



PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 3: Managing Firewall Administrator Accounts

Document Version: **2025-10-13**

Copyright © 2025 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks, PAN-OS, WildFire, RedLock, and Demisto are registered trademarks of Palo Alto Networks, Inc. All other marks mentioned herein may be trademarks of their respective companies.

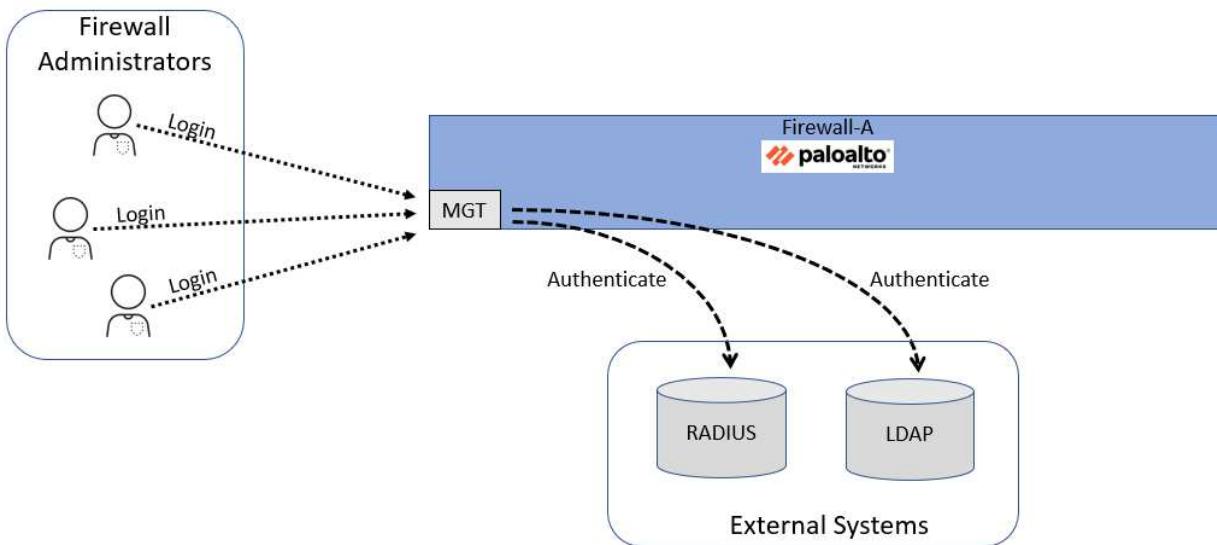
Contents

Introduction	3
Objective	3
Lab Topology	4
Theoretical Lab Topology	4
Lab Settings	5
Lab Guidance	5
1 Managing Firewall Administrator Accounts – High Level Lab Steps.....	6
1.1 Apply a Baseline Configuration to the Firewall	6
1.2 Create a Local Database Authentication Profile.....	6
1.3 Create a Local User Database Account.....	6
1.4 Create an Administrator Account	6
1.5 Commit the Configuration	6
1.6 Log in With New Admin Account.....	6
1.7 Configure LDAP Authentication	6
1.8 Commit the Configuration	7
1.9 Log in With New Admin Account.....	7
1.10 Configure RADIUS Authentication	7
1.11 Commit the Configuration	8
1.12 Log in With New Admin Account.....	8
1.13 Configure an Authentication Sequence.....	8
2 Managing Firewall Administrator Accounts – Detailed Lab Steps.....	9
2.1 Load Lab Configuration	9
2.2 Create a Local Database Authentication Profile.....	12
2.3 Create a Local User Database Account.....	14
2.4 Create an Administrator Account	16
2.5 Configure LDAP Authentication	21
2.6 Configure RADIUS Authentication	29
2.7 Configure and Authentication Sequence.....	38

Introduction

When you deploy the firewall into your production network, you need to make sure that other members of your team have administrative access to the device. You want to leverage an existing LDAP server that maintains account and password information for members of your team. However, your organization recently merged with another company whose administrative accounts are maintained in a RADIUS database.

No one has had time yet to migrate all the accounts from RADIUS into LDAP, so you need to configure the firewall to check both LDAP and RADIUS to authenticate an account when an administrator logs in.

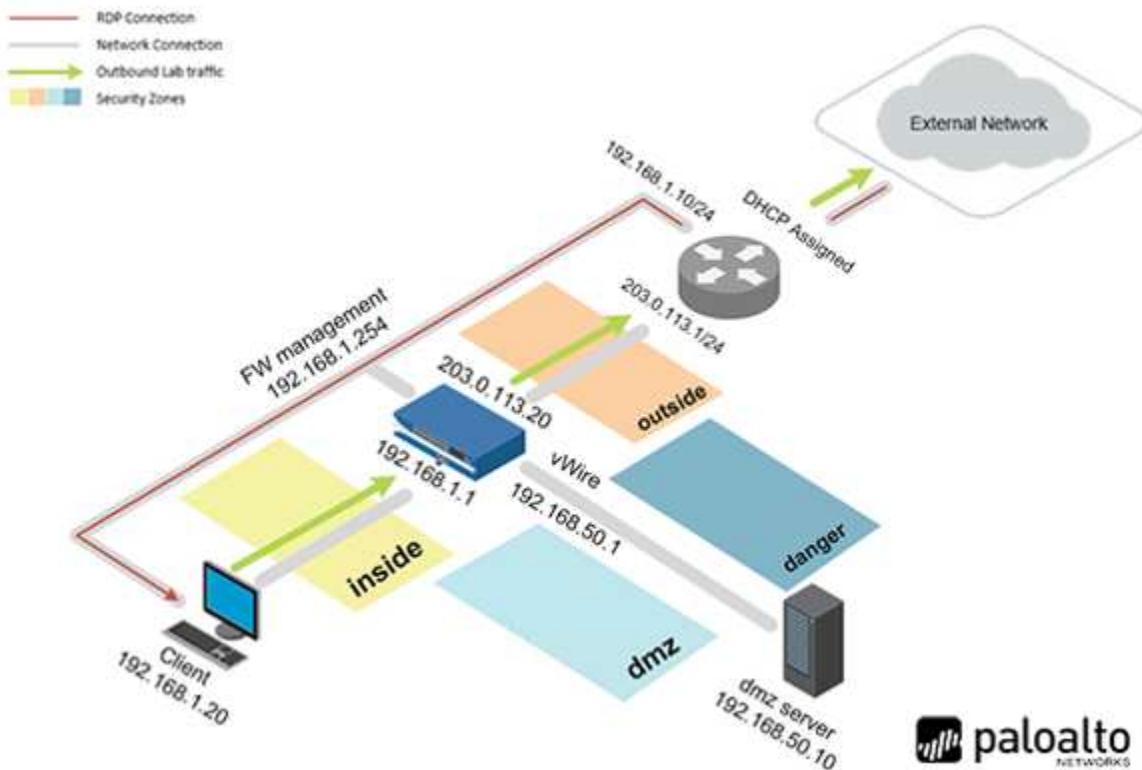


Objective

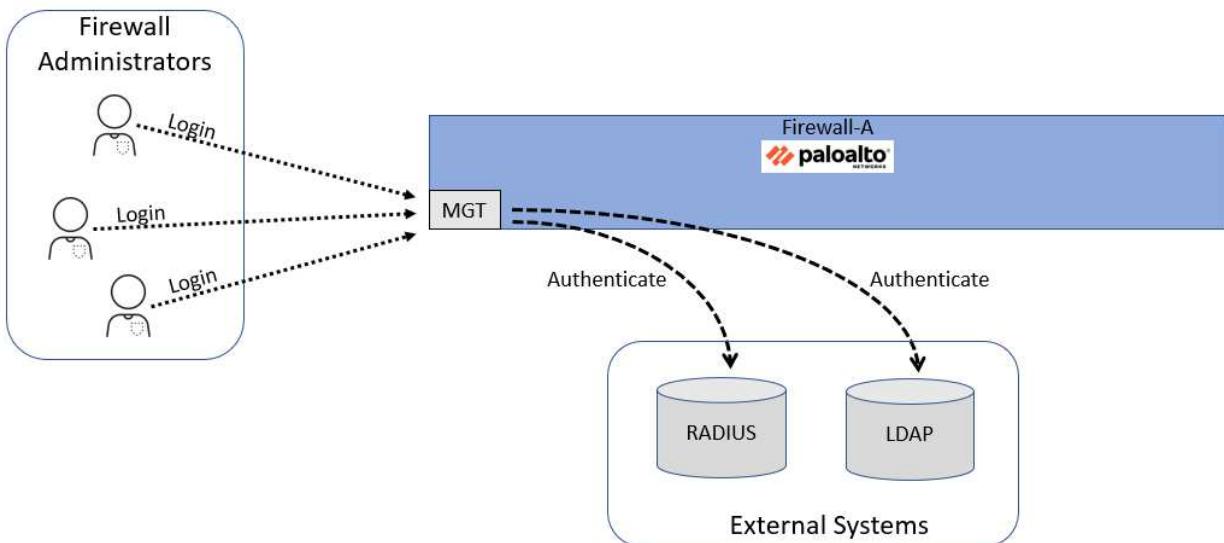
In this lab, you will perform the following tasks:

- 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.

