Configure

Overview

Unified Intelligence Center security offers multilayered and flexible functionality for a Security Administrator. Based on the requirements of the organization, you can configure users, groups, and provide appropriate permissions to create a flat or tiered access structure for Unified Intelligence Center functions. You can also configure Data Sources if you are a System Configuration Administrator.

You can access Unified Intelligence Center functions based on:

- Log in authentication.
- User Role (a user can have one or more of the six User Roles).
- User Groups in which the user is a member.
- For an object, the user can access, the object-level permissions that are assigned by the person who created that object.

User Permissions

About User Permissions

User Roles are associated with people and permissions are associated with entity types. Your User Role provides access to the corresponding entity types.

Entity types in Unified Intelligence Center are:

- Dashboards
- Reports

- Report Definitions
- Data Sources
- Value Lists
- Collections

Permissions are combined and the highest level permission prevails.

A user receives permission for an entity type from different sources. Permissions can be inherited from the AllUsers group or the permission assigned by the Security Administrator. Among all these permissions, the highest level permission is used when the user accesses the entity type.

User Permissions:

- **View**—When the user has View permissions for an entity type, that user can perform certain actions that depend on the entity type.

  For example, with View permission, you can perform the following actions:

  - Run, print, and refresh a report.
  - View, refresh, and run a dashboard.
  - View a Value List query.

  

  Note Permissions set on categories are not recursive. For all entities under Dashboard, Report, or Report Definition types, you need separate View or Edit permissions.

- **Edit**— When the user has Edit permission for an entity type, that user can modify, rename, or delete the entity type. Edit permission also includes View permission.

  For example, with Edit permission, you can perform the following actions:

  - Save As
  - Import reports
  - Export reports
  - Edit a Data Source
  - Delete a Custom Value List

  

  Note When setting permission for an entity type, if no permissions are granted, then the user will not have any access privileges to the entity type.

When you create an entity, you are the owner of that entity. By default, you have Edit permission for the entity, and you can set permissions for that entity for users in your Group only. By default, users without Security Administrator role cannot share entities they own with the **AllUsers** group. If you need users without

Security Administrator role to be able to set permissions for **AllUsers** group, set allow-allusers-group-ui property to *on* using the CLI command.

Note If the entity is still in progress and you do not want anyone to access it yet, you can make it “private” by leaving all permissions unchecked for both the All Users and the Groups.

For example, if you create a Dashboard for your Group and the dashboard has notes, you might want others in your Group to update the notes.

Even though you are a Dashboard Designer, if the Dashboards page contains dashboards created by (owned by) other Dashboard Designers, you may not be able to see those dashboards, based on your Group permissions and on the entity-level permissions those owners have set for their Dashboards.

Edit Permission Rules

The following rules are applicable for Reports, Report Definitions, Dashboards:

- To delete an entity, you need Edit permissions for the entity and the entity's parent folder.
- To delete a folder, you need Edit permissions for the folder, the folder's parent, and all the folders and/or entities belonging to the folder.
- A user can only Edit or Save an entity even if the immediate parent folder has no Edit permissions.
- A user can only use the Save As feature if the entity has no Edit permissions enabled.
- Any folder owner within the **Imported Report Definitions** can delete a folder if the administrator provides explicit Edit permissions on the **Imported Report Definitions** folder.

Set User Permissions

The User Permissions functionality allows Security Administrators to view and set permissions for user groups and for individual users for the selected entity type. Security Administrators can also set these permissions for each entity using the **Permissions** option (ellipsis actions) from the corresponding entity page.

To set permissions, perform the following steps:

Procedure

Step 1 In the left navigation pane, choose **Configure** > **Permissions**.

- **User Group Permissions**—Click this tab to set permissions to the User Groups.
- **User Permissions**—Click this tab to set permissions to the individual Users.

Note For illustration, the following procedure explains setting permissions to User Groups. To set permissions to individual Users, click the **User Permissions** tab and perform the same steps.

Note When you modify the permission of a user or a group for an entity, the changes are logged in the **CCBU-cuic.<timestamp>.startup.log** file with `PERMISSIONS_AUDIT_LOG` as prefix to the log.

