Troubleshooting the Phone System Integration

Troubleshooting the Phone System Integration

Diagnostic Tools

There are diagnostic tools available to help you troubleshoot phone system integrations. For more information, see the sections below.

Configuring Unity Connection for the Remote Port Status Monitor

You can use the Remote Port Status Monitor for viewing the real-time activity of each voice messaging port on Cisco Unity Connection. This information assists you in troubleshooting conversation flow and other problems.

After installing the Remote Port Status Monitor on your workstation, do the following procedure to configure Unity Connection.

Note For detailed information on using the Remote Port Status Monitor, see the training and Help information available at http://www.ciscounitytools.com/Applications/CxN/PortStatusMonitorCUC7x/PortStatusMonitorCUC7x.html.

Configuring Unity Connection for the Remote Port Status Monitor

Step 1 In Cisco Unity Connection Administration, expand **System Settings**> **Advanced** > **and select** > **Conversations**. On the Conversation Configuration page, check the **Enable Remote Port Status Monitor Output** check box.

Step 2 In the IP Addresses Allowed to Connect for Remote Port Status Monitor Output field, enter the IP addresses of your workstations and select Save.

Note You can enter up to 70 IP addresses. Each IP address must be separated from the following IP address by a comma.

Using the Check Telephony Configuration Test

You can use the Check Telephony Configuration test to troubleshoot the phone system integration.

For example, use this test if the following conditions exist:

- Calls to Unity Connection are failing.
- Ports are failing to register.

Using the Check Telephony Configuration Test

Step 1 In Cisco Unity Connection Administration, in the Related Links box in the upper right corner of any Telephony Integrations page, select **Check Telephony Configuration** and select **Go**.

If the test is not successful, the Task Execution Results displays one or more messages with troubleshooting steps. After correcting the problems, run the test again.

Step 2 In the Task Execution Results window, select **Close**.

Troubleshooting Call Control

Use the following troubleshooting information if the phone system integration has problems related to call control. Do the following tasks, as applicable:

- Use the Check Telephony Configuration test. See the Using the Check Telephony Configuration Test.
- Use traces to troubleshoot call control issues. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the Traces in Cisco Unity Connection Serviceability.
- *(Cisco Unified Communications Manager integrations only)* If you hear a fast busy tone when you call Cisco Unity Connection, verify the configuration for the phone system integration. See the applicable Integration Guide for Cisco Unity Connection at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Unity Connection Not Answering Any Calls

When the phone system settings in Connection Administration do not match the type of phone system that Unity Connection is connected to, Unity Connection may not answer calls.

Verifying the Phone System Settings in Cisco Unity Connection Administration

If the test is not successful, the Task Execution Results displays one or more messages with troubleshooting steps. After correcting the problems, run the test again.

1. In the Task Execution Results window, select **Close**.

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**.

2. On the applicable pages, confirm that the settings for the phone system, port groups, and ports match those indicated in the integration guide for your phone system.
3. Correct any incorrect values in Cisco Unity Connection Administration. If you change any values, select **Save** before leaving the page.
4. If prompted to reset a port group, on the applicable Port Group Basics page, select **Reset**. Otherwise, continue to Step 5.
5. In the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the phone system integration settings.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**.

Step 2 On the applicable pages, confirm that the settings for the phone system, port groups, and ports match those indicated in the integration guide for your phone system.

Step 3 Correct any incorrect values in Cisco Unity Connection Administration. If you change any values, select **Save** before leaving the page.

Step 4 If prompted to reset a port group, on the applicable Port Group Basics page, select **Reset**. Otherwise, continue to Step 5.

Step 5 In the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the phone system integration settings.

Unity Connection Not Answering Some Calls

When Unity Connection is not answering some calls, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Following are the tasks to troubleshoot sporadic answers on incoming calls:

1. Confirm that the routing rules are working correctly. See the Confirming Routing Rules.
2. Confirm that calls are sent to the correct voice messaging ports and that the ports are enabled. See the Confirming Voice Messaging Port Settings.

Confirming Routing Rules

By default, Unity Connection does not reject any calls. If routing rules have been changed, Unity Connection may have been unintentionally programmed to reject some internal or external calls.

Use traces to troubleshoot issues with routing rules. For detailed instructions on enabling the applicable traces and viewing the trace logs, see the Traces in Cisco Unity Connection Serviceability.

Confirming Voice Messaging Port Settings

If the phone system is programmed to send calls to a voice messaging port on Unity Connection that is not configured to answer calls, Unity Connection does not answer the call.

