



Server Utilities

This chapter includes the following sections:

- [Enabling Or Disabling Smart Access USB, on page 1](#)
- [Exporting Technical Support Data, on page 3](#)
- [Exporting Technical Support Data to Front Panel USB Device, on page 5](#)
- [Rebooting the Cisco IMC, on page 6](#)
- [Clearing the BIOS CMOS, on page 7](#)
- [Recovering from a Corrupted BIOS, on page 7](#)
- [Resetting the Cisco IMC to Factory Defaults, on page 8](#)
- [Exporting and Importing the Cisco IMC Configuration, on page 9](#)
- [Adding Cisco IMC Banner, on page 14](#)
- [Deleting Cisco IMC Banner, on page 14](#)
- [Enabling Secure Adapter Update, on page 15](#)
- [Updating and Activating the Device Connector Firmware, on page 15](#)
- [Recovering a PCIe Switch, on page 17](#)

Enabling Or Disabling 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 be logged in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server # scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope smart-access-usb	Enters the smart access USB command mode.
Step 3	Server /cimc/smart-access-usb # set enabled { yes no }	set enabled yes enables smart access USB. set enabled no disables the smart access USB. When you enable the smart access usb feature, the front panel USB device disconnects from the host operating system. When you disable the smart access usb feature, the front panel USB device disconnects from CIMC.
Step 4	Server /cimc/smart-access-usb *# commit	Commits the transaction to the system.
Step 5	Server /cimc/smart-access-usb # show detail	Displays the properties of the smart access USB.

Example

This example shows how to enable smart access USB:

```
Server# scope cimc
Server /cimc # scope smart-access-usb
Server /cimc/smart-access-usb # set enabled yes
Enabling smart-access-usb feature will
disconnect front panel USB devices from
host operating system.
Do you wish to continue? [y/N] y
Server /cimc/smart-access-usb *# commit
Server /cimc/smart-access-usb # show detail
  Enabled: yes
  Storage Device attached: no
Server /cimc/smart-access-usb #
```

This example shows how to disable smart access USB:

```
Server# scope cimc
Server /cimc # scope smart-access-usb
Server /cimc/smart-access-usb # set enabled no
Disabling smart-access-usb feature will
disconnect front panel USB devices from CIMC.
Do you wish to continue? [y/N] y
Server /cimc/smart-access-usb *# commit
Server /cimc/smart-access-usb # show detail
  Enabled: no
```

```
Storage Device attached: no
Server /cimc/smart-access-usb #
```

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.



Important If any firmware or BIOS updates are in progress, do not export the technical support data until those tasks are complete.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope tech-support	Enters the tech-support command mode.
Step 3	Server /cimc/tech-support # set remote-ip <i>ip-address</i>	Specifies the IP address of the remote server on which the technical support data file should be stored.
Step 4	Server /cimc/tech-support # set remote-path <i>path/filename</i>	Specifies the file name in which the support data should be stored on the remote server. When you enter this name, include the relative path for the file from the top of the server tree to the desired location. Tip To have the system auto-generate the file name, enter the file name as default.tar.gz .
Step 5	Server /cimc/tech-support # set remote-protocol <i>protocol</i>	Specifies the protocol to connect to the remote server. It can be of the following types: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		<p>Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.</p> <p>If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p>
Step 6	Server /cimc/tech-support # set remote-username <i>name</i>	Specifies the user name on the remote server on which the technical support data file should be stored. This field does not apply if the protocol is TFTP or HTTP.
Step 7	Server /cimc/tech-support # set remote-password <i>password</i>	Specifies the password on the remote server on which the technical support data file should be stored. This field does not apply if the protocol is TFTP or HTTP.
Step 8	Server /cimc/tech-support # commit	Commits the transaction to the system configuration.
Step 9	Server /cimc/tech-support # start	Begins the transfer of the data file to the remote server.
Step 10	(Optional) Server /cimc/tech-support # show detail	Displays the progress of the transfer of the data file to the remote server.
Step 11	(Optional) Server /cimc/tech-support # cancel	Cancels the transfer of the data file to the remote server.

