User Accounts for Management Access

The Firepower Management Center and managed devices include a default **admin** account for management access. This chapter discusses how to create custom user accounts for supported models. See Logging into the Firepower System for detailed information about logging into the Firepower Management Center or a managed device with a user account.

This chapter also describes Cisco Security Manager (CSM) single sign-on when you manage an ASA with CSM and the FirePOWER services module with the Firepower Management Center.

- About User Accounts, on page 1
- Requirements and Prerequisites for User Accounts, on page 5
- Guidelines and Limitations for User Accounts, on page 5
- Add an Internal User Account, on page 6
- Configure External Authentication, on page 10
- Customize User Roles for the Web Interface, on page 28
- Configure Cisco Security Manager Single Sign-on, on page 33
- Troubleshooting LDAP Authentication Connections, on page 34
- History for User Accounts, on page 36

About User Accounts

You can add custom user accounts on the Firepower Management Center and on managed devices, either as internal users or, if supported for your model, as external users on a LDAP or RADIUS server. Each Firepower Management Center and each managed device maintains separate user accounts. For example, when you add a user to the Firepower Management Center, that user only has access to the FMC; 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

Firepower devices support two types of users:

- Internal user—The device checks a local database for user authentication. For more information about internal users, see Add an Internal User Account, on page 6.
- External user—If the user is not present in the local database, the system queries an external LDAP or RADIUS authentication server. For more information about external users, see Configure External Authentication, on page 10.

Web Interface and CLI or Shell Access

When you configure user accounts, you enable web interface access and CLI or shell access separately. Firepower devices include a Firepower CLI that runs on top of Linux. CLI users can also access the Linux shell under TAC supervision or when explicitly instructed by Firepower user documentation. For detailed information about the management UIs, see Firepower System User Interfaces.

Caution On all devices, users with CLI Config level access or shell access can obtain `sudoers` privileges in the Linux shell, which can present a security risk. For system security reasons, we strongly recommend:

- If you establish external authentication, make sure that you restrict the list of users with CLI/shell access appropriately.
- When granting CLI access privileges, restrict the list of users with Config level access.
- Do not add users directly in the Linux shell; only use the procedures in this chapter.
- Do not access Firepower devices using the Linux shell or CLI expert mode unless directed by Cisco TAC or by explicit instructions in the Firepower user documentation.

Each device type supports different forms of access as detailed here:

- For Firepower Threat Defense, ASA FirePOWER, and NGIPSv, CLI access is available for direct management of the device.
  - You can create internal users on these devices using the CLI.
  - You can establish external users on Firepower Threat Defense devices.
  - Users who log into these devices through the management interface access the CLI. Users with CLI Config level access can access the Linux shell using the CLI **expert** command.

Caution We strongly recommend that you do not use the Linux shell unless directed by Cisco TAC or explicit instructions in the Firepower user documentation.

- The FMC has a web interface, a CLI, and Linux shell for direct management of the device.
  - The FMC supports two different internal **admin** users: one for the web interface, and another with CLI or shell access. These two **admin** users are different accounts and do not share the same password. 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/shell **admin**, use the FMC CLI command **configure password**.)
  - FMC internal users added in the web interface have web interface access only.
  - You can grant CLI or shell access to FMC external users.

- On the FMC by default, when any account with shell or CLI access logs in to the management interface, it directly accesses the Linux shell. When you enable the FMC CLI, these users first gain access to the CLI on logging in and may gain access to the shell with the **expert** command. See Firepower Management Center Command Line Reference.

- 7000 and 8000 Series devices have both a web interface and a CLI for direct management of the device.
  - 7000 and 8000 Series device internal users have web interface and CLI access.
  - You can enable CLI or shell access for 7000 and 8000 Series device external users.
  - Users who log into these devices through the management interface access the CLI. Users with CLI Config level access can access the shell using the shell **expert** command.

Caution We strongly recommend that you do not use the Linux shell unless directed by Cisco TAC or explicit instructions in the FMC documentation.

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.

Web Interface User Roles

The 7000 and 8000 Series devices have access to the following user roles: Administrator, Maintenance User, and Security Analyst.

The Firepower 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

Provides read-only access to the Firepower System database using an application that supports JDBC SSL connections. For the third-party application to authenticate to the Firepower System 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.

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.

CLI User Roles

On managed devices, user access to commands in the CLI depends on the role you assign.

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

None

The user cannot log into the device on the command line.

Config

The user can access all commands, including configuration commands. Exercise caution in assigning this level of access to users.

Basic

The user can access non-configuration commands only.

Note External CLI users on managed devices always have the Config user role. For the Firepower Threat Defense when using RADIUS, you can specify either Config or Basic.

Requirements and Prerequisites for User Accounts

Model Support

External user authentication is supported for the following models:

- Firepower Management Center
- Firepower Threat Defense
- 7000 and 8000 Series

Guidelines and Limitations for User Accounts

Defaults

- All devices include 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.
- 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.

Global Settings

By default the following settings apply to all user accounts on the Firepower 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.