Confirming that Calls are Sent to the Correct Voice Messaging Ports on Cisco Unity Connection

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.
2. On the Search Ports page, note which ports are designated to answer calls.
3. On the phone system, in the phone system programming, confirm that calls are being sent only to those voice messaging ports that are designated to answer calls. Change the phone system programming if necessary.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.

Step 2 On the Search Ports page, note which ports are designated to answer calls.

Step 3 On the phone system, in the phone system programming, confirm that calls are being sent only to those voice messaging ports that are designated to answer calls. Change the phone system programming if necessary.

Confirming that Voice Messaging Ports are Enabled

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.
2. On the Search Ports page, review the Enabled column.
3. If a voice messaging port is not enabled and should be in use, select the display name of port.
4. On the Port Basics page for the port, check the **Enabled** check box to enable the port.
5. On the Port menu, select **Search Ports**.
6. Repeat Step 3 through Step 5 for all remaining ports that should be in use.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.

Step 2 On the Search Ports page, review the Enabled column.

Step 3 If a voice messaging port is not enabled and should be in use, select the display name of port.

Step 4 On the Port Basics page for the port, check the **Enabled** check box to enable the port.

Step 5 On the Port menu, select **Search Ports**.

Step 6 Repeat Step 3 through Step 5 for all remaining ports that should be in use.

Troubleshooting an Integration of Unity Connection with Cisco Unified Communications Manager

Viewing or Editing IP Address of Cisco Unified Communications Manager

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations** > **and** select **Port Group**.
2. On the Search Port Groups page, select the display name of the port group for which you want to change Cisco Unified CM server settings.
3. On the Port Group Basics page, on the Edit menu, select **Servers**.
4. On the Edit Servers page, under Cisco Unified Communications Manager Servers, change the applicable settings and select **Save**.
5. If no status message appears, skip the remaining steps in this procedure. If a status message appears prompting you to reset the port group, on the Edit menu, select **Port Group Basics**.
6. On the Port Group Basics page, under Port Group, select **Reset**.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations** > **and** select **Port Group**.

Step 2 On the Search Port Groups page, select the display name of the port group for which you want to change Cisco Unified CM server settings.

Step 3 On the Port Group Basics page, on the Edit menu, select **Servers**.

Step 4 On the Edit Servers page, under Cisco Unified Communications Manager Servers, change the applicable settings and select **Save**.

Step 5 If no status message appears, skip the remaining steps in this procedure. If a status message appears prompting you to reset the port group, on the Edit menu, select **Port Group Basics**.

Step 6 On the Port Group Basics page, under Port Group, select **Reset**.

Ports Do Not Register or Repeatedly Disconnected in an SCCP Integration

When the Unity Connection voice messaging ports do not register with Cisco Unified CM in an SCCP integration, or if the Unity Connection ports repeatedly disconnect from Cisco Unified CM in an SCCP integration, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Following are the tasks to troubleshoot port registration problems:

1. Test the port group. See the Testing the Port Group.
2. Confirm that another port group on the Unity Connection server does not use the same device name prefix to connect ports to the Cisco Unified CM server. See the Confirming that Another Port Group Not Using the Same Device Name Prefix.
3. Confirm that another Unity Connection server does not use the same device name prefix to connect its ports to the Cisco Unified CM server. See the Confirming that Another Unity Connection Server Not Using the Same Device Name Prefix.

Note In addition to the tasks mentioned above, make sure that the order of the Cisco Unified CM servers in Unity Connection port group is same as the order of the Cisco Unified CM servers in the Cisco Unified CM Group.

Testing the Port Group

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.
2. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).
3. On the Port Group Basics page, in the Related Links list, select **Test Port Group** and select **Go**.
4. When prompted that the test terminate all calls in progress, select **OK**.
5. Follow the steps for correcting the problems.
6. Repeat Step 3 through Step 5 until the Task Execution Results displays no problems.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.

Step 2 On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 3 On the Port Group Basics page, in the Related Links list, select **Test Port Group** and select **Go**.

Note The Test Port and Test Port Group utilities do not test IPv6 connectivity. Even when Unity Connection is configured to use IPv6 for a SCCP integration, the tests confirm that Unity Connection can communicate with the phone system using IPv4 addressing.

Step 4 When prompted that the test terminate all calls in progress, select **OK**.

The Task Execution Results displays one or more messages with troubleshooting steps.

Step 5 Follow the steps for correcting the problems.

If Cisco Unified CM is configured to block pings or if pings are disabled for the system, portions of the test fails. You must configure Cisco Unified CM and the system to enable pings so that the test can accurately test the port registration.

Step 6 Repeat Step 3 through Step 5 until the Task Execution Results displays no problems.

