# PALO ALTO NETWORKS EDU 210

# Lab 3: Working with Firewall Administrator Accounts

**Document Version: 2021-09-27**

# Contents

## 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.

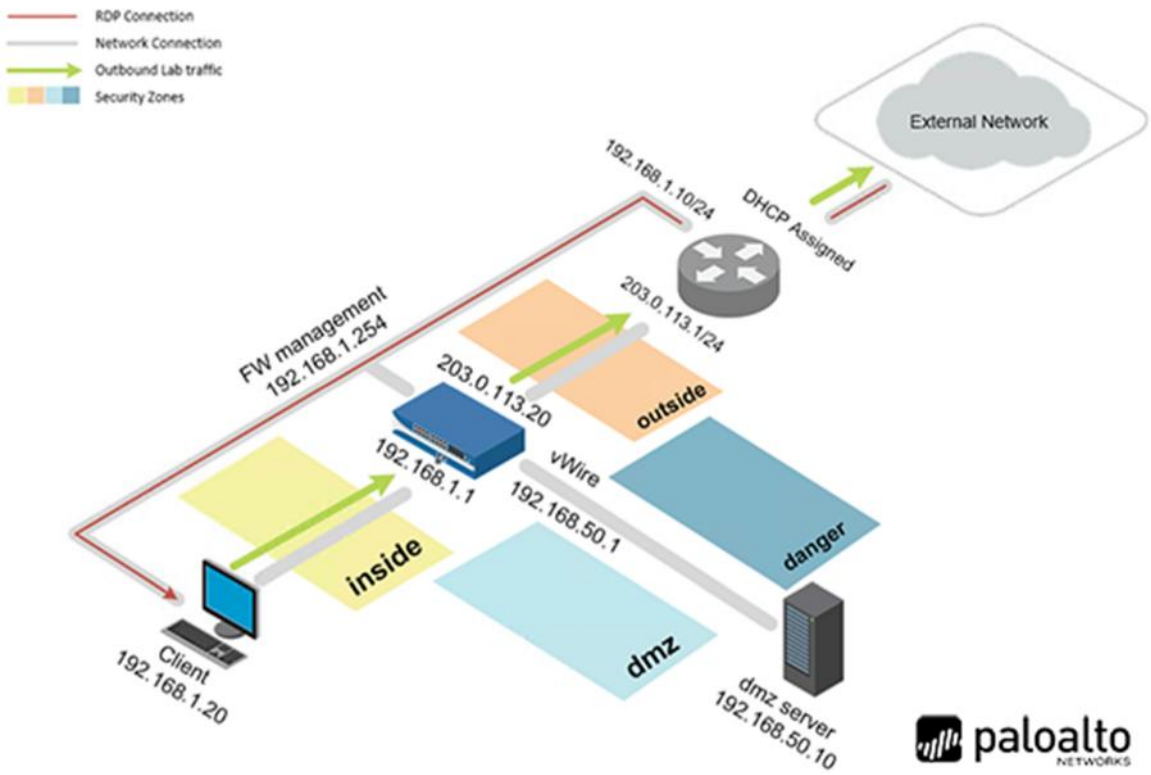
In this lab, you will provide management with those types of reports and to be able to restrict the applications.

## Objective

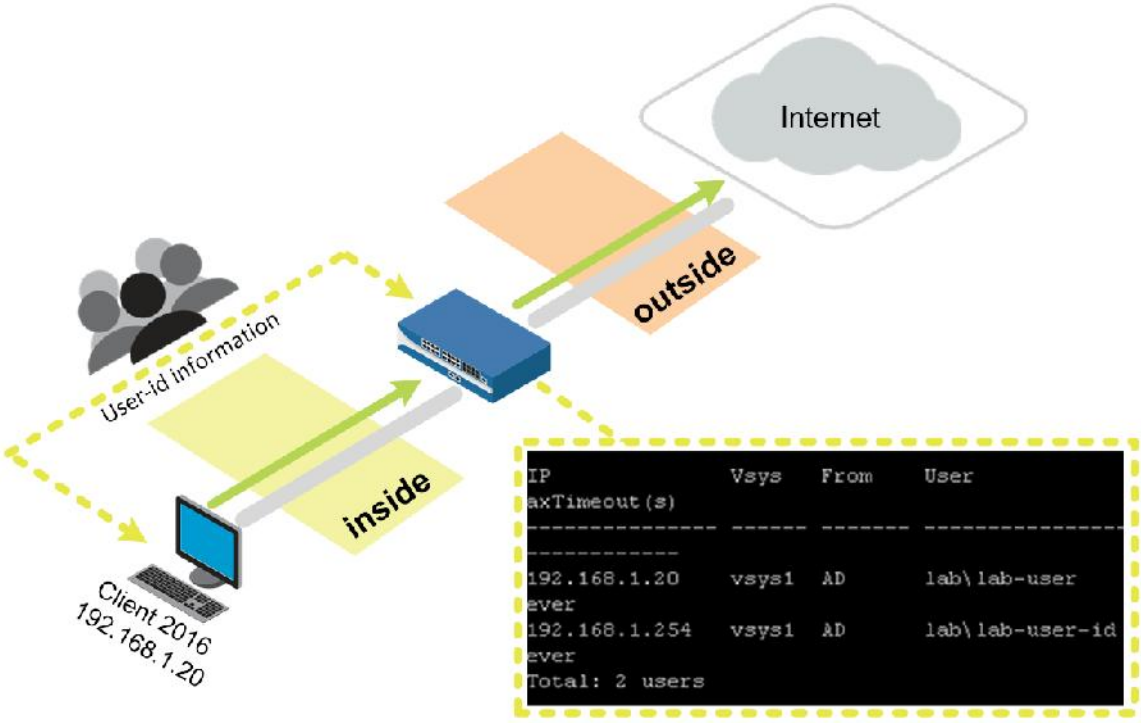
In this lab, you will perform the following tasks:

- 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.

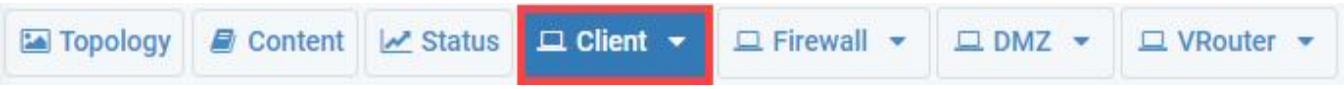
| **Virtual Machine** | **IP Address** | **Account** (if needed) | **Password** (if needed) |
|---|---|---|---|
| Client | 192.168.1.20 | lab-user | **Pal0Alt0!** |
| DMZ | 192.168.50.10 | root | **Pal0Alt0!** |
| Firewall | 192.168.1.254 | admin | **Pal0Alt0!** |
| VRouter | 192.168.1.10 | root | **Pal0Alt0!** |

# 3 Working with Firewall Configurations and Log Files

## 3.1 Apply a Baseline Configuration to the Firewall

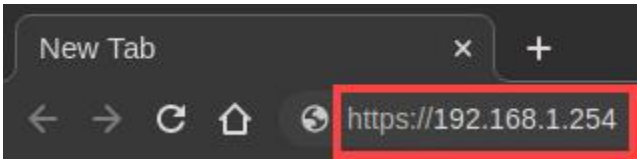
In this section, you will load the Firewall configuration file.

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

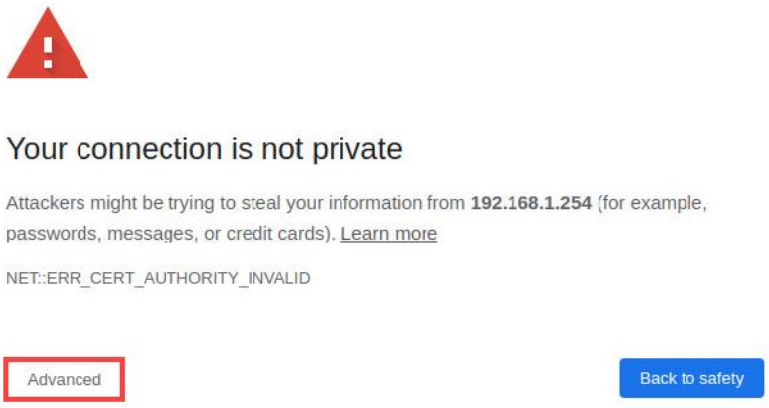



2. Double-click the **Chromium Web Browser** icon located on the *desktop*.


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

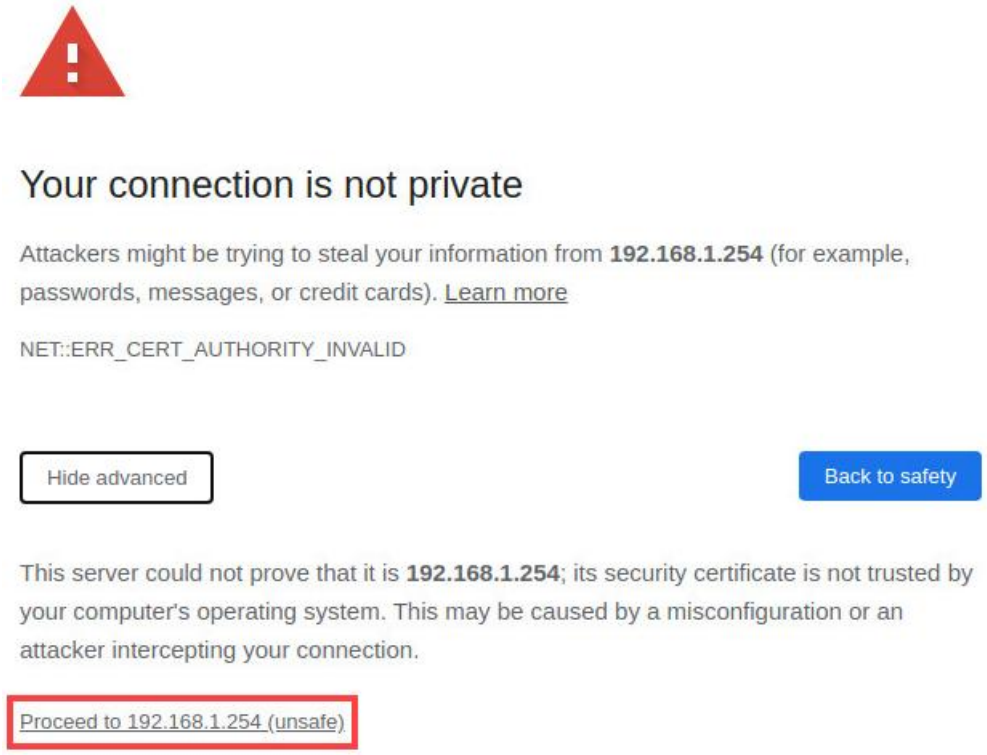



4. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.




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.

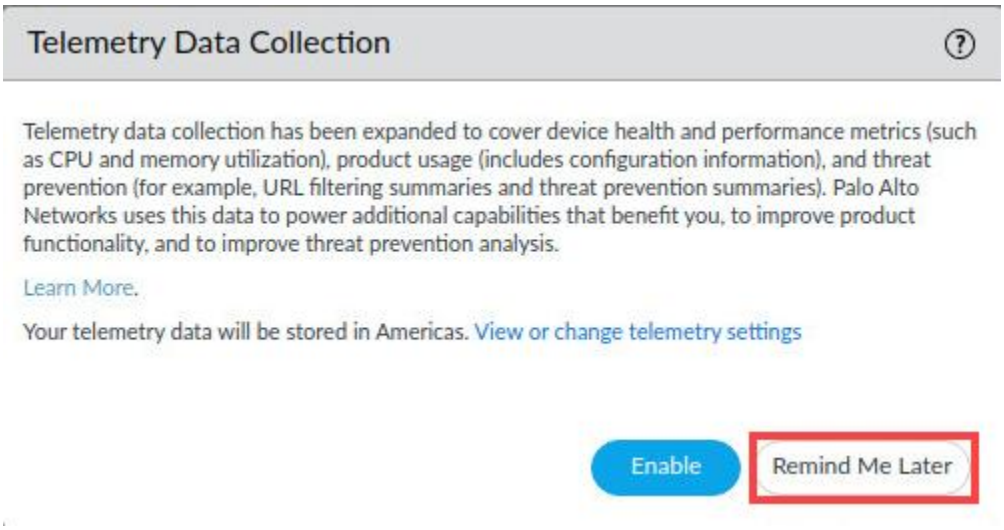
5. Click on **Proceed to 192.168.1.254 (unsafe)**.




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

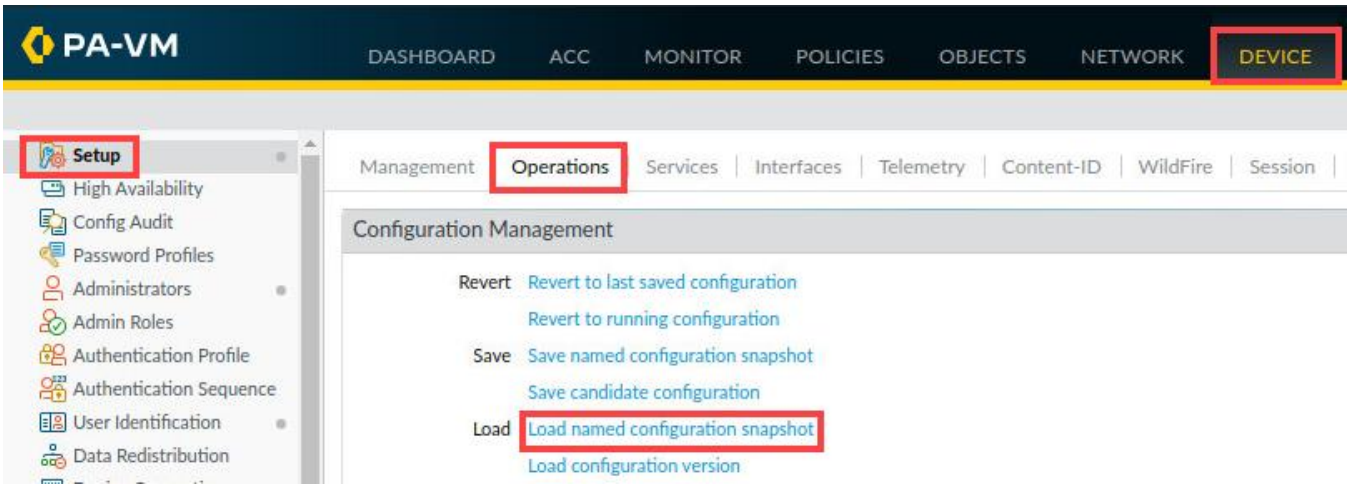
7. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.




Please Note

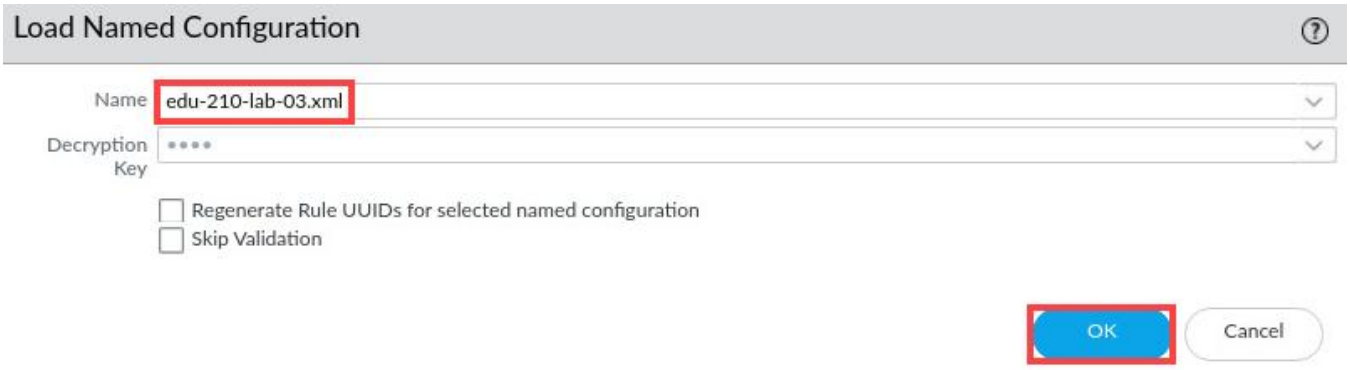
Before you can enable Telemetry Data Collection, you will need to install a device certificate. For this lab, you will not be using Telemetry Data Collection.

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

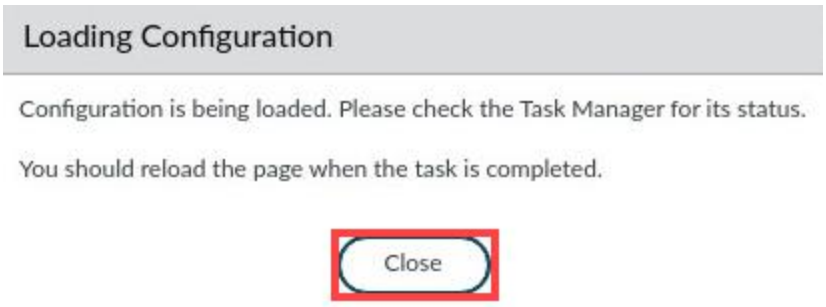


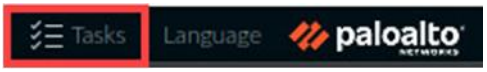
9. In the *Load Named Configuration* window, select **edu-210-lab-03.xml** from the *Name* dropdown box and click **OK**.




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.

