Troubleshooting Cisco Unified Mobility Advantage

First Published: September 24, 2009

Last Modified: August 16, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: N/A

CONTENTS

CHAPTER 1

Troubleshooting Cisco Unified Mobility Advantage

Where To Start Troubleshooting

All problems.

Solution Try the following, which are applicable when troubleshooting many problems:

- Make sure that the client device is functioning and connecting to the network properly. See the troubleshooting section or Frequently Asked Questions (FAQ) information in the client documentation for users of the relevant device at http://www.cisco.com/en/US/products/ps7271/products_user_guide_list.html for a list of simple things to verify for all problems before doing anything else, if any.
- Try, or have the user try, any troubleshooting tactics for the particular problem in the client documentation for the relevant device.
- Select the Test Config button on each page for the relevant adapter in the Cisco Unified Mobility Advantage Admin Portal to check for configuration errors.
- If you are using a secure connection between Cisco Unified Mobility Advantage and the relevant enterprise server, try temporarily changing the Connection Type to TCP, Plain, or nonsecure in the Enterprise Adapter for that server, and on the relevant enterprise server for connections to Cisco Unified Mobility Advantage. Then stop and restart Cisco Unified Mobility Advantage. Do not forget to switch all settings on all servers back to secure connections after you have resolved the problem, if required.
- Change the Trust Policy to All Certificates in the Security Context associated with the enterprise server that provides the inoperative functionality, or upload a certificate from each affected server to the trust store in Cisco Unified Mobility Advantage. Then stop and restart the server (on the Server Controls page). (The Security Context associated with the Cisco Adaptive Security Appliance cannot be set to Trust All Certificates.)
- Check the security policy of the relevant enterprise server with which Cisco Unified Mobility Advantage connects, to be sure you have deployed the required certificate from Cisco Unified Mobility Advantage.
- Disable and then re-enable the problem feature in the Admin Portal: Select **Enterprise Configuration > Manage Adapter Services**, then select the tab for the enterprise server that provides the feature. Disable the feature, then select **Submit**. See the bottom of the portal page to see whether you must stop and start the server before your change takes effect. Then enable the feature and select Submit. Again, stop and then restart the server if necessary.
- Check the Cisco Unified Mobility Advantage log files for errors. To find relevant information in the logs, search for "exception" until you find one with a keyword that may be related to the problem you are experiencing. For example, for problems with presence, look for an exception with CUP (Cisco Unified Presence).
- Make sure that the date and time are synchronized on all servers and mobile devices. If you did not specify a Network Time Protocol server during Cisco Unified Mobility Advantage installation, do so now. In the Unified Communications Operating System Administration pages, select **Settings > NTP servers**. See the online Help in the Unified Communications Operating System Administration pages for more information.
- Revisit configurations in both the relevant enterprise server and in Cisco Unified Mobility Advantage and re-enter the configuration settings. Then stop and restart Cisco Unified Mobility Advantage. A typing error or entry mismatch will cause features to fail. Configuration requirements for each feature are listed in the feature configuration modules.

"Lost Communication" Warning During Upgrade

The following warning appears during upgrade: The application has lost communication with the system. Check the status using CLI.

Solution Ignore this warning. The upgrade will continue. This warning appears iIf an L2 upgrade runs for more than 90 minutes. To see the upgrade status, sign in again to the OS Admin page and assume control.

Cisco Unified Mobility Advantage (Managed Server Service) Will Not Start

Cisco Unified Mobility Advantage (the Managed Server service) will not start.

Solution Try the following:

- Verify that your DNS server can resolve the Proxy Host Name you entered in the Admin Portal under System Management > Network Properties.

  To determine whether this is the problem, enter the command "file get cuma cuma.log" from the command-line interface to transfer the cuma.log file to an SFTP server. An error at startup usually appears as a cascading Java exception block.

- Click the Test Config buttons for each adapter page and correct any errors.

How To Solve Connection Problems

No Connectivity On Initial Tests

You are testing your initial configuration, but connections are not successful.

Solution Check the following:

- Make sure that the client device is functioning and connecting properly to the data network of the mobile service provider. See the relevant troubleshooting section or FAQ in the client documentation for the particular device for a list of simple things to verify for all problems before doing anything else.
- Make sure the mobile device has a consistently strong signal.
- In the Cisco Unified Mobility Advantage Admin Portal, verify:

  –**Enforce Device ID Check** is **False** or

  –(For each user of a Release 7.x client) **Allow Any Device** is **True** or you have entered an IMEI or ESN or UDID number.

  –(For each user of a Release 3.x client) **Allow Any Device** is **True**.

- Make sure you have installed a supported certificate on the Cisco Adaptive Security Appliance. See the Certificate Requirements section in the *Compatibility Matrix* at http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html.

- Check the following configurations. Cisco Adaptive Security Appliance configuration errors are a likely source of connection problems. The source of connection problems can be between the Cisco Adaptive Security Appliance and the Cisco Unified Mobility Advantage server as well as between the client and the Cisco Adaptive Security Appliance.
  - Ping the private IP address of the Cisco Unified Mobility Advantage server from the Cisco Adaptive Security Appliance.

    If the ping is unsuccessful, enter the command traceroute <private IP address of the Cisco Unified Mobility Advantage server> source inside and make sure the first hop is your default router.

    If the first hop is not your default router:

    - Check your configuration for the inside interface
    - Make sure your access list allows traffic through the inside interface

  - Ping an IP address on the internet from the Cisco Adaptive Security Appliance. The Cisco Adaptive Security Appliance must be able to reply to the client.

    If unsuccessful, check your configuration for the outside interface.

  - Ping the Cisco Adaptive Security Appliance from your Cisco Unified Mobility Advantage server and correct any problems.
- Check the BlackBerry Enterprise Server.
- Verify that the licensing on your Cisco Adaptive Security Appliance is correct. If not, contact your account representative.

Certificate Errors

Certificate error on client such as "Invalid certificate".

Solution Try the following:

- Make sure the client is connecting to the external interface of the Cisco Adaptive Security Appliance, not the internal address. A Wi-Fi connection to the corporate network connects to the internal address.
- Check all configurations on the Cisco Adaptive Security Appliance as described in the documentation, including interfaces.
- Check the Cisco Adaptive Security Appliance-to-client certificate.
- Check the Cisco Adaptive Security Appliance to Cisco Unified Mobility Advantage certificate, as well as the Security Context in Cisco Unified Mobility Advantage that you assigned in the Network Properties page.
- The OU on the signed certificate must match the Department value in the Security Context that you select on the Network Properties page.
- Check for firewall, routing, and other networking issues upstream of your Cisco Unified Mobility Advantage deployment.

Some Clients Cannot Connect on Initial Tests

Some clients are unable to connect.

