



CHAPTER 6

Configuring Cisco Emergency Responder 2.0 Serviceability

Cisco Emergency Responder (Cisco ER) 2.0 includes a Serviceability interface that allows you to access the Cisco ER 2.0 Serviceability features. These features are grouped under four main menus on the Serviceability web interface: Tools, SNMP, System Monitor, and CER Logs. For details on all Serviceability web pages, see [Appendix B, “Serviceability Web Interface For Cisco Emergency Responder.”](#)

These topics describe how to configure and use Cisco Emergency Responder (Cisco ER) 2.0 Serviceability features:

- [Using the Serviceability Tools, page 6-1](#)
- [Configuring SNMP, page 6-3](#)
- [Using the System Monitor Tools, page 6-6](#)
- [Using Cisco Emergency Responder Logs, page 6-9](#)

Using the Serviceability Tools

These topics describe the Cisco ER 2.0 Serviceability tools:

- [Using the Control Center, page 6-1](#)
- [Using the Event Viewer, page 6-2](#)

Using the Control Center

The Control Center allows you to perform actions on the services running on the selected Cisco ER 2.0 system.

To perform actions on the services running on the selected Cisco ER 2.0 system, follow these steps:

Procedure

-
- Step 1** From the Cisco ER Serviceability web interface, select **Tools>Control Center**.
The Control Center page appears.

- Step 2** To change the status of a service, click the radio button to the left of the Service Name and click the button corresponding to the desired action. Available actions are:
- Start
 - Stop
 - Restart



Note Cisco Tomcat and Cisco IDS services cannot be started, stopped, or restarted from the Cisco ER Serviceability website. These services can only be started, stopped, or restarted using the command line interface (CLI). See [Appendix F, “Command Line Interface”](#) for further information.

- Step 3** Click **Refresh** to refresh the page.

Related Topics

- [Control Center, page B-1](#)

Using the Event Viewer

The Event Viewer allows you to view events for the prior six months.

To view events for the prior six months, follow these steps:

Procedure

- Step 1** From the Cisco ER Serviceability web interface, select **Tools > Event Viewer**.
The Event Viewer page appears.
- Step 2** To find all events that occurred over the prior six months, click **Find** without entering any search criteria.
To find events that match specific criteria, enter search criteria:
- Select a specific month to view events from the month only.
 - If you select Type, you can then select the type on which to search from the pulldown menu to the right.
If you select Module, you can then select the module on which to search from the pulldown menu to the right.



Note For a list of available Types and Modules, see the [“Event Viewer” section on page B-2](#).

When you have entered your search criteria, click **Find**.

- Step 3** You can perform an ascending or descending sort of the results. To perform a sort, click the up arrow or down arrow next to the Time, Type, or Module column headings.

Related Topics

- [Event Viewer, page B-2](#)

Configuring SNMP

Cisco ER 2.0 supports SNMP V1/V2C and V3. You can use the Serviceability web interface to configure SNMP V1/V2C (Community String and Notification Destination) and SNMP V3 (User and Notification Destination).

Each SNMP version has security models and security levels. Users are assigned to groups that are defined by a security model and specified security levels. Each group also has a defined security access level to a set of MIB objects for reading and writing, which are known as *views*. The switch has a default view (all MIB objects) and defaults groups defined for SNMP V1 and V2C security models. SNMP V3 provides additional security features that cover message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

These topics describe how to configure SNMP V1/V2C and V3:

- [Configuring the SNMP Community String](#), page 6-3
- [Configuring the SNMP V1/V2C Notification String](#), page 6-4
- [Configuring SNMP Users](#), page 6-5
- [Configuring the SNMP V3 Notification Destination](#), page 6-5
- [Configuring MIB2](#), page 6-6

Configuring the SNMP Community String

By configuring SNMP, you can control SNMP access to the Cisco ER SNMP agent. A management station must first submit a valid community string for authentication.

You configure a community string by entering the Community String Name, the IP addresses of host that can be authenticated using the community string, and the access privileges allowed. The available access privileges are as follows:

- ReadOnly
- ReadWrite
- ReadWriteNotify
- NotifyOnly
- None

To configure the SNMP community string, follow these steps:

Procedure

-
- Step 1** From the Cisco ER Serviceability web interface, select **SNMP > V1/V2C Configuration > Community String**.
- The SNMP Community String Configuration page appears.
- Step 2** In the Community String Name text box, enter the name of the community string.
- Step 3** To specify specific hosts whose SNMP packets will be accepted, click the **Accept SNMP Packets only from these hosts** radio button, enter the IP addresses in the text box, and click **Insert**.
- To accept SNMP packets from any host, click the **Accept SNMP Packets from any host** radio button.

