



PALO ALTO NETWORKS EDU 210

Lab 3: Working with Firewall Administrator Accounts

Document Version: **2022-07-18**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

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

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology.....	4
Theoretical Lab Topology.....	4
Lab Settings.....	5
1 Working with Firewall Configurations and Log Files	6
1.1 Apply a Baseline Configuration to the Firewall.....	6
1.2 Create a Local Database Authentication Profile	11
1.3 Create a Local User Database Account	13
1.4 Create an Administrator Account.....	14
1.5 Configure LDAP Authentication.....	21
1.6 Configure RADIUS Authentication.....	32
1.7 Configure and Authentication Sequence	41

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.

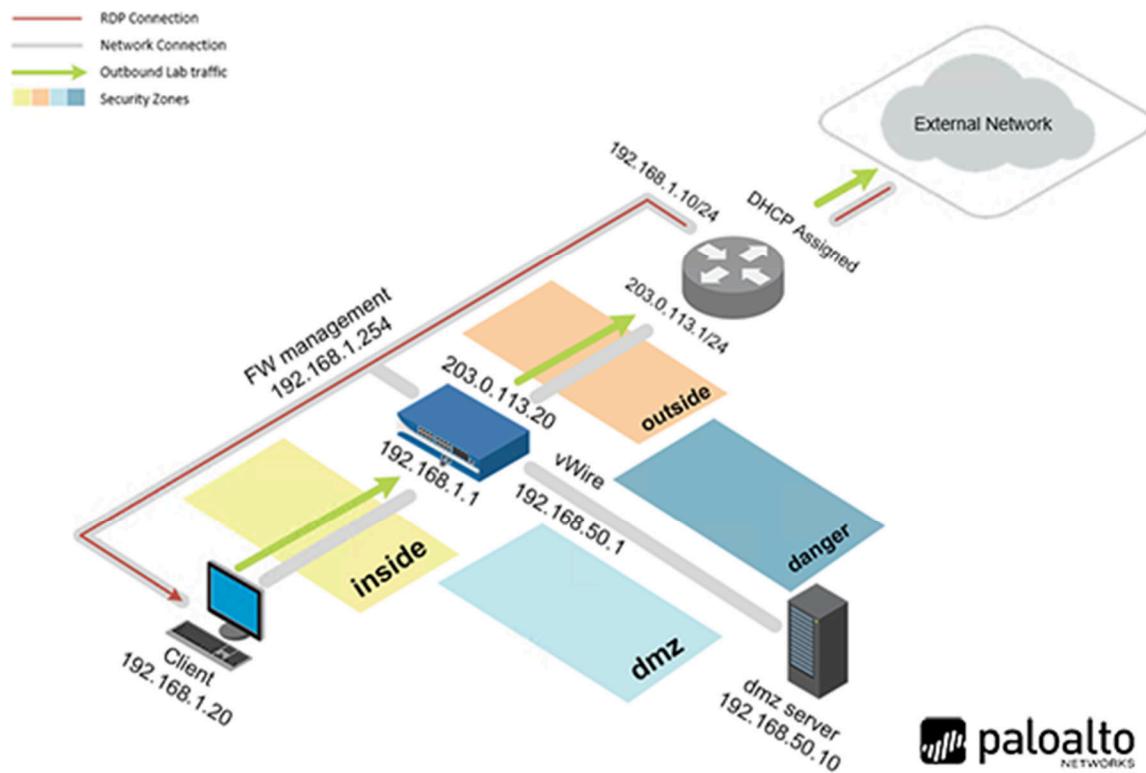
In this lab, you will provide management with those types of reports and to be able to restrict the applications.

Objective

In this lab, you will perform the following tasks:

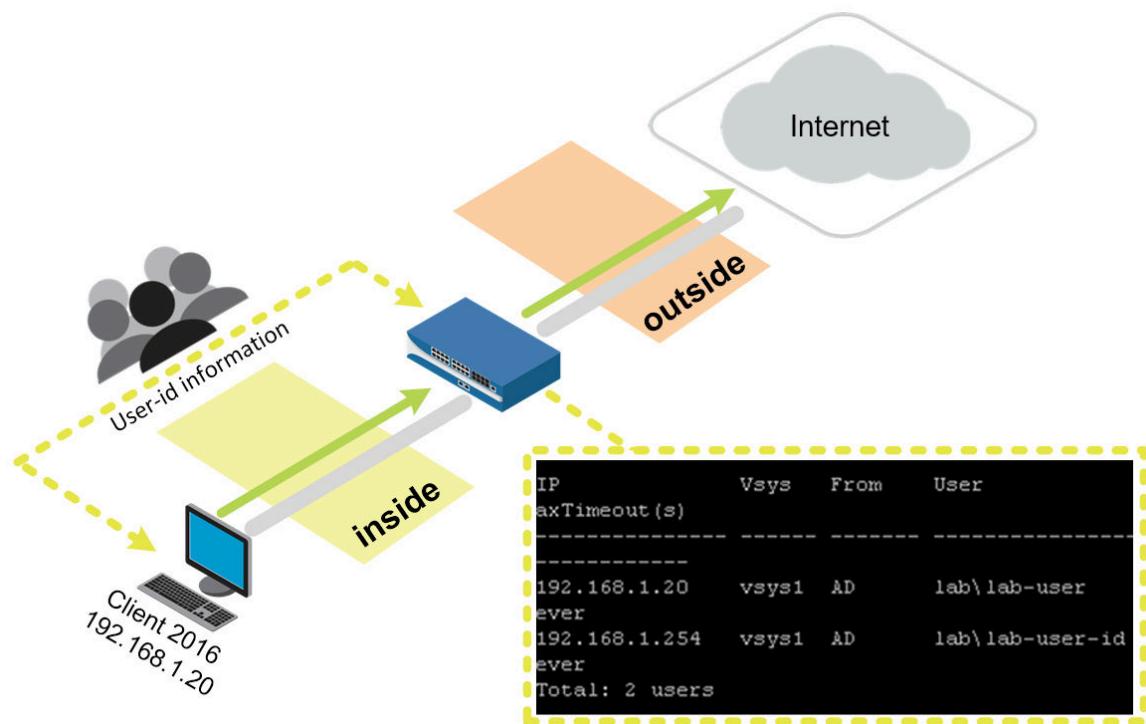
- Create a local firewall administrator account
- Configure an LDAP Server Profile
- Configure a RADIUS Server Profile
- Configure an LDAP Authentication Profile
- Configure a RADIUS Authentication Profile
- Configure an Authentication Sequence
- Create non-local firewall administrator accounts

Lab Topology



palo alto
NETWORKS

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!

1 Working with Firewall Configurations and Log Files

1.1 Apply a Baseline Configuration to the Firewall

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

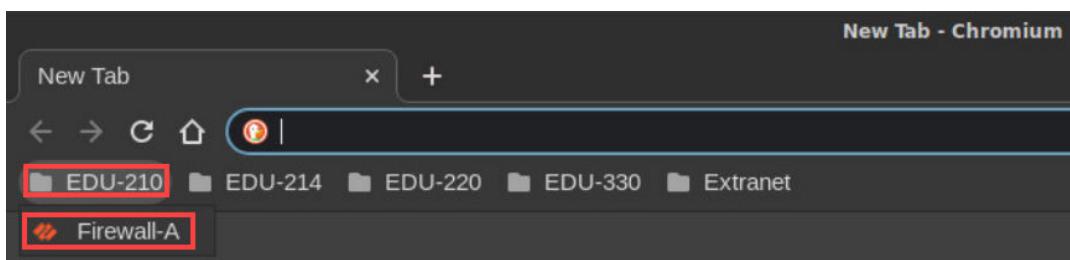
1. Click on the **Client** tab to access the Client PC.



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



3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.



4. You will see a "Your connection is not private" message. Next, 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.

5. 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 \(unsafe\)](#)

6. Log in to the firewall web interface as username **admin**, password **PaloAlt0!**.



The screenshot shows a login interface for a Palo Alto Networks device. The page has a yellow border. At the top is the Palo Alto Networks logo. Below the logo is a form with two input fields: one for the username containing "admin" and one for the password containing redacted dots. A blue "Log In" button is at the bottom. The entire form area is highlighted with a red box.

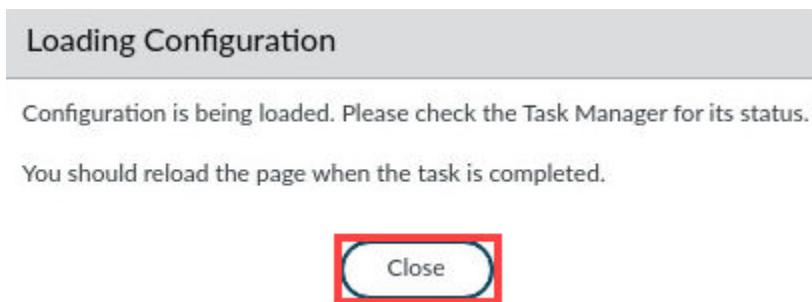
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

The screenshot shows the PA-VM web interface. The top navigation bar has tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE tab is highlighted with a red box. On the left, a sidebar menu is open, showing options like Setup (highlighted with a red box), High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, and Data Redistribution. The main content area is titled 'Configuration Management'. It contains several buttons: Revert (Revert to last saved configuration, Revert to running configuration), Save (Save named configuration snapshot, Save candidate configuration), Load (Load named configuration snapshot, Load configuration version). The 'Load named configuration snapshot' button is highlighted with a red box.

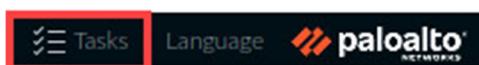
8. In the *Load Named Configuration* window, select **edu-210-lab-03.xml** from the *Name* dropdown box and click **OK**.

The screenshot shows the 'Load Named Configuration' dialog box. It has fields for 'Name' (set to 'edu-210-lab-03.xml') and 'Decryption Key' (set to '****'). There are two checkboxes at the bottom: 'Regenerate Rule UUIDs for selected named configuration' and 'Skip Validation'. At the bottom right are 'OK' and 'Cancel' buttons, with 'OK' highlighted with a red box.

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 successfully completed. Click **Close**.

