



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

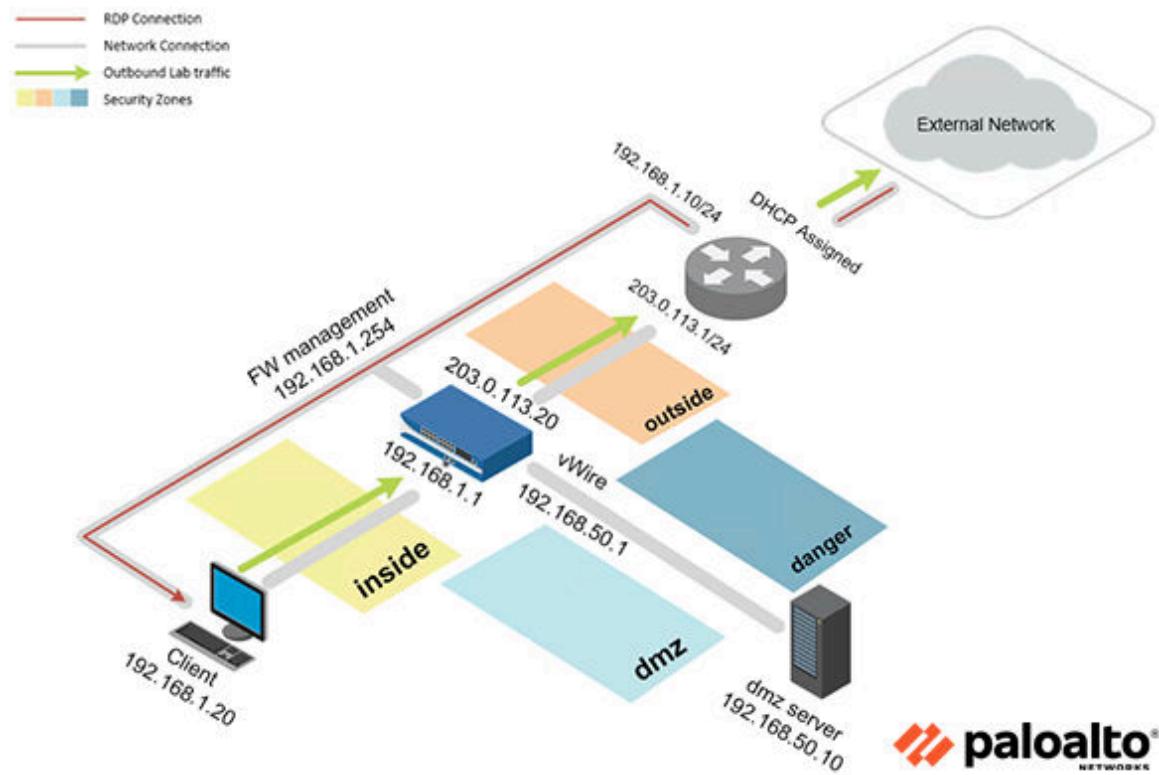
In this lab, you will configure the Firewall to use two-factor authentication using a certificate, along with a username and password.

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	PaloAlt0!
DMZ	192.168.50.10	root	PaloAlt0!
Firewall	192.168.1.254	admin	PaloAlt0!

1 Using Two-Factor Authentication to Secure the Firewall

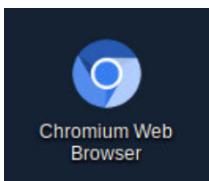
1.0 Load Lab Configuration

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

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



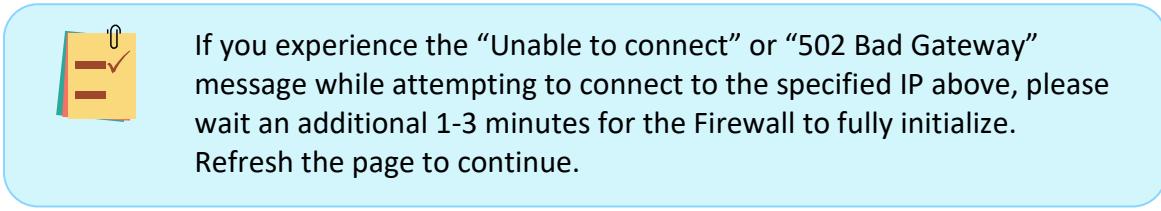
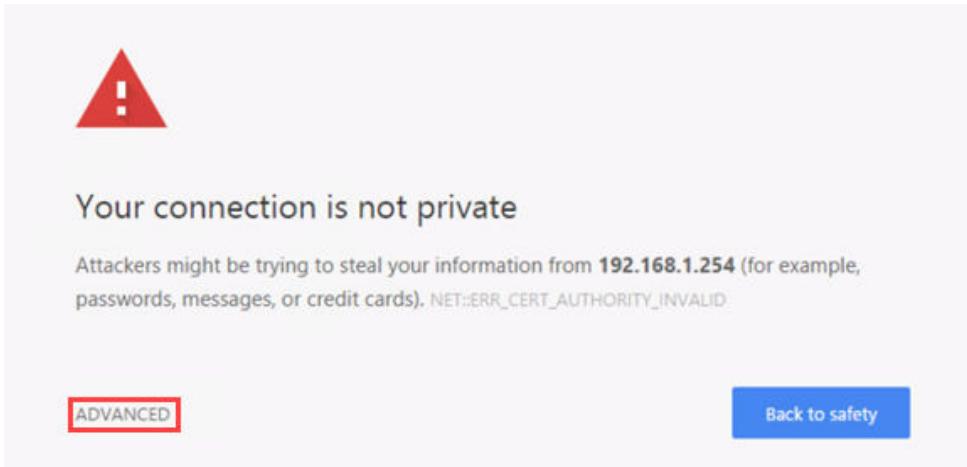
2. Log in to the **Client** PC as username lab-user, password Pal0Alt0!.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



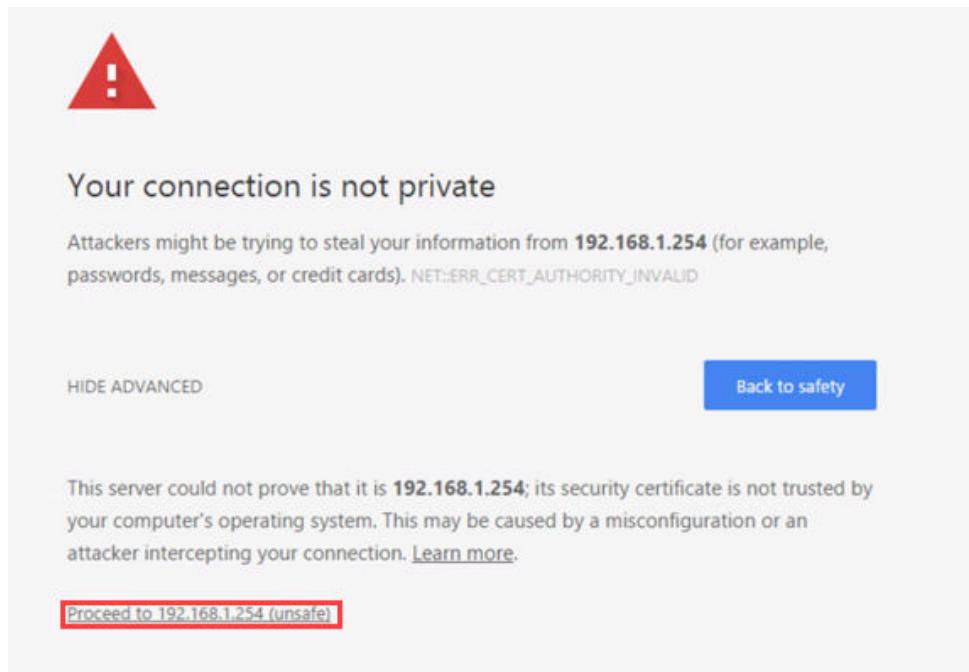
4. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.



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



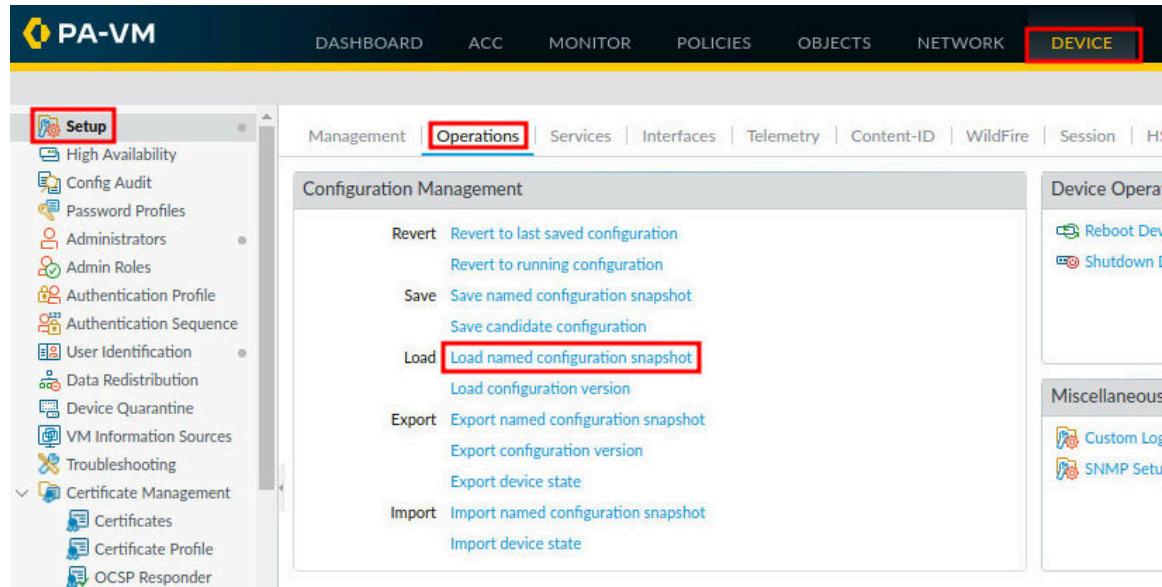
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



