Users

The management center includes default **admin** accounts for web and CLI access. This chapter discusses how to create custom user accounts. See Logging into the Management Center for detailed information about logging into the management center with a user account.

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.

Web Interface and CLI Access

The management center has a web interface, CLI (accessible from the console (either the serial port or the keyboard and monitor) or using SSH to the management interface), and Linux shell. For detailed information about the management UIs, see System User Interfaces.

See the following information about management center user types, and which UI they can access:

- admin user—The management center supports two different internal **admin** users: one for the web interface, and another with CLI access. The system initialization process synchronizes the passwords for these two **admin** accounts so they start out the same, but they are tracked by different internal mechanisms and may diverge after initial configuration. See the *Getting Started Guide* for your model for more information on system initialization. (To change the password for the web interface **admin**, use **System** (✿) > **Users** > **Users**. To change the password for the CLI **admin**, use the management center CLI command **configure password**.)

- Internal users—Internal users added in the web interface have web interface access only.

- External users—External users have web interface access, and you can optionally configure CLI access.

- SSO users—SSO users have web interface access only.

⚠

Caution   CLI users can access the Linux shell using the **expert** command. We strongly recommend that you do not use the Linux shell unless directed by Cisco TAC or explicit instructions in the management center documentation. CLI users can obtain `sudoers` privileges in the Linux shell, which can present a security risk. For system security reasons, we strongly recommend that you:

- Restrict the list of external users with CLI access appropriately.

- Do not add users directly in the Linux shell; only use the procedures in this chapter.

User Roles

CLI User Role

CLI external users on the management center do not have a user role; they can use all available commands.

Web Interface User Roles

User privileges are based on the assigned user role. For example, you can grant analysts predefined roles such as Security Analyst and Discovery Admin and reserve the Administrator role for the security administrator managing the device. You can also create custom user roles with access privileges tailored to your organization's needs.

To view the privileges assigned to predefined user roles, click **Copy** (⧉) for a role as though you are going to make a custom role based on the predefined role. You can then see all of the privileges assigned.

Figure 1: View User Role Privileges

The management center includes the following predefined user roles:

Access Admin

Provides access to access control policy and associated features in the **Policies** menu. Access Admins cannot deploy policies.

Administrator

Administrators have access to everything in the product; their sessions present a higher security risk if compromised, so you cannot make them exempt from login session timeouts.

You should limit use of the Administrator role for security reasons.

Discovery Admin

Provides access to network discovery, application detection, and correlation features in the **Policies** menu. Discovery Admins cannot deploy policies.

External Database User (Read Only)

Provides read-only access to the database using an application that supports JDBC SSL connections. For the third-party application to authenticate to the appliance, you must enable database access in the system settings. On the web interface, External Database Users have access only to online help-related options in the **Help** menu. Because this role's function does not involve the web interface, access is provided only for ease of support and password changes.

Intrusion Admin

Provides access to all intrusion policy, intrusion rule, and network analysis policy features in the **Policies** and **Objects** menus. Intrusion Admins cannot deploy policies.

Maintenance User

Provides access to monitoring and maintenance features. Maintenance Users have access to maintenance-related options in the **Health** and **System** menus.

Network Admin

Provides access to access control, SSL inspection, DNS policy, and identity policy features in the **Policies** menu, as well as device configuration features in the **Devices** menus. Network Admins can deploy configuration changes to devices.

Security Analyst

Provides access to security event analysis features, and read-only access to health events, in the **Overview**, **Analysis**, **Health**, and **System** menus.

Security Analyst (Read Only)

Provides read-only access to security event analysis features and health event features in the **Overview**, **Analysis**, **Health**, and **System** menus.

User with this role can also:

• From the health monitor pages for specific devices, generate and download troubleshooting files.

• Under user preferences, set file download preferences.

• Under user preferences, set the default time window for event views (with the exception of the **Audit Log Time Window**).

Security Approver

Provides limited access to access control and associated policies and network discovery policies in the **Policies** menu. Security Approvers can view and deploy these policies, but cannot make policy changes.

Threat Intelligence Director (TID) User

Provides access to Threat Intelligence Director configurations in the **Intelligence** menu. Threat Intelligence Director (TID) Users can view and configure TID.

User Passwords

The following rules apply to passwords for internal user accounts on the management center, with Lights-Out Management (LOM) enabled or disabled. Different password requirements apply for externally authenticated accounts or in systems with security certifications compliance enabled. See Configure External Authentication for the Management Center, on page 11 and Security Certifications Compliance for more information.

During management center initial configuration, the system requires the **admin** user to set the account password to comply with strong password requirements described in the table below. For physical management centers, the strong password requirements with LOM enabled are used, and for virtual management centers, the strong password requirements with LOM not enabled are used. At this time the system synchronizes the passwords for the web interface **admin** and the CLI access **admin**. After initial configuration, the web interface **admin** can remove the strong password requirement, but the CLI access **admin** must always comply with strong password requirements with LOM not enabled.

	LOM Not Enabled	**LOM Enabled**
Password Strength Checking On	Passwords must include: • At least eight characters, or the number of characters configured for the user by the administrator, whichever is greater. • No more than two sequentially repeating characters • At least one lower case letter • At least one upper case letter • At least one digit • At least one special character such as ! @ # * - _ + The system checks passwords against a special dictionary containing not only many English dictionary words, but also other character strings that could be easily cracked with common password hacking techniques.	Passwords must include: • Between eight and twenty characters (On MC 1000, MC 2500, and MC 4500 the upper limit is fourteen characters rather than twenty.) • No more than two sequentially repeating characters • At least one lower case letter • At least one upper case letter • At least one digit • At least one special character such as ! @ # * - _ + The rules for special characters vary between different series of physical management centers. We recommend restricting your choice of special characters to those listed in the final bullet above. Do not include the user name in the password. The system checks passwords against a special dictionary containing not only many English dictionary words, but also other character strings that could be easily cracked with common password hacking techniques.

	LOM Not Enabled	**LOM Enabled**

Password Strength Checking Off	Passwords must include the minimum number of characters configured for the user by the administrator. (See Add or Edit an Internal User, on page 9 for more information.)	Passwords must include:
		
		• Between eight and twenty characters (On MC 1000, MC 2500, and MC 4500 the upper limit is fourteen characters rather than twenty.)
		
		• Characters from at least three of the following four categories:
		
		    • Uppercase letters
		
		    • Lowercase letters
		
		    • Digits
		
		    • Special characters such as ! @ # * - _ +
		
		The rules for special characters vary between different series of physical management centers. We recommend restricting your choice of special characters to those listed in the final bullet above.
		
		Do not include the user name in the password.

Users and Domains

In a multidomain deployment, you can create user accounts in any domain in which you have been assigned Administrator access.

User Roles in Domains

Users can have different privileges in each domain. You can assign user roles in both ancestor and descendant domains. For example, you can assign read-only privileges to a user in the Global domain, but Administrator privileges in a descendant domain:

Figure 2: User Roles Per Domain

User Management

Users are only visible in the domain in which they are created.

If you add a user in the current domain but assign a user role in a subdomain, then that user will only show on the current domain's **Users** page, even though the user has a role in a subdomain. For example, from the Global domain, you add user **leaf** and assign a role for **Leaf1**, but because you were in the Global domain when you added the user, you can see it from the Global domain:

Figure 3: Global Domain Users

Username	Real Name	Domains
admin		Global
leaf		Global \ Leaf1

If you change domains to **Leaf1**, you cannot see the user **leaf**, but you can see the user **test**, which was added directly from the Leaf1 subdomain:

Figure 4: Subdomain Users

Username	Real Name	Domains
test		Global \ Leaf1

Logging In

Users added from the Global domain will log in with just their username, even if their roles are only in a subdomain. In this case, **leaf** only has a user role in the **Leaf1** subdomain, but because it was added from Global, do not include the subdomain in the login:

Figure 5: User Login When Added in Global

Username

leaf

Password

....

Log In

Users added directly in a subdomain need to log into the management center with the subdomain(s) as part of the login name, depending on which domain their user was added from: *subdomain1\subdomain2\username*. You do not need to enter the **Global** parent domain. For example, **test** was added from the **Leaf1** subdomain, so you need to include Leaf1 in the login name:

Figure 6: Global Domain User Login

Username
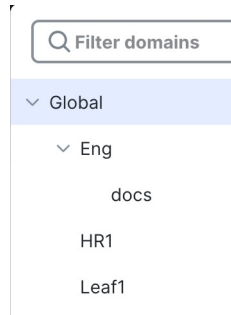
Leaf1\test

Password

....

Log In

When you log in, you are placed in the domain where your username was added. For example, the admin user defaults to the Global domain:

Figure 7: User Domain at Login

Global \ admin ⌄

However, after login, you can change to a subdomain by clicking the down arrow:

Figure 8: Change to a Subdomain

🔍 Filter domains

⌄ Global

⌄ Eng

docs

HR1

Leaf1

Guidelines and Limitations for User Accounts for Management Center

- The management center includes an **admin** user as a local user account for all forms of access; you cannot delete the **admin** user. The default initial password is **Admin123**; the system forces you to change this during the initialization process. See the *Getting Started Guide* for your model for more information about system initialization.

- By default, the following settings apply to all user accounts on the management center:

    - There are no limits on password reuse.

    - The system does not track successful logins.

    - The system does not enforce a timed temporary lockout for users who enter incorrect login credentials.

    - There are no user-defined limits on the number of read-only and read/write sessions that can be open at the same time.

    You can change these settings for all users as a system configuration. (**System** (⚙) > **Configuration** > **User Configuration**) See User Configuration.

- Ensure that you follow the principles of least privilege when assigning default access roles to users at initial setup. When a user first logs in to the system with their credentials, their account will be assigned this default access role. We recommend that the default access role be the lowest possible privilege required for anyone to log in to the system. For example, common users can be given the Security Analyst (Read-Only) role as the default access role, and administrators can be added to a separate administrator's group to give them full administrator rights. If you do not follow the principles of least privilege while assigning the default access role, users may be assigned an unintended privilege level on subsequent

logins. This could result in the users having privileges beyond their required access role. Note that this guideline applies to all users - internal, external, or CAC users.

If a user who has logged in with the default access role needs a temporary elevation of their privileges, a user with administrative privileges can temporarily provide that user the required higher level of access by assigning them a role with higher privilege. This privilege will be revoked after 24 hours of inactivity, and the user will return to their default access role.

If a user needs a permanent access role reassignment to a higher privilege level, such as System Admin, use the Group Controlled Access Roles method to provide admin access to the user. This method ensures that the provided access role persists beyond 24 hours and users will have the correct privilege level as per the group assignment. For more information on configuring Group Controlled Access Roles, see the Add an LDAP External Authentication Object for Management Center section.

Requirements and Prerequisites for User Accounts for Management Center

Model Support

Management Center

Supported Domains

• SSO configuration—Global only.

• All other features—Any.

User Roles

• SSO configuration—Only users with the Admin role authenticated internally or by LDAP or RADIUS can configure SSO.

• All other features—Any user with the Admin role.

• Configure Common Access Card Authentication with LDAP, on page 27 also supports the Network Admin role.

Add or Edit an Internal User

This procedure describes how to add custom internal user accounts for the management center.

The **System** > **Users** > **Users** shows both internal users that you added manually and external users that are added automatically when a user logged in with LDAP or RADIUS authentication. For external users, you can modify the user role on this screen if you assign a role with higher privileges; you cannot modify the password settings.

If you enable security certifications compliance or Lights-Out Management (LOM) on a device, different password restrictions apply. For more information on security certifications compliance, see Security Certifications Compliance.

✎

Note   Avoid having multiple Admin users simultaneously creating new users on the management center, as this may cause an error resulting from a conflict in user database access.

Procedure

Step 1   Choose **System** (✿) > **Users**.

Step 2   To create a new user:

a)   Click **Create User**.

b)   Enter a **User Name**.

The username must comply with the following restrictions:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_).

- Letters may be upper or lower case.

- Cannot include any punctuation or special characters other than period (.), hyphen (-), and underscore (_).

Step 3   To edit an existing user, click the **Edit** (✐) icon next to the user you want to edit.

Step 4   **Real Name**: Enter descriptive information to identify the user or department to whom the account belongs.

Step 5   The **Use External Authentication Method** check box is checked for users that were added automatically when they logged in with LDAP or RADIUS. You do not need to preconfigure external users, so you can ignore this field. For an external user, you can revert this user to an internal user by unchecking the check box.

Step 6   Enter values in the **Password** and **Confirm Password** fields.

The values must conform to the password options you set for this user.

Step 7   Set the **Maximum Number of Failed Logins**.

Enter an integer without spaces to specify the maximum number of times each user can try to log in after a failed login attempt before the account is locked. The default setting is 5 tries; use **0** to allow an unlimited number of failed logins. The **admin** account is exempt from being locked out after a maximum number of failed logins unless you enable security certification compliance.

Step 8   Set the **Minimum Password Length**.

Enter an integer without spaces to specify the minimum required length, in characters, of a user's password. The default setting is **8**. A value of **0** indicates that no minimum length is required.

Step 9   Set the **Days Until Password Expiration**.

Enter the number of days after which the user's password expires. The default setting is **0**, which indicates that the password never expires. If you change from the default, then the **Password Lifetime** column of the **Users** list indicates the days remaining on each user's password.

Step 10   Set the **Days Before Password Expiration Warning**.

Enter the number of warning days users have to change their password before their password actually expires. The default setting is **0** days.

Step 11 Set the following **Options**:

- **Force Password Reset on Login**: Forces users to change their passwords the next time they log in.

- **Check Password Strength**: Requires strong passwords. When password strength checking is enabled, passwords must comply with the strong password requirements described in User Passwords, on page 4.

- **Exempt from Browser Session Timeout**: Exempts a user's login sessions from termination due to inactivity. Users with the Administrator role cannot be made exempt.

Step 12 In the **User Role Configuration** area, assign the user roles. For more information about user roles, see Customize User Roles for the Web Interface, on page 81.

For external users, if the user role is assigned through group membership (LDAP), or based on a user attribute (RADIUS), you cannot remove the minimum access rights. You can, however, assign additional rights. If the user role is the default user role that you set on the device, then you can modify the role in the user account without limitations. When you modify the user role, the **Authentication Method** column on the **Users** tab provides a status of **External - Locally Modified**.

The options that you see depend on whether the device is in a single domain or multidomain deployment.

- Single domain: Check the user roles you want to assign the user.

- Multidomain: In a multidomain deployment, you can create user accounts in any domain in which you have been assigned Administrator access. Users can have different privileges in each domain. You can assign user roles in both ancestor and descendant domains. For example, you can assign read-only privileges to a user in the Global domain, but Administrator privileges in a descendant domain. For more information, including how to log in when a user is added in a subdomain, see Users and Domains, on page 6. See the following steps:

    a. Click **Add Domain**.

    b. Choose a domain from the **Domain** drop-down list.

    c. Check the user roles that you want to assign the user.

    d. Click **Save**.

Step 13 (Optional, for physical management centers only) If you have assigned the user the Administrator role, the **Administrator Options** appear. You can select **Allow Lights-Out Management Access** to grant Lights-Out Management access to the user. See Lights-Out Management Overview for more information about Lights-Out Management.

Step 14 Click **Save**.

Configure External Authentication for the Management Center

To enable external authentication, you need to add one or more external authentication objects.

About External Authentication for the Management Center

When you enable external authentication, the management center verifies the user credentials with an LDAP or RADIUS server as specified in an *external authentication object*.

You can configure multiple external authentication objects for web interface access. For example, if you have 5 external authentication objects, users from any of them can be authenticated to access the web interface. You can use only one external authentication object for CLI access. If you have more than one external authentication object enabled, then users can authenticate using only the first object in the list.

External authentication objects can be used by the management center and threat defense devices. You can share the same object between the different appliance/device types, or create separate objects.

Note The timeout range is different for the threat defense and the management center, so if you share an object, be sure not to exceed the threat defense's smaller timeout range (1-30 seconds for LDAP, and 1-300 seconds for RADIUS). If you set the timeout to a higher value, the threat defense external authentication configuration will not work.

For the management center, enable the external authentication objects directly on the **System** > **Users** > **External Authentication** tab; this setting only affects management center usage, and it does not need to be enabled on this tab for managed device usage. For threat defense devices, you must enable the external authentication object in the platform settings that you deploy to the devices.

Web interface users are defined separately from CLI users in the external authentication object. For CLI users on RADIUS, you must pre-configure the list of RADIUS usernames in the external authentication object. For LDAP, you can specify a filter to match CLI users on the LDAP server.

You cannot use an LDAP object for CLI access that is also configured for CAC authentication.

Note Users with CLI access can gain Linux shell access with the **expert** command. Linux shell users can obtain root privileges, which can present a security risk. Make sure that you:

- Restrict the list of users with CLI or Linux shell access.

- Do not create Linux shell users.

About LDAP

The Lightweight Directory Access Protocol (LDAP) allows you to set up a directory on your network that organizes objects, such as user credentials, in a centralized location. Multiple applications can then access those credentials and the information used to describe them. If you ever need to change a user's credentials, you can change them in one place.

Microsoft has announced that Active Directory servers will start enforcing LDAP binding and LDAP signing in 2020. Microsoft is making these a requirement because when using default settings, an elevation of privilege vulnerability exists in Microsoft Windows that could allow a man-in-the-middle attacker to successfully forward an authentication request to a Windows LDAP server. For more information, see 2020 LDAP channel binding and LDAP signing requirement for Windows on the Microsoft support site.

If you have not done so already, we recommend you start using TLS/SSL encryption to authenticate with an Active Directory server.

About RADIUS

Remote Authentication Dial In User Service (RADIUS) is an authentication protocol used to authenticate, authorize, and account for user access to network resources. You can create an authentication object for any RADIUS server that conforms to RFC 2865.

Secure Firewall devices support the use of SecurID tokens. When you configure authentication by a server using SecurID, users authenticated against that server append the SecurID token to the end of their SecurID PIN and use that as their password when they log in. You do not need to configure anything extra on the Secure Firewall device to support SecurID.

Add an LDAP External Authentication Object for the Management Center

Add an LDAP server to support external users for device management.

Before you begin

- You must specify DNS server(s) for domain name lookup on your device. Even if you specify an IP address and not a hostname for the LDAP server on this procedure, the LDAP server may return a URI for authentication that can include a hostname. A DNS lookup is required to resolve the hostname. See Modify Management Center Management Interfaces to add DNS servers.

- If you are configuring an LDAP authentication object for use with CAC authentication, do not remove the CAC inserted in your computer. You must have a CAC inserted at all times after enabling user certificates.

Procedure

Step 1   Choose **System** (⚙) > **Users**.

Step 2   Click the **External Authentication** tab.

Step 3   Click **Add icon** (➕) **Add External Authentication Object**.

Step 4   Set the **Authentication Method** to **LDAP**.

Step 5   (Optional) Check the check box for **CAC** if you plan to use this authentication object for CAC authentication and authorization.

You must also follow the procedure in Configure Common Access Card Authentication with LDAP, on page 27 to fully configure CAC authentication and authorization. You cannot use this object for CLI users.

Step 6   Enter a **Name** and optional **Description**.

Step 7   Choose a **Server Type** from the drop-down list.

Tip
If you click **Set Defaults**, the device populates the **User Name Template**, **UI Access Attribute**, **CLI Access Attribute**, **Group Member Attribute**, and **Group Member URL Attribute** fields with default values for the server type.

Step 8   For the **Primary Server**, enter a **Host Name/IP Address**.

If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used in this field. In addition, IPv6 addresses are not supported for encrypted connections.

Step 9   (Optional) Change the **Port** from the default.

Step 10   (Optional) Enter the **Backup Server** parameters.

Step 11   Enter **LDAP-Specific Parameters**.

a) Enter the **Base DN** for the LDAP directory you want to access. For example, to authenticate names in the Security organization at the Example company, enter `ou=security,dc=example,dc=com`. Alternatively click **Fetch DNs**, and choose the appropriate base distinguished name from the drop-down list.

b) (Optional) Enter the **Base Filter**. For example, if the user objects in a directory tree have a `physicalDeliveryOfficeName` attribute and users in the New York office have an attribute value of `NewYork` for that attribute, to retrieve only users in the New York office, enter `(physicalDeliveryOfficeName=NewYork)`.

If you are using CAC authentication, to filter only active user accounts (excluding the disabled user accounts), enter `(!(userAccountControl:1.2.840.113556.1.4.803:=2))`. This criteria retrieves user accounts within AD belonging to `ldpgrp` group and with `userAccountControl` attribute value that is not `2` (disabled).

c) Enter a **User Name** for a user who has sufficient credentials to browse the LDAP server. For example, if you are connecting to an OpenLDAP server where user objects have a `uid` attribute, and the object for the administrator in the Security division at your example company has a `uid` value of `NetworkAdmin`, you might enter `uid=NetworkAdmin,ou=security,dc=example,dc=com`.

d) Enter the user password in the **Password** and the **Confirm Password** fields.

e) (Optional) Click **Show Advanced Options** to configure the following advanced options.

- **Encryption**—Click **None**, **TLS**, or **SSL**.

  If you change the encryption method after specifying a port, you reset the port to the default value for that method. For **None** or **TLS**, the port resets to the default value of 389. If you choose SSL encryption, the port resets to 636.

- **SSL Certificate Upload Path**—For SSL or TLS encryption, click **Choose File** and choose the complete CA chain certificate.

  Note
  Do not choose a binary certificate (PKCS12, DER, and alike) file because threat defense does not support them.

  To remove the uploaded certificate, check the **Clear loaded certificate** check box. This option only appears when you have uploaded a certificate, and when you are in the Edit mode of the external authentication object.

  If you had previously uploaded a certificate and want to replace it, reupload the new certificate (complete CA chain), and redeploy the configuration to your devices to copy over the new certificate.

  Note
  TLS encryption requires a certificate on all platforms. We recommend that you *always* upload a certificate for SSL to prevent man-in-the-middle attacks.

- **User Name Template**—Provide a template that corresponds with your **UI Access Attribute**. For example, to authenticate all users who work in the Security organization of the Example company by connecting to an OpenLDAP server where the UI access attribute is `uid`, you might enter

uid=%s,ou=security,dc=example,dc=com in the **User Name Template** field. For a Microsoft Active Directory server, you could enter %s@security.example.com.

