Firepower /ssa/slot # show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F1546    2017-08-19T12:11:18.036    801162 Security Module 1 is in failed state.
 Error: Security Module is in failsafe mode. Applications are blocked from starting in this
 mode. Connect to security module for troubleshooting or to disable failsafe mode. The
app-instance can also be deleted. Security Module: 1. Application: cisco-asa.99.1.20.52.
```

```
Firepower /ssa/slot # show event
Creation Time               ID       Code     Description
--------------------------- -------- -------- -----------
2017-08-19T12:11:18.037    801163 E4197940 Slot 1 is in failed state. Error:Security Module
 is in failsafe mode. Applications are blocked from starting in this mode. Connect to
security module for troubleshooting or to disable failsafe mode. The app-instance can also
 be deleted. Security Module: 1. Application: cisco-asa.99.1.20.52.
```

Use the following CLIs to configure the security module:

```
Firepower-module> config ?
    syslog           => Configure syslog parameters for remote server and port
    vnic             => Configure specified VNIC
    memory           => Configure memory monitor
    disk             => Configure disk monitor
    process          => Configure process cpu monitor
   maxRestart      => Configure maximum restarts CSP. 0 shall mean Disable Restart. Default
 8
   restartTimeInter => Configure time in seconds to block all CSPs from starting if server
 restarts maxRestart in this interval. Default 3600
   restartCounters  => To reset the restart_count
```

- `config maxRestart`—Number of times a service/csp causes blade to reboot before the process manager stops starting the service. The default value is 8. The feature gets disabled if the value is set to 0 (Zero).

Note The FXOS maxRestart counter is increased when the logical app (ASA/Threat Defense) is not restarted properly. Afer restarting the logical app for 8 times, FXOS goes to failsafe mode. To recover FXOS from failsafe mode, you need to clear the maxRestart counter using the **config restartCounters reset** command, and reboot the logical device from chassis manager or reload FXOS.

- `config restartTimeInterval`—The time interval during which if the app reboots more than the number of times configured in maxRestart then the application does not restart. Default value is 3600 seconds.
- `show maxRestart`—Shows the maximum number of blade reboots permitted (default value is 8), the current number of restarts, and the time interval allowed for maximum number of reboots.

- `config restartCounters reset`—Resets the restart counter to 0.