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**

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

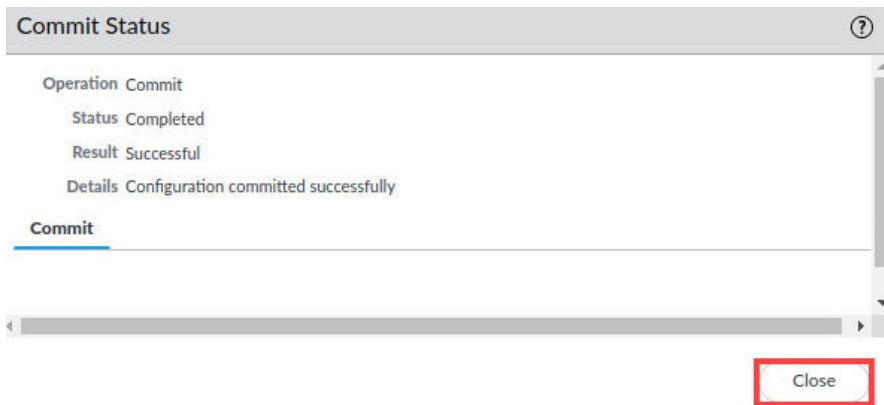
Preview Changes **Change Summary** **Validate Commit** Group By Location Type

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

Description

Commit **Cancel**

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



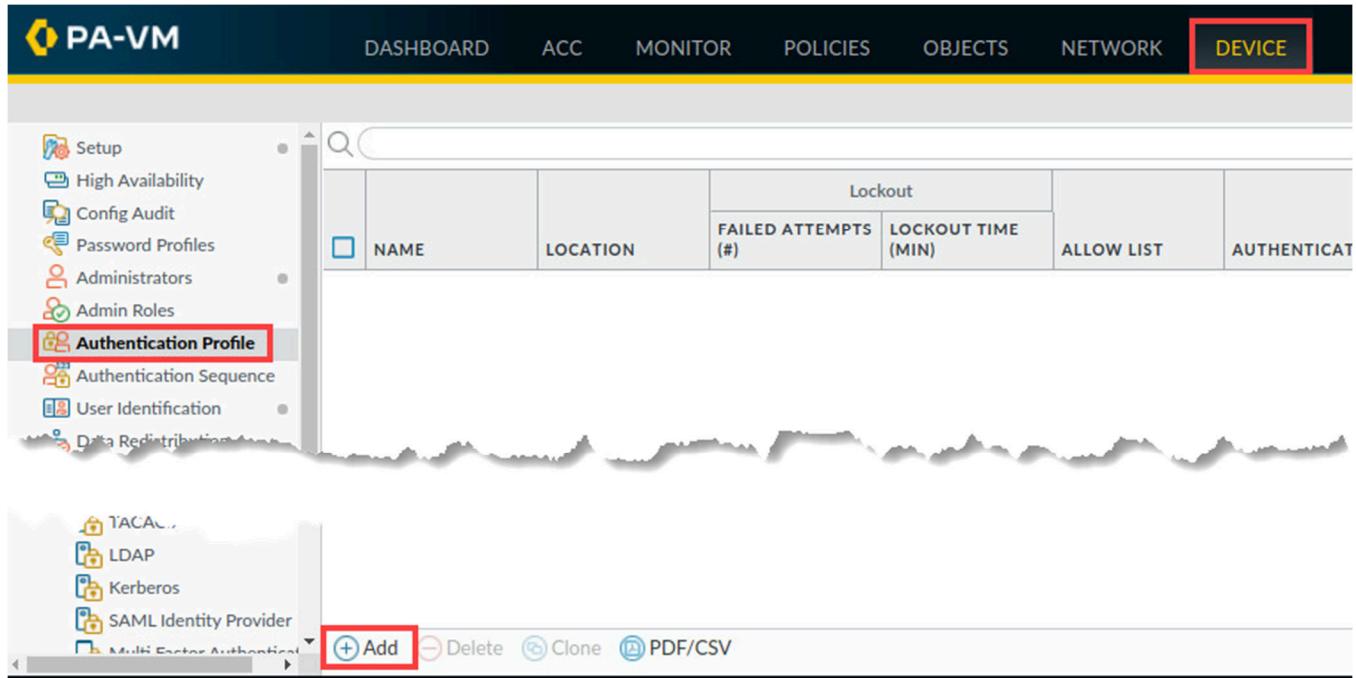
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

1.2 Create a Local Database Authentication Profile

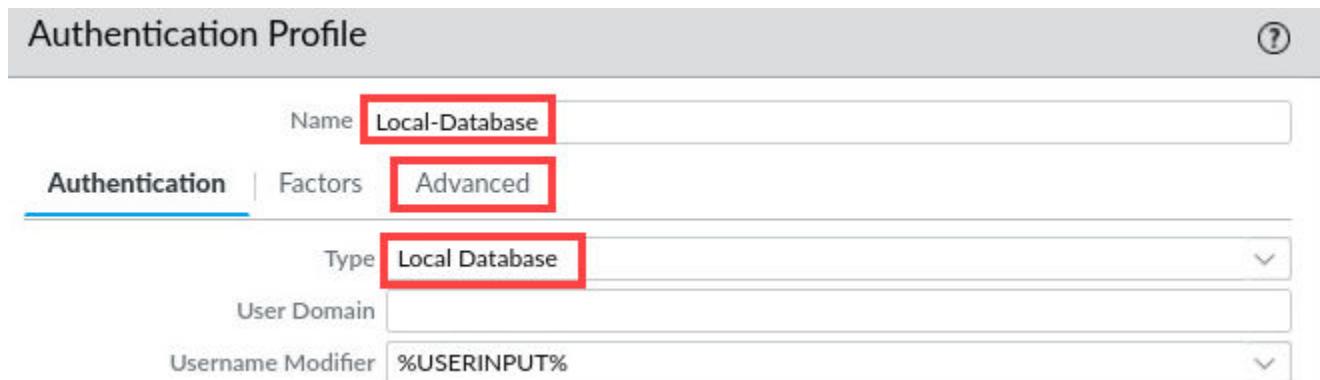
In this section, you will create a local database authentication profile. Local database profiles allow the firewall to authenticate administrators who need access to the firewall web interface through Captive Portal or GlobalProtect.

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



The screenshot shows the PA-VM web interface with the 'DEVICE' tab selected. On the left, a sidebar lists various configuration options, with 'Authentication Profile' highlighted. At the bottom of the main content area, there is a toolbar with several icons and a red box highlighting the '+ Add' button. The main table area is currently empty.

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**.



The screenshot shows the 'Authentication Profile' configuration window. The 'Name' field is set to 'Local-Database'. The 'Type' dropdown is set to 'Local Database'. The 'Advanced' tab is selected. Other tabs like 'Factors' and 'General' are visible but not selected. The 'User Domain' and 'Username Modifier' fields are also visible.

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

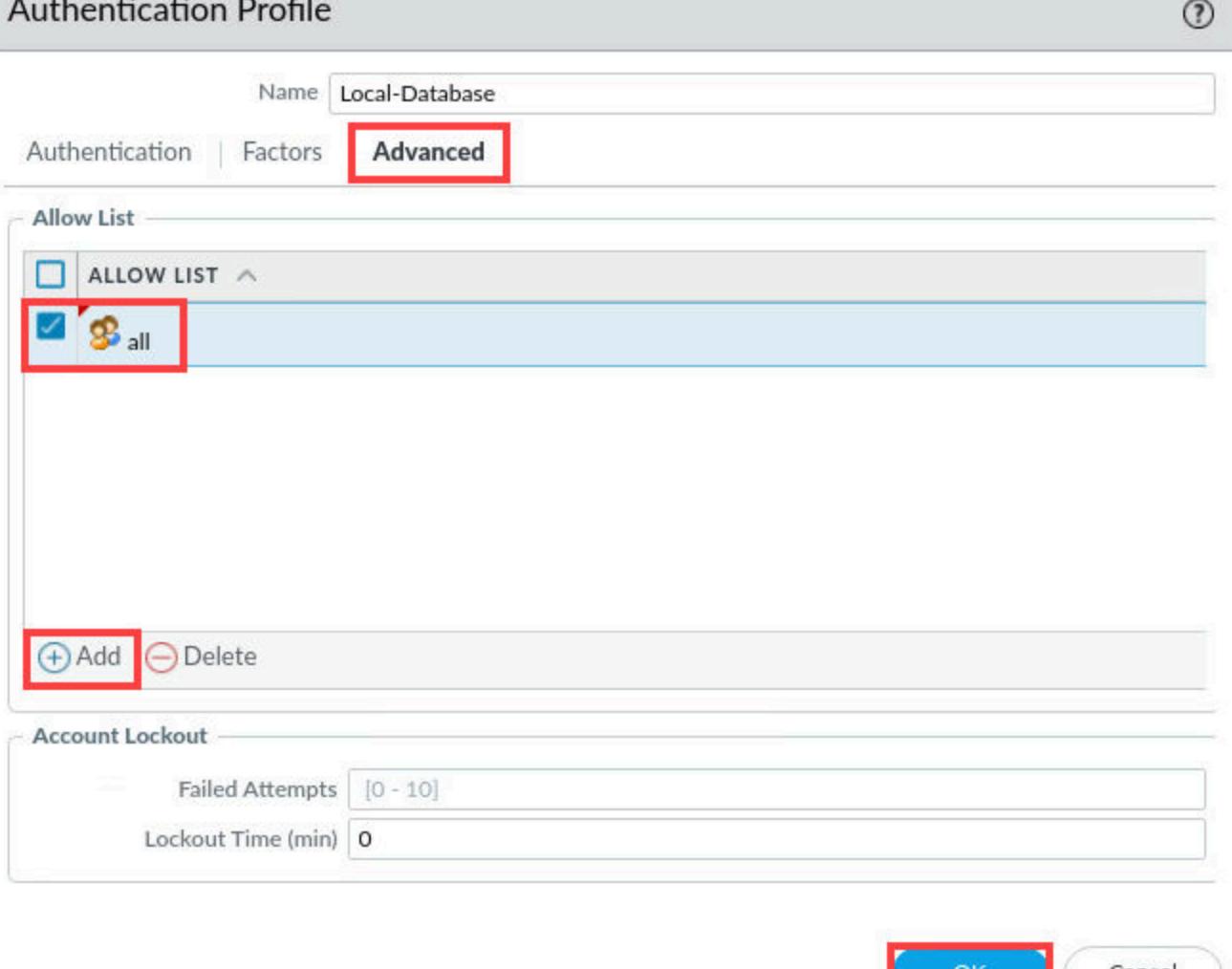
+ Add **- Delete**

Account Lockout

Failed Attempts: [0 - 10]