This field is required for CAC authentication.

- **Shell User Name Template**—Provide a template that corresponds with your **CLI Access Attribute** to authenticate CLI users. For example, to authenticate all users who work in the Security organization by connecting to an OpenLDAP server where the CLI access attribute is sAMAccountName, you might enter %s in the **Shell User Name Template** field.

- **Timeout (Seconds)**—Enter the number of seconds before rolling over to the backup connection, between 1 and 1024. The default is 30.

  Note
  The timeout range is different for threat defense and the management center, so if you share an object, be sure not to exceed the threat defense's smaller timeout range (1-30 seconds). If you set the timeout to a higher value, the threat defense LDAP configuration will not work.

Step 12 Configure **Attribute Mapping** to retrieve users based on an attribute.

- Enter a **UI Access Attribute**, or click **Fetch Attrs** to retrieve a list of available attributes. For example, on a Microsoft Active Directory Server, you may want to use the UI access attribute to retrieve users, because there may not be a uid attribute on Active Directory Server user objects. Instead, you can search the userPrincipalName attribute by typing userPrincipalName in the **UI Access Attribute** field.

  This field is required for CAC authentication.

- Set the **CLI Access Attribute** if you want to use a shell access attribute other than the user distinguished type. For example, on a Microsoft Active Directory Server, use the sAMAccountName CLI access attribute to retrieve CLI access users by typing sAMAccountName.

Step 13 (Optional) Configure **Group Controlled Access Roles**.

If you do not configure a user's privileges using group-controlled access roles, a user has only the privileges granted by default in the external authentication policy.

a) (Optional) In the fields that correspond to user roles, enter the distinguished name for the LDAP groups that contain users who should be assigned to those roles.

Any group you reference must exist on the LDAP server. You can reference static LDAP groups or dynamic LDAP groups. Static LDAP groups are groups where membership is determined by group object attributes that point to specific users, and dynamic LDAP groups are groups where membership is determined by creating an LDAP search that retrieves group users based on user object attributes. Group access rights for a role only affect users who are members of the group.

If you use a dynamic group, the LDAP query is used exactly as it is configured on the LDAP server. For this reason, the device limits the number of recursions of a search to 4 to prevent search syntax errors from causing infinite loops.

Example:

Enter the following in the **Administrator** field to authenticate names in the information technology organization at the Example company:

cn=itgroup,ou=groups, dc=example,dc=com

b) Choose a **Default User Role** for users that do not belong to any of the specified groups.

c) If you use static groups, enter a **Group Member Attribute**.

Example:

If the `member` attribute is used to indicate membership in the static group for default Security Analyst access, enter `member`.

d) If you use dynamic groups, enter a **Group Member URL Attribute**.

Example:

If the `memberURL` attribute contains the LDAP search that retrieves members for the dynamic group you specified for default Admin access, enter `memberURL`.

If you change a user's role, you must save/deploy the changed external authentication object and also remove the user from the **Users** screen. The user will be re-added automatically the next time they log in.

Step 14 (Optional) Set the **CLI Access Filter** to allow CLI users.

To prevent LDAP authentication of CLI access, leave this field blank. To specify CLI users, choose one of the following methods:

- To use the same filter you specified when configuring authentication settings, check the check box of **Same as Base Filter**.

- To retrieve administrative user entries based on attribute value, enter the attribute name, a comparison operator, and the attribute value you want to use as a filter, enclosed in parentheses. For example, if all network administrators have a `manager` attribute which has an attribute value of `shell`, you can set a base filter of `(manager=shell)`.

The usernames must be Linux-valid:

- Maximum 32 alphanumeric characters, plus period (.), hyphen (-), and underscore (_)

- All lowercase

- Cannot start with hyphen (-); cannot be all numbers; cannot include at sign (@) or slash (/)

Note
Users with CLI access can gain Linux shell access with the **expert** command. Linux shell users can obtain root privileges, which can present a security risk. Make sure that you restrict the list of users with CLI or Linux shell access.

Note
Do not create any internal users that have the same user name as users included in the **CLI Access Filter**. The only internal management center user should be **admin**; do not include an **admin** user in the **CLI Access Filter**.

Step 15 (Optional) Click **Test** to test connectivity to the LDAP server.

The test output lists valid and invalid user names. Valid user names are unique, and can include underscores (_), periods (.), hyphens (-), and alphanumeric characters. Note that testing the connection to servers with more than 1000 users only returns 1000 users because of UI page size limitations. If the test fails, see

Step 16   (Optional) You can also enter **Additional Test Parameters** to test user credentials for a user who should be able to authenticate: enter a **User Name** uid and **Password**, and then click **Test**.

If you are connecting to a Microsoft Active Directory Server and supplied a UI access attribute in place of uid, use the value for that attribute as the user name. You can also specify a fully qualified distinguished name for the user.

Tip
If you mistype the name or password of the test user, the test fails even if the server configuration is correct. To verify that the server configuration is correct, click **Test** without entering user information in the **Additional Test Parameters** field first. If that succeeds, supply a user name and password to test with the specific user.

Example:

To test if you can retrieve the JSmith user credentials at the Example company, enter JSmith and the correct password.

Step 17   Click **Save**.

Step 18   Enable use of this server. See .

Examples

Basic Example

The following figures illustrate a basic configuration of an LDAP login authentication object for a Microsoft Active Directory Server. The LDAP server in this example has an IP address of 10.11.3.4. The connection uses port 389 for access.

This example shows a connection using a base distinguished name of
OU=security, DC=it, DC=example, DC=com for the security organization in the information technology
domain of the Example company.

However, because this server is a Microsoft Active Directory server, it uses the `sAMAccountName` attribute to store user names rather than the `uid` attribute. Choosing the MS Active Directory server type and clicking **Set Defaults** sets the UI Access Attribute to `sAMAccountName`. As a result, the system checks the `sAMAccountName` attribute for each object for matching user names when a user attempts to log into the system.

In addition, a **CLI Access Attribute** of `sAMAccountName` causes each `sAMAccountName` attribute to be checked for all objects in the directory for matches when a user logs into a CLI account on the appliance.

Note that because no base filter is applied to this server, the system checks attributes for all objects in the directory indicated by the base distinguished name. Connections to the server time out after the default time period (or the timeout period set on the LDAP server).

Advanced Example

This example illustrates an advanced configuration of an LDAP login authentication object for a Microsoft Active Directory Server. The LDAP server in this example has an IP address of 10.11.3.4. The connection uses port 636 for access.

This example shows a connection using a base distinguished name of `OU=security,DC=it,DC=example,DC=com` for the security organization in the information technology domain of the Example company. However, note that this server has a base filter of `(cn=*smith)`. The filter restricts the users retrieved from the server to those with a common name ending in `smith`.

LDAP-Specific Parameters

Base DN *	OU=security,DC=it,DC=example,D(	Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter	(cn=*smith)		ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(|(cn=bsmith)(cn=csmith*)))
User Name *	CN=Admin,DC=example,DC=com		ex. cn=jsmith,dc=sourcefire,dc=com
Password *	•••••		
Confirm Password *	•••••		
▼Show Advanced Options			
Encryption	● SSL ○ TLS ○ None		
SSL Certificate Upload Path	Choose File certificate.pem		ex. PEM Format (base64 encoded version of DER)
User Name Template	%s		ex. cn=%s,dc=sourcefire,dc=com
Shell User Name Template	%s		ex. %s
Timeout (Seconds)	60		

Attribute Mapping

UI Access Attribute *	sAMAccountName	Fetch Attrs
CLI Access Attribute *	sAMAccountName	

The connection to the server is encrypted using SSL and a certificate named `certificate.pem` is used for the connection. In addition, connections to the server time out after 60 seconds because of the **Timeout (Seconds)** setting.

Because this server is a Microsoft Active Directory server, it uses the `sAMAccountName` attribute to store user names rather than the `uid` attribute. Note that the configuration includes a **UI Access Attribute** of `sAMAccountName`. As a result, the system checks the `sAMAccountName` attribute for each object for matching user names when a user attempts to log into the system.

In addition, a **CLI Access Attribute** of `sAMAccountName` causes each `sAMAccountName` attribute to be checked for all objects in the directory for matches when a user logs into a CLI account on the appliance.

This example also has group settings in place. The Maintenance User role is automatically assigned to all members of the group with a `member` group attribute and the base domain name of `CN=SFmaintenance,DC=it,DC=example,DC=com`.

The **CLI Access Filter** is set to be the same as the base filter, so the same users can access the appliance through the CLI as through the web interface.

Add a RADIUS External Authentication Object for Management Center

Add a RADIUS server to support external users for device management.

In a multidomain deployment, external authentication objects are only available in the domain in which they are created.

Procedure

Step 1   Choose **System** (⚙) > **Users**.

Step 2   Click **External Authentication**.

Step 3   Click **Add icon** (➕) **Add External Authentication Object**.

Step 4   Set the **Authentication Method** to **RADIUS**.

Step 5   Enter a **Name** and optional **Description**.

Step 6   Check the **RADIUS Server-Enabled Message Authenticator** check box to require the Message-Authenticator attribute in all RADIUS responses, ensuring that every response from the RADIUS server is securely verified by the Threat Defense.

This feature is enabled by default for new RADIUS servers. We recommend you enable it for existing servers after the upgrade. Disabling message authenticators may expose your firewalls to potential attacks. Ensure that your RADIUS server has the Message-Authenticator configuration.

Step 7   For the **Primary Server**, enter a **Host Name/IP Address**.

Step 8   (Optional) Change the **Port** from the default.

Step 9   Enter the **RADIUS Secret Key**.

Step 10   (Optional) Enter the **Backup Server** parameters.

Step 11   (Optional) Enter **RADIUS-Specific Parameters**.

     a) Enter the **Timeout** in seconds before retrying the primary server, between 1 and 1024. The default is 30.

       Note
The timeout range is different for the threat defense and the management center, so if you share an object, be sure not to exceed the threat defense's smaller timeout range (1-300 seconds). If you set the timeout to a higher value, the threat defense RADIUS configuration will not work.

     b) Enter the **Retries** before rolling over to the backup server. The default is 3.

     c) In the fields that correspond to user roles, enter the name of each user or identifying attribute-value pair that should be assigned to those roles.

Separate usernames and attribute-value pairs with commas.

Example:

If you know all users who should be Security Analysts have the value `Analyst` for their `User-Category` attribute, you can enter `User-Category=Analyst` in the **Security Analyst** field to grant that role to those users.

Example:

To grant the Administrator role to the users `jsmith` and `jdoe`, enter `jsmith, jdoe` in the **Administrator** field.

Example:

To grant the Maintenance User role to all users with a `User-Category` value of `Maintenance`, enter `User-Category=Maintenance` in the **Maintenance User** field.

     d) Select the **Default User Role** for users that do not belong to any of the specified groups.

If you change a user's role, you must save/deploy the changed external authentication object and also remove the user from the **Users** screen. The user will be re-added automatically the next time they log in.

Step 12   (Optional) **Define Custom RADIUS Attributes**.

If your RADIUS server returns values for attributes not included in the `dictionary` file in `/etc/radiusclient/`, and you plan to use those attributes to set roles for users with those attributes, you need to define those attributes. You can locate the attributes returned for a user by looking at the user's profile on your RADIUS server.

a)   Enter an **Attribute Name**.

When you define an attribute, you provide the name of the attribute, which consists of alphanumeric characters. Note that words in an attribute name should be separated by dashes rather than spaces.

b)   Enter the **Attribute ID** as an integer.

The attribute ID should be an integer and should not conflict with any existing attribute IDs in the `etc/radiusclient/dictionary` file.

c)   Choose the **Attribute Type** from the drop-down list.

You also specify the type of attribute: string, IP address, integer, or date.

d)   Click **Add** to add the custom attribute.

When you create a RADIUS authentication object, a new dictionary file for that object is created on the device in the `/var/sf/userauth` directory. Any custom attributes you add are added to the dictionary file.

Example:

If a RADIUS server is used on a network with a Cisco router, you might want to use the `Ascend-Assign-IP-Pool` attribute to grant a specific role to all users logging in from a specific IP address pool. `Ascend-Assign-IP-Pool` is an integer attribute that defines the address pool where the user is allowed to log in, with the integer indicating the number of the assigned IP address pool.

To declare that custom attribute, you create a custom attribute with an attribute name of `Ascend-IP-Pool-Definition`, an attribute ID of `218`, and an attribute type of `integer`.

You could then enter `Ascend-Assign-IP-Pool=2` in the **Security Analyst (Read Only)** field to grant read-only security analyst rights to all users with an `Ascend-IP-Pool-Definition` attribute value of `2`.

Step 13   (Optional) In the **CLI Access Filter** area **Administrator CLI Access User List** field, enter the user names that should have CLI access, separated by commas.

Make sure that these usernames match usernames on the RADIUS server. The names must be Linux-valid usernames:

   • Maximum 32 alphanumeric characters, plus period (.), hyphen (-), and underscore (_)

   • All lowercase

   • Cannot start with hyphen (-); cannot be all numbers; cannot include at sign (@) or slash (/)

To prevent RADIUS authentication of CLI access, leave the field blank.

Note
Users with CLI access can gain Linux shell access with the **expert** command. Linux shell users can obtain root privileges, which can present a security risk. Make sure that you restrict the list of users with CLI or Linux shell access.

Note

Remove any internal users that have the same user name as users included in the shell access filter. For the management center, the only internal CLI user is **admin**, so do not also create an **admin** external user.

Step 14   (Optional) Click **Test** to test management center connectivity to the RADIUS server.

Step 15   (Optional) You can also enter **Additional Test Parameters** to test user credentials for a user who should be able to authenticate: enter a **User Name** and **Password**, and then click **Test**.

Tip

If you mistype the name or password of the test user, the test fails even if the server configuration is correct. To verify that the server configuration is correct, click **Test** without entering user information in the **Additional Test Parameters** field first. If that succeeds, supply a user name and password to test with the specific user.

Example:

To test if you can retrieve the JSmith user credentials at the Example company, enter JSmith and the correct password.

Step 16   Click **Save**.

Step 17   Enable use of this server. See .

Examples

Simple User Role Assignments

The following figure illustrates a sample RADIUS login authentication object for a server running Cisco Identity Services Engine (ISE) with an IP address of 10.10.10.98 on port 1812. No backup server is defined.

The following example shows RADIUS-specific parameters, including the timeout (30 seconds) and number of failed retries before the Secure Firewall System attempts to contact the backup server, if any.

This example illustrates important aspects of RADIUS user role configuration:

Users ewharton and gsand are granted web interface Administrative access.

The user `cbronte` is granted web interface Maintenance User access.

The user `jausten` is granted web interface Security Analyst access.

The user `ewharton` can log into the device using a CLI account.

The following graphic depicts the role configuration for the example:

Roles for Users Matching an Attribute-Value Pair

You can use an attribute-value pair to identify users who should receive a particular user role. If the attribute you use is a custom attribute, you must define the custom attribute.

The following figure illustrates the role configuration and custom attribute definition in a sample RADIUS login authentication object for the same ISE server as in the previous example.

In this example, however, the `MS-RAS-Version` custom attribute is returned for one or more of the users because a Microsoft remote access server is in use. Note the `MS-RAS-Version` custom attribute is a string. In this example, all users logging in to RADIUS through a Microsoft v. 5.00 remote access server should receive the Security Analyst (Read Only) role, so you enter the attribute-value pair of `MS-RAS-Version=MSRASV5.00` in the **Security Analyst (Read Only)** field.

Enable External Authentication for Users on the Management Center

When you enable external authentication for management users, the management center verifies the user credentials with an LDAP or RADIUS server as specified in an External Authentication object.

Before you begin

Add one or more external authentication objects according to Add an LDAP External Authentication Object for the Management Center, on page 13 and Add a RADIUS External Authentication Object for Management Center, on page 21.

Procedure

Step 1	Choose **System** (⚙) > **Users**.
Step 2	Click **External Authentication**.
Step 3	Set the default user role for external web interface users.

Users without a role cannot perform any actions. Any user roles defined in the external authentication object overrides this default user role.

a) Click the **Default User Role** value (by default, none selected).

a) In the **Default User Role Configuration** dialog box, check the role(s) that you want to use.

b) Click **Save**.

Step 4	Click the **Slider enabled** (⬤) next to the each external authentication object that you want to use. If you enable more than 1 object, then users are compared against servers in the order specified. See the next step to reorder servers.

If you enable shell authentication, you must enable an external authentication object that includes a **CLI Access Filter**. Also, CLI access users can only authenticate against the server whose authentication object is highest in the list.

Step 5   (Optional) Drag and drop servers to change the order in which authentication they are accessed when an authentication request occurs.

Step 6   Choose **Shell Authentication** > **Enabled** if you want to allow CLI access for external users.

> **Note**
> The multidomain feature is not supported in CLI. Hence, the **Shell Authentication** option is available only in Global domain and not in Sub domains.
>
> The first external authentication object name is shown next to the **Enabled** option to remind you that only the first object is used for CLI.

Step 7   Click **Save and Apply**.

Configure Common Access Card Authentication with LDAP

If your organization uses Common Access Cards (CACs), you can configure LDAP authentication to authenticate management center users logging in to the web interface. With CAC authentication, users have the option to log in directly without providing a separate username and password for the device.

CAC-authenticated users are identified by their electronic data interchange personal identifier (EDIPI) numbers.

After 24 hours of inactivity, the device deletes CAC-authenticated users from the **Users** tab. The users are re-added after each subsequent login, but you must reconfigure any manual changes to their user roles.

⚠ **Caution**   When configuring CAC authentication with LDAP, ensure that you follow the principles of least privilege while assigning a default access role to the users. When a user first logs in to the system with their CAC credentials, their account will be assigned this default access role.

If you do not follow the principles of least privilege while assigning the default access role, users may be assigned an unintended privilege level on subsequent logins. This could result in the users having privileges beyond their required access role.

If a user who has logged in with the default access role needs a temporary elevation of their privileges, a user with administrative privileges can temporarily provide that user the required higher level of access by assigning them a role with higher privilege. This privilege will be revoked after 24 hours of inactivity, and the user will return to their default access role.

If a user needs a permanent access role reassignment to a higher privilege level, such as System Admin, use the **Group Controlled Access Roles** method to provide admin access to the user. This method ensures that the provided access role persists beyond 24 hours and users will have the correct privilege level as per the group assignment. For more information on configuring Group Controlled Access Roles, see the Add an LDAP External Authentication Object for Management Center section.

Before you begin

You must have a valid user certificate present in your browser (in this case, a certificate passed to your browser via your CAC) to enable user certificates as part of the CAC configuration process. After you configure CAC

authentication and authorization, users on your network must maintain the CAC connection for the duration of their browsing session. If you remove or replace a CAC during a session, your web browser terminates the session and the system logs you out of the web interface.

Procedure

Step 1 Insert a CAC as directed by your organization.

Step 2 Direct your browser to **https://***ipaddress_or_hostname*/, where *ipaddress* or *hostname* corresponds to your device.

Step 3 If prompted, enter the PIN associated with the CAC you inserted in step 1.

Step 4 If prompted, choose the appropriate certificate from the drop-down list.

Step 5 On the Login page, in the **Username** and **Password** fields, log in as a user with Administrator privileges. You **cannot** yet log in using your CAC credentials.

Step 6 Choose **System** > **Users** > **External Authentication**.

Step 7 Create an LDAP authentication object exclusively for CAC, following the procedure in Add an LDAP External Authentication Object for the Management Center, on page 13. You must configure the following:

- **CAC** check box.

- **LDAP-Specific Parameters** > **Show Advanced Options** > **User Name Template**.

- **Attribute Mapping** > **UI Access Attribute**.

Step 8 Click **Save**.

Step 9 Enable external authentication and CAC authentication as described in Enable External Authentication for Users on the Management Center, on page 26.

Step 10 Choose **System** (⚙) > **Configuration**, and click **HTTPS Certificate**.

Step 11 Import a HTTPS server certificate, if necessary, following the procedure outlined in Importing HTTPS Server Certificates.

The same certificate authority (CA) must issue the HTTPS server certificate and the user certificates on the CACs you plan to use.

Step 12 Under **HTTPS Client Certificate Settings**, choose **Enable Client Certificates**. For more information, see Requiring Valid HTTPS Client Certificates.

Step 13 Log in to the device according to Logging Into the Secure Firewall Management Center with CAC Credentials.

Configure SAML Single Sign-On

You can configure your management center to use Single Sign-On, a system by which a central identity provider (IdP) provides authentication and authorization for users logging into the management center as well as other applications within an organization. The applications configured to take part in such an SSO arrangement are said to be federated service provider applications. SSO users can log in once to gain access to all service provider applications that are members of the same federation.

About SAML Single Sign-On

A management center configured for SSO presents a link for single sign-on on the Login page. Users configured for SSO access click on this link and are redirected to the IdP for authentication and authorization, rather than supplying a username and password on the management center Login page. Once successfully authenticated by the IdP, SSO users are redirected back to the management center web interface and logged in. All the communication between the management center and the IdP to accomplish this takes place using the browser as an intermediary; as a result, the management center does not require a network connection to directly access the identity provider.

The management center supports SSO using any SSO provider conforming to the Security Assertion Markup Language (SAML) 2.0 open standard for authentication and authorization.

Note   The management center cannot sign SAML authentication request messages. Hence, if the IdP requires service provider's signature on the authentication requests, the SSO on the management center would fail.

The management center web interface offers configuration options for the following SSO providers:

- Okta

- OneLogin

- Azure

- PingID's PingOne for Customers cloud solution

- Other

Note   The Cisco Secure Sign On SSO product does not recognize the management center as a pre-integrated service provider.

SSO Guidelines for the Management Center

Keep the following in mind when you configure a management center to be a member of an SSO federation:

- The management center can support SSO with only one SSO provider at a time—you cannot configure the management center to use, for instance, both Okta and OneLogin for SSO.

- Management Center management centers in a high availability configuration can support SSO, but you must keep the following considerations in mind:

  - SSO configuration is not synchronized between the members of the high availability pair; you must configure SSO separately on each member of the pair.

  - Both management centers in a high availability pair must use the same IdP for SSO. You must configure a service provider application at the IdP for each management center configured for SSO.