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

Add an Internal User Account

Each device maintains separate user accounts. The Firepower Management Center and 7000 and 8000 Series have similar web interfaces. For the Firepower Threat Defense, NGIPSv, and ASA FirePOWER, you must add internal users at the CLI. You cannot add users at the CLI on the Firepower Management Center and 7000 and 8000 Series.

Add an Internal User at the Web Interface

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	FMC 7000 & 8000 Series	Any	Administrator

This procedure describes how to add custom internal user accounts at the web interface of a Firepower Management Center or 7000 & 8000 Series device.

The **System** > **Users** > **Users** shows both internal users that you added manually and external users that were 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.

In a multidomain deployment on the Firepower Management Center, users are only visible in the domain in which they are created. Note that if you add a user in the Global domain, but then assign a user role for a leaf domain, then that user still shows on the Global **Users** page where it was added, even though the user "belongs" to a leaf domain.

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.

When you add a user in a leaf domain, that user is not visible from the global domain.

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

Procedure

Step 1 Choose **System** > **Users**.

Step 2 Click **Create User**.

Step 3 Enter a **User Name**.

The username must comply with the following restrictions:

- Maximum 32 alphanumeric characters, plus hyphen (-), underscore (_) and period (.).
- Letters may be upper or lower case.
- Cannot include any punctuation or special characters other than hyphen (-), underscore (_) and period (.).

Step 4 The **Use External Authentication Method** checkbox is checked for users that were added automatically when they logged in with LDAP or RADIUS. You do not need to pre-configure 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 5 Enter values in the **Password** and **Confirm Password** fields.

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

Step 6 Set the **Maximum Number of Failed Logins**.

Enter an integer, without spaces, that determines 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 enabled security certification compliance.

Step 7 Set the **Minimum Password Length**.

Enter an integer, without spaces, that determines 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 8 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 9 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 10 Set user **Options**.

- **Force Password Reset on Login**—Forces users to change their passwords the next time they log in.
- **Check Password Strength**—Requires strong passwords. A strong password must be at least eight alphanumeric characters of mixed case and must include at least 1 numeric character and 1 special character. It cannot be a word that appears in a dictionary or include consecutive repeating characters.
- **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 11 (7000 or 8000 Series) Assign the appropriate level of **Command-Line Interface Access** as described in CLI User Roles, on page 4.

Note
Unlike for the 7000 or 8000 Series, you cannot enable shell access for Firepower Management Center internal users. (On the FMC you can enable shell access for external users, but we recommend against doing so for system security reasons.)

Step 12 In the **User Role Configuration** area, assign user role(s). For more information about user roles, see Customize User Roles for the Web Interface, on page 28.

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 you see depend on whether the device is in a single domain or multidomain (Firepower Management Center only) deployment.

- Single domain—Check the user role(s) you want to assign the user.
- Multidomain (Firepower Management Center only)—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. See the following steps:

  a. Click **Add Domain**.

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

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

  d. Click **Save**.

Step 13 (Optional, for physical FMCs 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 Overviewfor more information about Lights-Out Management.

Step 14 Click **Save**.

Add an Internal User at the CLI

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Firepower Threat Defense ASA FirePOWER NGIPSv	Any	Config

Use the CLI to create internal users on the Firepower Threat Defense, ASA FirePOWER, and NGIPSv devices. These devices do not have a web interface, so internal (and external) users can only access the CLI for management.

Procedure

Step 1 Log into the device CLI using an account with Config privileges.

The **admin** user account has the required privileges, but any account with Config privileges will work. You can use an SSH session or the Console port.

For certain Firepower Threat Defense models, the Console port puts you into the FXOS CLI. Use the **connect ftd** command to get to the Firepower Threat Defense CLI.

Step 2 Create the user account.

configure user add *username* {**basic** | **config**}

- *username*—Sets the username. The username must be Linux-valid:
  - Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
  - All lowercase
  - Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)
- **basic**—Gives the user basic access. This role does not allow the user to enter configuration commands.
- **config**—Gives the user configuration access. This role gives the user full administrator rights to all commands.

Example:

The following example adds a user account named johncrichton with Config access rights. The password is not shown as you type it.

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton      1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Note
Tell users they can change their own passwords using the **configure password** command.

Step 3 (Optional) Adjust the characteristics of the account to meet your security requirements.

You can use the following commands to change the default account behavior.

- **configure user aging** *username max_days warn_days*

  Sets an expiration date for the user's password. Specify the maximum number of days for the password to be valid followed by the number of days before expiration the user will be warned about the upcoming expiration. Both values are 1 to 9999, but the warning days must be less than the maximum days. When you create the account, there is no expiration date for the password.

- **configure user forcereset** *username*

  Forces the user to change the password on the next login.

- **configure user maxfailedlogins** *username number*

  Sets the maximum number of consecutive failed logins you will allow before locking the account, from 1 to 9999. Use the **configure user unlock** command to unlock accounts. The default for new accounts is 5 consecutive failed logins.

- **configure user minpasswdlen** *username number*

  Sets a minimum password length, which can be from 1 to 127.