Lockout Time (min): 0

OK **Cancel**

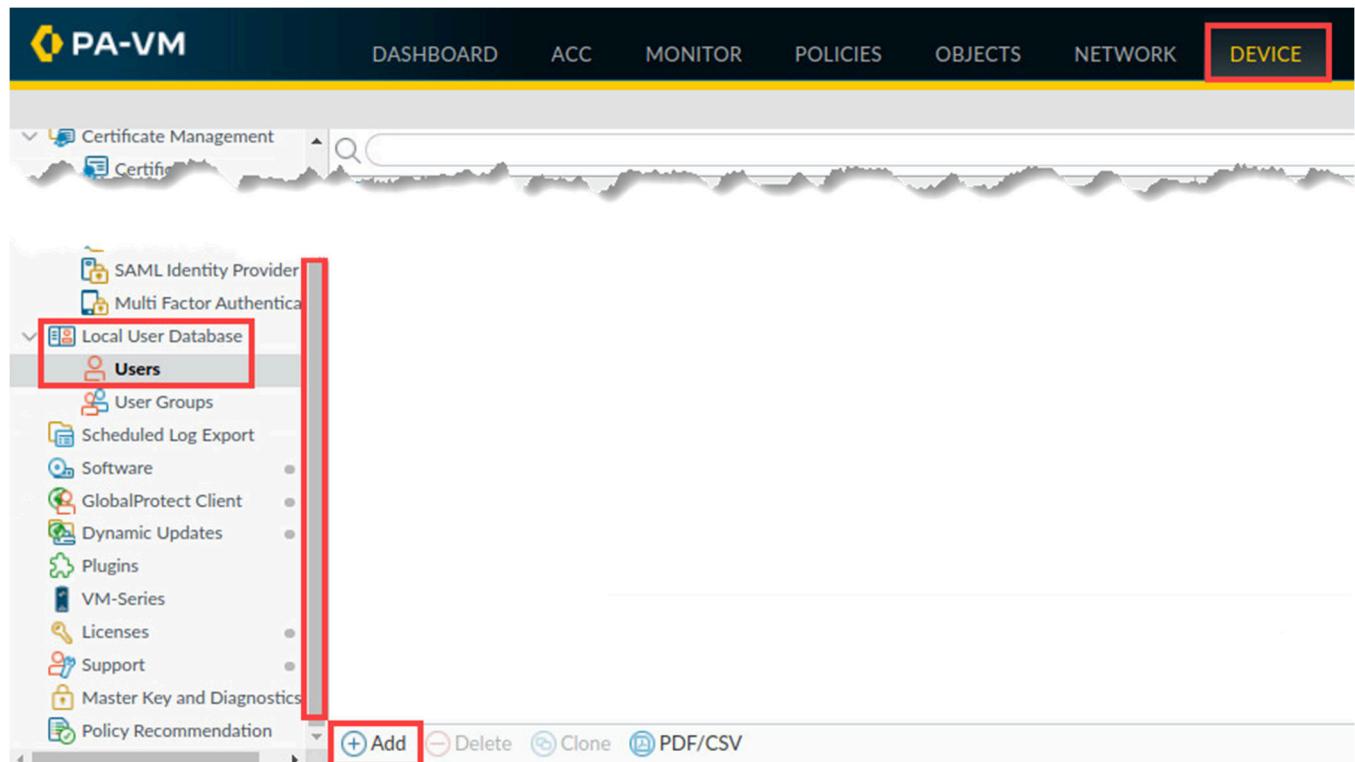


4. Leave the firewall web interface open to continue with the next task.

1.3 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 **Pa10Alt0!** for *Password* and *Confirm Password*. Click **OK**.

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

Name	adminBob
Mode	<input checked="" type="radio"/> Password <input type="radio"/> Password Hash
Password	*****
Confirm Password	*****
<input checked="" type="checkbox"/> Enable	
OK Cancel	

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

1.4 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 has tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE, with DEVICE highlighted. On the left, a sidebar menu includes: 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 of administrators. The columns are: NAME, ROLE, AUTHENTICATI..., PROFILE, PASSWORD PROFILE, CLIENT CERTIFICATE AUTHENTICATI... (WEB), and PUBLIC KEY AUTHENTICATI... (SSH). One row is shown for 'admin' with 'Superuser' as the role. At the bottom of the page, there is a toolbar with icons for L2/L3, LDAP, Kerberos, SAML Identity Provider, Multi Factor Authentication, and a plus sign labeled '+ Add'. Below the toolbar, there are buttons for '+ Add', 'Delete', and 'PDF/CSV'.

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. The 'Name' field contains 'adminBob' and the 'Authentication Profile' dropdown is set to 'Local-Database'. Below these fields are two checkboxes: 'Use only client certificate authentication (Web)' and 'Use Public Key Authentication (SSH)'. Under 'Administrator Type', the 'Dynamic' radio button is selected. A dropdown menu for 'Role' is open, showing 'Superuser'. At the bottom right are 'OK' and 'Cancel' buttons, with 'OK' highlighted with 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.

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



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

A screenshot of the 'Commit' window. It contains the following elements:

- A message: "Doing a commit will overwrite the running configuration with the commit scope."
- Two radio buttons: "Commit All Changes" (selected) and "Commit Changes Made By:(1) admin".
- A table with two rows:

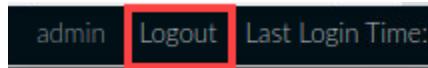
COMMIT SCOPE	LOCATION TYPE
device-and-network	
shared-object	
- Buttons at the bottom: "Preview Changes", "Change Summary", "Validate Commit", and a checked checkbox for "Group By Location Type".
- A note: "Note: This shows all the changes in login admin's accessible domain."
- A large text area labeled "Description" which is currently empty.
- Buttons at the bottom right: "Commit" (highlighted with a red box) and "Cancel".

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

A screenshot of the 'Commit Status' window. It displays the following information:

- "Operation Commit"
- "Status Completed"
- "Result Successful"
- "Details Configuration committed successfully"
- A "Commit" button at the bottom left.
- A "Close" button at the bottom right, highlighted with a red rectangular box.

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**.



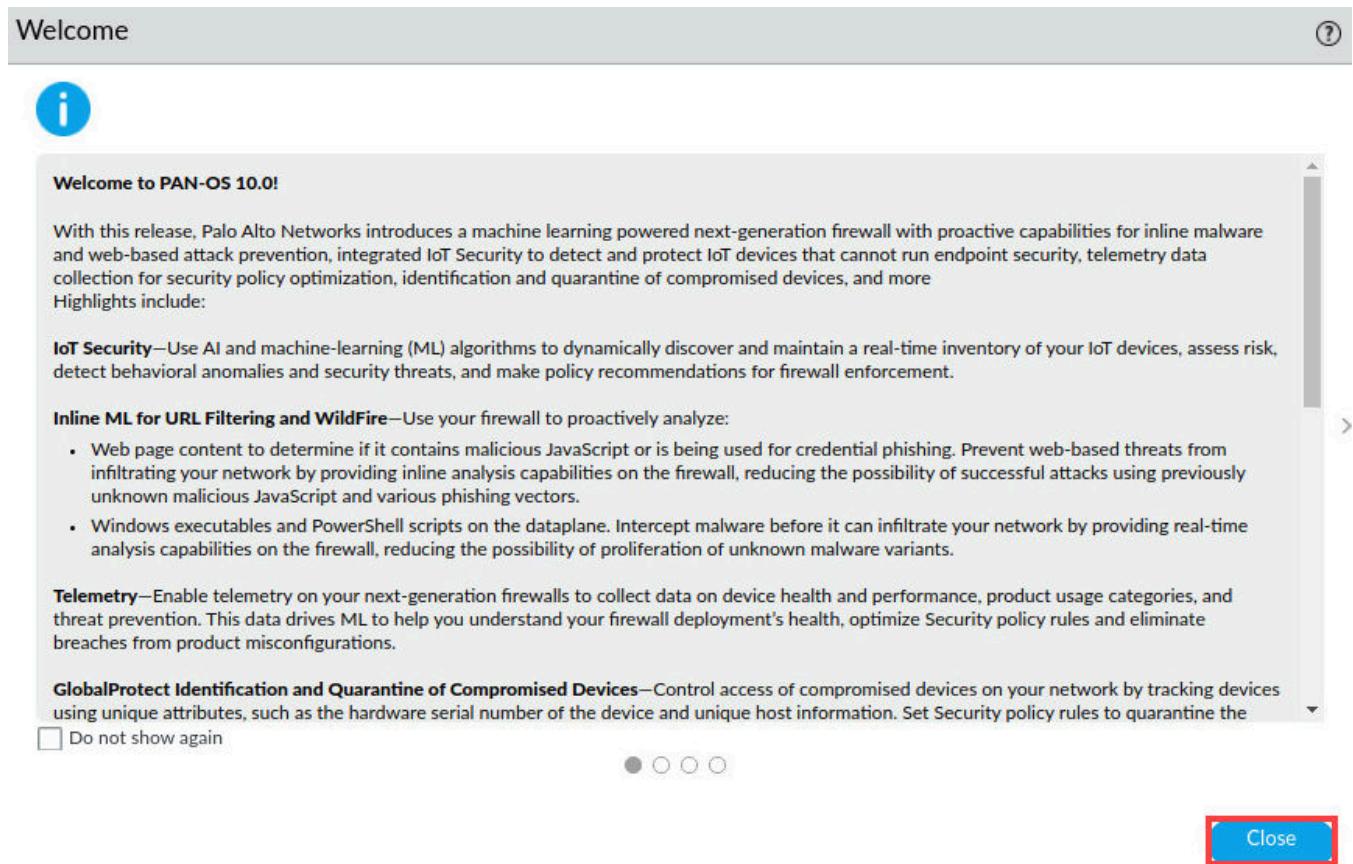
You have successfully logged out.



