Cisco Intersight Managed Mode Fabric Interconnect Admin Guide

First Published: 2022-11-17

Last Modified: 2024-07-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Communications, Services, Bias-free Language, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

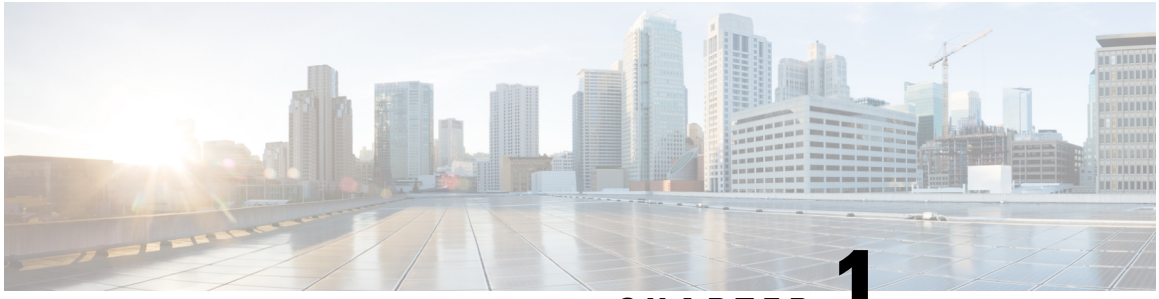
Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Bias-Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Communications, Services, Bias-free Language, and Additional Information



CHAPTER 1

Device Console

Device Console

Overview

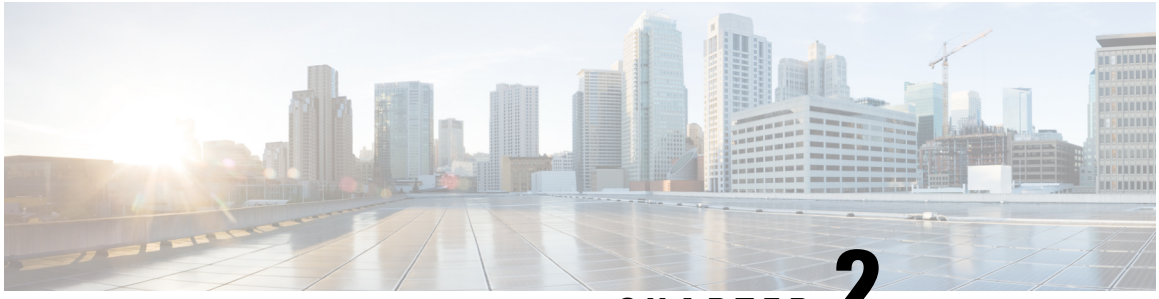
The Device Console is an application running on the Intersight Managed Mode Fabric Interconnect.

It provides system information such as the model, serial number, and firmware version of the Fabric Interconnects. It allows you to configure the Device Connector. It shows the Inventory details of the Servers, Chassis, and Fabric Extenders. You can also generate tech support bundles containing diagnostic information to troubleshoot and analyze issues. In addition, you can perform power and LED operations for servers.

Accessing the Device Console

To access the Device Console user interface, log in to the Fabric Interconnect using a management IP address or DNS hostname if available. You must have administrator privileges to access Device Console UI.