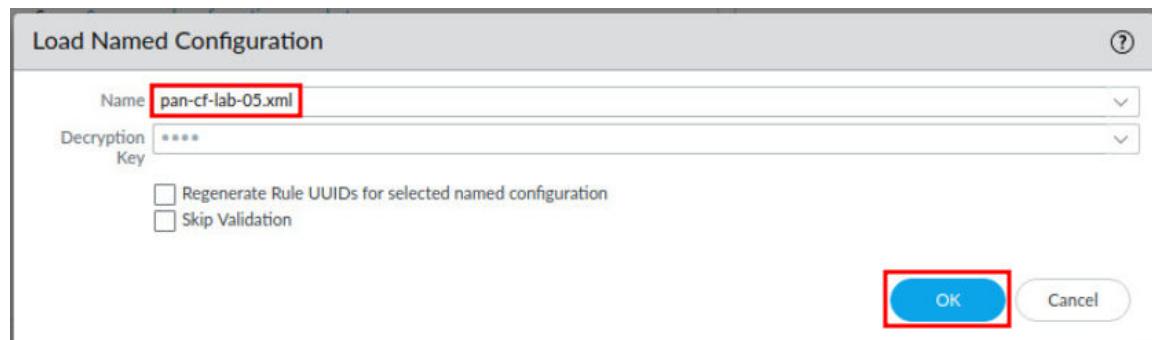
7. Log in to the Firewall web interface as username admin, password PaloAlt0!.



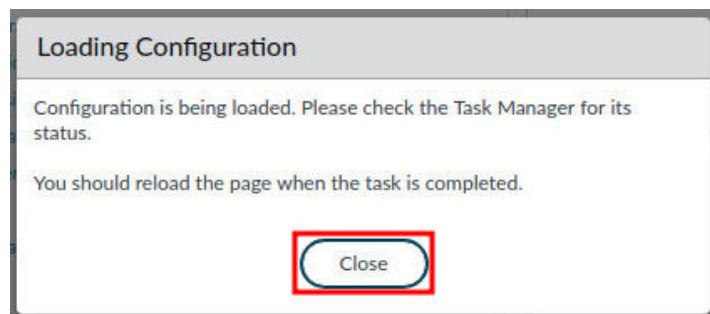
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



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



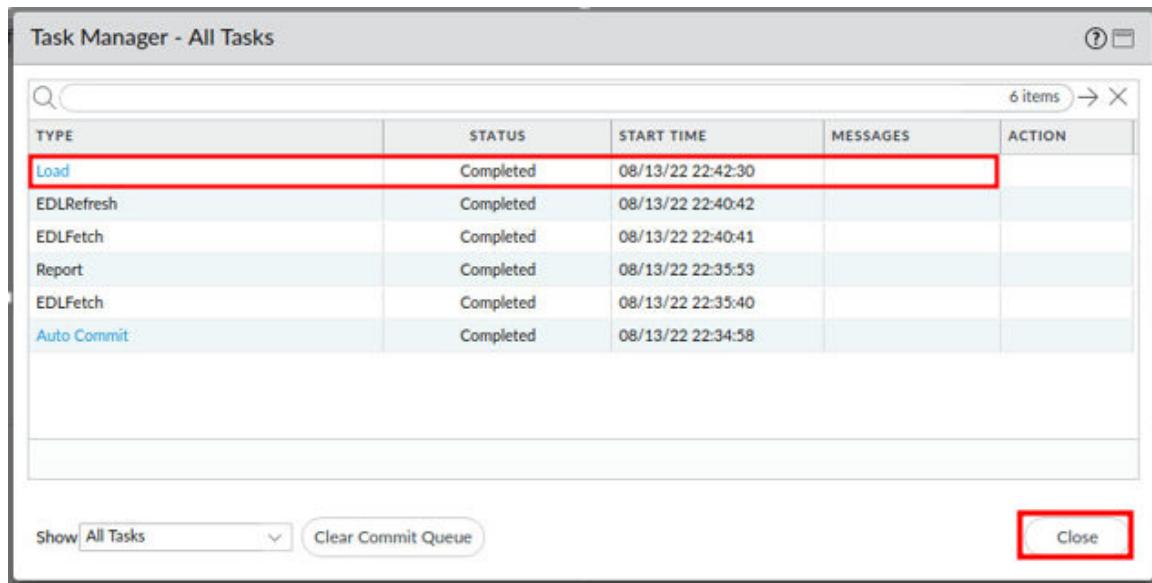
10. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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**.

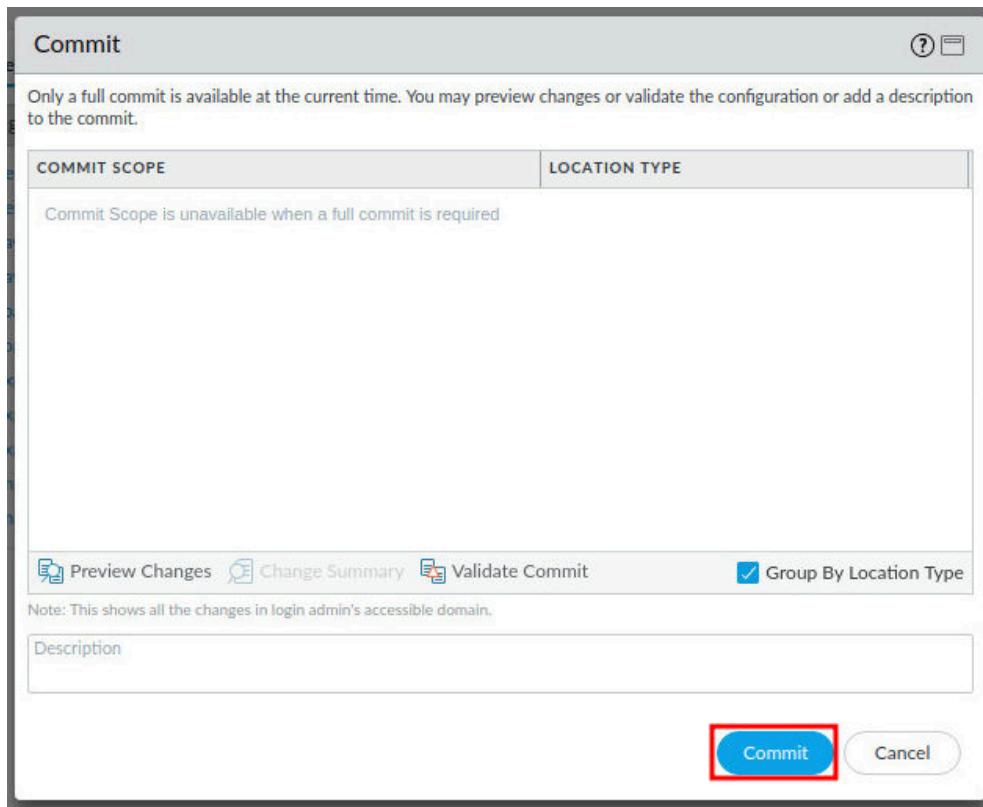


TYPE	STATUS	START TIME	MESSAGES	ACTION
Load	Completed	08/13/22 22:42:30		
EDLRefresh	Completed	08/13/22 22:40:42		
EDLFetch	Completed	08/13/22 22:40:41		
Report	Completed	08/13/22 22:35:53		
EDLFetch	Completed	08/13/22 22:35:40		
Auto Commit	Completed	08/13/22 22:34:58		

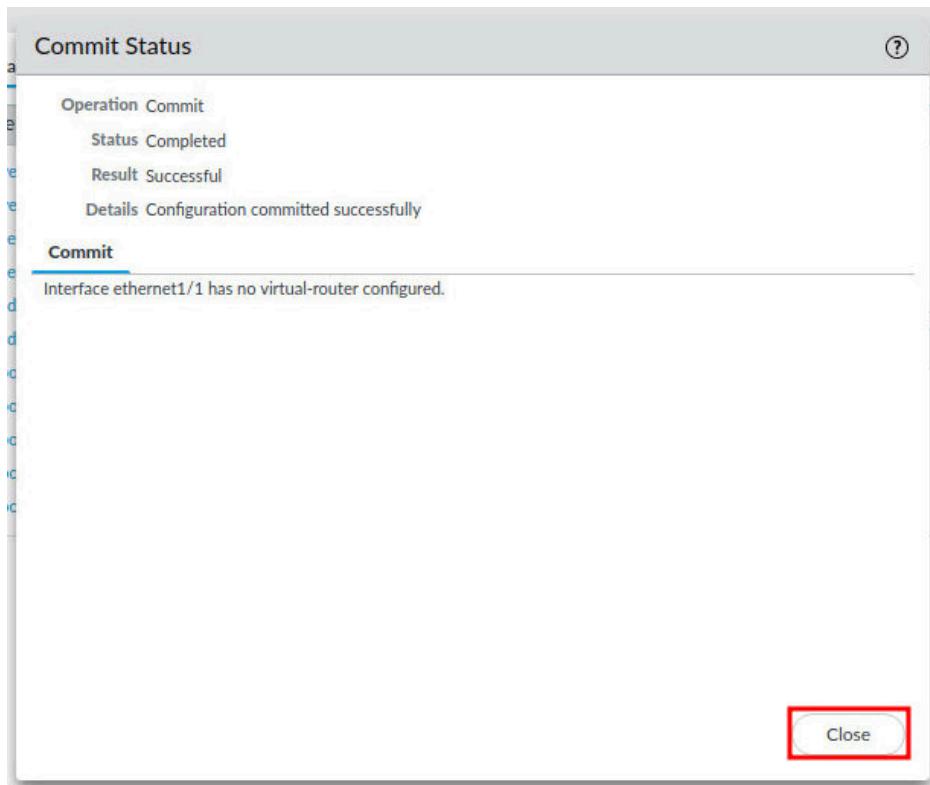
13. Click the **Commit** link located at the top-right of the web interface.



