



CYBERSECURITY FOUNDATION V2

Lab 5: Using Two-Factor Authentication to Secure the Firewall

Document Version: 2022-12-22

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
Lab Settings	5
1 Using Two-Factor Authentication to Secure the Firewall.....	6
1.0 Load Lab Configuration	6
1.1 Create Local User Account	11
1.2 Generate Certificates.....	12
1.3 Create a Certificate Profile	16
1.4 Export Certificate and Commit.....	20
1.5 Test Connectivity and Import Certificate on the Client	23

Introduction

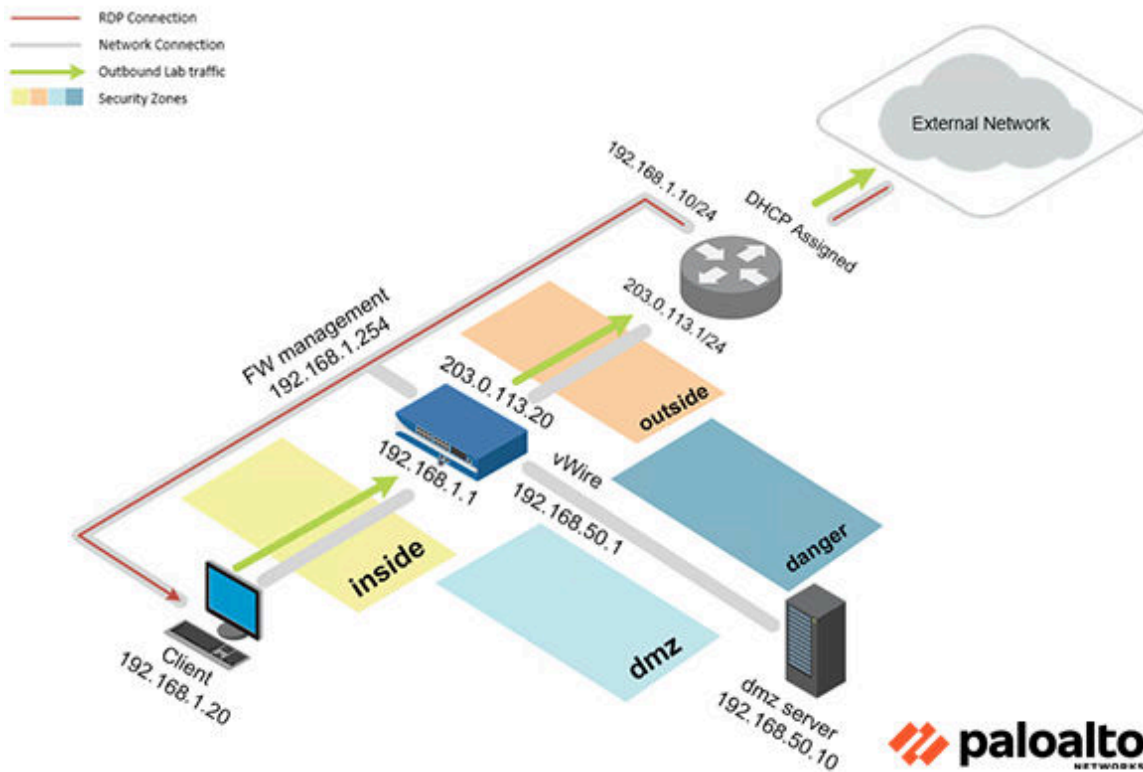
In this lab, you will configure the Firewall to use two-factor authentication using a certificate, along with a username and password.

Objective

In this lab, you will perform the following tasks:

- Create a Local User Account
- Generate Certificates
- Create a Certificate Profile
- Export Certificate and Commit
- Test Connectivity and Import Certificate on the Client

Lab Topology



Lab Settings

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

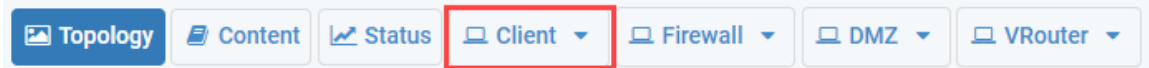
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Using Two-Factor Authentication to Secure the Firewall

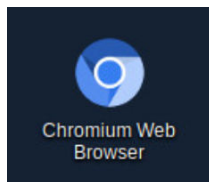
1.0 Load Lab Configuration

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

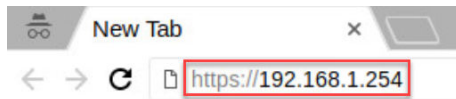
1. Click on the **Client** tab to access the *Client* PC.



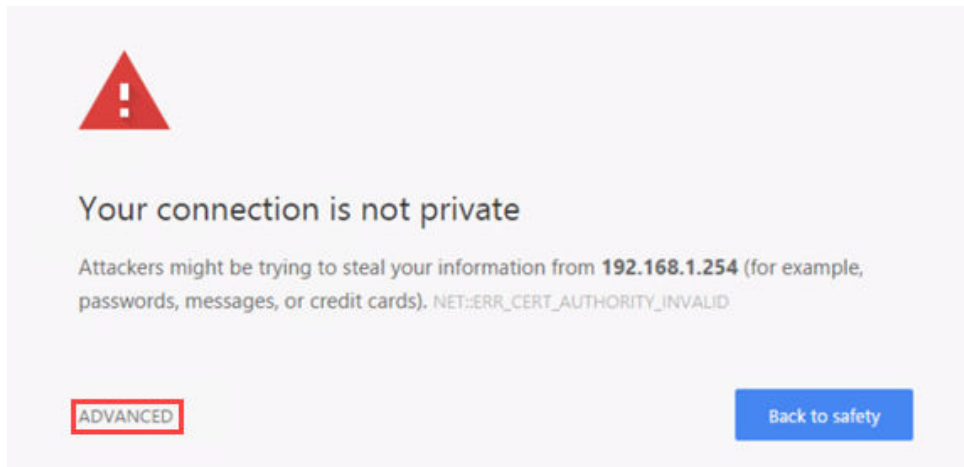
2. Log in to the **Client** PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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

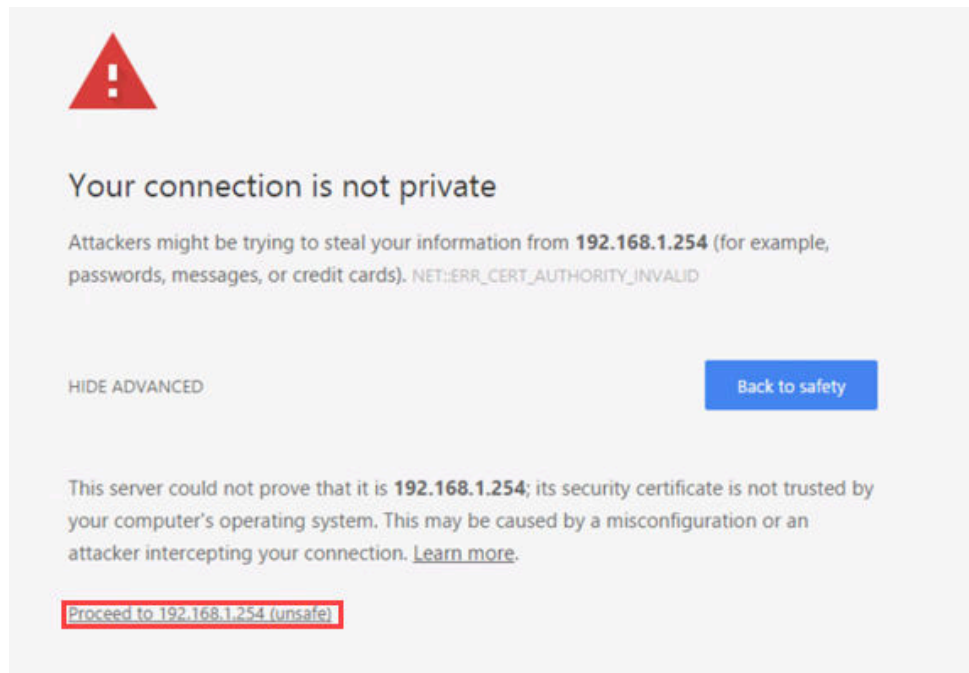


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

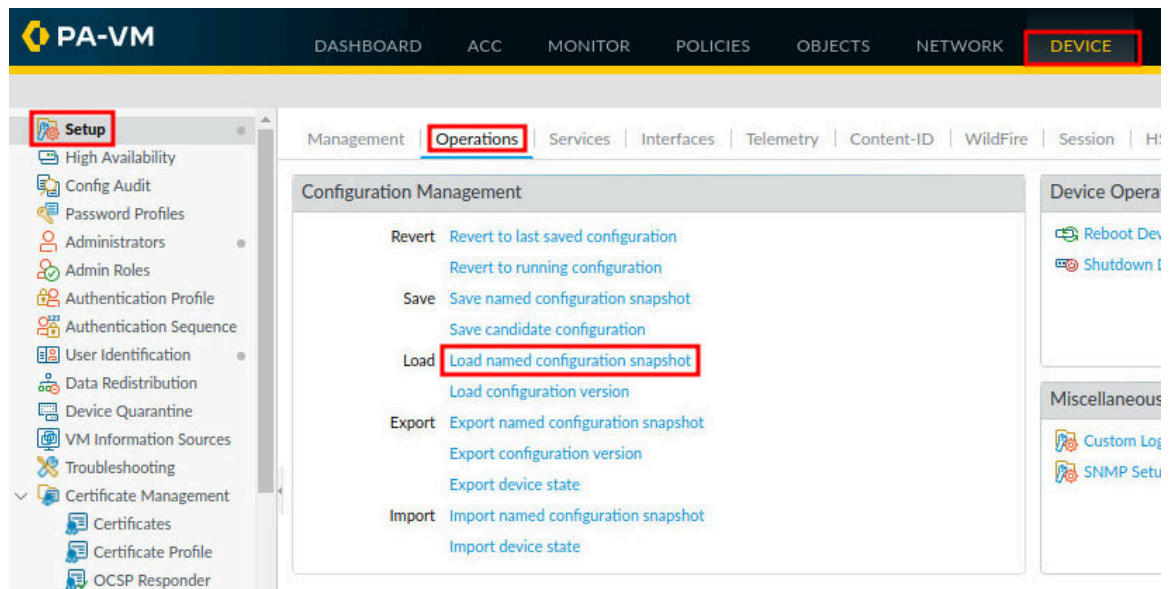
- Click on **Proceed to 192.168.1.254 (unsafe)**.



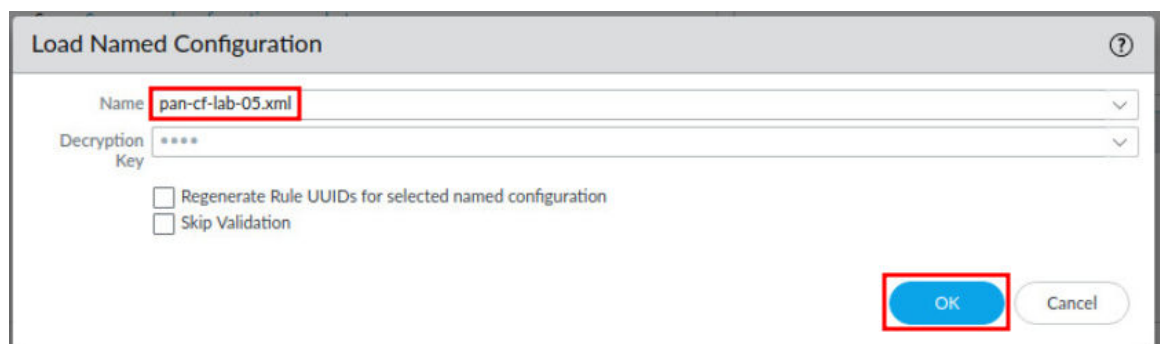
- Log in to the Firewall web interface as username admin, password Pal0Alt0!.



