



PALO ALTO NETWORKS EDU 210

Lab 3: Working with Firewall Administrator Accounts

Document Version: 2021-09-27

Contents

Introduction	3
Objective	3
Lab Topology	4
Theoretical Lab Topology.....	4
Lab Settings	5
3 Working with Firewall Configurations and Log Files	6
3.1 Apply a Baseline Configuration to the Firewall.....	6
3.2 Create a Local Database Authentication Profile	12
3.3 Create a Local User Database Account	14
3.4 Create an Administrator Account.....	15
3.5 Configure LDAP Authentication.....	22
3.6 Configure RADIUS Authentication.....	33
3.7 Configure and Authentication Sequence	42

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.

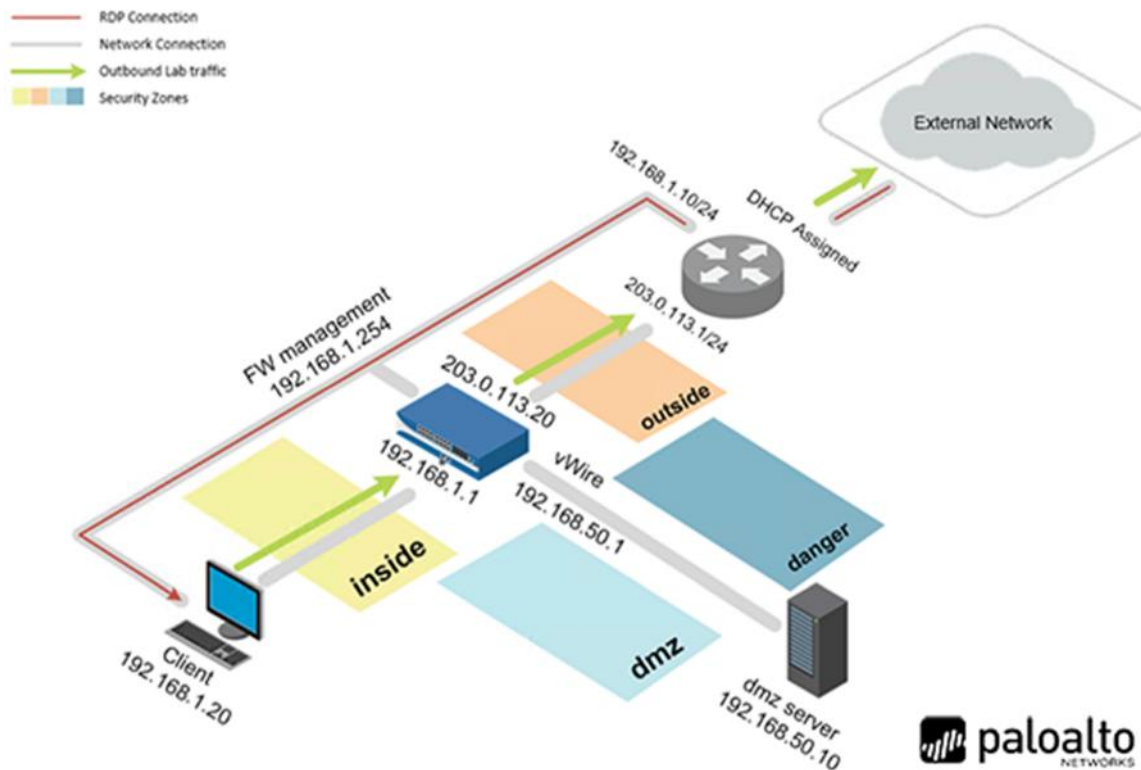
In this lab, you will provide management with those types of reports and to be able to restrict the applications.

Objective

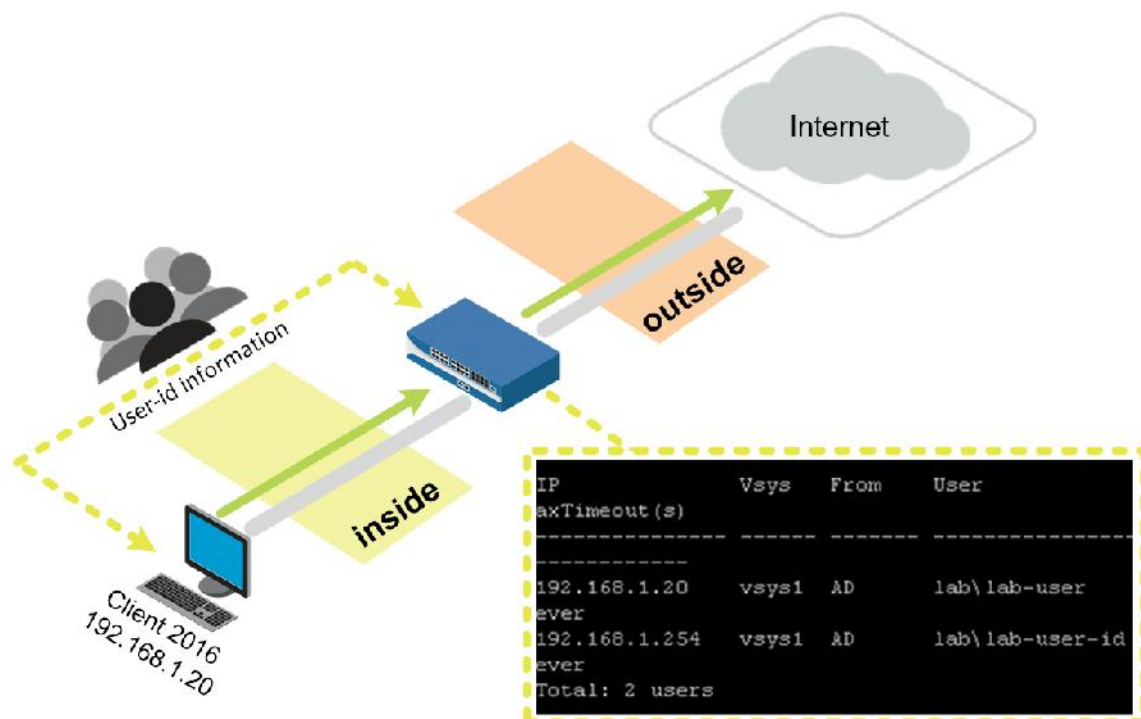
In this lab, you will perform the following tasks:

-) 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 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	Pa10Alt0!
DMZ	192.168.50.10	root	Pa10Alt0!
Firewall	192.168.1.254	admin	Pa10Alt0!
VRouter	192.168.1.10	root	Pa10Alt0!

3 Working with Firewall Configurations and Log Files

3.1 Apply a Baseline Configuration to the Firewall

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

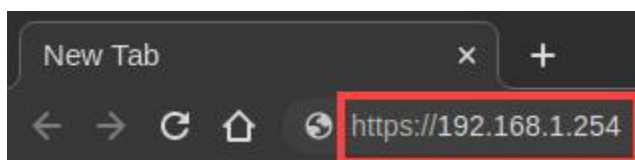
1. Click on the **Client** tab to access the *Client PC*.



2. Double-click the **Chromium Web Browser** icon located on the *desktop*.



3. In the *Chromium* address field, type **https://192.168.1.254** and press **Enter**.



4. You will see a “*Your connection is not private*” message. Click on the **ADVANCED** link.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Advanced

Back to safety



If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

- Click on **Proceed to 192.168.1.254 (unsafe)**.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Hide advanced

Back to safety

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

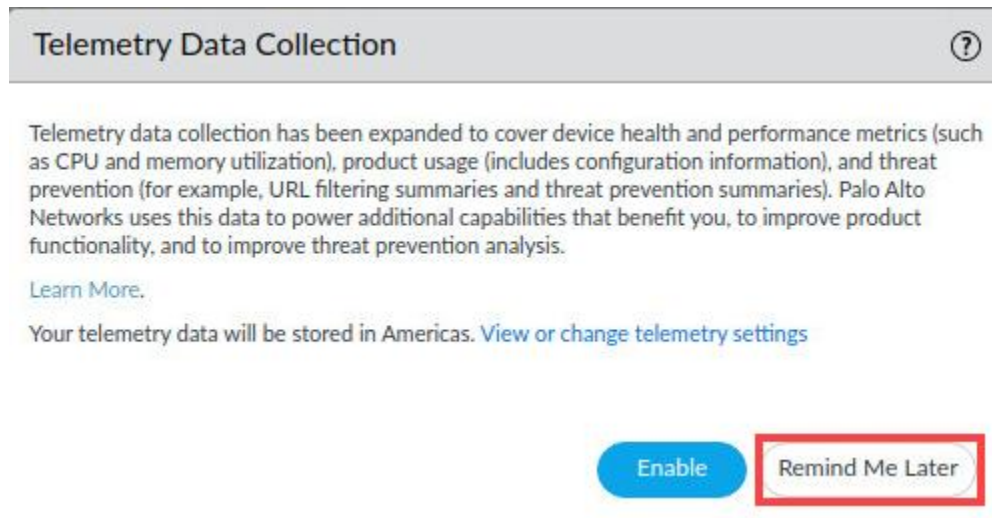
[Proceed to 192.168.1.254 \(unsafe\)](#)

- Log in to the firewall web interface as username **admin**, password **Pal0Alt0!**.



The image shows the Palo Alto Networks login page. It features the Palo Alto Networks logo at the top. Below the logo, there is a username field containing the text "admin" and a password field filled with dots. A blue "Log In" button is positioned below the password field. The entire login form is enclosed in a yellow rectangular border.

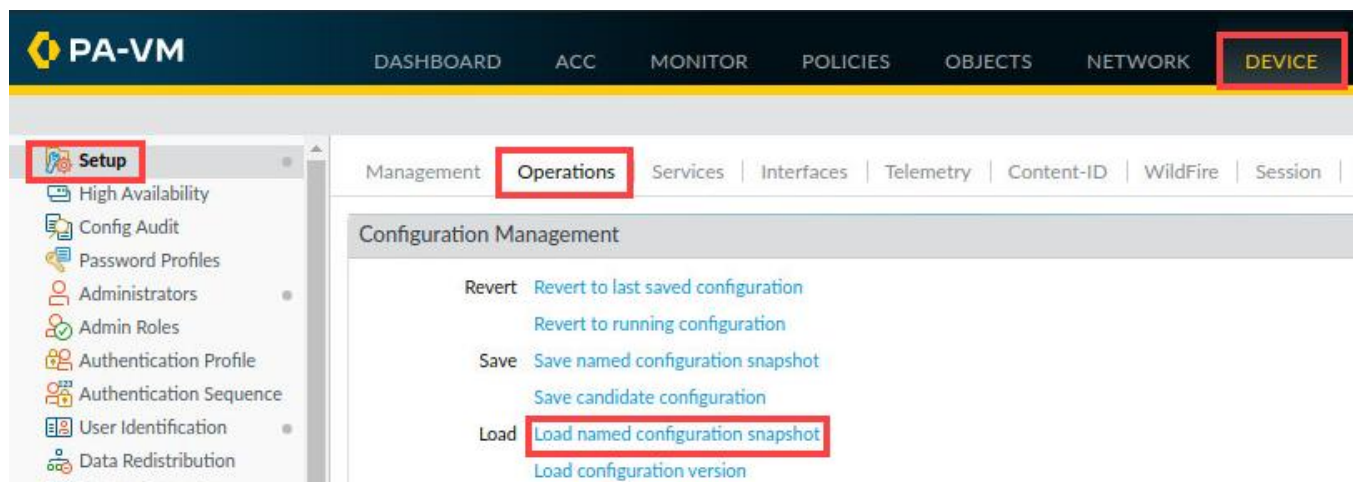
7. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.



Please Note

Before you can enable Telemetry Data Collection, you will need to install a device certificate. For this lab, you will not be using Telemetry Data Collection.

8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

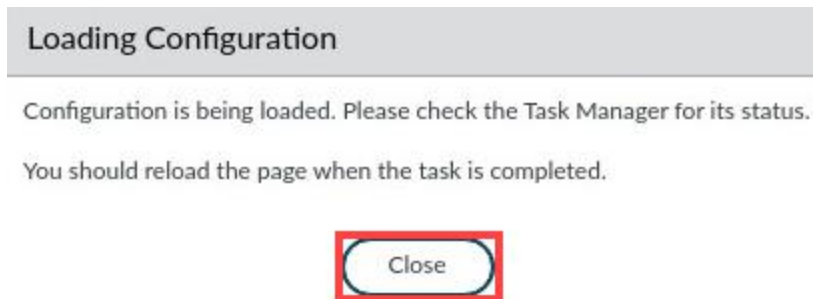


9. In the *Load Named Configuration* window, select **edu-210-lab-03.xml** from the *Name* dropdown box and click **OK**.



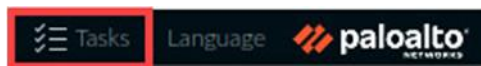
The **Load Named Configuration** dialog box is shown. The **Name** dropdown menu is open, and **edu-210-lab-03.xml** is selected. The **Decryption Key** dropdown menu is also open, showing four asterisks. Below these fields are two checkboxes: **Regenerate Rule UUIDs for selected named configuration** and **Skip Validation**, both of which are unchecked. At the bottom right, there are two buttons: **OK** (highlighted with a red box) and **Cancel**.

10. 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.



The **Loading Configuration** message box is shown. It contains the text: **Configuration is being loaded. Please check the Task Manager for its status.** and **You should reload the page when the task is completed.** At the bottom center, there is a **Close** button (highlighted with a red box).