Lab Topology



Theoretical Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	PaloAlt0!
DMZ	192.168.50.10	root	PaloAlt0!
Firewall	192.168.1.254	admin	PaloAlt0!
vRouter	192.168.1.10	root	PaloAlt0

Lab Guidance

There are two sections in this lab guide:

- High-Level Lab Steps
- Detailed Lab Steps

The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with a Palo Alto Networks firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.

Please
Note

You are not required to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Instead, please select the appropriate section based on your familiarity with Palo Alto Networks Firewalls.

1 Managing Firewall Administrator Accounts – High Level Lab Steps

It is recommended to use this section if you possess significant experience in working with Palo Alto Networks firewalls. In case you require more comprehensive instructions to achieve the objectives, please utilize the Detailed-Lab Steps section in Task 2.

1.1 Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select *lab-user*, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter admin for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-03.xml** to the Firewall.

1.2 Create a Local Database Authentication Profile

- Create a **Local Database Authentication Profile** called **Local-Database**.
- Set the **Allow List** for the **Local-Database Profile** to **all**.

1.3 Create a Local User Database Account

- Create an entry in the **Local User Database** called **adminBob** with **Pal0Alt0!** as the **Password**.

1.4 Create an Administrator Account

- Create an **Administrator** account using the **Local Database** entry for **adminBob**.
- Set the **Authentication Profile** to **Local-Database**.

1.5 Commit the Configuration

- Commit the changes to the firewall before proceeding.

1.6 Log in With New Admin Account

- Log out of the firewall web interface and log back into the firewall with **adminBob** as the **Username** and **Pal0Alt0!** as the **Password**.
- Use the **System log** to verify that the **adminBob** account was authenticated by the **local-database**.
- Log out of the firewall and log back into the firewall with the **admin/Pal0Alt0!** credentials.

1.7 Configure LDAP Authentication

- Use the information in the table below to configure an LDAP Server Profile.

Profile Name	LDAP-Server-Profile
Server Name	ldap.panw.lab
LDAP Server IP Address	192.168.50.89
Port field	389

Server Settings Type	Other
Base DN	dc=panw,dc=lab
Bind DN	cn=admin,dc=panw,dc=lab
Password / Confirm Password	Pal0Alt0!
Require SSL/TLS secured connection	unchecked

- Use the information in the table below to create an LDAP Authentication Profile.

Name	LDAP-Auth-Profile
Type	LDAP
Server Profile	LDAP-Server-Profile
Allow List (Advanced Tab)	all

- Use the information in the table below to create a new administrator account that will be authenticated by LDAP.

Name	adminSally
Authentication Profile	LDAP-Auth-Profile

1.8 Commit the Configuration

- Commit the changes to the firewall before proceeding.

1.9 Log in With New Admin Account

- Test LDAP Authentication by logging in with the **adminSally/Pal0Alt0!** credentials.
- Use the System log to verify that the **adminSally** account was authenticated using LDAP.

1.10 Configure RADIUS Authentication

- Use the information in the table below to configure a RADIUS Server Profile.

Profile Name	RADIUS-Server-Profile
Authentication Protocol	CHAP
Server Name	radius.panw.lab
RADIUS Server	192.168.50.150
Secret / Confirm Secret	Pal0Alt0!
Port	1812

- Use the information in the table below to create a RADIUS Authentication Profile.

Name	RADIUS-Auth-Profile
Type	RADIUS
Server Profile	RADIUS-Server-Profile
Allow List (Advanced Tab)	all

- Use the information in the table below to create a new administrator account that will be authenticated by RADIUS.

Name	adminHelga
Authentication Profile	RADIUS-Auth-Profile

1.11 Commit the Configuration

- Commit the changes to the firewall before proceeding.

1.12 Log in With New Admin Account

- Test RADIUS Authentication by logging in with the **adminHelga/Pa10Alt0!** credentials.
- Use the System log to verify that the **adminHelga** account was authenticated using RADIUS.

1.13 Configure an Authentication Sequence

- Create an authentication sequence called **LDAP-then-RADIUS** that uses the **LDAP-Auth-Profile** first and the **RADIUS-Auth-Profile** second.
- Commit the configuration.

2 Managing Firewall Administrator Accounts – Detailed Lab Steps

It is recommended to use this section if you prefer detailed guidance to complete the objectives for this lab. It is strongly recommended that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

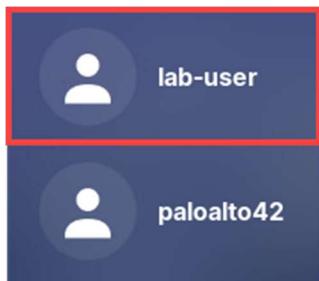
2.1 Load Lab Configuration

In this section, you will connect to the Firewall and load the Firewall configuration file.

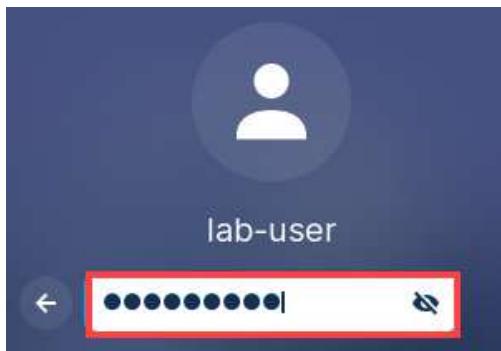
1. Click on the **Client** tab to access the Client PC.



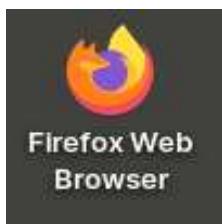
2. On the *Zorin* desktop, click **lab-user**.



3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.



4. Double-click the **Firefox Web Browser** icon located on the *Desktop*.



5. In the *Firefox* address field, type **https://192.168.1.254** and press **Enter**.



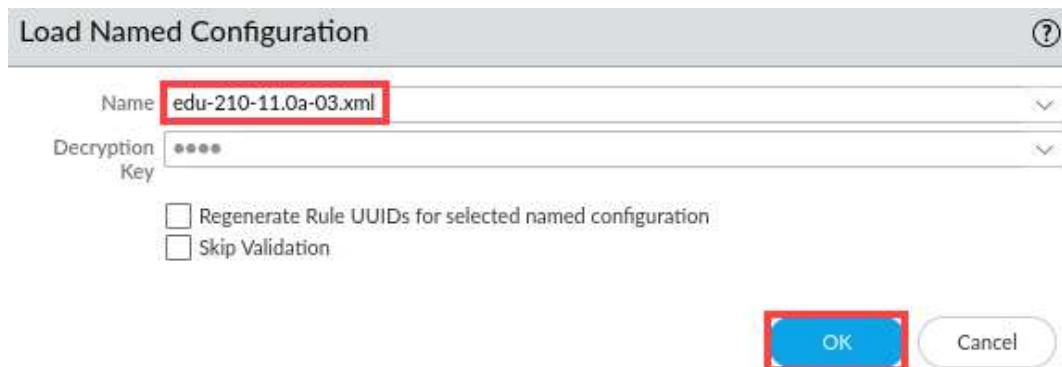
6. Log in to the Firewall web interface as username **admin**, password **Pa10Alt0!**.



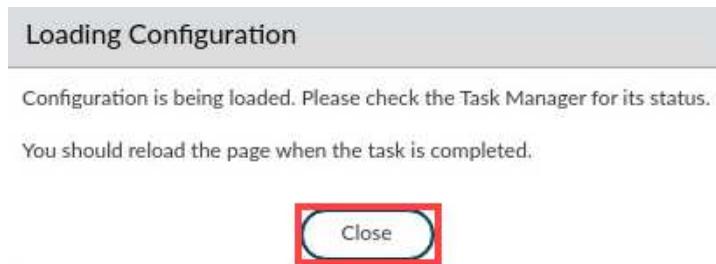
If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

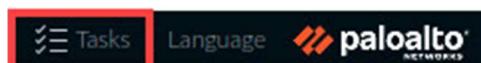
8. In the *Load Named Configuration* window, select **edu-210-11.0a-03.xml** from the *Name* drop-down box and click **OK**.



9. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



10. Click the **Tasks** icon located at the bottom-right of the web interface.



11. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**

Task Manager - All Tasks						
JOB ID	TYPE	STATUS	START TIME	MESSAGES	ACTION	ADMIN
14	Load	Completed	2023/07/28 18:54:07			System
2	Report	Completed	2023/07/28 18:51:30			
Show: All Tasks					Close	

12. Click the **Commit** link located at the top-right of the web interface.



13. In the *Commit* window, click **Commit** to proceed with committing the changes.

Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

Commit All Changes Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
Commit Scope is unavailable when a full commit is required				

 Preview Changes  Change Summary  Validate Commit

Note: This shows all the changes in login admin's accessible domain.

Description

Commit **Cancel**

14. When the commit operation is complete, click **Close** to continue.

Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit

Close



The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.2 Create a Local Database Authentication Profile

In this section, you will create a local database authentication profile. Local database profiles allow the firewall to authenticate administrators who need access to the firewall web interface through Captive Portal or GlobalProtect.

- In the PA-VM web interface, navigate to **Device > Authentication Profile**. Click **Add** at the bottom of the window.

