Troubleshooting IMAP Clients and ViewMail for Outlook

Troubleshooting IMAP Clients and ViewMail for Outlook

Troubleshooting Problems with Changing Passwords

When users change their Cisco Personal Communications Assistant (PCA) password in the Messaging Assistant, they also must update the password from their IMAP email client application so that the client can continue to access Unity Connection and retrieve voice messages. Likewise, when LDAP authentication is configured and the PCA password is changed in LDAP, the password configured in the IMAP email client application must be updated.

Users who use ViewMail for Outlook also must change the password in ViewMail for Outlook options when the PCA password has been changed. If the PCA password has been changed but ViewMail has not been updated, users typically see a message indicating that the invalid credentials were entered for the account when they try to use ViewMail features.

Troubleshooting Sign-In Problems with IMAP Email Clients (LDAP is Not Configured)

If users have trouble signing in to an IMAP client, or have trouble receiving voice messages in an IMAP client, consider the following possibilities:

- If the IMAP client application prompts a user for the Cisco Personal Communications Assistant (PCA) password, but does not accept it:
    - The Cisco Unity Connection user account may be locked because of too many invalid sign-in attempts.
    - The Unity Connection user account may have been locked by an administrator.
    - The Unity Connection user password may have expired.

- The Unity Connection user account may have been configured to require that the user specify a new password.
- The Unity Connection user may be entering the wrong password.

Users who belong to a class of service that allows access to the Messaging Assistant or to the Messaging Inbox can try to sign in to the Cisco PCA; the Cisco PCA displays an error message that explains why the sign-in attempt is failing. Users who cannot access the Messaging Assistant or the Messaging Inbox must contact an administrator for assistance.

- If Microsoft Outlook users are not prompted for their Cisco PCA password, confirm that the Remember Password check box on the Internet Email Settings (IMAP) page is not checked. If this option is checked and the password of the user has expired, changed, or is locked, Microsoft Outlook does not prompt the user to enter the Cisco PCA password. The result is that the user does not receive voice messages from Unity Connection and Outlook prompts for the username and password.

Troubleshooting Sign-In Problems with IMAP Email Clients (When LDAP is Configured)

If you are using LDAP authentication and using an IMAP email client to access Unity Connection voice messages, and if users who are integrated with the LDAP are unable to authenticate, consider the following possibilities:

- If you are using Active Directory, confirm that the server you are using for authentication is a global catalog server and that you are using port 3268 (if you are not using SSL to encrypt data that is transmitted between the LDAP server and the Unity Connection server) or port 3269 (if you are using SSL). Authentication settings are on the System Settings > LDAP > LDAP Authentication page in Connection Administration.

If you change any values on the LDAP Authentication page, and if IMAP clients are accessing Unity Connection, restart the Unity Connection IMAP Server service in Cisco Unity Connection Serviceability. If other web applications are accessing Unity Connection (for example, Cisco Personal Communications Assistant), restart the server.

- If the problem occurs even though you are already using a global catalog server or you are not using Active Directory, try to sign in to the Cisco PCA using an account that cannot sign in to an IMAP email client.
  - If that fails, then there are two likely causes: either the specifications on the LDAP Authentication page are incorrect, or there is a problem with user credentials on the LDAP server, for example, the password has expired or the user is specifying the wrong password.
  - If that succeeds, and if you have configured SSL to encrypt data that is transmitted between the LDAP server and the Unity Connection server, there may be a problem with the SSL certificate. To confirm, uncheck the Use SSL check box, change the port to 3268, restart the Unity Connection IMAP Server service in Cisco Unity Connection Serviceability, and try again.

Troubleshooting Sign-In Problems with IMAP Clients

If users have trouble signing into an IMAP client and recursively receive the pop-up to enter username and password, it indicates that the account has been locked, inactive, or the limit for the maximum concurrent session has reached. To troubleshoot the issue, verify if:

- User is trying to access the IMAP account with invalid credentials. This is confirmed by the presence of "authFail" instance in CiscoSysLog.

  To resolve the issue, navigate to Edit User Basics > Change Password (Web Application) page of Cisco Unity Connection Administration and reset the password for the user.

- User is trying to access inactive IMAP account. This is confirmed by the presence of "EvtSubAccountInactive" event is CiscoSysLog.

