



Release Notes for Cisco Unified Mobility Advantage, Release 7.1(3), 7.0(2), and 7.0.1

Revised: December 20, 2010

To view the release notes for previous versions of Cisco Unified Mobility Advantage and for Cisco Mobile and Cisco Unified Mobile Communicator clients, go to:
http://www.cisco.com/en/US/products/ps7270/prod_release_notes_list.html.

Contents

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [Related Documentation, page 2](#)
- [New and Changed Information, page 2](#)
- [Installation and Upgrade Notes, page 4](#)
- [Limitations and Restrictions, page 7](#)
- [Important Notes, page 10](#)
- [Caveats, page 13](#)
- [Troubleshooting, page 16](#)
- [Documentation Updates, page 16](#)
- [Cryptographic Information, page 17](#)

Introduction

Cisco Unified Mobility Advantage is part of the Cisco Unified Communications family of products.

Cisco Unified Mobility Advantage and clients Cisco Mobile and Cisco Unified Mobile Communicator extend your enterprise tools to mobile devices.



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

Cisco Unified Mobility Advantage is deployed behind the enterprise firewall and serves as the integration point for all enterprise services.

System Requirements

For system requirements including supported mobile phone models and service providers, see the *Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator* at http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html.

Related Documentation

See the *Documentation Guide* for your release of Cisco Unified Mobility Advantage, Cisco Unified Mobile Communicator, and Cisco Mobile at http://www.cisco.com/en/US/products/ps7270/products_documentation_roadmaps_list.html.

Tips for Searching Cisco Documentation

We recommend using the external Google Search (<http://www.google.com>) to find information.

Use the following formula in the search field:

<product name> *<release number>* *<topic keywords>* **site:cisco.com**

Examples of Google Search entries:

- meetingplace 7.0 recording disk space site:cisco.com
- mobility advantage 7.0 compatibility matrix site:cisco.com
- presence 7.0 disaster recovery site:cisco.com

New and Changed Information

- [Cisco Unified Mobility Advantage Release 7.1\(3\), page 2](#)
- [Cisco Unified Mobility Advantage Release 7.0\(2\), page 3](#)

Cisco Unified Mobility Advantage Release 7.1(3)

Release 7.1(3) of Cisco Unified Mobility Advantage introduces the following new and changed functionality:

- Support for deployments without a Cisco Adaptive Security Appliance, if both of the following conditions are met:
 - Only Cisco Mobile for BlackBerry Release 7.1 clients are deployed
 - Clients connect through a BlackBerry Enterprise Server configured with MDS
- Support for Cisco Mobile for BlackBerry Release 7.1, comparable to Release 7.x clients on other devices, with the following differences:

- Both types of Dial Via Office (Forward and Reverse) are supported, via selection on the client. If the environment supports both types, the user chooses which to use.
- Call Me links to join Cisco Unified MeetingPlace meetings appear in the native BlackBerry calendar, not (within) a dedicated meeting list in the Cisco Mobile application.
- Support for the Cisco Mobile client for iPhone 3G, comparable to Cisco Unified Mobile Communicator on other devices, with the following differences:
 - Call me feature lets users click to join Cisco Unified MeetingPlace meetings (audio only) from the meeting list, from the iPhone native calendar, and from email notifications (whether sent direct or forwarded to the user or sent to a group mail alias that includes the user); Cisco Unified MeetingPlace calls the user.
 - Notifications of new missed calls and voice messages when the Cisco Mobile is not running.
 - Dial Via Office - Forward
 - No presence
 - No text messaging
 - The meeting list in Cisco Mobile clients covers two days, while the meeting list in older clients is determined as in previous releases by settings in the Meeting Services tab in the Admin portal.
- Microsoft Exchange is optional. See the resulting limitations in [Limitations and Restrictions, page 7](#).
- Bulk administration for activating and deactivating users and adding and deleting devices.
- Changed feature details for all clients:
 - All clients now receive meeting notifications for meetings scheduled via the Cisco Unified MeetingPlace web interface, in addition to those scheduled via the Cisco Unified MeetingPlace Outlook plug-in.
 - Voice messages marked “Private” are now displayed as private in BlackBerry and iPhone clients.