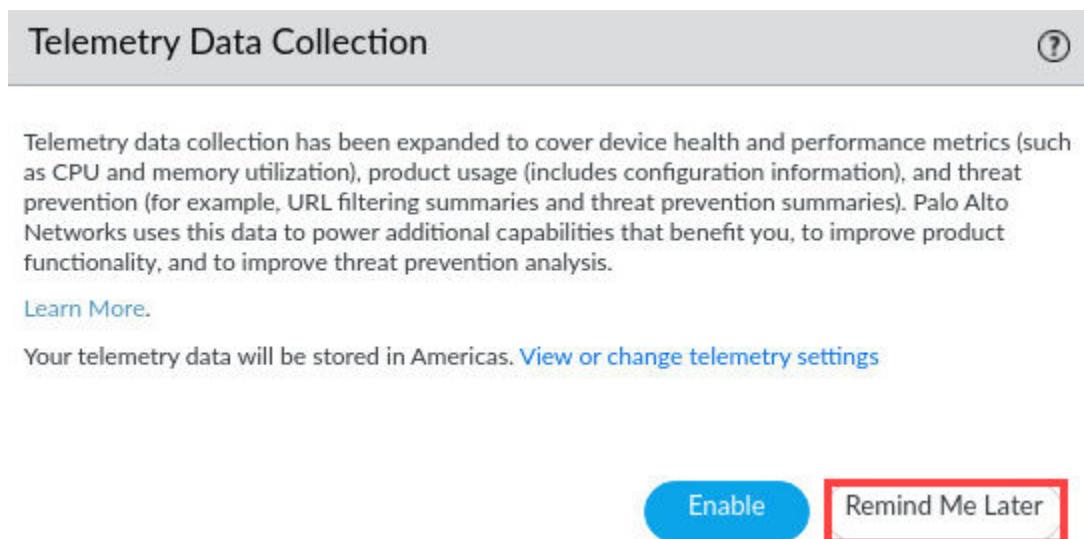
8. Log back into the firewall as username **adminBob**, password **Pal0Alt0!**. Click **Log In**.



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 17:09:49	general	informational	general		Connection to update server updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
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**.



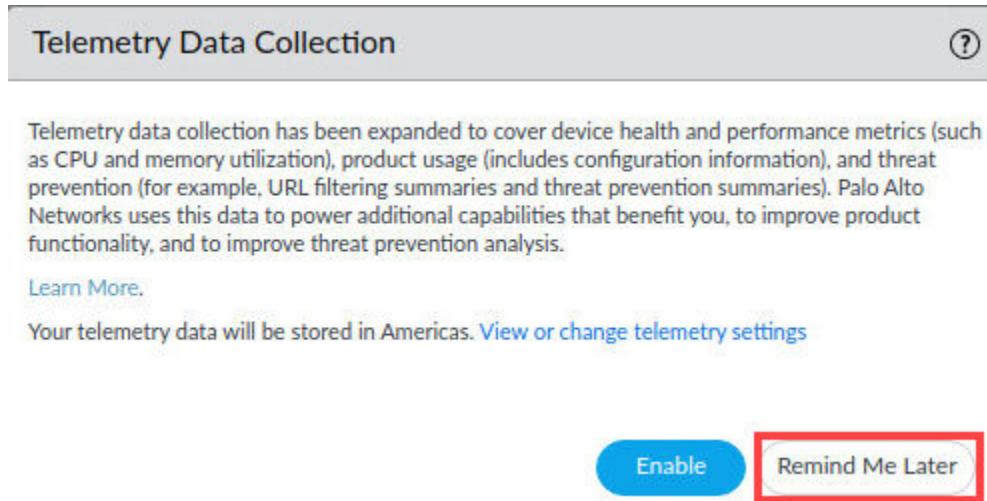
You have successfully logged out.

Log In

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

A screenshot of a web-based log-in interface. It features the Palo Alto Networks logo at the top. Below the logo are two input fields: one for the username containing "admin" and one for the password containing a series of dots. At the bottom is a blue "Log In" button. The entire form is enclosed in a yellow border.

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.

1.5 Configure LDAP Authentication

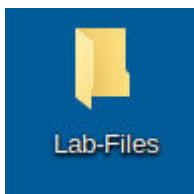
Your organization uses an LDAP server to maintain a database of users, including network administrators. Your team of security personnel is growing each month, and you want to leverage the existing LDAP server to authenticate administrators when they attempt to log into the firewall.

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.

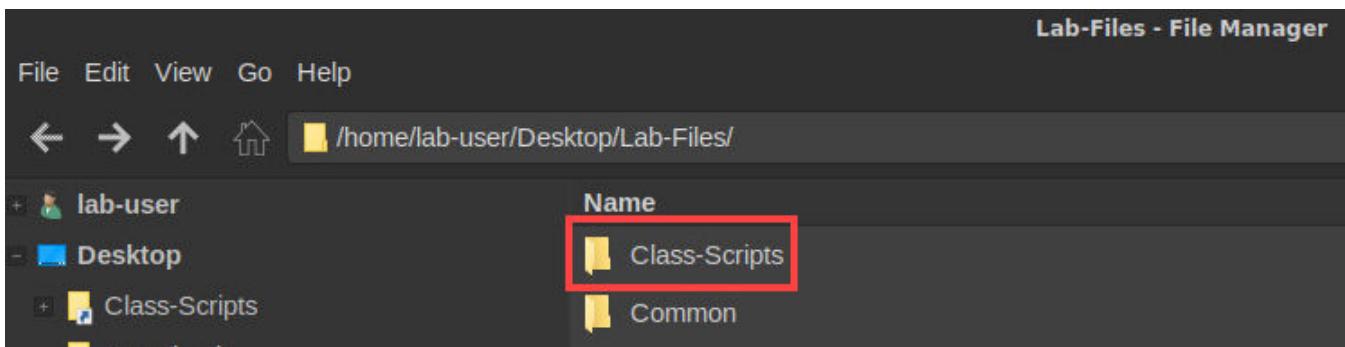
1. Minimize the PA-VM web interface.



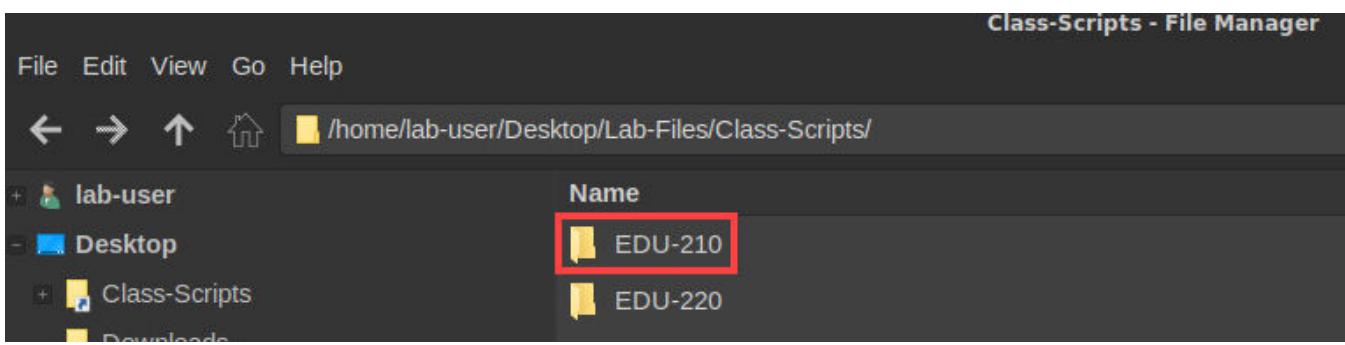
2. On the client desktop, open the **Lab-Files** folder.



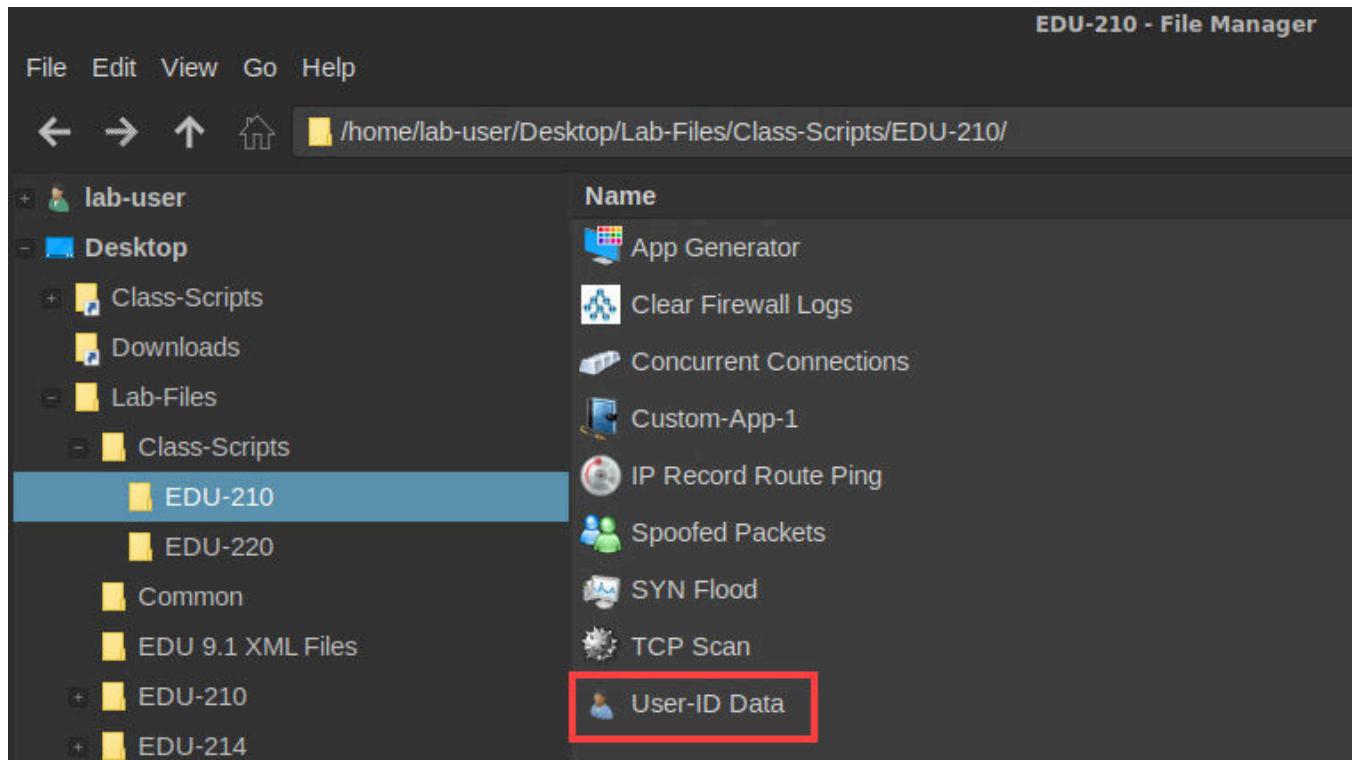
3. In the *Lab-Files* folder, open the **Class-Scripts**.



