CYBERSECURITY FOUNDATION V2

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

Document Version: 2022-12-22

Contents

Introduction

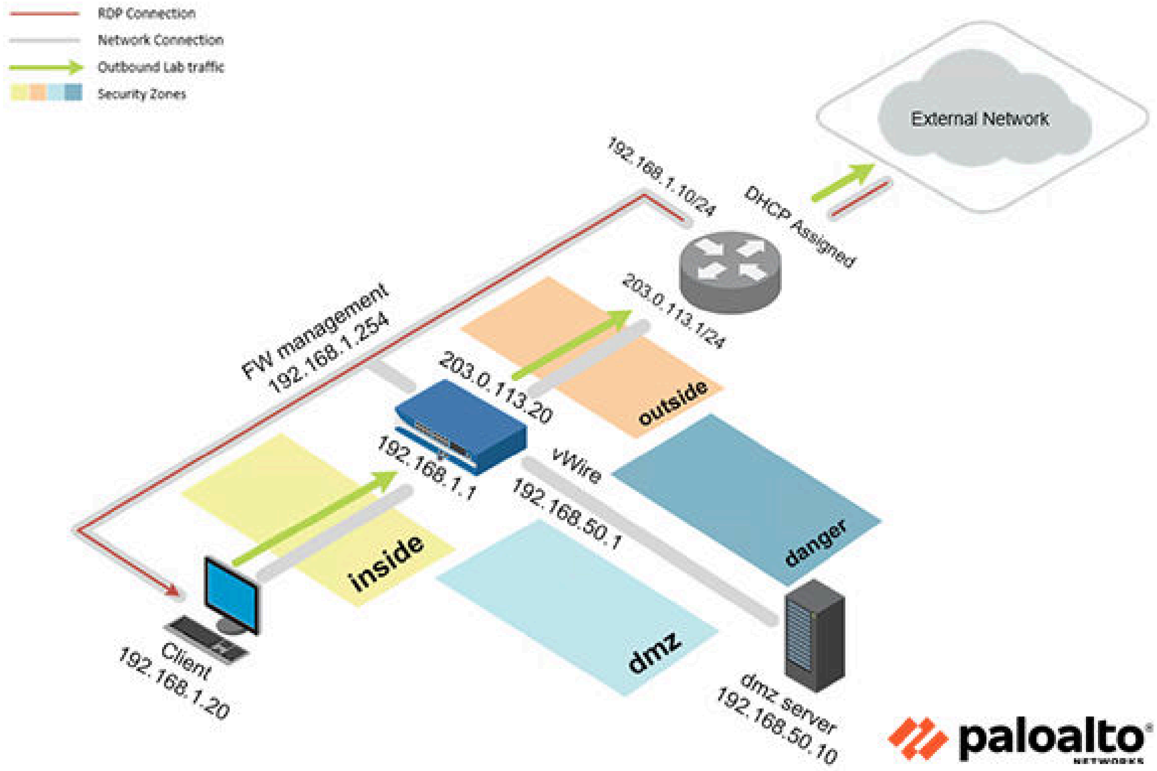
In this lab, you will configure the Firewall to use two-factor authentication using a certificate, along with a username and password.

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.

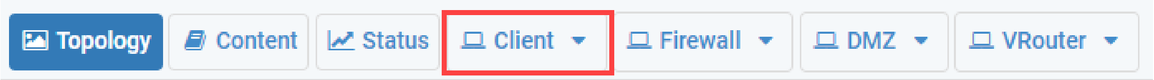
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Using Two-Factor Authentication to Secure the Firewall

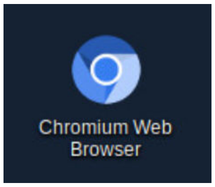
1.0 Load Lab Configuration

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

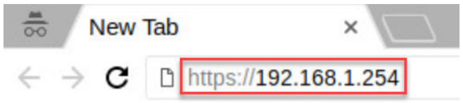
1. Click on the **Client** tab to access the *Client* PC.



