Troubleshooting Cisco Personal Communications Assistant (PCA)

Overview

The Cisco Personal Communications Assistant (PCA) is a portal that provides access to the Cisco Unity Connection web tools for users to manage messages and personal preferences in Unity Connection. The Unity Connection web tools include the Messaging Assistant, the Messaging Inbox, and the Cisco Unity Connection Personal Call Transfer Rules. The Cisco PCA is installed on the Unity Connection server during installation.

Following are the tasks to troubleshoot problems with Cisco Personal Communications Assistant:

- If there is an error message associated with the problem, review the Cisco PCA Error Messages.
- Review the Users cannot Access Cisco PCA Pages to consider the most common reasons why users cannot access the Cisco PCA pages, including use of an incorrect URL, incorrect browser settings, or the presence of unsupported software installed on the workstation.
- If users cannot browse to the Cisco PCA website at all or have trouble accessing the Cisco PCA applications, see the Troubleshooting User and Administrator Access chapter for the applicable troubleshooting procedures.
- If the problem is that Media Master does not show up correctly or at all, see the Troubleshooting MediaMaster chapter.
- If the problem is that the menu bar does not display any text, see the Missing Text on the Menu Bar (Microsoft Windows Only).
- Confirm that the Tomcat service is running. See the Verifying if Tomcat Service is Running.

- Confirm whether appropriate changes have been made in the browser settings to support the locales.

If you cannot resolve the problem and plan to report the problem to Cisco TAC, you are asked to provide information about your system and about the problem.

Users cannot Access Cisco PCA Pages

Users use the Cisco Personal Communications Assistant (PCA) website to access the Messaging Assistant, and the Personal Call Transfer Rules pages.

When a user cannot access the Cisco PCA pages, consider the following possible causes.

- **The Cisco PCA URL is case-sensitive**—Users can access the Cisco PCA at the following URL: http://<Cisco Unity Connection server>/ciscopca. Note, however, that the URL is case-sensitive.
- **The browser or client configuration is not configured properly**—When a user cannot access any of the Cisco PCA pages, it may be that the user browser or client workstation is not configured properly. Make sure that the browser and client workstation are configured as specified in the User Workstation Setup Guide for Cisco Unity Connection *Release 11.x*. The guide is available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user_setup/guide/b_11xcucuwsx.html.
- **Unsupported software is installed on the client workstation**—Confirm that the user does not have an unsupported combination of software or an unsupported third-party application installed on the workstation. See the Compatibility Matrix: Cisco Unity Connection and the Software on User Workstations, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/compatibility/matrix/cucclientmtx.html.

Also note that the users can access the Web Inbox URL, and link to the Messaging Assistant and Personal Call Transfer Rules pages from there. The Web Inbox URL is http://<Unity Connection server>/inbox.

Security Alert Displayed When Users Access Cisco Personal Communications Assistant Pages

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 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. See the following Adding the SSL Certificate to the Trusted Root Store on User Workstations procedure.
- Tell users to select 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 does not see the alert again.

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

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.

Users cannot Access Unity Connection Web Tools from Cisco PCA

When users can access the Cisco Personal Communications Assistant (PCA), but cannot access the Messaging Assistant, or the Personal Call Transfer Rules, consider the following possible causes:

- In order to access the Messaging Assistant, users must be given the proper class of service rights on the Class of Service > Edit Class of Service page or the Class of Service > New Class of Service page in Cisco Unity Connection Administration. The class of service that the user is assigned to must have the "Allow Users to Use the Messaging Assistant" setting enabled.

Note Web Inbox has replaced the Messaging Inbox. See the Troubleshooting Cisco Personal Communications Assistant (PCA) chapter for Web Inbox troubleshooting information.

- In order to access the Personal Call Transfer Rules, users must be given the proper class of service rights on the Class of Service > Edit Class of Service page or the Class of Service > New Class of Service page in Cisco Unity Connection Administration. The class of service that the user is assigned to must have the "Allow Users to Use Personal Call Transfer Rules" setting enabled.