  - In a high availability pair of management centers where both are configured to support SSO, before a user can use SSO to access the secondary management center for the first time, that user must first use SSO to log into the primary management center at least once.

  - When configuring SSO for management centers in a high availability pair:

      • If you configure SSO on the primary management center, you are not required to configure SSO on the secondary management center.

      • If you configure SSO on the secondary management center, you are required to configure SSO on the primary management center as well. (This is because SSO users must login into the primary management center at least once before logging into the secondary management center.)

• In a management center that uses multi-tenancy, the SSO configuration can be applied only at the global domain level, and applies to the global domain and all subdomains.

• Only users with the Admin role authenticated internally or by LDAP or RADIUS can configure SSO.

• The management center does not support SSO initiated from the IdP.

• The management center does not support logging in with CAC credentials for SSO accounts.

• Do not configure SSO in deployments using CC mode.

• SSO activities are logged in the management center audit log with Login or Logout specified in the Subsystem field.

Related Topics

High Availability

Domains

Logging Into the Secure Firewall Management Center with CAC Credentials

Security Certifications Compliance

Audit Records

SSO User Accounts

Identity providers can support user and group configuration directly, or they often can import users and groups from other user management applications such as Active Directory, RADIUS, or LDAP. This documentation focuses on configuring the management center to work with the IdP to support SSO assuming that IdP users and groups are already established; to configure an IdP to support users and groups from other user management applications, consult the IdP vendor documentation.

Most account characteristics for SSO users, including the user name and password, are established at the IdP. SSO accounts do not appear on the management center web interface Users page until those accounts log in the first time.

Note The system requires that user names for SSO accounts as well as the NameID attribute the IdP sends to the management center during the SAML login process must be both be valid email addresses. Many IdP's automatically use the username of the user trying to logon as the NameID attribute, but you should confirm this is the case for your IdP. Keep this in mind when configuring a service provider application at your IdP and creating IdP user accounts that are to be granted SSO access to the management center.

The following account characteristics for SSO users can be configured from the management center web interface under **System** (⚙) > **Users** > **Edit User**:

• Real Name

• Exempt from Browser Session Timeout

User Role Mapping for SSO Users

By default, all the users who are given SSO access to a management center are assigned the Security Analyst (Read Only) role. You can change this default, as well as override it for specific SSO users or groups using user role mapping. After you have established and successfully tested the management center SSO configuration, you can configure user role mapping.

User role mapping requires coordinating configuration settings at the management center with settings at the SSO IdP application. User roles can be assigned to users or to groups defined at the IdP application. Users may or may not be members of groups, and user or group definitions may or may not be imported to the IdP from other user management systems within your organization, such as Active Directory. For this reason, to effectively configure management center SSO user role mapping you must be familiar with how your SSO federation is organized and how users, groups and their roles are assigned at the SSO IdP application. This documentation focuses on configuring the management center to work with the IdP to support user role mapping; to create users or groups within the IdP, or import users or groups into the IdP from a user management application, consult the IdP vendor documentation.

In user role mapping, the IdP maintains a role attribute for the management center service provider application, and each user or group with access to that management center is configured with a string or expression for the role attribute. Requirements for the attribute value are different for each IdP. At the management center, the name of the role attribute, a list of expressions assigned to a list of management center user roles are part of the SSO configuration. When a user logs into the management center using SSO, the management center compares the value of the role attribute for that user (or that user's group, depending upon configuration) against the expressions for each management center user role. The management center assigns the user all the roles where the expression matches the attribute value the user has provided.

Note You can configure management center roles to be mapped based on individual user permissions or based on group permissions, but a single management center application cannot support role mapping for both groups and individual users.

Enable Single Sign-On at the Management Center

Before you begin

- At the SAML SSO management application, configure a service provider application for the management center and assign users or groups to the service provider application:

    - To configure a management center service provider application for Okta, see Configure the Management Center Service Provider Application for Okta, on page 34.

    - To configure a management center service provider application for OneLogin, see Configure the Management Center Service Provider Application for OneLogin, on page 46.

    - To configure a management center service provider application for Azure, see Configure the Management Center Service Provider Application for Azure, on page 59.

    - To configure a management center service provider application for PingID's PingOne for Customers cloud solution, see Configure the Management Center Service Provider Application for PingID PingOne for Customers, on page 72.

• To configure a management center service provider application for any SAML 2.0-compliant SSO provider, see Configure Management Center Service Provider Application for Any SAML 2.0-Compliant SSO Provider, on page 76.

Procedure

Step 1	Choose **System** (⚙) > **Users** > **Single Sign-On**.
Step 2	Click the **Single Sign-On (SSO) Configuration** slider to enable SSO.
Step 3	Click the **Configure SSO** button.
Step 4	At the **Select Firewall Management Center SAML Provider** dialog box, click the radio button for the SSO IdP of your choice and click **Next**.

What to do next

Proceed with the instructions appropriate to your choice of SSO provider:

• Configure the management center for Okta SSO; see Configure the Management Center for Okta SSO, on page 35.

• Configure the management center for SSO using PingID's PingOne for Customers cloud solution; see Configure the Management Center for SSO with the PingID PingOne for Customers, on page 74.

• Configure the management center for Azure SSO; see Configure the Management Center for Azure SSO, on page 61.

• Configure the management center for OneLogin SSO; see Configure the Management Center for OneLogin SSO, on page 48.

• Configure the management center for SSO using any SAML 2.0-compliant provider; see Configure the Management Center for SSO Using Any SAML 2.0-Compliant SSO Provider, on page 78.

Configure Single Sign-On with Okta

See the following tasks to configure SSO using Okta:
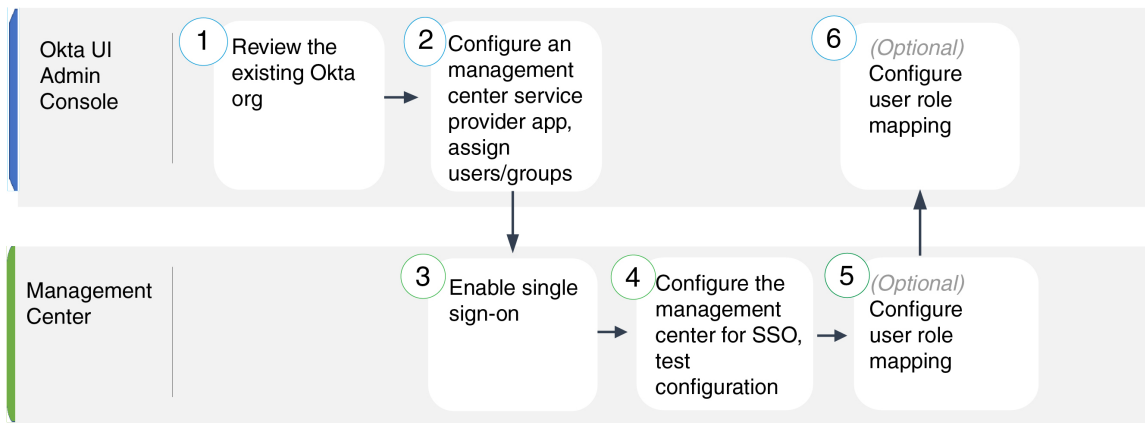
	Okta UI Admin Console	Review the Okta Org, on page 33
2	Okta UI Admin Console	Configure the Management Center Service Provider Application for Okta, on page 34
3	management center	Enable Single Sign-On at the Management Center, on page 31
4	management center	Configure the Management Center for Okta SSO, on page 35
5	management center	Configure User Role Mapping for Okta in the Management Center, on page 36
6	Okta UI Admin Console	Configure User Role Mapping at the Okta IdP, on page 37

Review the Okta Org

In Okta, the entity that encompasses all the federated devices and applications that a user can access with the same SSO account is called an *org*. Before adding the management center to an Okta org, be familiar with its configuration; consider the following questions:

- How many users will have access to the management center?

- Are users within the Okta org members of groups?

- Are user and group definitions native to Okta or imported from a user management application such as Active Directory, RADIUS, or LDAP?

- Do you need to add more users or groups to the Okta org to support SSO on the management center?

- What kind of user role assignments do you want to make? (If you choose not to assign user roles, the management center automatically assigns a configurable default user role to all SSO users.)

- How must users and groups within the Okta org be organized to support the required user role mapping?

Keep in mind that you can configure management center roles to be mapped based on individual user permissions or based on group permissions, but a single management center application cannot support role mapping for both groups and individual users.

This documentation assumes you are already familiar with the Okta Classic UI Admin Console, and have an account that can perform configuration functions requiring Super Admin permissions. If you need more information, see Okta's documentation available online.

Configure the Management Center Service Provider Application for Okta

Use these instructions at the Okta Classic UI Admin Console to create a management center service provider application within Okta and assign users or groups to that application. You should be familiar with SAML SSO concepts and the Okta admin console. This documentation does not describe all the Okta functions you need to establish a fully functional SSO org; for instance, to create users and groups, or to import user and group definitions from another user management application, see the Okta documentation.

Note   If you plan to assign user groups to the management center application, do not also assign users within those groups as individuals.

Note   The management center cannot support role mapping using multiple SSO attributes; you must select either user role mapping or group role mapping and configure a single attribute to convey user role information from OneLogin to the management center.

Before you begin

- Familiarize yourself with the SSO federation and its user and groups; see .

- Create user accounts and/or groups in your Okta org if necessary.

Note   The system requires that user names for SSO accounts as well as the NameID attribute the IdP sends to the management center during the SAML login process must be both be valid email addresses. Many IdP's automatically use the username of the user trying to logon as the NameID attribute, but you should confirm this is the case for your IdP. Keep this in mind when configuring a service provider application at your IdP and creating IdP user accounts that are to be granted SSO access to the management center.

- Confirm the login URL for the target management center (`https://ipaddress_or_hostname`).

Note   If your management center web interface can be reached with multiple URLs (for instance, a fully-qualified domain name as well as an IP address), SSO users must consistently access the management center using the login URL that you configure in this task.

Procedure

Step 1 From the Okta Classic UI Admin Console, create a service provider application for the management center. Configure the management center application with the following selections:

- Select `Web` for the **Platform**.

- Select `SAML 2.0` for the **Sign on method**.

- Provide a **Single sign on URL**.

  This is the management center URL to which the browser sends information on behalf of the IdP.

  Append the string `saml/acs` to the management center login URL. For example: `https://ExampleFMC/saml/acs`.

- Enable **Use this for Recipient URL and Destination URL**.

- Enter an **Audience URI (SP Entity ID)**.

  This is a globally unique name for the service provider (the management center), often formatted as a URL.

  Append the string `/saml/metadata` to the management center login URL. For example: `https://ExampleFMC/saml/metadata`.

- For **Name ID Format** choose `Unspecified`.

Step 2 (Optional if you are assigning groups to the application.) Assign individual Okta users to the management center application. (If you plan to assign groups to the management center application, do not assign users that are members of those groups as individuals.)

Step 3 (Optional if you are assigning individual users to the application.) Assign Okta groups to the management center application.

Step 4 (Optional) To make SSO setup at the management center easier, you can download the SAML XML metadata file for the management center service provider application from Okta to your local computer.

What to do next

Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Configure the Management Center for Okta SSO

Use these instructions at the management center web interface.

Before you begin

- Create a management center service provider application at the Okta Classic UI Admin Console; see Configure the Management Center Service Provider Application for Okta, on page 34.

- Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Procedure

Step 1 (This step continues directly from Enable Single Sign-On at the Management Center, on page 31.) At the **Configure Okta Metadata** dialog box, you have two choices:

- To enter the SSO configuration information manually:

  a. Click the **Manual Configuration** radio button.

  b. Enter the following values from the Okta SSO Service Provider application. (Retrieve these values from the Okta Classic UI Admin Console.)

    - **Identity Provider Single Sign-On (SSO) URL**

    - **Identity Provider Issuer**

    - **X.509 Certificate**

- If you saved the XML metadata file generated by Okta to your local computer (Step 4 in Configure the Management Center Service Provider Application for Okta, on page 34), you can upload the file to the management center:

  a. Click the **Upload XML File** radio button.

  b. Follow the on-screen instructions to navigate to and choose the XML metadata file on your local computer.

Step 2 Click **Next**.

Step 3 At the **Verify Metadata** dialog, review the configuration parameters and click **Save**.

Step 4 Click **Test Configuration**. If the system displays an error message, review the SSO configuration for the management center as well as the Okta service provider application configuration, correct any errors, and try again.

Step 5 When the system reports a successful configuration test, click **Apply**.

What to do next

You may optionally configure user role mapping for SSO users; see Configure User Role Mapping for Okta in the Management Center, on page 36. If you choose not to configure role mapping, by default all SSO users that log into the management center are assigned the user role you configure in Step 4 of Configure User Role Mapping for Okta in the Management Center, on page 36.

Configure User Role Mapping for Okta in the Management Center

The fields to configure for user role mapping in the management center web interface are the same regardless of your choice of SSO provider. However, the values you configure must take into account how the SAML SSO provider you use implements user role mapping.

Before you begin

- Review the Okta user group mapping information; see Review the Okta Org, on page 33.

- Configure the management center as an SSO service provider application; see Configure the Management Center Service Provider Application for Okta, on page 34.

- Enable and configure single sign-on at the management center; see Enable Single Sign-On at the Management Center, on page 31, and Configure the Management Center for Okta SSO, on page 35.

Procedure

Step 1	Choose **System** (⚙) > **Users** > **Single Sign-On**.
Step 2	Expand **Advanced Configuration (Role Mapping)**.
Step 3	From the **Default User Role** drop-down list, choose a default management center user role to assign users.
Step 4	In the **Group Member Attribute** field, enter an attribute configured in Okta for management center user role mapping for users or groups. (See Step 1 of Configure a User Attribute for Role Mapping at the Okta IdP, on page 38 or Step 1 of Configure a Group Attribute for Role Mapping at the Okta IdP, on page 39.)
Step 5	Next to each management center user role you wish to assign to SSO users, enter a regular expression. (The management center uses a restricted version of Google's RE2 regular expression standard supported by Golang and Perl.) The management center compares these values against the user role mapping attribute value the IdP sends to the management center with SSO user information. The management center grants users a union of all the roles for which a match is found.
Step 6	Click **Test Configuration**. If the system displays an error message, review the SSO configuration for the management center as well as the identity service provider application configuration, correct any errors, and try again.
Step 7	When the system reports a successful configuration test, click **Apply**.

What to do next

Configure user role mapping at the service provider application; see Configure User Role Mapping at the Okta IdP, on page 37.

Configure User Role Mapping at the Okta IdP

You can configure SSO user role mapping at the Okta Classic UI Admin Console based on individual user permissions or group permissions.

- To map based on individual user permissions, see Configure a User Attribute for Role Mapping at the Okta IdP, on page 38.

- To map based on group permissions, see Configure a Group Attribute for Role Mapping at the Okta IdP, on page 39.

When an SSO user logs in to the management center, Okta presents a user or group role attribute value configured at the Okta IdP, to the management center. The management center then compares that attribute value with the regular expressions assigned to each management center user role in the SSO configuration, and grants the user all the roles for which a match is found.. (If no match is found, the management center

grants the user a configurable default user role.) The expression you assign to each management center user role must comply with the restricted version of Google's RE2 regular expression standard supported by Golang and Perl. The management center treats the attribute value received from Okta as a regular expression using that same standard for purposes of comparison with the management center user role expressions.

Note A single management center cannot support role mapping for both groups and individual users; you must choose one mapping method for the management center service provider application and use it consistently. Furthermore, the management center can support group role mapping using only one group attribute statement per management center service provider application configured in Okta. Generally group-based role mapping is more efficient for a management center with many users. You should take into account user and group definitions established throughout your Okta org.

Configure a User Attribute for Role Mapping at the Okta IdP

Use these instructions at the Okta Classic UI Admin Console to add a custom role mapping attribute to the Okta default user profile.

Okta service provider applications may use one of two types of user profiles:

- Okta user profiles, which can be extended with any custom attribute.

- App user profiles, which can be extended only with attributes from a predefined list that Okta generates by querying a third-party application or directory (such as Active directory, LDAP, or Radius) for supported attributes.

You may use either type of user profile in your Okta org; consult Okta documentation for information on how to configure them. Whichever type of user profile you use, to support user role mapping with the management center you must configure a custom attribute in the profile to convey each user's role mapping expression to the management center.

This documentation describes role mapping using Okta user profiles; mapping with App profiles requires familiarity with the third-party user management application in use at your organization to set up custom attributes. See the Okta documentation for details.

Before you begin

- Configure a management center service provider application at the Okta IdP as described in Configure the Management Center Service Provider Application for Okta, on page 34.

- Configure SSO user role mapping at the management center as described in Configure User Role Mapping for Okta in the Management Center, on page 36.

Procedure

Step 1 Add a new attribute to the default Okta user profile:

- For **Data type** choose `string`.

- Provide the **Variable name** the Okta IdP will send to the management center, containing an expression to match for user role mapping. This variable name must match the string you entered at the management

center SSO configuration for **Group Member Attribute**. (See Step 5 in Configure User Role Mapping for Okta in the Management Center, on page 36.)

Step 2 For each user assigned to the management center service provider application using this profile, assign a value to the user role attribute you have just created.

Use an expression to represent the role or roles the management center will assign to the user. The management center compares this string against the expressions you assigned to each management center user role in Step 6 of Configure User Role Mapping for Okta in the Management Center, on page 36. (For purposes of comparison with the management center user role expressions, the management center treats the attribute value received from Okta as an expression complying with the restricted version of Google's RE2 regular expression standard supported by Golang and Perl.)

Configure a Group Attribute for Role Mapping at the Okta IdP

Use these instructions at the Okta Admin Console to add a custom role mapping group attribute to the management center service provider application. The management center can support group role mapping using only one group attribute statement per Okta management center service provider application.

Okta service provider applications may use one of two types of groups:

- Okta groups, which can be extended with any custom attribute.

- Application groups, which can be extended only with attributes from a predefined list that Okta generates by querying a third-party application or directory (such as Active directory, LDAP, or Radius) for supported attributes.

You may use either type of group in your Okta org; consult Okta documentation for information on how to configure them. Whichever type of group you use, to support user role mapping with the management center you must configure a custom attribute for the group to convey its role mapping expression to the management center.

This documentation describes role mapping using Okta groups; mapping with application groups requires familiarity with the third-party user management application in use at your organization to set up custom attributes. See the Okta documentation for details.

Before you begin

- Configure a management center service provider application at the Okta IdP; see Configure the Management Center Service Provider Application for Okta, on page 34.

- Configure user role mapping at the management center; Configure User Role Mapping for Okta in the Management Center, on page 36.

Procedure

Create a new SAML group attribute for the management center service provider application:

- For **Name**, use the same string you entered at the management center SSO configuration for **Group Member Attribute**. (See Step 4 in Configure User Role Mapping for Okta in the Management Center, on page 36.)

- For **Filter**, specify an expression to represent the role or roles the management center will assign to the members of the group. Okta compares this value against the names of the groups of which a user is a member, and sends the management center the group names that match. The management center in turn compares those group names against the regular expressions you assigned to each management center user role in Step 5 of Configure User Role Mapping for Okta in the Management Center, on page 36.

Okta User Role Mapping Examples

As the following examples demonstrate, the SSO configurations at the management center to support user role mapping are the same for both individual users and for groups. The difference lies in the settings at the management center service provider application in Okta.

✎

Note   You can configure management center roles to be mapped based on individual user permissions or based on group permissions, but a single management center application cannot support role mapping for both groups and individual users. Furthermore, the management center can support group role mapping using only one group attribute statement per management center service provider application configured in Okta.

Okta Role Mapping Example for Individual User Accounts

In role mapping for individual users, the Okta management center service application has a custom attribute whose name matches the name of the Group Member Attribute on the management center. (In this example, `UserRole`). The user profile in Okta also has a custom attribute (in this example, a variable named `FMCrole`.) The definition for the application custom attribute `UserRole` establishes that when Okta passes user role mapping information to the management center, it will use the custom attribute value assigned for the user in question.

The following diagrams illustrate how the relevant fields and values in the management center and Okta configurations correspond to each other in user role mapping for individual accounts. Each diagram uses the same SSO configurations at the management center and at the Okta UI Admin Console, but the configuration for each user at the Okta UI Admin Console differs to assign each user different roles at the management center.