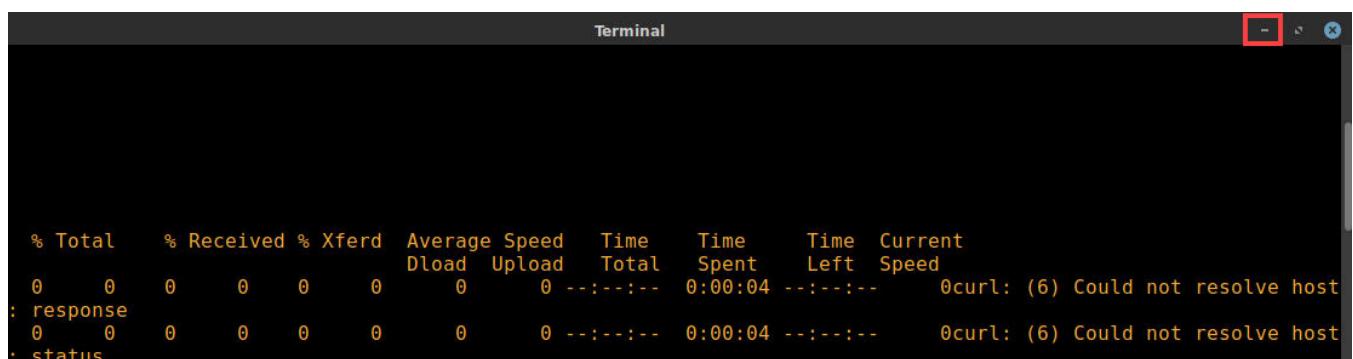
4. In the *Class-Scripts* folder, open the **EDU-210** folder.



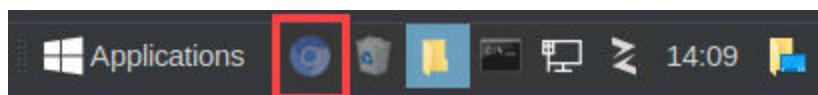
5. Execute the *User-ID Data* script by double-clicking it.



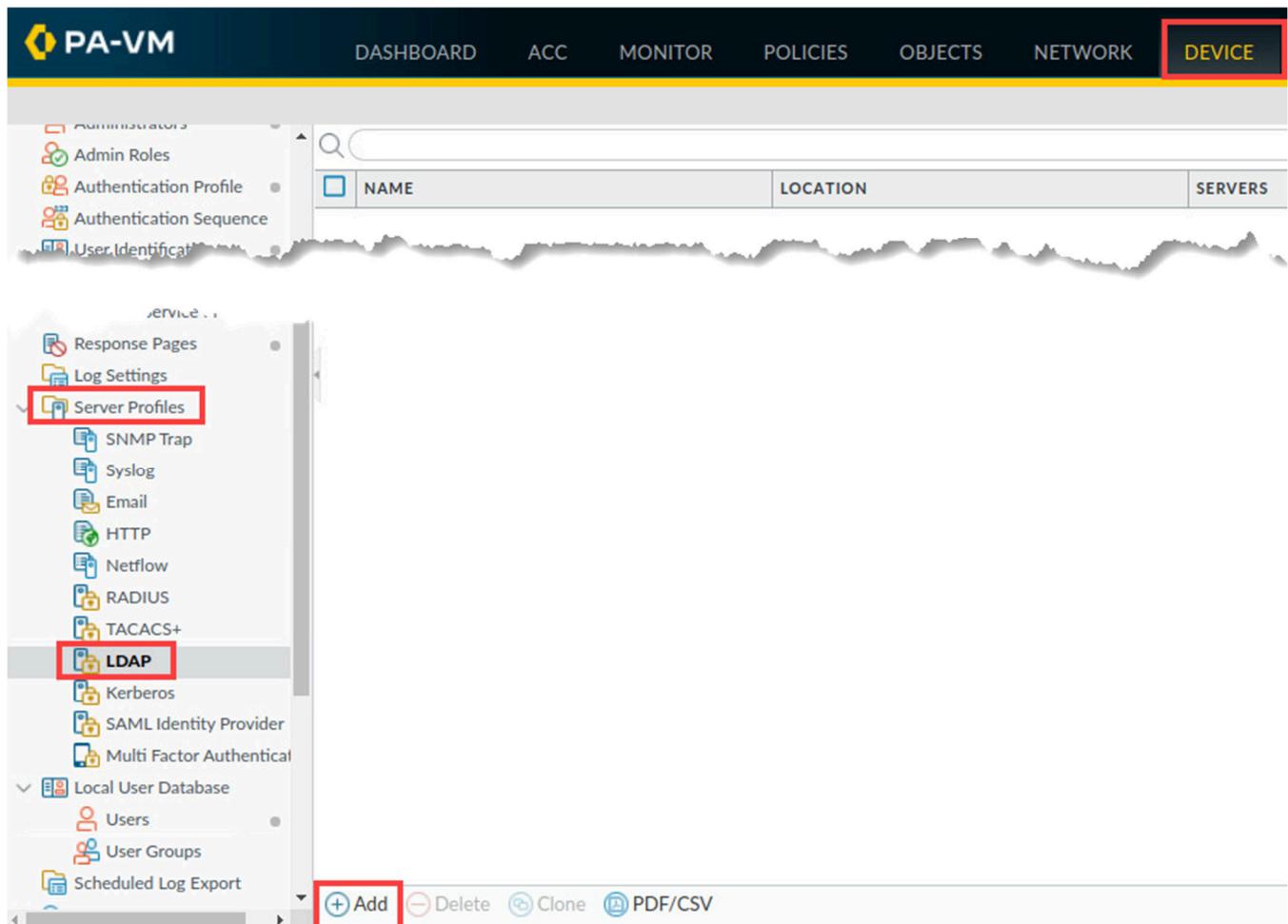
6. Notice the *Terminal* window will pop up. **Minimize** the terminal window and let it run for the remainder of the lab.



7. 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	<input type="text" value="LDAP Server Profile"/>	
<input type="checkbox"/> Administrator Use Only		
Server List		
NAME	LDAP SERVER	PORT
ldap.panw.lab	192.168.50.89	389
<input type="button" value="(+ Add)"/> <input type="button" value="(- 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 **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 checked="" type="checkbox"/> Require SSL/TLS secured connection <input type="checkbox"/> Verify Server Certificate for SSL sessions	
<input style="background-color: #0070C0; color: white; border-radius: 5px; padding: 5px; margin-right: 10px;" type="button" value="OK"/> <input style="border-radius: 5px; padding: 5px;" 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.

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

	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

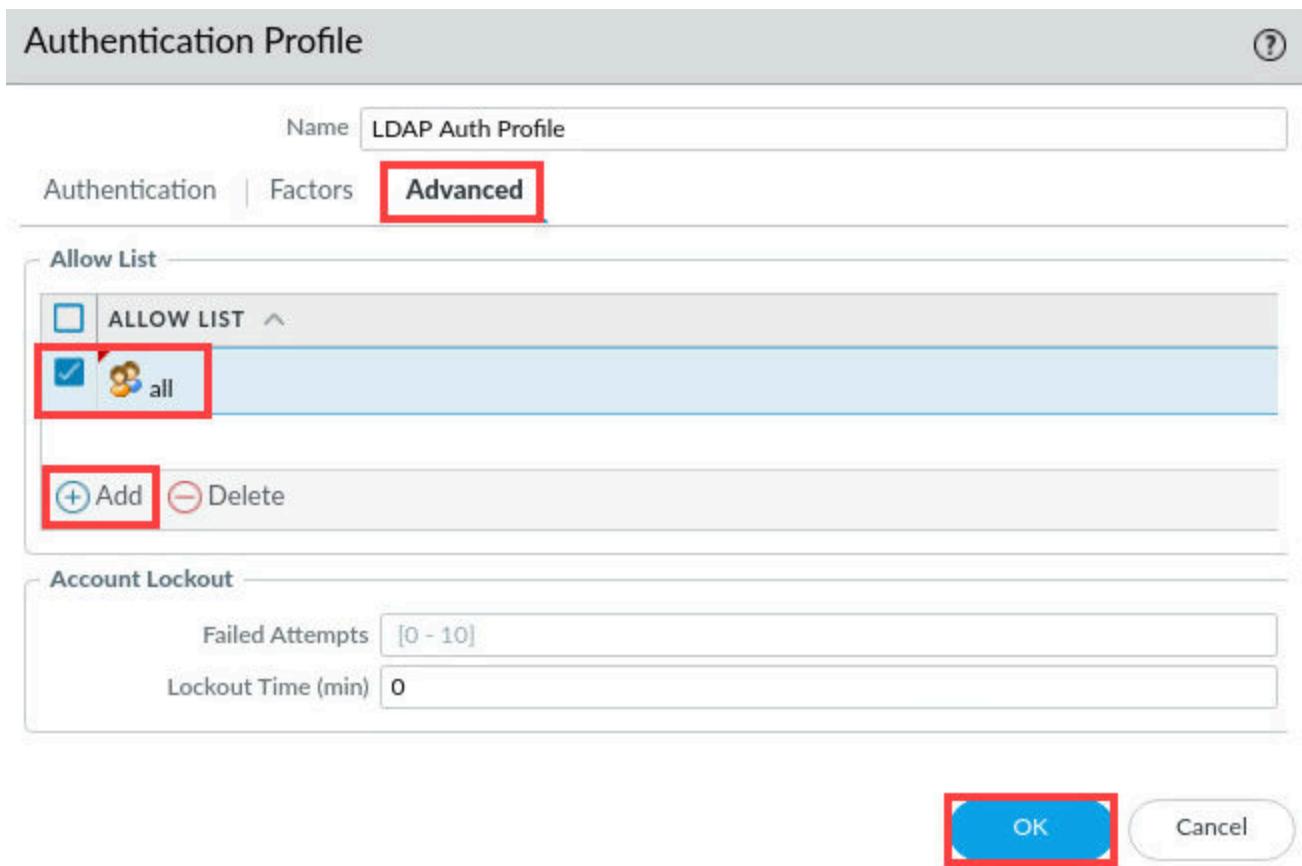
12. Select **Device > Authentication Profile**. Click **Add**.