Device Console



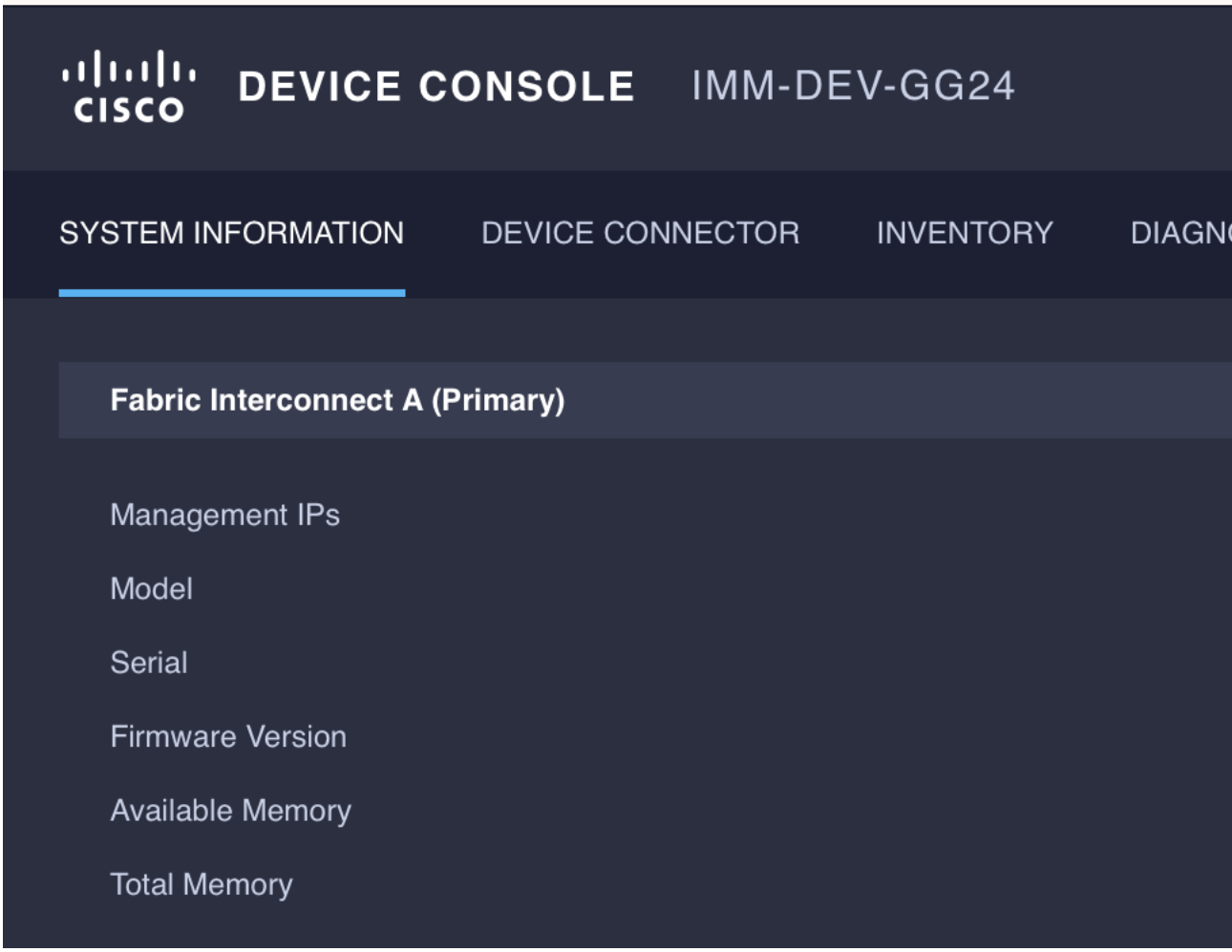
CHAPTER 2

System Information

Device Console User Interface

The Device Console UI consists of the following main elements:

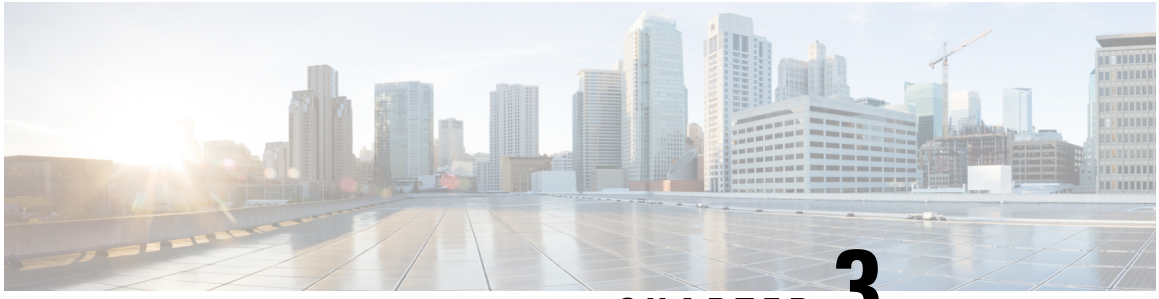
- A central pane that includes four tabs: System Information, Device Connector, Inventory and Diagnostic Data.
- A top navigation menu that contains the Help menu and Logout button.



System Information

The **System Information** tab provides details for the Fabric Interconnects, which includes a summary of the fabric interconnects properties, memory size, and firmware versions.

Details	Description
Management IP	Displays the Cisco UCS management IP address.
Model	Displays the Cisco UCS Fabric Interconnect series model.
Serial	Displays the host ID/serial number of the server.
Firmware Version	Displays the current firmware version running on the Fabric Interconnect.
Available Memory	Displays the available memory.
Total Memory	Displays the total allocated memory.