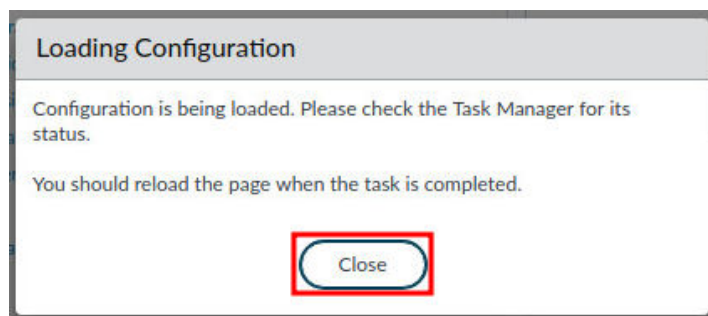
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named configuration snapshot underneath the *Configuration Management* section.



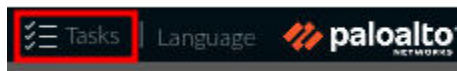
9. In the *Load Named Configuration* window, select **pan-cf-lab-05.xml** from the *Name* dropdown box and click **OK**.



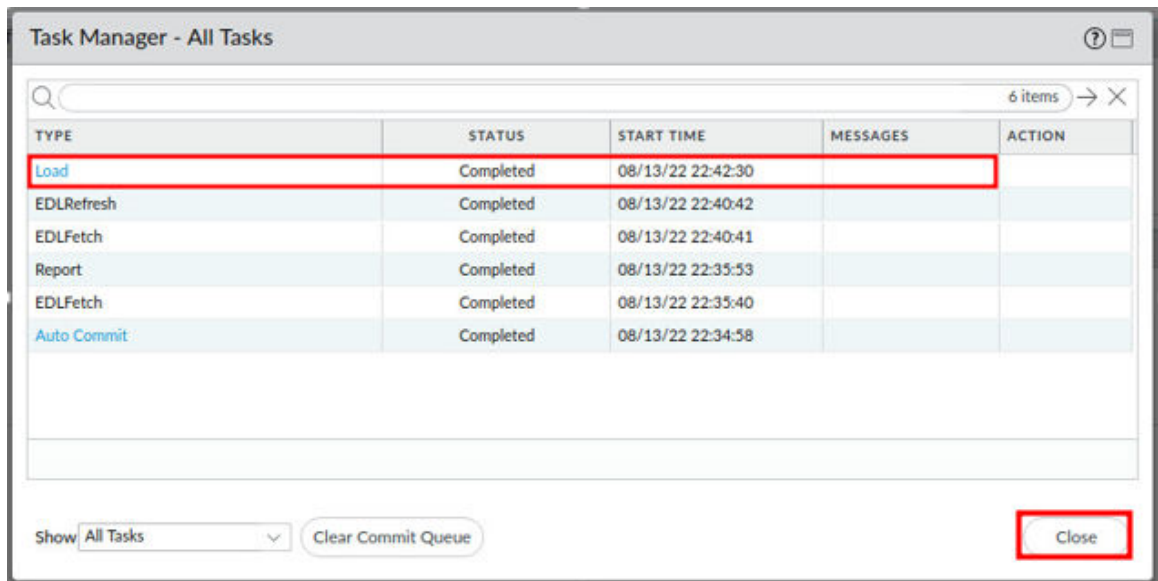
10. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. Please check the Task Manager for its status. You should reload the page when the task is completed. Click **Close** to continue.



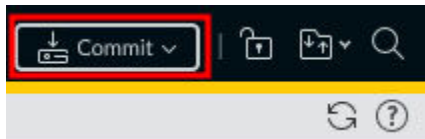
11. Click the **Tasks** icon located at the bottom-right of the web interface.



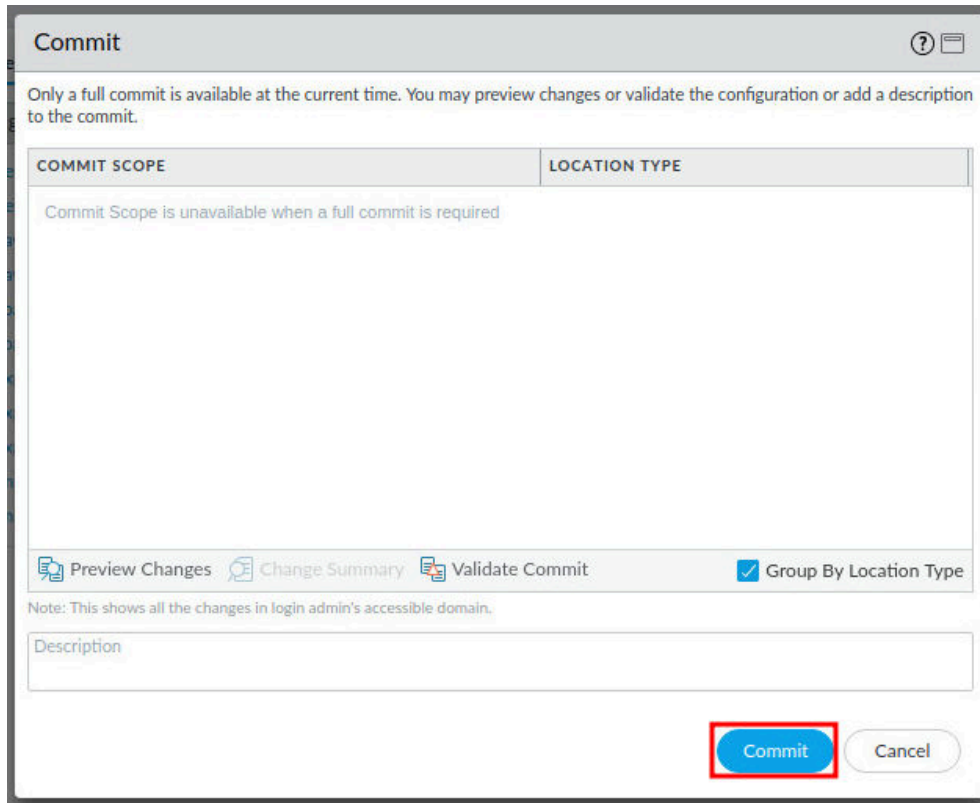
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



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

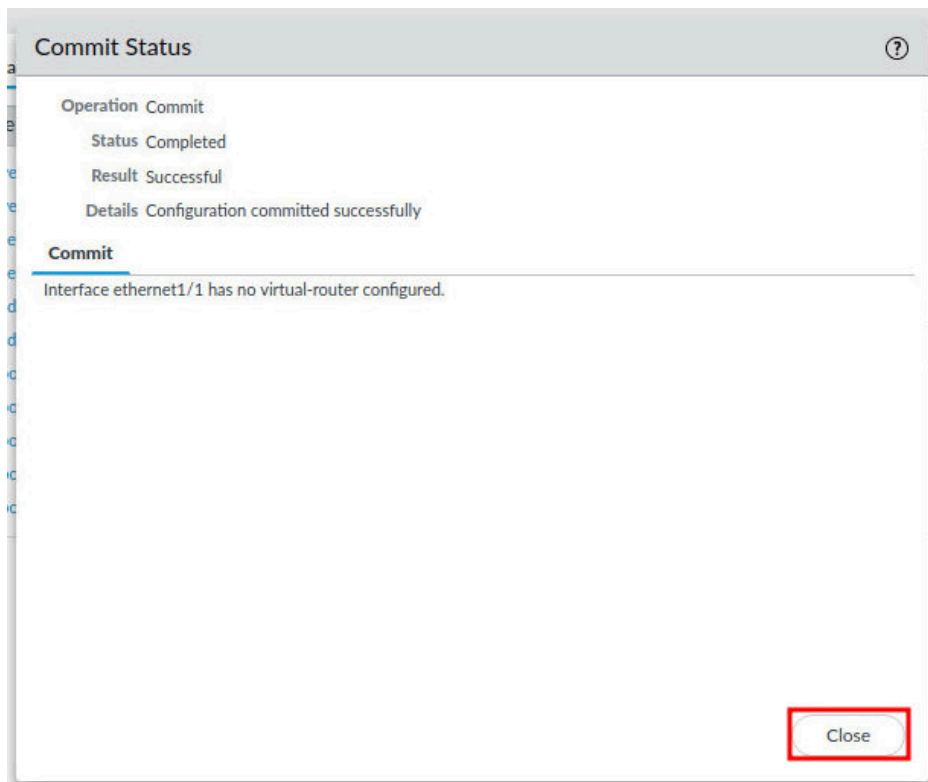


14. In the *Commit* window, click **Commit** to proceed with committing the changes.



The screenshot shows the 'Commit' window in a network management interface. The window title is 'Commit'. Below the title bar, there is a message: '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.' Below this message is a table with two columns: 'COMMIT SCOPE' and 'LOCATION TYPE'. The 'COMMIT SCOPE' column contains the text 'Commit Scope is unavailable when a full commit is required'. Below the table, there are three icons with labels: 'Preview Changes', 'Change Summary', and 'Validate Commit'. To the right of these icons is a checkbox labeled 'Group By Location Type' which is checked. Below the icons is a note: 'Note: This shows all the changes in login admin's accessible domain.' Below the note is a text input field labeled 'Description'. At the bottom right of the window, there are two buttons: 'Commit' (highlighted with a red rectangle) and 'Cancel'.

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



The screenshot shows the 'Commit Status' window in a network management interface. The window title is 'Commit Status'. Below the title bar, there is a table with the following content:

Operation	Commit
Status	Completed
Result	Successful
Details	Configuration committed successfully

Below the table, there is a section titled 'Commit' with a sub-header 'Interface ethernet1/1 has no virtual-router configured.' At the bottom right of the window, there is a button labeled 'Close' (highlighted with a red rectangle).

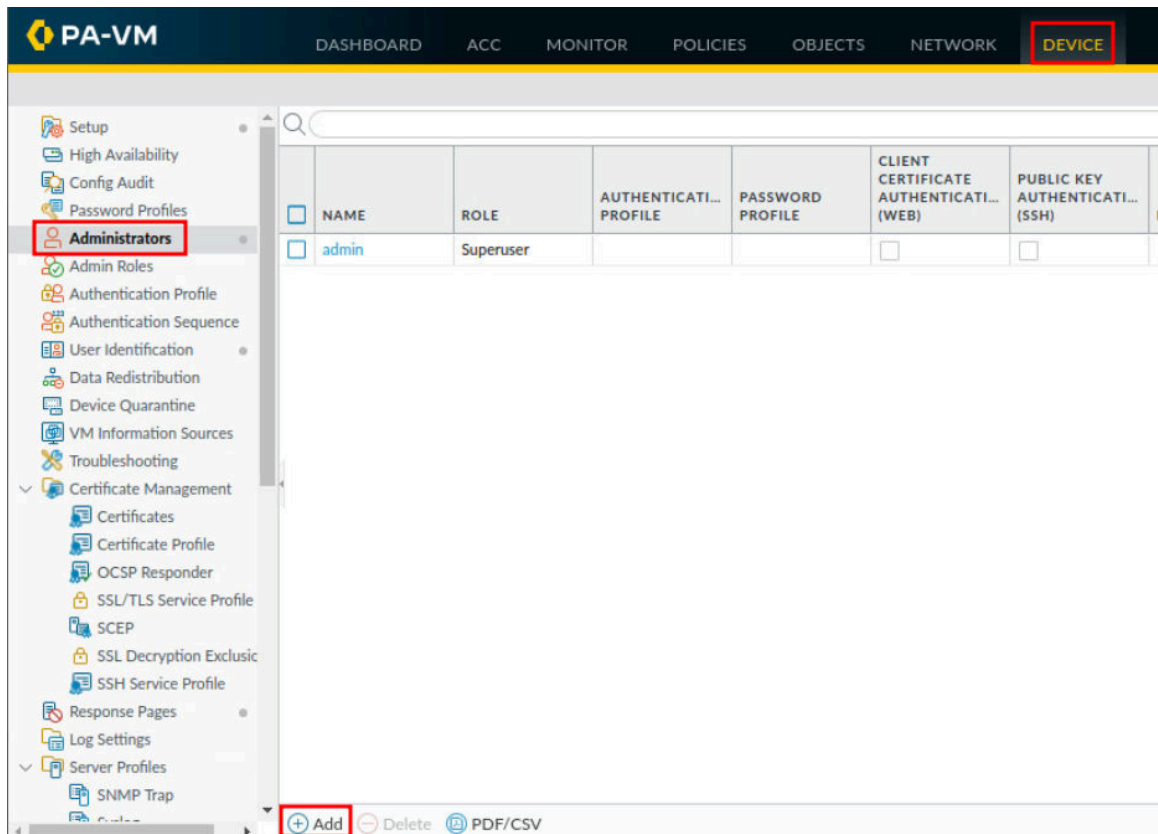


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

1.1 Create Local User Account

In this section, you will create a local user account, *lab-user*. This account will be used for authentication against the Firewall.