Step 2 Select the **Entity Type**.

The available list of entities gets populated in the **Name** panel.

Step 3 Select the required entity value. The available list of user groups and the corresponding user permissions are listed in the **User Group** panel.

Step 4 Highlight the User Group to which you want to set the permissions.

- Highlighting the User Group row displays the list of associated users in the **Users** panel.
- Selecting the User row displays the list of associated User Groups in the **Groups** panel. You can select multiple users.

Step 5 Click **Set Permissions**.

Step 6 In the **Set Permissions** dialog box, select the appropriate check boxes to grant **View** and **Edit** permissions.

Step 7 Click **Update**.
The updated permissions are reflected in the **User Group** tab.

Note
- By default, the entity owner carries the Edit permission for that entity. No other user can change these settings for that entity.
- The inherited permission settings are disabled.

Users

User Roles

Your User Role allows you to access the application functionality that corresponds to that role.

With appropriate User Role, you can:

- Assign a user to one or more of the six User Roles.
- Assign multiple User Roles to individual users depending on the size, staff, geographical distribution, and security practices of your call center.
- Distribute each user role to many users.

Note Role changes to a user who is currently signed in, must sign out and sign in again for the changes to take effect.

When you modify the user roles, the changes are logged in the **CCBU-cuic.<timestamp>.startup.log** file with `ROLES_AUDIT_LOG` as prefix to the changes.

Caution Do not modify the user information of a user who is currently signed in, as the user will be automatically signed out.

Note The Login User role, earlier identified for all the users who could sign in to Unified Intelligence Center is now integrated within the system. To activate or inactivate a user, you can use the toggle button in the **Edit User** > **User Information** tab.

An active login user can:

- Sign in to Unified Intelligence Center.
- Access **Configure** > **Users** and edit their information. For example, to change their Alias or Last Name.

User Role	Supported Functions
System Configuration Administrator	Manages Data Sources and Scheduler.
Security Administrator	The initial, default Security Administrator is the user who is defined as the System Application User during the installation. Manages Users, User Groups, and User Permissions. Also, System Administrators can: • Assign User Roles—User Roles are associated with people. User Roles are assigned to users to control access to various functions and what objects you can create. • Assign users to User Groups. • Assign Permissions—Permissions are associated with objects (Dashboards, Reports, Report Definitions, Data Sources, Value Lists, and Collections). • Use the **Run As** feature to verify other users' permissions.
Dashboard Designer	Manages Dashboards.
Value List Collection Designer	Manages Value Lists and Collections.
Report Designer	Manages Reports. Can access Scheduler to work on reports with appropriate permissions.
Report Definition Designer	Manages Report Definitions.

Note For users who have been synched into Unified Intelligence Center from Unified CCE or Packaged CCE, you cannot edit the Report Designer and the Dashboard Designer roles.

Set Administrator Credentials

Cisco Unified Intelligence Center has an administrator user who is created at the install time. The new user can be provided with all the roles and permission after executing the command *utils cuic user make-admin* <*user-name*> successfully.

To provide the new user with the administrator credentials, perform the following steps:

Procedure

Step 1 Log in to the CLI using administrator credentials.

Step 2 On the CLI, run the command *utils cuic user make-admin* <user-name>.

Step 3 The <user-name> here should be the complete user name of the user including the authenticator prefix as listed in the Unified Intelligence Center User List page.

Step 4 If the command executes successfully, it will provide all the roles to this new user and copy all the permissions from the administrator to this user.

Step 5 Restart Intelligence Center Reporting service for the changes to be visible.

- The administrator's group memberships are not copied to this user by this CLI command. They will have to be manually updated. But after running the CLI, since this new user would have become a Security Administrator, he can do that himself.
- For any entity (reports, report definitions etc), if this new user's permissions provide higher privileges than the administrator, they will be left as it is and will not be overwritten by this CLI command.

Note This CLI is useful when using Unified Intelligence Center in SSO mode. Since the Administrator created at install time is not an SSO user, the *make-admin* CLI can be used for providing Administrative roles and permissions to an SSO user.

User Actions

Note You can only view your name and modify parameters such as email and phone number on the Users page without an Administrative role. You cannot change your role or group membership.

