MANAGING FIREWALL ADMINISTRATOR ACCOUNTS

TREAT YOUR ACCOUNT LIKE A TOOTHBRUSH: DON'T LET ANYONE ELSE USE IT

- Firewall authentication and authorization
- Create a local firewall administrator account
- Create a non-local firewall administrator account
- Create a firewall administrator account for non-interactive login

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Learning Objectives

After you complete this module,
you should be able to:

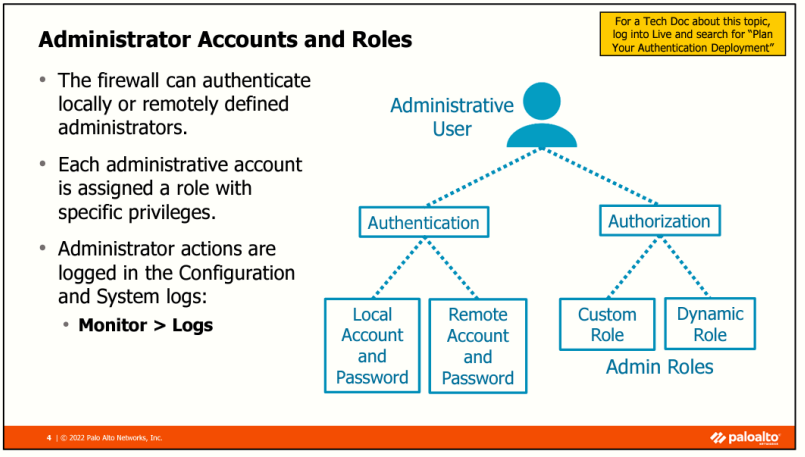
- Describe the firewall authentication and authorization process and firewall components
- Create a local firewall administrator account
- Create a non-local firewall administrator account
- Create a firewall account that supports non-interactive login

This module covers the topics listed here. Read through the list before proceeding.

After you complete this module, you should be able to:

- Describe the firewall authentication and authorization process and firewall components
- Create a local firewall administrator account
- Create a non-local firewall administrator account
- Create a firewall account that supports non-interactive login

This section describes firewall authentication and authorization concepts.



By default, only the predefined *admin* account has access to the firewall. However, you can add administrator accounts to the firewall for delegation and auditing purposes. Each additional administrator account you create can have its own set of administrative privileges. Specify administrative privileges by creating one or more Admin Role Profiles with specific sets of privileges, and then assign an Admin Role Profile to each administrator account.

PAN-OS® software provides flexibility when administrator accounts and admin roles are created. You can create and manage accounts and admin roles locally on the firewall or incorporate a supported authentication, authorization, and accounting service. PAN-OS software supports remote user accounts in Active Directory, Kerberos, LDAP, RADIUS, TACACS+, and SAML. PAN-OS software supports remote role assignment in RADIUS or TACACS+ using Vendor-Specific Attributes (VSAs).

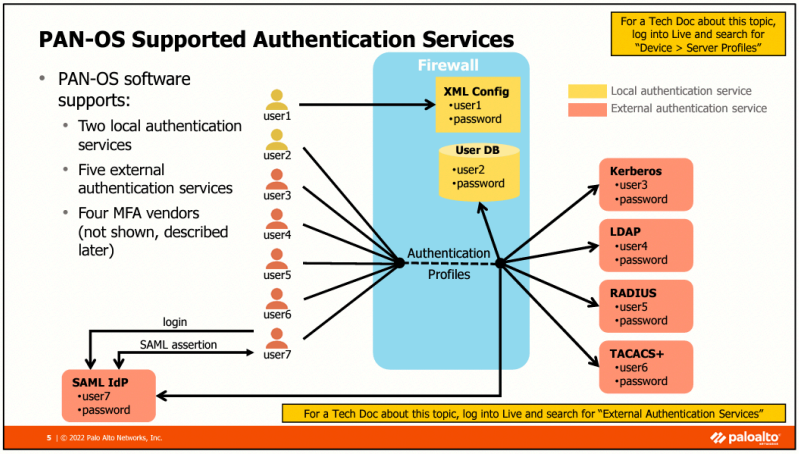
No matter which user makes changes to the running configuration, all changes are logged in the firewall's System and Configuration logs. The System log records the time when an administrator logs in, and the Configuration log records any changes that they make.

To create a local administrator account:

1. Create an Admin Role Profile.
2. Create a local administrator account.

To create a non-local administrator account:

1. Create an Admin Role Profile.
2. Create a Server Profile.
3. Create an Authentication Profile.
4. Create an authentication sequence (optional).
5. Create a non-local administrator account.



PAN-OS software supports three types of authentication services: local, external, and multi-factor authentication (or MFA).

The local authentication services are labeled "local" because they operate on the firewall itself. There are two local authentication services: local without a database and local with a database.

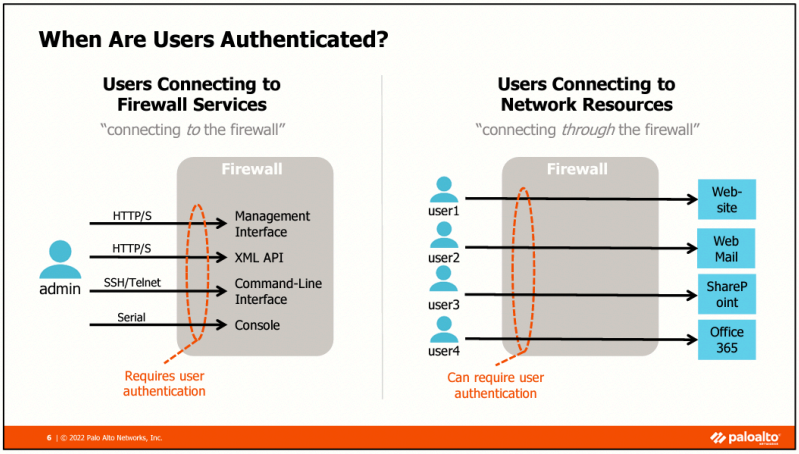
In local authentication without a database, the administrator's username and password information is stored on the firewall in the XML configuration file of the firewall. User accounts stored in the XML configuration file can be used only to authenticate logins to the firewall. The firewall cannot use this type of authentication service to authenticate user traffic flowing *through* the firewall.

In local authentication with a database, username and password information is stored on the firewall in a local user database. The firewall can use this service to authenticate logins *to* the firewall and user traffic flowing *through* the firewall.

The external authentication services are labeled "external" because they operate outside of the firewall. Five external authentication services are supported: Kerberos, LDAP, RADIUS, TACACS+, and SAML. The firewall can use all these services to authenticate logins *to* the firewall and user traffic flowing *through* the firewall.