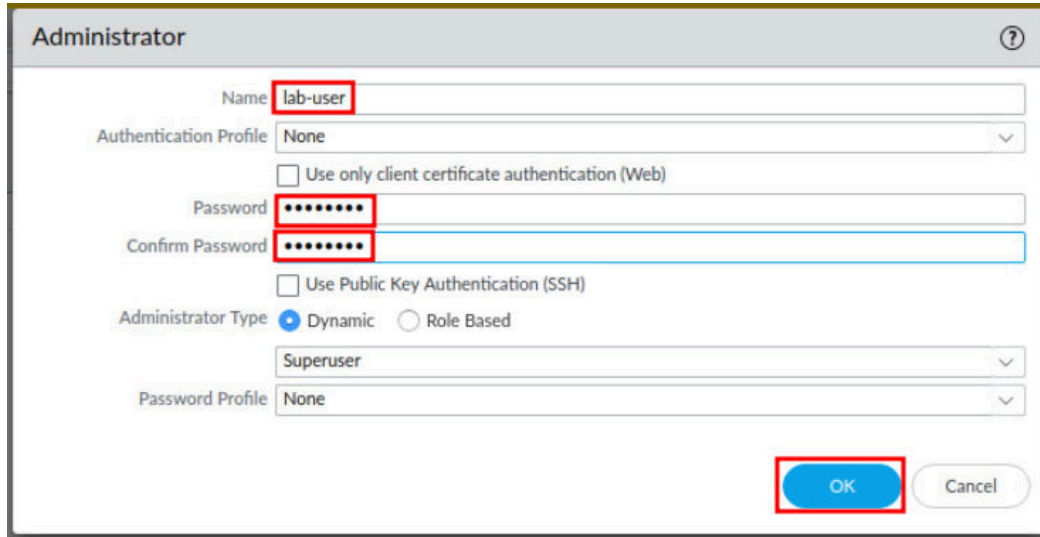
1. Navigate to **Device > Administrators > Add**.



	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"/>

+ Add - Delete PDF/CSV

2. In the *Administrator* window, type `lab-user` in the *Name* field. Then, type `Pa10Alt0` in the *Password* and *Confirm Password* fields. Finally, click the **OK** button.

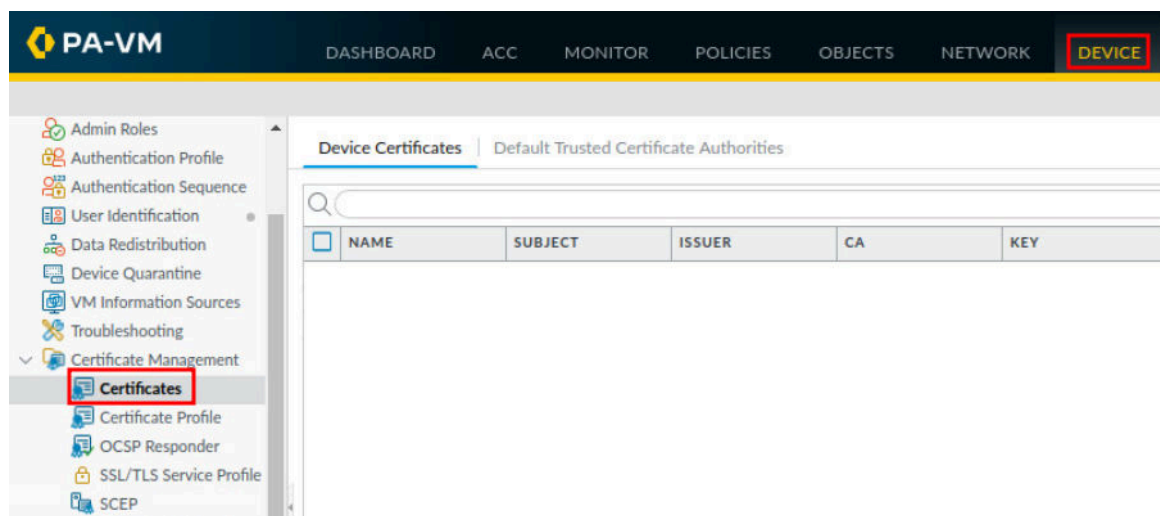


The screenshot shows the 'Administrator' configuration window. The 'Name' field contains 'lab-user'. The 'Authentication Profile' is set to 'None'. The 'Password' and 'Confirm Password' fields both contain 'Pa10Alt0'. The 'Administrator Type' is set to 'Dynamic'. The 'Superuser' checkbox is checked. The 'Password Profile' is set to 'None'. The 'OK' button is highlighted with a red box.

1.2 Generate Certificates

In this section, you will generate two certificates. The first is a self-signed Root Certificate Authority (CA) certificate, which is the top-most certificate in the certificate chain. The Firewall can use this certificate to automatically issue certificates for other uses. In this lab, you will use the Root CA certificate to generate a certificate for use on the Client machine that is associated with the local user account, **lab-user**.

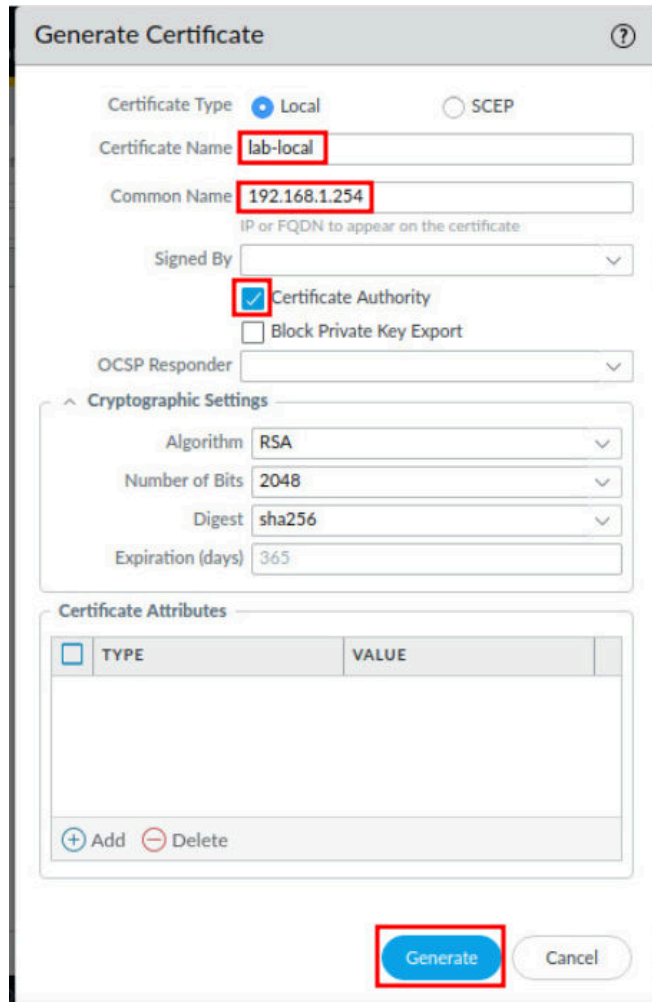
1. Navigate to **Device > Certificate Management > Certificates**.



- Click on the **Generate** button at the bottom-center of the center section.



- In the *Generate Certificate* window, type `lab-local` in the *Certificate Name* field. Then, type `192.168.1.254` in the *Common Name* field. Next, click the **Certificate Authority** checkbox. Finally, click the **Generate** button.



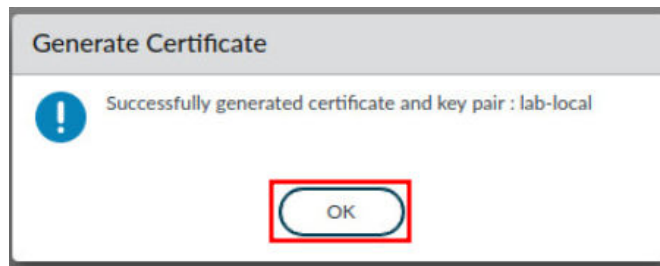
The **Generate Certificate** dialog box is shown. It has a title bar with a question mark icon. The **Certificate Type** is set to **Local**. The **Certificate Name** field contains `lab-local`. The **Common Name** field contains `192.168.1.254`. Below this is a dropdown for **Signed By**. The **Certificate Authority** checkbox is checked. There is an unchecked checkbox for **Block Private Key Export**. Below that is a dropdown for **OCSP Responder**. The **Cryptographic Settings** section is expanded, showing **Algorithm** as **RSA**, **Number of Bits** as **2048**, **Digest** as **sha256**, and **Expiration (days)** as **365**. The **Certificate Attributes** section is at the bottom, showing a table with columns **TYPE** and **VALUE**. There are **+ Add** and **- Delete** buttons. At the bottom right, there is a **Generate** button and a **Cancel** button.

TYPE	VALUE
------	-------



This will generate a certificate for the Firewall to act as a Certificate Authority (CA). By the Firewall being a CA, you can now issue a certificate for the local account you created earlier, *lab-user*.

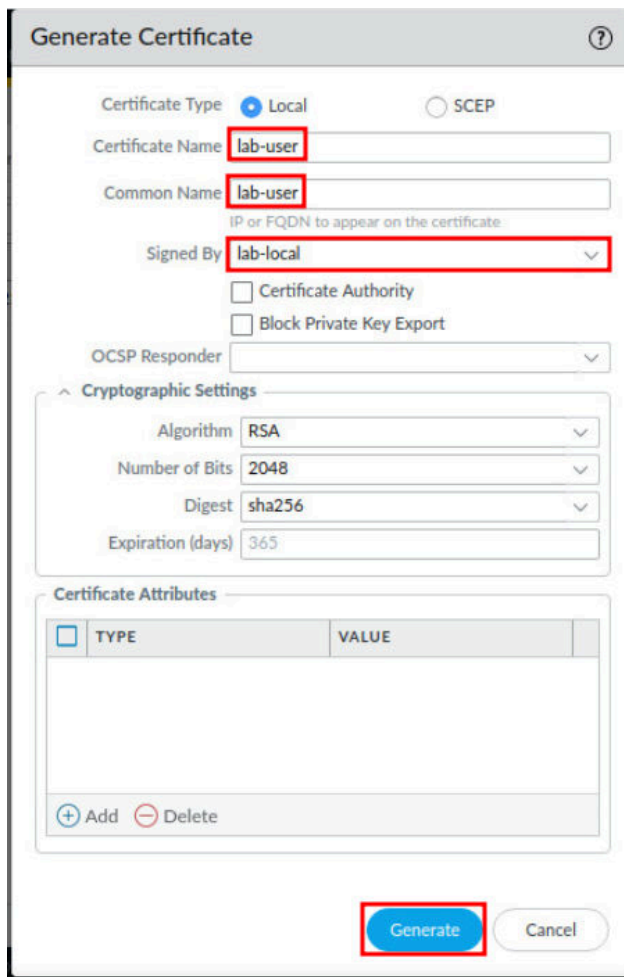
4. In the *Generate Certificate* window, click **OK** to continue.