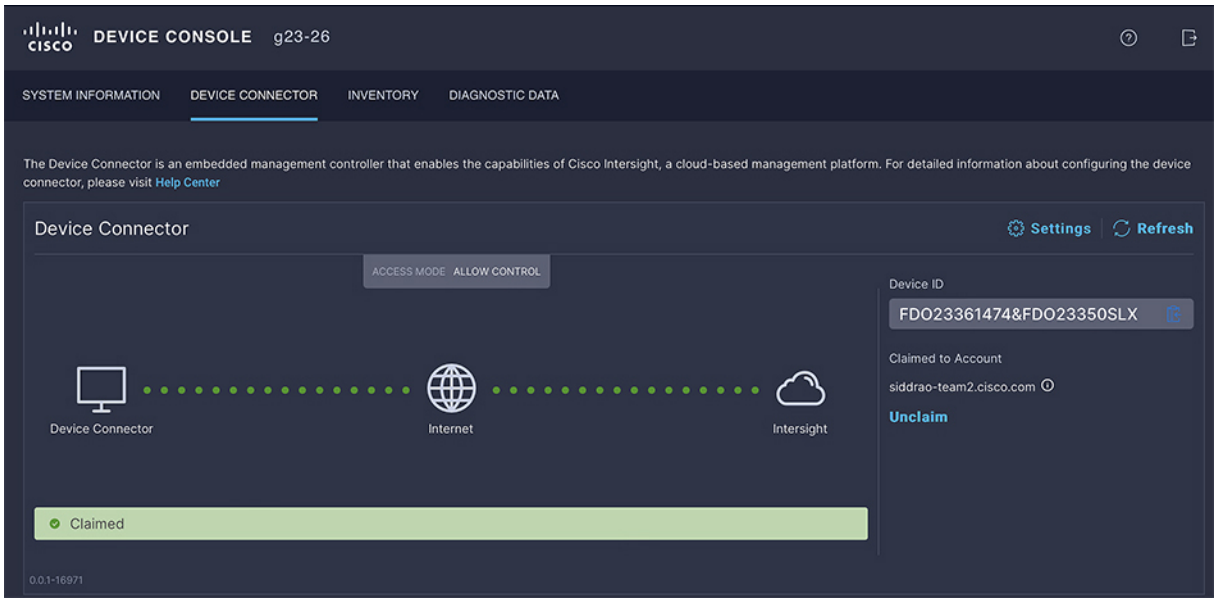


CHAPTER 3

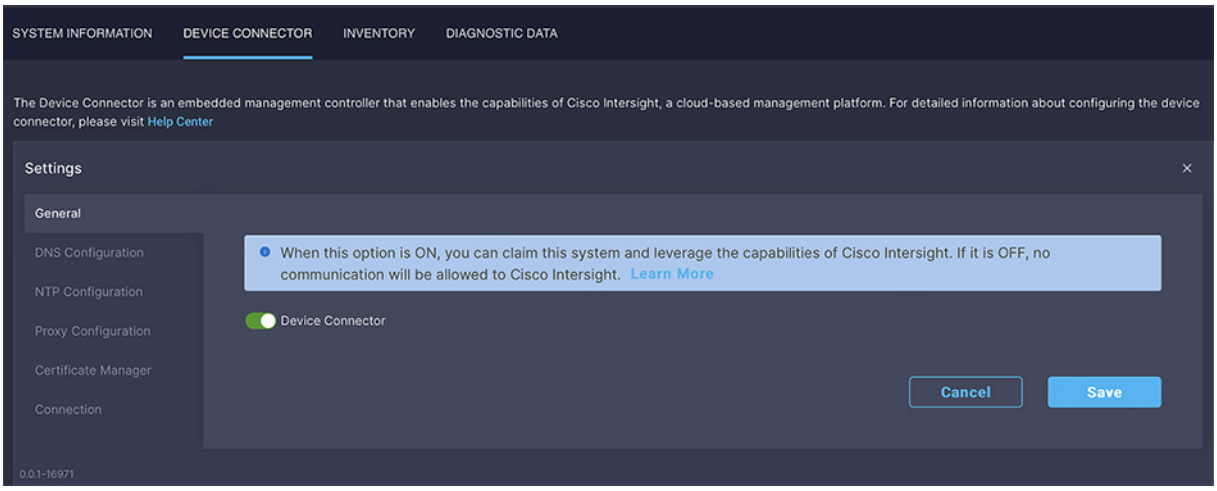
Device Connector

Device Connector

The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight. The Device Connector tab provides connectivity details of Device Connector with Intersight.



You can also configure the parameters for the Device Connector through **Settings**.



Property	Essential Information
Device Connector	Graphically shows the following: • Status of the connection between the Device Connector, Internet, and Intersight • The Access Mode of the Device Connector • Claim status of the device.

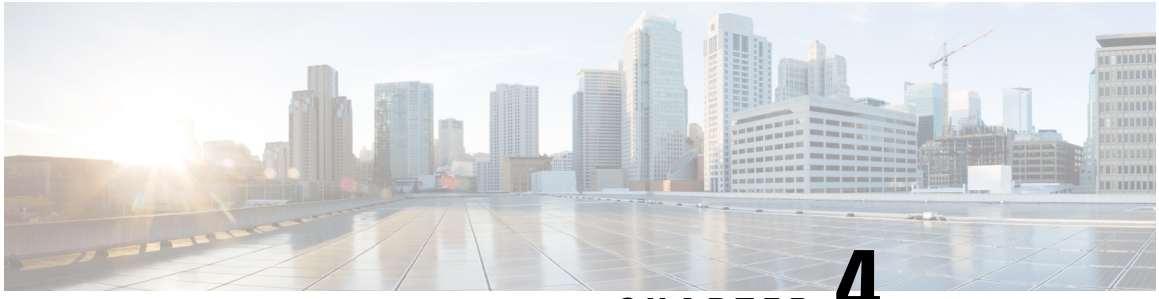
Property	Essential Information
Settings	

Property	Essential Information

	Allows you to configure the following Device Connector settings:
	• **General**—Allows you to enable or disable Cisco Intersight management. This can be one of the following:
	  • On—Enables Cisco Intersight management. You can claim this system and leverage the capabilities of Cisco Intersight.
	  • Off—Disables Cisco Intersight management. No communication will be allowed to Cisco Intersight.
	  Access Mode—Allows you to configure access as Read-only or Allow Control.
	  • Read-only—When the Read-only access mode is selected, you cannot configure the device through Intersight.
	  • Allow Control—When the Allow Control access mode is selected, you have full control to configure the device through Intersight.
	• **DNS Configuration**—Allows you to configure the domain name settings (Fully Qualified Domain Name) and DNS server settings (IP address or Fully Qualified Domain Name.
	• **NTP Configuration**—Allows you to configure the NTP settings (IP address or Fully Qualified Domain Name).
	  Note The changes to the Device Console DNS and NTP configuration are temporary and for diagnostic or recovery purposes. Persistent changes to the Device Console configuration must be made through the Domain Profile deployed to the Fabric Interconnect.
	• **Proxy Configuration**—Allows you to configure whether HTTPS proxy settings are disabled or manually configured. This can be one of the following:
	  • Off—Select this option if you want to disable the HTTPS proxy settings configuration.