Confirming that Another Port Group Not Using the Same Device Name Prefix

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).
2. On the Port Group Basics page, note the value of the Device Name Prefix field.
3. Select **Next** to view the next port group for which the integration method is SCCP (Skinny).

4. If the value of the Device Name Prefix field is different from the value that you noted in Step 2, skip to Step 7. If the value of the Device Name Prefix field matches the value for another port group, enter the device name prefix for ports on the Cisco Unified CM server that have a different device name prefix.
5. Select **Save**.
6. Select **Reset**.
7. Repeat Step 3 through Step 6 for all remaining port groups for which the integration method is SCCP (Skinny).

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 2 On the Port Group Basics page, note the value of the Device Name Prefix field.

This value of the Device Name Prefix field must be unique for each port group. Otherwise, more than one port may attempt to connect to an SCCP device, causing the ports to repeatedly disconnect from Cisco Unified CM and to disconnect calls that the ports are handling.

Step 3 Select **Next** to view the next port group for which the integration method is SCCP (Skinny).

Step 4 If the value of the Device Name Prefix field is different from the value that you noted in Step 2, skip to Step 7. If the value of the Device Name Prefix field matches the value for another port group, enter the device name prefix for ports on the Cisco Unified CM server that have a different device name prefix.

Step 5 Select **Save**.

Step 6 Select **Reset**.

Step 7 Repeat Step 3 through Step 6 for all remaining port groups for which the integration method is SCCP (Skinny).

Confirming that Another Unity Connection Server Not Using the Same Device Name Prefix

SUMMARY STEPS

1. In Cisco Unity Connection Administration on the first Unity Connection server, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).
2. On the Port Group Basics page, note the value of the Device Name Prefix field.
3. In Cisco Unity Connection Administration on the second Unity Connection server, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).
4. On the Port Group Basics page, note the value of the Device Name Prefix field.
5. If the value of the Device Name Prefix field is different from the value you noted on the first Unity Connection server in Step 2, skip to Step 8. If the value of the Device Name Prefix field matches the value for another port group, enter the device name prefix for ports on the Cisco Unified CM server that have a different device name prefix.
6. Select **Save**.
7. Select **Reset**.
8. Select **Next**.
9. Repeat Step 5 through Step 8 for all remaining port groups for which the integration method is SCCP (Skinny).

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration on the first Unity Connection server, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 2 On the Port Group Basics page, note the value of the Device Name Prefix field.

Step 3 In Cisco Unity Connection Administration on the second Unity Connection server, expand **Telephony Integrations**, then select **Port Group**. On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 4 On the Port Group Basics page, note the value of the Device Name Prefix field.

The value of the Device Name Prefix field must be unique for each port group. Otherwise, more than one port may attempt to connect to an SCCP device, causing the ports to repeatedly disconnect from Cisco Unified CM and to disconnect calls that the ports are handling.

Step 5 If the value of the Device Name Prefix field is different from the value you noted on the first Unity Connection server in Step 2, skip to Step 8. If the value of the Device Name Prefix field matches the value for another port group, enter the device name prefix for ports on the Cisco Unified CM server that have a different device name prefix.

Step 6 Select **Save**.

Step 7 Select **Reset**.

Step 8 Select **Next**.

Step 9 Repeat Step 5 through Step 8 for all remaining port groups for which the integration method is SCCP (Skinny).

Ports Do Not Register in an IPv6 Configuration

When the Cisco Unity Connection voice messaging ports do not register with Cisco Unified CM in an integration that is configured to use IPv6 addressing, and the CsMgr logs errors in the application syslog during startup, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Task List for Troubleshooting Port Registration Problems in an IPv6 Configuration

1. Confirm that IPv6 is enabled.
   - To check using the command-line interface (CLI), enter **show network ipv6 settings**.
   - To check using Cisco Unified Operating System Administration, see the Confirming that IPv6 is Enabled Using Cisco Unified Operating System Administration.
2. Confirm that Unity Connection is configured to use the appropriate addressing mode and preferences. See the Confirming the IPv6 Addressing Mode and Preferences Settings
3. If you have configured an IPv6 host name for the Unity Connection and/or Cisco Unified CM servers rather than configuring by IPv6 address, confirm that the DNS server can resolve the host name properly. To check using the CLI, enter **utils network ipv6 ping** <IPv6 host name>.
4. If you have configured the port group(s) in Unity Connection with an IPv6 host name for the Cisco Unified CM server(s) rather than with an IPv6 address, confirm that the DNS server can resolve the Cisco Unified CM host name correctly. Likewise, if you have configured Cisco Unified CM to contact the Unity

Connection server by IPv6 host name (for example, on a SIP trunk, for the Destination Address IPv6 field), confirm that the DNS server can resolve the Unity Connection host name correctly.