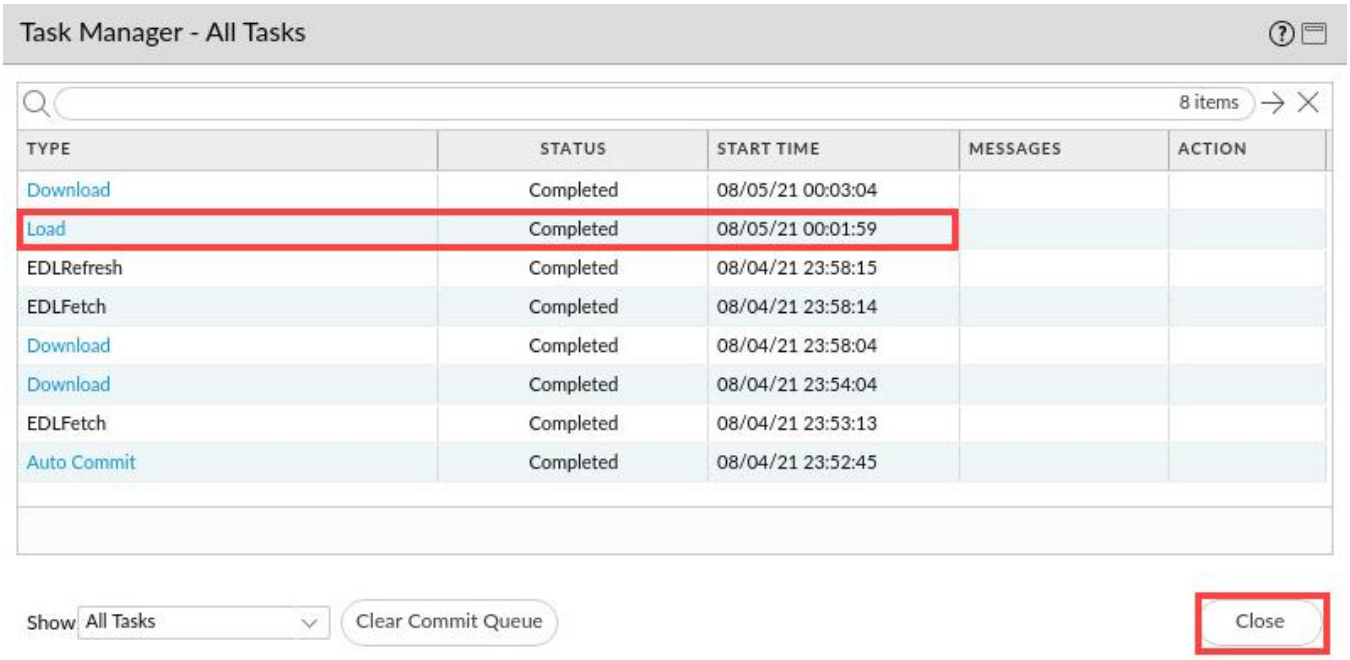



11. Click the **Tasks** icon located at the bottom-right of the web interface.



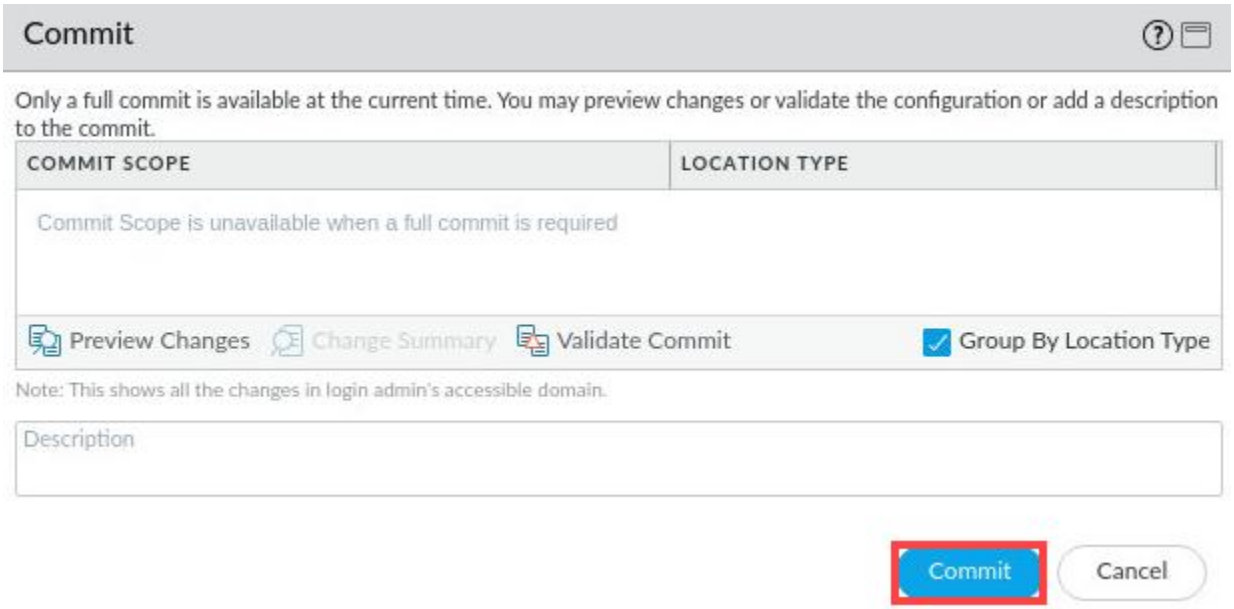

  

12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



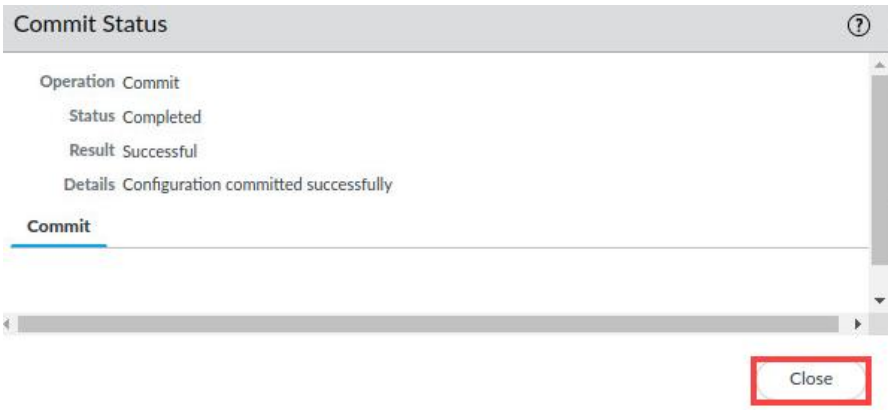

13. Click the **Commit** link located at the top-right of the web interface.


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



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



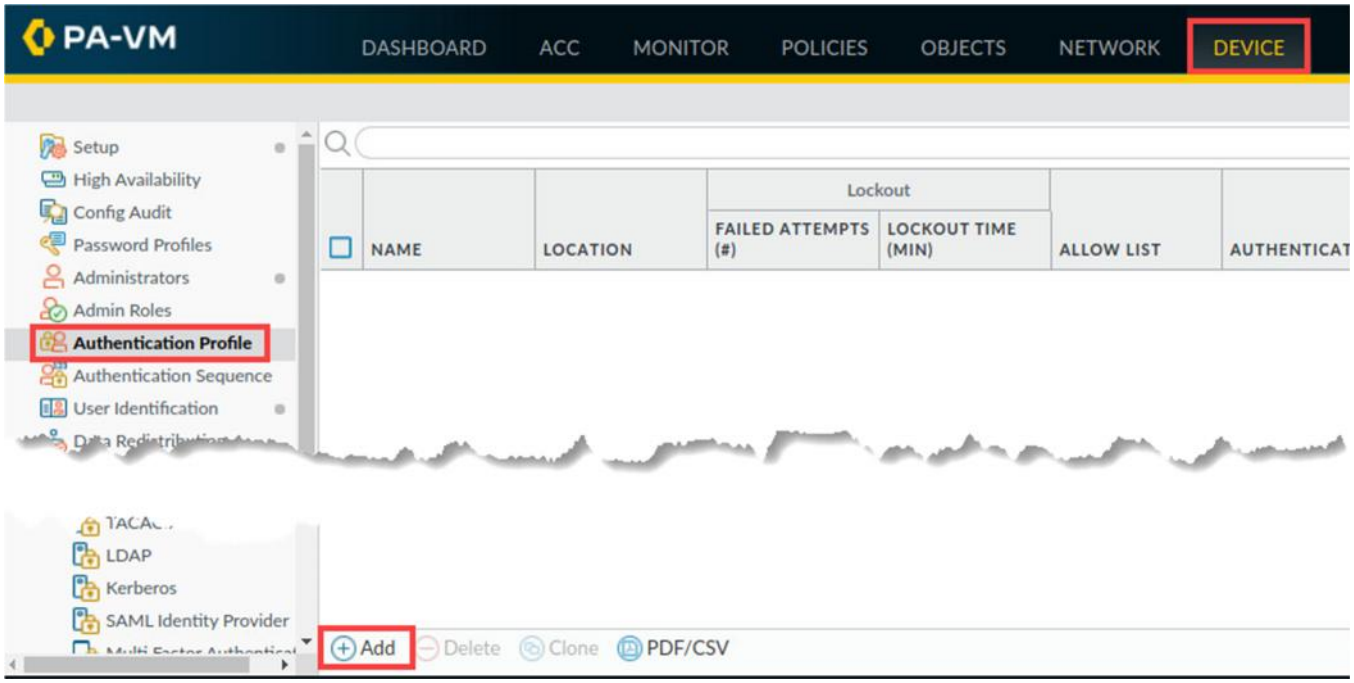

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

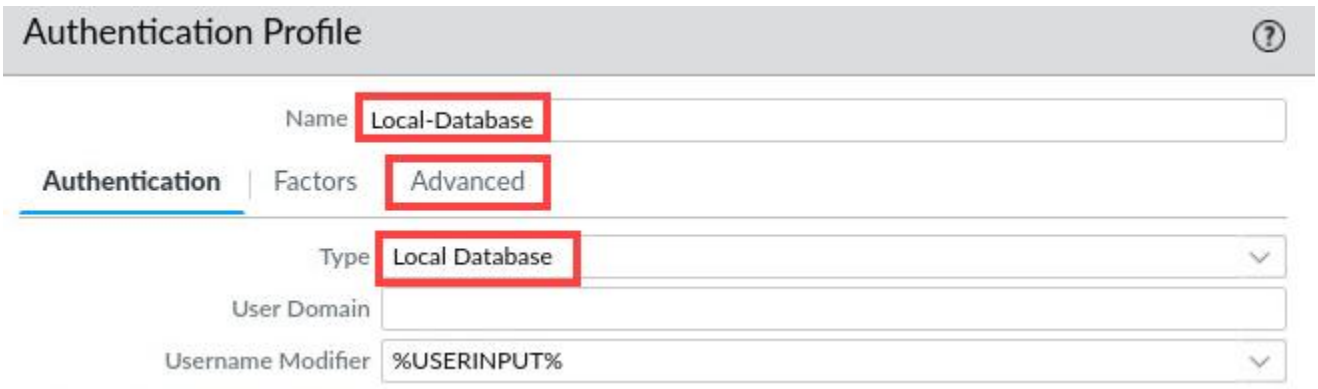
## 3.2 Create a Local Database Authentication Profile

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.

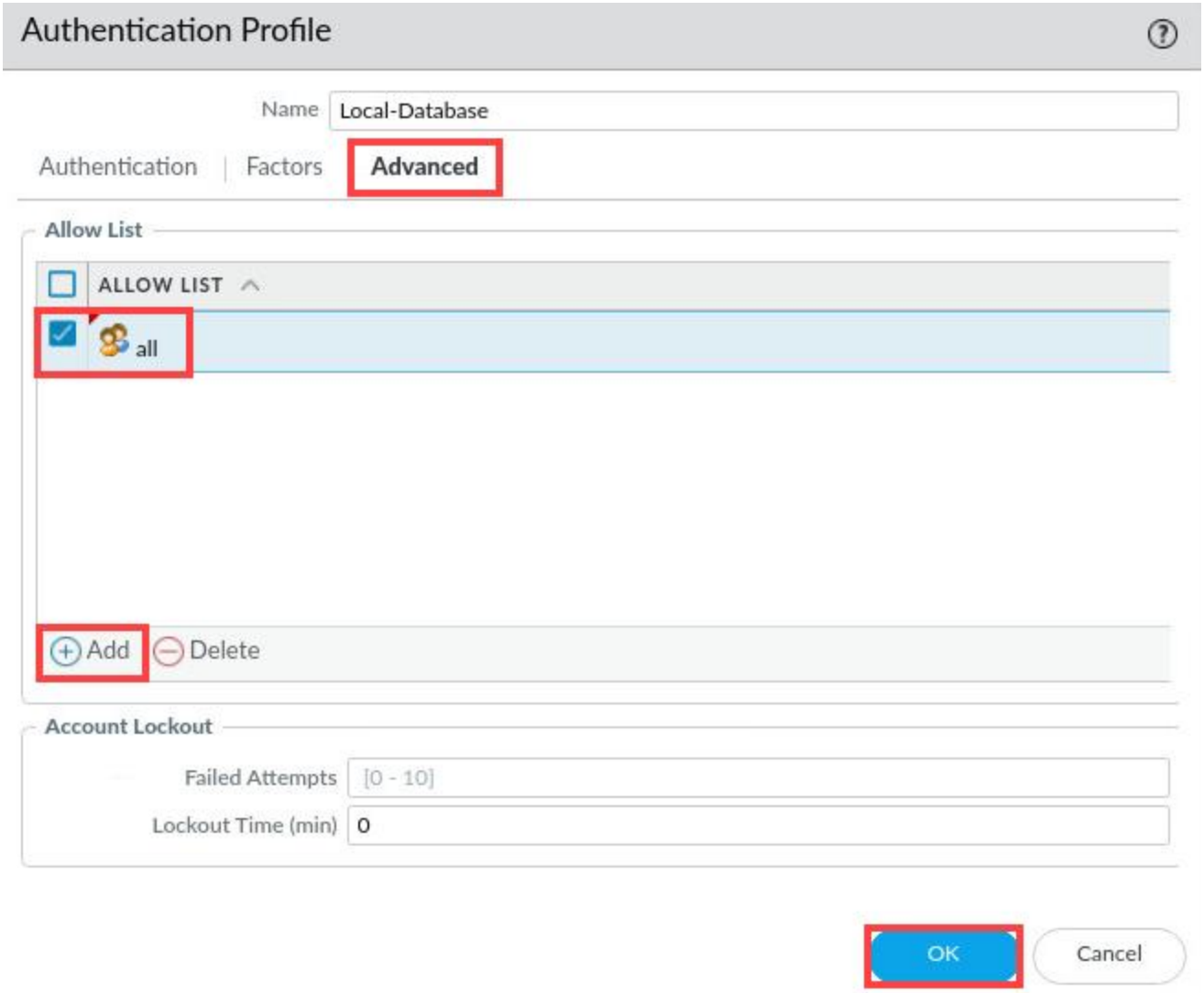
1. In the *PA-VM* web interface, navigate to **Device > Authentication Profile**. Click **Add** at the bottom of the window.




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.**



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

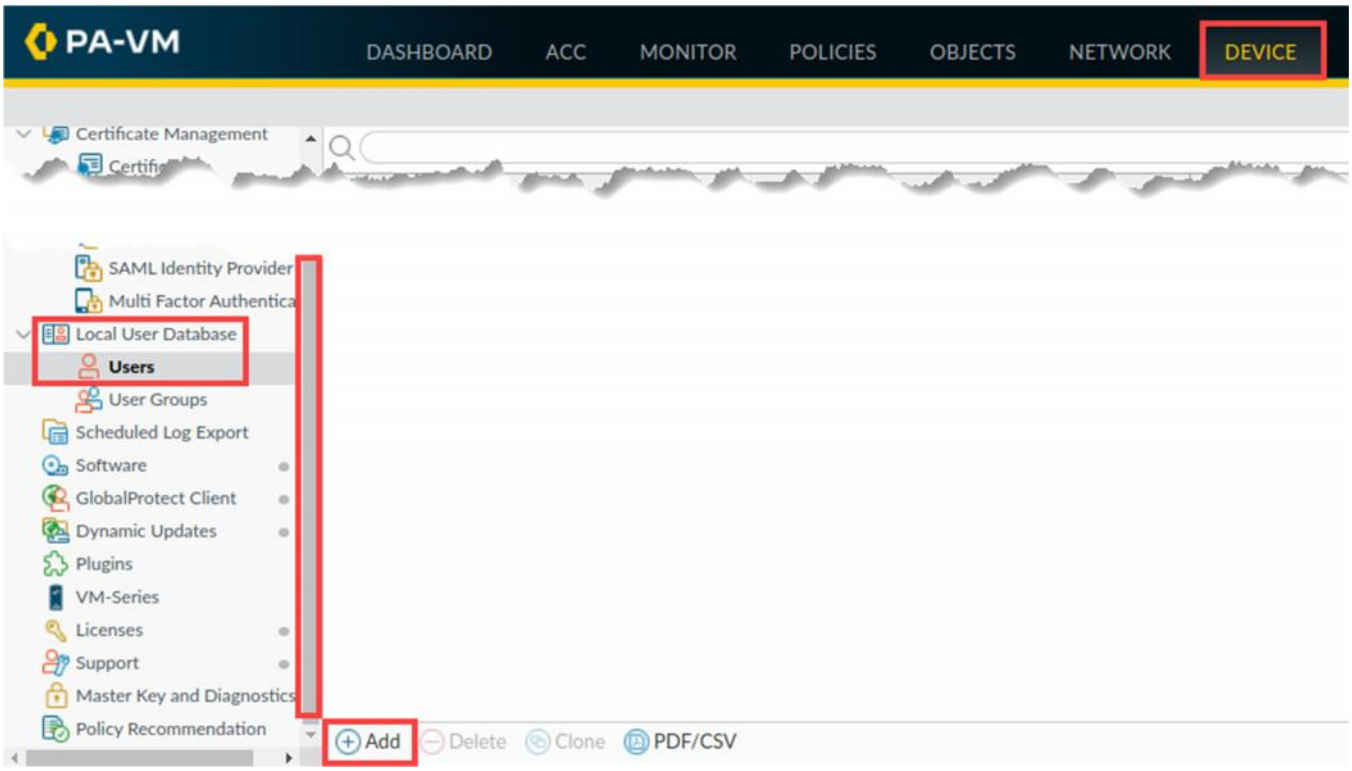



4. Leave the firewall web interface open to continue with the next task.

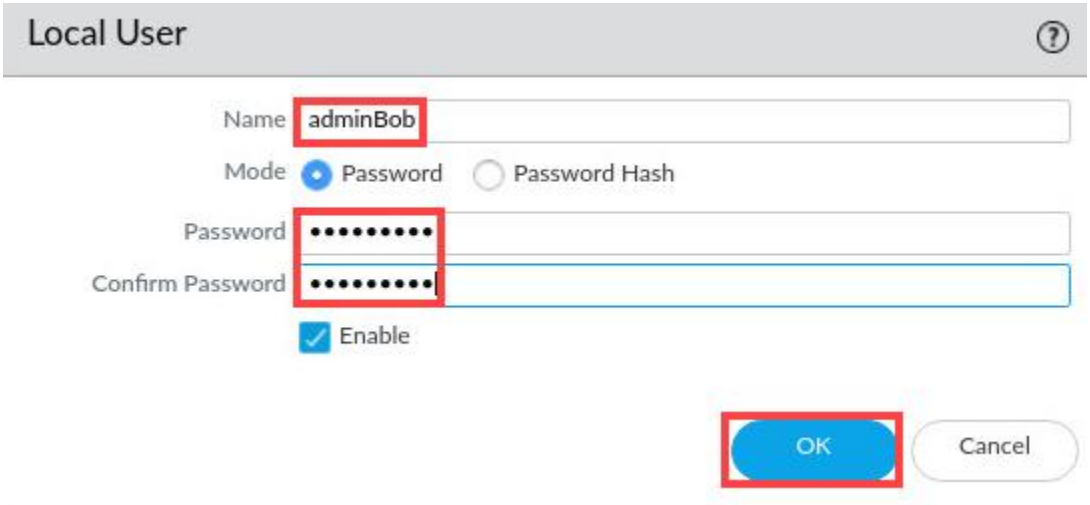
## 3.3 Create a Local User Database Account

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 **`Pal0Alt0!`** for *Password* and *Confirm Password*. Click **OK**.