Property	Essential Information
	This is the default HTTPS proxy setting. • On—Select this option if you want to enable the HTTPS proxy settings configuration. • Proxy Hostname/IP—Enter the proxy hostname or IP address. • Proxy Port— Enter the proxy port number. • Authentication—Enable this option to authenticate access to the proxy server. Enter the Username and Password to authenticate access. **Note** Proxy authentication is now enabled for Fabric Interconnect in Intersight Managed Mode. This feature allows the Fabric Interconnect Device Connector to authenticate through a password-based authentication type on the configured proxy server. • The device connector does not mandate the format of the login credentials, they are passed as-is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name will depend on the configuration of the HTTP proxy server. • **Certificate Manager**—Allows you to view a list of trusted certificates and import a valid trusted certificate. • **Connection**—Displays the result of the connection check between the Device Connector and Intersight . To know more about configuring and troubleshooting a device connector, see Configuring Device Connector.
Device ID	The unique serial number of the device.
Claimed to Account	ID of the Intersight user who claimed the device.

Property	Essential Information
Unclaim	Unclaim a claimed device. **Note** Use the Unclaim option on the Device Connector only when you do not have access to the account that the target was originally claimed to, or if you lose connection to Intersight and you want to unclaim the target locally from the endpoint. For more details on unclaiming a target see Unclaim Target.



CHAPTER 4

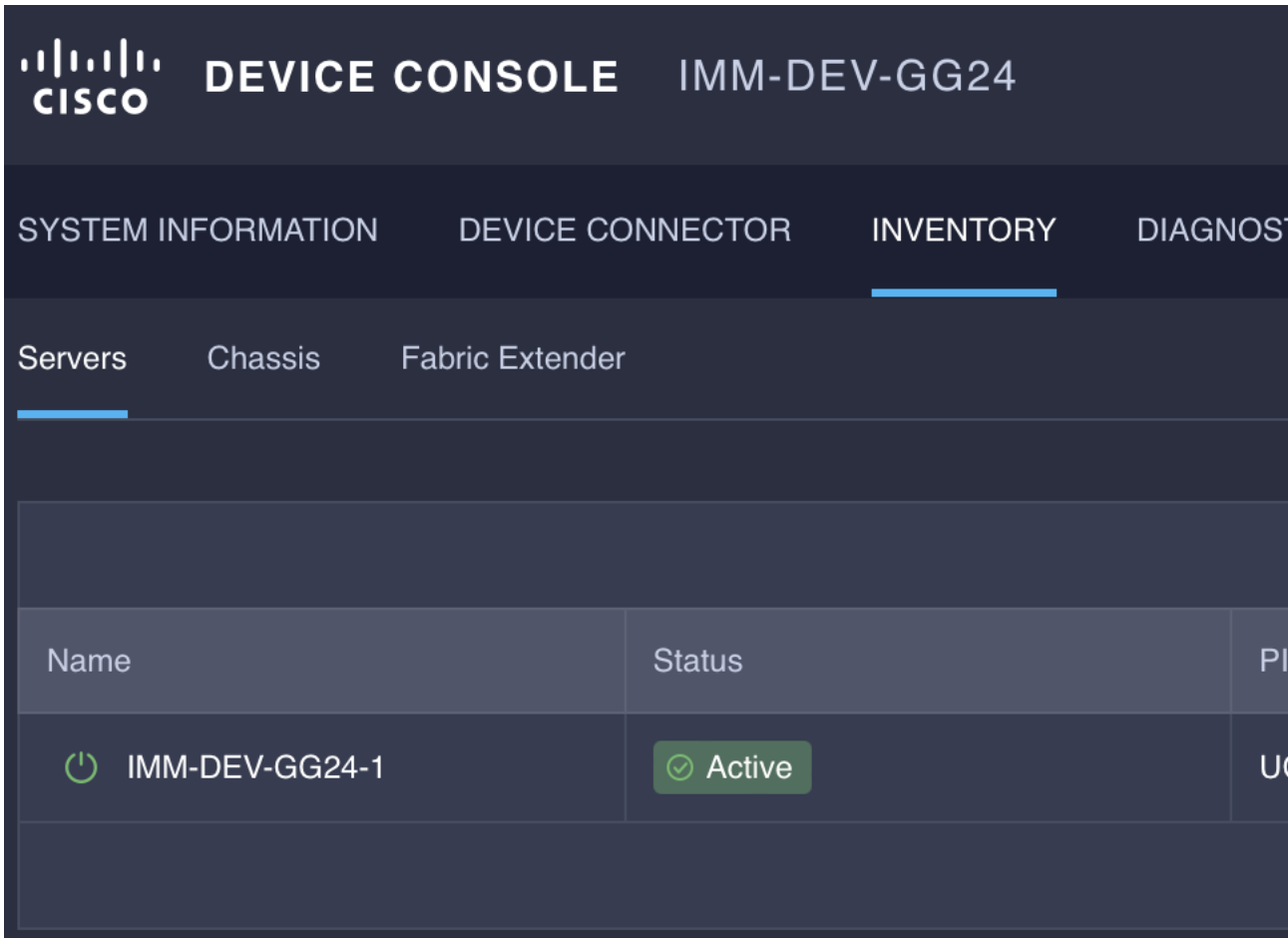
Inventory

Inventory

The **Inventory** tab includes three subtabs: Servers, Chassis, and Fabric Extender that provide detailed inventory details for servers, chassis, and Fabric Extender. In addition, these subtabs also include the ability to launch the API Explorer to perform Redfish™ based operations such as power cycling the server and retrieving BIOS tokens.