Solution Try the following:

- In the Cisco Unified Mobility Advantage Admin Portal, check the following:

  –Enforce Device ID Check is False or

  –(For each user of a Release 7.x client) **Allow Any Device** is **True** or you have entered an IMEI or ESN or UDID number.

  –(For each user of a Release 3.x client) **Allow Any Device** is **True**.

  Reprovision the device after making any change.

- Make sure your Cisco Adaptive Security Appliance has the licenses you need to support the number of client connections. You should have obtained these licenses when you purchased Cisco Unified Mobility Advantage.
- Check the following using the Cisco Adaptive Security Appliance command line interface:

To	Use This Command in the Cisco Adaptive Security Appliance
Check the Maximum tls-proxy sessions set	sh tls-proxy
Set a new maximum number of connections	tls-proxy maximum-sessions <number>

Frequent Disconnects

Clients are unable to maintain connection to the server.

Solution Check to see if there is a new .oar file.

How to Solve Problems with Activation, Download, and Provisioning

User Activation Unsuccessful

User activation and deactivation are not working.

Solution Try the following:

- Check the cuma.log file for problems connecting to LDAP (Active Directory) as Admin.
- Make sure that your Admin user DN and Password are correct.

- If you configured your Active Directory adapter to Follow Referrals, make sure the DNS hostnames of all cascaded Active Directory servers are resolvable.
- Check other settings, for example the Key field, in the Advanced Settings page in the Enterprise Adapter for Active Directory.

  When you check the Active Directory adapter configurations in the Cisco Unified Mobility Advantage Admin Portal, be sure to select the **Test Config** button on each page.
- See if you can access LDAP with your credentials using a freeware LDAP browser such as the one described in the following topic.

Making Sure Your Active Directory Credentials Work

These instructions tell you how to obtain and use one available freeware LDAP browser to verify that your Active Directory credentials work. You can use other tools for this purpose if you prefer.

Procedure

Step 1 Get the browser from http://www-unix.mcs.anl.gov/~gawor/ldap/.

Step 2 Enter information into the LDAP browser:

Tab	Parameter	Value
Name	Name	Any value.
Connection	Host	IP address or domain name of your Active Directory server, as entered into the Active Directory configuration in the Cisco Unified Mobility Advantage Admin Portal.
	Anonymous Bind	Uncheck this option.
	Append Base DN	Check this option.
	User DN	Admin User DN that you entered in the Active Directory configuration in the Cisco Unified Mobility Advantage Admin Portal.
	Password	Password for the Admin User.

Step 3 Select **Fetch DNs**.

Step 4 Select **Save**.

If you cannot connect and view the Active Directory structure, there is a problem with your access credentials.

Cannot Find User to Activate

I am trying to activate users but some users are unexpectedly not found in Active Directory or missing from the list of search results.

Solution Try the following:

- Try searching for just the first name or just the last name. For example, try this when searching for a user whose first name includes two names.
- Make sure that you have entered the correct Filter Criteria and Search Base into the Advanced Settings of the Active Directory configuration.
- Users whose configurations in Active Directory are missing required information do not appear in Cisco Unified Mobility Advantage. Make sure the information for the user in Active Directory includes the first and last name, user ID, email address, and Distinguished Name attributes (or their equivalents as specified in the Active Directory adapter configuration in Cisco Unified Mobility Advantage).
- Only 1000 user IDs can be fetched from Active Directory.

Searching Active Directory from User Activation/Deactivation Page Results in Errors

Searching AD from the User Activation/Deactivation page spins forever, and the logs show socket timeout exceptions.

Solution Do a dnslookup on the top level domain, and make sure that all resulting servers on the list are listening on port 389. Telnetting to this top level domain on port 389 will also fail. Remove the offending server from the DNS list and stop and restart Cisco Unified Mobility Advantage.

Desired Add Phone Option is Unavailable

The option you or a user want to choose when adding a phone is not available.

Solution Make sure you have selected the desired option in **Handset Platform Management > Provisioning Management**.

Problems with Bulk Activation

If you experience problems with bulk activation, check the following:

Solution

- Determine whether all required macros are active in the template. You should see drop-down lists when you click a cell in each of these columns: Allow Any Device, Country Name, Provider Name, and Phone Model.

  In order to activate all macros, you may need to enable Excel to allow ALL macros; merely allowing macros in the template spreadsheet may not enable all macros. See the documentation for your version

of Excel for information about enabling macros. When you are finished working in the template, be sure to reset the macro security to a safer option.

- Make sure you can successfully add problem users and devices individually.

All Users Unable to Download Client Software

All users of Nokia Symbian and Windows Mobile phones cannot download the client software to their mobile devices.

Solution

- Verify the server address and port in the Admin Portal in System Management > Network Properties. These must match the IP addresses and ports configured in the Cisco Adaptive Security Appliance.
- See if this is a firewall issue: Verify that you can telnet to the host and port listed in the provisioning message. Use Telnet, not a PC-based web browser.

Some Users Unable to Download Client Software

Some users cannot download the client software to their mobile devices.

Solution

- Have the user try any troubleshooting tips for installation issues in the documentation for users.
- Check settings for that user in the Admin Portal in **End Users > Search Maintenance**. Also select the **Info** button on that page to make sure that the phone information is correct.

Provision Client Gives Error

Connection errors while provisioning the client. Download was successful.

Solution

- Have the user try the solutions in the Troubleshooting section of the user documentation for the relevant device, if any. For example, check for a strong, consistent connection to the mobile service provider data network.
- (For each user of a Release 7.x client) Make sure that the IMEI or ESN or UDID number is entered correctly in the **Device Identity Maintenance** tab for the user, or set **Allow Any Device** to **True**, then attempt to reprovision.
- (For each user of a Release 3.x client) Set **Allow Any Device** to **True**, then attempt to reprovision.
- This problem can occur with mobile device service providers that have a signing requirement in addition to "Mobile2Market" for Windows Mobile Standard Edition devices. These providers include, but are not limited to, Orange and South Korea Telecom. Set **Allow Any Device** to **True** in the Device Identity Maintenance tab for the user.

BlackBerry or iPhone Provisioning or Alert Messages Not Received

BlackBerry or iPhone users do not receive provisioning or alert messages.

Solution These messages are sent by email. Users must configure Microsoft Outlook to ensure that Cisco Unified Mobility Advantage alerts are sent to their iPhone or BlackBerry device instead of to the "Junk E-mail" folder in Outlook.

Give users the following information:

- The Admin email address in **System Management > SMTP Server Configuration**.
- Instructions for configuring Outlook so that it does not treat provisioning messages as Junk Mail. See the following procedure.

Configuring Microsoft Outlook to Properly Handle Provisioning Email Messages

Ensure that Outlook does not treat provisioning messages as Junk Mail.