Cisco Unified Mobility Advantage Release 7.0(2)

This release introduces the following new features:

- Support for Cisco Unified Mobile Communicator Release 7.0 for Nokia Symbian phones. For details, see the Release Notes for this client at http://www.cisco.com/en/US/products/ps7270/prod_release_notes_list.html and the *Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator* at http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html.
- Support for a wider range of Windows Mobile phones. For details, see the *Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator* at http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html.
- Support for certain Cisco Media Convergence Servers series 7825. For details, see the *Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator* at http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html.
- When you configure connections to enterprise servers in Cisco Unified Mobility Advantage, a new “Test Config” button allows you to immediately verify that your entered values are valid.

- You can now specify the format in which phone numbers appear in your Active Directory, so that user call logs can identify phone numbers by name even if the numbers in Active Directory do not follow the North American Numbering Plan.
- On the Add/Remove User page, user IDs are now listed along with first and last names, allowing you to distinguish between identically-named users.

For new and changed information for the Windows Mobile client, see the *Release Notes for Cisco Unified Mobile Communicator for Windows Mobile Phones, Release 7.x* at http://www.cisco.com/en/US/products/ps7270/prod_release_notes_list.html.

For information about the features and benefits of the original 7.0(1) release, see the data sheet at http://www.cisco.com/en/US/products/ps7271/prod_literature.html.

Installation and Upgrade Notes

- [All Cisco Unified Mobility Advantage Installations and Upgrades, page 4](#)
- [Cisco Unified Mobility Advantage 7.1\(3\) Upgrades, page 6](#)
- [Cisco Unified Mobility Advantage Release 7.0\(2\), page 3](#)

All Cisco Unified Mobility Advantage Installations and Upgrades

- [Obtaining Software, page 4](#)
- [Joining the Installer ISO Files for Cisco Unified Mobility Advantage, page 4](#)

Obtaining Software

To order software and licenses, contact your Cisco sales representative or go to <http://www.cisco.com/en/US/ordering/index.shtml>.

To access the latest software updates for all versions of Cisco Unified Mobility Advantage, go to <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=281001413>.

Cisco Unified Mobile Communicator and Cisco Mobile client releases may occur independently of Cisco Unified Mobility Advantage server releases.

- For the latest Cisco Unified Mobile Communicator release, visit <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=281001428>.
- For the latest Cisco Mobile release, visit the Apple App Store using iTunes or the App Store application on the iPhone.

Joining the Installer ISO Files for Cisco Unified Mobility Advantage

Downloaded software images are non-bootable. They can be used only for upgrades.

To obtain a disk for new installations, you must order the software on DVD.

If you download the Cisco Unified Mobility Advantage installer from Cisco.com, the installer is split into two parts because of its size.

For example:

- Part 1: CUMA-UCSInstall_UCOS_7.0.2.10000-4.sgn.iso_part1of2
- Part 2: CUMA-UCSInstall_UCOS_7.0.2.10000-4.sgn.iso_part2of2

You must join these two parts before you can use the installer.

Procedure

- Step 1** Go to <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=281001413>.
- Step 2** Download both parts of the installer.
- Step 3** Make sure to view or download the ReadMe.
The ReadMe provides the name of the final joined file and the MD5 value that you will need to complete this process.
If you click Download Now, you see the ReadMe link.
If you add the parts to your Download Cart, click the name of one of the parts to see the ReadMe link.
- Step 4** Join the parts:

Platform	Procedure
Unix or Linux	<p>Enter the following command into the CLI:</p> <pre>cat Part1 Part2 > Product_Installer_version.sgn.iso</pre> <p>Using the example filenames above:</p> <pre>cat UCSInstall_UCOS_7.0.2.10000-4.sgn.iso_part1of2 UCSInstall_UCOS_7.0.2.10000-4.sgn.iso_part2of2 > UCSInstall_UCOS_7.0.2.10000-4.sgn.iso</pre>
Windows	<ol style="list-style-type: none"> 1. Select Start > Run. 2. Type cmd. 3. Select OK. 4. Enter the following command into the command prompt: <pre>COPY /B Part1+Part2 Product_Installer_version.sgn.iso</pre> <p>Using the example filenames above:</p> <pre>COPY /B UCSInstall_UCOS_7.0.2.10000-4.sgn.iso_part1of2+ UCSInstall_UCOS_7.0.2.10000-4.sgn.iso_part2of2 UCSInstall_UCOS_7.0.2.10000-4.sgn.iso</pre>

- Step 5** Remove any text that precedes **UCSInstall_UCOS** in the filename of the joined file.
For example, if the filename is **CUMA-UCSinstall_UCOS_7.1.3.10000-11.sgn.iso** change the name to **UCSinstall_UCOS_7.1.3.10000-11.sgn.iso**.
Make no other changes to the filename.
- Step 6** Use an MD5 checksum utility to verify that the MD5 sum of the final file matches the MD5 number specified in the ReadMe for your release.
For Unix or Linux, a checksum utility is part of the OpenSSL package.
For Windows, you can download a utility from the internet.

