Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data

Exporting Technical Support Data

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Technical Support Data**.

Step 4 In the **Export Technical Support Data** dialog box, complete the following fields:

Name	Description
Export Technical Support Data to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

Name	Description

Export Technical Support Data through drop-down list	**Note** **Front Panel USB** option is visible only if **Smart Access USB** is enabled and a USB storage device is connected to the server.
	
	You can export the technical support data to a remote server or to a USB storage device connected to a server. You can choose one of the following:
	• **Remote**— This allows you to export the technical support data to a remote server using one of the following protocols:
	  • **TFTP**
	  • **FTP**
	  • **SFTP**
	  • **SCP**
	  • **HTTP**
	  Note If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint.
	  The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
	• **Front Panel USB**—This allows you to export the technical support data to a USB storage device connected to the server.

Server IP/Hostname field	The IP address or hostname of the server on which the support data file should be stored. Depending on the setting in the **Export Technical Support Data to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server. **Note** If the server includes any of the supported network adapter cards, the data file also includes technical support data from the adapter card.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Export**.

What to do next

Provide the generated report file to Cisco TAC.

Downloading Technical Support Data to a Local File

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate Technical Support Data for Local Download**.

Step 4 In the **Download Technical Support Data to Local File** dialog box, complete the following fields:

Name	Description
Generate Technical Support Data radio button	Cisco IMC disables this radio button when there is no technical support data file to download. Click **Generate** to create the data file. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file.
Regenerate Technical Support Data radio button	Cisco IMC displays this radio button when a technical support data file is available to download. To replace the existing support data file with a new one, select this option and click **Regenerate**. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file.
Download to local file radio button	Cisco IMC enables this radio button when a technical support data file is available to download. To download the existing file, select this option and click **Download**. **Note** If the server includes any of the supported network adapter cards, the data file also includes technical support data from the adapter card.
Generate button	Allows you to generate the technical support data file.
Download button	Allows you to download the technical support data file after it is generated.

Step 5 Click **Generate** to create the data file. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file..

What to do next

Provide the generated report file to Cisco TAC.

Resetting to Factory Default

On rare occasions, such as an issue with the current running firmware or troubleshooting a server, you might require to reset the server components to the factory default. When this happens, all user-configurable settings are reset.

This procedure is not part of the normal server maintenance. After you reset the server components, you are logged off and must log in again. You might also lose connectivity and might need to reconfigure the network settings. Some of the inventory information might not be available during this transition.

When you reset the BMC to factory settings, the serial number is displayed in the Cisco IMCXXXXXX format, where XXXXXX is the serial number of the server.

Important **When you move VIC adapters from other generation C-Series servers (for example M4 servers) to the M5 generation C-Series servers or M5 servers to other generation servers, you must reset the adapters to factory defaults.**

Before you begin

You must log in as a user with admin privileges to reset the server components to factory defaults.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Reset to Factory Default**.

Step 4 In the **Reset to Factory Default** dialog box, review the following information:

Actions	Description
Reset to factory Default Setting of drop-down list	Allows you to select the chassis or BMCs for which you want to reset the factory default setting. This can be one of the following: • **Chassis** • **BMC1** • **BMC2**

Name	Description
All checkbox	If checked, it resets all the components of the server to factory settings. Expand to select the specific component that you want to reset to factory settings.
BMC checkbox	If checked, it resets the BMC to factory settings. **Note** After you reset the BMC to factory settings, the serial number is displayed in the Cisco IMCXXXXXX format, where XXXXXX is the serial number of the server. After factory defaults of BMC NIC Mode, **Shared LOM Extended** is configured by default.
Storage checkbox	If checked, it resets all the available storage adapters to factory settings. When you reset a storage adapter, the data on the disk is not modified but the virtual drive meta data will be erased which may result in data loss. Expand to select the specific storage adapters that you want to reset to factory settings. **Note** The host must be powered on to reset storage adapters to factory defaults.
VIC checkbox	If checked, it resets all the available VICs to factory settings. Expand to select the specific VICs that you want to reset to factory settings. **Note** The host must be powered on to reset VIC adapters to factory defaults.
Reset button	Resets the selected components to the factory settings. **Note** When you reset to factory default settings, the network configuration mode is set to **Cisco Card** mode by default for C125 M5 servers. For other C-Series servers, NIC mode is set to **Shared LOM Extended** by default.