The screenshot shows the PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE link is highlighted with a red box. On the left, a sidebar lists various management options: Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile (which is also highlighted with a red box), Authentication Sequence, User Identification, and Data Redistribution. Below the sidebar is a table titled 'Lockout' with columns for NAME, LOCATION, FAILED ATTEMPTS (#), LOCKOUT TIME (MIN), ALLOW LIST, and AUTHENTICAT. At the bottom of the page, there is a toolbar with icons for TACACS, LDAP, Kerberos, SAML Identity Provider, Multi Factor Authentication, and an 'Add' button, which is also highlighted with a red box. Other buttons in the toolbar include Delete, Clone, and PDF/CSV.

- In the *Authentication Profile* window, under the *Authentication* tab, enter **Local-Database** for the *Name*, for *Type*, use the drop-down list to select **Local Database**.

The screenshot shows the 'Authentication Profile' configuration dialog. The 'Name' field contains 'Local-Database' and the 'Type' dropdown is set to 'Local Database'. The 'Authentication' tab is selected. Other tabs available are 'Factors' and 'Advanced'. Below the tabs, there are fields for 'User Domain' and 'Username Modifier'. Under the 'Single Sign On' section, there are fields for 'Kerberos Realm' and 'Kerberos Keytab', with an 'Import' button. At the bottom right are 'OK' and 'Cancel' buttons.

3. Select the **Advanced** tab, in the *Allow List* section, click **Add**. Select **All** and click **OK**.

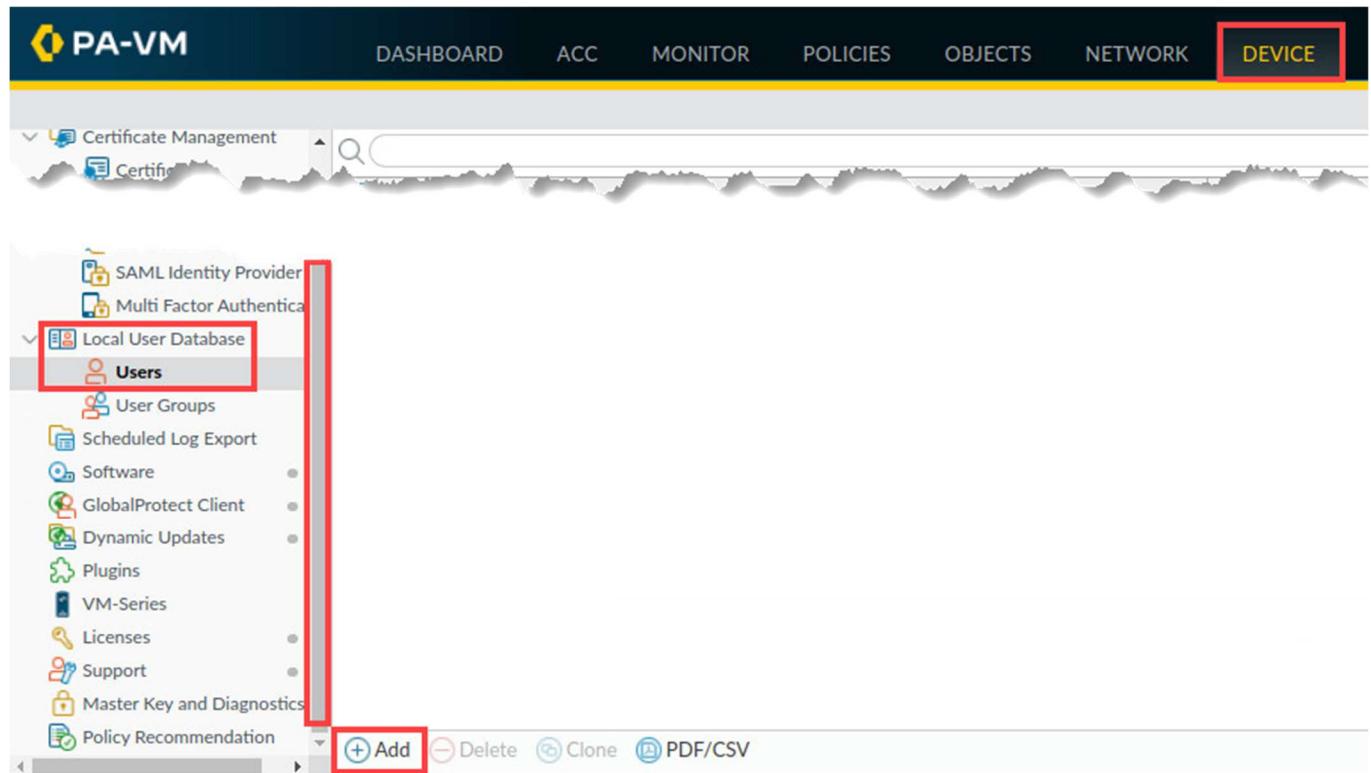
The screenshot shows the 'Authentication Profile' configuration page. The 'Name' field is set to 'Local-Database'. The 'Advanced' tab is selected. In the 'Allow List' section, there is a list named 'all' with a checked checkbox. Below the list are 'Add' and 'Delete' buttons, with 'Add' being highlighted with a red box. At the bottom right, there are 'OK' and 'Cancel' buttons, with 'OK' being highlighted with a red box.

4. Leave the firewall web interface open to continue with the next task.

2.3 Create a Local User Database Account

In this section, you will create a new entry in the Local User Database on the firewall. This entry will be for a new team member, **adminBob**.

1. In the web interface, select **Device > Local User Database > Users**. In the bottom left corner of the window, click **Add**. You may need to use the scroll bar to locate the Local User Database drop down.



2. In the *Local User* window, type **adminBob** for the *Name* field. Enter **Pa10Alt0!** for *Password* and *Confirm Password*. Click **OK**.

The screenshot shows the 'Local User' configuration dialog box. It has fields for Name (containing 'adminBob'), Mode (set to 'Password' with a radio button), Password (containing '*****'), Confirm Password (containing '*****'), and a checked 'Enable' checkbox. At the bottom are 'OK' and 'Cancel' buttons, with the 'OK' button highlighted with a red box.

3. Leave the firewall web interface open to continue with the next task.

2.4 Create an Administrator Account

In this task, you will create an administrator account for adminBob. The adminBob account will use the Local-Database Authentication Profile.

1. In the web interface, select **Device > Administrators**. Click **Add** at the bottom of the window.

The screenshot shows the PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE link is highlighted with a red box. On the left, a sidebar menu lists various options like Setup, High Availability, Config Audit, Password Profiles, Administrators (which is selected and highlighted with a red box), Admin Roles, Authentication Profile, and Authentication Sequence. The main content area displays a table titled "Administrators" with columns: NAME, ROLE, AUTHENTICATI..., PROFILE, PASSWORD PROFILE, CLIENT CERTIFICATE AUTHENTICA..., and PUBLIC KEY AUTHENTICA... (WEB). A single row is shown for "admin" with "Superuser" in the ROLE column. At the bottom of the page, there is a toolbar with icons for Email, LDAP, Kerberos, SAML Identity Provider, Multi Factor Authentication, and a red box around the "+ Add" button. Below the toolbar, there are links for Delete, PDF/CSV, and a red box around the "OK" button.

2. In the *Administrator* window, enter **adminBob** for the *Name*. For the *Authentication Profile*, select **Local-Database**. Click **OK**.

The screenshot shows the "Administrator" configuration dialog box. It has fields for Name (set to "adminBob"), Authentication Profile (set to "Local-Database"), and Administrator Type (set to "Dynamic"). There are also checkboxes for "Use only client certificate authentication (Web)" and "Use Public Key Authentication (SSH)". A note below says "Superuser". At the bottom right are "OK" and "Cancel" buttons, with "OK" highlighted by a red box.

Please Note

Note that when you select Local-Database for the Authentication Profile, there is no option to enter a Password for the administrator. The password information for this account is maintained in the Local-database on the firewall.

- Click the **Commit** button at the upper right of the *PA-VM* web interface.



- In the *Commit* window, click **Commit** to proceed with committing the changes.

A screenshot of the 'Commit' window. At the top, it says 'Doing a commit will overwrite the running configuration with the commit scope.' Below that are two radio buttons: 'Commit All Changes' (selected) and 'Commit Changes Made By: (1) admin'. A table shows 'COMMIT SCOPE' (device-and-network, shared-object) and 'LOCATION TYPE'. At the bottom, there are buttons for 'Preview Changes', 'Change Summary', 'Validate Commit', and 'Group By Location Type' (checked). A note says 'Note: This shows all the changes in login admin's accessible domain.' A large text area for 'Description' is empty. At the bottom right are 'Commit' (red box) and 'Cancel' buttons.

- When the commit operation is complete, click **Close** to continue.

A screenshot of the 'Commit Status' window. It shows the 'Operation Commit' status as 'Completed' and the 'Result' as 'Successful'. The 'Details' section says 'Configuration committed successfully'. A 'Commit' button is at the bottom left, and a 'Close' button (red box) is at the bottom right.

- Log out of the firewall web interface by clicking the **Logout** button in the bottom left corner of the window.



7. In the *Log In* window, click **Log In**.



8. Log back into the firewall as username **adminBob**, password **Pa10Alt0!**. Click **Log In**.



9. In the *Welcome* window, click **Close**.

Welcome

Welcome to PAN-OS 11.0!

