



Chassis Profiles and Templates

- [About the Cisco UCS S3260 Storage Server, page 1](#)
- [Chassis Profiles, page 2](#)
- [Chassis Profile Template Details, page 4](#)
- [Chassis Profile Details, page 4](#)
- [Viewing Chassis Profile Configuration Status, page 6](#)
- [Chassis Discovery Policy, page 7](#)
- [Chassis Maintenance Policy, page 8](#)
- [Chassis Firmware Package Policy, page 8](#)
- [Disk Zoning Policies, page 9](#)
- [Compute Connect Policy, page 10](#)
- [Viewing System IO Configuration Status, page 12](#)

About the Cisco UCS S3260 Storage Server

The Cisco UCS S3260 Storage Server is a dense storage rack server with dual server nodes, optimized for large datasets used in environments such as big data, cloud, object storage, and content delivery. It belongs to the Cisco UCS C-Series rack-mount servers product family.

The Cisco UCS S3260 Storage Server is designed to operate in a standalone environment and as part of the Cisco Unified Computing System with Cisco UCS Manager integration. It assumes almost the same characteristics of its predecessors, the Cisco UCS C3160 Rack Server, but with the following additional features:

- System IO Controllers (SIOC).
- Support of up to two server modules.
- Capability to operate in a standalone mode.
- Chassis level functionality in the standalone mode—Shared components such as storage adapters, fans and power supply units are configured at the chassis level.

- Data Center Ethernet connectivity to a server host through a shared dual virtual interface card (VIC).
- Individual hard disk drives (HDD) can be assigned to either server in the dedicated or shared mode.

In addition, one of the server slots in the Cisco UCS S3260 Storage Server can be utilized by a storage expansion module for an additional four 3.5" drives. The server modules can also accommodate two solid state drives (SSD) for internal storage dedicated to that module. The chassis supports Serial Attached SCSI (SAS) expanders that can be configured to assign the 3.5" drives to individual server modules.

For more information, see the *Cisco UCS 3260 Quick Reference Guide*.

Chassis Profiles

A chassis profile defines the storage, firmware and maintenance characteristics of a chassis. You can create a chassis profile for the Cisco UCS S3260 Storage Server. When a chassis profile is associated to a chassis, Cisco UCS Central automatically configures the chassis to match the configuration specified in the chassis profile.

A chassis profile includes four types of information:

- **Chassis definition**—Defines the specific chassis to which the profile is assigned.
- **Maintenance policy**—Includes the maintenance policy to be applied to the profile.
- **Firmware specifications**—Defines the chassis firmware package that can be applied to a chassis through this profile. Cisco UCS Central 2.0(1a) introduces delivery of critical fixes and security updates through service packs. In addition to the Blade and Rack server bundles for firmware updates, you must also download the service pack bundles to complete the firmware upgrade. Service packs are specific and cumulative to a maintenance release and are supported for Cisco UCS Manager version 3.1(3) and above. You can choose the firmware to be updated by using a service pack.
- **Disk zoning policy**—Includes the zoning policy to be applied to the storage disks.

Guidelines and Recommendations for Chassis Profiles

In addition to any guidelines or recommendations that are specific to the policies included in chassis profiles and chassis profile templates, such as the disk zoning policy, adhere to the following guidelines and recommendations that impact the ability to associate a chassis profile with a chassis:

- Each chassis can be associated with only one chassis profile. Similarly, each chassis profile can be associated with only one chassis at a time.
- Chassis profiles are supported only on the Cisco UCS S3260 Storage Server.
- C bundles earlier than Cisco UCS Manager Release 3.1(2) are not supported on the Cisco UCS S3260 Storage Server.

Creating or Editing a Chassis Profile Template

- Step 1** In the **Actions** bar, type **Create Chassis Profile Template** and press enter.
- Step 2** In **Basic**, select the **Organization** where you want to create the chassis profile template.
- Enter a **Name** and optional **Description** and **User Label** to help identify the chassis profile template.
 - Choose a **Template Instantiation Mode**:
 - Initial**—Chassis profiles created from this template inherit all the properties of the template, but will not be updated when this template is updated.
 - Updating**—Chassis profiles created from this template remain connected and are automatically updated when this template is updated.
- Step 3** Click the **Policies** tab to assign existing policies to the chassis profile template.
You can click on a policy and use the drop-down option on the right to assign the policy to the template.
- Step 4** Click **Create**.
-