Users cannot Save Changes on Pages in Cisco PCA

When user browser settings are set to cache temporary Internet pages automatically, users can create a bookmark or favorite to access a Messaging Assistant, or Personal Call Transfer Rules web page. However, the page is read-only. Explain to users that they should bookmark the Cisco PCA home page rather than individual pages. Also note that users should not change their browser settings as a workaround; when the browser is not set to automatically check for newer versions of temporary Internet files, the Media Master control is not displayed correctly.

Cisco PCA Error Messages

In addition to browser error messages (such as "File not found" or "Unauthorized access"), users may see Cisco PCA-specific error messages, Java plugin error messages, and Tomcat error messages when signing in

to the Cisco PCA, or when using the Messaging Assistant, the Messaging Inbox, or Cisco Unity Connection Personal Call Transfer Rules.

The four types of error messages that users may encounter are described in the following table:

Browser error messages	Browser error messages may indicate that the Cisco PCA failed to install, the user does not have network access to the Unity Connection server, the browser is not configured correctly, or the user does not have the required security certificate installed (if the Cisco PCA uses SSL connections).
Cisco PCA-specific error messages	Cisco PCA-specific error messages are displayed on the Sign-In page or another Cisco PCA page, and typically indicate problems with user credentials or actions within the Cisco PCA.
Java Plugin error messages	Java Plugin-specific error or warning messages are pop-up alerts that occur on pages that load the Java plugin to integrate the Media Master in a web page. These messages typically appear the first time that the Java plugin is loaded when you navigate to a page that contains the Media Master.
Tomcat error messages	Tomcat errors occur when there is a system error, such as file corruption or insufficient memory on the Unity Connection server. A Tomcat error message usually lists the sequence of application errors. Each exception is followed by a description of what the Tomcat service was attempting to do when the error occurred, and for some exceptions, a message explaining the error is also offered. The "Exception" and "Root Cause" sections in the error message may offer additional information about the problem.

Error Message: "Sign-In Status – Account Has Been Locked."

When users encounter the error message "Sign-in status – account has been locked," it is possible that the user exceeded the number of failed sign-in attempts that is allowed. (This limit is set on the System Settings > Authentication Rules page in Cisco Unity Connection Administration.) It may also be possible that the user forgot his or her credentials, or an unauthorized user attempted to gain access.

Use the following task list to determine the source of the problem and correct it.

1. To confirm that the account is locked, in Cisco Unity Connection Administration, go to the Users > Edit Password Settings page for the individual user, and select Web Application from the Choose Password menu. Under Web Applications Password Settings, you can verify the status of the user credentials to determine whether the password was locked by an administrator, there were failed sign-in attempts, or the password was locked after an excessive number of failed sign-in attempts.
2. To unlock the user account, in Cisco Unity Connection Administration, go to the Users > Edit Password Settings page for the individual user, and select Web Application from the Choose Password menu. Under Web Applications Password Settings, select Unlock Password.

Note When the default application administration account is locked, for example, because the password has expired or because of too many unsuccessful sign in attempts, no application administration account is allowed to sign in to Cisco Unified Serviceability. (You specify the account name and password for the default application administration account during installation, and you create and administer additional application administration accounts in Cisco Unity Connection Administration.) To unlock the account, change the password using the utils cuc reset password CLI command. Changing the password also unlocks the account. (If an account has been hacked, you do not want to unlock it without also changing the password.)

Error Message: "Apache Tomcat/<Version> – HTTP Status 500 – Internal Server Error."

File corruption at the time of installation or a Tomcat memory corruption can cause users to encounter the error message "Apache Tomcat/<version> – HTTP status 500 – internal server error." To confirm that this is the cause of the problem, check the Tomcat error page for the indicated root cause for the exception. If an exception message similar to the one below exists, there is a file or memory corruption:

java.lang.ClassFormatError: <classpath>/<classname> (Illegal constant pool index)

Contact Cisco TAC.

Error Message: "Site is Unavailable."

If users encounter the error message "Site is unavailable," confirm that the Apache Tomcat service is running. See the Verifying if Tomcat Service is Running.

