



Cisco Personal Communications Assistant

About Cisco PCA Installation, Repair, and Removal with Cisco Unity Version 4.0(4)

The installation of the Cisco PCA is an integral part of the Cisco Unity installation process, and therefore “hidden” from the installer. For new Cisco Unity installations, the Cisco PCA installation uses Windows Script Host technology with support scripts (javascript). During upgrades, Cisco PCA uses Windows Software Installer technology to uninstall existing Cisco PCA-related files and applications before installing new ones.

If you have the Cisco Unity installation disks, you can restore corrupt or missing Cisco PCA files and applications by running an installation script at a command prompt. When you restore the Cisco PCA, the installation script removes any existing Cisco PCA-related files and applications, including the Tomcat service and its integration to the IIS server.

If you no longer want the Cisco PCA on your Cisco Unity server, another script allows you to safely remove all Cisco PCA files.



Note

When an installer uses a different installation account to upgrade Cisco Unity than the one that was used to install the previous version of Cisco Unity, several Cisco PCA-related registry keys remain on the upgraded system. The “orphaned” registry keys are not used with Cisco Unity version 4.0(4), do not harm your system, and do not need to be removed when troubleshooting.




Caution

Do not use Add/Remove Programs to remove or repair the Cisco PCA files and applications.

About Cisco PCA Logging with Cisco Unity Version 4.0(4)

There are two types of Cisco PCA logging, as described in [Table 16-1](#). Errors, warnings, and exception traces captured in log files can often indicate the source of a problem. In addition, when you report a problem to Cisco TAC, you may be asked to send log files.

Table 16-1 Types of Cisco PCA Log Files

<p>Setup Process Logging</p>	<p>When the Cisco PCA is initially installed, the cscoserv_script.log is created. The log file contains information about the installation and configuration of the Cisco PCA. When you restore the Cisco PCA by using the setup.js script, the cscoserv_script.log is updated. When you remove the Cisco PCA by using the uninstall.js script, and then reinstall it, the cscoserv_script.log is created again. The respective log file contains information about the restored or removed installation.</p> <p>The cscoserv_script.log is stored in the current user temporary file directory (for example, Documents and Settings\<User>\Local Settings\Temp).</p> <p> Note In previous versions of Cisco PCA, Windows Installer provided logging. When an older Cisco PCA installation is removed during an upgrade to Cisco Unity version 4.0(4), Windows Installer logs data to the cscoserv_msi_remove.log. After the upgrade, the Cisco PCA uses the cscoserv_script.log described above to log changes to the Cisco PCA installation.</p>
<p>Application Logging</p>	<p>The Cisco PCA logs events in the following files in the CommServer\Cscoserv\Tomcat\Logs directory:</p> <ul style="list-style-type: none"> • The ciscopca_log.<date>.txt file contains a daily archive of system level logs. • The ciscopca_event_log.txt file and its archived versions contain application error logs. When the ciscopca_event_log.txt file reaches its size limit, the file is archived. Archived files have a number appended to the original filename (for example, ciscopca_event_log.txt.1). A maximum of 50 archived files are stored; when 50 archived files exist, Cisco PCA begins overwriting them, beginning with the first archived file. • The ciscopca_diags_log.txt file and its archived versions contain application logs. When the ciscopca_diags_log.txt reaches its size limit, the file is archived. Archived files have a number appended to the original filename (for example, ciscopca_diags_log.txt.1). A maximum of 50 archived files are stored; when 50 archived files exist, Cisco PCA begins overwriting them, beginning with the first archived file.

Procedures for Troubleshooting the Cisco PCA and Its Components for Cisco Unity Version 4.0(4)

When the Cisco PCA fails to operate properly, do the following tasks in the order presented:

1. If there is an error message associated with the problem, review the [“Cisco PCA Error Messages”](#) section on page 16-3 or the [“Procedures for Troubleshooting the Media Master Control Bar”](#) section on page 16-13 (as applicable), and then return to this section as needed.

