Release Notes for Cisco Unified Communications Manager Release 7.1(4)

January 21, 2013

Note Cisco Unified Communications Manager Release 7.1(4) is a fresh install only.

In the past, export licenses, government regulations, and import restrictions have limited Cisco System's ability to supply Cisco Unified Communications Managers worldwide. Cisco has obtained an unrestricted US export classification for Cisco Unified Communications Manager 7.1(4).

Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You will also not be allowed to fresh install a restricted version on a system that contains an unrestricted version.

This document contains information pertinent to Cisco Unified Communications Manager Release 7.1(4) and is built on the Release Notes for Cisco Unified Communications Manager Release 7.1(3).

To view the release notes for previous versions of Cisco Unified Communications Manager, choose the Cisco Unified Communications Manager version from the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html.

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

Before you install or upgrade Cisco Unified Communications Manager, Cisco recommends that you review the Service Updates, page 4 for information pertinent to installing or upgrading, and the Important Notes, page 4 for information about issues that may affect your system.

Introduction

Cisco Unified Communications Manager, the call-processing component of the Cisco Unified Communications System, extends enterprise telephony features and capabilities to IP phones, media processing devices, voice-over-IP (VoIP) gateways, mobile devices, and multimedia applications.

System Requirements

The following sections comprise the system requirements for this release of Cisco Unified CM.

Server Support

Make sure that you install and configure Cisco Unified CM on a Cisco Media Convergence Server (MCS) or a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

To find which MCS are compatible with this release of Cisco Unified CM, refer to the Supported Servers for Cisco Unified Communications Manager Releases: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/prod_brochure0900aecd8062a4f9.html.

Note Make sure that the matrix shows that your server model supports Cisco Unified CM Release 7.1(4).

Note Be aware that some servers that are listed in the *Cisco Unified Communications Manager Software Compatibility Matrix* may require additional hardware support for Cisco Unified CM Release 7.1(4). Make sure that your server meets the minimum hardware requirements, as indicated in the footnotes of the *Cisco Unified Communications Manager Software Compatibility Matrix*. Cisco Unified CM requires a minimum of 2 GB of memory, 72 GB disk drive, and 2 GHz processor.

Uninterruptible Power Supply

Cisco recommends that you connect each Cisco Unified Communications Manager server to an uninterruptible power supply (UPS) to provide backup power and protect your system against a power failure.

Note You must connect MCS-7816 and MCS-7825 servers to a UPS to prevent file system corruption during power outages.

When Cisco Unified Communications Manager runs on one of the servers that are listed in Table 1, basic integration to the UPS model APC SmartUPS 1500VA USB and APC 750VA XL USB gets supported.

Integration occurs via a single point-to-point Universal Serial Bus (USB) connection. Serial and SNMP connectivity to UPS does not get supported, and the USB connection must be point-to-point (in other words, no USB hubs). Single- and dual-USB UPS models get supported with the APC SmartUPS 1500VA USB and APC 750VA XL USB. The feature activates automatically during bootup if a connected UPS gets detected.

Alternatively, you can execute the CLI command **show ups status** that shows the current status of the USB-connected APC smart-UPS device and starts the monitoring service if it is not already started. The CLI command also displays detected hardware, detected versions, current power draw, remaining battery runtime, and other relevant status information.

When the feature is activated, graceful shutdown will commence as soon as the low battery threshold is reached. Resumption or fluctuation of power will not interrupt or abort the shutdown, and administrators cannot stop the shutdown after the feature is activated.

For unsupported Cisco Unified Communications Manager releases, MCS models and/or UPS vendor/make/models, you can cause an external script to monitor the UPS. When low battery gets detected, you can log on to Cisco Unified Communications Manager by using Secure Shell (SSH), access the CLI, and execute the **utils system shutdown** command.

Table 1 Supported Servers for Basic Integration

HP Servers	IBM Servers
MCS-7816-H3	MCS-7815-I1
MCS-7825-H1	MCS-7815-I2
MCS-7825-H2	MCS-7816-I3
MCS-7825-H3	MCS-7816-I3
MCS-7825-H4	MCS-7825-I1
MCS-7828-H3	MCS-7825-I2
MCS-7828-H4	MCS-7825-I3
MCS-7835-H2	MCS-7825I-30
MCS-7845-H2	MCS-7825-I4
MCS-7835-H3	MCS-7828-I3
MCS-7845-H3	MCS-7828-I4
	MCS-7828-I4
	MCS-7835-I1
	MCS-7835I-30
	MCS-7845-I2
	MCS-7835-I3
	MCS-7845-I3

The Latest Software Upgrades for Unified CM 7.1 on Cisco.com

You can access the latest software upgrades for Unified CM 7.1 from http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Note After you perform a switch version when you upgrade Unified CM, IP phones request a new configuration file. This request results in an automatic upgrade to the device firmware.

Service Updates

After you install or upgrade to this release of Cisco Unified Communications Manager, 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 Communications Manager 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

The view documentation that supports Cisco Unified CM Release 7.1(4), go to 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 7.1(4) as part of Cisco Unified Communications System Release 7.1 testing, see

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

Important Notes

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Communications Manager Release 7.1(4).

New License Required when Replacing Motherboard (CSCtz12589 and CSCtz12651)

A new license file is required if you are installing a replacement motherboard in publisher servers or single servers that are not part of a cluster.

Unrestricted Release Limitations

After you install an unrestricted release, you can never upgrade to a restricted version. You will not even be allowed to fresh install a restricted version on a system that contains an unrestricted version.

CSCtd87058 BAT Impact

If your Cisco Unified CM is unrestricted, Cisco recommends that you do not edit the following fields by using BAT - Import/Export:

- Configuring a Phone Security Profile - Device Security Mode field. Default specifies Non Secure
- Cisco IOS Conference Bridge Configuration Settings - Device Security Mode field. Default specifries Not Selected.
- Configuring Voice Mail Port Wizard - Device Security Mode field. Default value specifies Not Selected.
- Configuring Voice Mail Port - Device Security Mode field. Default specifies Not Selected
- Configuring SIP Trunk Security Profile - Device Security Mode field. Default specifies Non Secure.
- Configuring a Minimum Security Level for Meet-Me Conferences - Minimum Security Level field. The default specifies Non Secure

Signaling and Media Encryption is Disabled

Be aware that Cisco Unified CM UI allows you to provision signaling or media encryption for lines or trunks (for example, endpoints, gateways, trunks, SIP, MGCP, H.323, H.225), however, none of those settings is actually enabled internally in Unified CM. (This is one of the unrestricted requirements).

Device Packs for Cisco Unified CM 7.1(3) Can Be Installed on Unified CM 7.1(4)

Be aware that device packs for Cisco Unified CM can be installed on Cisco Unified CM 7.1(4).

CSCtc52250 Deleting a User

If you attempt to delete a user that is associated with ten thousand or more devices, a DDR block on the database occurs. This occurs because when the user gets deleted, all the associations get deleted immediately, which overwhelms the system with device update data.

To avoid the DDR block, remove the associations before you delete the user.

Note This information applies to users configured in Cisco Unified CM as well as users from corporate LDAP directory sync.

CSCsv52801 Unified CM Does Not Support DTMF RFC2833 Negotiation to an H323 Gateway

RFC2833 negotiation to an H323 gateway does not get supported on Unified CM even if the other endpoint supports RFC2833. However, out-of-band DTMF is supported.

MGCP and SIP gateways do support RFC2833 negotiation, as well as out-of-band DTMF.

Disaster Recovery System Caution

When you restore your data, the hostname, server IP address, and the deployment type must be the same as it was during the backup. DRS does not restore across different hostnames, IP addresses and deployment types.

CSCtb95488 Phones That Support Monitoring and Recording Features

The "Monitoring and Recording" chapter of the *Cisco Unified Communications Manager Features and Services Guide, Release 7.1(2),* includes a partial list of devices that support monitoring and recording in the "Agent Devices" subsection of the "Devices That Support Call Monitoring and Call Recording" section.

The list of devices that support the monitoring and recording features varies per version and device pack.

Use the Cisco Unified Reporting application to generate a complete list of devices that support monitoring and recording for a particular release and device pack. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.

   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go**.
   - by choosing **File > Cisco Unified Reporting** at the Cisco Unified Cisco Unified Real-Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click **System Reports** in the navigation bar.
3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.
4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.
5. To generate a report of all devices that support monitoring, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   Product: All

   Feature: Monitor

   The List Features pane displays a list of all devices that support the monitoring feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.
6. To generate a report of all devices that support recording, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   Product: All

   Feature: Record

   The List Features pane displays a list of all devices that support the recording feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.

For additional information about the Cisco Unified Reporting application, refer to the *Cisco Unified Reporting Administration Guide*, which you can find at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

LogCollectionPort Service: selectLogFiles Operation

Description

The selectLogFiles operation retrieves log files based on a selection criteria. This API takes FileSelectionCriteria object as an input parameter and returns the file name and location for that object.

The LogCollectionService URL is

http://hostname/logcollectionservice/services/LogCollectionPort

Parameters

The selectLogFiles operation includes the following elements:

- ServiceLogs—Array of strings. The available service options depends on the services that are activated on the Cisco Unified CM. The actual available options are as those returned by the listNodeServiceLogs operation at run time. For example:
  - Cisco Syslog Agent
  - Cisco Unified CM SNMP Service
  - Cisco CDP Agent
- SystemLogs—Array of strings.

Note SystemLogs element is not available in Cisco Unified CM release 7.1.3, and therefore should be empty.

- JobType—The collection type. The available options are:
  - DownloadtoClient
  - PushtoSFTPServer

  If you select PushtoSFTPServer, then the following elements are also required:
  - IPAddress
  - UserName
  - Password
  - Port
  - Remote Download Folder
- SearchStr—A non-null string.
- Frequency—The frequency of log collection. The available options are:
  - OnDemand
  - Daily
  - Weekly
  - Monthly

Note Only OnDemand option is currently supported for Frequency element. The other options (Daily, Weekly, and Monthly) are applicable for schedule collection that is currently not supported.