You can configure Multi-Factor Authentication (MFA) to ensure that each user authenticates using multiple methods (factors) when accessing highly sensitive services and applications. For example, you can force administrators to enter a login name and password and then enter a verification code that they receive by phone before allowing the administrator to access the web management interface of the firewall. This approach helps to prevent attackers from gaining access to the firewall or through the firewall. PAN-OS software supports four MFA vendors.

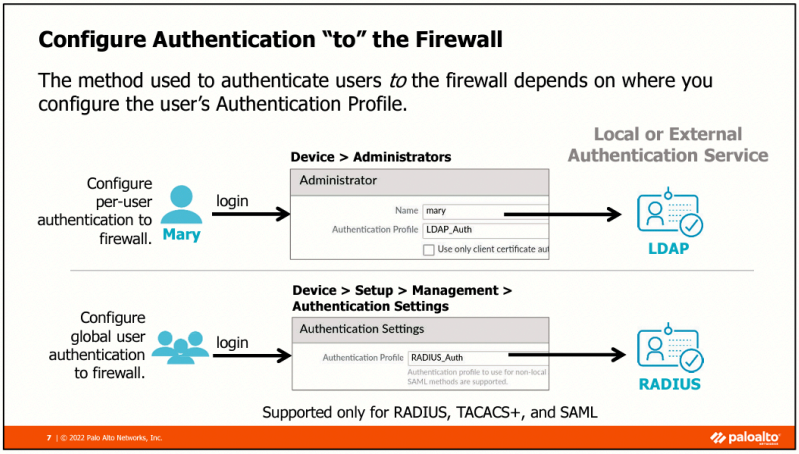
Notice that every authentication service except the local-without-a-database service requires an Authentication Profile. The firewall uses an Authentication Profile to link a set of users to a specific authentication service. Only those authentication services that use an Authentication Profile can authenticate user traffic flowing *through* the firewall.



The firewall authenticates users in two scenarios. First, the firewall authenticates any administrative user connecting to the firewall to access firewall services, such as the firewall web interface. Second, you can configure the firewall to authenticate users trying to access network resources *through* a firewall, such as user1 accessing the internet.

In the first scenario, the firewall verifies user credentials before granting access to services running on the firewall. In the example, the firewall prompts the user *admin* for their credentials before the firewall grants access to the web interface or XML API interface, the command-line interface, or the console port.

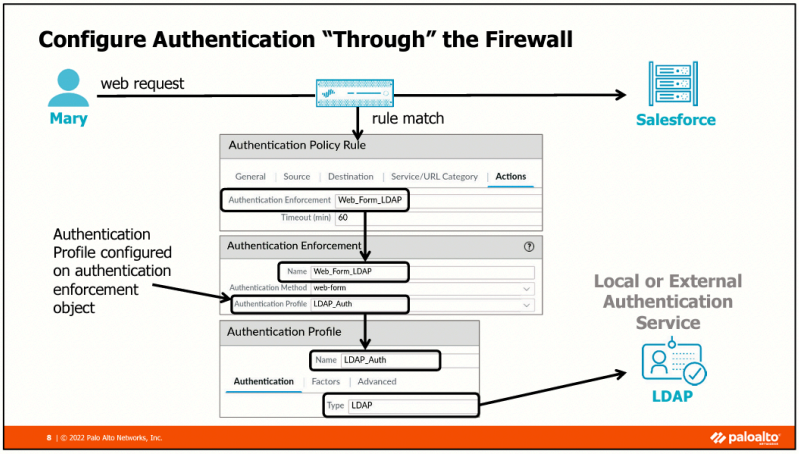
In the second scenario, the firewall can be configured through an Authentication policy to prompt users for their credentials before the firewall grants access to network services. In the example, the firewall prompts user1 for their credentials before it will grant the user access to the website.



The method used to authenticate users to the firewall depends on where you configure the Authentication Profile of the user. An Authentication Profile defines the authentication service that validates the login credentials. You can configure each user individually on the firewall with their own Authentication Profile that points to an authentication service. Or you can configure all users on a firewall to use the same Authentication Profile and authentication service.

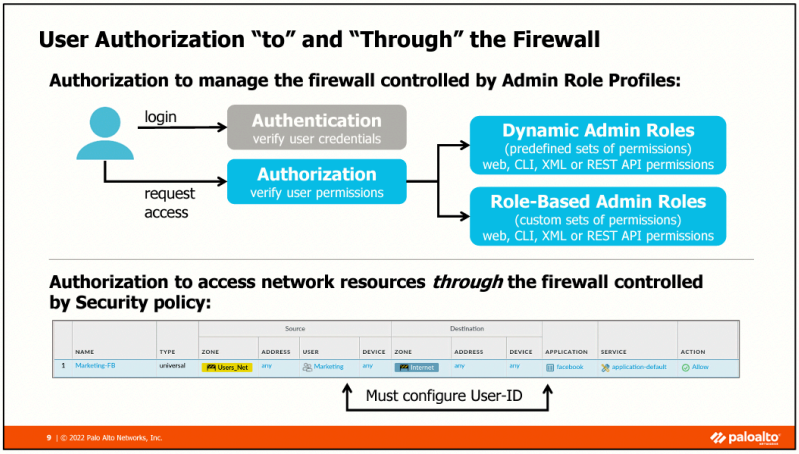
To individually configure each user with an authentication service, assign an Authentication Profile to a user account when you add the user account to the firewall. In the example, the user Mary is assigned the Authentication Profile **LDAP_Auth**, which directs the firewall to use an external LDAP service to authenticate Mary's credentials.

To configure the firewall to authenticate all users using the same authentication service, assign an Authentication Profile to the authentication settings of the firewall. In the example, the Authentication Profile **Radius_Auth** is assigned to the authentication settings of the firewall. All users will have their credentials authenticated by RADIUS. You are allowed to configure the authentication settings of a firewall to only use RADIUS, TACACS+, or SAML. SAML can authenticate only users using web-based services.



You also can configure the firewall to authenticate user credentials when users attempt to access network resources *through* the firewall. In this scenario, you do not assign an Authentication Profile to an individual user or to the authentication settings of the firewall. Instead, you assign an Authentication Profile to an Authentication policy via an authentication enforcement object. This configuration is shown here.