Step 5 Click **Reset** to reset the selected components to the factory-default settings.

A reboot of Cisco IMC, while the host is performing BIOS POST (Power on Self Test) or is in EFI shell, powers down the host for a short amount of time. Cisco IMC powers on when it is ready. Upon restart, the network configuration mode is set to **Cisco Card** mode by default.

Exporting and Importing the Cisco IMC Configuration

Exporting and Importing the Cisco IMC Configuration

To perform a backup of the Cisco IMC configuration, you take a snapshot of the system configuration and export the resulting Cisco IMC configuration file to a location on your network. The export operation saves information from the management plane only; it does not back up data on the servers. Sensitive configuration information such as user accounts and the server certificate are not exported.

You can restore an exported Cisco IMC configuration file to the same system or you can import it to another Cisco IMC system, provided that the software version of the importing system is the same as or is configuration-compatible with the software version of the exporting system. When you import a configuration file to another system as a configuration template, you must modify system-specific settings such as IP addresses and host names. An import operation modifies information on the management plane only.

The Cisco IMC configuration file is an XML text file or JSON file whose structure and elements correspond to the Cisco IMC command modes.

Note The configuration file is supported in XML format in Cisco UCS M5 and M6 servers in GUI, CLI, XML API and Redfish API interfaces.

The configuration file is supported in JSON format in Cisco UCS M7 servers in GUI, CLI, XML API and Redfish API interfaces.

When performing an export or import operation, consider these guidelines:

- You can perform an export or an import while the system is up and running. While an export operation has no impact on the server or network traffic, some modifications caused by an import operation, such as IP address changes, can disrupt traffic or cause a server reboot.
- You cannot execute an export and an import simultaneously.

You can perform an import or an export operation on the following features:

- Cisco IMC version

Note You can only export this information.

- Network settings
- Technical support
- Logging control for local and remote logs
- Power policies
- BIOS - BIOS Parameters

Note Precision boot is not supported.

- Communication services
- Remote presence
- User management - LDAP
- Event management
- SNMP

Exporting the Cisco IMC Configuration

Note For security reasons, this operation does not export user accounts or the server certificate.

Before you begin

Obtain the backup remote server IP address.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Configuration**.

Step 4 In the **Export Configuration** dialog box, complete the following fields:

Name	Description
Select Component for Export drop-down list	The component type. This can be one of the following: • **BMC** • **VIC Adapter(s)** Depending on the component you choose, the configuration of that component is exported.

Name	Description
Export To drop-down list	The location where you want to save the configuration file. This can be one of the following: • **Local**: Select this option and click **Export** to save the configuration file to a drive that is local to the computer running the Cisco IMC GUI.. When you select this option, Cisco IMC GUI displays a **File Download** dialog box that lets you navigate to the location to which the configuration file should be saved. • **Remote Server**: Select this option to import the configuration file from a remote server. When you select this option, Cisco IMC GUI displays the remote server fields. • **Front Panel USB**: Select this option to export the configuration file to a USB storage device connected to the server. **Note** • The configuration file is supported in XML format in Cisco UCS M5 and M6 servers in GUI, CLI, XML API and Redfish API interfaces. • The configuration file is supported in JSON format in Cisco UCS M7 servers in GUI, CLI, XML API and Redfish API interfaces. • Front Panel USB option to export Cisco IMC configuration is available only if Smart Access USB is enabled and a USB storage device is connected to the server. • This option is available only when you choose **BMC** in the Select Component drop-down list.