5. Confirm that the Cisco Unified CM server is configured correctly for IPv6, and has the correct settings for signalling and media preferences. See the "Internet Protocol Version 6 (IPv6)" chapter of the applicable *Cisco Unified Communications Manager Features and Services Guide* for your release of Cisco Unified CM, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Confirming that IPv6 is Enabled Using Cisco Unified Operating System Administration

SUMMARY STEPS

1. In Cisco Unified Operating System Administration, Settings > **IP** and select **Ethernet IPv6**.
2. On the Ethernet IPv6 Configuration page, review the **Enable IPv6** check box, and check it if it is not already checked.
3. If you checked the Enable IPv6 check box in Step 2, configure the Address Source for the Unity Connection server. To apply the change, check Update with Reboot, and select **Save**. The Unity Connection server reboots in order for the change to take effect.

DETAILED STEPS

Step 1 In Cisco Unified Operating System Administration, Settings > **IP** and select **Ethernet IPv6**.

Step 2 On the Ethernet IPv6 Configuration page, review the **Enable IPv6** check box, and check it if it is not already checked.

Step 3 If you checked the Enable IPv6 check box in Step 2, configure the Address Source for the Unity Connection server. To apply the change, check Update with Reboot, and select **Save**. The Unity Connection server reboots in order for the change to take effect.

Confirming the IPv6 Addressing Mode and Preferences Settings

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.
2. On the Edit General Configuration page, review the option selected for **IP Addressing Mode**, which controls where Unity Connection listens for incoming traffic:
3. If you change any values on the page, select **Save** to save the changes. When you change the IP Addressing Mode, you must stop and restart the Conversation Manager service on the Tools > Service Management page in Cisco Unity Connection Serviceability in order for the change to take effect.
4. If the IP addressing mode was configured for IPv4 and IPv6 in Step 2, do the following substeps to review the call control signalling and/or media addressing mode settings for the Cisco Unified Communications Manager integration:

DETAILED STEPS

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

Step 2 On the Edit General Configuration page, review the option selected for **IP Addressing Mode**, which controls where Unity Connection listens for incoming traffic:

- IPv4
- IPv6
- IPv4 and IPv6

Step 3 If you change any values on the page, select **Save** to save the changes. When you change the IP Addressing Mode, you must stop and restart the Conversation Manager service on the Tools > Service Management page in Cisco Unity Connection Serviceability in order for the change to take effect.

Step 4 If the IP addressing mode was configured for IPv4 and IPv6 in Step 2, do the following substeps to review the call control signalling and/or media addressing mode settings for the Cisco Unified Communications Manager integration:

a) Expand Telephony Integrations, then select Port Group.
b) On the Search Port Groups page, select the display name of the port group that you want to verify.
c) On the Port Group Basics page, on the Edit menu, select **Servers**.
d) In the IPv6 Addressing Mode section, verify the option selected for the applicable setting(s):

- **Preference for Signaling**—*(Applicable to both SCCP integrations and SIP integrations)* This setting determines the call control signaling preference when registering with Cisco Unified CM via SCCP or when initiating SIP requests.
- **Preference for Media**—*(Applicable only to SIP integrations)* This setting determines the preferred addressing mode for media events when communicating with dual-stack (IPv4 and IPv6) devices.

1. If you made any changes to the page, select **Save**.

Determining the Correct Port Group Template

When adding a phone system integration for Cisco Unified CM, there are two valid options for the Port Group Template field: SCCP or SIP. The SIP port group template is valid only for integrations with Cisco Unified CM 5.0(1) and later.

To integrate Unity Connection with a phone system through PIMG or TIMG units, in the Port Group Template field, you must select SIP to DMG/PIMG/TIMG.

Unable to Create Secure Ports

While using encryption on Cisco Unity Connection, you may face the following issues:

- Appearance of " Encrypted security mode is not supported on this version of Connection. Reconfigure the port group to use Authenticated mode." and " Secure RTP is not supported on this version of Connection. Reconfigure the port group to disable Secure RTP." error message.

  If you get the above error messages on Port Group Basics page while configuring the security ports, verify the following:

  - You must deploy the Restricted version of Cisco Unity Connection.
  - Unity Connection must be registered with CSSM or satellite through Export Controlled Functionality enabled Register Token.

- Check the status of encryption on Unity Connection using "utils cuc encryption status" CLI command. If the encryption status is disabled for Unity Connection. You must run the "utils cuc encryption enable" CLI command to enable the encryption on Unity Connection.