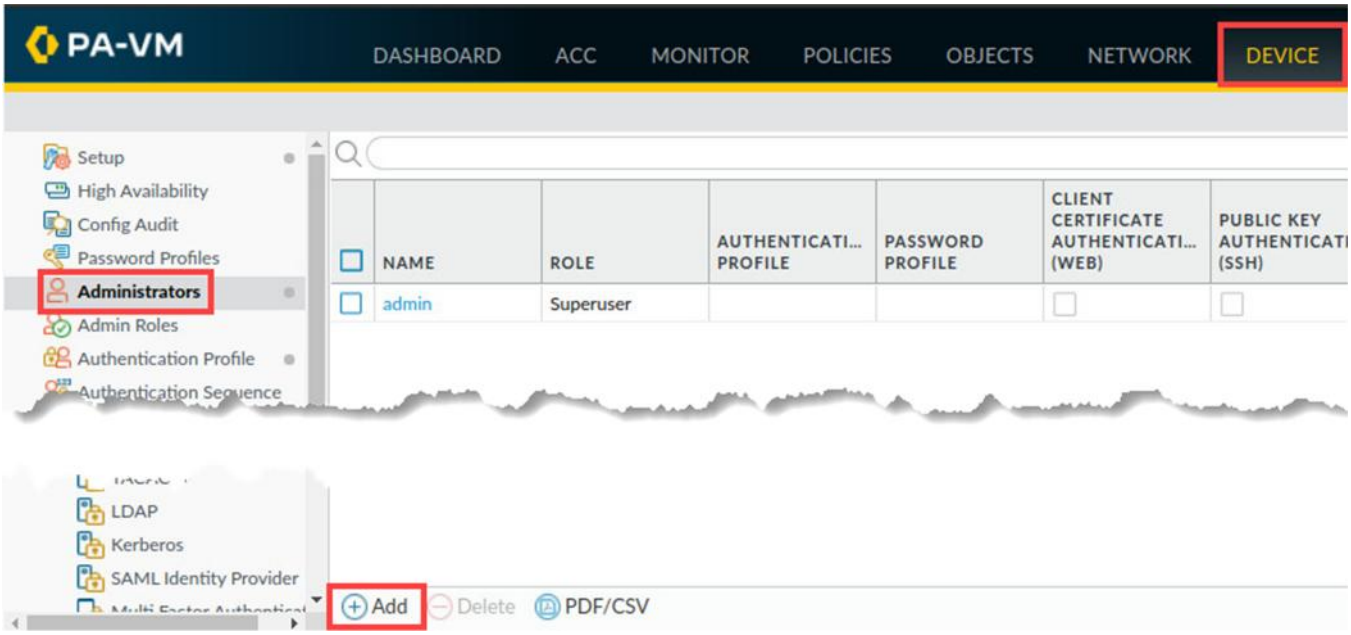



3. Leave the firewall web interface open to continue with the next task.

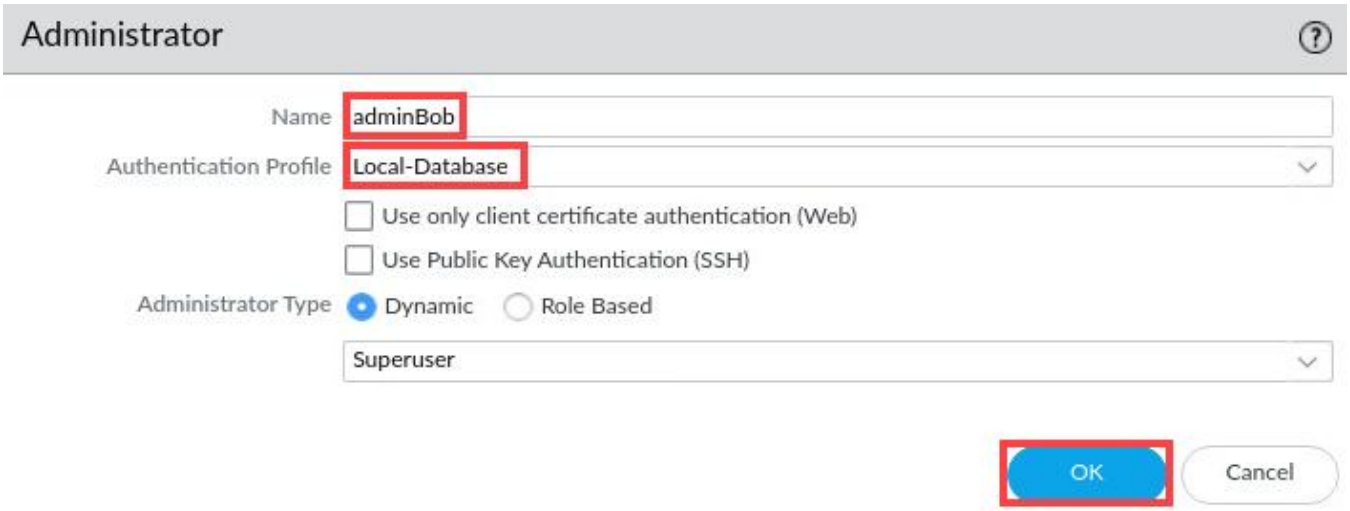
## 3.4 Create an Administrator Account

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**.

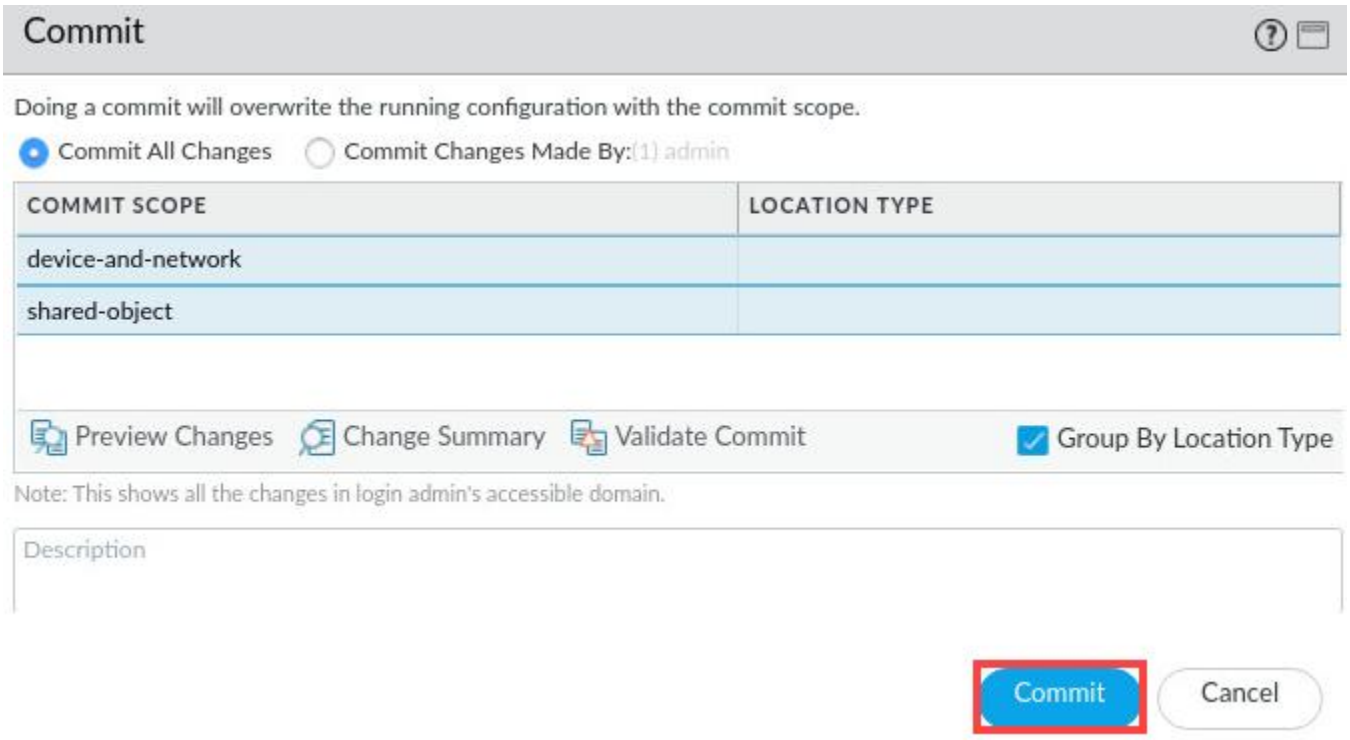



Please Note

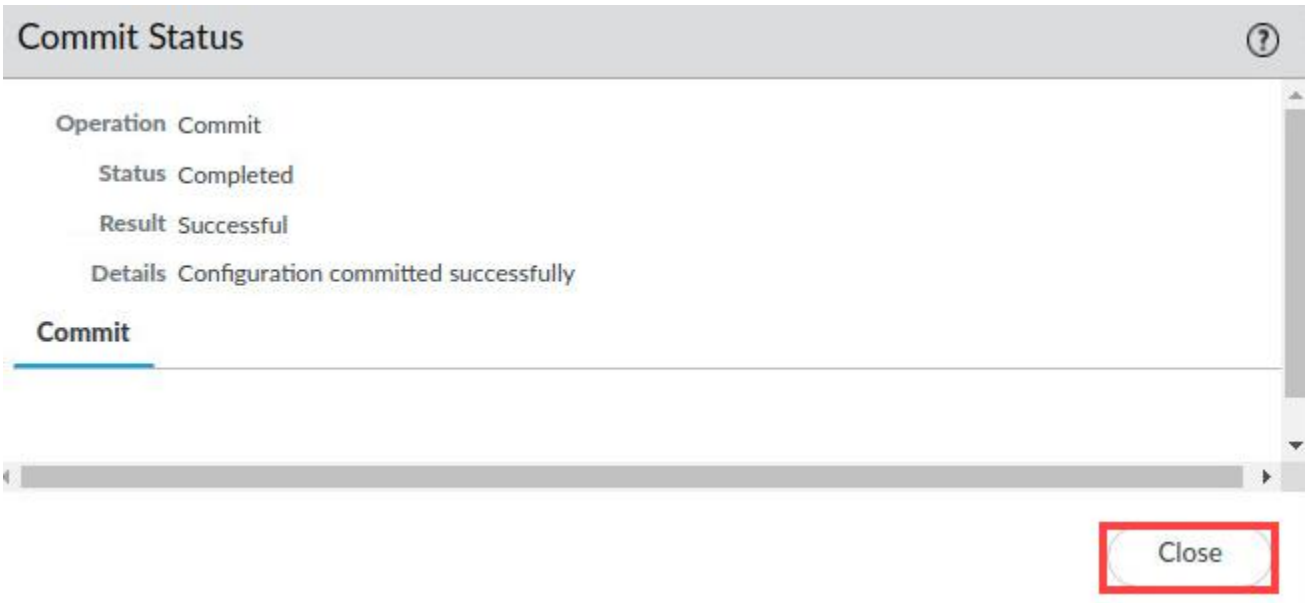
Note that when you select Local-database for the Authentication Profile, there is no option to enter a Password for the administrator. The password information for this account is maintained in the Local-database on the firewall.

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

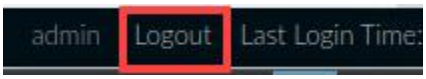

4. In the *Commit* window, click **Commit** to proceed with committing the changes.




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



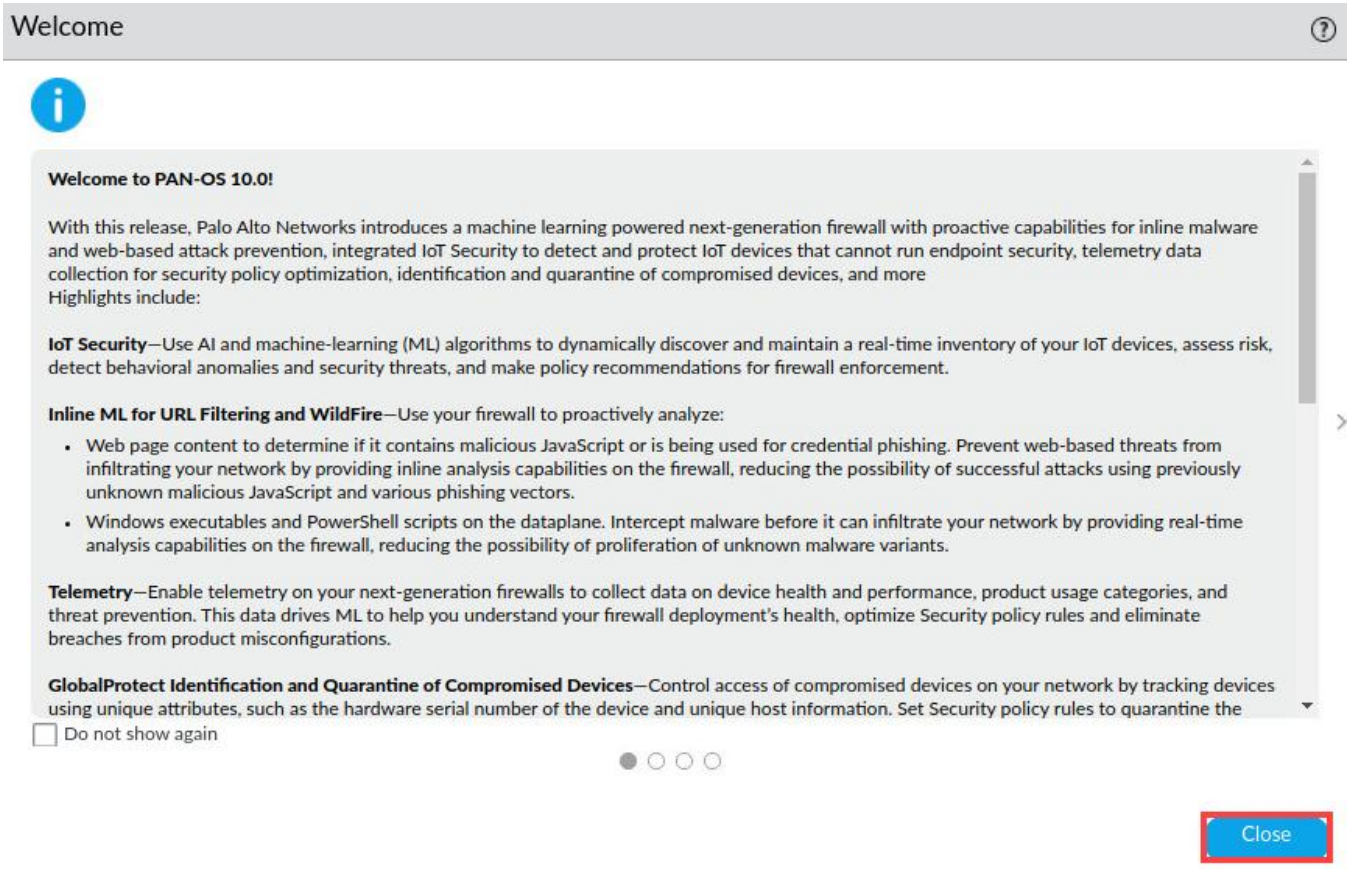
6. Log out of the firewall web interface by clicking the **Logout** button in the bottom-left corner of the window.



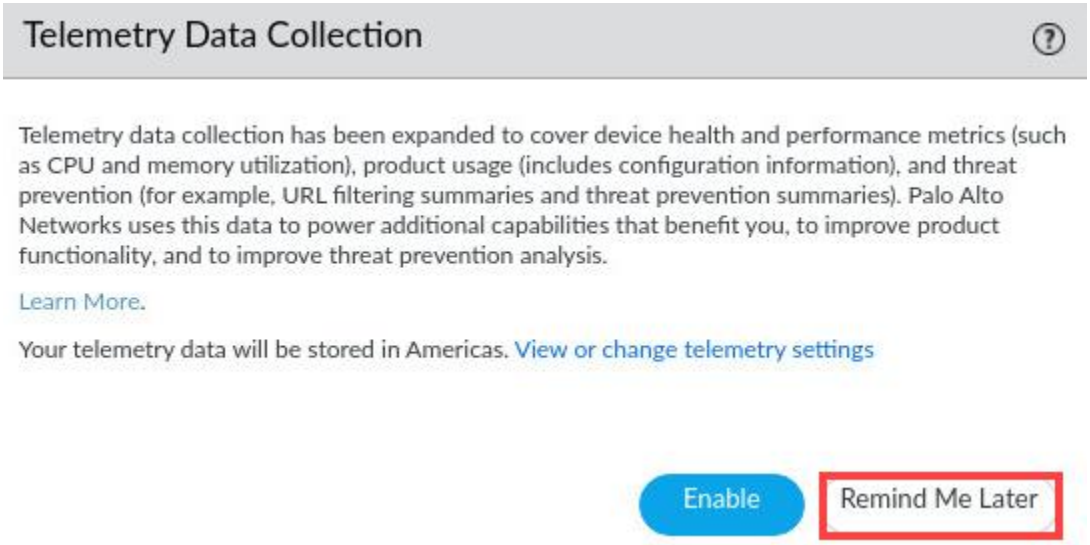

7. In the *Log In* window, click **Log In**.


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

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

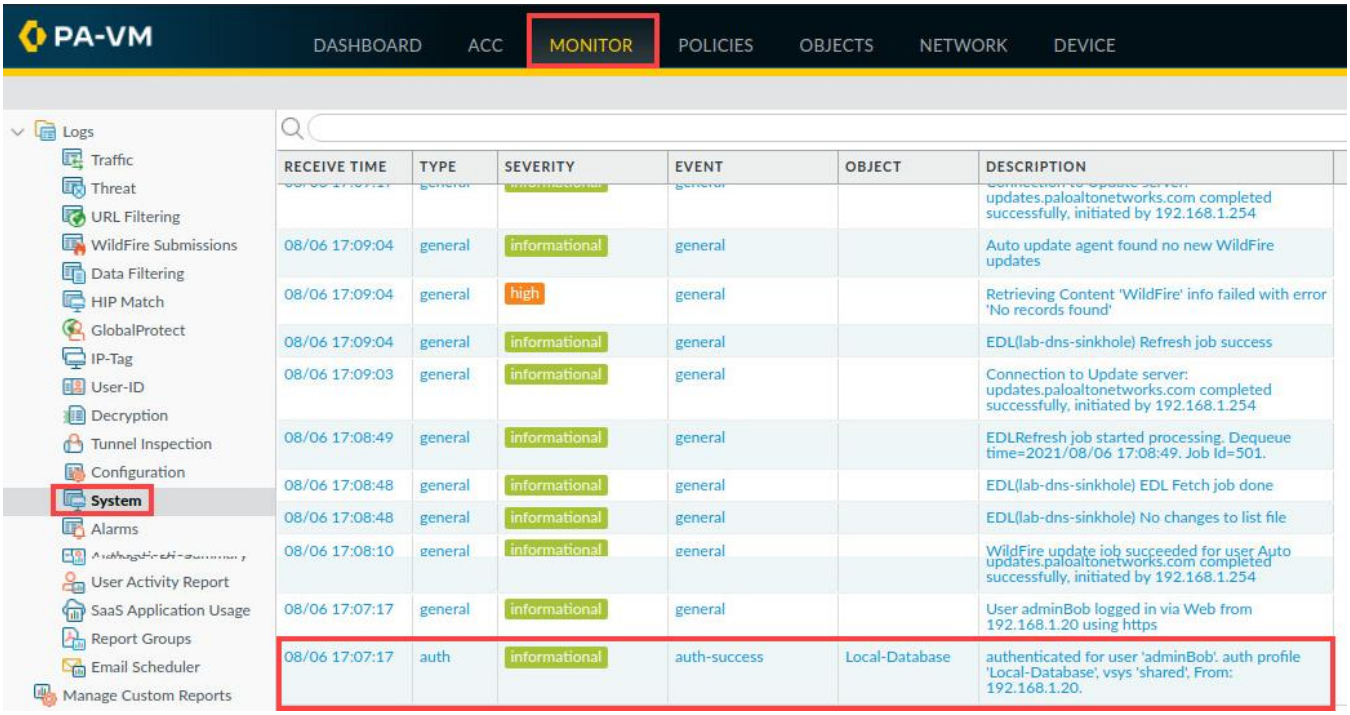



10. In the *Telemetry Data Collection* window, click **Remind Me Later**.



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

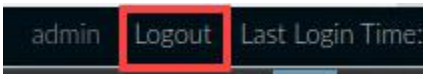



Please Note

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.