The MD5 number is provided in the ReadMe for your release.

Cisco Unified Mobility Advantage 7.1(3) Upgrades

- Upgrades to this release are supported from Cisco Unified Mobility Advantage Release 7.0(2) only.
- Before you begin the upgrade:
 - See [Rebooting MCS 7825-I2 Servers After October 1, 2009 Will Brick the Server](#), page 11.
 - Determine whether you need to leave I/O throttling enabled (to prevent the server from becoming overloaded during normal use and disrupting service or causing a core dump) or disable I/O throttling (to avoid extremely long upgrade times).

Follow instructions in the *Upgrading Cisco Unified Mobility Advantage* documentation module for Release 7.1(3) at

http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html.

- Changing the Hostname or IP address on the Cisco Unified Mobility Advantage server is not supported in this version as it will cause upgrades to fail. If you change it, you must contact Cisco technical support. See [Open Caveats in Cisco Unified Mobility Advantage](#), page 13.
- Changes to the Phone Number Format field in the Active Directory adapter in Cisco Unified Mobility Advantage may not be compatible with some configurations. Specifically, if a + appears in the incoming phone number when you call a desk phone from any phone number including an international number, you may need to change the existing Phone Number Format that you configured.
- See also the open caveats lists for the server and for any clients you will deploy.
- For additional important information about upgrades, see the documentation module on upgrading Cisco Unified Mobility Advantage at http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html.

Cisco Unified Mobility Advantage Release 7.0(2)

Cisco Unified Mobility Advantage Release 7.0(2) is available only as an upgrade from Release 7.0(1). For all new installations of Release 7.0(2), including installations on hardware that was not supported in Release 7.0(1), you must first install, configure, and successfully start Release 7.0(1), then upgrade.

For installation and upgrade instructions for system administrators, including instructions for upgrading client software, see the *Installation and Administration Guide for Cisco Unified Mobility Advantage, Release 7.0*.

For client installation instructions for users, see the user documentation at http://cisco.com/en/US/products/ps7271/products_user_guide_list.html.

Limitations and Restrictions

- (Release 7.1.3) In order to display Caller ID in call history on the client, you need to configure several things including the Phone Number Format field in the Active Directory adapter. However, that field can accommodate only one phone number format, so if your Active Directory database includes numbers in different formats, not all phone numbers may be identified by name in call history.
- (Release 7.1.3):
 - For deployments with Cisco Mobile for iPhone clients: Account credentials can contain only characters that are available on the iPhone keypad.
 - If caller ID is blocked for the iPhone, Dial via Office - Forward calls cannot be completed.
 - Because the Cisco Mobile client for iPhone is distributed via the Apple App Store, and the client for Verizon BREW phones is distributed by Verizon, rather than via Cisco Unified Mobility Advantage, references in the Admin Portal to “Application Version” for these clients appear as “Not Available.”
- (Release 7.1.3) If you deploy Cisco Unified Mobility Advantage without Microsoft Exchange, the following features will not be available:

Client	Feature
Cisco Mobile	<ul style="list-style-type: none"> • Meeting List • Call and voicemail identification for personal Exchange contacts
Release 7.0 clients	<ul style="list-style-type: none"> • Ability to derive availability status from the Exchange calendar of each user • Personal contacts from the Exchange contact list of each user • Call and voicemail identification by name for personal Exchange contacts • Meeting notifications
Release 3.x clients	<ul style="list-style-type: none"> • Ability to derive availability status from the Exchange calendar of each user • Personal contacts from the Exchange contact list of each user • Call and voicemail identification by name for personal Exchange contacts • Meeting notifications

- (Release 7.1.3) Cisco Mobile for BlackBerry clients can connect using your corporate WiFi. Your network and devices must be configured to provide this capability independently of Cisco Mobile.
- (Release 7.1.3) If the BlackBerry Mobile Voice System (MVS) client application is co-resident with Cisco Mobile for BlackBerry, you must disable the Dial via Office feature for all clients, or instruct Cisco Mobile for BlackBerry users not to use it.
- All Cisco Unified Mobility Advantage users must be configured on a single server in the Cisco Unified Communications Manager cluster.
- Cisco Unified Mobility Advantage does not support redundancy or clustering in this release.