Action	Description
Toolbar Actions	
Search	Searches for a user based on First Name, Last Name, or User Name.

Action	Description
All	Lists all active users with associated user roles: • Administrator • SC—System Configuration Administrator • SA—Security Administrator • Report Designer • RD—Report Definition Designer • R—Report Designer • VL—Value List Collection Designer • Report Viewer • D—Dashboard Designer • R—Report Designer
Administrators	Lists all users with an Administrator role. The combination of Security Administrator and System Administrator user role qualifies to be an Administrator.
Inactive	Lists all inactive users. Use the **Edit Users** page to activate or deactivate users.
Refresh	Refreshes the **Users** page.
Create User	Creates a new user. For more information, see *Create Users*.
Ellipsis (…) Actions	
Edit	Edits user details. You can also click on the User Name to edit the user details.

Action	Description
Run As	Refreshes the Unified Intelligence Center web page and reflects the user interface that user is in. Perform this action to verify that the user roles and permissions are appropriately configured. **Note** • When you Run As another user, the top of the page shows both your logged in identity and your Run As identity. • You cannot Run As yourself. • You can Run As one level of user. A Security Admin cannot Run As User A and, as User A, then Run As User B. • You can Run As a different user. Refresh the open Unified Intelligence Center browser tabs to reflect the new user. • To leave the Run As mode, click **Stop Running As** and refresh the open Unified Intelligence Center tabs. **Caution** When the signed in user is in the Run As mode of another user, modifying the user account information of either of the users stops the Run As mode.
Delete	Deletes a user. Only users with a Security Administrator role can delete a user. You cannot delete a user who owns an entity (Dashboards, Reports, Report Definitions, Schedules, Value Lists, or Collections). To know the list of entities that the user owns, run the "Resource Ownership and Access" stock report. Delete those entities and then delete the user. The *Resource Ownership and Access* report is available as part of the *Admin Security* template from the software page, https://software.cisco.com/download/home/282163829/type/284697222/release/11.5%25281%2529. You cannot delete a user who has been synched into Unified Intelligence Center from Unified CCE or Packaged CCE.

Related Topics

Create Users, on page 8

Create Users

To create a user, perform the following steps:

Procedure

Step 1 In the left navigation pane, choose **Configure** > **Users**.

Step 2 On the **Create User** > **User Information** tab, enter the following:

Field	Description
User Name	User name (domain\name). Use the toggle button to activate or deactivate the user. Maximum length: 280 characters (includes domain name). **Note** You cannot deactivate users who have been synched into Unified Intelligence Center from Unified CCE or Packaged CCE.
Alias	The alias name for this user.
First Name, Last Name	The first name and last name of the user.
Roles	Assign one or more roles to this user. **Note** For a change to take effect, the user must log out, then log in.
Time Zone Settings	The time zone settings to reflect in the report. The time zone is also used for the user's scheduled reports and takes precedence over the time zone that is used by the report server. **Note** If no time zone is set, then the system uses the time zone of the report server. The **Start of the Week** is used in Scheduled Report, Report Views, and Permalink. To set the Start of the Week: • Select the **Locale Based (Sunday)** option to identify Sunday as the start of the week. • Select the **Custom** option to choose from the seven days of the week from the list.
Organization Information	The organization information to be associated with the user, such as the company name, email address, phone number, and user description.

Step 3 Click **Next** to assign a User Group to the created user.

Step 4 In the **Assign User Group** tab, use the arrow keys to move the User Groups from the **Available** list to the **Selected** list.

Note Higher-level permissions persist and override other permissions.

Step 5 Click **Save**.

Create Users - OAMP Console

In addition to creating users in the **Configure** > **Users** page, the user can sign in to Unified Intelligence Center only if the user exist in the Administration - OAMP console (Operation Administration Maintenance and Provisioning) as a Super User or if Active Directory has been configured in the Administration Console for that user's domain.

Users created in the **Configure** > **Users** page help set up roles and assign User Groups before they log in.

For example, if the Security Administrator is aware that 10 new users will be activated in the Administration Console, then the Security Administrator can create those users in the Unified Intelligence Center **Configure** > **Users** page, assigning them User Roles and User Groups.

