Release Notes for Cisco Intercompany Media Engine Release 8.6(1)

June 12, 2012

This document contains information pertinent to Cisco Intercompany Media Engine (IME) Release 8.6(1).

Contents

This document includes the following information:

Introduction

The Cisco Intercompany Media Engine server and software function as a key component of the Cisco Intercompany Media Engine feature that provides a technique for establishing direct IP connectivity between enterprises by combining peer-to-peer technologies with the existing public switched telephone network (PSTN) infrastructure.

These release notes are based on software versions Cisco Intercompany Media Engine: 8.6.1.10000-18.

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

System Requirements

The following sections comprise the system requirements for this release of Cisco Intercompany Media Engine.

Server Support

Make sure that you install and configure Cisco Intercompany Media Engine on a Cisco Media Convergence Server (MCS).

The following servers are compatible with this release:

- MCS-7825-H3
- MCS-7825-I3
- MCS-7825-H4
- MCS-7825-I4
- MCS-7825-I5
- MCS-7845-H2
- MCS-7845-I2
- MCS-7845-H3
- MCS-7845-I3

Uninterruptible Power Supply

Cisco recommends that you connect each Cisco Intercompany Media Engineserver to an uninterruptible power supply (UPS) to provide backup power and protect your system against a power failure.

Note You must connect MCS-7825 servers to a UPS to prevent file system corruption during power outages.

Upgrading to Cisco Intercompany Media Engine 8.6(1)

The following sections contain information that is pertinent to upgrading to this release of Cisco Intercompany Media Engine.

Before You Begin

Caution When you upgrade to Cisco Intercompany Media Engine 8.6(1) 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 In Cisco Intercompany Media Engine 8.6(1), the image available for download from Cisco.com is a bootable image that can be burned to DVD and used for both upgrades and fresh installs. Cisco Intercompany Media Engine 8.6(1) upgrade DVDs ordered from Cisco are also bootable for use with upgrades or fresh installs.

If performing an L2 upgrade, choose no for automatic reboot.

Pre-Upgrade Tasks

Before you begin the upgrade, perform the following tasks:

- Ensure that you have the necessary license files for the new release.

  For more information on obtaining and installing licenses, see the License File Upload chapter in the *Cisco Intercompany Media Engine Installation and Configuration Guide*.
- Before you begin the upgrade, back up your system. This is particularly important if you are upgrading software on HP7825H3 or HP7828H3 hardware as there is no option to revert to the previous version.
- If you are upgrading software on HP7825H3 or HP7828H3 hardware, ensure that you have a 16GB USB device available to migrate your data to the new system.
- Before you upgrade to a later release, refer to the documentation for your currently installed COP files to identify any special considerations related to upgrading Cisco Intercompany Media Engine.
- If upgrading from 8.5(1) or earlier complete the Installing the COP file, page 6.

Caution Any existing data on the USB device that is needed for the HP7825H3 or HP7828H3 upgrade is lost during migration.

Overview of the Software Upgrade Process

With this version of Cisco Intercompany Media Engine, you cannot install upgrade software on your server while the system continues to operate.

Caution If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Intercompany Media Engine. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation.

When you install 8.6 upgrade software, there will be a temporary server outage while the IME software is installed. Once you kick off the upgrade using the command the data will be exported, and the system will be automatically rebooted at which point the server outage will begin. The duration of this outage will depend on your configuration and amount of data. During the upgrade, progress can be monitored via the console until such time that command line interface has been restored. Once restored, you can use the command line interface to continue to monitor upgrade progress.

If an administrator user makes changes during the upgrade process (export of data), that data could be lost after upgrade.

When you initiate the upgrade, you can indicate to activate the partition with the new upgrade software or return to using the partition with the previous version of the software at upgrade completion. With the exception of HP 7825H3 and HP7828H3 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 since you upgraded the software will get lost.

Note You can only make changes 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.

You can upgrade from a DVD (local source), a local copy of the ISO image, or from a network location (remote source) that the Cisco Intercompany Media Engine server can access.

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*. If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Intercompany Media Engine. If you do not back up your system data before starting the software upgrade process your data will be lost if your upgrade fails for some reason. If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

Making Configuration Changes During an Upgrade

This section describes the restrictions that apply to the configuration and provisioning changes that you can make during an upgrade.