Servers

The **Servers** subtab provides detailed information about all the servers connected through the Fabric Interconnect. This information is based on the data stored in the local database on the Fabric Interconnect.



Details	Description
Name	Displays the name of the server.
Status	Displays the lifecycle state of the server. The values can be: • None — When the server has been recommissioned but discovery is yet to start. • Active — When the server is discovered. • Decommissioned —When the server is removed from the Cisco UCS configuration. However, the server hardware physically remains in the Cisco UCS instance. • DiscoveryFailed — When the server discovery has failed. • SlotMismatch — When the configuration of a blade server is not correct and server rediscovery is required in the slot.
PID	Displays the PID of the server.
Serial	Displays the host ID/serial number of the server.

Details	Description
User Label	Displays a user label that contains the serial number, PID, and the VID. This serial number is displayed in the management software of the server.

In this subtab, you can perform the following server actions:

- Power On/Off
- Launch KVM
- Launch API Explorer
- Generate Tech Support Bundle

Note The resulting techsupport bundles can be downloaded from the **Diagnostic Data** tab.

Performing Redfish™ Based Server Operations from the API Explorer

Redfish™ Based Server Operations - Examples

For an overview of Redfish™ based server operations and examples, see https://intersight.com/apidocs/introduction/overview/

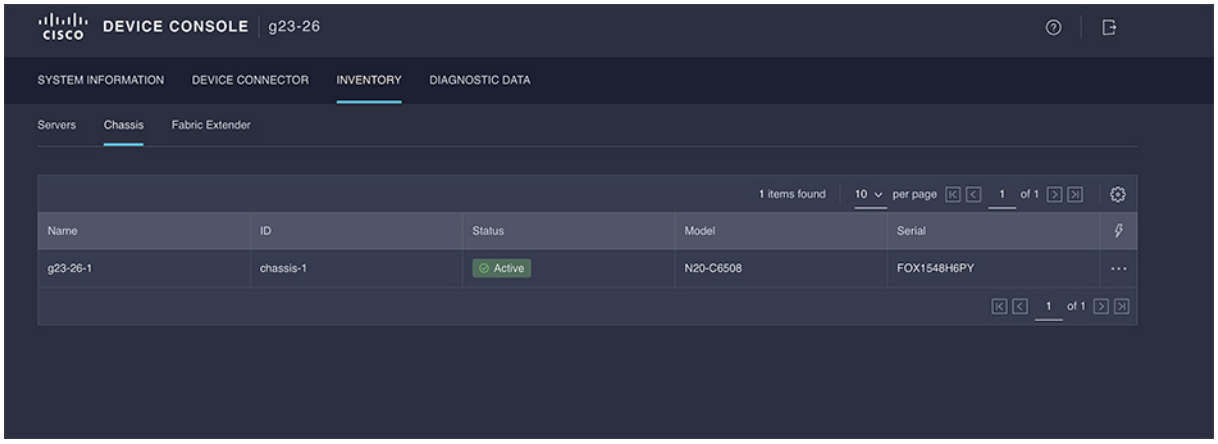
Launching the API Explorer

To perform Redfish™ Based server operations from the API Explorer, do the following:

1. On the **Servers** table view, select the server and click the ellipsis (…).
2. From the ellipsis (…), select **Launch API Explorer**.

Chassis

The **Chassis** subtab provides detailed information about all the chassis connected through the Fabric Interconnect.



Details	Description
Name	Displays the name for the chassis.
ID	Displays the unique ID for the chassis.
Status	Displays the status of the chassis. The values can be: • Active — When the chassis is discovered. • Decommissioned —When the Chassis is physically present and connected, but temporarily removed from the Cisco UCS configuration. • DiscoveryFailed — When the chassis discovery has failed.
Model	Displays the chassis model.
Serial	Displays the host ID/serial number of the chassis.

In this subtab, you can perform the following chassis operations:

- Launch API Explorer (IOM 1)
- Launch API Explorer (IOM 2)
- Generate Tech Support Bundle

Performing Redfish™ Based Chassis Operations from the API Explorer

Redfish™ Based Chassis Operations - Examples

For an overview of Redfish™ based chassis operations and examples, see https://intersight.com/apidocs/introduction/overview/

Launching the API Explorer

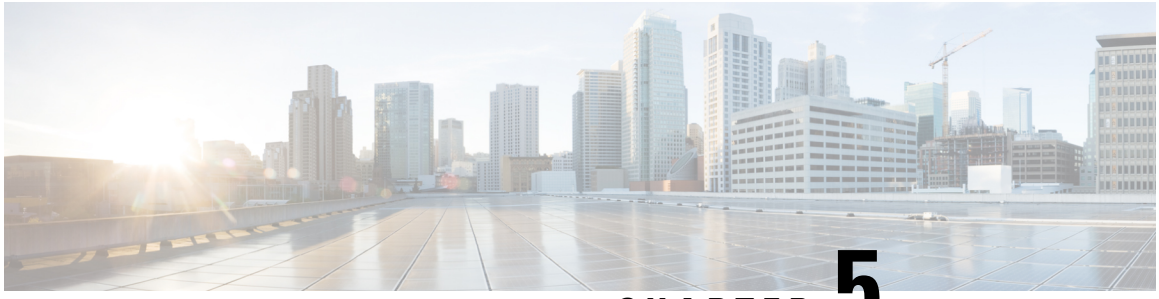
To perform Redfish™ Based chassis operations from the API Explorer, do the following:

1. On the **Chassis** table view, select the chassis and click the ellipsis (…).
2. From the ellipsis (…), select **Launch API Explorer**.