Example

This example creates a technical support data file and transfers the file to a TFTP server:

```

Server# scope cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # set remote-ip 192.0.20.41
Server /cimc/tech-support* # set remote-protocol tftp
Server /cimc/tech-support *# set remote-path /user/user1/default.tar.gz
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
Tech Support upload started.

Server /cimc/tech-support # show detail

Tech Support:
  Server Address: 192.0.20.41
  Path: default.tar.gz
  Protocol: tftp
  Username:
  Password: *****
  Progress (%): 5
  Status: Collecting

Server /cimc/tech-support #

```

What to do next

Provide the generated report file to Cisco TAC.

Exporting Technical Support Data to Front Panel USB Device

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.



Important

- Make sure that the Smart USB option has been enabled and that the USB device is connected to the front panel.
- If any firmware or BIOS updates are in progress, do not export the technical support data until those tasks are complete.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope tech-support	Enters the tech-support command mode.
Step 3	Server /cimc/tech-support # scope fp-usb	Enters the USB mode.
Step 4	Server /cimc/tech-support /fp-usb # start filename	Creates a technical support data file and transfers the file to a USB device. If you do not specify the file name, it will take a default file name.

Example

This example creates a technical support data file and transfers the file to a USB device connected to the front panel:

```
Server# scope cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # scope fp-usb
Server /cimc/tech-support/fp-usb # start techsupportUSB.tar.gz
Tech Support collection started.

Server /cimc/tech-support/fp-usb # show detail

Tech Support:
  Path(on USB device): techsupportUSB.tar.gz
  Progress(%): 6
  Status: COLLECTING

Server /cimc/tech-support/fp-usb #
```

What to do next

Provide the generated report file to Cisco TAC.

Rebooting the Cisco IMC

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reboot the Cisco IMC. This procedure is not part of the normal maintenance of a server. After you reboot the Cisco IMC, you are logged off and the Cisco IMC will be unavailable for a few minutes.



Note If you reboot the Cisco IMC while the server is performing power-on self test (POST) or is operating in the Extensible Firmware Interface (EFI) shell, the server will be powered down until the Cisco IMC reboot is complete.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # reboot	The Cisco IMC reboots.

Example

This example reboots the Cisco IMC:

```
Server# scope cimc
Server /cimc # reboot
```

Clearing the BIOS CMOS

On rare occasions, troubleshooting a server may require you to clear the server's BIOS CMOS memory. This procedure is not part of the normal maintenance of a server.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the bios command mode.
Step 2	Server /bios # clear-cmos	After a prompt to confirm, clears the CMOS memory.

Example

This example clears the BIOS CMOS memory:

```
Server# scope bios
Server /bios # clear-cmos
```

```
This operation will clear the BIOS CMOS.
Note: Server should be in powered off state to clear CMOS.
Continue?[y|n] y

Server /bios #
```

Recovering from a Corrupted BIOS



Note This procedure is not available in some server models.

In addition to this procedure, there are three other methods for recovering from a corrupted BIOS:

- Use the Cisco Host Upgrade Utility (HUU). This is the recommended method.
- Use the Cisco IMC GUI interface.
- If your server model supports it, use the BIOS recovery function of the hardware jumper on the server motherboard. For instructions, see the Cisco UCS Server Installation and Service Guide for your server model.

Before you begin

- You must be logged in as admin to recover from a corrupted BIOS.

- Have the BIOS recovery ISO image ready. You will find the BIOS recovery ISO image under the Recovery folder of the firmware distribution package.
- Schedule some down time for the server because it will be power cycled at the end of the recovery procedure.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the bios command mode.
Step 2	Server# recover	Launches a dialog for loading the BIOS recovery image.

Example

This example shows how to recover from a corrupted BIOS:

```
Server# scope bios
Server /bios # recover
This operation will automatically power on the server to perform BIOS FW recovery.
Continue?[y|N]y
```

What to do next

Power cycle or reset the server.

