CHAPTER 1

Getting Started in Cisco Unified Presence Administration

June 11, 2009

Completing Cisco Unified Presence Post-Installation Setup

The first time you sign in to Cisco Unified Presence Administration after a fresh installation of Cisco Unified Presence, a post-installation deployment wizard starts.

You are required, only once after a fresh installation, to configure the Cisco Unified Communications Manager Publisher and AXL information on the Cisco Unified Presence publisher node. If you are installing a subsequent Cisco Unified Presence node, you are not required to enter the Cisco Unified Communications Manager publisher information because the subsequent Cisco Unified Presence node will obtain this information from the publisher Cisco Unified Presence node.

Note The next time you sign in to Cisco Unified Presence Administration, the application automatically detects that you have completed the post-installation configuration and the Cisco Unified Presence Administration window displays.

Before You Begin

- Obtain the IP address of Cisco Unified Communications Manager publisher (if you are not using DNS).
- Always run the Post Installation Deployment wizard immediately after you perform a fresh installation of Cisco Unified Presence, and *before* you back up or restore your data in the Disaster Recovery System.

Caution The operation fails if you install Cisco Unified Presence and attempt to back up or restore data in the Disaster Recovery System before you run the Post Installation Deployment wizard. For more information, see the *Disaster Recovery System Guide for Cisco Unified Presence*.

Procedure

Step 1 Sign in to Cisco Unified Presence Administration.

Step 2 Complete the Post Installation Deployment wizard, as follows:

Window	Configuration Steps
Post Installation Deployment Window Page 1 of 4	**a.** Enter the Cisco Unified Communications Manager publisher hostname in the Hostname field. **b.** **[optional]** Enter the Cisco Unified Communications Manager publisher IP address in the IP address field. **Note** If your network does not have DNS, you must enter an IP address because the hostname will not automatically resolve to an IP address. If the hostname can resolve to an IP address using DNS, you can leave the IP address blank and the application detects the IP address automatically. **c.** Change and confirm the security password provided during the initial installation of Cisco Unified Presence. **d.** Select **Next.**
Post Installation Deployment Window Page 2 of 4	**a.** Enter the user ID for the appropriate application user, who is assigned the Standard AXL API Access role on the associated Cisco Unified Communications Manager publisher server. **Note** By default, the Standard AXL API Access role is assigned to the CCMAdministrator application user. **b.** Enter and confirm the AXL password. **c.** Select **Next.**

Window	Configuration Steps
Post Installation Deployment Window Page 3 of 4	Verify that your configuration and complete one of the following actions: – Select **Back** to correct an error. – Select **Confirm** to proceed.
Post Installation Deployment Window Page 4 of 4	Perform one of the following actions: – Select **Home** to view the Cisco Unified Presence Administration window. – Select **System Dashboard** to view the Cisco Unified Presence System Dashboard window. – Select **Topology** to view the System Topology window.

Troubleshooting Tips

- If an error message displays, you can check that AXL is running on Cisco Unified Communications Manager and that you have the correct User ID and password. Using a browser, enter *http://<<CUCM Hostname>>/axl*. You will be prompted for the User ID and password. If the details that you enter are correct, a web page displays confirmation that AXL is running and ready to receive requests.
- You cannot run the Post Installation Deployment wizard a second time. If you need to change the publisher address of Cisco Unified Communications Manager or AXL information after this initial configuration, use the Cisco Unified Communications Manager Publisher page in Cisco Unified Presence Administration.
- The IP address field [Page 1 of 4] is a required field if your network does not have DNS because the hostname that you enter will not resolve to an IP address. If the hostname resolves to an IP address, you can leave the IP address blank and the application detects the IP address automatically.

Related Topics

- •, page 1-3
- Changing Cisco Unified Communications Manager Publisher Information, page 4-1
- *Disaster Recovery System Guide for Cisco Unified Presence*

How to Access Cisco Unified Presence Administration

-
- Signing In to Cisco Unified Presence Administration, page 1-4
- Signing Out of Cisco Unified Presence Administration, page 1-4
-

Signing In to Cisco Unified Presence Administration

Before You Begin

- Obtain the server name or IP address of your Cisco Unified Presence server.
- Obtain the application username and password that you specified during the Cisco Unified Presence installation.
- If this is your first time to sign in to Cisco Unified Presence Administration after installing Cisco Unified Presence, you must complete the Post Installation Deployment wizard.
- Turn off the Security Alert dialog if required.