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



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



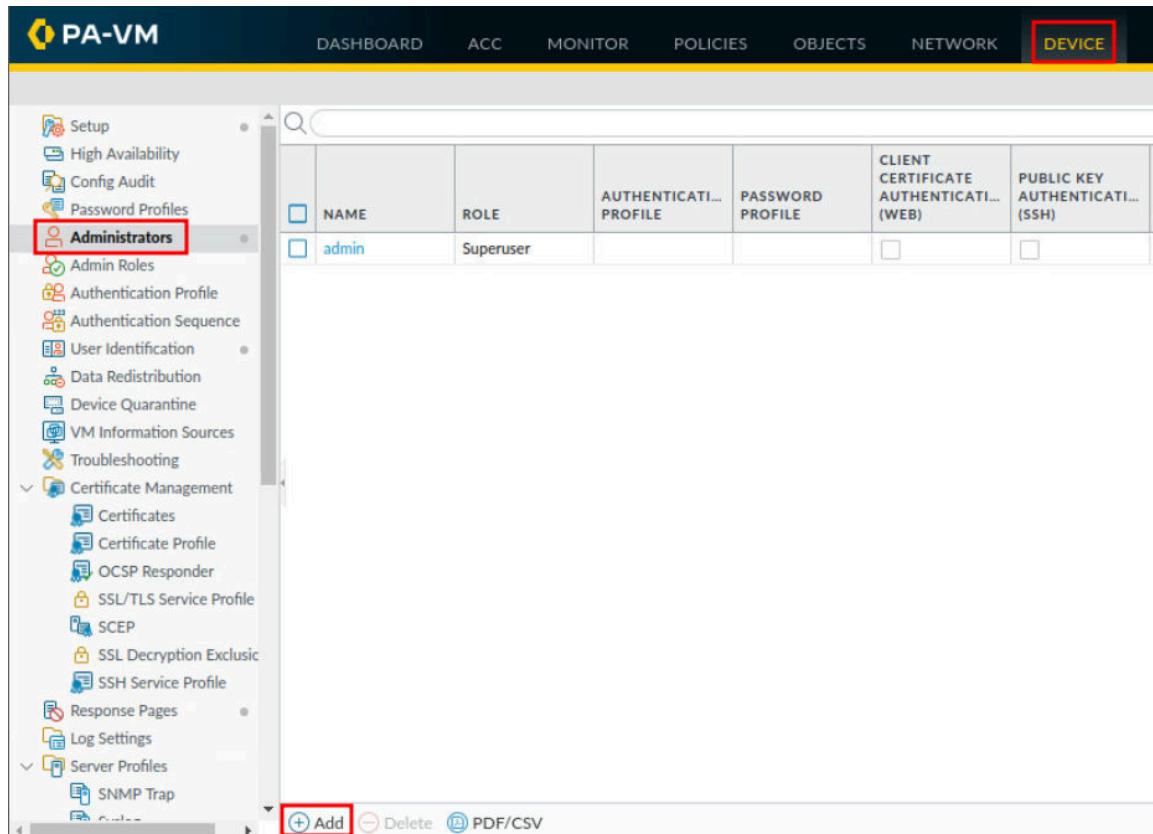


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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.

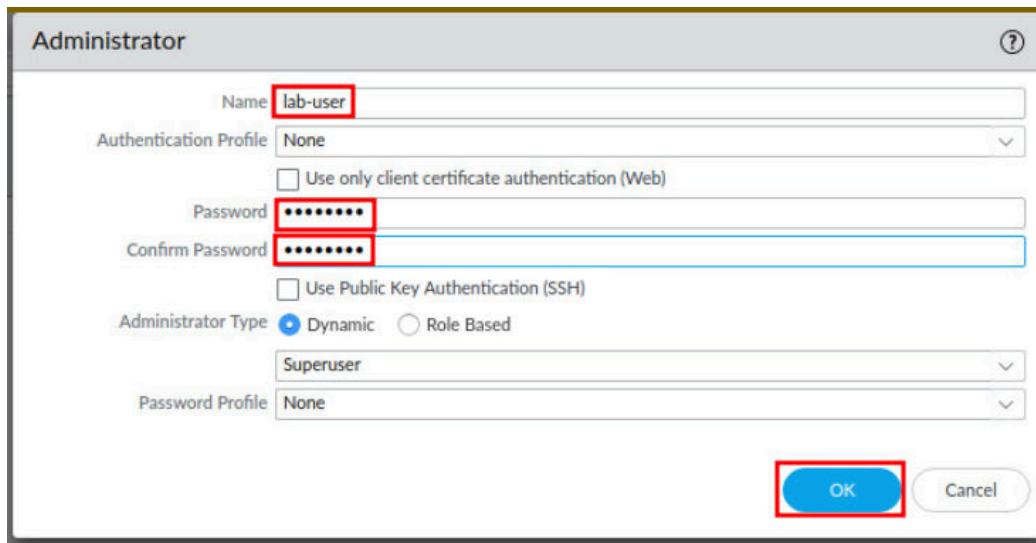
1. Navigate to **Device > Administrators > Add**.



The screenshot shows the PA-VM interface with the 'DEVICE' tab selected. On the left, the 'Administrators' option is highlighted with a red box. At the bottom of the interface, there is a red box around the '+ Add' button. The main area displays a table with one row, showing a user named 'admin' with a role of 'Superuser'. The table columns are: NAME, ROLE, AUTHENTICATI..., PROFILE, PASSWORD PROFILE, CLIENT CERTIFICATE AUTHENTICATI..., and PUBLIC KEY AUTHENTICATI... (SSH).

NAME	ROLE	AUTHENTICATI...	PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI...	PUBLIC KEY AUTHENTICATI...
admin	Superuser					

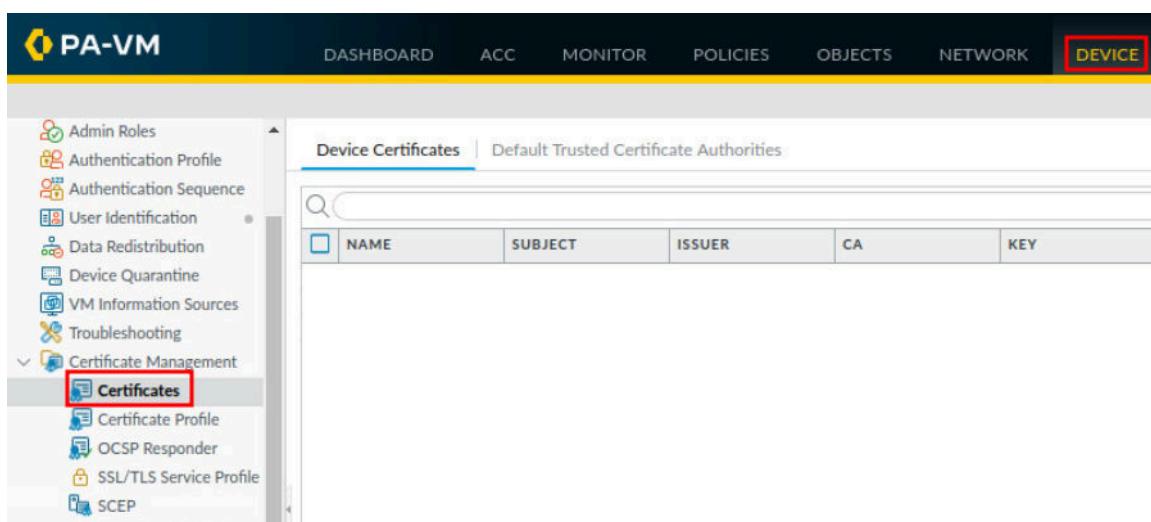
2. In the *Administrator* window, type **lab-user** in the *Name* field. Then, type **Pal0Alt0** in the *Password* and *Confirm Password* fields. Finally, click the **OK** button.



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**.