- In this diagram sue@example.com uses the `FMCrole` value `FMCAdmin` and the management center assigns her the Administrator role.
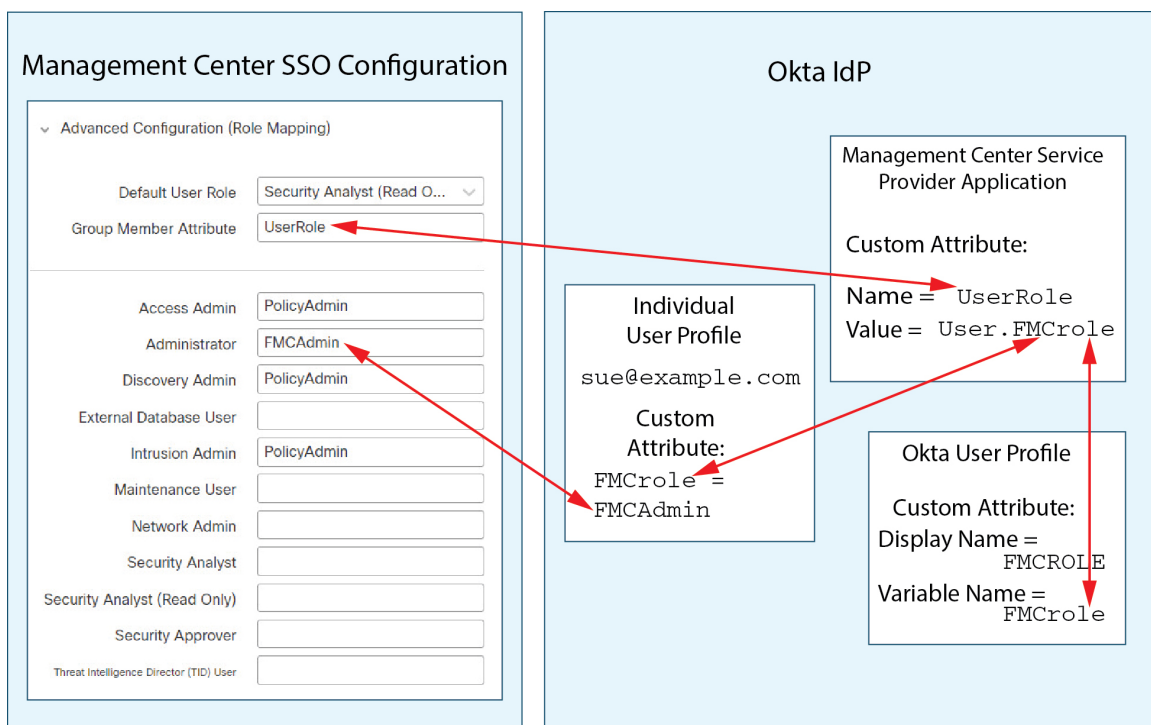
- In this diagram fred@example.com uses the FMCrole value PolicyAdmin, and the management center assigns him the roles Access Admin, Discovery Admin, and Intrusion Admin.
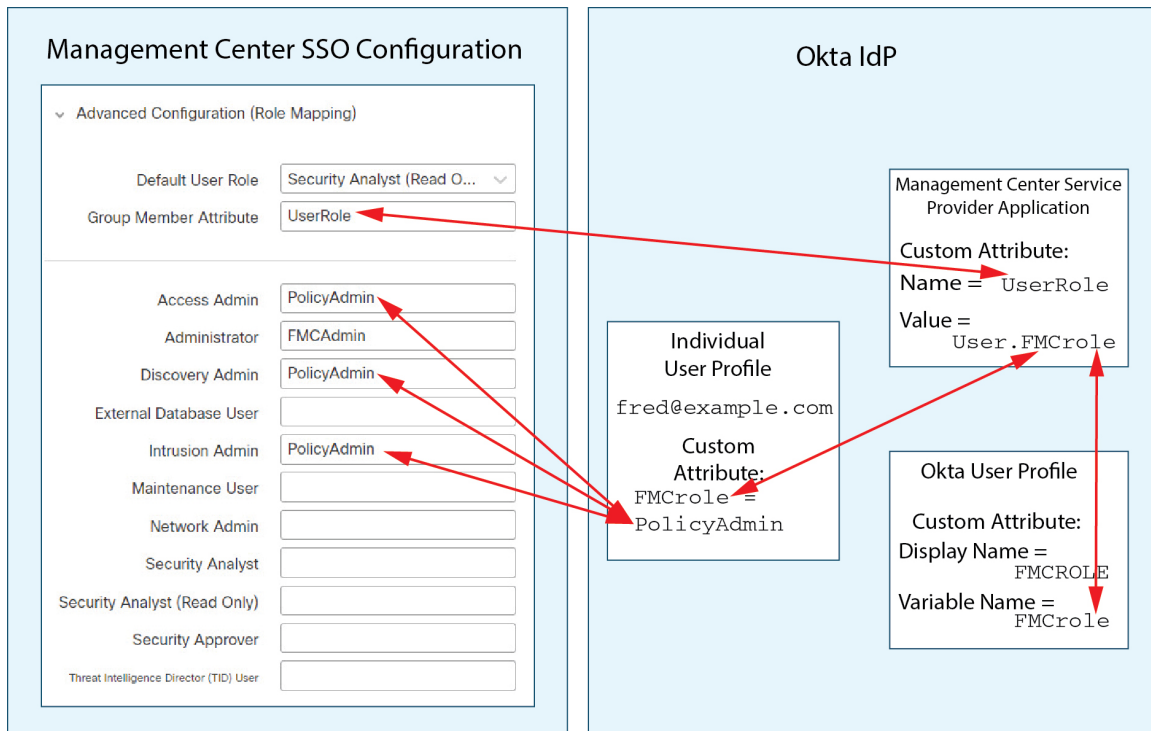
- Other users assigned to the Okta service application for this management center are assigned the default user role Security Analyst (Read Only) for one of the following reasons:

    - They have no value assigned to the FMCrole variable in their Okta user profile.

    - The value assigned to the FMCrole variable in their Okta user profile does not match any expression configured for a user role in the SSO configuration at the management center.

Okta Role Mapping Example for Groups

In role mapping for groups, the Okta management center service application has a custom group attribute whose name matches the name of the **Group Member Attribute** on the management center (in this example, UserRole). When Okta processes a request for management center SSO login, it compares the user's group membership against the expression assigned to the management center service application group attribute (in this case ^(.*)Admin$). Okta sends to the management center the user's group membership(s) that match the group attribute. The management center compares the group names it receives against the regular expressions it has configured for each user role, and assigns user roles accordingly.

The following diagrams illustrate how the relevant fields and values in the management center and Okta configurations correspond to each other in user role mapping for groups. Each diagram uses the same SSO configurations at the management center and at the Okta UI Admin Console, but the configuration for each user at the Okta UI Admin Console differs to assign each user different roles at the management center.

- In this diagram fred@example.com is a member of the Okta IdP group Admin, which matches the expression ^(.*)Admin$. Okta sends the management center Fred's Admin group membership, and the management center assigns him the Administrator role.

Management Center SSO Configuration
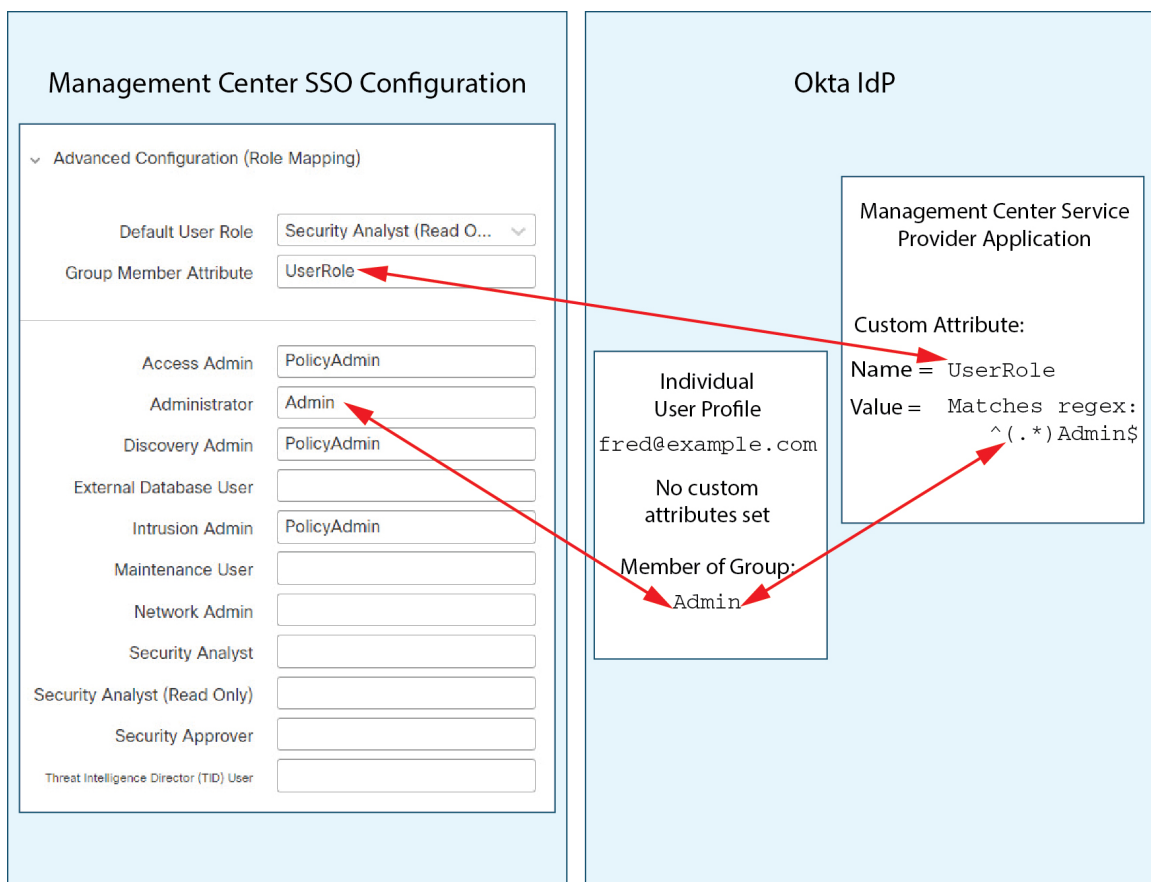
Okta IdP

- In this diagram sue@example.com is a member of the Okta IdP group `PolicyAdmin`, which matches the expression `^(.*)Admin$`. Okta sends the management center Sue's `PolicyAdmin` group membership, and the management center assigns her the roles Access Admin, Discovery Admin, and Intrusion Admin.

Sue is also a member of the Okta group `Maint`, but because this group name does not match the expression assigned to the group membership attribute in the Okta management center service application, Okta does not send information about Sue's `Maint` group membership to the management center, and her membership in the `Maint` group plays no part in the roles the management center assigns to her.
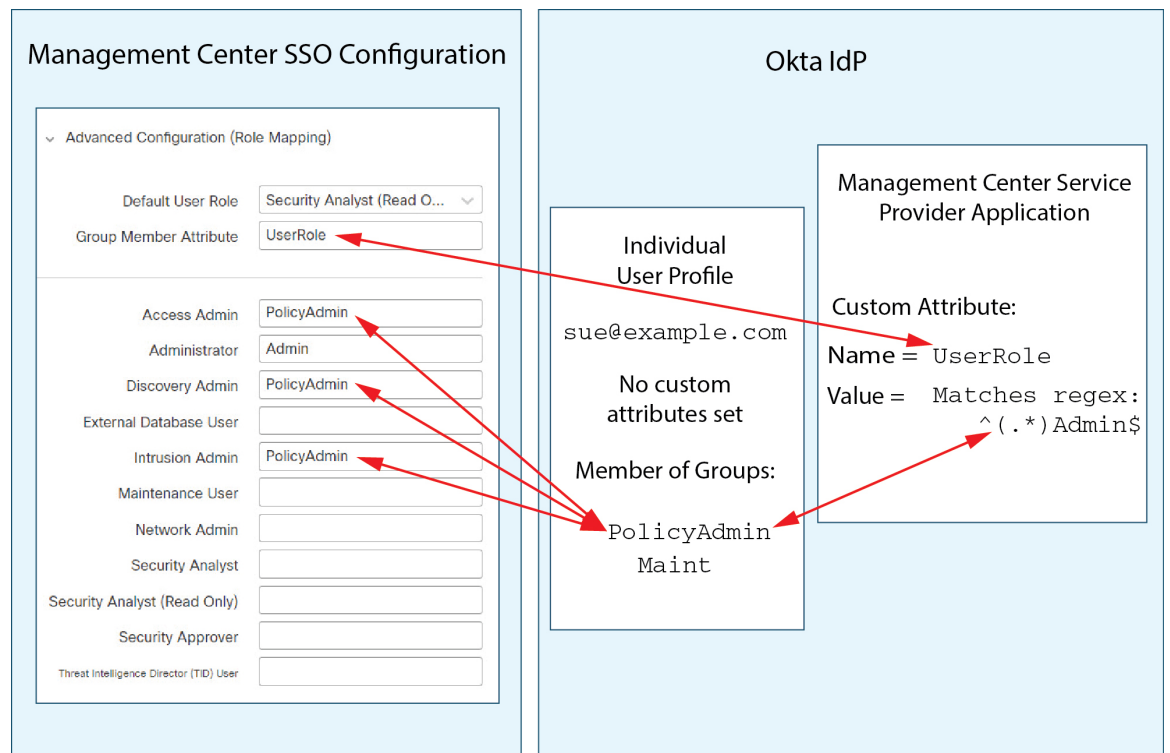
- In this diagram sean@example.com is a member of the Okta IdP group `Maint`. This group name does not match the expression `^(.*)Admin$`, so, when sean@example.com logs into the management center, Okta does not send information about Sean's `Maint` group membership to the management center and Sean is assigned the default user role (Security Analyst (Read Only)) rather than the Maintenance User role.

Management Center SSO Configuration

∨ Advanced Configuration (Role Mapping)

Default User Role	Security Analyst (Read O... ∨
Group Member Attribute	UserRole
Access Admin	PolicyAdmin
Administrator	Admin
Discovery Admin	PolicyAdmin
External Database User	
Intrusion Admin	PolicyAdmin
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	

Okta IdP

Individual
User Profile
sean@example.com

No custom
attributes set

Member of Group:
Maint

Management Center Service
Provider Application

Custom Attribute:

Name = UserRole

Value = Matches regex:
^(.*)Admin$

These diagrams illustrate the importance of advance planning when establishing a role mapping strategy. In this example, any Okta user with access to this management center who is a member of only the `Maint` group can be assigned only the default user role. The management center supports using only one custom group attribute in its Okta Service Application configuration. The expression you assign to that attribute and the group names you establish to match against it must be carefully crafted. You can add more flexibility to role mapping by using regular expressions in the user role assignment strings in the management center SSO configuration. (The expression you assign to each management center user role must comply with the restricted version of Google's RE2 regular expression standard supported by Golang and Perl.)

Configure Single Sign-On with OneLogin

See the following tasks to configure SSO using OneLogin:
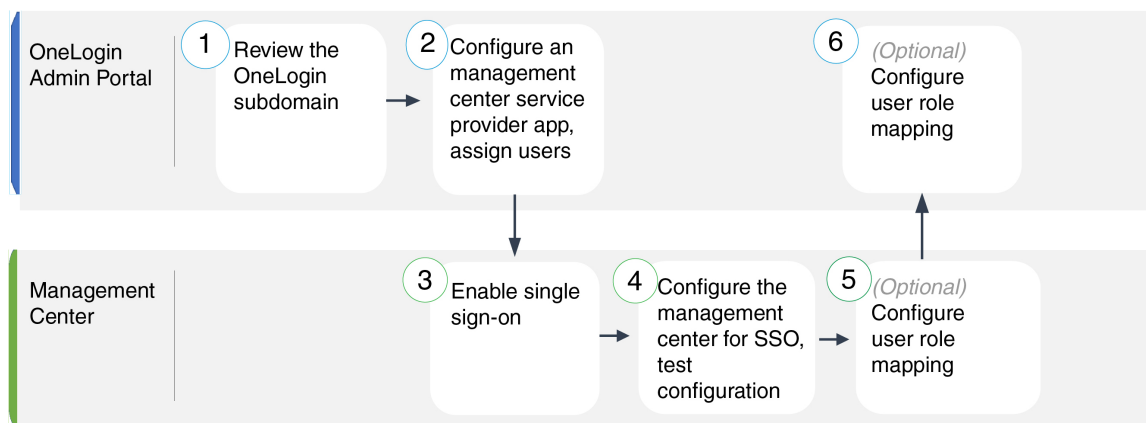
1	management center	Review the OneLogin Subdomain, on page 46
2	management center	Configure the Management Center Service Provider Application for OneLogin, on page 46
3	OneLogin Admin Portal	Enable Single Sign-On at the Management Center, on page 31
4	OneLogin Admin Portal	Configure the Management Center for OneLogin SSO, on page 48
5	OneLogin Admin Portal	Configure User Role Mapping for OneLogin in the Management Center, on page 49
6	management center	Configure User Role Mapping at the OneLogin IdP, on page 50

Review the OneLogin Subdomain

In OneLogin, the entity that encompasses all the federated devices and applications that a user can access with the same SSO account is called a subdomain. Before adding the management center to a OneLogin subdomain, be familiar with its configuration; consider the following questions:

- How many users will have access to the management center?

- Are users within the OneLogin subdomain members of groups?

- Are users and groups from a third-party directory such as Active Directory, Google Apps, or LDAP synchronized with the OneLogin subdomain?

- Do you need to add more users or groups to the OneLogin subdomain to support SSO on the management center?

- What kind of management center user role assignments do you want to make? (If you choose not to assign user roles, the management center automatically assigns a configurable default user role to all SSO users.)

- How must users and groups within the OneLogin subdomain be organized to support the required user role mapping?

Keep in mind that you can configure management center roles to be mapped based on individual users or based on groups, but a single management center application cannot support role mapping for both groups and individual users.

This documentation assumes you are already familiar with the OneLogin Admin Portal, and have an account with Super User privilege. To configure user role mapping, you will also need a subscription to the OneLogin Unlimited plan, which supports Custom User Fields. If you need more information, see the OneLogin documentation available online.

Configure the Management Center Service Provider Application for OneLogin

Use these instructions at the OneLogin Admin Portal to create a management center service provider application within OneLogin and assign users or groups to that application. You should be familiar with SAML SSO concepts and the OneLogin Admin Portal. This documentation does not describe all the OneLogin functions

you need to establish a fully functional SSO org; for instance, to create users and groups, or to import user and group definitions from another user management application, see the OneLogin documentation.

Note If you plan to assign user groups to the management center application, do not also assign users within those groups as individuals.

Note The management center cannot support role mapping using multiple SSO attributes; you must select either user role mapping or group role mapping and configure a single attribute to convey user role information from OneLogin to the management center.

Before you begin

- Familiarize yourself with the OneLogin subdomain and its users and groups; see .

- Create user accounts in your OneLogin subdomain if necessary.

Note The system requires that user names for SSO accounts as well as the NameID attribute the IdP sends to the management center during the SAML login process must be both be valid email addresses. Many IdP's automatically use the username of the user trying to logon as the NameID attribute, but you should confirm this is the case for your IdP. Keep this in mind when configuring a service provider application at your IdP and creating IdP user accounts that are to be granted SSO access to the management center.

- Confirm the login URL for the target management center (`https://ipaddress_or_hostname/`).

Note If your management center web interface can be reached with multiple URLs. (for instance, a fully-qualified domain name as well as an IP address), SSO users must consistently access the management center using the login URL that you configure in this task.

Procedure

Step 1 Create the management center service provider application using the **SAML Test Connector (Advanced)** as its basis.

Step 2 Configure the application with the following settings:

- For the **Audience (Entity ID)**, append the string `/saml/metadata` to the management center login URL. For example: `https://ExampleFMC/saml/metadata`.

- For **Recipient**, append the string `/saml/acs` to the management center login URL. For example: `https://ExampleFMC/saml/acs`.

- For **ACS (Consumer) URL Validator**, enter an expression that OneLogin uses to confirm it is using the correct management center URL. You can create a simple validator by using the ACS URL and altering it as follows:

  - Append a `^` to the beginning of the ACS URL.

  - Append a `$` to the end of the ACS URL.

  - Insert a `\` preceding every `/` and `?` within the ACS URL.

For example, for the ACS URL `https://ExampleFMC/saml/acs`, an appropriate URL validator would be `^https:\/\/ExampleFMC\/saml\/acs$`.

- For **ACS (Consumer) URL**, append the string `/saml/acs` to the management center login URL. For example: `https://ExampleFMC/saml/acs`.

- For **Login URL**, append the string `/saml/acs` to the management center login URL. For example: `https://ExampleFMC/saml/acs`.

- For the **SAML Initiator**, choose `Service Provider`.

Step 3   Assign OneLogin users to the management center service provider application.

Step 4   (Optional) To make SSO setup at the management center easier, you can download the SAML XML metadata for the management center service provider application from OneLogin to your local computer.

What to do next

Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Configure the Management Center for OneLogin SSO

Use these instructions at the management center web interface.

Before you begin

- Create a management center service provider application at the OneLogin Admin Portal; see Configure the Management Center Service Provider Application for OneLogin, on page 46.

- Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Procedure

Step 1   (This step continues directly from Enable Single Sign-On at the Management Center, on page 31.) At the **Configure OneLogin Metadata** dialog, you have two choices:

- To enter the SSO configuration information manually:

  a. Click the **Manual Configuration** radio button.

    b. Enter the following SSO configuration values from the OneLogin service provide application:

- **Identity Provider Single Sign-On URL**: Enter the **SAML 2.0 Endpoint (HTTP)** from OneLogin.

- **Identity Provider Issuer**: Enter the **Issuer URL** from OneLogin.

- **X.509 Certificate**: Enter the **X.509 Certificate** from OneLogin.

- If you saved the XML metadata file generated by OneLogin to your local computer (Step 4 in Configure the Management Center Service Provider Application for OneLogin, on page 46), you can upload the file to the management center:

    a. Click the **Upload XML File** radio button.

    b. Follow the on-screen instructions to navigate to and choose the XML metadata file on your local computer.

Step 2   Click **Next**.

Step 3   At the **Verify Metadata** dialog, review the configuration parameters and click **Save**.

Step 4   Click **Test Configuration**. If the system displays an error message, review the SSO configuration for the management center as well as the OneLogin service provider application configuration, correct any errors, and try again.

Step 5   When the system reports a successful configuration test, click **Apply**.

What to do next

You may optionally configure user role mapping for SSO users; see Configure User Role Mapping for OneLogin in the Management Center, on page 49. If you choose not to configure role mapping, by default all SSO users that log into the management center are assigned the user role you configure in Step 4 of Configure User Role Mapping for OneLogin in the Management Center, on page 49.

Configure User Role Mapping for OneLogin in the Management Center

The fields to configure for user role mapping at the management center web interface are the same regardless of your choice of SSO provider. But the values you configure must take into account how the SAML SSO provider you use implements user role mapping.

Before you begin

- Review the OneLogin users and groups, see Review the OneLogin Subdomain, on page 46.

- Configure an SSO service provider application for the management center; see Configure the Management Center Service Provider Application for OneLogin, on page 46.

- Enable and configure single sign-on at the management center; see Enable Single Sign-On at the Management Center, on page 31, and Configure the Management Center Service Provider Application for OneLogin, on page 46.

Procedure

Step 1   Choose **System** (⚙) > **Users** > **Single Sign-On**.

Step 2   Expand **Advanced Configuration (Role Mapping)**.

Step 3   From the **Default User Role** drop-down list, choose a default management center user role to assign users.

Step 4   In the **Group Member Attribute** field, enter an attribute configured in OneLogin for management center user role mapping for users or groups. See Step 1 of Configure User Role Mapping for Individual Users at the OneLogin IdP, on page 51 or Step 1 of Configure User Role Mapping for Groups at the OneLogin IdP, on page 52.

Step 5   Next to each management center user roll you wish to assign to SSO users, enter a regular expression. The management center compares these values against the user role mapping attribute the IdP sends to the management center with SSO user information. The management center grants users a union of all the roles for which a match is found.