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



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

Task Manager - All Tasks

8 items

TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/05/21 00:03:04		
Load	Completed	08/05/21 00:01:59		
EDLRefresh	Completed	08/04/21 23:58:15		
EDLFetch	Completed	08/04/21 23:58:14		
Download	Completed	08/04/21 23:58:04		
Download	Completed	08/04/21 23:54:04		
EDLFetch	Completed	08/04/21 23:53:13		
Auto Commit	Completed	08/04/21 23:52:45		

Show All Tasks Clear Commit Queue

Close

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






14. 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 SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

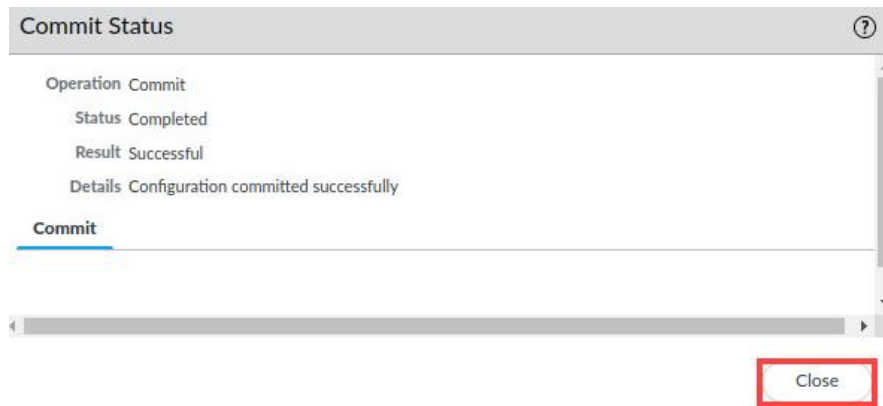
 Preview Changes
  Change Summary
  Validate Commit
 ☒ Group By Location Type

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

Description

Commit Cancel

15. When the *Commit* operation successfully completes, click **Close** to continue.



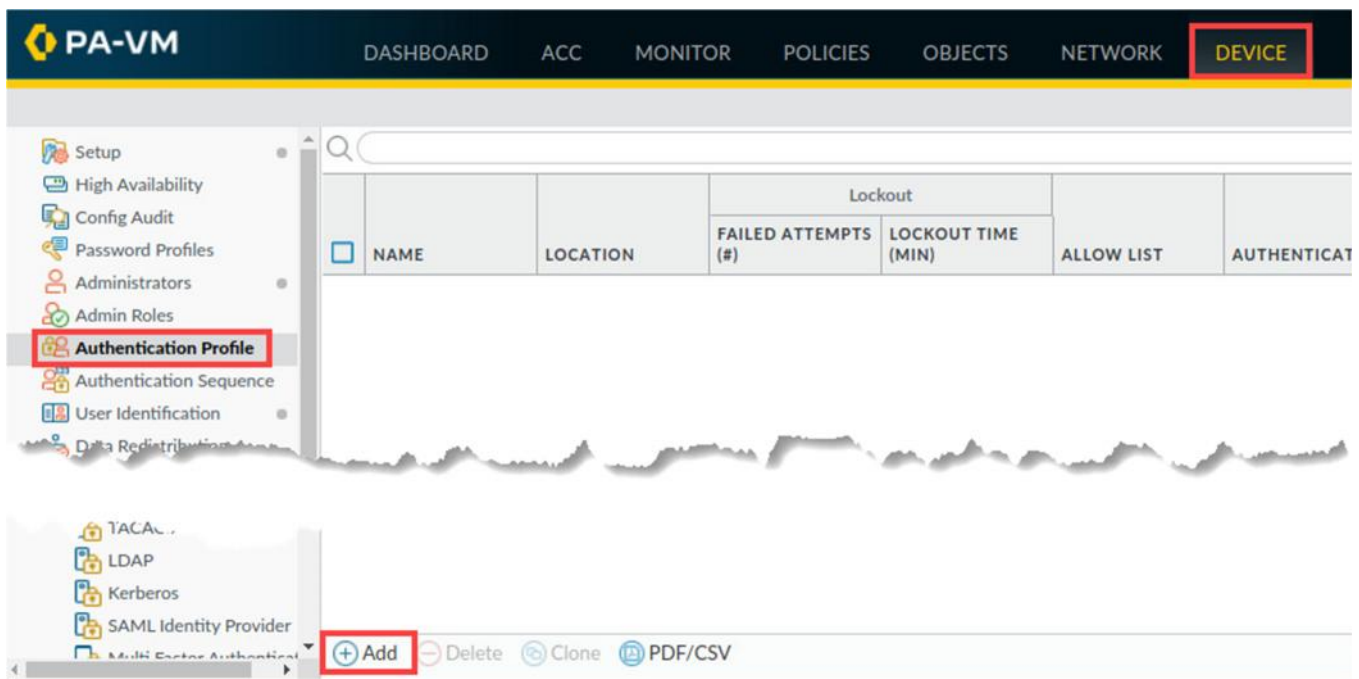
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

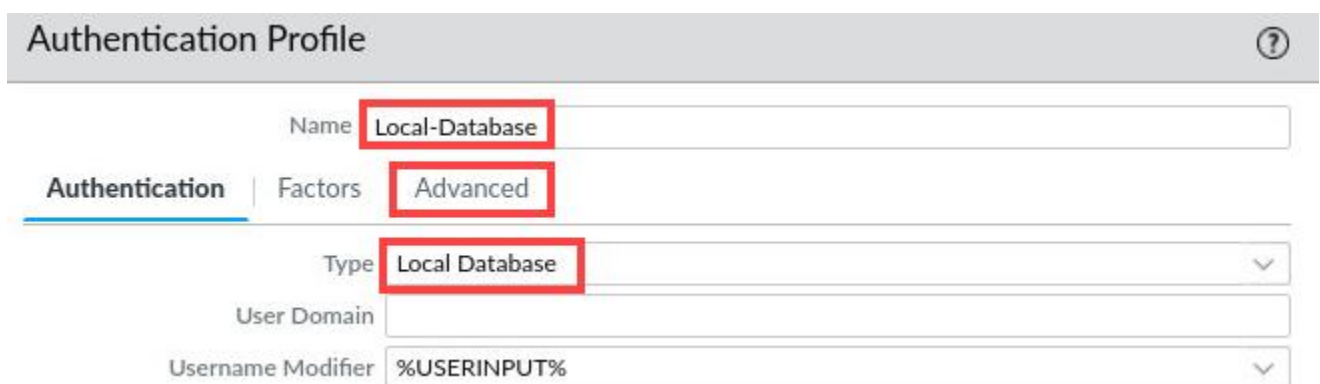
3.2 Create a Local Database Authentication Profile

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.

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



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



Authentication Profile ⓘ

Name **Local-Database**

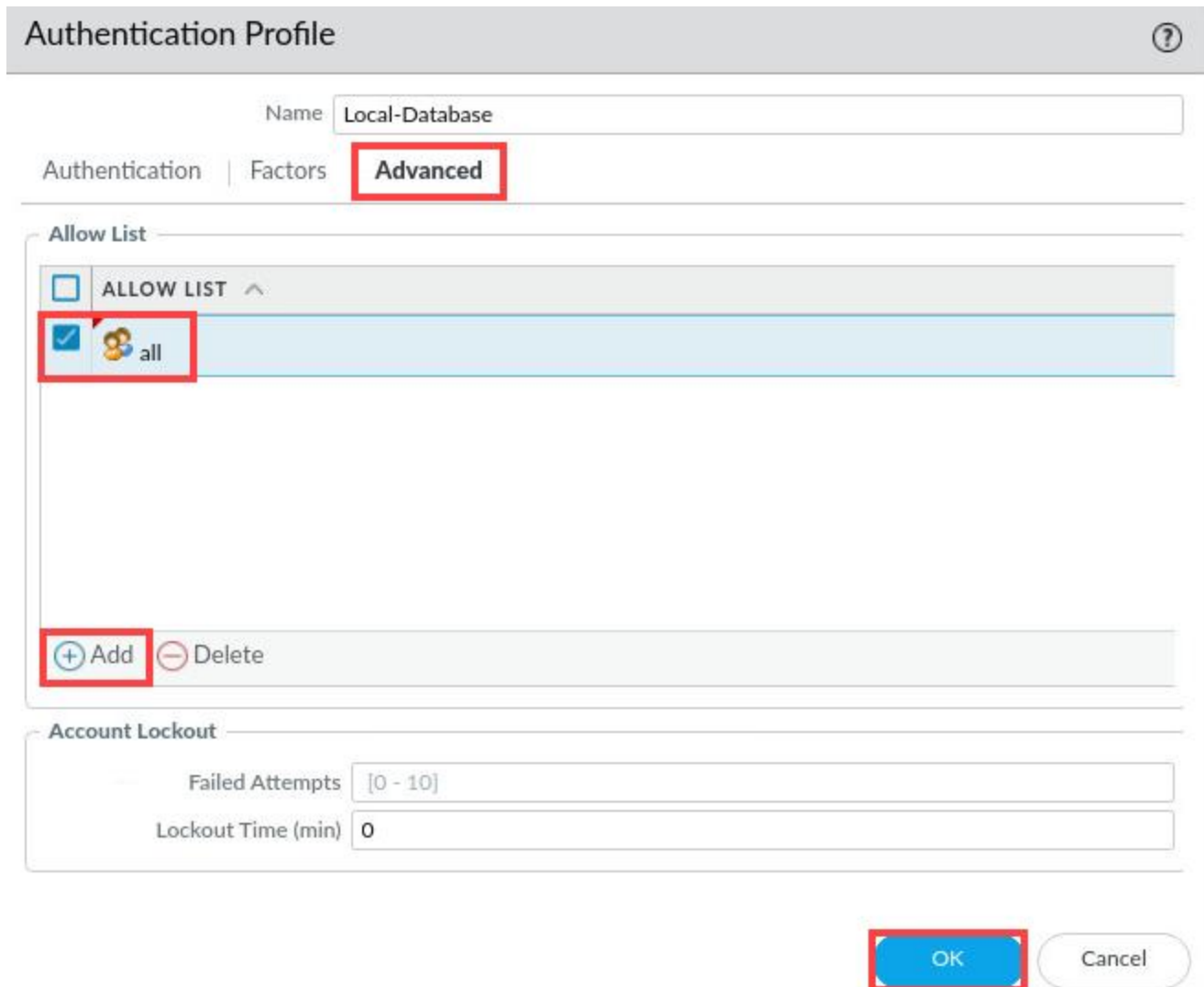
Authentication | Factors **Advanced**

Type **Local Database** ▼

User Domain

Username Modifier **%USERINPUT%** ▼

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




Authentication Profile ⓘ

Name: Local-Database

Authentication | Factors | **Advanced**

Allow List

☐ ALLOW LIST ^

☒  all

Account Lockout

Failed Attempts: [0 - 10]

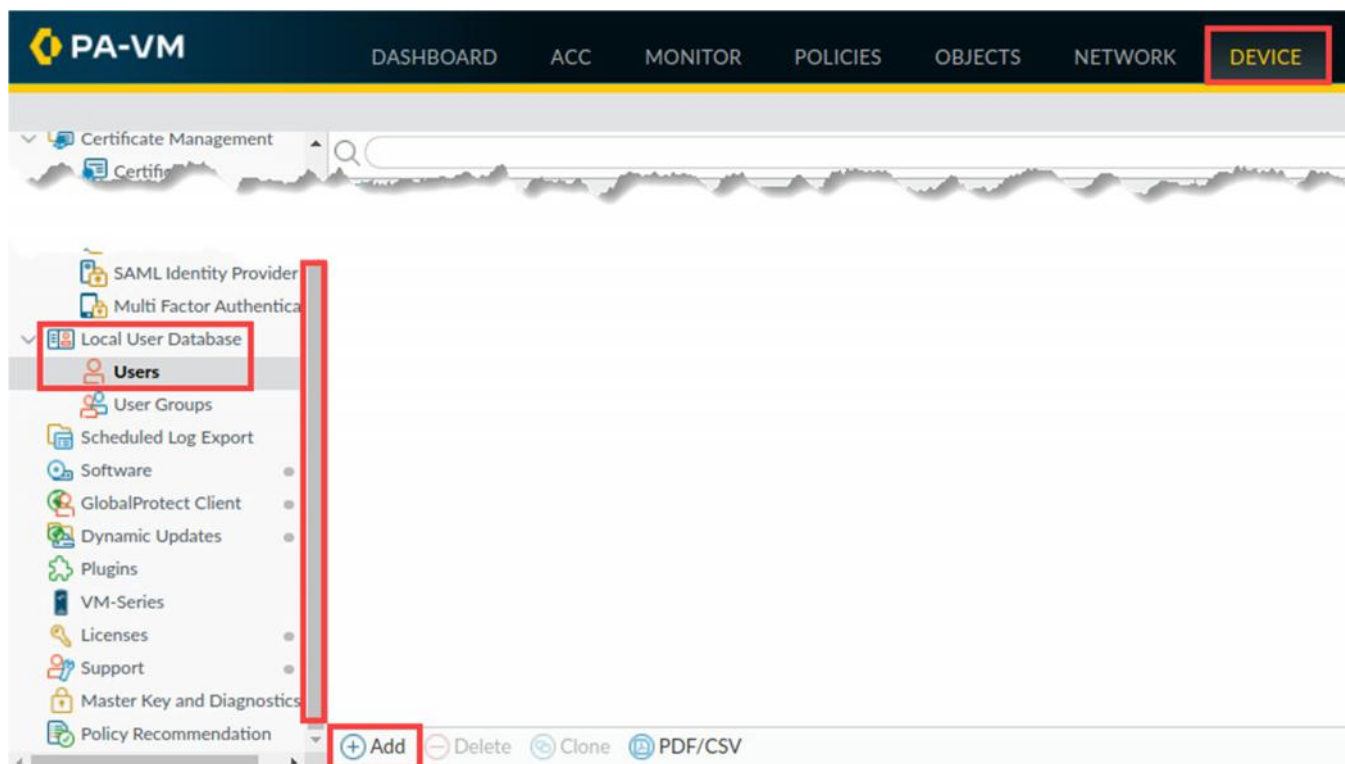
Lockout Time (min): 0

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

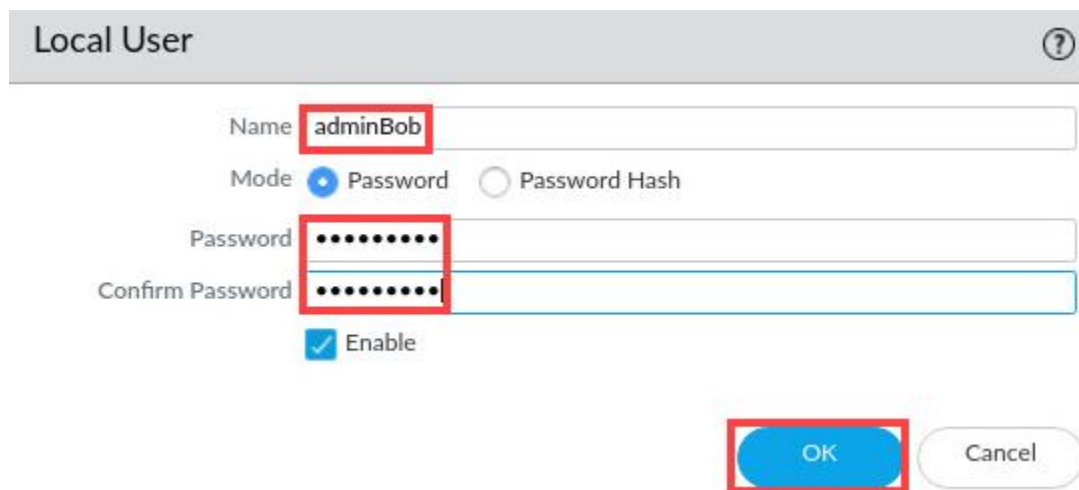
3.3 Create a Local User Database Account

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 Users 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 dropdown.



2. In the *Local User* window, type **adminBob** for the *Name* field. Enter **Pa10A1t0!** for *Password* and *Confirm Password*. Click **OK**.

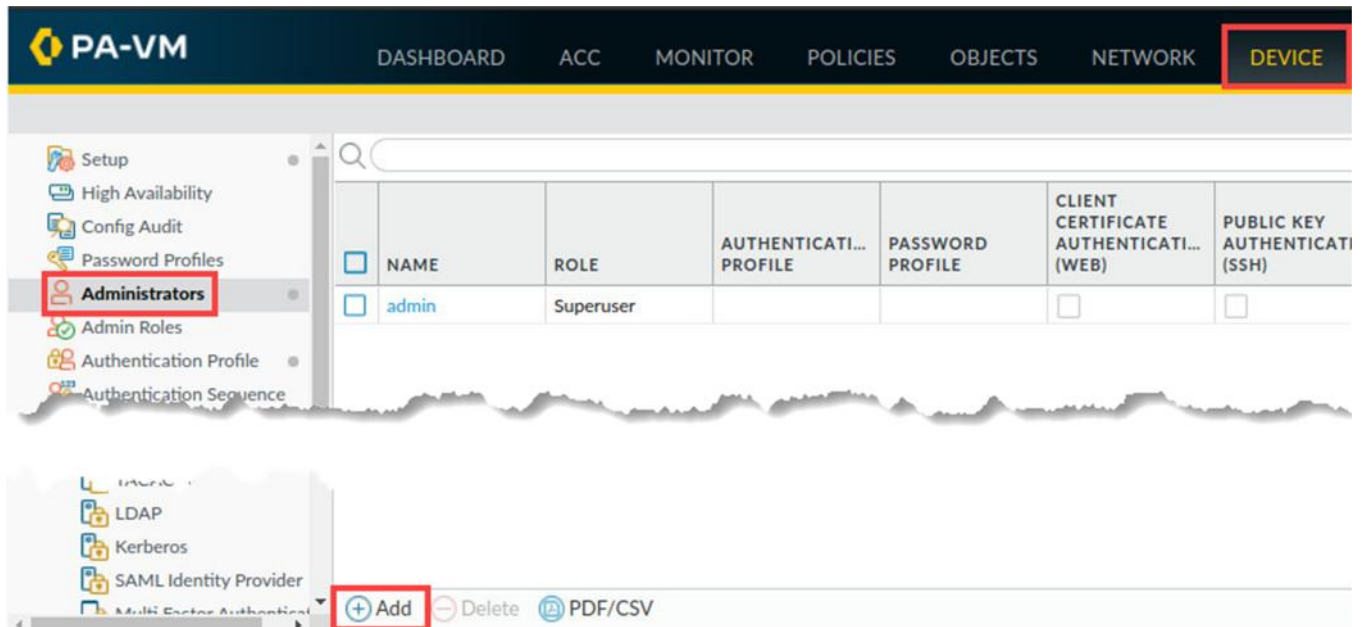
The screenshot shows the 'Local User' configuration window. The 'Name' field is set to 'adminBob' (highlighted with a red box). The 'Mode' is set to 'Password' (selected with a radio button). The 'Password' and 'Confirm Password' fields are filled with dots (highlighted with a red box). The 'Enable' checkbox is checked. At the bottom, there is an 'OK' button (highlighted with a red box) and a 'Cancel' button.