Administration Changes

The administrator must not make any configuration changes to Cisco Intercompany Media Engine during an upgrade.

Any configuration changes that you make during an upgrade could get lost after the upgrade completes, and some configuration changes can cause the upgrade to fail.

If you are upgrading your system, you must complete the upgrade tasks in this section before you perform any configuration tasks.

Caution If you fail to follow these recommendations, unexpected behavior may occur; for example, ports may not initialize as expected.

Upgrade Tasks

To successfully complete the upgrade, perform the upgrade tasks in the following order before you begin making configuration changes.

Note Cisco strongly recommends that you do not perform configuration tasks until the upgrade completes and you have switched the servers over to the upgraded partition.

Procedure

Step 1 Stop all configuration tasks; that is, do not perform configuration tasks in the CLI (with the exception of performing the upgrade).

Tip For detailed information about the upgrade process, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

Step 2 If upgrading from 8.5(1) or earlier complete the Installing the COP file, page 6.

Step 3 Upgrade the Cisco Intercompany Media Engine.

Step 4 When all other upgrade tasks are complete, you can perform any needed configuration tasks as required.

Supported Upgrades

For information about supported upgrades, the Cisco Intercompany Media Engine Compatibility Matrix at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

Obtaining the Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com.

You can access the upgrade file during the installation process from either a local DVD or from a remote FTP or SFTP server. Be aware that directory names and filenames that you enter to access the upgrade file are case-sensitive

Upgrade Paths

For information about supported Cisco Intercompany Media Engine upgrades, see the *Cisco Unified Communications Manager Software Compatibility Matrix* at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

Ordering the Upgrade Media

To upgrade to Cisco Intercompany Media Engine Release 8.6(1) from a release prior to 8.0(1), use the Product Upgrade Tool (PUT) to obtain a media kit and license or purchase the upgrade from Cisco Sales.

To use the PUT, you must enter your Cisco contract number (Smartnet, SASU or ESW) and request the DVD/DVD set. If you do not have a contract for Unified CM, you must purchase the upgrade from Cisco Sales.

For more information about supported Cisco Intercompany Media Engine upgrades, see the *Cisco Unified Communications Manager Software Compatibility Matrix* at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

See the "Software Upgrades" chapter of the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

Software Upgrade Procedures

This section provides procedures for upgrading from either a local or a remote source and contains the following topics:

Installing the COP file

For upgrades from an 8.5(x) or earlier release to an 8.6(x) release, this patch (COP file) must be applied prior to initiating the upgrade. Before you upgrade from compatible versions of Cisco Intercompany Media Engine, install the COP file named **ciscocm.refresh_upgrade_v1.1.cop.sgn** that you can find

underfrom www.Cisco.com, select **Support > Download Software** . Navigate to **Products >Voice and Unified Communications > IP Telephony > Call Control > Cisco Intercompany Media Engine > Unified Communications Manager / CallManager / Cisco Unity Connection Utilities-COP-Files**.

Upgrading from a Local Source

To upgrade the software from local DVD, follow this procedure:

Procedure

Step 1 If upgrading from 8.5(1) or earlier complete the Installing the COP file, page 6.

Step 2 If you are upgrading software on HP7825H3 or HP7828H3 hardware insert the 16GB USB device to facilitate data migration from the old system to the new installation.

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Intercompany Media Engine. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation.

Step 3 If you do not have a Cisco-provided upgrade disk, create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.

Step 4 Just copying the .iso file to the DVD will not work. Most commercial disk burning applications can create ISO image disks. Insert the new DVD into the disc drive on the local server that is to be upgraded.

Step 5 Log in to the Cisco Intercompany Media Engine server.

Step 6 Enter utils system upgrade initiate and select the appropriate option for the location of the upgrade media.

Step 7 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 8 Continue the upgrade process.

Step 9 Choose the upgrade version that you want to install.

Step 10 In the next window, monitor the progress of the download.

Step 11 If you want to run the upgraded software at the completion of the upgrade process and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and is running the upgraded software.

Step 12 If you want to install the upgrade and then manually switch to the upgraded partition at a later time, do the following steps:

a. Choose **Do not switch to new version after upgrade**.

   The Upgrade Status window displays the Upgrade log.

b. To restart the system and activate the upgrade, on the IME CLI enter ***utils system switch versions***. The system restarts and is running the upgraded software.