Note The **User Name** (domain\name) on the **User Information** tab must *match exactly* with that user's domain and user name (all uppercase letters for the domain name; all lower case for the username). If they do not match, when the user signs in, they will be considered as a different user.

For more information, see the *User Management* chapter in the *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.

User Groups

Overview

User Groups are constructs that allow security administrators to partition Unified Intelligence Center functionality.

Creating User Groups expedites the process of provisioning users when multiple users need the same access to dashboards and reports, or when users require distinct permissions and features based on regional or organizational requirements.

User groups have no impact on how data is stored in the database. They are used only for assigning permissions to all the user members of the group through one operation instead of repeating the same operation for each user.

System-Defined All Users Group

All users are automatically a member of the system-defined *All Users* group.

All Users always appears on the User Groups window. The security administrator cannot delete it.

System-Defined Administrator User Group

The security administrator is automatically a member of the system-defined Administrators group and can add other security administrators to it.

Additional Security Administrators must be added to the Administrators group. Having the role does not automatically make them members of that group.

Customer-Defined User Groups

Security administrators can create any number of user groups and can add users to them. From those other user groups, one is designated as the user's *Group* (also called *My Group*).

Groups and Child Groups

Rules for Groups and Child Groups

- A group can be both a Parent and a Child. For example, Group 2 can be child of Group 1. Group 2 can also be a parent of Group 3.
- A Group is not required to have Child Groups.
- A Group may have any number of Child Groups.
- A Child Group cannot be a Parent to its own Parent Group and a Parent Group cannot be a Child of its own Child Group. For example, Group 3 is a child of Groups 1 and 2. Group 3 cannot also be a parent of Group 1 or Group 2.
- A Group can have both Groups and Users as children. For example, Group 2 can be a child of Group 1. User Lee can be a child of Group 1.
- A Group is not required to have a Parent Group.
- **Child Groups Do Not Inherit the Members of their Parent Groups**—Adding a user as a member of a group does not mean that user is also a member of its children. For example, Group 2 and Group 3 are children of Group 1. The security administrator adds User A as a member of Group 1. User A does not automatically become a member of Group 2 or Group 3. To make User A a member of Group 2, the security administrator must add User A as a member of Group 2.

User Group Actions

Action	Description
Toolbar Actions	
Search	Searches for a user group.
Refresh	Refreshes the **User Groups** page.
New	Creates a new user group. For more information, see *Create User Group*.
Ellipsis (…) Actions	
Edit	Edits the user group details. You can also click on the User Group Name to edit the user group details. In the edit mode, click the icon next to the User Group name to edit the User Group properties; Name and Description.
Delete	Deletes a user group. Only users with a Security Administrator role can delete a user group. You cannot delete a user group associated with any entities.

Create User Group

To create a user group, perform the following:

Procedure

Step 1 In the left navigation pane, choose **Configure** > **User Groups**.

Step 2 In the **User Groups** window, click **New**.

Step 3 In the **Create New User Group** window, enter the **Name** and **Description** for the group.

Step 4 Click **Next**.

Step 5 In the **Groups** section, perform the following:

a) **Available**—Lists the available groups that can be the parent of the User Group being created. Use the arrow icons to move accordingly.

b) **Selected**—Lists the groups selected to be the parent group for the User Group being created. Use the arrow icons to move accordingly.

Step 6 In the **Users** section, perform the following:

a) **Available** —Lists all the available users that are available to be children of this group. Use the arrow icons to move accordingly.

b) **Selected**—Lists the users that are currently children of this group. Use the arrow icons to move accordingly.

Step 7 Click **Save**.

Data Sources

Overview

Unified Intelligence Center supports the following types of data sources:

- Query based SQL Data Source
  - Microsoft SQL Server
  - IBM informix
- Streaming Data Source

Currently, Unified Intelligence Center does not support usage of integrated security for establishing TLS connections to MS SQL Server databases. However, while establishing a JDBC connection to MS SQL Server, Unified Intelligence Center needs to use TLS (v1.0, v1.1 or v1.2) for transmitting the database credentials to the server. As a JDBC client, CUIC offers the following cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

Related Topics

Streaming Data Source, on page 16

Data Source Actions

Action	Description
Toolbar Actions	
Refresh	Refreshes the Data Sources page.
New	Creates a new data source. For more information, see *Create Data Source*.

