Cisco Unified Intelligence Center

- Overview, on page 1
- Access Unified Intelligence Center, on page 2
- Default Locale in Unified Intelligence Center, on page 2
- Browser Support and Self-Signed Certificates, on page 3
- Stock Reports, on page 6
- Customize Report Templates, on page 6

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.

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.

For more information, see *Business Metrics* related information in *Cisco Unified Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.

Access Unified Intelligence Center

The URL for logging in to the Unified Intelligence Center reporting application is:

HTTPS

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

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

Note Cisco Unified Intelligence Center does not support HTTP.

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)			

Browser Support and Self-Signed Certificates

Unified Intelligence Center supports:

- Firefox ESR 68 and higher ESRs
- Edge Chromium (Microsoft Edge V79 and later)
- Chrome 76.0.3809 and higher

Note In the above mentioned browsers, ensure to manually close the certificate acceptance window to load the Live Data reports.

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:

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.

Stock Reports

The following report bundles are available as stock reports for Cisco Unified Intelligence Center:

- Realtime and Historical Transitional templates - Introductory templates designed for new users. These templates are simplified versions of the All Fields templates, and are similar to templates available in other contact center solutions.
- Realtime and Historical All Fields templates - Templates that provide data from all fields in a database. These templates are most useful as a basis for creating custom reports, and include templates for precision queue routing data.
- Realtime and Historical Outbound templates - Templates for reporting on Outbound Option activity. Import these templates if your deployment includes Outbound Option.
- Live Data templates - Templates for reports that use the Live Data stream processing system as a data source. Refresh rates for these reports are much faster than the Realtime or Historical reports--usually less than every 3 seconds. Reports are available for Agent, Agent Skill Group, Precision Queue, Skill Group, Recent State History and Recent Call History.
- Contact Sharing templates - Templates for reporting on a Contact Sharing system. You can use the Contact Sharing reports to understand the current configuration and behavior of the Contact Sharing system. You can view data on the active configuration of the Contact Sharing routing, the number of calls routed to each target system for each group, and the calls that have errors during the routing process.
- Cisco Unified Intelligence Center Admin Security templates - Templates to report on Cisco Unified Intelligence Server audit trails, permissions, and template ownership.
- License Consumption Report - Use this report to monitor the agent license consumption and other related ports such as the VRU-IVR ports and the outbound dialer ports. It helps you ascertain the number of licenses you must procure to cover the peak or maximum license usage during the license agreement period.

The report bundles are available as downloads from Cisco.com. Click the **Intelligence Center Reports** link on the downloads page (https://software.cisco.com/download/type.html?mdfid=282163829&catid=null). Depending on how it was deployed, your installation of Unified Intelligence Center may include all or a subset of these reports.

For information on importing report bundles or custom reports, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_installation_guides_list.html. Navigate to Initial Configuration>Configure Cisco Unified Intelligence Center>Import Report Bundles.

Customize Report Templates

You can modify existing report templates or create custom reports templates if you determine that the stock report templates do not meet your reporting needs. For example, you might customize an existing report template to monitor a department's activity and performance by creating a collection with objects from only that department.

See the *Cisco Unified Intelligence Center Report Customization Guide* at https://www.cisco.com/en/US/products/ps9755/tsd_products_support_series_home.html for directions on customizing report templates.