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 by a red box. The main area displays a table of authentication profiles. One row is visible, showing 'Local-Database' as the name, with other columns for location, failed attempts, lockout time, allow list, and authentication type. At the bottom of the table, there are buttons for 'Add', 'Delete', 'Clone', and 'PDF/CSV'. The 'Add' button is also highlighted with a red box.

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'. The 'Type' dropdown is set to 'LDAP'. The 'Server Profile' dropdown is set to 'LDAP Server Profile'. The 'Advanced' button is highlighted with a red box. The 'Factors' tab is also visible.

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



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

The screenshot shows the PA-VM interface with the 'DEVICE' tab selected. In the sidebar, the 'Administrators' link is highlighted with a red box. The main table lists two administrators: 'admin' and 'adminBob'. The 'Add' button at the bottom left of the table is highlighted with a red box.

	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"/>

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



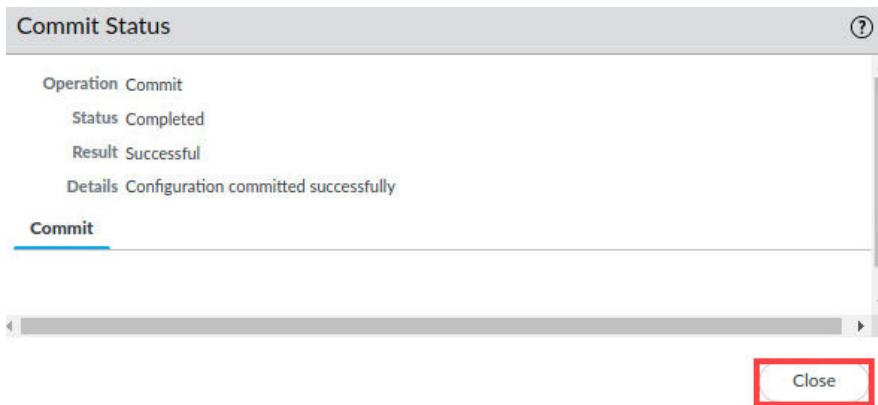
The adminSally account is one which exists in the LDAP server.

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

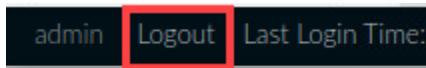


18. In the *Commit* window, click **Commit** to proceed with committing the changes.

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**.



You have successfully logged out.

Log In

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

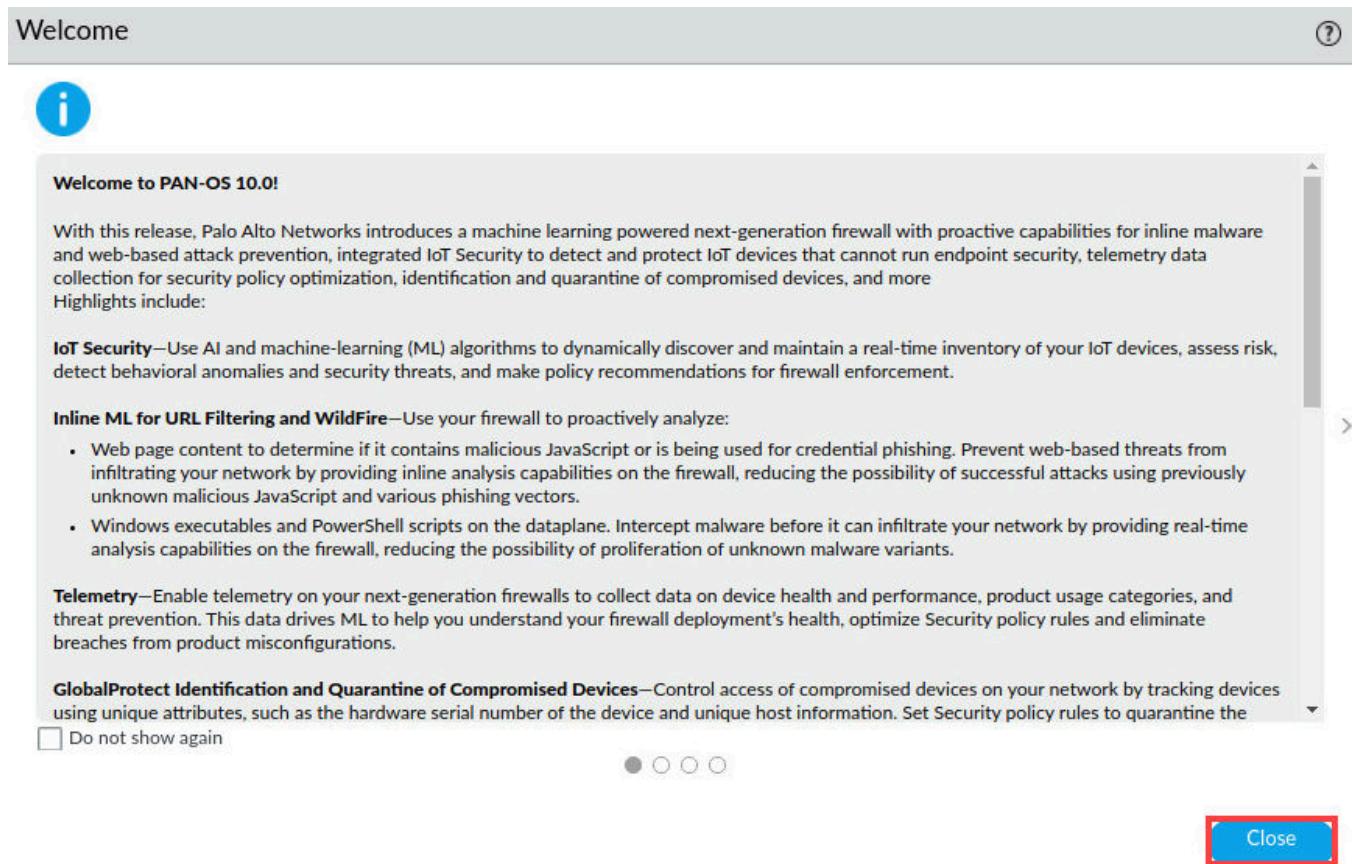


adminSally

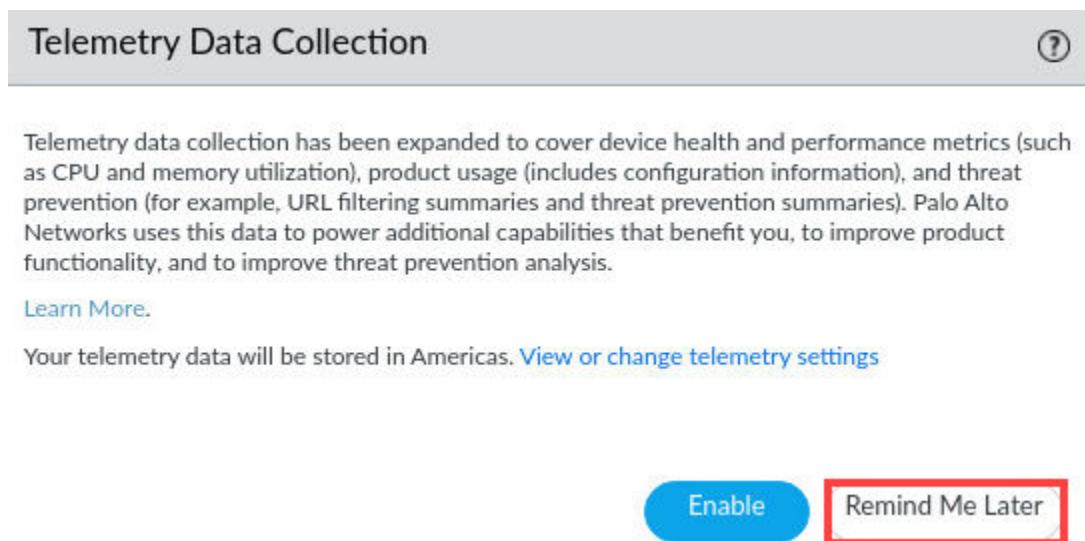
.....

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.

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. The left sidebar has a 'Logs' section with various categories like Traffic, Threat, URL Filtering, etc., and a 'System' category which is also highlighted with a red box. The main area displays a log table with columns: RECEIVE TIME, TYPE, SEVERITY, EVENT, OBJECT, and DESCRIPTION. The log entries show various system events, and the last entry, at 08/06 17:57:59, is highlighted with a red box and labeled 'auth-success' in the 'EVENT' column. The 'DESCRIPTION' column for this entry details the authentication attempt for user 'adminSally' against an LDAP server.

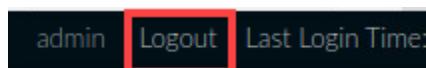
RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
08/06 17:58:25	general	informational	general		User adminSally accessed Monitor tab
08/06 17:58:11	general	informational	general		WildFire update job succeeded for user Auto update agent
08/06 17:58:10	general	informational	general		WildFire package 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.

Log In

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



admin

.....

