CHAPTER 9

Troubleshooting the Phone System Integration in Cisco Unity Connection 8.x

See the following sections:

Diagnostic Tools in Cisco Unity Connection 8.x

There are diagnostic tools available to help you troubleshoot phone system integrations:

Configuring Cisco Unity Connection for the Remote Port Status Monitor

You can use the Remote Port Status Monitor for a real-time view of the 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 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.

To Configure Cisco Unity Connection for the Remote Port Status Monitor

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Conversations**.

Step 2 On the Conversation Configuration page, check the **Enable Remote Port Status Monitor Output** check box.

Step 3 In the IP Addresses Allowed to Connect for Remote Port Status Monitor Output field, enter the IP addresses of your workstations.

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

Step 4 Select **Save**.

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

Do the following procedure.

To Use 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 in Cisco Unity Connection 8.x

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" section on page 9-72.
- 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 in Cisco Unity Connection 8.x" section on page 2-3.

- *(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 Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Cisco Unity Connection 8.x Is Not Answering Any Calls

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

To Verify the Phone System Settings in Cisco Unity Connection Administration

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 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.

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

Cisco Unity Connection 8.x Is Not Answering Some Calls

When Cisco 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.

Task List for Troubleshooting Sporadic Answers on Incoming Calls

1. Confirm that the routing rules are working correctly. See the "Confirming Routing Rules" section on page 9-73.
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" section on page 9-74.

Confirming Routing Rules

By default, Cisco Unity Connection does not reject any calls. If routing rules have been changed, 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 in Cisco Unity Connection 8.x" section on page 2-3.

Confirming Voice Messaging Port Settings

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

To Confirm That Calls Are Being Sent to the Correct Voice Messaging Ports on Cisco Unity Connection

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.

If a voice messaging port is disabled or set incorrectly, it does not answer calls. Do the following procedure.

To Confirm That Voice Messaging Ports Are Enabled

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 Cisco Unity Connection 8.x with Cisco Unified Communications Manager

See the following sections for information on troubleshooting a Cisco Unified Communications Manager integration:

Viewing or Editing the IP Address of a Cisco Unified Communications Manager Server

Do the following procedure to view or change the IP address or other settings of a Cisco Unified Communications Manager server.

To Change Cisco Unified Communications Manager Server Settings

Step 1 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then 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 Are Repeatedly Disconnected in an SCCP Integration

When the Cisco Unity Connection voice messaging ports do not register with Cisco Unified CM in an SCCP integration, or if the 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.

Task List for Troubleshooting Port Registration Problems

1. Test the port group. See the "Testing the Port Group" section on page 9-75.
2. Confirm that another port group on the 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 Does Not Use the Same Device Name Prefix" section on page 9-76.
3. Confirm that another 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 Cisco Unity Connection Server Does Not Use the Same Device Name Prefix" section on page 9-77.

Testing the Port Group

Revised November 16, 2010

Do the following procedure.

To Test the Port Group

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 On the Port Basics page, you can test a single port in an SCCP integration by selecting **Test Port** in the Related Links list and selecting **Go**.

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

Step 4 When prompted that the test will 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.

Caution If Cisco Unified CM is configured to block pings or if pings are disabled for the system, portions of the test will fail. 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 Does Not Use the Same Device Name Prefix

Do the following procedure.

To Confirm That Another Port Group Does Not Use the Same Device Name Prefix

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, note the value of the Device Name Prefix field.

Caution 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 4 Select **Next** to view the next port group for which the integration method is SCCP (Skinny).

Step 5 If the value of the Device Name Prefix field is different from the value that you noted in Step 3, 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 Repeat Step 4 through Step 7 for all remaining port groups for which the integration method is SCCP (Skinny).

Confirming That Another Cisco Unity Connection Server Does Not Use the Same Device Name Prefix

Do the following procedure.

To Confirm That Another Cisco Unity Connection Server Does Not Use the Same Device Name Prefix

Step 1 In Cisco Unity Connection Administration on the first Cisco Unity Connection server, 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, note the value of the Device Name Prefix field.

Step 4 In Cisco Unity Connection Administration on the second Connection server, expand **Telephony Integrations**, then select **Port Group**.

Step 5 On the Search Port Groups page, select the name of a port group for which the integration method is SCCP (Skinny).

Step 6 On the Port Group Basics page, note the value of the Device Name Prefix field.

Caution 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 7 If the value of the Device Name Prefix field you noted in Step 6 is different from the value you noted on the first Connection server in Step 3, skip to Step 10. 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 8 Select **Save**.

Step 9 Select **Reset**.

Step 10 Select **Next**.

Step 11 Repeat Step 7 through Step 10 for all remaining port groups for which the integration method is SCCP (Skinny).

Ports Do Not Register in an IPv6 Configuration (Cisco Unity Connection 8.5 and Later)

Added November 16, 2010

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 by using the command-line interface (CLI), enter **show network ipv6 settings**.
   - To check by using Cisco Unified Operating System Administration, see the "Confirming that IPv6 is Enabled by Using Cisco Unified Operating System Administration" section on page 9-78.
2. Confirm that Connection is configured to use the appropriate addressing mode and preferences. See the "Confirming the IPv6 Addressing Mode and Preferences Settings" section on page 9-78
3. If you have configured an IPv6 host name for the 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 by using the CLI, enter **utils network ipv6 ping** <IPv6 host name>.
4. If you have configured the port group(s) in 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 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 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 by Using Cisco Unified Operating System Administration

To Confirm that IPv6 Is Enabled by Using Cisco Unified Operating System Administration

Step 1 In Cisco Unified Operating System Administration, from the Settings menu, select **IP**, then 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 Connection server. To apply the change, check Update with Reboot, and select **Save**. The Connection server will reboot in order for the change to take effect.