Fabric Extender

The **Fabric Extender** subtab provides detailed information about all the Fabric Extender (FEX) connected through the Fabric Interconnect.

Details	Description
Name	Displays the name for the FEX.
Identifier	Displays the unique ID for the FEX.
Lifecycle	Displays the current state of the FEX lifecycle. The values can be: • Online — When the FEX is connected. • Decomissioned — When the FEX is physically present and connected, but temporarily removed from the Cisco UCS configuration. • Unclaimed — When the FEX has not been claimed to the Intersight account. • Discovery Failure — When the discovery of FEX has failed.
Model	Displays the FEX model.
Serial	Displays the host ID/serial number of the FEX.
Description	Displays the description for the FEX, if any.

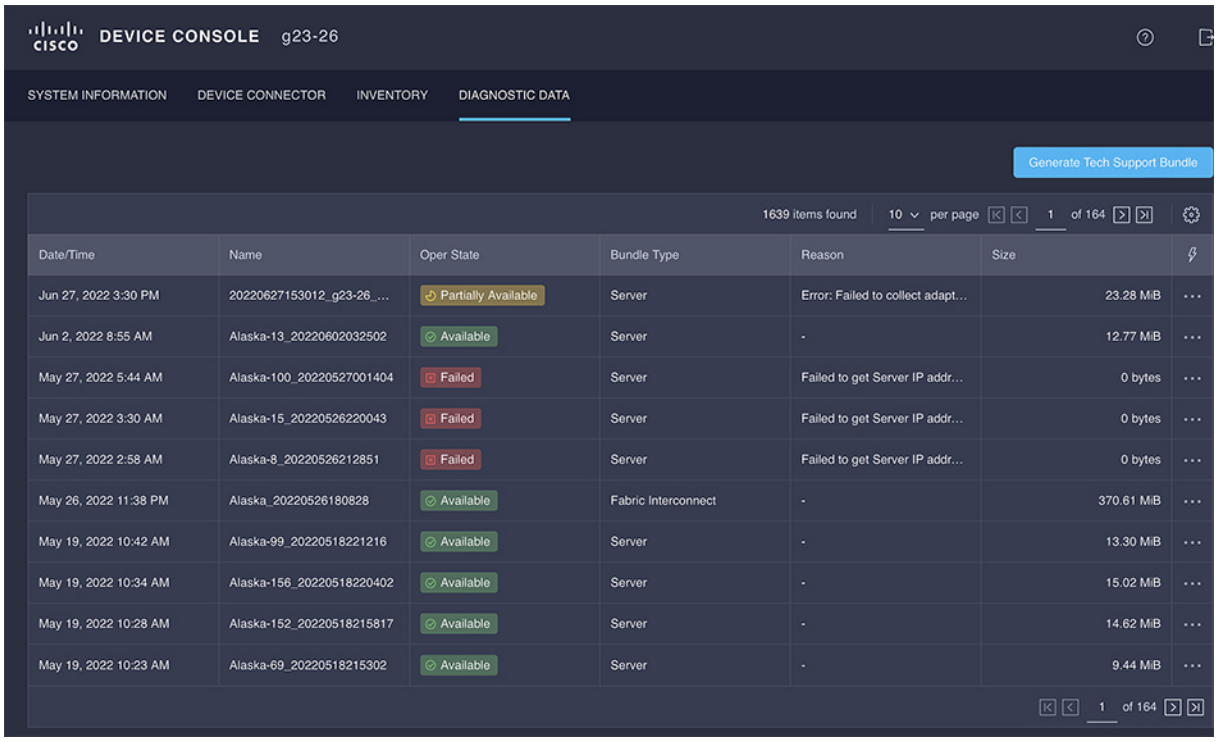


CHAPTER 5

Diagnostic Data

Diagnostic Data

From the **Diagnostic Data** tab, you can collect diagnostic data for severs, chassis and Fabric Interconnects for troubleshooting and further analysis.



You can generate tech support bundles for the following:

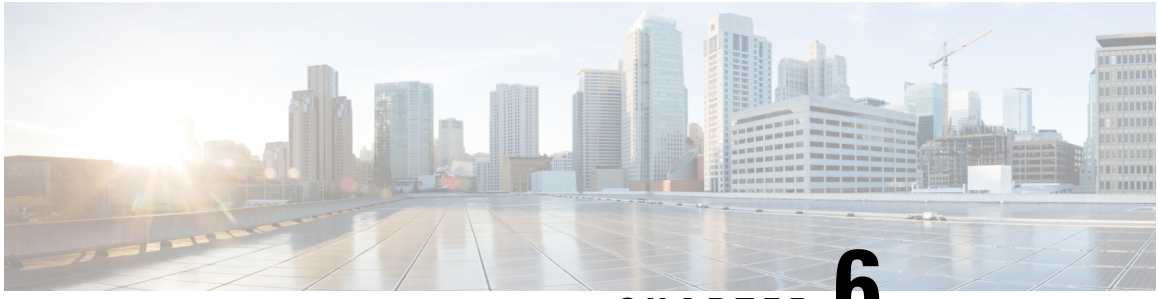
- Chassis—Contains technical support data for a given chassis including IOMs..
- Server—Contains technical support data for blade and rack servers including all adapters. For blade severs, tech support data is collected for IOMs. For blade severs, tech support data is collected for IOMs.

