CHAPTER 8

Configuring System Settings

The administration console shows the status of key system functions. The following sections describe the system status display and how to configure system settings:

Understanding System Status

The administration console home page displays the system configuration status for the following key functions:

- Scheduling—Configuration required before you can schedule meetings.
- Attending—Configuration required before anyone can attend meetings.
- OBTP—Configuration required for One-Button-to-Push (OBTP) functionality.
- System—Cisco TelePresence Exchange System will only launch meetings if valid licenses are provisioned.

A green check-mark icon next to the function indicates that the system configuration is complete for the corresponding function. A red stop-sign icon indicates that the system configuration is missing or incomplete for the corresponding function.

If any of the key functions display a red icon, the What's Wrong field provides a description of the configuration issue that needs to be addressed. Click the fix link (the button with the hammer icon) to open the configuration page on which the issue can be resolved.

Note The system configuration status also is displayed in the System Status panel (below the navigation pane) on all administration console pages.

Note The system status display refreshes each time that you navigate to a new page.

Resource Operational States

The live system ping displays the overall health of the other platforms that communicate with the Cisco TelePresence Exchange System. The system monitors these platforms by sending status messages periodically. Systems that respond to the message display a green icon and systems that are not responding to the message display a red icon. Systems that are in maintenance mode display a yellow icon.

Understanding Alarms

You can use the Alarms window to get a detailed view of system health, and as a starting point when debugging system errors or failures.

The Cisco TelePresence Exchange System retains alarm details for up to 30 days from the time the alarm was generated. The system automatically purges alarms that exceed this 30-day limit. If the total number of alarms retained by the system reaches 100,000, the system retains only the most recent 100,000 alarms and automatically purges the rest.

Procedure

To view and filter alarms for the system, do the following procedure:

Step 1 From the navigation pane, choose **System > Alarms**.

The Alarms window is displayed showing details on alarms for the past 30 days.

Fields on the **System > Alarms** window are described in Table 8-1.

Step 2 To view more information about a specific alarm, click anywhere in the alarm row.

Alarm details are listed on the right side of the window.

Step 3 (Optional) To filter the information that is displayed on the Alarms window, do one of the following:

- To filter on the Severity information that is displayed on the Alarms window, click the T icon next to the column heading, and check the check boxes next to each item that you want to display on the window.

  To display Alarms for all items, check All.
- To filter on any specific heading other than Severity, click the T icon next to the column heading, and enter the specific item on which you want to filter.

Step 4 To activate the filter, click **Filter**.

To deactivate a filter, click the **T** icon next to the appropriate column heading and click Clear.

Note When you click **Clear Filters**, the system clears all defined filters.

Table 8-1 Alarms Field Descriptions

Field	Description
Severity	Text description and icon indicating the level of severity of the alarm. (Levels range from Emergency to Info.)
Time	Time and date stamp indicating when the alarm was generated.
Summary	Text description of the alarm.
Server	Name of the server on which the alarm occurred.

Understanding Cluster Nodes

The Cisco TelePresence Exchange System is a cluster node, which is composed of at least two administration servers, two call engines, and two database engines.

After installation of a Cisco TelePresence Exchange System completes, the cluster node registers itself to the database (every five minutes). When the administration server discovers the new cluster node, it appears in the cluster node list within the administration console.

Fields on the **System > Cluster Nodes** window are described in Table 8-2.

Table 8-2 Cluster Node Field Descriptions

Field	Description
Node Name	Node name of the node. Click the node name to view only the information for that node.
Host Name	Hostname of the node.
IP Address	The IP address of the node. See the "Common Field Properties" section on page 2-4.
Cluster	Name of the cluster to which the node belongs. Currently, **Default Cluster** is the only cluster name.
Operational State	The current operational state of the node: Offline, Online, Maintenance or Unknown.
Node Type	The server type of the node: ADMIN, ENGINE, or DATABASE.

Configuring Time Zones

You can activate any number of time zones for the administration console. All of the supported time zones are listed alphabetically on the System > Time Zones page by continent and city. A time zone with a check in the Active check box is active and assignable by the system within various configuration panels of the administration console.