Step 6   Click **Test Configuration**. If the system displays an error message, review the SSO configuration for the management center as well as the identity service provider application configuration, correct any errors, and try again.

Step 7   When the system reports a successful configuration test, click **Apply**.

What to do next

Configure user role mapping at the service provider application; see Configure User Role Mapping at the OneLogin IdP, on page 50.

Configure User Role Mapping at the OneLogin IdP

You can configure SSO user role mapping at the Onelogin Admin portal based on individual permissions or based on group permissions.

- To map based on individual user permissions, see Configure User Role Mapping for Individual Users at the OneLogin IdP, on page 51.

- To map based on group permissions, see Configure User Role Mapping for Groups at the OneLogin IdP, on page 52.

When an SSO user logs into the management center, OneLogin presents to the management center a user or group role attribute value that gets its value from a custom user field configured at the OneLogin IdP. The management center compares that attribute value against the regular expressions assigned to each management center user role in the SSO configuration, and grants the user all the roles for which a match is found.. . (If no match is found, the management center grants the user a configurable default user role.) The expression you assign to each management center user role must comply with the restricted version of Google's RE2 regular expression standard supported by Golang and Perl. The management center treats the attribute value received from Okta as a regular expression using that same standard for purposes of comparison with the management center user role expressions.

Note

A single management center cannot support role mapping for both groups and individual users; you must choose one mapping method for the management center service provider application and use it consistently. The management center can support role mapping using only one custom user field configured in OneLogin. Generally group-based role mapping is more efficient for a management center with many users. You should take into account user and group definitions established throughout your OneLogin subdomain.

Configure User Role Mapping for Individual Users at the OneLogin IdP

Use the OneLogin Admin Portal to create a custom parameter for the management center service provider application and a custom user field. These provide the means for OneLogin to pass user role information to the management center during the SSO login process.

Before you begin

Procedure

Step 1   Create a custom parameter for the management center service provider application.

-

- For the **Value**, provide a mnemonic name such as `FMCUserRole`. This must match the name of the customer user field you will configure in Step 2 of this procedure.

Step 2   Create a custom user field to contain user role information for each OneLogin user with access the management center.

- For the field **Name**, provide a mnemonic name such as `FMCUserRole`. This must match the value provided for the application custom parameter described in Step 1 of this procedure.

- For the **Short name**, provide an abbreviated alternate name for the field. (This is used for OneLogin programmatic interfaces.)

Step 3   For each user with access to the management center service provider application, assign a value to the custom user field you created in Step 2 of this procedure.

When a user logs into the management center using SSO, the value you assign to this field for that user is the value the management center compares against the expressions you assigned to management center user roles

in the SSO configuration. (See Step 5 in Configure User Role Mapping for OneLogin in the Management Center, on page 49.)

What to do next

- Test your role mapping scheme by logging into the management center using SSO from various accounts and confirming that users are assigned management center user roles as you expect.

Configure User Role Mapping for Groups at the OneLogin IdP

Use the OneLogin Admin Portal to create a custom parameter for the management center service provider application and a custom user field. Assign OneLogin users to groups. Then create one or more mappings between the custom user field and the user group so OneLogin assigns a value to the custom user field based on the user's group membership. These provide the means for OneLogin to pass group-based user role information to the management center during the SSO login process.

OneLogin service provider applications may use one of two types of groups:

- Groups native to OneLogin.

- Groups synchronized from third-party applications such as Active Directory, Google Apps, or LDAP.

You may user either type of group for management center group role mapping. This documentation describes role mapping using OneLogin groups; using third-party application groups requires familiarity with the third-party user management application in use at your organization. See the OneLogin documentation for details.

Before you begin

- Review the OneLogin subdomain and its users and groups; see Review the OneLogin Subdomain, on page 46.

- Create and configure a management center service provider application in OneLogin; see Configure the Management Center Service Provider Application for OneLogin, on page 46.

- Configure SSO user role mapping as described in Configure User Role Mapping for OneLogin in the Management Center, on page 49.

Procedure

Step 1 Create a custom parameter for the management center service provider application.

- For the **Field Name**, use the same name you used for the **Group Member Attribute** in the management center SSO configuration. (See Step 4 in Configure User Role Mapping for OneLogin in the Management Center, on page 49.)

- For the **Value**, provide a mnemonic name such as `FMCUserRole`. This must match the name of the customer user field you will configure in Step 2 of this procedure.

Step 2   Create a custom user field to contain user role information for each OneLogin user with access the management center.

- For the field **Name**, provide a mnemonic name such as `FMCUserRole`. This must match the value provided for the application custom parameter described in Step 1 of this procedure.

- For the **Short name**, provide an abbreviated alternate name for the field. (This is used for OneLogin programmatic interfaces.)

Step 3   Create one or more user field mappings to assign group-based values to the custom user field you created in Step 2 of this procedure. Create as many mappings as you need to assign the correct management center user role to each OneLogin user group.

- Create one or more **Conditions** for the mapping, comparing the user **Group** field against group names.

- If you create multiple **Conditions**, choose whether a user's group must match `any` or `all` of the conditions for the mapping to take place.

- Create an **Action** for the mapping, to assign a value to the custom user field you created in Step 2 of this procedure. Provide the field **Name**, and the string that OneLogin assigns to this custom user field for all users that meet the **Conditions** you specified.

  The management center compares this string against the expressions you assign to each management center user role in Step 5 of .

- **Reapply All Mappings** when you have completed your changes.

What to do next

- Test your role mapping scheme by logging into the management center using SSO from various accounts and confirming that users are assigned management center user roles as you expect.

OneLogin User Role Mapping Examples

As the following examples demonstrate, the SSO configurations at the management center to support user role mapping are the same for both individual users and for groups. The difference lies in the settings at the management center service provider application in OneLogin.

Note   A single management center cannot support role mapping for both groups and individual users; you must choose one mapping method for the management center service provider application and use it consistently. The management center can support role mapping using only one custom user field configured in OneLogin. Generally group-based role mapping is more efficient for a management center with many users. You should take into account user and group definitions established throughout your OneLogin subdomain.

OneLogin Role Mapping Example for Individual User Accounts

In role mapping for individual users, the OneLogin management center service application has a custom parameter whose name matches the name of the Group Member attribute on the management center (in this example, `UserRole`). OneLogin also has a custom user field defined (in this example, `FMCUserRole`). The

definition for the application custom parameter `UserRole` establishes that when OneLogin passes user role mapping information to the management center, it will use the value of the custom user field `FMCUserRole` for the user in question.

The following diagrams illustrate how the relevant fields and values in the management center and OneLogin configurations correspond to each other in user role mapping for individual accounts. Each diagram uses the same SSO configurations at the management center and at the OneLogin Admin portal, but the configuration for each user at the OneLogin Admin portal differs to assign each user different roles at the management center.

- In this diagram fred@example.com uses the `FMCUserRole` value `PolicyAdmin` and the management center assigns him the roles Access Admin, Discovery Admin, and Intrusion Admin.
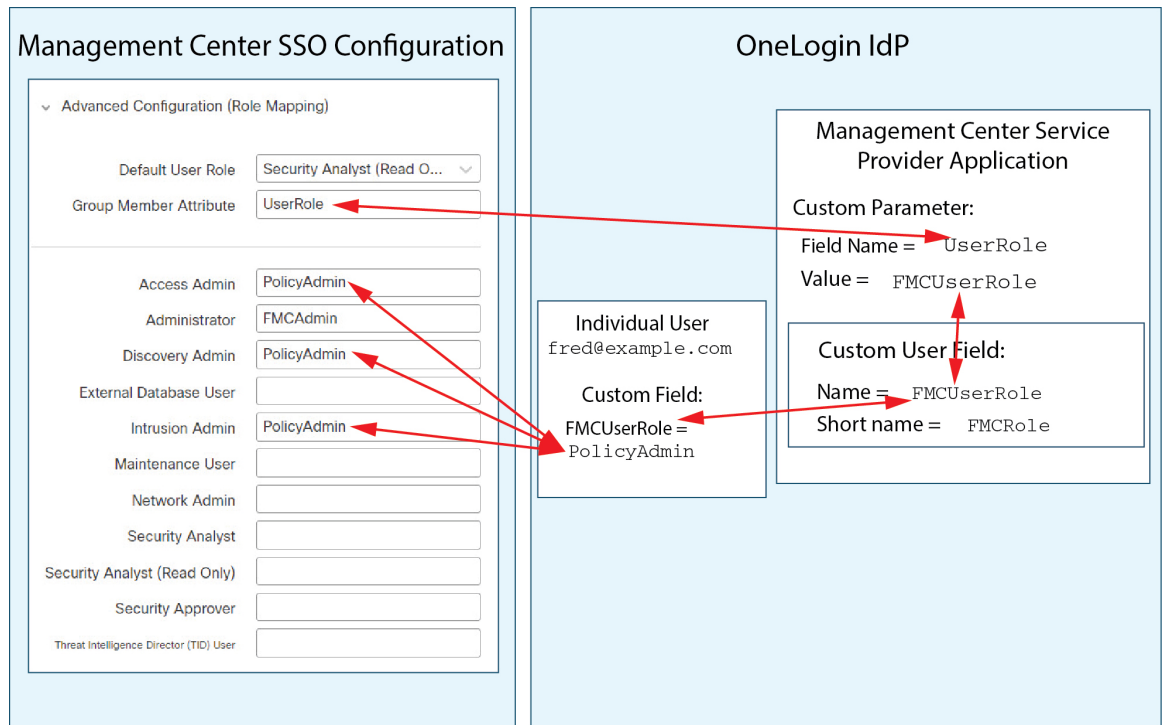
- In this diagram sue@example.com uses the `FMCUserRole` value `FMCAdmin`, and the management center assigns her the Administrator role.
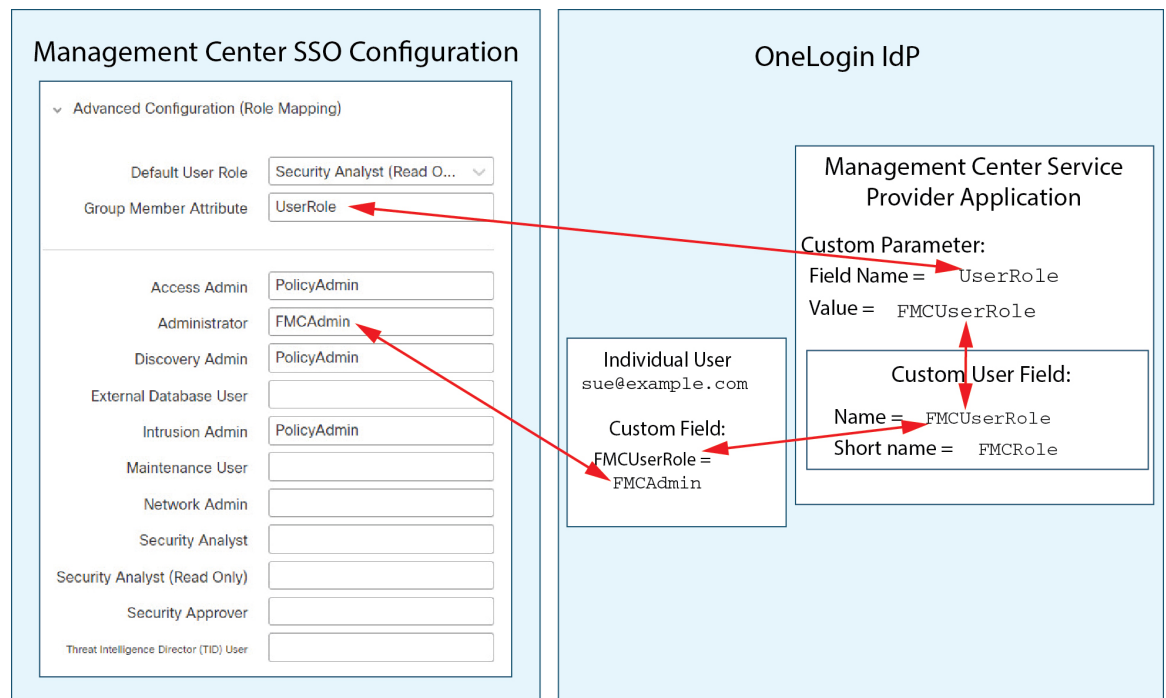
- Other users assigned to the OneLogin service application for this management center are assigned the default user role Security Analyst (Read Only) for one of the following reasons:

  - They have no value assigned to the FMCUserRole custom user field.

  - The value assigned to the FMCUserRole custom user field does not match any expression configured for a user role in the SSO configuration at the management center.

OneLogin Role Mapping Example for Groups

In role mapping for groups, the OneLogin management center service application has a has a custom parameter whose name matches the name of the Group Member attribute on the management center (in this example, UserRole). OneLogin also has a custom user field defined (in this example, FMCUserRole). The definition for the application custom parameter UserRole establishes that when OneLogin passes user role mapping information to the management center, it will use the value of the custom user field FMCUserRole for the user in question. To support user group mapping, you must establish a mapping within OneLogin to assign a value for each user's FMCUserRole field based on that user's OneLogin group membership.

The following diagrams illustrate how the relevant fields and values in the management center and OneLogin configurations correspond to each other in user role mapping for groups. Each diagram uses the same SSO configurations at the management center and at the OneLogin Admin portal, but the configuration for each user at the OneLogin Admin portal differs to assign each user different roles at the management center.

- In this diagram fred@example.com is a member of the OneLogin IdP group FMCPolicyAdminGroup. A OneLogin mapping assigns the value PolicyAdmin to the custom user field FMCUserRole for members of the FMCPolicyAdminGroup. The management center assigns Fred and other members of the FMCPolicyAdminGroup the roles Access Admin, Discovery Admin, and Intrusion Admin.
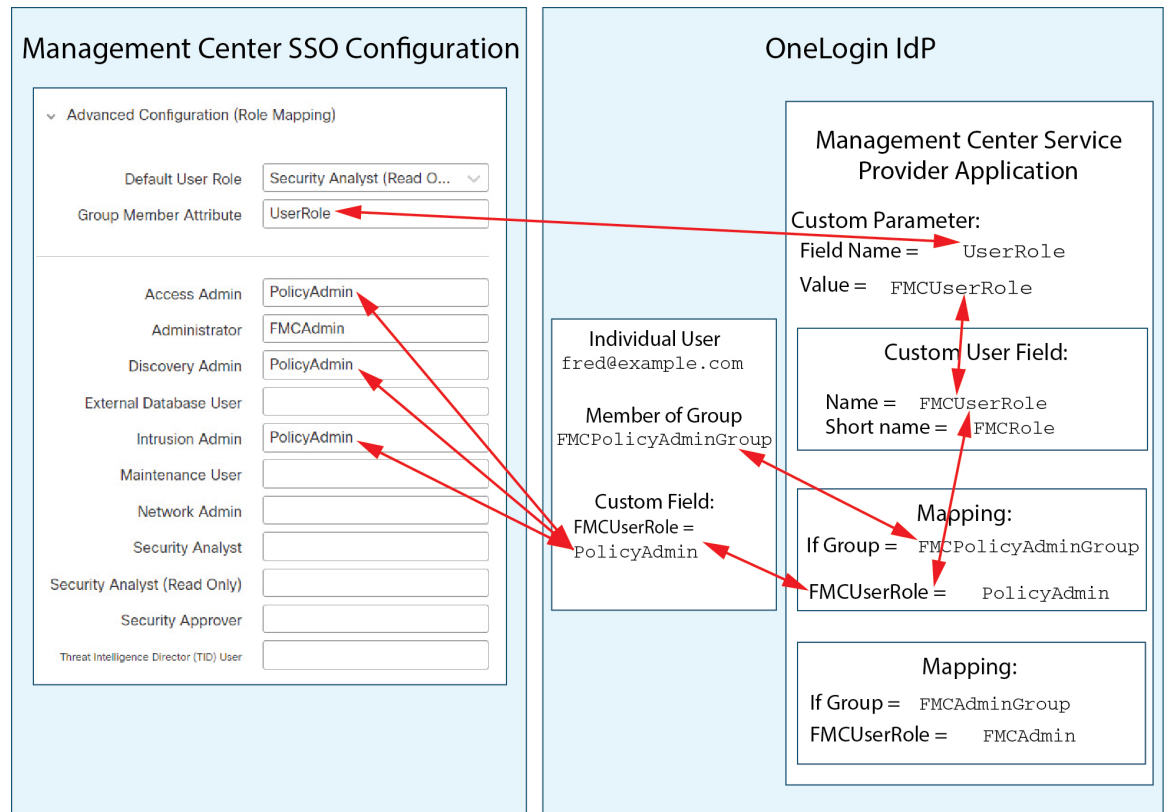
- In this diagram sue@example.com is a member of the OneLogin IdP group `FMCAdminGroup`. A OneLogin mapping assigns the value FMCAdmin to the custom user field `FMCUserRole` for members of the `FMCAdminGroup`. The management center assigns Sue and other members of the `FMCAdminGroup` the Administrator role.
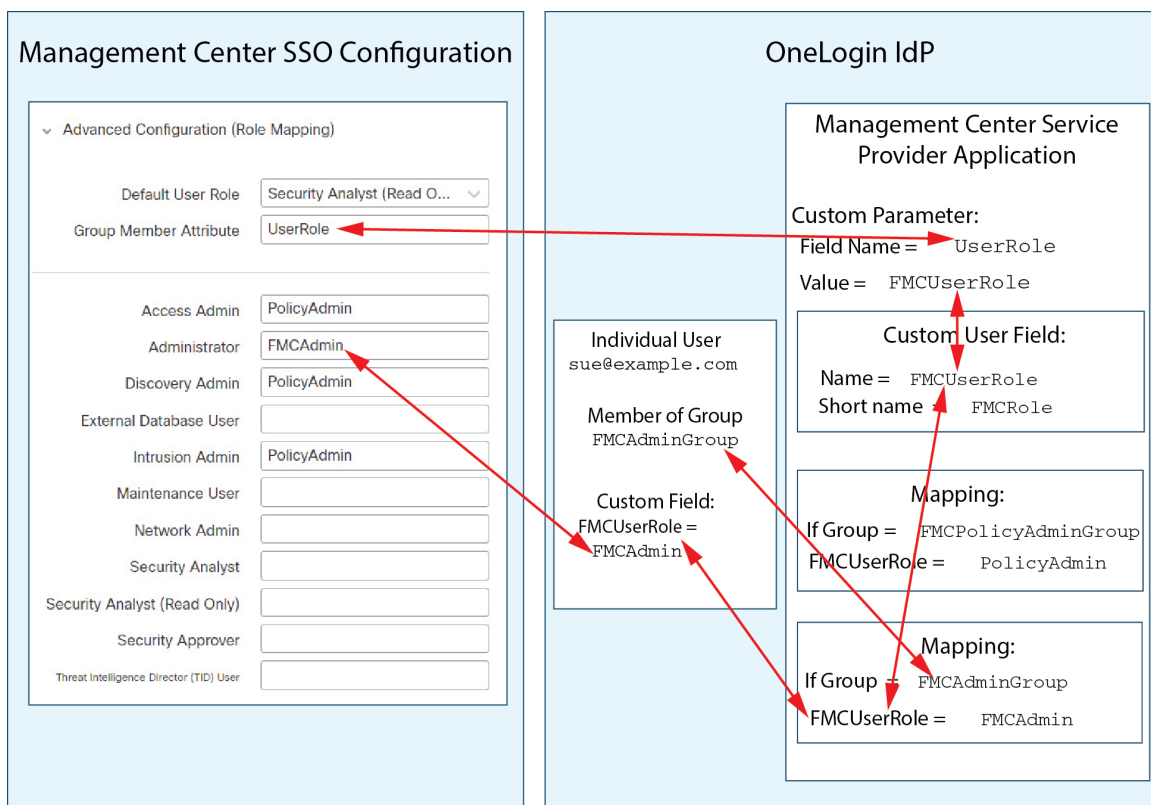
- In this diagram sean@example.com is a member of the Idp group `FMCMaintGroup`. There is no OneLogin mapping associated with this group, so OneLogin does not assign a value to the custom user field `FMCUserRole` for Sean. The management center assigns Sean the default user role (Security Analyst (Read Only)) rather than the Maintenance User role.
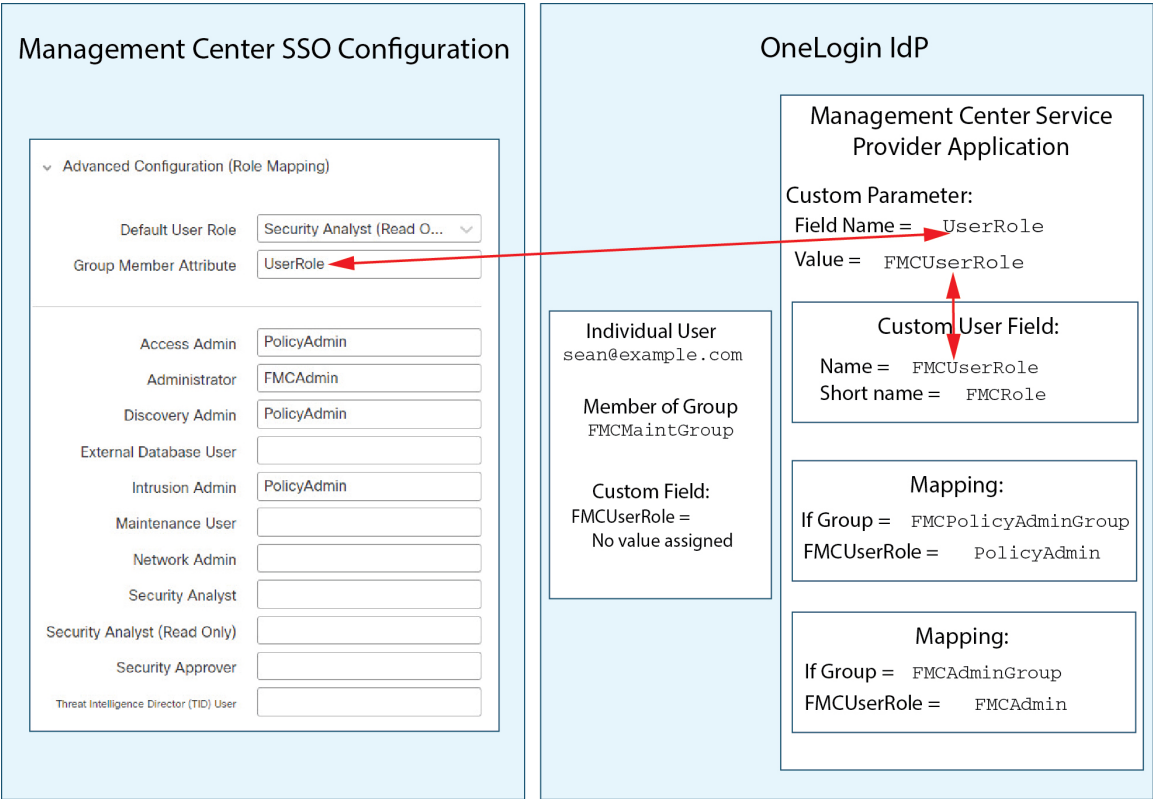
Configure Single Sign-On with Azure AD

