SIOC Management

- SIOC Management in Cisco UCS Manager , on page 1
- Acknowledging an SIOC, on page 2
- Resetting the CMC, on page 3
- CMC Secure Boot, on page 3

SIOC Management in Cisco UCS Manager

You can manage and monitor all System Input/Output Controllers (SIOC) in a Cisco UCS domain through Cisco UCS Manager.

SIOC Removal or Replacement

You can remove or replace an SIOC from a chassis. Removal or replacement of an SIOC is a service-affecting operation, which requires you to power down the entire chassis.

Guidelines for SIOC Removal

- To remove the active SIOC, or both SIOCs, shut down and remove power from the entire chassis. You must disconnect all power cords to completely remove power.
- Removal of SIOCs from a chassis results in the entire chassis being disconnected from Cisco UCS Manager.

SIOC Removal

Do the following to remove an SIOC from the system:

1. Shut down and remove power from the entire chassis. You must disconnect all power cords to completely remove power.
2. Disconnect the cables connecting the SIOC to the system.
3. Remove the SIOC from the system.

SIOC Replacement

Do the following to remove an SIOC from the system and replace it with another SIOC:

1. Shut down and remove power from the entire chassis. You must disconnect all power cords to completely remove power.
2. Disconnect the cables connecting the SIOC to the system.
3. Remove the SIOC from the system.
4. Connect the new SIOC to the system.
5. Connect the cables to the SIOC.
6. Connect power cords and then power on the system.
7. Acknowledge the new SIOC.

   The server connected to the replaced SIOC is rediscovered.

Note If the firmware of the replaced SIOC is not the same version as the peer SIOC, then it is recommended to update the firmware of the replaced SIOC by re-triggering chassis profile association.

Acknowledging an SIOC

Cisco UCS Manager has the ability to acknowledge a specific SIOC in a chassis. Perform the following procedure when you replace an SIOC in a chassis.

Caution This operation rebuilds the network connectivity between the SIOC and the fabric interconnects to which it is connected. The server corresponding to this SIOC becomes unreachable, and traffic is disrupted.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **acknowledge sioc** {**1** | **2**}	Acknowledges the specified SIOC in the chassis.
Step 3	UCS-A /chassis* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example acknowledges SIOC 1 and commits the transaction:

```
UCS-A# scope chassis 3
UCS-A /chassis # acknowledge sioc 1
UCS-A /chassis* # commit-buffer
UCS-A /chassis #
```

Resetting the CMC

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope sioc** {**1** | **2**}	Enters the specified SIOC in the chassis.
Step 3	UCS-A /chassis/sioc # **scope cmc**	Enters the CMC of the selected SIOC slot.
Step 4	UCS-A /chassis/sioc/cmc # **reset**	Resets the CMC.
Step 5	UCS-A /chassis/sioc/cmc* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example resets the CMC on SIOC 1 and commits the transaction:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope sioc 1
UCS-A /chassis/sioc # scope cmc
UCS-A /chassis/sioc/cmc # reset
UCS-A /chassis/sioc/cmc* # commit-buffer
```

CMC Secure Boot

With Chassis Management Controller (CMC) secure boot, only Cisco-signed firmware images can be installed and run on the CMC. When the CMC is updated, the image is certified before the firmware is flashed. If certification fails, the firmware is not flashed. This prevents unauthorized access to the CMC firmware.

Guidelines and Limitations for CMC Secure Boot

- CMC secure boot is supported only on the Cisco UCS S3260 chassis.
- When chassis association is in progress, enabling secure boot on one of the SIOCs will result in a failed operation.
- After CMC secure boot is enabled, it cannot be disabled.
- CMC secure boot is specific to the SIOC on which it is enabled. If you replace the SIOC on which CMC secure boot is enabled, the **Secure boot operational state** field will now display the secure boot status of the new SIOC.
- After CMC secure boot is enabled on a chassis, you cannot move the chassis back to standalone mode and downgrade the firmware to a CMC firmware image earlier than Cisco IMC Release 2.0(13).

- The **Secure boot operational state** field shows the secure boot status. This can be one of the following:
  - **Disabled**—When CMC secure boot is not enabled. This is the default state.
  - **Enabling**—When CMC secure boot is being enabled.
  - **Enabled**—When CMC secure boot is enabled.

Enabling CMC Secure Boot

Cisco UCS Manager Release 3.1(2) introduces the ability to enable Chassis Management Controller (CMC) secure boot so that only Cisco-signed firmware images can be installed and run on the CMC.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope sioc** {**1** | **2**}	Enters the specified SIOC in the chassis.
Step 3	UCS-A /chassis/sioc # **scope cmc**	Enters the CMC of the selected SIOC slot.
Step 4	UCS-A /chassis/sioc/cmc # **enable secure-boot**	Enables CMC secure boot. If you run this command when the secure boot state is **enabled**, Cisco UCS Manager will display an error message and the operation will fail. **Note** This is an irreversible operation. You cannot disable CMC secure boot.
Step 5	UCS-A /chassis/sioc/cmc* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example enables CMC secure boot on SIOC 1 and commits the transaction:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope sioc 1
UCS-A /chassis/sioc # scope cmc
UCS-A /chassis/sioc/cmc # enable secure-boot
Warning: This is an irreversible operation.
Do you want to proceed? [Y/N] Y
UCS-A /chassis/sioc/cmc* # commit-buffer
```