- Step 4** To remove an existing host, select the host's IP address and click **Remove**.
- Step 5** From the Access Privileges pulldown menu, select the access privilege for the host, then click **Insert**.
-

Related Topics

- [SNMP Community String Configuration, page B-4](#)

Configuring the SNMP V1/V2C Notification String

Using the SNMP V1/V2C notification string, you can select the host and port destination to which SNMP V1/V2C trap messages are sent. Every notification string must be authenticated. When using SNMP V1/V2C, authentication is done using the community string.

To configure the SNMP V1/V2C notification string, follow these steps:

Procedure

-
- Step 1** From the Cisco ER Serviceability web interface, select **SNMP > V1/V2C Configuration > Notification Destination**.
- The SNMP Notification Destination Configuration page appears.
- Step 2** To add a new SNMP Notification Destination, click **Add New**.
- Step 3** From the Host IP Addresses pulldown menu, select **Add New**. Additional fields appear.
- Step 4** Enter the Host IP Address and Port Number in the text boxes.
- Step 5** Click either the **V1** or **V2C** radio button to select the SNMP version.
- If you click **V1**, the Community String pulldown menu appears. Proceed to [Step 7](#).
- If you click **V2C**, the Notification Type pulldown menu appears.
- Step 6** From the Notification Type pulldown menu, select **Inform** or **Trap**. The Community String pulldown menu appears.
- Step 7** From the Community String pulldown menu, select the community string to use.
- Step 8** Click **Insert**.
- You will see a message saying that the SNMP master agent needs to be restarted for the changes to take effect. Click **OK** to restart the SNMP master agent or **Cancel** to continue without restarting the master agent.
- The notification destination is added to the list of destinations on the SNMP Notification Destination Configuration page.
- Step 9** To add additional notification destinations, repeat [Step 2](#) through [Step 8](#).
-

Related Topics

- [SNMP V1/V2c Notification Destination Configuration, page B-6](#)

Configuring SNMP Users

SNMP V3 provides additional security features that cover message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

To configure SNMP users, follow these steps:

Procedure

- Step 1** From the Cisco ER Serviceability web interface, select **SNMP>V3 Configuration>User**.
The SNMP User Configuration page appears.
- Step 2** To add a new SNMP User, click **Add New**.
- Step 3** In the User Name text box, enter the name of the new user.
- Step 4** To require authentication, click the **Authentication Required** checkbox, enter a password in the **Password** text box, reenter the password in the **Reenter Password** textbox, and click either the **MD5** or **SHA** radio button to select the Protocol to be used. Click **Insert** to add the user.
- Step 5** To require information privacy, click the **Privacy Required** checkbox, enter a password in the **Password** textbox, reenter the password in the **Reenter Password** textbox, and click the **DES** checkbox.



Note You will see a message saying that the SNMP master agent needs to be restarted for the changes to take effect. Click **OK** to restart the SNMP master agent or **Cancel** to continue without restarting the master agent.

The new user is added to the list of users on the SNMP User Configuration page.

- Step 6** To add additional users, repeats [Step 2](#) through [Step 4](#).
-

Related Topics

- [SNMP User Configuration, page B-7](#)

Configuring the SNMP V3 Notification Destination

The SNMP V3 Notification Destination String provides a greater amount of security because each notification string is associated with a user. When configuring a user, you can specify the desired level of authentication and security.

To configure the SNMP V3 notification string, follow these steps:

Procedure

- Step 1** From the Cisco ER Serviceability web interface, select **SNMP>V3 Configuration>Notification Destination**.
The SNMP Notification Destination Configuration page appears.
- Step 2** To add a new SNMP Notification Destination, click **Add New**.
- Step 3** From the Host IP Addresses pulldown menu, select **Add New**. Additional fields appear.