- ToDate—The end date for file collection. Format is **mm/yy/dd hh:mm AM/PM.** The ToDate element is required if you use absolute time range.
  File collection time range can be absoulte or relative. If you prefer relative time range, then the following elements are required:
  - RelText
  - RelTime

  If you prefer absolute time range, then the following elements are required:
  - ToDate

  - FromDate

- FromDate—The start date for file collection. Format is **mm/yy/dd hh:mm AM/PM.** The FromDate element is required if you use absolute time range.
- RelText—The file collection time range. The available options are:
  - Week
  - Day
  - Month
  - Hours
  - Minutes
- RelTime—The file collection time value. Gives all files from the specified time up to present. The available range is 1 to 100.
  For example, if the RelText is “Day” and RelTime is 1, then we get all files modified in the previous one day.
- TimeZone—The time zone value. The format is **Client: (GMT ±*n*)** ***Name of the time zone*** where, n is the offset time of the specified time zone and GMT. For example:
  - Client: (GMT-0:0) Greenwich Mean Time
  - Client: (GMT-8:0) Pacific Standard Time
- Port—The port number of the node.
- IPAddress—The IP address of the node.
- UserName—The service administrator username for the node.
- Password—The service administrator password for the node.
- ZipInfo—Indicates whether to compress the files during collection. This element is applicable only for PushtoSFTPServer option. The avilable options are:
  - True—The files are compressed.
  - False—The files are not compressed.
- RemoteFolder—The remote folder where the files are to be uploaded. This option is used only if you choose to upload trace files to SFTP or FTP server.

Request Example

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1:SelectLogFiles soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://schemas.cisco.com/ast/soap/">
   <FileSelectionCriteria href="#id0"/>
  </ns1:SelectLogFiles>
  <multiRef id="id0" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xsi:type="ns2:SchemaFileSelectionCriteria"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns2="http://cisco.com/ccm/serviceability/soap/LogCollection/">
   <ServiceLogs xsi:type="soapenc:Array" soapenc:arrayType="xsd:string[45]">
    <item>Cisco Syslog Agent</item>
    <item>Event Viewer-Application Log</item>
```

```
    <item>Install Logs</item>
    <item>Event Viewer-System Log</item>
    <item>Security Logs</item>
   </ServiceLogs>

    <SystemLogs xsi:type="xsd:string" xsi:nil="true"/>

   <JobType href="#id2"/>
   <SearchStr xsi:type="xsd:string"/>
   <Frequency href="#id1"/>
   <ToDate xsi:type="xsd:string" xsi:nil="true"/>
   <FromDate xsi:type="xsd:string" xsi:nil="true"/>
   <TimeZone xsi:type="xsd:string">Client:(GMT-8:0)Pacific Standard Time</TimeZone>
   <RelText href="#id3"/>
   <RelTime xsi:type="xsd:byte">5</RelTime>
   <Port xsi:type="xsd:byte">0</Port>
   <IPAddress xsi:type="xsd:string">MCS-SD4</IPAddress>
   <UserName xsi:type="xsd:string" xsi:nil="true"/>
   <Password xsi:type="xsd:string" xsi:nil="true"/>
   <ZipInfo xsi:type="xsd:boolean">false</ZipInfo>
  </multiRef>
    <multiRef id="id1" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xsi:type="ns4:Frequency"
xmlns:ns4="http://cisco.com/ccm/serviceability/soap/LogCollection/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">OnDemand</multiRef>
    <multiRef id="id2" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xsi:type="ns3:JobType"
xmlns:ns3="http://cisco.com/ccm/serviceability/soap/LogCollection/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">DownloadtoClient</multiRef>
    <multiRef id="id3" soapenc:root="0"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xsi:type="ns4:RelText"
xmlns:ns4="http://cisco.com/ccm/serviceability/soap/LogCollection/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">Hours</multiRef>
 </soapenv:Body>
</soapenv:Envelope>
```

Response Example

The response returns a FileSelectionResult object, which contains the list of matching file names and their location in the server.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>
<ns1:SelectLogFilesResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://schemas.cisco.com/ast/soap/">
<FileSelectionResult xsi:type="ns2:SchemaFileSelectionResult"
xmlns:ns2="http://cisco.com/ccm/serviceability/soap/LogCollection/">
<Node xsi:type="ns2:Node">
<name xsi:type="xsd:string">MCS-SD4</name>
<ServiceList soapenc:arrayType="ns2:ServiceLogs[1]" xsi:type="soapenc:Array"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
<item xsi:type="ns2:ServiceLogs">
<name xsi:type="xsd:string" xsi:nil="true"/>
<SetOfFiles soapenc:arrayType="ns2:file[5]" xsi:type="soapenc:Array">
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000305.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000305.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2097082</filesize>
```

```
<modifiedDate xsi:type="xsd:string">Thu Jan 29 04:14:05 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000306.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000306.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2097083</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 05:41:26 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000307.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000307.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2096868</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 07:08:56 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000308.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000308.txt</absolu
tepath>
<filesize xsi:type="xsd:string">2096838</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 08:36:17 PST 2009</modifiedDate>
</item>
<item xsi:type="ns2:file">
<name xsi:type="xsd:string">syslogmib00000309.txt</name>
<absolutepath
xsi:type="xsd:string">/var/log/active/cm/trace/syslogmib/sdi/syslogmib00000309.txt</absolu
tepath>
<filesize xsi:type="xsd:string">100657</filesize>
<modifiedDate xsi:type="xsd:string">Thu Jan 29 08:40:20 PST 2009</modifiedDate>
</item>
</SetOfFiles>
</item>
</ServiceList>
</Node>
</FileSelectionResult>
<ScheduleList soapenc:arrayType="ns3:Schedule[0]" xsi:type="soapenc:Array"
xmlns:ns3="http://cisco.com/ccm/serviceability/soap/LogCollection/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"/>
</ns1:SelectLogFilesResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Fault

If the specified frequency is null, it will throw a remote exception, “LogCollection frequency is null.” If the array of ServiceLogs and System Logs is null, it throws a remote exception, “No Service/Syslog are provided for the collection.” If a matching file is not found, it throws a remote exception, “The File Vector from the server is null.”

Perform DRS Backup After You Regenerate Certificates

After you regenerate certificates in Cisco Unified Communications Operating System, you must perform a backup so that the latest backup contains the regenerated certificate(s). If your backup does not contain the regenerated certificates and you must perform restoration tasks for any reason, you must manually unlock each phone in your system so that the phone can register with Cisco Unified Communications Manager. For information on performing a backup, refer to the *Disaster Recovery System Administration Guide*.

Important Information About Create File Format Capability in BAT

The Create File Format window provides the option to set the maximum number of Lines, Speed Dials, and so on. The file format that gets created by using BAT stores the selected Device, Line, Intercom, Speed Dial, BLF Speed Dial, BLF Directed Call Park, and IP Phone Service fields in the database. Because the database column length only allows up to 32K characters, the BAT Administrator cannot choose all the fields with maximum allowed number because this will exceed 32K. When the file format length exceeds 32K, BAT displays the following error message:

“Cannot Insert a file format with characters more than 32K"

The BAT Administrator must use BAT Phone Templates to define the common attributes.

Limitation Between QSIG PRI and SIP Trunk for MWI

In previous releases of Cisco Unified CM, to route an MWI request from QSIG PRI to a SIP trunk, the route pattern that was specified had to point directly to the SIP trunk.

If the route pattern pointed to a Route List/Route Group that included the SIP trunk, MWI failed. After the first failure, all subsequent MWI indications to any number in the cluster failed.

In Cisco Unified CM 7.x, the MWI routing gets handled differently.

If MessageWaiting gets a SsDataInd signal while in the mwi_nailed_up_ssinfores state, MessageWaiting will not process any subsequent MWIs.

SDL traces should look like the example below, which indicates that a previous MWI request caused the system to hit the limitation.