Creating a Chassis Profile from a Template

- Step 1** In the **Actions** bar, type **Create Chassis Profile from Template** and press Enter.
- Step 2** Choose the chassis profile template that you want to use from the **Chassis Profile Template to Instantiate**, and select the **Organization** where you want to create the chassis profile.
- Step 3** Determine the type of **Chassis Profile Naming Convention** that you want to use. This can be one of the following:
- Manual Entry**—Enter the chassis profile names as comma separated values. A chassis profile will be created for each value entered.
 - Advanced**—Enter the prefix, suffix, number of chassis profiles, the first number, and the number of digits.
The chassis profiles are created using the format prefixXXsuffix. For example, three chassis profiles starting at 400 and using 4 digits would be called prefix0400suffix, prefix0401suffix, and prefix0402suffix.
- Note** You can create up to 99 chassis profiles at one time from a single template.
- Step 4** Click **Create**.
-

Manually Assigning a Chassis to a Chassis Profile

-
- Step 1** Click **Browse Tables** and choose **Profiles**.
- Step 2** On the **Profiles** page, choose the chassis profile that you want to modify.
- Step 3** On the **Chassis Profile** page, click the **Tools** icon and choose **Assign Chassis Manually**.
- Step 4** Choose the chassis that you want to assign to the chassis profile.
- Step 5** Click **Assign**.
-

Chassis Profile Template Details

The Chassis Profile Template details page displays detailed information on the chassis profile template. From here you can:

- View audit logs.
- Create a chassis profile from this chassis profile template.
- Delete, clone, or rename the chassis profile template.

Chassis Profile Details

The Chassis Profile details page displays detailed information on the chassis profile. From here you can:

- View logs and configuration status.
- Create a chassis profile template from this chassis profile.
- Bind or unbind from the chassis profile template.
- Assign or unassign a chassis.
- Reapply the configuration to the associated chassis.
- Delete, clone, or rename the chassis profile.
- Acknowledge and decommission a chassis.
- Turn on or turn off the Locator LED for a chassis.
- Launch Cisco UCS Manager for the specific Cisco UCS domain.

**Note**

- Your browser must have pop-ups enabled.
- For Cisco UCS Manager release 3.1(2) or later, this launches the HTML5 GUI. If the Cisco UCS Manager credentials match the credentials for your Cisco UCS Central login, then the system will automatically log in to the Cisco UCS Manager GUI without prompting for the login information.
- For Cisco UCS Manager release 3.1(1) or previous, this launches the Java-based GUI.

Editing a Chassis Profile

-
- Step 1** From the **Chassis Profile Details** view, select **Edit** and press Enter.
- Step 2** In **Basic**, enter a **Description** and **User Label** to help identify the chassis profile.
- Step 3** Click the **Policies** tab to assign the existing policies to the chassis profile. You can click on a policy and use the drop-down list on the right to assign the Chassis Firmware Package policy to the profile.
- Step 4** Click **Create**.
-

Local Chassis Profiles

The Local Chassis Profile details page displays detailed information on a local chassis profile. Local chassis profiles are managed by Cisco UCS Manager.

From here you can:

- View logs.
- Acknowledge and decommission a chassis.
- Turn on or turn off the Locator LED for a chassis.
- Launch Cisco UCS Manager for the specific Cisco UCS domain.

**Note**

- Your browser must have pop-ups enabled.
- For Cisco UCS Manager release 3.1(2) or later, this launches the HTML5 GUI. If the Cisco UCS Manager credentials match the credentials for your Cisco UCS Central login, then the system will automatically log in to the Cisco UCS Manager GUI without prompting for the login information.
- For Cisco UCS Manager release 3.1(1) or previous, this launches the Java-based GUI.

Viewing Chassis Profile Configuration Status

-
- Step 1** Click the **Browse Tables** icon and choose **Profiles**.
- Step 2** Click **Chassis Profiles**.
- Step 3** Select the chassis profile for which you want to view configuration status.
- Step 4** On the detailed view for your selection, click the **Alerts** icon and choose **Configuration Status**. The **Configuration Status** page displays.
- Step 5** Click **Close** to close the window.
-

Chassis Profile Faults

To view consolidated faults of both the chassis profile and associated chassis, click the **Alerts** icon on the chassis profile page and choose **Faults**. The following information is displayed:

- **Filters**—Filter the data in the table by severity, fault type, and timestamp.
- **Code**—Unique identifier associated with the fault.
- **Timestamp**—Day and time at which the fault occurred.
- **Cause**—Brief description of what caused the fault.
- **Affected Object**—The name and location of the component that this issue affects, and the domain name where it is found.
- **Fault Details**—More information about the log message.
- **Severity**—Displays an icon denoting the fault severity. The icon key displays below the table.
- **Action**—Any action required by the fault.

Chassis Profile Inventory Faults

You can view faults from each chassis associated with a chassis profile. To view chassis faults, click the **Faults** icon in the **Chassis Fault Summary** section of a **Chassis Profile** details page. The **Faults Logs** page displays information on the type and severity level of the fault and allows you to monitor and acknowledge the faults.