2. Confirm that the `CommServer\Cscoserv` directory exists on the Cisco Unity server, and that it contains `Java2SDK`, `Tomcat`, `bin`, and `ciscopca` directories. If any directories are missing, follow the procedures in the [“Restoring the Cisco PCA”](#) section on page 16-7 to fix the problem.
3. Confirm that the Tomcat service is installed and that the service has started. See the [“Verifying That the Tomcat Service Is Installed and Started”](#) section on page 16-8.
4. Confirm that the World Wide Web Publishing service is installed and that the service has started. See the [“Verifying That the World Wide Web Publishing Service Is Started”](#) section on page 16-9.
5. Confirm that IIS and the Cisco PCA components are configured correctly. See the [“Verifying That IIS and the Cisco PCA Components Are Configured Correctly”](#) section on page 16-9.
6. Confirm that the IIS and Tomcat integration is configured correctly. See the [“Verifying That the IIS and Tomcat Integration Is Configured Correctly”](#) section on page 16-11.

Finally, to restore or remove the Cisco PCA files and applications, see the procedures in the [“Restoring the Cisco PCA”](#) section on page 16-7 or the [“Removing the Cisco PCA”](#) section on page 16-13, as applicable.

If you cannot resolve the problem and plan to report the problem to Cisco TAC, you will be asked to provide information about your system and about the problem. See the [“Reporting Problems to Cisco TAC”](#) section on page 1-3 for details.

Cisco PCA Error Messages

In addition to browser error messages (such as “File not found” or “Unauthorized access”), subscribers may see Cisco PCA-specific error messages and Tomcat error messages when logging on to the Cisco PCA, when using the Cisco Unity Assistant, or when using the Cisco Unity Inbox. The types of error messages are described below:

- Browser error messages may indicate that the Cisco PCA failed to install, the subscriber does not have network access to the Cisco Unity server, the browser is not configured correctly, or the subscriber does not have the required security certificate installed if the Cisco PCA uses SSL connections.
- Cisco PCA-specific errors are displayed on the Log On page or another Cisco PCA page, and typically indicate problems with user credentials or actions within the Cisco PCA.
- Tomcat errors occur when there is a system error, such as a file corruption or insufficient memory on the Cisco Unity server. A Tomcat error page usually lists the sequence of application errors, starting from the least likely exception to the root exception. 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 offer further insight into the problem.

All three types of error messages are presented in this section. Messages are presented in alphabetical order according to the text of the message. Possible causes and troubleshooting tips for resolving each issue are also listed. Some problems have more than one possible cause. The recommended actions are listed after each cause, and are offered in the suggested order of completion.

If subscribers cannot browse to the Cisco PCA website at all, experience incomplete or blank Cisco PCA pages, or have trouble accessing the Cisco PCA applications, see the [“Subscriber and Administrator Access”](#) chapter for the applicable troubleshooting procedures.

Error Message Access Denied.

Possible Cause Subscriber password has expired.

Recommended Action Check the ciscopca_event_log.txt file in the CommServer\Cscoserv\Tomcat\Logs directory on the Cisco Unity server to investigate why the subscriber credentials were rejected. You can also check the Windows event log for security-related events.

Subscribers can change their Cisco PCA passwords in Windows by pressing Ctrl-Alt-Delete and then clicking Change Password. (If the Cisco Unity server is on a different domain than the one that subscribers typically access with their Windows passwords, subscribers will need to specify the domain name for the Cisco Unity server.)

Possible Cause AvXml directory security is not set correctly in IIS; Anonymous access may be disabled, or secure connections may be enabled. To confirm this is the case, open the ciscopca_log.txt, ciscopca_event_log.txt, or ciscopca_diags_log.txt files located in the CommServer\Cscoserv\Tomcat\Logs directory and search for an “IOException” message that mentions HTTP returning a code 401 or 403. If such a message exists, directory security is not set correctly in IIS.

Recommended Action To correct directory security settings, see the “[Verifying That IIS and the Cisco PCA Components Are Configured Correctly](#)” section on page 16-9. Both the Anonymous Access and Integrated Windows Authentication check boxes should be checked.

Error Message Access Denied - Your Account is currently locked. Contact your Cisco Unity Administrator for assistance.

Possible Cause The subscriber exceeded the number of failed logon attempts that is allowed. (The limit is set on the System > Authentication page in the Cisco Unity Administrator.) The subscriber may have forgotten his or her credentials, or an unauthorized user has attempted to gain access.

Recommended Action Check the ciscopca_event_log.txt file in the CommServer\Cscoserv\Tomcat\Logs directory on the Cisco Unity server to investigate why the subscriber credentials were rejected.