- **configure user strengthcheck** *username* {**enable** | **disable**}

  Enables or disables password strength checking, which requires a user to meet specific password criteria when changing their password. When a user's password expires or if the **configure user forcereset** command is used, this requirement is automatically enabled the next time the user logs in.

Step 4 Manage user accounts as necessary.

Users can get locked out of their accounts, or you might need to remove accounts or fix other issues. Use the following commands to manage the user accounts on the system.

- **configure user access** *username* {**basic** | **config**}

  Changes the privileges for a user account.

- **configure user delete** *username*

  Deletes the specified account.

- **configure user disable** *username*

  Disables the specified account without deleting it. The user cannot log in until you enable the account.

- **configure user enable** *username*

  Enables the specified account.

- **configure user password** *username*

  Changes the password for the specified user. Users should normally change their own password using the **configure password** command.

- **configure user unlock** *username*

  Unlocks a user account that was locked due to exceeding the maximum number of consecutive failed login attempts.

Configure External Authentication

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

About External Authentication

When you enable external authentication for management and administrative users of your Firepower system, the device verifies the user credentials with an LDAP or RADIUS server as specified in an *external authentication object*.

External authentication objects can be used by the Firepower Management Center, 7000 and 8000 Series, and Firepower Threat Defense devices. You can share the same object between the different appliance/device types, or create separate objects.

For the FMC, enable the external authentication objects directly on the **System** > **Users** > **External Authentication** tab; this setting only affects FMC usage, and it does not need to be enabled on this tab for managed device usage. For the 7000 and 8000 Series and Firepower 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/shell users in the external authentication object. For CLI/shell users on RADIUS for the 7000 or 8000 Series and the Firepower Management Center, you must pre-configure the list of RADIUS usernames in the external authentication object. For Firepower Threat Defense, you can either define users on the RADIUS server (with the Service-Type attribute), or you can pre-define the user list in the external authentication object like for the other platforms. For LDAP, you can specify a filter to match CLI users on the LDAP server.

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

Note Users with Linux shell access can obtain root privileges, which can present a security risk. Make sure that you:

- restrict the list of users with Linux shell access
- do not create Linux shell users

External Authentication for the Firepower Management Center and 7000 and 8000 Series

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 or shell access. If you have more than one external authentication object enabled, then users can authenticate using only the first object in the list. External CLI users on 7000 or 8000 Series devices always have Config privileges; other user roles are not supported.

External Authentication for the Firepower Threat Defense

For the Firepower Threat Defense, you can only activate one external authentication object.

Only a subset of fields in the external authentication object are used for Firepower Threat Defense SSH access. If you fill in additional fields, they are ignored. If you also use this object for other device types, those fields will be used.

Attention External authentication is not supported on Firepower Threat Defense virtual devices.

LDAP users always have Config privileges. RADIUS users can be defined as either Config or Basic 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.

Firepower 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 Firepower device to support SecurID.

Add an LDAP External Authentication Object

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Firepower Threat Defense 7000 and 8000 Series FMC	Any	Administrator

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

For the Firepower Threat Defense, only a subset of fields are used for CLI access. See Configure External Authentication for SSH for details about which fields are used.

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

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 FMC Management Interfaces or Modify Device Management Interfaces at the CLI 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 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 26 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**, **Shell 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. In the LDAP directory tree, Base DN is the entry that contains the subtree in which your users exists. 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**. To limit the number of authenticated users, extend the Base DN filter by specifying the attribute and value for the user objects. 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 retrieve only active user accounts (excluding the disabled user accounts), enter `(!(userAccountControl:1.2.840.113556.1.4.803:=2))`. This criteria filters user accounts within AD belonging to `ldpgrp` group and with `userAccountControl` attribute value that is not `2` (disabled).

a) 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`.

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

c) (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, you must choose a certificate by clicking **Choose File**.

  If you previously uploaded a certificate and want to replace it, upload the new certificate and redeploy the configuration to your devices to copy over the new certificate.

  Note
  TLS encryption requires a certificate on all platforms. For SSL, the Firepower Threat Defense also requires a certificate. For other platforms, SSL does not require a certificate. However, 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.

- **Timeout**—Enter the number of seconds before rolling over to the backup connection. The default is 30.

Step 12 (Optional) Configure **Attribute Matching** 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 **Shell 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` shell access attribute to retrieve CLI/shell access users by typing `sAMAccountName`.

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

Group controlled access roles allows you to grant privileges to the users belonging to the specified groups. 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.

Note
Configuring group controlled access roles does not limit the filter criteria on the LDAP server. To extend the user filter beyond the Base DN, use the Base Filter option.

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 Firepower 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 **Shell Access Filter** to allow CLI/shell users.

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

- To use the same filter you specified when configuring authentication settings, choose **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 (maximum 450 characters, including the enclosing 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 hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Note
For the 7000 or 8000 Series and Firepower Management Center, do not create any internal users that have the same user name as users included in the **Shell Access Filter**. The only internal FMC user should be **admin**; do not include an **admin** user in the **Shell Access Filter**.

For the Firepower Threat Defense, if you previously configured the same username for an internal user, the Firepower Threat Defense first checks the password against the internal user, and if that fails, it checks the LDAP server. Note that you cannot later add an internal user with the same name as an external user; only pre-existing internal users are supported.

