Getting Started

Access

You can access the Serviceability application several ways:

- By entering `https://<server name or IP address>:8443/ccmservice/` in a browser window and then entering a valid username and password.
- By choosing **Cisco Unified Serviceability** in the Navigation menu in the Cisco Unified Communications Manager Administration console.
- By choosing **Application** > **Serviceability Webpage** in the Cisco Unified Real-Time Monitoring Tool (Unified RTMT) menu and then entering a valid username and password.
- By choosing **Cisco Unified Serviceability** in the Navigation menu in Cisco Unity Connection.
- By choosing **Cisco Unified Serviceability** in the Navigation menu in Cisco IM and Presence Administration..

Tip After you log in to Cisco Unified Serviceability, you can access all administrative applications that display in the Navigation menu, except for Cisco Unified OS Administration and Disaster Recovery System, without logging in again. The web pages that you can access within Cisco Unified Serviceability depend on your assigned roles and privileges. Cisco Unified OS Administration and Disaster Recovery System require a separate authentication procedure.

The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application.

Tip Unified Communications Manager only: Any user who has the "Standard CCM Admin Users" role assigned can access Cisco Unified Serviceability. For information on how to assign this role to a user, refer to the *Cisco Unified Communications Manager Administration Guide*.

$\mathcal{P}$

| **Tip** | Cisco Unity Connection only: Any user who has the System Administrator role or Technician role assigned can access Cisco Unified Serviceability. For information on how to assign this role to a user, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*. |

If you get a security alert that the site is not trusted, this indicates that the server certificate has not yet downloaded.

To access Cisco Unified Serviceability, perform the following procedure:

Procedure

Step 1 In a supported browser, browse to the server where the Cisco Unified Serviceability service runs.

| **Tip** | In the supported browser, enter `https://<server name or IP address>:8443/ccmservice/,` where server name or IP address equals the server where the Cisco Unified Serviceability service runs and 8443 equals the port number for HTTPS. |

| **Tip** | If you enter `http://<server name or IP address>:8080` in the browser, the system redirects you to use HTTP. HTTP uses the port number 8080. |

| **Note** | If the system prompts you about certificates, see topics related to installing the server certificate. |

Step 2 Enter a valid username and password; click **Login**.

To clear the username and password, click **Reset**.

When you log in to Cisco Unified Serviceability, the last successful system login attempt and the last unsuccessful system login attempt for each user along with the user id, date, time and IP address is displayed in the main Cisco Unified Serviceability window.

Related Topics

Access Cisco Unified IM and Presence Serviceability

After you sign into Cisco Unified IM and Presence Serviceability, you can access all applications that display in the Navigation list box without having to sign in to each application. Select the application you require from the list box, and select **Go**.

Before you begin

If you have already signed in to one of the applications that display in the Navigation list box (not Cisco Unified IM and Presence OS Administration or IM and Presence Disaster Recovery System), you can access Cisco Unified IM and Presence Serviceability without signing in. From the Navigation list box, select Cisco Unified IM and Presence Serviceability; then, select **Go**.

Procedure

Step 1 Enter `https://<server name or IP address>`, where the server name or IP address equals the server where the Cisco Unified IM and Presence Serviceability service runs.

Step 2 Sign in to Unified Communications Manager IM and Presence Administration.

Step 3 If the system prompts you about certificates, you must enable HTTPS to secure communications between the browser client and the web server.

Step 4 Enter the application user and application user password that you specified during installation when the system prompts you for a username and password.

Step 5 After Unified Communications Manager IM and Presence Administration displays, select **Navigation** > **Cisco Unified IM and Presence Serviceability** from the menu in the upper right corner of the main window.

When you log in to Cisco Unified IM and Presence Serviceability, the last successful system login attempt and the last unsuccessful system login attempt for each user along with the user id, date, time and IP address is displayed in the main Cisco Unified IM and Presence Serviceability window.

Install Server Certificate

Note For additional information about using HTTPS with Unified Communications Manager, refer to Cisco Unified Communications Manager Security Guide.

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the Tomcat web server, uses a certificate and a public key to encrypt the data that is transferred over the Internet. HTTPS, which ensures the identity of the server, supports applications, such as Cisco Unified Serviceability. HTTPS also ensures that the user login password transports securely over the web.

Note Ensure that the browser certificate and the server certificate are an exact match.

Note Because of the way Internet Explorer 7 handles certificates, this browser displays an error status after you import the server certificate. This status persists if you reenter the URL or refresh or relaunch the browser and does not indicate an error. Refer to the Install Internet Explorer 7 Certificate, on page 4 for more information.

HTTPS

When you first attempt to access Cisco Unified Serviceability, a Security Alert dialog box, which indicates that the server is not trusted because the server certificate does not exist in the Trusted folder, displays. When the dialog box displays, perform one of the following tasks:

- By clicking **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 clicking **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 clicking **No**, you cancel the action. No authentication occurs, and you cannot access the web application.

Note The system issues the certificate by using the hostname. If you attempt to access a web application by using the IP address, the Security Alert dialog box displays, even though you installed the certificate.

Install Internet Explorer 7 Certificate

Internet Explorer 7 adds security features that change the way that the browser handles Cisco certificates for website access. Because Cisco provides a self-signed certificate for the Unified Communications Manager or Cisco Unity Connection server, Internet Explorer 7 flags the Cisco Unified Communications Manager Administration or Cisco Unity Connection website as untrusted and provides a certificate error, even when the trust store contains the server certificate.