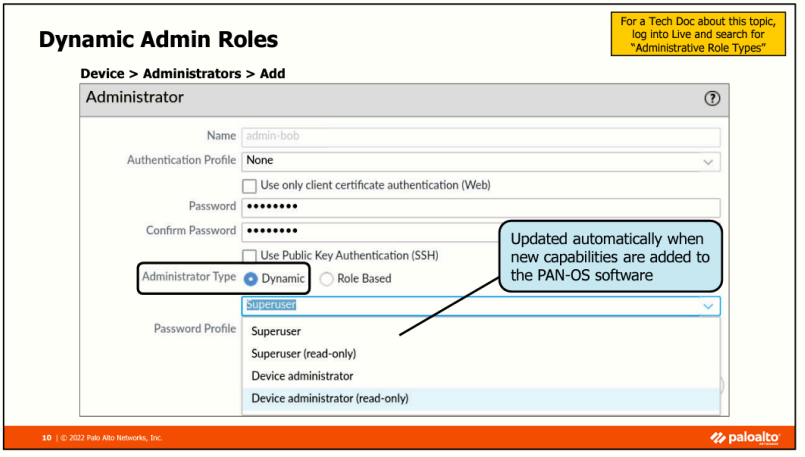
In the example, Mary attempts to access Salesforce through the firewall. The web request matches a rule in the Authentication policy. The rule's action is to invoke an authentication enforcement object labeled **Web-Form-LDAP**. The **Web-Form-LDAP** object is linked to an Authentication Profile labeled **LDAP_Auth** that in turn is linked to an external LDAP service. The firewall will prompt Mary for her credentials and then authenticate those credentials using the LDAP service.



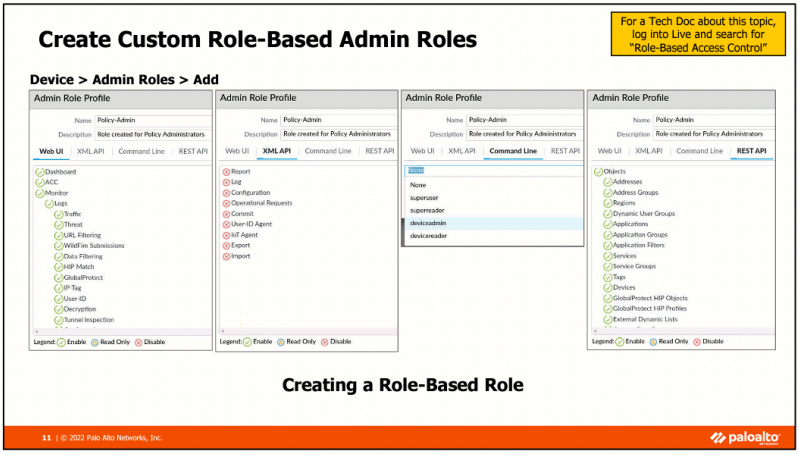
After authentication, a user connecting *to* the firewall will attempt to view information or modify configuration settings. Authorization to perform activities on the firewall is granted to users through Admin Role Profiles. An Admin Role Profile contains a set of permissions that is granted to a user when an Admin Role Profile is assigned to the user.

There are two types of Admin Role Profiles. Dynamic Admin Role Profiles are built-in and have a predefined sets of permissions. These permissions control what a user can or cannot do on a firewall using the web interface, CLI commands, using XML API, or the REST API. When new features are added, the firewall automatically updates the definitions of dynamic roles; you never need to manually update them. Role-Based Admin Role Profiles are custom roles you can configure for more granular access control over the functional areas of the web interface, CLI commands, XML API, and REST API. For example, you can create an Admin Role profile for your operations staff that provides access to the firewall and network configuration areas of the web interface and a separate profile for your security administrators that provides access to security policy definitions, logs, and reports.

If you have configured user authentication of traffic flowing *through* the firewall to network resources, then users are granted access to network resources by configuring application-based Security policy rules. You also must configure Authentication policy to authenticate users accessing network resources *through* the firewall.



There are six Dynamic Admin Roles with predefined privileges labeled Superuser, Superuser (read-only), Device administrator, Device administrator (read-only), and, if your firewall is capable of virtual systems, Virtual system administrator and Virtual system administrator (read-only). These are Dynamic Profiles because they are updated automatically when new capabilities are added to the PAN-OS software, and you cannot manually modify their permissions. The primary permissions differences between the Superuser role and a Device administrator is that a Device administrator cannot define new accounts or virtual systems. A Virtual system administrator can manage only those virtual systems assigned to them. A virtual system administrator does not have access to the firewalls network-level functions such as network interfaces, VLANs, virtual wires, virtual routers, IPSec tunnels, GRE tunnels, DHCP, DNS Proxy, QoS, LLDP, or network profiles. Read-only roles mean just that: You can read (view) data but not modify it.

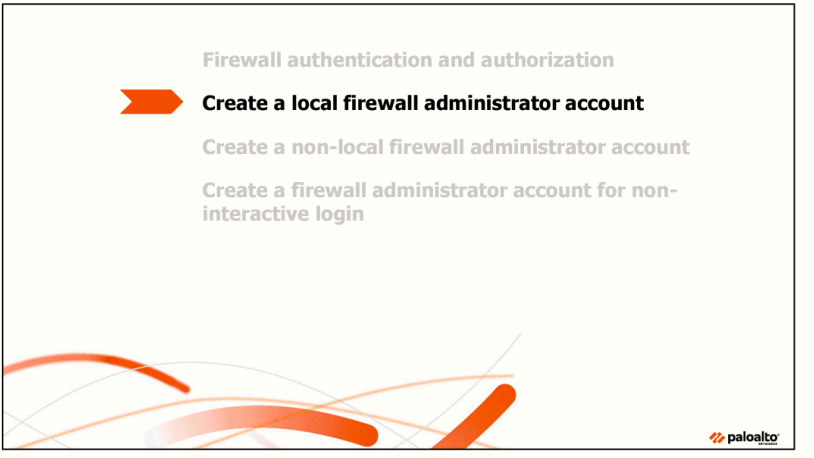


Use the **Device > Admin Roles** page to define Role-Based Profiles that specify sets of custom privileges that you assign to administrative user accounts on the firewall.

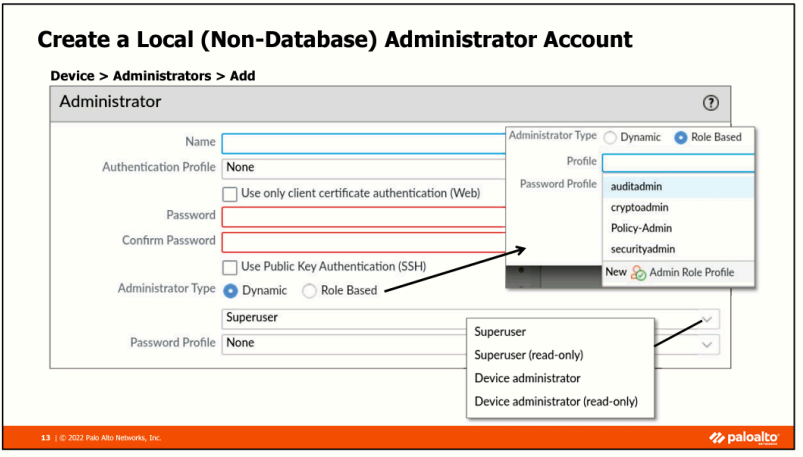
You define four types of privileges in a Role-Based Profile: **Web UI**, **XML API**, **Command Line**, and **REST API**. These permissions are represented by four tabs in the web interface, which you use to assign very granular privileges to a Role-Based Profile.