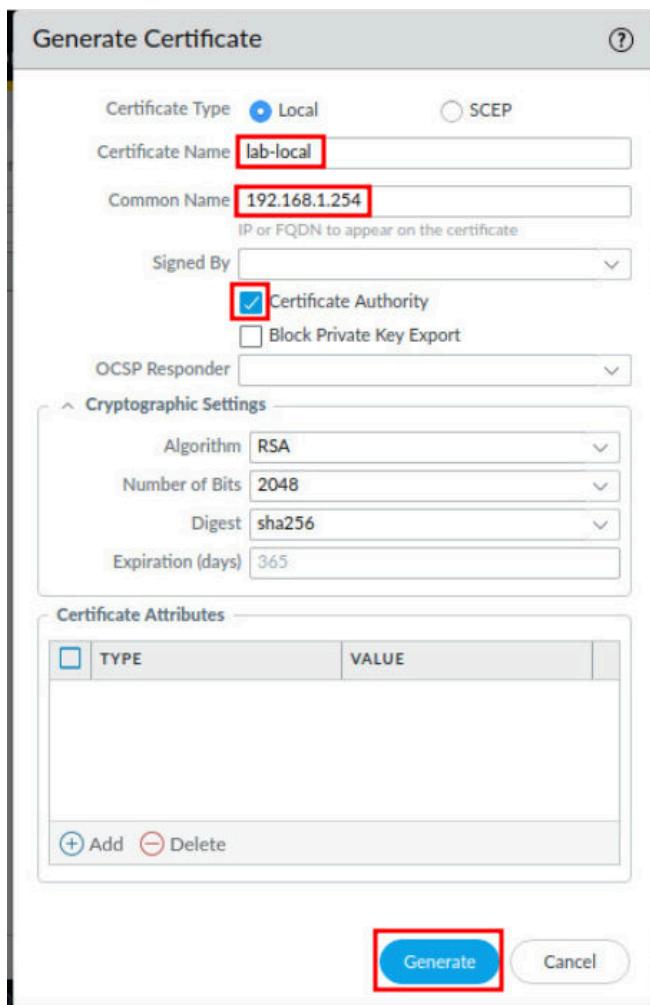
1. Navigate to **Device > Certificate Management > Certificates**.



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



3. 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.



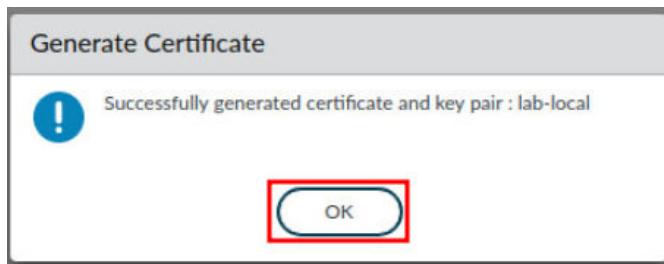
The screenshot shows the 'Generate Certificate' dialog box. It has the following settings:

- Certificate Type:** Local (selected)
- Certificate Name:** lab-local (highlighted with a red box)
- Common Name:** 192.168.1.254 (highlighted with a red box)
- Signed By:** (dropdown menu)
- Certificate Authority:** (highlighted with a red box)
- Block Private Key Export:**
- OCSP Responder:** (dropdown menu)
- Cryptographic Settings:**
 - Algorithm:** RSA
 - Number of Bits:** 2048
 - Digest:** sha256
 - Expiration (days):** 365
- Certificate Attributes:** A table with columns: TYPE and VALUE. It contains no rows.
- Buttons:** Generate (highlighted with a red box) and Cancel.



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*.

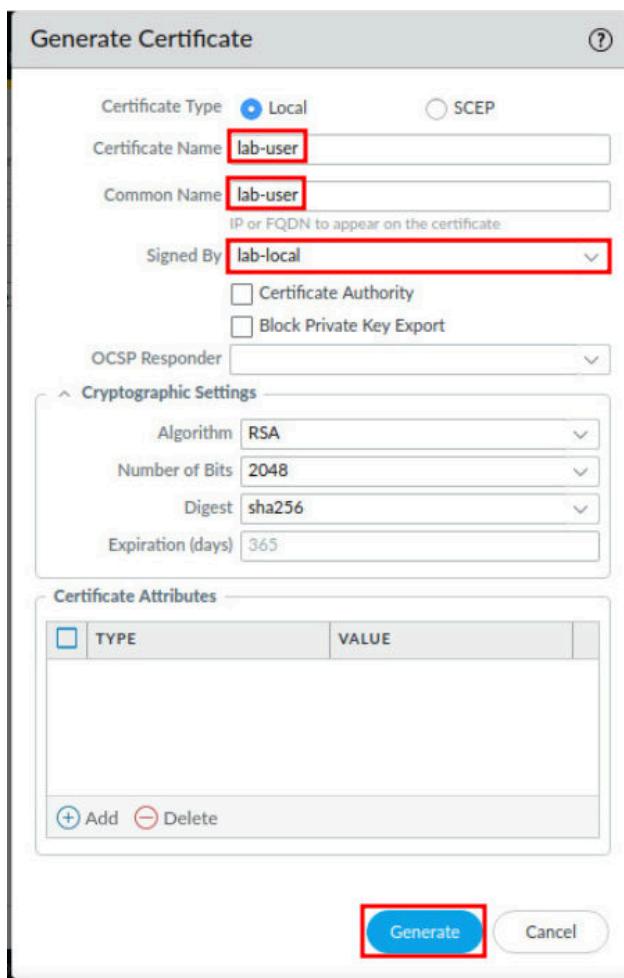
4. In the *Generate Certificate* window, click **OK** to continue.



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.

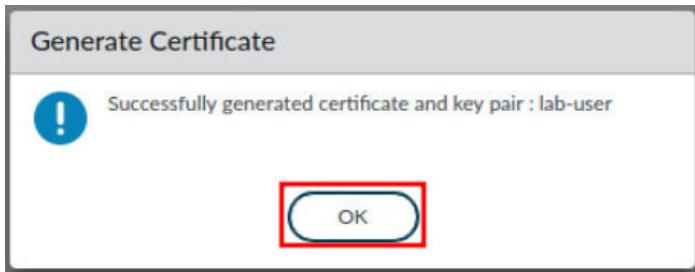


The screenshot shows the 'Generate Certificate' configuration window. The 'Certificate Type' is set to 'Local'. The 'Certificate Name' and 'Common Name' fields both contain 'lab-user'. The 'Signed By' dropdown is set to 'lab-local'. Under 'Cryptographic Settings', the algorithm is 'RSA', number of bits is '2048', digest is 'sha256', and expiration is '365'. The 'Certificate Attributes' section is empty. At the bottom, the 'Generate' button is highlighted with a red rectangle.



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.

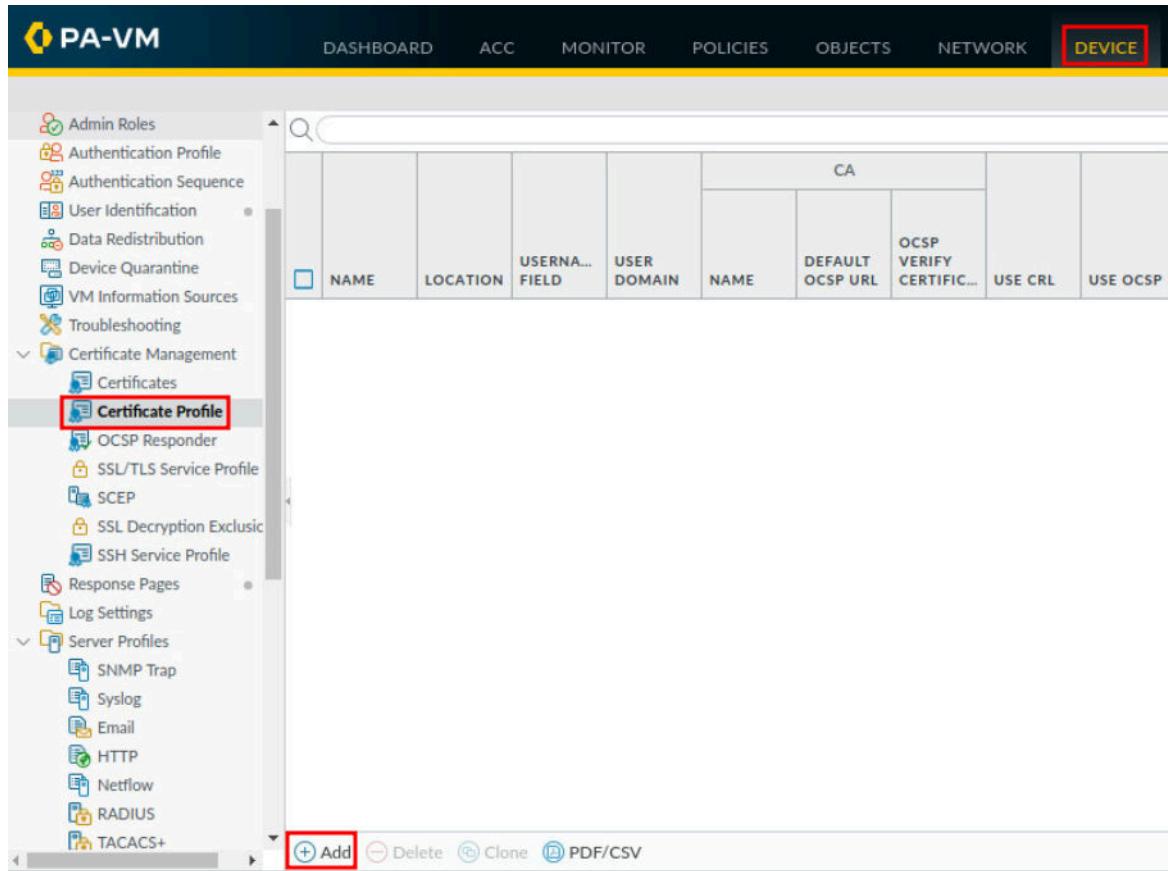
7. In the *Generate Certificate* window, click **OK** to continue.