```
2009/07/15 23:36:15.902| 002| SdlSig    | SsDataInd                              |
mwi_nailed_up_ssinfores       | MessageWaiting(2,100,126,4352)  |
MessageWaitingManager(2,100,125,1)| (2,100,124,1).15384643-(*:10.40.30.12)  | [R:NP -
HP: 0, NP: 0, LP: 0, VLP: 0, LZP: 0 DBP: 0]SsType=33554444 SsKey=0 SsNode=2
SsParty=39330436 DevId=(0,0,0) BCC=9 OtherParty=39330437 NodeOtherParty=2 clearType =
0 CSS=169e2389-5c0b-4500-88e7-2cb6244fd8b1 CNumInfo = 0 CNameInfo = 0 ssDevType=6
ssOtherDevType=5FDataType=1opId=81invokeId=-29584resultExp=0 fac.fid=28 fac.l=32
fac.fid=28 fac.l=1 fac.fid=28 fac.l=1 ssCause = 0 ssUserState = 2 ssOtherUserState = 1
```

Cisco Unified Communications Manager Assistant Wizard Constraint

Be aware that you can run the IPMA Wizard only once. Attempts to run it more than once will fail.

Creating a Custom Help Desk Role and Custom Help Desk User Group

Some companies want their help desk personnel to have privileges to be able to perform certain tasks, such as adding a phone, adding an end user, or adding an end user to a user group in Cisco Unified Communications Manager Administration.

Performing the steps in the following example allows help desk personnel to add a phone, add an end user, and add the end user to the Standard CCM End Users user group, which allows an end user to access and update the Cisco Unified CM User Options.

Example—Allows Help Desk Personnel to Add Phone, Add End User, and Add End User to User Group

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management > Role**.

Step 2 Click **Add New**.

Step 3 From the Application drop-down list box, choose **Cisco Unified CM Administration**; then, click **Next**.

Step 4 In the Name field, enter the name of the role; for example, Help Desk.

Step 5 In the Description field, enter a short description; for example, for adding phones and users.

Step 6 Choose one of the following options, which depends on where you want the help desk personnel to perform the task:

a. If you want the help desk personnel to add a phone in the Phone Configuration window and then add an end user in the End User Configuration window. check the **read** and **update** privileges check boxes for the User web page resource and the Phone web pages resource; then, click **Save**.

b. If you want the help desk personnel to add both a phone and a user at the same time in the User and Phone Add window, check the **read** and **update** privileges check boxes for the User and Phone add resource and the User web page resource; then, click **Save**.

Step 7 By performing the following tasks, you create a custom user group for the help desk:

a. In Cisco Unified Communications Manager Administration, choose **User Management > User Group**; then, click **Add New**.

b. Enter the name of the custom user group; for example, Help Desk.

c. From the Related Links drop-down list box, choose **Assign Roles to User Group**; then, click **Go**.

d. Click the **Assign Role to Group** button.

e. Check the check box for the custom role that you created in Step 1 through Step 6; in this example, Help Desk. In addition, check the check box for the Standard CCM Admin Users role; then, click **Add Selected**.

f. In the User Group Configuration window, verify that the roles display in the Role Assignment pane; then, click **Save**.

Next Steps

In Cisco Unified Communications Manager Administration, the help desk personnel can add the phone, add the user, and add the end user to the user group.

- To add a phone in the Phone Configuration window, choose **Device > Phone**; then, to add an end user in the End User window, choose **User Management > End User**.
- To add both a phone and user at the same time in the User and Phone Add window, choose **User Management > User and Phone Add**.
- To associate the end user with the Standard CCM End Users user group, choose **User Management > User Group**.

Tip For more information on how to perform these tasks in Cisco Unified Communications Manager Administration, refer to the *Cisco Unified Communications Manager Administration Guide*.

Do Not Unplug a USB Device While It Is In Use

Do not unplug a USB device that is in use from the Cisco Unified Communications Manager server. If you do, the USB device will become inaccessible, and messages will display on the server console.

Removing Hard Drives

Cisco only supports replacing failed hard drives. Cisco does not support drive pulling/swapping as a method of fast upgrade reversion, restore, or server recovery. For information on replacing a failed hard drive, refer to the *Troubleshooting Guide for Cisco Unified Communications Manager*.

CSCsx96370 Multiple Tenant MWI Modes Service Parameter

The Multiple Tenant MWI Modes service parameter, which supports the Cisco CallManager service, specifies whether to apply translation patterns to voice-message mailbox numbers. Valid values specify True, which means that Cisco Unified Communications Manager uses translation patterns to convert voice-message mailbox numbers into directory numbers when your voice-messaging system issues a command to set a message waiting indicator, or False, which means that Cisco Unified Communications Manager does not translate the voice-message mailbox numbers that it receives from your voice-messaging system.

Be aware that this service parameter supports Cisco Unified Communications Manager integrations with Cisco Unity Connection or Cisco Unity. If your voice-mail extensions require translation in Cisco Unified Communications Manager, set the Multiple Tenant MWI Modes service parameter to **True** after you install Cisco Unified Communications Manager 7.1(4).

Considerations for LDAP Port Configuration

When you configure the LDAP Port field in Cisco Unified Communications Manager Administration, you specify the port number that the corporate directory uses to receive LDAP requests. How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers:

Your configuration may require that you enter a different port number than the numbers that are listed in the following bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

LDAP Port for When the LDAP Server Is Not a Global Catalog Server

- 389—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.)
- 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

LDAP Port for When the LDAP Server Is a Global Catalog Server

- 3268—When SSL is not required.
- 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

Configuring the Hostname/IP Address for the Cisco Unified Communications Manager Server

Table 2 lists the locations where you can configure a host name for the Cisco Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Cisco Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

Caution Before you change the host name or IP address for any locations that are listed in Table 2, refer to *Changing the IP Address and Host Name for Cisco Unified Communications Manager 7.1(2)*. Failing to update the host name or IP address correctly after it is configured may cause problems for Cisco Unified Communications Manager.

Table 2 Host Name Configuration in Cisco Unified Communications Manager

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Host Name/ IP Address field **System > Server** in Cisco Unified Communications Manager Administration	You can add or change the host name for any server in the cluster.	2-63	alphabetic	alphanumeric
Hostname field Cisco Unified Communications Manager installation	You can add the host name for any server in the cluster.	1-63	alphabetic	alphanumeric
Hostname field **Settings > IP > Ethernet** in Cisco Unified Communications Operating System	You can change, not add, the host name for any server in the cluster.	1-63	alphabetic	alphanumeric
set network hostname *hostname* Command Line Interface	You can change, not add, the host name for any server in the cluster.	1-63	alphabetic	alphanumeric

Tip The host name must follow the rules for ARPANET host names. Between the first and last character of the host name, you can enter alphanumeric characters and hyphens.

Before you configure the host name in any location in Table 2, review the following information:

- The Host Name/IP Address field in the Server Configuration window, which supports device-to-server, application-to-server, and server-to-server communication, allows you to enter an IPv4 address in dotted decimal format or a host name.

  After you install Cisco Unified Communications Manager on the publisher database server, the host name for the publisher automatically displays in this field. Before you install Cisco Unified Communications Manager on the subscriber server, enter either the IP address or the host name for the subscriber server in this field on the publisher database server.

  In this field, only configure a host name if Cisco Unified Communications Manager can access the DNS server to resolve host names to IP addresses; make sure that you configure the Cisco Unified Communications Manager name and address information on the DNS server.

Tip In addition to configuring Cisco Unified Communications Manager information on the DNS server, you enter DNS information during the Cisco Unified Communications Manager installation.

- During the Cisco Unified Communications Manager installation of the publisher database server, you enter the host name, which is mandatory, and IP address of the publisher server to configure network information; that is, if you want to use static networking.

  During the Cisco Unified Communications Manager installation on the subscriber server, you enter the hostname and IP address of the publisher database server, so Cisco Unified Communications Manager can verify network connectivity and publisher-subscriber validation. Additionally, you must enter the host name and the IP address for the subscriber server. When the Cisco Unified Communications Manager installation prompts you for the host name of the subscriber server, enter the value that displays in the Server Configuration window in Cisco Unified Communications Manager Administration; that is, if you configured a host name for the subscriber server in the Host Name/IP Address field.

Related Topics

- "Server Configuration" chapter, *Cisco Unified Communications Manager Administration Guide*
- *Installing Cisco Unified Communications Manager, Release 7.1(2)*
- *Cisco Unified Communications Operating System Administration Guide*
- *Command Line Interface Reference Guide for Cisco Unified Solutions Release 7.1(3)*
- *Changing the IP Address and Host Name for Cisco Unified Communications Manager7.1(2)*

Adding or Updating SIP Dial Rules Causes Cisco TFTP Service to Rebuild All Phone Configuration Files

When you add or update a SIP dial rule in Cisco Unified Communications Manager Administration, be aware that the Cisco TFTP service rebuilds all phone configuration files, which may cause CPU to spike on the server where the Cisco TFTP service runs, especially if you have a large system with many phones. To ensure that CPU does not spike, add or update the SIP dial rule during a maintenance window or temporarily stop the Cisco TFTP service in Cisco Unified Serviceability before you make the configuration change. If you stop the Cisco TFTP service, remember to restart the service in Cisco Unified Serviceability after you add or update the SIP dial rule.

CSCta10219 Unicast Music on Hold May Not Play

After you invoke music on hold (MOH) several times, unicast MOH may not play. You can invoke MOH by using hold, transfer, conference, park, and so on.

The unicast MOH may resume playing on later hold attempts

Workaround - Option 1

Upgrade to a version of Cisco Unified Communications Manager that contains a fix for this issue.

Workaround - Option 2

Configure the MOH servers to send out multicast MOH and unicast MOH on the same MOH resources.

Procedure

Step 1 Configure each MOH audio source ID for multicast.

Step 2 Configure each MOH server to multicast.

Step 3 Make sure that Media Resource Groups (if any are defined) do not have multicast enabled.

Be aware that no network (router) changes to forward multicast MOH packets are required if Media Resource Groups (MRG) are not configured to enable multicast MOH.

Note The MOH servers transmit multicast streams for each MOH source and MOH codec, so network traffic to the local network may increase. The multicast streams will remain continuous and run at all times.

The MOH servers send the multicast streams to the local router; but, if the rounter is not configured to forward the MOH multicast packets, impact to the LAN traffic will be minimal. By default, routers do not forward multicast MOH packets.

SFTP Server Products

Cisco allows you to use any SFTP server product with applications that require SFTP access 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 version of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to http://www.cisco.com/pcgi-bin/ctdp/Search.pl. For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to 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 http://www.titanftp.com/)

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

CSCsu08609 Blind Transfer or Unanswered Conference Call over QSIG PRI Trunk

A blind transfer or an unanswered conference call that gets forwarded to voice-mail over QSIG PRI trunk reaches the general greeting instead of the called party.

Important Information About Delete Transaction by Using Custom File in BAT

Do not use the insert or export transaction files that are created with bat.xlt for the delete transaction. Instead, you must create a custom file with the details of the records that need to be deleted. Use only this file for the delete transaction. In this custom delete file, you do not need a header, and you can enter values for name, description, or user.