You must activate a time zone to allow configuration of the time of day within the administration console such as setting the starting time for a meeting. You also choose a time zone from the list of activated time zones when scheduling backups.

When creating or editing a user, you can assign the user any activated time zone. The user sees alarms, diagnostics, and other time displays in the selected time zone when using the administration console, and the time zone is selected by default when the user schedules meetings.

Procedure

To activate a time zone, do the following procedure:

Step 1 From the navigation pane, choose **System > Time Zones**.

The Time Zones window is displayed.

Step 2 To activate a time zone, check the **Active** check box next to the desired time zone.

The time zone is now active.

Step 3 To determine which time zones are active, click the **T** icon next to the Active heading.

Step 4 In the panel that is displayed, check the **Active** check box and click **Filter**.

Configuring Users

Topics in this section include:

Adding Users

Before You Begin

Configure the time zones served by this Cisco TelePresence Exchange System.

Only system administrators can modify user settings.

Procedure

To add a new user, do the following procedure:

Step 1 From the navigation pane, choose **System > Users**.

The Users window is displayed.

Step 2 Click **Add A New User**.

Step 3 Enter the settings as indicated in Table 8-3 to configure the user.

Step 4 To save your changes, click **Save**.

Editing User Settings

Before You Begin

Only system administrators can modify user settings.

Procedure

To edit user settings, do the following procedure:

Step 1 From the navigation pane, choose **System > Users**.

The Users window is displayed.

Step 2 In the item table, click the applicable user ID.

The User Details window is displayed.

Tip You can also reach the User Details window for the account that you used to log in by clicking the username link in the banner pane. For more details, see the "Banner Pane" section on page 2-2.

Step 3 From the toolbar, click **Edit This User**.

The Edit User window is displayed. Fields contain the currently-configured values.

Step 4 Modify field entries as required.

Fields are described in Table 8-3.

Step 5 To save your changes, click **Save**.

Deleting Users

Before You Begin

Only system administrators can delete users.

Procedure

To delete a user, do the following procedure:

Step 1 From the navigation pane, choose **System > Users**.

The Users window is displayed.

Step 2 In the item table, check the check box next to the entry that you want to delete. You can delete multiple users at one time by checking the check box next to each entry that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

Tip If you prefer to view the details of a user prior to deleting it, in the Users window, you can click the applicable **User ID** to go to the User page. After verifying that you have chosen the correct user to delete, click **Delete This User**, and then in the Deletion Confirmation dialog box, click **Delete** to confirm the deletion.

User Fields

Table 8-3 User Field Descriptions

Field	Description
First Name	The first name of the user. See the "Common Field Properties" section on page 2-4.
Last Name	The last name of the user. See the "Common Field Properties" section on page 2-4.
User ID	Unique ID assigned to this user. The user enters the user ID when logging in to the administration console.
Email Address	Email address of the user.
Password	Password assigned to the user during system installation or by the system administrator. The user enters the password when logging in to the administration console.
Verify Password	Password entered again for verification.
Role	See the "User Roles" section on page 8-6.
Timezone	Drop-down list displays the active time zones. Choose the time zone that matches the location of the user. See the "Configuring Time Zones" section on page 8-3.

User Roles

Table 8-4 lists the roles that you can assign to users in the Cisco TelePresence Exchange System administration console.

Table 8-4 User Roles

Role	Privileges
SYSTEM system administrator	System administrators can configure all system settings in the admin console and can add new users of any role.
ADMIN administrator	Administrators can configure all system settings in the admin console and can add only new API users.

Table 8-4 User Roles (continued)

Role	Privileges
PROVISIONING provisioning user	Provisioning users can configure only the settings in the Customers and Endpoint Management areas of the admin console. For all other pages in the admin console, provisioning users have read-only privileges.
READONLY read-only user	Read-only users can view but not edit any pages of the admin console.
API API user	Unlike the other user roles, the API role is assigned to billing and operational systems instead of people. The API user role allows other systems to access the Cisco TelePresence Exchange System API. The API user role does not allow access to the admin console.
SERVICEDESK service desk user	Service desk users can schedule, modify, and cancel meetings. Users with this role can also manage Meet-Me and Rendezvous meetings that are currently in progress, performing functions such as muting or unmuting participants, dialing out to additional endpoints, or increasing the duration of the meeting. Users with this role have view-only access to other areas of the administration console.