Note Internet Explorer 7, which is a Windows Vista feature, also runs on Windows XP Service Pack 2 (SP2), Windows XP Professional x64 Edition, and Windows Server 2003 Service Pack 1 (SP1). Java Runtime Environment (JRE) must be present to provide Java-related browser support for IE.

Be sure to import the Unified Communications Manager or Cisco Unity Connection certificate to Internet Explorer 7 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 7 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 7 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Unified Communications Manager or Cisco Unity Connection certificate to the root certificate trust store for Internet Explorer 7.

Procedure

Step 1 Browse to application on the Tomcat server by entering the hostname (server name) or IP address in the browser.

The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.

Step 2 To access the server, click **Continue to this website (not recommended)**

The administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the **View Certificates** link in the report.

Step 4 Verify the certificate details.

The Certification Path tab displays "This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store."

Step 5 Select the General tab in the Certificate window and click **Install Certificate**.

The Certificate Import wizard launches.

Step 6 To start the wizard, click **Next**.

The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click **Next**.

Step 8 Verify the setting and click **Finish**.

A security warning displays for the import operation.

Step 9 To install the certificate, click **Yes**.

The Import wizard displays "The import was successful."

Step 10 Click **OK**. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click **Tools** > **Internet Options** in the Internet Explorer toolbar and select the Content tab. Click **Certificates** and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list.

After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname or IP address or refresh or relaunch the browser.

Serviceability Interface

In addition to performing troubleshooting and service-related tasks in Cisco Unified Serviceability, you can perform the following tasks:

- Cisco Unified Communications Manager only: To access Dialed Number Analyzer to test and diagnose a deployed Unified Communications Manager dial plan configuration, analyze the test results and use the results to tune the dial plan, activate the Cisco Dialed Number Analyzer service by choosing **Tools** > **Service Activation** and choosing **Tools** > **Dialed Number Analyzer**.

- You must activate the Cisco Dialed Number Analyzer Server service needs along with the Cisco Dialed Number Analyzer service by choosing **Tools** > **Service Activation** and choosing **Tools** > **Dialed Number Analyzer Server**. This service needs to be activated only on the node that is dedicated specifically for the Cisco Dialed Number Analyzer service.

For more information on how to use the Dialed Number Analyzer, refer to the *Cisco Unified Communications Manager Dialed Number Analyzer Guide*.

- Unified Communications Manager only: To access Cisco Unified Communications Manager CDR Analysis and Reporting from **Tools** > **CDR Analysis and Reporting**, perform the required procedures, as described in the *CDR Analysis and Reporting Administration Guide*.

> **Note** You cannot access the Cisco Unified Communications Manager CDR Analysis and Reporting tool unless you are a member of the Cisco CAR Administrators user group. Refer to the "Configuring the CDR Analysis and Reporting Tool" chapter in the *CDR Analysis and Reporting Administration Guide* for information on how to become a member of the Cisco CAR Administrators user group.

- To display documentation for a single window, choose **Help** > **This Page** in Cisco Unified Serviceability.

- To display a list of documents that are available with this release (or to access the online help index), choose **Help** > **Contents** in Cisco Unified Serviceability.

- To verify the version of Cisco Unified Serviceability that runs on the server, choose **Help** > **About** or click the **About** link in the upper right corner of the window.

- To go directly to the home page in Cisco Unified Serviceability from a configuration window, choose **Cisco Unified Serviceability** from the Navigation drop-down list box in the upper right corner of the window.

> **Note** In some scenarios, you cannot access the Cisco Unified Serviceability from Cisco Unified OS Administration. A "Loading, please wait" message displays indefinitely. If the redirect fails, log out from Cisco Unified OS Administration, select Cisco Unified Serviceability from the Navigation drop-down list box, and log in to Cisco Unified Serviceability.

- To go directly to the home page in Cisco Unified IM and Presence Serviceability from a configuration window, select **Cisco Unified IM and Presence Serviceability** from the Navigation drop-down list box in the upper right corner of the window.

- To access other application GUIs, choose the application from the Navigation drop-down list box in the upper right corner of the window; then, click **Go**.

- To log out of Cisco Unified Serviceability, click the **Logout** link in the upper right corner of the Cisco Unified Serviceability window.

- In each Cisco Unified Serviceability configuration window, configuration icons display that correspond to the configuration buttons at the bottom of the window; for example, you can either click the Save icon or the Save button to complete the task.

> **Tip** Cisco Unified Serviceability does not support the buttons in your browser. Do not use the browser buttons, for example, the Back button, when you perform configuration tasks.

🔍

Tip When a session has been idle for more than 30 minutes, the Cisco Unified Serviceability user interface allows you to make changes before indicating that the session has timed out and redirecting you to the login window. After you log in again, you may have to repeat those changes. This behavior occurs in the Alarm, Trace, Service Activation, Control Center, and SNMP windows. If you know that the session has been idle for more than 30 minutes, log out by using the Logout button before making any changes in the user interface.

Cisco Unified Serviceability Icons

Table 1: Cisco Unified Serviceability Icons

Icon	Purpose
	Adds a new configuration
	Cancels the operation
	Clears the configuration that you specify
	Deletes the configuration that you select
	Shows the online help for the configuration
	Refreshes the window to display the latest configuration
	Restarts the service that you select
	Saves the information that you entered
	Sets the default for the configuration
	Starts the service that you select
	Stops the service that you select

Serviceability Interface