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

3.4 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.



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

Administrator

Name

adminBob

Authentication Profile

Local-Database

☐ Use only client certificate authentication (Web)

☐ Use Public Key Authentication (SSH)

Administrator Type

☒ Dynamic
 ☐ Role Based

Superuser

OK

Cancel

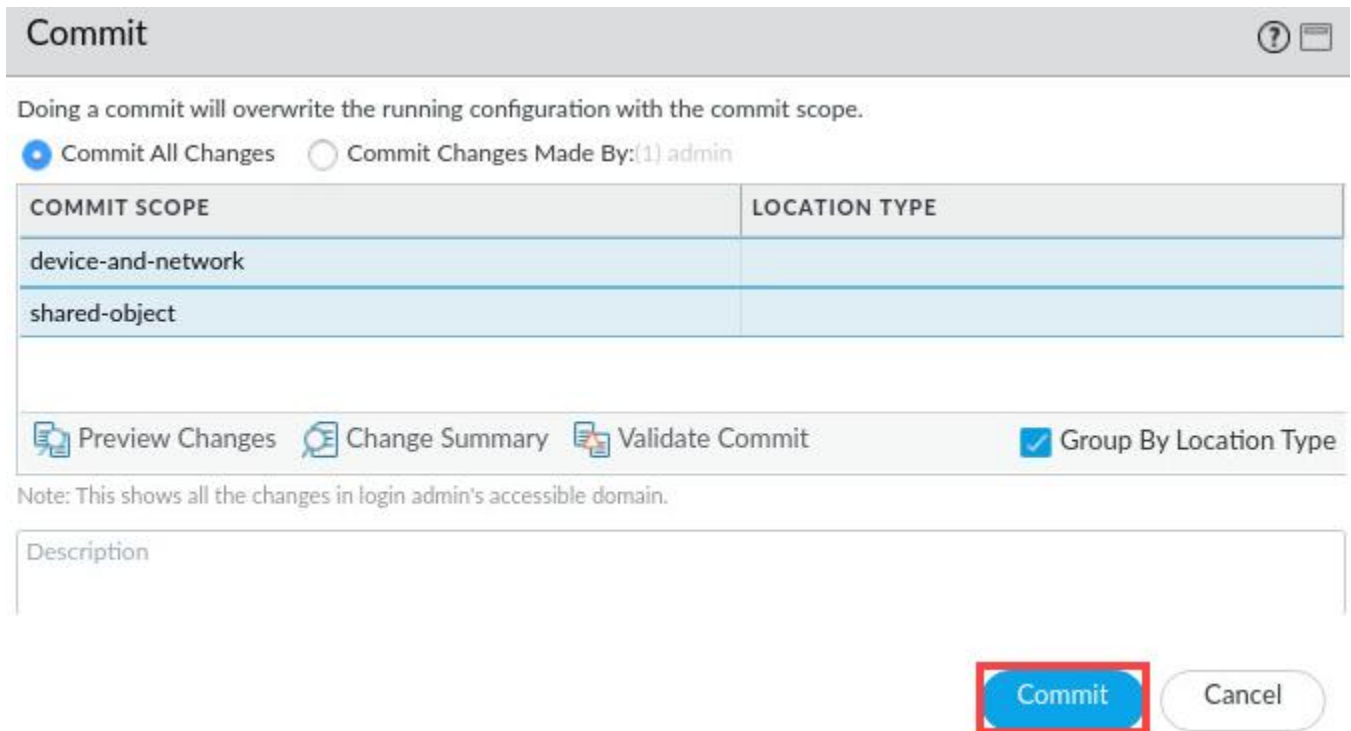
Please Note

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.

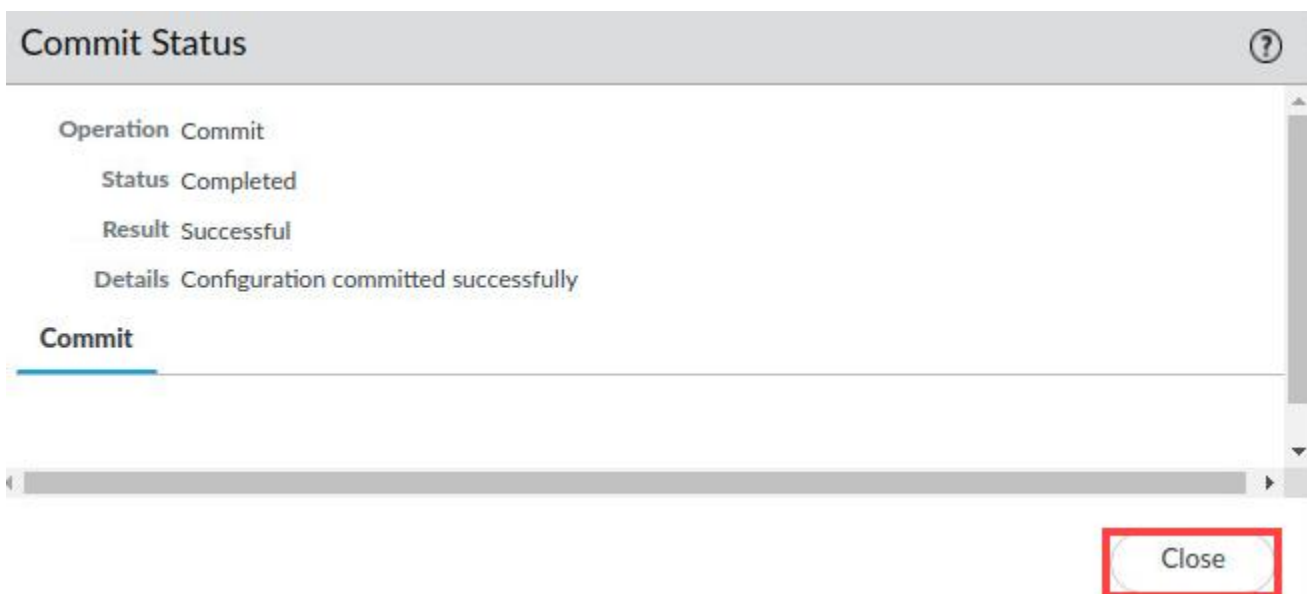


- In the *Commit* window, click **Commit** to proceed with committing the changes.

A screenshot of the 'Commit' window. The title bar says 'Commit'. Below the title bar, a message states: 'Doing a commit will overwrite the running configuration with the commit scope.' There are two radio buttons: 'Commit All Changes' (selected) and 'Commit Changes Made By: (1) admin'. Below this is a table with two columns: 'COMMIT SCOPE' and 'LOCATION TYPE'. The table has two rows: 'device-and-network' and 'shared-object'. Below the table are three icons with labels: 'Preview Changes', 'Change Summary', and 'Validate Commit'. To the right of these is a checkbox labeled 'Group By Location Type' which is checked. Below this is a note: 'Note: This shows all the changes in login admin's accessible domain.' At the bottom right, there are two buttons: 'Commit' (highlighted with a red box) and 'Cancel'.

COMMIT SCOPE	LOCATION TYPE
device-and-network	
shared-object	

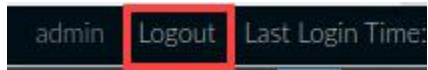
- In the *Commit Status* window, click **Close**.

A screenshot of the 'Commit Status' window. The title bar says 'Commit Status'. Below the title bar, there is a summary of the commit operation: 'Operation Commit', 'Status Completed', 'Result Successful', and 'Details Configuration committed successfully'. Below this is a tab labeled 'Commit'. At the bottom right, there is a 'Close' button highlighted with a red box.

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit

6. 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**.



You have successfully logged out.



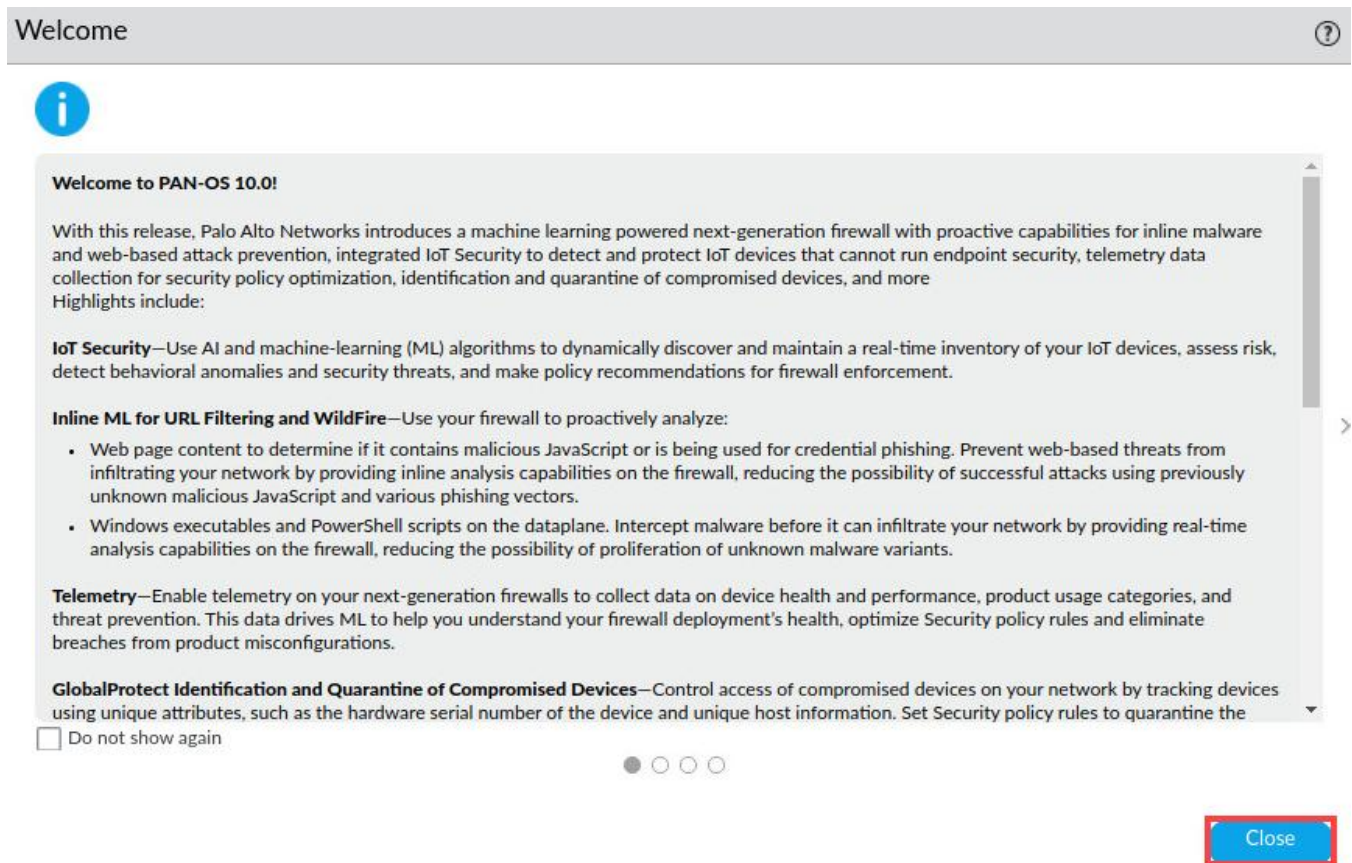
8. Log back into the firewall as username **adminBob**, password **Pa10A1t0!**. Click **Log In**.



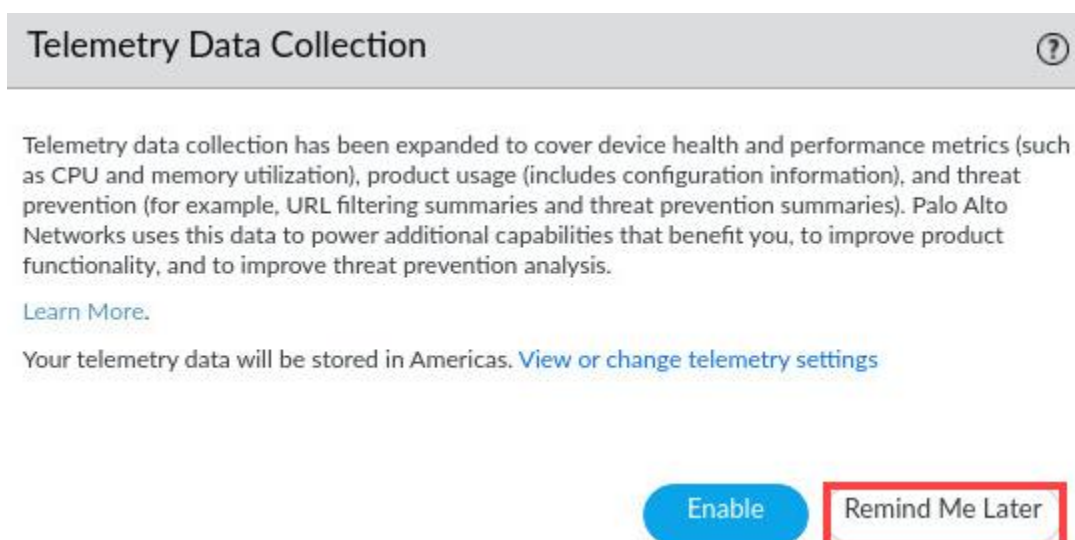
adminBob



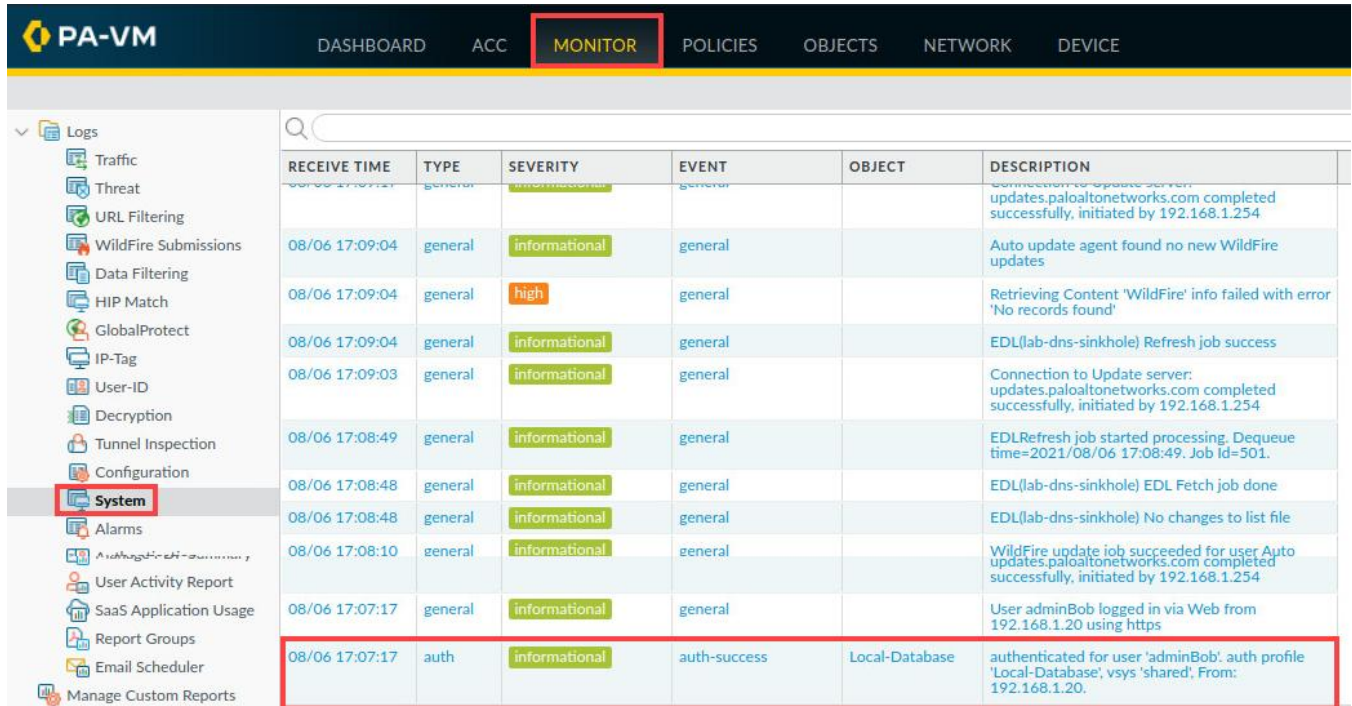
9. In the *Welcome* window, click **Close**.