- Fabric Interconnect—Contains technical support data for Fabric Interconnect. The data can be for either the peer or local Fabric Interconnect.

Generating and Downloading Tech Support Bundles

To generate and download a tech support bundle, do the following:

1. In the **Diagnostic Data** tab, click **Generate Tech Support Bundle** in the right side of the screen above the Diagnostic Data table view.
2. In the **Generate Tech Support Bundle** dialog box, select either **Chassis**, **Server** or **Fabric Interconnect** to generate relevant tech support bundles.
   - **Chassis**—From the **Chassis** drop-down, select the chassis for which the tech support bundle must be generated. Click **Generate**. You can see the progress for the tech support bundle generation in the **Diagnostic Data** table view. Once the generation is complete, you will see the status under the **Oper State** as **Available**. In the relevant row for the chassis, from the ellipsis (…), click **Download** to start the download. This operation may take several minutes to complete. The downloaded file is saved in your default download location.
   - **Server**—From the **Server** drop-down, select the server for which the tech support bundle must be generated. Click **Generate**. You can see the progress for the tech support bundle generation in the **Diagnostic Data** table view. Once the generation is complete, you will see the status under the **Oper State** as **Available**. In the relevant row for the server, from the ellipsis (…), click **Download** to start the download. This operation may take several minutes to complete. The downloaded file is saved in your default download location.
   - **Fabric Interconnect**—You can choose either **Local Switch** or **Local Peer Switches** to generate the tech support bundles. Click **Generate**. You can see the progress for the tech support bundle generation in the **Diagnostic Data** table view. Once the generation is complete, you will see the status under the **Oper State** as **Available**. In the relevant row for the Fabric Interconnect, from the ellipsis (…), click **Download** to start the download. This operation may take several minutes to complete. The downloaded file is saved in your default download location.



CHAPTER 6

Device Console CLI

Device Console CLI

You can use the Device Console CLI interface if you want to troubleshoot your devices, or if your devices are not connecting to Cisco Intersight. Below are the commands that you can use:

Device Connector

You can perform the following operations on the Device Connector:

- Connect to the Device Connector—To connect to the Device Connector through the Intersight CLI shell, use the **connect device-connector** command.

  connect device-connector
- Show the Device Connector version—To show the Device Connector version, use the **show version** command.

  show version
- Update the Device Connector—To update the Device Connector image on the Fabric Interconnect-B and then Fabric Interconnect-A, use the **update-device-connector** command.

Note Images are not accessible to the customers. This operation is used by TAC for recovery purpose.

update-device-connector workspace:/ | **volatile:/** *filename*

System Information

You can perform the following operations to view system information:

- Show the system clock—To display the system date and time, use the **show clock** command.

  show clock

Note Setting the time on the FI requires NTP. NTP should be configured in the Device Console and in the NTP Policy of the Domain Profile.

- Show CLI history—To display the history of CLI commands run in the session, use the **show cli history** command.

  show cli history
- Show SSH key—To display the list of SSH public key of the host, use the **show sshkey** command.

  show sshkey
- Show IP debug information—To display the ip address and the interfaces on both the management and default namespaces, use the **show mgmt-ip-debug** command.

  show mgmt-ip-debug
- Show IP table information—To displays the ip table entries on both the management and default namespaces, use the **show mgmt-ip-tables** command.

  show mgmt-ip-tables
- Show the contents of a file—To display the contents of a file, use the **show file** command.

  show file *file-path*
- Show processes—To display a list of all processes that are currently running, use the **show processes** command.

  show processes
- Show audit log—To display the audit log of the Fabric Interconnect, use the **show audit** command.

  show audit

Servers

You can perform the following operations on the servers:

- Connect to the IOM/IFM —To connect to an IO module or to an Intelligent Fabric module, use the **connect iom** command.

  connect iom *chassis-id*

Note This command is not applicable for the chassis of Cisco UCS X-Series Direct.

- Connect to the CIMC—To connect to the CIMC (Cisco Integrated Management Controller), use the **connect cimc** command.

  connect cimc *chassis-id/blade-id* | *rack-id*

  For Cisco UCS X-Series Direct,

connect **cimc** *chassis-id/blade-id*

Note You can clear the memory counters using the reset memory error command

reset_all_memory_errors

- Connect to the Adapter —To connect to an adapter, use the **connect adapter** command. This command can be used to connect to the adapters on B-Series, C-Series, and X-Series servers.

  For B-Series/X-Series servers:

  connect **adapter** *chassis-id/blade-id/adapter-id*

  For C-Series servers:

  connect **adapter** *rack-id/adapter-id*

Syntax Description

chassis-id	Chassis identification number
blade-id	Blade identification number
rack-id	Rack identification number
adapter-id	Adapter identification number

- Upgrade CIMC on a B-Series server—To upgrade the Cisco Integrated Management Controller (CIMC) on a B-Series server, use the following command:

  upgrade-equipment cimc -- type blade -- chassisid x -- slotid y --imagepath /bootflash/intersight-cache//*/ucs-intersight-server-xxxx.y.y.yy.bin*
- Upgrade BIOS on a B-Series server—To upgrade the BIOS on a B-Series server, use the following command:

  upgrade-equipment bios -- type blade -- chassisid x -- slotid y --imagepath /bootflash/intersight-cache//*/ucs-intersight-server-xxxx.y.y.yy.bin*

PMON Processes

PMON (Process Monitor) processes includes all the internal processes associated with the **mgmt plugin**. PMON processes help in restarting the processes during FI recovery/troubleshooting.

