Admin User Management Drawer

Choose **Admin User Management drawer** > **Admin User Management**Admin User Management page, where you view and maintain the Super Users for the Administration console.

Super Users are authorized to add and maintain the functions that are controlled in the Administration console, such as adding devices and starting or stopping services.

Note Super Users can also sign in to Unified Intelligence Center Reporting.

Note Any drop-down list that contains only a single item does not expand when you click the drop-down list. This is a known issue in the Internet Explorer 11 Compatibility mode for Unified Intelligence Administration, Cisco Unified OS Administration, Cisco Unified Serviceability, and Disaster Recovery System.

- Manage All Super Users, on page 1
- Edit Configuration Data for Super User, on page 2

Manage All Super Users

The Admin Users page is a list of the names and roles for all configured Super Users in the system. This list always contains at least one row that shows the System Application User who is configured during installation and who becomes the initial Super User for Unified Intelligence Center. See Users in the Administration Console.

To navigate to this page, click the **Admin User Management drawer** > **Admin User Management**.

The rows on the Users page contain two columns. There is a checkbox to the left of each row for selecting that user. Click the check box in the heading row to select all users. Use the Filter feature to narrow the list of names.

Table 1: Rows on This Page

Field	Description
User Name	The User ID used to log in to the operations console.

Field	Description
Role	The role is Super User for all user names.

Table 2: Actions From This Page

To	Do This
Add a new Super User	Click **Add New** to open a blank Edit Configuration Data for Super User page. You can add as many Super Users as you need.
Delete a Super User	Check the box next to the User Name and click **Delete**. You cannot delete: • the Super User defined in the installation. • the Super User who is currently signed in.
Edit an existing Super User	The User Name is a link. Click the User Name to open that user's Edit Configuration Data for Super User page.
Search for a Super User	Enter values in the filter fields.
Select a User Name	Check the check box in the left column of the row for that user.
Select all Users Names	Check the check box in the top (header) row of the list.

Related Topics

Users in the Administration Console
Filter
Edit Configuration Data for Super User, on page 2

Super Users and Security

There is no limit to the number of additional Super Users that the default Super User (the System Application User) can create.

Although only the initial, default Super User (the System Application User) has full permissions in Unified Intelligence Center Reporting, *all* Super Users have *identical permissions in the Administration console*.

Be aware that any Super User can delete or change the password of another Super User, even if that other Super User is currently logged in.

Edit Configuration Data for Super User

Use this page to create configuration data for a new Super User or to edit the configuration data for an existing Super User.

To navigate to this page, choose **Admin User Management drawer** > **Admin User Management** to open the Users page. Then click **Add New** to add and configure a new user or click an existing User Name to edit the configuration for that user.

This page has three tabs - **General**, **Credentials**, and **Policy.**

If a field is grayed-out, then that field it not editable. An asterisk indicates that the field is required.

Actions on this page are **Save** and **Cancel.**

Table 3: General Tab

Field	Description
Admin Password	Password to authenticate changes made to the **General**, **Credentials**, and **Policy** tabs..
User Name	The user Id for the user.
User Password	User Password. To require a secure password, enable **Check for Trivial Passwords** on the Policy tab.
Confirm User Password	The same User password as above to confirm spelling.
Role	The only role is Super User.

Note The values on the **General** tab apply to the specific Super User being added or edited.

Table 4: Credentials Tab

Field	Description
Locked by Administrator	If checked, this Super User is locked out.
User Cannot Change / Must Change	This pertains to the user password. Select either **User Cannot Change** or **User Must Change at Next Login**. You cannot select both.
Does Not Expire	This pertains to the user password. If the **Credential Expires After (days)** field on the **Policy** tab is checked, then this field is disabled. If the **Credential Expires After (days)** field on the **Policy** tab is clear, check **Does Not Expire** to enable a persistent password for the Super User. **Note** DO NOT check the **Does Not Expire** box if you have checked **User Must Change at Next Login**, as the user will not be prompted to change the password at the next login.

Field	Description
Reset Hack Count	Check this box to reset the hack count for this user and clear the **Time Locked Due to Failed Login Attempts** field. After the counter resets, the user can try logging in again. **Note** If the user is locked out of the account due to failed logins exceeding the number set for **Failed Login** (on the **Policy** tab), then you can unlock the account by checking this box and clicking **Save**.
Failed Sign On Attempts	Displays the number of failed logon attempts since the last successful logon, since the hack count was reset for this Super User credential, or since the reset failed logon attempts time has expired.
Time Last Changed	Displays the last time this user's credentials were changed.
Time of Last Failed **Login** Attempt	Displays the date and time of the last logon attempt by the user.
Time Locked by Administrator	Displays the date and time that this user account was locked.
Time Locked Due to Failed **Logon** Attempts	Displays the date and time that the system last locked this user account due to failed logon attempts.

Note The values on the **Credentials** tab apply to the specific Super User being added or edited.

The credentials for Administration Super Users are encrypted into the local database. Super Users are not authenticated through Active Directory.

Table 5: Policy Information

Field	Description
Failed Sign On*	Specify the number of allowed failed logon attempts. When this threshold is reached, the system locks the account. By default, Unified Intelligence Center allows maximum five login attempts and the **No Limit For Failed Sign On** check box is unchecked. If you want to allow unlimited logon attempts, enter a value of zero or check the **No Limit For Failed Sign On** check box.
Reset Failed Logon Attempts every (minutes)*	Specify the number of minutes before the counter is reset for failed logon attempts. After the counter resets, the user can try logging in again. Allowed range is zero to 120; default is 30.
Lockout Duration (minutes)	Specify the number of minutes an account remains locked when the number of failed logon attempts exceeds the specified threshold. Allowed range is zero to 120; default is 30. Checking the **Administrator Must Unlock** check box means that the account must be unlocked manually.

Field	Description
Minimum Duration Between Credential Changes (minutes)*	Specify the number of minutes that are required before a user can change credentials again. Allowed range is zero to 120; default is zero.
Credentials Expires After (days)*	Enter an integer here to define in how many days this user's credentials shall expire. After this many days has elapsed, the user will no longer be able to logon. Optionally you can check **Never Expires** to have the credentials never expire.
Minimum Credential Length*	Minimum number of characters for the password.
Stored Number of Previous Credentials	Specify the number of previous passwords that the system stores. The system does not allow changing the password if the new password matches with any of the stored passwords. The maximum permissible value for this field is 15; the default value is 5, indicating that the new password should not be the same as the last 5 passwords.
Inactive Days Allowed*	Specify the number of days that a password can remain inactive before the account gets locked. Allowed range is zero to 5000; default is zero.
Expiry Warning Days*	Specify the number of days before a user password expires to start warning notifications. Allowed range is zero to 90; default is zero.
Check for Trivial Passwords	Check this check box for the system to disallow credentials that are easily hacked, such as common words, repeated character patterns, and so on.

Note The Policy information is applicable to all Super Users.