New and Changed Information for Cisco Unified Communications Manager Release 8.6(2)

Contents

New and Changed Information for Cisco Unified Communications Manager Release 8.6(2) contains information about the following topics:

Note The Cisco Unified Communications Manager 8.6(2) documentation collection consists of the following: New and Changed Information, Release Notes, the Documentation Guide and the Compatibility Matrix. You must use these documents in conjunction with the complete documentation collection for Unified CM 8.6(1).

Installation, Upgrade, and Migration

This section contains information about the following topics:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Before You Begin

This section provides important pre-installation and pre-upgrade reminders and cautionary notes.

Caution When you upgrade to Cisco Unified Communications Manager (Unified CM) 8.6(2), the system reboots as part of the upgrade process. Therefore, you may want to perform the upgrade during a scheduled down time for your organization to avoid service interruptions.

Caution If you are upgrading your software on HP 7825H3 or HP 7828H3 hardware, there is no option to revert to the previous version of Unified CM. You must back up your system before you begin the upgrade.

To perform an upgrade on one of these machines you must use a 16 GB USB key to migrate data from the old system to the new installation.

If you are upgrading software on HP7825H3 or HP7828H3 hardware, ensure that you have a 16 GB USB device available to migrate your data to the new system. For Cisco Unity Connection and Cisco Unified Communications Manager Business Edition 5000, a 128 GB external USB device is required.

Note When you upgrade to Cisco Unified Communications Manager 8.6(2), the system reboots several times as part of the upgrade process and the service outage period is longer than with traditional upgrades. Therefore, you may want to perform the upgrade during a scheduled down time for your organization to avoid service interruptions. After you start the upgrade (either from the command line or graphical user interface), the data is migrated, the system reboots automatically, and the temporary service outage begins. The duration of this outage depends on your configuration and the amount of data that needs to be migrated.

When the upgrade is complete, you can choose to activate the partition with the new upgrade software or return to using the partition with the previous version of the software. With the exception of HP 7825H3 and HP 7828H3 hardware upgrades, the previous software remains in the inactive partition until the next upgrade. Your configuration information migrates automatically to the upgraded version in the active partition.

If for any reason you decide to back out of the upgrade, you can restart the system to the inactive partition that contains the older version of the software. However, any configuration changes that you made you upgraded the software will be lost.

Note You can make changes only to the database on the active partition. The database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching the partition.

Caution Be sure to back up your system data before starting the software upgrade process. For more information, see the *Disaster Recovery System Administration Guide*.

Before you proceed with the installation, consider the following recommendations:

- You will face a problem during RAID creation when you install Cisco Unified Communications Manager 8.5 or an earlier version on 7825 H3 and 7528 H3 servers that currently have Cisco Unified Communications Manager 8.6 installed on it. To resolve the issue:
  a. Boot the Unified CM server with the Unified CM 8.6 recovery disc.
  b. When prompted, choose option **C** to wipe off all data from the system. Option C indicates "Cleaning the system to set to bare metal state."

  You can now proceed with the installation of the earlier versions of Unified CM.
- When you insert or remove a USB drive, you might see error messages on the console similar to "sdb: assuming drive cache: write through." You can safely ignore these messages.

Unified CM on Virtualized Servers with Small Hard Drives

Unified CM can be installed on virtual servers with smaller hard drives to support deployments with fewer users.

For deployments of 2,500 users with a small disk (55 GB), log files must be cleaned up by an administrator before an upgrade. Alternately, an administrator can configure the system to automatically clean log files more frequently.

A deployment of 2,500 users with a small disk (55 GB) should be used only for a deployment where the total number of users on the cluster is less than 2,500. If this deployment option is used, each node in the cluster must use the same deployment. Migration from this deployment to large deployments is not supported.

VMware Specs-Based Support

Cisco supports Unified Communications applications running in a virtual environment if they meet certain criteria. VMware Specs-based support now supports the following CPUs at 2.4+ GHz speed:

- E7-2800
- E7-4800
- E7-8800

For information on VMware specs-based support, see http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment.

Supported OVA Templates

Cisco Unified Communications Manager 8.6 enhances user scalability, growing to 10,000 users per server and 80,000 users per megacluster. CTI scalability improves even more, providing 100 percent coverage for these user counts. For more information, see

http://docwiki.cisco.com/wiki/OVA_Template_Details_for_Unifed_CM_Release_8.6

Software Upgrades

Note If you upgrade to the U.S. export unrestricted version of Unified CM, you will not be able to upgrade later to, or to perform a fresh install of the U.S. export restricted version of this software. IP phone security configurations are modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

Command Line Interface

This section contains information about the following topic:

set account enable

This command enables the OS user account that was disabled because of password inactivity.

Note If the OS admin account is expired, you cannot enable *user-id*. While enabling inactivity, please make sure that the OS admin account does not become inactive before other admin accounts.

Command syntax

Set account enable *user-id*

Parameters

- *user-id* specifies the user ID of the account that was disabled.

Cisco Unified Communications Manager Administration

This section contains information about the following topics:

New and Updated Enterprise and System Parameters

Enterprise Parameters

There are no new or updated enterprise parameters for Unified CM 8.6(2).

Service Parameters

There are no new or updated system parameters for Unified CM 8.6(2).

Menu Changes

Main Window

There are no new or updated changes for the main window for Unified CM 8.6(2).

