Introduction to Cisco Unified Intelligence Center

Overview

Cisco Unified Intelligence Center is a reporting platform for users of Cisco Contact Center products. It is a web-based application that provides Historical, Real-time, and Live Data reporting and dashboards.

Unified Intelligence Center serves the following primary purposes:

- Obtains data from the base solution's database. The base solution can be any of the Contact Center products.
- Allows you to create custom queries to obtain specific data.
- Customizes the visual presentation of the reports.
- Customizes the report data.
- Allows different groups of people to view specific data based on their roles.

Unified Intelligence Center users can use the new interface to perform the following tasks:

- Create and view Reports.
- Schedule reports to run at selected intervals.
- Import and export reports and report folders.

Customer Journey Analyzer

Unified Intelligence Center users can use the reporting platform to launch Customer Journey Analyzer using **Analyzer** from the left navigation pane.

You can customize the default Analyzer URL using the CLI **set cuic analyzer url <urlname>**.

For more information on the CLI, see *Cisco Unified Intelligence Center Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

The Customer Journey Analyzer mines historical data from multiple data sources and systems to generate specific business views of data. The Analyzer visually displays trends to help you identify patterns and gain insight for continuous improvement.

Note You must have completed the on boarding process for Cloud Connect to access Customer Journey Analyzer. Cloud Connect allows Cisco Contact Center on premises customers to connect to cloud services, such as Customer Journey Analyzer to use Business Metrics.

Access Unified Intelligence Center

The URLs for logging in to the Unified Intelligence Center reporting application are:

HTTPS

https://<HOST>:8444/cuicui/Main.jsp

Where HOST is the DNS name of a Unified Intelligence Center node.

By default, Unified Intelligence Center does not support HTTP. From the command-line interface, you can set the cuic properties > http-enabled to *on* to enable HTTP. With HTTP enabled, Unified Intelligence Center loads the login page with HTTPS. After successful login, Unified Intelligence Center loads the main page with HTTP.

HTTP

http://<HOST>:8081/cuicui/Main.jsp

Where, HOST is the DNS name of a Unified Intelligence Center node.

When http-enabled is *off*, Unified Intelligence Center redirects all HTTP requests to HTTPS.

Note Permalinks work in both HTTP and HTTPS.

Default Locale in Unified Intelligence Center

Note To specify a locale, install the language pack.

First time access to Cisco Unified Intelligence Center displays the sign in page in the browser locale. To change the locale, click the username on the top-right corner of your screen and select the required locale from the drop-down list.

When you select a locale, the browser retains the locale information even after you sign out and sign in back to Cisco Unified Intelligence Center within the same browser.

Table 1: Supported Languages

Brazilian Portuguese	Chinese (Simplified)	Chinese (Traditional)	Danish	Dutch
English (U.S.)	French (France)	German	Italian	Japanese
Korean	Russian	Spanish (Spain)	Swedish	Polish
Turkish	Finnish	Norwegian	Čeština (Czech)	Bulgarian
Català (Catalan)	Hrvatski (Croatian)	Magyar (Hungarian)	Slovenčina (Slovak)	Slovenščina (Slovenian)
Српски (Serbian)	Română (Romanian)			

Synchronize Cluster

System Configuration Administrator can use the Synchronize Cluster feature (link below the username on the top-right corner of your user interface screen) to notify all nodes in the cluster to clear their local cache. This action synchronizes and empties all caches in the cluster. Clearing the locale cache forces each node to go directly to the database for the requested information.

Each node gets fresh data from the database. The data is automatically put into the local cache and accessed during future requests. Data remains consistent in the database and hence there is no loss of information.

For more information, see *Unified Intelligence Center Cache* section in the *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

Browser Support and Self-Signed Certificates

Unified Intelligence Center supports:

- Internet Explorer 11 (Native mode with Windows 10)
- Firefox ESR 52 and higher ESRs
- Edge Chromium (Microsoft Edge V79 and later)
- Chrome 60 and higher

Note To access OAMP, Internet Explorer 11 compatibility mode is required. Chrome support is only for the new user interface.

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.