Role-based privileges on the **Command Line** tab are predefined. No customization is possible. The privileges are:

- **None**: No access granted to the command-line interface
- **superuser**: Full access to the firewall, including defining new administrator accounts and virtual systems. You must have Superuser privileges to create an administrative user with Superuser privileges.
- **superreader**: Read-only access to all options of the firewall
- **deviceadmin**: Full access to all firewall settings except for defining new accounts or virtual systems.
- **devicereader**: Read-only access to all firewall settings except password profiles (no access) and administrator accounts (only the logged-in account is visible).



This section describes how to create additional firewall administrator or operator accounts.



Use the web interface to create an administrator account that is local to the firewall. The privileges of the administrator account are determined by the role profile assigned to the account. The web interface assumes a local account and prompts for a password when you do not select an Authentication Profile.

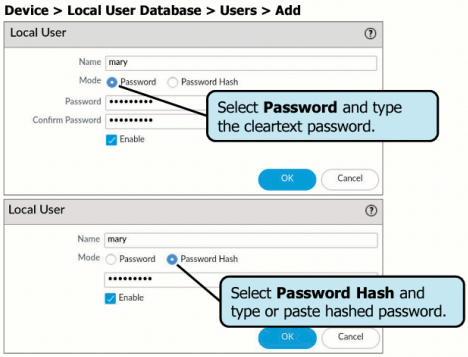
In this example, a Dynamic Profile is selected, which means that user privileges are defined using one of the predefined roles. These roles affect the web interface and the CLI. The following is a brief description of the predefined roles:

- **Superuser**: All access to all options of the firewall
- **Superuser (read only)**: Read-only access to all options of the firewall
- **Device administrator**: Full access to the firewall except for creation of virtual systems and administrative accounts
- **Device administrator (read only)**: Read-only access to the firewall except for viewing other administrative accounts
- **Virtual system administrator**: Full access to a specific virtual system. The virtual system administrator does not have control over firewall-level or network-level functions.
- **Virtual system administrator (read only)**: Read-only access to a specific virtual system. The virtual system administrator (read-only) does not have access to firewall-level or network-level functions.

To ensure that locally stored passwords are strong passwords and are reset periodically, PAN-OS software enables you to set global minimum password complexity requirements and password-aging values at **Device > Setup > Management > Minimum Password Complexity**. By default, there are no minimum requirements and password aging is not enabled.

Those administrator accounts whose passwords might require more frequent resets to meet organizational or legal requirements can be assigned a Password Profile. A Password Profile specifies password-aging values that override the global password-aging values. Configure Password Profiles at **Device > Password Profiles**.

Create a User in the User Database



- Users can be created in the local database:
  - Not recommended if an external authentication service is available
- Users can be added as firewall administrators (**Device > Administrators**).
- Users can be used by the firewall to authenticate traffic flowing *through* the firewall.

For a Tech Doc about this topic, log into Live and search for "Device > Local User Database > Users"

You can add user accounts to a local database on the firewall that stores authentication information for firewall administrators, Captive Portal end users, and end users who authenticate to a GlobalProtect portal and GlobalProtect gateway. Local database authentication requires no external authentication service with all account management performed on the firewall. The users in the database can be added as firewall administrators, or they can be used to authenticate user traffic flowing *through* the firewall.

To add a user to the local user database of the firewall, start by browsing to **Device > Local User Database > Users** and click **Add**. Enter a name to identify the user. Usernames are case-sensitive and can be up to 31 characters in length. Usernames can include alphanumeric characters, spaces, hyphens, and underscores. Each username must be unique within the user database.

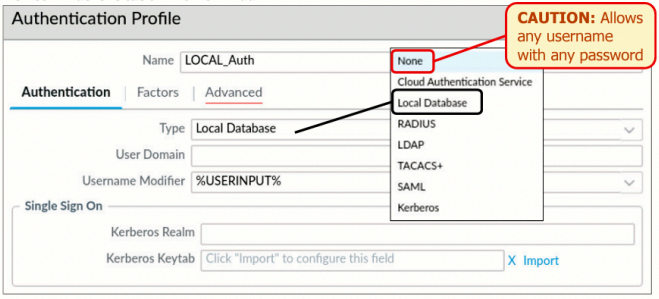
In **Mode** specify how to enter the password: If you select **Password**, enter and confirm a cleartext password. If you select **Password Hash**, type or copy-and-paste a hashed password string. The **Password Hash** option most commonly is used if you want to reuse the password from a Linux account, but you do not know the cleartext password. The firewall can accept any string up to 63 characters in length, regardless of the algorithm used to generate the hash.

Select the **Enable** check box to activate the user account.

Create a Local Database Authentication Profile

For a Tech Doc about this topic, log into Live and search for "Authentication Profile"

Device > Authentication Profile > Add



Links a username to the authentication service that authenticates the user's credentials

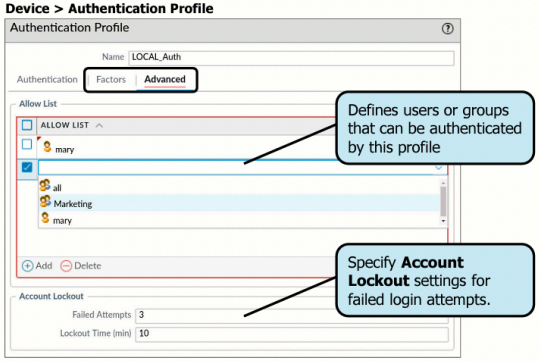
15 | © 2022 Palo Alto Networks, Inc.

An Authentication Profile links a username to the authentication service that the firewall must use to authenticate the user's login credentials. An Authentication Profile is one of the configuration options that you must choose when you define a firewall user account where the user exists in the local firewall user database.

To create an Authentication Profile, first browse to **Device > Authentication Profile** and click **Add**. Type the name of the new profile and then configure the **Authentication** tab. Select **Local Database** to link to the local user database of the firewall. The field options vary, depending on the **Type** you select from the drop-down list. The available **Type** options are shown in the screenshot. Select **None** only in limited scenarios: It is not intended for most users. Selection of **None** could enable undesired users to log in to your firewall.

For more information about the other options in this window, log into Live and search for PAN-OS admin guide or see *PAN-OS 10.2 Administrator's Guide* at https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin.html.