  To resolve the issue, navigate to Edit User Basic page of Cisco Unity Connection Administration and update the User Status to **Active**.

- The limit for maximum concurrent IMAP sessions has reached. This is confirmed by the presence of EvtIMAPLogonSessionLimitExceeded of CiscoSysLog. To resolve the issue, see the Unable to Login to IMAP Client section.

Unable to Login to IMAP Client

If the users have trouble signing into an IMAP client and recursively receive the pop-up to enter username and password, it can be because the limit for the maximum concurrent session has reached. This is confirmed by the presence of EvtIMAPLogonSessionLimitExceeded of CiscoSysLog. To resolve the issue, do the following:

1. Fetch the Alias of the user experiencing the problem from CiscoSysLog.
2. Run the following command to fetch the current value of imapsessioncount for the user:

   ```
   run cuc dbquery unitydirdb select * from vw_subscribertimelastcall where
   subscriberobjectid = (select objectid from vw_subscriber where alias =<Alias>')
   ```

   where imapsessioncount is the number of IMAP sessions currently open for the user.

3. Ask the user to hang up one of the IMAP sessions if the value of imapsessioncount matches the configured maximum limit for concurrent IMAP sessions.

   For multiple users, if the value of imapsessioncount is within the configured maximum limit or is not decrementing even after reducing the number of open IMAP sessions, disable the feature for immediate solution or contact Cisco TAC. For information on disabling the feature, see "Restricting the Maximum Concurrent Sessions "section of *Security Guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html

Messages Sent from an IMAP Client Not Received

If users cannot send messages through the Unity Connection server from an IMAP client—for example, messages remain in the Outbox, an SMTP error is displayed in the client, or users receive non-delivery receipts (NDRs)—consider the following possibilities:

- If Unity Connection is not configured to allow clients to connect from untrusted IP addresses on the System Settings > SMTP Configuration > Server page in Cisco Unity Connection Administration, the

IP address of the client must appear in the IP address access list in Unity Connection. See the Checking the IP Address Access List.

- If Unity Connection is configured to allow clients to connect from untrusted IP addresses on the System Settings > SMTP Configuration > Server page in Connection Administration, two additional settings on this page can affect the ability of an IMAP client to send messages.
    - If the Require Authentication From Untrusted IP Addresses check box is checked, the client must be configured to authenticate with the outgoing SMTP server.
    - If the Transport Layer Security From Untrusted IP Addresses field is set to Required, the client must be configured to use Secure Sockets Layer (SSL) when connecting to the Unity Connection server.
- The email address of the message sender must exactly match a primary or proxy SMTP address configured in Unity Connection, as follows:
    - If the message is being sent from an IMAP client that is authenticated with the Unity Connection server, the email address must exactly match either the primary SMTP address that is displayed on the User Basics page for the user in Connection Administration or one of the SMTP proxy addresses that are configured on the SMTP Proxy Addresses page for the user.
    - If the message is being sent from an IMAP client that is not authenticated with the Unity Connection server, the email address can match a primary or proxy address that is configured for any user on the Unity Connection server.
- The email address of the message recipient must match a primary or proxy SMTP address that is configured for a Unity Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found, Unity Connection relays the message to the SMTP smart host, or sends an NDR to the sender, depending on the option selected in the When a Recipient Cannot be Found setting on the System Settings > General Configuration page in Connection Administration. By default, Unity Connection sends an NDR.
- The message exceeds the maximum length or number of recipients per message that are configured on the System Settings > SMTP Server Configuration page in Connection Administration. (By default, the maximum allowed message length is 10 MB.)
- The IMAP client is unable to reach the Unity Connection SMTP server because of network connectivity issues or because access is blocked by a firewall.

In many of these error cases, the IMAP client may display an SMTP error when attempting to send a message to the Unity Connection server. This error includes an error code and a text description that can help narrow down the source of the problem. If the client application does not display SMTP errors to the user, or if you still have not identified the problem after checking the potential causes above, the SMTP and MTA micro traces (all levels) are helpful for diagnosing issues related to SMTP connectivity and message transport. When examining the logs, start with the SMTP log first, then review the MTA log. (The SMTP service authenticates the client and receives the message; the MTA service processes the message and addresses it to the correct Unity Connection user or contact.) For detailed instructions on enabling the traces and viewing the trace logs, see the Using Diagnostic Traces for Troubleshooting.