- Applications that run continuously may reduce battery life. See the user docs for tips on battery conservation.
- To connect using corporate WiFi, clients that connect through the Cisco Adaptive Security Appliance must be able to connect to the external port of that appliance.
- Limitations and restrictions related to Presence:
 - Presence is not supported on Cisco Mobile for iPhone clients.
 - All Cisco Unified Mobility Advantage users must be on a single server in the Cisco Unified Presence cluster.
 - There can be only one Cisco Unified Mobility Advantage server for each Cisco Unified Presence sub-cluster.
 - Cisco Unified Presence and Cisco Unified Mobility Advantage must both be associated with the same Active Directory server.
 - If Cisco Unified Communications Manager is not integrated with the corporate Active Directory, Cisco Unified Mobility Advantage will be able to provide presence capabilities to users only if their user ID in Cisco Unified Communications Manager exactly matches their user ID in Active Directory.
 - Cisco Unified Mobile Communicator users cannot select Available to override an Idle status that occurs while Cisco Unified Personal Communicator is running.
 This ensures that other Cisco Unified Personal Communicator users do not mistakenly believe the user can receive instant messages in Cisco Unified Personal Communicator.
 - Cisco Unified Mobile Communicator does not support the LCS Federation feature in Cisco Unified Presence.
 - Contact groups are not supported in Cisco Unified Mobile Communicator. If a user adds a contact to Cisco Unified Mobile Communicator, the contact appears in the General group in Cisco Unified Personal Communicator.
 - Cisco Unified Mobile Communicator clients do not display "nickname" in Directory listings.
 - Directory searches search only Active Directory, not the Cisco Unified Presence directory.
 - Directory search results do not include presence information for contacts.
 - For upgrades from server Release 3.x, if Cisco Unified Presence is not deployed in Cisco Unified Mobility Advantage Release 7.x, Release 3.x clients will no longer have the Presence feature.
 - If you deploy multiple Cisco Unified Mobility Advantage servers and you also deploy Cisco Unified Presence, users of clients that support availability status may see availability status for users with whom they cannot exchange instant messages via Cisco Unified Mobile Communicator.
- Users cannot change contact information for Active Directory contacts.
- (Windows Mobile phones only) Service providers that have a signing requirement in addition to “Mobile2Market” currently cannot support the restriction of access to devices having specific IMEI numbers. These providers include, but are not limited to, Orange and SK Telecom.
- Numbers that cannot be dialed from user desk phones also cannot be dialed using Dial Via Office. For example, Cisco Unified Communications Manager does not support p’s and w’s (pauses and waits, respectively) in dialed numbers.
- When making Dial Via Office - Reverse Callback calls to an international alternate callback number, users must precede the country code with the international dialing prefix configured in Cisco Unified Communications Manager, not a plus (+), in the callback number.

- BlackBerry and Symbian devices running Cisco Unified Mobile Communicator Release 3.x can operate with this release, but new features are not supported on those devices. The following features are not supported on Release 3.x clients:
 - The ability to restrict access to a specific device.
 - The dial via office feature.
 - The ability to enable and disable the Mobile Connect feature via the device.
- Presence on Release 3.x clients differs slightly from presence on Cisco Unified Personal Communicator. For example:
 - In order to see presence updates of a contact on a Release 3.x client, that contact must also be a Cisco Unified Mobile Communicator or Cisco Mobile user.
 - Users can set their own presence only from the mobile client. Automatic or manual settings from other clients do not apply. However, if a user sets preferences in the User Portal to change availability status based on the meeting schedule of the user, the status of the user will update as specified.
 - Away, In a Meeting, and On the Phone statuses for other users appear in Release 3.x clients as Busy
 - Out of Office and offline statuses for other users appear in Release 3.x clients as Do Not Disturb.
- On some phones, it is not possible for the client to determine whether the GPRS wireless transmission capability of the phone is enabled. Therefore, some features may appear not to work, when in reality the phone is not connected to the wireless network.
- Cisco Unified Mobile Communicator does not verify that the device on which it is being installed is supported.
- Cisco Unified Mobile Communicator and Cisco Mobile clients support only one call at a time.
- Dial via office - Reverse Callback calls that are not successfully completed may produce the following unexpected result: The called person receives a call from the voice mail of the caller. This situation can occur when:
 - The caller tries to cancel the call.
 - The caller takes another call before the system callback occurs.
 - The caller does not answer a callback to an alternate number.
 - The caller is in an area with weak signal and the call back from the system is dropped.
 - The network is busy. (This situation is rare.)
- Some phone models may have one or more of the following limitations:
 - Extended characters may not be supported.
 - Voicemail audio output may not route to a connected headset, including Bluetooth headsets.
 - Minor look and feel issues.
 - The volume of some alert tones may not be adjustable.
- (Deployments with Microsoft Exchange 2007 only) Voice mail messages that should be marked as Urgent are marked as Normal.
- Text messaging is supported between Cisco Unified Mobility Advantage clients only. Also, if you deploy multiple Cisco Unified Mobility Advantage servers, users of clients that support text messaging who are configured on one server cannot exchange text messages with users configured on another server.