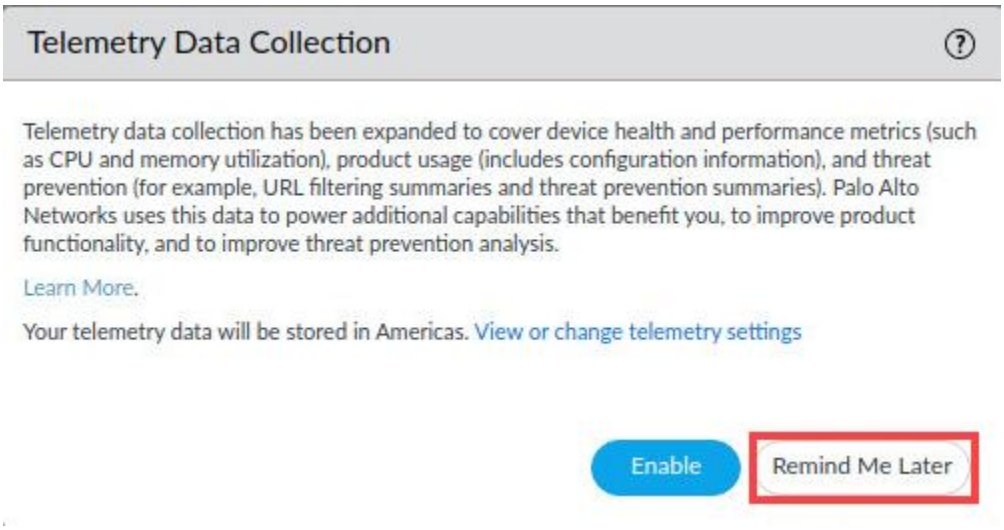


13. In the *Log In* window, click **Log In**.


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

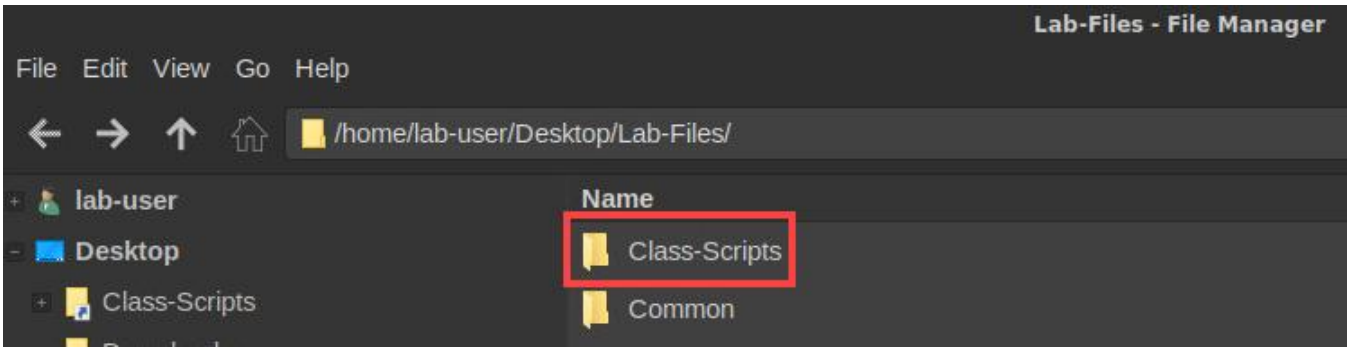
Your organization uses an LDAP server to maintain a database of users, including network administrators. Your team of security personnel is growing each month, and you want to leverage the existing LDAP server to authenticate administrators when they attempt to log into the firewall.

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.

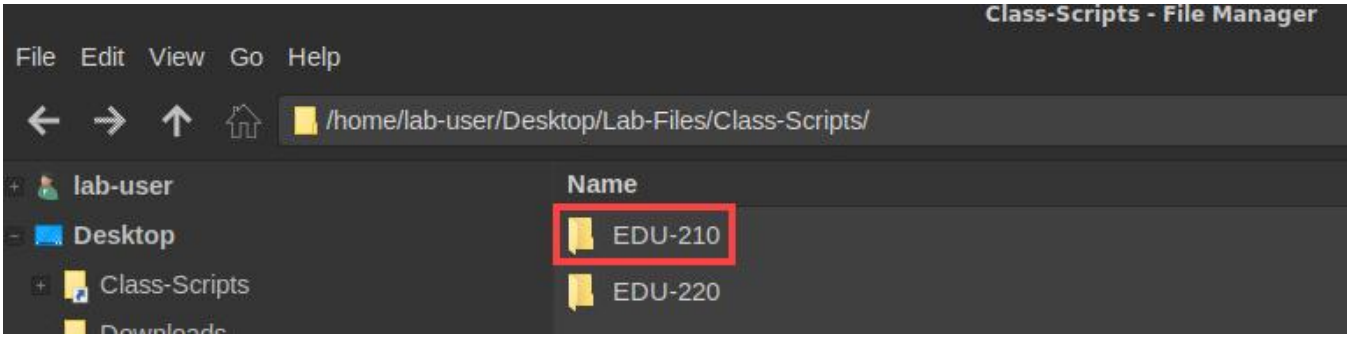
1. Minimize the PA-VM web interface.

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

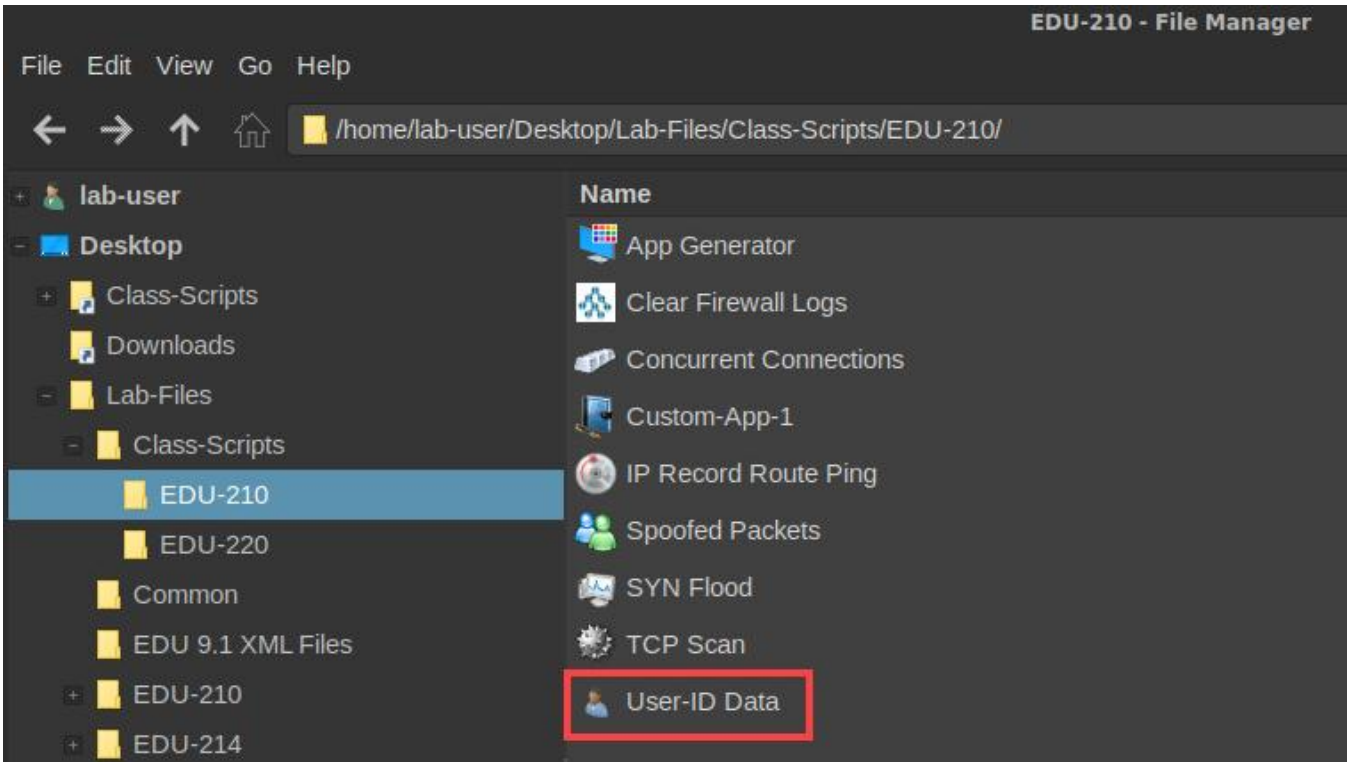

3. In the *Lab-Files* folder, open the **Class-Scripts**.



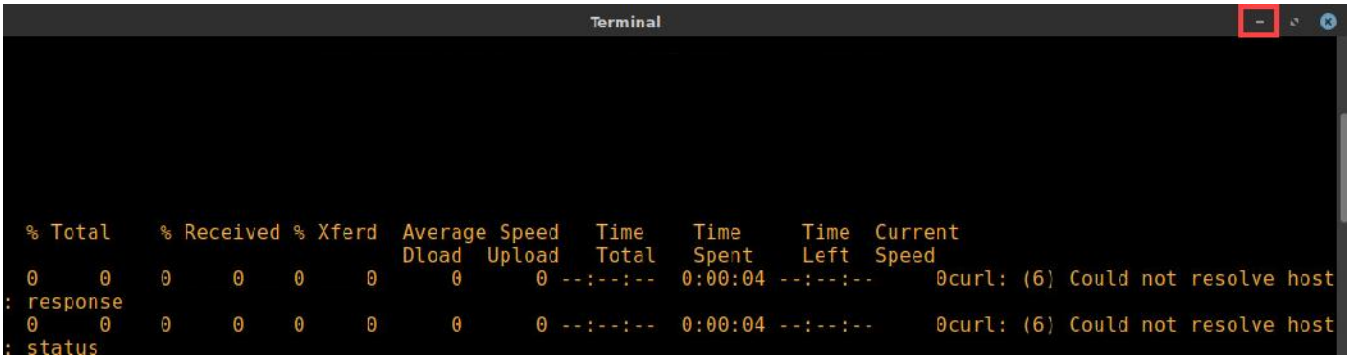

4. In the *Class-Scripts* folder, open the **EDU-210** folder.



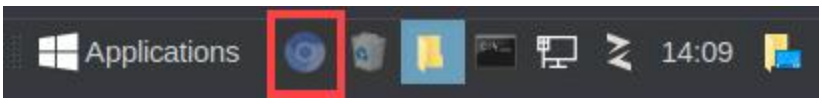
5. Execute the *User-ID Data* script by **double-clicking** it.



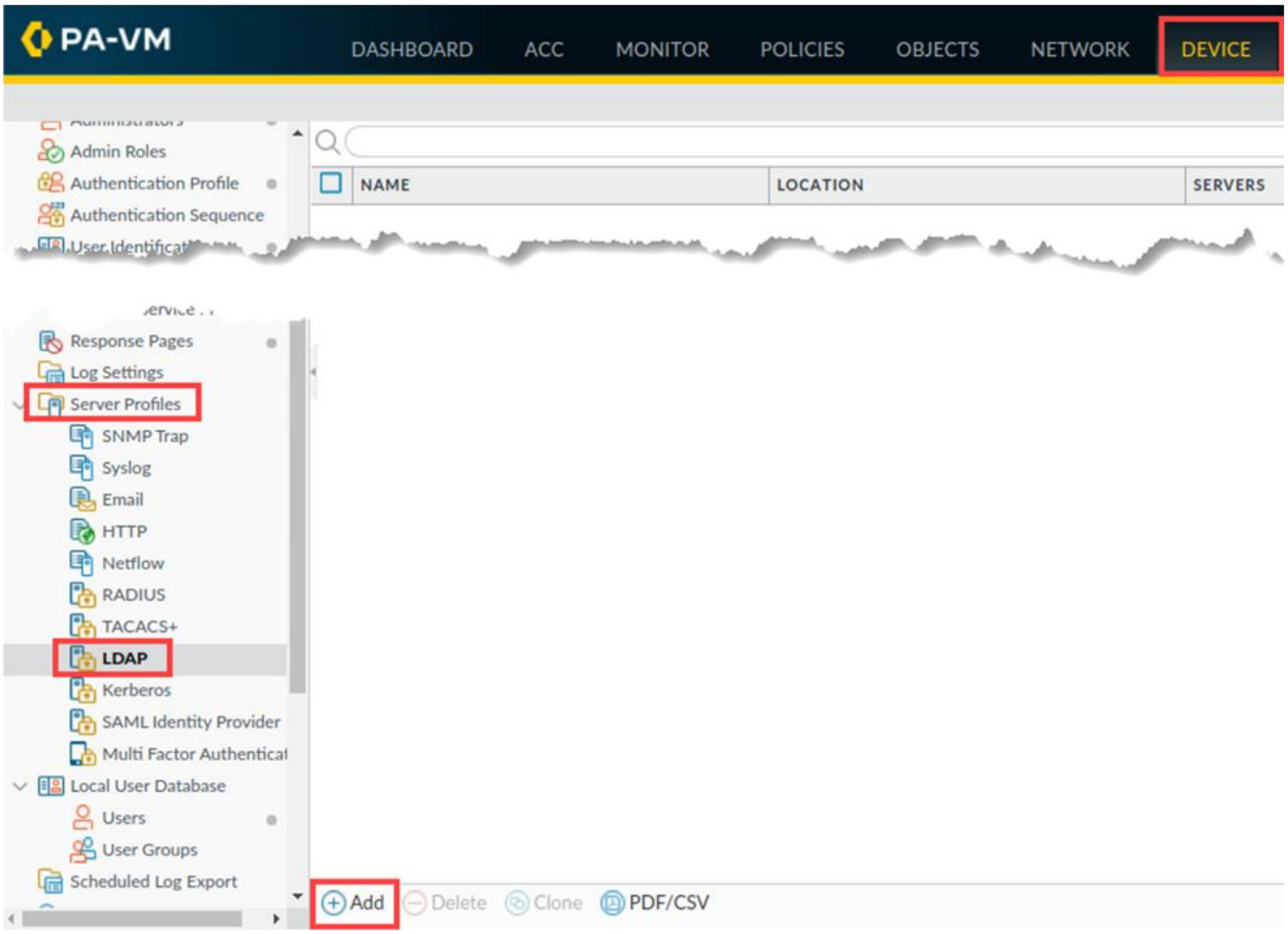

6. Notice the *Terminal* window will pop up. **Minimize** the terminal window and let it run for the remainder of the lab.



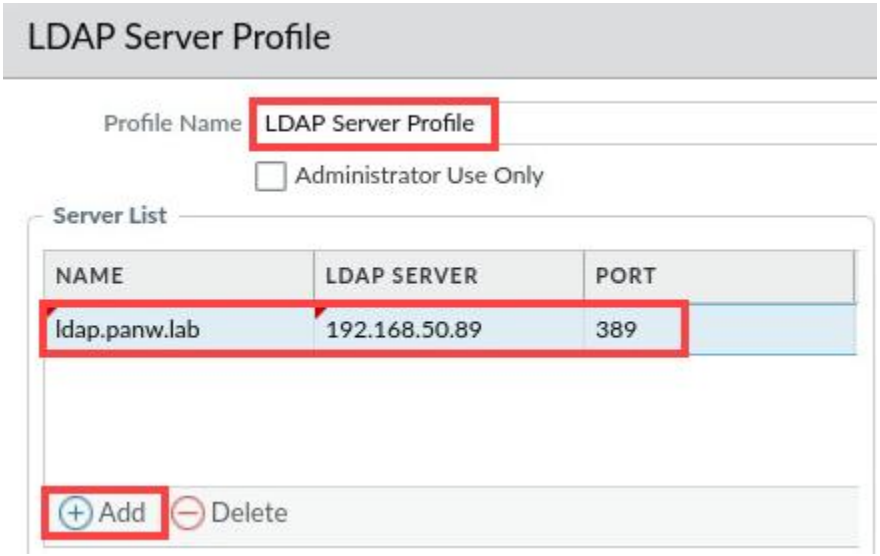

7. Reopen the *PA-VM firewall* by clicking on the **Chromium** icon in the taskbar.



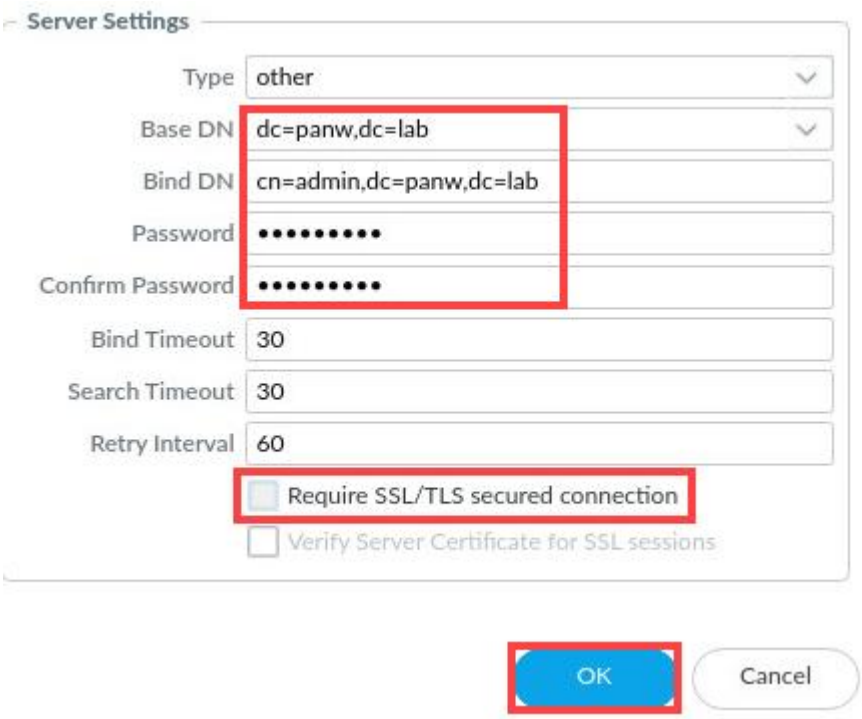
8. In the web interface, select **Device > Server Profiles > LDAP**. At the bottom of the window, click **Add**.