Problems Faced When Unity Connection is Configured for Cisco Unified Communications Manager Authentication or Encryption

If problems occur when Unity Connection is configured for Cisco Unified Communications Manager authentication and encryption for the voice messaging ports, use the following task list to determine the cause and to resolve the problem. Do the tasks in the order presented until the problem is resolved.

Note For information on integrating Unity Connection with Cisco Unified CM, see the applicable Cisco Unified CM integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Follow the tasks to troubleshoot problems when Cisco Unified CM authentication or encryption is configured:

1. Confirm that the Cisco Unified CM CTL client is configured for mixed mode. See the Confirming that Cisco Unified Communications Manager CTL Client is Configured for Mixed Mode.
2. Test the port group configuration. See the Testing the Port Group Configuration.
3. For SCCP integrations, confirm that the security mode setting for the ports in Unity Connection matches the security mode setting for the ports in Cisco Unified CM. See the Matching the Security Mode Setting for Ports in Unity Connection and Cisco Unified Communications Manager (SCCP Integrations Only).
4. For a SIP trunk integration, confirm that the security mode setting for the Unity Connection port group matches the security mode setting for the Cisco Unified CM SIP trunk security profile. See the Matching the Security Mode Setting for Unity Connection Port Group and Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only), on page 13 section.
5. For SIP trunk integrations, confirm that the Subject Name field of the Unity Connection SIP certificate matches the X.509 Subject Name field of the Cisco Unified CM SIP trunk security profile. See the Matching the Subject Name Fields of Unity Connection SIP Certificate and Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only), on page 14 section.
6. For SIP trunk integrations, confirm that Unity Connection and the SIP trunk use the same port. See the Matching the Port Used by Unity Connection SIP Security Profile and Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only), on page 14 section.
7. Copy the Unity Connection root certificate to the Cisco Unified CM servers. See the Copying the Unity Connection Root Certificate to Cisco Unified Communications Manager.
8. For secure SIP integration, confirm the certificate expiration of Cisco Unified CM. See the CTL File with Expired Cisco Unified CM Certificate (Secure SIP Integration Only)

Confirming that Cisco Unified Communications Manager CTL Client is Configured for Mixed Mode

SUMMARY STEPS

1. In Cisco Unified Communications Manager Administration, on the System menu, select **Enterprise Parameters**.

2. On the Enterprise Parameters Configuration page, under Security Parameters, locate the **Cluster Security Mode** field.
3. Confirm that the setting is **1**, which means that the CTL client is configured for mixed mode.

DETAILED STEPS

Step 1 In Cisco Unified Communications Manager Administration, on the System menu, select **Enterprise Parameters**.

Step 2 On the Enterprise Parameters Configuration page, under Security Parameters, locate the **Cluster Security Mode** field.

Step 3 Confirm that the setting is **1**, which means that the CTL client is configured for mixed mode.

Testing the Port Group Configuration

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.
2. On the Search Port Groups page, select the name of a port group.
3. On the Port Group Basics page, in the Related Links list, select **Test Port Group** and select **Go**.
4. When prompted that the test terminates all calls in progress, select **OK**.
5. Follow the steps for correcting the problems.
6. Repeat Step 3 through Step 5 until the Task Execution Results displays no problems.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.

Step 2 On the Search Port Groups page, select the name of a port group.

Step 3 On the Port Group Basics page, in the Related Links list, select **Test Port Group** and select **Go**.

Note The Test Port and Test Port Group utilities do not test IPv6 connectivity. Even when Unity Connection is configured to use IPv6 for a SCCP integration, the tests confirm that Unity Connection can communicate with the phone system using IPv4 addressing.

Step 4 When prompted that the test terminates all calls in progress, select **OK**.

The Task Execution Results displays one or more messages with troubleshooting steps.

Step 5 Follow the steps for correcting the problems.

If Cisco Unified CM is configured to block pings or if pings are disabled for the system, portions of the test fails. You must configure Cisco Unified CM and the system to enable pings so that the test can accurately test the port registration.

Step 6 Repeat Step 3 through Step 5 until the Task Execution Results displays no problems.

Matching the Security Mode Setting for Ports in Unity Connection and Cisco Unified Communications Manager (SCCP Integrations Only)

SUMMARY STEPS

1. In Cisco Unified Communications Manager Administration, on the Voice Mail menu, select **Cisco Voice Mail Port**. On the Find and List Voice Mail Ports page, select **Find**.
2. In the Device Security Mode column, note the security mode setting for the ports.
3. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.
4. On the Search Ports page, select the name of the first port.
5. On the Port Basics page, in the Security Mode field, select the setting that you noted in Step 2 and select **Save**.
6. Select **Next**.
7. Repeat Step 5 and Step 6 for all remaining ports.