You can perform the following operations to view Pmon processes on the Fabric Interconnect:

- Manage pmon processes—To start, stop, and view the status of the pmon or connector processes, use the **pmon** command.

  pmon { **start** | **stop** | **state** } [**connector**]

Technical Support

You can perform the following operations to fetch the technical support bundle:

- Show tech-support—To download the contents of the tech-support bundle for a specific device, use the **show tech-support** command.
  - **show tech-support server** *blade-id*
  - **show tech-support chassis** *chassis-id*
  - **show tech-support fex** *fex-id*
  - **show tech-support switch** *switch-id*

Directory Operations

You can perform the following directory operations:

- Change directory—To change directories, use the **cd** command.

  cd { **workspace:/** [*path*] | **volatile:/** [*path*] | [*path*] | **usbdrive1:/** | **usbdrive2:/** }
- View current directory—To view the current working directory, use the **pwd** command.

  pwd
- List contents of a directory—To list the contents of the current working directory, use the **ls** command.

  ls
- Create a directory—To create a directory under allowed directories, use the **mkdir** command.

  mkdir { **workspace:/** [*path*] | **volatile:/** [*path*] | [*path*] | **usbdrive1:/** | **usbdrive2:/** }
- Delete a directory—To remove a directory, use the **rmdir** command.

  rmdir { **workspace:/** [*path*] | **volatile:/** [*path*] | [*path*] | **usbdrive1:/** | **usbdrive2:/** }
- Copy a file—To copy a file from one directory to another, use the **cp** command.

  cp [*from-filesystem:*] [*from-path*] *filename* [*to-filesystem:*] *to-path* [*dest-filename*]
- Move a file—To move a file from one directory to another, use the **mv** command.

  mv [*from-filesystem:*] [*from-path*] *filename* [*to-filesystem:*] *to-path* [*dest-filename*]
- Delete a file—To remove a file from a directory, use the **rm** command.

  rm { **workspace:/** [*path*] | **volatile:/** [*path*] | [*path*] | **usbdrive1:/** | **usbdrive2:/** }

Other Operations

These are the other operations that you can perform:

- Activate secure-fpga—To enable secure Field-Programmable Gate Array (FPGA) on the Fabric Interconnect, use the **activate secure-fpga** command.

  activate secure-fpga
- Set Management IP—To configure management IP address, network mask, and gateway address on a Fabric Interconnect, use the **set management-network** command.

  set management-network *ip-address* *netmask/preix_length* *gateway*

- Show management log—To display the management log of the services running on a Fabric Interconnect, use the **tail-mgmt-log** command.

  tail-mgmt-log *module_name*
- Use SSH to connect—To log in to a host that supports SSH, use the **ssh** command.

  ssh *host-name*
- Use Telnet to connect—To log in to a host that supports Telnet, use the **telnet** command.

  telnet *host-name* [*port-num*]
- Display IPv4 network routes—To view the route to an IPv4 network host, use the **traceroute** command.

  traceroute [**-s** *source-address*] *address*
- Display IPv6 network routes—To view the route to an IPv6 network host, use the **traceroute6** command.

  traceroute6 [**-s** *source-address*] *address*
- Diagnose network connectivity—To diagnose basic network connectivity for IPv4 addresses, use the **ping** command.

  ping [**-c** *count*] [**-s** *packet-size*] [**-i** *interval*] [**-w** *timeout*] { *host-ip-address* | *host-name* }
- Diagnose network connectivity—To diagnose basic network connectivity for IPv6 addresses, use the **ping6** command.

  ping6 [**-c** *count*] [**-s** *packet-size*] [**-i** *interval*] [**-w** *timeout*] { *host-ip-address* | *host-name* }
- Reboot—To reboot the system, use the **reboot** command.
- Connect to NX-OS—To connect to NX-OS, use the **connect nxos** command.
- Erase configuration—To erase configuration on the Fabric Interconnect, use the **erase-configuration** command.
- Change administrator password—To change the administrator password on the Fabric Interconnect, use the **change-password** command.
- Clear the SSH public key—To clear from cache the SSH public key of a remote host, use the **clear-sshkey** command.

  clear-sshkey *host-name*
- Update the name of the Fabric Interconnect and the Peer FI using **change-domain-name** command.
- Change the manageable mode of the server using **change-mode** command.
- Clear the screen using **clear** command.
- Clear an entry from the Intersight firmware cache using **clear-firmware-cache** command.
- For initial HA setup, start cluster server using **cluster-start** command.

Note It is used internally while adding an FI to a cluster.

- Connect to an endpoint using **connect** command.
- To view the list of entries in the Intersight firmware cache, use the **list-firmware-cache** command.
- To view the list of server operations and their usage (led-status power power-status led), use the **server** command.
- To update the Device management package on Fabric Interconnect, use the **update-management-package** command.

Note Packages are not accessible to the customers. This operation is used by TAC for recovery purpose.

update-management-package **workspace:/** | **volatile:/** *filename*

- **help** command displays help.
- Exit the program using **exit** command.