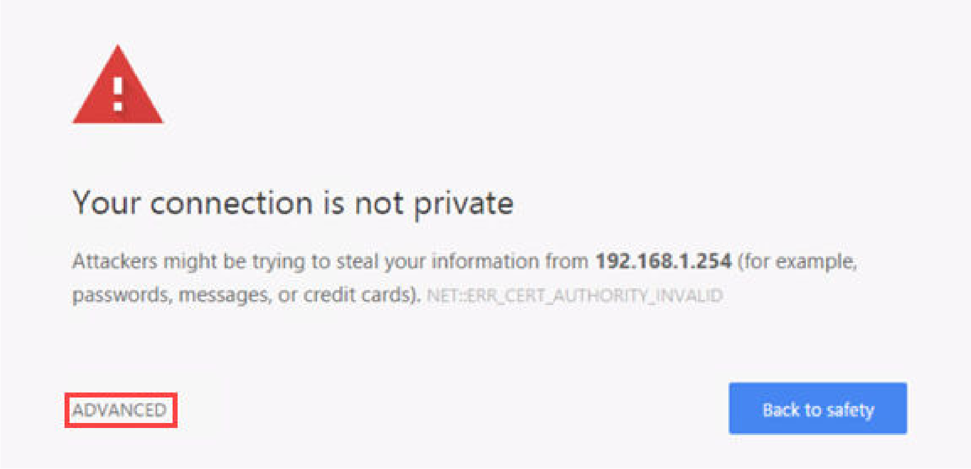
2. Log in to the **Client** PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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.

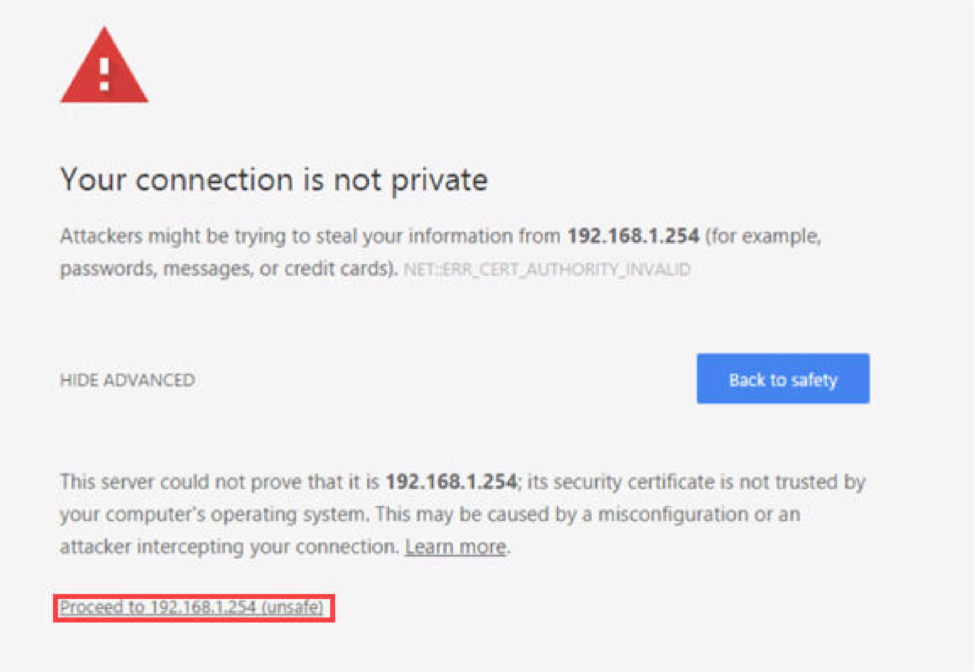


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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.

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

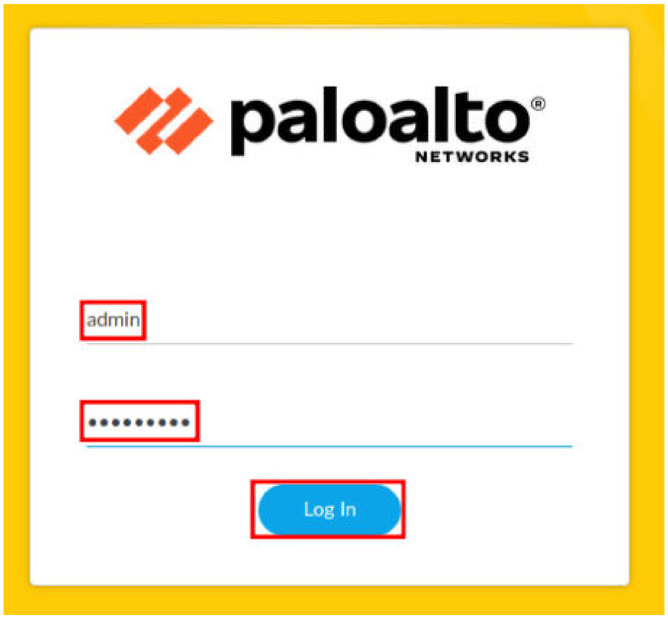


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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