Procedure

Step 1 Sign in to Microsoft Outlook on your computer.
Step 2 Select **Tools > Options**.
Step 3 Select **Preferences**.
Step 4 Select **Junk e-mail**
Step 5 Select **Safe Senders**.
Step 6 Select **Add**.
Step 7 Enter the email address that your Administrator gave you.
Step 8 Select **OK**.
Step 9 Select **OK** again.
Step 10 Continue to check the Junk mailbox; if necessary, disable junk-mail blocking during provisioning.

Need to Change Admin Portal Password

Problem I need to change the Admin Portal password.

Solution See either of the following related topics, depending on your situation:

Changing the Password from the Admin Portal

If you are able to sign in to 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

How to Solve Problems Logging In to Client or User Portal

User Cannot Sign In

User credentials are not valid.

Solution Make sure to update Cisco Unified Mobility Advantage with any changes to the Organizational Unit.

Users Receive Security Warning When Accessing the User Portal

When users access the User Portal, they see a security alert that there is a problem with the security certificate. They can enter the portal, however.

Solution Obtain and deploy a signed certificate for the Cisco Unified Mobility Advantage server. See the Security documentation module for this release.

How to Solve Problems with Call History

No Call History for Any or Many Users

Call log monitoring is not working at all, or is not working for many users.

Solution

Note After making any configuration changes in either Cisco Unified Communications Manager or Cisco Unified Mobility Advantage, and before testing each change on a mobile device, do the following:

- Restart Cisco Unified Mobility Advantage.
- Have the user sign out of Cisco Unified Mobile Communicator and then log back in.

- Make sure **Enable Corporate PBX integration** is set to **Yes** in the Manage Adapter Services > Call Control Service page.
- If you change a CTI user ID and password in Cisco Unified Communications Manager, then you must change the corresponding CTI user ID and password in the Enterprise Adapter for Cisco Unified Communications Manager in Cisco Unified Mobility Advantage. Stop Cisco Unified Mobility Advantage before making this change, or your change will not be saved.

  If you make changes to your Cisco Unified Communications Manager configuration, check the Cisco Unified Communications Manager adapter configurations in the Cisco Unified Mobility Advantage Admin Portal by selecting the **Test Config** button at the bottom of the page to be sure you have entered the changes correctly.
- Check the Cisco Unified Communications Manager adapter configurations in the Cisco Unified Mobility Advantage Admin Portal by selecting the **Test Config** button at the bottom of the adapter page.
- Carefully revisit the Configuring Features documentation for Call History monitoring. Step through the configurations again and check for errors. Be sure not to overlook any Before You Begin or What To Do Next sections in the procedures.

No Call History for One User

No call logs appear for one or a few users.

Solution

Make sure that you have added the desk phone to the Controlled Devices list for one of the CTI-enabled accounts in Cisco Unified Communications Manager. Then deactivate the user in Cisco Unified Mobility Advantage and activate the user again.

Note that if the user has a shared line configured, for example a physical desk phone and a configured and working installation of Cisco IP Communicator soft phone, and both have the same directory number, then call history should work if either of the two phones is registered with Cisco Unified Communications Manager.

Native Call History Shows Dial Via Office Calls As Incoming

Dial via Office - Reverse Callback calls appear as incoming calls in the native call history on the mobile device.

Solution This is inherent in the way the feature works. Cisco Unified Communications Manager calls the mobile device as well as the number dialed, then connects the two calls.

iPhone Users Do Not Receive Notifications of New Missed Calls When Cisco Mobile is Not Running

iPhone users are unable to receive notifications of new missed calls and voice messages when Cisco Mobile is not running.

Solution

- Have users check their settings on the client. For more information, see the user documentation for Cisco Mobile at http://cisco.com/en/US/products/ps7271/products_user_guide_list.html.
- These notifications require a valid Apple Push Notification Service (APNS) certificate. The certificate that shipped with Cisco Unified Mobility Advantage expires on September 2, 2010. To obtain the new certificate from Cisco, see *Uploading a New APNS Certificate to Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/prod_maintenance_guides_list.html.
- Make sure you have not deleted or modified the APNS security context (the context name will include **apns**).

  If you need to recreate this security context, see *Uploading a New APNS Certificate to Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/prod_maintenance_guides_list.html.
- Check the user account in **End Users > Search/Maintenance** and make sure the phone was added as an iPhone.
- See the prerequisites and required configuration in the "Providing Missed Call and Voicemail Notifications for iPhone Clients" topic in the *Deploying Clients* documentation module for this release at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.

Calls Missing from Call History

Calls are missing from the call history in Cisco Unified Mobile Communicator.

Solution Check the following:

- When you restart Cisco Unified Mobility Advantage, you must have all users sign in to the client as soon as possible after the restart in order to avoid interruptions in the call history.
- Have the user check the troubleshooting section of the user documentation for Cisco Unified Mobile Communicator for their device.

- If you are using Cisco Unified Communications Manager Release 4.x, make sure that you have identified the correct Active Directory attribute for Work Phone in the Advanced Settings tab of the Active Directory adapter configuration. This value must be unique for each person configured in Active Directory.
- See whether the expiry time in Manage Adapter Services > Call Control Service affects the missing messages.

Incorrect Call Time in Call History

Calls in call history do not display the correct call time.

Solution Make sure your Cisco Unified Mobility Advantage server and your Microsoft Exchange server are synchronized. Cisco strongly recommends using a Network Time Protocol (NTP) server. See the *Cisco Unified Communications Operating System Administration Guide For Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.

Call History Shows Error Status

Call history shows Error status.

Solution

The primary Primary DN for the user must be configured in Cisco Unified Communications Manager, connected, registered, and able to dial and receive internal and external calls.

If you make changes to achieve these requirements, have the user sign out of the client and sign in again.

Call History Does Not Identify Calls by Name

Only the number, not the name of the caller (or called person) appears in the call history. The call should be identified by name.

Solution

- The following are common configuration omissions:
  - Directory Lookup rules names for this purpose must start with indir_ or outdir_ for incoming and outgoing calls respectively.
  - Prioritize the list of Directory Rules so that a rule is not missed because a number matches a different rule first. Put the most restrictive rules first, least restrictive last.
  - Changes to Directory Lookup rules do not take effect until you restart Cisco Unified Mobility Advantage.
- If the unidentified number is for a newly added contact:

  Make sure your Cisco Unified Mobility Advantage server and your Microsoft Exchange server are synchronized. Cisco strongly recommends using a Network Time Protocol (NTP) server. See the *Cisco Unified Communications Operating System Administration Guide For Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.

- Make sure that the phone number format of the numbers that Cisco Unified Mobility Advantage is searching for matches the phone number format of the directories being searched. You specified transformations for this purpose in several places:
  - The indir_ and outdir_ rules you configured in the Directory Lookup settings.

    If you have a Cisco Unified Communications Manager release greater than Release 4.x, you specified these rules in Cisco Unified Communications Manager.

