Release Notes for Cisco Intercompany Media Engine Release 8.5(1)

March 22, 2011

This document contains information pertinent to Cisco Intercompany Media Engine (IME) Release 8.5(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.

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, page 2
- Uninterruptible Power Supply, page 2

Server Support

Make sure that you install and configure Cisco Intercompany Media Engine on a Cisco Media Convergence Server (MCS), a Cisco Unified Computing System (UCS) server, or a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

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 Engine server 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 8.5(1)

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

- Before You Begin, page 3
- Special Upgrade Information, page 3
- The Latest Software Upgrades for Cisco Intercompany Media Engine on Cisco.com, page 5
- Upgrading From an Engineering Special, page 5

Before You Begin

1. Before you upgrade the software version of Cisco Intercompany Media Engine verify your current software version.

   To do that, from the CLI, execute the **show version active** command.
2. Read the "Special Upgrade Information" section on page 3.

Special Upgrade Information

The following sections include information that you must know before you begin the upgrade process.

- Write-Cache, page 3
- Making Configuration Changes During an Upgrade, page 3

Write-Cache

A disabled write-cache on the server causes the upgrade process to run more slowly. Multiple factors, including dead batteries on older servers, can cause the write-cache to get disabled.

If you determine that your write-cache is disabled because of a dead battery, you need to replace the hard disk controller cache battery. Follow your local support procedures to get this battery replaced.

To determine the status of the write-cache, from the CLI, execute the **show hardware** command.

Making Configuration Changes During an Upgrade

The administrator must not make any configuration changes to Cisco Intercompany Media Engine during an upgrade. Configuration changes include any changes that you make by using the command line interface (CLI).

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

Note When the IME server gets upgraded, the services that communicate with IME service on the Cisco Unified Communications Manager stops. This causes the Cisco Unified Communications Manager to temporarily stop learning routes until the upgrade completes, and the IME server gets switched to the new release. During this time, an alert displays on Cisco Unified Communications Manager, indicating that the IME service is down.

To minimize impact on the Cisco Unified Communications Manager, Cisco recommends that you upgrade the IME server during a quiescent period. The upgrade procedure takes 20-30 minutes, so the time that the IME service is unavailable is minimal.

Check System Health

Before beginning the upgrade, check system health by using the CLI command **show ime dht peerIDStatus**

The health of each peer should be GREEN (meaning no network problems) before you upgrade.

Example

```
admin:show ime dht peerIDStatus

Peer ID = 159ee0371f25ca4059f4dec844d33245
    Peer State.......................... = JOINED
    DHT Health.......................... = GREEN
    DHT Stored Records.................. = 3
    DHT Stored Data (Bytes)............. = 18015
    Route Table Size.................... = 8
    Num Client Conn..................... = 7
    Num Server Conn..................... = 1
```

Upgrade

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

Procedure

Step 1 Stop all configuration tasks; that is, do not perform configuration tasks.

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

Step 2 Perform the upgrade.

Step 3 When the upgrade completes, you can perform configuration tasks as required.

Ordering the Upgrade Media

To upgrade to Cisco IME Release 8.5(1), use the Product Upgrade Tool (PUT) to obtain a media kit and license or to 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 Cisco Unified Communications Manager, you must purchase the upgrade from Cisco Sales.

For more information about supported Cisco IME 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

For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide.*

Upgrading From an Engineering Special

If you want to upgrade to this release of Cisco IME and you are currently running an Engineering Special (ES), contact TAC to obtain the fixes that are included in the ES that you currently use.

The Latest Software Upgrades for Cisco Intercompany Media Engine on Cisco.com

You can access the latest software upgrades for this release of Cisco Intercompany Media Engine from http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

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 Unified Communications Manager System testing. The recommendations, which are not exclusive, represent an addition to interoperability recommendations for each individual voice application or voice infrastructure product.

For a list of software and firmware versions of IP telephony components and contact center components that were tested for interoperability with Cisco Unified Communications Manager 8.5(1) as part of Cisco Unified Communications System Release 8.1 testing, see

http://www.cisco.com/go/unified-techinfo

Note Be aware that the release of Cisco IP telephony products does not always coincide with Cisco Unified Communications Manager releases. If a product does not meet the compatibility testing requirements with Cisco Unified CM, you need to wait until a compatible version of the product becomes available before you can upgrade to Cisco Unified CM Release 8.5(1). For the most current compatibility combinations and defects that are associated with other Cisco Unified CM products, refer to the documentation that is associated with those products.

Important Notes

The following section contains important information that applies to Cisco Intercompany Media Engine Release 8.5(1).

- Cisco Intercompany Media Engine Limitations and Interactions, page 6
- CSCtf84703 utils system upgrade initiate listall - CLI Command Issue, page 7
- CSCtl01801 IME serviceability - missing documentation for call types, page 7
- CSCti60604 Several syntax and command changes needed in IME ASA setup guide, page 8
- Validation Parameters, page 9
- Set the VAP Interface Between the Cisco IME Servers and the Associated Cisco Unified CMs to Encrypted, page 10
- NTP Server Configuration, page 10
- Customer Information, page 10
- CSCti38763 Certificates switched in Configure TLS within the Local Enterprise of IME Installation and Configuration guide, page 10

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.

CSCtf84703 utils system upgrade initiate listall - CLI Command Issue

Symptom

Executed the **utils system upgrade initiate listall** CLI command, but no filtered items display.

Conditions

Upgrading Cisco IME by using the CLI.

Workaround

Examine the upgrade log for filter log messages which indicate filtered items and the reason for them being filtered out of the valid upgrade item list.

CSCtl01801 IME serviceability - missing documentation for call types

Symptom

On-line help for the call types drop-down list on "CDR Search for Different Call Types" page is missing. This is at **CUCM serviceability > tools > CDR analysis and reporting > CDR > search > call types**.

Conditions

None.

Workaround

Call Types:

Successful IME Calls: calls that are succesfully route through IME trunk.

Failed IME Calls: calls that attempt to route through the IME trunk, but fail.

IME Calls with Fallback to Alternate Route: calls that initially route through the IME trunk, but due to some reason, the fallback mechanism initiates and these calls are re-routed mid-call to an alternate route. The 'alternate route' is typically a PSTN route.

Successful Fallback Calls to Alternate Route: calls which successfully fall back to the alternate route. The 'alternate route' is typically a PSTN route.

Failed Fallback Calls to Alternate Route: calls that fail and fall back to the alternate route.

Calls on Alternate Route due to IME Redirection: calls that attempt to route (at call setup) to IME, but for some reason route to Alternate route. The 'alternate route' is typically a PSTN route.

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 8.5(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 8.5(1) As of December 7, 2010 describe possible unexpected behaviors in Cisco Intercompany Media Engine Release 8.5(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 8.5(1) As of December 7, 2010" section on page 13 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 8.5(1) As of December 7, 2010" section on page 13 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 12.

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 8.5(1) As of December 7, 2010

The following information comprises unexpected behavior (as of December 7, 2010) that you may encounter in Release 8.5(1) of Cisco Intercompany Media Engine.

Table 1 Open Caveats for Cisco Intercompany Media Engine Release 8.5(1)

Identifier	Headline
CSCtj68794	Netdump client fails with address resolution error
CSCtk34504	IME license fails to install, exception generated

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.