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.



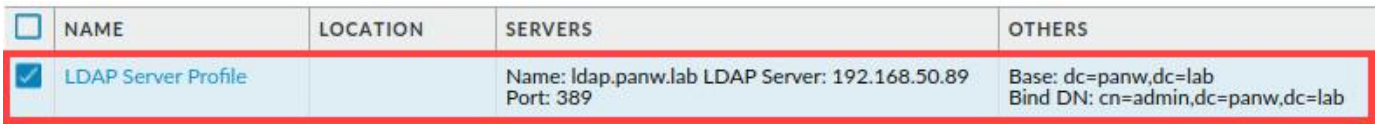
10. In the *Server Settings* section, Enter **dc=panw,dc=lab** for *Base DN*, enter **cn=admin,dc=panw,dc=lab** for *Bind DN*, enter **Pal0Alt0!** for *Password* and *Confirm Password* and uncheck **Require SSL/TLS secured connection**. Click **OK**.




Please Note

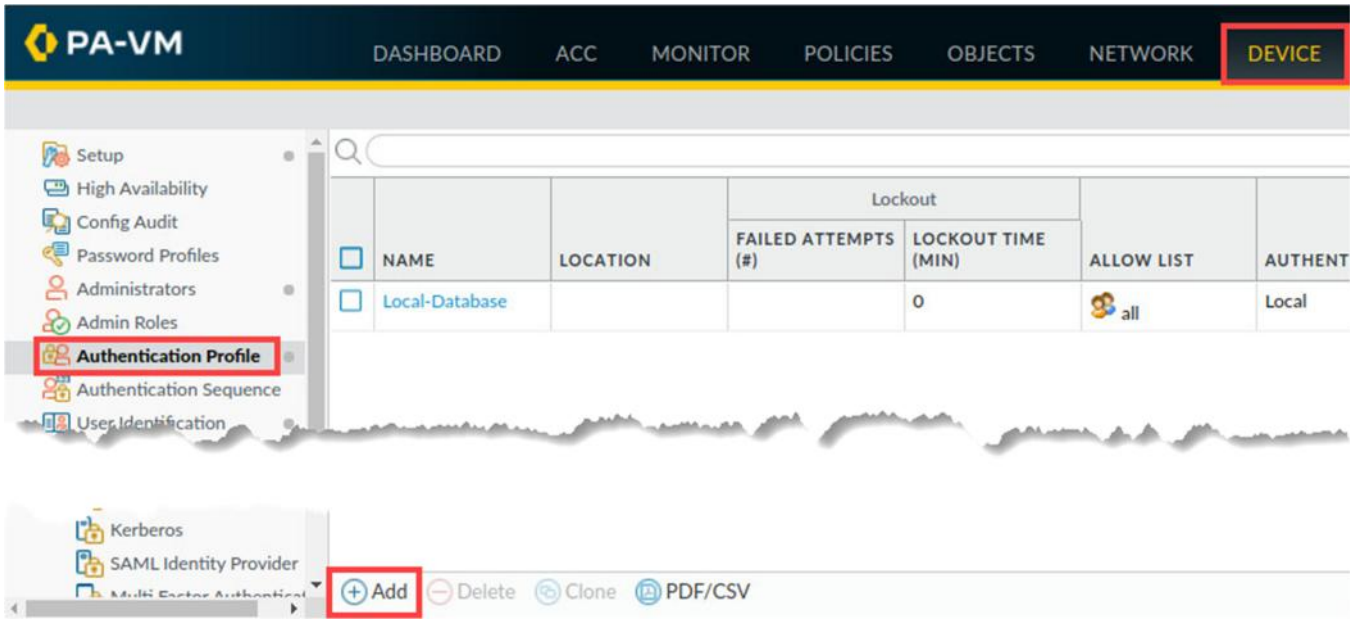
With your LDAP Server Profile in place, you will now create an Authentication Profile and reference the LDAP Server Profile you just created.

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

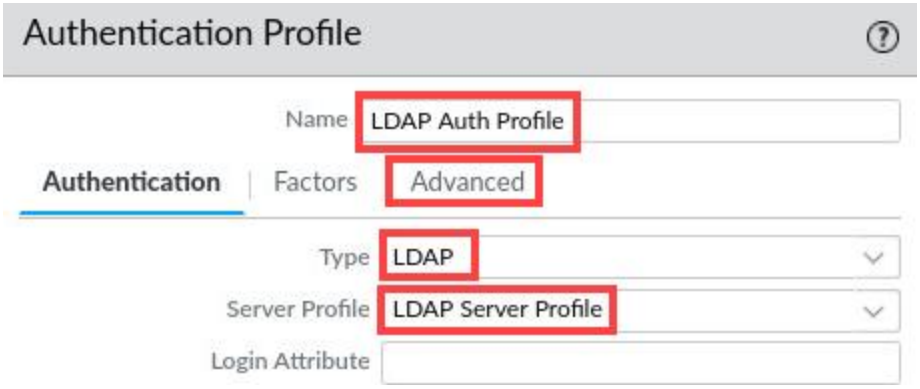


| NAME | LOCATION | SERVERS | OTHERS |
|---|---|---|---|
| LDAP Server Profile | | Name: ldap.panw.lab LDAP Server: 192.168.50.89 Port: 389 | Base: dc=panw,dc=lab Bind DN: cn=admin,dc=panw,dc=lab |

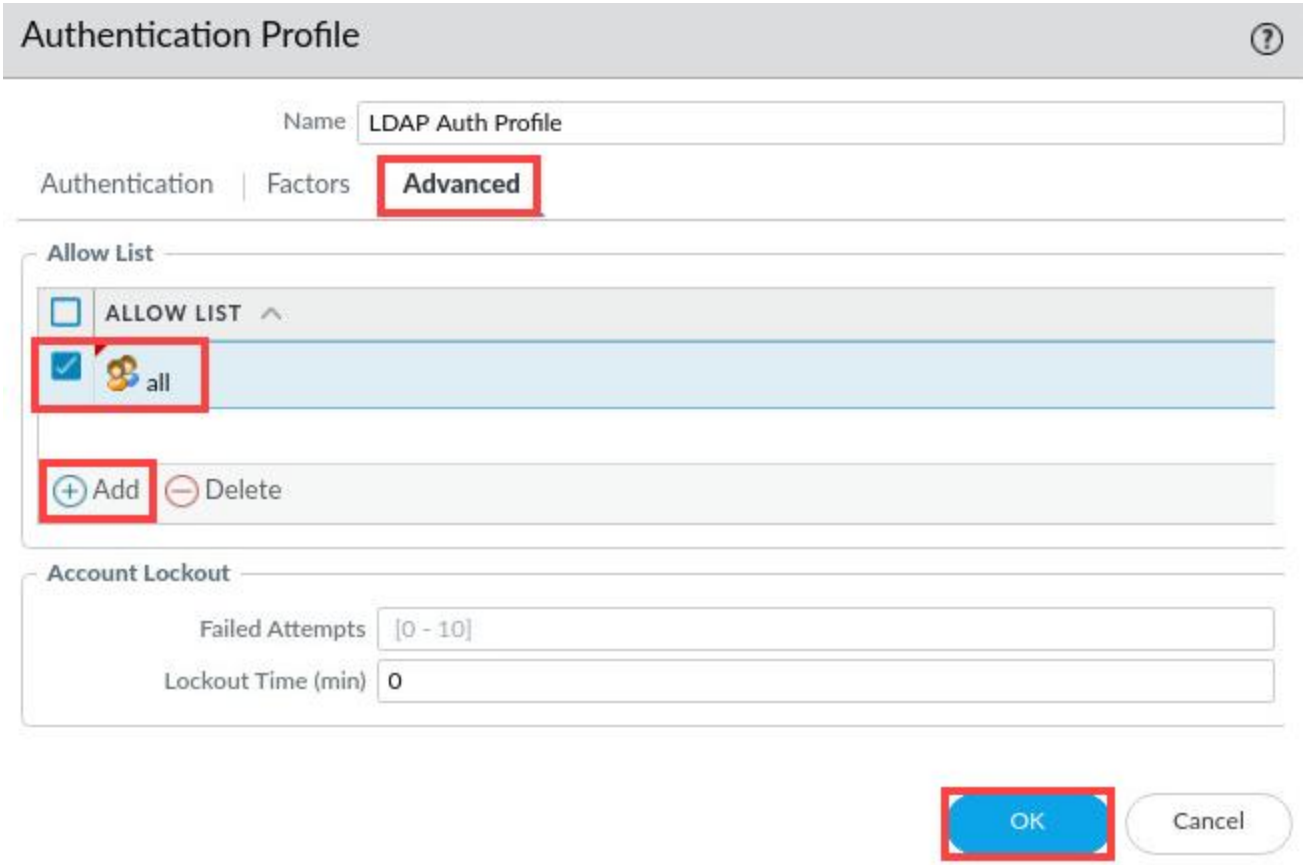
12. Select **Device > Authentication Profile**. Click **Add**.



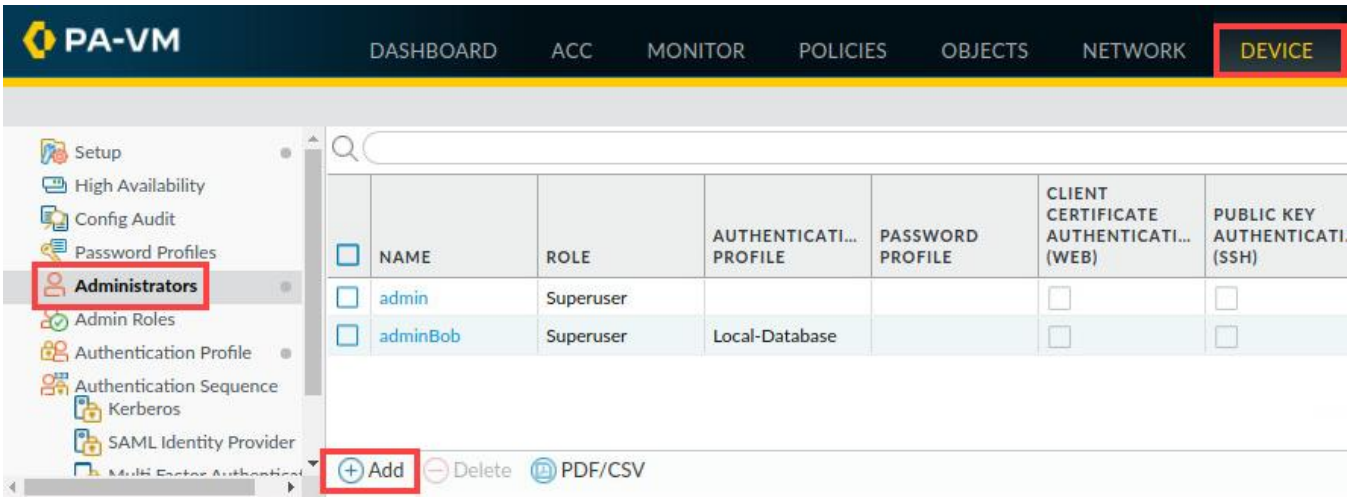

13. In the *Authentication Profile* window, type **`LDAP Auth Profile`** for the *Name*. Select **LDAP** for the *Type* and **LDAP Server Profile** for the *Server Profile*. Click **Advanced**.



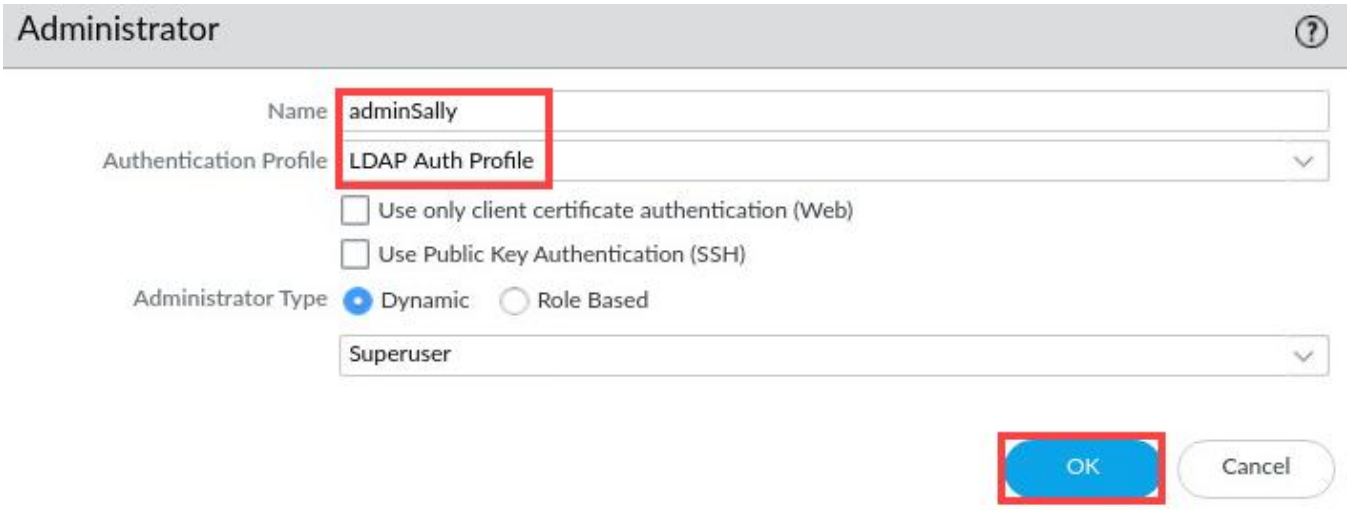
14. On the *Advanced* tab, in the *Allow List,* click **Add**. Select **all** and click **OK**.




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



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

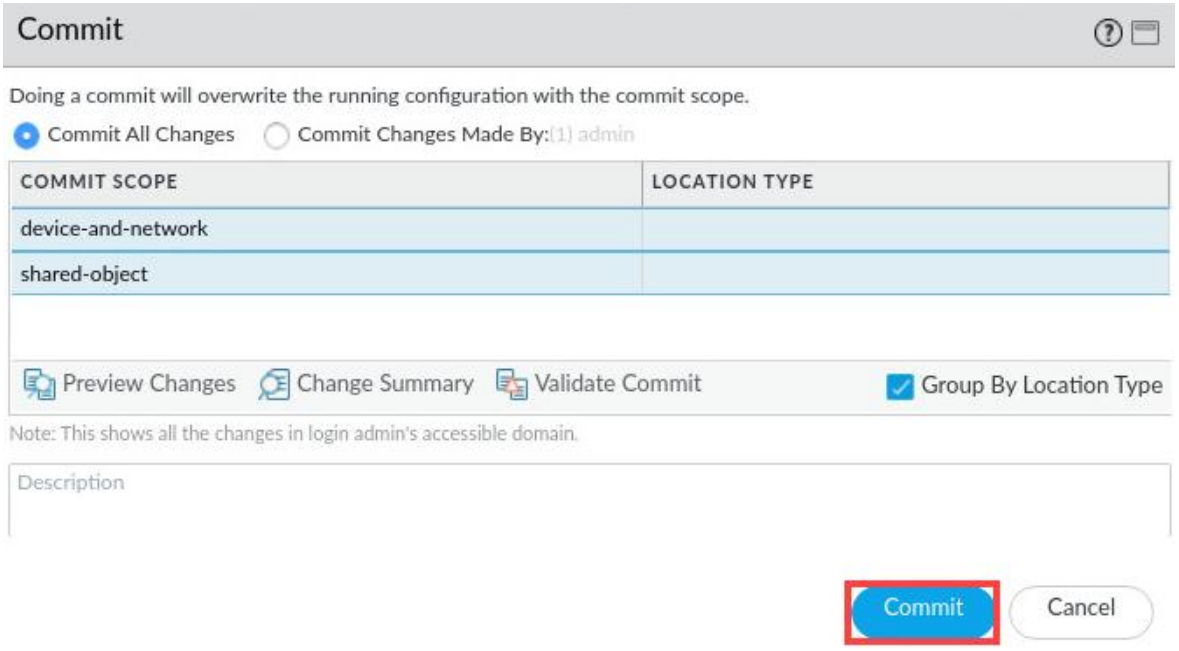



Please Note

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

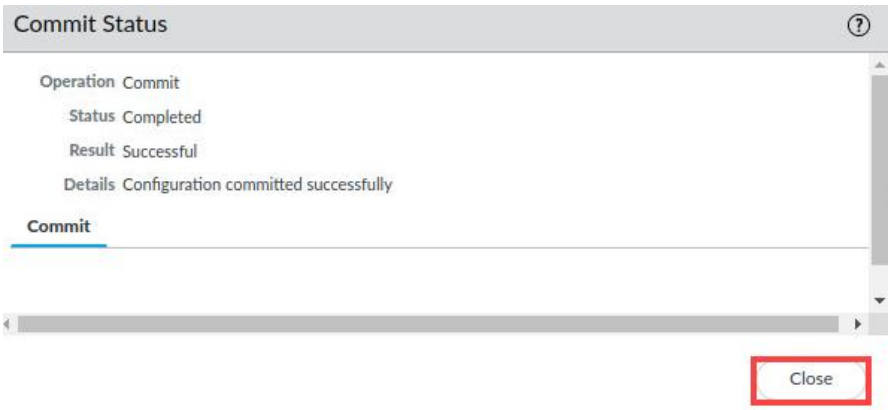
17. Click the **Commit** link located at the top-right of the web interface.