    If you have Cisco Unified Communications Manager Release 4.x, you specified these rules in Cisco Unified Mobility Advantage, in the Cisco Unified Communications Manager adapter, in the Directory Lookup tab.
  - The pattern you entered for the Phone Number Format in the Active Directory adapter.

    Cisco Unified Mobility Advantage uses this pattern to transform numbers when searching for matches in the home phone, mobile phone and business phone numbers in Active Directory. If you change the Phone Number Format, restart Cisco Unified Mobility Advantage in **Server Controls > Cisco > Control Server**.
- See if the unidentified number is the gateway number. In some companies, the gateway is configured to pass the gateway number in place of Caller ID when Caller ID is blocked, for emergency response purposes.

Calls in History List Cannot Be Dialed Direct From Mobile Device

Problem Calls listed in the Call History should be dialable directly from the mobile device but they are not.

Solution

Check your Directory Lookup rules. Common configuration omissions include the following:

- Directory Lookup rules names for this purpose must start with indir_ or outdir_ for incoming and outgoing calls respectively.
- Prioritize the list of Directory Rules so that a rule is not missed because a number matches a different rule first. Put the most restrictive rules first, least restrictive last.
- Changes to Directory Lookup rules do not take effect until you restart Cisco Unified Mobility Advantage.

See also other troubleshooting topics related to call history.

How to Solve Problems With Dial Via Office

Dial Via Office is Not Working For All or Many Users

Dial Via Office (Reverse Callback and Forward types) is not working for all or many users.

Solution Try the following:

Note After making any configuration changes in either Cisco Unified Communications Manager or Cisco Unified Mobility Advantage, and before testing each change, do the following:

- Restart Cisco Unified Mobility Advantage.
- Have the user sign out of the client and then sign in again.

- Check the Cisco Unified Communications Manager adapter configurations in the Cisco Unified Mobility Advantage Admin Portal by selecting the **Test Config** button at the bottom of the adapter page.
- Verify that the MobileConnect feature is working correctly independently of Cisco Unified Mobility Advantage. This ensures that Cisco Unified Communications Manager can reach the device, based on the configured mobility identity number and the rerouting calling search space on the device configuration page.
- Make sure you have correctly configured the Calling Search Space, Reroute Calling Search Space, and Device Pool settings on the system, and that you have assigned the correct values for each to your Handoff Number and Enterprise Feature Access Directory Number partition configurations, and to each Cisco Unified Mobile Communicator device (including iPhones).
- Try disabling secure connections between Cisco Unified Communications Manager and Cisco Unified Mobility Advantage by temporarily setting the transport type to a nonsecure type on each server. If the problem is resolved, revisit your server security configurations.
- Carefully revisit all information and procedures required to configure this feature. Step through the configurations again and check for errors. Be sure not to overlook any Before You Begin or What To Do Next sections in the procedures.
- Make sure calls to the Enterprise Feature Access Directory Number are routed properly.
- If you change the cluster security mode in Cisco Unified Communications Manager to mixed mode, you must restart Cisco Unified Communications Manager to re-enable the dial-via-office feature.
- Dial a problem number to and from your desk phone to ensure that those calls are routable.
- Username and password must be the same on Active Directory and Cisco Unified Communications Manager.
- The phone number entered for the Mobility Identity in Cisco Unified Communications Manager must exactly match the phone number entered into Cisco Unified Mobility Advantage, including number of digits, prefixes, etc.

Dial Via Office is Not Working For One or More Users

Dial Via Office is not working for one user, or for users at particular locations or having particular mobile phone service providers.

Solution

- Make sure the mobile device has a strong signal.
- There may be a networking issue with the local GSM mobile data connection leading to timeouts (Reverse Callback type only).
- Have the user check the Dial via Office settings in the client, including the **Callback To** number.
- Have the user sign out of the client and then sign in again.
- The Primary DN (usually the desk phone) must be connected and working properly.
- Confirm that the user is associated with the line (the Cisco Unified Mobile Communicator device)
- Make sure you have configured the Cisco Unified Mobile Communicator device such that it is in the correct Calling Search Space for Mobile Connect to work. If Mobile Connect does not work, Dial Via Office will not work.
- All Cisco Unified Mobile Communicator devices must be in the same Device Pool as the Cisco Unified Communications Manager server.
- Make sure you have assigned the correct Calling Search Space and Reroute Calling Search space to the device.
- Make sure the Mobility Identity phone number entered into Cisco Unified Communications Manager:
  - Is identical to the phone number entered into Cisco Unified Mobility Advantage, including number of digits, prefixes, etc.
  - Is unique in the system. If this number is assigned to a Remote Destination, delete the Remote Destination.
- Try using Dial Via Office to dial an internal number using the extension.
- Try using Dial Via Office to dial an external number (7 digits and 10 digits).
- If nothing else works, reset Cisco Unified Mobile Communicator in the Cisco Unified Communications Manager User Options web page: Select **User Options > Device**, then select your mobile device for **Device Name**. Select **Reset**. (This will not erase any data in Cisco Unified Mobile Communicator.)

Dial Via Office - Forward Is Unsuccessful for All Users

Users are unable to make calls using Dial Via Office.

Solution

- Use the **Test Config** button in the Cisco Unified Communications Manager adapter in the Admin portal.
- Make sure the Cisco Unified Communications Manager version is specified as 7.1+ in the adapter.
- Check your system-level configurations in Cisco Unified Communications Manager:
  - Ensure that you have correctly configured the **Number of Digits for Caller ID Partial Match** in Cisco Unified Communications Manager so that the Caller ID of incoming calls from Cisco Unified Mobile Communicator clients matches the Mobility Identity configured for each user.
  - Check for “typos” (data entry errors) in the Dial via Office Service Access Number or Enterprise Feature Access Directory Number.

- Make sure your gateway is configured to correctly route Dial via Office Service Access Number calls to the Enterprise Feature Access Directory Number.
- Validate the DID number on the voice gateway from the client. The user must be enabled for mobile voice access.
- Check the troubleshooting tips for Dial Via Office - Reverse Callback. Configurations for that feature area also required for Dial Via Office - Forward.

- Step carefully through the information and configurations described in the documentation module for configuring Dial Via Office. Pay special attention to the information that precedes and follows procedures within a topic, to the descriptions in the tables in the procedures, and to details in topics that do not include procedures.
- After making any changes, have the user sign out of the client and then sign in again.

Dial Via Office - Forward Is Unsuccessful for One or More Users

One or more users is unable to make calls using Dial Via Office, but some users can make Dial Via Office calls.