Procedure

Step 1 Start your operating system browser, Internet Explorer (IE) 6.x.

Step 2 Enter the following case-sensitive URL in the address bar of the web browser:

https://<*server-name*>

where: <*server-name*> equals the name or IP address of the server

Step 3 Select **Cisco Unified Presence Administration**.

Step 4 Select the appropriate option when the Security Alert dialog box displays.

Step 5 Complete the following actions in the Logon window:

a. Enter the application user password that you specified during Cisco Unified Presence installation.

b. Select **Submit**.

Troubleshooting Tips

- For security purposes, Cisco Unified Presence Administration signs you out after 30 minutes, and you must sign back in to continue using it.
- If multiple users sign in to Cisco Unified Presence Administration simultaneously, it can cause performance to suffer. Try to limit the number of users and administrators that sign in simultaneously to Cisco Unified Presence Administration.

Related Topics

- Completing Cisco Unified Presence Post-Installation Setup, page 1-1
- Disabling the Security Alert Dialog, page 1-7

Signing Out of Cisco Unified Presence Administration

Select **Log Off** in the upper, right corner of the main Cisco Unified Presence Administration window.

About the Cisco Unified Presence Administration Interface

- Cisco Unified Presence Administration Menu Options, page 1-5
- Cisco Unified Communications Manager Publisher Link, page 1-5

Cisco Unified Presence Administration Menu Options

After you sign in, the main Cisco Unified Presence Administration window displays. The window includes the list box called Navigation in the upper, right corner. To access the applications in the list box, select the application that you want and select Go. The choices in the list box include the following Cisco Unified Presence applications:

- Cisco Unified Presence Administration— Shows as the default option when you access Cisco Unified Presence. Use Cisco Unified Presence Administration to configure system parameters, applications, and much more.
- Cisco Unified Serviceability—Takes you to the main Cisco Unified Presence Serviceability window that is used to configure trace files and alarms and to activate and deactivate services.
- Cisco Unified OS Administration—Takes you to a sign in window, so you can configure and administer the Cisco Unified Presence platform.
- Disaster Recovery System—Takes you to the Cisco Disaster Recovery System, a program that provides full data backup and restore capabilities for all servers in a Cisco Unified Presence cluster.

These applications include additional security, so you must enter a User ID and password before you can access these applications.

Both Cisco Unified Presence Administration and Cisco Unified Serviceability share the same security access and therefore do not require authentication when navigating between these two applications. However, authentication is required if you navigate from Cisco Unified Presence Administration to either the Cisco Unified Communications Operating System platform or Disaster Recovery System for Cisco Unified Presence, or vice versa.

Cisco Unified Communications Manager Publisher Link

The Cisco Unified Presence Administration main window provides a link directly to the associated Cisco Unified Communications Manager publisher server. To access Cisco Unified Communications Manager Administration, select the IP address of the Cisco Unified Communications Manager Publisher at the bottom of the window.

How to Configure Accessibility in Cisco Unified Presence Administration

Cisco Unified Presence Administration and Cisco Unified Presence User Options provide functionality that allows users to access buttons on the window without using a mouse. You can perform the following procedures from any point on the window, so the user does not need to scroll or tab through various fields.

- Accessing the Icons in the Window, page 1-5
- Accessing the Buttons in the Window, page 1-6

Accessing the Icons in the Window

Many windows in Cisco Unified Presence have icons that display at the top of the window; for example, an icon of a disk for Save, an icon that is a plus sign (+) for Add, and so on.

Procedure

Step 1 Press **Alt**, press **1**, and then press **Tab**.

Step 2 The cursor will highlight the first icon from the left. Press **Tab** again to move to the next icon.

Step 3 Press **Enter** to perform the function of the icon.

Accessing the Buttons in the Window

Many of the windows in Cisco Unified Presence have buttons that display at the bottom of the window; for example, a button for Save, a button for Add, and so on.