5. Click on the **Generate** button at the bottom-center of the center section.



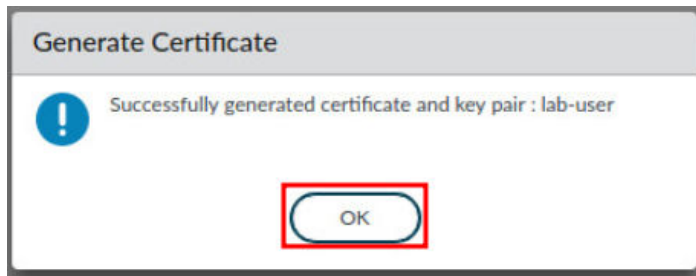
6. In the *Generate Certificate* window, type lab-user in the *Certificate Name* field. Then, type lab-user in the *Common Name* field. Next, select **lab-local** in the *Signed By* dropdown. Finally, click the **Generate** button.

A screenshot of the 'Generate Certificate' dialog box with various fields filled out. The 'Certificate Type' is set to 'Local'. The 'Certificate Name' and 'Common Name' fields both contain 'lab-user'. The 'Signed By' dropdown menu is set to 'lab-local'. Below this, there are checkboxes for 'Certificate Authority' and 'Block Private Key Export', both of which are unchecked. The 'OCSP Responder' field is empty. The 'Cryptographic Settings' section is expanded, showing 'Algorithm' as RSA, 'Number of Bits' as 2048, 'Digest' as sha256, and 'Expiration (days)' as 365. The 'Certificate Attributes' section is also expanded, showing a table with columns 'TYPE' and 'VALUE'. At the bottom, there are buttons for 'Add' and 'Delete'. The 'Generate' button at the bottom center is highlighted with a red rectangular box.



In setting the Common Name as *lab-user*, this will later be used as an authentication field, to map to the local user account, *lab-user*. Notice, you are using the previous root CA certificate, *lab-local*, to sign this certificate.

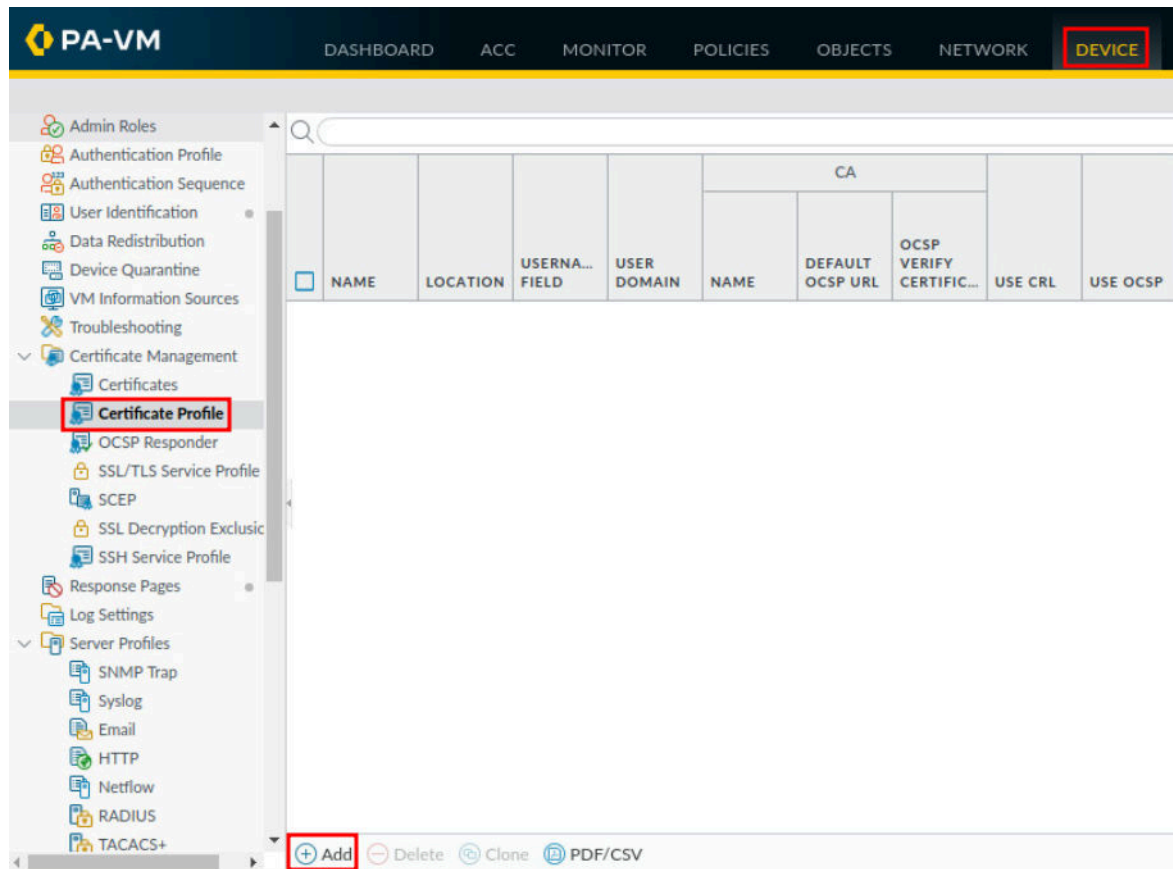
7. In the *Generate Certificate* window, click **OK** to continue.



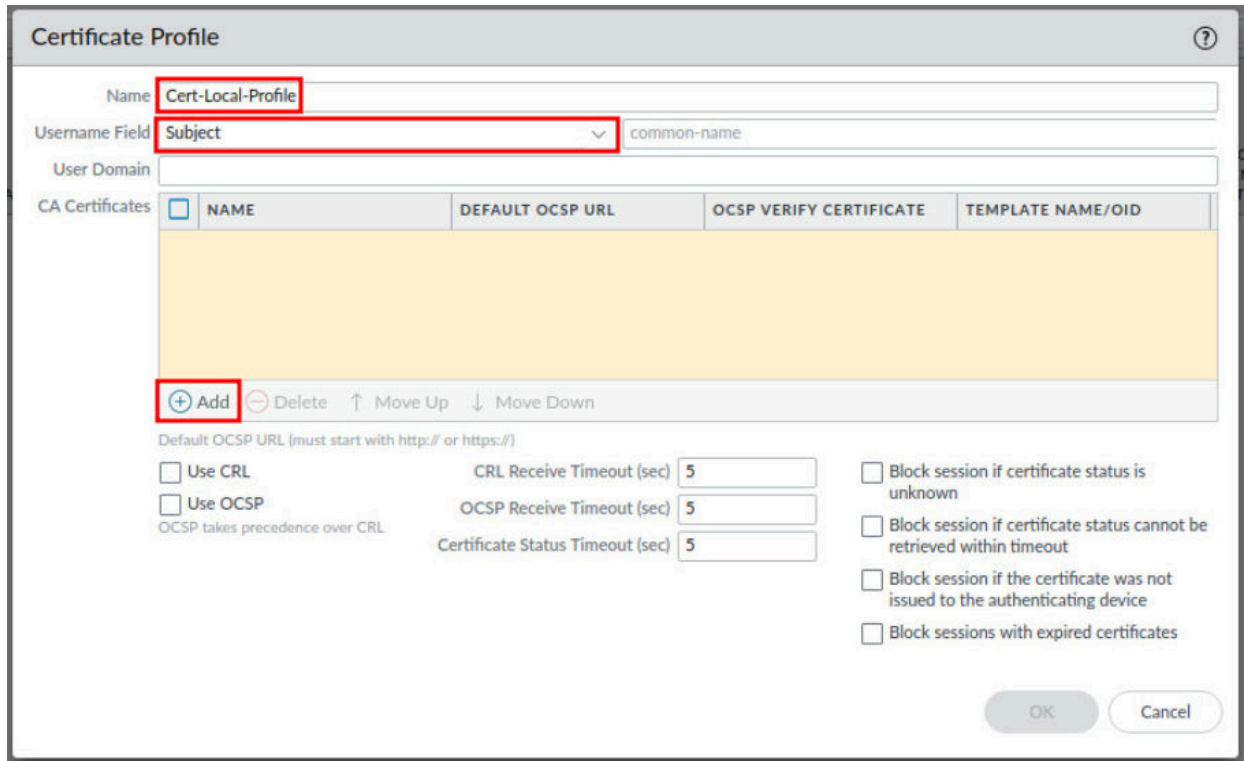
1.3 Create a Certificate Profile

In this section, you will create a certificate profile. A certificate profile defines user and device authentication for multiple services on the Firewall. The profile specifies which certificates to use, how to verify certificate revocation status, and how that status constrains access. In this lab, the certificate profile is created to tell the Firewall to use the *common-name* of the certificate as a username. Then, you will tell the Firewall to use this Certificate Profile to authenticate users.

1. Navigate to **Device > Certificate Management > Certificate Profile > Add**.



2. In the *Certificate Profile* window, type **Cert-Local-Profile** in the *Name* field. Then, select **Subject** in the *Username Field* dropdown. Next, click on the **Add** button.

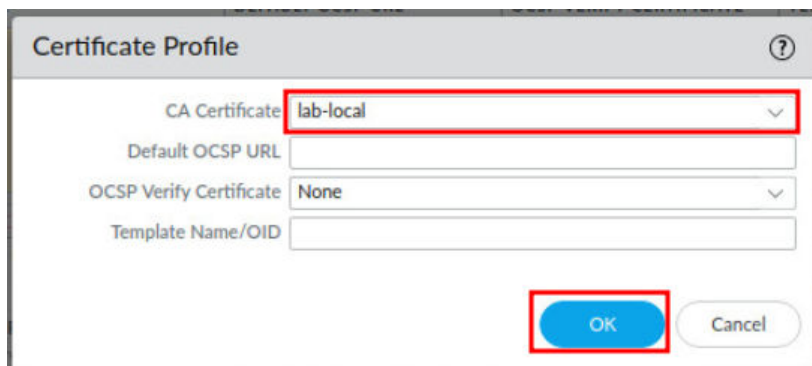


The screenshot shows the 'Certificate Profile' window. The 'Name' field is set to 'Cert-Local-Profile'. The 'Username Field' dropdown is set to 'Subject', and the 'common-name' field is visible. The 'CA Certificates' section is empty. The 'Add' button is highlighted with a red box. Below the table, there are checkboxes for 'Use CRL' and 'Use OCSP', and input fields for 'CRL Receive Timeout (sec)', 'OCSP Receive Timeout (sec)', and 'Certificate Status Timeout (sec)', all set to 5. There are also checkboxes for 'Block session if certificate status is unknown', 'Block session if certificate status cannot be retrieved within timeout', 'Block session if the certificate was not issued to the authenticating device', and 'Block sessions with expired certificates'. The 'OK' and 'Cancel' buttons are at the bottom right.



Notice the Username Field, when set to *Subject*, it will use “common-name” as the default. The Firewall will now use the “common-name” as the username. The *lab-user* certificate you generated earlier has a common-name of *lab-user* and will therefore use *lab-user* to authenticate the client machine.

3. In the *Certificate Profile* window, select **lab-local** in the *CA Certificate* dropdown. Then, click the **OK** button.