- For limitations and restrictions specific to Cisco Unified Mobile Communicator Release 7.0 for Nokia Symbian phones, see the Release Notes for that application at http://www.cisco.com/en/US/products/ps7270/prod_release_notes_list.html.

Limitations in Release 7.0(1) only:

- If telephone numbers in your Active Directory do not use the format (###) ###-####, then user call history will not identify phone numbers by name.

Important Notes

The following issues apply to all releases of Cisco Unified Mobility Advantage covered by this document, except as noted.

- [Requirement when Upgrading Cisco Unified Communications Manager, page 10](#)
- [\(Cisco Unified Mobility Advantage Release 7.1 Only\) APNS Certificate Expires on September 2, 2010, page 10](#)
- [Capacity, page 11](#)
- [Rebooting MCS 7825-I2 Servers After October 1, 2009 Will Brick the Server, page 11](#)
- [Per-User Changes to Enterprise Server Configurations, page 11](#)
- [How to Change the Admin Portal Password, page 11](#)
- [After a Cisco Unified Mobility Advantage Restart, Users Should Sign In As Soon As Possible, page 12](#)
- [Important Caveat When Upgrading Cisco Unified MeetingPlace, page 12](#)

Requirement when Upgrading Cisco Unified Communications Manager

Whenever a Cisco Unified Communications Manager cluster upgrade is performed, you must restart Cisco Unified Mobility Advantage. This ensures that Cisco Unified Mobility Advantage is in the right state to handle mobile client registrations.

(Cisco Unified Mobility Advantage Release 7.1 Only) APNS Certificate Expires on September 2, 2010

A valid Apple Push Notification Service (APNS) certificate is required to provide missed call and voicemail notification services to iPhone users of Cisco Unified Mobile Communicator (Cisco Mobile, Release 7.1) clients that connect to Cisco Unified Mobility Advantage servers, when the client is not running.

The certificate included with Cisco Unified Mobility Advantage expires on September 2, 2010. To avoid interruption in notification services, you must replace the expired certificate with a new one.

See instructions in *Uploading a New APNS Certificate to Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/prod_maintenance_guides_list.html.

Capacity

The capacity of a Cisco Unified Mobility Advantage server depends on the hardware. For details, see the hardware requirements section for your server release in the *Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator* at http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html.

If you deploy multiple Cisco Unified Mobility Advantage servers, each deployment is independent of the others.

Multiple Cisco Unified Mobility Advantage servers cannot be associated with a single Cisco Unified Communications Manager server.

Rebooting MCS 7825-I2 Servers After October 1, 2009 Will Brick the Server

A defect in the HostRAID BIOS 2106 (included with System BIOS version 1.42 and 1.43) on 7825-I2 Media Convergence Servers will prevent the server from booting successfully if the server is rebooted after October 1, 2009.

For complete information including a workaround for avoiding or recovering from this issue, see:

- Guest: <http://www.cisco.com/en/US/ts/fn/632/fn63255.html>
- Registered User: <http://www.cisco.com/en/US/customer/ts/fn/632/fn63255.html>

To download the Engineering Special to use with this workaround, visit: <http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281001413>.

Per-User Changes to Enterprise Server Configurations

Any time you change a configuration for any user in any of the enterprise servers that are integrated with Cisco Unified Mobility Advantage, the user must sign in again to the client.

(Release 7.1.3) For instructions on forcing the user to sign out, see the Security documentation module at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.