Related Topics

- *API User Guide for the Cisco TelePresence Exchange System*, available at http://www.cisco.com/en/US/products/ps11276/products_programming_reference_guides_list.html.
- Managing Active Meetings, page 13-32

Configuring Database Backups

You can configure regular backups of the database server that run automatically at scheduled times, or you can do a manual, on-demand backup as needed.

After each database backup completes, the system marks the backup attempt with one of the following statuses in the Status column of the Database Backup window: success, failed, missing (server cannot find file to delete), or deleted.

When a database backup is in process, the system notes the status as In Progress.

When the system (or administrator) cancels a database backup, the system notes the status as Cancelled.

Retention Policy

You can define how many copies of database backups that you retain, and define the retention method in terms of backup number, size (MB), and time (days). You can define multiple retention methods.

When the number of database backups exceeds the retention policy settings, the system deletes database backups in accordance with the following rules:

- The system applies the retention policy during each database backup.
- The system deletes the oldest successful backup first.

- When there are multiple retention policies in use, the system deletes the oldest successful backup that exists among all defined policies.
- No system warning is given before the database backup deletion occurs.

Note

- Cisco recommends that the administrator not perform manual deletions of database backup files on the server. Manual deletions can cause the defined retention policy to delete more database backup files than necessary.
- For details on reviewing the number of database backups stored on the backup server, see the "Viewing Past Database Server Backups and Restores" section on page 24-1.
- For details on running a manual backup or restoring a backup to a database server, see the "Managing Database Backups" chapter.

Before You Begin

Create a directory on a server on which you can save the database backups.

Ensure that you have the log in information (username and password) for the server on which you are saving the database backups.

Test access to the designated backup server by using either FTP or SFTP.

Procedure

To configure a database backup, do the following procedure:

Step 1 From the navigation pane, choose **System > Database Backup**.

The Backup Summary window is displayed.

Step 2 To configure a backup, click **Configure Backups** (near the top of the window).

Step 3 To indicate how often you want the backup to automatically run, select one of the following options:

- To do a database backup at the same time each day, click the **Daily at** radio button.
- To do a database backup at the same time for multiple days during the week, click the **Weekly on** radio button, and then check the check box next to the days of the week that you want the automatic backup to run.

Step 4 In the two **at** fields, enter the time of day that you want the backup to run (such as 2:00).

Step 5 From the drop-down list next to the time of day entry fields, choose either **AM** or **PM**.

Step 6 From the drop-down list next to the AM/PM drop-down list, choose the time zone.

Step 7 To enter details for the server on which you want to save the database backup, enter the following:

a. Enter either the server name (if DNS is in use) or the IP address.

b. Enter the directory path to the server.

c. Enter the username and password for the server.

d. Choose the transfer protocol from the drop-down list.

e. Enter the port number.

By default, the port number field auto-populates with one of the following port numbers to match the transfer protocol that you select in Step 7d.

When you select FTP as the transfer protocol, the port number 21 auto-populates.

When you select SFTP as the transfer protocol, the port number 22 auto-populates.

Step 8 To define a retention policy for the database backups, choose one or more of the following options:

- To define the number of database backups that you want to save, check the **This many backups** check box and enter a number in the field.
- To place a size limit on the memory that is allocated for the database backups on the server, check the **Until total size reaches** check box, and then enter the appropriate number in the MB field.

Note Although the size of a database file can increase as a system gathers more logs, Cisco recommends that the administrator plan for a database file of approximately 400 MB per backup.

- To save database backups for a set number of days, check the **Backups for up to** check box, and then enter a number in the days field.

Step 9 To save your configuration, click **Save**.

Note If you modified the field for the path, a warning message is displayed to inform you that the system is attempting to move the files from the previous path to the new one. If you modified the field for the host, the system does not attempt to move the files.

Step 10 (Optional) Click **Synchronize Server Status**.