Solution

- Have the user check the connection status in the client (in Settings > General > Connection Status.)
- Verify that the data connection is active on the phone.
- Verify that the user has set required settings on the client and performed any troubleshooting steps in the user documentation. See the user documentation for details.
- Verify that the user has not blocked caller ID for their outgoing calls. The system must be able to identify the calling number.
- Check troubleshooting tips for Dial Via Office - Reverse. The configurations for that feature are also required for this feature.
- In Cisco Unified Communications Manager:
  - Make sure the correct Date/Time Group is associated with the Device Pool that is associated with the Cisco Unified Mobile Communicator device.
  - Make sure the Mobility Identity configured for the user in Cisco Unified Communications Manager exactly matches the Caller ID that you see when the user calls a desk phone. If these values do not match exactly, configure Cisco Unified Communications Manager to accept a partial match. For details, see the documentation module for configuring the Dial Via Office feature.
  - Carefully review the per-user and per-device requirements, restrictions, and configurations in the documentation module for configuring the Dial Via Office feature. Pay special attention to topics without procedures, to information preceding and following procedures, and to descriptions in tables in procedures.
- After making any changes, have the user sign out of the client and then sign in again.

How to Solve Voicemail Problems

Users Cannot Access Voicemail

Users cannot access voicemail.

Solution

- If user credentials for voicemail are different from user credentials for signing in to the client, make sure users enter their voicemail credentials into the User Portal.
- Verify that IMAP is enabled for the user in Microsoft Exchange (for Cisco Unity) or in Cisco Unity Connection.
- Check the voicemail adapter configurations in the Cisco Unified Mobility Advantage Admin Portal by selecting the **Test Config** button at the bottom of the Basic Settings page.

  If you find problems, see the feature configuration documentation for voicemail for this release.
- Make sure your system uses the supported transcoding protocols. See the Compatibility Matrix at http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html.
- Have users sign out and sign in to Cisco Unified Mobile Communicator again after you make any changes

Users are Unable to Receive New Voice Messages While Signed In

Users can retrieve new voice messages only upon signing in to the iPhone client or Cisco Unified Mobile Communicator. The do not receive voice messages after they sign in, while the client is running.

Solution Make sure your Cisco Unified Mobility Advantage server and your Microsoft Exchange server are synchronized. Cisco strongly recommends using a Network Time Protocol (NTP) server. See the *Cisco Unified Communications Operating System Administration Guide For Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.

iPhone Users Do Not Receive Voicemail Notifications When Cisco Mobile is Not Running

iPhone users are unable to receive notifications of new missed calls and voice messages when Cisco Mobile is not running.

Solution

- Have users check their settings on the client. For more information, see the user documentation for Cisco Mobile at http://cisco.com/en/US/products/ps7271/products_user_guide_list.html.
- These notifications require a valid Apple Push Notification Service (APNS) certificate. The certificate that shipped with Cisco Unified Mobility Advantage expires on September 2, 2010. To obtain the new certificate from Cisco, see *Uploading a New APNS Certificate to Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/prod_maintenance_guides_list.html.

- Make sure you have not deleted or modified the APNS security context (the context name will include **apns**).

  If you need to recreate this security context, see *Uploading a New APNS Certificate to Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/prod_maintenance_guides_list.html.
- Check the user account in **End Users > Search/Maintenance** and make sure the phone was added as an iPhone.
- See the prerequisites and required configuration in the "Providing Missed Call and Voicemail Notifications for iPhone Clients" topic in the *Deploying Clients* documentation module for this release at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.

Unable to Access Voicemail Using DTMF

Entering the DTMF code to access voicemail does not route the call properly.

Solution Make sure that all DTMF access codes are unique in Cisco Unified Communications Manager.

Error On Accessing Voicemail

Error: "Unauthorized" when accessing voicemail.

Solution

- Check Cisco Unity or Cisco Unity Connection and see if the account has been locked as a result of too many incorrect sign-in attempts.
- If voicemail credentials differ from Active Directory credentials, make sure the user entered username and password correctly in the User Portal as well as in the client settings.

Missing Voice Messages

User sees some voice messages in Outlook that do not appear on Cisco Unified Mobile Communicator.

Solution

- The messages may be older than the expiry period configured in Cisco Unified Mobility Advantage in the Manage Adapter Services for the voicemail adapter.
- See if calls to the desk phone number are being sent to the native voicemail of the mobile device. If so, see Calls to Desk Phone Number Go to Mobile Voicemail Instead of Corporate Voicemail

Some Users Do Not Receive Voice Messages

Some users receive voice messages but others do not.

Solution

- Make sure that the users are signed in to Cisco Unified Mobile Communicator.

- If the company has more than one voicemail or Exchange server, you must create an enterprise adapter for each.
- If client credentials differ from voicemail credentials, make sure that users have entered the voicemail credentials in the settings on the client or in the User Portal.

Calls to Desk Phone Number Go to Mobile Voicemail Instead of Corporate Voicemail

Calls to the desk phone number go to the native voice mailbox of the mobile device instead of to the voice mailbox of the desk phone number.

Solution

In Cisco Unified Communications Manager, select **Device > Phone**, locate the Cisco Unified Mobile Communicator device for the user, select either link in the **Associated Mobility Identity** section, and increase the **Answer Too Soon Timer** value.

For example, enter 3000 instead of 1500.

Users Cannot Receive Secure Voice Messages

Users cannot receive secure messages.

Solution

- This feature is supported only with Cisco Unity Release 7.0 and Cisco Unity Connection Release 7.0.
- For Cisco Unity, check the adapter configuration and Make sure that the SOAP information and user ID and password are entered correctly.

  You can check the configuration by selecting the **Test Config** button at the bottom of the Basic Settings page.
- If applicable, configure Cisco Unity to allow Cisco Unified Mobility Advantage to provide secure voice messages to Release 7.x clients. See the "How to Install and Configure Voicemail Web Services" in the *Installation and Configuration Guide for Visual Voicemail for Release 7.0* at http://www.cisco.com/en/US/docs/voice_ip_comm/cupa/visual_voicemail/7.0/english/install/guide/install.html. Voicemail Web Services is a separate installer and was introduced in Cisco Unity Release 7.0(2) ES21.

Voice Message Arrival Is Delayed

Voice messages arrive on the client long after they have been left.

Solution

- Verify that this problem is specific to Cisco Unified Mobility Advantage and its clients. If it occurs in other situations, see your voicemail system documentation for troubleshooting tips.
- Have the system check more frequently for new voice messages. In the Admin Portal, select the **[+]** beside **Enterprise Configuration** then select **Enterprise Adapter**. Select the pencil image to edit the voicemail adapter. Select **Basic Settings**, then decrease the value in **Polling Period (sec)** and select

Submit. The default is 600 seconds (10 minutes.) Setting this value too low may impact performance. You may need to experiment to find the optimal value for your deployment.

Caller Name Is Missing from Voice Messages

Caller name is missing from a voicemail entry.