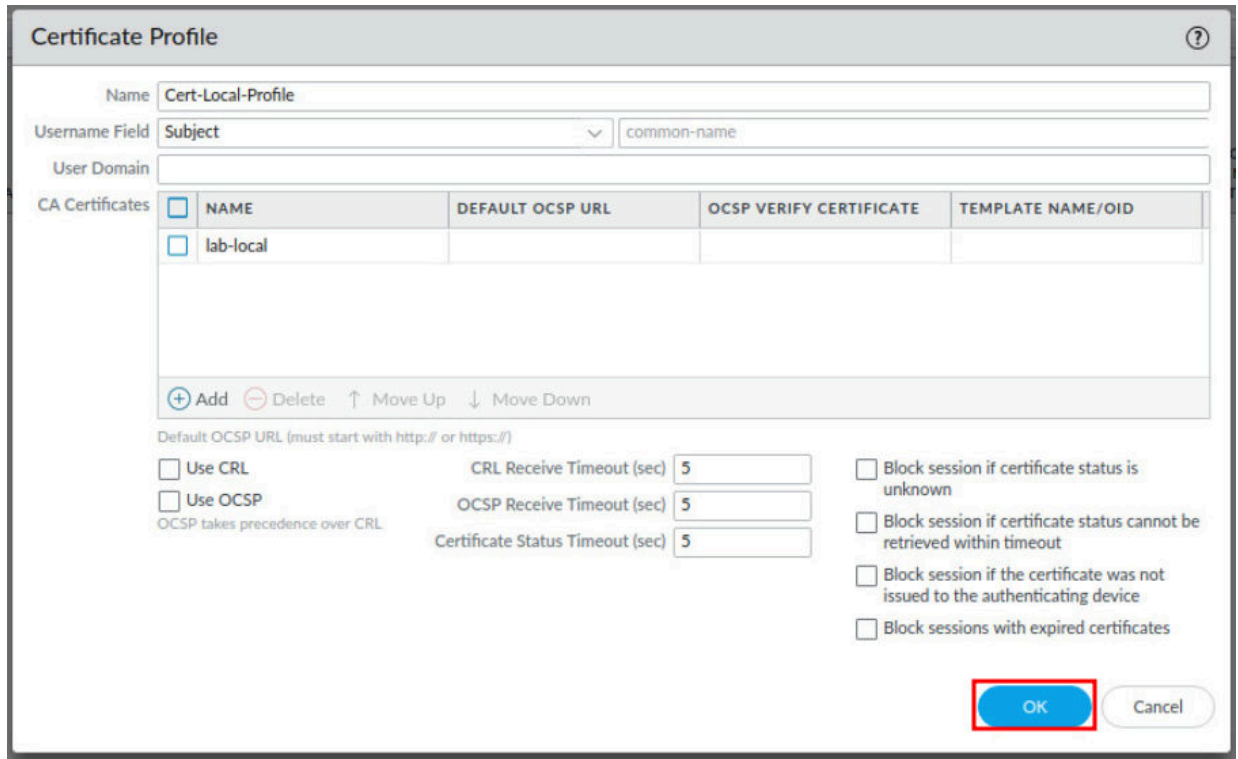


The screenshot shows the 'Certificate Profile' window. The 'CA Certificate' dropdown is set to 'lab-local'. The 'Default OCSP URL' field is empty. The 'OCSP Verify Certificate' dropdown is set to 'None'. The 'Template Name/OID' field is empty. The 'OK' button is highlighted with a red box. The 'Cancel' button is at the bottom right.



This maps back to the *lab-local* CA certificate you created earlier, and the Firewall will use this to verify the authenticity of the client supplied certificate, *lab-user*.

4. In the *Certificate Profile* window, click the **OK** button.



Certificate Profile

Name:

Username Field:

User Domain:

CA Certificates	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
<input type="checkbox"/>	lab-local			

+ Add - Delete ↑ Move Up ↓ Move Down

Default OCSP URL (must start with http:// or https://)

☐ Use CRL ☐ Use OCSP
OCSP takes precedence over CRL

CRL Receive Timeout (sec)

OCSP Receive Timeout (sec)

Certificate Status Timeout (sec)

☐ Block session if certificate status is unknown

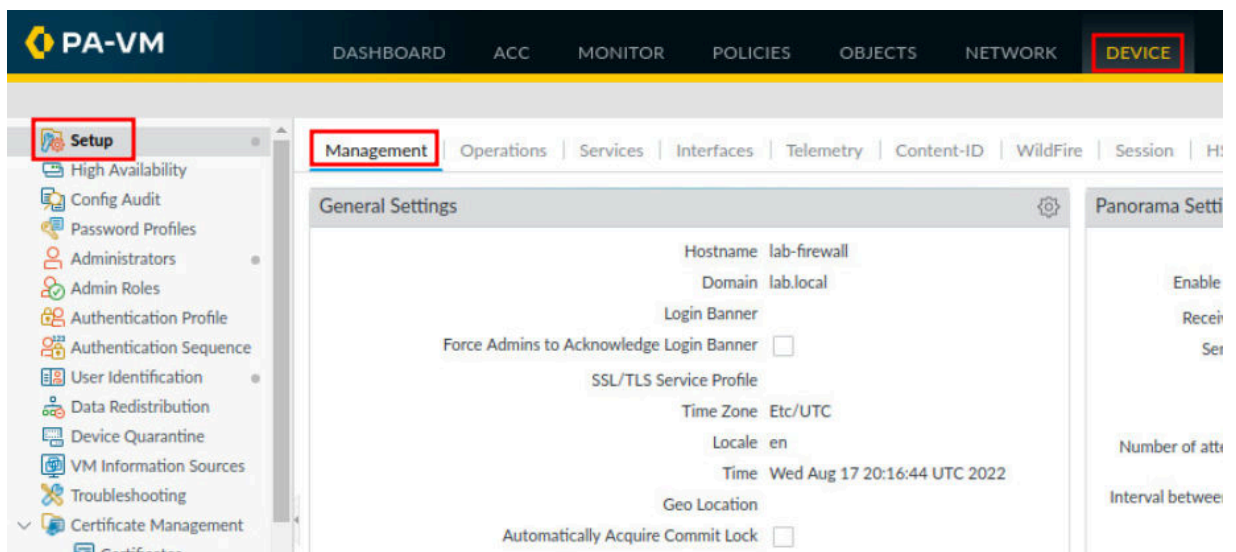
☐ Block session if certificate status cannot be retrieved within timeout

☐ Block session if the certificate was not issued to the authenticating device

☐ Block sessions with expired certificates

OK Cancel

5. Navigate to **Device > Setup > Management**.



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

Setup Management Operations Services Interfaces Telemetry Content-ID WildFire Session Hi

General Settings

Hostname lab-firewall

Domain lab.local

Login Banner

Force Admins to Acknowledge Login Banner ☐

SSL/TLS Service Profile

Time Zone Etc/UTC

Locale en

Time Wed Aug 17 20:16:44 UTC 2022

Geo Location

Automatically Acquire Commit Lock ☐

Panorama Settings

Enable

Receive

Serial

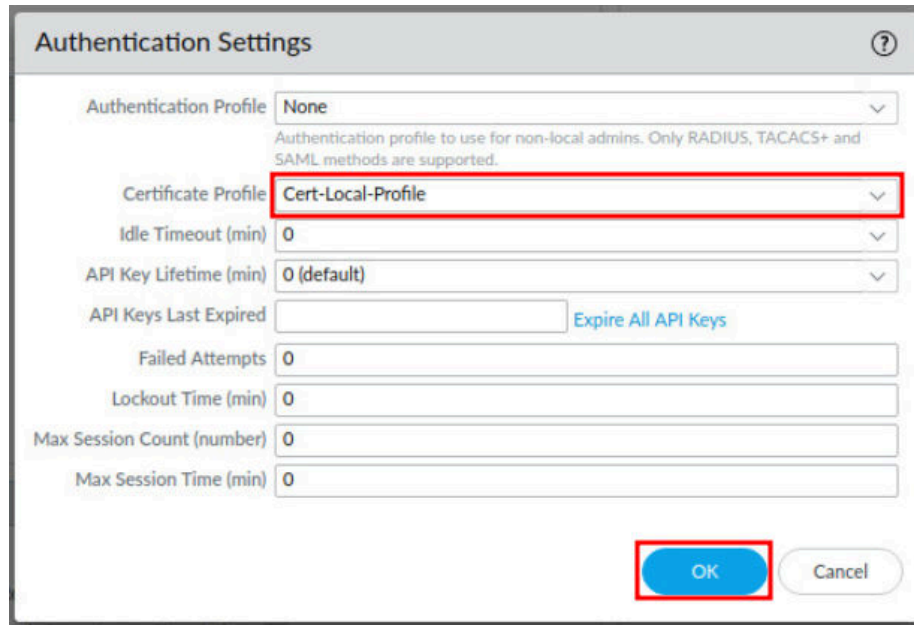
Number of att

Interval between

- Click the **gear** icon on the *Authentication Settings* section, located in the center.



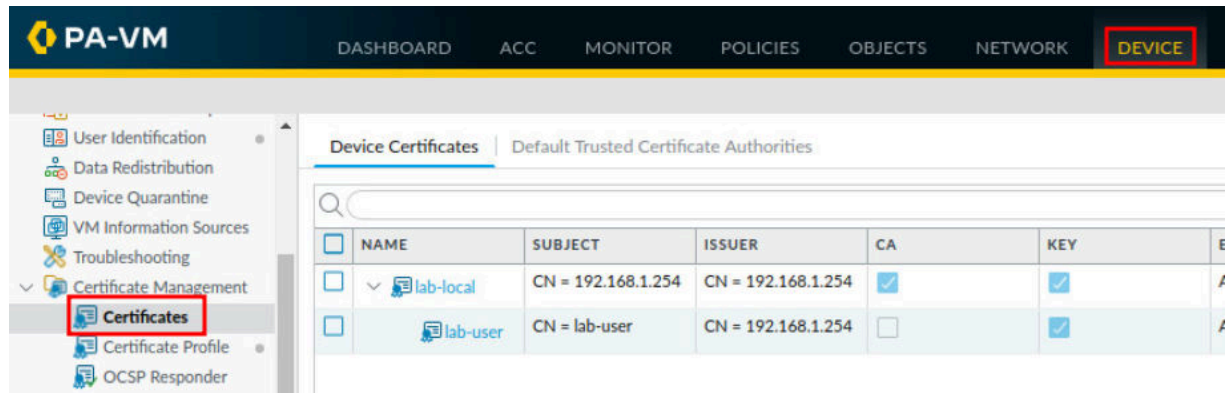
- In the *Authentication Settings* window, select **Cert-Local-Profile** for the *Certificate Profile* dropdown. Then, click on the **OK** button.



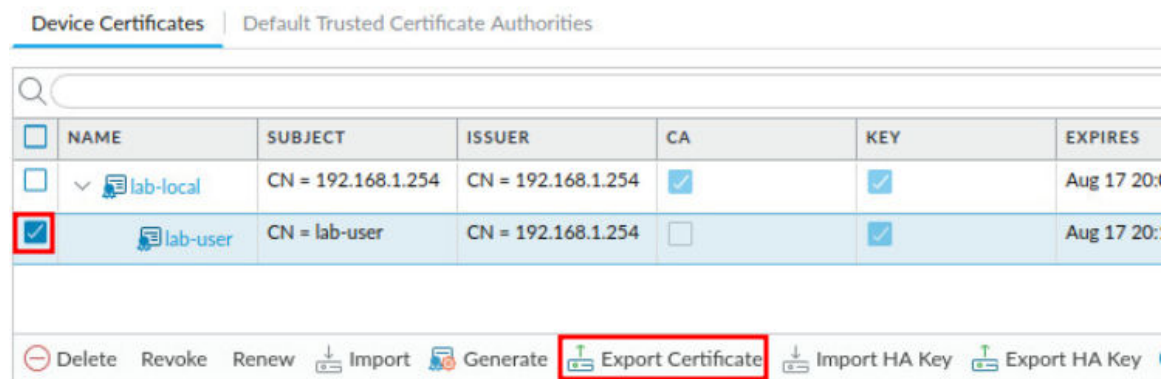
1.4 Export Certificate and Commit

In this section, you will export the *lab-user* certificate you generated on the Firewall. Then, you will commit changes, causing the Firewall to start using certificates for authentication.