With this release, Palo Alto Networks introduces new and enhanced cloud-delivered security services, including the industry's first ML-powered exploit prevention. In concert with our ML-Powered next-generation firewalls, these services extend best-in-class security. PAN-OS 11.0 leverages cloud compute for artificial intelligence (AI) and deep learning techniques to secure the modern enterprise with unmatched performance. Highlights include:

- Advanced Threat Prevention Support for Zero-day Exploit Prevention Using Inline Deep Learning**—The Advanced Threat Prevention subscription service now supports additional deep learning and heuristic analysis engines to prevent malicious zero-day Injection attacks (Inbound threats), such as SQLi and Command Injection attacks. These attacks target vulnerable applications that do not sufficiently validate, filter, or sanitize user-supplied data.
- Skip Software Version Upgrade**—Upgrade or downgrade standalone and Panorama managed devices running 10.1 or later more efficiently by skipping up to three software versions. With the ability to skip multiple software releases during an upgrade or downgrade, this process shortens time needed for the maintenance window and enables you to take faster advantage of the latest PAN-OS innovations. This feature also enhances the capabilities of the multi-image download option and pre-install validation check, which reduces the number of steps in the process.
- Web Proxy**—The new on-premises Web Proxy capability provides you with additional options for migration from an existing web proxy-based architecture to a consolidated platform, and helps you transition to the cloud without sacrificing security or efficiency. By configuring seamless synchronization between your on-premises proxy device and the cloud-based proxy, you can enable Prisma Access as a SASE solution for your SWG-based network architecture to ensure consistent policy application regardless of location.
- DHCPv6 Client with Prefix Delegation**—The firewall now supports a stateful DHCPv6 Client to obtain IPv6 addresses and other parameters. This feature also supports Prefix Delegation by assigning prefixes received from the DHCP server to configured pools. A prefix from the pool is distributed using SLAAC to a host-facing (inherited) interface.
- User Context for the Cloud Identity Engine**—Provides unparalleled visibility into your user identification and device information (such as tags, quarantine

Close

10. Select **Monitor > Logs > System**. Look for an entry with **Type > Auth**. You may need to scroll through the logs to find the auth type.

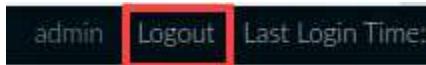
RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
09/21 03:52:13	general	informational	general		User adminBob accessed tab: monitor
09/21 03:51:46	general	informational	general		User adminBob logged in via Web from 192.168.1.20 using https
09/21 03:51:46	auth	informational	auth-success	Local-Database	authenticated for user 'adminBob': auth profile 'Local-Database', vsys 'shared', From: 192.168.1.20.
09/21 03:51:45	url-filtering	high	url-download-failure		PAN-DB cloud list loading failed (ERROR:Couldn't resolve host name).
09/21 03:51:45	url-filtering	high	url-cloud-connection-failure		CURL ERROR: Could not resolve host: s0000.urlcloud.paloaltonetworks.com
09/21 03:51:33	general	informational	general		User admin logged out via Web from 192.168.1.20
09/21 03:51:16	general	informational	general		Commit job succeeded. Completion time=2023/09/21 03:51:17. JobId=22. User:admin
09/21 03:50:59	sslmgr	informational	sslmgr-config-p2-success		SSLMGR daemon configuration load phase-2 succeeded

Please Note

Note that the entry in the firewall system log indicates that adminBob was successfully authenticated against the **Local-Database**.

If you do not see an entry in the System log indicating a successful authentication for adminBob, you can use a filter (subtype eq auth) as the syntax.

11. Log out of the Firewall.



12. In the *Log In* window, click **Log In**.



13. Log back into the firewall with the **admin/Pal0Alt0!** credentials.



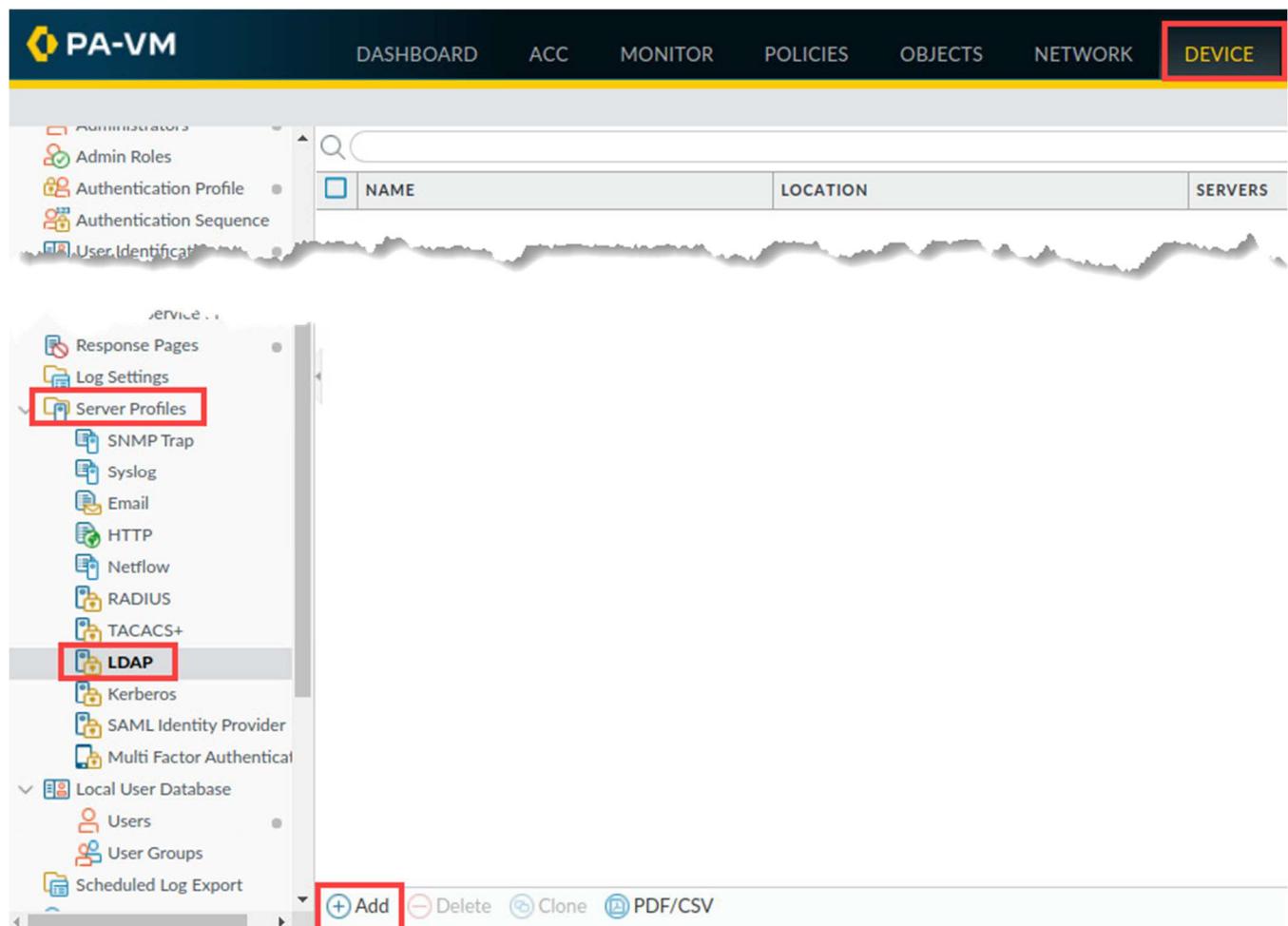
14. Leave the firewall web interface open to continue with the next task.

2.5 Configure LDAP Authentication

Your organization uses an LDAP server to maintain a database of users, including network administrators. Your team of security personnel is growing each month and you want to leverage the existing LDAP server to authenticate administrators when they attempt to log into the firewall.

The first step in this process is to define an LDAP server profile which contains specific information that the firewall can use when sending queries for authentication.

1. In the web interface, select **Device > Server Profiles > LDAP**. At the bottom of the window, click **Add**.



2. In the **LDAP Server Profile** window, enter **LDAP Server Profile** for the **Profile Name**. Under the **Server List**, click **Add**. Enter **ldap.panw.lab** for the **Name**, **192.168.50.89** for the **LDAP Server**, and confirm **389** populates for the **Port** number.

LDAP Server Profile

Profile Name	LDAP Server Profile							
<input type="checkbox"/> Administrator Use Only								
Server List <table border="1"> <thead> <tr> <th>NAME</th> <th>LDAP SERVER</th> <th>PORT</th> </tr> </thead> <tbody> <tr> <td>ldap.panw.lab</td> <td>192.168.50.89</td> <td>389</td> </tr> </tbody> </table>			NAME	LDAP SERVER	PORT	ldap.panw.lab	192.168.50.89	389
NAME	LDAP SERVER	PORT						
ldap.panw.lab	192.168.50.89	389						
<input type="button" value="(+ Add)"/> <input type="button" value="(- Delete)"/>								

3. In the **Server Settings** section, enter **dc=panw,dc=lab** for **Base DN**, enter **cn=admin,dc=panw,dc=lab** for **Bind DN**, enter **Pa10Alt0!** for **Password** and **Confirm Password** and uncheck **Require SSL/TLS secured connection**. Click **OK**.