Solution

- If the call was forwarded, the caller name may not be available.
- Make sure your Cisco Unified Mobility Advantage server and your Microsoft Exchange server are synchronized. Cisco strongly recommends using a Network Time Protocol (NTP) server. See the *Cisco Unified Communications Operating System Administration Guide For Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.
- If the call history also does not identify the caller by name, modify the Directory Lookup settings or the Phone Number Format field in the Active Directory adapter in Cisco Unified Mobility Advantage. The same rules are used to identify voice messages and calls in the call history.

  To identify the person who left the voice message, the system checks for matching information elsewhere in the corporate infrastructure and supplies the corresponding name if available. The system checks for matches of the following information, in the following locations, in order:

  - Email address of the caller in Cisco Unified Mobility Advantage
  - Email address of the caller in Exchange
  - Email address of the caller in Active Directory
  - Mobile phone number of the caller in Cisco Unified Mobility Advantage
  - Phone number of the caller in Exchange (Business, Business 2, Home, Home2, Car, and Mobile fields)
  - Phone number of the caller in Active Directory (telephoneNumber, homePhone, and mobile attributes)
  - Phone number of the caller in IMAP

  For details of how the phone number of the caller is transformed for matching, see the sections on Directory Lookups and the description of the Phone Number Format field in the Active Directory adapter in Cisco Unified Mobility Advantage. See also troubleshooting information for call history.
- The system may be set up to pass the gateway number in place of blocked caller IDs. This is done in some companies to assist in locating callers in case of emergency.

How to Solve Problems with Contacts

Search Does Not Find Existing Contact

A user searched for a contact that exists in Active Directory, but the search did not find the contact.

Solution

- Try searching for just the first name or just the last name. For example, try this when searching for a user whose first name includes two names.
- The contact must be in the Active Directory Search Base you specified in the Active Directory adapter, or in the personal contact list of the user.
- Make sure all required attributes are configured in Active Directory for the user. These are the attributes you configured in the Active Directory adapter for Distinguished Name, First Name, Last Name, User ID, and Email.
- All matching results may not be displaying. Consider changing the maximum number of search results displayed, as described in the following topic.

Modifying the Maximum Search Results

You can change the default maximum number of contacts to display on the client when a user searches the directory.

Procedure

Step 1 Select the [+] beside **System Management**.
Step 2 Select **System Properties**.
Step 3 Enter the number of results to display in **Max Search Results**.
Step 4 Restart Cisco Unified Mobility Advantage.

Personal Contacts Are Not Available

The personal contact list from Exchange does not display for any user.

Solution Make sure Outlook Web Access is enabled in Microsoft Exchange, and the Transport Type you specified in the Exchange adapter matches the connection security mode that is set in Exchange.

How to Solve Problems with Meeting Features

Link to Join Meeting Does Not Work

Call Me link does not work.

Solution

- Have the user check the Server Status on the device.

- Check the phone numbers in the user profile in Cisco Unified MeetingPlace, or make sure Mobile Connect is enabled in the Cisco Unified Mobile Communicator Mobile Identity in Cisco Unified Communications Manager.
- The Cisco Unified MeetingPlace profile of the user must have **Can dial out from meetings** set to **Yes**.
- Verify that the callback number entered into Settings on the client works if the same number is entered as the callback number when joining a meeting from the computer.

  If the same number does not work when joining from a computer, make sure that the Calling Search Space and route patterns that are configured in Cisco Unified Communications Manager for Cisco Unified MeetingPlace callbacks can accommodate external numbers such as mobile numbers.
- Call Me links can fail to work temporarily if the phone is not synchronized with the Cisco Unified MeetingPlace server. For example, if the time on the phone shows as 11:55, the meeting will appear to be joinable, but if the time on the Cisco Unified MeetingPlace server is only 11:50 and the meeting is not yet joinable, the link will not work.

Meetings Missing From Meeting List (iPhone Clients Only)

Expected meetings do not appear in the meeting list of a user.

Solution

- Have the user check the Server Status on the iPhone client.
- Make sure the meetings appear in the Exchange calendar of the user. Meetings that do not appear in Exchange will not appear in the clients.
- Meetings that were scheduled before you modified the notification templates will not have the cump:// link that is required for meetings to be included in the list. Have meeting schedulers reschedule these meetings, including recurring meetings, so that users receive updated meeting notifications.

Dial-In Numbers Are Missing from Meeting Notifications

Dial-in numbers do not appear in conference notifications or meeting details on the client, but do appear in email notifications.

Solution

- Make sure the formats of dial-in phone numbers match one of the required formats for dial-in numbers in Cisco Unified MeetingPlace. See the documentation for configuring meetings features in Cisco Unified Mobility Advantage.
- If the format of the dial-in number does not match one of the required patterns, try adding a plus in front of your number.

Some Meeting Notifications Do Not Arrive (Release 7.0 and 3.x Clients Only)

Notification for some meetings never arrive.

Solution

- Meetings that were scheduled before you modified the notification templates will not have the cump:// link that is required for meeting notifications in Cisco Unified Mobile Communicator clients. Have meeting schedulers reschedule these meetings, including recurring meetings, so that users receive updated meeting notifications.
- Make sure your Cisco Unified Mobility Advantage server and your Microsoft Exchange server are synchronized. Cisco strongly recommends using a Network Time Protocol (NTP) server. See the *Cisco Unified Communications Operating System Administration Guide For Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html.

Meeting Notifications Not Arriving or Arriving Late (Release 7.0 and 3.x Clients Only)

Meeting notifications are not arriving, or are arriving late.

Solution Modify the polling parameters. Note that for Release 7.0 clients, this procedure also controls updates to availability status based on the meeting schedule of users.

Modifying Polling for Meeting Notifications

If users of Release 7.0 clients and Release 3.x clients are not receiving meeting notifications or notifications arrive late, modify the polling parameters that govern when and how Cisco Unified Mobility Advantage polls for new meeting notifications.

Note If you deployed Cisco Unified Presence as part of this solution, this procedure also affects adjusting the availability status of users of Release 7.0 clients based on their meeting schedules.

Procedure

Step 1 Sign in to the Cisco Unified Mobility Advantage Admin Portal.

Step 2 Select the **[+]** beside **Enterprise Configuration**.

Step 3 Select **Manage Adapter Services**.

Step 4 Select **Meeting Service**.

Step 5 Modify settings:

Option	Description	Default
Polling Period (sec)	Frequency with which Cisco Unified Mobility Advantage checks the Exchange calendar of each user A longer polling period may pick up existing meetings sooner but may not pick up updates and new meetings as soon.	600
Max Threads	Maximum number of concurrent threads used to fetch appointment information	25

Option	Description	Default
Polling Offset (min)	Amount of "scan ahead" time used by the server to check for meetings. For example, with a 10 minute offset, notifications are sent at 5:20 for a meeting that starts at 5:30. Increasing the polling offset sends notifications for existing meetings sooner. However, notifications cannot be sent for meetings that are scheduled or moved within the offset period, until the next polling period.	10

Step 6 Select **Submit**.