- Step 4** Enter the Host IP Address and Port Number in the text boxes.
- Step 5** From the Notification Type pulldown menu, select **Inform** or **Trap**.
If you select **Trap**, the Security Level pulldown menu appears. Proceed to [Step 7](#).
If you select **Inform**, you are prompted to enter a remote engine ID.
- Step 6** Enter the remote engine ID.
- Step 7** From the Security Level pulldown menu, select the desired security level.
- Step 8** Click the radio button to the left of the User Name to select a user to be associated with the notification destination.
- Step 9** To add additional notification destinations, repeat [Step 2](#) through [Step 8](#).
-

Related Topics

- [SNMP V3 Notification Destination Configuration, page B-9](#)

Configuring MIB2

The SNMP MIB2 tool lets you specify a contact person for a MIB2 managed node and the physical location of the managed node.

To configure MIB2, follow these steps:

Procedure

- Step 1** From the Cisco ER Serviceability web interface, select **SNMP>System Group Configuration>MIB2 System Group Configuration**.
- The SNMP MIB2 Configuration page appears.
- Step 2** In the System Contact text box, enter the name of the contact.
- Step 3** In the Location text box, enter the location of the managed node.
- Step 4** Click the **Update** icon in the upper left corner of the page.
- Step 5** To modify the information, click the **Clear** icon in the upper left corner of the page, enter new information in the System Contact and Location text boxes, and click the **Update** icon again.
-

Related Topics

- [MIB2 SystemGroup Configuration, page B-11](#)

Using the System Monitor Tools

These topics describe how to use the System Monitor tools:

- [Using the CPU and Memory Usage Tool, page 6-7](#)
- [Using the Processes Tool, page 6-8](#)
- [Using the Disk Usage Tool, page 6-8](#)

Using the CPU and Memory Usage Tool

You can use the CPU and Memory Usage tool to monitor and log this information. By default, the information is refreshed every 30 seconds. You change how often the information refreshes, or you can disable the auto-refresh feature.

To use the CPU and Memory Usage tool, follow these steps:

Procedure

-
- Step 1** From the Cisco ER Serviceability web interface, select **System Monitor > CPU & Memory Usage**. The CPU and Memory Usage page appears.
- The page is divided into two sections, **Processors** and **Memory**. For details on the information that is displayed, see [Table B-12 on page B-11](#).
- Step 2** To change the rate at which the page refreshes, enter a value (in seconds) in the **Set the screen refresh value** text box and click **Set**. The minimum value you can enter is 5 seconds.
- Step 3** To disable the auto-refresh feature, click the **Disable Auto-Refresh** check box in the upper left corner.
- Step 4** To create a log file of the CPU usage, click the **Start Log** button in the Processors section of the page. Similarly, to create a log file of the Memory usage, click the **Start Log** button in the Memory section of the page.
- You can create up to 25 log files.
- The default interval for logging is 10 seconds. To change the logging interval, follow these steps:
- To change the CPU logging interval, enter a value between 5 seconds and 600 seconds in the **Set CPU Logging Interval** text box and click **Set**.
 - To change the Memory logging interval, enter a value between 5 seconds and 600 seconds in the **Set Memory Logging Interval** text box and click **Set**.
- Step 5** To download the log files, click **Download CPU Log File** or **Download Memory Log File**.
- The system displays a Log Files page that shows all the current log files. Thereafter, log files are recycled; when a new log file is added, the oldest log file is deleted.
- Step 6** To download individual files, click the check box to the left of the log file name(s) you want to download. To download all log files, click the check box to the left of the File Name column heading. When you have selected the files, click **Download**. If you select multiple files for download, the system will create and download a zipped folder called CPULogs (for Processor log files) and MemoryLogs (for Memory log files).
- Step 7** You can also view the log files online without downloading them. To do so, click the file name. The system displays the contents of the log file.
-

Related Topics

- [CPU and Memory Usage, page B-11](#)

Using the Processes Tool

You can use the Processes tool to monitor and log process information. By default, the information is refreshed every 30 seconds; the minimum refresh value is 5 seconds. You change how often the information refreshes, or you can disable the auto-refresh feature.