Log In

29. In the *Telemetry Data Collection* pop-up, 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**

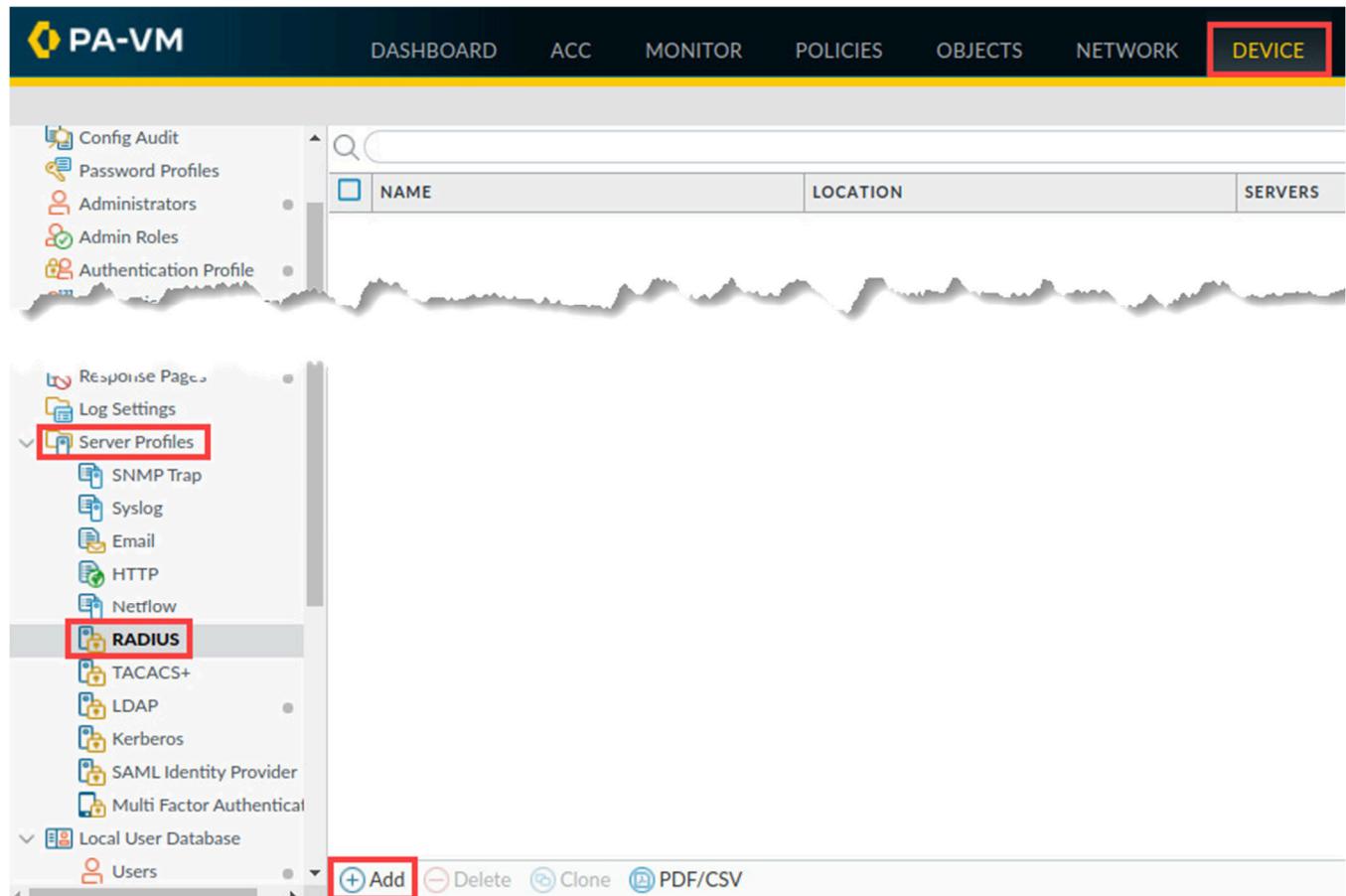
30. Leave the firewall web interface open to continue with the next task.

1.6 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 **Pal0Alt0!** 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.

The screenshot shows the PA-VM interface with the 'DEVICE' tab selected. On the left, a sidebar lists various configuration options. The 'Authentication Profile' option is highlighted with a red box. Below the sidebar, a table displays existing authentication profiles: 'Local-Database' and 'LDAP Auth Profile'. At the bottom of the table, there are buttons for '+ Add', 'Delete', 'Clone', and 'PDF/CSV'. The '+ Add' button is also highlighted with a red box.

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 contains 'RADIUS Auth Profile'. The 'Advanced' tab is selected. Under the 'Type' section, 'RADIUS' is selected. Under the 'Server Profile' section, 'RADIUS Server Profile' is selected. A checkbox for 'Retrieve user group from RADIUS' is present but unchecked.

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

+ 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**.

PA-VM

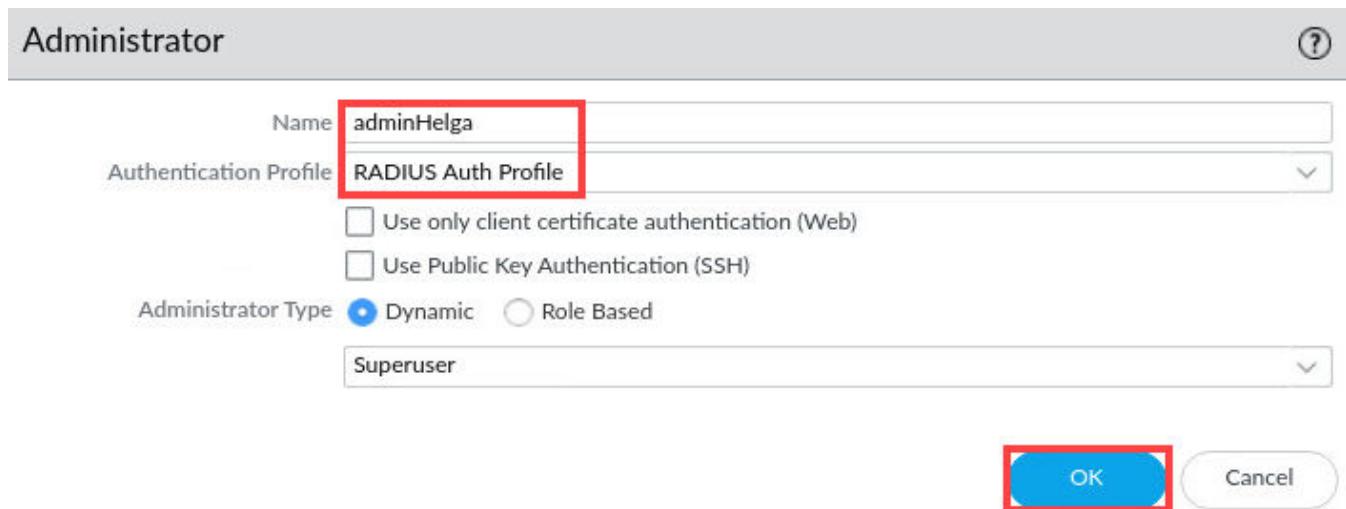
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

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

	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"/>

+ Add **- Delete** **PDF/CSV**

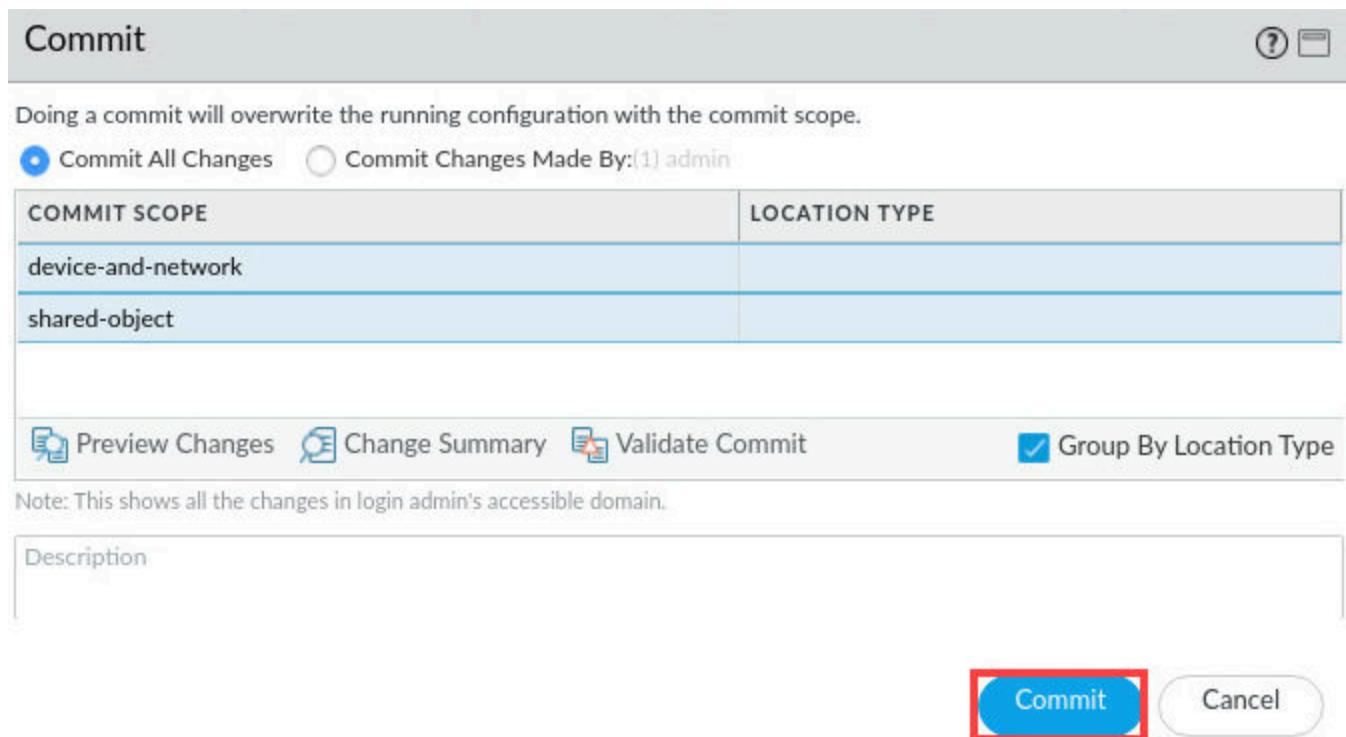
7. In the *Administrator* window, enter **adminHelga** for the *Name*. For the *Authentication Profile*, select **RADIUS Auth Profile**. Click **OK**.



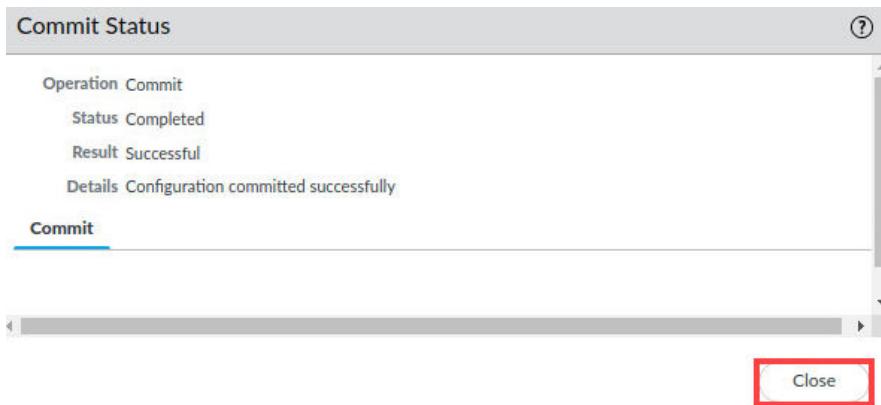
8. Click the **Commit** link located at the top-right of the web interface.