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 Troubleshooting LDAP Authentication Connections, on page 34.

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:

- Firepower Management Center—Enable External Authentication for Users on the Firepower Management Center, on page 25
- Firepower Threat Defense—Configure External Authentication for SSH
- 7000 and 8000 Series—About External Authentication for 7000/8000 Series Devices

Step 19 If you later add or delete users on the LDAP server, you must refresh the user list and redeploy the Platform Settings on managed devices. This step is not required for the Firepower Management Center.

a) Click the **Refresh** (↻) next to each LDAP server.

If the user list changed, you will see a message advising you to deploy configuration changes for your device.

b) For 7000 and 8000 Series devices, make a small configuration change in the Platform Settings so that the settings are marked as Out-of-Date. 7000 and 8000 Series Platform Settings are not automatically marked as Out-of-Date for LDAP shell user list updates.

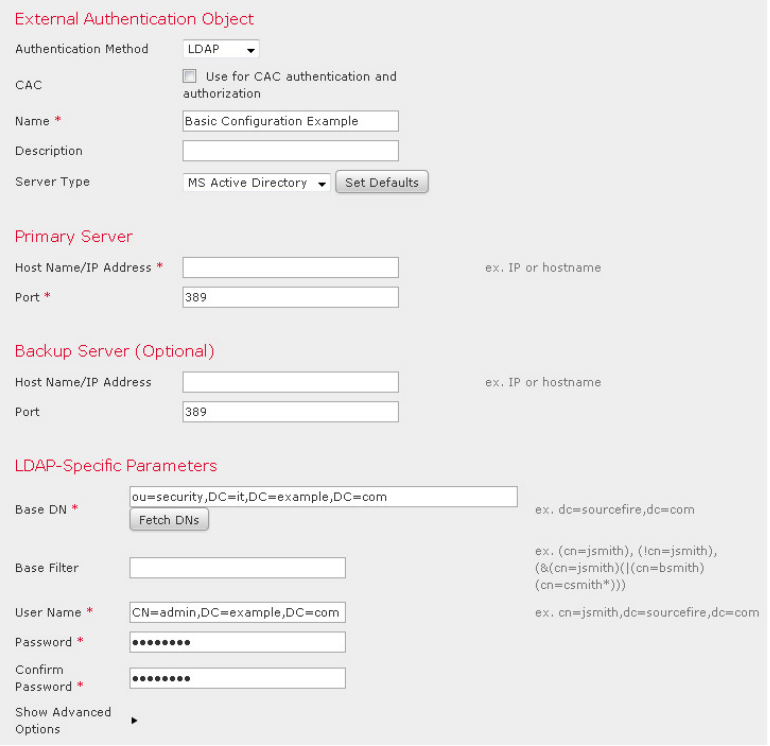
Note that the Firepower Threat Defense Platform Setttings *are* automatically marked as Out-of-Date, so you do not need to perform this workaround.

c) Deploy configuration changes; see Deploy Configuration Changes.

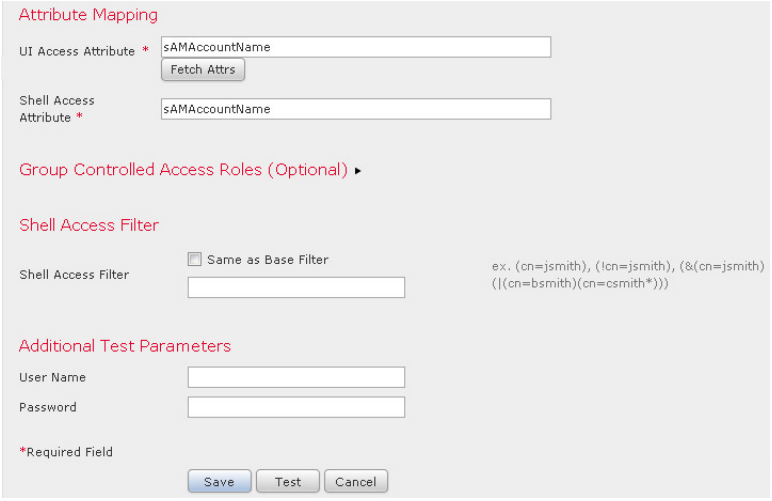
Examples

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.



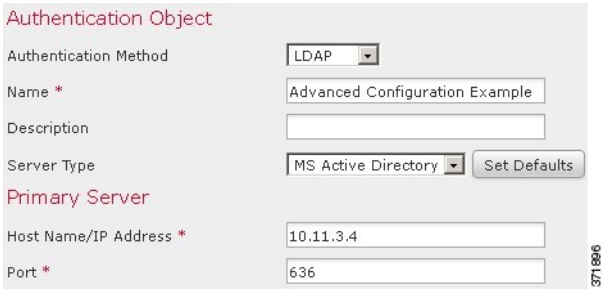
However, because this server is a Microsoft Active Directory server, it uses the `sAMAccountName` attribute to store user names rather than the `uid` attribute. Choosing the MS Active Directory server type and clicking **Set Defaults** sets the UI Access Attribute to `sAMAccountName`. As a result, the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

In addition, a Shell 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 shell or CLI account on the appliance.