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**.



The screenshot shows the PA-VM Device Management interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE (which is highlighted with a red box). On the left, a sidebar menu lists various management categories: Admin Roles, Authentication Profile, Authentication Sequence, User Identification, Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting, Certificate Management (which is expanded), Certificates, Certificate Profile (highlighted with a red box), OCSP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusive, SSH Service Profile, Response Pages, Log Settings, Server Profiles (expanded), SNMP Trap, Syslog, Email, HTTP, Netflow, RADIUS, and TACACS+. At the bottom of the sidebar, there are buttons for '+ Add', 'Delete', 'Clone', and 'PDF/CSV'. The main content area features a search bar and a table titled 'CA'. The table has columns for NAME, LOCATION, USERNA... FIELD, USER DOMAIN, NAME, DEFAULT OCSP URL, OCSP VERIFY CERTIFIC..., USE CRL, and USE OCSP. There is also a column header 'CA' with sub-headers for NAME, DEFAULT OCSP URL, OCSP VERIFY CERTIFIC..., USE CRL, and USE OCSP.

2. In the *Certification 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' dialog box. The 'Name' field contains 'Cert-Local-Profile'. The 'Username Field' dropdown is set to 'Subject', which is highlighted with a red box. Below the dropdown, the 'common-name' value is shown. The 'CA Certificates' section is empty. At the bottom, there is an 'Add' button with a red box around it, along with other buttons for 'Delete', 'Move Up', and 'Move Down'. Configuration options for OCSP and CRL are listed, along with several checkboxes for session blocking based on certificate status. 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' dialog box. The 'CA Certificate' dropdown is set to 'lab-local', which is highlighted with a red box. Other fields include 'Default OCSP URL', 'OCSP Verify Certificate' (set to 'None'), and 'Template Name/OID'. The 'OK' button is highlighted with a red box, while the 'Cancel' button is not.



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*.

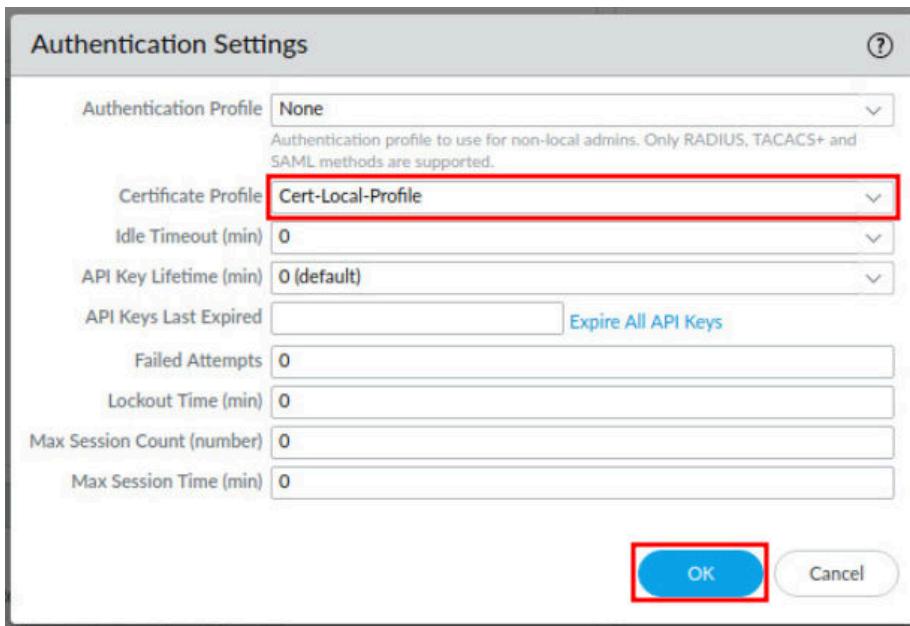
- In the *Certificate Profile* window, click the **OK** button.

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

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



7. In the *Authentication Settings* window, select **Cert-Local-Profile** for the *Certification 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**.

The screenshot shows the PA-VM interface with the 'DEVICE' tab selected. In the left sidebar under 'Certificate Management', the 'Certificates' option is highlighted with a red box. The main pane displays a table of device certificates. The 'lab-user' certificate is selected, indicated by a checked checkbox in the first column. The table columns are NAME, SUBJECT, ISSUER, CA, KEY, and EXPIRES. The 'lab-user' row shows CN = lab-user and CN = 192.168.1.254 for both SUBJECT and ISSUER, with the CA and KEY checkboxes checked.

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

The screenshot shows the PA-VM interface with the 'DEVICE' tab selected. The 'Certificates' table shows the 'lab-user' certificate selected, indicated by a checked checkbox in the first column. The 'Export Certificate' button at the bottom of the table is highlighted with a red box. The table columns are NAME, SUBJECT, ISSUER, CA, KEY, and EXPIRES. The 'lab-user' row shows CN = lab-user and CN = 192.168.1.254 for both SUBJECT and ISSUER, with the CA and KEY checkboxes checked.

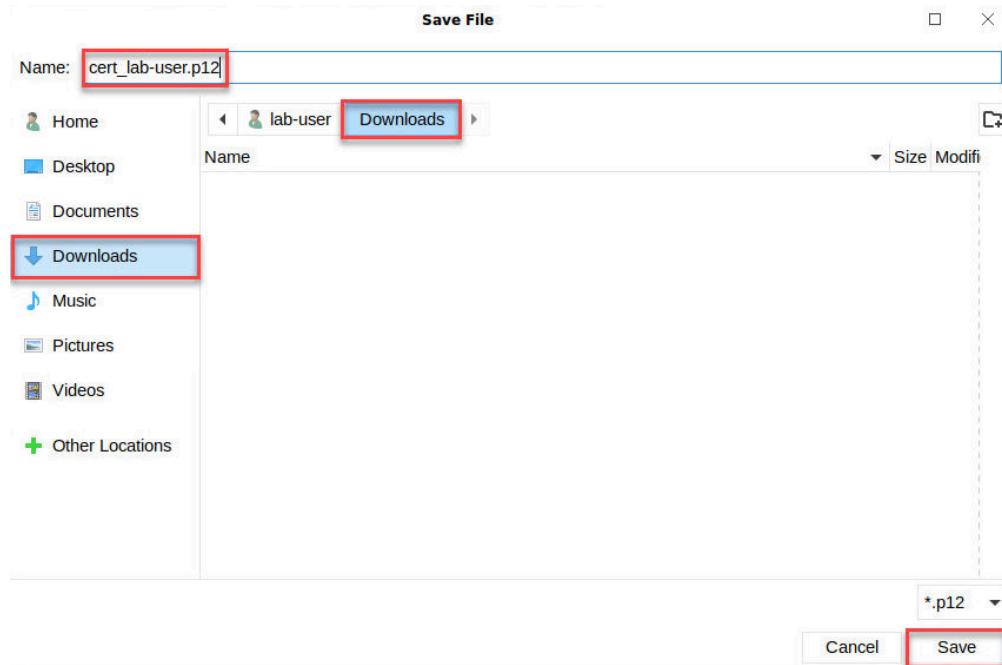
3. In the *Export Certificate - lab-user* window, select **Encrypted Private Key and Certificate (PKCS12)** in the *File Format* dropdown. Then, type **paloalto** for the *Passphrase* and *Confirm Passphrase* fields, then click on the **OK** button.

The screenshot shows the 'Export Certificate - lab-user' dialog box. The 'File Format' dropdown is set to 'Encrypted Private Key and Certificate (PKCS12)'. The 'Passphrase' and 'Confirm Passphrase' fields both contain the value 'paloalto'. The 'OK' button at the bottom right is highlighted with a red box.

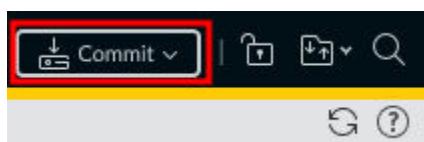


By using an *Encrypted Private Key and Certificate*, this creates an additional security measure, as the passphrase is required to install the certificate on a client machine.

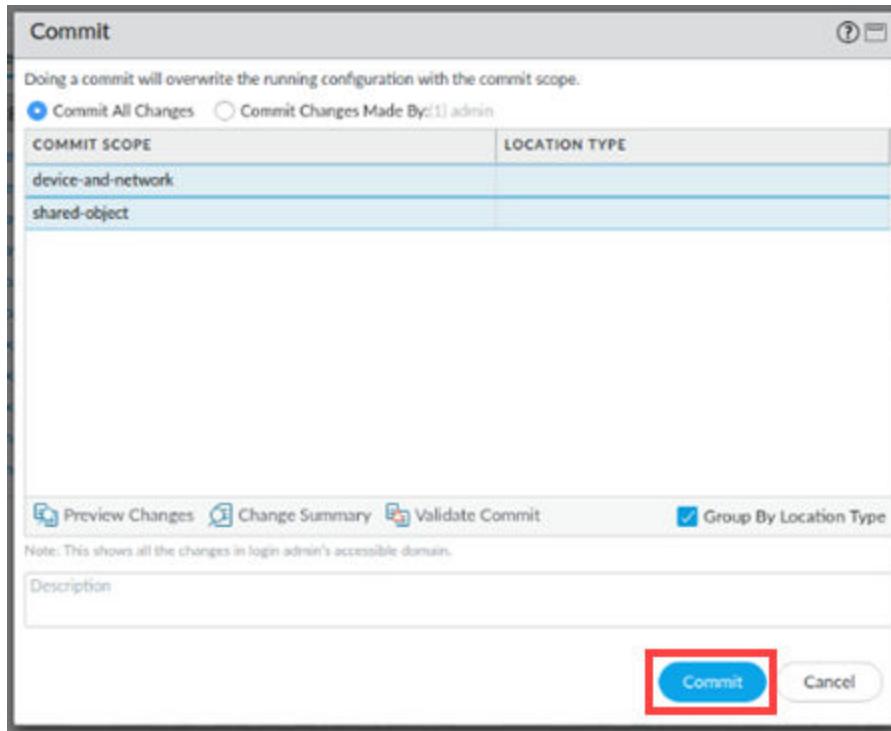
4. In the *Save File* window pop-up, verify the name of ***cert_lab-user.p12*** is correct in the *Name* field, verify the **.p12** file is being saved in the **Downloads** folder, and click **Save**.