Error Message: "Failed to <Save Message>" While Using PC Microphone in Cisco Unity Connection Administration or Cisco PCA

While uploading an existing .wav file, or saving a new recorded message as a voice name or greeting using the PC microphone, the user receives an error message for failed operation. For example, if a user is saving a new greeting using PC microphone, the user receives "Failed to Save Greeting" error message. This error message appears if the user is using either the Cisco Unity Connection Administration (CUCA) or the Cisco Personal Communications Assistant (CPCA) web application of Cisco Unity Connection. The following exception also appears in the client side Java Console logs:

Exception in thread "Timeout guard" java.security.AccessControlException: access denied (java.net.SocketPermission 10.93.231.234:8443 connect,resolve)

To send the recorded message successfully, add the below entry in the client side JRE security profile file, that is commonly named as **java.policy** using the IP address of the Unity Connection server. For a cluster, you may need to add an entry for each of publisher and subscriber.

permission java.net.SocketPermission "10.93.237.101:8443", "connect,resolve";

If you get a permission error while trying to modify the java.policy security profile file, you may need to set the permissions of the file to not inherent permissions from its parent and not be read-only.

Error Message: "Application Blocked by Security Settings. Your security settings have blocked a self-signed application from running

The users receive an error message: "Application Blocked by Security Settings. Your security settings have blocked a self-signed application from running", under the following conditions:

- While uploading an existing .wav file or saving a new recorded message as a voice name or
- While uploading an existing .wav file or saving a new recorded message as a greeting.

Using Media Master bar with Java version 7 latest update on IE as the web browser.

To correct the problem, follow the given steps:

1. Select Security tab of Java Control panel.
2. Select Add in the Exception Site List window.
3. Type the URL into the empty field that is provided under Location.
4. Continue to select Add and enter URLs until your list is complete. Select OK to save the URLs that you entered.
5. If you select Cancel, the URLs are not saved.

Error Message "Access denied" When Trying to Play Recordings through Media Master Using Phone

If a user opens Cisco Personal Communications Assistant (CPCA) through Web Inbox and try to play recordings, the user receives the error "Access Denied". To correct the problem, open Cisco PCA directly in a new window instead of opening through Web Inbox and play the recordings

Missing Text on the Menu Bar (Microsoft Windows Only)

If the menu bar of the Cisco Personal Communications Assistant web tool is missing text and only displays down arrows to signify the menu items, do the following procedure.

Re-Registering DLLs Required for the Cisco Personal Communications Assistant Menu Bar

Step 1 On the user workstation, select Start and select Run.

Step 2 In Run window, enter **regsvr32 msscript.ocx** and select OK.

Step 3 In the dialog box that indicates that the DLL registration succeeded, select OK.

Step 4 Select Start and select Run.

Step 5 In Run window, enter regsvr32 dispex.dll and select OK.

Step 6 In the dialog box that indicates that the DLL registration succeeded, select OK.

Step 7 Select Start and select Run.

Step 8 In Run window, enter regsvr32 vbscript.dll and select OK.

Step 9 In the dialog box that indicates that the DLL registration succeeded, select OK.

Verifying if Tomcat Service is Running

Do the following tasks to confirm that the Tomcat service is running and if necessary, to restart the Tomcat service:

1. Confirm that the Tomcat service is running using either Real-Time Monitoring Tool (RTMT) or the Command Line Interface (CLI). Do the applicable procedure:
   - Confirming That the Tomcat Service Is Running Using Real-Time Monitoring Tool (RTMT)
   - Confirming That the Tomcat Service Is Running Using the Command Line Interface (CLI)
2. If necessary, restart the Tomcat service using the Command Line Interface (CLI). See the Restarting the Tomcat Service Using the Command Line Interface (CLI).

Confirming That the Tomcat Service Is Running Using Real-Time Monitoring Tool (RTMT)

Step 1 Launch Real-Time Monitoring Tool (RTMT).

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

Step 2 On the System menu, select **Server** > **Critical Services**.

Step 3 On the System tab, locate Cisco Tomcat and view its status. The status is indicated by an icon.

Confirming That the Tomcat Service Is Running Using the Command Line Interface (CLI)

Step 1 Use the Command Line Interface (CLI) command **utils service list** to list all of the services.

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

Step 2 Scan the CLI output for the Cisco Tomcat service and confirm that its status is **Started**.

Restarting the Tomcat Service Using the Command Line Interface (CLI)

To restart the Cisco Tomcat service, use the CLI command **utils service restart Cisco Tomcat**.

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