# Users

Managed devices include a default **admin** account for CLI access. This chapter discusses how to create custom user accounts.

# About Users

You can add custom user accounts on managed devices, either as internal users or as external users on a LDAP or RADIUS server. Each managed device maintains separate user accounts. For example, when you add a user to the FMC, 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.
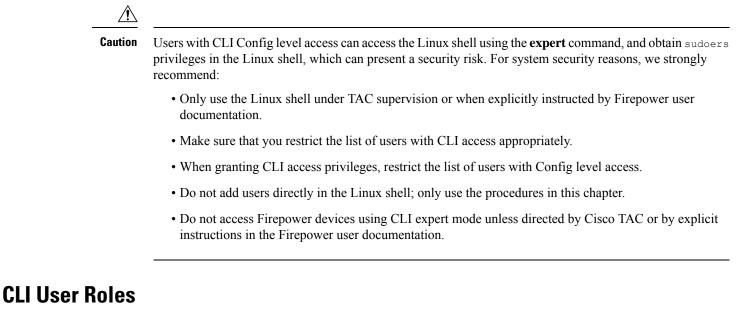
## Internal and External Users

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.

## CLI Access

Firepower devices include a Firepower CLI that runs on top of Linux. You can create internal users on devices using the CLI. You can establish external users on FTD devices using the FMC.

⚠️

**Caution**  Users with CLI Config level access can access the Linux shell using the **expert** command, and obtain `sudoers` privileges in the Linux shell, which can present a security risk. For system security reasons, we strongly recommend:

- Only use the Linux shell under TAC supervision or when explicitly instructed by Firepower user documentation.

- Make sure that you restrict the list of users with CLI 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 CLI expert mode unless directed by Cisco TAC or by explicit instructions in the Firepower user documentation.

# CLI User Roles

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

**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. Only internal users and FTD external RADIUS users support the Basic role.

# Requirements and Prerequisites for User Accounts for Devices

**Model Support**

- FTD—Internal and external users

**Supported Domains**

Any

**User Roles**

Configure external users—Admin FMC user

Configure internal users—Config CLI user

# Guidelines and Limitations for User Accounts for Devices

**Usernames**

- You cannot add the same username for both internal and external users. If the external server uses a duplicate username, the deployment to the device fails.

- 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 (/)

**Defaults**

All devices include an **admin** user as a local user account; you cannot delete the **admin** user. The default initial password is **Admin123**; the system forces you to change this during the initialization process. The agent stores the modified credentials in the Windows registry and uses the same encryption as the FMC, which is Cipher Block Chaining (CBC). See the getting started guide for your model for more information about system initialization.

# Add an Internal User at the CLI

Use the CLI to create internal users on the FTD.

**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 FTD models, the Console port puts you into the FXOS CLI. Use the **connect ftd** command to get to the FTD 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.

  **Caution**
  Do not use the Linux **passwd** command in Expert Mode to change the admin user password. This command can cause file system corruption. Only use the regular FTD CLI **configure user password admin** command (if you are not admin) or **configure password** command (if you are admin). If you don't know the password and can't log in at all, see the password recovery procedure.

- **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 for the FTD

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

## About External Authentication for the FTD

When you enable external authentication for FTD users, the FTD 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 FMC and FTD devices. You can share the same object between the different appliance/device types or create separate objects. For the FTD, you can only activate one external authentication object in the platform settings that you deploy to the devices.

**Note**   The timeout range is different for the FTD and the FMC, so if you share an object, be sure not to exceed the FTD'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 FTD external authentication configuration will not work.

Only a subset of fields in the external authentication object are used for FTD 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.

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

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. For LDAP, you can specify a filter to match CLI users on the LDAP server.

> **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 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.

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 for FTD

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

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

**Sharing External Authentication Objects**

External LDAP objects can be used by the FMC and FTD devices. You can share the same object between the FMC and devices or create separate objects. Be sure that both the FTD and the FMC can reach the LDAP server, even if you are not sharing the object. The FMC is essential to retrieving the user list and downloading it to the device.