The system restarts running the upgraded software.

Upgrading from a Local ISO File Copy

To upgrade the software from local local ISO file copy, follow this procedure:

Procedure

Step 1 If upgrading from 8.5(1) or earlier complete the Installing the COP file, page 6.

Step 2 If you are upgrading software on HP7825H3 or HP7828H3 hardware insert the 16GB USB device to facilitate data migration from the old system to the new installation.

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Intercompany Media Engine. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation.

Step 3 Using SFTP place the ISO imageon the IME Server.
The user id is **adminsftp** and the password is the configured administration password. After you start the SFTP session, you must change to the **upgrade** directory and put the ISO image in that location.

Step 4 Log in to the Cisco Intercompany Media Engine server.

Step 5 Enter utils system upgrade initiate and select option 4 **Local Upload Directory**.

Step 6 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 7 Continue the upgrade process.

Step 8 Choose the upgrade version that you want to install.

Step 9 In the next window, monitor the progress of the download.

Step 10 If you want to run the upgraded software at the completion of the upgrade process and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and is running the upgraded software.

Step 11 If you want to install the upgrade and then manually switch to the upgraded partition at a later time, do the following steps:

a. Choose **Do not switch to new version after upgrade**.

   The Upgrade Status window displays the Upgrade log.

b. To restart the system and activate the upgrade, on the IME CLI enter ***utils system switch versions***. The system restarts and is running the upgraded software.

The system restarts running the upgraded software.

Upgrading from a Remote Source

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Intercompany Media Engine. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation.

Supported SFTP Servers

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Intercompany Media Engine. For information on which vendors have certified their products with your version of Cisco Intercompany Media Engine, refer to the following URL:

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

For information on using GlobalSCAPE with supported Cisco Intercompany Media Engine versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

Cisco does not support using the SFTP product free FTDP. This is because of the 1GB file size limit on this SFTP product.

For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

To upgrade the software from a network location or remote server, use the following procedure.

Procedure

Step 1 If upgrading from 8.5(1) or earlier complete the Installing the COP file, page 6.

Step 2 If you are upgrading software on HP7825H3 or HP7828H3 hardware insert the 16GB USB device to facilitate data migration from the old system to the new installation.

Step 3 Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.

Step 4 Log in to Cisco Intercompany Media Engine server.

Step 5 Enter ***utils system upgrade initiate***.

Step 6 From the **Source** list, choose **Remote Filesystem**.

Step 7 In the **Directory** field, enter the path to the directory that contains the patch file on the remote system.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter `/patches`

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

Step 8 In the **Server** field, enter the server name or IP address.

Step 9 In the **User Name** field, enter your user name on the remote server.

Step 10 In the **User Password** field, enter your password on the remote server.

Step 11 Select the transfer protocol from the **Transfer Protocol** field.

Step 12 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

Step 13 Choose the upgrade version that you want to install.

Step 14 In the next window, monitor the progress of the download.

Note If you lose your connection with the server, you may see the following message when you try to access the Software Upgrades menu again:

Warning: Another session is installing software, click Assume Control to take over the installation.

If Assume Control does not display, you can also monitor the upgrade with the Real Time Monitoring Tool.

Step 15 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and runs the upgraded software.

Step 16 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, complete the following steps:

a. Choose **Do not switch to new version after upgrade**.

The Upgrade Status window displays the Upgrade log.

b. To restart the system and activate the upgrade, on the IME CLI enter utils system switch versions. The system restarts and is running the upgraded software.

Reverting to a Previous Version

After upgrading, you can revert to the software version that was running before the upgrade, by using the Switch Version option to switch the system to the software version on the inactive partition.

This section contains the following topics:

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Intercompany Media Engine. To perform an upgrade on one of these machines you must use a 16GB USB device to facilitate data migration from the old system to the new installation.

Note After upgrading IME from 8.5.1.10000-13 to 8.6.1.10000-15 and switching back to 8.5.1, the inactive version displays inaccurately as Inactive Master Version: 0.0.0.0-0 but the active version is displayed correctly.

Service Updates

After you install or upgrade to this release of Cisco Intercompany Media Engine, check to see if Cisco has released critical patches or Service Updates. Service Updates, or SUs, contain fixes that were unavailable at the time of the original release, and often include security fixes, firmware updates, or software fixes that could improve operation.