Action	Description
Switch Nodes	Click the **Switch** link on the data source card to switch over nodes (Primary and Secondary). On the confirmation dialog box, click **OK** to confirm the switch over. **Indicators** • *—indicates the current reporting source. • Green icon—indicates an online data source. • Red icon—indicates an offline data source. **Note** Switch Over is not applicable for the Streaming data source. Switch Over is applicable only if the **Enable Failover** check box is checked.
Ellipsis (…) Actions	
Edit	Edits the data source details. In the edit mode, you can click the icon next to the Data Source name to edit the Data Source Description.
Permissions	Assigns appropriate permissions to access and manage the Data Source. **Groups**—Grants **View** and **Edit** permissions for the Data Source. • Security Administrators can grant these permissions to various groups. • Entity owners can grant these permissions to groups that they are directly associated with. **Users**—Grants **View** and **Edit** permissions for the Data Source to various users. Applicable only to Security Administrators. **Note** • Higher permissions (View and Edit) from either an individual user or the user group takes precedence. • Only the first 200 records (alphabetical order) are displayed in the **Members** or **Groups** panel. To view more records, see **Configure** > **Groups**. • When you modify a permission and want to switch between **Groups** and **Users** tabs, you will be prompted to either save or discard the changes.
Delete	Deletes a data source. **Note** You cannot delete a data source that is referenced in Report Definitions and Value Lists. You cannot delete stock data sources (CUIC, UCCE Historical, or UCCE Real-Time).

Related Topics

Create Data Source, on page 15

Data Source Rules

- Set up a database with an SQL user account and password, with read-only permission for the database.
- The database server must allow SQL authentication to enable TCP/IP and remote network connection.
- Do not block the database port by firewalls or any other security software (such as Cisco Security Agent).

Note Windows integrated authentication connection to MS SQL Server is not supported.

Create Data Source

You can create or edit a data source only if you are assigned with a System Configuration Administrator role.

To create a data source, perform the following steps:

Procedure

Step 1 In the left navigation pane, choose **Configure** > **Data Sources**.

Step 2 In the **Data Sources** window, click **New**.

Step 3 In the **Create Data Source** dialog box, enter the datasource **Name**, **Description**, and select the **Data Source Type**.

Step 4 Click **Next**.

Step 5 In the data source details page, enter the following (Primary Node tab):

Field	Description
Host Settings	
Datasource Host	The hostname or IP address of the target data source.
Port	The port number that allows Unified Intelligence Center to communicate with the database. **Note** The port number is a mandatory field only for the Informix database.
Database Name	Enter the name of the database.
Instance	Enter the instance of the database. **Note** The name of the database instance is a required field only for Informix databases.
Time zone	Select the time zone that the database is located in.

Field	Description
Authentication Settings	
Database User ID	The user ID required to access the database.
Password	The password for the user ID required to access the database.
Charset	The character set that is used by the database.
Max Pool Size	The maximum pool size. **Note** Value ranges from 5 to 200. The default Max Pool Size value is 100 and is common for both the primary and secondary data source tabs.

Step 6 Click **Test Connection** to ensure that the database is accessible and the credentials provided are correct.

Step 7 Click the **Secondary Node** tab to configure a failover for the data source.

Step 8 Check the **Enable Failover** check box to configure a failover for the data source.

Step 9 Enter the required details for the failover data source. (Refer step 5)

Step 10 Click **Save**.

Streaming Data Source

Live Data report uses the Streaming data source (stock data source) and the fields are not editable. On the data source card, the primary and secondary hostname or IP address and the Timezone details are displayed.

Note

- When you launch the Data Sources listing page for the first time (after configuring streaming data source), you will be prompted to accept certificates.
- When using Self-Signed certificates, you must accept them explicitly before you can use Cisco Unified Intelligence Center functionalities which includes using Live Data Reports. For more information, see *Browser Support and Self -Signed Certificates* section in *Cisco Unified Intelligence Center User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html.