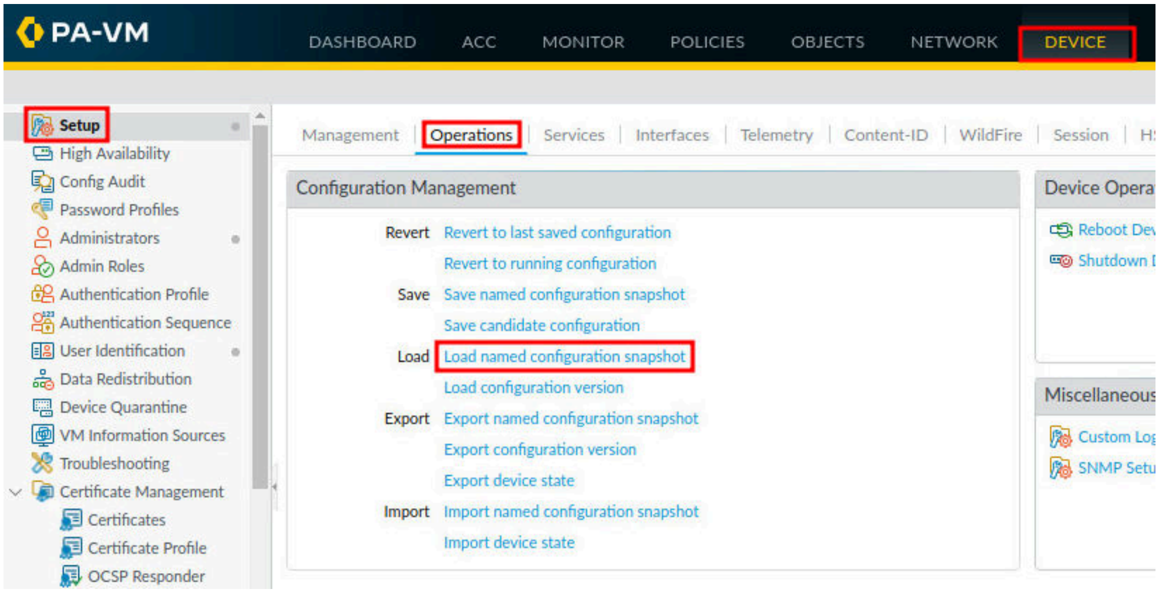
7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.



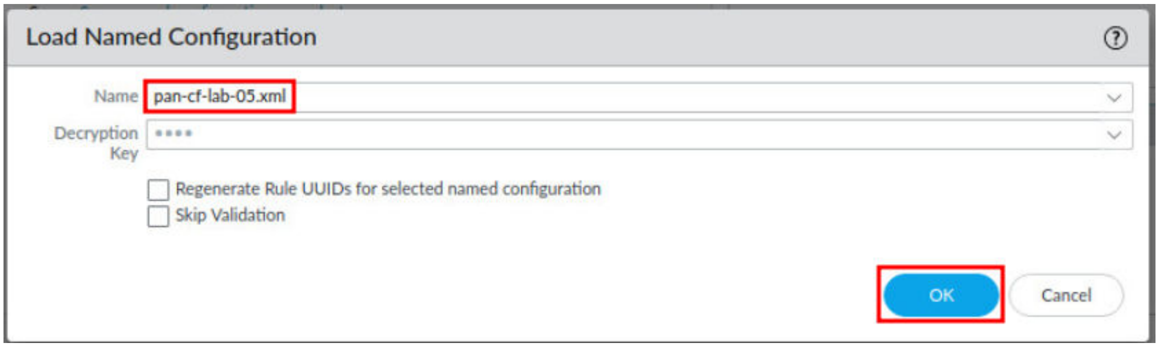
admin

••••••••••

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**.