System

The System menu contains the following updates:

- **System > Device Pool**—A new field has been added to the Device Pool Configuration window:
  - Redirecting Party Transformation CSS—This drop-down menu enables transforming the redirecting party number on the device to E164 format. Cisco Unified Communications Manager includes the transformed number in the diversion header of invite messages for SIP trunks and in the Redirecting Number Information Element of setup message (for H.323 and MGCP) sent out of Cisco Unified Communications Manager.
  - Remove MER V.150—The SIP trunk removes V.150 MER SDP lines in outbound offers. Select this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Cisco Unified Communications Manager.
  - Remove Pre-MER V.150—The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Select this option to reduce ambiguity when your cluster is contained in a network of MER compliant devices that are incapable of processing offers with pre-MER lines.

Call Routing

There are no updates or new fields for this menu in Unified CM 8.6(2).

Advanced Features

The Advanced Features menu contains the following updates:

- The EMCC Remote Cluster option (**Advanced Features > EMCC > EMCC Remote Cluster**) has been renamed as Cluster View.
- The Cluster View option has been moved to **Advanced Features > Cluster View**.

Media Resources

There are no updates or new fields for Media Resources in Unified CM 8.6(2).

Device

The Device menu contains the following updates:

- **Device > Gateway**—New fields were added to the 'Outbound Calls' section of the Gateway Configuration window:
  - Redirecting Party Transformation CSS—This drop-down menu enables transforming the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of H.323 setup message that is sent out of Cisco Unified Communications Manager.
  - Use Device Pool Redirecting Party Transformation CSS—Check this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to the device. If this check box is not checked, the device uses the Redirecting Party Transformation CSS that is configured in the H.323 Gateway Configuration window.

- **Device > Gateway**—New fields were added to the ‘PRI Protocol Type Specific Information’ section of Gateway Configuration window:
  - Redirecting Party Transformation CSS—This setting enables transforming the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of MGCP setup message sent out of Cisco Unified Communications Manager.
  - Use Device Pool Redirecting Transformation CSS—Check this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to the device. If this check box is not checked, the device uses the Redirecting Party Transformation CSS that is configured in the MGCP Gateway Configuration window.
- **Device > Gateway**—New fields were added to the ‘BRI Protocol Type Specific Information’ section of the Gateway Configuration window:
  - Redirecting Party Transformation CSS—This setting enables transforming the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of MGCP setup message sent out of Cisco Unified Communications Manager.
  - Use Device Pool Redirecting Transformation CSS—Check this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to the device. If this check box is not checked, the device uses the Redirecting Party Transformation CSS that is configured in the MGCP Gateway Configuration window.
- **Device > Phone**—The Allow Presentation Sharing using BFCP check box was added to the Protocol Specific Information section of the Phone Configuration window for specific third-party endpoints. BFCP allows users to share a presentation within an ongoing video conversation. This check box was added for the following third-party endpoints:
  - Generic Desktop Video Endpoint
  - Generic Multiple Screen Room System
  - Generic Single Screen Room System
  - Third-Party SIP Device (Advanced)
- **Device > Trunk**—New fields were added to the ‘Outbound Calls’ section of Trunk Configuration window:
  - Redirecting Party Transformation CSS—This drop-down menu enables transforming the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed redirecting party number in the diversion header of invite messages for SIP trunks and in the Redirecting Number Information Element of setup message (for H.323 and MGCP) sent out of Cisco Unified Communications Manager.
  - Use Device Pool Redirecting Party Transformation CSS—Check this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to the device. If this check box is not checked, the device uses the Redirecting Party Transformation CSS that is configured in the Trunk Configuration window.
- **Device > Device Settings > SIP Profile**—The Allow Presentation Sharing using BFCP check box was moved to the Trunk Specific Configuration section of the SIP Profile Configuration window. BFCP allows users to share a presentation within an ongoing video conversation. This check box enables BFCP on the SIP trunks between the video endpoints. BFCP configuration for SIP lines is performed on the Phone Configuration window.

Application

No updates or new fields exist for this menu.

Bulk Administration

No updates or new fields exist for this menu.

Cisco Unified Communications Manager Features and Applications

This section contains information about the following topics:

Auto Update Statistics (AUS)

Description

In earlier releases of Cisco Unified Communications Manager, the Cisco Database Layer Monitor service parameters **Maintenance Throttling for Tables** and **Maintenance Throttling for Stored Procedures** controlled the process for updating statistics about indexes. With Release 8.6(2), Unified CM uses Automatic Update Statistics, an intelligent statistics update feature that monitors the changes made in the database tables and updates only tables that need statistic updates. This feature saves considerable bandwidth, especially on VMware deployments of Unified CM. Automatic Update Statistics is now the default indexing method.

Unified CM Administration Configuration Tips

No configuration tips exist for this feature.

GUI Changes

No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(2), you can enable this feature through the CLI.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Session Persistency

Session persistency allows mobile users to roam between different networks (e.g. Wi-Fi, VPN over 3G/4G) without having to re-register with Cisco Unified Communications Manager. It also allows users to maintain registration with Cisco Unified Communications Manager in the case of network connectivity loss.

The Session persistency feature provides dynamic IP address/port change via keep-alive registration, to facilitate connectivity during roaming between networks, and a configurable TCP reconnect timer to allow the users to remain connected in case of a temporary network connectivity loss or roaming. The reconnect timer must be enabled at the product level. The timer is in effect only when the mobile device tears down the original TCP connection explicitly.

Note Session persistency is designed for mobile devices, including Cisco Cius SP (4G) and other SIP endpoints. It is not designed for Cisco desk phones, which do not roam or dynamically change their IP address/ports. Session persistency is also not designed for Cisco Cius Wi Fi units.

Unified CM Administration Configuration Tips

Dynamic IP address/port change allows an endpoint to connect to a different IP address/port via keep-alive registration. No Cisco Unified Communications Manager Administration configuration is required for Dynamic port change.

