Users

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

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 management center, that user only has access to the 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 Cisco Defense Orchestrator (CDO): Read-Only, Edit-Only, Deploy-only, Admin, and Super Admin. User roles are configured for each user on each tenant. If a CDO 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 CDO 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 cannnot.

To know more about user roles in CDO, see User Roles.

The following table maps the user roles in On-Prem Firewall Management Center to their equivalent roles in the cloud-delivered Firewall Management Center in CDO.

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

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

On-Prem Firewall Management Center User Role	Equivalent Cloud-delivered Firewall Management Center User Role	Capabilities
Access Admin, Discovery Admin, Intrusion Admin, Maintenance User	Edit Only	You can search, filter, or view the following: • 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 You can back up or restore a device but cannot deploy policies to the devices.
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 CDO.
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 CDO.

On-Prem Firewall Management Center User Role	Equivalent Cloud-delivered Firewall Management Center User Role	Capabilities
Security Analyst, Security Analyst (Read Only)	Read Only	You can view device information, policies, objects, and their related settings but cannot do the following: • Create or edit objects • Create or edit policies • Modify device configurations • Backup or restore devices
Security Approver	Deploy Only	You can view most settings and deploy staged changes to devices but cannot create or modify objects or policies.

Create a CDO User Record with Your CDO Username

Only a CDO user with "Super Admin" privileges can create the CDO user record. The Super Admin should create the user record with the same email address that was specified in the **Create Your CDO Username** task above.

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

Procedure

Step 1 Login to CDO.

Step 2 From the CDO navigation bar, click **Settings** > **User Management**.

Step 3 Click the blue plus button (+) 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 Select the user's role from the drop-down menu.

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 threat defense device identifies the second reset packet as part of a new connection request and logs the connection with Block action.