Procedure

Step 1 Press **Alt**, press **2**, and then press **Tab**.

Step 2 The cursor will highlight the first button from the left. Press **Tab** again to move to the next button.

Step 3 Press **Enter** to perform the function of the button.

How to Secure Communication Between Browsers and Cisco Unified Presence

Web Browser Sessions

You access the Cisco Unified Presence Administration program from a PC that is not the web server and that does not have Cisco Unified Presence installed. No browser software is provided on the server so you must have a browser installed on the computer from which you want to access Cisco Unified Presence Administration. Cisco Unified Presence Administration supports Microsoft Internet Explorer (IE) 6.x.

As you work in a browser session, consider the following:

- The cookies on the client machine store your find and list search preferences. If you navigate to other menu items and return to this menu item, or if you close the browser and then open a new browser window, the system retains your Cisco Unified Presence search preferences until you modify your search.

- When the Find and List window displays for a feature, records from an active (prior) query may also display in the window.
- To add additional search criteria as you filter records, select the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, select the – button to remove the last added criterion. Alternatively, select Clear Filter to remove all added search criteria.
- When the matching records display, you can change the number of items that display in each window by choosing a different value from the Rows per Page list box.

Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the web server (for Microsoft Windows users), uses a certificate and a public key to encrypt the data that is transferred over the internet. HTTPS also ensures that the user sign in password transports securely via the web. The following Cisco Unified Presence applications support HTTPS, which ensures the identity of the server:

- Cisco Unified Presence Administration
- Cisco Unified Serviceability
- Cisco Unified Presence User Options
- Real-Time Monitoring Tool (RTMT)
- The XML (AXL) application programming interface

A self-signed certificate is generated on the web server at installation (the certificate is also migrated during upgrades).

Security Alerts

When you (or a user) access Cisco Unified Presence Administration from a browser client, a Security Alert dialog box asks whether you trust the server. When the dialog box displays, you must perform one of the following tasks:

- By selecting **Yes**, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.
- By selecting **View Certificate > Install Certificate**, you indicate that you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.
- By selecting **No**, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must select Yes or install the certificate using the **View Certificate > Install Certificate** option.

Disabling the Security Alert Dialog

You can save the CA Root certificate in the trusted folder, so the Security Alert dialog box does not display each time that you access the web application.

Procedure

Step 1 Browse to the application on the web server.

Step 2 Select **View Certificate** when the Security Alert dialog box displays.

Step 3 Select **Install Certificate** in the Certificate pane.

Step 4 Select **Next**.

Step 5 Select **Place all certificates in the following store**.

Step 6 Select **Browse**, and browse to Trusted Root Certification Authorities.

Step 7 Select **Next**.

Step 8 Select **Finish**.

Step 9 Select **Yes** to install the certificate.

Step 10 Select **OK**. when a message states that the import was successful.

Step 11 Select **OK** in the lower, right corner of the dialog box.

Step 12 To trust the certificate, so you do not receive the dialog box again, select **Yes**.

Troubleshooting Tips

If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Displaying Cisco Unified Presence Administration in Internet Explorer with HTTPS

Procedure

Step 1 Open your IE browser.

Step 2 Select **Tools > Internet Options.**

Step 3 Select the Security tab.

Step 4 Select **Trusted sites**.

Step 5 Select **Sites**.

Step 6 Enter the web address of Cisco Unified Presence Administration, for example, https://<hostname>.

Step 7 Select **Add**.

Step 8 Select **OK.**

Troubleshooting Tips

- If you use version 6.1 of Internet Explorer to sign in to the Cisco Unified Presence Administration, the interface list boxes may be turned off after you sign in for the first time. This condition occurs if the Cisco Unified Presence server is not recognized as a trusted site. Add the Cisco Unified Presence server hostname to the list of trusted sites.

- If you access the web application by using the hostname and install the certificate in the trusted folder and then try to access the application by using the localhost or IP address, the Security Alert dialog box displays to indicate that the name of the security certificate does not match the name of the site.
- If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

How to Find and Delete Components in Cisco Unified Presence Administration

Finding a Network Component

Cisco Unified Presence allows you to locate specific network components on the basis of specific criteria. This find and list functionality is common to all the components in your network.