10. In the *Telemetry Data Collection* window, click **Remind Me Later**.



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



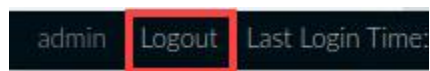
RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
08/06 17:09:04	general	informational	general		Auto update agent found no new WildFire updates
08/06 17:09:04	general	high	general		Retrieving Content 'WildFire' info failed with error 'No records found'
08/06 17:09:04	general	informational	general		EDL(lab-dns-sinkhole) Refresh job success
08/06 17:09:03	general	informational	general		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
08/06 17:08:49	general	informational	general		EDLRefresh job started processing. Dequeue time=2021/08/06 17:08:49. Job Id=501.
08/06 17:08:48	general	informational	general		EDL(lab-dns-sinkhole) EDL Fetch job done
08/06 17:08:48	general	informational	general		EDL(lab-dns-sinkhole) No changes to list file
08/06 17:08:10	general	informational	general		WildFire update job succeeded for user Auto updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
08/06 17:07:17	general	informational	general		User adminBob logged in via Web from 192.168.1.20 using https
08/06 17:07:17	auth	informational	auth-success	Local-Database	authenticated for user 'adminBob'. auth profile 'Local-Database', vsys 'shared'. From: 192.168.1.20.

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.

12. Log out of the firewall.



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



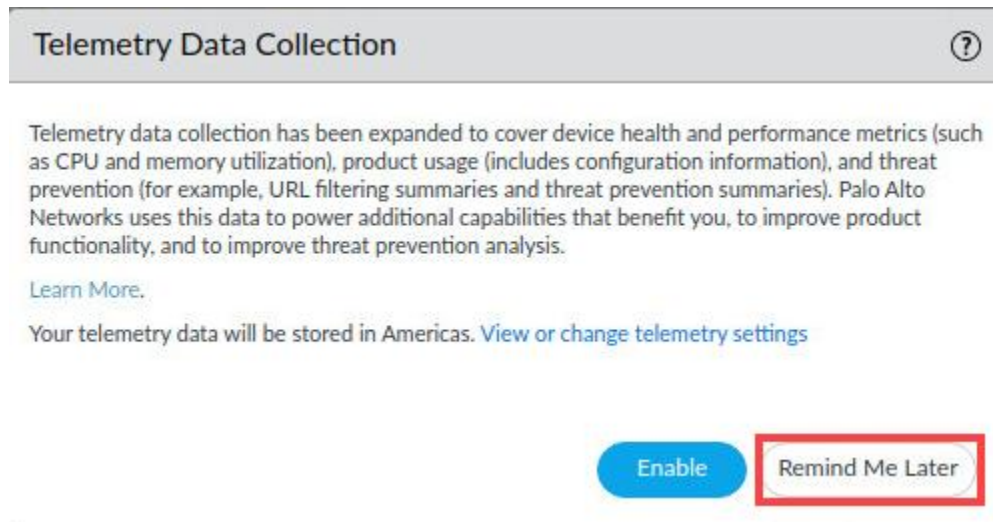
You have successfully logged out.



14. Log back into the firewall with the **admin/Pa10Alt0!** credentials.



15. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.



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

3.5 Configure LDAP Authentication

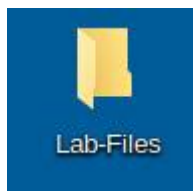
Your organization uses an LDAP server to maintain a database of users, including network administrators. Your team of security personnel is growing each month, and you want to leverage the existing LDAP server to authenticate administrators when they attempt to log into the firewall.

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

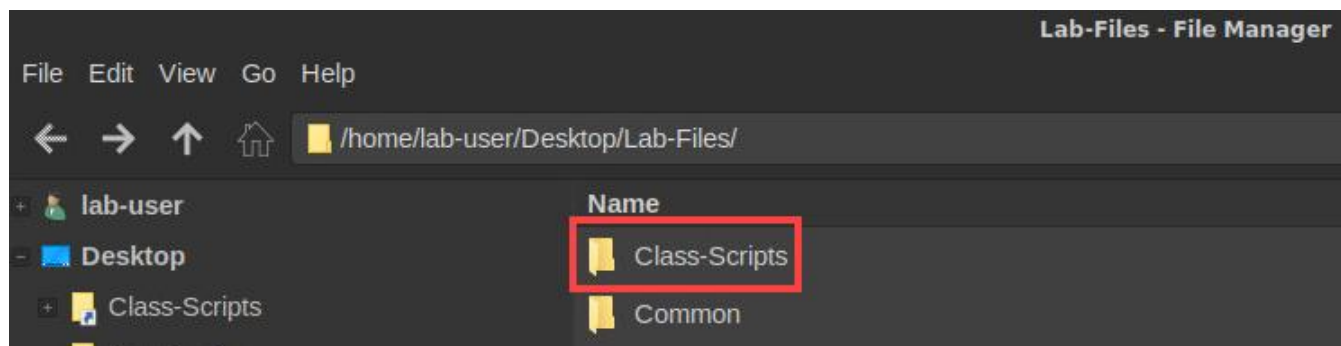
1. Minimize the PA-VM web interface.



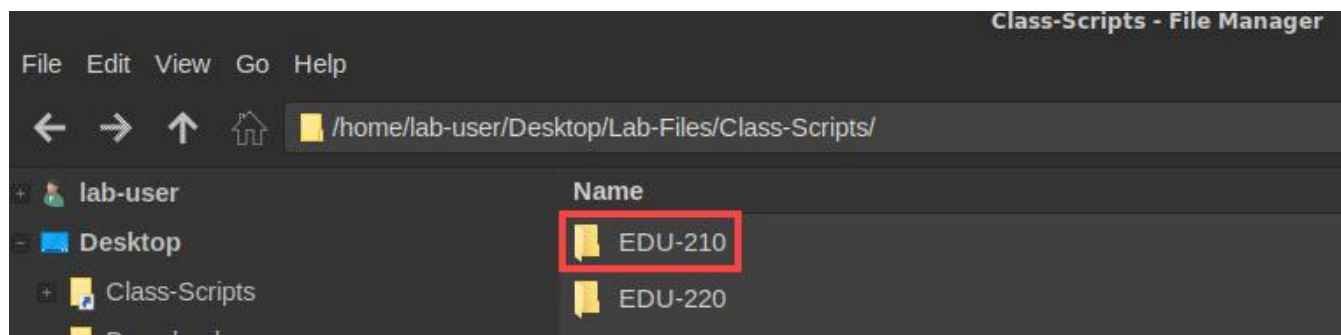
2. On the client desktop, open the **Lab-Files** folder.



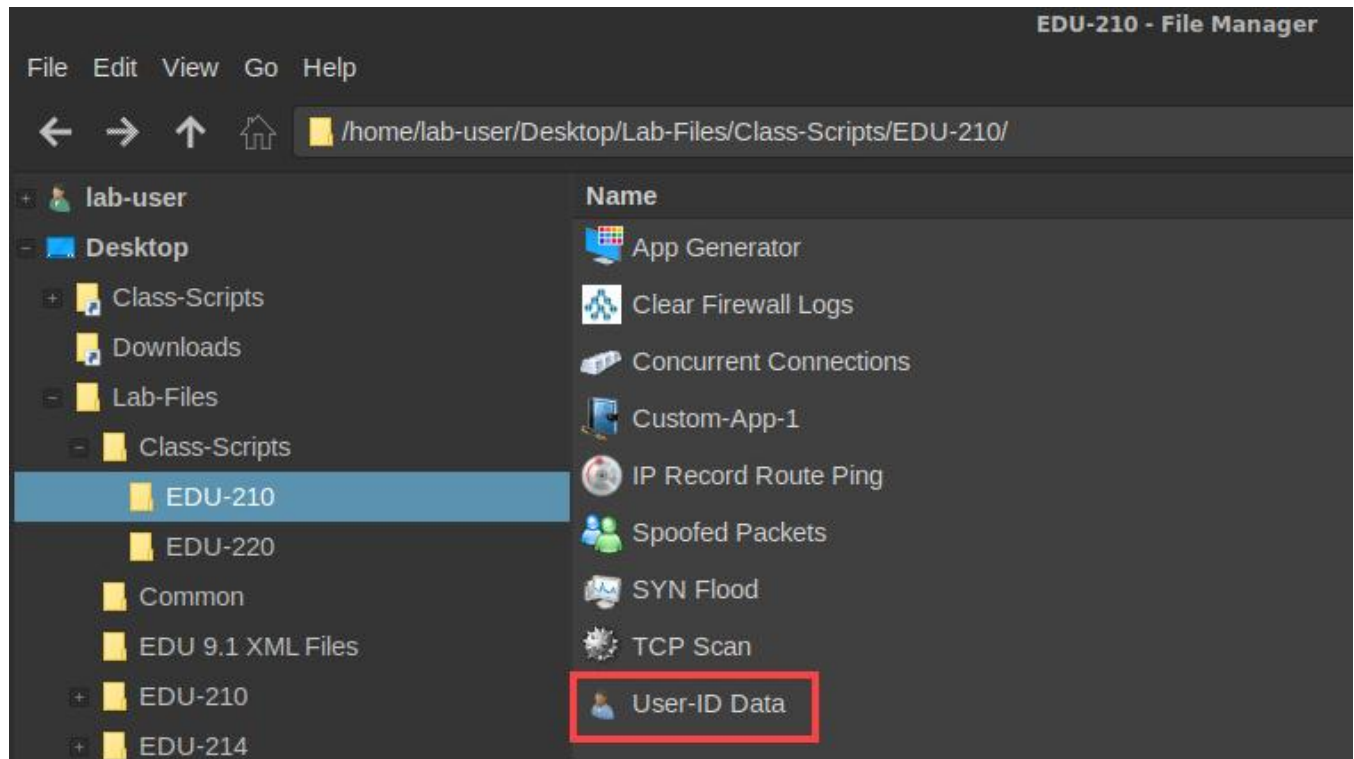
3. In the *Lab-Files* folder, open the **Class-Scripts**.



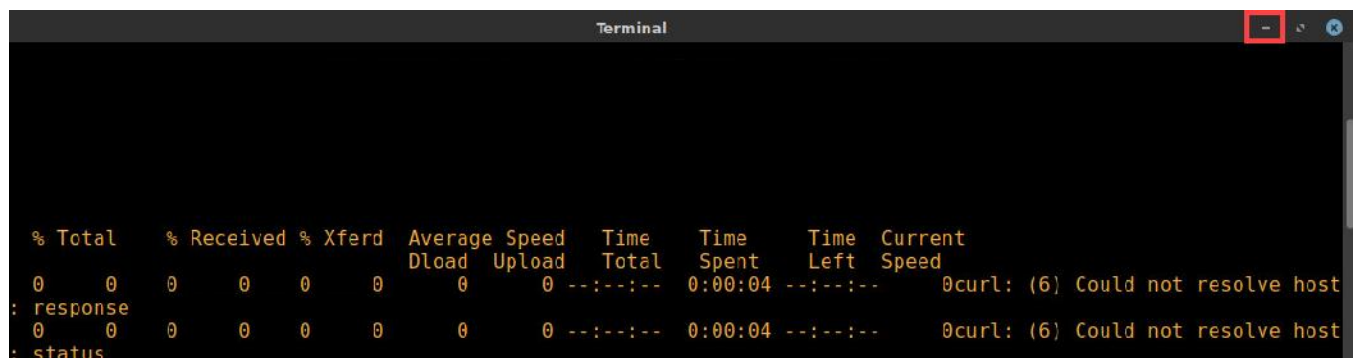
4. In the *Class-Scripts* folder, open the **EDU-210** folder.



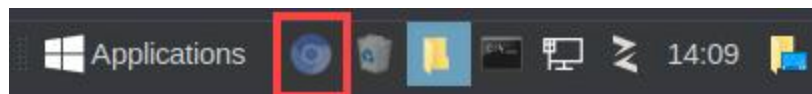
- Execute the *User-ID Data* script by **double-clicking** it.