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



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

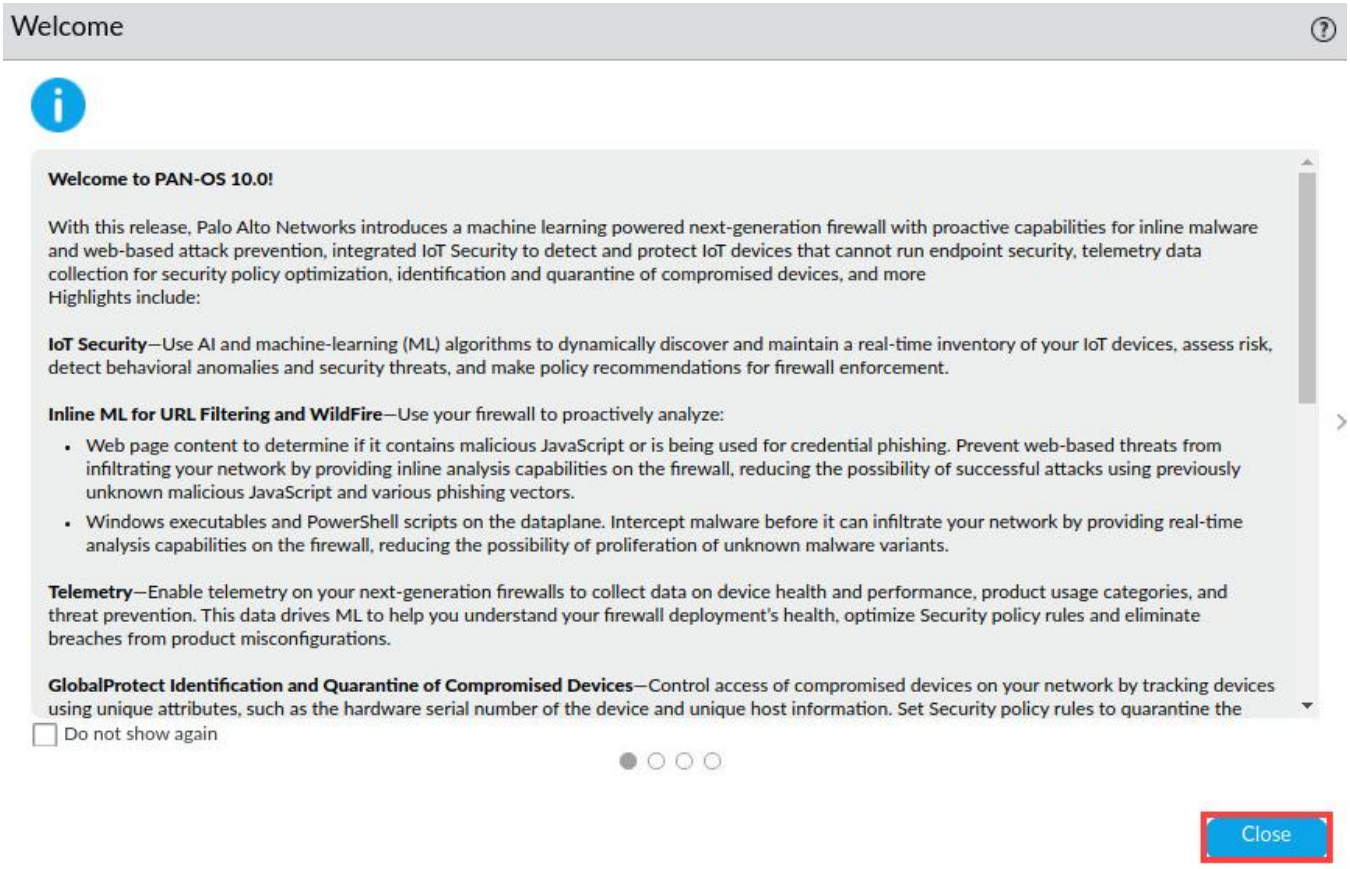



20. Log out of the firewall web interface by clicking the **Logout** button in the bottom-left corner of the window.

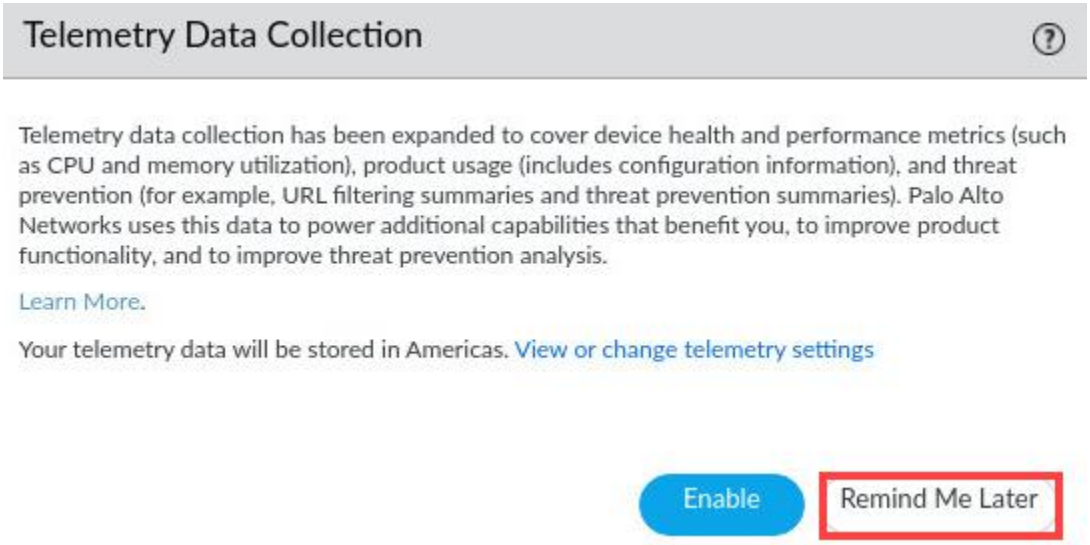

21. In the *Log In* window, click **Log In**.


22. Log back into the firewall as username **`adminSally`**, password **`Pal0Alt0!`**. Click **Log In**.

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

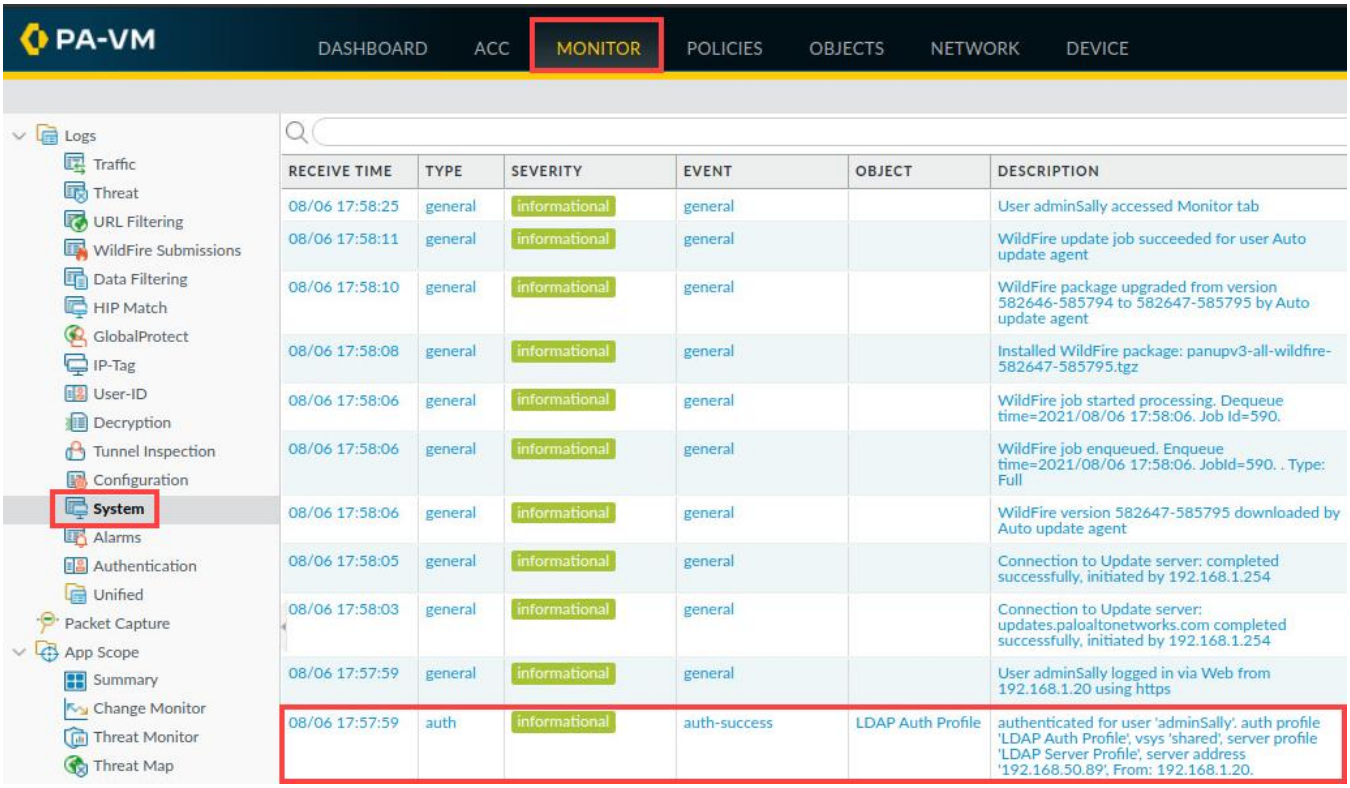



24. In the *Telemetry Data Collection* window, click **Remind Me Later**.



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

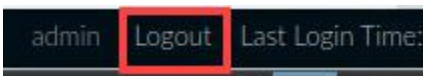



Please Note

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.

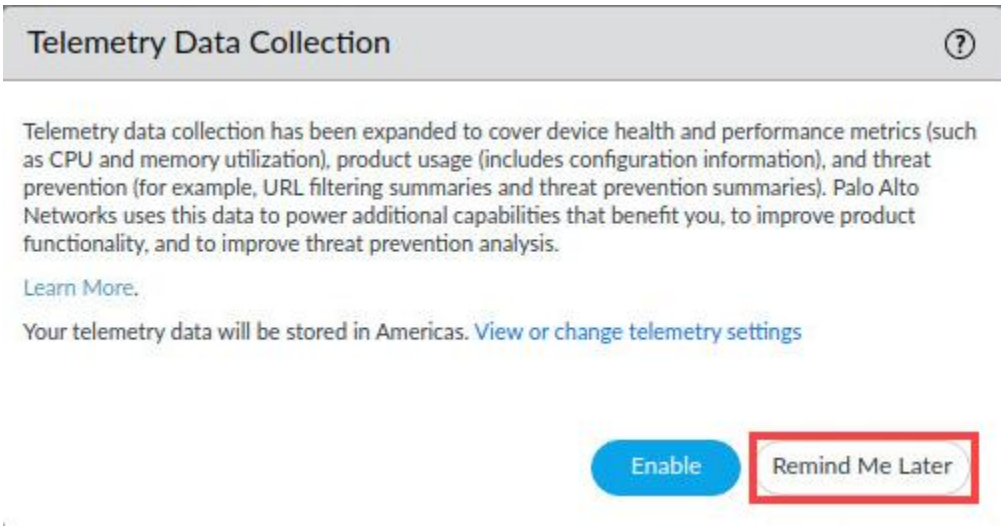


27. In the *Log In* window, click **Log In**.


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


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



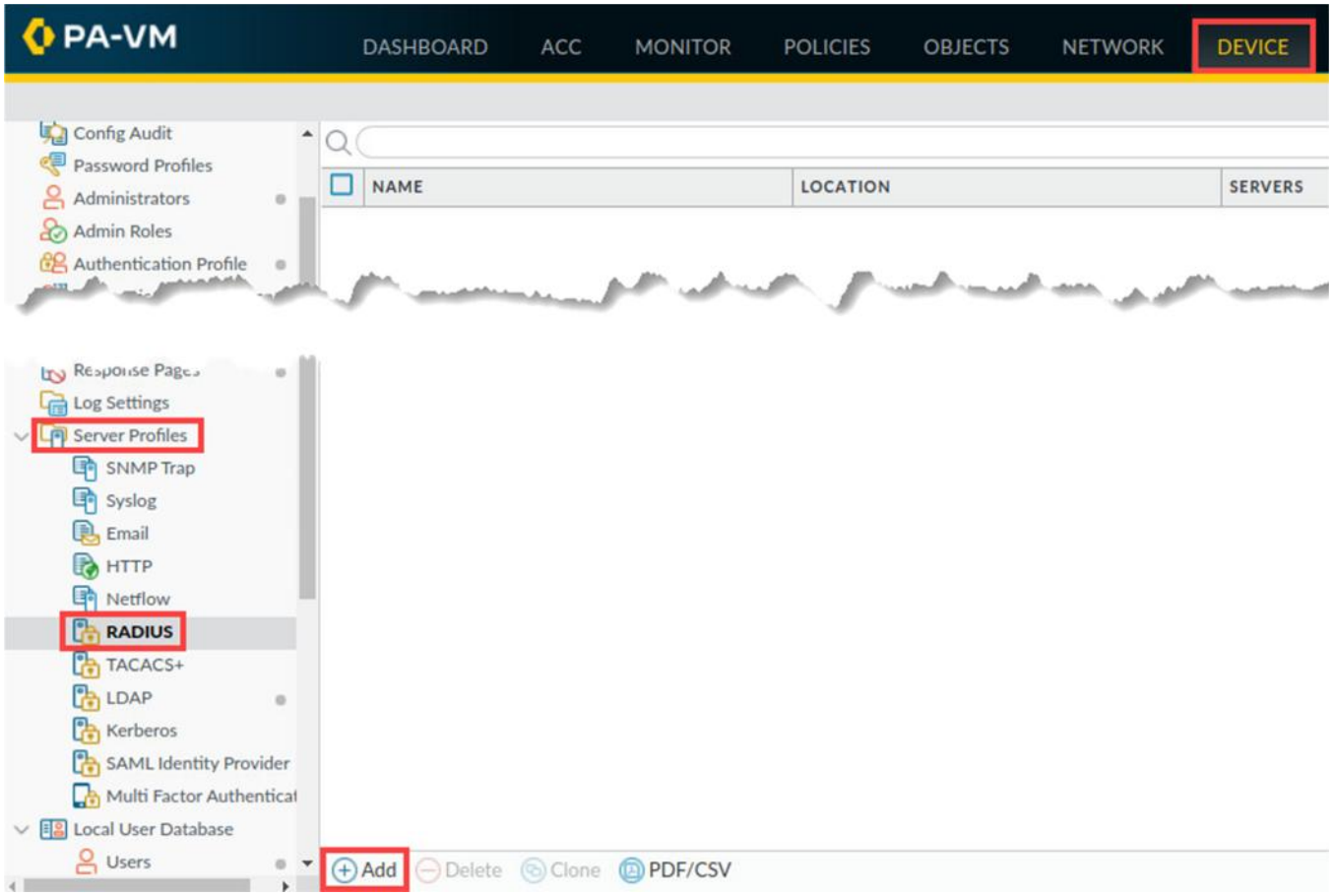

30. Leave the firewall web interface open to continue with the next task.

## 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.

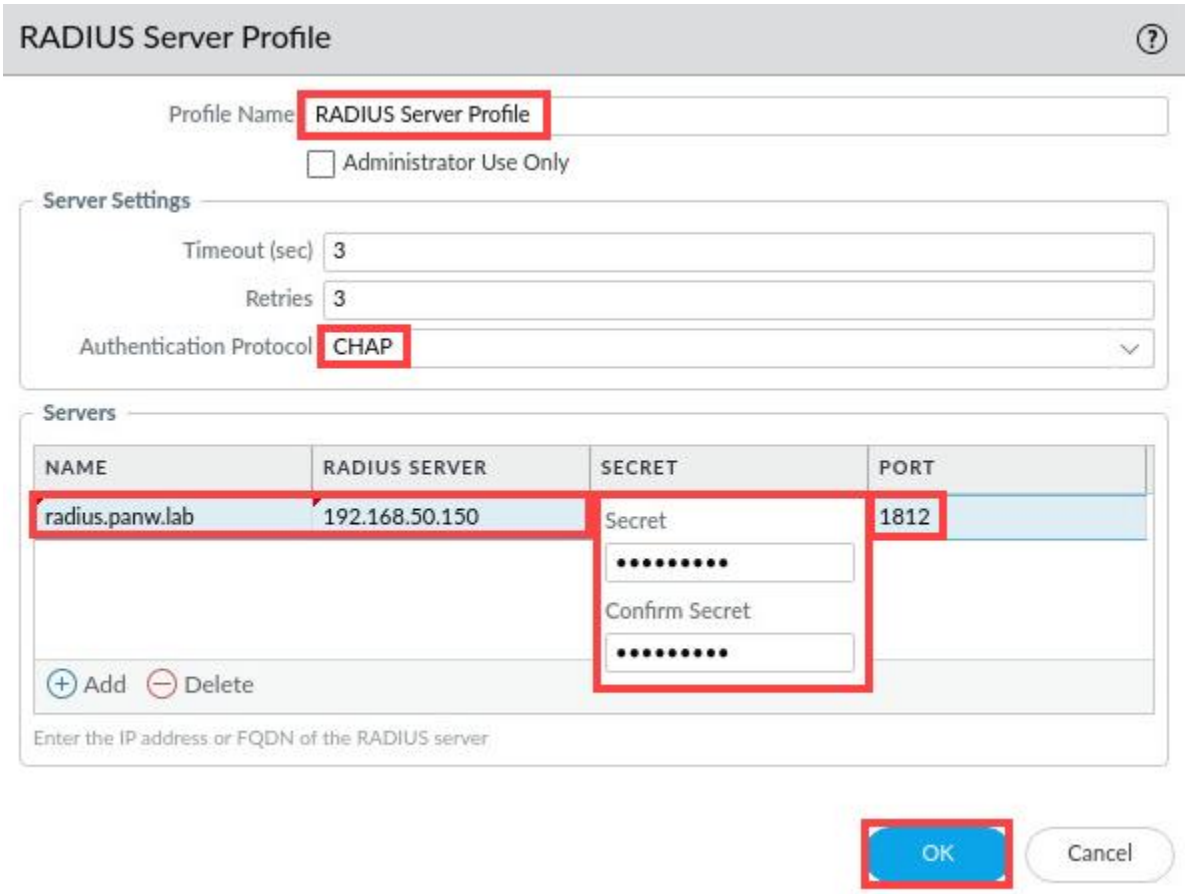
For this section, you will configure RADIUS Authentication and test that the user adminHelga can log in.