Step 7 Restart Cisco Unified Mobility Advantage.

What to Do Next

This adjustment may require some trial and error. If applicable, monitor availability status as well as notifications to be sure these features are working as desired. If necessary, continue to modify values until the problem goes away.

User Receives Error: Unable to Join Meeting: Timed Out (-33)

A user trying to join a Cisco Unified MeetingPlace meeting with the Meeting ID receives this error.

Solution The Cisco Unified MeetingPlace profile of the user must have **Can dial out from meetings** set to **Yes**.

BlackBerry Users Do Not Receive Alerts

Alerts are sent to the Junk folder in Microsoft Outlook instead of to the BlackBerry device.

Solution You must provide users with:

- The procedure for preventing Outlook from treating these messages as junk mail.
- The Admin email address. The Admin email address can be viewed under **System Management > SMTP Server Configuration**.

Configuring Microsoft Outlook to Properly Handle Provisioning Email Messages

Ensure that Outlook does not treat provisioning messages as Junk Mail.

Procedure

Step 1 Sign in to Microsoft Outlook on your computer.
Step 2 Select **Tools > Options**.
Step 3 Select **Preferences**.
Step 4 Select **Junk e-mail**
Step 5 Select **Safe Senders**.
Step 6 Select **Add**.
Step 7 Enter the email address that your Administrator gave you.
Step 8 Select **OK**.
Step 9 Select **OK** again.
Step 10 Continue to check the Junk mailbox; if necessary, disable junk-mail blocking during provisioning.

How to Solve Problems with Availability Status (Presence)

Note that availability status is supported only for Release 7.0 clients.

Availability Status Is Incorrect

Availability status is not showing correctly.

Solution

- If presence is not working on initial tests, check the Cisco Unified Presence adapter configurations in the Cisco Unified Mobility Advantage Admin Portal by selecting the **Test Config** button on each page.
- Have the user verify the troubleshooting steps in the user documentation for the relevant device, if any.
- Make sure that availability status is showing correctly on other devices, such as Cisco Unified Personal Communicator. The problem may not be specific to Cisco Unified Mobility Advantage.
- If a user reports that his availability status appears different on different clients, for example Cisco Unified Personal Communicator: Have the user sign out and in again to force the synchronization. You can also force the sign out in the Cisco Unified Mobility Advantage Admin Portal, in the Search Maintenance page for the user. (Roll your mouse over the icons to see which icon to select.)

  See the documentation for Cisco Unified Presence, including but not limited to the section on integration with Cisco Unified Mobility Advantage and any troubleshooting information. See http://cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html.
- (Release 7.0 Clients Only) Modify the polling parameters for this feature using the procedure below. Note that this procedure also controls polling periods for receiving meeting notifications for Release 7.0 and Release 3.x clients.

Modifying Polling for Availability Status Based on Meeting Schedule (Release 7.0 Clients Only)

Cisco Unified Mobility Advantage can update the availability status of users of Release 7.0 clients based on their meeting schedule. If users are experiencing problems with updates to this information, consider adjusting settings described in this topic.

Caution This procedure also modifies the polling period for receiving meeting notifications on these client releases.

Before You Begin

Make sure that you have enabled Outlook integration in Cisco Unified Presence. See the documentation for Cisco Unified Presence, for example the *Integration Note for Configuring Cisco Unified Presence Release 7.0 with Microsoft Exchange* at http://www.cisco.com/en/US/docs/voice_ip_comm/cups/7_0/english/integration_notes/ExchInt.html.

Procedure

Step 1 Sign in to the Cisco Unified Mobility Advantage Admin Portal.

Step 2 Select the **[+]** beside **Enterprise Configuration**.

Step 3 Select **Manage Adapter Services**.

Step 4 Select **Meeting Service**.

Step 5 Modify settings:

Option	Description	Default
Polling Period (sec)	Frequency with which Cisco Unified Mobility Advantage checks the Exchange calendar of each user A longer polling period may pick up existing meetings sooner but may not pick up updates and new meetings as soon.	600
Max Threads	Maximum number of concurrent threads used to fetch appointment information	25
Polling Offset (min)	Amount of "scan ahead" time used by the server to check for meetings. For example, with a 10 minute offset, notifications are sent at 5:20 for a meeting that starts at 5:30. Increasing the polling offset sends notifications for existing meetings sooner. However, notifications cannot be sent for meetings that are scheduled or moved within the offset period, until the next polling period.	10

Step 6 Select **Submit**.

Step 7 Restart Cisco Unified Mobility Advantage.

What to Do Next

Be sure to check the results of your changes on meeting notifications as well as on availability status. Continue to adjust this polling period as necessary. This process may require some trial and error.

Viewing the Sign-in Status of a Cisco Unified Mobile Communicator User on Cisco Unified Presence

To help troubleshoot availability status issues, you can determine whether a mobility user appears as signed in on the Cisco Unified Presence.

Procedure

Step 1 Sign in to Cisco Unified Presence Administration.

Step 2 Select **Diagnostics > Presence Viewer**.

Step 3 Enter a valid user ID.

Tip Select **Search** to find the ID for a user.

Step 4 Select **Submit**

Step 5 Look at the Mobility Integration section for the status.

User Cannot Change Status from Idle to Available

User cannot change availability status from Idle to Available.

Solution This is intended. Idle status results only when Cisco Unified Personal Communicator is running but the user is not using the computer. Since users cannot send instant messages between Cisco Unified Personal Communicator and Cisco Unified Mobile Communicator, this limitation ensures that other Cisco Unified Personal Communicator users do not mistakenly believe the user is available to receive instant messages in Cisco Unified Personal Communicator.

Lost or Stolen Mobile Device

A mobile device is lost or stolen.

Solution See the Security documentation module for this release.

BlackBerry Client Exits Unexpectedly

Problem Cisco Mobile for BlackBerry exits unexpectedly.

Solution This can occur if you restrict IT Policies after granting them (for example, changing **Allow External Connections** from **True** to **False**). To resolve this issue, change the policy back to the less-restrictive value documented in the *Enabling Support for Clients* documentation module for your release of Cisco Unified Mobility Advantage, allow the revised IT policy to propagate to the end user devices, and have all users restart the client application.

How to View Error and Warning Logs

Specifying Options for Server Logs

You can specify how log files and messages are collected and stored.

Procedure

Step 1 Select the [+] beside **System Management**.

Step 2 Select **Log Configuration**.