To check for updates, from www.Cisco.com, select **Support > Download Software** . Navigate to the "Voice and Unified Communications" section and select **IP Telephony > Call Control > Cisco Unified Communications Manager (CallManager) >** *the appropriate version of Cisco Intercompany Media Engine for your deployment*.

For continued notification of updates for your Cisco products, subscribe to the Cisco Notification Service at:

http://www.cisco.com/cisco/support/notifications.html

Related Documentation

You can view documentation that supports this release of Cisco Intercompany Media Engine at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Limitations and Restrictions

A list of compatible software releases represents a major deliverable of Cisco Intercompany Media Engine System testing. The recommendations, which are not exclusive, represent an addition to interoperability recommendations for each individual voice application or voice infrastructure product.

Important Notes

The following section contains important information that applies to Cisco Intercompany Media Engine Release 8.6(1).

Cisco Intercompany Media Engine Limitations and Interactions

This section describes the limitations for the Cisco Intercompany Media Engine (Cisco IME) and the interactions with other features.

Limitations

- Cisco IME learned routes do not get generated when a user makes a Mobile Voice Access call from a remote destination to another enterprise.
- When endpoints with Cisco IME-enrolled DIDs are remotely located with VPN connectivity into the enterprise, latency and jitter characteristics for calls with these endpoints will be amplified and could result in the Cisco IME-enabled ASAs triggering more frequent fallbacks to the PSTN. If fallbacks occur too frequently for a specific endpoint, it might be necessary either to configure these devices with a device pool that has a fallback profile with no fallback enabled, to lower the fallback sensitivity levels, or to remove the enrolled DID from Cisco IME.
- When a Cisco IME call gets placed and a loss of Internet connectivity between enterprises occurs, the originating Cisco Unified Communications Manager initiates a call over the PSTN. The initial Invite from the originating Cisco Unified Communications Manager causes the called phone in the terminating enterprise to ring. When the PSTN call reaches the phone in the terminating cluster, a second call occurs on the called phone. If the first call still exists on the phone, the user called party sees two calls on the phone—the actual call and a ghost call.

Interactions (Number-to-Remote-Destination Mapping)

If the Remote Destination exists as a learned pattern in the Cisco IME network, calls that are targeted for Remote Destination get rerouted over Cisco IME.

CSCti60604 Several syntax and command changes needed in IME ASA setup guide

The following procedures have been corrected for Caveat CSCti60604:

Configuring NAT for Cisco Intercompany Media Engine Proxy

To configure auto NAT rules for the Cisco UCM server, complete the following steps:

Step 1 Run the following command to set up a network object for the real address of Cisco UCM that you want to translate: **hostname(config)# object network name**

Example: **hostname(config)# object network ucm_real_1**

Step 2 Run the following command to specify the real IP address of the Cisco UCM host for the network object: **hostname(config-network-object)# host ip_address**

Example: **hostname(config-network-object)# host 192.168.10.30**

Step 3 (Optional) Run the following command to provide a description of the network object: **hostname(config-network-object)# description string**

Example: **hostname(config-network-object)# description “Cisco UCM #1 Real IP Address”**

Step 4 Repeat steps 1 through 3 for any other Cisco UCM nodes that you want to translate. **hostname(config-network-object)# host ip_address**

Example: object ucm_real_2 will contain host 192.160.10.31

Step 5 Run the following command to set up a network object for the outside (translated) addresses of Cisco UCMs: **hostname(config)# object network name**

Example: **hostname(config) # object network ucm_map_1**

Step 6 Run the following command to specify the translated IP address of the Cisco UCM host for the network object: **hostname(config-network-object)# host ip_address**

Example: **hostname(config-network-object) # host 209.165.200.227**

Step 7 (Optional) Run the following command to provide a description of the network object:**hostname(config-network-object)# description string**

Example: **hostname(config-network-object)# description "Cisco UCM Translated IP Address"**

Step 8 Repeat steps 5 through 7 for any other Cisco UCM nodes that you want to translate.