Load Named Configuration

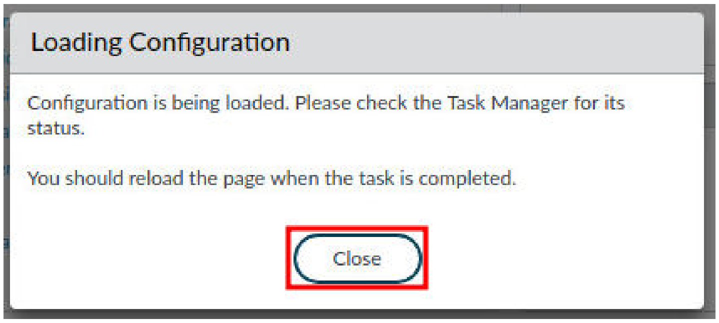
Name: pan-cf-lab-05.xml

Decryption Key: ••••

□ Regenerate Rule UUIDs for selected named configuration

□ Skip Validation

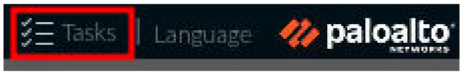
10. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

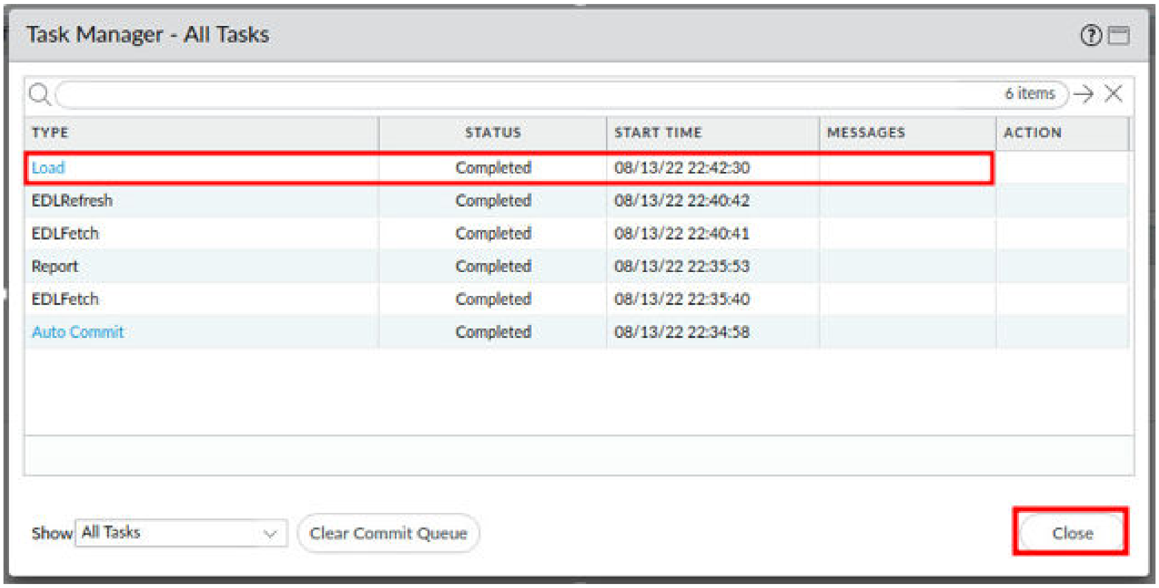
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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