Resetting the Cisco IMC to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the Cisco IMC 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 Cisco IMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

When you upgrade from version 1.5(1) to version 1.5(2), the hostname in the Cisco IMC interface is retained as is. However, after upgrading to version 1.5(2), if you do a factory reset, the hostname changes to CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.

When you downgrade from version 1.5(2) to version 1.5(1), the hostname is retained as is. However, if you do a factory reset, the hostname changes to ucs-cxx-mx format.



Note If you reset Cisco IMC 1.5(x), 2.0, and 2.0(3) versions to factory defaults, **Shared LOM** mode is configured by default. For C3160 servers, if you reset Cisco IMC to factory defaults, **Dedicated** mode is configured to **Full** duplex with 100 Mbps speed by default.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # factory-default	After a prompt to confirm, the Cisco IMC resets to factory defaults.

The Cisco IMC factory defaults include the following conditions:

- SSH is enabled for access to the Cisco IMC CLI. Telnet is disabled.
- HTTPS is enabled for access to the Cisco IMC GUI.
- A single user account exists (user name is **admin** , password is **password**).
- DHCP is enabled on the management port.
- The previous actual boot order is retained.
- KVM and vMedia are enabled.
- USB is enabled.
- SoL is disabled.

Example

This example resets the Cisco IMC to factory defaults:

```
Server# scope cimc
Server /cimc # factory-default
This operation will reset the CIMC configuration to factory default.
All your configuration will be lost.
Continue?[y|N]y
Server /cimc #
```

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 whose structure and elements correspond to the Cisco IMC command modes.

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**
- If any firmware or BIOS updates are in progress, do not export the Cisco IMC configuration until those tasks are complete.
 - If you are exporting Cisco IMC configuration to a front panel USB device, make sure that the Smart Access USB option has been enabled.
 - 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

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope import-export	The configuration file is exported to the specified path and file name on the front panel USB device.
Step 3	Server /cimc/import-export # export-config <i>protocol ip-address path-and-filename</i>	<p>The configuration file will be stored at the specified path and file name on a remote server at the specified IPv4 or IPv6 address or a hostname. The remote server could be one of the following types:</p> <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP <p>Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.</p> <p>If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p>
Step 4	Server /cimc/import-export # export-config usb path-and-filename	Exports the configuration data to the connected USB.
Step 5	Enter the Username, Password and Pass Phrase.	Sets the username, password and the pass phrase for the file being exported. Starts the backup operation.

To determine whether the export operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to back up the Cisco IMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Passphrase:***
Export config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export:
  Operation: EXPORT
  Status: COMPLETED
  Error Code: 100 (No Error)
  Diagnostic Message: NONE

Server /cimc/import-export #
```

Importing a Cisco IMC Configuration



Important

- If any firmware or BIOS updates are in progress, do not import the Cisco IMC configuration until those tasks are complete.
- If you are importing Cisco IMC configuration through a front panel USB device, make sure that the Smart Access USB option has been enabled.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope import-export	Enters the import-export command mode.
Step 3	Server /cimc/import-export # import-config protocol ip-address path-and-filename	The configuration file at the specified path and file name on the remote server at the specified IPv4 or IPv6 address or a hostname will be imported. The remote server can be one of the following: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP

	Command or Action	Purpose
		<ul style="list-style-type: none"> • HTTP <p>Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.</p> <p>If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p>
Step 4	Server /cimc/import-export # import-config <i>usb path and filename</i>	The configuration file is imported to the specified path and file name on the front panel USB device.
Step 5	Enter the Username, Password and Pass Phrase.	Sets the username, password and the pass phrase for the file being imported. Starts the import operation.

To determine whether the import operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to import a Cisco IMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # import-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Passphrase:***
Import config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export:
  Operation: Import
  Status: COMPLETED
  Error Code: 100 (No Error)
```

```
Diagnostic Message: NONE
Server /cimc/import-export #
```

Adding Cisco IMC Banner

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # upload-banner	A prompt to enter the banner displays.
Step 3	Enter the banner and press CTRL+D.	At the prompt, enter y . This results in a loss of the current session, when you log back on again, the new banner appears.
Step 4	(Optional) Server /chassis # show-banner	The banner that you have added displays.