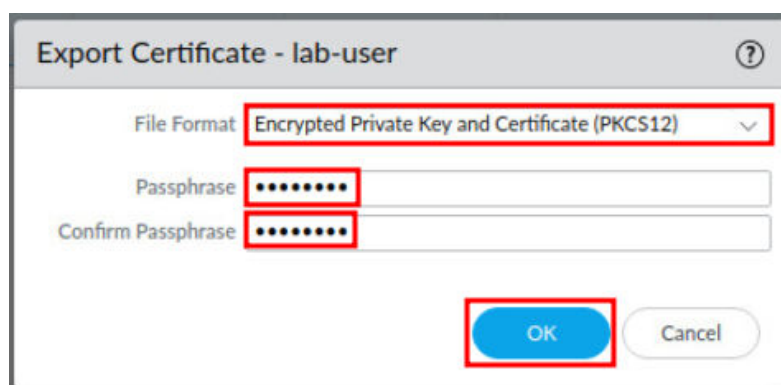
1. Navigate to **Device > Certificate Management > Certificates**.



2. Select the **lab-user** certificate and click on the **Export Certificate** button.



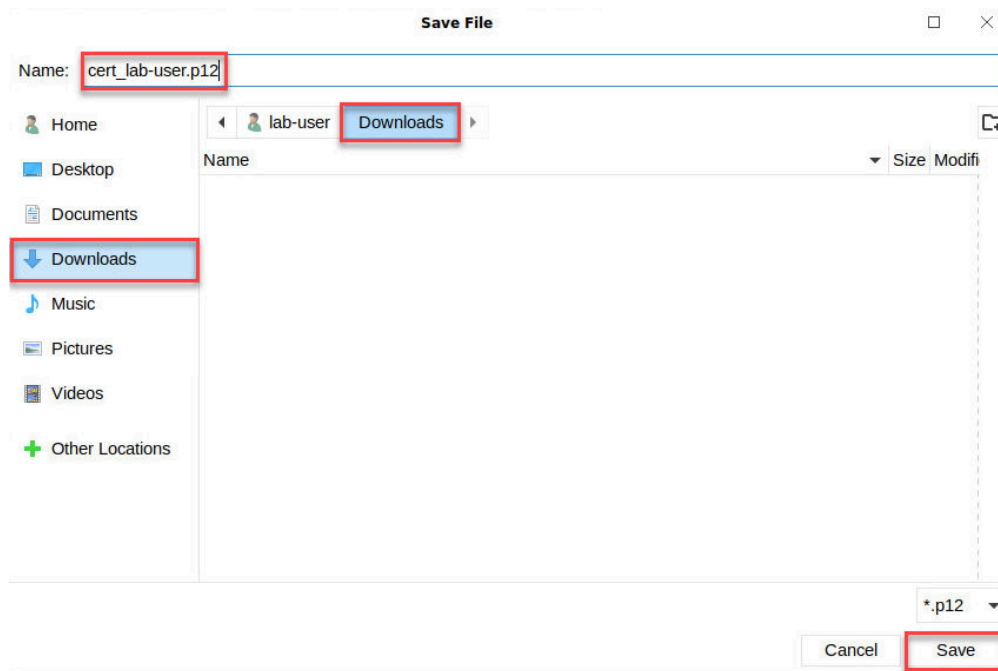
3. In the *Export Certificate - lab-user* window, select **Encrypted Private Key and Certificate (PKCS12)** in the **File Format** dropdown. Then, type *paloalto* for the **Passphrase** and **Confirm Passphrase** fields, then click on the **OK** button.



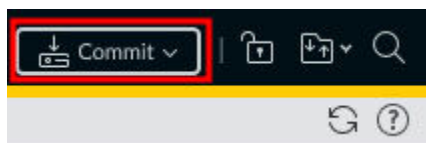


By using an *Encrypted Private Key and Certificate*, this creates an additional security measure, as the passphrase is required to install the certificate on a client machine.

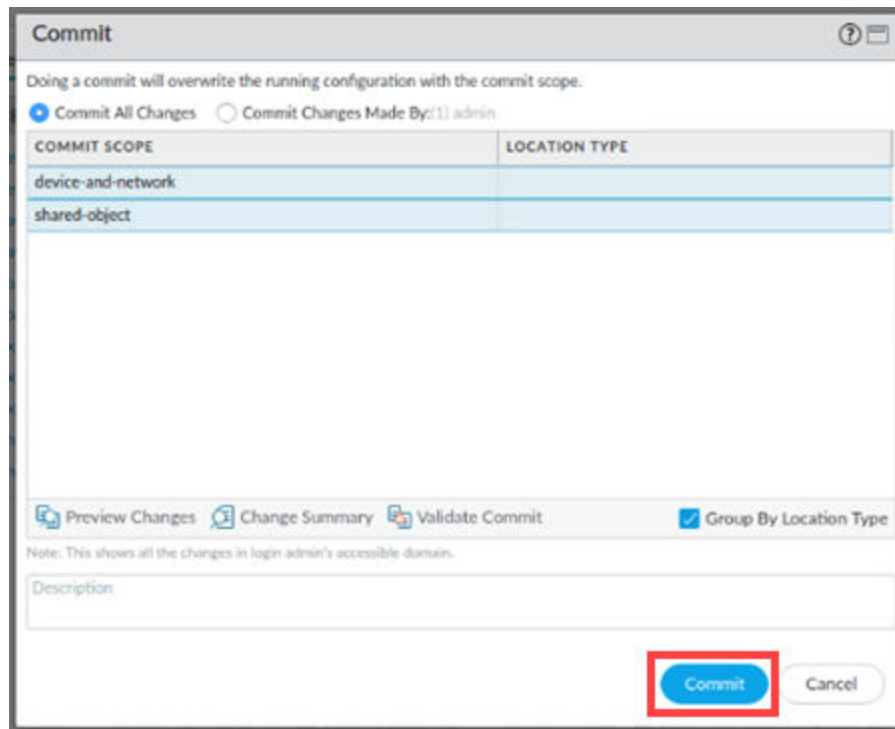
4. In the *Save File* window pop-up, verify the name of ***cert_lab-user.p12*** is correct in the *Name* field, verify the ***.p12*** file is being saved in the ***Downloads*** folder, and click **Save**.



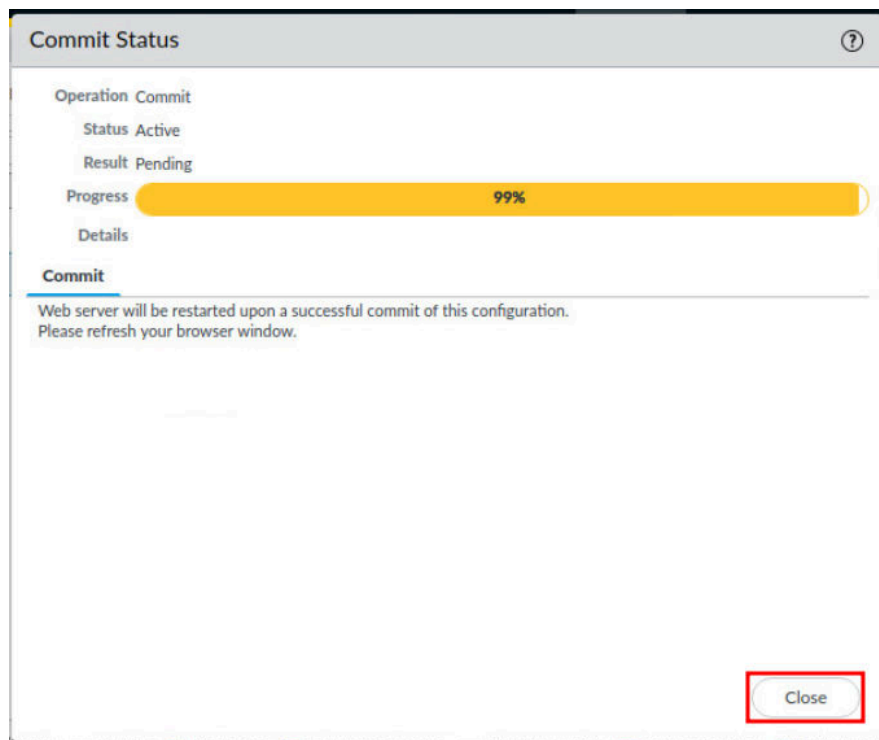
5. Click the **Commit** link located at the top-right of the web interface.



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



7. When the commit operation reaches 99%, click **Close** to continue.





Notice the warning about the Web server being restarted, this is because of the authentication changes you made. You will need to click the Close button when it gets to 99%, since the web server is restarting, you will not see it get to 100%.

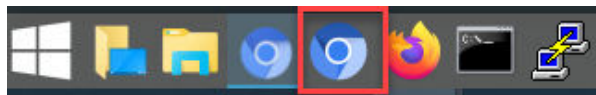
8. Click the **X** in the upper-right to close the *Chromium Web Browser*.



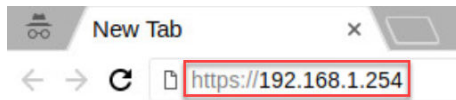
1.5 Test Connectivity and Import Certificate on the Client

In this section, you will test connectivity to the Firewall. Then, you will import the *lab-user* certificate on the *Client* machine and try again.

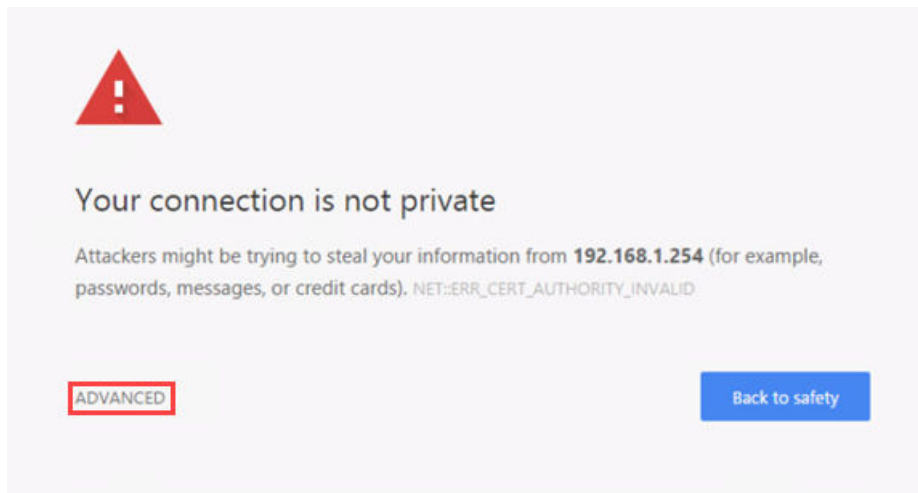
1. Open **Chromium** from the taskbar.