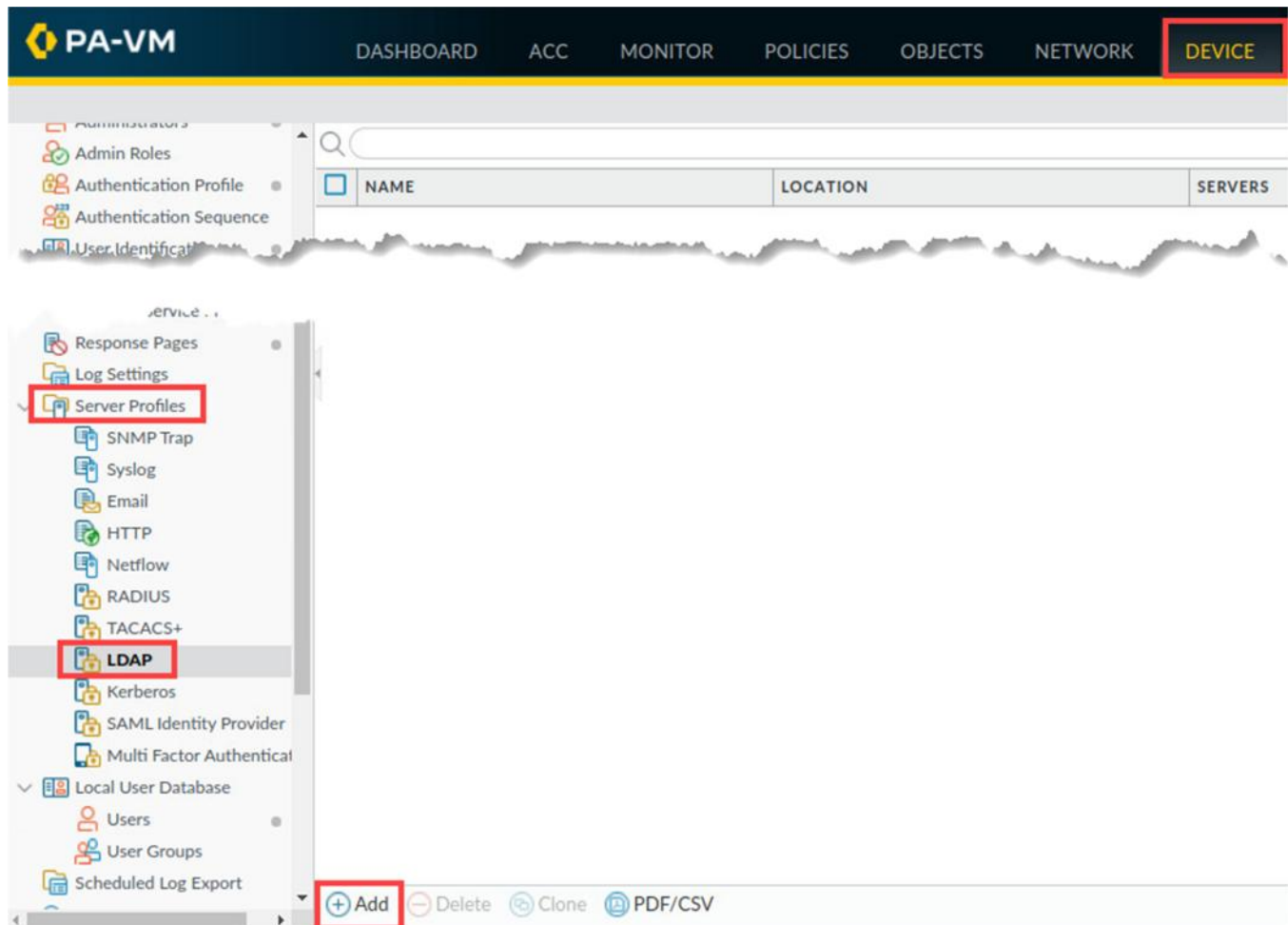
- Notice the *Terminal* window will pop up. **Minimize** the terminal window and let it run for the remainder of the lab.



- Reopen the *PA-VM firewall* by clicking on the **Chromium** icon in the taskbar.



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



9. 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 or the *Port* number.

LDAP Server Profile

Profile Name **LDAP Server Profile**

☐ Administrator Use Only

Server List

NAME	LDAP SERVER	PORT
ldap.panw.lab	192.168.50.89	389

Add **Delete**

10. In the *Server Settings* section, Enter **dc=panw,dc=lab** for *Base DN*, enter **cn=admin,dc=panw,dc=lab** for *Bind DN*, enter **Pa10A1t0!** 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

☐ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

OK Cancel

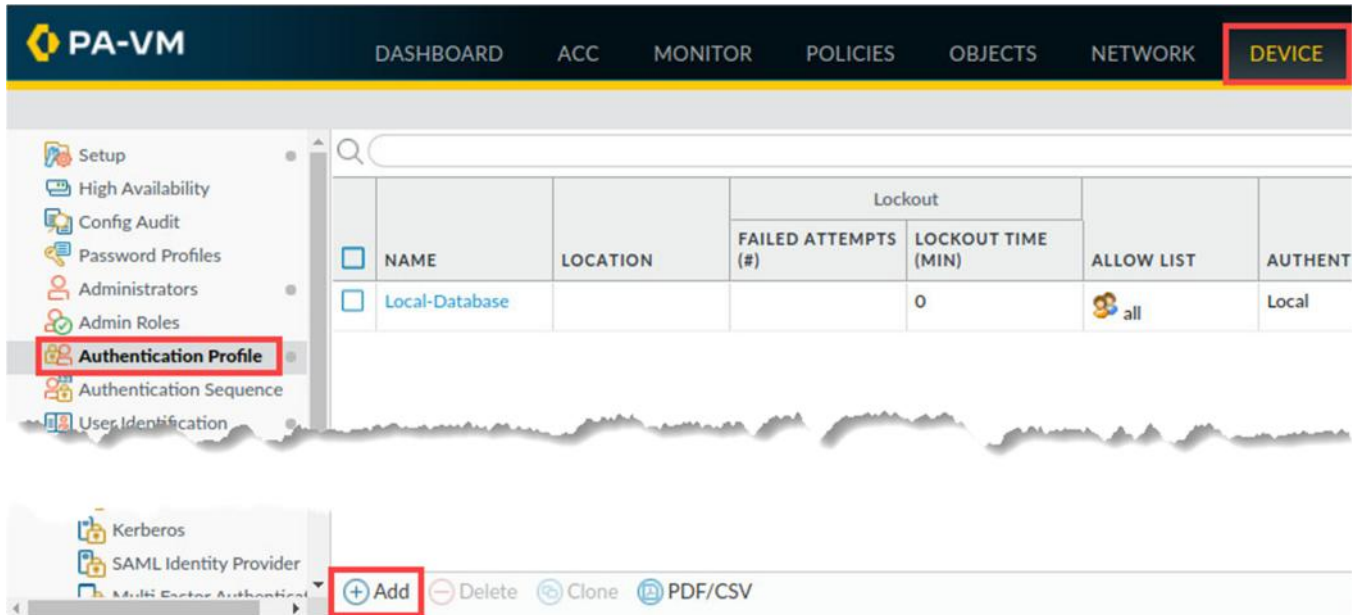
Please Note

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

11. Verify the *LDAP Server Profile* is now showing in the *LDAP Profile* list.

<input type="checkbox"/>	NAME	LOCATION	SERVICES	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

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



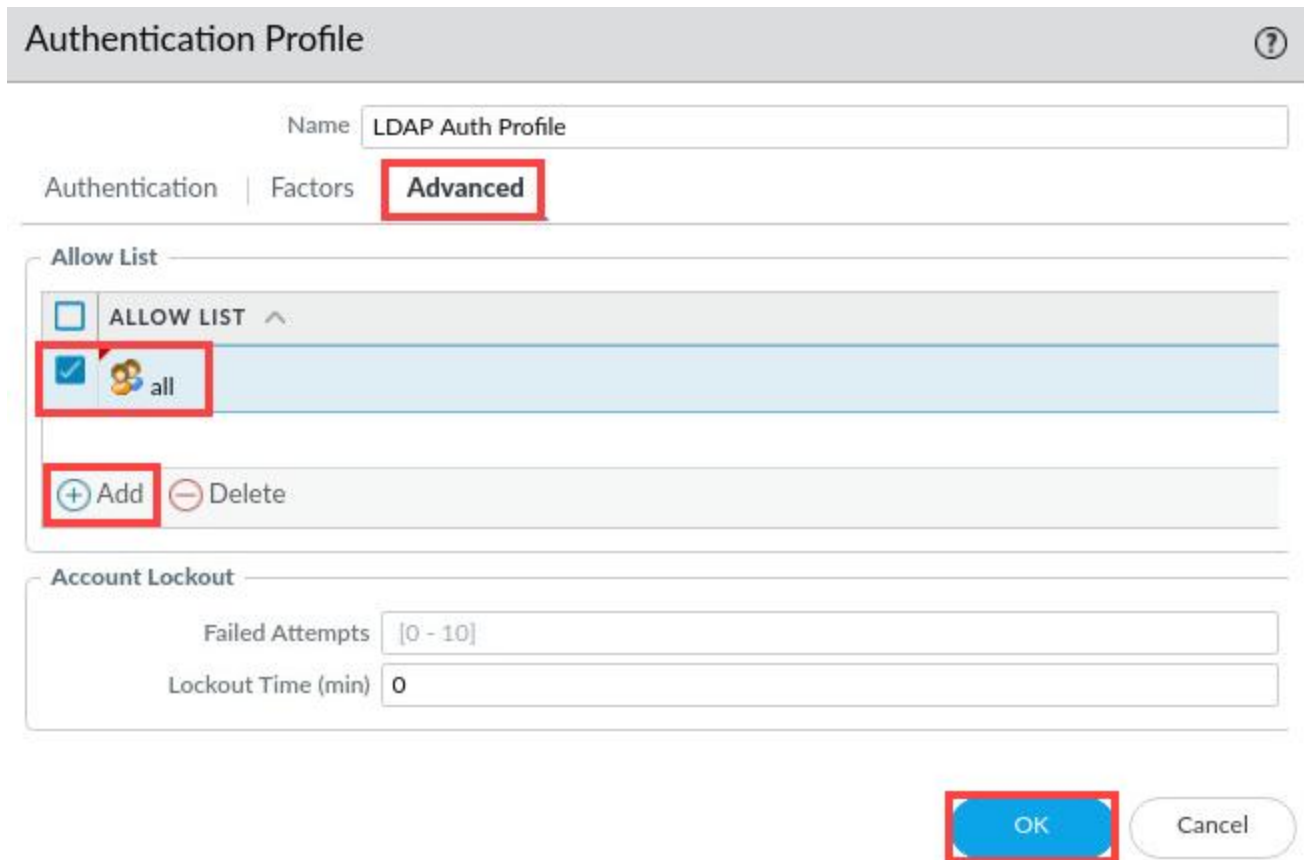
The screenshot shows the PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE' (highlighted with a red box). On the left sidebar, 'Authentication Profile' is selected and highlighted with a red box. The main content area displays a table with columns: NAME, LOCATION, Lockout (FAILED ATTEMPTS (#), LOCKOUT TIME (MIN)), ALLOW LIST, and AUTHENT. A row is visible with 'Local-Database' in the NAME column and '0' in the LOCKOUT TIME column. Below the table, there are buttons: '+ Add' (highlighted with a red box), '- Delete', 'Clone', and 'PDF/CSV'.

13. 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 is set to 'LDAP Auth Profile' (highlighted with a red box). The 'Authentication' tab is selected, and the 'Advanced' sub-tab is also highlighted with a red box. The 'Type' dropdown menu is set to 'LDAP' (highlighted with a red box). The 'Server Profile' dropdown menu is set to 'LDAP Server Profile' (highlighted with a red box). The 'Login Attribute' field is empty.

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



Authentication Profile

Name: LDAP Auth Profile

Authentication | Factors | **Advanced**

Allow List

☐ ALLOW LIST ^

☒ all

+ Add **- Delete**

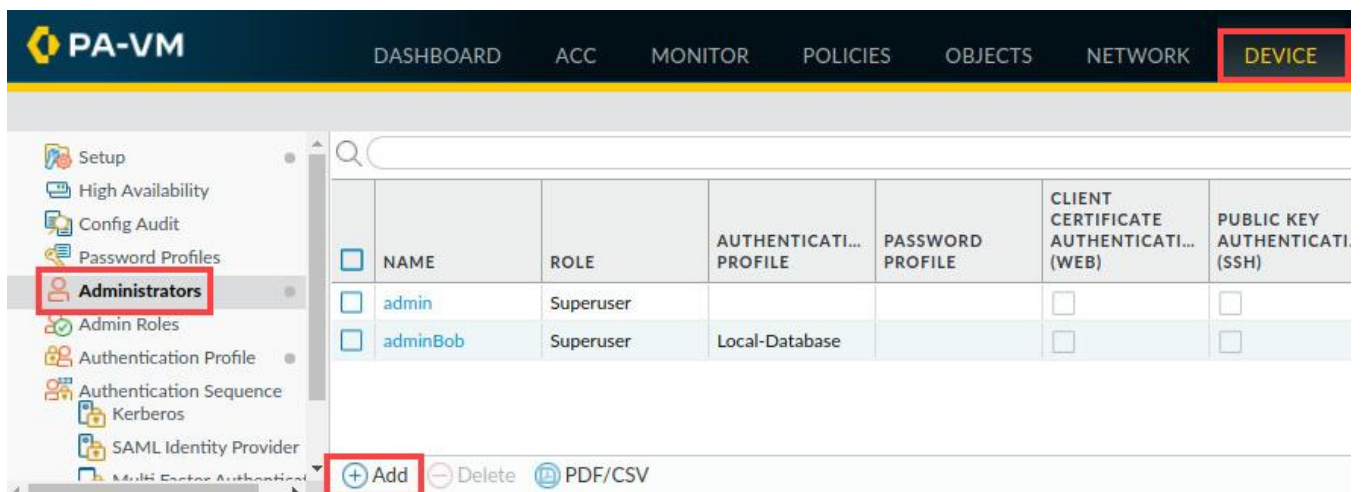
Account Lockout

Failed Attempts: [0 - 10]

Lockout Time (min): 0

OK Cancel

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



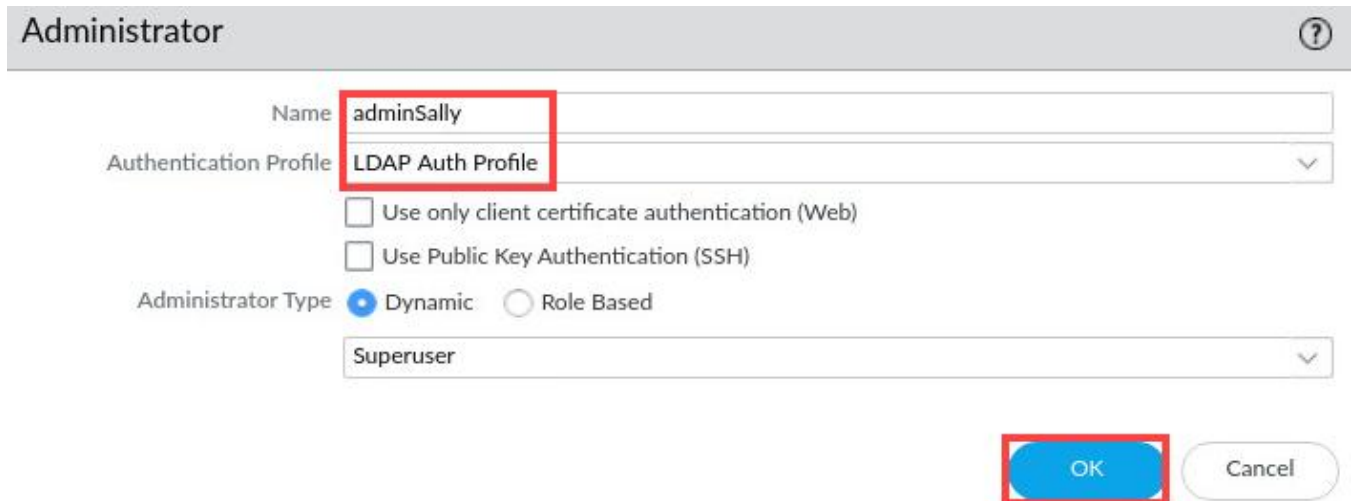
PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

Setup
High Availability
Config Audit
Password Profiles
Administrators
Admin Roles
Authentication Profile
Authentication Sequence
Kerberos
SAML Identity Provider
Multi Factor Authentication

<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"/>

+ Add **- Delete** PDF/CSV

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



The screenshot shows the 'Administrator' configuration window. The 'Name' field is set to 'adminSally' and the 'Authentication Profile' is set to 'LDAP Auth Profile'. Both fields are highlighted with a red box. Below these fields are two unchecked checkboxes: 'Use only client certificate authentication (Web)' and 'Use Public Key Authentication (SSH)'. The 'Administrator Type' is set to 'Dynamic' (selected with a radio button) and 'Role Based' is unselected. The 'Superuser' dropdown is set to 'Superuser'. At the bottom right, the 'OK' button is highlighted with a red box, and the 'Cancel' button is also visible.