**Note** For LDAP, the timeout range is different for the FTD and the FMC, so if you share an object, be sure not to exceed the FTD's smaller timeout range (1-30 seconds). If you set the timeout to a higher value, the deployment to the FTD will fail.

**FTD Supported Fields**

Only a subset of fields in the LDAP object are used for FTD SSH access. If you fill in additional fields, they are ignored. If you also use this object for the FMC, those fields will be used. This procedure only covers the supported fields for the FTD. For other fields, see Add an LDAP External Authentication Object for the FMC.

**Usernames**

Usernames must be Linux-valid usernames and be lower-case only, using alphanumeric characters plus period (.) or hyphen (-). Other special characters such as at sign (@) and slash (/) are not supported. You cannot add the **admin** user for external authentication. You can only add external users (as part of the External Authentication object) in the FMC; you cannot add them at the CLI. Note that internal users can only be added at the CLI, not in the FMC.

If you previously configured the same username for an internal user using the **configure user add** command, the FTD 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.

**Privilege Level**

LDAP users always have Config privileges.

**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 FTD Management Interfaces at the CLI to add DNS servers.

**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** | Enter a **Name** and optional **Description**. |
| **Step 6** | Choose a **Server Type** from the drop-down list. |
| **Step 7** | 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 8** | (Optional) Change the **Port** from the default. |
| **Step 9** | (Optional) Enter the **Backup Server** parameters. |

**Step 10**     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)`.

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, 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 FTD 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.

- (Not Used) **User Name Template**—Not used by the FTD.

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

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

**Step 11**     Configure **Attribute Mapping** to retrieve users based on an attribute.

- Enter a **UI Access Attribute**. **Note**: This field is not used for device CLI access; however, it is a required field, so you need to enter a value. You can just enter the same value that you enter for the **CLI Access Attribute**.

- Set the **CLI Access Attribute** if you want to use a CLI 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`.

    **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**

Deploying an external authentication object that allows a large number of users with CLI access may cause deployments to time out and fail while waiting for the users to be created.

**Step 12** Set the **CLI Access Filter**.

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 hyphen (-) and underscore (_)

- All lowercase

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

**Note**

If you previously configured the same username for an internal user, the FTD 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 13** Click **Save**.

**Step 14** Enable use of this server. See External Authentication.

**Step 15** If you later add or delete users on the LDAP server, you must redeploy the Platform Settings on managed devices. The FMC redownloads the user list and deploys it to the device. 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.

## External Authentication Object

| | |
|---|---|
| Authentication Method | LDAP ▾ |
| CAC | ☐ Use for CAC authentication and authorization |
| Name * | Basic Configuration Example |
| Description | |
| Server Type | MS Active Directory ▾ |
| | Set Defaults |

### Primary Server

| | | |
|---|---|---|
| Host Name/IP Address * | | ex. IP or hostname |
| Port * | 389 | |

### Backup Server (Optional)

| | | |
|---|---|---|
| Host Name/IP Address | | ex. IP or hostname |
| Port | 389 | |

### LDAP-Specific Parameters

| | | |
|---|---|---|
| Base DN * | ou=security, DC=it, DE=example, C | ex. dc=sourcefire,dc=com |
| | Fetch DNs | |
| Base Filter | | 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

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.

Attribute Mapping

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

▸ Group Controlled Access Roles (Optional)

CLI Access Filter

| | | | |
|---|---|---|---|
| CLI Access Filter ⓘ | ☐ Same as Base Filter | | ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(!)(cn=bsmith)(cn=csmith*))) |
| (Mandatory for FTD devices) | | | |

Additional Test Parameters

| | |
|---|---|
| User Name | |
| Password | |

*Required Field

Cancel    Test    Save

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 the FTD.

Note that because no base filter is applied to this server, the FTD 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.

External Authentication Object

| | |
|---|---|
| Authentication Method | LDAP ▾ |
| CAC | ☐ Use for CAC authentication and authorization |
| Name * | Advanced Configuration Example |
| Description | |
| Server Type | MS Active Directory ▾   Set Defaults |

Primary Server

| | | |
|---|---|---|
| Host Name/IP Address * | 10.11.3.4 | ex. IP or hostname |
| Port * | 636 | |

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 (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.