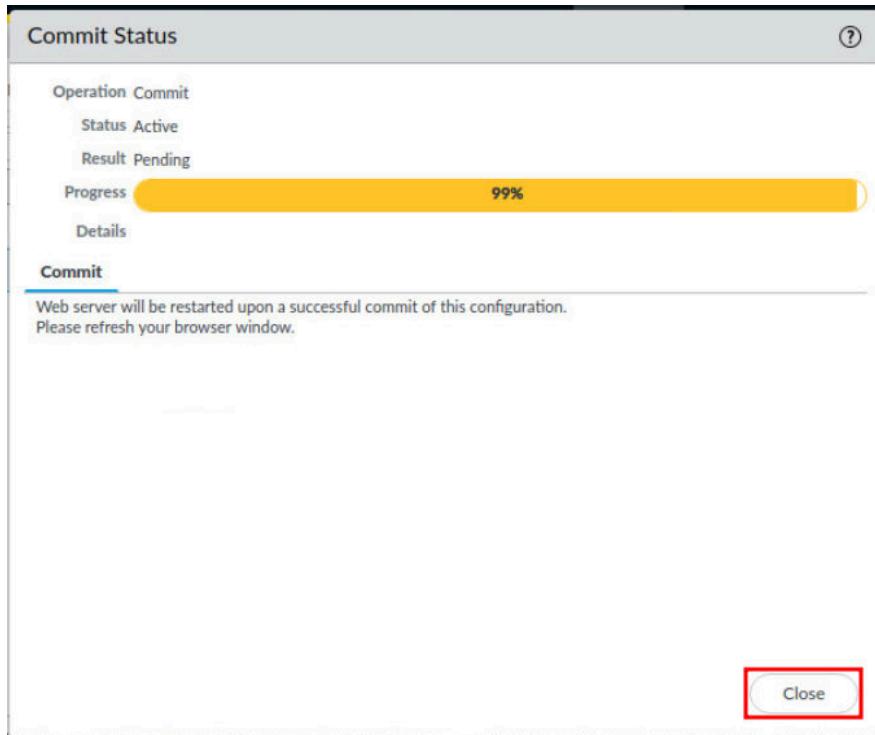
5. Click the **Commit** link located at the top-right of the web interface.



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*.



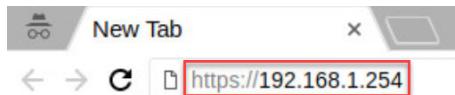
1.5 Test Connectivity and Import Certificate on the Client

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.

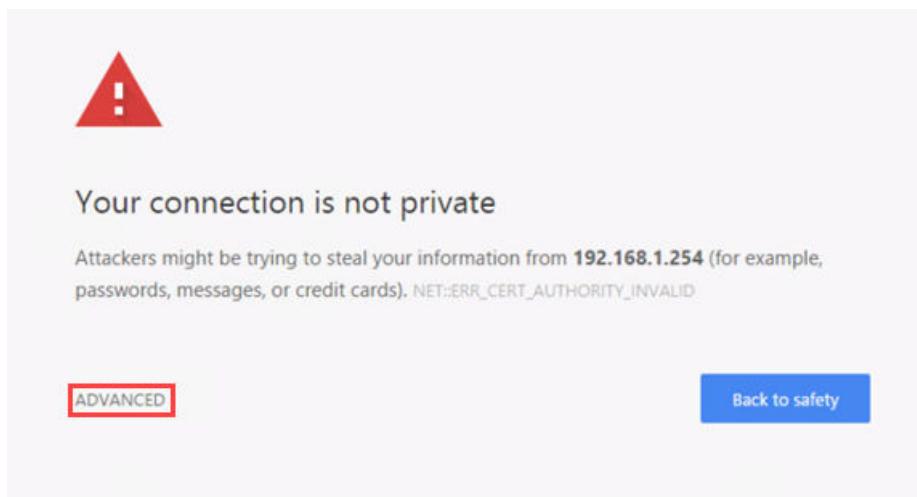
1. Open **Chromium** from the taskbar.



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



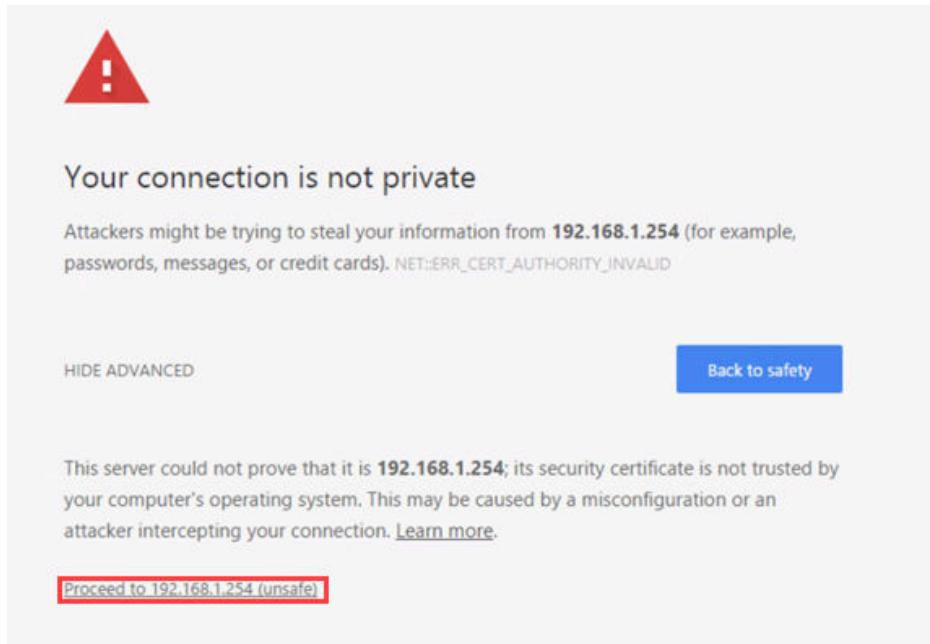
3. You will see a “*Your connection is not private*” message. Click on the **ADVANCED** Link.



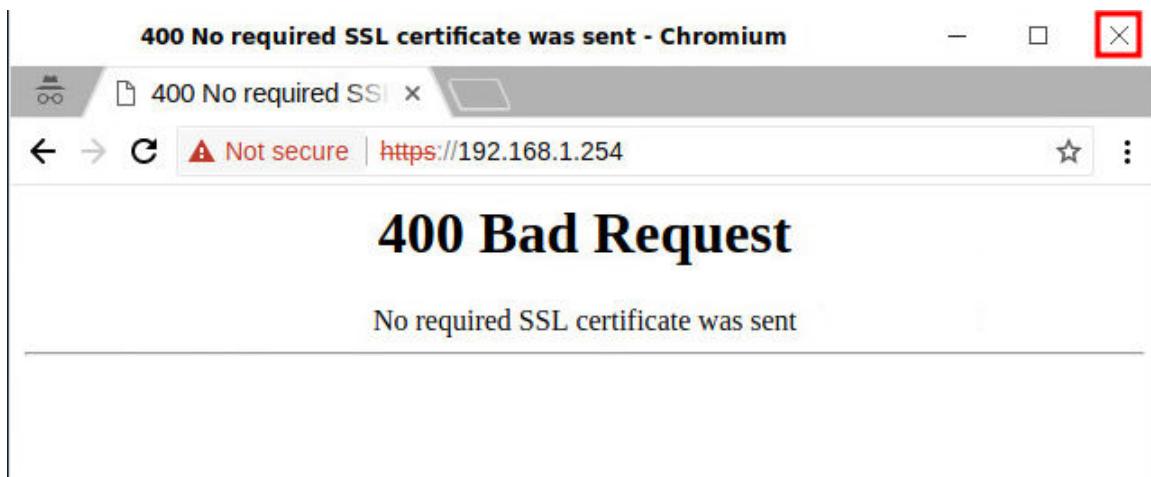


This message is displayed because the Firewall has a self-signed certificate by default. The client does not have a Certificate Authority that can validate the certificate.

