Getting Started

Overview

Unified CCX users can access reports using Cisco Unified Intelligence Center and Cisco Finesse. Unified Intelligence Center is a comprehensive, end-to-end reporting solution for Unified CCX. You can access Historical and Live Data reports.

With Unified Intelligence Center, you can complete the following tasks:

- Generate and view reports.
- Filter data in the reports by setting parameters.
- View help for a report.
- Create and view dashboards.
- View permalinks for reports and dashboards.
- Configure thresholds for grid data cells.
- Schedule reports to run at selected intervals.
- Import reports.
- Export reports and report folders.

Authorized Users

The following user groups can access the reports:

- Agents—User can access the Live Data agent reports.
- Supervisors—User can access the Live Data agent and supervisor reports.

Note To access Unified Intelligence Center Live Data reports, the supervisor should be assigned an agent extension.

- Reporting users—User can access Historical reports and Live Data reports.

Note
- Live Data reports can only be run by agents, supervisors, and reporting users.
- For more information on the maximum number of reporting users supported to run Live-Data Reports concurrently on Cisco Unified Intelligence Center, see the *Reporting Scaling Considerations* section in *Solution Design Guide for Cisco Unified Contact Center Express*.

Start Unified Intelligence Center

Access Unified Intelligence Center only after the administrator completes the post installation tasks for Unified CCX.

Procedure

Step 1 Open a web browser.

Step 2 Use one of the following methods to access Unified Intelligence Center:

- Enter the URL `https://<host address>` and click **Cisco Unified Contact Center Express Reporting**.
- Enter the URL `https://<host address>:8444/cuicui/Main.jsp`.

Note Host address is the DNS name or IP address of the Unified CCX node.

Unified Intelligence Center does not support HTTP.

Step 3 Enter your username and password.

Step 4 Click **Sign In**.

Note If your administrator has set up custom logon message in Cisco Unified OS Administration, the message appears in a pop-up window. Click **OK** to log in.

Custom logon messages are not displayed to users signing in with SSO.

Trust Self-Signed Certificates

Self-Signed Certificates

Ensure that the pop-ups are enabled for Cisco Unified Intelligence Center.

After you enter the Cisco Unified Intelligence Center URL in your browser, the procedure to add a certificate is as follows:

Install certificates on Windows operating system:

The procedure to add a certificate varies for each browser. The procedure for each browser is as follows:

Internet Explorer

Note If you are using a Windows client, signed in as a Windows user, you must run Internet Explorer as an administrator to install the security certificates. In your Start menu, right-click Internet Explorer and select Run as administrator.

Contact your administrator if you do not have the required permissions to install the security certificates.

1. A page appears with the warning that there is a problem with the website's security certificate. Click **Continue to this website (not recommended)** link to open the Cisco Unified Intelligence Center sign in page. The sign in screen appears with a certificate error in the address bar.
2. Click on the certificate error that appears in the address bar and then click **View Certificates**.
3. In the **Certificate** dialog box, click **Install Certificate** to open the **Certificate Import Wizard**.
4. On the **Certificate Import Wizard**, click **Next**.
5. Select **Place all certificates in the following store** and click **Browse**.
6. Select **Trusted Root Certification Authorities** and click **OK**.
7. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears.
8. Click **Yes** to install the certificate. The **Certificate Import** dialog box appears.
9. Click **OK** and close the **Certificate Import** dialog box.
10. Enter your credentials and click **Sign In**.

Note To remove the certificate error from the desktop, you must close and reopen your browser.

Firefox

1. A page appears with the warning that states this connection is untrusted.
2. On the browser tab, click **I Understand the Risks** > **Add Exception**.
3. On the **Add Exception** dialog box, ensure that **Permanently store this exception** box is checked.

4. Click **Confirm Security Exception**.

   The warning page closes automatically.

5. Enter your credentials and click **Sign In**.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

Chrome and Edge Chromium (Microsoft Edge)

1. A page appears with the warning that states that there is a problem with your website's security certificate.

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

   The sign in page opens and a certificate error appears in the address bar of your browser.

2. Click on the **Certificate Error**, and then,

   In Chrome, click **Certificate (Invalid)**.

   In Microsoft Edge, click **Certificate (not valid)**.