Confirming the IPv6 Addressing Mode and Preferences Settings

To Confirm the IPv6 Addressing Mode and Preferences Settings

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 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.

e. 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 Cisco 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.

Problems That Occur When Cisco Unity Connection Is Configured for Cisco Unified Communications Manager Authentication or Encryption

If problems occur when Cisco 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 Cisco 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.

Task List for Troubleshooting Problems When Cisco Unified Communications Manager Authentication or Encryption Is Configured

1. Confirm that the Cisco Unified CM CTL client is configured for mixed mode. See the "Confirming That the Cisco Unified Communications Manager CTL Client Is Configured for Mixed Mode" section on page 9-80.
2. Test the port group configuration. See the "Testing the Port Group Configuration" section on page 9-80.
3. For SCCP integrations, confirm that the security mode setting for the ports in Connection matches the security mode setting for the ports in Cisco Unified CM. See the "Matching the Security Mode Setting for Ports in Cisco Unity Connection and Cisco Unified Communications Manager (SCCP Integrations Only)" section on page 9-81.
4. For a SIP trunk integration, confirm that the security mode setting for the 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 the Cisco Unity Connection Port Group and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)" section on page 9-82.
5. For SIP trunk integrations, confirm that the Subject Name field of the 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 the Cisco Unity Connection SIP Certificate and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)" section on page 9-82.
6. For SIP trunk integrations, confirm that Connection and the SIP trunk use the same port. See the "Matching the Port Used by the Cisco Unity Connection SIP Security Profile and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)" section on page 9-83.
7. Copy the Connection root certificate to the Cisco Unified CM servers. See the "Copying the Cisco Unity Connection Root Certificate to the Cisco Unified Communications Manager Servers" section on page 9-83.

Confirming That the Cisco Unified Communications Manager CTL Client Is Configured for Mixed Mode

Do the following procedure.

To Confirm That the Cisco Unified Communications Manager CTL Client Is Configured for Mixed Mode

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

Revised November 16, 2010

Do the following procedure.

To Test the Port Group Configuration

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 Connection is configured to use IPv6 for a SCCP integration, the tests confirm that Connection can communicate with the phone system by using IPv4 addressing.

Step 4 When prompted that the test will 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.

Caution If Cisco Unified CM is configured to block pings or if pings are disabled for the system, portions of the test will fail. 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 Cisco Unity Connection and Cisco Unified Communications Manager (SCCP Integrations Only)

Do the following procedure.

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

Step 1 In Cisco Unified Communications Manager Administration, on the Voice Mail menu, select **Cisco Voice Mail Port**.

Step 2 On the Find and List Voice Mail Ports page, select **Find**.

Step 3 In the Device Security Mode column, note the security mode setting for the ports.

Step 4 Sign in to Cisco Unity Connection Administration.

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

Step 6 On the Search Ports page, select the name of the first port.

Step 7 On the Port Basics page, in the Security Mode field, select the setting that you noted in Step 3 and select **Save**.

Step 8 Select **Next**.

Step 9 Repeat Step 7 and Step 8 for all remaining ports.

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

Do the following procedure.

To Match the Security Mode Setting for the Cisco Unity Connection Port Group and the 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 Sign in to Cisco Unity Connection Administration.

Step 6 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.

Step 7 On the Search Port Groups, select the name of the applicable port group.

Step 8 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 the Cisco Unity Connection SIP Certificate and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Do the following procedure.

To Match the Subject Name Fields of the Cisco Unity Connection SIP Certificate and the 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 Sign in to Cisco Unity Connection Administration.

Step 6 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Certificate**.

Step 7 On the Search SIP Certificates page, select the name of the SIP certificate.

Step 8 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 the Cisco Unity Connection SIP Security Profile and the Cisco Unified Communications Manager SIP Trunk Security Profile (SIP Trunk Integrations Only)

Do the following procedure.

To Match the Port Used by the Cisco Unity Connection SIP Security Profile and the 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 Sign in to Cisco Unity Connection Administration.

Step 6 In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Security Profile**.

Step 7 On the Search SIP Security Profiles page, select the name of the SIP security profile with "TLS."

Step 8 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 Cisco Unity Connection Root Certificate to the Cisco Unified Communications Manager Servers

Do the applicable procedure:

- To Copy the Root Certificate for Cisco Unified Communications Manager 4.x, page 9-83
- To Copy the Root Certificate for Cisco Unified Communications Manager 5.x, page 9-84
- To Copy the Root Certificate for Cisco Unified Communications Manager 6.x, 7.x, and Later, page 9-85

To Copy the Root Certificate for Cisco Unified Communications Manager 4.x

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 Cisco Unity Connection server where you want to save the Connection root certificate as a file.

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

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

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

Step 6 Copy the Cisco 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 connection to the Cisco Unified CM servers.

To Copy the Root Certificate for Cisco Unified Communications Manager 5.x

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 Cisco Unity Connection server where you want to save the Connection root certificate as a file.

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

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

When Cisco 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 will not function correctly.

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

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

Caution The Cisco 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 will not let the Connection voice messaging ports register until the Cisco Unified CM system clock has passed the time stamp in the 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 Cisco 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 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 Cisco Unity Connection software.

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

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 Cisco Unity Connection server where you want to save the Connection root certificate as a file.

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

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

When Cisco 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 will not function correctly.

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

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

Caution The Cisco 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 will not let the Connection voice messaging ports register until the Cisco Unified CM system clock has passed the time stamp in the 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 Cisco 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 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**.