CHAPTER 21

Diagnostics Settings

GUI: Cisco Unified Communications Manager Business Edition 3000 Administrative Interface

The Diagnostics page allows you to run diagnostics for your system, gather diagnostic information for your system, and download the diagnostic information. On the Diagnostics page, you can collect logs, enable or disable loopback for T1/E1 interfaces, and download the USB diagnostics file.

The following topics contain information about the tabs and settings that are displayed on the Diagnostics page (**Monitoring > Diagnostics**):

For more information, see the "How to Diagnose a Problem" section on page 46-39.

Collect Logs

Table 21-1 describes the settings that you can use to enable or disable detailed logging, generate logs, and download the log file under the Collect Logs tab.

Table 21-1 Settings on the Collect Logs Tab

Setting	Description
Enable Logging	To enable the system to collect debug level log data, click **Enable Logging**. After you click this button, it grays out and the Disable Logging button becomes enabled. You can now attempt to reproduce your system issue. **Tip** Turning on logging may impact system performance, so enable logging only when necessary. After you finish collecting log data, remember to disable logging by clicking **Disable Logging**.

Table 21-1 Settings on the Collect Logs Tab (continued)

Setting	Description
Disable Logging	When you have reproduced the system issue, click **Disable Logging** to stop the system from collecting log data. After you click this button, it grays out and the Enable Logging button becomes enabled.
Generate Log File	To prepare a log file, click **Generate Log File**. **Tip** You can generate a log file without enabling/disabling the logging functionality by clicking **Generate Log File** at any time and downloading the current log collection file. The system displays the progress of the log file generation. When the log file is complete, a link displays that you can click to download the file to your PC. The link contains the time and date that the log file was created. **Tip** Be sure to download the file to a location on your PC that contains enough disk space to accommodate the size of the log file.

USB Key

Cisco USB key allows you to perform the server diagnostics and collect the required log files when the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface is not accessible. You can use the USB Key tab to download the diagnostics file.

Note Ensure that the USB key has a storage space of 4 GB. If there is not sufficient storage space, the files smaller than 4 GB will be copied to the USB.

To download the USB diagnostics file, click **Download Diagnostics File**. The USB diagnostics file allows the Value Added Reseller (VAR) and Cisco Technical Assistance Center (TAC) to provide additional troubleshooting assistance, especially when you cannot access the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface.

Packet Capture

The Unified CMBE 3000 Administrative Interface supports capturing the network packets on a server. While troubleshooting, it is sometimes necessary to collect network packets that are being sent to and from the network interface on a Unified CMBE 3000 server.

Table 21-2 describes the settings on the Packet Capture tab.

Note Packet Capture is resource-intensive and the system might be less responsive while it is enabled.

Table 21-2 Settings on the Packet Capture Tab

Setting	Description
Capture Packets	Packet Capture allows you to capture the network packets in two ways: • **Capture packets to and from IP address**—Choose this option to capture the network packets to and from a particular IP address. • **Capture all packets**—Choose this option to capture all the network packets.
Start Packet Capture	To start packet capture, click **Start Packet Capture**. The time stamp displays the current date and packet capture start time. If the packet capture file exists on a system, the following warning message appears: **Warning** **You can keep only one packet capture file on the server at a time. If you generate a new one, the existing file will be replaced with the new one.** While the packet capture is running, you can also attempt to reproduce the problem.
Stop Packet Capture	To stop the packet capturing, click **Stop Packet Capture**. The time stamp displays the current date and packet Capture stop time. Packet capture stops when it captures 100,000 network packets. The captured packets are saved in Packetcapture< Timestamp in YYYY-MM-DD_hh-mm-ss>.cap file format. The time stamp displays the time when the packet capturing was started.
Download the log file to your PC	A link allows you to download the captured network packets to your PC. **Note** You should have the corresponding software tools installed on your PC to view the downloaded network packets.

Ping

Unified CMBE 3000 Administrative Ping utility interface allows you to check the network connectivity for the desired IP Address or a hostname to which you want reach. While check the connectivity, you can mention the number of attempts that the system can try.

Table 21-3 describes the test characters that the ping facility sends.

Table 21-3 Settings on the Ping Tab

Setting	Description
Ping function	To check connectivity by using the Ping utility, perform the following: • Type the **hostname** or **IP address** to be reached. If DNS is not available on server, entering hostname will not work • Select the number of the **Ping Attempts** from the drop-drown list. After reaching the specified number of attempts mentioned in the drop-down list, the Ping operation will be automatically stopped. By default, the number is “1”. The other available attempts are 5, 25, and 100.
Start Ping	To start a ping session, Click the **Start Ping** button. Ping stops automatically after reaching the specified iteration number. The output shows the results of the Ping Attempts with the results summarized at the end.
Cancel Ping	After you click the **Start Ping** button, the button label changes to **Cancel Ping** and allows you to cancel the ping session. Ping statistics will not be available if ping is cancelled. **Note** If you click the **Cancel Ping** button in the middle of a ping process, the ping operation is cancelled for the remaining iterations. A message appears in the Ping output box stating “Ping Cancelled”.

Gateway Loopback

Table 21-4 describes the settings on the Gateway Loopback tab. Your service provider uses loopback test to diagnose connection problems in the network and may ask you to put your T1/E1 interfaces (ports) into loopback mode. You can use the settings on the Gateway Loopback tab to enable or disable loopback mode for the internal gateway ports.

Caution Do not add, update, or delete any of the internal gateway ports when you put a port in loopback mode. Adding, updating, or deleting a port can reset the internal gateway and will pull the port out of loopback mode.

Note You can use the Gateway Loopback tab to initiate loopback for internal gateways only. It is not applicable for external gateways.

Table 21-4 Settings on the Gateway Loopback tab

Setting	Description
Port	Displays all the internal PSTN gateway ports.
Connection Name	Displays the name of the gateway to which the port belongs.
Description	Provides a brief description of the port.
Status	Displays the status of the port, that is, up, down, or unregistered.
Enable Loopback	To put a port in loopback mode, click **Enable Loopback**. After you click this option, you can either **Disable Loopback** or **Cancel**. After you put a port in loopback mode, the gateway to which that port belongs is unregistered. You can verify this through the Health Summary page. **Tip** You cannot enable loopback if the gateway for that port is not configured.
Disable Loopback	When your service provider completes the testing and asks you to disable loopback, click **Disable Loopback** to recover the port from loopback. After you click this option, it changes to **Enable Loopback**.