



Users

The Firewall Management Center includes default **admin** accounts for web and CLI access. This chapter discusses how to create custom user accounts.

- [About Users, on page 1](#)
- [Create a User Record with Your Security Cloud Control Username, on page 4](#)
- [Troubleshooting LDAP Authentication Connections, on page 5](#)
- [Configure User Preferences, on page 6](#)

About Users

You can add custom user accounts on managed devices, either as internal users or as external users on a LDAP or RADIUS server. Each managed device maintains separate user accounts. For example, when you add a user to the Firewall Management Center, that user only has access to the Firewall Management Center; you cannot then use that username to log directly into a managed device. You must separately add a user on the managed device.

Internal and External Users

Managed devices support two types of users:

- Internal user—The device checks a local database for user authentication.
- External user—If the user is not present in the local database, the system queries an external LDAP or RADIUS authentication server.

User Roles

Web Interface User Roles

There are a variety of user roles in Security Cloud Control (Security Cloud Control): Read-Only, Edit-Only, Deploy-only, Admin, and Super Admin. User roles are configured for each user on each tenant. If a Security Cloud Control user has access to more than one tenant, they may have the same user ID but different roles on different tenants. A user may have a read-only role on one tenant and a Super Admin role on another. When the interface or the documentation refers to a Read-only user, Deploy Only, Edit Only, an Admin user, or a Super Admin user we are describing that user's permission level on a particular tenant. Note that you

cannot create user roles in the cloud-delivered Firewall Management Center because it uses Security Cloud Control user roles.

Read Only

Read Only users can view all device configurations but not change them.

Deploy Only

Deploy Only users can audit queued changes made to device configurations and deploy them but cannot change them.

Edit Only

Edit Only users can make changes to all device configurations but cannot deploy them to devices.

Super Admin and Admin

Super Admin and Admin users can access everything in the product. The difference between Super Admin and Admin users is that Super Admins can create accounts for other users on a tenant and modify existing user roles, while admins cannot.

To know more about user roles in Security Cloud Control, see [User Roles](#).

The following table maps the user roles in On-Premises Firewall Management Center to their equivalent roles in the cloud-delivered Firewall Management Center in Security Cloud Control.



Tip We recommend that you read through the table only if you are familiar with the user roles in On-Premises Firewall Management Center.

Table 1: Secure Firewall Management Center and Cloud-delivered Firewall Management Center User Role Mapping

On-Premises Firewall Management Center User Role	Equivalent Cloud-delivered Firewall Management Center User Role	Capabilities
Access Admin, Discovery Admin, Intrusion Admin, Maintenance User	Edit Only	<p>You can search, filter, or view the following:</p> <ul style="list-style-type: none"> • Access control policies and associated features • Intrusion policies • Intrusion rules • Network discovery rules • Custom detectors • Correlation policies • Objects • Rulesets • Interfaces • VPN configurations • Monitoring- and maintenance-related settings <p>You can back up or restore a device but cannot deploy policies to the devices.</p>
Administrator	Super Admin	You can access all features of the cloud-delivered Firewall Management Center and perform tasks, including create, read, modify, or delete policies or objects and deploy those changes to the devices. You can also edit user roles or create user records in Security Cloud Control.
Network Admin	Admin	You can access all features of the cloud-delivered Firewall Management Center and perform tasks, including create, read, modify, or delete policies or objects and deploy those changes to the devices. However, you cannot edit user roles or create user records in Security Cloud Control.


On-Premises Firewall Management Center User Role	Equivalent Cloud-delivered Firewall Management Center User Role	Capabilities
Security Analyst, Security Analyst (Read Only)	Read Only	<p>You can view device information, policies, objects, and their related settings but cannot do the following:</p> <ul style="list-style-type: none"> • Create or edit objects • Create or edit policies • Modify device configurations • Backup or restore devices
Security Approver	Deploy Only	<p>You can view most settings and deploy staged changes to devices but cannot create or modify objects or policies.</p>

Create a User Record with Your Security Cloud Control Username

Only a Security Cloud Control user with **Super Admin** privileges can create the Security Cloud Control user record. The **Super Admin** must create the user record with the same email address that was specified in the **Create Your Security Cloud Control Username** task above.

Use the following procedure to create a user record with an appropriate user role:

Procedure

-
- Step 1** Login to Security Cloud Control.
- Step 2** In the left pane, choose **Settings > User Management**.
- Step 3** Click  to add a new user to your tenant.
- Step 4** Provide the email address of the user.
- Note**
The user's email address must correspond to the email address of the Cisco Secure Log-On account.
- Step 5** From the **Role** drop-down list, select the user's [role](#).
- Step 6** Click **OK**.
-

Troubleshooting LDAP Authentication Connections

If you create an LDAP authentication object and it either does not succeed in connecting to the server you select or does not retrieve the list of users you want, you can tune the settings in the object.