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



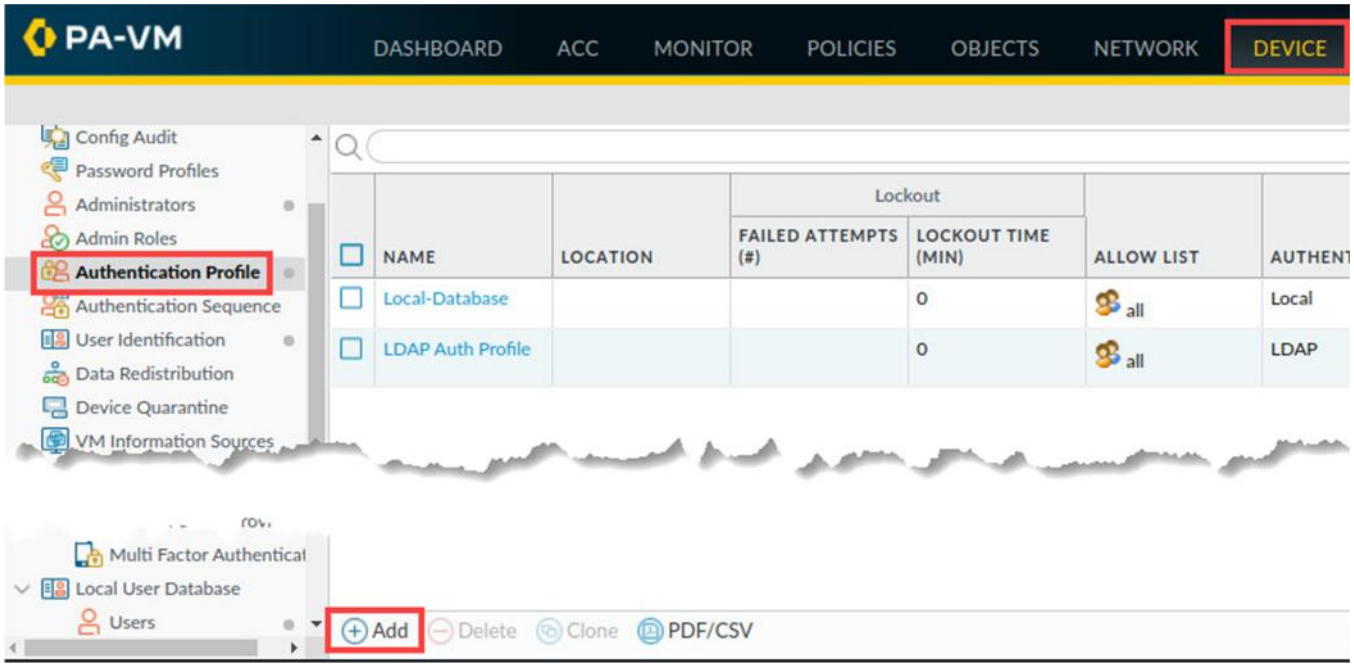

  

2. In the *RADIUS Server Profile* window, enter **`RADIUS Server Profile`** for the *Profile Name*. For the *Authentication Protocol*, select **CHAP**. Under the *Servers* section, click **Add.** For the server *Name* field, enter **`radius.panw.lab`.** For the *RADIUS Server* field, enter **`192.168.50.150`.** Enter **`Pal0Alt0!`** for *Secret* and *Confirm Secret***.** Leave the *Port* set to **1812.** Click **OK.**

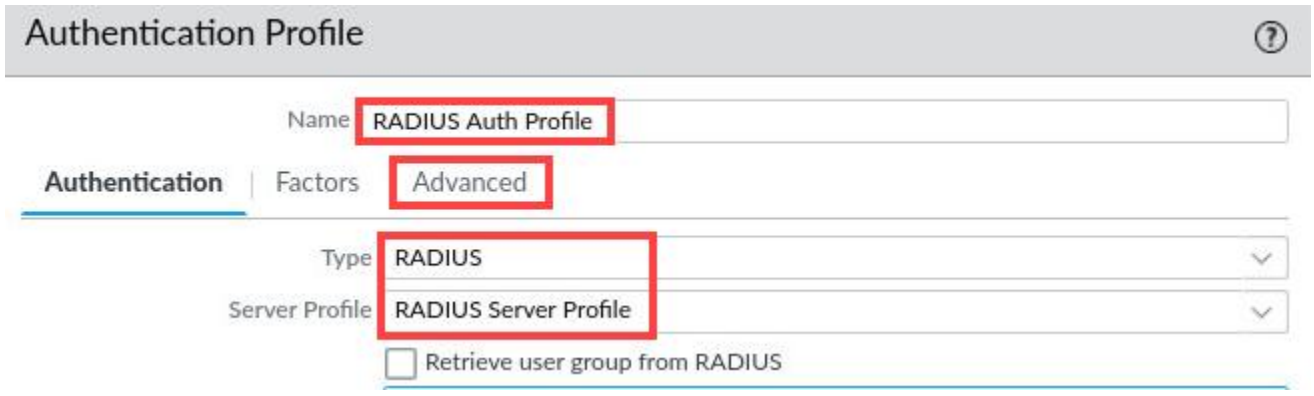


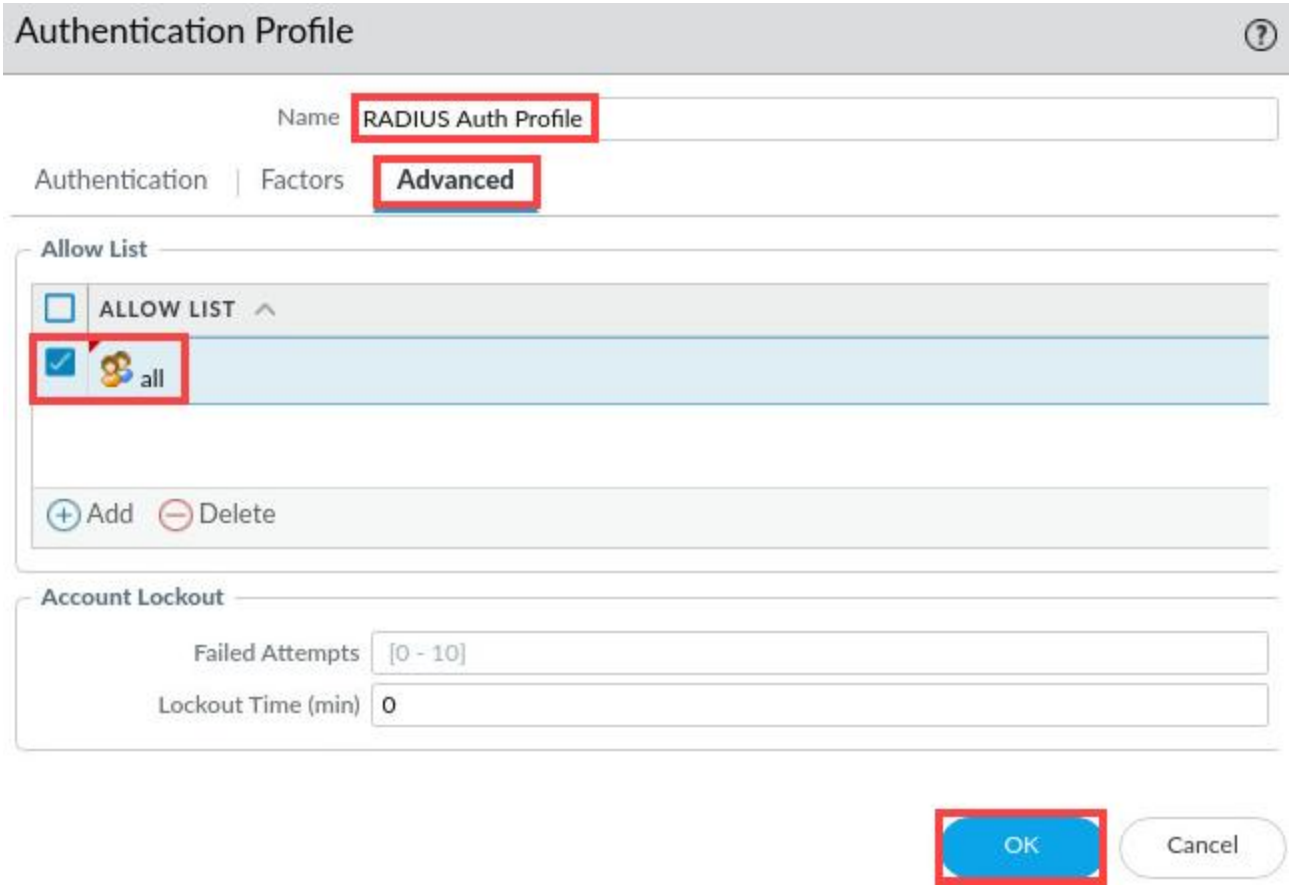
3. Navigate to **Device > Authentication** Profile. Click **Add**.



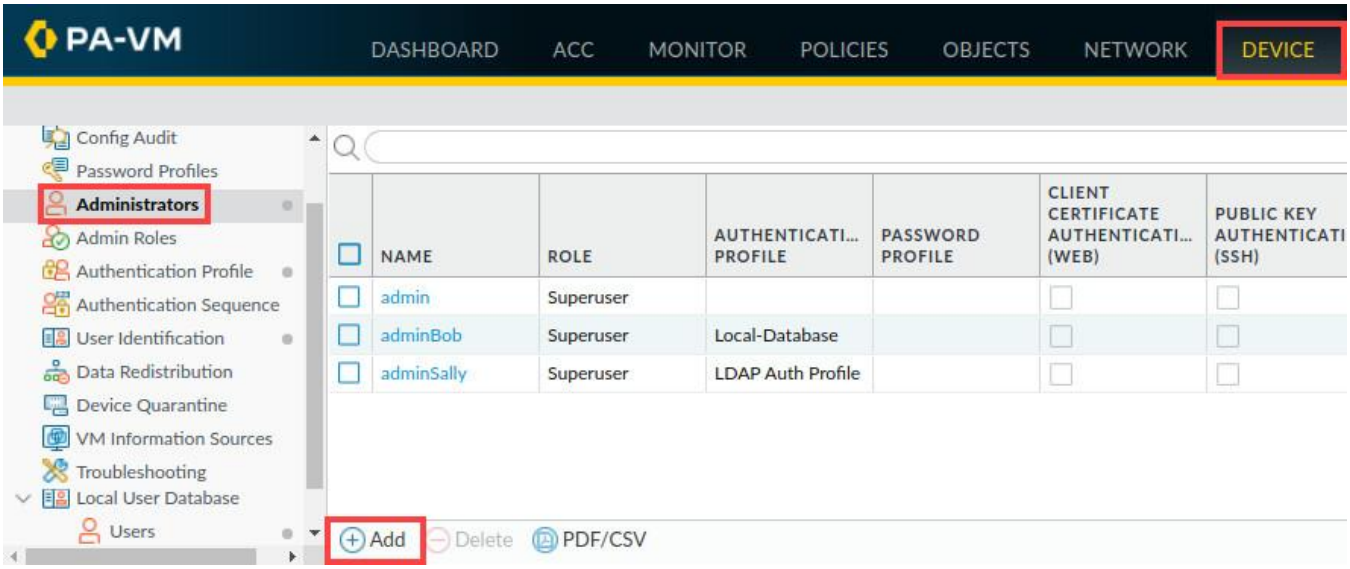

4. In the *Authentication Profile* window, enter **`RADIUS Auth Profile`** for the *Profile Name*. For the *Type*, select **RADIUS**. For the *Server Profile*, select **RADIUS Server Profile**. Click the **Advanced** tab.



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

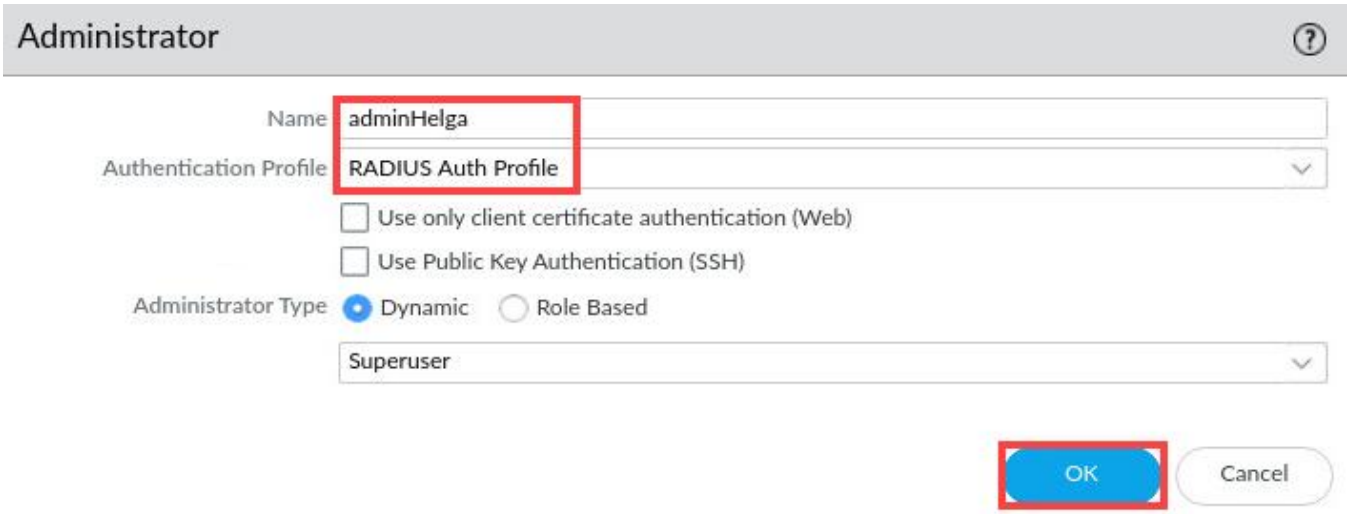



6. To test *RADIUS Authentication*, create an *administrator* account named **adminHelga** by selecting **Device > Administrators**. Click **Add**.



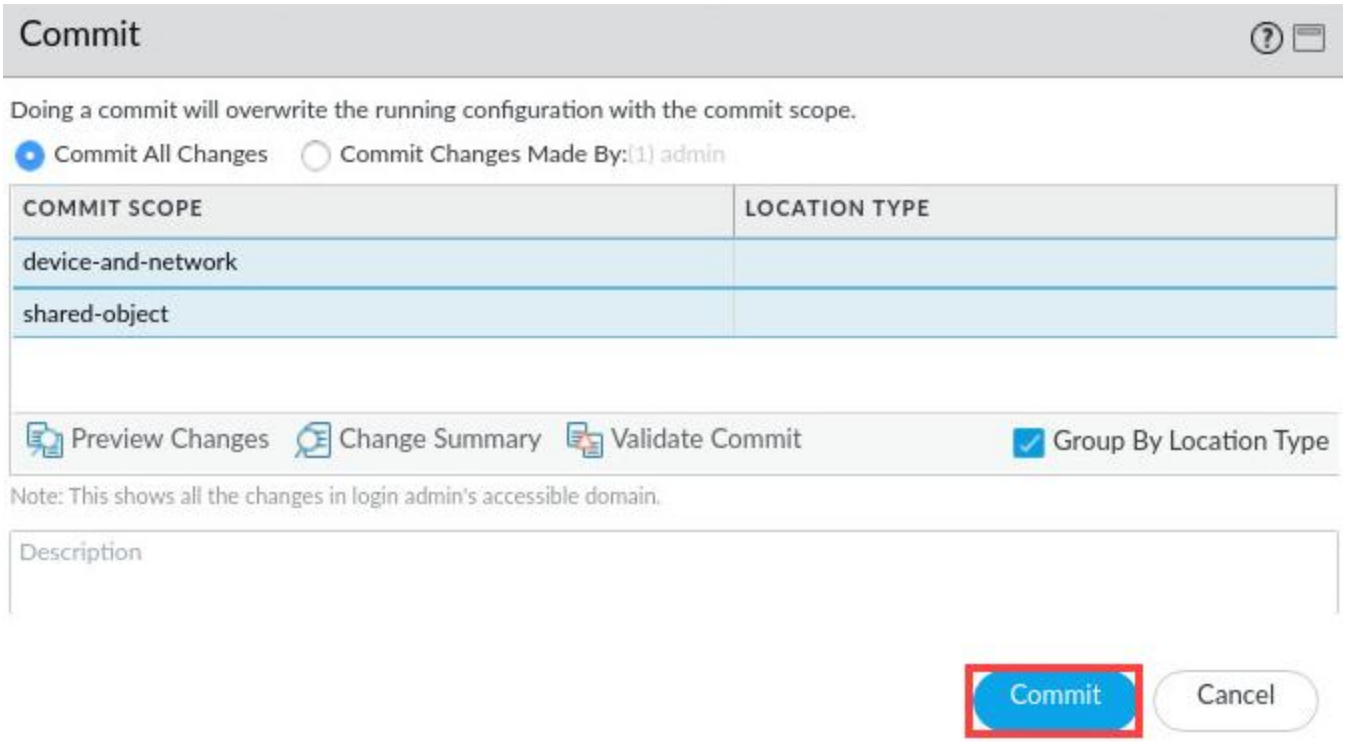

  

7. In the *Administrator* window, enter **`adminHelga`** for the *Name*. For the *Authentication Profile*, select **RADIUS Auth Profile**. Click **OK**.