If the system cannot locate the backup file on the new server, the system does not mark the file as missing at that time. Instead, the system preserves the historical backup entries that are associated with that backup. The system remembers that the backup was successful on that particular server.

If the system locates the backup file from the previous host on the new server, the backup entry is updated to display the presence on the new server.

Understanding Backward Compatibility

Release 1.1 is backward compatible with Release 1.0. This means that you can use the Release 1.0 APIs with a Release 1.1 system.

For information on using backward compatibility, refer to the *API User Guide for the Cisco TelePresence Exchange System*, available at http://www.cisco.com/en/US/products/ps11276/products_programming_reference_guides_list.html.

Changing Global Configuration Settings

Global Configuration settings are those which apply to the system as a whole, rather than to a specific entity such as a service provider, organization, or meeting.

The following sections describe how to configure these global configuration settings:

- Configuring Number of Rows to Display Per List Page, page 8-10
- Configuring Meet-Me Default Screens, page 8-10

Configuring Number of Rows to Display Per List Page

You can control the number of rows that display on the page at one time in lists in the administration console (for example, on the Alarms, Time Zones, or Meetings list pages) by changing the value of the Number of Rows to Display Per List Page field. The new value takes effect for all users of the administration console.

Procedure

To configure the Number of Rows to Display Per List Page setting, do the following procedure:

Step 1 From the navigation pane, choose **System > Global Configuration**.

The Global Configuration window is displayed.

Step 2 Modify the Number of Rows to Display Per List Page field value as required.

Fields on the page are described in Table 8-5.

Step 3 To save your changes, click **Save**.

The change takes effect immediately after you save the page.

Configuring Meet-Me Default Screens

The MeetMe Default Screens global setting allows you control over the number of segments that the system reserves for unprovisioned endpoints that do not have a media profile associated with them (in other words, for dial-in calls or for dial-out situations where no media profile is specified by the meeting scheduler). In these cases, if the meeting is hosted on a CTMS bridge, the system reserves MeetMe Default Screens + 1 segments (the additional segment is to account for the possibility of 30 FPS presentation sharing). If the meeting is hosted on a TPS bridge, the system reserves MeetMe Default Screens. The system always reserves one screen for these endpoints on an MCU MSE 8510 bridge.

The value of MeetMe Default Screens is also used to calculate the amount of capacity to reserve for a Rendezvous meeting. In this case, the system multiplies the value that you specify for Number of Endpoints by a fixed number of segments for the type of bridge (MeetMe Default Screens + 1 for CTMS, MeetMe Default Screens for TPS, and 1 for MSE 8510). This gives a “worst-case” estimation assuming that all endpoints that join will use the same amount of bandwidth. The system then adds the value of the Additional Capacity field on to the total.

Note Lowering the MeetMe Default Screens value may cause capacity problems for all meetings concurrently hosted on the bridge if unprovisioned endpoints with more screens than are reserved join the meeting. We recommend that you provision all endpoints that have more screens than the MeetMe Default Screens value.

At attend time, the system uses the value of MeetMe Default Screens to determine the number of segments to allocate when an unprovisioned or remote endpoint joins the meeting, using the same bridge type-based calculation (MeetMe Default Screens + 1 for CTMS, MeetMe Default Screens for TPS, or 1 for MSE 8510).

For more information on capacity reservation and allocation, see Appendix B, "Organization Bandwidth, Endpoint Capacity, Protocols and Bridge Selection."

Procedure

To configure MeetMe Default Screens, do the following procedure:

Step 1 From the navigation pane, choose **System > Global Configuration**.

The Global Configuration window is displayed.

Step 2 Modify the MeetMe Default Screens field value as required.

Fields on the page are described in Table 8-5.

Step 3 To save your changes, click **Save**.

Step 4 After saving your changes, restart the call engine servers in order for the change to take effect.

Configuring the SIP Load Balancer Address

The administrator defines the SIP load-balancer address for call engines that employ the ACE for redundancy. Generally, the administrator defines the SIP load-balancer address on the system after installation and in situations in which the IP address of the call engines or the ACE changes.

