



Server Utilities

This chapter includes the following sections:

- [Exporting Technical Support Data, page 1](#)
- [Rebooting the CIMC, page 3](#)
- [Clearing the BIOS CMOS, page 3](#)
- [Recovering from a Corrupted BIOS, page 4](#)
- [Resetting the CIMC to Factory Defaults, page 5](#)
- [Exporting and Importing the CIMC Configuration, page 6](#)
- [Generating Non maskable Interrupts to the Host, page 8](#)

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 CIMC command mode.
Step 2	Server /cimc # scope tech-support	Enters the tech-support command mode.
Step 3	Server /cimc/tech-support # set remote-ip ip-address	Specifies the IP address of the remote server on which the technical support data file should be stored.

	Command or Action	Purpose
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
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	Server /cimc/tech-support # show detail	(Optional) Displays the progress of the transfer of the data file to the remote server.
Step 11	Server /cimc/tech-support # cancel	(Optional) Cancels the transfer of the data file to the remote server.

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.

Rebooting the CIMC

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



Note

If you reboot the CIMC 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 CIMC reboot is complete.

Procedure

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

This example reboots the CIMC:

```
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.

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

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 CIMC 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.

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 CIMC to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CIMC 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 CIMC, 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 CIMC 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.

Procedure

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

The CIMC factory defaults include the following conditions:

- SSH is enabled for access to the CIMC CLI. Telnet is disabled.
- HTTPS is enabled for access to the CIMC GUI.
- A single user account exists (user name is **admin** , password is **password**).
- DHCP is enabled on the management port.
- The boot order is EFI, CDROM, PXE (using LoM), FDD, HDD.
- KVM and vMedia are enabled.
- USB is enabled.
- SoL is disabled.

This example resets the CIMC 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]
```

Exporting and Importing the CIMC Configuration

Exporting and Importing the CIMC Configuration

To perform a backup of the CIMC configuration, you take a snapshot of the system configuration and export the resulting CIMC 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 CIMC configuration file to the same system or you can import it to another CIMC 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 CIMC configuration file is an XML text file whose structure and elements correspond to the CIMC 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.

Exporting the CIMC Configuration



Note

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



Important

If any firmware or BIOS updates are in progress, do not export the CIMC configuration until those tasks are complete.

Before You Begin

Obtain the backup remote server IP address.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.

	Command or Action	Purpose
Step 2	Server /cimc # scope import-export	Enters the import-export command mode.
Step 3	Server /cimc/import-export # export-config <i>protocol ip-address path-and-filename</i>	Starts the backup operation. The configuration file will be stored at the specified path and file name on a remote server at the specified IP address. The remote server could be one of the following types: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP

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

This example shows how to back up the CIMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
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 CIMC Configuration



Important

If any firmware or BIOS updates are in progress, do not import the CIMC configuration until those tasks are complete.

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, CIMC does not overwrite the current values with those saved in the configuration file.

Procedure

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

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

This example shows how to import a CIMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # import-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Import config started. Please check the status using "show detail".
Server /cimc/import-export #
```

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.

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # generate-nmi	Generates the crash dump file for the server. To use this command, the server must be powered on, and you must be logged in as an administrator.

This example shows how to generate NMI signals to the host:

```
Server # scope chassis
Server /chassis # generate-nmi
This operation will send NMI to the host and may cause reboot of the OS.
OS reboot depends on it's NMI configuration.
Do you want to continue? [y|N] y
Server /chassis #
```