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



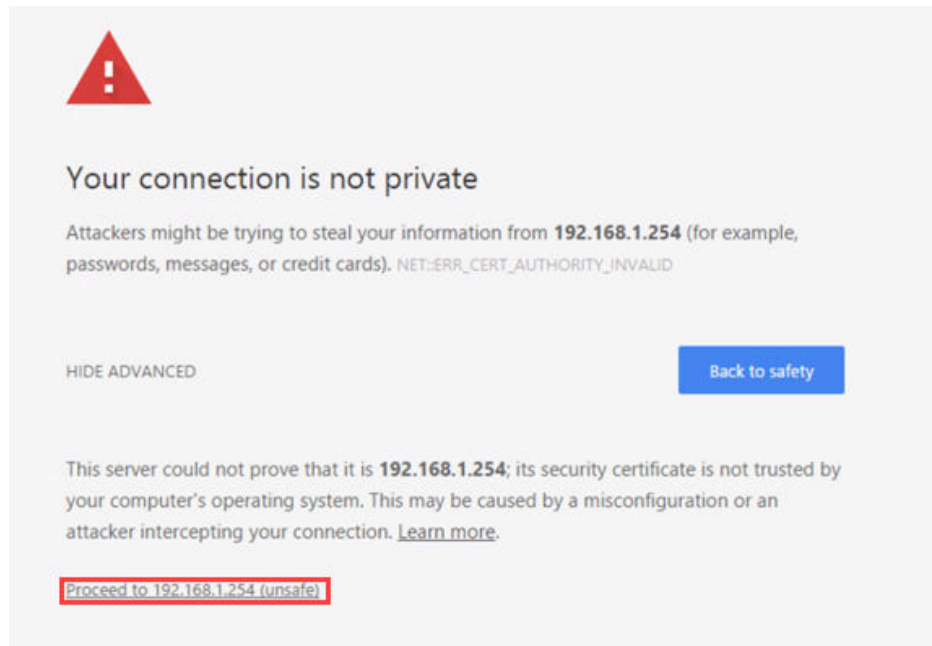
3. You will see a “Your connection is not private” message. Click on the **ADVANCED** Link.



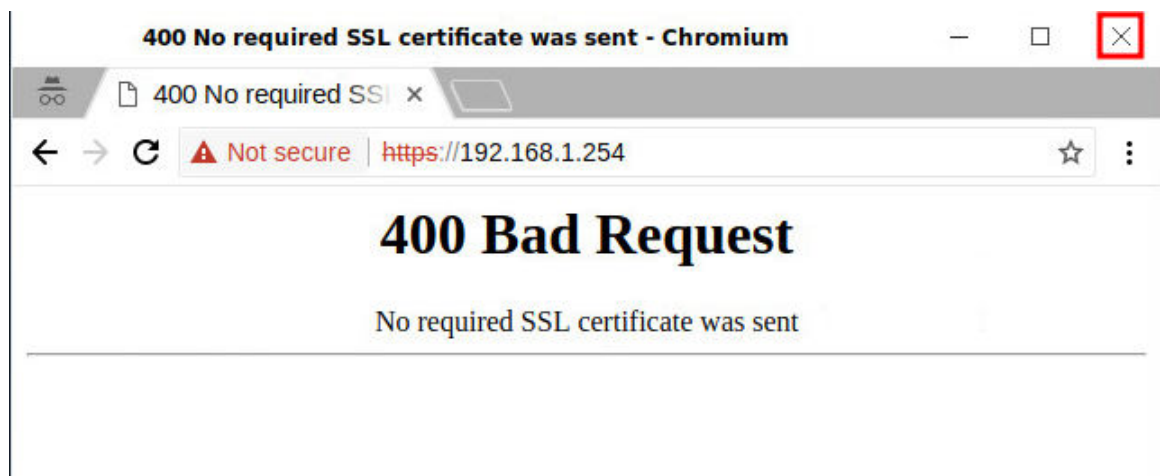


This message is displayed because the Firewall has a self-signed certificate by default. The client does not have a Certificate Authority that can validate the certificate.

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



5. You will see a “400 Bad Request - No Required SSL certificate was sent” message. Click the **X** in the upper-right to close Chromium.

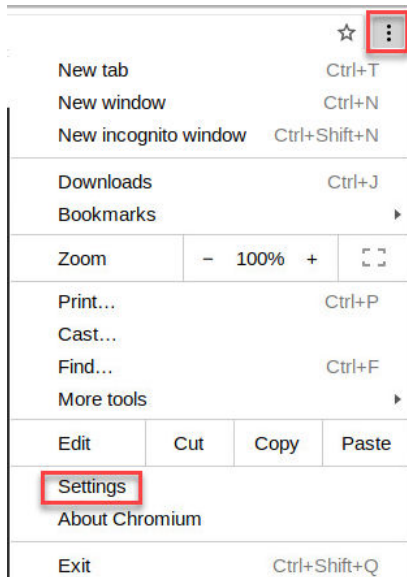


Notice you get a *HTTP 400 Bad Request* error. This is because the *lab-user* certificate is not installed on the *Client* machine. The Firewall administrators are not allowed to login unless they have the certificate installed and have an account and password. These two factors make up the Two-Factor Authentication in this lab.

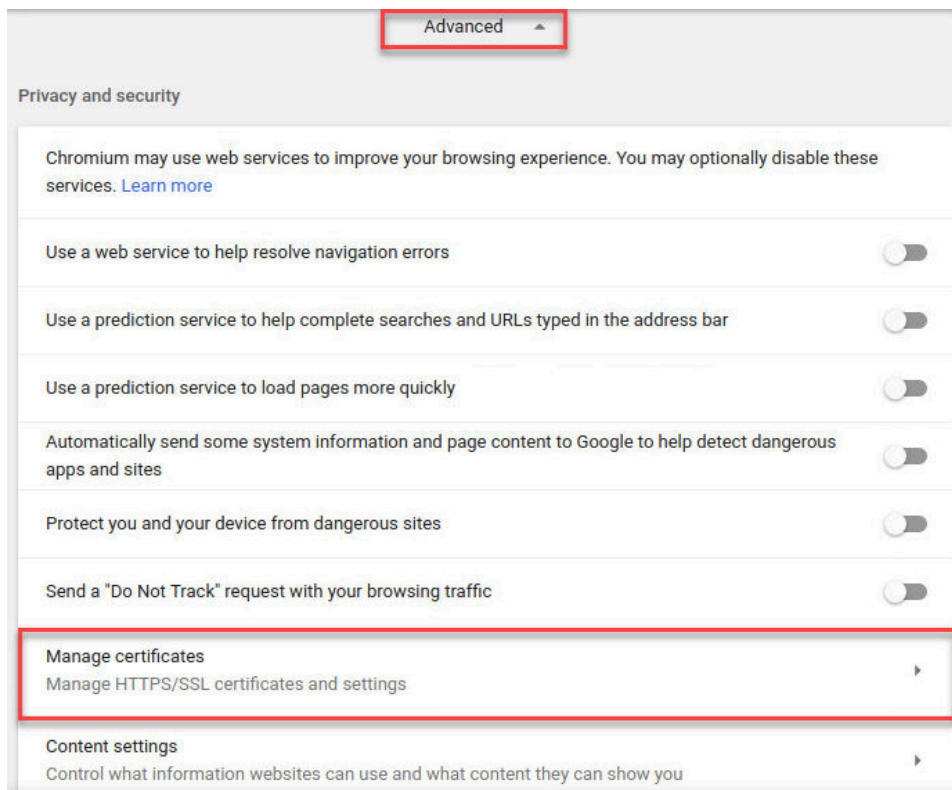
6. To install the *lab-user* certificate, open **Chromium** from the taskbar.



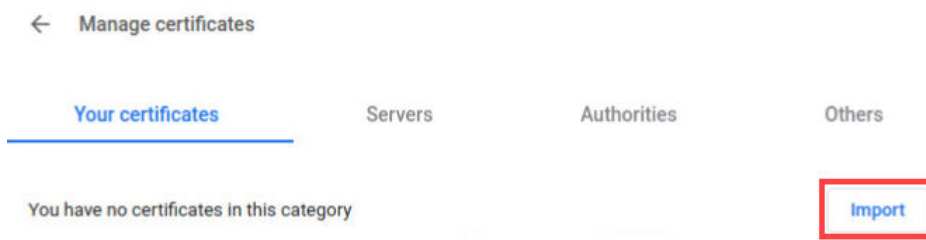
7. Click on the **ellipsis** icon and open the **Settings** in *Chromium*.



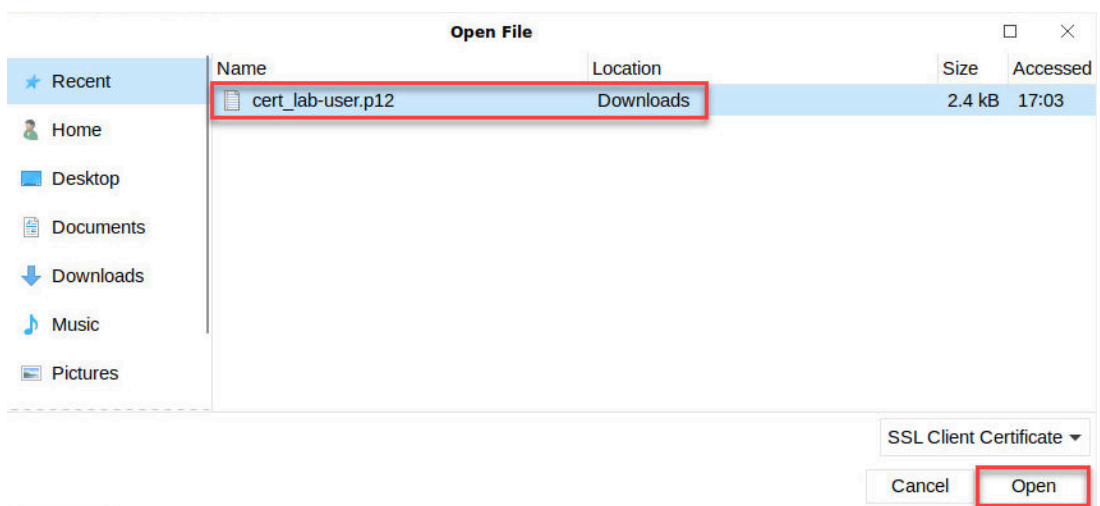
8. Scroll down and click on the **Advanced** settings in *Chromium* and then click on **Manage Certificates**.



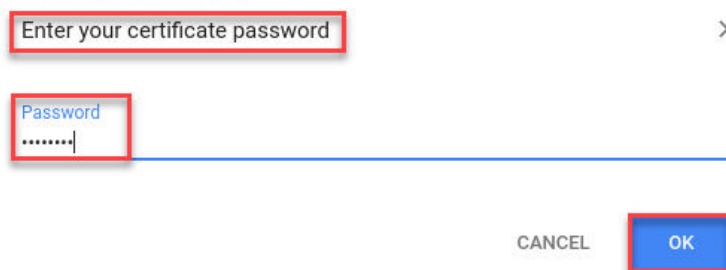
9. In the *Manage Certificates* window, click **Import**.



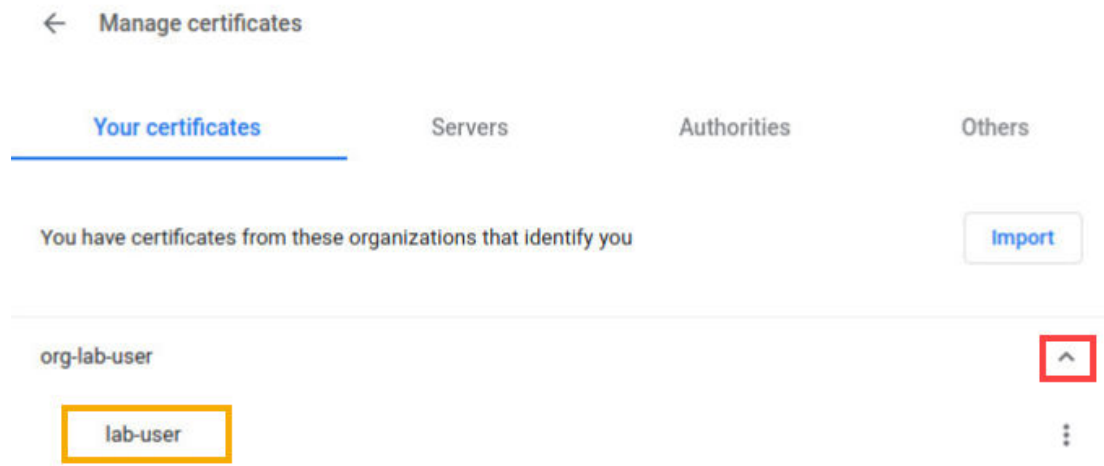
10. In the *Open File* window, select **cert_lab-user.p12** and then click the **Open** button.