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



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

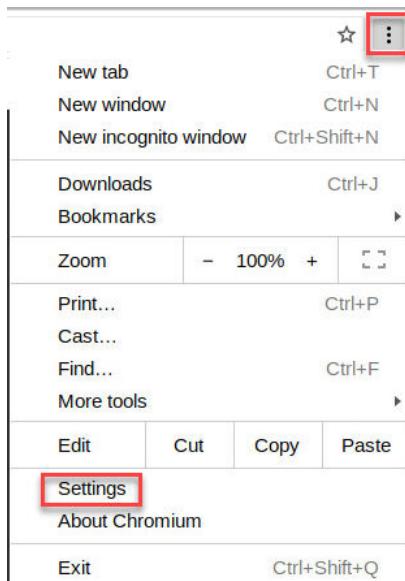


Notice you get a *HTTP 400 Bad Request* error. This is because the *lab-user* certificate is not installed on the *Client* machine. The Firewall administrators are not allowed to login unless they have the certificate installed and have an account and password. These two factors make up the Two-Factor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

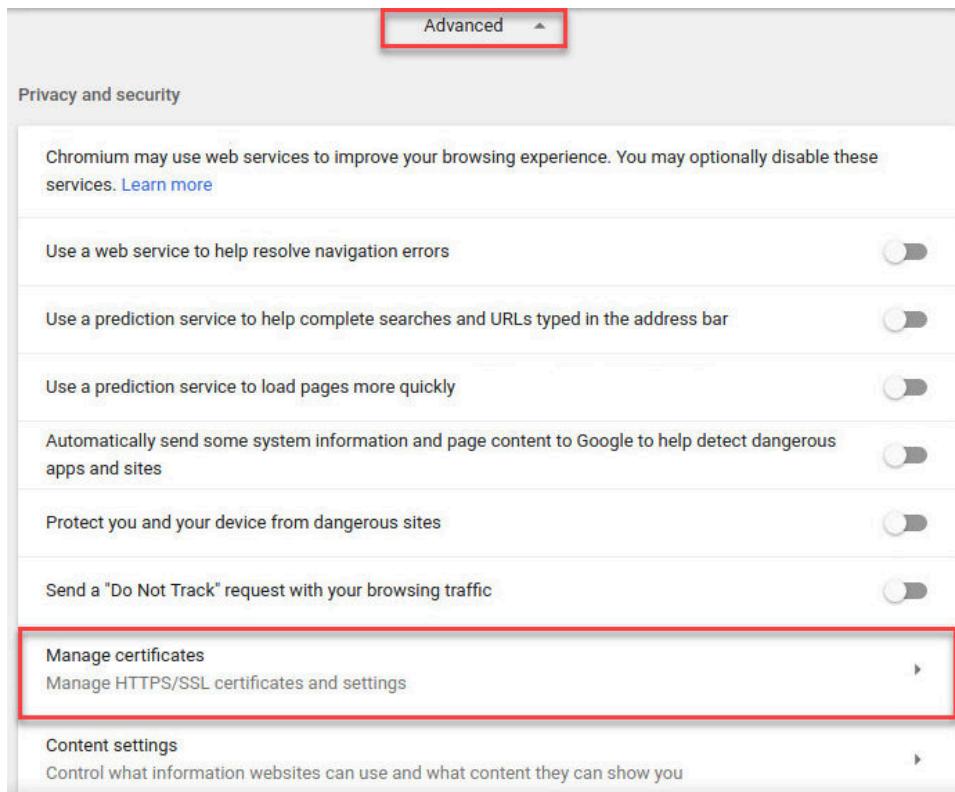
6. To install the *lab-user* certificate, open **Chromium** from the taskbar.



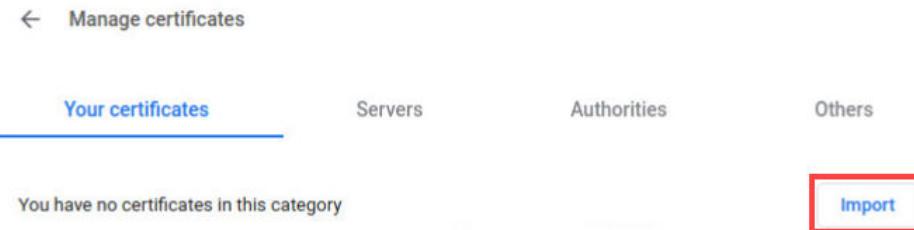
7. Click on the **ellipsis** icon and open the **Settings** in *Chromium*.



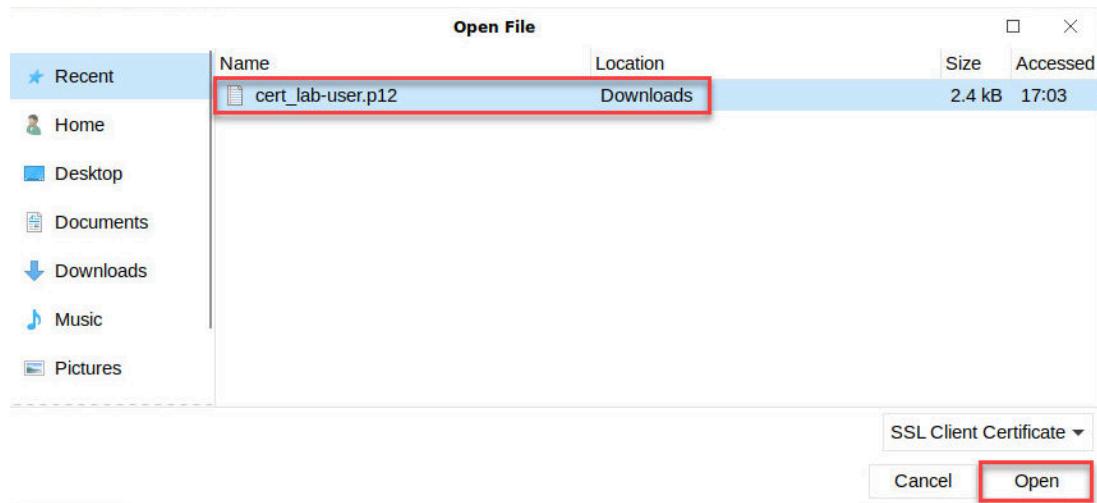
8. Scroll down and click on the **Advanced** settings in *Chromium* and then click on **Manage Certificates**.

A screenshot of the Chromium Privacy and security settings page. At the top, there's a 'Privacy and security' section with a note about web services and a 'Learn more' link. Below it are several toggle switches for various privacy features: 'Use a web service to help resolve navigation errors' (off), 'Use a prediction service to help complete searches and URLs typed in the address bar' (off), 'Use a prediction service to load pages more quickly' (off), 'Automatically send some system information and page content to Google to help detect dangerous apps and sites' (off), 'Protect you and your device from dangerous sites' (off), and 'Send a "Do Not Track" request with your browsing traffic' (off). Further down, there's a section titled 'Manage certificates' with a sub-option 'Manage HTTPS/SSL certificates and settings'. This entire 'Manage certificates' section is highlighted with a large red rectangular box. Below it is another section titled 'Content settings' with a sub-option 'Control what information websites can use and what content they can show you'.

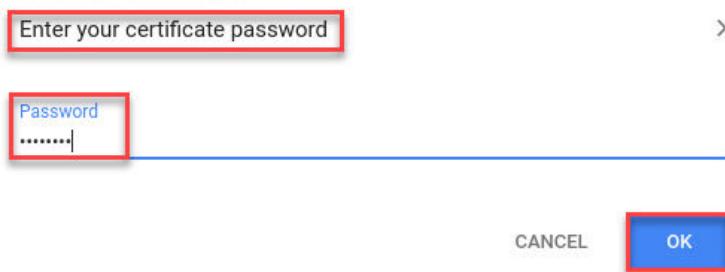
9. In the *Manage Certificates* window, click **Import**.



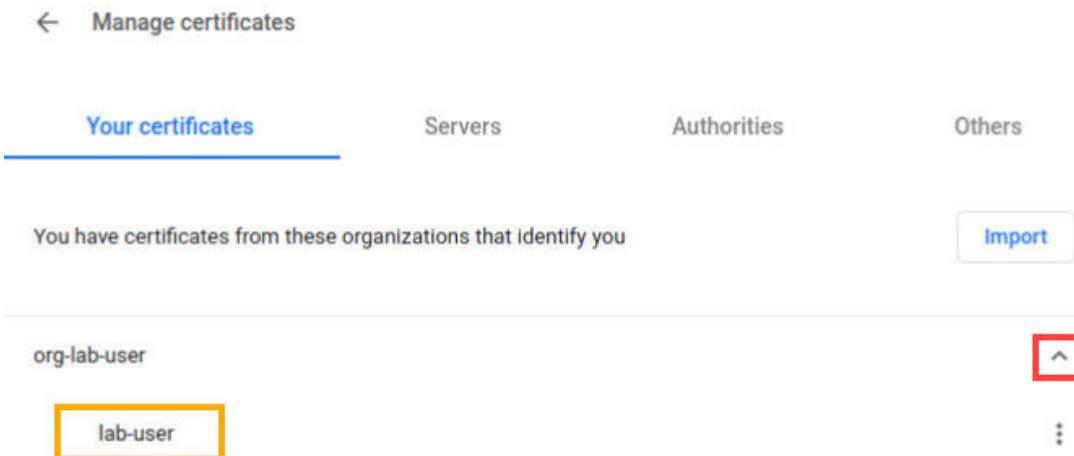
10. In the *Open File* window, select **cert_lab-user.p12** and then click the **Open** button.



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.