TAPS Name Change in Bulk Administration Tool

Documentation refers to the Tool for Auto-Registered Phone Support (TAPS) as Cisco Unified Communications Manager Auto-Register Phone Tool in the Online Help for Bulk Administration. All references to 'Cisco Unified Communications Manager Auto-Register Phone Tool' in the Bulk Administration Tool Online Help should be read as 'Tool for Auto-Registered Phone Support (TAPS)'. This makes the terminology compliant with the Bulk Administration user interface.

For More Information

For information on configuring additional features in Bulk Administration Tool, refer to the BAT documentation for Cisco Unified CM.

Basic Uninterruptible Power Supply (UPS) Integration

When Cisco Unified Communications Manager 6.1(4) runs on an MCS 7825H2 or MCS 7835H2, basic integration to the UPS model APC SmartUPS 1500VA USB and APC 750VA XL USB gets supported. Integration occurs via a single point-to-point Universal Serial Bus (USB) connection. Serial and SNMP connectivity to UPS does not get supported, and the USB connection must be point-to-point (in other words, no USB hubs). Single- and dual-USB UPS models get supported. The feature activates automatically during bootup if a connected UPS gets detected.

Alternatively, on MCS-7835H2, you can execute the **show ups** CLI command that shows the current status of the USB-connected APC smart-UPS device and starts the monitoring service if it is not already started.

On supported servers, the CLI command also displays detected hardware, detected versions, current power draw, remaining battery runtime, and other relevant status information.

When the feature is activated, graceful shutdown will commence as soon as the low battery threshold is reached. Resumption or fluctuation of power will not interrupt or abort the shutdown.

For unsupported Cisco Unified Communications Manager releases, MCS models, and/or UPS vendor/make/models, you can cause an external script to monitor the UPS. When low battery gets detected, you can log on to Cisco Unified Communications Manager by using Secure Shell (SSH), access the CLI, and execute the **utils system shutdown** command.

Strict Version Checking

Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco Unified Communications Manager.

Note Make sure that the restore runs on the same Cisco Unified Communications Manager version as the backup. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore.

In essence, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful Cisco Unified Communications Manager database restore.

Serviceability Not Always Accessible from OS Administration

In some scenarios, you cannot access Cisco Unified Serviceability from Cisco Unified OS Administration. The window displays a “Loading, please wait” message indefinitely.

If the redirect fails, log out of Cisco Unified OS Administration, select Cisco Unified Serviceability from the navigation menu, and log in to Cisco Unified Serviceability.

Voice Mailbox Mask Interacts with Diversion Header

When a call gets redirected from a DN to a voice-messaging server/service that is integrated with Unified CM by using a SIP trunk, the voice mailbox mask on the voice-mail profile for the phone modifies the diverting number in the SIP diversion header. Be aware that this behavior is expected because the Unified CM server uses the diversion header to choose a mailbox.

Best Practices for Assigning Roles to Serviceability Administrators

Cisco recommends that you configure application users, rather than end users, to access remote nodes to perform such tasks as starting and stopping services. Starting and stopping services requires that the Standard Serviceability Administration and Standard RealtimeAndTraceCollection roles be assigned.

For Serviceability, the Administrator That Is Created During Installation Must Not Be Removed

Removing the Administrator that is created during installation can cause communication with remote nodes via Serviceability Administration to fail.

Connecting to Third-Party Voice Messaging Systems

Administrators can connect third-party voice-messaging systems to Cisco Unified Communications Manager. Ensure the voice-messaging system has a simplified message desk interface (SMDI) that is accessible with a null-modem EIA/TIA-232 cable (and an available serial port). To connect the EIA/TIA-232 cable to Cisco Unified Communications Manager Release 5.0 or later, use a Cisco certified serial-to-USB adapter with the part number USB-SERIAL-CA=.

User Account Control Pop-up Window Displays During Installation of RTMT

When you install RTMT on the Microsoft Vista platform, the system displays the User Account Control pop-up window to indicate that an unidentified program wants access to your computer. This occurs because of a limitation in the InstallAnywhere software. This one-time pop-up displays only when you are installing RTMT. To continue, select **Allow**.

CiscoTSP Limitations on Windows Vista Platform

Always perform the first-time installation of the CiscoTSP and Cisco Unified Communications Manager TSP Wave Driver on a Vista machine as a fresh install.

If secure connection to Cisco Unified Communications Manager is to be used, turn off the Windows firewall.

If Cisco Unified Communications Manager TSP Wave Driver is used for inbound audio streaming, turn off the Windows firewall.

If Cisco Unified Communications Manager TSP Wave Driver is used for audio streaming, disable all other devices in the “Sound, video and game controllers” group.

Time Required for Disk Mirroring

Disk mirroring on server model 7825 I3 with 160 GB SATA disk drives takes approximately 3 hours.

Disk mirroring on server model 7828 I3 with 250 GB SATA disk drives takes approximately 4 hours.

Serviceability Session Timeout Is Not Graceful

When a session has been idle for more than 30 minutes, the Cisco Unified Serviceability user interface allows you to make changes before it indicates that the session timed out and redirects you to the login window. After you log in again, you may need to repeat those changes. This behavior occurs in the Alarm, Trace, Service Activation, Control Center, and SNMP windows.

Workaround

If you know that the session has been idle for more than 30 minutes, log out by using the Logout button before making any changes in the user interface.

Serviceability Limitations When You Modify the IP Address

When you modify the IP Address field, you cannot access the RTMT profiles, custom counters, custom alerts, and generic queries for Trace & Log Collection Tool (TLC) for that server.

You should manually remove any RTMT profiles, custom counters, custom alerts, and generic queries for Trace and Log Collection Tool (TLC) that were set for the old IP Address. When you modify the IP Address field, you will need to re-create the RTMT profile, custom counters, custom alerts, and generic queries for TLC the next time that you log in to the server on RTMT.

Cisco AMC Service includes two user-configurable service parameters, Primary Collector and Failover Collector. These service parameters use Host Name/IP Address to designate the primary and failover AMC server. If you change the IP address of the AMC primary collector or failover collector, you should check these service parameters and update them accordingly.

Cisco Serviceability Reporter service includes one user-configurable service parameter, RTMT Reporter Designated Node. This service parameter uses Host Name/IP Address to designate the node on which RTMTReporter runs. If you changed the IP address of the RTMT Reporter Designated Node, you should check this service parameter and update it accordingly.

CSCtj61834 MLPP Default Domain Name Displays MLPP ID Value

When you configure the MLPP Domain Name in Cisco Unified Communications Manager, the default name for MLPP Domain Name displays the MLPP ID value 000000 instead of Default as stated on the help page.

CSCtr40861 Incoming Calling Party Numbers should be up to 16 characters

When configuring the Incoming Calling Party Numbers setting, the number of characters you can enter is 16 not 8 for:

- Incoming Calling Party National Number Prefix
- Incoming Calling Party International Number Prefix
- Incoming Calling Party Unknown Number Prefix
- Incoming Calling Party Subscriber Number Prefix

You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#).

CSCtr84167 Block Offnet to Offnet Transfer

When you enable the service parameter Block Offnet to Offnet Transfer and make a blind transfer with Cisco Unity Connection, the Q.931 SETUP message which Cisco Unified Communications Manager sends to the PSTN gateway for an outbound PRI call still reaches the gateway. This transfer results in a dropped call.

CSCtr21486 Troubleshooting Guide Update to Switch Version

When there is a version mismatch between a subscriber server and publisher server, the Cisco Unified Communications Manager history file does not log a switch version entry.

MDCX Sendonly Message Suppressed for MGCP Calls

For all MGCP calls, Cisco Unified Communications Manager suppresses the media layer from sending any MDCX (M:sendonly) messages to the MGCP gateway. This is done to prevent one-way audio scenarios.

CSCtx86215 Database Replication

This section of the Cisco Unified Communications Manager System Issues chapter in the *Troubleshooting Guide for Cisco Unified Communications Manager* requires this addition:

Extension Mobility does not work when database replication breaks between the Unified CM node running Extension Mobility and the Unified CM node to which the phone is registered.

CSCuc10415 Tip for Adding a New Server

The following tip needs to be added to the "Server settings" topic in the Cisco Unified Communications Manager Administration Guide.

To avoid errors, Cisco recommends that you add a server to the system with a name that has less than 47 characters. Then, update the server name to the target length.

CSCuc79185 Device Mobility Calling Search Space is Used When Device CSS is <none>

The following note is missing from the "Phone Settings" topic in the *Cisco Unified Communications Manager Administration Guide*:

When set to <none>, Unified CM uses the device mobility calling search space, which is configured on the device pool.

CSCtw44980 Missing Exceptions for Voice-Mail Pilot

The following information is missing for the Voice Mail Pilot Name field description in the "Voice-Mail Pilot Settings" topic in the *Cisco Unified Communications Manager Administration Guide*:

Allowed characters are numeric (0-9), plus (+), asterisk (*), and pound (#).

CSCud34740 Application User AXL Password Must Not Contain Special Characters

The following note is missing from the Application User Settings topic in the Cisco Unified Communications Manager Administration Online Help:

Note Do not use special characters when you create an AXL password for an application user.

CSCud70447 Missing Etoken Recovery Steps in Troubleshooting Guide

The *Cisco Unified Communications Manager Troubleshooting Guide* is missing the following procedure for troubleshooting if you lose all security tokens (etokens):

Perform the following procedure if you lose the security tokens and you need to update the CTL file.

Tip Perform the following procedure during a scheduled maintenance window, because you must reboot all servers in the cluster for the changes to take effect.

Step 1 On every Cisco Unified CallManager, Cisco TFTP, or alternate TFTP server, verify that CTLFile.tlv exists from the OS SSH command line.

file list tftp CTLFile.tlv

Step 2 Delete CTLFile.tlv.

file delete tftp CTLFile.tlv

Step 3 Repeat step 1 and step 2 for every Cisco Unified CallManager, Cisco TFTP, and alternate TFTP server.

Step 4 Obtain at least two new security tokens.

Step 5 By using the Cisco CTL client, create the CTL File, as described in "Installing the Cisco CTL Client" and "Configuring the Cisco CTL Client".

Tip If the clusterwide security mode is in mixed mode, the Cisco CTL client displays the message No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode. For the system to function, you must create the CTL File and set CallManager Cluster to Mixed Mode. Click OK; then, choose Set CallManager Cluster to Mixed Mode and complete the CTL file configuration.

Step 6 Reboot all the servers in the cluster.

Step 7 After you create the CTL file on all the servers and reboot all servers in the cluster, delete the CTL file from the phone, as described in "Deleting the CTL File on the Cisco Unified IP Phone".

CSCud95087 Limitation of SIP Forking on Trunk Not Documented

The following information is missing from "Understanding Session Initiation Protocol" in the *Cisco Unified Communications Manager System Guide*:

- Cisco Unified CallManager Release 4.x does not accept provisional responses (such as 180 Ringing) from more than five destinations. It does not accept a successful response (200 Ok) from any destination that is not among the first five to respond.
- Cisco Unified CallManager Release 5.x and Cisco Unified Communications Manager Release 6.x do not accept provisional responses (such as 180 Ringing) from more than 20 destinations. They do not accept a successful response (200 Ok) from any destination that is not among the first 20 to respond.

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 Unified Communications 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 Unified Communications Manager Release 7.1 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 Unified Communications Manager Release 7.1(4) As of November 17, 2009 describe possible unexpected behaviors in Cisco Unified Communications Manager Release 7.1, which are sorted by component.