Procedure

To configure a SIP Load Balancer Address, do the following procedure:

Step 1 From the navigation pane, choose **System > Global Configuration**.

The Global Configuration window is displayed.

Step 2 Modify the SIP Load Balancer Address field value as required.

Fields on the page are described in Table 8-5.

Step 3 To save your changes, click **Save**.

Step 4 After saving your changes, restart the call engine servers in order for the change to take effect.

Configuring an ISDN Dial Out Prefix

When you define an ISDN Dialout Prefix value, the system adds a prefix to the beginning of all ISDN dial out calls. For example, if the endpoint number is 4013164407 and the defined ISDN prefix number is 9, then the call will be sent out as 94013164407.

The Cisco VCS call manager references the ISDN Dialout Prefix to determine whether to send the call to the ISDN gateway. If the configured ISDN Dialout Prefix does not match the value that is configured within the Cisco VCS, then all ISDN dial outs fail. When the call is sent to the ISDN gateway, the ISDN prefix is removed, restoring the original number.

The system default for the ISDN Dialout Prefix is 9. The administrator can modify the default ISDN Dialout Prefix setting when the value of 9 is already in use by another system, or to match a different value that is set in the Cisco VCS.

Note The ISDN Dialout Prefix must not match the prefix of any provisioned or unprovisioned endpoints. If the prefixes match, the Cisco TelePresence Exchange System will not properly recognize the endpoint, causing problems such as failure to start a meeting if the endpoint is configured as a host.

Note ISDN calls may fail if the ISDN Dialout Prefix is set to null or does not match the value that is configured within the Cisco VCS.

Procedure

To configure an ISDN dial out prefix other than the system default value of 9, do the following procedure:

Step 1 From the navigation pane, choose **System > Global Configuration**.

The Global Configuration window is displayed.

Step 2 Modify the ISDN Dialout Prefix field value as required.

Fields on the page are described in Table 8-5.

Step 3 To save your changes, click **Save**.

Step 4 After saving your changes, restart the call engine servers in order for the change to take effect.

Global Configuration Fields

Table 8-5 Global Configuration Field Descriptions

Field	Description
Number of Rows to Display Per List Page	The number of rows that display on the page at one time in lists in the administration console (for example, on the Alarms, Time Zones, or Meetings list pages). The range of this field is 10 to 100. The default value is 20 items.
MeetMe Default Screens	Enter a value which the Cisco TelePresence Exchange System uses to calculate the number of segments to reserve for unprovisioned endpoints that do not have a media profile associated with them (in other words, for dial-in calls or for dial-out situations where no media profile is specified by the meeting scheduler). The system calculates the number of segments based on the type of media bridge resource that is scheduled to host the meeting, as follows: • CTMS—MeetMe Default Screens +1 • TPS—MeetMe Default Screens • MCU MSE 8510—1 segment, regardless of this value. For Rendezvous meetings, the system multiplies the value that you specify for Number of Endpoints by the same bridge type-based calculation as above (MeetMe Default Screens + 1 for CTMS, MeetMe Default Screens for TPS, and 1 for MSE 8510) and then adds the value of the Additional Capacity field to calculate the total capacity to reserve. **Note** Lowering the MeetMe Default Screens value may cause capacity problems on the bridge if unprovisioned endpoints with more screens than are reserved join the meeting. At attend time, the system uses the value of MeetMe Default Screens to determine the number of segments to allocate when an unprovisioned or remote endpoint joins the meeting, using the same bridge type-based calculation (MeetMe Default Screens + 1 for CTMS, MeetMe Default Screens for TPS, or 1 for MSE 8510).
SIP Load Balancer Address	Enter the address used to load balance SIP messages for call engines that employ the Cisco Application Control Engine (ACE) for redundancy. You typically enter the SIP load-balancer address on the system after installation and in situations in which the IP address of the call engines or the ACE changes.
ISDN Dialout Prefix	By default, the ISDN Dialout Prefix value is 9. The value must match the setting in the Cisco TelePresence Video Communication Server (Cisco VCS), and must not match the prefix of any provisioned or unprovisioned endpoints.