Do the applicable security audit to determine whether an unauthorized user was attempting to access the Cisco PCA. (You can also check the Windows event log for security-related events.) To unlock the subscriber account, in the Cisco Unity Administrator, go to the Subscribers > Subscribers > Account Page for the individual subscriber. In the event that the subscriber has forgotten his or her password, note that you cannot change Cisco PCA passwords in the Cisco Unity Administrator. Instead, subscribers can change their Cisco PCA passwords only in Windows by pressing Ctrl-Alt-Delete and then clicking Change Password. (If the Cisco Unity server is on a different domain than the one that subscribers typically access with their Windows passwords, subscribers will need to specify the domain name for the Cisco Unity server.)

Refer to the “Subscriber Account Settings” section in the “Subscriber Settings” chapter of the *Cisco Unity System Administration Guide* for more information on unlocking subscriber accounts. For information on the lockout policy that applies when subscribers access the Cisco PCA, refer to the “Authentication Settings” section in the “System Settings” chapter of the *Cisco Unity System Administration Guide*. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag404/ex/index.htm.

Error Message Apache Tomcat/<version> - HTTP Status 500 - Internal Server Error

Possible Cause Possible file corruption at the time of installation or a Tomcat memory corruption. To confirm this is the case, 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)
```

Recommended Action See the [“Restoring the Cisco PCA”](#) section on page 16-7.

Error Message HTTP Status 401 - You are not authorized to view this page.

Possible Cause Jakarta directory security is not set correctly in IIS; the Anonymous Access or Integrated Windows Authentication check boxes may not be checked.

Recommended Action To correct directory security settings, see the [“Verifying That IIS and the Cisco PCA Components Are Configured Correctly”](#) section on page 16-9. Both the Anonymous Access and Integrated Windows Authentication check boxes should be checked.

Error Message HTTP Status 500.

Possible Cause Low system resources can prevent on-demand JSP page compilation of modified and first-time visited Cisco PCA pages. To confirm that low system resource is the cause for the error, check the CommServer\Cscoserv\Tomcat\Work\Standalone\Localhost\Ciscopca directory for .class or .java files that have a size of 0 KB.

Also, 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 problem with low system resources on the Cisco Unity server:

```
java.lang.ClassFormatError: <classpath>/<classname> (Truncated class file)
```

Finally, check the system resources on the Cisco Unity server: On the Cisco Unity server, start Task Manager (press Ctrl-Alt-Delete and then click Task Manager). On the Performance tab, check the Mem Usage index at the bottom of the window. When the difference between <in-use>/<system-max> is less than 32 MB, system memory resources are too low for the server to run the Cisco PCA properly.

Recommended Action On the Cisco Unity server, close any services and running applications that you can. If you are unsure which services and applications you can safely close or if you cannot close enough to gain the required system resources, contact your network administrator or Cisco TAC for further assistance.

When enough system memory resources are freed, delete the .class or .java files that have a size of 0 KB in the CommServer\Cscoserv\Tomcat\Work\Standalone\Localhost\Ciscopca directory. Contact your network administrator or Cisco TAC for further assistance.



Caution

Do not remove the CommServer\Cscoserv\Tomcat\Work\Standalone\Localhost\Ciscopca directory or any of its subdirectories. Removing the directories will result in disrupted Tomcat services and require that you restart the Tomcat service. Instead, delete the .class and .java files individually.

Error Message Site is unavailable.

Symptom The error occurs when a subscriber browses to `http://<Cisco Unity server>/ciscopca`, and when Internet connection issues, a firewall, or SSL restrictions are not factors.

Possible Cause ISAPI redirection filter failed to load.

Recommended Action Do [Step 1](#) through [Step 5](#) in the “[To Verify That IIS Is Configured Correctly](#)” procedure on [page 16-9](#). If the problem is still not resolved, restore the Cisco PCA by doing the procedure in the “[Restoring the Cisco PCA](#)” section on [page 16-7](#).

Possible Cause The Tomcat service is stopped.

Recommended Action See the “[Verifying That the Tomcat Service Is Installed and Started](#)” section on [page 16-8](#).

Possible Cause The IIS and Tomcat integration is not configured correctly.

Recommended Action See the “[Verifying That the IIS and Tomcat Integration Is Configured Correctly](#)” section on [page 16-11](#).

Possible Cause The World Wide Web Publishing service is stopped.

Recommended Action See the “[Verifying That the World Wide Web Publishing Service Is Started](#)” section on [page 16-9](#).

Error Message There is no mailbox for this account. Try logging on with a different account. If you still cannot log on, contact your Cisco Unity administrator.

Possible Cause The user entered credentials for a Cisco Unity installation or service account that does not have a mailbox.

Recommended Action Create a subscriber account for the user. As a best practice, we recommend that Cisco Unity administrators not use the same subscriber account to log on to the Cisco Unity Administrator that they use to log on to the Cisco PCA to manage their own Cisco Unity accounts.

Error Message Unknown authentication provider. Try logging on again in a few minutes. If the problem persists, contact your Cisco Unity administrator.

Possible Cause AvXML directory security is not set correctly in IIS; the Anonymous Access or Integrated Windows Authentication check boxes may not be checked. To confirm this is the case, open the `ciscopca_log.txt`, `ciscopca_event_log.txt`, or `ciscopca_diags_log.txt` files located in the `CommServer\Cscoserv\Tomcat\Logs` directory and search for an “IOException” message that mentions HTTP returning a code 401 or 403. If such a message exists, directory security is not set correctly in IIS.

Recommended Action To correct directory security settings, see the “[Verifying That IIS and the Cisco PCA Components Are Configured Correctly](#)” section on [page 16-9](#). Both the Anonymous Access and Integrated Windows Authentication check boxes should be checked.

Possible Cause HTTP proxy or web browser caches are interfering with presentation of the Cisco PCA Log On page. A cached Log On page is displayed instead of one from the Cisco PCA server.

To confirm this is the case, open the `ciscopca_event_log.txt` or `ciscopca_diags_log.txt` files located in the `CommServer\Cscoserv\Tomcat\Logs` directory and search for messages that mention “Provider Sessions” like the ones below. If such messages exist, HTTP Proxy or web browser caches are interfering.

- “Perform - Attribute “PROVIDER” unknown/unset value: <value>”
- “Perform - Session attribute “PROVIDER” unknown/unset value: <value>”
- “Perform - authentication provider mismatch - Session Attribute: <dynamic-value>, Form property: <value>”
- “LogonUser - unknown authentication provider - returning error”

Recommended Action Verify that HTTP proxy servers are configured so that they do not cache any .jsp and .do pages that are requested from the Cisco Unity server. Ask your network administrator for guidance. Also, make sure that the browsers on subscriber workstations are set to automatically check for newer versions of temporary Internet files.

Error Message Unable to contact server. Try logging on again in a few minutes. If the problem persists, contact your Cisco Unity administrator.

Possible Cause The Cisco Unity server is down, or a network connection has failed.