To use the Processes tool, follow these steps:

Procedure

- Step 1** From the Cisco ER Serviceability web interface, select **System Monitor > Processes**.
The Processes page appears. For details on the information that is displayed, see [Table B-13 on page B-13](#).
You can perform an ascending or descending sort of the results. To perform a sort, click the up arrow or down arrow next to the column heading that you want to sort by. For example, to perform a descending sort based on the process, click the down arrow next to the Process column heading. Similarly, to perform an ascending sort based on the process ID, click the up arrow next to the PID column heading.
- Step 2** To change the rate at which the page refreshes, enter a value in the **Set the screen refresh value** text box in the upper right corner and click **Set**. The minimum value you can enter is 5 seconds.
- Step 3** To disable the auto-refresh feature, click the **Disable Auto-Refresh** check box in the upper left corner.
- Step 4** To view the details of a process, click the check box to the left of the process name and click **View Selected Processes**. You can select a maximum of ten processes.
The Selected Processes displays the details of the process. On this page you can also set the refresh rate and disable the auto-refresh feature. To start a log of the process, click **Start Log**. To end logging, click **Stop Log**.
To change the Process logging interval, enter a value between 5 seconds and 600 seconds in the **Set Process Logging Interval** text box and click **Set**.
- Step 5** To download the log files, click **Download Process Logs** from the Process Log Files page. (To download log files, click **Download Log File** from the Processes page.)
- Step 6** To download individual files, click the check box to the left of the log file name(s) you want to download. To download all log files, click the check box to the left of the File Name column heading. When you have selected the files, click **Download**. If you select multiple files for download, the system will create and download a zipped folder called ProcessLogs.
- Step 7** You can also view the log files online without downloading them. To do so, click the file name. The system displays the contents of the log file in a separate window.
-

Related Topics

- [Processes, page B-13](#)

Using the Disk Usage Tool

The Disk Usage tool displays the percentage of available disk space used by the different partitions in the system.

To use the Disk Usage tool, follow these steps:

Procedure

-
- Step 1** From the Cisco ER Serviceability web interface, select **System Monitor > Disk Usage**.
The Disk Usage page appears. For details on the Disk Usage page, see [Table B-17 on page B-15](#).
- Step 2** To perform an ascending or descending sort, click the up arrow or down arrow next to the column heading that you want to sort by. For example, to perform a descending sort based on the partition, click the down arrow next to the Partition column heading. Similarly, to perform an ascending sort based on the available disk space, click the up arrow next to the Available Space column heading.
-

Related Topics

- [Disk Usage, page B-15](#)

Using Cisco Emergency Responder Logs

Cisco ER 2.0 provides an interface to collect system and application logs. These logs share the same user interface and log files can be viewed and downloaded in the same manner. The following procedure applies to all of the CER logs.

Cisco ER 2.0 logs are organized into three types. The three types, and the logs within these types, are as follows:

- CER Logs
 - CER Admin
 - CER Server
 - CER Phone Tracking
 - JTAPI
 - Tomcat
 - Event Viewer
 - Audio Driver
- Platform Logs
 - CLI
 - CLM
 - Certificate Management/IPSec
 - DRS
 - Install/Upgrade
 - Remote Support
 - Syslog
 - Servm

- DB Logs
 - Cerdbmon
 - Install DB

To view the Cisco ER logs, follow these steps:

Procedure

-
- Step 1** From the Cisco ER Serviceability web interface, select **System Logs**>*Log Type*>*Log Name*.
The selected Log Files page appears. See the [Related Topics](#) section below for details on each of these page.
- You can perform an ascending or descending sort of the results. To perform a sort, click the up arrow or down arrow next to the column heading that you want to sort by.
- Step 2** You can download the log files to your local system using the **Download** button.
- To select individual files, click the check box to the left of the log file name you want to download. To select all log files, click the check box to the left of the File Name column heading. When you have selected the files, click **Download**. If you select multiple files for download, the system will create and download a zipped folder called CPULogs. The names of the zipped folders are based on the type of logs they contain, as follows:
- CERAdmin
 - CERServer
 - CER Phone Tracking
 - Syslog
 - JTAPI
 - Tomcat
 - Install
 - DRS
 - CLILog
 - CMILog
 - ServmLogs
 - RemoteSupportLogs
 - InstallDBLogs
 - CertificateManagement&IPSecLogs
 - CerdbmonLogs
- Step 3** You can also view the log files online without downloading them. To do so, click the file name. The system displays the contents of the log file in a separate window. Click **Reload Log File** to refresh the log file you are viewing. Click **Download Log** to download the log file you are viewing.
-

Related Topics

- [System Logs Menu, page B-15](#)