Authentication Profile: Advanced Tab

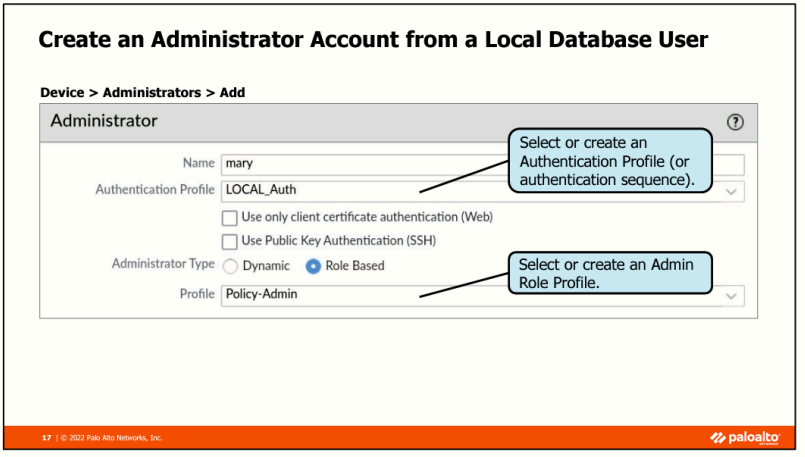


Use the **Advanced** tab to select specific users and/or user groups that the firewall can authenticate using this Authentication Profile. You can select **all** rather than specify a long list of specific users and groups. If you do not add any entries to the list, then no users will be authenticated using this Authentication Profile.

The **Failed Attempts** option in the **Account Lockout** section enables you to enter the number of consecutive failed login attempts allowed before the firewall locks the user account, thus preventing the user from accessing the firewall. By limiting the number of login attempts, you can help protect your network from brute-force login attacks. The default value is 0, which means an unlimited number of login attempts. The range is from 0 to 10.

The **Lockout Time (min)** option enables you to specify how long a user account is locked by the firewall after a user reaches the **Failed Attempts** value. The default value is 0, which means an account will be locked until the administrator manually unlocks the user account. The range is from 0 to 60. Use of a value of 0 ensures that a firewall administrator is aware of multiple failed login attempts, but a 0 value can create additional work for an administrator.

You configure the **Factors** tab as part of MFA.

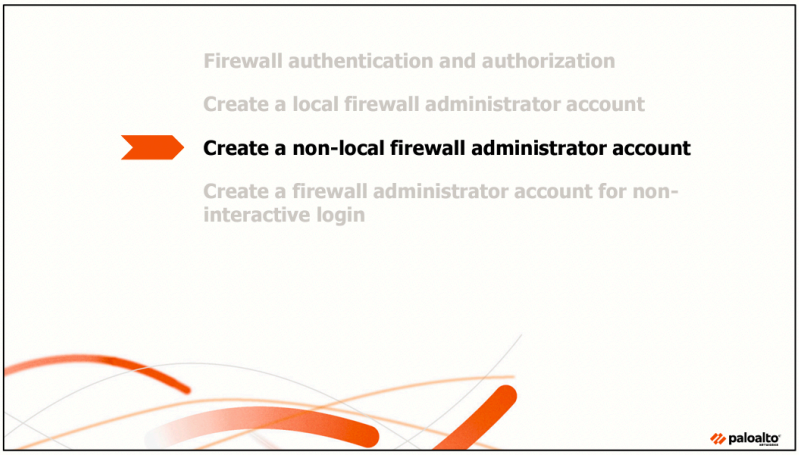


After you have added a user to the local user database and created an Authentication Profile that links to the local user database, you can create a firewall administrator account based on a local database user. Browse to **Device > Administrators** and click **Add**. Type the user's name as it appears in the local user database, select the **Authentication Profile** that links to the local user database, and then select either a predefined or custom Admin Role Profile. Because it is a local user, you can specify a Password Profile that controls the user's password-aging attributes.

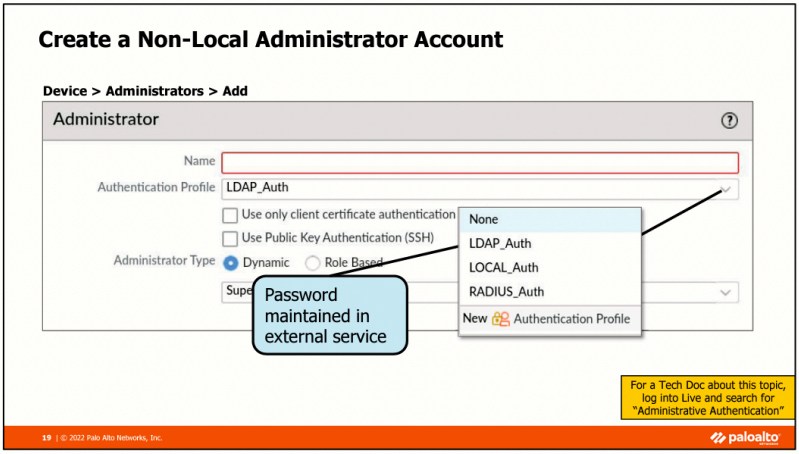
If you do not add a local user as a firewall administrator, then the firewall still can use the user information to authenticate user requests for access to network resources *through* the firewall only and not access to the firewall.

If you select the **Use only client certificate authentication (Web)** option, then a username and password are not required during login to the firewall web interface. Instead, a user certificate is required to authenticate user login to the firewall.

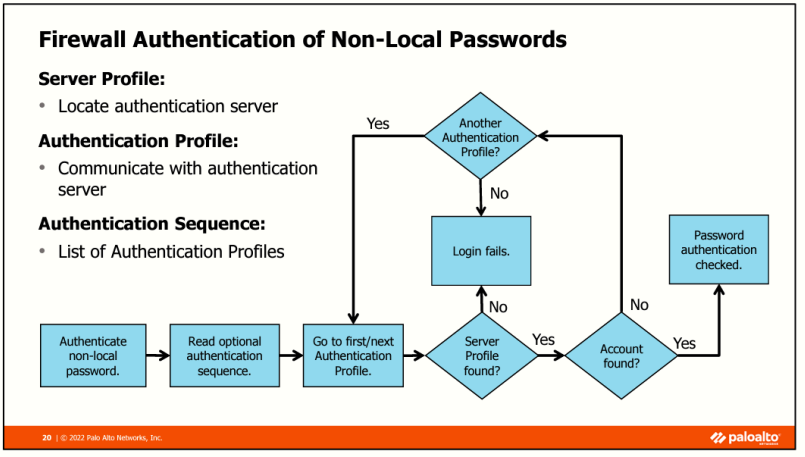
If you select the **Use Public Key Authentication (SSH)** option, then an SSH key is required during login to the command-line interface (CLI) of the firewall. The administrator must generate an SSH public/private key pair on the user's system. Then the administrator must upload the user's public key to the firewall. The user's public key enables the firewall to authenticate the user's login without requiring the user to interactively enter a username and password. This configuration helps to protect against usernames and passwords being stolen from network traffic.