DETAILED STEPS

Step 1 In Cisco Unified Communications Manager Administration, on the Voice Mail menu, select **Cisco Voice Mail Port**. On the Find and List Voice Mail Ports page, select **Find**.

Step 2 In the Device Security Mode column, note the security mode setting for the ports.

Step 3 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port**.

Step 4 On the Search Ports page, select the name of the first port.

Step 5 On the Port Basics page, in the Security Mode field, select the setting that you noted in Step 2 and select **Save**.

Step 6 Select **Next**.

Step 7 Repeat Step 5 and Step 6 for all remaining ports.

Matching the Security Mode Setting for Unity Connection Port Group and Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Step 1 In Cisco Unified Communications Manager Administration, on the System menu, select **SIP Profile** > **SIP Trunk Security Profile**.

Step 2 On the Find and List SIP Trunk Security Profiles page, select **Find**.

Step 3 Select the name of the SIP trunk security profile.

Step 4 On the SIP Trunk Security Profile Configuration page, note the setting of the Device Security Mode field.

Step 5 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.

Step 6 On the Search Port Groups, select the name of the applicable port group.

Step 7 On the Port Group Basics page, in the Security Mode field, select the setting that you noted in Step 4 and select **Save**.

Matching the Subject Name Fields of Unity Connection SIP Certificate and Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Step 1 In Cisco Unified Communications Manager Administration, on the System menu, select **SIP Profile > SIP Trunk Security Profile**.

Step 2 On the Find and List SIP Trunk Security Profiles page, select **Find**.

Step 3 Select the name of the SIP trunk security profile.

Step 4 On the SIP Trunk Security Profile Configuration page, note the setting of the X.509 Subject Name field.

Step 5 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Certificates**.

Step 6 On the Search SIP Certificates page, select the name of the SIP certificate.

Step 7 On the Edit SIP Certificate page, in the Subject Name field, enter the setting that you noted in Step 4 and select **Save**.

Matching the Port Used by Unity Connection SIP Security Profile and Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Step 1 In Cisco Unified Communications Manager Administration, on the System menu, select **SIP Profile > SIP Trunk Security Profile**.

Step 2 On the Find and List SIP Trunk Security Profiles page, select **Find**.

Step 3 Select the name of the SIP trunk security profile.

Step 4 On the SIP Trunk Security Profile Configuration page, note the setting of the Incoming Port field.

Step 5 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Security Profile**.

Step 6 On the Search SIP Security Profiles page, select the name of the SIP security profile with "TLS."

Step 7 On the Edit SIP Security Profile page, in the Port field, enter the setting that you noted in Step 4 and select **Save**.

Copying the Unity Connection Root Certificate to Cisco Unified Communications Manager

Copying the Root Certificate for Cisco Unified Communications Manager 4.x

Procedure

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security** > **Root Certificate**.
2. On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.
3. In the Save As dialog box, browse to the location on the Unity Connection server where you want to save the Unity Connection root certificate as a file.
4. In the Filename field, confirm that the extension is **.0** (rather than .htm), and select **Save**.
5. In the Download Complete dialog box, select **Close**.
6. Copy the Unity Connection root certificate file to the C:\Program Files\Cisco\Certificates folder on all Cisco Unified CM servers in this Cisco Unified CM phone system integration.
7. In Cisco Unity Connection Administration, in the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the Unity Connection to the Cisco Unified CM servers.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security** > **Root Certificate**.

Step 2 On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.

Step 3 In the Save As dialog box, browse to the location on the Unity Connection server where you want to save the Unity Connection root certificate as a file.

Step 4 In the Filename field, confirm that the extension is **.0** (rather than .htm), and select **Save**.

The certificate must be saved as a file with the extension .0 (rather than .htm) or Cisco Unified CM does not recognize the certificate.

Step 5 In the Download Complete dialog box, select **Close**.

Step 6 Copy the Unity Connection root certificate file to the C:\Program Files\Cisco\Certificates folder on all Cisco Unified CM servers in this Cisco Unified CM phone system integration.

Step 7 In Cisco Unity Connection Administration, in the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the Unity Connection to the Cisco Unified CM servers.

Copying the Root Certificate for Cisco Unified Communications Manager 5.x

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security** > **Root Certificate**.
2. On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.
3. In the Save As dialog box, browse to the location on the Unity Connection server where you want to save the Unity Connection root certificate as a file.
4. In the Filename field, confirm that the extension is **.pem** (rather than .htm), and select **Save**.
5. In the Download Complete dialog box, select **Close**.
6. Copy the Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.
7. If prompted, restart the Unity Connection software.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security** > **Root Certificate**.

Step 2 On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.

Step 3 In the Save As dialog box, browse to the location on the Unity Connection server where you want to save the Unity Connection root certificate as a file.