Name	Description
Export To drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server to which the configuration file will be exported. Depending on the remote server type selected in the **Export to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Passphrase	The passphrase that uses the AES256 algorithm to encrypt the LDAP and SNMP v3 user passwords in the exported configuration files. Enter a string of 6 to 127 characters. Do not enter the following characters: ! # $ & < > ? ; ' | ` ~ \ % ^ ( )"

Step 5 Click **Export**.

Importing the Cisco IMC Configuration

Before you begin

If you want to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is disabled on this server before you do the import. If SNMP is enabled when you perform the import, Cisco IMC does not overwrite the current values with those saved in the configuration file.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Import Configuration**.

Step 4 In the **Import Configuration** dialog box, complete the following fields:

Name	Description
Select Component for Import drop-down list	The component type. This can be one of the following: • **BMC** • **VIC Adapter(s)** Depending on the component you choose, the configuration of that component is imported.
Import From drop-down list	The location of the configuration file. This can be one of the following: • **Local**: Select this option to import the configuration file to a drive that is local to the computer running Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import. • **Remote Server**: Select this option to import the configuration file from a remote server. When you select this option, Cisco IMC GUI displays the remote server fields. • **Front Panel USB**: Select this option to import the configuration file from a USB storage device connected to the server. **Note** • The configuration file is supported in XML format in Cisco UCS M5 and M6 servers in GUI, CLI, XML API and Redfish API interfaces. • The configuration file is supported in JSON format in Cisco UCS M7 servers in GUI, CLI, XML API and Redfish API interfaces. • Front Panel USB option to import Cisco IMC configuration is available only if Smart Access USB is enabled and a USB storage device is connected to the server. • This option is available only when you choose **BMC** in the Select Component drop-down list.

Name	Description
Import From drop-down list	**Note** These options are available only when you choose **Remote**. The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server on which the configuration file resides. Depending on the remote server type selected in the **Import From** drop-down list, the name of the field might vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Passphrase	The passphrase that uses the AES256 algorithm to encrypt the LDAP and SNMP v3 user passwords in the imported configuration files. Enter a string of 6 to 127 characters. Do not enter the following characters: ! # $ & < > ? ; ' | ` ~ \ % ^ ( )" **Note** If you edit the encrypted sections in the configuration file and try to import it, the edits will be ignored and the import operation displays a partially successful message.

Step 5 Click **Import**.

Generating Non Maskable Interrupts to the Host

In some situations, the server might hang and not respond to traditional debug mechanisms. By generating a non maskable interrupt (NMI) to the host, you can create and send a crash dump file of the server and use it to debug the server.

Depending on the type of operating system associated with the server, this task might restart the OS.

Before you begin

- You must log in as a user with admin privileges.
- The server must be powered on.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate NMI to Host**.

Step 4 In the **Generate NMI to Host** dialog box, review the following information:

Actions	Description
Generate NMI to drop-down list	Allows you to select the server for which you want to generate the non maskable interrupt (NMI). This can be one of the following: • **Server 1** • **Server 2**

Step 5 Click **Send**.

This action sends an NMI signal to the host, which might restart the OS.

Adding or Updating the Cisco IMC Banner

You can add or update the Cisco IMC banner by entering important information such as copyright or customized messages. Complete the following steps:

Before you begin

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Add/Update Cisco IMC Banner**.

Step 4 In the **Add/Update Cisco IMC Banner** dialog box, complete the following fields:

Name	Description
Banner (80 Chars per line. Max 2K Chars.) field	Enter copyright information or messages that you want to display on the login screen, before logging on to the Web UI or the command line interface.
Restart SSH checkbox	When checked, the active SSH sessions are terminated after you click the **Save Banner** button.

Step 5 Click **Save Banner**.