Recommended Action Confirm that the Cisco Unity server is running, and that all network connections are functioning properly. Restart the Cisco Unity server, as necessary. To verify that the problem is caused by a Cisco Unity server or a network failure, you can try switching to an available failover Cisco Unity server to see whether the same error message occurs on the failover server. Alternatively, you can change the “unityurl” configuration setting to point to a Cisco Unity server that is running, and then restart the Tomcat service.

Possible Cause AvXml directory security is not set correctly in IIS; Anonymous access may be disabled or secure connections may be enabled. To confirm this is the case, open the `ciscopca_log.txt`, `ciscopca_event_log.txt`, or `ciscopca_diags_log.txt` files located in the `CommServer\Cscoserv\Tomcat\Logs` directory and search for an “IOException” message that mentions HTTP returning a code 401 or 403. If such a message exists, directory security is not set correctly in IIS.

Recommended Action To correct directory security settings, see the [“Verifying That IIS and the Cisco PCA Components Are Configured Correctly”](#) section on page 16-9. Anonymous access should be enabled and secure connections should be disabled.

Restoring the Cisco PCA

Do the following procedure to restore corrupt or missing Cisco PCA files and applications.



Caution

Do not use Add/Remove Programs to remove or repair the Cisco PCA files and applications.

To Restore the Cisco PCA Files and Applications

- Step 1** On the Cisco Unity server, close all applications and file folders. (If any Cisco PCA files are in use or if the \CommServer\cscoserv directory is open, the restore can fail.)
- Step 2** Insert the Cisco Unity disc that contains the cscoserv directory. For example, for the Cisco Unity 4.0(4) release, the cscoserv directory is on Cisco Unity DVD 1 and on Cisco Unity CD 1.
- Step 3** Open a command prompt, and change to your DVD or CD-ROM drive.
- Step 4** Enter `cd cscoserv` and press **Enter**.
- Step 5** Enter `cscript setup.js source="<DVD or CD drive>:\cscoserv\setup.msi" target="<Cisco Unity drive>:\commserver"` and press **Enter**.
- For example, if your DVD or CD-ROM drive is drive D and Cisco Unity is installed on drive C, enter:
- ```
cscript setup.js source="d:\cscoserv\setup.msi" target="c:\commserver"
```
- Step 6** Wait a few minutes while the script runs. When the script stops running, "Done" appears in the command window.
- The cscoserv\_script.log file is saved to the current user temporary file directory (for example, Documents and Settings\<User>\Local Settings\Temp). You can observe the progress of the script by opening the log file in a browser and refreshing the browser periodically.
- Step 7** When the script has finished running, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 8** Confirm that Tomcat and the World Wide Web Publishing Service are started. If not, restart them. (You do not need to restart the Cisco Unity server to implement your changes.)
- If Tomcat is not displayed in the Services Control Panel or if the Cisco PCA still does not work, contact Cisco TAC for further assistance.
- 

## Verifying That the Tomcat Service Is Installed and Started

Do the following procedure to verify that the Tomcat service is installed and started.

### To Verify That the Tomcat Service Is Installed and Started

---

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 2** In the right pane, locate **Tomcat** and verify that its status is **Started** and its Startup Type is **Automatic**. If the Tomcat service is not listed in the services manager, it is likely that either the Cisco PCA or the Tomcat service failed to install, or that the Tomcat service registration failed. To correct the problem, you will need to restore the Cisco PCA files and applications. See the ["Restoring the Cisco PCA" section on page 16-7](#).
- If the Tomcat service is listed in the services manager, but is not started, right-click it, and click **Start**.
-

## Verifying That the World Wide Web Publishing Service Is Started

Do the following procedure to verify that the World Wide Web Publishing service is installed and started.

### To Verify That the World Wide Web Publishing Service Is Installed and Started

- 
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 2** In the right pane, locate **World Wide Web Publishing** and verify that its status is **Started** and its Startup Type is **Automatic**.
- If the World Wide Web Publishing service is not listed in the services manager, it is possible that IIS was not installed correctly. To correct the problem, you will first need to repair the IIS installation. Then restore the Cisco PCA files and applications (see the [“Restoring the Cisco PCA”](#) section on page 16-7).
- If the World Wide Web Publishing service is listed in the services manager but is not started, right-click it, and click **Start**.
- 

## Verifying That IIS and the Cisco PCA Components Are Configured Correctly

The Cisco PCA depends on the Tomcat service being correctly configured to load the Cisco PCA application upon startup. It also depends on IIS and the Tomcat service being able to communicate. The Tomcat service installation requires Tomcat and Java2SDK. The `jk_nt_service` application handles the Windows service interface for Tomcat, and it requires that the Tomcat service be configured so that the startup and shutdown control port matches its own. The `jk_nt_service.exe` and its configuration file (`wrapper.properties`) are located in the `CommServer\Cscoserv\Windows\Service` directory.

