Troubleshooting User and Administrator Access

Unity Connection Not Responding to Key Presses

When Unity Connection is integrated with Cisco Unified Communications Manager using SCCP, Unity Connection may not respond to key presses. In such situations, DTMF digits are not recognized when processed through VoIP dial-peer gateways. To avoid this problem, certain gateways must be configured to enable DTMF relay available in Cisco IOS software version 12.0(5) and later.

In Cisco IOS software-based gateways that use H.245 out-of-band signaling, you need to enable DTMF relay. However, in the Catalyst 6000 T1/PRI and FXS gateways, DTMF relay is enabled by default.

Enabling DTMF Relay

Step 1 On a VoIP dial-peer servicing Unity Connection, use the following command:

```
dtmf-relay h245-alphanumeric
```

Step 2 Create a destination pattern that matches the Cisco Unified CM voicemail port numbers. For example, if the system has voicemail ports 1001 through 1016, enter the dial-peer destination pattern 10xx.

Step 3 Repeat Step 1 and Step 2 for all remaining VoIP dial-peers servicing Unity Connection.

What to do next

Verifying DTMF settings

Step 1 In Cisco Unity Connection Administration, navigate to Telephony Integrations > Port Group.

Step 2 On the Search Port Groups page, select the port group of which you want to verify the DTMF settings.

Step 3 On the Port Group Basics page, navigate to Edit > Advanced Settings.

Step 4 On the Edit Advanced Settings page, verify that the Use DTMF KPML and Use DTMF RFC 2833 check boxes are checked.

Users Do Not Hear Sign-in or Desired Prompt When Calling Unity Connection

When a user calls Unity Connection directly and unexpectedly hears the Opening Greeting or another prompt rather than the sign-in prompt, the problem can be caused by either of the following:

- The call matched a direct call routing rule other than the Attempt Sign-In rule, and the rule directed the call to a destination other than the Attempt Sign-In conversation.
- The calling extension is not found in the search scope set by the call routing rule that sends the call to the Attempt Sign-In conversation.

Unity Connection uses the search scope of the call when it reaches the Attempt Sign-In conversation to identify which user is attempting to sign in. If the user extension is in a partition that is not a member of the search space that is assigned as the search scope of the call by the routing rule, Unity Connection routes the call to the Opening Greeting.

To resolve this problem, in Cisco Unity Connection Administration, check the direct call routing rules to determine which rule is processing the call and to check the search scope that is set by the rule. You can also enable the Arbiter micro trace (levels 14, 15, and 16 call routing), the Routing Rules micro trace (level 11 rules creation/deletion/evaluation), and the CDE micro trace (level 4 search space). (For detailed instructions on turning on traces and collecting logs, see the Using Diagnostic Traces for Troubleshooting section.

Unity Connection also provides Port Status Monitor tool that you can use to troubleshoot call routing problems. To use Port Status Monitor tool for troubleshooting issues, do the following:

Using Port Status Monitor

Step 1 Download and install Port Status Monitor from Cisco unity tools http://ciscounitytools.com.

Step 2 Enable CDE, Routing Rules, ConvSub, PhaseServer, and PhaseServertoMonitor traces.

Step 3 In Cisco Unity Connection Administration, navigate to System Settings > Advanced > Conversations.

Step 4 On the Conversation Configuration page, make sure that the Enable Remote Port Status Monitor Output checkbox is checked and the IP address of the local machine, that is being used to connect to the server, is specified in the IP Addresses Allowed To Connect For Port Status Monitor Output (comma-separated) text box.

Step 5 Analyze the PSM output to diagnose the problem.

Administration Accounts Unable to Sign-In to Cisco Unity Connection Serviceability

If the default application administration account is locked because of password expiration or too many unsuccessful sign in attempts, you can reset the password using the **utils cuc reset password** CLI command to unlock the account.

User Account is Locked over TUI/VUI Interface

Problem statement:

When a user hears the "Your account is locked and cannot be opened. For help please contact System Administrator " prompt while accessing the voicemail account through TUI/VUI interface.

Resolution:

Do either of the following to resolve the problem:

- Navigate to **Edit User Basics** > **Password Settings** page of Cisco Unity Connection Administration and uncheck the **Locked by Administrator** check box to unlock the user account.
- Navigate to the **Edit User Basics** page of Cisco Unity Administration and update the **Voicemail Application Access** to **Active** to activate the inactive user account.

Related Diagnostic Traces:

- If the CiscoSysLog contains the event "EvtSubAccLockedMaxHack", this confirms that the user has exceeded the maximum number of Sign-in attempts and the user account has been locked.
- If the CiscoSysLog contains the event "EvtSubAccountInactive", this confirms that the user has not accessed TUI/VUI interface for more than pre-configured number of days for user inactivity timeout and the user account has been disabled.

User Account is Disabled over Web Applications

Problem statement:

When a user is getting the "Account has been disabled" error message while accessing the Cisco Unity Connection web interfaces, such as Cisco PCA, Cisco Unity Connection Administration, and Web Inbox.

Resolution:

To resolve the issue, navigate to the **Edit User Basics** page of Cisco Unity Administration and update the **Voicemail Application Access** to **Active** to activate the inactive user account.