- **Filters**—Filter the data in the table by severity, fault type, and timestamp.
- **Code**—Unique identifier associated with the fault.
- **Timestamp**—Day and time at which the fault occurred.
- **Cause**—Brief description of what caused the fault.
- **Affected Object**—The name and location of the component that this issue affects, and the domain name where it is found.
- **Fault Details**—More information about the log message.
- **Severity**—Displays an icon denoting the fault severity. The icon key displays below the table.
- **Action**—Whether user acknowledgment is required.

Chassis Discovery Policy

The chassis discovery policy determines whether a specific chassis is included in a fabric port channel after chassis discovery. This allows for different chassis connectivity modes per fabric interconnect. By default, the chassis discovery policy is set to global. This means that connectivity control is configured when the chassis is newly discovered, using the settings configured for Chassis/FEX Link Grouping Policy on the domain group system policy. Depending on the domain group equipment policy setting, the chassis links are either all set to port channel or single links.

When you set the chassis discovery policy manually for a chassis, you have the following options:

- **None**—All links functions as single links.
- **Port Channel**—All links functions as a port channel.
- **Global**—All links use the settings in the Equipment policy for the entire domain group.

For more information, see .

**Note**

The chassis discovery policy is applicable only when the hardware configuration supports fabric port channels, and the chassis is directly connected to a fabric interconnect.

Configuring a Chassis Discovery Policy

-
- Step 1** Click the **Browse Tables** icon and choose **Chassis**.
 - Step 2** Click a chassis.
 - Step 3** On the chassis page, click the **Tasks** icon and choose **Discovery Policy**.
 - Step 4** Choose whether to use the global domain group policy, force all links to function as a port channel, or force all links to function as single links.
 - Step 5** Click **Save**.
-

Chassis Maintenance Policy

A chassis maintenance policy determines when a chassis is rebooted when changes are made to the chassis profile. By default, the chassis maintenance policy always requires that a user acknowledges the changes before the reboot occurs.

Creating or Editing a Chassis Maintenance Policy

All chassis maintenance policies require user acknowledgment before any maintenance-related configuration can be applied to the chassis.

-
- Step 1** In the **Actions** bar, type **Create Maintenance Policy** and press Enter.
 - Step 2** In the **Maintenance Policy Create** dialog box, choose **Chassis**.
 - Step 3** Choose the **Organization** where you want to create the policy, and enter the **Name** and optional **Description**. The name is case sensitive.
 - Step 4** Click **Evaluate** to view the impact of the policy.
 - Step 5** Click **Create**.
-

Chassis Firmware Package Policy

The Chassis Firmware Package Policy page displays details about an individual chassis firmware package policy. From this page, you can edit the policy or view the chassis to which the policy is associated.

Creating or Editing a Chassis Firmware Package Policy

- Step 1** In the **Actions** bar, type **Create Chassis Firmware Package Policy** and press Enter.
- Step 2** In the **Chassis Firmware Package Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.
- Step 3** Enter a **Name** and optional **Description**.
The policy name is case-sensitive.
- Step 4** Select the **Chassis Version** of the firmware, as required for your environment.
Note Only Cisco UCS Manager version 3.1(2) and above C bundles are supported.
- Step 5** Select the applicable **Service Pack Version** for the firmware.
If the service pack version you select is for Cisco UCS Manager release earlier than 3.1(3), the following Warning message displays:
Package Version of all bundles in the pack must match
Ensure that the service pack you download is compatible with the supported Cisco UCS Manager version. For more information about applicable service packs, see *About Service Packs* in the *Cisco UCS Central Administration Guide*.
For more information on downloading images, see *Downloading Firmware from Cisco.com* in the *Cisco UCS Central Administration Guide*.
- Step 6** In the **Components** tab, click **Add** to select any components that want to exclude from the firmware update. The included and excluded components display. The following components can be excluded:
- Chassis adapter
 - Chassis board controller
 - Chassis management controller
 - Local disk
 - SAS expander
 - Storage controller
- a) To exclude all components, click **Excluded Components**.
- b) To remove an excluded component, select it and click **Delete**.
- Step 7** Click **Create**.
Note To understand the impact of the policy, click **Evaluate**.
- Step 8** The **Configuration Settings** window displays the images of the service pack bundles that get updated.
-

Disk Zoning Policies

Disk zoning policies allow you to manage the disks on your chassis servers when associated in a chassis profile.

Depending on the storage controller, the disk-sharing modes that are supported for your disk zoning policy may vary. For more information about disk-sharing modes supported on the storage controllers, see the Storage Server Features and Components Overview section in the *Cisco UCS Manager Storage Management Guide*.