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

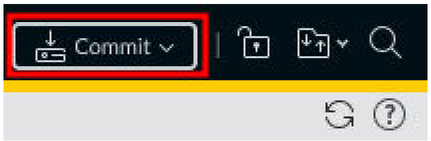

Task Manager - All Tasks

6 items

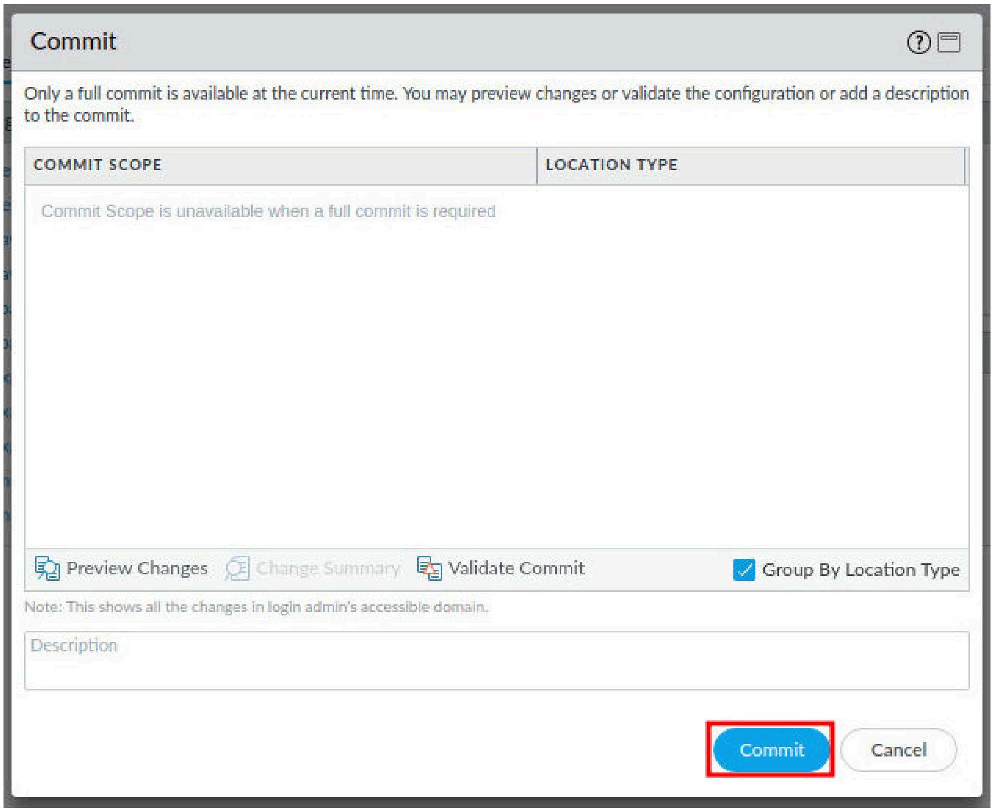
TYPE	STATUS	START TIME	MESSAGES	ACTION
Load	Completed	08/13/22 22:42:30		
EDLRefresh	Completed	08/13/22 22:40:42		
EDLFetch	Completed	08/13/22 22:40:41		
Report	Completed	08/13/22 22:35:53		
EDLFetch	Completed	08/13/22 22:35:40		
Auto Commit	Completed	08/13/22 22:34:58		

Show All Tasks

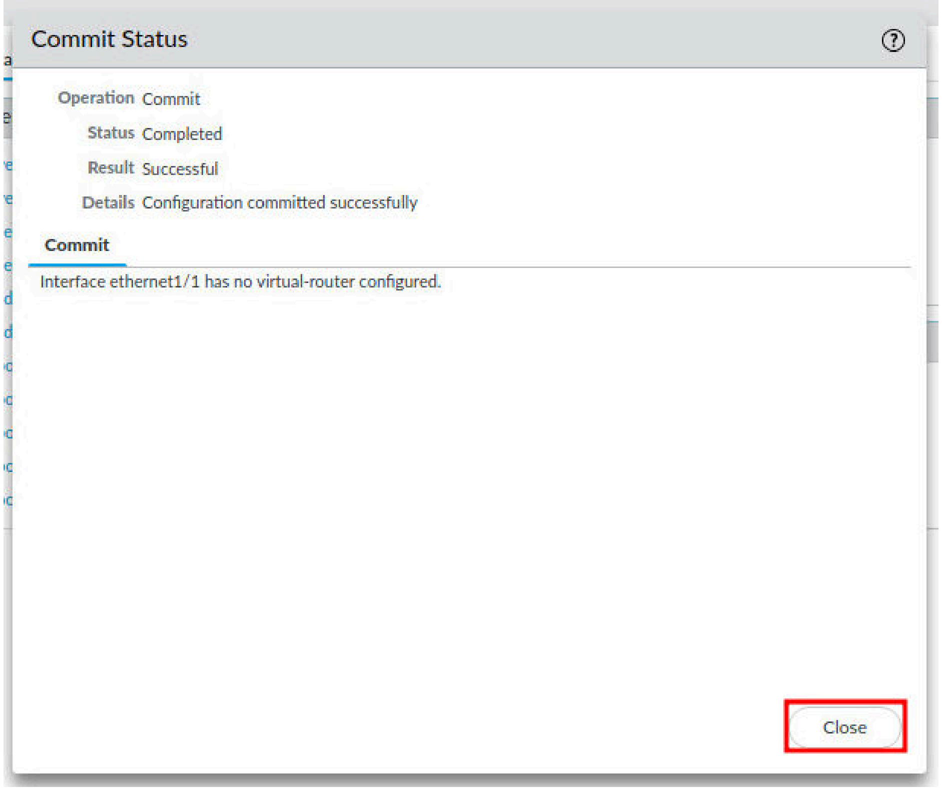
13. Click the **Commit** link located at the top-right of the web interface.