Checking the IP Address Access List

If you choose not to allow connections from untrusted IP address lists, the IP address of each client must be configured in the IP access list, and the Allow Unity Connection check box must be checked. If the access list is not configured properly, the client may display an SMTP error code of 5.5.0, indicating that the Unity Connection was refused.

Checking the Cisco Unity Connection IP Address Access List

Step 1 In Cisco Unity Connection Administration, expand **System Settings** > **SMTP Configuration**, then select **Server**.

Step 2 On the SMTP Configuration Page, on the Edit menu, select **Search IP Address Access List**.

Step 3 Confirm that the IP address in use by the IMAP client appears as an entry in the list, and that the Allow Unity Connection check box is checked.

Step 4 To add a new IP address to the list, select **Add New**.

Step 5 On the New Access IP Address page, enter an IP address or you can enter a single ***** (asterisk) to match all possible IP addresses and select **Save**.

Step 6 On the IP Address page, check the **Allow Connection** check box to allow connections from the IP address that you entered in Step 4. To reject connections from this IP address, uncheck the check box.

Step 7 If you have made any changes on the IP Address page, select **Save**.

Messages are Received in an Email Account Instead of a Voice Mailbox

If users unexpectedly receive voice messages in their corporate or other email accounts rather than their Cisco Unity Connection mailboxes, consider the following possibilities:

- The email address of the message recipient must match a primary or proxy SMTP address that is configured for a Unity Connection user, or an SMTP proxy address that is configured for a VPIM contact. If no such match is found and Unity Connection is configured to relay the message to the SMTP smart host, the message is relayed to the applicable email address. Confirm that the message recipient has a proxy SMTP address configured for the applicable email address. See the "SMTP Proxy Addresses" section in the User Settings" appendix of the System Administration Guide for Cisco Unity Connection *Release 11.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/troubleshooting/guide/b_11xcuctsg.html.
- If the user email profile has an Exchange account, the Cached Exchange Mode setting in Outlook must be enabled.
- If message actions for the recipient are configured to relay messages of a particular type (voice, email, fax or delivery receipt) to the user at the corporate email address, this is the expected behavior.

Voice Messages Not Received in an IMAP Account

If users do not receive incoming voice messages in the email client inbox, check the Junk-Email or other spam folder. The mail client may automatically filter voice messages to this folder. For information on configuring spam filtering to exclude a class of messages, refer to the email client documentation.

You may also need to check the configuration of any email appliance or server-side anti-spam filters in your organization to see if voice messages are being routed to Junk mail, voice attachments are being removed, or the policy is otherwise interfering with the delivery of voice messages to user mail clients.

Intermittent Message Corruption When Using ViewMail for Outlook

In cases where user email profiles have an Exchange account and the users are using ViewMail for Outlook, they may experience the following intermittent problems:

- When using ViewMail for Outlook to reply to a voice message, the recipient receives a corrupt voice message that cannot be played.
- When using ViewMail for Outlook to forward a voice message with an introduction to another Unity Connection user, the recipient hears only the introduction; the original message is not heard.
- When using ViewMail for Outlook to forward a voice message to another Unity Connection user, the message is delivered to the Exchange mailbox of the recipient instead of to the Unity Connection mailbox of the recipient. Additionally, the message is corrupt, and cannot be played.

For each of these problems, the solution is to enable the Cached Exchange Mode setting in Outlook.

Recording or Playback Devices Not Appearing in ViewMail Account Settings in ViewMail for Outlook

If a particular recording or playback device that is connected to the computer does not appear as an option in the Audio Devices lists while composing a message or in the ViewMail Account Settings dialog, restart Outlook. ViewMail for Outlook does not recognize devices that were recently added to the computer until you restart Outlook.

Unable to Play Messages through ViewMail for Outlook 8.5 and Later

If the “Recording or Playback Messages Failed - no recording device” error message appears while recording or playing voice messages through ViewMail for Outlook 8.5 and later, make sure that the proxy is not enabled in the Internet Explorer. If you want to play or record voice messages while proxy is enabled, you need to add the hostname or IP address of Unity Connection in the proxy exception list to avoid failure in recording or playing voice messages through ViewMail.