This section contains two procedures. Do the procedures in order to verify that IIS and the Tomcat service are configured correctly. Enter any missing values and correct settings that do not match what is indicated here. Restart IIS and the Tomcat service if you make any corrections, and then check to see whether the Cisco PCA operates properly afterward.

### To Verify That IIS Is Configured Correctly

- 
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** Right-click `<System-name>`, and then click **Properties**.
- Step 3** On the Internet Information Services tab, confirm that **WWW Service** is selected in the Master Properties list, and then click **Edit**.
- Step 4** Click the **ISAPI Filters** tab, and click **cpcaflt** from the list of filter names.
- Step 5** In the Details section, verify that the executable is **isapi\_redirect.dll** and that its status is **Loaded**. Note that it is not loaded properly if either of the following are true:
- Either no arrow, or a red arrow, is displayed on the left.
  - The Priority is listed as “Unknown.”

- Step 6** If you determined in [Step 5](#) that the `isapi_redirect.dll` executable is not loaded properly, reload it by doing the following sub-steps:
- Verify that no other filter is loading the same `.dll` file or a similar file in another location. This can happen when a legacy setting has already used a Tomcat redirector before the current Cisco Unity software was installed.
  - Delete the offending duplicate entry (keep the `cpcaflt` entry), and click **Apply**.
  - Click **OK** to close the dialog box and return to the Internet Information Services window.
  - In the Services Control Panel, stop the Tomcat service. (On the Windows Start menu, click **Programs > Administrative Tools > Services**. In the right pane, right-click **Tomcat** and click **Stop**.)
  - Right-click the `<System-name>`, and click **Restart IIS**.
  - Confirm that IIS is set to restart, and click **OK**.
  - Verify that the ISAPI filter is loaded by repeating [Step 1](#) through [Step 5](#).
  - If the filter is loaded, restart the Tomcat service in the Services Control Panel.
- Step 7** As needed, click **OK** to close any remaining dialog boxes and return to the Internet Information Services window.
- Step 8** Expand `<System-name>`, and expand **Default Web Site**.
- Step 9** Under Default Web Site, click **Jakarta**, and then verify that `isapi_redirect.dll` is listed in the right pane.
- Step 10** Right-click **Jakarta**, and click **Properties**.
- Step 11** In the Jakarta Properties dialog box, do the following sub-steps:
- On the Virtual Directory tab, verify that the Local Path is set to the `CommServer\Cscoserv\Windows\Iis\Bin` directory.
  - Click the **Directory Security** tab.
  - Under Anonymous Access and Authentication Control, click **Edit**.
  - In the Authentication Methods dialog box, verify that the **Anonymous Access** check box is checked and the **Integrated Windows Authentication** check box is checked.
  - Click **OK** to close the Authentication Methods dialog box.
  - Click **OK** to close the Jakarta Properties dialog box.
- Step 12** Under Default Web Site, right-click **AvXml**, and click **Properties**.
- Step 13** In the AvXml Properties dialog box, do the following sub-steps:
- On the Virtual Directory tab, verify that the Local Path is set to the `\InetPub\Wwwroot\AvXml` directory.
  - Click the **Directory Security** tab.
  - Under Anonymous Access and Authentication Control, click **Edit**.
  - In the Authentication Methods dialog box, verify that the **Anonymous Access** check box is checked.
  - Click **OK** to close the Authentication Methods dialog box.
  - Under Secure Communication, click **Edit**. (If the button is greyed out, skip to [Step 14](#).)
  - In the Secure Communications dialog box, verify that the **Require Secure Channel (SSL)** check box is unchecked.
  - In the Client Certificates section, verify that **Ignore Client Certificates** is selected and the **Enable Client Certificate Mapping** check box is unchecked.

- i. Click **OK** to close the Secure Communications dialog box.
- j. In the AvXml Properties dialog box, click **Apply**.
- k. Click **OK** to close the AvXml Properties dialog box.

**Step 14** Close the Internet Information Services window.

---

#### To Verify That the Tomcat Service Is Configured Correctly

---

**Step 1** On the Cisco Unity server, browse to the directory **CommServer\Cscoserv\Windows\Service**.

**Step 2** Use a text editor to open the **wrapper.properties** file.

**Step 3** Verify that the value for wrapper.tomcat\_home is set to **CommServer\Cscoserv\Tomcat**, which is the Tomcat installation directory.

The value must be an absolute path (for example, C:\CommServer\Cscoserv\Tomcat).

**Step 4** Verify that the wrapper.java\_home value is set to **CommServer\Cscoserv\Java2SDK**, which is the java sdk root.

The value must be an absolute path (for example, C:\CommServer\Cscoserv\Java2SDK).

**Step 5** Close the **wrapper.properties** file.

---

## Verifying That the IIS and Tomcat Integration Is Configured Correctly

The IIS and Tomcat integration depends on the proper installation and configuration of the isapi\_redirect.dll file in IIS. The redirector file is located in CommServer\Cscoserv\Windows\iis\Bin directory, and it uses two support files (uriworkermap.properties and workers.properties), which are located in the CommServer\Cscoserv\Windows\iis directory.