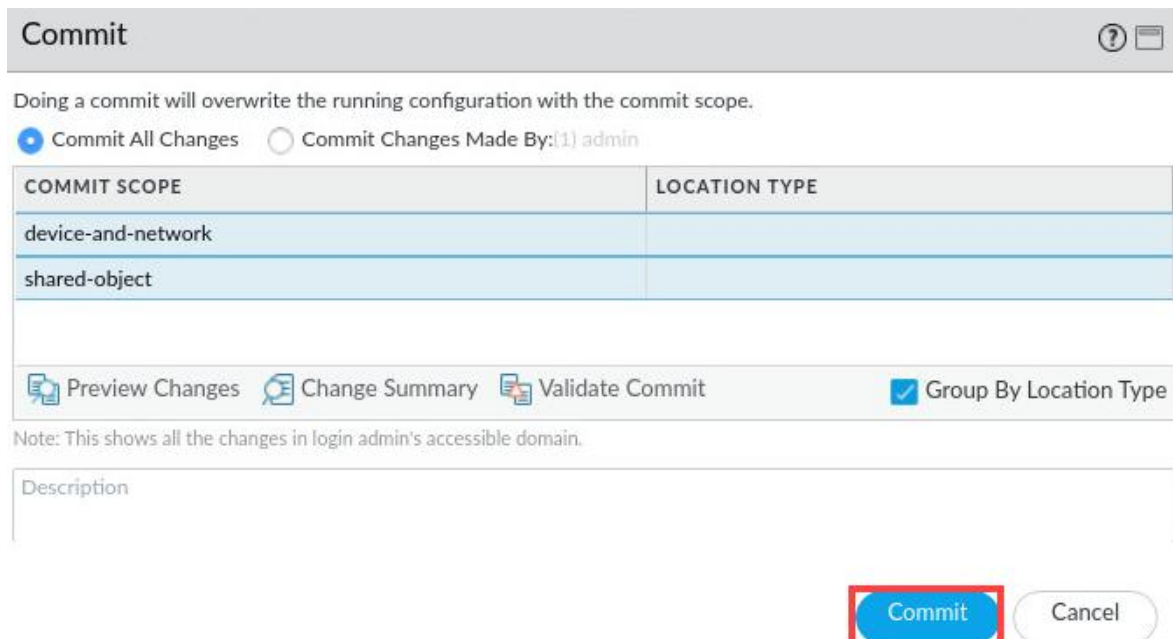
**Please
Note**

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

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



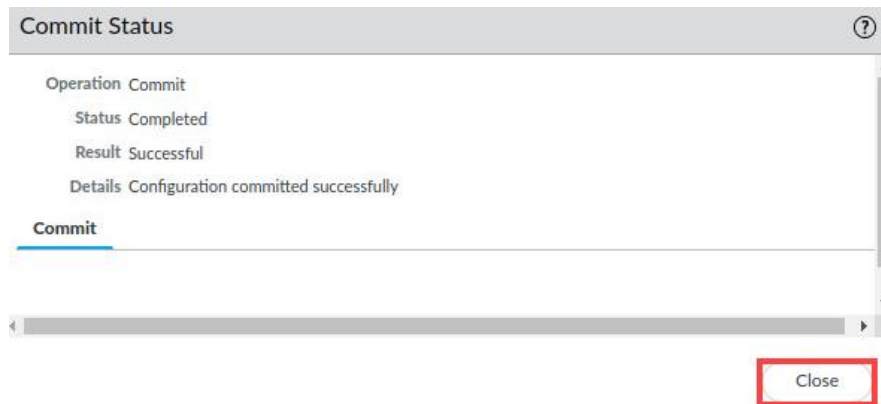
18. In the *Commit* window, click **Commit** to proceed with committing the changes.



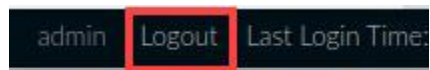
The screenshot shows the 'Commit' configuration window. At the top, it states: 'Doing a commit will overwrite the running configuration with the commit scope.' Below this, there are two radio buttons: 'Commit All Changes' (selected) and 'Commit Changes Made By: (1) admin'. A table with two columns, 'COMMIT SCOPE' and 'LOCATION TYPE', is displayed. The table has two rows: 'device-and-network' and 'shared-object'. Below the table, there are four buttons: 'Preview Changes', 'Change Summary', 'Validate Commit', and 'Group By Location Type' (which is checked). A note at the bottom states: 'Note: This shows all the changes in login admin's accessible domain.' At the bottom right, the 'Commit' button is highlighted with a red box, and the 'Cancel' button is also visible.

COMMIT SCOPE	LOCATION TYPE
device-and-network	
shared-object	

19. When the *Commit* operation successfully completes, click **Close** to continue.



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



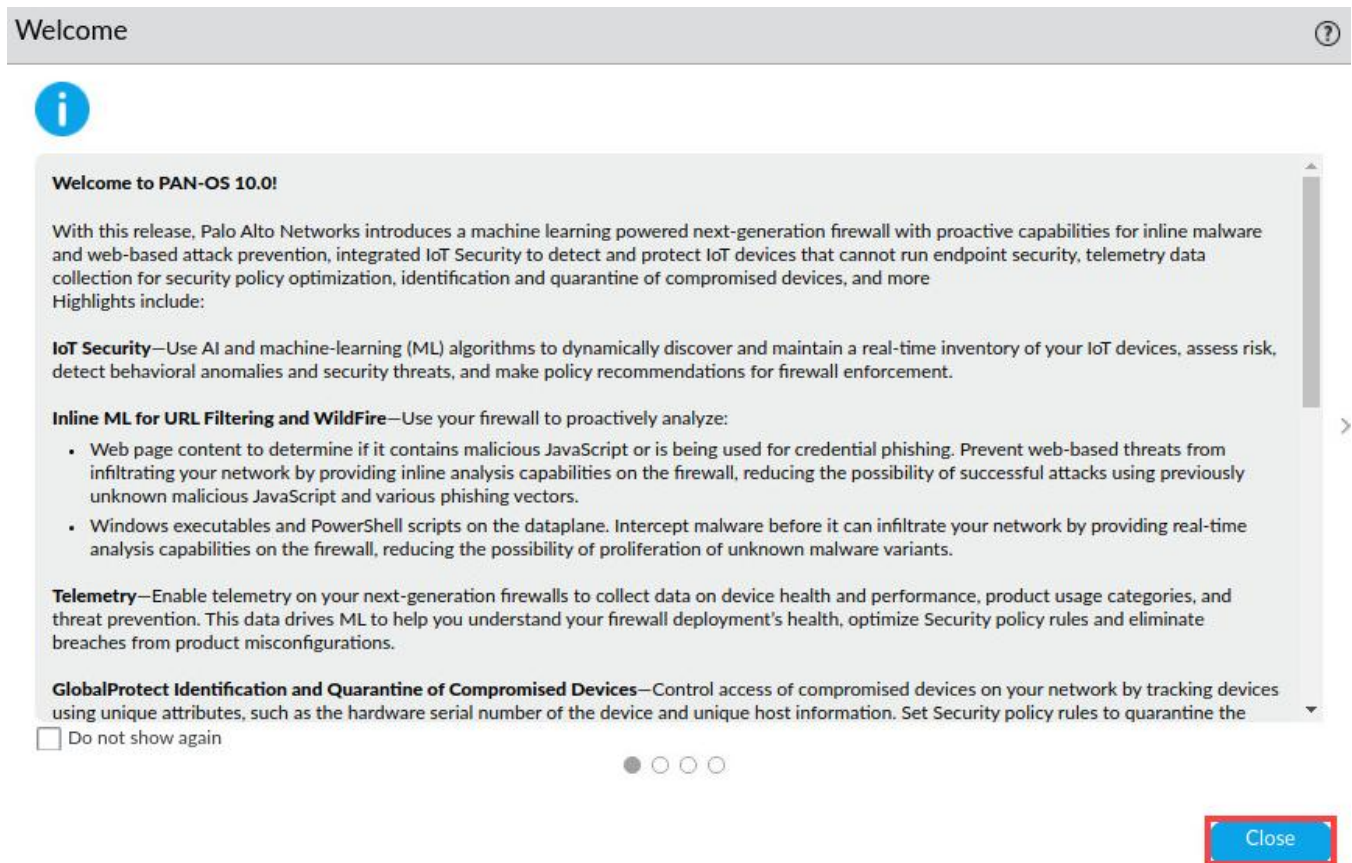
21. In the *Log In* window, click **Log In**.



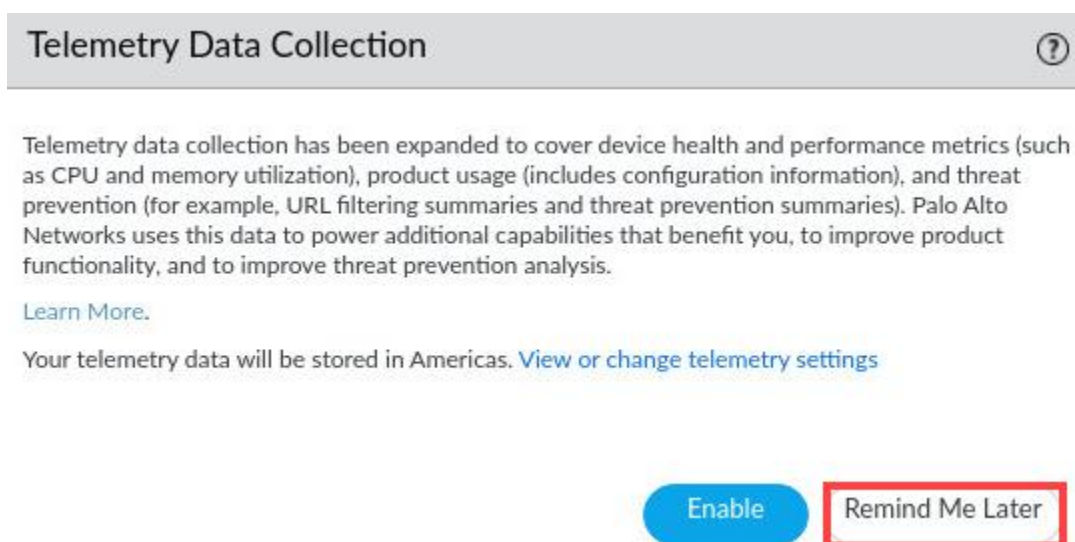
22. Log back into the firewall as username **adminSally**, password **Pa10A1t0!**. Click **Log In**.



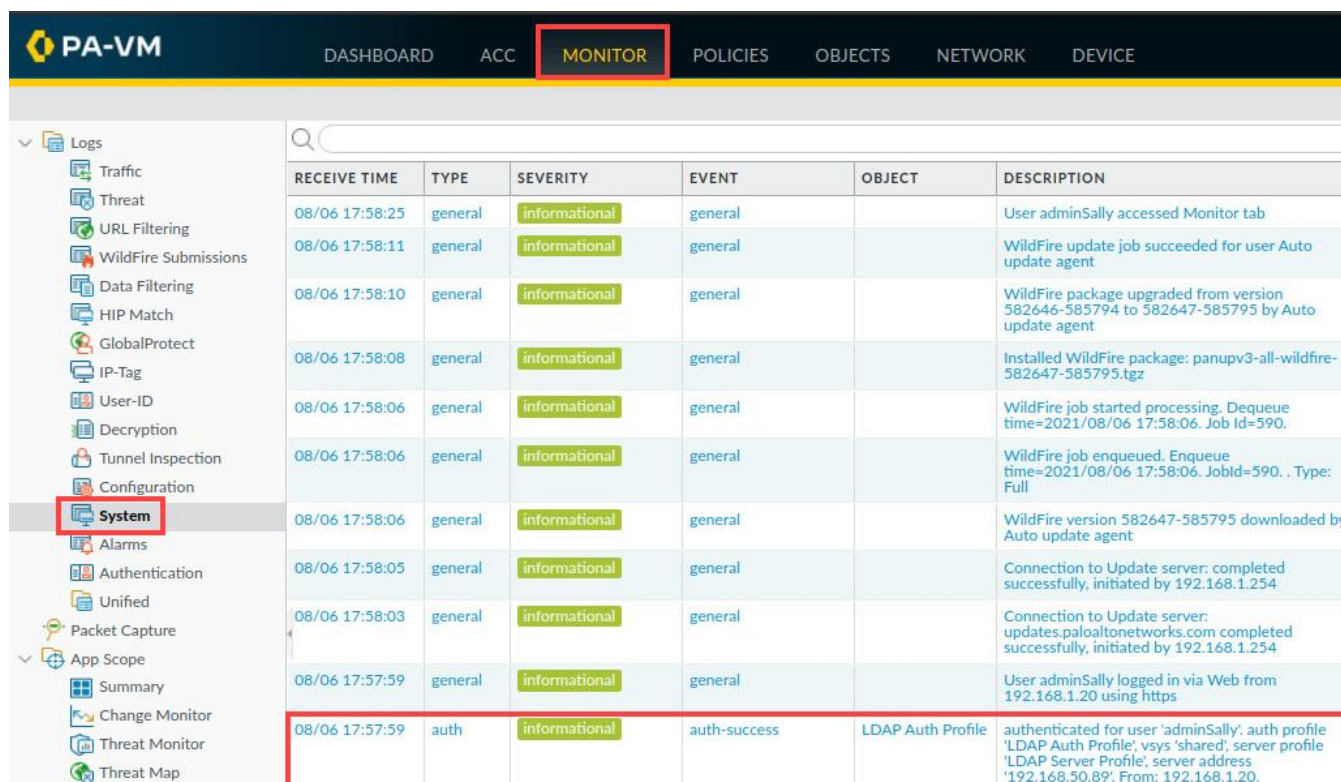
23. In the *Welcome* window, click **Close**.



24. In the *Telemetry Data Collection* window, click **Remind Me Later**.



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



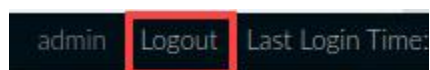
RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
08/06 17:58:25	general	informational	general		User adminSally accessed Monitor tab
08/06 17:58:11	general	informational	general		WildFire update job succeeded for user Auto update agent
08/06 17:58:10	general	informational	general		WildFire package upgraded from version 582646-585794 to 582647-585795 by Auto update agent
08/06 17:58:08	general	informational	general		Installed WildFire package: panupv3-all-wildfire-582647-585795.tgz
08/06 17:58:06	general	informational	general		WildFire job started processing. Dequeue time=2021/08/06 17:58:06. Job Id=590.
08/06 17:58:06	general	informational	general		WildFire job enqueued. Enqueue time=2021/08/06 17:58:06. JobId=590. Type: Full
08/06 17:58:06	general	informational	general		WildFire version 582647-585795 downloaded by Auto update agent
08/06 17:58:05	general	informational	general		Connection to Update server: completed successfully, initiated by 192.168.1.254
08/06 17:58:03	general	informational	general		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
08/06 17:57:59	general	informational	general		User adminSally logged in via Web from 192.168.1.20 using https
08/06 17:57:59	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.

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.

26. Log out of the firewall.



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



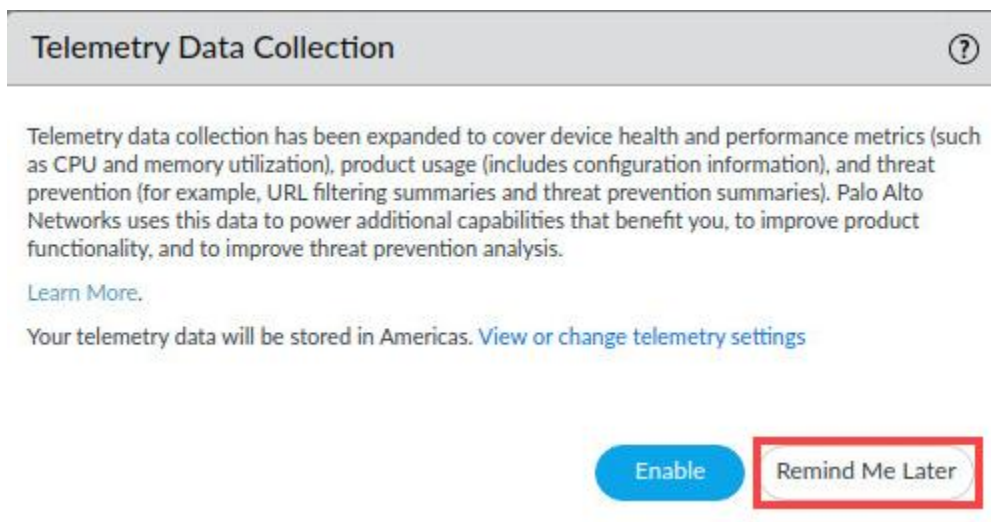
You have successfully logged out.