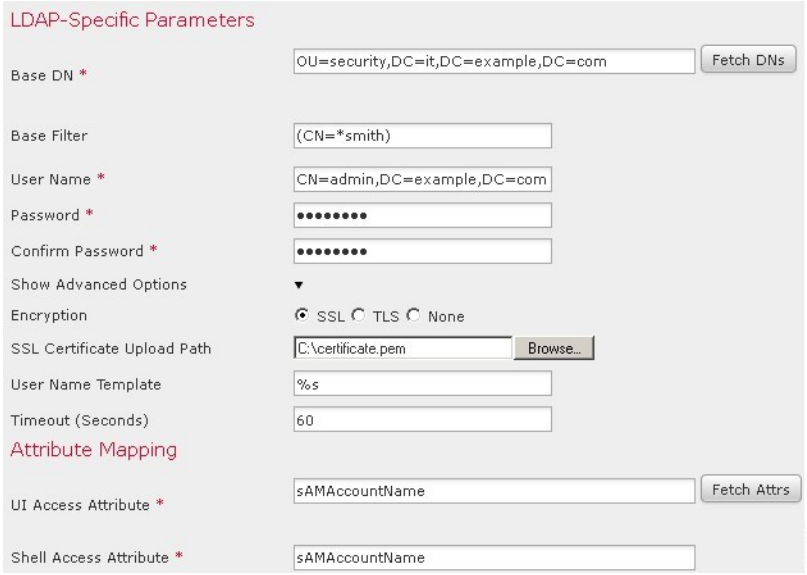
Note that because no base filter is applied to this server, the Firepower System checks attributes for all objects in the directory indicated by the base distinguished name. Connections to the server time out after the default time period (or the timeout period set on the LDAP server).

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`.

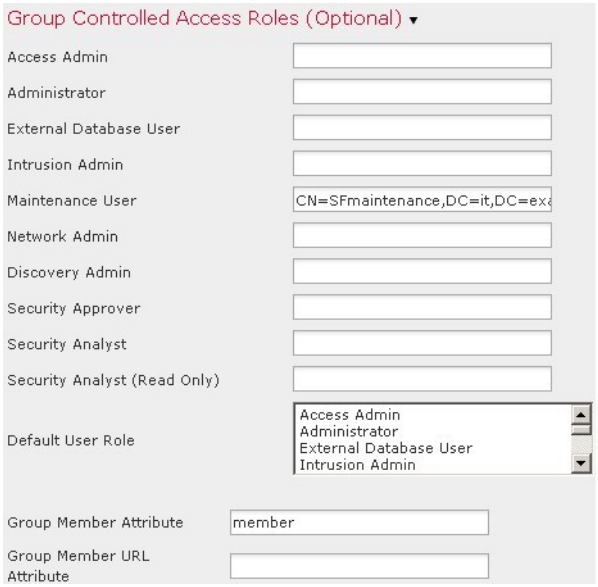


The connection to the server is encrypted using SSL and a certificate named `certificate.pem` is used for the connection. In addition, connections to the server time out after 60 seconds because of the **Timeout** setting.

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 Firepower System checks the `sAMAccountName` attribute for each object for matching user names when a user attempts to log into the Firepower System.

In addition, a Shell 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/shell 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 shell access filter is set to be the same as the base filter, so the same users can access the appliance through the shell or CLI as through the web interface.

Add a RADIUS External Authentication Object

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Firepower Threat Defense 7000 and 8000 Series FMC	Any	Administrator

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

For the Firepower Threat Defense, only a subset of fields are used for CLI access. See Configure External Authentication for SSH for details about which fields are used.

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 External Authentication Object**.

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

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

Step 6 For the **Primary Server**, enter a **Host Name/IP Address**.

Step 7 (Optional) Change the **Port** from the default.

Step 8 Enter the **RADIUS Secret Key**.

Step 9 (Optional) Enter the **Backup Server** parameters.

Step 10 (Optional) Enter **RADIUS-Specific Parameters**.

a) Enter the **Timeout** in seconds before retrying the primary server. The default is 30.

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 11 (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 12 (Optional) (7000 or 8000 Series and Firepower Management Center) In the **Shell Access Filter** area **Administrator Shell Access User List** field, enter the user names that should have CLI/shell 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 hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

For the Firepower Threat Defense, you can optionally use this method to define CLI users, or you can instead define CLI users on the RADIUS server by setting the Service-Type attribute for each user. For more information about the Service-Type attribute, see Configure External Authentication for SSH. You may want to use the **Shell Access Filter** method for Firepower Threat Defense so you can use the same external authentication object with Firepower Threat Defense and other platform types. Note that if you want to use RADIUS-defined users, you must leave the **Shell Access Filter** empty.

To use the same RADIUS server for the Firepower Threat Defense, 7000 or 8000 Series, and FMC while using the Service-Type attribute method for the Firepower Threat Defense, create two external authentication objects that identify the same RADIUS server: one object includes the predefined **Shell Access Filter** users (for use with the FMC and the 7000 or 8000 Series), and the other object leaves the **Shell Access Filter** empty (for use with Firepower Threat Defenses).