(Release 7.0.x) See the “Configuring and Managing Users and Their Devices in Cisco Unified Mobility Advantage” chapter in the *Installation and Administration Guide for Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.

How to Change the Admin Portal Password

- [Changing the Password from the Admin Portal, page 11](#)
- [Changing the Password Without the Current Admin Portal Password, page 12](#)

Changing the Password from the Admin Portal

If you are able to log into the Admin Portal, you can change the password from the Admin Portal.

Procedure

- Step 1** Sign in to the Admin Portal.
 - Step 2** Select the [+] beside **System Management**.
 - Step 3** Select **System Properties**.
 - Step 4** Enter the new password in the **Admin Password** and **Confirm Admin Password** fields.
 - Step 5** Select **Submit**.
 - Step 6** Restart Cisco Unified Mobility Advantage.
-

Changing the Password Without the Current Admin Portal Password

If you have forgotten the Admin Portal password but you know the platform administrator credentials, you can change the Admin Portal password from the command-line interface.

Procedure

- Step 1** Use SSH to access the Cisco Unified Mobility Advantage server using your platform administrator credentials.
 - Step 2** Enter the following command to reset the password:

```
set password cuma
```
 - Step 3** Enter the following command to restart Cisco Unified Mobility Advantage and activate the new password:

```
utils service restart CUMA Admin
```
-

After a Cisco Unified Mobility Advantage Restart, Users Should Sign In As Soon As Possible

After you restart Cisco Unified Mobility Advantage, users must sign in to the client as soon as possible in order to avoid missing items in Call History on the client.

Important Caveat When Upgrading Cisco Unified MeetingPlace

This issue applies only to Cisco Unified Mobility Advantage Release 7.1(3).

If you upgrade Cisco Unified MeetingPlace, be sure to back up all of the notification templates you will customize when configuring the meeting features, then restore those templates after the upgrade. For more information about preserving customizations to your notification templates, see the documentation for Cisco Unified MeetingPlace.

Caveats

- [Using Bug Toolkit, page 13](#)
- [Open Caveats in Cisco Unified Mobility Advantage, page 13](#)
- [Open Caveats in Related Products, page 14](#)
- [Resolved Caveats in Cisco Unified Mobility Advantage, page 15](#)
- [Closed Caveats, page 16](#)

Using Bug Toolkit

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of the following:

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

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

Before You Begin

To access Bug Toolkit, you need the following items:

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

Procedure

-
- | | |
|---------------|--|
| Step 1 | To access the Bug Toolkit, go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs . |
| Step 2 | Log in with your Cisco.com user ID and password. |
| Step 3 | To look for information about a specific problem, enter the bug ID number in the “Search for Bug ID” field, then click Go . |
-

For information about how to search for bugs, create saved searches, and create bug groups, click **Help** in the Bug Toolkit page.

Open Caveats in Cisco Unified Mobility Advantage

- [Open Caveats in Release 7.1\(3\), page 14](#)
- [Open Caveats in Release 7.0\(2\), page 14](#)

Open Caveats in Release 7.1(3)

You should be aware of the following issues in Cisco Unified Mobility Advantage. Check for Service Updates to see if fixes are available for these issues.

Table 1 Open Caveats for Cisco Unified Mobility Advantage

Identifier	Severity	Product	Component	Headline
CSCsq70236	3	uma-server	admin-portal	Error is displayed when tried to download created context
CSCsw36661	3	uma-server	core	sym - placed handset calls to registered users duplicated in calls view
CSCsx12096	3	uma-server	user-portal	Directory Contact search results limited to 1000 contacts with no indication
CSCtb87180	3	uma-server	core	DVO Service status error
CSCtc03794	3	uma-server	core	Critical BIOS Update for x306m-8849 / 7825-I2 - CUMA 7.1
CSCtd01995	3	uma-server	install	RIM - wrong server address in provisioning email
CSCtc01526	4	uma-server	installer	CUMA upgrade failed - 'A Cisco DB' process not running

Open Caveats in Release 7.0(2)

The caveats in [Table 2](#) describe possible unexpected behavior in this release. These caveats may also be open in previous releases. Bugs are listed in order of severity.