What to do next

Viewing Cisco IMC Last Reset Reason

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, view the following information under the **Last Reset Reason** area.

Name	Description
Component field	The component that was last reset.

Name	Description
Status field	The reason why the component was last reset. This can be one of the following: • **watchdog-reset**—The watchdog timer expired due to kernel panic or hung task. • **ac-cycle**— PSU power cables are removed (no power input). • **graceful-reboot**— Cisco IMC reboot occurs. • **OOM-reset**—Cisco IMC reboots when memory reaches full capacity (without watchdog-timer).

Downloading Hardware Inventory to a Local File

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate Inventory Data**.

Step 4 In the **Generate Inventory Data** dialog box, complete the following fields:

Name	Description
Generate Inventory Data radio button	Cisco IMC displays this radio button when there is no hardware inventory data file to download.
Download to local file radio button	Cisco IMC enables this radio button when a inventory data file is available to download. To download the existing file, select this option and click **Download**.

Step 5 Click **Generate** to create the data file. When data collection is complete, select the **Download Inventory Data to Local File** radio button and click **Download** to download the file locally.

Exporting Hardware Inventory Data to a Remote Server

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Hardware Inventory Data to Remote**.

Step 4 In the **Export Hardware Inventory Data** dialog box, complete the following fields:

Name	Description
Export Hardware Inventory Data to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IP address or hostname of the server on which the data file should be stored. Depending on the setting in the **Export Hardware Inventory Data to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Export**.

Uploading a PID Catalog

Before you begin

You must log in as a user with admin privileges to upload a PID catalog.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Work** pane, click the **Upload PID Catalog** link.

The **Upload PID Catalog** dialog box appears.

Depending on the location of the catalog file, choose one of the options.

Step 4 In the **Upload PID Catalog from Local File** dialog box, click **Browse** and use the **Choose File to Upload** dialog box to select the catalog file that you want to upload.

Name	Description
File field	The PID catalog file that you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate file.

Step 5 In the **Upload PID Catalog from Remote Server** dialog box, complete the following fields:

Name	Description
Upload PID Catalog from Remote Server drop-down list	The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP**
Server IP/Hostname field	The IP address or hostname of the server on which the PID catalog information is available. Depending on the setting in the Upload PID Catalog from drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the catalog file on the remote server.
Username field	Username of the remote server.
Password field	Password of the remote server.

Name	Description
Upload button	Uploads the selected PID catalog. **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Cancel button	Closes the wizard without making any changes to the firmware versions stored on the server.

Activating a PID Catalog

Caution BMC reboots automatically once a PID catalog is activated.

You must reboot the server after activating a PID catalog.

Before you begin

You must log in as a user with admin privileges to activate a PID catalog.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Work** pane, click the **Activate PID Catalog** link.

The **Activate PID Catalog** dialog box appears. Complete the following fields:

Name	Description
Activate button	Allows you to activate the PID catalog.

Note The **Activate PID Catalog** link is greyed out when you log on to the system for the first time. It gets activated once you upload a PID catalog to the server. After you upload a PID file, the link remains active and you can activate the PID multiple times.

Deleting a PID Catalog

Caution BMC reboots automatically once a PID catalog is deleted.

You must reboot the server after deleting a PID catalog.

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the Utilities pane, click **Delete PID Catalog** and click **OK** to confirm.

Note You can delete a PID catalog only if it has been previously updated and activated.

Enabling Smart Access USB

When you enable the smart access USB feature, the front panel USB device disconnects from the host operating system and connects to Cisco IMC. After enabling the smart access USB feature, you can use the front panel USB device to export technical support data, import or export Cisco IMC configuration, or update Cisco IMC, BIOS, and VIC firmware.

The supported file systems for smart access USB are as follows:

- EXT2
- EXT3
- EXT 4
- FAT 32
- FAT 16
- DOS

Note Huge file support is not supported in BMC. For EXT 4 file system, huge file support has to be turned off.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area, click **Enable Smart Access USB**.