Example: object ucm_map_2 will contain host 209.165.200.228

Step 9 Run the following command to specify the address translation on the network objects created in this example:

Example:

```
hostname(config)# object network ucm_real_1
hostname(config-network-object)# nat (inside,outside) static ucm_map_1
hostname(config-network-object)# exit
hostname(config)# object network ucm_real_2
hostname(config-network-object)# nat (inside,outside) static ucm_map_2
```

(Optional) Configuring TLS within the Local Enterprise

The trustpoint needs to be enrolled before an identity certificate can be exported. The following step was added after step 2 of the procedure(Optional) Configuring TLS within the Local Enterprise:

Enroll the trustpoint before exporting the identity certificate. **(config mode) crypto ca enroll <trustpoint>**

The trustpoint in this case is local-asa.

Enabling SIP Inspection for the Cisco Intercompany Media Engine Proxy

In Step 9 and 12 of the procedure Enabling SIP Inspection for the Cisco Intercompany Media Engine Proxy, the "inspect" syntax is incorrect. The correct syntax is:

inspect sip [sip_map] uc-ime <uc_ime_map> tls-proxy <proxy_name>

Validation Parameters

The Cisco IME server relies on validation parameters to establish the security (number of calls required to learn a route) for call validation. By default, the system uses "medium security" values, and these values are designed to provide a sufficient level of security for most Cisco IME deployments. These "medium security" values will require multiple calls to numbers enrolled at a remote Cisco IME server before any routes can be learned to Cisco Unified Communications Manager servers attached to that Cisco IME server. It may take 2 hours or more before a route is learned even if there is a sufficient call volume to numbers enrolled at a remote Cisco IME server. During system installation and configuration,

you may wish to see a validation happen quickly. This can be done by lowering the validation parameter settings. It is very important to note: if you set these parameters low for testing, be sure to set them back to their default settings as soon as installation/testing is complete. This will insure good security for normal system operation.

To set the values to minimum security levels, use the ime validator minsecurity CLI command. To reset the values to default security levels, use the ime validator defaultsecurity CLI command.

Set the VAP Interface Between the Cisco IME Servers and the Associated Cisco Unified CMs to Encrypted

Cisco recommends that you set the VAP interface between the Cisco IME servers and the associated Cisco Unified Communications Manager servers to encrypted.

Check to see if the authentication mode for all vapservers is already set to "Encrypted" by executing the **show ime vapserver all** command from the Cisco IME server CLI.

If they are not set to encrypted, refer to the *Cisco Intercompany Media Engine Installation and Configuration Guide* for instructions.

Note To set encryption, you will have to change the configuration setting on the Cisco Unified Communications Manager, set the vapserver authentication mode on the Cisco IME server, and install certificates.

When adding a new vapserver using the add ime vapserver CLI command, you get prompted for the parameters, including the encryption mode.

NTP Server Configuration

The Cisco IME server requires a properly functioning NTP server configuration.

To verify NTP operation, execute the **utils ntp status** CLI command and insure that the Cisco IME server is connected to the appropriate NTP server and that the UTC and local times are correct.

Customer Information

The Cisco IME server stores contact information for your location which allows Cisco IME administration to contact you if the server is not configured properly (if, for example, it rejects connections from other servers).

To display the customer information settings, execute the **show ime customerinfo** command.

To change or add to the customer information settings, exectue the **set ime customerinfo** command. You will be prompted for contact information.

CSCti38763 Certificates switched in Configure TLS within the Local Enterprise of IME Installation and Configuration guide

The following changes are made to the procedure Configure TLS within the Local Enterprise of the *Intercompany Media Engine Installation and Configuration Guide:*

Step 7 Commands:

hostname(config)# **tls-proxy** proxy_name

hostname(config-tlsp)# **server trust-point** trustpoint_name

hostname(config-tlsp)# **client trust-point** proxy_trustpoint

hostname(config-tlsp)# **client cipher-suite** aes128-sha1 aes256-sha1 3des-sha1 null-sha1

Example:

hostname(config)# tls-proxy local_to_remote-ent

hostname(config-tlsp)# server trust-point local-asa

hostname(config-tlsp)# client trust-point local-ent

hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1

Step 7 Purpose:

Updates the TLS proxy for outbound connections.

Where proxy_name is the name you entered in Step 1 of the task Creating the TLS Proxy.

Where trustpoint_name for the **server trust-point** command is the name you entered in Step 1 of this procedure.

