Setting Up Access to Cisco Personal Communications Assistant

Setting Up Access to Cisco Personal Communications Assistant

Introduction

The Cisco Personal Communications Assistant (PCA) is installed on the Cisco Unity Connection server during installation. It is a website that provides users with access to the Cisco Unity web tools, which allow users to manage messages and personal preferences in Unity Connection. The web tools available in the Cisco PCA include:

- Messaging Assistant
- Cisco Unity Connection Personal Call Transfer Rules

To learn more about the tools listed above, see the applicable *User Guide for Cisco Unity Connection* and the Help for each tool.

Configuring a Web Browser to Access Cisco PCA

The browsers on each user workstation must be set up to use the Cisco PCA and the Cisco Unity Connection web tools. See the applicable section, depending on the browser installed on the computer:

For the list of versions supported for each browser, see the *Compatibility Matrix for Cisco Unity Connection* , available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html.

Apple Safari

Do the following tasks to set up Safari for accessing the Cisco PCA.

1. Confirm that the software required for correct browser configuration is installed. See the "Software Requirements-User Workstations" section of the *System Requirements for Cisco Unity Connection Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html.

2. Configure Safari:
   a. Enable Java.
   b. Enable Java Script.
   c. Accept cookies only from sites that you navigate to.

Microsoft Internet Explorer

Do the following tasks to set up Internet Explorer for accessing the Cisco PCA.

1. Confirm that the software required for correct browser configuration is installed. See the "Software Requirements-User Workstations" section of the *System Requirements for Cisco Unity Connection Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html.
2. Configure Internet Explorer:
   a. Enable Active scripting.
   b. Download and run ActiveX controls.
   c. Enable Java scripting.
   d. Accept all cookies.
   e. Automatically check for newer versions of temporary Internet files.
   f. Enable Medium-High privacy.

Mozilla Firefox

Do the following tasks to set up Firefox for accessing the Cisco PCA.

1. Confirm that the software required for correct browser configuration is installed. See the "Software Requirements-User Workstations" section of the *System Requirements for Cisco Unity Connection Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html.
2. If users are running Firefox on Apple MAC OS X or Microsoft Windows workstations, skip to Task 3.

   If users are running Firefox on Linux Red Hat workstations, confirm that they are using the correct sound card by referring to the sound card support matrix on the Alsa-project.org website. (Note that the Java Runtime Environment (JRE) plug-in software uses the Advanced Linux Sound Architecture (ALSA) driver to access system sound devices and to control playback and recording functionality. Depending on the sound card, playback and recording capabilities may be limited.)
3. Configure Firefox:
   a. Enable Java.
   b. Enable Java Script > Enable Change Images in Java Script Advanced.
   c. Allow sites to set cookies. (For security purposes, we recommend that you set this to Allow Sites to Set Cookies for the Originating Web Site Only.)

Changing the GUI Language for the Cisco PCA

Do the following tasks to change the GUI language that is used in the Cisco PCA.

1. Download and install the applicable languages. For instructions, see the applicable documentation:

- • For a new Unity Connection server, see the "Installing Unity Connection Language Files" section of the "Maintaining Cisco Unity Connection Server" chapter of the *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection*, Release 14, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html.
- • For an existing Unity Connection server, see the "Removing Unity Connection Languages" section of the "Maintaining Cisco Unity Connection Server" chapter of the *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 14*, at at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html.

2. On the user workstation, select a language in the web browser. The language selected in the browser must be one of the languages that the Cisco PCA offers and it must be installed on the Unity Connection server. For a list of supported languages, see the "Available Languages for Unity Connection Components" section of the *System Requirements for Cisco Unity Connection Release 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html.

Managing Security Alerts Using Self-Signed Certificates with SSL Connections

If you use the self-signed certificate generated during installation to provide an SSL, Unity Connection to the Cisco PCA, the web browser of the user displays a message to alert the user that the authenticity of the site cannot be verified, and therefore its content cannot be trusted. Similarly, if you use a self-signed SSL certificate to secure IMAP email client access to Unity Connection, some email clients supported for use with Unity Connection display SSL security messages.

Although users can still access Unity Connection despite the alerts, consider one of the following options to manage or eliminate security alerts when users browse to the Cisco PCA and/or access their messages from an IMAP email client:

- Add the SSL certificate to the Trusted Root Store on each user workstation. In this way, you can ensure that users never see the security alert. Do the following Adding the SSL Certificate to the Trusted Root Store on User Workstations, on page 3 procedure.
- Tell users to choose the "Accept Permanently" (or similar) option when the browser or email client displays the alert and asks them how to proceed. After instructing the browser and/or email client to always accept the certificate, the user will not see the alert again.

Adding the SSL Certificate to the Trusted Root Store on User Workstations

Procedure

	Command or Action	Purpose
Step 1	From the OS Administration application on the Unity Connection server, right-click to download the certificate and save it as a file.	
Step 2	Copy the certificate to each user workstation, and then import it using tools in the browser or IMAP client, as applicable.	