28. Log back into the firewall with the **admin/Pa10Alt0!** credentials.



29. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.



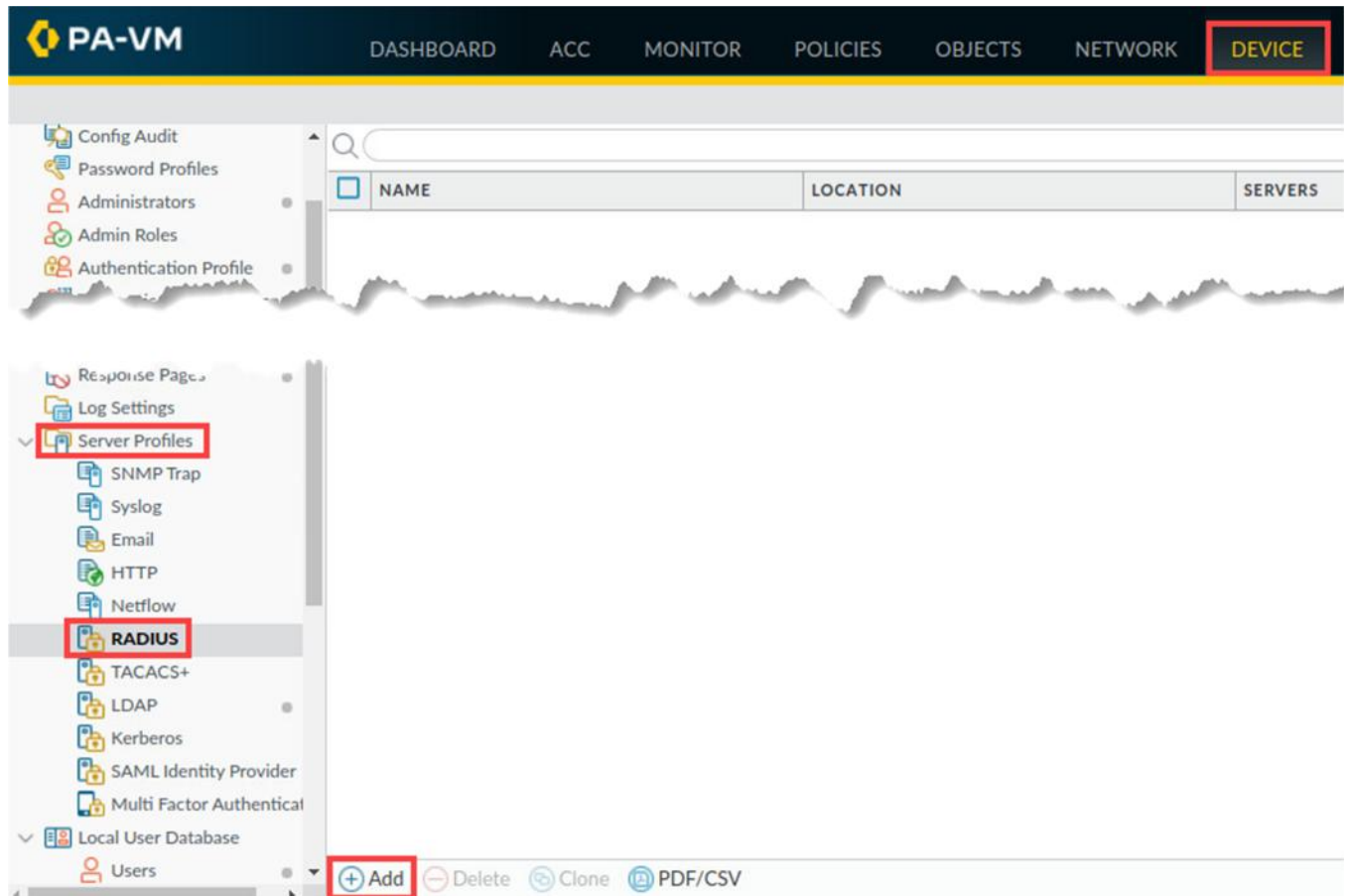
30. Leave the firewall web interface open to continue with the next task.

3.6 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 that the user adminHelga can log in.

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



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 **Pa10A1t0!** for *Secret* and *Confirm Secret*. Leave the *Port* set to **1812**. Click **OK**.

RADIUS Server Profile

Profile Name **RADIUS Server Profile**

☐ Administrator Use Only

Server Settings

Timeout (sec) 3

Retries 3

Authentication Protocol **CHAP**

Servers

NAME	RADIUS SERVER	SECRET	PORT
radius.panw.lab	192.168.50.150	Secret Confirm Secret	1812

+ Add

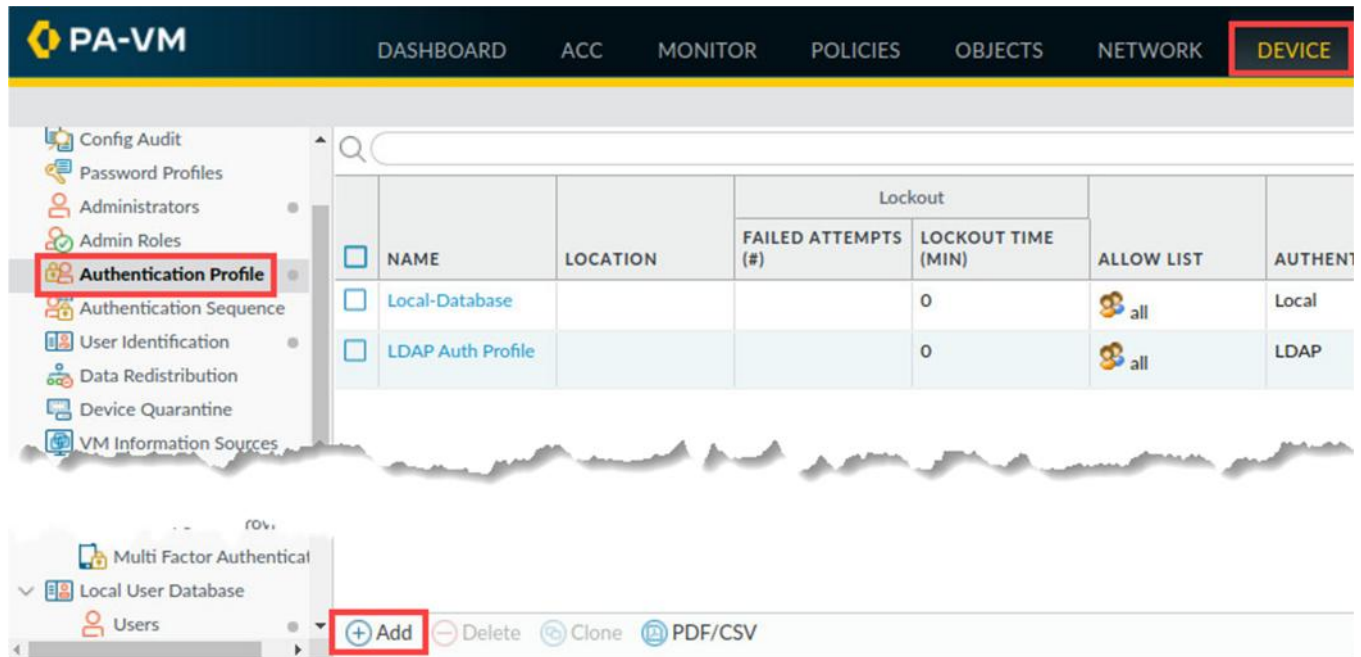
- Delete

Enter the IP address or FQDN of the RADIUS server

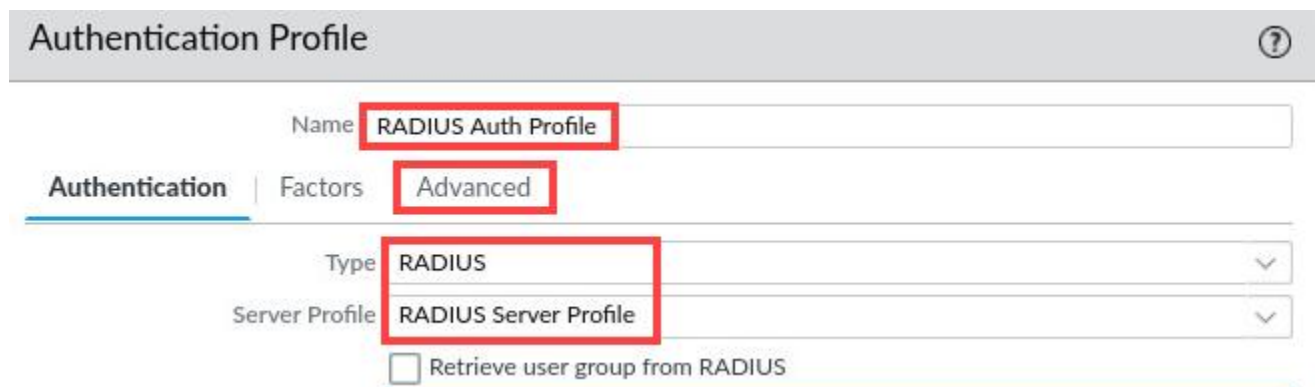
OK

Cancel

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



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.



The screenshot shows the 'Authentication Profile' configuration window. The 'Name' field is set to 'RADIUS Auth Profile'. The 'Authentication' tab is selected, and the 'Advanced' sub-tab is active. The 'Type' is set to 'RADIUS' and the 'Server Profile' is set to 'RADIUS Server Profile'. There is an unchecked checkbox for '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

☐ ALLOW LIST ^

☒  all

Account Lockout

Failed Attempts [0 - 10]

Lockout Time (min) 0

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

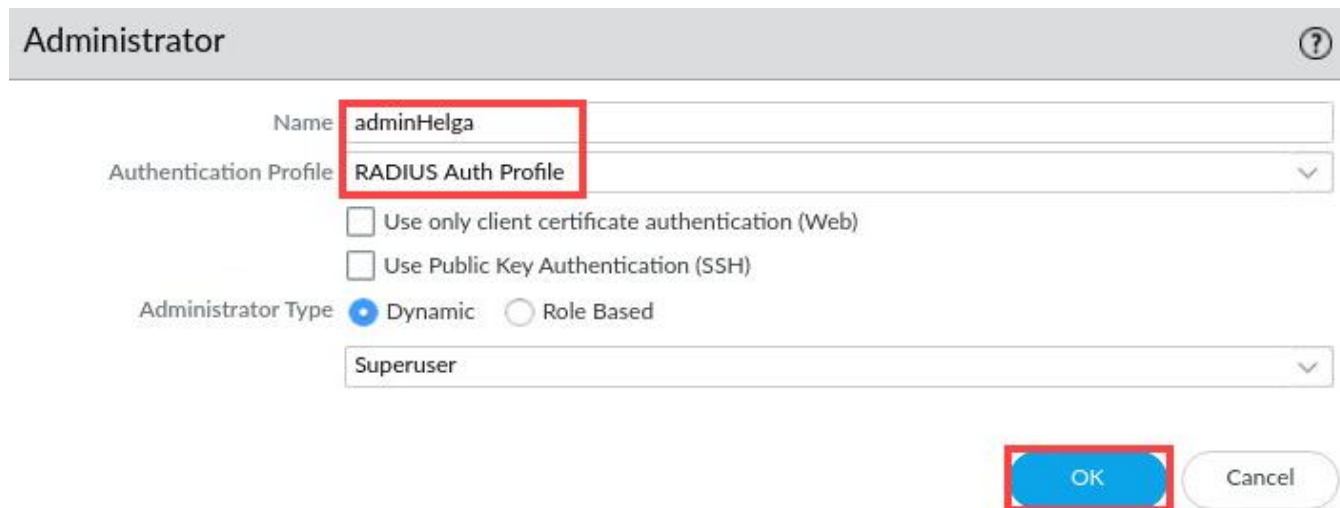
PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

Config Audit
Password Profiles
Administrators
Admin Roles
Authentication Profile
Authentication Sequence
User Identification
Data Redistribution
Device Quarantine
VM Information Sources
Troubleshooting
Local User Database
Users

	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**.



The **Administrator** window is shown with the following configuration:

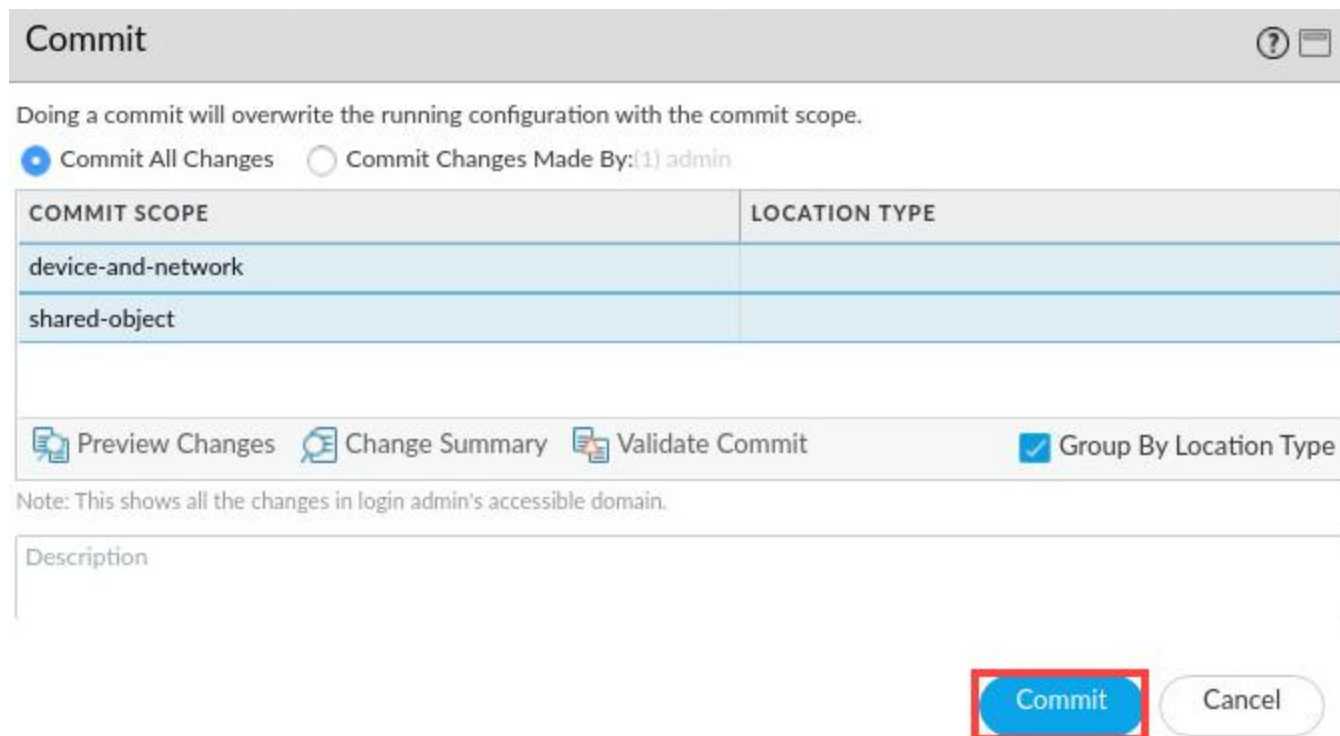
- Name:** adminHelga
- Authentication Profile:** RADIUS Auth Profile
- ☐ Use only client certificate authentication (Web)
- ☐ Use Public Key Authentication (SSH)
- Administrator Type:** Dynamic (selected), Role Based
- Superuser:** Superuser

Buttons: **OK** (highlighted), **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.