Table 2 Open Caveats for Cisco Unified Mobility Advantage

Identifier	Severity	Component	Headline
CSCsq70236	3	admin-portal	Error is displayed when tried to download created context
CSCsu48169	3	core	Managed server status inconsistent from admin portal and CUMA console
CSCsw36661	3	core	sym - placed handset calls to registered users duplicated in calls view
CSCsx12096	3	user-portal	Directory Contact search page truncates results with no indication

Open Caveats in Related Products

Open caveats in related products may impact this product. See open caveats for your release or model of the following products, as applicable:

- Cisco Unified Mobile Communicator
- Cisco Media Convergence Server
- Unified Communications Operating System

- Disaster Recovery System
- Cisco Unified Communications Manager
- Cisco Adaptive Security Appliance
- Cisco Unified Presence
- Cisco Unity
- Cisco Unity Connection
- Cisco Unified MeetingPlace

Resolved Caveats in Cisco Unified Mobility Advantage

- [Resolved Caveats in Release 7.1\(3\), page 15](#)
- [Resolved Caveats in Release 7.0\(2\), page 15](#)
- [Resolved Caveats for Client Releases, page 16](#)

Resolved Caveats in Release 7.1(3)

The following caveats were listed in the Release Notes for the previous release of Cisco Unified Mobility Advantage and have now been resolved.

Table 3 *Resolved Caveats for Cisco Unified Mobility Advantage*

Identifier	Severity	Product	Component	Headline
CSCsu48169	3	uma-server	core	Managed server status inconsistent from admin portal and CUMA console

Resolved Caveats in Release 7.0(2)

This section lists caveats that are resolved but that may have been open in previous releases.

Bugs are listed in order of severity and then in alphanumeric order by bug identifier. Because defect status continually changes, be aware that this document reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of resolved defects, access the Bug Toolkit (see the [“Using Bug Toolkit” section on page 13](#)).

Table 4 *Resolved Caveats for Cisco Unified Mobility Advantage, Release 7.0(2)*

Identifier	Severity	Component	Headline
CSCsk48708	3	core	CUMA sends authentication request frequently when password is configured
CSCso67882	3	admin-portal	CallControl app user password should accept special chars
CSCso72314	3	admin-portal	CTI password does not accept the '@' character
CSCsq33308	3	core	sym bc - cumc changes status back to meeting from any other statuses

Table 4 Resolved Caveats for Cisco Unified Mobility Advantage, Release 7.0(2)

Identifier	Severity	Component	Headline
CSCsr07790	3	admin-portal	CUCM credentials set to default after 3.0 to 7.0 Upgrade.
CSCsu93768	3	core	can't change status for self & not updated for watchers if CUP failover
CSCsu93775	3	core	Synchronization error when add contact after CUP failover
CSCsu93832	3	core	bc - no contacts sync with user portal after cup failover
CSCsu97943	3	admin-portal	CUMA server stopped unexpectedly

Resolved Caveats for Client Releases

Resolved caveats for client releases are listed in the release notes for the relevant devices at http://www.cisco.com/en/US/products/ps7270/prod_release_notes_list.html.

Closed Caveats

Cisco Unified Mobility Advantage Release 7.1(3) has no significant closed caveats.

Closed caveats specific to client releases are in the *Release Notes for Cisco Mobile* at http://www.cisco.com/en/US/products/ps7270/prod_release_notes_list.html.

Troubleshooting

Troubleshooting information for users is in the user documentation for each device type at http://www.cisco.com/en/US/products/ps7271/products_user_guide_list.html. Some tips may be in a general Troubleshooting section, while others may be located in the relevant topic.

For Cisco Unified Mobility Advantage, Release 7.1(3), tips for system administrators are in the *Troubleshooting* documentation module at http://www.cisco.com/en/US/products/ps7270/prod_troubleshooting_guides_list.html.

For Cisco Unified Mobility Advantage, Release 7.0, troubleshooting information for system administrators is in a chapter in the *Installation and Administration Guide* at http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html.

Documentation Updates

For the latest versions of all documentation for Cisco Unified Mobility Advantage, go to http://www.cisco.com/en/US/products/ps7270/tsd_products_support_series_home.html.

Mobile Identity Requirements (Dial Via Office Feature)

A phone number entered as a Mobile Identity cannot contain more than 15 digits.

If your deployment includes mobile devices with phone numbers having more than 15 digits (this may occur, for example, for phones that are based in another country, if a country code is required to dial out to those phones from Cisco Unified Communications Manager), you may need to set up application dial rules to route calls to a shorter version of that number. Then enter the shortened version of the number as the Mobile Identity phone number.

Cryptographic Information

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008-2010 Cisco Systems, Inc. All rights reserved.