The screenshot shows the 'Manage certificates' interface. At the top, there are tabs: 'Your certificates' (which is selected and highlighted in blue), 'Servers', 'Authorities', and 'Others'. Below the tabs, a message says 'You have certificates from these organizations that identify you'. On the right, there's an 'Import' button. The main list area shows a group named 'org-lab-user' with an expand arrow (highlighted with a red box). Inside the group, a certificate named 'lab-user' is listed and highlighted with an orange box. There's also a three-dot menu icon next to it.

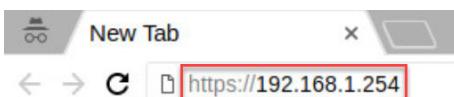
13. Click the X in the upper-right to close *Chromium*.



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



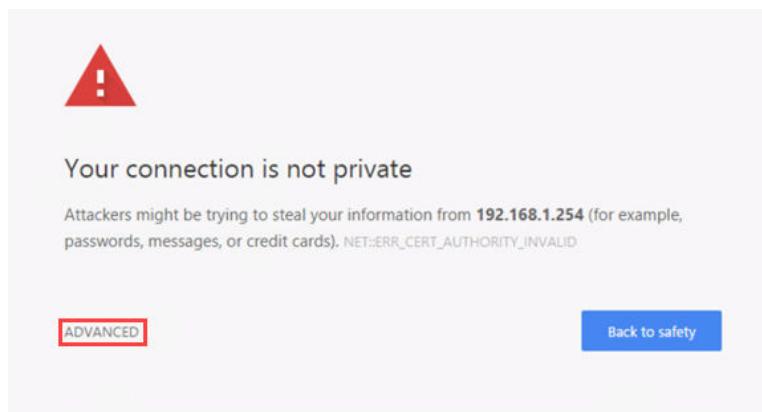
15. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.



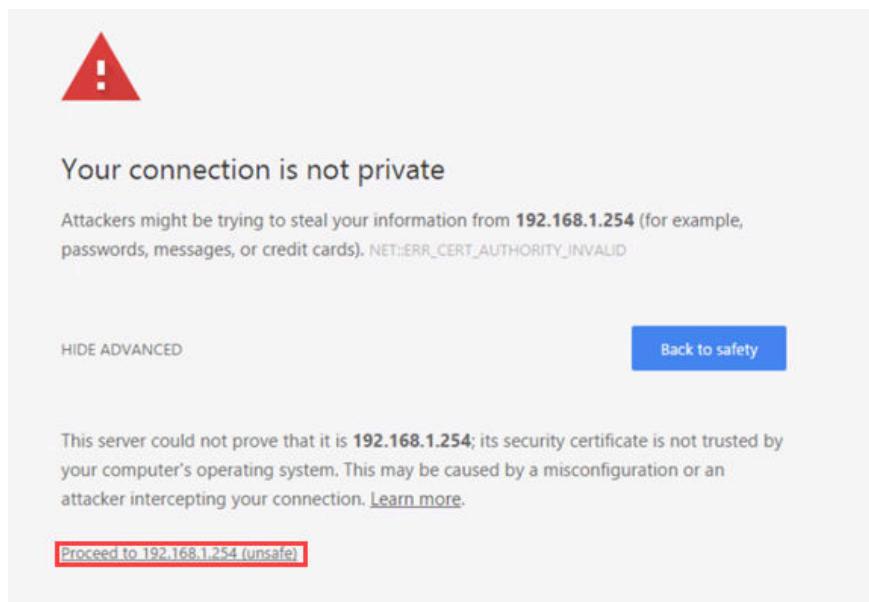
16. In the *Select a certificate* window, verify the **lab-user** certificate is selected and click **OK**.



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)**.

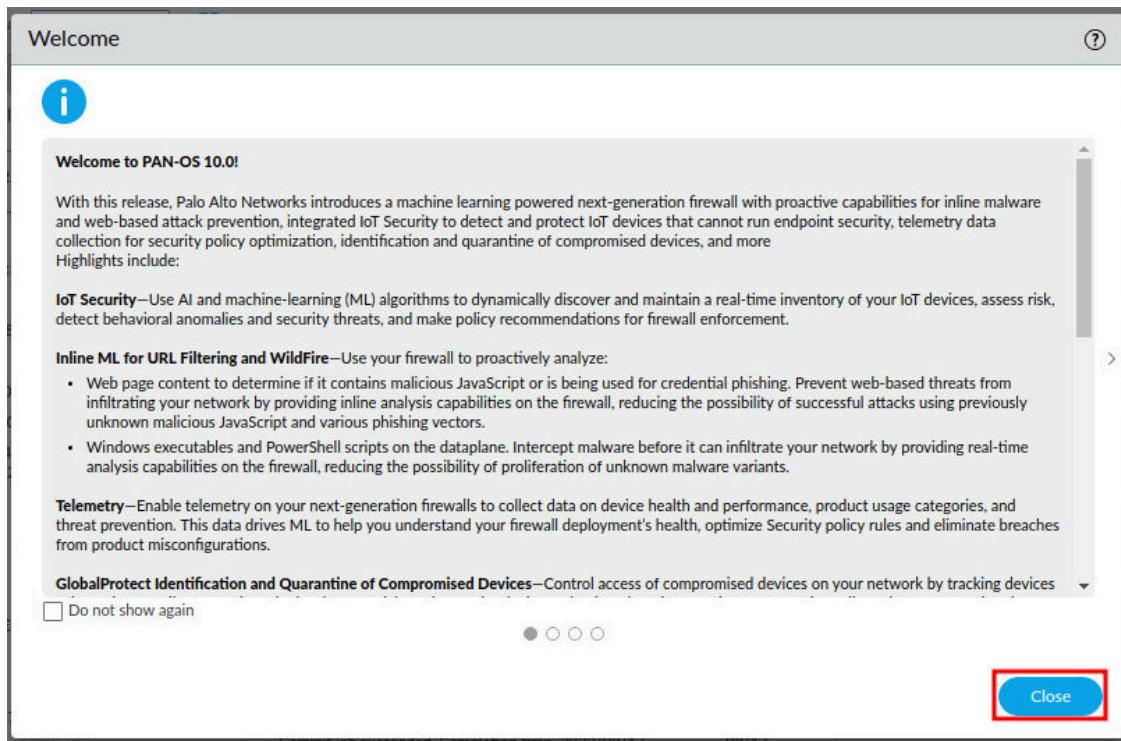


19. The Firewall login window will be displayed. Type PaloAlt0 for the *Password* field. Then, click the **Log In** button.

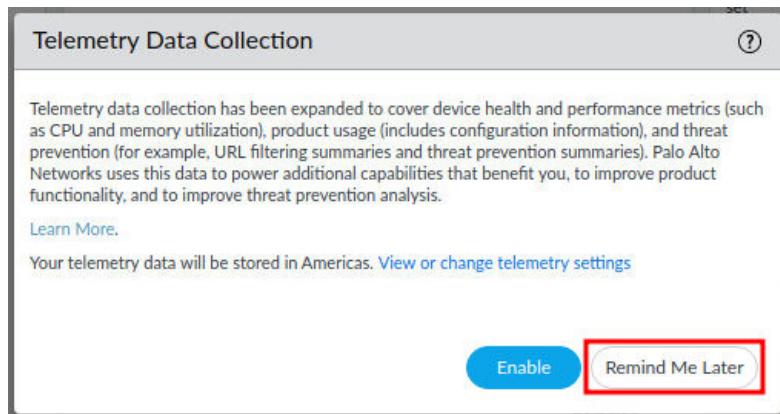


Notice that *lab-user* is pre-populated for the Username because the Certificate Profile you created earlier used the subject, common-name for the Username field.

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.

General Information				
Device Name	lab-firewall			
MGT IP Address	192.168.1.254			
MGT Netmask	255.255.255.0			
MGT Default Gateway	192.168.1.10			
MGT IPv6 Address	unknown			
MGT IPv6 Link Local Address	fe80::250:56ff:fe8a:7c78/64			
MGT IPv6 Default Gateway				
MGT MAC Address	00:50:56:8a:7c:78			
Model	PA-VM			
Serial #	015351000081504			
CPU ID	ESX:54060500FFFBAB0F			
UUID	42192814-3BDF-2001-28C9-D710BBE29EC2			
VM Cores	3			
VM Memory	5590196			
VM License	VM-50			
VM Capacity Tier	5.5 GB			
VM Mode	VMware ESXi			
Software Version	10.0.6			
GlobalProtect Agent	0.0.0			
Application Version	8601-7487 (08/02/22)			
Threat Version	8601-7487 (08/02/22)			

Logged In Admins				
Admin	From	Client	Session Start	Idle For
admin	192.168.1.20	Web	08/17 19:59:17	00:40:35s
lab-user	192.168.1.20	Web	08/17 20:34:45	00:00:00s

Data Logs				
No data available.				

System Logs				
Description	Time			
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254	08/17 21:06:39			
PAN-DB was upgraded to version 20220817.20317.	08/17 21:04:10			
PAN-DB was upgraded to version 20220817.20315.	08/17 20:59:09			
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254	08/17 20:57:28			
PAN-DB was upgraded to version 20220817.20314.	08/17 20:54:08			
PAN-DB was upgraded to version 20220817.20313.	08/17 20:49:06			
PAN-DB was upgraded to version 20220817.20312.	08/17 20:44:05			
Connection to Update server:	08/17			

lab-user | Logout | Last Login Time: 08/17/2022 20:34:45 | Session Expire Time: 09/16/2022 20:34:45

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