The **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 the FTD.

In the following example, the CLI access filter is set to be the same as the base filter.



# Add a RADIUS External Authentication Object for FTD

Add a RADIUS server to support external users for the FTD.

**Sharing External Authentication Objects**

You can share the same object between the FMC and devices or create separate objects. Note that the FTD supports defining users on the RADIUS server, while the FMC requires you to predefine the user list in the external authentication object. You can choose to use the predefined list method for the FTD, but if you want to define users on the RADIUS server, you must create separate objects for the FTD and the FMC.

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

**FTD Supported Fields**

Only a subset of fields in the RADIUS object are used for FTD SSH access. If you fill in additional fields, they are ignored. If you also use this object for the FMC, those fields will be used. This procedure only covers the supported fields for the FTD. For other fields, see Add a RADIUS External Authentication Object for FMC in the Firepower Management Center Administration Guide.

**Usernames**

You cannot add the **admin** user for external authentication. You can only add external users (as part of the External Authentication object) in the FMC; you cannot add them at the CLI. Note that internal users can only be added at the CLI, not in the FMC.

If you previously configured the same username for an internal user using the **configure user add** command, the FTD 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. For users defined on the RADIUS server, be sure to set the privilege level to be the same as any internal users; otherwise you cannot log in using the external user password.

**Procedure**

**Step 1**     Define users on the RADIUS server using the Service-Type attribute.

The following are supported values for the Service-Type attribute:

- Administrator (6)—Provides Config access authorization to the CLI. These users can use all commands in the CLI.

- NAS Prompt (7) or any level other than 6—Provides Basic access authorization to the CLI. These users can use read-only commands, such as **show** commands, for monitoring and troubleshooting purposes.

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 sign (@) or slash (/)

Alternatively, you can predefine users in the external authentication object (see, Step 12, on page 14). To use the same RADIUS server for the FTD and FMC while using the Service-Type attribute method for the FTD, create two external authentication objects that identify the same RADIUS server: one object includes the predefined **CLI Access Filter** users (for use with the FMC), and the other object leaves the **CLI Access Filter** empty (for use with FTDs).

**Step 2**     In the FMC, choose **System** (⚙) > **Users**.

**Step 3**     Click **External Authentication**.

**Step 4**     Click  (➕)**Add External Authentication Object**.

**Step 5**     Set the **Authentication Method** to **RADIUS**.

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

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

Only IPv4 is supported.

**Note**

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.

**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 (Seconds)** in seconds before retrying the primary server, between 1 and 300. The default is 30.

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

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

**Step 12**    (Optional) Instead of using RADIUS-defined users (see, Step 1, on page 13), in the **CLI Access Filter** area **Administrator CLI Access User List** field, enter the user names that should have CLI access, separated by commas. For example, enter `jchrichton, aerynsun, rygel`.

You may want to use the **CLI Access Filter** method for FTD so you can use the same external authentication object with FTD and other platform types.

**Note**
If you want to use RADIUS-defined users, you must leave the **CLI Access Filter** empty.

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 (/)

**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**
Deploying an external authentication object that allows a large number of users with CLI access may cause deployments to time out and fail while waiting for the users to be created.

**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. See External Authentication

---

**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 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 FTD Devices

Enable External Authentication in the Threat Defense Platform Settings, and then deploy the settings to the managed devices. See External Authentication for more information.

# 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 Firepower Threat Defense device identifies the second reset packet as part of a new connection request and logs the connection with Block action.

# History for Users

| Feature | Minimum FMC | Minimum FTD | Details |
|---|---|---|---|
| Support for the Service-Type attribute for FTD users defined on the RADIUS server. | 6.4.0 | Any | For RADIUS authentication of FTD 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.<br><br>New/modified screens: **System(⚙)** > **Users** > **External Authentication** > **Add External Authentication Object** > **Shell Access Filter** |
| External authentication for FTD SSH access. | 6.2.3 | Any | You can now configure external authentication for SSH access to the FTD using LDAP or RADIUS.<br><br>New/modified screens: **Devices** > **Platform Settings** > **External Authentication** |