If the connection fails when you test it, try the following suggestions to troubleshoot your configuration:

- Use the messages displayed at the top of the web interface screen and in the test output to determine which areas of the object are causing the issue.
- Check that the user name and password you used for the object are valid:
 - Check that you have the rights to browse to the directory indicated in your base-distinguished name by connecting to the LDAP server using a third-party LDAP browser.
 - Check that the user name is unique to the directory information tree for the LDAP server.
 - If you see an LDAP bind error 49 in the test output, the user binding for the user failed. Try authenticating to the server through a third-party application to see if the binding fails through that connection as well.
- Check that you have correctly identified the server:
 - Check that the server IP address or host name is correct.
 - Check that you have TCP/IP access from your local appliance to the authentication server where you want to connect.
 - Check that access to the server is not blocked by a firewall and that the port you have configured in the object is open.
 - If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used for the server.
 - Check that you have not used an IPv6 address for the server connection if you are authenticating CLI access.
 - If you used server type defaults, check that you have the correct server type and click **Set Defaults** again to reset the default values.
- If you typed in your base-distinguished name, click **Fetch DNs** to retrieve all the available base distinguished names on the server, and select the name from the list.
- If you are using any filters, access attributes, or advanced settings, check that each is valid and typed correctly.
- If you are using any filters, access attributes, or advanced settings, try removing each setting and testing the object without it.
- If you are using a base filter or a CLI access filter, make sure that the filter is enclosed in parentheses and that you are using a valid comparison operator (maximum 450 characters, including the enclosing parentheses).
- To test a more restricted base filter, try setting it to the base distinguished name for the user to retrieve just that user.

- If you are using an encrypted connection:
 - Check that the name of the LDAP server in the certificate matches the host name that you use to connect.
 - Check that you have not used an IPv6 address with an encrypted server connection.
- If you are using a test user, make sure that the user name and password are typed correctly.
- If you are using a test user, remove the user credentials and test the object.
- Test the query that you are using by connecting to the LDAP server and using this syntax:

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

For example, if you are trying to connect to the security domain on `myrtle.example.com` using the `domainadmin@myrtle.example.com` user and a base filter of `(cn=*)`, you could test the connection using this statement:

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

If you can test your connection successfully but authentication does not work after you deploy a platform settings policy, check that authentication and the object you want to use are both enabled in the platform settings policy that is applied to the device.

If you connect successfully but want to adjust the list of users retrieved by your connection, you can add or change a base filter or CLI access filter or use a more restrictive or less restrictive base DN.

While authenticating a connection to Active Directory (AD) server, rarely the connection event log indicates blocked LDAP traffic although the connection to AD server is successful. This incorrect connection log occurs when the AD server sends a duplicate reset packet. The Firewall Threat Defense device identifies the second reset packet as part of a new connection request and logs the connection with Block action.

Configure User Preferences

Depending on your user role, you can specify certain preferences for your user account.

Change the Web Interface Appearance

You can change the way the web interface appears when you are using the light theme.

Procedure

-
- Step 1** From the drop-down list under your username, choose **User Preference**.
 - Step 2** Under **Light theme variant**, click the **Use new design** toggle button to enable or disable the new design.

Enable the toggle to use the left navigation menu and disable it to use the top navigation menu.

Note

This toggle works only if you are using the light theme. If you want to switch between dark theme and light theme, you must do this from the **General Preference** page in Cisco Security Cloud Control. For more information, see [Change the Security Cloud Control Web Interface Appearance](#).

Setting Your Default Time Zone

This setting determines the times displayed in the web interface for your user account only, for things like task scheduling and viewing dashboards. This setting does not change the system time or affect any other user, and does not affect data stored in the system, which generally uses UTC.

**Warning**

The Time Zone function (in User Preferences) assumes that the system clock is set to UTC time. **DO NOT ATTEMPT TO CHANGE THE SYSTEM TIME.** Changing the system time from UTC is **NOT** supported, and doing so will require you to reimage the device to recover from an unsupported state.

**Note**

This feature does not affect the time zone used for time-based policy application. Set the time zone for a device in **Devices > Platform Settings**.

Procedure

- Step 1** From the drop-down list under your user name, choose **User Preferences**.
- Step 2** Click **Time Zone** drop-down.
- Step 3** Choose the continent or country and the state name that corresponds with the time zone you want to use.

Configure How-To Settings

How To is a widget that provides walkthroughs to navigate through tasks on the Firewall Management Center. The walkthroughs guide you to perform the steps required to achieve a task by taking you through each step, one after the other irrespective of the various UI screens that you may have to navigate, to complete the task. The **How To** widget is enabled by default.

For a list of feature walkthroughs supported in the Firewall Management Center, see [Feature Walkthroughs Supported in Secure Firewall Management Center](#).

Procedure

- Step 1** From the drop-down list under your user name, choose **User Preferences**.

- Step 2** Click the **How-To Settings** tab.
- Step 3** Check the **Enable How-Tos** check box to enable How-Tos.
- Step 4** Click **Save**.
-

What to do next

To open the How To widget, choose **Help** (?) > **On-screen Assistance** > **How-Tos**. You can search for How-To walkthroughs that address tasks of interest.