Step 4 In the Filename field, confirm that the extension is **.pem** (rather than .htm), and select **Save**.

The certificate must be saved as a file with the extension .pem (rather than .htm) or Cisco Unified CM does not recognize the certificate.

When Unity Connection is integrated with both Cisco Unified CM 4.x and Cisco Unified CM 5.x servers, you must copy the .pem file to the Cisco Unified CM 5.x server and the .0 file to the Cisco Unified CM 4.x server. Otherwise, authentication and encryption do not function correctly.

Step 5 In the Download Complete dialog box, select **Close**.

Step 6 Copy the Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.

The Unity Connection system clock must be synchronized with the Cisco Unified CM system clock for Cisco Unified CM authentication to function immediately. Otherwise, Cisco Unified CM does not let the Unity Connection voice messaging ports register until the Cisco Unified CM system clock has passed the time stamp in the Unity Connection device certificates.

a) On the Cisco Unified CM server, in Cisco Unified Operating System Administration, on the Security menu, select **Certificate Management > Upload Certificate/CTL**.
b) On the Cisco IPT Platform Administration page, select **Upload Trust Certificate** and **CallManager – Trust**, then select **OK**.
c) Browse to the Unity Connection root certificate that you saved in Step 4.
d) Follow the on-screen instructions.
e) Repeat Step 6a. through Step 6d. on all remaining Cisco Unified CM servers in the cluster.
f) In Cisco Unity Connection Administration, in the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the Unity Connection to the Cisco Unified CM servers.

   If the test is not successful, the Task Results list displays one or more messages with troubleshooting steps. After correcting the problems, run the test again.

g) In the Task Results window, select **Close**.

Step 7 If prompted, restart the Unity Connection software.

Copying the Root Certificate for Cisco Unified Communications Manager 6.x, 7.x, and Later

SUMMARY STEPS

1. In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security** > **Root Certificate**.
2. On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.
3. In the Save As dialog box, browse to the location on the Unity Connection server where you want to save the Unity Connection root certificate as a file.
4. In the Filename field, confirm that the extension is **.pem** (rather than .htm), and select **Save**.
5. In the Download Complete dialog box, select **Close**.
6. Copy the Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.

DETAILED STEPS

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Security** > **Root Certificate**.

Step 2 On the View Root Certificate page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.

Step 3 In the Save As dialog box, browse to the location on the Unity Connection server where you want to save the Unity Connection root certificate as a file.

Step 4 In the Filename field, confirm that the extension is **.pem** (rather than .htm), and select **Save**.

The certificate must be saved as a file with the extension .pem (rather than .htm) or Cisco Unified CM does not recognize the certificate.

When Unity Connection is integrated with both Cisco Unified CM 4.x and Cisco Unified CM 5.x and later servers, you must copy the .pem file to the Cisco Unified CM 5.x and later server and the .0 file to the Cisco Unified CM 4.x server. Otherwise, authentication and encryption do not function correctly.

Step 5 In the Download Complete dialog box, select **Close**.

Step 6 Copy the Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.

The Unity Connection system clock must be synchronized with the Cisco Unified CM system clock for Cisco Unified CM authentication to function immediately. Otherwise, Cisco Unified CM does not let the Unity Connection voice messaging ports register until the Cisco Unified CM system clock has passed the time stamp in the Unity Connection device certificates.

a) On the Cisco Unified CM server, sign in to Cisco Unified Operating System Administration.
b) In Cisco Unified Operating System Administration, on the Security menu, select **Certificate Management**.
c) On the Certificate List page, select **Upload Certificate**.
d) On the Upload Certificate page, in the Certificate Name field, select **CallManager-Trust**.
e) In the Root Certificate field, enter **Cisco Unity Connection Root Certificate**.
f) To the right of the Upload File field, select **Browse**.
g) In the Choose File dialog box, browse to the Unity Connection root certificate that you saved in Step 4.
h) Select **Open**.
i) On the Upload Certificate page, select **Upload File**.
j) Select **Close**.
k) Restart the Cisco Unified CM server.
l) Repeat Step 6a. through Step 6k. on all remaining Cisco Unified CM servers in the cluster.
m) In Cisco Unity Connection Administration, in the Related Links list, select **Check Telephony Configuration** and select **Go** to verify the Unity Connection to the Cisco Unified CM servers.

   If the test is not successful, the Task Results list displays one or more messages with troubleshooting steps. After correcting the problems, run the test again.

n) In the Task Results window, select **Close**.