Tip For more information about an individual defect, click the associated Identifier in the "Open Caveats for Cisco Unified Communications Manager Release 7.1(4) As of November 17, 2009" section on page 27 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 Unified Communications Manager interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Unified Communications Manager 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 Unified Communications Manager maintenance releases may not be as clearly identified.

The following examples show 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 Unified Communications Manager release that includes that interim version. You can use these examples as guidance to better understand the presentation of information in these fields.

- 7.0(2.20000-x) = Cisco Unified Communications Manager Release 7.0(2a)
- 7.0(2.10000-x) = Cisco Unified Communications Manager Release 7.0(2)
- 6.1(3.3000-1) = Cisco Unified Communications Manager 6.1(3b)
- 6.1(3.2000-1) = Cisco Unified Communications Manager 6.1(3a)
- 6.1(3.1000-x) = Cisco Unified Communications Manager 6.1(3)
- 5.1(3.7000-x) = Cisco Unified Communications Manager 5.1(3f)

Note Because defect status continually changes, be aware that the "Open Caveats for Cisco Unified Communications Manager Release 7.1(4) As of November 17, 2009" section on page 27 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 25.

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 Unified Communications Manager Release 7.1(4) As of November 17, 2009

The following information comprises unexpected behavior (as of November 17, 2009) that you may encounter in Release 7.1(4) of Cisco Unified Communications Manager.

Table 3 Cisco Unified Communications Manager Release 7.1(4) Open Caveats as of November 17, 2009

Id	Component	Headline
CSCta97266	cmcti	CTIManager cores when run traffic with L2 upgrade and memory leaking.
CSCtd17972	cp-mediacontrol	No video in sTransfer of RT call to TB over SIP ICT.
CSCtd17335	cp-mediacontrol	Video lost on hairpin sTransfer call with RT video after hold/resume.
CSCtd16828	cp-mediacontrol	No video in hairpin conference involving RT video and polycom.
CSCtd20045	cp-mediacontrol	No video between polycom and CUVA on SIP hairpin call.
CSCtc97854	cp-mobility	AAR does not work when the called extension has remote destination associated.
CSCtc95198	cp-sip-trunk	SIP ICT call to SIP gateway failed with multiple-nodes.
CSCsl81015	cpi-security	Intermittent Alertsmessage appear in RTMT (Write failed: Connection reset by peer). The message occurs when CDR SFTPs files to the publisher server from the subcriber server.
CSCtb66354	cpi-vendor	IBM Director Agent reports defunct drive - false RAID alert.
CSCtc36390	database-ids	Informix crash file exists on the system.
CSCtd03873	ipma-service	IPMA call redirected to manager instead of receiving a busy tone.
CSCtc47459	qed	Services Provisioning parameter is missing for 7931 SIP.
CSCtc77209	video	Tandberg hairpin video call with btransfer includes no video.

Documentation Updates

This section contains information on documentation omissions, errors, and updates for the following Release 7.1(3) documentation, which is our latest documentation set:

Installation, Upgrade, and Migration

This section contains information on the following topics:

Installing Licenses While Replacing a Publisher Node

This section replaces the section "Replacing the Publisher Node" in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*. Follow this process to replace a publisher server with a new server.

Table 4 Replacing the Publisher Node Process Overview

	Description	For More Information
Step 1	Perform the tasks in the "Server or Cluster Replacement Preparation Checklist" section.	*Replacing a Single Server or Cluster for Cisco Unified Communications Manager*
Step 2	Gather the necessary information about the old publisher server.	See the "Gathering System Configuration Information to Replace or Reinstall a Server" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 3	Back up the publisher server to a remote SFTP server by using the Disaster Recovery System and verify that you have a good backup.	See the "Creating a Backup File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 4	Get new licenses of all the license types before system replacement.	Get new licenses of all the license types: Software License Feature, CCM Node License Feature, and Phone License Feature. You only need new licenses if you are replacing the publisher node. For more information, see the "Obtaining a License File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 5	Shut down and turn off the old server.	
Step 6	Connect the new server.	

	Description	For More Information
Step 7	Install the same Cisco Unified Communications Manager release on the new server that was installed on the old server, including any Engineering Special releases. Configure the server as the publisher server for the cluster.	See the "Installing Cisco Unified Communications Manager on the New Publisher Server" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 8	Restore backed-up data to the publisher server by using Disaster Recovery System.	For more information, see the "Restoring a Backup File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 9	Reboot all nodes in the cluster. If the server is not in a cluster, then reboot the server.	
Step 10	Upload all of the new license files to the publisher server.	Upload new license files for all of the license types: Software License Feature, CCM Node License Feature, and Phone License Feature. For more information, see the "Uploading a License File" section in the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*.
Step 11	Delete all invalid license files (those based on the old server MAC address).	"Deleting Invalid License Files" section on page 29
Step 12	Perform the post-replacement tasks in the "Post-Replacement Checklist" section.	*Replacing a Single Server or Cluster for Cisco Unified Communications Manager*

Deleting Invalid License Files

The license files that get restored to the server by Disaster Recovery System are invalid because they are bound to the MAC address of the old server. To delete all invalid license files from your server, follow these steps:

Step 1 Obtain the MAC address of the new server by running the **show status** CLI command.

The MAC address displays in the field License MAC.

Step 2 View each license file on the server to determine which license files are invalid.

a. In Cisco Unified Communications Manager Administration, choose **System > Licensing > License File Upload**.

b. Choose a license file from the Existing License Files drop-down list.

c. Click the **View File** button.

d. The license file MAC address displays in the HOSTID field.

If the license file MAC address does not match the server MAC address, then the license is invalid.

e. Record the file name of each invalid license file.

f. Repeat this process for each license file on the server.

Step 3 Delete each invalid license file from the server by running the CLI command **file delete license** *filename*, where *filename* is the name of the license file.

For more information about this command, refer to the document *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Server Replacement

This section contains information on the following topics:

Password Validation During a Server Replacement

If you replace a server that was previously upgraded from an older product release, the Cisco Unified Communications Manager installation program may deny your passwords. This happens because the password validation rules might get stronger in the new product release, but passwords do not get revalidated during an upgrade; however, when you perform a fresh installation on the server that you are replacing, the new, stronger password validation occurs.

If this happens, choose new passwords that the installation program will accept. For more information about passwords, see the document *Installing Cisco Unified Communications Manager*.

Rebooting Servers While You Are Replacing a Publisher Server

This section comprises an update to the document *Replacing a Single Server or Cluster for Cisco Unified Communications Manager Release 7.1(2)*. It applies to the procedure for replacing a publisher server in a cluster.

After you restore data to the new publisher server, reboot all the cluster nodes. The document says to reboot just the publisher server, but you must reboot all of the cluster nodes to enable database replication.

Troubleshooting

This section contains information on documentation omissions, errors, and updates for the *Troubleshooting Guide for Cisco Unified Communications Manager.*

Two New dbreplication Commands Exist

The *Troubleshooting Guide for Cisco Unified Communications Manager* omits two dbreplication commands.

utils dbreplication runtimestate

Use this command

- To determine the status of a replication reset.
- Along with **utils dbreplicaiton status** | **utils dbreplication quickaudit**, to determine the general health of replication.

utils dbreplication quickaudit

Use this command to run a quick database check on selected content on dynamic tables.

Bulk Administration Tool

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified Communications Manager Bulk Administration Guide*.

The following information is missing from the online help for *Cisco Unified Communications Manager Bulk Administration Guide*:

Deleting Unassigned Directory Numbers

Use the following procedure to delete unassigned directory numbers by creating a query to locate the phone records.

Procedure

Step 1 Choose **Bulk Administration > Phones > Delete Phones > Delete Unassigned DN**.

The Delete Unassigned Directory Numbers window displays.

Step 2 From the first Delete Bulk Unassigned Directory Number where drop-down list box, choose one of the following criteria:

- Pattern
- Description
- Route Partition

From the second Delete Bulk Unassigned Directory Number where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable.

Step 4 Click **Find**.

A list of discovered phones displays by

- Pattern
- Description
- Partition

Tip To find all unassigned directory numbers that are registered in the database, click **Find** without entering any search text.

Step 5 In the Job Information area, enter the Job description.

The default description is Delete Unassigned DN - Query

Step 6 To delete the unassigned directory numbers immediately, click the Run Immediately radio button. To delete the phone records at a later time, click Run Later.

Step 7 To create a job for deleting the phone records, click **Submit**.

Note Make sure to browse the entire list of displayed results before submitting the job.

Step 8 To schedule and/or activate this job, use the Job Configuration window.

Cisco Unified Communication Manager CDR Analysis and Reporting

This section contains information on documentation omissions, errors, and updates for the *CDR Analysis and Reporting Administration Guide*.

Changed Values of Mobility Cell Pick

The Mobility section of "CDR Examples" chapter in *Cisco Unified Communications Manager - Call Detail Records Administration Guide* has wrong values for some field names. The corrected values follow:

FieldNames	Enterprise Call to 22285	Server Call to Cell Phone	Final Handout Call
callingPartyNumber	22202	2202	22202
originalCalledPartyNumber	22285	22285	22285
finalCalledPartyNumber	22285	9728324124	22285
lastRedirectDn	22285	22285	22285
origCause_Value	393216	393216	0
dest_CauseValue	393216	393216	16
lastRedirectRedirectReason	0	0	415
lastRedirectRedirectOnBehalfOf	0	24	24
joinOnBehalfOf	0	24	24

Purpose of Cisco Unified Communications Manager CDR Analysis and Reporting

The *CDR Analysis and Reporting Administration Guide* omits the following statement about the primary purpose of the Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) software:

> CAR is not intended to replace call accounting and billing solutions that third-party companies provide. You can find the companies that provide these solutions and that are members of the Cisco Technology Developer Program by searching the home page of the Cisco Developer Community at this URL: http://developer.cisco.com/web/cdc/home.

The following online document has been revised to include the omitted statement:

- book: *CDR Analysis and Reporting Administration Guide, Release 7.1(2)*
  chapter: CDR Analysis and Reporting Overview

"Mailing a Report" Recipients

The "Mailing a Report" chapter in the *Cisco Unified Communications Manager Call Detail Records Administration Guide* omits this information:

When the Mailing option gets enabled,

- End users receive the individual billing summary.
- Managers receive the individual billing summary, department billing summary, Top n Report, and the QoS report.
- CAR Administrators receive all reports.

Cisco Unified Communications Manager Security

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified Communications Manager Security Guide*.

You Can Use HTTPS Protocol with Different Browsers and Operating Systems

The *Cisco Unified Communications Manager Security Guide* incorrectly states that the HTTPS is only compatible with Microsoft Windows products. The following paragraph provides the corrected information:

HTTPS, or Hypertext Transfer Protocol over Secure Sockets Layer (SSL), secures communication between a compatible browser and web server. HTTPS uses certificates to ensure server identities and to secure the browser connection.

Definition of Locally Significant Certificate