Where proxy_trustpoint for the **client trust-point** command is the name you entered in Step 2 of the task Creating Trustpoints and Generating Certificates.

NoteIn this step, you are creating different trustpoints for the client and the server.

Step 9 Commands:

hostname(config)**# tls-proxy** proxy_name

hostname(config-tlsp)**# server trust-point** proxy_trustpoint

hostname(config-tlsp)**# client trust-point** trustpoint_name

hostname(config-tlsp)**# client cipher-suite** aes128-sha1 aes256-sha1 3des-sha1 null-sha1

Example:

hostname(config)# tls-proxy remote_to_local-ent

hostname(config-tlsp)# server trust-point local-ent

hostname(config-tlsp)# client trust-point local-asa

hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1

Step 9 Purpose:

Updates the TLS proxy for inbound connections.

Where proxy_name is the name you entered in Step 5 of the task Creating the TLS Proxy.

Where proxy_trustpoint for the **server trust-point** command is the name you entered in Step 2 of the task Creating Trustpoints and Generating Certificates.

Where trustpoint_name for the **client trust-point** command is the name you entered in Step 1 of this procedure.

Caveats

The following sections contain information on how to obtain the latest resolved caveat information and descriptions of open caveats of severity levels 1, 2, and 3.

Caveats describe unexpected behavior on a Cisco Intercompany Media Engine server. Severity 1 caveats represent the most serious caveats, severity 2 caveats represent less serious caveats, and severity 3 caveats represent moderate caveats.

Resolved Caveats

You can find the latest resolved caveat information for Cisco Intercompany Media Engine Release 8.6(1) by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

Tip You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to http://tools.cisco.com/Support/BugToolKit.

UsingBug Toolkit

The system grades known problems (bugs) according to severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Toolkit, follow these steps:

Procedure

Step 1 Access the Bug Toolkit, http://tools.cisco.com/Support/BugToolKit.

Step 2 Log in with your Cisco.com user ID and password.

Step 3 If you are looking for information about a specific problem, enter the bug ID number in the “Search for Bug ID” field, and click **Go**.

Tip Click **Help** on the Bug Toolkit page for information about how to search for bugs, create saved searches, create bug groups, and so on.

Open Caveats

Open Caveats for Cisco Intercompany Media Engine Release 8.6(1) As of June 9, 2011 describe possible unexpected behaviors in Cisco Intercompany Media Engine Release 8.6(1), which are sorted by component.

Tip For more information about an individual defect, click the associated Identifier in the "Open Caveats for Cisco Intercompany Media Engine Release 8.6(1) As of June 9, 2011" section on page 18 to access the online record for that defect, including workarounds.

Understanding the Fixed-in Version Field in the Online Defect Record

When you open the online record for a defect, you will see data in the "First Fixed-in Version" field. The information that displays in this field identifies the list of Cisco Intercompany Media Engine interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Intercompany Media Engine releases.

Some more clearly defined versions include identification for Engineering Specials (ES) or Service Releases (SR); for example 03.3(04)ES29 and 04.0(02a)SR1. However, the version information that displays for the Cisco Intercompany Media Engine maintenance releases may not be as clearly identified.

The following example shows how you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Cisco Intercompany Media Engine release that includes that interim version. You can use this examples as guidance to better understand the presentation of information in these fields.

- 8.0(2.20000-x) = Cisco Intercompany Media Engine Release 8.0(2)

Because defect status continually changes, be aware that the "Open Caveats for Cisco Intercompany Media Engine Release 8.6(1) As of June 9, 2011" section on page 18 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the "UsingBug Toolkit" section on page 17.

Tip Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides. To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats for Cisco Intercompany Media Engine Release 8.6(1) As of June 9, 2011

The following information comprises unexpected behavior (as of June 9, 2011) that you may encounter in Release 8.6(1) of Cisco Intercompany Media Engine.

Table 1 Open Caveats for Cisco Intercompany Media Engine Release 8.6(1)

Identifier	Headline
CSCtj68794	Netdump client fails with address resolution error
CSCtk34504	IME license fails to install, exception generated
CSCtq74591	IME Refresh upgrade on 7825H3 failed

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop by using a reader application. Be aware that the RSS feeds are a free service, and Cisco currently supports RSS version 2.0.