Related Diagnostic Traces:

If the audit logs contains "User with alias <user alias> marked inactive since the user has not logged in since last <configured no. of days>", this confirms that the user has not accessed TUI/VUI interface for more than pre-configured number of days for user inactivity timeout and the user account has been disabled.

Troubleshooting Sign-in Problems with Visual Voicemail (Pin Based Authentication)

Problem statement:

When the user is getting the "Your account is locked. Contact your administrator to unlock your account" error message while logging into Visual Voicemail (VVM).

Resolution:

Do either of the following to resolve the problem:

- Navigate to **Edit User Basics** > **Password Settings** page of Cisco Unity Connection Administration and uncheck the **Locked by Administrator** check box to unlock the user account.
- Navigate to the **Edit User Basics** page of Cisco Unity Administration and update the **Voicemail Application Access** to **Active** to activate the inactive user account.

Related Diagnostic Traces:

- If the audit logs contains "Failed to Login to Cisco Unity Connection VMWS", this confirms that the user has exceeded the maximum number of Sign-in attempts and the user account has been locked.
- If the audit logs contains "User with userName <alias> is inactive due to inactivity timeout", this confirms that the user has not accessed TUI/VUI interface for more than pre-configured number of days for user inactivity timeout and the user account has been disabled.

Troubleshooting Sign-in Problems with Visual Voicemail (Password Based Authentication)

Problem statement:

When the user is getting the "Please enter a valid username and password pair" error message while logging into Visual Voicemail (VVM) with valid credentials.

Resolution:

Do either of the following to resolve the problem:

- Navigate to **Edit User Basics** > **Password Settings** page of Cisco Unity Connection Administration and uncheck the **Locked by Administrator** check box to unlock the user account.

- Navigate to the **Edit User Basics** page of Cisco Unity Administration and update the **Voicemail Application Access** to **Active** to activate the inactive user account.

Related Diagnostic Traces:

The audit log contains "Failed to Login to VMREST", this confirms that user account has been either locked or disabled due to inactivity timeout.

Error Message Appears While Updating the Phone PIN through Cisco Unity Connection Administration or Cisco PCA

If the "Bad response from CUCM. Reason: Requested resource is not available " error message appears while updating the phone PIN through Cisco Unity Connection Administration or Cisco PCA, make sure that:

- The username and password of primary AXL server entered on the Edit AXL Servers page are correct.
- The AXL server is up and running.
- The Ignore Certificate Errors check box is checked. If the check box is not checked, confirm that Unity Connection has successfully validated the certificates for AXL server.

To troubleshoot more problems related to PIN synchronization, see the traces in "Micro Traces for Selected Problems" section of the "Troubleshooting Cisco Unity Connection" chapter.

User Display Name Not Get Updated after AD Synchronization

When a user is imported from Active Directory to Unity Connection first time, Display Name of the user is formed with First Name and Last Name. If Administrator changes the First name and Last Name of the user on Active Directory, then the Display Name of the user may not be updated on Unity Connection automatically after AD synchronization.

In this case, you need to update the Display Name of the users manually either through **Edit User Basics** page of Cisco Unity Connection Administration or using Bulk Administration Tool (BAT).

To update the Display Name of the users through BAT, do the following:

- On Cisco Unity Connection Administration, navigate **Tools** > **Bulk Administration Tool**.
- Export all users into CSV file on the Bulk Administration Tool page. The CSV file contains all the user related fields such as Alias, Extension, First Name etc.
- Copy the Alias, First Name and Last Name information of all the users into a new CSV file.
- In CSV file, create a new column for Display Name of the users and fill the column for user's Display Name formed by First Name and Last Name.
- Select **Update** on Bulk Administration Tool page and upload the CSV file for updating the Display Name of all the users.

  For more information on Bulk Administration Tool, see "Bulk Administration Tool" chapter of *System Administration Guide* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag.html

Not Able to Access Web Applications on Unity Connection

If you are not able to log in any web application of Unity Connection, check the status of HAProxy service and Tomcat service.

1. Do the following tasks to confirm that the HAProxy service is running and if necessary, restart the HAProxy service. Use either Real-Time Monitoring Tool (RTMT) or Command Line Interface (CLI).

   Using RTMT:

   - Launch Real-Time Monitoring Tool (RTMT).

   Note For details on using RTMT, see the applicable *Cisco Unified Real Time Monitoring Tool Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

   - On the System menu, select **Server** > **Critical Services**.
   - On the System tab, locate Cisco HAProxy and view its status. The status is indicated by an icon.

   Using CLI:

   - Use the Command Line Interface (CLI) command **utils service list** to list all of the services.

   Note For details on using CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

   - Scan the CLI output for the Cisco HAproxy service and confirm that its status is **Started**.

2. If HAProxy service is not started, then restart the service using the CLI command **utils service restart Cisco HAProxy**.

3. If problem still persists, perform above steps for **Cisco Tomcat** service to confirm that the service is running on the system.If Tomcat service is not started, then restart the service using the CLI command **utils service restart Cisco Tomcat**.

Related Diagnostic Traces: If the CiscoSysLog contains **CiscoHAProxyServiceDown**, this confirms that the Cisco HAProxy service is not running on the system, you need to restart the service.