This is a toggle button. To disable smart access, click **Disable Smart Access USB**. This button is visible only after you enable smart access USB. When you disable the smart access USB feature, the front panel USB device disconnects from Cisco IMC and connects to the host operating system.

Enabling or Disabling Cisco Intersight Management

When you enable the Intersight management, it establishes a bi-directional communication between the Intersight Cloud application and the M5 server.

Note Port numbers 8888-8889 are reserved for Intersight communication.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, click **Device Connector**.

Step 3 In the **Intersight Management** area, click **On** to enable the Intersight management.
The Connection area displays the connection status of the Intersight management. If the device connector has not been able to establish a connection to Intersight management, review the recommendations provided in the **Details & Recommendations** drop-down list to fix the connection issues.

Step 4 Select the **Access Mode** as **Read-only** or **Allow Control.**
When the **Read-only** access mode is selected, then you cannot configure the device through Intersight. Therefore, any configuration that comes to the device connector through cloud is rejected with an error code. If the **Allow Control** mode is selected, then you have full control to configure the device through Intersight.

Step 5 To disable the Intersight management, click **Off**.
When you disable the Intersight management, the Connection area displays the connection status as **Administratively Disabled**.

Configuring HTTPS Proxy Settings for Device Connector

You can manually configure the HTTPS proxy settings of the server.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, click **Device Connector**.

Step 3 In the **Connections** area, click **HTTPS Proxy Settings** and enter the proxy settings:

Action Name	Description
Off button	Disables the HTTPS proxy settings.
Manual button	Allows you to manually configure the HTTPS proxy settings.
Proxy Hostname/IP field	The IP address or the host name of the proxy server.
Proxy Port field	The port number of the proxy server.
Authentication toggle button	Enabling this option allows you to provide the credentials for the proxy server.
Username field	The credentials for the proxy server.
Password field	

Step 4 In the **HTTPS Proxy Settings** dialog box, after adding the information, click **Save**.

Viewing Intersight Device Connector Properties

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, click **Device Connector**.

Step 3 In the **Intersight Management** area, review the following information:

Action Name	Description
Enabled radio button	Allows you to enable or disable the Intersight management. This can be one of the following: • **On**—Enables the Intersight management. You can claim this system and leverage the capabilities of Cisco Intersight. • **Off**—Disables the Intersight management. No communication will be allowed to Cisco Intersight.

Step 4 In the **Connection** area, review the following information:

Name	Description
Status field	Displays the status of the connection to Intersight. This can be one of the following: • **Administratively Disabled**—Indicates that the Intersight management has been disabled. • **DNS Misconfigured**— Indicates that the DNS details have not been configured in BMC. • **UCS Connect Network Error**—Indicates the invalid network configurations. • **Certificate Error**—Indicates invalid certificate. • **Claimed**—Indicates that the device is claimed in Intersight. • **Not Claimed**—Indicates that the device is registered, but not claimed in Intersight.
Retry Connection link	Allows you to retry the connection to Intersight. This option appears only when there are Intersight connection issues.
Details & Recommendations drop-down list	Lists the details and recommendations to fix the connection issues based on the status.
HTTPS Proxy Settings dialog box	Allows you to manually configure HTTPS proxy settings required for the Intersight connection.
Serial Number field	Displays the serial number of the BMC.
Security Token field	Appears when the connection status is **Not Claimed**. Use the security token to securely onboard the server in Intersight.

Step 5 In the **Connections** area, click **HTTPS Proxy Settings** and review the following information:

Action Name	Description
Off button	Disables the HTTPS proxy settings.
Manual button	Allows you to manually configure the HTTPS proxy settings.
Proxy Hostname/IP field	The IP address or the host name of the proxy server.
Proxy Port field	The port number of the proxy server.
Authentication toggle button	Enabling this option allows you to provide the credentials for the proxy server.
Username field	The credentials for the proxy server.
Password field	

Viewing Intersight Device Connector Properties

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, click **Device Connector**.