The **Commit** window is shown with the following configuration:

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
device-and-network	
shared-object	

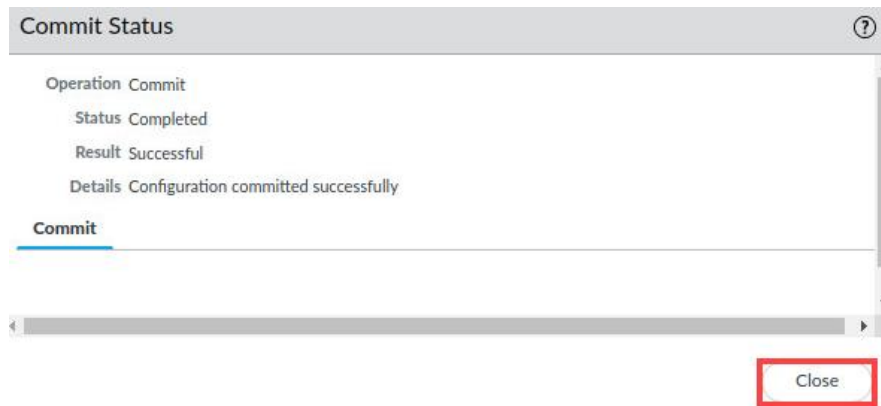
Buttons: Preview Changes Change Summary Validate Commit ☒ Group By Location Type

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

Description

Buttons: **Commit** (highlighted), **Cancel**

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**.



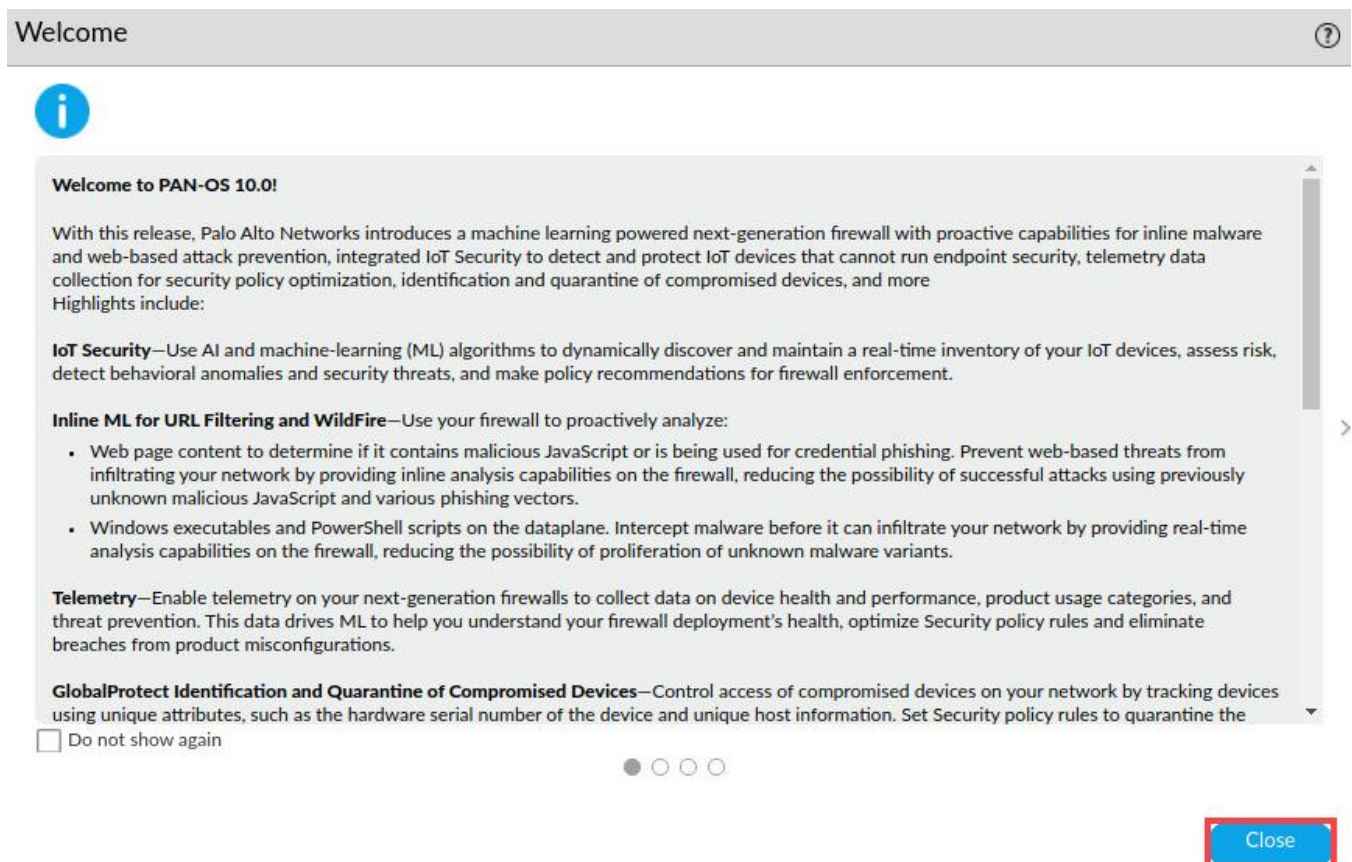
You have successfully logged out.



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



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



15. In the *Telemetry Data Collection* window, click **Remind Me Later**.

Telemetry Data Collection ?

Telemetry data collection has been expanded to cover device health and performance metrics (such as CPU and memory utilization), product usage (includes configuration information), and threat prevention (for example, URL filtering summaries and threat prevention summaries). Palo Alto Networks uses this data to power additional capabilities that benefit you, to improve product functionality, and to improve threat prevention analysis.

[Learn More.](#)

Your telemetry data will be stored in Americas. [View or change telemetry settings](#)

Enable
Remind Me Later

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

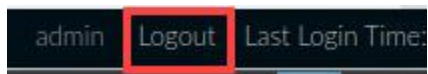
PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE						
<div>Logs</div> <ul style="list-style-type: none"> Traffic Threat URL Filtering WildFire Submissions Data Filtering HIP Match GlobalProtect IP-Tag User-ID Decryption Tunnel Inspection Configuration System Alarms Authentication 						
	RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
	08/06 18:38:38	general	informational	general		User adminHelga accessed Monitor tab
	08/06 18:38:13	general	informational	general		User adminHelga logged in via Web from 192.168.1.20 using https
	08/06 18:38:13	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.
	08/06 18:38:13	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'
	08/06 18:38:10	general	informational	general		WildFire update job succeeded for user Auto update agent
	08/06 18:38:09	general	informational	general		WildFire package upgraded from version 582654-585802 to 582655-585803 by Auto update agent

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)

17. Log out of the firewall.



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



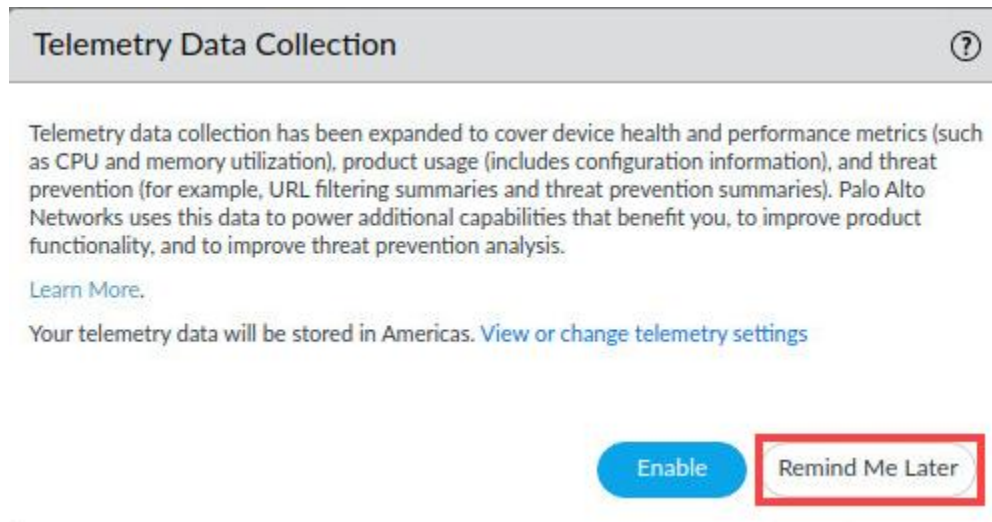
You have successfully logged out.



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



20. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.



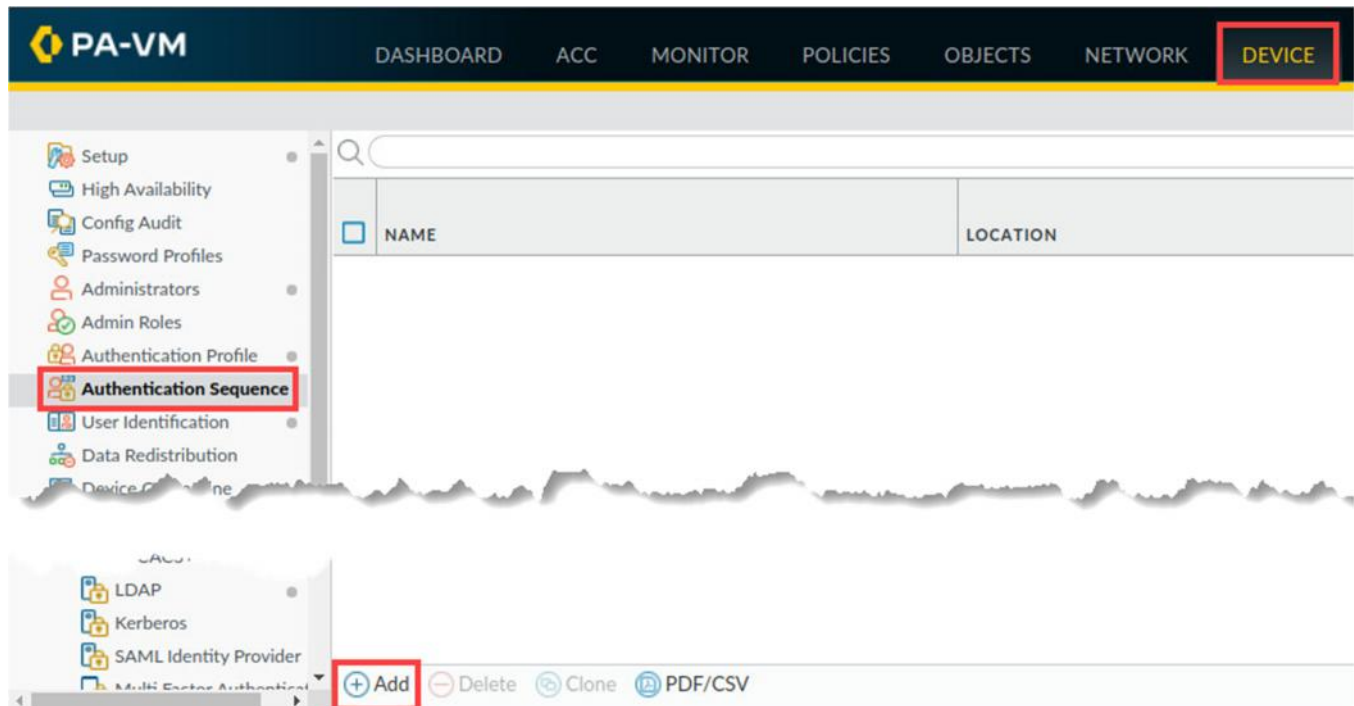
21. Leave the firewall web interface open to continue with the next task.

3.7 Configure and Authentication Sequence

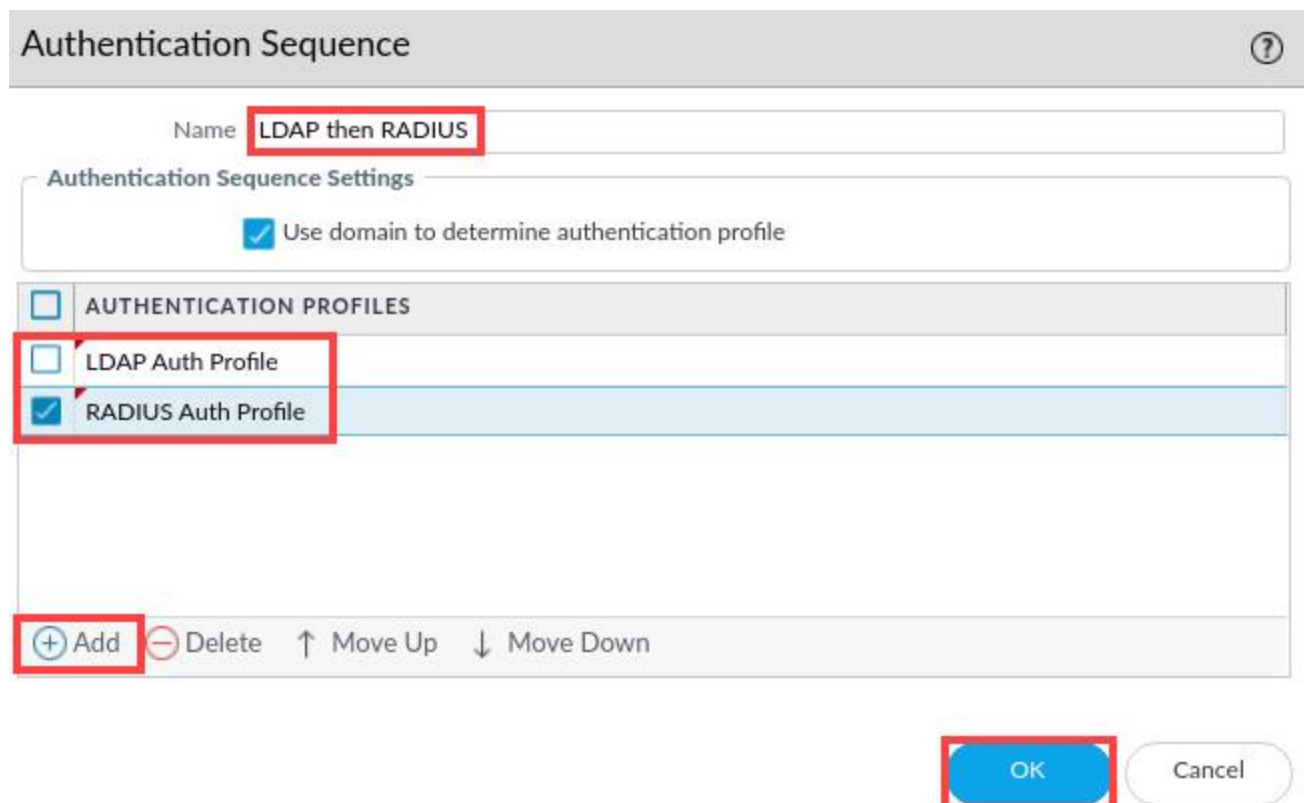
Since the acquisition, some administrator accounts exist in LDAP, and other accounts exist in RADIUS. With administrator accounts in these two different systems, you need to configure the firewall so that it can check both external databases when an administrator attempts to log in.

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**.



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.

- 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
shared-object	

Preview Changes

Change Summary

Validate Commit

☒ Group By Location Type

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

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