The Time to Wait for Seamless Reconnect After TCP Drop or Roaming (seconds) parameter is configured in Cisco Unified Communications Manager by entering value for reconnect timer, in seconds, in the “Product Specific Configuration Layout” window.

To set Session Persistency feature parameters, perform the following steps:

Procedure

Step 1 Navigate to the appropriate Product Specific Configuration Layout window in Cisco Unified Communications Manager.

Step 2 Enter a value for Time to Wait for Seamless Reconnect After TCP Drop or Roaming (in seconds).

Note The default value is 5 seconds with a range of 0 to 300 seconds. Be aware that entering a value of 0 in the field disables the feature. To save the new timer value, check the "Override Common Settings" check box.

Note For more information about the parameter, click the "?" icon in the Product Specific Configuration Layout window.

GUI Changes

The Time to Wait for Seamless Reconnect After TCP Drop or Roaming (seconds) field has been added to the following windows:

- Phone Configuration window (**Device > Phone > Add New > Cius**); Product Specific Configuration Layout portion of window
- Common Phone Profile window (**Device > Device Settings > Common Phone Profile**); Product Specific Configuration Layout portion of window
- Enterprise Phone Configuration window (**System > Enterprise Phone Configuration**)

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(2), you can use this feature.

Serviceability Considerations

You can configure Session persistency at the Device, Common Phone Profile, or Enterprise Phone Configuration levels through Cisco Unified Communications Manager Administration.

When a refresh register with IP address change is accepted, a DeviceRegistered alarm (EndPointRegistered) is sent to the Serviceability layer with the new IP address.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Cisco Proxy TFTP Server

Cisco Unified Communications Manager 8.6(2) and later introduces the Cisco Proxy TFTP Server feature, which enables all endpoints in a large-scale deployment to download the configuration file and register to Unified CM. This feature also allows you to add any number of alternate TFTP servers.

Deployment Models

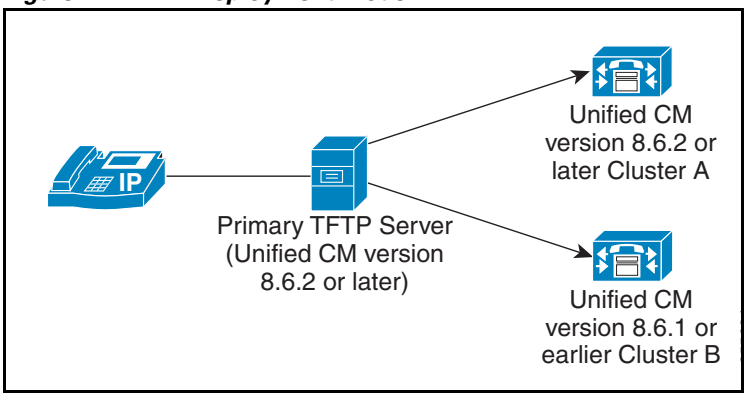
Cisco Proxy TFTP Server supports the following deployment models:

- Deployment Model 1
- Deployment Model 2

Deployment Model 1

For the deployment model illustrated in Figure 1, the primary TFTP server must be running Unified CM 8.6(2) or later.

Figure 1 Deployment Model 1



In Figure 1, two remote clusters, Cluster A and Cluster B, have been configured to the primary TFTP server. However, you can configure any number of remote clusters to the primary TFTP server.

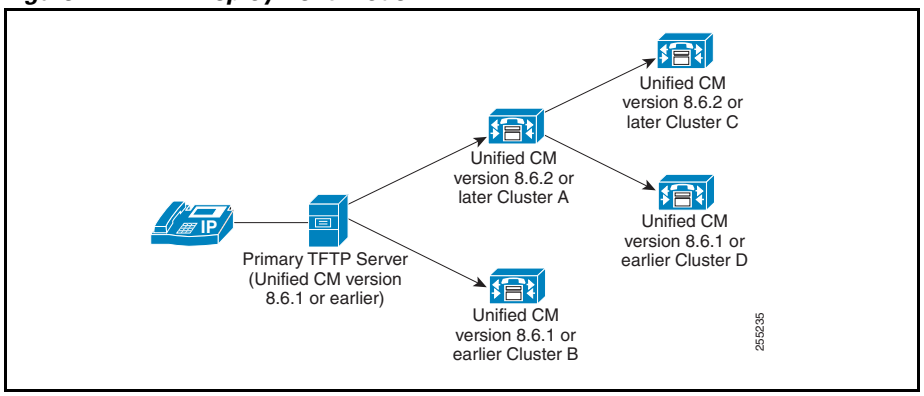
When an endpoint sends a request for a configuration file, the primary TFTP server checks the local cache and the configured remote clusters. Thus, an endpoint (configured to the primary TFTP server Cluster, Cluster A and Cluster B) receives the configuration file and registers to the Cisco Unified Communications Manager.

Note Cisco recommends that you use Deployment Model 1 for superior system performance. However, if you do not wish to change your existing Centralized TFTP (8.6(1) or earlier), you can use Deployment Model 2.

Deployment Model 2

In the deployment model illustrated in Figure 2, the centralized Unified CM TFTP server acts as a primary TFTP server.

Figure 2 Deployment Model 2



In Figure 2, two remote clusters, Cluster A and Cluster B, have been configured to the Primary TFTP Server. However, you can configure any number of remote clusters to the Primary TFTP Server.

In deployment model 2, two more remote clusters have been added to Cluster A. When an endpoint sends a request for the configuration file, the Primary TFTP Server checks the local cache and the configured remote clusters (Cluster A and Cluster B). Cluster A then checks its configured remote clusters (Cluster C and Cluster D). Thus, all the endpoints configured to the Primary TFTP Server Cluster (Cluster A, Cluster B, Cluster C and Cluster D) receive the configuration file and register to the Cisco Unified Communications Manager.

