



Server Utilities

This chapter includes the following sections:

- [Exporting Technical Support Data, on page 1](#)
- [Resetting to Factory Default, on page 2](#)
- [Exporting and Importing the Cisco IMC Configuration, on page 3](#)
- [Generating Non Maskable Interrupts to the Host, on page 7](#)
- [Adding or Updating the Cisco IMC Banner, on page 8](#)
- [Viewing Cisco IMC Last Reset Reason, on page 9](#)
- [Downloading Hardware Inventory to a Local File, on page 9](#)
- [Exporting Hardware Inventory Data to a Remote Server, on page 10](#)

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** 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	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.
Download to local file radio button	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.

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:
 - 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 Configuration

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

- 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
- 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
Export To drop-down list	<p>The location where you want to save the XML configuration file. This can be one of the following:</p> <ul style="list-style-type: none"> • Local: Select this option and click Export to save the XML configuration file to a drive that is local to the computer running the .. <p>When you select this option, displays a File Download dialog box that lets you navigate to the location to which the configuration file should be saved.</p> <ul style="list-style-type: none"> • Remote Server: Select this option to import the XML configuration file from a remote server. <p>When you select this option, displays the remote server fields.</p>
Export To drop-down list	<p>The remote server type. This can be one of the following:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>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 <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?.</i> Click Yes or No 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>
Path and Filename field	The path and filename 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, 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
Import From drop-down list	<p>The location of the XML configuration file. This can be one of the following:</p> <ul style="list-style-type: none"> • Local: Select this option to import the XML configuration file to a drive that is local to the computer running . When you select this option, displays a Browse button that lets you navigate to the file you want to import. • Remote Server: Select this option to import the XML configuration file from a remote server. When you select this option, displays the remote server fields.

Name	Description
Import From drop-down list	<p>Note These options are available only when you choose Remote.</p> <p>The remote server type. This can be one of the following:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>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 <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?</i>. Click Yes or No 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>
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	<p>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: ! # \$ % & < > ? ; ' ` ~ \ % ^ ()"</p> <p>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.</p>

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: <ul style="list-style-type: none"> • 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.
Status field	The reason why the component was last reset. This can be one of the following: <ul style="list-style-type: none"> • watchdog-reset—The watchdog-timer resets when the Cisco IMC memory reaches full capacity. • ac-cycle— PSU power cables are removed (no power input). • graceful-reboot— Cisco IMC reboot occurs.

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	displays this radio button when there is no hardware inventory data file to download.
Download to local file radio button	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	<p>The remote server type. This can be one of the following:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>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 <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?</i>. Click Yes or No 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>

Name	Description
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 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**.