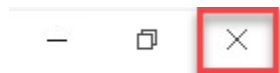
11. In the *Enter your certificate password* window, enter **paloalto** and click **OK**.



12. In the *Manage Certificates* window, expand the **org-lab-user** view and verify the **lab-user** certificate has been imported.



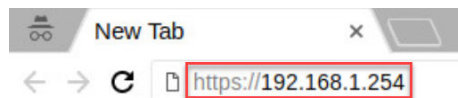
13. Click the **X** in the upper-right to close *Chromium*.



14. Open **Chromium** from the taskbar.



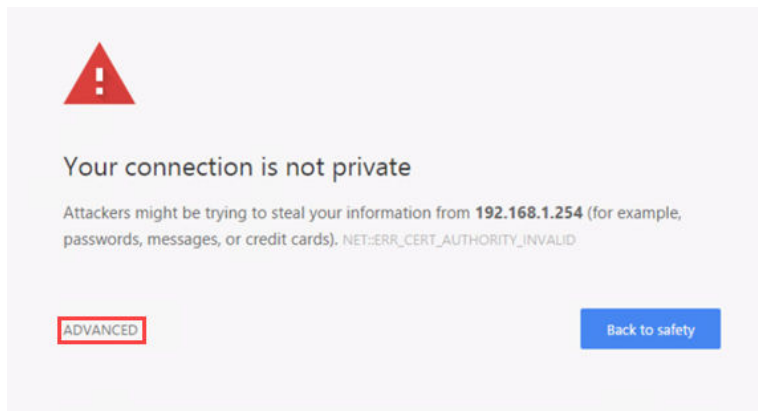
15. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.



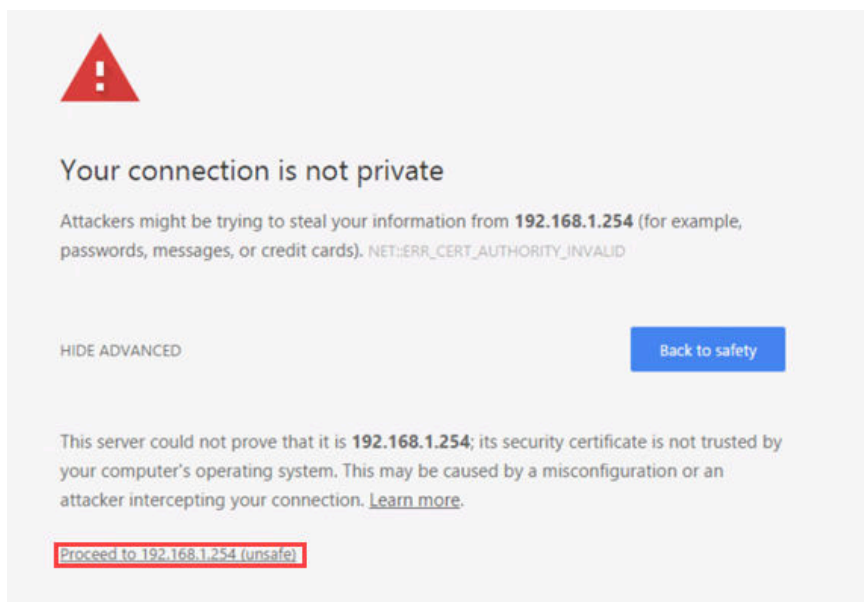
16. In the *Select a certificate* window, verify the **lab-user** certificate is selected and click **OK**.



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



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



19. The Firewall login window will be displayed. Type `Pa10Alt0` for the *Password* field. Then, click the **Log In** button.

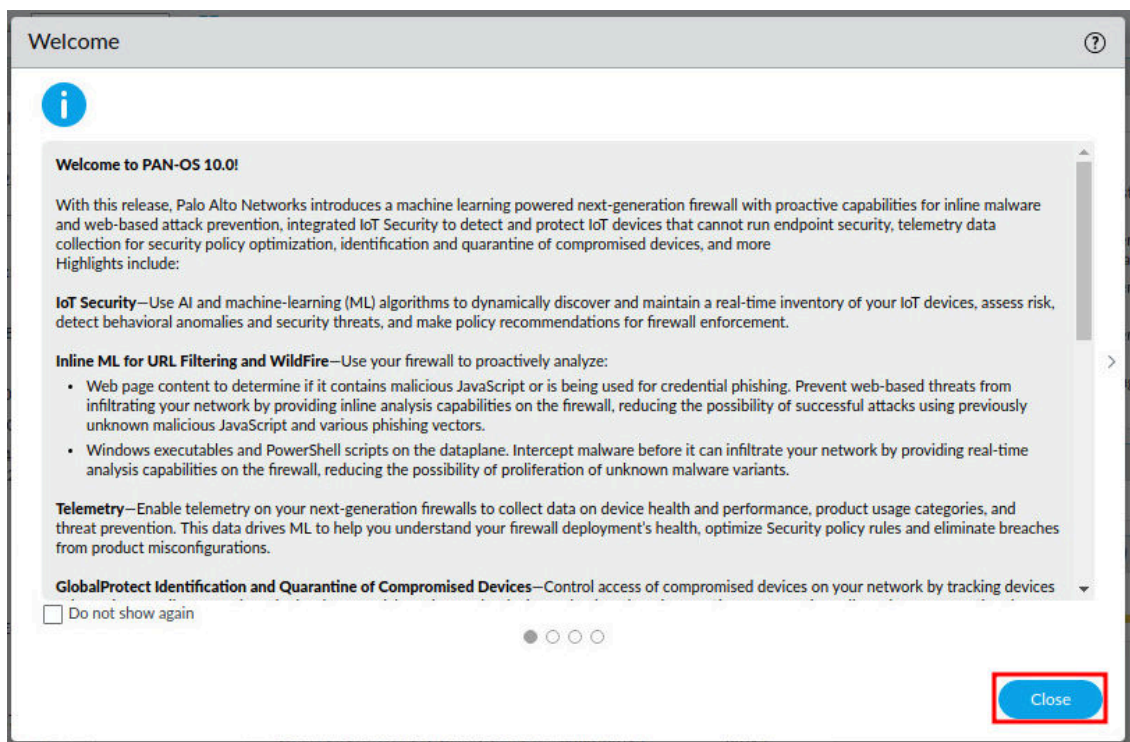


The image shows the Palo Alto Networks Firewall login window. It features the Palo Alto Networks logo at the top. Below the logo, there is a text input field for the username, which is pre-populated with "lab-user". Below the username field is a password field, represented by a series of dots, which is highlighted with a red rectangle. At the bottom of the login window is a blue "Log In" button, also highlighted with a red rectangle.

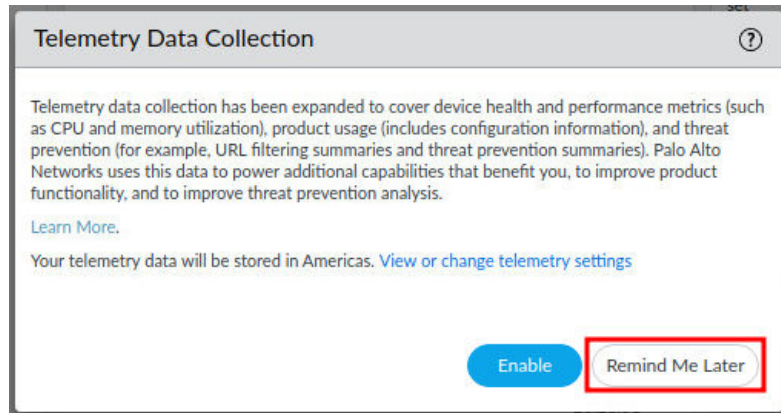


Notice that *lab-user* is pre-populated for the Username because the Certificate Profile you created earlier used the subject, common-name for the Username field.

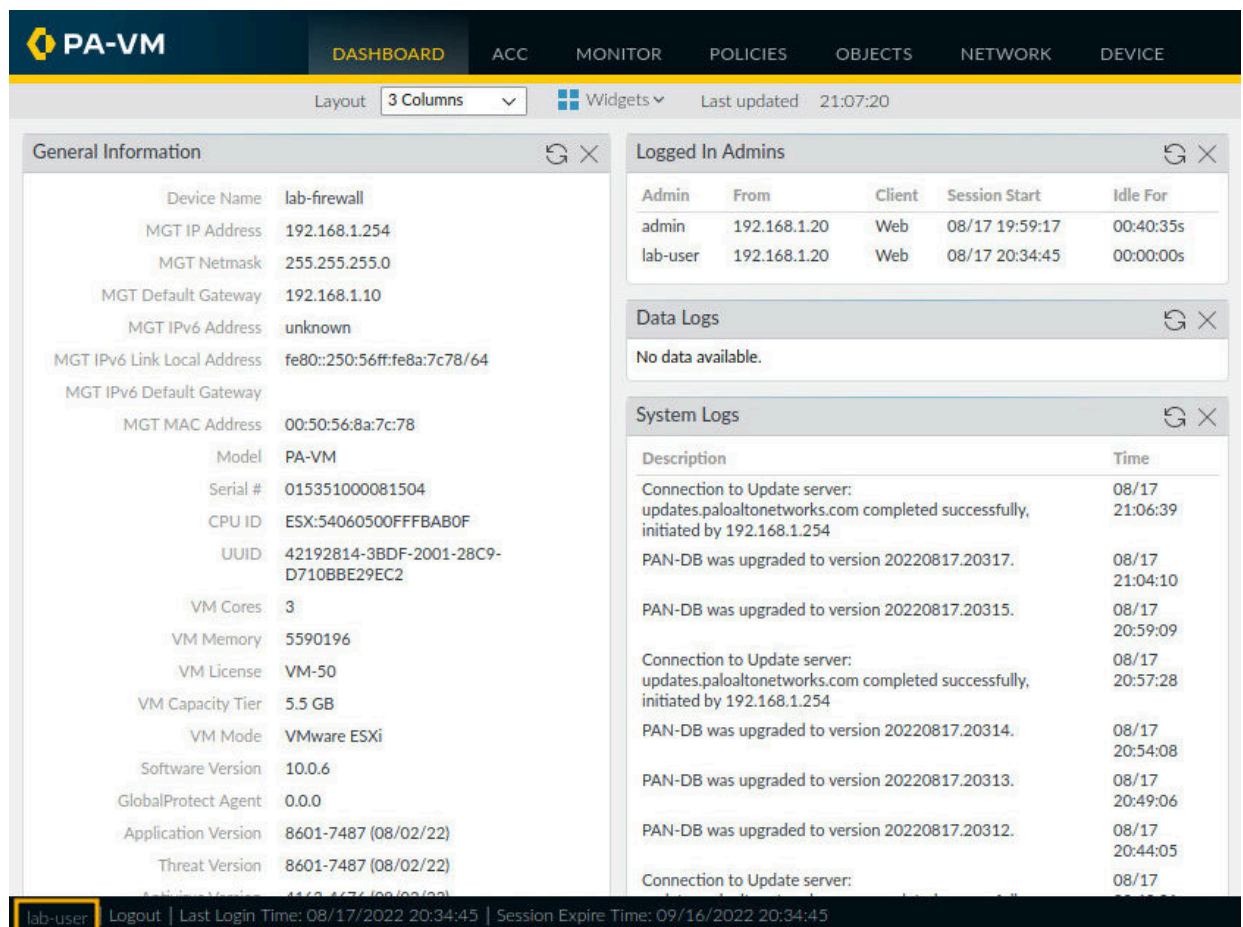
20. On the *Welcome* window, click the **Close** button.



21. If you see the *Telemetry Data Collection* window, click the **Remind Me Later** button.



22. You are now at the *Palo Alto Networks Web GUI*, logged on as *lab-user*. Notice the username in the lower-left.



23. The lab is now complete; you may end the reservation.