See the following tasks to configure SSO using Azure:
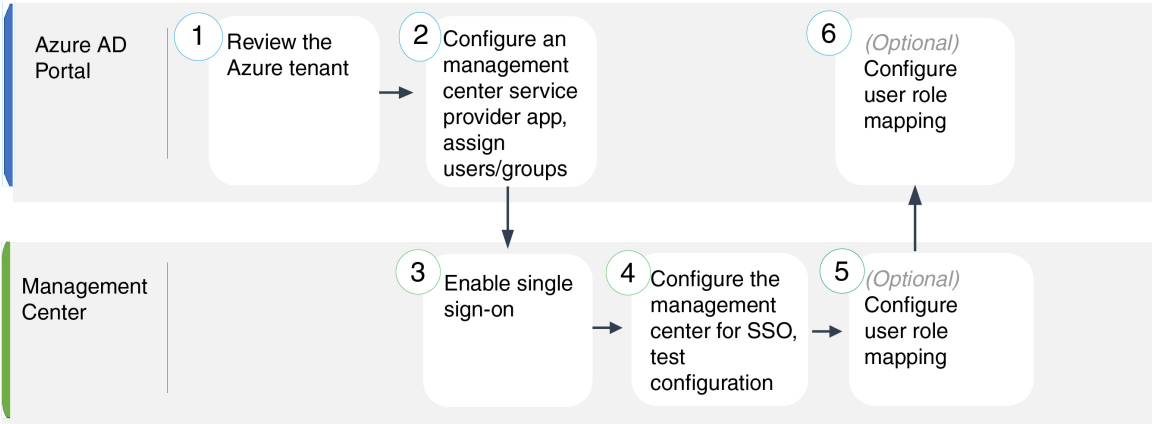
①	Azure AD Portal	Review the Azure Tenant, on page 59
②	Azure AD Portal	Configure the Management Center Service Provider Application for Azure, on page 59

3	management center	Enable Single Sign-On at the Management Center, on page 31
4	management center	Configure the Management Center for Azure SSO, on page 61
5	management center	Configure User Role Mapping for Azure in the Management Center, on page 62
6	Azure AD Portal	Configure User Role Mapping in the Azure IdP, on page 63

Review the Azure Tenant

Azure AD is Microsoft's multitenant cloud based identity and access management service. In Azure, the entity that encompasses all the federated devices that a user can access with the same SSO account is called a *tenant*. Before adding the management center to an Azure tenant, be familiar with its organization; consider the following questions:

- How many users will have access to the management center?

- Are users within the Azure tenant members of groups?

- Are users and groups from another directory product?

- Do you need to add more users or groups to the Azure tenant to support SSO on the management center?

- What kind of management center user role assignments do you want to make? (If you choose not to assign user roles, the management center automatically assigns a configurable default user role to all SSO users.)

- How must users and groups within the Azure tenant be organized to support the required user role mapping?

- Keep in mind that you can configure management center roles to be mapped based on individual users or based on groups, but a single management center application cannot support role mapping for both groups and individual users.

This documentation assumes you are already familiar with the Azure Active Directory Portal and have an account with application admin privileges for the Azure AD tenant. Keep in mind that the management center supports Azure SSO only with tenant-specific single sign-on and single sign-out endpoints. You must have an Azure AD Premium P1 or above license and Global Administrator permissions; see Azure documentation for more information.

Configure the Management Center Service Provider Application for Azure

Use the Azure Active Directory Portal to create a management center service provider application within your Azure Active Directory tenant and establish basic configuration settings.

Note   If you plan to assign user groups to the management center application, do not also assign users within those groups as individuals.

Note The management center cannot support role mapping using multiple SSO attributes; you must select either user role mapping or group role mapping and configure a single attribute to convey user role information from OneLogin to the management center.

Before you begin

- Familiarize yourself with your Azure tenant and its users and groups; see .

- Create user accounts and/or groups in your Azure tenant if necessary.

Note The system requires that user names for SSO accounts as well as the NameID attribute the IdP sends to the management center during the SAML login process must be both be valid email addresses. Many IdP's automatically use the username of the user trying to logon as the NameID attribute, but you should confirm this is the case for your IdP. Keep this in mind when configuring a service provider application at your IdP and creating IdP user accounts that are to be granted SSO access to the management center.

- Confirm the login URL for the target management center (`https://ipaddress_or_hostname`)

Note If your management center web interface can be reached with multiple URLs (for instance, a fully-qualified domain name as well as an IP address), SSO users must consistently access the management center using the login URL that you configure in this task.

Procedure

Step 1 Create the management center service provider application using the Azure AD SAML Toolkit as its basis.

Step 2 Configure the application with the following settings for **Basic SAML Configuration**:

- For the **Identifier (Entity ID)** append the string `/saml/metadata` to the management center login URL. For example: `https://ExampleFMC/saml/metadata`.

- For the **Reply URL (Assertion Consumer Service URL)** append the string `/saml/acs` to the management center login URL. For example: `https://ExampleFMC/saml/acs`.

- For the **Sign on URL** append the string `/saml/acs` to the management center login URL. For example: `https://ExampleFMC/saml/acs`.

Step 3 Edit the **Unique User Identifier Name (Name ID)** claim for the application to force the username for sign-on at the management center to be the email address associated with the user account:

- For **Source** choose `Attribute`.

• For **Source attribute**: Choose `user.mail`.

Step 4   Generate a certificate to secure SSO on the management center. Use the following options for the certificate:

• Select Sign SAML Response and Assertion for the Signing Option.

• Select SHA-256 for the Signing Algorithm.

Step 5   Download the Base-64 version of the certificate to your local computer; you will need it when you configure Azure SSO at the management center web interface

Step 6   In the SAML-based Sign-on information for the application, note the following values:

• **Login URL**

• **Azure AD Identifier**

You will need these values when you configure Azure SSO at the management center web interface.

Step 7   (Optional) to make SSO setup at the management center easier, you can download the SAML XML metadata file for the management center service provider application (called the **Federation Metadata XML** in the Azure Portal) to your local computer.

Step 8   Assign existing Azure users and groups to the management center service application.

Note
If you plan to assign user groups to the management center Application, do not also assign users within those groups as individuals.

Note
If you plan to configure user role mapping, you can configure roles to be mapped based on individual user permissions or based on group permissions, but a single management center application cannot support role mapping for both groups and individual users.

What to do next

Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Configure the Management Center for Azure SSO

Use these instructions at the management center web interface.

Before you begin

• Create a management center service provider application at the Azure AD Portal; see Configure the Management Center Service Provider Application for Azure, on page 59.

• Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Procedure

Step 1   (This step continues directly from Enable Single Sign-On at the Management Center, on page 31.) At the **Configure Azure Metadata** dialog, you have two choices:

- To enter the SSO configuration information manually:

  a. Click the **Manual Configuration** radio button.

  b. Enter the values you retrieved from the Azure SSO Service Provider application:

    - For **Identity Provider Single Sign-On URL** enter the **Login URL** you noted in Step 6 of Configure the Management Center Service Provider Application for Azure, on page 59.

    - For **Identity Provider Issuer** enter the **Azure AD Identifier** you noted in Step 6 of Configure the Management Center Service Provider Application for Azure, on page 59.

    - For the **X.509 Certificate**, use the certificate you downloaded from Azure in Step 5 of Configure the Management Center Service Provider Application for Azure, on page 59. (Use a text editor to open the certificate file, copy the contents, and paste it into the **X.509 Certificate** field.)

- If you saved the XML metadata file generated by Azure to your local computer (Step 7 of Configure the Management Center Service Provider Application for Azure, on page 59), you can upload the file the management center:

  a. Click the **Upload XML File** radio button.

  b. Follow the on-screen instructions to navigate to and choose the XML metadata file on your local computer.

Step 2   Click **Next**.

Step 3   At the **Verify Metadata** dialog, review the configuration parameters and click **Save**.

Step 4   Click **Test Configuration**. If the System displays an error message, review the SSO configuration for the management center as well as the Azure service provider application, correct any errors, and try again.

Step 5   When the system reports a successful configuration test, click **Apply**.

What to do next

You may optionally configure role mapping for SSO users; see Configure User Role Mapping for Azure in the Management Center, on page 62. If you choose not to configure role mapping, by default all SSO users that log into the management center are assigned the default user role you configure in Step 4 of Configure User Role Mapping for Azure in the Management Center, on page 62.

Configure User Role Mapping for Azure in the Management Center

The fields to configure for user role mapping at the management center web interface are the same regardless of your choice of SSO provider. But the values you configure must take into account how the SAML SSO provider you use implements user role mapping.

Before you begin

- Review the existing Azure users and groups; see Review the Azure Tenant, on page 59.

- Configure an SSO service provider application for the management center; see Configure the Management Center Service Provider Application for Azure, on page 59.

- Enable and configure single sign-on at the management center; see Enable Single Sign-On at the Management Center, on page 31, and Configure the Management Center for Azure SSO, on page 61.

Procedure

Step 1	Choose **System** (⚙) > **Users** > **Single Sign-On**.
Step 2	Expand **Advanced Configuration (Role Mapping)**.
Step 3	From the **Default User Role** drop-down list, choose a default management center user role to assign users.
Step 4	In the **Group Member Attribute** field, enter an attribute configured in Azure for management center user role mapping for users or groups. See Step 1 of Configure User Role Mapping for Individual Users at the Azure IdP, on page 64 or Step 1 of Configure User Role Mapping for Groups at the Azure IdP, on page 65.
Step 5	Next to each management center user roll you wish to assign to SSO users, enter a regular expression. The management center compares these values against the user role mapping attribute the IdP sends to the management center with SSO user information. The management center grants users a union of all the roles for which a match is found.
Step 6	Click **Test Configuration**. If the system displays an error message, review the SSO configuration for the management center as well as the identity service provider application configuration, correct any errors, and try again.
Step 7	When the system reports a successful configuration test, click **Apply**.

What to do next

Configure user role mapping at the service provider application; see Configure User Role Mapping in the Azure IdP, on page 63.

Configure User Role Mapping in the Azure IdP

You can configure SSO user role mapping at the Azure AD Portal based on individual user permissions or based on group permissions.

- To map based on individual user permissions, see Configure User Role Mapping for Individual Users at the Azure IdP.

- To map based on group permissions, see Configure User Role Mapping for Groups at the Azure IdP.

When an SSO user logs in to the management center, Azure presents a user or group role attribute value that gets its value from an application role configured at the Azure AD portal, to the management center. The management center then compares that attribute value with the regular expressions assigned to each management center user role in the SSO configuration, and grants the user all the roles for which a match is found. . (If no match is found, the management center grants the user a configurable default user role.) The expression you assign to each management center user role must comply with the restricted version of Google's RE2 regular

expression standard supported by Golang and Perl. The management center treats the attribute value received from Okta as a regular expression using that same standard for purposes of comparison with the management center user role expressions.

> **Note** A single management center cannot support role mapping for both groups and individual users; you must choose one mapping method for the management center service provider application and use it consistently. The management center can support role mapping using only one claim configured in Azure. Generally group-based role mapping is more efficient for a management center with many users. You should take into account user and group definitions established throughout your Azure tenant.

Configure User Role Mapping for Individual Users at the Azure IdP

To establish role mapping for individual users of the management center service application in Azure, use the Azure AD Portal to add a claim to the application, add roles to the application's registration manifest, and assign roles to users.

Before you begin

- Review the Azure tenant; see Review the Azure Tenant, on page 59.

- Create and configure a management center service provider application in Azure; see Configure the Management Center Service Provider Application for Azure, on page 59.

- Configure SSO user role mapping as described in Configure User Role Mapping for Azure in the Management Center, on page 62.

Procedure

Step 1 Add a user claim to the SSO configuration for the management center service application with the following characteristics:

- **Name**: Use the same string you entered for the **Group Member Attribute** in the management center SSO configuration. (See Step 5 in Configure User Role Mapping for Azure in the Management Center, on page 62.)

- **Name identifier format**: Choose `Persistent`.

- **Source**: Choose `Attribute`.

- **Source attribute**: Choose `user.assignedroles`.

Step 2 Edit the manifest for the management center service application (in JSON format) and add application roles to represent management center user roles you wish to assign to SSO users. The simplest approach is to copy an existing application role definition and change the following properties:

- `displayName`: The name for the role that will appear in the AD Azure Portal.

- `description`: A brief description of the role.

- `Id`: An alphanumeric string that must be unique among ID properties within the manifest.

- value: A string to represent one or more management center user roles. (Note: Azure does not permit spaces in this string.)

Step 3 For each user assigned to the management center Service application, assign one of the application roles you have added to the manifest for that application. When a user logs in to the management center using SSO, the application role you assign to that user is the value Azure sends to the management center in the claim for the service application. The management center compares the claim against the expressions you assigned to management center user roles in the SSO configuration (See Step 6 of Configure User Role Mapping for Azure in the Management Center, on page 62.), and assigns the user all the management center user roles for which there is a match.

What to do next

- Test your role mapping scheme by logging into the management center using SSO from various accounts and confirming that users are assigned management center user roles as you expect.

Configure User Role Mapping for Groups at the Azure IdP

To establish role mapping for user groups for the management center service application in Azure, use the Azure AD Portal to add a claim to the application, add roles to the application's registration manifest, and assign roles to groups.

Before you begin

- Review the Azure tenant; see Review the Azure Tenant, on page 59.

- Create and configure a management center service provider application in Azure; see Configure the Management Center Service Provider Application for Azure, on page 59.

- Configure SSO user role mapping as described in Configure User Role Mapping for Azure in the Management Center, on page 62.

Procedure

Step 1 Add a user claim to the SSO configuration for the management center service application with the following characteristics:

- **Name**: Use the same string you entered for the **Group Member Attribute** in the management center SSO configuration. (See Step 5 in Configure User Role Mapping for Azure in the Management Center, on page 62.)

- **Name identifier format**: Choose Persistent.

- **Source**: Choose Attribute.

- **Source attribute**: Choose user.assignedroles.

Step 2 Edit the manifest for the management center service application (in JSON format) and add application roles to represent management center user roles you wish to assign to SSO users. The simplest approach is to copy an existing application role definition and change the following properties:

- `displayName`: The name for the role that will appear in the Ad Azure Portal.

- `description`: A brief description of the role.

- `Id`: An alphanumeric string that must be unique among id properties within the manifest.

- `value`: A string to represent one or more management center user roles. (Azure does not permit spaces in this string.)

Step 3   For each group assigned to the management center Service application, assign one of the application roles you have added to the manifest for that application. When a user logs in to the management center using SSO, the application role you assign to that user's group is the value Azure sends to the management center in the claim for the service application. The management center compares the claim against the expressions you assigned to management center user roles in the SSO configuration (see Step 6 of Configure User Role Mapping for Azure in the Management Center, on page 62), and assigns the user all the management center user roles for which there is a match.

What to do next

Test your role mapping scheme by logging into the management center using SSO from various accounts and confirming that users are assigned management center user roles as you expect.

Azure User Role Mapping Examples

As the following examples demonstrate, the SSO configurations at the management center to support user role mapping are the same for both individual users and for groups. The difference lies in the settings at the management center service provider application in Azure.

Note   You can configure management center roles to be mapped based on individual permissions or based on group permissions, but a single management center application cannot support role mapping for both groups and individual users. The management center can support role mapping using only one claim configured in Azure.

Azure Role Mapping Example for Individual User Accounts

In role mapping for individual users, the Azure management center service application has custom roles defined within its manifest. (In this case, FMCAdmin and PolicyAdmin.) These roles can be assigned to users; Azure stores role assignments for each user in that user's assignedroles attribute. The application also has a custom user claim defined, and this claim is configured to get its value from the assigned user role for a user logging into the management center using SSO. Azure passes the claim value to the management center during the SSO login process, and the management center compares the claim value against strings assigned to each management center user role in the management center SSO configuration.

The following diagrams illustrate how the relevant fields and values in the management center and Azure configurations correspond to each other in user role mapping for individual accounts. Each diagram uses the same SSO configurations at the management center and at the Azure AD portal, but the configuration for each user at the Azure AD portal differs to assign each user different roles at the management center.

- In this diagram sue@ example.com uses the assignedroles attribute value `FMCAdmin`, and the management center assigns her the management center Administrator role.

Management Center SSO Configuration

Advanced Configuration (Role Mapping)

Default User Role	Security Analyst (Read O...
Group Member Attribute	UserRole

Access Admin	PolicyAdmin
Administrator	FMCAdmin
Discovery Admin	PolicyAdmin
External Database User	
Intrusion Admin	PolicyAdmin
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	

Azure IdP

Management Center Service Provider Application
Custom User Claim:
Claim Name = UserRole
Source Attribute =
user.assignedroles

Individual User
sue@example.com

User Attribute
assignedroles =
FMCAdmin

Custom Application Role Definitions in Manifest:
"displayName" : "FMC Admin"
"value" : "FMCAdmin"

"displayName" : "Access, Discovery, Intrusion Admins"
"value" : "PolicyAdmin"

- In this diagram fred @ example .com uses the assignedroles attribute value `PolicyAdmin`, and the management center assigns him the roles Access Admin, Discovery Admin, and Intrusion Admin.

Management Center SSO Configuration

Advanced Configuration (Role Mapping)

Default User Role	Security Analyst (Read O...
Group Member Attribute	UserRole

Access Admin	PolicyAdmin
Administrator	FMCAdmin
Discovery Admin	PolicyAdmin
External Database User	
Intrusion Admin	PolicyAdmin
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	

Azure IdP

Management Center Service Provider Application
Custom User Claim:
Claim Name = UserRole
Source Attribute =
user.assignedroles

Individual User
fred@example.com

User Attribute
assignedroles =
PolicyAdmin

Custom Application Role Definitions in Manifest:
"displayName" : "FMC Admin"
"value" : "FMCAdmin"

"displayName" : "Access, Discovery, Intrusion Admins"
"value" : "PolicyAdmin"

- Other users assigned to the Azure service application for this management center are assigned the default user role Security Analyst (Read Only) for one of the following reasons:

• They have no value assigned to their assignedroles attribute.

• The value assigned to their assignedroles attribute does not match any expression configured for a user role in the SSO configuration at the management center.

Azure Role Mapping Example for Groups

In role mapping for groups, the Azure management center service application has custom roles defined within its manifest. (In this case, FMCAdmin, AccessAdmin, Discovery Admin, and Maint.) These roles can be assigned to groups; Azure passes role assignments for each group to group members' assignedroles attribute. The application also has a custom user claim defined, and this claim is configured to get its value from the assigned user role for a user logging into the management center using SSO. Azure passes the claim value to the management center during the SSO login process, and the management center compares the claim value against strings assigned to each management center user role in the management center SSO configuration.

The following diagrams illustrate how the relevant fields and values in the management center and Azure configurations correspond to each other in user role mapping for groups. Each diagram uses the same SSO configurations at the management center and at the Azure AD portal, but the configuration for each user at the Azure AD portal differs to assign each user different roles at the management center.

• In this diagram sue@example.com is a member of the groups `FMCAccessAdmins` and `FMCDiscoveryAdmins`. From these groups she inherits the custom roles `AccessAdmin` and `DiscoveryAdmin`. When Sue logs into the management center using SSO the management center assigns her the roles Access Admin and Discovery Admin.

Management Center SSO Configuration

Advanced Configuration (Role Mapping)

Default User Role	Security Analyst (Read O...
Group Member Attribute	UserRole

Access Admin	AccessAdmin
Administrator	FMCAdmin
Discovery Admin	DiscoveryAdmin
External Database User	
Intrusion Admin	
Maintenance User	Maint
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	

Azure IdP

Management Center Service Provider Application

Custom User Claim:

Claim Name = `UserRole`

Source Attribute = `user.assignedroles`

Individual User
`sue@example.com`

Member of Groups
`FMCAccessAdmins`
`FMCDiscAdmins`

User Attribute

`assignedroles =`
`AccessAdmin`
`DiscoveryAdmin`

Custom Application Role Definitions in Manifest:
```
"displayName" : "FMC Admin"
"value" : "FMCAdmin"

"displayName" : "Access Admin"
"value" : "AccessAdmin"

"displayName" :
        "Discovery Admin"
"value" : "DiscoveryAdmin"

"displayName" :
        "Maintenance User"
"value" : "Maint"
```

Group Definitions and Role Assignments:

Group	Role
FMCAdmins	FMCAdmin
FMCAccessAdmins	AccessAdmin
FMCDiscAdmins	DiscoveryAdmin
FMCMaintUsers	None assigned

- In this diagram fred@example.com is a member of the `FMCAdmins` group, from which he inherits the custom role `FMCAdmin`. When Fred logs into the management center using SSO the management center assigns him the Administrator role.