Use Cases and Best Practices

Consider the following scenarios that detail how Proxy TFTP can be used and the best practices for implementation.

1. The cluster can act as just a proxy TFTP cluster with no other purpose. In this case, the cluster has no relationship with the other clusters, and does not process calls. For this scenario, the Remote Cluster TFTP is manually defined and rollback to pre-8.0 is recommended. Autoregistration will not work in this scenario
2. The cluster is a remote cluster that is also acting as a Proxy TFTP server for remote clusters. In this case, the cluster has no relationship with other clusters and does not process calls. The remote cluster is manually defined, and Autoregistration should not be enabled.

Configuration Checklist for TFTP

Cisco proxy TFTP server can be configured manually as well as dynamically. This section provides the following configuration checklists for TFTP:

- Manual Configuration
- Dynamic Configuration

Manual Configuration

To configure Cisco Proxy TFTP Server manually in your network, complete the following procedure.

Procedure

Step 1 Create a new cluster by taking the following actions:

a. In Cisco Unified Communications Manager Administration, select **Advanced Features > Cluster View**.

b. Enter the cluster Id and fully qualified domain name in the appropriate fields.

Step 2 Check the **Enable** check box for TFTP service.

Step 3 Click the TFTP hyperlink.

The Remote Cluster Manually Override Configuration window displays.

Step 4 Choose **Manually Configure Remote Service addresses**.

Step 5 Enter IP addresses for the TFTP servers of the remote clusters.

Step 6 Click **Save**.

Dynamic Configuration

Complete the following procedure to configure Cisco Proxy TFTP Server dynamically in your network.

Procedure

Step 1 Configure EMCC.

Step 2 In Cisco Unified Communications Manager Administration, choose **Advanced Features > Cluster View > Update Remote Cluster Now.**

Proxy TFTP Server vs. Centralized TFTP Server

For large scale deployments, the Centralized TFTP server has the following limitations:

- Occasionally endpoints are unable to download the configuration file because the primary TFTP server takes more time to get the configuration file from the alternate TFTP servers. By the time the primary TFTP server gets the file, the endpoints get timed out. As a result, endpoints never get registered to their Unified CM.
- Only ten alternate TFTP servers can be added.

These limitations are not applicable to Cisco Proxy TFTP Server.

Phone Behavior With Proxy TFTP Server

For phones that are configured to remote clusters, first-time phone registration may take a few minutes. The time delay is due to Proxy TFTP Server searching for the configuration file in the remote clusters. The delay will vary based on the number of endpoints and the number of remote clusters that are configured. However, subsequent registrations will not have any delay.

System Requirements for Proxy TFTP Server

The following system requirements exist for Cisco Proxy TFTP Server:

- Cisco Unified Communications Manager Release 8.6(2) or later
- Cisco TFTP service must be activated and in running state

Interactions and Restrictions

This section provides the details of interactions and restrictions for Cisco Proxy TFTP Server. See the following topics:

- Proxy TFTP Server Interactions, page 13
- Proxy TFTP Server Restrictions, page 13

Proxy TFTP Server Interactions

Cisco TFTP service of the Proxy TFTP server interacts with the TFTP services of the remote clusters. In the Cluster View window (**Advanced Features > Cluster View**), for a particular remote cluster, TFTP service can have a maximum of three IP addresses, and the Proxy TFTP server will interact with all three IP addresses if they are configured.

Note You must ensure that the Cisco TFTP service is active and in running state on the configured IP addresses.

Proxy TFTP Server Restrictions

This section lists the restrictions and limitations of the Cisco Proxy TFTP Server with other Cisco Unified Communications Manager Administration components.

Phones Unable to Register with Cluster

Follow these steps if phones in your cluster are no longer able to register correctly with the cluster.

1. Verify that full security mesh is established between the home and Proxy TFTP clusters:

- Perform a bulk import of the CallManager certificates from the Proxy TFTP server to the home cluster.
- Perform a bulk import of the CallManager certificates from the home clustser to the Proxy TFTP server.

2. On the home cluster, keep the **Prepare Cluster for Rollback to pre 8.0** set to **False**. This makes sure that phones will have Security by Default (SBD) enabled during normal operation.
3. On the Proxy TFTP cluster, set the **Prepare Cluster for Rollback to pre 8.0** to **False**.This makes sure that SBD is enabled on the Proxy TFTP server as well.

Caution When the Proxy TFTP cluster is set up, do not remove the cluster view configuration from the Proxy TFTP configuration. Removing the cluster view from the Proxy TFTP configuration can result in phones receiving a 404 file not found error, which sends the phones a default ITL file from the Proxy TFTP server. This scenario requires that the ITL files be manually deleted from the phones to correctly register back to the home cluster.

Registering Problems For Phones With Security By Default (SBD) Loads For Previous Versions of Cisco Unified Communications Manager 8.0

For remote cluster TFTP servers running on Cisco Unified Communications Manager 8.0 and later, the phones with Security By Default (SBD) loads can register to these remote cluster Unified CMs through a proxy TFTP server. However, the Identity Trust List (ITL) file is unavailable in previous versions of Unified CM earlier than 8.0. Therefore, for the remote cluster TFTP servers running a pre-8.0 version of Unified CM, the phones with SBD loads are unable to register to the remote cluster Unified CMs through a proxy TFTP server.

To overcome this issue, perform the following steps:

Procedure

Step 1 Connect the endpoint directly to the remote cluster Unified CM by taking the following actions:

a. Disable the DHCP option.

a. Enter the TFTP IP address on the phone manually.