Example

This example shows how to add the Cisco IMC banner:

```
Server # scope chassis
Server /chassis # upload-banner
Please paste your custom banner here, when finished, press enter and CTRL+D.
hello world
This will terminate all open SSH session to take an immediate action.
Do you wish to continue? [y/N] yy
Server /chassis # show-banner
hello world
Server /chassis #
```

Deleting Cisco IMC Banner

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # delete-banner	At the prompt, enter y . This results in a loss of the current session, when you log back on again, the banner is deleted.
Step 3	(Optional) Server /chassis # show-banner	The banner that you have added displays.

Example

This example shows how to delete the Cisco IMC banner:

```
Server # scope chassis
Server /chassis # delete-banner
This will terminate all open SSH session to take an immediate action.
Do you wish to continue? [y/N] yy
Server /chassis # show-banner

Server /chassis #
```

Enabling Secure Adapter Update

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope adapter-secure-update	Enters the adapter-secure-update command mode.
Step 3	Server /cimc/adapter-secure-update # enable-security-version-check {yes no}	Enter yes at the prompt. Note If you enter no at the prompt, secure adapter update is disabled.
Step 4	(Optional) Server /cimc/adapter-secure-update # enable-security-version-check status	Displays the secure update status.

Example

This example shows how to enable the secure adapter update:

```
Server# scope cimc
Server /cimc # scope adapter-secure-update
Server /cimc/adapter-secure-update # enable-security-version-check yes
Server /cimc/adapter-secure-update # enable-security-version-check status
enable-security-version-check: Enabled
Server /cimc/adapter-secure-update #
```

Updating and Activating the Device Connector Firmware

This feature is available only on some C-Series servers.

Before you begin

You must be logged in as admin to perform this action.

Procedure

	Command or Action	Purpose
Step 1	Server # scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope device-connector	Enters the device connector command mode.
Step 3	Server /cimc/device-connector # update-and-activate protocol IP Address path	<p>Specifies the protocol, IP address of the remote server, and the file path to the firmware file on the server. The protocol can be one of the following:</p> <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP <p>Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.</p> <p>If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p>
Step 4	(Optional) Server /cimc/device-connector # show detail	Displays the status of the update.

Example

This example shows how to upgrade and activate the device connector firmware:

```
Server # scope cimc
Server /cimc # scope device-connector
Server /cimc/device-connector # update-and-activate tftp 10.10.10.10
c240-m5-cimc.4.0.1.227-cloud-connector.bin
Device connector firmware update initialized.
Please check the status using "show detail".
Server /cimc/device-connector # show detail
Device Connector Information:
  Update Stage: DOWNLOAD
  Update Progress: 5
  DC FW Version: 1.0.9-343
Server /cimc/device-connector # show detail
Device Connector Information:
  Update Stage: INSTALL
  Update Progress: 90
  DC FW Version:
Server /cimc/device-connector # show detail
Device Connector Information:
  Update Stage: NONE
  Update Progress: 100
Server /cimc/device-connector #
```

Recovering a PCIe Switch

When firmware on a switch is corrupt, you can use this option to recover the switch.

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # show nvmeadapter	Displays the NVMe adapters and the name of the PCIe switch.
Step 3	Server /chassis # recover-pcie-switch <i>PCIe Switch Name</i>	Enter y at the host reboot prompt. Recovers the selected PCIe Switch.

Example

This example shows how to recover a PCIe switch:

```
Server # scope chassis
Server /chassis # show nvmeadapter
PCI Slot
-----
```

```
PCIe-Switch
Server /chassis/persistent-memory # recover-pcie-switch PCIe-Switch
Host will be powered on for this operation.
Continue?[y|N]y
Server /chassis #
```