Step 3 Enter information:

Item	Description
Log Level	Determines the level of information captured for the log file. Default is **Info**. • Debug—Records the largest amount of information in the logs. • Info—Records informational logs, warnings, errors, and fatal logs • Warning—Records logs that are generated if the server encounters problems that impact a single user, more than one user, or impacts the system • Error—Records logs that are generated if the server encounters problems that impact more than one user or impacts the system. If you select Error, only actual errors are displayed in the log. • Fatal—Records logs that are generated if the server encounters problems that impact the Cisco Unified Mobility Advantage system
Log File Size (MB)	Determines the size of each log file that is generated by the Admin Server and Managed Server. Value of this field should be between 1 and 999. Default is 20.
Number of Log Files	Determines the maximum number of log files that are preserved by the Admin Server and the Managed Server. Value of this field should be between 1 and 9999.

Item	Description
	Default is 100.

Step 4 Select **Submit**

Viewing Server Log Files

Procedure

Step 1 Use a tool such as PuTTY to remotely access the server using SSH.

Step 2 Sign in as the platform administrator using the sign-in information that you entered during installation.

Step 3 Determine which type of log file to view:

For These Problems	View This Type of Log
View This Type of Log	admin_init.log
Problems with the Admin portal	admin.log
Problems after the system is up and running	cuma.log
Most other problems	cuma.log

There may be more than one instance of each log type. After a log file reaches the maximum size you specify in the Administration portal, the older information is separated into a separate file stamped with the date and time of the separation, for example **admin.log**<date and timestamp>.

Step 4 Use the command line interface (CLI) to find the logs to view:

To	For This Service	Use This Command
List the files available for viewing	admin service This service runs the Admin portal	file list admin *
	managed server	file list cuma *

Step 5 View a log file:

To	For This Service	Use This Command
Download a log file (You must use SFTP)	admin service	file get admin admin.log where admin.log is one of the files in the list you viewed.
	managed server	file get cuma cuma.log

To	For This Service	Use This Command
		where cuma.log is one of the files in the list you viewed.
Tail a log file (View the last few lines of a log file in real time)	admin service	file tail admin admin.log where admin.log is one of the files in the list you viewed.
	managed server	file tail cuma cuma.log where cuma.log is one of the files in the list you viewed.
End the tail (Stop viewing the tail)	All	Press Control-C.

Step 6 Search in the log file for exception until you find an **exception** associated with a keyword that indicates the source of the problem.
For example, if the problem is related to Presence, look for an exception with the Cisco Unified Presence server.

Collecting Log Files from the iPhone Client

If iPhone users experience problems and you believe log files might help troubleshoot them, collect log files from the client.

This process zips up the log files and attaches the zip file to an email message that can be sent to an email address of your choice.

Procedure

Step 1 In the client, select **Settings > Troubleshooting**.
Step 2 Set **Detailed Logging** to **ON**.
Step 3 Perform the steps that cause the problem, in order to capture detailed logs for the issue.
Step 4 Select **Problem Reporting**.
Step 5 Select the types of files to collect.
Standard log files are always included.
Step 6 Select **Email Problem Report**.
Step 7 Type a description of the problem in the body of the message.
Include symptoms of the problem including text of any error message, steps leading up to the problem, circumstances required to see the problem, time the problem occurred, etc.
Step 8 Enter the email address to which you want to send the logs.
Step 9 Send the message.

Collecting Native Log Files from the iPhone

If the iPhone client unexpectedly quits and you are unable to obtain log files directly from the client to determine the problem, you may need to retrieve native log files from the iPhone.

Procedure

Step 1 Download and install the software from the following link:

- MacOS: http://support.apple.com/downloads/iPhone_Configuration_Utility_2_0_for_Mac_OS_X
- Windows: http://support.apple.com/downloads/iPhone_Configuration_Utility_2_0_for_Windows

Step 2 Plug the iPhone into your PC.

Step 3 Select the iPhone under **Devices** on the left.

Step 4 Select **Console**.

Step 5 Clear any existing log information.

Step 6 Reproduce the problem.

Step 7 Highlight the log information in the Console window.

Step 8 Select **Save selection As** and save the file.

How To Recover From Server Failure

Recovering from Server Failure - Try This First

First, try the following:

To	Do This
Obtain a disaster recovery disk	Visit the Software Downloads area on Cisco.com: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281001413.
Check for and correct disk file system issues	1 Insert the disaster recovery disk and restart the computer, so it boots from the CD. 2 Enter option [F]|[f] and wait while the process completes. 3 Enter option [M][m] and wait while the process completes. 4 Enter option [V]|[v] and wait while the process completes. 5 Enter [Q]|[q] to quit this recovery disk program.

What to Do Next

If this process does not resolve the problem, see Recovering from Server Failure - Solution of Last Resort, page 33.

Recovering from Server Failure - Solution of Last Resort

Caution Use the process in this topic only if the Cisco Unified Mobility Advantage server is completely unrecoverable and no other solution has solved the problem, including using the Disaster Recovery Disk to check for and automatically correct disk file system issues.

To	Do This
Reformat the hard drive	This process wipes the master boot record and reverts the BIOS settings to factory defaults. **1** Insert the Disaster Recovery disk and restart the computer, so it boots from the CD. **2** Enter **W** for Windows preinstallation setup. **3** Enter **Yes** to continue. **4** Wait for reformatting to complete.
Reinstall Cisco Unified Mobility Advantage	**Important** • The version you install MUST be identical to the version from which your backup was made, including the release number of any service update or engineering special. • Use the same IP address you previously used. See the installation chapter in *Installing and Configuring Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html.
Restore Cisco Unified Mobility Advantage data from your backup.	See the *Disaster Recovery System Administration Guide for Cisco Unified Mobility Advantage* at http://www.cisco.com/en/US/products/ps7270/prod_maintenance_guides_list.html

Additional Resources for Troubleshooting

If you experience problem that is not addressed in this documentation, or solutions provided here do not solve the problem, see the following community forums:

- Cisco Community Central

  http://www.myciscocommunity.com

- Cisco NetPro (Networking Professional Connection)

  http://forums.cisco.com

In either forum, look in the Unified Communications Applications forum.

Enabling Remote Account Access for Cisco TAC Personnel

If you contact Cisco TAC for support, the technician may ask you to enable remote account access for him or her. Only TAC personnel can use this access, and only if there is an open case. You specify the duration of this access when you enable it.

Before You Begin

- You will need the platform administrator sign-in credentials you entered during installation. These are distinct from the Admin Portal sign-in credentials.
- You should also have the information summarized in the Admin Portal in **System Management > Configuration Summary**.

Procedure

Step 1 Use SSH to access the Cisco Unified Mobility Advantage server and sign in as the platform administrator.

Step 2 Run the CLI command **utils remote_account enable**.

Step 3 Run the CLI command **utils remote_account create** [account name] [life] where account name is any value and life is the duration of this access in days (1 to 30).
Example: utils remote_account rootroot 30.

This command creates a remote account with name rootroot for a life of 30 days and generates the passphrase for it.

Step 4 Give the TAC technician the Account name and Passphrase that appear.
The technician will use this information to access the server remotely. Only TAC personnel can decrypt the passphrase and access the server.