This section contains several procedures. Do the procedures in order to verify that the IIS and Tomcat integration is configured correctly. Enter any missing values and correct settings that do not match what is indicated here. Restart IIS and the Tomcat service if you make any corrections, and then check to see whether the Cisco PCA operates properly afterward.

#### To Verify the IIS and Tomcat Integration Is Configured Correctly

---

**Step 1** On the Cisco Unity server, browse to the directory **CommServer\Cscoserv\Windows\Iis**.

**Step 2** Use a text editor to open the **workers.properties** file.

**Step 3** Verify that the value for workers.tomcat\_home is set to the Tomcat installation directory (for example, C:\CommServer\Cscoserv\Tomcat).

The value must be the absolute path to the root of the Tomcat installation directory.

**Step 4** Verify that the workers.java\_home value is set to a proper java sdk root (for example, C:\CommServer\Cscoserv\Java2SDK).

The value must be the absolute path to the root of a Java 2 SDK version 1.3 or later.

**Step 5** Close the **workers.properties** file.

**Step 6** Use the text editor to open **uriworkermap.properties**.

**Step 7** Verify that the file contains the following:

- /ciscopca=\$(default.worker)
- /ciscopca/\*=\$(default.worker)
- default.worker=ajp13

**Step 8** Close the **uriworkermap.properties** file.

---

#### To Verify That the Tomcat Server Is Configured Correctly

---

**Step 1** On the Cisco Unity server, browse to the directory **CommServer\Cscoserv\Tomcat\Webapps**.

**Step 2** Verify that the directory contains the **ciscopca.xml** file. If it does, use a text editor to open it.

**Step 3** Verify that the file contains `<Context path="/ciscopca">`. This defines the Cisco PCA application profile.

**Step 4** Verify that the value for the path attribute is `"/ciscopca"` and the docBase attribute is the absolute path to the ciscopca directory (for example, `C:\CommServer\Cscoserv\Ciscopca`).

**Step 5** Verify that the value for the reloadable attribute is `"False"`. The value controls whether Tomcat forces the Cisco PCA to reload when files change.

**Step 6** Verify that the value for the debug attribute is `"0"`. The values sets minimal logging.

**Step 7** Verify that the value for the privileged attribute is `"True"`.

**Step 8** Verify that the file contains the `"<Logger></Logger>"` object declaration within the ciscopca `"<Context ></Context>"` declaration. The value indicates where engine events are logged for the Cisco PCA.

**Step 9** Close the **ciscopca.xml** file.

---

#### To Verify That the Cisco PCA Web Application Is Configured Correctly

---

**Step 1** On the Cisco Unity server, browse to the directory **CommServer\Cscoserv\Ciscopca\WEB-INF**.

**Step 2** Use a text editor to open the **web.xml** file.

**Step 3** Find **unityurl** and verify that the value enclosed by `"<param-value id="unityurl">"` and `"</param-value>"` is a valid IP address or DNS name for the Cisco Unity server that is hosting the AvXml web service/portal.

The value cannot be either of the following:

- 127.0.0.1
- "localhost"

**Step 4** Close the **web.xml** file.

---

## Removing the Cisco PCA

Do the following procedure if you no longer want the Cisco PCA files and applications on your Cisco Unity server.

**Caution**

Do not use Add/Remove Programs to remove or repair the Cisco PCA files and applications.

**To Remove the Cisco PCA Files and Applications**

- Step 1** On the Cisco Unity server, close all applications and file folders. (If any Cisco PCA files are in use or if the \CommServer\cscoserv directory is open, the removal can fail.)
- Step 2** Open a command prompt.
- Step 3** Enter `cscript <Cisco Unity drive>\commserver\cscoserv\uninstall.js` and press **Enter**.
- Step 4** Wait a few minutes while the script runs.

The cscoserv\_script.log file is saved to the current user temporary file directory (for example, Documents and Settings\

You do not need to restart the Cisco Unity server to implement your changes.

## Procedures for Troubleshooting the Media Master Control Bar

Problems that subscribers can experience when using the Media Master control bar in the Cisco Unity Administrator, Cisco Unity Assistant, Cisco Unity Inbox, or ViewMail are listed below. Possible causes and troubleshooting tips for resolving each issue are also listed. Some problems have more than one possible cause. The recommended actions are listed after each cause, and are offered in the suggested order of completion.

**Symptom** The Media Master control bar appears as a red X.

**Possible Cause** Subscriber does not have the browser configured correctly, or does not have the Media Master installed locally because the subscriber does not have local administrative rights to the workstation.

**Recommended Action** Make sure that the browser is configured to download and run ActiveX controls. If that does not correct the problem, tell the subscriber to log off of the Cisco PCA. Log on to the subscriber workstation and then log on to the Cisco PCA by using an account that has local administrative rights to the workstation. Browse to a page that contains the Media Master control bar. Log off. When the subscriber logs on to the Cisco PCA again, the Media Master bar should appear. For more details, see the [“Media Master Control Bar Does Not Show Up Correctly in Cisco Unity Applications”](#) section on page 13-5.

**Symptom** The play and record buttons are greyed out on the Media Master control bar. In the Cisco PCA, subscribers may also see either of the following error messages:

```
Unable to connect to the voice server.
Unable to access the audio stream on the voice server.
```

**Possible Cause** Subscriber does not have the browser configured correctly.

**Recommended Action** Make sure that the browser is configured to automatically check for newer versions of temporary Internet files.

**Possible Cause** The Media Master control bar may not be able to locate the Cisco Unity server because the CommServer\Cscoserv\Ciscopca\WEB-INF\Web.xml “unityurl” setting contains either the 127.0.0.1 IP address or the “localhost” host name, rather than a network IP address or a valid DNS name. (Note that occasionally the “unityurl” setting does contain a valid DNS name, but the symptom is still exhibited. In all cases, however, when “pinging” the IP address for the Cisco Unity server from the subscriber workstation fails, the buttons will appear greyed out on the Media Master control bar.)

**Recommended Action** Replace the unityurl value with a proper IP address or DNS name, as necessary. Then restart the Tomcat service. See [Step 3](#) in the [“To Verify That the Cisco PCA Web Application Is Configured Correctly” procedure on page 16-12.](#)

**Possible Cause** The AvMMProxySvr service is not started or is down.

**Recommended Action** Restart the AvMMProxySvr service.

**Possible Cause** Network configuration is interfering with COM/DCOM operations.

**Recommended Action** Because the Media Master control bar relies on Distributed Component Object Model (DCOM) communication to communicate with the Cisco Unity server, verify that DCOM communication is enabled on the subscriber workstation and on the Cisco Unity server. The Media Master will not work when DCOM communications are blocked.

If there is one, verify that the firewall is configured so that it does not block DCOM communications. Remember to check for software on subscriber workstations that offer a personal firewall.

As applicable, disable or remove security software from the subscriber workstation as necessary. Some security software—including anti-virus and VPN client software—block DCOM communications.

**Symptom** The Media Master control bar does not play or does not record when the subscriber specifies the computer multimedia devices as the playback and recording device, and the multimedia devices work properly otherwise.

**Possible Cause** Network configuration is interfering with COM/DCOM operations.

**Recommended Action** Because the Media Master control bar relies on Distributed Component Object Model (DCOM) communication to communicate with the Cisco Unity server, verify that DCOM communication is enabled on the subscriber workstation and on the Cisco Unity server. The Media Master will not work when DCOM communications are blocked.

If there is one, verify that the firewall is configured so that it does not block DCOM communications. Remember to check for software on subscriber workstations that offer a personal firewall.

As applicable, disable or remove security software from the subscriber workstation as necessary. Some security software—including anti-virus and VPN client software—block DCOM communications.

**Recommended Action** Verify that the AvCsMgr and AvCsGateway services are running as a distinguished Cisco Unity account (as specified during installation) and not the Local System account.

**Symptom** The Media Master control bar does not play or does not record when the subscriber specifies the phone as the playback and recording device.

**Possible Cause** Network configuration is interfering with COM/DCOM operations.

**Recommended Action** Because the Media Master control bar relies on Distributed Component Object Model (DCOM) communication to communicate with the Cisco Unity server, verify that DCOM communication is enabled on the subscriber workstation and on the Cisco Unity server. The Media Master will not work when DCOM communications are blocked.

If there is one, verify that the firewall is configured so that it does not block DCOM communications. Remember to check for software on subscriber workstations that offer a personal firewall.

As applicable, disable or remove security software from the subscriber workstation as necessary. Some security software—including anti-virus and VPN client software—block DCOM communications.

**Recommended Action** Verify that the AvCsMgr and AvCsGateway services are running as a distinguished Cisco Unity account (as specified during installation) and not the Local System account.

---

*Cisco Unity 4.0(4) Troubleshooting Guide (With Microsoft Exchange)  
Copyright © 2004, Cisco Systems, Inc.  
All rights reserved.*