Step 3 In the **Intersight Management** area, review the following information:

Action Name	Description
Enabled radio button	Allows you to enable or disable the Intersight management. This can be one of the following: • **On**—Enables the Intersight management. You can claim this system and leverage the capabilities of Cisco Intersight. • **Off**—Disables the Intersight management. No communication will be allowed to Cisco Intersight.

Step 4 In the **Connection** area, review the following information:

Name	Description
Status field	Displays the status of the connection to Intersight. This can be one of the following: • **Administratively Disabled**—Indicates that the Intersight management has been disabled. • **DNS Misconfigured**— Indicates that the DNS details have not been configured in BMC. • **UCS Connect Network Error**—Indicates the invalid network configurations. • **Certification Validation Error**—Indicates invalid certificate. • **Claimed**—Indicates that the device is claimed in Intersight. • **Not Claimed**—Indicates that the device is registered, but not claimed in Intersight.
Access Mode	The mode will be **Allow Control** by default.
Details & Recommendations drop-down list	Lists the details and recommendations to fix the connection issues based on the status.
Device ID	This indicates the ID of the device.
Claim Code	This is the security code required to claim the device from Intersight. **Note** This code is available only when **Connection** status is **Not Claimed**.

Step 5 In the **Settings** area, review the following information:

Name	Description
General tab	**Access Mode** • **Read-only** — When the **Read-only** access mode is selected, you cannot configure the device through Intersight. • **Allow Control** — When the **Allow Control** mode is selected, you will have full control to configure the device through Intersight. **Configuration from Intersight only** This option is configurable only when **Allow Control** mode is enabled. The Configure Lockout options are as follows: **OFF**— To manage the device both locally and from Intersight you can turn OFF the option **Configuration from Intersight only** . The setting will terminate all the existing sessions (webUI, XML and CLI). **ON** — To lock out Cisco IMC configuration for Intersight you can turn ON the option **Configuration from Intersight only** . The setting will terminate all the existing sessions (webUI, XML and CLI). **Note** When you are logged in as admin in the Configuration Lock Out mode, the admin role will be mapped to the User role, so the interfaces behave as user logged in with the User role.
Proxy Configuration tab	Allows you to manually configure HTTPS proxy settings required for the Intersight connection.
HTTPS Proxy field radio button	OFF - Disables the HTTPS proxy settings. ON - Enables the HTTPS proxy settings.
Proxy Hostname/IP field	The IP address or the host name of the proxy server.
Proxy Port field	The port number of the proxy server.
Authentication toggle button	Enabling this option allows you to provide the credentials for the proxy server. **Note** 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.
Username field **Password** field	The credentials for the proxy server.

Name	Description
Certificate Manager tab	Allows you to view a list of trusted certificates and import a valid trusted certificate. • **Import**—Allows you to select and Import a CA signed certificate. **Note** The imported certificates must be in the *.pem (base64 encoded) format. • You can view the list of certificates with the following information: • **Name**—Common name of the CA certificate. • **In Use**—Whether the certificate in the trust store was used to successfully verify the remote server. • **Issued By**—The issuing authority for the certificate. • **Expires**—The expiry date of the certificate. **Note** You cannot delete bundled certificates (certificates with the lock icon).

Recovering PCIe Switch

Before you begin

- You must log in as a user with admin privileges.
- The server must be powered on.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Recover PCIe Switch**.

Step 4 In the **Recover PCIe Switch** dialog box, review the following information:

Name	Description
Controller drop-down	Lists the PCIe switches available on the server. You can select the switch on which you want to perform the recover controller action from this list.
Recover Controller button	Clicking on the recover controller button initiates the recovery of the chosen controller.

Name	Description
Cancel button	Cancels the action and closes the dialog box.