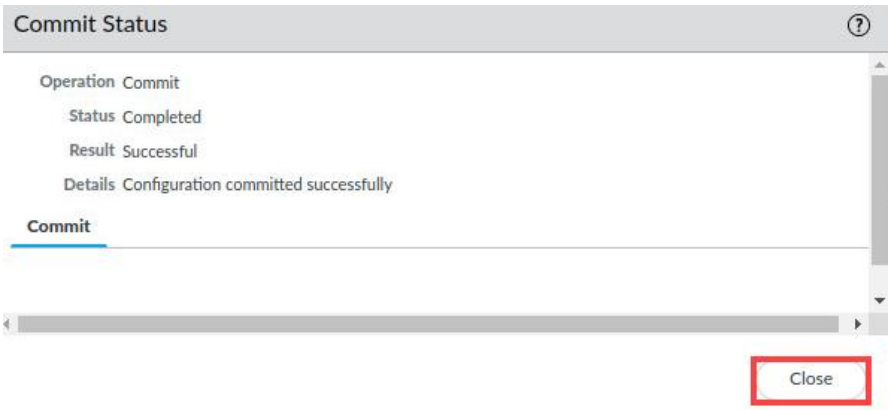

8. Click the **Commit** link located at the top-right of the web interface.


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

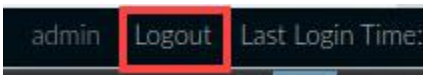


10. When the *Commit* operation successfully completes, click **Close** to continue.



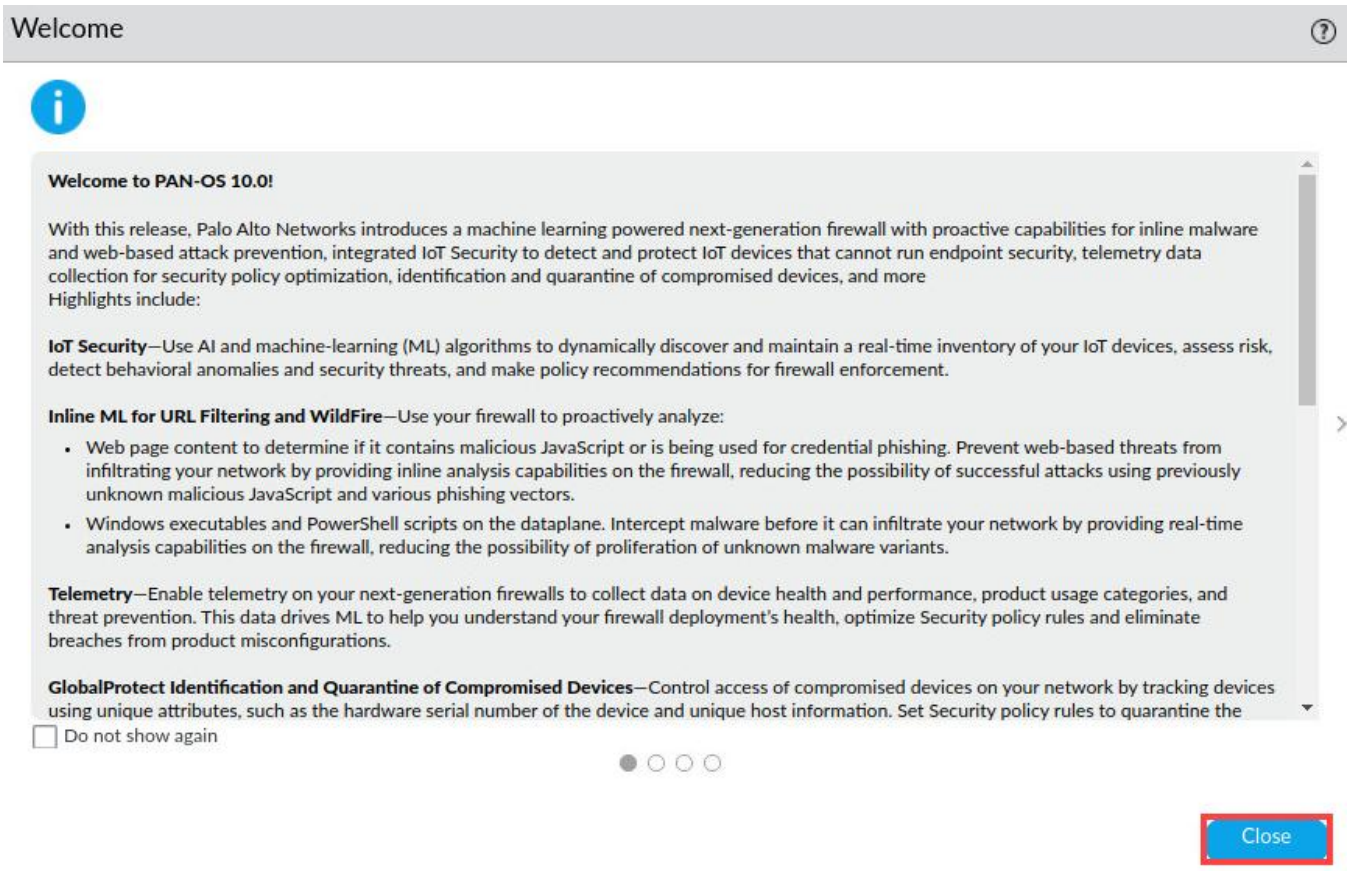

11. Log out of the firewall web interface by clicking the **Logout** button in the bottom-left corner of the window.




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

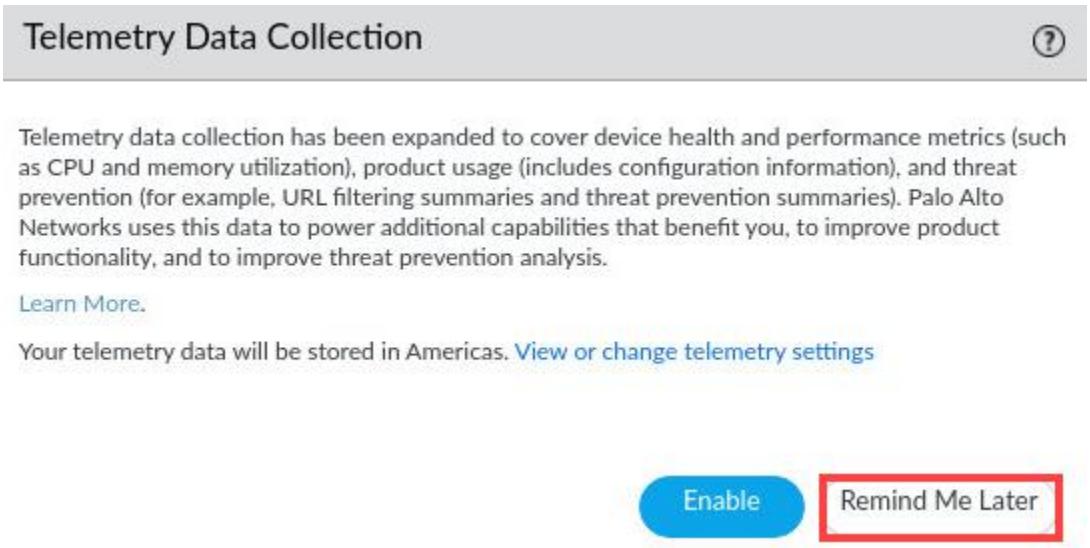
13. Log back into the firewall as username **`adminHelga`**, password **`Pal0Alt0!`**. Click **Log In**.


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

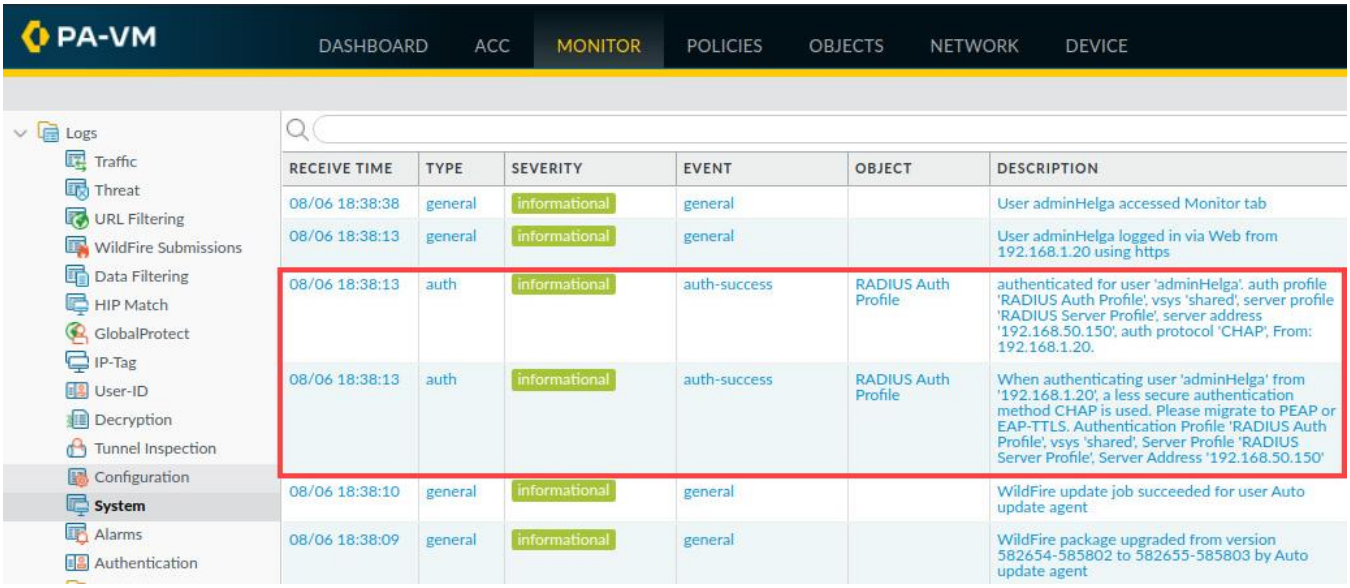


15. In the *Telemetry Data Collection* window, click **Remind Me Later**.




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




Please Note

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

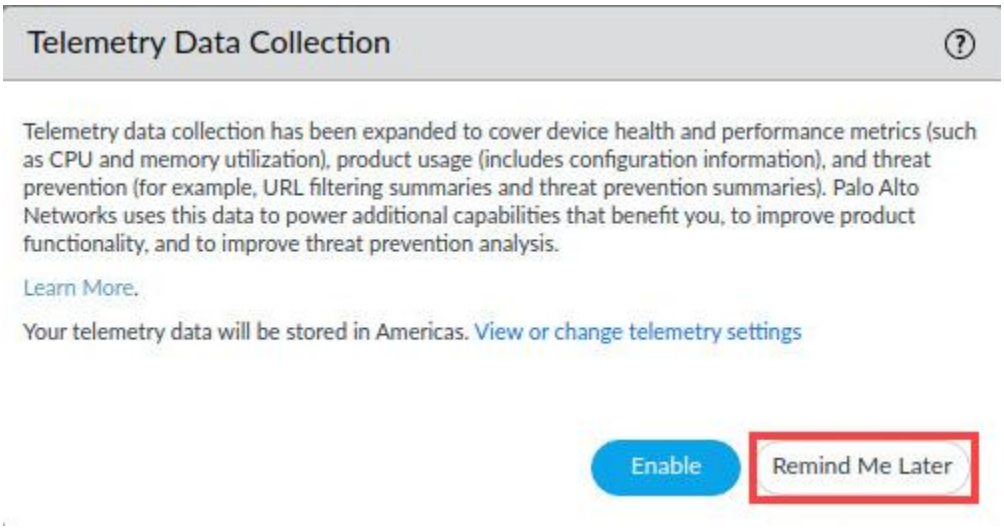
If you do not see an entry in the System log indicating a successful authentication for adminHelga, you can use a filter ( subtype eq auth )

17. Log out of the firewall.


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


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

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



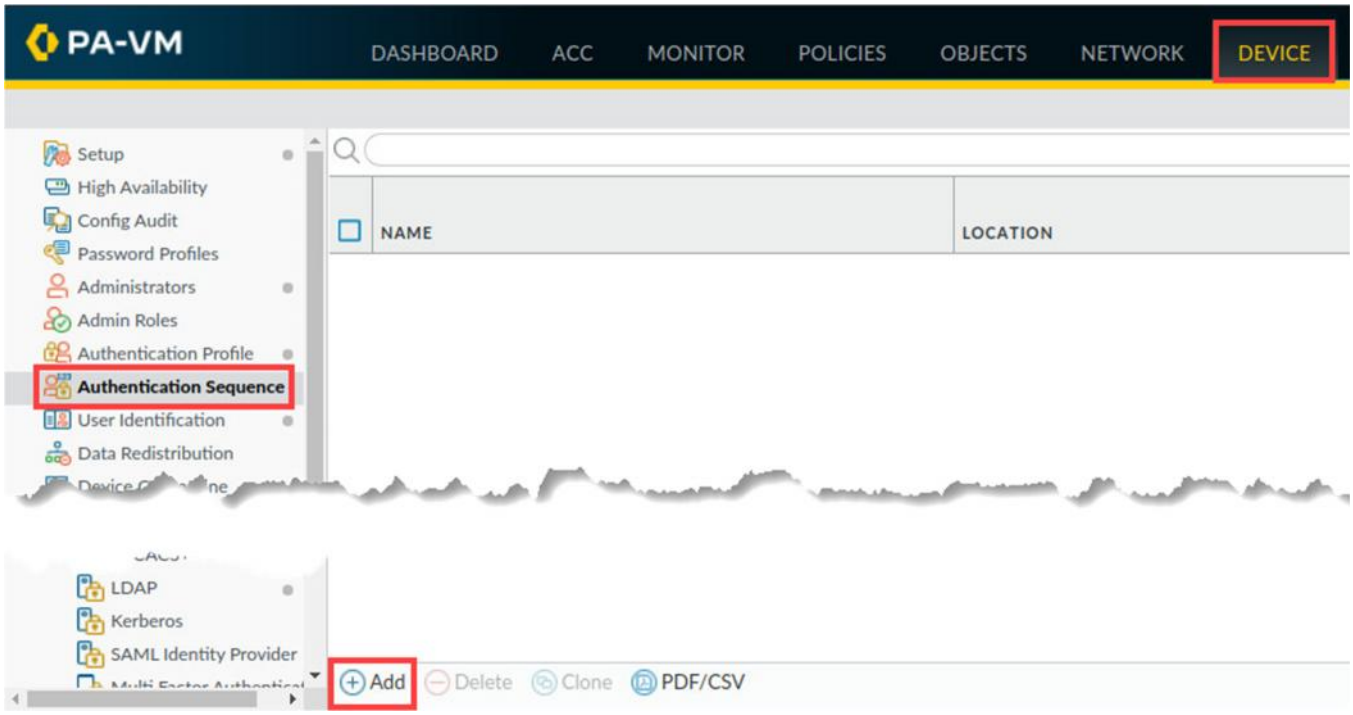

21. Leave the firewall web interface open to continue with the next task.

## 3.7 Configure and Authentication Sequence

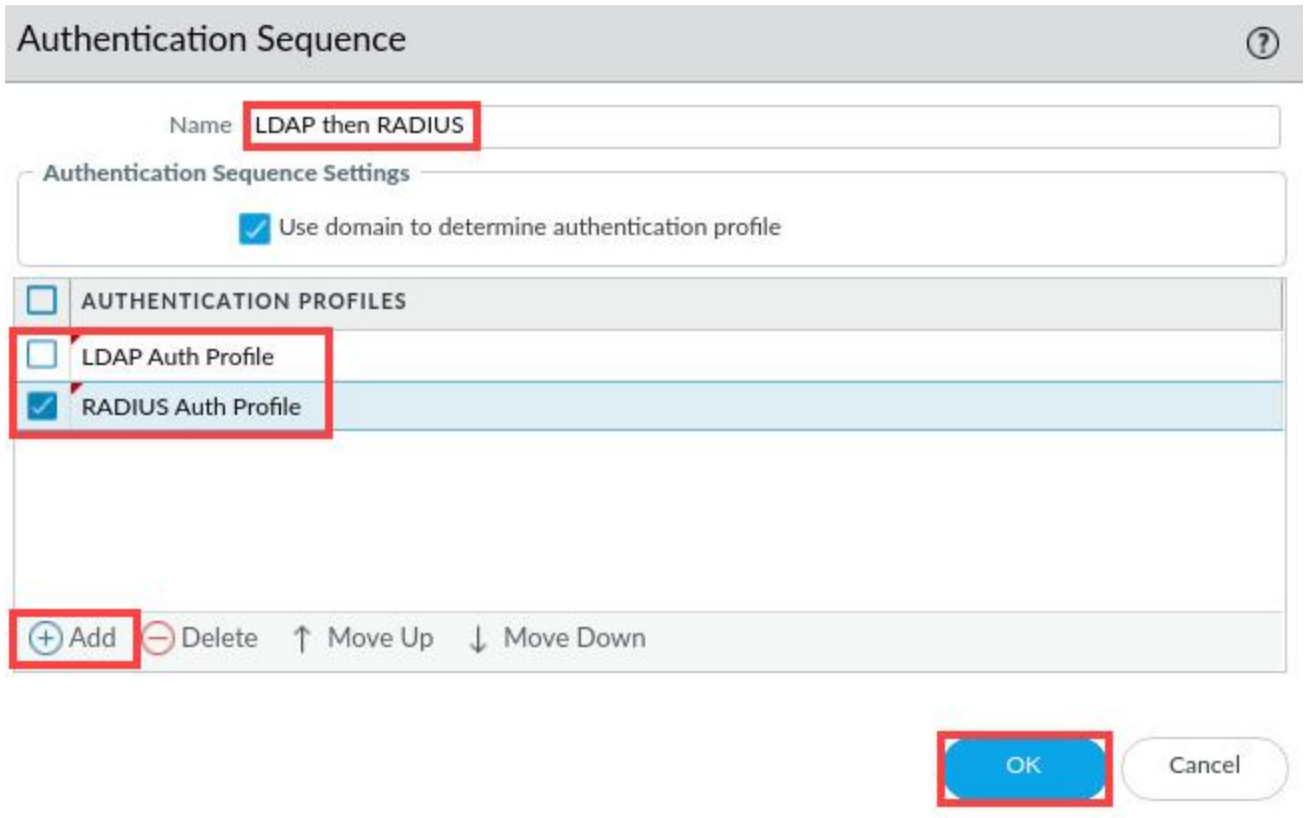
Since the acquisition, some administrator accounts exist in LDAP, and other accounts exist in RADIUS. With administrator accounts in these two different systems, you need to configure the firewall so that it can check both external databases when an administrator attempts to log in.

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**.



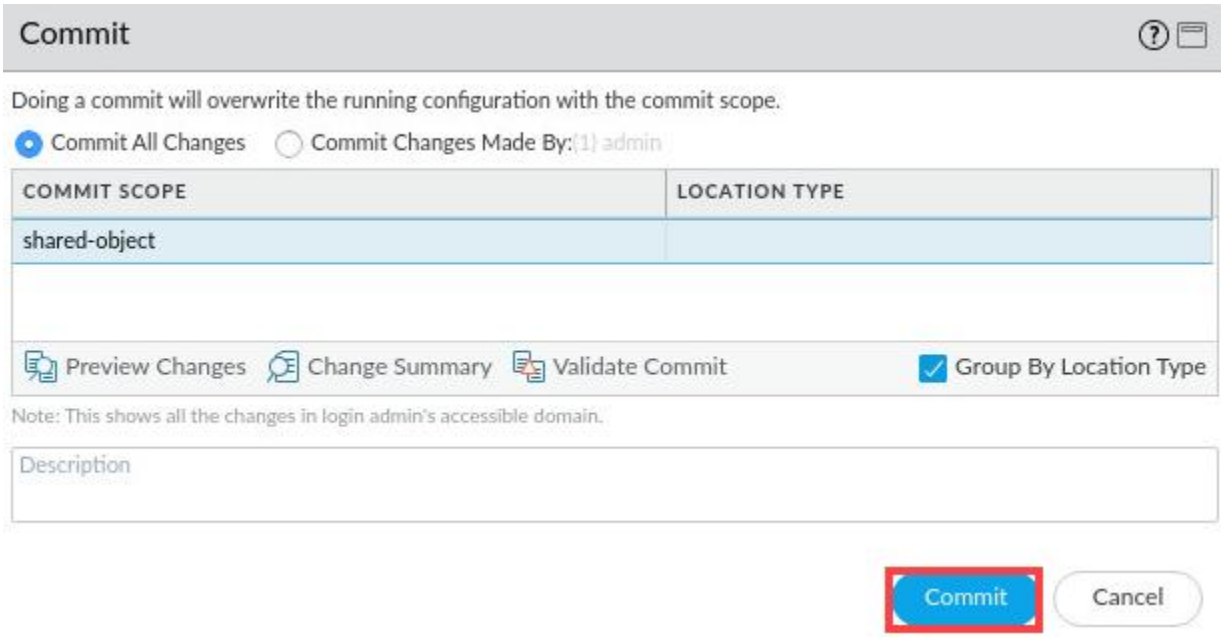

2. In the *Authentication Sequence* window, type **`LDAP then RADIUS`** for the *Name*. Under the *Authentication Profiles*, click **Add**. Select **LDAP Auth Profile**. Click **Add** again and select **RADIUS Auth Profile**. Click **OK**.



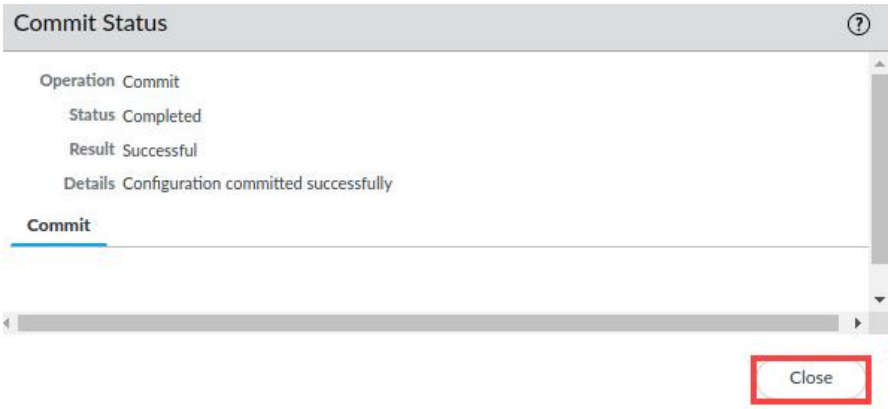
Note the Move Up and Move Down buttons. These allow you to change the order of the Authentication Profiles, if necessary. In this example, the firewall will use the LDAP-Auth-Profile first when an administrator logs in to attempt authentication; if the user account does not exist in LDAP (or if the LDAP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

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.