The phone gets the required SBD load and registers to the Unified CM.

Step 2 Enable the DHCP option and reset the phone manually.

The phone gets registered to the remote cluster through proxy TFTP.

Note This procedure is applicable only if you have new phones with SBD load or if you plan to move the phones from a Unified CM with SBD support to a Unified CM without SBD support. This procedure is not applicable if the number of phones in a cluster is large.

Registering Problems While Moving A Phone From One Remote Cluster to Another

When you move a phone from one remote cluster to another, you must delete the old ITL files from the phone, so that it registers successfully to the new Unified CM.

Phones Takes Time to Register While Upgrading The Remote Cluster

When a remote cluster is upgraded, phones request a new load file which must be downloaded to the PTFTP local cache. If you plug in an Ethernet cable to a phone and then configure the phone to the Unified CM, the phone takes about 30 minutes to register. However, if you configure the phone to the Unified CM and then plug in the Ethernet cable the phone gets registered immediately.

Installing and Activating Cisco Proxy TFTP Server

After you install Cisco Unified Communications Manager, your network can support the Cisco Proxy TFTP Server feature if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see Configuration Checklist for TFTP, page 11.

Configuring Proxy TFTP Server

In Cisco Unified Communications Manager Administration, use the **Advanced Features > Cluster View** menu path to configure remote clusters.

Table 1 provides detailed descriptions of the remote cluster settings that you configure in the Cluster View window (**Advanced Features > Cluster View**).

Table 1 Cluster View Settings

Field	Description
Remote Cluster Information	
Cluster Id	Enter the cluster ID of the remote cluster. Valid values include alphanumeric characters, (a through z, A through Z, and 0 through 9) period (.), and hyphen (-).
Description	Enter a description for the remote cluster. This field accepts up to 128 characters. You may use any character except quotes (“), close angle bracket (>), open angle bracket (<), back slash (\), dash (-), ampersand (&), and percent sign (%).
Fully Qualified Name	Enter the fully qualified name of the remote cluster/IP address. This field accepts up to 50 characters and allows the following characters: alphanumeric (a through z, A through Z, and 0 through 9), period (.), dash (-), asterisk (*), and space ( ).
Remote Cluster Service Information	

Table 1 Cluster View Settings (continued)

Field	Description
EMCC	For the EMCC service, the following column headings detail the configuration for this service: • Enabled—Check this check box to enable the EMCC service. • Service—This entry specifies the EMCC service. • Remote Activated—Valid values specify true or false. • Address 1—This column lists the first address for this service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.
PSTN Access	For the PSTN Access, the following column headings detail the configuration for this service: • Enabled—Check this check box to enable PSTN Access. • Service—This entry specifies the PSTN Access. • Remote Activated—Valid values specify true or false. • Address 1—This column lists the first address for this service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.
RSVP Agent	For the RSVP Agent, the following column headings detail the configuration for this service: • Enabled—Check this check box to enable the RSVP Agent. • Service—This entry specifies the RSVP agent. • Remote Activated—Valid values specify true or false. • Address 1—This column lists the first address for this service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.

Table 1 Cluster View Settings (continued)

Field	Description
TFTP	For the TFTP service, the following column headings detail the configuration for this service: • Enabled—Check this check box to enable the TFTP service. • Service—This entry specifies the TFTP service. • Remote Activated—Valid values specify true or false. **Note** The value of the Remote Activated column is set to True whenever remote IP addresses are configured either manually or dynamically. • Address 1—This column lists the first address for this service. **Note** When you upgrade from Cisco Unified Communications Manager 8.6 (1) to Cisco Unified Communications Manager 8.6(2) or later, Address 1 is automatically updated by the system. However, if this field is blank after the upgrade due to DNS lookup failure or some other reason, you must manually update it with the appropriate IP address of the TFTP service. • Address 2—This column lists the second address for this service. • Address 3—This column lists the third address for this service.
Enabled All Services	Click this button to enable all services (EMCC, PSTN Access, and RSVP Agent).
Disabled All Services	Click this button to disable all services (EMCC, PSTN Access, and RSVP Agent).
Update Remote Cluster Now	Click this button to update the remote cluster immediately.

Cluster View Manually Override Configuration

You can manually configure remote server addresses for TFTP service by clicking the TFTP hyperlink in the Remote Cluster Service Configuration window. Table 2 provides detailed descriptions of the remote cluster configuration settings that you configure in the Remote Cluster Manually Override Configuration window (**Advanced Features > Cluster View > TFTP**).

Table 2 Cluster View Manually Override Configuration Settings

Field	Description
Use automatically determined remote server addresses	Choose this option to use automatically determined remote server addresses.
Manually Configure remote cluster addresses	Choose this option to manually configure remote server addresses.
Address 1	Enter the first address for the TFTP service.
Address 2	Enter the second address for the TFTP service.
Address 3	Enter the third address for the TFTP service.

Unified CM Administration Configuration Tips

See Configuration Checklist for TFTP, page 11 and Configuring Proxy TFTP Server, page 15.

GUI Changes

The following GUI changes have been made for this feature:

- The EMCC Remote Cluster option (**Advanced Features > EMCC > EMCC Remote Cluster**) has been renamed as Cluster View.
- The Cluster View option has been moved to **Advanced Features > Cluster View**.