Creating or Editing a Disk Zoning Policy

-
- Step 1** In the **Actions** bar, type **Create Disk Zoning Policy** and press Enter.
- Step 2** In the **Basic** tab, enter the **Name** and optional **Description**.
- Step 3** Choose whether to enable **Preserve Configuration**.
If enabled, any disk zoning that is configured on the chassis remains as is when the chassis is associated to a chassis profile. If disabled, enter your disk zoning preferences in the **Disk Slots** tab.
- Step 4** In **Disk Slots**, assign the disks as follows:
- **Unassigned**—The disks are not visible to any server, and can be allocated as dedicated, shared, or chassis hot spare. Specify a **Slot Range** for the unassigned disks.
 - **Dedicated**—Disks are assigned to the specified controller, and are not visible to any other controllers in the chassis. Specify the **Slot Range** for disks to assign to a server and a controller and choose the **Server ID** and **Controller ID** from the drop-down. For HBA controllers, you can assign the disks to a combination of either server and controller.

Note Beginning Cisco UCS Central 2.0 and Cisco UCS Manager release 3.1(3), disk zoning supports a second RAID controller (1 or 2) on Cisco S3260 Storage servers.
For the RAID controllers, you can select only one server per combination of the controllers 1 or 2. An Unsupported Hardware Configuration message displays if you select an unsupported server.
 - **Shared**—Disks are visible to multiple servers and controllers, and can be used for disk failover. When you specify a slot range, these disks are seen by all controllers in the Cisco C3260 chassis.

Note Cisco UCS Central 2.0 and Cisco UCS Manager 3.1(3) do not support selection of server and controller for shared mode.
 - **Chassis Global Hot Spares**—Disks will be made available to a controller if no hot spares on that controller are available. You can the select disk slot you want to reserve as hot spare. An error displays when you select an unsupported configuration.
- Step 5** Click **Create**.
-

Compute Connect Policy

Starting with Cisco UCS Central release 2.0, you can create a Compute Connect Policy that lets you utilize a Cisco UCS C3260 chassis' second Cisco Storage I/O Control (SIOC). Cisco SIOCs allow prioritization of storage resources during periods of contention. The Compute Connect Policy is applied to a Cisco UCS C3260 chassis through a chassis profile and depends on infrastructure, CMC, and server firmware. When the policy is successfully applied to a chassis, the CMC performs a reboot and the server receives two adapter instances.



Note The Compute Connect Policy is supported on Cisco UCS Manager 3.1(3) and later.

Cisco produces the Cisco UCS C3260 chassis in two configurations:

- Single Server
- Dual Server

Before Cisco UCS Central release 2.0, the data path was only through a single SIOC. The CIMC firmware now supports using both SIOCs to process data. There are two single-server configurations for the Cisco UCS C3260 chassis:

- Single Server—Uses an HDD expansion tray in the second slot to provide four more disk slots.
- Single Server with IO Expander Tray—Provides an extra mezzanine storage controller and two PCI slots.

The Compute Connect Policy introduces two new values available during the policy creation process:

- Single-Server Single SIOC (legacy mode)
- Single-Server Dual SIOC



Note An attempt to push the policy to any chassis models other than a Cisco UCS C3260 chassis results in an error message. For Cisco UCS Manager releases prior to 3.1(3), Cisco recommends that you maintain this policy as unassigned in the **Global Chassis Profile** before associating it to the chassis.

Creating a Compute Connect Policy

Before You Begin

- Cisco C3260 Chassis should be in Single Server Configuration
- The chassis, server, and Cisco UCS Manager firmware should be release 3.1(3) or later

-
- Step 1** In the **Actions** bar, type **Create Compute Connect Policy** and press Enter.
- Step 2** In the **Compute Connect Policy** dialog box, choose the organization where you want to create the Compute Connect Policy.
- Step 3** In the **Compute Connect Policy** dialog box, complete the following fields:
- **Name**—The name of the policy. This name can be between 1 and 16 alphanumeric characters other than **-** (hyphen), **_** (underscore), **:** (colon), and **.** (period), and you cannot change this name after the object is saved.
 - **Description**—A description of the policy. Cisco recommends that you include information about where and when the policy can be used. Enter up to 256 characters.

- **Server SIOC Connectivity**—Choose a connectivity mode:
- **Single Server Single SIOC**
- **Single Server Dual SIOC**

Step 4 Click **Create** to create the new policy.

Viewing System IO Configuration Status

Step 1 Click the **Browse Tables** icon and choose **Chassis**.

Step 2 Click a storage chassis.

Step 3 On the storage chassis page, click **System IO Controller**.

Step 4 Click a system IO controller to expand it.

Step 5 Click the **Tools** icon and choose **Configuration Status**.

Step 6 On the storage chassis page, click **System IO Controller**.

On the **System IO Controller** dialog box, you can view the SIOC, the CMC, and the chassis discovery configuration status.

Step 7 Click **Close**.