Server Settings

Type	other
Base DN	dc=panw,dc=lab
Bind DN	cn=admin,dc=panw,dc=lab
Password	*****
Confirm Password	*****
Bind Timeout	30
Search Timeout	30
Retry Interval	60
<input type="checkbox"/> Require SSL/TLS secured connection	
<input type="checkbox"/> Verify Server Certificate for SSL sessions	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Please
Note

With your LDAP Server Profile in place, you will now create an Authentication Profile and reference the LDAP Server Profile you just created.

4. Verify the *LDAP Server Profile* is showing.

	NAME	LOCATION	SERVERS	OTHERS
<input checked="" type="checkbox"/>	LDAP Server Profile		Name: ldap.panw.lab LDAP Server: 192.168.50.89 Port: 389	Base: dc=panw,dc=lab Bind DN: cn=admin,dc=panw,dc=lab

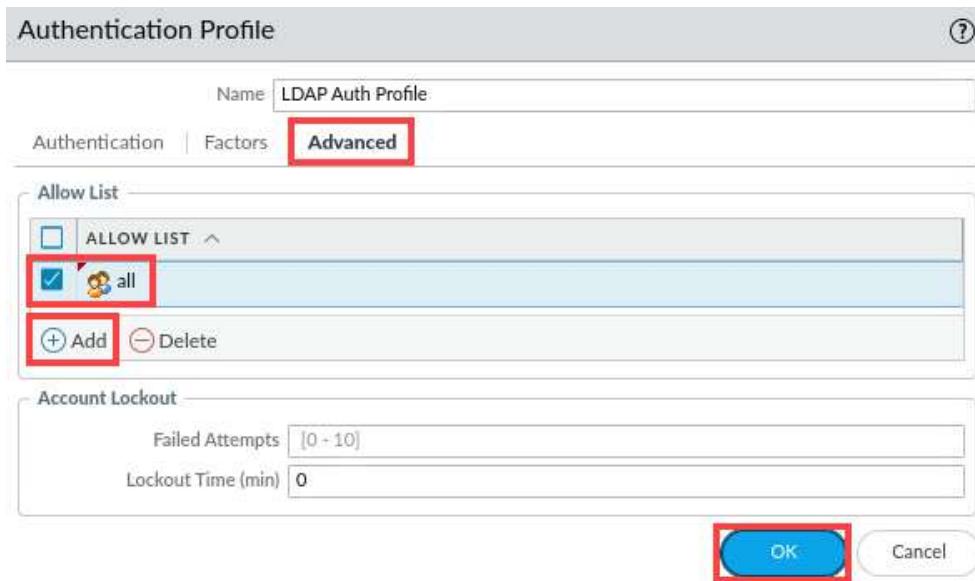
5. Select **Device > Authentication Profile**. Click **Add**.

The screenshot shows the PA-VM interface with the 'DEVICE' tab selected. On the left, a sidebar lists various configuration options, with 'Authentication Profile' highlighted. The main area displays a table of authentication profiles. One profile, 'Local-Database', is listed. Below the table, there are buttons for 'Add', 'Delete', 'Clone', and 'PDF/CSV'. The 'Add' button is specifically highlighted with a red box.

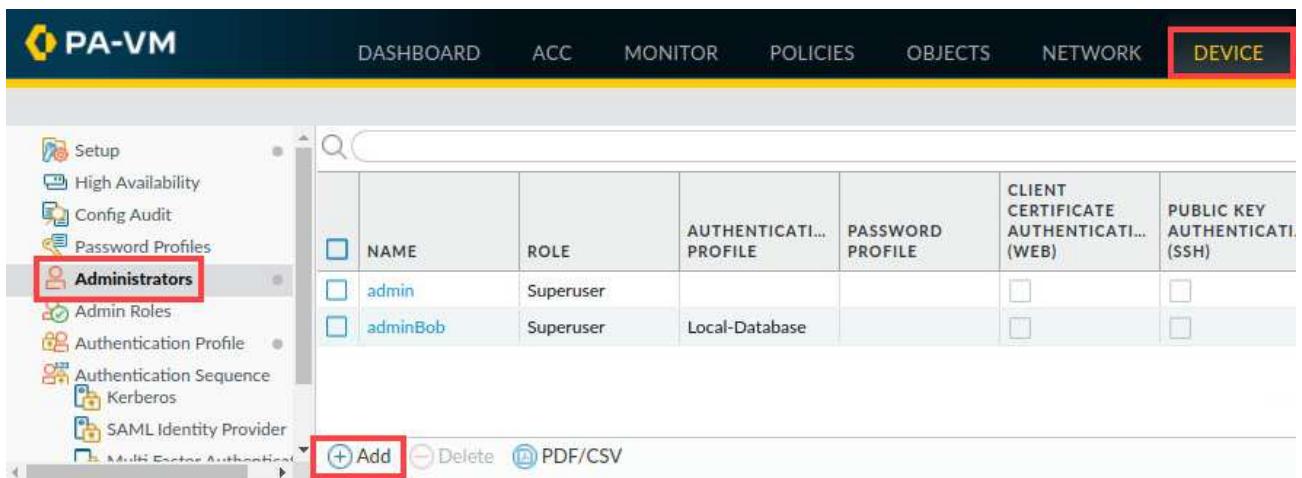
6. In the *Authentication Profile* window, type **LDAP Auth Profile** for the *Name*. Select **LDAP** for the *Type* and **LDAP Server Profile** for the *Server Profile*. Click **Advanced**.

The screenshot shows the 'Authentication Profile' configuration window. The 'Name' field contains 'LDAP Auth Profile'. The 'Type' dropdown is set to 'LDAP'. The 'Server Profile' dropdown is set to 'LDAP Server Profile'. The 'Factors' tab is selected, and the 'Advanced' button is highlighted with a red box. The 'Login Attribute' field is also visible.

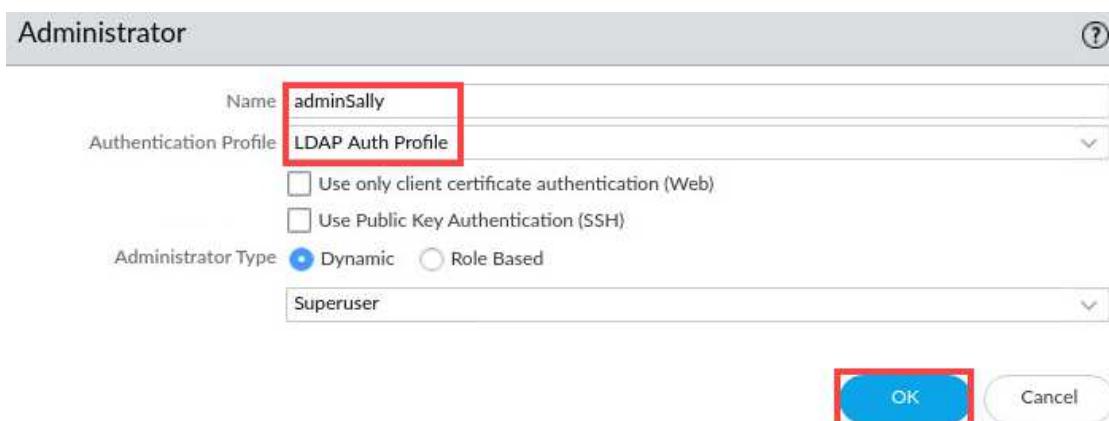
7. On the *Advanced* tab, in the *Allow List*, click **Add**. Select **all** and click **OK**.



8. Navigate to **Device > Administrators** and click **Add**.



9. In the *Administrator* window, type **adminSally** for the *Name*. Select **LDAP Auth Profile** for the *Authentication Profile*. Click **OK**.



Please
Note

The *adminSally* account is one which exists in the LDAP server.

- Click the **Commit** link located at the top-right of the web interface.



- In the *Commit* window, click **Commit** to proceed with committing the changes.

Commit

Doing a commit will overwrite the running configuration with the commit scope.

Commit All Changes Commit Changes Made By: (1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
device-and-network	Device and Network Configuration			
shared-object	Shared			

Preview Changes Change Summary Validate Commit

Note: This shows all the changes in login admin's accessible domain.

Description

Commit **Cancel**

- When the commit operation successfully completes, click **Close** to continue.

Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit

Close

13. Log out of the firewall web interface by clicking the **Logout** button in the bottom left corner of the window.



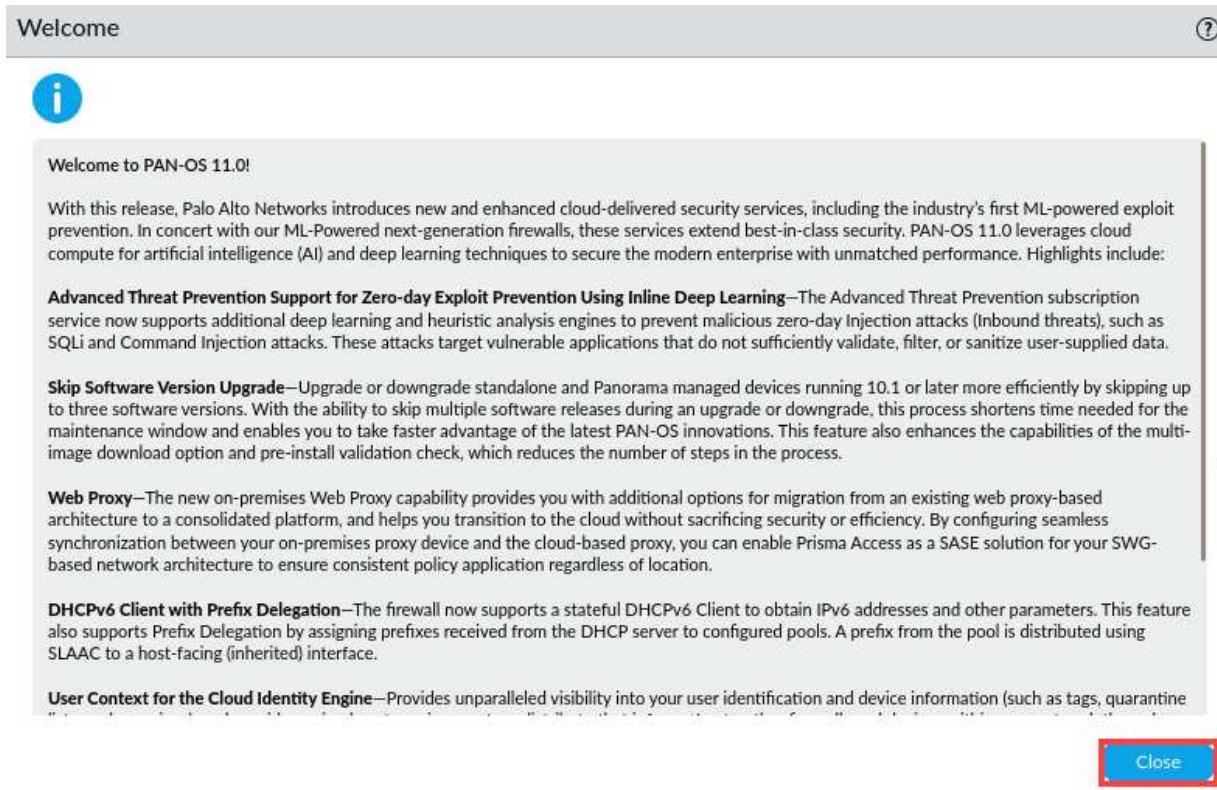
14. In the *Log In* window, click **Log In**.



15. Log back into the firewall as username **adminSally**, password **Pa10Alt0!**. Click **Log In**.



16. In the *Welcome* window, click **Close**.



The screenshot shows the 'Welcome' window for PAN-OS 11.0. At the top left is a blue circular icon with a white 'i'. At the top right are a magnifying glass icon and a question mark icon. The main content area has a light gray background with a dark gray sidebar on the right. The sidebar contains a small downward arrow icon. The text in the main area is as follows:

Welcome to PAN-OS 11.0!

With this release, Palo Alto Networks introduces new and enhanced cloud-delivered security services, including the industry's first ML-powered exploit prevention. In concert with our ML-Powered next-generation firewalls, these services extend best-in-class security. PAN-OS 11.0 leverages cloud compute for artificial intelligence (AI) and deep learning techniques to secure the modern enterprise with unmatched performance. Highlights include:

Advanced Threat Prevention Support for Zero-day Exploit Prevention Using Inline Deep Learning—The Advanced Threat Prevention subscription service now supports additional deep learning and heuristic analysis engines to prevent malicious zero-day Injection attacks (Inbound threats), such as SQLi and Command Injection attacks. These attacks target vulnerable applications that do not sufficiently validate, filter, or sanitize user-supplied data.

Skip Software Version Upgrade—Upgrade or downgrade standalone and Panorama managed devices running 10.1 or later more efficiently by skipping up to three software versions. With the ability to skip multiple software releases during an upgrade or downgrade, this process shortens time needed for the maintenance window and enables you to take faster advantage of the latest PAN-OS innovations. This feature also enhances the capabilities of the multi-image download option and pre-install validation check, which reduces the number of steps in the process.

Web Proxy—The new on-premises Web Proxy capability provides you with additional options for migration from an existing web proxy-based architecture to a consolidated platform, and helps you transition to the cloud without sacrificing security or efficiency. By configuring seamless synchronization between your on-premises proxy device and the cloud-based proxy, you can enable Prisma Access as a SASE solution for your SWG-based network architecture to ensure consistent policy application regardless of location.

DHCPv6 Client with Prefix Delegation—The firewall now supports a stateful DHCPv6 Client to obtain IPv6 addresses and other parameters. This feature also supports Prefix Delegation by assigning prefixes received from the DHCP server to configured pools. A prefix from the pool is distributed using SLAAC to a host-facing (inherited) interface.

User Context for the Cloud Identity Engine—Provides unparalleled visibility into your user identification and device information (such as tags, quarantine

Close

17. Navigate to **Monitor > Logs > System**. Look for an entry with **Type > Auth**. You may need to scroll through the logs to find the *auth* type.

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
09/21 04:05:49	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:49	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:48	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:48	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:48	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:48	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:48	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:48	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:48	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:48	url-filtering	high	url-cloud-connection-failure		Cloud is not ready. There was no update from the cloud in the last 20 minutes.
09/21 04:05:43	general	informational	general		User adminSally logged in via Web from 192.168.1.20 using https
09/21 04:05:43	auth	informational	auth-success	LDAP Auth Profile	authenticated for user 'adminSally' auth profile 'LDAP Auth Profile', vsys 'shared', server profile 'LDAP Server Profile', server address '192.168.50.89'; From: 192.168.1.20.
09/21 04:05:43	auth	medium	auth-server-up		LDAP auth server 192.168.50.89 is up !!!
09/21 04:05:31	general	informational	general		User admin logged out via Web from 192.168.1.20

Please
Note

Note that the entry in the firewall system log indicates that adminSally was successfully authenticated against the **LDAP Server**.

If you do not see an entry in the System log indicating a successful authentication for adminSally, you can use a filter (subtype eq auth) as the syntax.

18. Log out of the Firewall.



19. In the *Log In* window, click **Log In**.



You have successfully logged out.

Log In

20. Log back into the firewall with the **admin/Pal0Alt0!** credentials.

A screenshot of a web browser showing the Palo Alto Networks login interface. The page has a white background with a yellow border around the main content area. At the top is the Palo Alto Networks logo. Below it is a form with two input fields: the first field contains the text "admin" and the second field contains a redacted password. At the bottom is a blue "Log In" button.

21. Leave the firewall web interface open to continue with the next task.

2.6 Configure RADIUS Authentication

Your organization has recently acquired another company. The newly acquired company maintains all network administrator accounts in a RADIUS server. You need to incorporate RADIUS authentication for the firewall so the new network administrators who have joined your team can access the firewall for management purposes.

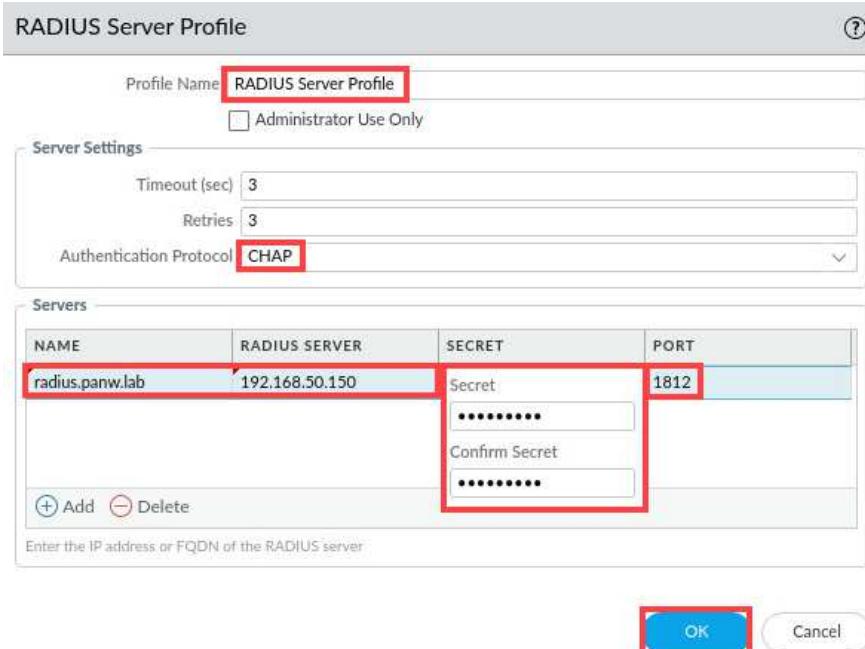
For this section, you will configure RADIUS Authentication and test the user adminHelga can login in.

1. Navigate to Device > Server Profiles > RADIUS. Click Add.

The screenshot shows the PA-VM interface with the following navigation path:

- Main menu: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE (highlighted with a red box).
- Left sidebar:
 - Config Audit
 - Password Profiles
 - Administrators
 - Admin Roles
 - Authentication Profile
- Central pane:
 - Search bar: NAME, LOCATION, SERVERS
 - Table header: NAME, LOCATION, SERVERS
- Left sidebar (continued):
 - Response Pages
 - Log Settings
 - Server Profiles (highlighted with a red box)
 - SNMP Trap
 - Syslog
 - Email
 - HTTP
 - Netflow
 - RADIUS (highlighted with a red box)
 - TACACS+
 - LDAP
 - Kerberos
 - SAML Identity Provider
 - Multi Factor Authentication
 - Local User Database
 - Users
- Bottom right: + Add, Delete, Clone, PDF/CSV

2. In the **RADIUS Server Profile** window, enter **RADIUS Server Profile** for the **Profile Name**. For the **Authentication Protocol**, select **CHAP**. Under the **Servers** section, click **Add**. For the server **Name** field, enter **radius.panw.lab**. For the **RADIUS Server** field, enter **192.168.50.150**. Enter **Pa10Alt0!** for **Secret** and **Confirm Secret**. Leave the **Port** set to **1812**. Click **OK**.