Service Parameter and Enterprise Parameter Changes

No service parameter and enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(2) and later, you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Cluster-Wide Call Park

Description

Cisco Unified Communications Manager 8.6(2) allows you to enable call parking for cluster-wide configurations. The following changes are introduced with this feature:

- Park codes for all nodes in a Cisco Unified Communications Manager cluster are now allocated from a single entity, the lowest active node in the cluster. Therefore, Unified CM ignores the Cisco Unified Communications Manager field on the Call Park Configuration web page.
- The single entity allocates park codes from a pool of all configured park codes, regardless of which Unified CM is assigned.
- Unified CM allocates park codes through strict enforcement of the partition order in the Calling Search Space (CSS) of the parking party. This update provides a predictable behavior that is easy for administrators to understand.
- The parked calls limit is no longer 100 calls per cluster. Available park codes and system resources determine the number of parked calls.
- CTI monitoring of parked call Directory Numbers (DNs) is unavailable. This function will be restored in Unified CM Release 9.0.

CallPark Softkey

After the called party presses the CallPark softkey to park a call, Unified CM 8.6(2) takes the following actions to allocate a park code:

- The unique Unified CM node with the active CallParkCodeManager process allocates a park code.
- Unified CM checks the partition list of the CSS of the parking party for available park codes by searching each partition in order. If Unified CM finds a code, the system allocates the code and marks it as unavailable. If Unified CM does not find an available code in any of the partitions, the call park attempt fails.

Previous Call Park Behavior

In previous releases of Unified CM, the following actions occurred:

- The Unified CM node where the call originates (any node in the cluster) allocated a park code from the pool of codes that were assigned to that Unified CM node.
- Unified CM checked the list of available park codes, regardless of their partition order, to detect whether these codes existed in the CSS of the parking party. If Unified CM found an available code, the system allocated the code and marked it as unavailable. If Unified CM found no available code on the partitions, the call park attempt failed.

New Call Park Behavior

With these new Call Park behaviors, centralized Unified CM deployments that host multiple locations on a single cluster (such as retail stores and bank branches) can now place the park codes for each location into the partitions that are devoted to those locations. This placement prevents parties at one store from retrieving calls parked at another store. Also, the new Call Park behaviors reduce the difficulty of administering the feature, because administrators no longer need to place park codes in the CSS of each inbound trunk.

Finally, this behavior follows the partition order of a CSS when searching for objects, which aligns with the search behaviors of other Unified CM features described in the SRND. This behavior makes Call Park easier to understand, because administrators no longer need to assign park codes to every Unified CM node on the side where a call originates.

Enabling Cluster-Wide Call Park

To enable Cluster-Wide Call Park, perform the following steps:

Step 1 From Cisco Unified Communications Manager Administration, select **Advanced Service Parameters > Global Features**

Step 2 Set the Enable Clusterwide CallPark Number/Ranges service parameter to True.

Step 3 Restart all Unified CM services.

Unified CM Administration Configuration Tips

No tips.

GUI Changes

No GUI changes.

Service Parameter and Enterprise Parameter Changes

You enable Cluster-Wide Call Park with the service parameter Enable Clusterwide CallPark Number/Ranges.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(2), you can enable this feature service parameter.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Redirecting Number Transformation

Cisco Unified Communications Manager 8.6(2) and later supports the Redirecting Number Transformation feature, which enables transforming redirecting party number on a device (a gateway or a trunk) to E164 format.

GUI Changes

The following GUI changes were made for this feature:

- **System > Device Pool**—A new field has been added to the Device Pool Configuration window:

Redirecting Party Transformation CSS—This drop-down menu enables transforming the redirecting party number on the device to E164 format. Cisco Unified Communications Manager includes the transformed number in the diversion header of invite messages for SIP trunks and in the Redirecting Number Information Element of the setup message (for H.323 and MGCP) sent from Unified CM.

- **Device > Gateway**—New fields were added to the Outbound Calls section of Gateway Configuration window:
  - Redirecting Party Transformation CSS—This drop-down menu enables transforming the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of H.323 setup message that is sent out of Cisco Unified Communications Manager.
  - Use Device Pool Redirecting Party Transformation CSS—This check box is checked to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to the device. If this check box is not checked, the device uses the Redirecting Party Transformation CSS that is configured in the H.323 Gateway Configuration window.
- **Device > Gateway**—New fields were added to the PRI Protocol Type Specific Information section of Gateway Configuration window:
  - Redirecting Party Transformation CSS—This setting enables transforming the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of MGCP setup message that is sent out of Cisco Unified Communications Manager.
  - Use Device Pool Redirecting Transformation CSS—Check this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to the device. If this check box is not checked, the device uses the Redirecting Party Transformation CSS that is configured in the MGCP Gateway Configuration window.
- **Device > Gateway**—New fields were added to the BRI Protocol Type Specific Information section of Gateway Configuration window:
  - Redirecting Party Transformation CSS—This drop-down menu enables transforming the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of MGCP setup message that is sent out of Cisco Unified Communications Manager.
  - Use Device Pool Redirecting Transformation CSS—Check this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to the device. If this check box is not checked, the device uses the Redirecting Party Transformation CSS that is configured in the MGCP Gateway Configuration window.

- **Device > Trunk**—New fields were added to the Outbound Calls section of Trunk Configuration window:
  - Redirecting Party Transformation CSS—This drop-down menu enables transforming the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed redirecting party number in the diversion header of invite messages for SIP trunks and in the Redirecting Number Information Element of setup message (for H.323 and MGCP) that is sent out of Cisco Unified Communications Manager.
  - Use Device Pool Redirecting Party Transformation CSS—Check this check box to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to the device. If this check box is not checked, the device uses the Redirecting Party Transformation CSS that is configured in the Trunk Configuration window.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(2), you can use this feature.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

User Tips

No user tips exist for this feature.

Endpoint Support for the Binary Floor Control Protocol

Cisco Unified Communications Manager 8.6(2) provides support for the Binary Floor Control Protocol (BFCP) for specific Cisco and third-party video endpoints. BFCP allows users to share a presentation within an ongoing video conversation.