This section describes how to create additional firewall administrator or operator accounts.



You might use the web interface to create administrator accounts whose passwords are maintained in a supported external service. For example, the account password might be maintained in Active Directory. To indicate that the account password is maintained in a supported external service, create an Authentication Profile that connects to an external service and then specify that Authentication Profile when you create an administrator account.



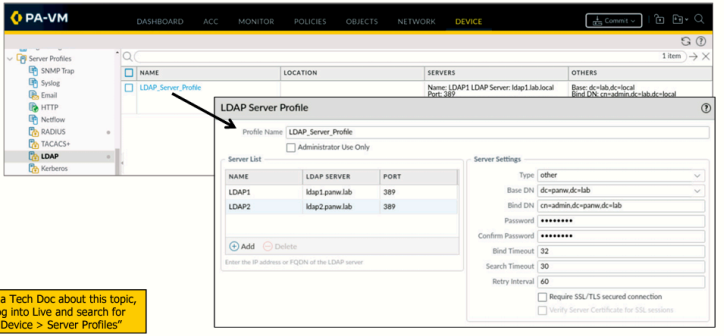
Non-local account passwords must be authenticated through their external authentication service. Before you can access an external authentication service, you must create the appropriate profiles on the firewall. An Authentication Profile contains the information necessary to authenticate an administrator account with an external authentication service after one of the service's servers has been located. An Authentication Profile uses a Server Profile, which you create to locate an external authentication service's servers. You configure a Server Profile with a list of one or more external authentication service's servers.

A firewall can consult multiple external services to authenticate an account. You specify an ordered list of Authentication Profiles by adding them to an optional authentication sequence on the firewall. If you have created an authentication sequence, then specify the authentication sequence instead of an Authentication Profile when you add a user account on the firewall.

The flowchart shows how a firewall authenticates a non-local account. If the administrator account specifies an authentication sequence, then the firewall attempts to authenticate the account using the ordered list of specified Authentication Profiles. Each Authentication Profile specifies a Server Profile with a list of servers for the external authentication service. The firewall connects to each external service until either the user is located, or no Authentication Profiles are left. If no Authentication Profiles are left, then the login attempt fails.

Configure Server Profiles

Device > Server Profiles



For a Tech Doc about this topic, log into Live and search for "Device > Server Profiles"

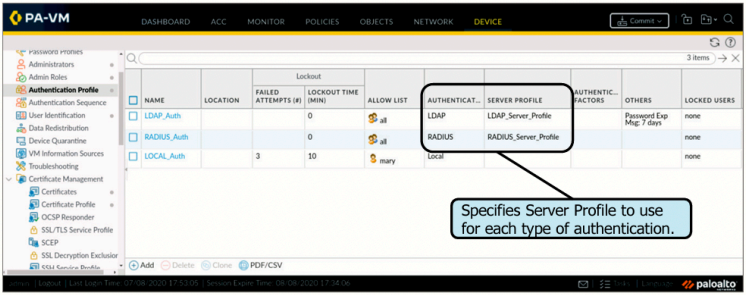
Server Profiles define connections that the firewall can make to external servers of specific types. For authentication purposes, you can create Server Profiles for RADIUS, TACACS+, LDAP, Kerberos, or SAML servers.

Authentication Profiles require Server Profiles to validate login information for administrator accounts that are not created on the firewall.

Configure Authentication Profiles

For a Tech Doc about this topic, log into Live and search for "Authentication Profile"

Device > Authentication Profiles

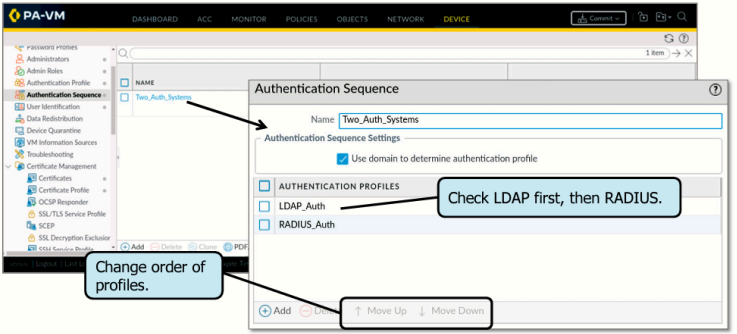


An Authentication Profile specifies which authentication server and settings are used to authenticate an administrator account. You specify an Authentication Profile when you create an administrator account where the account name and password are maintained on an external service.

Configure an Authentication Sequence

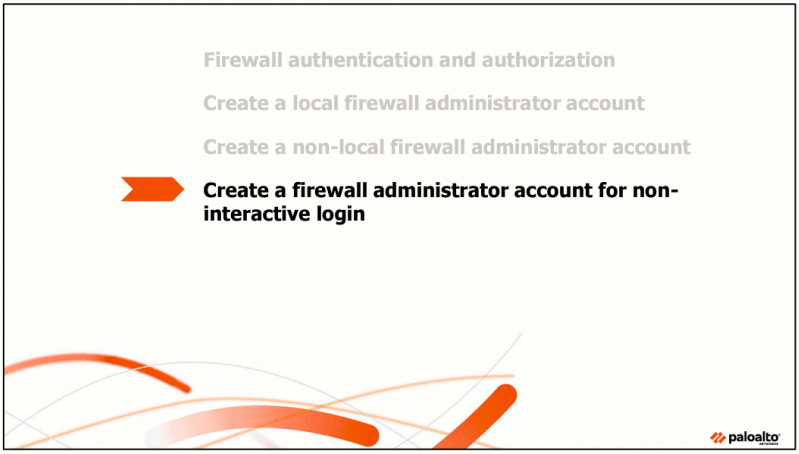
For a Tech Doc about this topic, log into Live and search for "Configure an Authentication Profile and Sequence"