Never use CHAP in a production environment because it is not secure. We are using it in the lab for the sake of simplicity.

3. Navigate to **Device > Authentication Profile**. Click **Add**.

NAME	LOCATION	Lockout		ALLOW LIST	AUTHENT
		FAILED ATTEMPTS (#)	LOCKOUT TIME (MIN)		
Local-Database		0	0		all
LDAP Auth Profile		0	0		all

4. In the *Authentication Profile* window, enter **RADIUS Auth Profile** for the *Profile Name*. For the *Type*, select **RADIUS**. For the *Server Profile*, select **RADIUS Server Profile**. Click the **Advanced** tab.

Authentication Profile

Name	RADIUS Auth Profile	
Authentication	Factors	Advanced
Type	RADIUS	
Server Profile	RADIUS Server Profile	
<input type="checkbox"/> Retrieve user group from RADIUS		

5. Under the *Allow List*, click **Add**. Select **all** and click **OK**.

Authentication Profile

Name	RADIUS Auth Profile	
Authentication	Factors	Advanced
Allow List		
<input type="checkbox"/> ALLOW LIST		
<input checked="" type="checkbox"/> all		
+ Add - Delete		
Account Lockout		
Failed Attempts [0 - 10]		
Lockout Time (min) 0		
OK Cancel		

6. To test *RADIUS Authentication*, create an *administrator* account named **adminHelga** by selecting **Device > Administrators**. Click **Add**.

<input type="checkbox"/> NAME	ROLE	AUTHENTICATI... PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)
<input type="checkbox"/> admin	Superuser			<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> adminBob	Superuser	Local-Database		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> adminSally	Superuser	LDAP Auth Profile		<input type="checkbox"/>	<input type="checkbox"/>

7. In the *Administrator* window, enter **adminHelga** for the *Name*. For the *Authentication Profile*, select **RADIUS Auth Profile**. Click **OK**.

Administrator

Name:

Authentication Profile:

Use only client certificate authentication (Web)
 Use Public Key Authentication (SSH)

Administrator Type: Dynamic Role Based

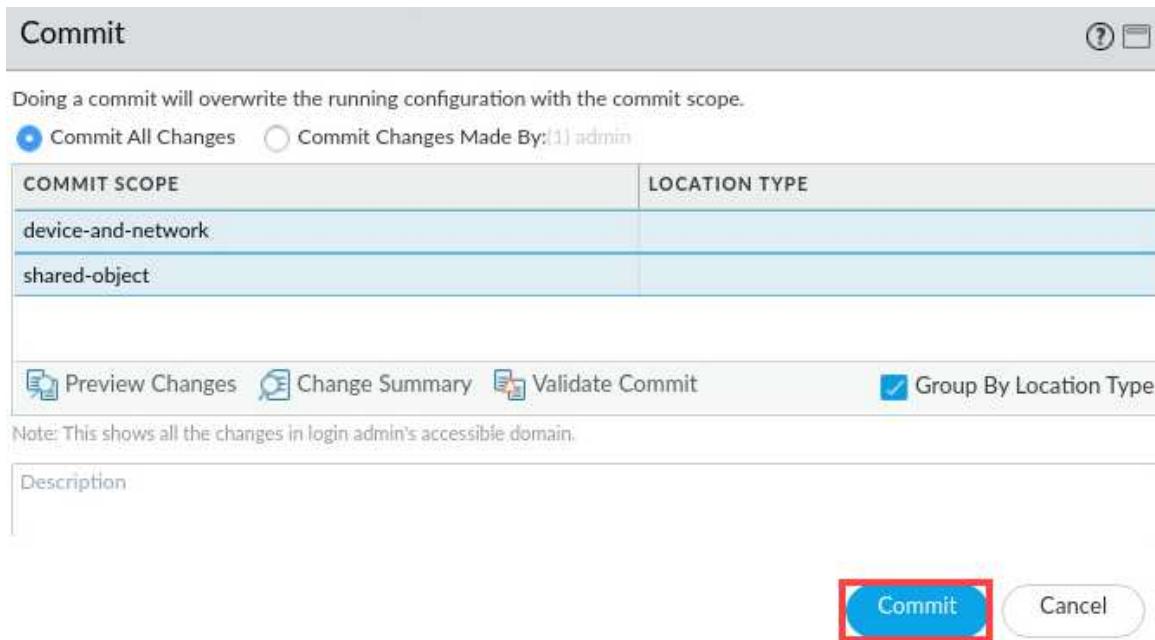
Superuser:

OK Cancel

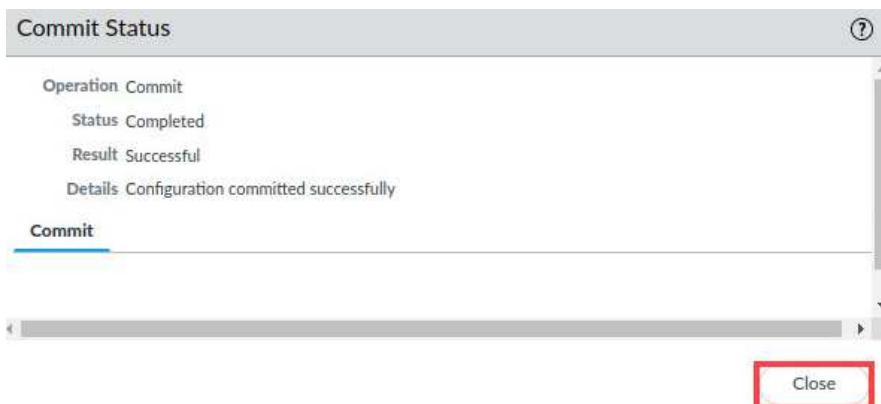
8. Click the **Commit** link located at the top-right of the web interface.



9. In the **Commit** window, click **Commit** to proceed with committing the changes.



10. When the commit operation successfully completes, click **Close** to continue.



11. Log out of the firewall web interface by clicking the **Logout** button in the bottom left corner of the window.



12. In the *Log In* window, click **Log In**.



You have successfully logged out.