The following example shows how presentation sharing using BFCP works:

An ongoing video conversation exists between two video phones. User A decides to show User B a slide presentation that is saved on a laptop. User A attaches the laptop to a Cisco EX90 video phone and presses the Present button on the phone. The SIP INVITE message gets initiated to the other phone,

forming the invitation for a BFCP stream. After the BFCP session is negotiated, an additional stream is added to the audio and video streams. The BFCP stream allows User B to see the desktop on User A's laptop.

BFCP Support on Cisco Video Endpoints

For the following Cisco video endpoints, BFCP is enabled by default through the endpoint Qualification and Evaluation of device (QED) settings. Because BFCP is automatically enabled, Cisco Unified Communications Manager does not provide configuration options for these endpoints.

- Cisco E20
- Cisco TelePresence Codec C40
- Cisco TelePresence Codec C60
- Cisco TelePresence Codec C90
- Cisco TelePresence EX60
- Cisco TelePresence EX90
- Cisco TelePresence Quick Set C20
- Cisco TelePresence Profile 42 (C20)
- Cisco TelePresence Profile 42 (C60)
- Cisco TelePresence Profile 52 (C40)
- Cisco TelePresence Profile 42 (C60)
- Cisco TelePresence Profile 52 (C40)
- Cisco TelePresence Profile 52 (C60)
- Cisco TelePresence Profile 52 Dual (C60)
- Cisco TelePresence Profile 65 (C60)
- Cisco TelePresence Profile 65 Dual (C90)
- Cisco TelePresence
- Cisco TelePresence 1000
- Cisco TelePresence 1100
- Cisco TelePresence 1300-47
- Cisco TelePresence 1300-65
- Cisco TelePresence 1310-65
- Cisco TelePresence 3000
- Cisco TelePresence 3200
- Cisco TelePresence 500-32
- Cisco TelePresence 500-37

BFCP Support on Third-Party Phones

For the following third-party video endpoints, BFCP is disabled by default, but support can be enabled in the Protocol Specific Information section of the Phone Configuration window:

- Generic Desktop Video Endpoint
- Generic Multiple Screen Room System

- Generic Single Screen Room System
- Third Party SIP Device (Advanced)

Cisco Unified Communications Manager Administration Configuration Tips

Presentation sharing using BFCP is supported only on full SIP networks. The entire network, including the endpoints and all the intermediary devices and trunks, must be SIP. BFCP must be enabled on all SIP trunks and lines.

To configure BFCP on SIP trunks, check the **Allow Presentation Sharing using BFCP** check box in the Trunk Specific Configuration section of the SIP Profile Configuration window.

To configure BFCP on SIP lines:

- For Cisco video endpoints that support BFCP, no configuration on the SIP line is required.
- For third-party video endpoints that support BFCP, enable BFCP by checking the **Allow Presentation Sharing using BFCP** check box in the Protocol Specific Information section of the Phone Configuration window.

GUI Changes

The following GUI changes were made for this feature:

- **Device Settings > SIP Profile**—The **Allow Presentation Sharing using BFCP** check box has been moved to the Trunk Specific Configuration section of the SIP Profile Configuration window.
- **Device Settings > Phone**—The **Allow Presentation Sharing using BFCP** check box has been added to the Protocol Specific Information section of the Phone Configuration window for the following third-party phones:
  - Generic Desktop Video Endpoint
  - Generic Multiple Screen Room System
  - Generic Single Screen Room System
  - Third-party SIP Device (Advanced)

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(2), you can use this feature.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

User Tips

No user tips exist for this feature.

New Feature for Restoring the Database of a Publisher Node

When using the Disaster Recovery System to restore the publisher node of a Cisco Unified Communications Manager cluster, you can restore the publisher database using the database from one of the subscriber nodes.

If the backup file that you select for the restore process includes a CCMDB database component, a drop-down list box appears in the Restore wizard that allows you to choose the node from which to restore database data. When you use this option, Cisco Unified Communications Manager restores the publisher database from the database of the chosen subscriber node, and restores all nondatabase components from the backup file that was selected during the restore process.

If the backup file that you select does not include a database component, the drop-down list box does not appear.

This feature is intended for situations where you need to restore the user-facing features from the subscriber node and a backup file for the publisher exists. If no backup of the publisher node exists, this feature is not available.

Unified CM Administration Configuration Tips

No configuration tips exist for this feature.

GUI Changes

A new drop-down list box has been added to the Disaster Recovery System Restore wizard, which can be accessed by clicking **Restore > Restore Wizard.** The following drop-down list box appears if the backup file that is selected includes the CCMDB database component. If the backup file does not include the CCMDB database component, the drop-down list box does not appear.

- Select Server Name—This drop-down list box allows you to select the cluster node from which you want to restore the publisher database.

Service Parameter and Enterprise Parameter Changes

No service parameter and enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(2) and later, you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Binary Floor Control Protocol

Cisco Unified Communications Manager supports Binary Floor Control Protocol (BFCP) between Cisco Unified Communications Manager and a Cisco TelePresence MCU.

Security

There are no new or updated security features for Unified CM 8.6(2).

Cisco Unified IP Phones

This section contains information about the following topic:

- Cisco Unified Real-Time Monitoring Tool, page 26

Cisco Unified Real-Time Monitoring Tool

Windows 7 support

You can install Cisco Unified Real-Time Monitoring Tool (Unified RTMT) on a computer running Windows 7.

Note To create a Unified RTMT certificate store on a Windows 7 platform, you must have a username with full administrative privileges.