Device > Authentication Sequence > Add

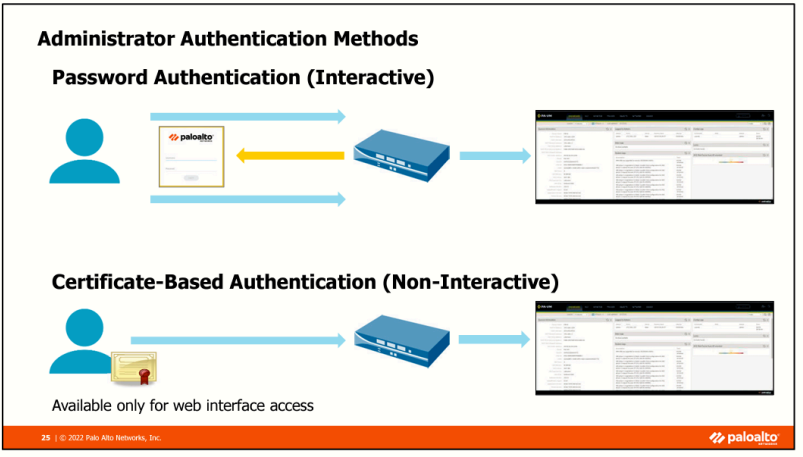


An authentication sequence is optional if you have defined multiple external services. After you have defined your Authentication Profiles, you create the Authentication Sequence that lists the Authentication Profiles that should be checked to authenticate an administrator account and the order in which they should be checked. The Authentication Profiles should be in order from the most preferred method listed first to the least preferred method listed last. You can use the **Move Up** button or **Move Down** button to change the order of the listed profiles.

If you have configured an authentication sequence, the firewall checks against each profile in sequence until one profile successfully authenticates the user. In our example, the firewall will first try to authenticate the user account using the LDAP_Auth profile. If the firewall fails to authenticate the user account using the LDAP_Auth, then the firewall will attempt to authenticate the user account using the RADIUS_Auth profile. A user account is denied access only if authentication fails for all the profiles in the sequence.



This section describes how to create a firewall administrator account for non-interactive logins.

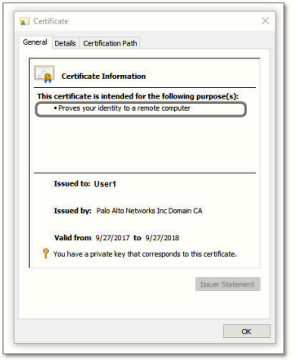


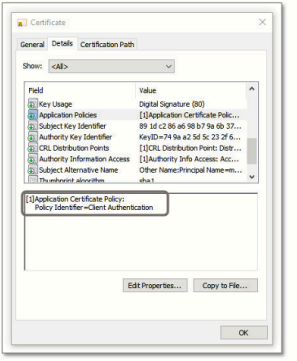
Palo Alto Networks firewalls support interactive and non-interactive authentication. In the example at the top, the user attempts to access the firewall. The firewall receives the user's access request and responds with an interactive authentication page that requires the user to enter a valid username and a password. The credentials can be either authenticated locally at the firewall or sent to an external authentication service.

As a more secure alternative to password-based authentication to the firewall web interface, you can configure certificate-based authentication for administrator accounts that are local to the firewall. Certificate-based authentication involves the exchange and verification of a digital signature instead of a password. In the example at the bottom, a user with a client certificate attempts to access the firewall. The firewall receives the user's access request and transparently uses the client certificate to authenticate the user. This type of authentication occurs locally at the firewall. If the certificate is deemed a valid certificate and the user is authorized to access the service or application, then the user will be granted access.

Certificate-based authentication is available only when the firewall web interface is accessed, not the command-line interface.

User Certificate

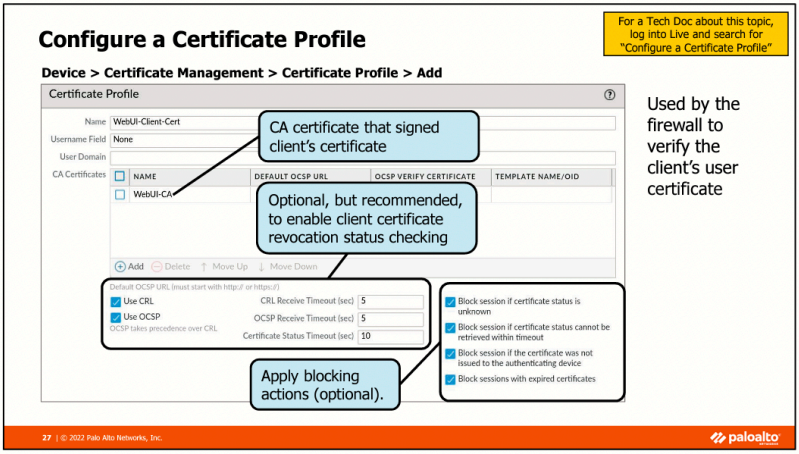




You can rely on a certificate and the information and public key it contains when the issuing certificate authority (or CA) is trusted and the signature in a certificate is valid. The receiving entity can recompute and compare the signature to ensure that a certificate has not been intercepted and altered by a malicious third party.

If the certificate of the issuing CA is not added to the certificate store of a client, the client receives a certificate warning message when browsing to secure websites verified by that CA.

After you have generated or imported a CA certificate at the firewall, configure your administrator accounts to use client certificates for non-interactive authentication to the web interface. A step in the process is to generate a client certificate for each administrative account. The root CA certificate will be used during generation of the client certificate. You should export the certificate after it has been generated and then import the certificate into the browser on your administrative workstation. Note that configuration of certificate-based authentication for any administrator automatically will disable the username and password logins for all administrators on the firewall. The administrators will require a certificate to authenticate to the firewall for administrative purposes.



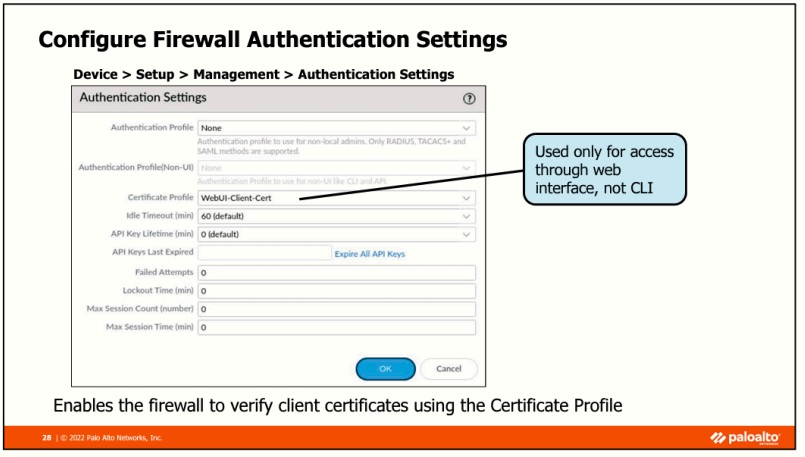
A Certificate profile defines user and device authentication for Authentication Portal, multi-factor authentication (MFA), GlobalProtect, site-to-site IPSec VPN, external dynamic list (EDL) validation, Dynamic DNS (DDNS), User-ID agent and TS agent access, and web interface access to Palo Alto Networks firewalls or Panorama. The profiles specify which certificates to use, how to verify certificate revocation status, and how that status constrains access. You can configure a separate Certificate Profile for each service.