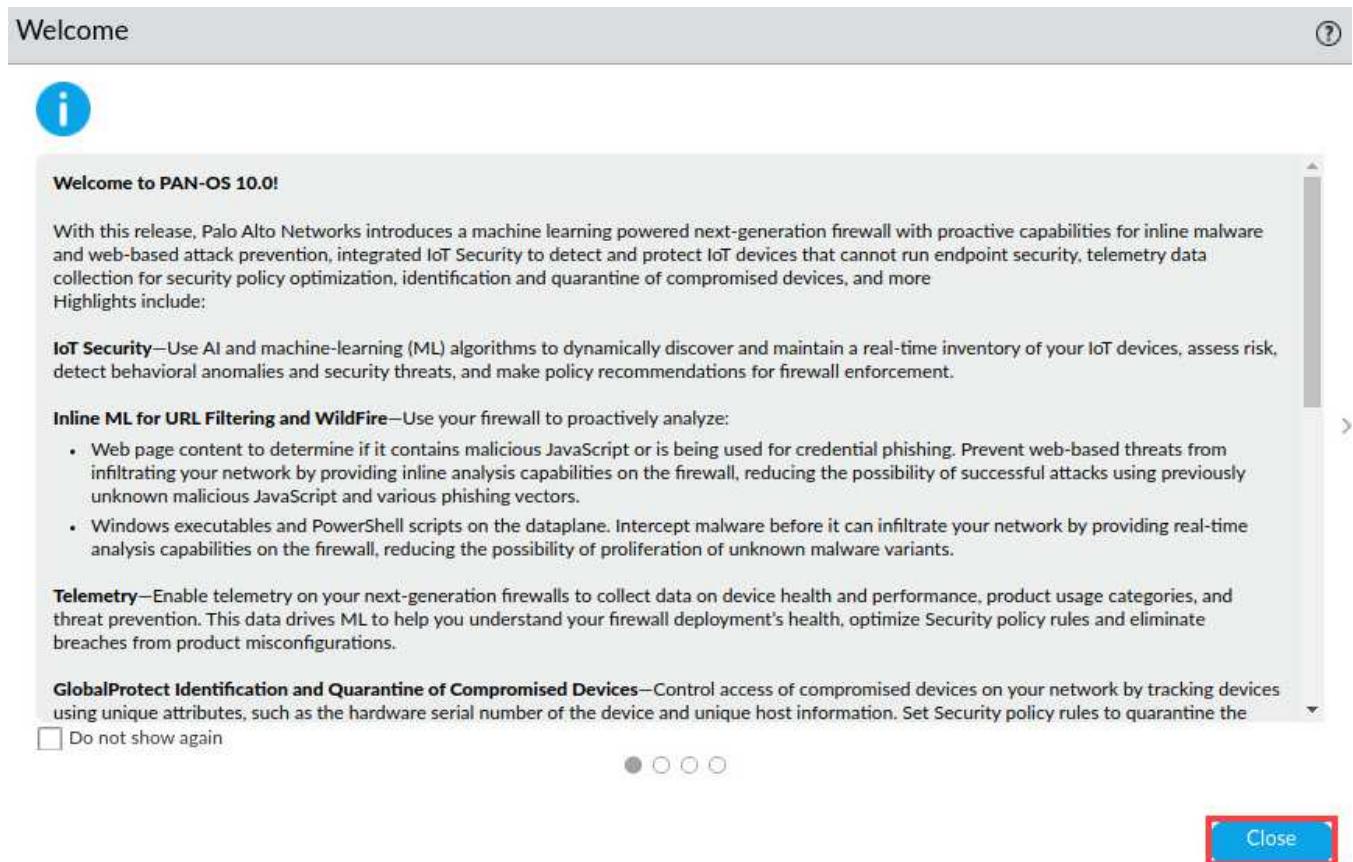
Log In

13. Log back into the firewall as username **adminHelga**, password **Pa10Alt0!**. Click **Log In**.



adminHelga

Log In

14. In the *Welcome* window, click **Close**.15. Select **Monitor > Logs > System**. Look for an entry with **Type > Auth**. You may need to scroll through the logs to find the *auth* type.

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
09/21 04:14:26	url-filtering	high	url-cloud-connection-failure		CURL ERROR: Could not resolve host: s0000.urlcloud.paloaltonetworks.com
09/21 04:14:01	dns-security	medium	PAN_ELOG_EVENT_...	dns-signature	DNS Security cloud query timeout.
09/21 04:13:55	general	informational	general		User adminHelga logged in via Web from 192.168.1.20 using https
09/21 04:13:55	auth	informational	auth-success	Radius Auth Profile	When authenticating user 'adminHelga' from '192.168.1.20', a less secure authentication method CHAP is used. Please migrate to PEAP or EAP-TTLS. Authentication Profile 'Radius Auth Profile', vsys 'shared', Server Profile 'RADIUS Server Profile', Server Address '192.168.50.150'
09/21 04:13:55	auth	informational	auth-success	Radius Auth Profile	authenticated for user 'adminHelga'. auth profile 'Radius Auth Profile', vsys 'shared', server profile 'RADIUS Server Profile', server address '192.168.50.150', auth protocol 'CHAP', From: 192.168.1.20,
09/21 04:13:42	general	informational	general		User admin logged out via Web from 192.168.1.20

Please Note

Note that the entry in the firewall system log indicates that adminHelga was successfully authenticated against the **RADIUS Profile**.

If you do not see an entry in the System log indicating a successful authentication for adminHelga, you can use a filter (subtype eq auth) as the syntax.

16. Log out of the Firewall.



17. In the *Log In* window, click **Log In**.



18. Log back into the firewall with the **admin/Pal0Alt0!** credentials.



19. Leave the firewall web interface open to continue with the next task.

2.7 Configure and Authentication Sequence

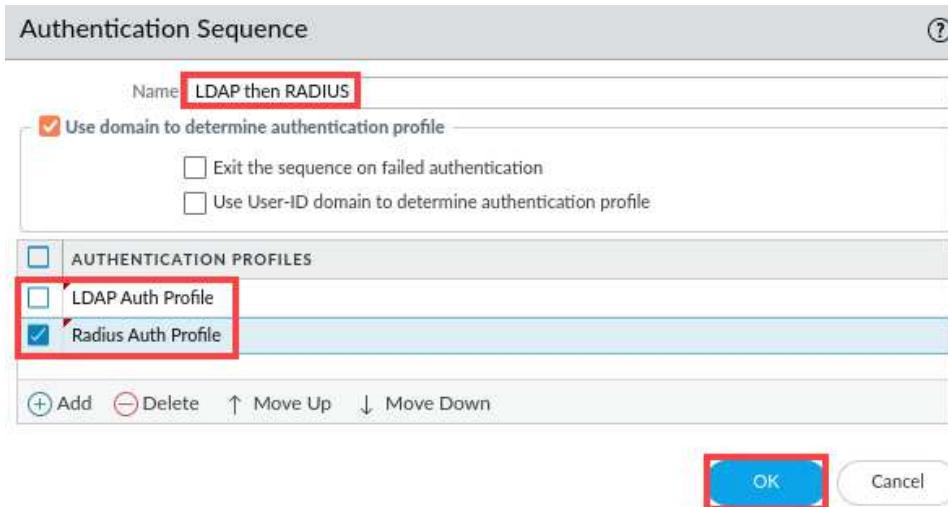
Since the acquisition, some administrator accounts exist in LDAP and other accounts exist in RADIUS. With administrator accounts in these two different systems, you need to configure the firewall so that it can check both external databases when an administrator attempts to log in.

In this section you will accomplish this by creating an Authentication Sequence. The sequence will instruct the firewall to check an account against LDAP first and then against RADIUS if the account does not exist in LDAP (or if the LDAP server is unavailable).

1. Navigate to Device > Authentication Sequence. Click Add.

The screenshot shows the PA-VM interface with the 'DEVICE' tab selected. The left sidebar contains a list of configuration items: Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, **Authentication Sequence**, User Identification, Data Redistribution, and Device Configuration. The 'Authentication Sequence' item is highlighted with a red box. The main content area displays a table with columns 'NAME' and 'LOCATION'. Below the table, a list of authentication providers is shown: LDAP, Kerberos, SAML Identity Provider, and Multi Factor Authentication. A red box highlights the '+ Add' button located at the bottom of this list.

2. In the *Authentication Sequence* window, type **LDAP** then **RADIUS** for the *Name*. Under the *Authentication Profiles*, click **Add**. Select **LDAP Auth Profile**. Click **Add** again and select **RADIUS Auth Profile**. Click **OK**.

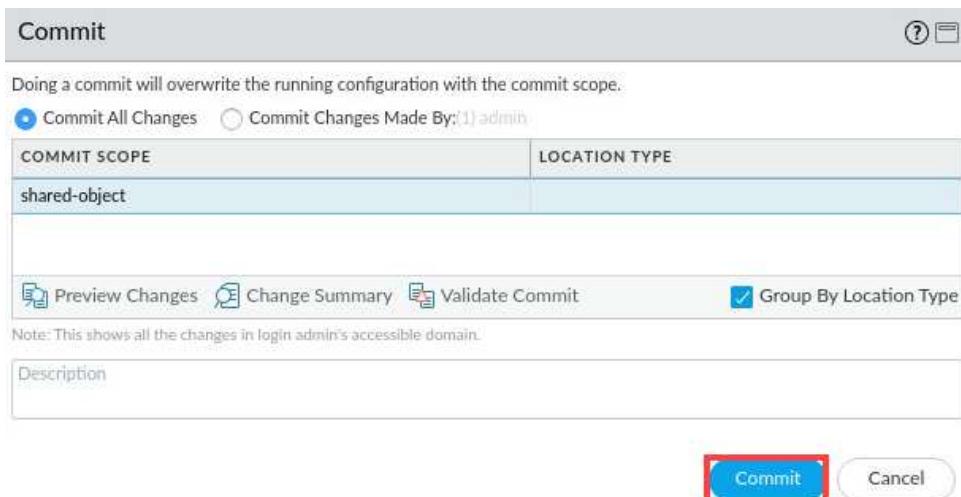


Note the Move Up and Move Down buttons. These allow you to change the order of the Authentication Profiles if necessary. In this example, the firewall will use the LDAP-Auth-Profile first when an administrator logs in to attempt authentication; if the user account does not exist in LDAP (or if the LDAP server is unavailable), the firewall will use the RADIUS-Auth-Profile to attempt authentication.

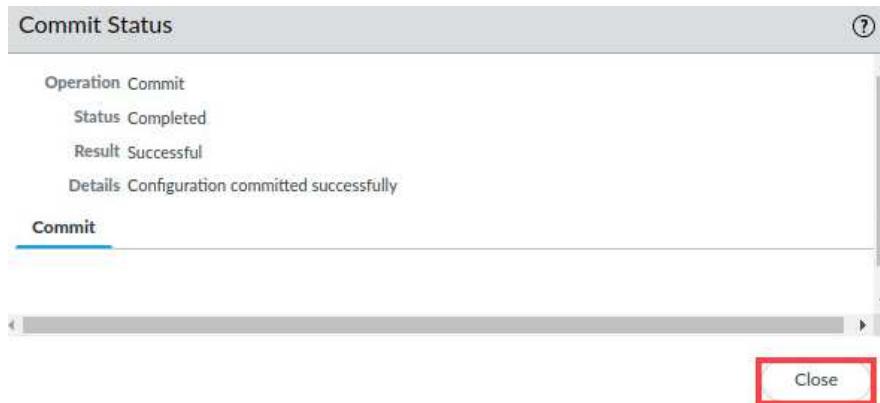
3. Click the **Commit** link located at the top-right of the web interface.



4. In the *Commit* window, click **Commit** to proceed with committing the changes.



5. When the commit operation successfully completes, click **Close** to continue.



6. The lab is now complete; you may end your reservation.