Management Center SSO Configuration

Advanced Configuration (Role Mapping)

Default User Role	Security Analyst (Read O...
Group Member Attribute	UserRole

Access Admin	AccessAdmin
Administrator	FMCAdmin
Discovery Admin	DiscoveryAdmin
External Database User	
Intrusion Admin	
Maintenance User	Maint
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	

Azure IdP

Management Center Service Provider Application
Custom User Claim:

Claim Name = `UserRole`

Source Attribute = `user.assignedroles`

Individual User
`fred@example.com`

Member of Groups
`FMCAdmins`

User Attribute
assignedroles =
`FMCAdmin`

Custom Application Role Definitions in Manifest:

```
"displayName" : "FMC Admin"
"value" : "FMCAdmin"

"displayName" : "Access Admin"
"value" : "AccessAdmin"

"displayName" :
        "Discovery Admin"
"value" : "DiscoveryAdmin"

"displayName" :
        "Maintenance User"
"value" : "Maint"
```

Group Definitions and Role Assignments:

Group	Role
FMCAdmins	FMCAdmin
FMCAccessAdmins	AccessAdmin
FMCDiscAdmins	DiscoveryAdmin
FMCMaintUsers	None assigned

• In this diagram sean@example.com is a member of the `FMCMaintUsers` group, but because no custom role has been assigned to `FMCMaintUsers` within the Azure management center service provider application, Sean has no roles assigned to him, and when he logs into the management center using SSO, the management center assigns him the default role Security Analyst (Read Only).

Management Center SSO Configuration

⌄ Advanced Configuration (Role Mapping)

Default User Role	Security Analyst (Read O... ⌄
Group Member Attribute	UserRole

Access Admin	AccessAdmin
Administrator	FMCAdmin
Discovery Admin	DiscoveryAdmin
External Database User	
Intrusion Admin	
Maintenance User	Maint
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	

Azure IdP

Management Center Service Provider Application
Custom User Claim:

Claim Name = `UserRole`

Source Attribute =
`user.assignedroles`

Individual User
`sean@example.com`

Member of Groups
`FMCMaintUsers`

No Assigned Roles

Custom Application
Role Definitions in Manifest:
`"displayName" : "FMC Admin"`
`"value" : "FMCAdmin"`

`"displayName" : "Access Admin"`
`"value" : "AccessAdmin"`

`"displayName" :`
`        "Discovery Admin"`
`"value" : "DiscoveryAdmin"`

`"displayName" :`
`        "Maintenance User"`
`"value" : "Maint"`

Group Definitions
and Role Assignments:

Group	Role
FMCAdmins	FMCAdmin
FMCAccessAdmins	AccessAdmin
FMCDiscAdmins	DiscoveryAdmin
FMCMaintUsers	None assigned

Configure Single Sign-On with PingID

See the following tasks to configure SSO using PingID's PingOne for Customers product:

PingOne for Customers Administrator's Console

1 Review the PingOne environment

2 Configure an management center service provider app

Management Center

3 Enable single sign-on

4 Configure the management center for SSO, test configuration
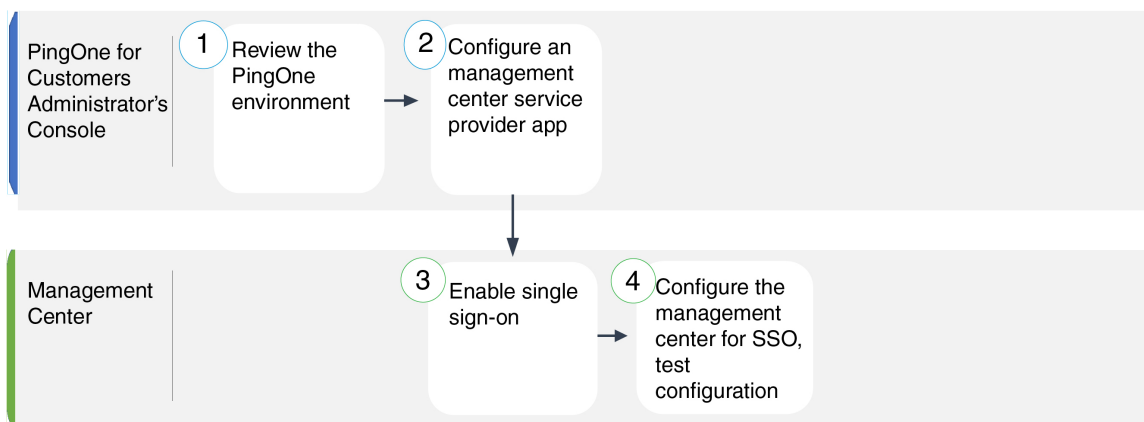
①	PingOne for Customers Administrator's Console	Review the PingID PingOne for Customers Environment, on page 72.
②	PingOne for Customers Administrator's Console	Configure the Management Center Service Provider Application for PingID PingOne for Customers, on page 72.
③	management center	Enable Single Sign-On at the Management Center, on page 31.
④	management center	Configure the Management Center for SSO with the PingID PingOne for Customers, on page 74.

Review the PingID PingOne for Customers Environment

PingOne for Customers is PingID's cloud-hosted identity-as-a-service (IDaaS) product. In PingOne for Customers, the entity that encompasses all the federated devices that a user can access with the same SSO account is called an environment. Before adding the management center to a PingOne environment, be familiar with its organization; consider the following questions:

- How many users will have access to the management center?

- Do you need to add more users to support SSO access to the management center?

This documentation assumes you are already familiar with the PingOne for Customers Administrator Console and have an account with the Organization Admin role.

Configure the Management Center Service Provider Application for PingID PingOne for Customers

Use the PingOne for Customers Administrator Console to create a management center service provider application within your PingOne for Customers environment and establish basic configuration settings. This documentation does not describe all the PingOne for Customers functions you need to establish a fully functional SSO environment; for instance, to create users see the PingOne for Customers documentation.

Before you begin

- Familiarize yourself with your PingOne for Customers environment and its users.

- Create additional users if necessary.

Note The system requires that user names for SSO accounts as well as the NameID attribute the IdP sends to the management center during the SAML login process must be both be valid email addresses. Many IdP's automatically use the username of the user trying to logon as the NameID attribute, but you should confirm this is the case for your IdP. Keep this in mind when configuring a service provider application at your IdP and creating IdP user accounts that are to be granted SSO access to the management center.

• Confirm the login URL for the target management center (`https://ipaddress_or_hostname`)

✎

Note   If your management center web interface can be reached with multiple URLs (for instance, a fully-qualified domain name as well as an IP address), SSO users must consistently access the management center using the login URL that you configure in this task.

Procedure

Step 1   Use the PingOne for Customer Administrator Console to create the application in your environment using these settings:

• Choose the **Web App** application type.

• Choose the **SAML** connection type.

Step 2   Configure the application with the following settings for the SAML Connection:

• For the **ACS URL**, append the string `/sam/acs` to the management center login URL. For example: `https://ExampleFMC/saml/acs`.

• For the **Signing Certificate**, choose Sign Assertion & Response.

• For the **Signing Algorithm** choose RSA_SHA256.

• For the **Entity ID**, append the string `/saml/metadata` to the management center login URL. For example: `https://ExampleFMC/saml/metadata`.

• For the **SLO Binding** select HTTP POST.

• For the **Assertion Validity Duration** enter 300.

Step 3   In the SAMLConnection information for the application, note the following values:

• **Single Sign-On Service**

• **Issuer ID**

You will need these values when you configure SSO using PingID's PingOne for Customers product at the management center web interface.

Step 4   For **SAML ATTRIBUTES**, make the following selections for a single required attribute:

• **PINGONE USER ATTRIBUTE:** `Email Address`

• **APPLICATION ATTRIBUTE:** `saml_subject`

Step 5   Download the signing certificate in X509 PEM (`.crt`) format and save it to your local computer.

Step 6   (Optional) to make SSO setup at the management center easier, you can download the SAML XML metadata file for the management center service provider application to your local computer.

Step 7   Enable the application.

What to do next

Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Configure the Management Center for SSO with the PingID PingOne for Customers

Before you begin

- Create a management center service provider application at the PingOne for Customers Administrator Console; see Configure the Management Center Service Provider Application for PingID PingOne for Customers, on page 72.

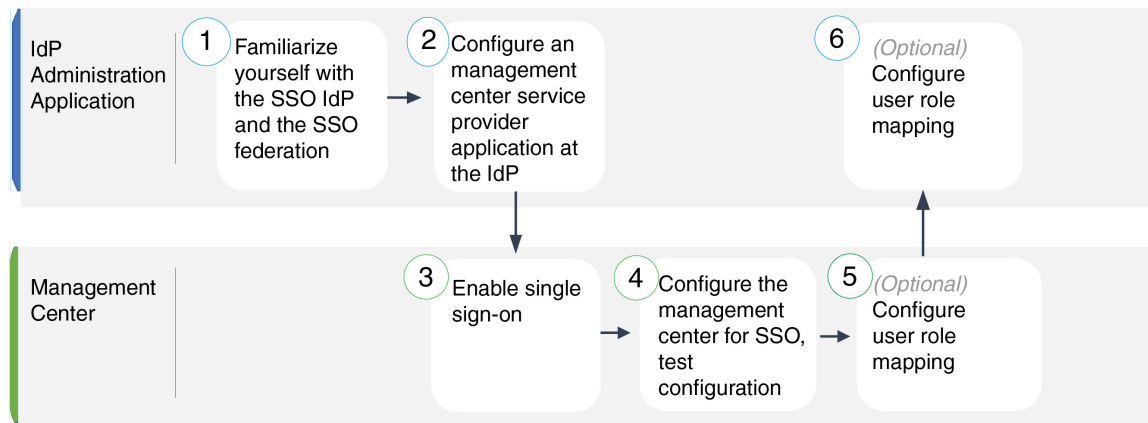- Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Procedure

Step 1   (This step continues directly from Enable Single Sign-On at the Management Center, on page 31.) At the **Configure PingID Metadata** dialog, you have two choices:

- To enter the SSO configuration information manually:

  a.   Click the **Manual Configuration** radio button.

  b.   Enter the values you retrieved from the PingOne for Customers Administrator Console:

    - For **Identity Provider Single Sign-On URL** enter the **Single Signon Service** you noted in Step 3 of Configure the Management Center Service Provider Application for PingID PingOne for Customers, on page 72.

    - For **Identity Provider Issuer** enter the **Issuer ID** you noted in Step 3 of Configure the Management Center Service Provider Application for PingID PingOne for Customers, on page 72.

    - For the **X.509 Certificate**, use the certificate you downloaded from PingOne for Customers in Step 5 of Configure the Management Center Service Provider Application for PingID PingOne for Customers, on page 72. (Use a text editor to open the certificate file, copy the contents, and paste it into the **X.509 Certificate** field.)

- If you saved the XML metadata file generated by PingOne for Customers to your local computer (Step 6 of Configure the Management Center Service Provider Application for PingID PingOne for Customers, on page 72), click the **Upload XML File** radio button to upload the file to the management center:

Step 2   Click **Next**.

Step 3   At the **Verify Metadata** dialog, review the configuration parameters and click **Save**.

Step 4   Expand **Advanced Configuration (Role Mapping)**.

Step 5   From the **Default User Role** drop-down list, choose a default management center user role to assign users.

Step 6   In the **Group Member Attribute** field, enter an attribute configured in PingID PingOne for management center user role mapping for users or groups.

Step 7   Next to each management center user role you wish to assign to SSO users, enter a regular expression. The management center compares these values against the user role mapping attribute the IdP sends to the management center with SSO user information. The management center grants users a union of all the roles for which a match is found.

Step 8   Click **Test Configuration**. If the System displays an error message, review the SSO configuration for the management center as well as the PingOne for Customers service provider application, correct any errors, and try again.

Step 9   When the system reports a successful configuration test, click **Apply**.

Configure Single Sign-On with Any SAML 2.0-Compliant SSO Provider

The management center supports single sign-on with any SSO identity provider (IdP) compliant with the SAML 2.0 SSO protocol. Generic instructions to use a wide range of SSO providers must address the tasks to be performed at a high level; establishing SSO using a provider not specifically addressed in this documentation requires that you be proficient with the IdP of your choice. These tasks help you determine the steps to configure the management center for single sign-on using any SAML 2.0-compliant SSO provider:

IdP Administration Application

1. Familiarize yourself with the SSO IdP and the SSO federation
2. Configure an management center service provider application at the IdP
6. (Optional) Configure user role mapping

Management Center

3. Enable single sign-on
4. Configure the management center for SSO, test configuration
5. (Optional) Configure user role mapping

1	IdP Administration Application	Familiarize Yourself with the SSO Identity Provider and the SSO Federation, on page 76.
2	IdP Administration Application	Configure Management Center Service Provider Application for Any SAML 2.0-Compliant SSO Provider, on page 76.
3	management center	Enable Single Sign-On at the Management Center, on page 31.
4	management center	Configure the Management Center for SSO Using Any SAML 2.0-Compliant SSO Provider, on page 78.

5	management center	Configure User Role Mapping in the Management Center for SAML 2.0-Compliant SSO Providers, on page 79.
6	IdP Administration Application	Configure Management Center User Role Mapping at the IdP for SAML 2.0-Compliant SSO Providers, on page 81.

Familiarize Yourself with the SSO Identity Provider and the SSO Federation

Read the IdP vendor documentation with the following considerations in mind:

- Does the SSO provider require that users subscribe to or register with any services before using the IdP?

- What terminology does the SSO provider use for common SSO concepts? For instance, to refer to a group of federated service provider applications, Okta uses "org" where Azure uses "tenant."

- Does the SSO provider support SSO exclusively, or a suite of functions—for instance, multifactor authentication or domain management? (This can affect configuration of some elements shared between features—especially users and groups.)

- What permissions does an IdP user account need to configure SSO?

- What configurations does the SSO provider require you to establish for a service provider application? For instance, Okta automatically generates an X509 Certificate to secure its communications with the management center, while Azure requires that you generate that certificate using the Azure portal interface.

- How are users and groups created and configured? How are users assigned to groups? How are users and groups granted access to service provider applications?

- Does the SSO provider require that at least one user be assigned to a service provider application before the SSO connection can be tested?

- Does the SSO provider support user groups? How are user and group attributes configured? How can you map attributes to management center user roles in the SSO configuration?

- Do you need to add more users or groups to the federation to support SSO on the management center?

- Are users within the federation members of groups?

- Are user and group definition native to the IdP or imported from a user management application such as Active Directory, RADIUS, or LDAP?

- What kind of user role assignments do you want to make? (If you choose not to assign user roles, the management center automatically assigns the user a configurable default user role to all SSO users.)

- How must users and groups within the federation be organized to support your plan for user role mapping?

Configure Management Center Service Provider Application for Any SAML 2.0-Compliant SSO Provider

Generally SSO providers require that you configure a service provider application at the IdP for each federated application. All IdPs that support SAML 2.0 SSO need the same configuration information for service provider

applications, but some IdP's automatically generate some configuration settings for you, while others require that you configure all settings yourself.

Note	If you plan to assign user groups to the management center Application, do not also assign users within those groups as individuals.

Note	The management center cannot support role mapping using multiple SSO attributes; you must select either user role mapping or group role mapping and configure a single attribute to convey user role information from the IdP to the management center.

Before you begin

- Familiarize yourself with the SSO federation and its users and groups; see Familiarize Yourself with the SSO Identity Provider and the SSO Federation, on page 76.

- Confirm your IdP account has the necessary permissions to perform this task.

- Create user accounts and/or groups in your SSO federation if necessary.

Note	The system requires that user names for SSO accounts as well as the NameID attribute the IdP sends to the management center during the SAML login process must be both be valid email addresses. Many IdP's automatically use the username of the user trying to logon as the NameID attribute, but you should confirm this is the case for your IdP. Keep this in mind when configuring a service provider application at your IdP and creating IdP user accounts that are to be granted SSO access to the management center.

- Confirm the login URL for the target management center (`https://ipaddress_or_hostname`)

Note	If your management center web interface can be reached with multiple URLs. (for instance, a full-qualified domain name as well as an IP address), SSO users must consistently access the management center using the login URL that you configure in this task.

Procedure

Step 1 Create a new service provider application at the IdP.

Step 2 Configure values required by the IdP. Be sure to include the fields listed below, required to support SAML 2.0 SSO functionality with the management center. (Because different SSO service providers use different terminology for SAML concepts, this list provides alternate names for these fields to help you find the right settings in the IdP application.):

- Service Provider Entity ID, Service Provider Identifier, Audience URI: A globally unique name for the service provider (the management center), formatted as a URL. To create this, append the string `/saml/metadata` to the management center login URL, such as `https://ExampleFMC/saml/metadata`.

- Single Sign on URL, Recipient URL, Assertion Consumer Service URL: The service provider (management center) address to which the browser sends information on behalf of the IdP. To create this, append the string `saml/acs` to the management center login URL, such as `https://ExampleFMC/saml/acs`.

- X.509 Certificate: Certificate to secure communications between the management center and the IdP. Some IdP's may automatically generate the certificate, and some may require that you explicitly generate it using the IDP interface.

Step 3 (Optional if you are assigning groups to the application) Assign individual users to the management center application. (If you plan to assign groups to the management center application, do not assign members of those groups as individuals.)

Step 4 (Optional if you are assigning individual users to the application.) Assign user groups to the management center application.

Step 5 (Optional) Some IdP's provide the ability to generate a SAML XML metadata file containing the information you have configured in this task formatted to comply with SAML 2.0 standards. If your IdP provides this ability, you can download the file to your local computer to ease the SSO configuration process at the management center.

What to do next

Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Configure the Management Center for SSO Using Any SAML 2.0-Compliant SSO Provider

Use these instructions at the management center web interface. To configure the management center for SSO using any SAML 2.0-compliant SSO provider, you need information from the IdP.

Before you begin

- Review the organization of your SSO federation, and its users and groups.

- Configure a management center service provider application at the IdP; see Configure the Management Center for SSO Using Any SAML 2.0-Compliant SSO Provider, on page 78.

- Gather the following SSO configuration information for the service provider application from the IdP. Because different SSO service providers use different terminology for SAML concepts, this list provides alternate names for these fields to help you find the right values in the IdP application:

  - Identity Provider Single Sign-On URL, Login URL: The IdP URL where the browser sends information on behalf of the management center.

  - Identity Provider Issuer, Identity Provider Issuer URL, Issuer URL: A globally unique name for the IdP, often formatted as a URL.

  - An X.509 digital certificate to secure communications between the management center and the IdP.

- Enable single sign-on; see Enable Single Sign-On at the Management Center, on page 31.

Procedure

Step 1   (This step continues directly from Enable Single Sign-On at the Management Center, on page 31.) At the **Configure SAML Metadata** dialog, you have two choices:

- To enter the SSO configuration information manually:

  a. Click the **Manual Configuration** radio button.

  b. Enter the following values previously obtained from the SSO Service Provider application:

    - **Identity Provider Single Sign-On URL**

    - **Identity Provider Issuer**

    - **X.509 Certificate**

- If you saved an the XML metadata file generated at the IdP (Step 5 in Configure Management Center Service Provider Application for Any SAML 2.0-Compliant SSO Provider, on page 76), you can upload the file to the management center:

  a. Click the **Upload XML File** radio button.

  b. Follow the on-screen instructions to navigate to and choose the XML metadata file on your local computer.

Step 2   Click **Next**.

Step 3   At the **Verify Metadata** dialog, review the configuration parameters and click **Save**.

Step 4   Click **Test Configuration**. If the system displays an error message, review the SSO configuration for the management center as well as the service provider application configuration at the IdP, correct any errors, and try again.

Step 5   When the system reports a successful configuration test, click **Apply**.

What to do next

You may optionally configure user role mapping for SSO users; see Configure User Role Mapping in the Management Center for SAML 2.0-Compliant SSO Providers, on page 79. If you choose not to configure role mapping, by default all SSO users that log into the management center are assigned the default user role you configure in Step 4 of Configure User Role Mapping in the Management Center for SAML 2.0-Compliant SSO Providers, on page 79.

Configure User Role Mapping in the Management Center for SAML 2.0-Compliant SSO Providers

To implement SAML SSO user role mapping you must establish coordinating configurations at the IdP and at the management center.

- At the IdP, establish user or group attributes to convey user role information and assign values to them; the IdP sends these to the management center once it has authenticated and authorized an SSO user.

• At the management center, associate values with each of the management center user roles you want to assign to users.

When the IdP sends the user or group attribute associated with an authorized user, the management center, the management center compares the attribute value with the values associated with each management center user role, assigns the user all the roles that match, . The management center performs this comparison by treating both values as regular expressions that comply with the restricted version of Google's RE2 regular expression standard supported by Golang and Perl.

The fields to configure for user role mapping at the management center web interface are the same regardless of your choice of SSO provider. But the values you configure must take into account how the SAML SSO provider you use implements user role mapping. Your IdP may enforce syntactical limitations on user or group attributes; if so, you must devise a user role mapping scheme using role names and regular expressions compatible with those requirements.

Before you begin

• Configure an SSO service provider application for the management center; see Configure Management Center Service Provider Application for Any SAML 2.0-Compliant SSO Provider, on page 76.

• Enable and configure single sign-on at the management center, see Enable Single Sign-On at the Management Center, on page 31, and Configure the Management Center for SSO Using Any SAML 2.0-Compliant SSO Provider, on page 78.

Procedure

Step 1 Choose **System** ( ) > **Users** > **Single Sign-On**.

Step 2 Expand **Advanced Configuration (Role Mapping)**.

Step 3 Select a management center user role to assign users as a default value from the **Default User Role** drop-down.

Step 4 Enter a **Group Member Attribute**. This string must match an attribute name configured at the IdP management center service provider application for user role mapping using either users or groups. (See Step 1 of Configure Management Center User Role Mapping at the IdP for SAML 2.0-Compliant SSO Providers, on page 81.)

Step 5 Next to each management center user roll you wish to assign to SSO users, enter a regular expression. The management center compares these values against the user role mapping attribute the IdP sends to the management center with SSO user information. The management center grants users a union of all the roles for which a match is found.

Step 6 Click **Test Configuration**. If the system displays an error message, review the SSO configuration for the management center as well as the identity service provider application configuration, correct any errors, and try again.

Step 7 When the system reports a successful configuration test, click **Apply**.

What to do next

Configure user role mapping at the service provider application; see Configure Management Center User Role Mapping at the IdP for SAML 2.0-Compliant SSO Providers, on page 81.

Configure Management Center User Role Mapping at the IdP for SAML 2.0-Compliant SSO Providers

The detailed steps for configuring user role mapping are different for each IdP. You must determine how to create a custom user or group attribute for the service provider application, and assign values to the attribute for each user or group at the IdP to convey user or group privileges to the management center. Keep in mind the following:

- If your IdP imports user or group profiles from a third-party user management application (such as Active directory, LDAP, or Radius), this may affect how you can use attributes for role mapping.

- Take into account user and group role definitions throughout your SSO federation.