The definition of Locally Significant Certificate (LSC) in the *Cisco Unified Communications Manager Security Guide* need correction as follows: A third-party certificate authority (CA) cannot issue an LSC. An LSC represents a digital X.509v3 certificate that CAPF issues. It gets installed on a phone or JTAPI/TAPI/CTI application.

Cisco Unified Communications Operating System

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified Communications Operating System Administration Guide*.

Incorrect Values for Phase One DH an dPhase Two DH

The Security chapter of the *Cisco Unified Communications Operating System Administration Guide* incorrectly specifies the values for Phase One DH and Phase Two DH. On the IPSEC Policy Configuration window, the Phase One DH and Phase Two DH pulldown menus contain the values 2, 1, and 5.

Using Certificates Issued by a Third-Party Certificate Authority

This information supplements the documentation about using certificates that are issued by a third-party certificate authority (CA) that is in the *Cisco Unified Communications Operating System Administration Guide*.

- For all certificate types except CAPF, obtain and upload a CA root certificate and an application certificate on each node.
- For CAPF, obtain and upload a CA root certificate and an application certificate only on the first node.
- CAPF and Cisco Unified Communications Manager CSRs include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the ExtensionRequest mechanism, you must enable the X.509 extensions, as follows:
  - The CAPF CSR uses the following extensions:

    ```
    X509v3 extensions:
    X509v3 Key Usage:
    Digital Signature, Certificate Sign
    X509v3 Extended Key Usage:
    TLS Web Server Authentication, IPSec End System
    ```

  - The CSRs for Cisco Unified Communications Manager, Tomcat, and IPSec use the following extensions:

    ```
    X509v3 Key Usage:
    Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
    X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
    ```

- Upload the CA root certificate of the CA that signed an application certificate. If a subordinate CA signs an application certificate, you must upload the CA root certificate of the subordinate CA, not the root CA.
- You upload CA root certificates and application certificates by using the same Upload Certificate dialog box. When you upload a CA root certificate, choose the certificate name with the format *certificate type***-trust**. When you upload an application certificate, choose the certificate name that only includes the certificate type. For example, choose **tomcat-trust** when you upload a Tomcat CA root certificate; choose **tomcat** when you upload a Tomcat application certificate.
- When you upload a CAPF CA root certificate, it gets copied to the CallManager-trust store, so you do not need to upload the CA root certificate for CallManager separately.

Revised Procedure to Shut Down the System

The "System Restart" chapter in the *Cisco Unified Communications Operating System Administration Guide* requires the following revisions to the Shut Down the System section:

- Replace the text of the first caution with the following text:

  Do not press the power button on the server to shut down the server or to reboot the server. If you do, you may accidentally corrupt the file system, which may prevent you from being able to reboot your server.

- Replace the text after the first caution with the following text:

  To shut down the system, follow Procedure 1 or Procedure 2.

- Replace the note text with the following text:

  The hardware may require several minutes to power down.

- Insert the following text after the note:

  Procedure 2

  Run the CLI command **utils system shutdown** or the command **utils system restart**. For information on how to run CLI commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Cisco Unified Communications Manager Administration

This section contains information on documentation omissions, errors, and updates for the *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager Features and Services Guide*, and the *Cisco Unified Communications Manager System Guide*.

Cisco Unified Communications Manager Administration Guide

Cisco Unified Communications Manager System Guide

Cisco Unified Communications Manager Features and Services Guide

How the Number of Client Matter Codes Affects System Start Up Time

The "Client Matter Codes" chapter of the *Cisco Unified Communications Manager Administration Guide* omits the following information:

Because the number of CMCs directly impacts the time that is required for Cisco Unified Communications Manager to start up, limit the number of CMCs to 60,000. If you configure more CMCs than that, expect significant delays. For example, a system with 400,000 CMCs requires approximately 1 hour to start up; a system with 1 million CMCs requires approximately 4 hours to start up.

SIP Profile Configuration No Longer Includes a Call Stats Check Box

The SIP Profile Configuration Settings section of the "SIP Profile Configuration? chapter of the *Cisco Unified Communications Manager Administration Guide* includes information about the Check Stats check box.

That check box no longer exists.

NTP Reference Configuration Settings Omits Two Available Modes

The Phone NTP Reference Configuration Settings section of the "System Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* omits information about two available Modes.

The additional information specifies:

- Multicast
- Anycast

IP Subnet Example Incorrectly Contains a Period (.) Instead of a Slash (/)

The "SIP Route Patterns Configuration Settings" chapter of the *Cisco Unified Communications Manager Administration Guide* contains the following examples:

IPv4 address examples: 172.18.201.119 or 172.18.201.119/32 (explicit IP host address); 172.18.0.0/16 (IP subnet); 172.18.201.18.21 (IP subnet).

The examples should specify:

IPv4 address examples: 172.18.201.119 or 172.18.201.119/32 (explicit IP host address); 172.18.0.0/16 (IP subnet); 172.18.201.18/21 (IP subnet).

Default Setting of the User Must Change at Next Login Check Box Is Incorrect

The "User Management Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* contains incorrect information about the default setting of the User Must Change at Next Login check box.

The correct information is that the default setting for this check box specifies checked.

Device Name Field Omits Information About Valid Characters and Number of Characters Allowed

The Phone Configuration Settings section of the "Cisco Unified IP Phone Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* does not include information about valid characters for the Device Name field. That information follows:

Enter a name to identify software-based telephones, H.323 clients, and CTI ports.

For device names that are not based on a MAC address, as a general rule, you can enter 1 to 15 characters comprised of alphanumeric characters (a-z, A-D, 0-9). In most cases you can use dot (.), dash (-), and underscore (_) as well.

Note Because the rules for the device name field depend on the device type, Cisco recommends that you refer to the product documentation to determine which character set is valid for your device, as well as the number of characters allowed.

Valid Characters Not Included in the Description of the Transcoder Device Name Field

The Transcoder Configuration Settings section of the "Transcoder Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* did not include the characters that are allowed in the Device Name field.

That information follows:

You can enter up to 15 characters in the Device Name field. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-) and underscore (_).

Valid Characters Not Included in the Description of the IOS Conference Bridge Name Field

The IOS Conference Bridge Configuration Settings section of the "Conference Bridge Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* does not include the characters that are allowed in the Device Name field.

That information follows:

You can enter up to 15 characters in the Device Name field. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-) and underscore (_).

Invalid Characters for Cisco Conference Bridge (WS-SVC-CMM) Description Field Omitted

The Description field in the Cisco Conference Bridge (WS-SVC-CMM) Configuration Settings section of the "Conference Bridge Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* does not include the invalid characters.

Invalid characters comprise quotes ("), angle brackets (<>), backslash (), ampersand,(&), and percent sign (%).

Application Dial Rule Configuration Settings Table Is Incorrect

The Application Dial Rule Configuration Settings table in the "Application Dial Rules Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* contains some incomplete and erroneous information. The correct information follows.

Table 5 Application Dial Rule Configuration Settings

Field	Description
Name	Enter a name in the Name field. The name must be at least one character in length and can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). Ensure each application dial rule name is unique.
Description	Enter a description of the application dial rule in the Description field. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>)
Number Begins With	Enter the initial digits of the directory numbers to which you want to apply this application dial rule. Valid characters include numeric digits (0-9), plus sign (+), asterisk (*), and number sign (#). Be aware that you cannot enter more than 50 characters in this field.
Number of Digits	Enter the length of the dialed numbers to which you want to apply this application dial rule. This field • Supports numeric characters (0-9) only. • Must contain a value that is equal to or greater than 0 and less than 100.
Total Digits to be Removed	Enter the number of digits that you want Cisco Unified Communications Manager to remove from the beginning of dialed numbers that apply to this dial rule. This field • Supports numeric characters (0-9) only. • Must contain a value that is equal to or greater than 0 and less than 100. • Cannot contain a value that is more than the value in the Number of Digits field.
Prefix With Pattern	Enter the pattern to prepend to dialed numbers that apply to this application dial rule. Valid values include numeric digits (0-9), plus (+), asterisk (*), and pound (#). Be aware that you cannot enter more than 50 characters in this field.
Application Dial Rule Priority	Choose the dial rule priority as top, bottom, or middle.

Valid Characters for Voice Mail Profile Name Field Omitted

In the Voice-Mail Profile Configuration Settings section of the “Voice Mail Configuration” chapter of the *Cisco Unified Communications Manager Administration Guide*, the description of the Voice Mail Profile Name field does not include information about valid characters.

The valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), period(.), dash(-), underscore(_).

Meet-Me Number/Pattern Configuration Settings Description Field Description Is Incorrect

The Meet-Me Number/Pattern Configuration Settings section in the"Call Routing Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* incorrectly states that you can enter up to 30 alphanumeric characters in the description field. In fact, you can enter up to 50 alphanumeric characters.

User Documentation Misnames Single Button Barge Field

The Device Profile Configuration Settings section in the "Device Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide* incorrectly calls the Single Button Barge field, Single Button Barge/cBarge.

The description of that field also incorrectly includes information about cBarge.

Allowed Prefix Digits Incorrect for AAR Group Configuration

The AAR Group Configuration Settings section in the "Call Routing Configuration" chapter of the Cisco *Cisco Unified Communications Manager Administration Guide* incorrectly enumerates the valid characters that are allowed in the Prefix Digits field.

The characters that are allowed comprise numeric characters (0-9), alpha characters (A - D), asterisk (*), pound sign (#), plus sign (+), and dash (-).

Service Parameters Expanded Explanation

The "Service Parameters" chapter of the *Cisco Unified Communications Manager Administration Guide* omits the following information:

To configure service parameters, you must select a single server and a single service on that server. After you make the selection you can configure parameters for the service on that single serve and on others that apply to the service on all servers within the cluster; these get marked as clusterwide.

Unlike enterprise parameters that apply to all services, each service gets configured with a separate set of service parameters.

Do Not Begin Starting and Ending Directory Numbers with a Zero (0)

Note

In the *Cisco Unified Communications Manager Administration Guide*, in Table 3 of the "Cisco Unified Communications Manager Configuration" chapter, under Auto-registration Information, the descriptions of Starting Directory Number and Ending Directory Number omit the information that neither number should begin with a zero (0).

Number of Locations and Regions That Cisco Unified Communications Manager Supports

The Cisco Unified Communications Manager Administration documentation incorrectly states the number of locations and regions that Cisco Unified Communications Manager supports. The correct limits follow:

- Cisco Unified Communications Manager supports up to 2000 locations.
- Cisco Unified Communications Manager supports up to 2000 regions.

The following online documents have been revised with the correct limits:

- book: *Cisco Unified Communications Manager Administration Guide, Release 7.1(2)*
  chapter: Location Configuration
- book: *Cisco Unified Communications Manager Administration Guide, Release 7.1(2)*
  chapter: Region Configuration
- book: *Cisco Unified Communications Manager System Guide, Release 7.1(2)*
  chapter: System-Level Configuration Settings

Intercom Route Partition Configuration Settings Description Field Information Is Incorrect

The Intercom Route Partition Configuration Settings description field in the "Configuring Intercom" chapter of the *Cisco Unified Communications Manager Administration Guide* omits a complete list of the non-alphanumeric characters that are not allowed in the description. The unacceptable characters comprise double-quotes ("), angle brackets (<>), square bracket ([ ]), ampersand (&), and percentage sign (%).

Valid Characters in Name Field of Role Configuration Window

In the *Cisco Unified Communications Manager Administration Guide*, be aware that the description for the Name field in the Role Configuration window in the "Role Configuration" chapter is incomplete. The complete description follows:

> Enter a name for the role. Roles can comprise up to 128 characters.
>
> Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.

Directory Number Chapter Includes Incorrect Information on Alerting Name and Display Name Fields

The "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly describes the Alerting Name field. In addition, The chapter does not describe the relationship between the Alerting Name field and Display (Internal Caller ID) field.

Incorrect Information

For the Alerting Name field, enter a name that you want to display on the phone of the caller.

This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. If you configure an alerting name for a directory number with shared-line appearances, when the phone rings at the terminating PINX, the system performs the following tasks:

- Forwards the name of the caller that is assigned to the directory number.

- Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist); the originating PINX may modify the CONR, depending on the route pattern configuration.

If you do not configure an alerting name, "Name Not Available" may display on the caller phone. If you do not enter a name for the Display (Internal Caller ID) field, the information in the Alerting Name field displays in the Display (Internal Caller ID) field.

Setting the Always Display Original Dialed Number service parameter to True impacts the alerting name functionality. If you set the service parameter to True, the alerting name does not display on the calling phone; only the original dialed number displays.

Correct Information

For the Alerting Name field, enter a name that you want to display on the phone of the caller when the called phone is ringing.

This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. When the phone rings at the terminating PINX, if you configured an alerting name for a directory number with shared-line appearances, the system performs the following tasks:

- Forwards the alerting name of the called party, if configured, to the caller.
- Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist)

Depending on the state of the call and your configuration, the alerting name, directory number, or display (internal caller ID) configuration may display on the phone, as described in the following bullets.

- Alerting state—The alerting name displays, as configured in the Directory Number window.
- Connected state—If you configure the Display (Internal Caller ID) and the Alerting Name fields, the display (internal caller ID) name displays.
- Connected State—If you configured the Alerting Name field but not the Display (Internal Caller ID) field, the directory number displays.

Setting the Always Display Original Dialed Number service parameter to True impacts the alerting name functionality. If you set the service parameter to True, the original dialed number and the alerting name displays during the call.

End User Chapter Includes Incorrect Information for Manager User ID Field

The “End User Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide* incorrectly describes the Manager User ID field.

Incorrect Description

For the Manager User ID field, enter the user ID of the end user manager ID. The manager user ID that you enter must already exist in the directory as an end user.

Correct Description

For the Manager User ID field, enter the user ID of the end user manager ID. The manager user ID that you enter does not have to exist in the same cluster as the end user; therefore, Cisco Unified Communications Manager does not require that you enter a user ID that already exists in the database.

Device Pool Configuration Chapter Does Not State That You Can Enter -1 in the Connection Monitor Duration Field

The "Device Pool Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* does not state that, for the Connection Monitor Duration field, you can enter -1 or leave the field blank to use the configuration for the enterprise parameter. When you configure the Connection Monitor Duration field in the Device Pool Configuration window, use the following information:

This setting defines the time that the Cisco Unified IP Phone monitors its connection to Cisco Unified Communications Manager before it unregisters from SRST and reregisters to Cisco Unified Communications Manager.

To use the configuration for the enterprise parameter, you can enter -1 or leave the field blank. The default value for the enterprise parameter equals 120 seconds.

Change this setting if you need to disable the connection monitor or if you want to extend the connection monitor time. The maximum number of seconds that you can enter in the field equals 2592000.

Tip When you change the value of the connection monitor duration, it applies only to the device pool that is being updated. All other device pools use the value in their own connection monitor duration fields or use the value that is configured in the enterprise parameter.

Trunk Configuration Chapter Does Not State That You Can Enter Hostname in Destination Address Field

The "Trunk Configuration' chapter in the *Cisco Unified Communications Manager Administration Guide* does not state that you can enter a hostname in the Destination Address field, which supports SIP trunks. Use the following information when you configure the Destination Address field:

The Destination Address represents the remote SIP peer with which this trunk will communicate. The allowed values for this field specify a valid V4 dotted IP address, a hostname, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is checked.

For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual-stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field.

SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk.

For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and check the Destination Address is an SRV Destination Port check box.

If the remote end is a Cisco Unified Communications Manager cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster.

Device Name of Cisco Unified Mobile Communicator Must Not Exceed 15 Characters

The description of the Device Name field on the "Phone Configuration" chapter omits the following note:

Note Ensure that the device name of a Cisco Unified Mobile Communicator does not exceed 15 characters. If the device name of a Cisco Unified Mobile Communicator exceeds 15 characters, migration of this device will fail upon upgrade to a different release of Cisco Unified Communications Manager. If an existing Cisco Unified Mobile Communicator device name specifies a longer name, shorten the device name to 15 or fewer characters.

Recording Destination Address Field Description

In the "Recording Profile Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide*, the description of the Recording Destination Address field on the Recording Profile Configuration window omits the following information:

This field allows any characters except the following characters: double quotation marks (“), back quote (‘), and space ( ).

Call Stats Check Box Not Available to Enable Voice Quality Metrics

The Call Diagnostics and Voice-Quality Metrics section of the "Phone Features" chapter of the *Cisco Unified Communications Manager System Guide* incorrectly states that you can check the Call Stats check box on the SIP Profile Configuration window to enable voice quality metrics on Cisco Unified IP Phones for SIP.

That check box no longer exists.

Number of Digits Field Description Is Incorrect

The Application Dial Rules Configuration Error Checking section of the "Dial Rules Overview" chapter of the *Cisco Unified Communications Manager System Guide* misstates information about the Number of Digits field.

The correct information follows:

The Number of Digits field supports digits between 1 and 100, as well as the plus sign (+), the asterisk (*), and the number sign (#). Enter the number of digits of the dialed numbers to which you want to apply this application dial rule. You cannot allow this field to be blank for a dial rule.

OpenLDAP Version 2.3.41 Not Listed in LDAP Synchronization Documentation

The "Understanding the Directory" chapter in the *Cisco Unified Communications Manager System Guide* does not state the version of OpenLDAP that is supported for LDAP Synchronization with Cisco Unified Communications Manager Release 7.1(4).

OpenLDAP 2.3.41 Can Synchronize with Cisco Unified Communications Manager Database

DirSync allows you to synchronize data from corporate directories to Cisco Unified Communications Manager. Cisco Unified Communications Manager Release 7.1(4) allows synchronization from OpenLDAP 2.3.41 to the Cisco Unified Communications Manager database. In addition, Unified CM 7.1(4) allows synchronization from the following types of directories that were available in previous releases:

- Microsoft Active Directory 2000 and Microsoft Active Directory 2003
- Microsoft Active Directory 2008
- iPlanet Directory Server 5.1

- Sun ONE Directory Server 5.2
- Sun Java System Directory Server 6.0, 6.1, and 6.2

For more information, refer to the "Understanding the Directory" section of the *Cisco Unified Communications Manager System Guide*.

Application Dial Rules Configuration Error Checking Information Is Incorrect

The Application Dial Rules Configuration Error Checking section in the "Dial Rules Overview" chapter of the *Cisco Unified Communications Manager System Guide* contains incomplete or erroneous information. The correct information follows:

The application dial rules perform the following error checking in the Dial Rule Creation section of the Dial Rules Configuration window:

- The Name field must contain at least one character and supports up to 50 alphanumeric characters, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). Ensure each application dial rule name is unique.
- The Description field supports up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>)
- The Number Begins With field supports numeric characters (0-9) as well as plus sign (+), asterisk (*), and number sign (#). The length cannot exceed 50 characters.
- The Number of Digits field supports numeric characters (0-9) only. Ensure that the number is equal to or greater than 0 and less than 100. You cannot allow this field to be blank for a dial rule.
- The Remove Digits field supports numeric characters (0-9) only. Ensure that the number is equal to or greater than 0 and less than 100, and the value in this field cannot be more than the value in the Number of Digits field.
- The Prefix With Pattern field supports numeric characters (0-9) as well as plus sign (+), asterisk (*), and number sign (#). The length cannot exceed 50 characters.
- Ensure that dial rules are unique.
- You cannot allow both the Remove Digits field and the Prefix With Pattern field to be blank for a dial rule.

Time-of-Day Routing Chapter Omits Information About Defined Time Periods

The "Time-of-Day Routing" chapter of the *Cisco Unified Communications Manager System Guide* omits the following information.

If you define a time period with a specific date, on that specified date, that period overrides other periods that are defined on a weekly basis.

Example

Consider the following example:

- A time period, afterofficehours, that is defined as 00:00 to 08:00 from Monday to Friday exists.
- A time period, newyearseve, that is defined as 14:00 to 17:00 on December 31st exists.

In this case, on December 31st, the afterofficehours period does not get considered because it gets overridden by the more specific newyearseve period.

Licensing Chapter Does Not State That You Should Use Microsoft Outlook to Receive Licenses

The "Licensing" chapter in the *Cisco Unified Communications Manager System Guide* does not state that Cisco recommends that you use Microsoft Outlook when you receive Cisco Unified Communications Manager licenses.

Voice Mail Chapters Do Not Describe MWI Service Parameter

The voice mail chapters in the *Cisco Unified Communications Manager System Guide* do not describe the Multiple Tenant MWI Modes service parameter. For information on this service parameter, see the "CSCsx96370 Multiple Tenant MWI Modes Service Parameter" section on page 15.

How the Number of Client Matter Codes Affect System Start Up Time

The Interactions and Restrictions section of the "Client Matter Codes and Forced Authorization Codes" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following information:

Because the number of CMCs directly impacts the time that is required for Cisco Unified Communications Manager to start up, limit the number of CMCs to 60,000. If you configure more CMCs than that, expect significant delays. For example, a system with 400,000 CMCs requires approximately 1 hour to start up; a system with 1 million CMCs requires approximately 4 hours to start up.

Barge Initiators Cannot Conference In Additional Callers

The Restrictions section of the "Barge and Privacy" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following information.

- The barge initiator cannot conference in additional callers.

IPMASecureSysUser Password Change Procedure

The *Cisco Unified Communications Manager Features and Services Guide* omits the following information.

If you change the IPMASecureSysUser password, you must then go to the **IPMASecureSysUser config > CAPF Profile config** window for the profile that was selected on the IPMA Service Parameters window, change the Certificate Operation to "Install/Upgrade," provide the authentication string, and restart the IPMA service.

CSCsy92863 Intercom Route Partition Online Help Is Incorrect

The Intercom Route Partition Configuration Settings description field in the "Configuring Intercom" chapter of the *Cisco Unified Communications Manager Administration Guide* omits a complete list of the non-alphanumeric characters that are not allowed in the description. The unacceptable characters comprise double-quotes ("), angle brackets (<>), square bracket ([ ]), ampersand (&), percentage sign (%).

Mobile Connect Support Restrictions

The "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following restriction:

The Mobile Connect feature gets supported only for Primary Rate Interface (PRI) public switched telephone network (PSTN) connections.

For SIP trunks, Mobile Connect gets supported via IOS gateways or intercluster trunks.

Configuring an H.323 Gateway for System Remote Access by Using Hairpinning

The "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following (final) step in the "Configuring an H.323 Gateway for System Remote Access by Using Hairpinning" procedure:

Step 5 In the Cisco Unified Communications Manager, create a new route pattern to redirect the incoming MVA number to the H.323 gateway that has the vxml script loaded. Ensure that the Incoming CSS of the gateway can access the partition in which the new route pattern gets created.

Enterprise Feature Access Two-Stage Dialing

The "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* omits the following (final) steps in the "Enterprise Feature Access Two-Stage Dialing" procedure:

Step 8 Ensure that the outbound VOIP dial-peer that is used on the gateway for the initial call leg over to the remote destination (mobile phone) has DTMF-relay configuration in it, so the DTMF codes can get passed through to Cisco Unified Communications Manager.

Step 9 Configure dial-peers on the gateway that receives the second-stage inbound call to the Enterprise Feature Access DID, so the call gets forwarded to the Cisco Unified Communications Manager. Ensure that the VOIP dial-peer has the DTMF-relay configuration in it.

Note If a generic dial-peer is already configured to forward the calls to Cisco Unified Communications Manager and is consistent with the EFA DN, you do not need to perform this step. Ensure that the VOIP dial-peer for this call leg also has a configured DTMF-relay command.

Refer to the *Cisco Unified Communications Solution Reference Network Design (SRND) Based on Cisco Unified Communications Manager* for the list of steps that you need to configure Enterprise Feature Access.

Valid Characters in Name Field of Access List Configuration Window

In the *Cisco Unified Communications Manager Features and Services Guide*, be aware that the description for the Name field in the Access List Configuration window in the "Cisco Unified Mobility" chapter is incomplete. The complete description follows:

Enter a text name for the access list.

This name can comprise up to 50 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Valid Characters in Name and Description Fields of Remote Destination Profile Window

In the *Cisco Unified Communications Manager Features and Services Guide*, be aware that the description for the Name and Description fields on the Remote Destination Profile Configuration window in the "Cisco Unified Mobility" chapter is incomplete. The complete descriptions follow.

Name

Enter a text name for the remote destination profile.

This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.

Description

Enter a text description of the remote destination profile.

This field can comprise up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Valid Characters in Name Field of Geolocation Filter Configuration Window

In the *Cisco Unified Communications Manager Features and Services Guide*, be aware that the description for the Name field in the Geolocation Filter Configuration window in the "Geolocations and Location Conveyance" chapter is incomplete. The complete description follows:

Enter a unique name for this geolocation filter. Default name cannot be blank.

This field can contain up to 50 ASCII characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Valid Characters in Name Field of Geolocation Configuration Window

In the *Cisco Unified Communications Manager Features and Services Guide*, the description for the Name field in the Geolocation Configuration window in the "Geolocations and Location Conveyance" chapter is incomplete. The complete description follows:

Enter a unique name for this geolocation.

The name can contain up to 50 ASCII characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

IPv6 Chapter Incorrectly Describes How IPv6 Addresses Display in the Find and List Phones Window

The "Internet Protocol Version 6 (IPv6)" chapter in the *Cisco Unified Communications Manager Features and Services Guide* incorrectly describes how the IP address displays for an IPv6 Only phone in the Find and List Phones window in Cisco Unified Communications Manager Administration.

Incorrect Information

After you configure the phone in Cisco Unified Communications Manager Administration, you can view the IP address for the phone in the Find and List Phones window. For phones that have an IPv4 address only or both IPv4 and IPv6 addresses, the IPv4 address displays in the window; for phones that have an IPv6 address only, the IPv6 address displays in the window.

Correct Information

After you configure the phone in Cisco Unified Communications Manager Administration, you can view the IP address for the phone in the Find and List Phones window. For phones that have an IPv4 address only or both IPv4 and IPv6 addresses, the IPv4 address displays in the window. For phones with an IPv6 address only, the IP Address displays as 0.0.0.0 in the IP Address column in the Find and List Phones window. To identify the IPv6 address for the phone, click the **Device Name** link in the Find and List Phones window, which causes the Phone Configuration window to display. For the IPv6 Only device, the Phone Configuration window displays an IPv4 address of 0.0.0.0, listed as IP Address, above the IPv6 address.

Intercom Calls Cannot Be Placed on Hold

The Restrictions section of the "Intercom" chapter in the *Cisco Unified Communications Manager Features and Services Guide* incorrectly indicates that intercom calls can be placed on hold. Actually, the system does not allow intercom calls to be placed on hold.

IPv6 Chapter Does Not Contain Information on NTP Server

The "Internet Protocol Version 6 (IPv6)" chapter in the *Cisco Unified Communications Manager Features and Services Guide* does not contain the following information on NTP Servers and IPv6.

To avoid potential compatibility, accuracy, and network jitter problems, ensure that the external NTP servers that you specify for the primary node are NTP v4 (version 4). If you are using IPv6 addressing, ensure that the external NTP servers are NTP v4.

Cisco Unified Communications Manager Does Not Support Logical Partitioning for Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express Calls

Cisco Unified Communications Manager does not support the logical partitioning feature for calls that involve Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express.

The following document omits this limitation:

- book: *Cisco Unified Communications Manager Features and Services Guide, Release 7.1(2)*
  chapter: Logical Partitioning
  topic: Limitations

Mobile Voice Access Directory Number Field Description

In the "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide*, the description of the Mobile Voice Access Directory Number field on the Mobile Voice Access window omits the following information:

Enter a value between 1 and 24 digits in length. You may use the following characters: 0 to 9.

Cisco Unified Serviceability

This section contains information on documentation omissions, errors, and updates for Cisco Unified Serviceability.

Password Description Omitted

The Application Billing Server Parameter Settings table in "Configuring CDR Repository Manager" chapter of the Cisco Unified Communications Manager Serviceability Guide omits this information:

Password - Enter the password that is used to access the application billing server.

Cluster Service Activation Node Recommendations

The "Configuring Services" chapter in the *Cisco Unified Serviceability Administration Guide* does not include the following information that describes service activation recommendations for specific nodes in a cluster. Table 6 provides a general summary of the cluster activation recommendations for a feature service in these nodes: publisher, subscriber, TFTP, and MOH. For specific recommendations that are associated with activating a particular feature service, refer to the Cluster Service Activation Recommendations section in the "Configuring Services" chapter.

Table 6 Cluster Service Activation Node Recommendations

Feature Service	Publisher	Subscriber	TFTP	MOH	Comments
Cisco CallManager	Deactivated	**Activated**	Deactivated	Deactivated	
Cisco TFTP	Deactivated	Deactivated	**Activated**	Deactivated	
Cisco Messaging Interface	Deactivated	Deactivated	Deactivated	Deactivated	Do not activate this service if you plan to use Cisco Unity voice-messaging system.
Cisco Unified Mobile Voice Access Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use this application, activate this service on the first node only.
Cisco IP Voice Media Streaming App	Deactivated	Deactivated	Deactivated	**Activated**	Do not activate this service on the first node or on any nodes that run the Cisco CallManager service.
Cisco CTIManager	Deactivated	**Activated**	Deactivated	Deactivated	Activate this service on each subscriber node to which JTAPI/TAPI applications will connect.
Cisco Extension Mobility	Deactivated	**Optional**	Deactivated	Deactivated	If you use EM, activate this service on all subscriber nodes in the cluster.
Cisco Extended Functions	Deactivated	**Optional**	Deactivated	Deactivated	If you use extended functions, activate this service on one or more servers.
Cisco Dialed Number Analyzer	Deactivated	**Optional**	Deactivated	Deactivated	If you need DHCP service, activate this service on the node with the least amount of call-processing activity.
Cisco DHCP Monitor Service	Deactivated	Deactivated	Deactivated	Deactivated	Activate this service on the node that has DHCP enabled.

Table 6 Cluster Service Activation Node Recommendations (continued)

Feature Service	Publisher	Subscriber	TFTP	MOH	Comments
Cisco CallManager Attendant Console Server	Deactivated	**Optional**	Deactivated	Deactivated	To use Cisco Unified Communications Manager Attendant Console, activate this service on every subscriber node in the cluster that runs the Cisco CallManager service.
Cisco IP Manager Assistant	Deactivated	**Optional**	Deactivated	Deactivated	If you use IPMA, activate this service on any subscriber nodes (primary and backup - up to six servers for three pairs maximum) in the cluster.
Cisco Web Dialer Web Service	Deactivated	**Optional**	Deactivated	Deactivated	If you use Web Dialer, activate this service on one or more subscriber node(s).
Cisco SOAP-CDROnDemand Service	**Optional**	Deactivated	Deactivated	Deactivated	If you want to collect CDR files by using SOAP, activate the service on the first node only.
Cisco CAR Web Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use CAR, activate this service on the first node only.
Cisco AXL Web Service	**Optional**	Deactivated	Deactivated	Deactivated	If you need this service, activate the service on the first node only.
Cisco Bulk Provisioning Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use BAT, activate the service on the first node only.
Cisco TAPS Service	**Optional**	Deactivated	Deactivated	Deactivated	If you use TAPS, activate the service on the first node only.
Cisco Serviceability Reporter	**Activated**	Deactivated	Deactivated	Deactivated	Activate this service on the first node only.
Cisco CallManager SNMP Service	**Activated**	**Activated**	**Activated**	**Activated**	If you use SNMP, activate this service on all servers in the cluster (optional, but activation recommended).
Cisco CTL Provider	**Optional**	**Optional**	**Optional**	**Optional**	If you use CTL, activate this service on all servers in the cluster.
Cisco Certificate Authority Proxy Function (CAPF)	**Optional**	Deactivated	Deactivated	Deactivated	If you use CAPF, activate this service on the first node only.
Cisco DirSync	**Optional**	Deactivated	Deactivated	Deactivated	If you use DirSync, activate this service on the first node only.

Activated = activated at installation

Optional = activate only if the application is needed

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.