CTL File with Expired Cisco Unified CM Certificate (Secure SIP Integration Only)

If secure SIP integration of Cisco Unity Connection failed, confirm the expiration of Cisco Unified CM Certificate by performing the following steps:

Step 1 In Cisco Unified Operating System Administration, navigate to **Security** > **Certificate Management**. On Certificate Management page, check the Expiration date for CallManager certificate in the certificate list. If CallManager certificates are expired, you must regenerate the certificates for Cisco Unified CM.

To generate the RSA based certificate of Cisco Unified CM, see "Generate and Upload Certificates" section of "Setting Up a Cisco Unified Communications Manager SIP Trunk Integration" chapter of *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 14*, available at https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

Step 2 After successful generating the certificates of Cisco Unified CM, generate the CTL files for the new certificates of Cisco Unified CM. For this, run **utils ctl update CTLFile** CLI command on the publisher node of Cisco Unified CM.

Step 3 Restart the TFTP and CallManager services on all of the nodes in the cluster that run these services.

Step 4 In Cisco Unity Connection Administration, navigate to **Telephony Integration** > **Port Group**. On Search Port Groups page, select the associated Port Group. On the Port Group Basics page, Select **Reset** under Reset Status field.

If you are still facing the issue for secure voice messaging ports, contact Cisco TAC.

Troubleshooting PIN Synchronization between Unity Connection and Cisco Unified CM

This chapter explains various problems that may occur while using PIN Synchronization feature along with the resolution.

Unable to Update PIN through Cisco Unity Connection Administration or Cisco PCA

While updating the voicemail PIN through Cisco Unity Connection Administration and Cisco Personal Communications Assistant (CPCA) with PIN Synchronization feature enabled, you may receive any of the following error messages:

- "Failed to update PIN on CUCM. Reason: Trivial credential"
- "Failed to update PIN on CUCM: Invalid credential length"
- "Failed to update PIN on CUCM. Reason: Duplicate credential found in history"

If you receive the above error messages, make sure that you entered a valid PIN as per the Credential Policy Configuration on Cisco Unified CM.

- "Bad response from CUCM. Reason: Requested resource is not available" or

  "Failed to connect to remote AXL server. Check IP address, port number, credentials, Call Manager version, and network status for any errors."

  If you receive any of the above error message, verify 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.

    To verify this, in Cisco Unity Connection Administration, navigate to **Telephony Integration** > **Phone System** and select the Phone System associated with the user. On the Phone System Basics page, navigate to **Edit** > **Cisco Unified Communication Manager AXL Servers**. On the Edit AXL Server page, select Test under section AXL Servers.
  - Proper tomcat certificates are uploaded for the AXL server.

    To verify this, on the Edit AXL Server page, select Test under section AXL Servers. To ignore the certificate validation errors, check the **Ignore Certificate Errors** check box on the Edit AXL Servers page.

- "Failed to update PIN on CUCM. Reason: Error getting the pin"

If you receive the "Failed to update PIN on CUCM. Reason: Error getting the pin" error message, make sure that the publisher server of Cisco Unified CM is up and running.

Unable to Update PIN through Telephone User Interface (TUI)

With PIN Synchronization feature enabled, if a user hears the "Your PIN has not been changed, for help press 0 or contact to your system administrator" error prompt while updating the phone PIN through TUI, you must verify the following:

- The username and password of primary AXL server entered on the Edit AXL Servers page are correct.
- The AXL server is up and running. To verify this, select Test on the Edit AXL Server page.
- Either Unity Connection has successfully validated the certificates for AXL server or **Ignore Certificate Errors** check box is checked on the Edit AXL Servers page.
- Authentication Rules on Cisco Unity Connection Administration are same as the Credential Policy Configuration on Cisco Unified CM and.
- A user has entered the valid PIN as per the credential policies.
- The publisher server of Cisco Unified CM is up and running.

Using Diagnostic Traces for PIN Synchronization

Related Diagnostic Traces:

If the CiscoSysLog contains the event "EvtAXLServerConnectionFailed", this confirms that Unity Connection is not able to connect with the AXL server.

You can also use Unity Connection traces to troubleshoot PIN Synchronization problems. You need to enable the following micro traces to troubleshoot the problems:

Error Scenario	Traces to set
PIN synchronization is failed on Cisco Unity Connection Administration	Cuca (all levels)
PIN synchronization is failed on Cisco PCA	CiscoPCA (level 00,01,02,13)
PIN synchronization is failed through Telephone User Interface	CDL (level 10 and 11) and ConvSub (level 01,03,04,05)
PIN synchronization is failed through API	VMREST (all levels)
PIN synchronization is failed through Bulk Administration Tool	Bulk Administration Tool (all levels)
AXL server issues	AxlAccess (level 00,01)
Certificate validation issues	Cuca (all levels)

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