Installing RTMT

You can choose the following added default installation paths to install Unified RTMT on Cisco Unified Communications Manager Business Edition 3000.

- Windows 7 32 bit—C:\Program Files\Cisco\Unified Serviceability\JRtmt
- Windows 7 64 bit—C:\Program Files (x86)\Cisco\Unified Serviceability\JRtmt

Cisco Unified Communications Manager Business Edition 3000

This section contains the following topics:

Country/Locale Settings

Country Pack supports the following countries: NANP, India, United Kingdom, China, Australia, France, Russia, Canada, Spain, Italy, and Saudi Arabia.

Diagnostics Settings

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, download the USB diagnostics file, capture network packets, and enable or disable loopback for T1/E1 interfaces.

Collect Logs

Use the Collect Log option of the Diagnostics Settings feature to download and trace the enable logging, disable logging, and generate a log file on a Unified CMBE 3000 server.

Table 3 describes the settings that you can use to enable or disable detailed logging, generate logs, cancel logs, and download the log file on the Collect Logs tab.

Table 3 Settings on the Collect Logs Tab

Setting	Description
Enable Logging	To enable the system to collect log data, click **Enable Logging**. After you click this button, it dims and the Disable Logging button becomes enabled. The time stamp next to the Enable Logging button displays the enabled log start date and time. You can now attempt to reproduce the issue with your system. **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 3 Settings on the Collect Logs Tab (continued)

Setting	Description
Disable Logging	After you reproduce the system issue, click **Disable Logging** to stop the system from collecting log data. After you click this button, it dims and the Enable Logging button becomes enabled. The time stamp next to the Disable Logging button displays the log file stop date and time.
Generate a log file in preparation for download	**All available files**—Choose this option to collect all the available log files. **All files within a specific time range**—Choose this option to specify the time range (from and to date and time) for which you want to collect logs.
Generate Log File	To prepare a log file, click **Generate Log File**. **Tip** You can generate a log file without enabling or disabling the logging functionality by clicking **Generate Log File** at any time and downloading the generated log files. **Note** If you generate a new log file, the existing log file will be replaced with the new log file. The progress bar indicates the progress of log collection. After a log file is created, a link appears that lets you download the generated log file to your PC. **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. To stop the log generation process in the middle, click **Cancel.**

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 4 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 4 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 5 describes the test characters that the ping facility sends.

Table 5 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 the server, entering the hostname will not work. • Select the number of the **Ping Attempts** from the drop-drown list. After reaching the specified number of attempts, the Ping operation will stop automatically. 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 canceled. **Note** If you click the **Cancel Ping** button in the middle of a ping process, the ping operation is canceled for the remaining iterations. A message appears in the Ping output box stating “Ping Canceled”.

Troubleshooting Issues

T1/E1 and ECAN Statistics are activated based on the following circumstances on Unified CMBE 3000.

Enable or Disable T1/E1 and ECAN Statistics Logging

Description

When enabling or disabling the T1/E1 and ECAN statistics logging in the Administrative Interface, if the alarm is activated, the T1/E1 status does not increase.

The T1/E1 and ECAN statistics is activated based on the following:

- Enable logging on the Administrative Interface.
- When the error count related to T1/E1 increases, the T1/E1 statistics is logged for every 30 seconds in FGASyslog.
- When there is no error count related to T1/E1, the T1/E1 statistics is logged for every 2 minutes in FGASyslog.
- ECAN is collected for every 1 minute and it is collected on all active channels only.
- The ECAN logging stops if FGA resets.

Resolution

- To enable T1/E1 and ECAN statistics perform the following steps:
  - Click **Enable Logging** on the Diagnostics page (**Monitoring > Diagnostics**). The T1/E1 and ECAN statistics logging is also enabled.
  - Click the **Generate Log File** on the Diagnostics page, and download the file to your PC to view the FGASyslog file, which contains the T1/E1 and ECAN statistics logs.

To disable T1/E1 and ECAN statistics click **Disable Logging** on the Diagnostics page (**Monitoring > Diagnostics**). The T1/E1 and ECAN statistics logging is also disabled.

Installed Software Settings

The Installed Software page allows you to view the Optional Software Packages on your Unified CMBE 3000 server. You can use the **Maintenance > Upgrade** page to install the Optional Software Packages that are required for your Unified CMBE 3000 system.

Table 6 lists the name of the Cisco Option Package (COP) files and their respective naming conventions.

Table 6 COP files and Their Respective Naming Conventions

File Type	Naming convention
Unified CM Localization COP files	cm-locale-<>.cop
PO Localization COP files	po-locale-<>.cop
Device Pack COP file	cmterm-devicepack<>.cop
Common cmterm COP file	cmterm-<>.cop
Unified CM Connection Pack COP files	cm-conp-CP-<>.cop
General COP files	ucos<>.cop
General COP files	ciscocm<>.cop
CSA COP files	platform-csa-<>.cop
Country pack files	cm-locale-arabic_saudi_arabia_CP-8.6.1.9902-208.cop

Table 7 describes the settings that are displayed on the Installed Software page (**Maintenance > Installed Software**).

Table 7 Settings on the Installed Software Page

Setting	Description
System Software	**Active Version** refers to the latest installed Unified CMBE 3000 version on your system. **Inactive Version** refers to the previous version of Unified CMBE 3000. The Inactive Version is not displayed if there is no previous version of Unified CMBE 3000 available. **Note** Both the active and inactive versions are available in read-only mode.
Optional Software Packages	**Optional Software Packages** display the name and installation date of the installed the Optional Software Packages on your system. **Note** By default, the optional software packages are sorted by their names. The Optional Software Packages can also be sorted by the installation date on your system.