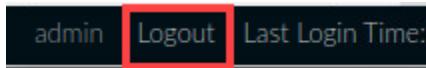
9. In the *Commit* window, click **Commit** to proceed with committing the changes.



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.



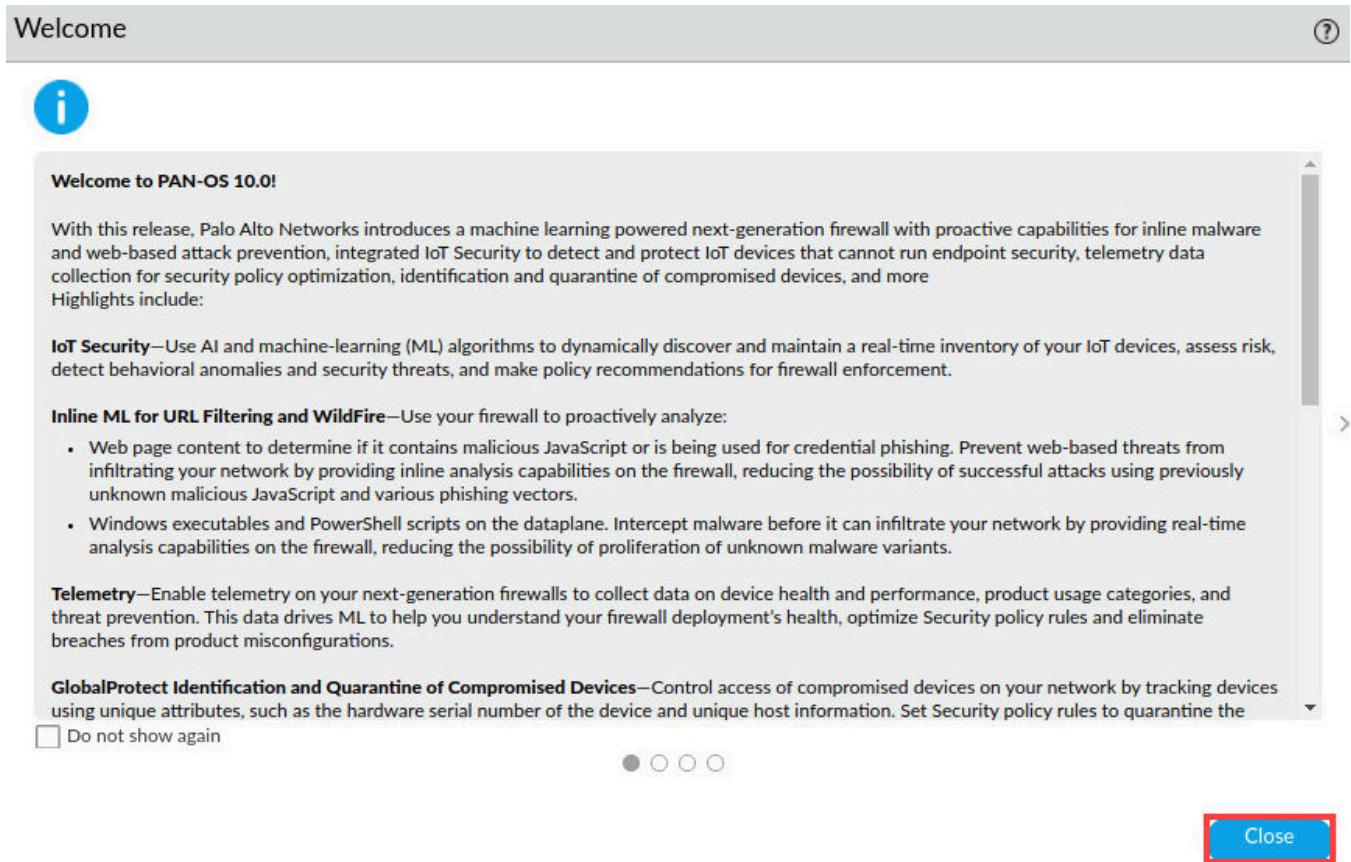
12. In the *Log In* window, click **Log In**.



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 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.

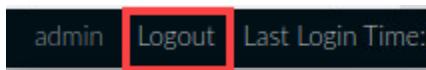
RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
08/06 18:38:38	general	informational	general		User adminHelga accessed Monitor tab
08/06 18:38:13	general	informational	general		User adminHelga logged in via Web from 192.168.1.20 using https
08/06 18:38:13	auth	informational	auth-success	RADIUS Auth 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-TLS. 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.

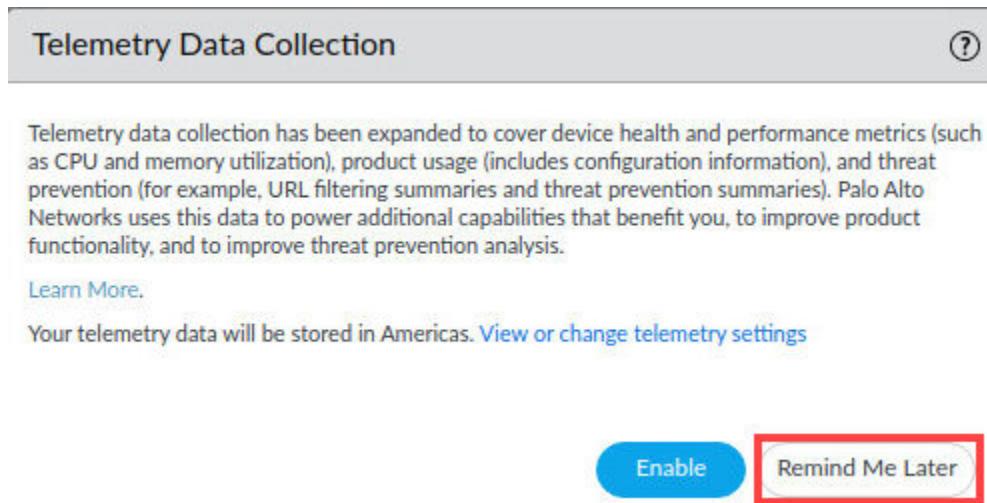
Log In

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



The screenshot shows the Palo Alto Networks login interface. It features the company logo at the top. Below it is a form with two text input fields: one for the username ('admin') and one for the password (represented by a series of dots). A large yellow rectangular box surrounds the entire form area. At the bottom of the form is a blue 'Log In' button, which is also highlighted with a red box.

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



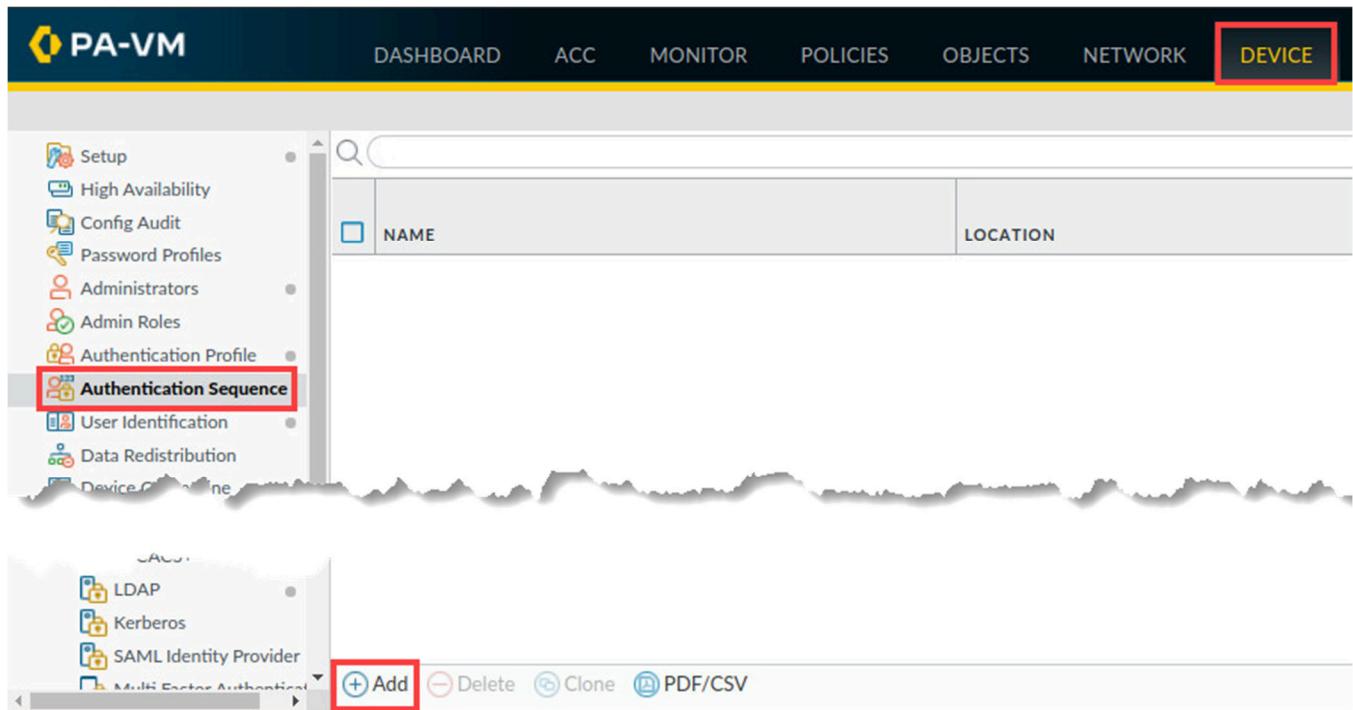
21. Leave the firewall web interface open to continue with the next task.

1.7 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**.

The screenshot shows the 'Authentication Sequence' dialog box. The 'Name' field contains 'LDAP then RADIUS'. Under 'Authentication Sequence Settings', there's a checkbox for 'Use domain to determine authentication profile' which is checked. The 'AUTHENTICATION PROFILES' section contains two entries: 'LDAP Auth Profile' and 'RADIUS Auth Profile', with 'RADIUS Auth Profile' selected and checked. At the bottom of the dialog, there are buttons for '+ Add', 'Delete', 'Move Up', 'Move Down', 'OK', and 'Cancel'. The 'OK' button is highlighted with a red box.



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.