To prevent RADIUS authentication of CLI/shell access for 7000 or 8000 Series and Firepower Management Center users, leave the field blank.

Note
For the 7000 or 8000 Series and Firepower Management Center, remove any internal users that have the same user name as users included in the shell access filter. For the Firepower Management Center, the only internal CLI/shell user is **admin**, so do not also create an **admin** external user.

For the Firepower Threat Defense, if you previously configured the same username for an internal user, the Firepower Threat Defense first checks the password against the internal user, and if that fails, it checks the RADIUS server. Note that you cannot later add an internal user with the same name as an external user; only pre-existing internal users are supported.

Step 13 (Optional) Click **Test** to test FMC connectivity to the RADIUS server.

This function can only test FMC connectivity to the RADIUS server; there is no test function for managed device connectivity to the RADIUS server.

Step 14 (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 15 Click **Save**.

Step 16 Enable use of this server:

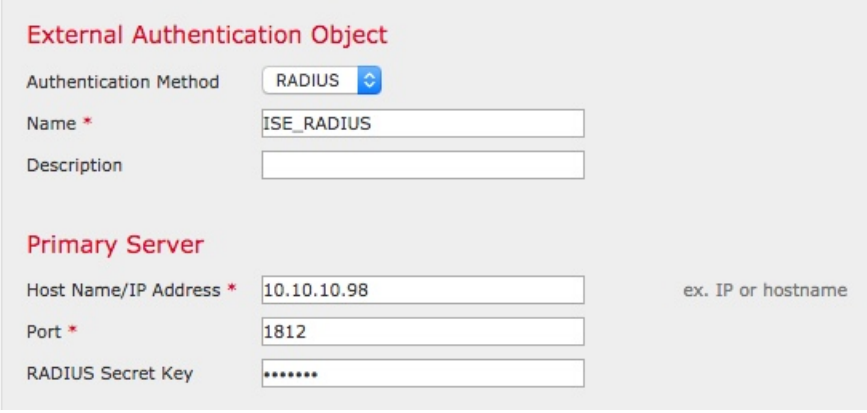
- Firepower Management Center—Enable External Authentication for Users on the Firepower Management Center, on page 25
- Firepower Threat Defense—Configure External Authentication for SSH
- 7000 and 8000 Series—About External Authentication for 7000/8000 Series Devices

---

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 Firepower System attempts to contact the backup server, if any.

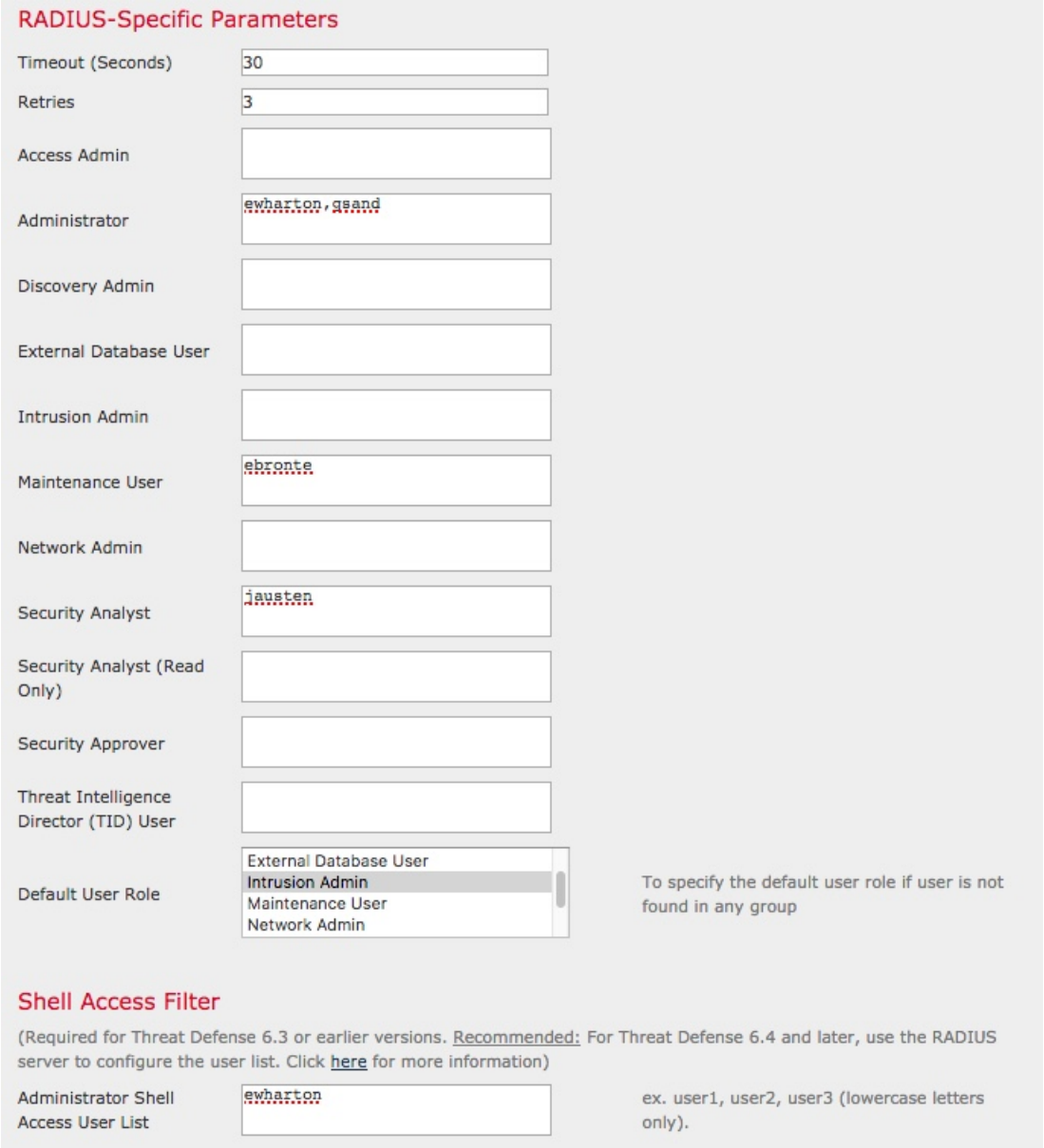
This example illustrates important aspects of RADIUS user role configuration:

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/shell account.



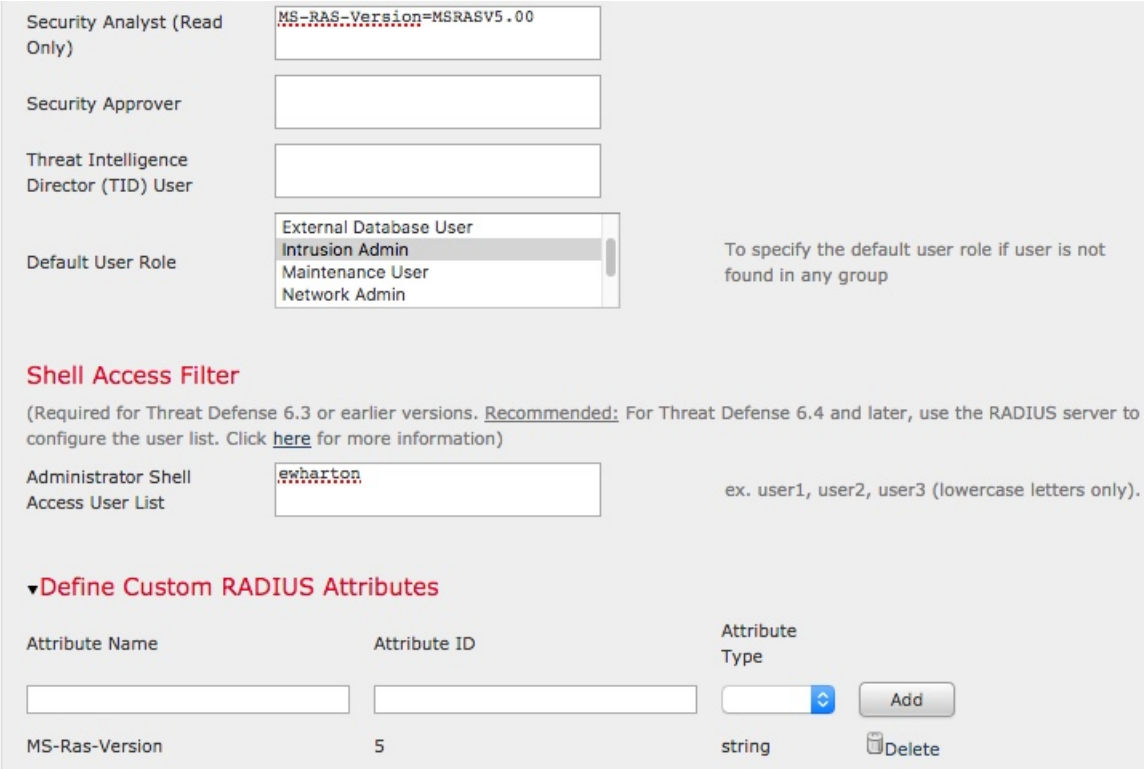
The following graphic depicts the role configuration for the example:

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 Firepower Management Center

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	FMC	Any	Admin

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

Before you begin

Add 1 or more external authentication objects according to Add an LDAP External Authentication Object , on page 12 and Add a RADIUS External Authentication Object, on page 20.

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 Roles** 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 **Shell Access Filter**. Also, CLI/shell 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/shell access for external users.

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/shell

Step 7 Click **Save and Apply**.

Enable External Authentication for Users on Managed Devices

Enable External Authentication in the device Platform Settings, and then deploy the settings to the managed devices. See the following procedures for your managed device type:

- Firepower Threat Defense—Configure External Authentication for SSH
- 7000 and 8000 Series—About External Authentication for 7000/8000 Series Devices

Attention External authentication is not supported on Firepower Threat Defense virtual devices.