   The **Certificate** dialog box appears.

3. In the **Details** tab, click **Copy to File**.

   The **Certificate Export Wizard** dialog box appears.

4. Click **Next**.

5. Keep the default selection **DER encoded binary X.509 (.CER)** and click **Next**.

6. Click **Browse** and select the folder in which you want to save the certificate.

7. Enter a recognizable **File name** and click **Save**.

8. Click **Next**.

9. Click **Finish**.

   A successful export message appears.

10. Click **OK** and close the **Certificate Export Wizard**.

11. Browse to the folder where you have saved the certificate file (.cer file), right click on the file, and click **Install Certificate**.

    The **Certificate Import Wizard** dialog box appears.

12. Keep the default selection **Current User** and click **Next**.

13. Select **Place all certificates in the following store** and click **Browse**.

    The **Select Certificate Store** dialog box appears.

14. Select **Trusted Root Certification Authorities** and click **OK**.

15. Click **Next**.

16. Click **Finish**.

A **Security Warning** dialog box appears asking if you want to install the certificate.

17. Click **Yes**. A **Certificate Import** dialog box states that the import was successful appears.
18. Click **OK**.
19. Enter your credentials and click **Sign In**.

Close the browser and sign in to Cisco Unified Intelligence Center. The security error does not appear in the address bar.

Install certificates on macOS:

The procedure to download a certificate varies for each browser. The procedure for each browser is as follows:

Chrome and Edge Chromium (Microsoft Edge)

1. A warning page appears which states that your connection is not private. To open the Cisco Unified Intelligence Center sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.
2. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (Not Valid)**.

   A certificate dialog box appears with the certificate details.
3. Drag the **Certificate** icon to the desktop.
4. Double-click the certificate. The **Keychain Access** application opens.
5. In the right pane of Keychains dialog, browse to the certificate, right-click on the certificate, and select **Get Info** from the options that are listed. A dialog appears with more information about the certificate.
6. Expand **Trust**. From the **When using this certificate** drop-down, select **Always Trust**.
7. Close the dialog box that has more information about the certificate. A confirmation dialog box appears.
8. Authenticate the modification of Keychains by providing a password.
9. The certificate is now trusted, and the certificate error does not appear on the address bar.

Firefox

1. In your Firefox browser, enter the Cisco Unified Intelligence Center URL. A warning page appears which states that there is a security risk.
2. Click **Advanced** and then click **View Certificate** link. The **Certificate Viewer** dialog box appears.
3. Click **Details** and then click **Export**. Save the certificate (**.crt** file) in a local folder.

Note If **.crt** file option is not available, select **.der** option to save the certificate.

4. From the menu, select **Firefox** > **Preferences**. The **Preferences** page is displayed.
5. In the left pane, select **Privacy & Security**.
6. Scroll to the **Certificates** section and click **View Certificates ...**. The **Certificate Manager** window is displayed.
7. Click **Import** and select the certificate.
8. The certificate is now authorized, and the certificate error does not appear on the address bar.

Screen Resolution Support

Supported screen resolution for Cisco Unified Intelligence Center: 1366 x 768 or higher.

View Cisco Unified Intelligence Center Help

In Cisco Unified Intelligence Center, two types of help are available:

- **Application-specific help**: This help content explains how to use Unified Intelligence Center in general.
- **Report-specific help/Template help**: This help content explains how to use the report. The help can describe the fields or provide details of the relationship between the fields, or it can explain how to interpret the data in the report. This help is available only if it has been created for the report.

  For more information on how to add the template help to report, see *Add Template Help* section.

Get Help on Cisco Unified Intelligence Center

- Click the **Help** icon on the top right corner of each of the entity listing page to view help contents specific to that entity.
- Click the **Online Help** button on the home page to access the help window for Cisco Unified Intelligence Center.

Note Ensure to accept the certificate to view the help content.

Get Help on a Report

To get help on a report, perform the following steps

Procedure

Step 1 From the **Reports** page, click the required report to open the report in the run mode.

Step 2 Click the **Template Help** icon in the report toolbar.

The report template help appears in a new browser window.

You can configure template help for the report from the **Reports** page > **Add Help**. For more information, see *Add Template Help* section.