Before You Begin

If you are searching for an intercluster peer, ensure that the Intercluster Sync Agent service is running. If the Intercluster Sync Agent service is not running when the InterCluster Find and List window displays, a warning message will inform you that the service is necessary for the propagation of availability information across multiple clusters in Cisco Unified Presence.

Procedure

Step 1 Select a component in Cisco Unified Presence Administration. For example, select **Presence > Gateways**.

Step 2 To find all records in the database, ensure that the dialog box is empty; go to Step 4.

Step 3 To filter or search records, complete one of the following actions:

- From the first list box, select a search parameter.
- From the second list box, select a search pattern.
- From the third list box, select a search pattern.
- Specify the appropriate search text, if applicable.

Step 4 Select **Find**.

Step 5 From the list of records that display, perform one or more of the following actions:

If you want to:	Action
View a record	Select the link for the record.
Add a selected record	Complete the following actions: a. Check the check box adjacent to the component you want to view. b. Select **Add Selected**.
Reverse the sort order in the record list	Select the up or down arrow, if available, in the list header.

Troubleshooting Tips

If you use the "Search" capability in the Presence Viewer, a popup window displays in which you can select one or more users using a Find and List query. If you select more than one user, the Presence Viewer will display Next and Previous buttons in the upper right hand corner of the window to allow you to navigate through the users that you have selected.

Related Topics

- Web Browser Sessions, page 1-6
- Finding Licensed Users, page 2-2

Deleting a Network Component

Before You Begin

Find the network component.

Procedure

Step 1 From the list of matching records, select the gateway that you want to delete.

Step 2 Perform one of the following actions to delete the gateway:

If you want to:	Action
Delete a selected record	**a.** Check the appropriate record. **b.** Complete one of the following actions: • Select **Delete Selected** at the bottom of the window**.** • Select the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window.
Delete all records	**a.** Check **Select All.** **b.** Select **Delete Selected.**

Troubleshooting Tips

- If the network component is not in use, Cisco Unified Presence deletes it. If it is in use, a message displays.
- You cannot edit or delete an incoming ACL list that is associated with a Federated Domain entry. These ACL lists are automatically added when you add a Federated Domain entry to the database.
- When you delete a federated domain, the associated incoming ACL is also deleted. The associated presence gateway is also deleted if no other federated domains are associated with the presence gateway.
- You cannot delete a standard role.
- If you delete any of the following components, you must restart the SIP proxy server before any changes that you make take effect:
  - TLS peer subject
  - TLS context
  - Application Listener

  To restart the proxy server, select **Presence > Routing > Settings**.

Related Topics

Finding a Network Component, page 1-9

Where to Find More Information

- *Installation and Upgrade Guide for Cisco Unified Presence*

  This document describes procedures to follow when installing or upgrading Cisco Unified Presence.
- *Cisco Unified Communications Operating System Maintenance Guide for Cisco Unified Presence*

  This document provides information about software upgrades, and informs you how to access and use the utilities that are available through the operating system interface and the command line interface.
- *Serviceability Configuration and Maintenance Guide for Cisco Unified Presence*

This document provides step-by-step instructions for configuring, maintaining, and administering alarms, traces and real-time monitoring of Cisco Unified Presence components.

- *Cisco Unified Presence Deployment Guide*

  This document provides an overview of the configuration process for Cisco Unified Presence and Cisco Unified Communications Manager, as well as information about integrating Cisco Unified Presence with Microsoft Live Communications Server, Microsoft Active Directory, and Microsoft Office Communicator.

- *Disaster Recovery System Guide for Cisco Unified Presence*

  This document describes how to configure the backup settings, back up Cisco Unified Presence data, and restore the data.

- For product compatibility information relating to a Cisco Unified Presence release, refer to the *Hardware and Software Compatibility Information for Cisco Unified Presence* at the following URL:
  http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

- For port information relating to a Cisco Unified Presence release, refer to the *Port Usage Information for Cisco Unified Presence* at the following URL:
  http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html