Configure Common Access Card Authentication with LDAP

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	FMC 7000 and 8000 Series	Any	Administrator Network Admin

If your organization uses Common Access Cards (CACs), you can configure LDAP authentication to authenticate FMC or 7000 and 8000 Series users logging into 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 , on page 12. 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 Firepower Management Center, on page 25 or Enable External Authentication to 7000/8000 Series Devices.

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

Step 13 Log into the device according to Logging Into the Firepower Management Center with CAC Credentials or Logging Into a 7000 or 8000 Series Device with CAC Credentials.

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 Web Interface User Roles, on page 3.

Note CLI/shell user roles for managed devices are limited to Config and Basic roles. See CLI User Roles, on page 4 for more information.

Create Custom User Roles

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	FMC 7000 & 8000 Series	Any	Administrator

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 device.

Caution Users with menu-based User Management permissions have the ability to elevate their own privileges or create new user accounts with extensive privileges, including the Administrator user role. For system security reasons we strongly recommend you restrict the list of users with User Management permissions appropriately.

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 device:
  a. On the old device, click the **Export** ( ) to save the role to your PC.
  b. On the new device, choose **System** > **Tools** > **Import/Export**.
  c. Click **Upload Package**, then follow the instructions to import the saved user role to the new device.

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

Step 5 (Optional) Add a **Description**.

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** 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 device, 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 31.

Step 9 Click **Save**.

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: Example Access Control Custom Roles

Custom Role Permission	Example: Access Control Editor	Example: Intrusion & Network Analysis Editor	Example: Policy Approver
Access Control	yes	no	yes
Access Control Policy	yes	no	yes
Modify Access Control Policy	yes	no	no
Intrusion Policy	no	yes	yes
Modify Intrusion Policy	no	yes	no
Deploy Configuration to Devices	no	no	yes

Deactivate User Roles

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	FMC 7000 & 8000 Series	Any	Administrator

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

For the Firepower Management Center, 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 31. Only one user role at a time can be the escalation target role.

Step 2 Configure a Custom User Role for Escalation, on page 32.

Step 3 (For the logged in user) Escalate Your User Role, on page 32.

Set the Escalation Target Role

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	FMC	Any	Administrator

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

Smart License	Classic License	Supported Device	Supported Domains	Access
Any	Any	FMC	Any	Administrator

Users for whom you want to enable escalation must belong to a custom user role with escalation enabled. This procedure describes how to enable escaltion 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 Set the Escalation Target Role, on page 31.

Procedure

Step 1 Begin configuring your custom user role as described in Create Custom User Roles, on page 28.

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

Smart License	Classic License	Supported Device	Supported Domains	Access
Any	Any	FMC	Any	Any

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.

Configure Cisco Security Manager Single Sign-on

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	ASA FirePOWER	Any	Administrator

Single sign-on enables integration between Cisco Security Manager (CSM) Version 4.7 or higher and the Firepower Management Center, which allows you to access the Firepower Management Center from CSM without additional authentication to log in. When managing an ASA with the ASA FirePOWER module, you may want to modify the policies deployed to the module. You can select the managing Firepower Management Center in CSM and launch it in a web browser.

Note You cannot log in with single sign-on if your organization uses CACs for authentication.

Before you begin

- In NAT environments, the Firepower Management Center and CSM must reside on the same side of the NAT boundary.

Procedure

Step 1 From CSM, generate a single sign-on shared encryption key that identifies the connection. See your CSM documentation for more information.

Step 2 From the Firepower Management Center, choose **System** > **Users**.

Step 3 Choose **CSM Single Sign-on**.

Step 4 Enter the **CSM hostname** or **IP** address and the server **Port**.

Step 5 Enter the **Shared key** that you generated from CSM.

Step 6 (Optional) Click the **Use Proxy For Connection** check box if you want to use the Firepower Management Center's proxy server to communicate with CSM.

Step 7 Click **Submit**.

Step 8 Click **Confirm Certificate** to save the Certificate.

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 the user has 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 shell 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 shell access filter, make sure that the filter is enclosed in parentheses and that you are using a valid comparison operator.
- 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 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 shell access filter or use a more restrictive or less restrictive base DN.

History for User Accounts

Feature	Version	Details
Support for the Service-Type attribute for Firepower Threat Defense users defined on the RADIUS server	6.4	For RADIUS authentication of Firepower Threat Defense CLI users, you used to have to pre-define the usernames in the RADIUS external authentication object and manually make sure that the list matched usernames defined on the RADIUS server. You can now define CLI users on the RADIUS server using the Service-Type attribute and also define both Basic and Config user roles. To use this method, be sure to leave the shell access filter blank in the external authentication object. New/Modified screens: **System** > **Users** > **External Authentication** > **Add External Authentication Object** > **Shell Access Filter** Supported platforms: Firepower Threat Defense
External Authentication for Firepower Threat Defense SSH Access	6.2.3	You can now configure external authentication for SSH access to the Firepower Threat Defense using LDAP or RADIUS. New/Modified screens: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: Firepower Threat Defense