User Email Account Does Not Appear in ViewMail Options in ViewMail for Outlook

If you have recently added an email account to Outlook but the account does not appear as an option when you try to add it as an Associated Email Account in ViewMail Options, restart Outlook. ViewMail for Outlook does not recognize email accounts that were recently added to Outlook until you restart Outlook.

ViewMail for Outlook Form Does Not Appear

If the ViewMail for Outlook form does not appear after you have installed ViewMail on a user workstation, consider the following:

- Only new messages are displayed with the form. Messages that were in the user mailbox prior to installing ViewMail do not display with the form.

- You must close and restart Outlook after installing ViewMail. If the user is running a synchronization program for a PDA device, the Outlook.exe process may not have fully exited when Outlook was shut down. If that is the case, close the synchronization program and then close and restart Outlook.
- The ViewMail form may have been disabled by Outlook. To determine if Outlook has disabled the form, select Help > About Microsoft Office Outlook > Disabled Items to see whether vmoexchangeextension.dll is in the list.

Collecting Diagnostics from ViewMail for Outlook on the User Workstation

To troubleshoot problems with the Cisco ViewMail for Microsoft Outlook form, you can enable diagnostics on the user workstation.

Enabling ViewMail for Outlook Diagnostics and View the Log Files on the User Workstation

Step 1 On the user workstation, on the Outlook Tools menu, select the ViewMail tab.

Step 2 Select Settings.

Step 3 In the **Cisco ViewMail Settings** > **dialog box, check the** > **Turn on diagnostic traces** check box and select **OK**.

Step 4 Reproduce the problem.

Step 5 Review the resulting log files by selecting the **Email Log Files** option on the ViewMail tab and sending the resulting message with logs attached to an email address.

Collecting Diagnostics from ViewMail for Outlook on the User Workstation

To troubleshoot problems with the ViewMail for Outlook form, you can enable diagnostics on the user workstation.

Enabling ViewMail for Outlook Diagnostics and View the Log Files on the User Workstation

Step 1 On the user workstation, on the Outlook Tools menu, select ViewMail for Outlook Options.

Step 2 Select the Diagnostics tab.

Step 3 Enable the following diagnostics:

- **Enable VMO Outlook Extension Diagnostics**
- **Enable VMO Multimedia Diagnostics**

1. If the problem is related to secure messages or recording and playback through the phone, enable the following diagnostics:

- **Enable VMO Telephone Record/Playback Diagnostics**
- **Enable VMO HTTP Diagnostics**

1. Select **OK**.
2. Reproduce the problem.
3. Review the resulting log files, which are stored in the C:\Documents and Settings\All Users\Application Data\Cisco Systems\VMO\1.0\Logs folder.

Collecting Diagnostics on Unity Connection for IMAP Client Problems

You can use Unity Connection traces to troubleshoot IMAP client problems from the server side. You need to enable the following micro traces to troubleshoot IMAP client problems:

- SMTP (all levels)
- MTA (all levels)
- CuImapSvr (all levels)
- CsMalUmss (all levels)
- CML (all levels)

For detailed instructions on enabling and collecting diagnostic traces, see the Using Diagnostic Traces for Troubleshooting section.

Login via IMAP Fails for LDAPS if IP Address of LDAP Server is Configured

It has been observed that login via IMAP clients for LDAP imported users, fails for LDAP-SSL case, if IP address of LDAP server is configured under LDAP authentication on CUCA page instead of FQDN or hostname of LDAP server. This would not impact the Java applications i.e. login via Cisco PCA would work fine for all the LDAP imported users. Customers who for some reason do not enable DNS must use the following workaround to use any non Java application to authenticate using SSL (CTI, TSP, etc.) The /etc/openldap/ldap.conf file contains information necessary for the openLDAP library to function properly. An issue involving certificates and openLDAP exists where openLDAP must be able to verify the certificate in order to connect to an LDAP server. The problem is, certificates are issued with a Fully Qualified Domain Name (FQDN), and if the customer's are not making use of DNS for any reason, they are required to enter an IP Address on the LDAP Authentication web page (System->LDAP->LDAP Authentication). Part of the openLDAP verification is to match the FQDN with the server being accessed. Since the uploaded certificate uses FQDN and the web form is using IP Address, openLDAP cannot connect. The fix for this is for the customer to use DNS if possible.