A Certificate Profile can contain one or more certificates. When you configure the certificates that your profile will use for authenticating your administrative accounts, you can either select an existing certificate or import a certificate from your enterprise CA.

A best practice when you configure your Certificate Profile is to enable Online Certificate Status Protocol (or OCSP) and/or a certificate revocation list (or CRL) for certificate status verification in your Certificate Profiles. OCSP allows the firewall to verify the certificate expiration dates. The firewall checks the revocation status of a certificate, typically using HTTP with a request-response format. The authority responding can reply with a status of good, revoked, or unknown for the certificate in question. A CRL is a list of serial numbers for certificates that have been revoked. The list is generated and published periodically by the CA that issued the corresponding certificates. If you configure both methods, the firewall first tries OCSP. If OCSP fails to respond within the given time frame in the **Certificate Status Timeout** field, then the firewall will attempt to verify the validity of the certificate using the CRL method.

Select the **Block session if certificate status is unknown** check box if you want the firewall to block sessions when the OCSP or CRL service returns a certificate revocation status of **unknown**.

Select the **Block session if certificate status cannot be retrieved within timeout** check box if you want the firewall to block sessions after it registers an OCSP or CRL request timeout.



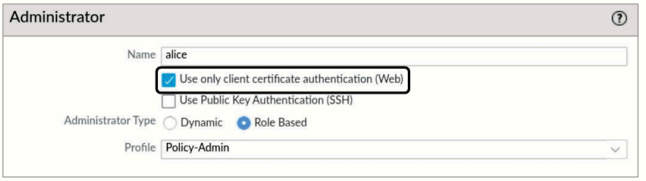
After you have created your Certificate Profile, browse to **Device > Setup > Management** and click the **Authentication Settings** gear icon. For the **Certificate Profile**, select from the drop-down list the profile that you created. Specification of a **Certificate Profile** enables certificate authentication only for web interface users, not for CLI users.

This configuration enables the firewall to verify the client certificates for any administrator accounts that you have configured for certificate-based firewall access.

It is important to remember that configuration of certificate-based authentication for any administrator will automatically disable the username and password logins for all administrators on the firewall. All administrators will require a certificate to authenticate to the firewall for administrative purposes.

Create an Administrator Account for Non-Interactive Login

Device > Administrators > Add



- Selection of the check box configures the firewall to perform certificate-based authentication:
  - Authenticates access only to the firewall web interface, not to the CLI
- No longer prompted for an Authentication Profile
- Still must authorize user actions by specifying an Admin Role Profile

To create a firewall administrator account, browse to **Device > Administrators** and click **Add**. Enter the user's name in the **Name** field.

Select the **Use only client certificate authentication (Web)** check box to configure the firewall to use certificate-based authentication for this user. Use of certificate-based authentication replaces all other forms of either local or external authentication. If you select the check box, the **Authentication Profile** drop-down list no longer is available in this dialog box.

Certificate-based authentication is available only to users who attempt to access the firewall through the web interface. Certificate-based authentication is not available for command-line (CLI) access to the firewall.

As is the case with all users who access the firewall, you assign the user either a **Dynamic** or a **Role Based** Authentication Profile. The options on the **Profile** drop-down list vary depending on whether you select the **Dynamic** or the **Role Based** radio button.

Module Summary

Now that you have completed this module, you should be able to:

- Describe the firewall authentication and authorization process and firewall components
- Create a local firewall administrator account
- Create a non-local firewall administrator account
- Create a firewall account that supports non-interactive login

Now that you have completed the module, you should be able to perform the tasks listed.

Additional Resources

For a digital review of this module, log into Beacon and search for:

"Next-Generation Firewall Setup and Management Connection"

Items Review Questions

1. When creating a custom admin role, which four types of privileges can be defined? (Choose four.)
   a. WebUI
   b. Panorama
   c. REST API
   d. Command Line
   e. Java API
   f. XML API

2. True or false? Server Profiles define connections that the firewall can make to external servers.
   a. true
   b. false

3. Global user authentication is supported by which three authentication services? (Choose three.)
   a. SAML
   b. LDAP
   c. RADIUS
   d. Certificate
   e. TACACS +

4. True or false? Certificate-based authentication replaces all other forms of either local or external authentication.
   a. true
   b. false

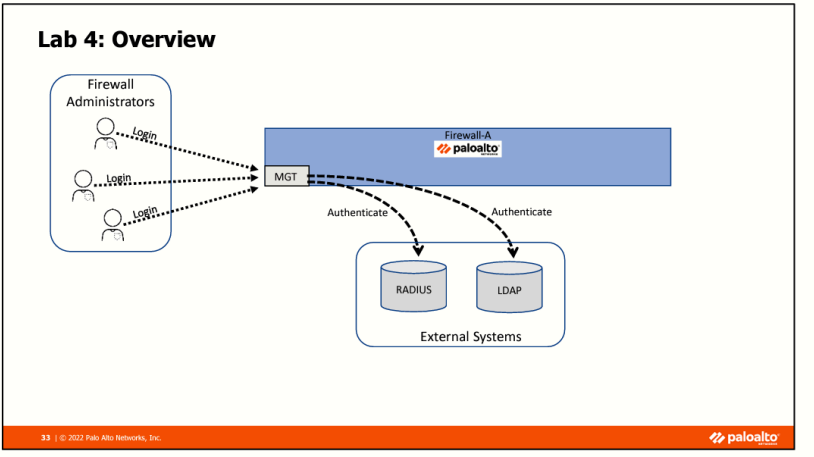
Items Review Questions

1. When creating a custom admin role, which four types of privileges can be defined? (Choose four.)
   a. WebUI
   b. Panorama
   c. REST API
   d. Command Line
   e. Java API
   f. XML API

2. True or false? Server Profiles define connections that the firewall can make to external servers.
   a. true
   b. false

3. Global user authentication is supported by which three authentication services? (Choose three.)
   a. SAML
   b. LDAP
   c. RADIUS
   d. Certificate
   e. TACACS +

4. True or false? Certificate-based authentication replaces all other forms of either local or external authentication.
   a. true
   b. false



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 4: Managing Firewall Administrator Accounts

- Load a baseline configuration
- Create a local firewall administrator account
- Configure an LDAP Server Profile
- Configure a RADIUS Server Profile
- Configure an LDAP Authentication Profile
- Configure a RADIUS Authentication Profile
- Configure an Authentication Sequence
- Create non-local firewall administrator accounts

Answers to Review Questions

1. a, c, d, f
2. a (true)
3. a, c, e
4. a (true)