- The management center cannot support role mapping using multiple SSO attributes; you must select either user role mapping or group role mapping and configure a single attribute to convey user role information from the IdP to the management center.

- Group role mapping is generally more efficient for a management center with many users.

- If you assign user groups to management center applications, do not also assign users within those groups as individuals.

- For the purpose of determining a match with management center user roles, the management center treats user and group role attribute values received from the IdP as regular expressions complying with the restricted version of Google's RE2 regular expression standard supported by Golang and Perl. Your IdP may enforce certain syntactical limitations on user or group attributes. if so, you must devise a user role mapping scheme using role names and regular expressions compatible with those requirements.

Before you begin

- Confirm your IdP account has the necessary permissions to perform this task.

- Configure a management center service provider application at the IdP (see Configure Management Center Service Provider Application for Any SAML 2.0-Compliant SSO Provider, on page 76).

Procedure

| **Step 1** | At the IdP, create or designate an attribute to be sent to the management center to contain role mapping information for each user sign-in. This may be a user attribute, a group attribute, or a different attribute that obtains its value from a source such as user or group definitions maintained by the IdP or a third party user management application. |
| **Step 2** | Configure how the attribute gets its value. Coordinate the possible values with the values associated with the user roles in the management center SSO configuration. |

Customize User Roles for the Web Interface

Each user account must be defined with a user role. This section describes how to manage user roles and how to configure a custom user role for web interface access. For default user roles, see User Roles, on page 2.

Create Custom User Roles

Custom user roles can have any set of menu-based and system permissions, and may be completely original, copied from a predefined or another custom user role, or imported from another management center.

✎

Note (Requires Version 7.2.6+) Although you can enable access to content updates without product upgrades, we recommend against the reverse: product without content. That is, if you enable **Product Upgrades** in a custom user role, also enable **Content Updates**. Otherwise, you could have trouble manually uploading upgrade packages and upgrading older ASA FirePOWER and NGIPSv devices.

Procedure

Step 1 Choose **System** (⚙) > **Users**.

Step 2 Click **User Roles**.

Step 3 Add a new user role with one of the following methods:

- Click **Create User Role**.

- Click the **Copy** (🗐) next to the user role you want to copy.

- Import a custom user role from another management center:

  a. On the other management center, click the **Export**(📤) to save the role to your computer.

  b. On the new management center, choose **System** (⚙) > **Tools** > **Import/Export**.

  c. Click **Upload Package**, then follow the instructions to import the saved user role to the new management center.

Step 4 Enter a **Name** for the new user role. User role names are case sensitive.

Step 5 (Optional) Add a **Description**. Limit the description length to 128 characters.

Step 6 Choose **Menu-Based Permissions** for the new role.

When you choose a permission, all of its children are chosen, and the multi-value permissions use the first value. If you clear a high-level permission, all of its children are cleared also. If you choose a permission but not its children, it appears in italic text.

Copying a predefined user role to use as the base for your custom role preselects the permissions associated with that predefined role.

You can apply restrictive searches to a custom user role. These searches constrain the data a user can see in the tables on the pages available under the Analysis menu. You can configure a restrictive search by first creating a private saved search and selecting it from the **Restrictive Search** drop-down menu under the appropriate menu-based permission.

Step 7 (Optional) Check the **External Database Access (Read Only)** check box to set database access permissions for the new role.

This option provides read-only access to the database using an application that supports JDBC SSL connections. For the third-party application to authenticate to the management center, you must enable database access in the system settings.

Step 8 (Optional) To set escalation permissions for the new user role, see Enable User Role Escalation, on page 84.

Step 9 Click **Save**.

The custom role is saved. If the system determines it is a read-only role, it labels the role with '(Read Only)'. This is relevant when configuring the number of concurrent sessions for read-only vs read-write users. You cannot make a role read-only by adding '(Read Only)' to the role name. For more information on concurrent session limits, see User Configuration.

Example

You can create custom user roles for access control-related features to designate whether users can view and modify access control and associated policies.

The following table lists custom roles that you could create and user permissions granted for each example. The table lists the privileges required for each custom role. In this example, Policy Approvers can view (but not modify) access control and intrusion policies. They can also deploy configuration changes to devices.

Table 1: Sample Access Control Custom Roles

Menu-Based Permission	Example Roles		
	Access Control Editor	**Intrusion & Network Analysis Editor**	**Policy Approver**
Access Control	yes	no	yes
Access Control Policy	yes	no	yes
Modify Access Control Policy	no	no	no
Intrusion Policy	no	yes	yes
Modify Intrusion Policy	no	yes	no
Deploy Configuration to Devices	no	no	yes

Deactivate User Roles

Deactivating a role removes that role and all associated permissions from any user who is assigned that role. You cannot delete predefined user roles, but you can deactivate them.

In a multidomain deployment, the system displays custom user roles created in the current domain, which you can edit. It also displays custom user roles created in ancestor domains, which you cannot edit. To view and edit custom user roles in a lower domain, switch to that domain.

Procedure

Step 1	Choose **System** (⚙) > **Users**.
Step 2	Click **User Roles**.
Step 3	Click the slider next to the user role you want to activate or deactivate.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

If you deactivate, then reactivate, a role with Lights-Out Management while a user with that role is logged in, or restore a user or user role from a backup during that user's login session, that user must log back into the web interface to regain access to IPMItool commands.

Enable User Role Escalation

You can give custom user roles the permission, with a password, to temporarily gain the privileges of another, targeted user role in addition to those of the base role. This feature allows you to easily substitute one user for another during an absence, or to more closely track the use of advanced user privileges. Default user roles do not support escalation.

For example, a user whose base role has very limited privileges can escalate to the Administrator role to perform administrative actions. You can configure this feature so that users can use their own passwords, or so they use the password of another user that you specify. The second option allows you to easily manage one escalation password for all applicable users.

To configure user role escalation, see the following workflow.

Procedure

Step 1	Set the Escalation Target Role, on page 84. Only one user role at a time can be the escalation target role.
Step 2	Configure a Custom User Role for Escalation, on page 85.
Step 3	(For the logged in user) Escalate Your User Role, on page 86.

Set the Escalation Target Role

You can assign any of your user roles, predefined or custom, to act as the system-wide escalation target role. This is the role to which a custom role can escalate, if it has the ability. Only one user role at a time can be the escalation target role. Each escalation lasts for the duration of a login session and is recorded in the audit log.

Procedure

Step 1	Choose **System** (⚙) > **Users**.
Step 2	Click **User Roles**.
Step 3	Click **Configure Permission Escalation**.
Step 4	Choose a user role from the **Escalation Target** drop-down list.
Step 5	Click **OK** to save your changes.
	Changing the escalation target role is effective immediately. Users in escalated sessions now have the permissions of the new escalation target.

Configure a Custom User Role for Escalation

Users for whom you want to enable escalation must belong to a custom user role with escalation enabled. This procedure describes how to enable escalation for a custom user role.

Consider the needs of your organization when you configure the escalation password for a custom role. If you want to easily manage many escalating users, you might want to choose another user whose password serves as the escalation password. If you change that user's password or deactivate that user, all escalating users who require that password are affected. This action allows you to manage user role escalation more efficiently, especially if you choose an externally-authenticated user that you can manage centrally.

Before you begin

Set a target user role according to .

Procedure

Step 1	Begin configuring your custom user role as described in .
Step 2	In **System Permissions**, choose the **Set this role to escalate to: Maintenance User** check box.
	The current escalation target role is listed beside the check box.
Step 3	Choose the password that this role uses to escalate. You have two options:

- Choose **Authenticate with the assigned user's password** if you want users with this role to use their own passwords when they escalate, .
- Choose **Authenticate with the specified user's password** and enter that username if you want users with this role to use the password of another user.

> **Note**
> When authenticating with another user's password, you can enter any username, even that of a deactivated or nonexistent user. Deactivating the user whose password is used for escalation makes escalation impossible for users with the role that requires it. You can use this feature to quickly remove escalation powers if necessary.

Step 4   Click **Save**.

Escalate Your User Role

When a user has an assigned custom user role with permission to escalate, that user can escalate to the target role's permissions at any time. Note that escalation has no effect on user preferences.

Procedure

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

If you do not see this option, your administrator did not enable escalation for your user role.

Step 2   Enter the authentication password.

Step 3   Click **Escalate**. You now have all permissions of the escalation target role in addition to your current role.

Escalation lasts for the remainder of your login session. To return to the privileges of your base role only, you must log out, then begin a new session.

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.

Configure User Preferences

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

In a multidomain deployment, user preferences apply to all domains where your account has access. When specifying home page and dashboard preferences, keep in mind that certain pages and dashboard widgets are constrained by domain.

Changing Your Password

All user accounts are protected with a password. You can change your password at any time, and depending on the settings for your user account, you may have to change your password periodically.

When password strength checking is enabled, passwords must comply with the strong password requirements described in Guidelines and Limitations for User Accounts for Management Center, on page 8.

If you are an LDAP or a RADIUS user, you cannot change your password through the web interface.

Procedure

Step 1	From the drop-down list under your user name, choose **User Preferences**.
Step 2	Click **Change Password**.
Step 3	Optionally, check the **Show password** check box to see the password while using this dialog.
Step 4	Enter your **Current Password**.
Step 5	You have two options:

  • Enter your new password for **New Password** and **Confirm Password**.
  • Click **Generate Password** to have the system create a password for you which complies with the listed criteria. (Generated passwords are non-mnemonic; take careful note of the password if you choose this option.)

Step 6	Click **Apply**.

Changing an Expired Password

Depending on the settings for your user account, your password may expire. The password expiration time period is set when your account is created. If your password has expired, the Password Expiration Warning page appears.

Procedure

On the Password Expiration Warning page, you have two choices:

- Click **Change Password** to change your password now. If you have zero warning days left, you **must** change your password.

  Tip
  When password strength checking is enabled, passwords must comply with the strong password requirements described in Guidelines and Limitations for User Accounts for Management Center, on page 8.

- Click **Skip** to change your password later.

Change the Web Interface Appearance

You can change the way the web interface appears.

Procedure

From the drop-down list under your user name, choose a theme:

- **Light**

- **Dusk**

- **Classic** (the look and feel before Version 6.6)

Specifying Your Home Page

You can specify the page within the web interface to use as your home page for the appliance. The default home page is the default dashboard (**Overview** > **Dashboards** > **Dashboard**), except for user accounts with no dashboard access, such as External Database users. (See Specifying Your Default Dashboard, on page 95 to set the default dashboard.)

In a multidomain deployment, the home page you choose applies to all domains where your user account has access. When choosing a home page for an account that frequently accesses multiple domains, keep in mind that certain pages are constrained to the Global domain.

Procedure

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

Step 2   Click **Home Page**.

Step 3   Choose the page you want to use as your home page from the drop-down list.

The options in the drop-down list are based on the access privileges for your user account. For more information, see User Roles, on page 2.

Step 4   Click **Save**.

Configuring Event View Settings

Use the Event View Settings page to configure characteristics of event views on the management center. Note that some event view configurations are available only for specific user roles. Users with the External Database User role can view parts of the event view settings user interface, but changing those settings has no meaningful result.

Procedure

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

Step 2   Click **Event View Settings**.

Step 3   In the **Event Preferences** section, configure the basic characteristics of event views; see Event View Preferences, on page 90.

Step 4   In the **File Preferences** section, configure file download preferences; see File Download Preferences, on page 91.

Step 5   In the **Default Time Windows** section, configure the default time window or windows; see Default Time Windows, on page 92.

Step 6   In the **Default Workflow** sections, configure default workflows; see Default Workflows, on page 94.

Step 7   Click **Save**.

Event View Preferences

Use the Event Preferences section of the Event View Settings page to configure basic characteristics of event views. This section is available for all user roles, although it has little to no significance for users who cannot view events.

The following fields appear in the Event Preferences section:

- The **Confirm "All" Actions** field controls whether the appliance forces you to confirm actions that affect all events in an event view.

  For example, if this setting is enabled and you click **Delete All** on an event view, you must confirm that you want to delete all the events that meet the current constraints (including events not displayed on the current page) before the appliance will delete them from the database.

- The **Resolve IP Addresses** field allows the appliance, whenever possible, to display host names instead of IP addresses in event views.

Note that an event view may be slow to display if it contains a large number of IP addresses and you have enabled this option. Note also that for this setting to take effect, you must use management interfaces configuration to establish a DNS server in the system settings.

- The **Expand Packet View** field allows you to configure how the packet view for intrusion events appears. By default, the appliance displays a collapsed version of the packet view:

  - **None** - collapse all subsections of the Packet Information section of the packet view

  - **Packet Text** - expand only the Packet Text subsection

  - **Packet Bytes** - expand only the Packet Bytes subsection

  - **All** - expand all sections

Regardless of the default setting, you can always manually expand the sections in the packet view to view detailed information about a captured packet.

- The **Rows Per Page** field controls how many rows of events per page you want to appear in drill-down pages and table views.

- The **Refresh Interval** field sets the refresh interval for event views in minutes. Entering 0 disables the refresh option. Note that this interval does not apply to dashboards.

- The **Statistics Refresh Interval** controls the refresh interval for event summary pages such as the Intrusion Event Statistics and Discovery Statistics pages. Entering 0 disables the refresh option. Note that this interval does not apply to dashboards.

- The **Deactivate Rules** field controls which links appear on the packet view of intrusion events generated by standard text rules:

  - **All Policies** - a single link that deactivates the standard text rule in all the locally defined custom intrusion policies

  - **Current Policy** - a single link that deactivates the standard text rule in only the currently deployed intrusion policy. Note that you cannot deactivate rules in the default policies.

  - **Ask** - links for each of these options

To see these links on the packet view, your user account must have either Administrator or Intrusion Admin access.

File Download Preferences

Use the File Preferences section of the Event View Settings page to configure basic characteristics of local file downloads. This section is only available to users with the Administrator, Security Analyst, or Security Analyst (Read Only) user roles.

Note that if your appliance does not support downloading captured files, these options are disabled.

The following fields appear in the File Preferences section:

- The **Confirm 'Download File' Actions** check box controls whether a File Download pop-up window appears each time you download a file, displaying a warning and prompting you to continue or cancel.

⚠

Caution   Cisco strongly recommends you do **not** download malware, as it can cause adverse consequences. Exercise caution when downloading any file, as it may contain malware. Ensure you have taken any necessary precautions to secure the download destination before downloading files.

Note that you can disable this option any time you download a file.

- When you download a captured file, the system creates a password-protected .zip archive containing the file. The **Zip File Password** field defines the password you want to use to restrict access to the .zip file. If you leave this field blank, the system creates archive files without passwords.

- The **Show Zip File Password** check box toggles displaying plain text or obfuscated characters in the **Zip File Password** field. When this field is cleared, the **Zip File Password** displays obfuscated characters.

Default Time Windows

The time window, sometimes called the time range, imposes a time constraint on the events in any event view. Use the Default Time Windows section of the Event View Settings page to control the default behavior of the time window.

User role access to this section is as follows:

- Administrators and Maintenance Users can access the full section.

- Security Analysts and Security Analysts (Read Only) can access all options except **Audit Log Time Window**.

- Access Admins, Discovery Admins, External Database Users, Intrusion Admins, Network Admins, and Security Approvers can access only the **Events Time Window** option.

Note that, regardless of the default time window setting, you can always manually change the time window for individual event views during your event analysis. Also, keep in mind that time window settings are valid for only the current session. When you log out and then log back in, time windows are reset to the defaults you configured on this page.

There are three types of events for which you can set the default time window:

- The **Events Time Window** sets a single default time window for most events that can be constrained by time.

- The **Audit Log Time Window** sets the default time window for the audit log.

- The **Health Monitoring Time Window** sets the default time window for health events.

You can only set time windows for event types your user account can access. All user types can set event time windows. Administrators, Maintenance Users, and Security Analysts can set health monitoring time windows. Administrators and Maintenance Users can set audit log time windows.

Note that because not all event views can be constrained by time, time window settings have no effect on event views that display hosts, host attributes, applications, clients, vulnerabilities, user identity, or compliance allow list violations.

You can either use **Multiple** time windows, one for each of these types of events, or you can use a **Single** time window that applies to all events. If you use a single time window, the settings for the three types of time window disappear and a new **Global Time Window** setting appears.

There are three types of time window:

- *static*, which displays all the events generated from a specific start time to a specific end time

- *expanding*, which displays all the events generated from a specific start time to the present; as time moves forward, the time window expands and new events are added to the event view

- *sliding*, which displays all the events generated from a specific start time (for example, one day ago) to the present; as time moves forward, the time window "slides" so that you see only the events for the range you configured (in this example, for the last day)

The maximum time range for all time windows is from midnight on January 1, 1970 (UTC) to 3:14:07 AM on January 19, 2038 (UTC).

The following options appear in the **Time Window Settings** drop-down list:

- The **Show the Last - Sliding** option allows you configure a sliding default time window of the length you specify.

  The appliance displays all the events generated from a specific start time (for example, 1 hour ago) to the present. As you change event views, the time window "slides" so that you always see events from the last hour.

- The **Show the Last - Static/Expanding** option allows you to configure either a static or expanding default time window of the length you specify.

  For **static** time windows, enable the **Use End Time** check box. The appliance displays all the events generated from a specific start time (for example, 1 hour ago) to the time when you first viewed the events. As you change event views, the time window stays fixed so that you see only the events that occurred during the static time window.

  For **expanding** time windows, disable the **Use End Time** check box. The appliance displays all the events generated from a specific start time (for example, 1 hour ago) to the present. As you change event views, the time window expands to the present time.

- The **Current Day - Static/Expanding** option allows you to configure either a static or expanding default time window for the current day. The current day begins at midnight, based on the time zone setting for your current session.

  For **static** time windows, enable the **Use End Time** check box. The appliance displays all the events generated from midnight to the time when you first viewed the events. As you change event views, the time window stays fixed so that you see only the events that occurred during the static time window.

  For **expanding** time windows, disable the **Use End Time** check box. The appliance displays all the events generated from midnight to the present. As you change event views, the time window expands to the present time. Note that if your analysis continues for over 24 hours before you log out, this time window can be more than 24 hours.

- The **Current Week - Static/Expanding** option allows you to configure either a static or expanding default time window for the current week. The current week begins at midnight on the previous Sunday, based on the time zone setting for your current session.

For **static** time windows, enable the **Use End Time** check box. The appliance displays all the events generated from midnight to the time when you first viewed the events. As you change event views, the time window stays fixed so that you see only the events that occurred during the static time window.

For **expanding** time windows, disable the **Use End Time** check box. The appliance displays all the events generated from midnight Sunday to the present. As you change event views, the time window expands to the present time. Note that if your analysis continues for over 1 week before you log out, this time window can be more than 1 week.

Default Workflows

A workflow is a series of pages displaying data that analysts use to evaluate events. For each event type, the appliance ships with at least one predefined workflow. For example, as a Security Analyst, depending on the type of analysis you are performing, you can choose among ten different intrusion event workflows, each of which presents intrusion event data in a different way.

The appliance is configured with a default workflow for each event type. For example, the Events by Priority and Classification workflow is the default for intrusion events. This means whenever you view intrusion events (including reviewed intrusion events), the appliance displays the Events by Priority and Classification workflow.

You can, however, change the default workflow for each event type. The default workflows you are able to configure depend on your user role. For example, intrusion event analysts cannot set default discovery event workflows.

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.

Specifying Your Default Dashboard

The default dashboard appears when you choose **Overview** > **Dashboards** > **Dashboard**. Unless changed, the default dashboard for all users is the Summary dashboard. You can change the default dashboard if your user role is Administrator, Maintenance, or Security Analyst.

In a multidomain deployment, the default dashboard you choose applies to all domains where your user account has access. When choosing a dashboard for an account that frequently accesses multiple domains, keep in mind that certain dashboard widgets are constrained by domain.

Procedure

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

Step 2 Click **Dashboard Settings**.

Step 3 Choose the dashboard you want to use as your default from the drop-down list.

Step 4 Click **Save**.

Configure How-To Settings

How To is a widget that provides walkthroughs to navigate through tasks on the 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 management center, see Feature Walkthroughs Supported in Secure Firewall Management Center.

Note
- The walkthroughs are generally available for all UI pages, and are not user role sensitive. However, depending on the privileges of the user, some of the menu items will not appear on the management center interface. Thereby, the walkthroughs will not execute on such pages.

- This feature is not available in the Classic theme.

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** > **How-Tos**. You can search for How-To walkthroughs that address tasks of interest. For more information, see Search for How To Walkthroughs.

History for Management Center User Accounts

Feature	Minimum Management Center	Minimum Threat Defense	Details
Added new field for assigning Shell user name template.	7.0.0	Any	Provision to specify a template for CLI access attributes for LDAP external authentication—**Shell User Name Template** was introduced. Thus, CLI attribute would have its own template to identify the LDAP CLI users. New/modified screens: **System**(⚙) > **Users** > **External Authentication**
Added support of Single Sign-On using any SAML 2.0-compliant SSO provider.	6.7.0	Any	Added the ability to support Single Sign-On for external users configured at any third-party SAML 2.0-compliant identity provider (IdP). This includes the ability to map user or group roles from the IdP to management center user roles. Only users with the Admin role authenticated internally or by LDAP or RADIUS can configure SSO. New/modified screens: **System**(⚙) > **Users** > **Single Sign-On**
Themes for the web interface.	6.6.0	Any	You can choose the look and feel of the web interface. Choose the Light or Dusk theme, or use the Classic theme that appeared in previous releases. New/modified screens: User Name > **User Preferences** > **General** > **UI Theme**
Added a new field for name in user accounts.	6.6.0	Any	Added a field that can identify the user or department responsible for an internal user account. New/modified screens: **System**(⚙) > **Users** > **Users**> **Real Name** field
Cisco Security Manager Single Sign-on no longer supported.	6.5.0	Any	Single Sign-on between the management center and Cisco Security Manager is no longer supported as of Firepower 6.5. New/modified screens: **System**(⚙) > **Users**> **CSM Single Sign-on**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Enhanced password security.	6.5.0	Any	New requirements for strong passwords now appear in a single place in this chapter and are cross-referenced from other chapters. New fields in the change password interface added: **Show Password** and **Generate Password**. New/modified screens: User Name > **User Preferences** > **General** > **Change Password**