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


Commit
Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.
COMMIT SCOPE
LOCATION TYPE
Commit Scope is unavailable when a full commit is required
Preview Changes
Change Summary
Validate Commit
Group By Location Type
Note: This shows all the changes in login admin's accessible domain.
Description
Commit
Cancel

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


Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit

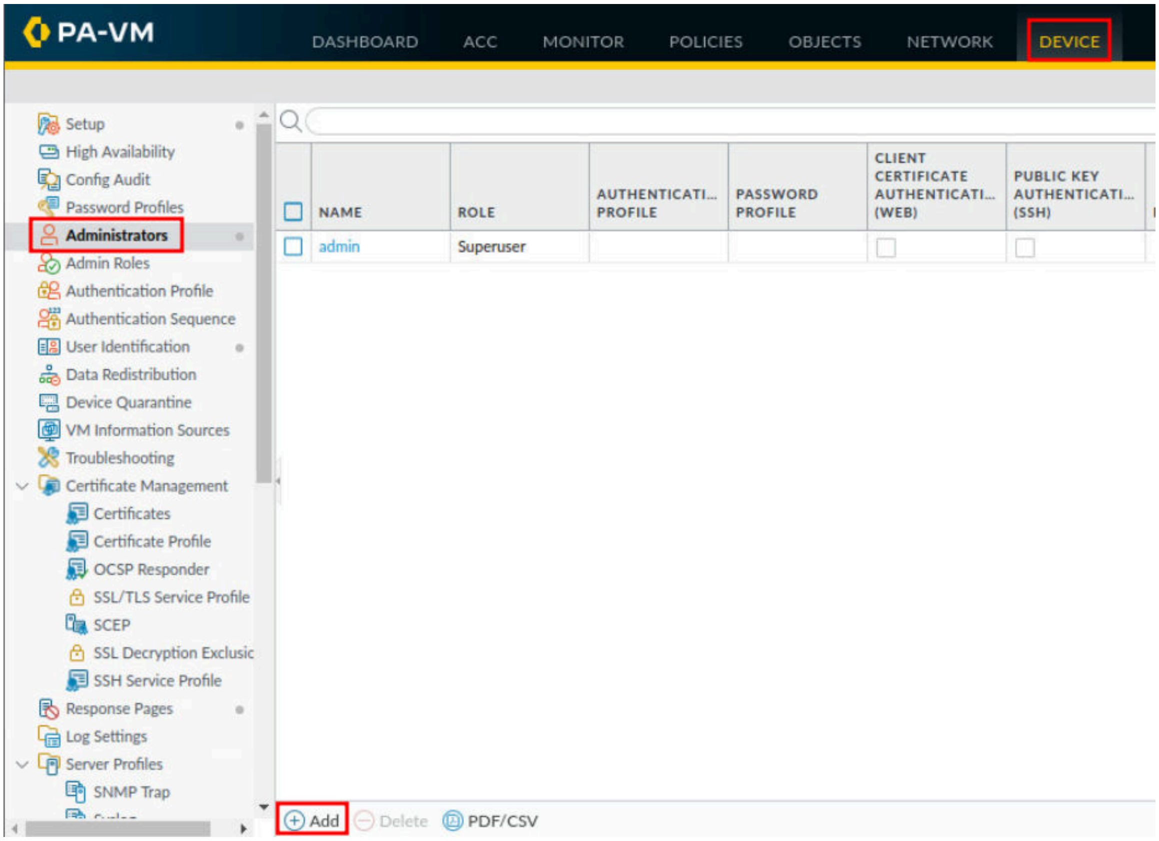
Interface ethernet1/1 has no virtual-router configured.

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

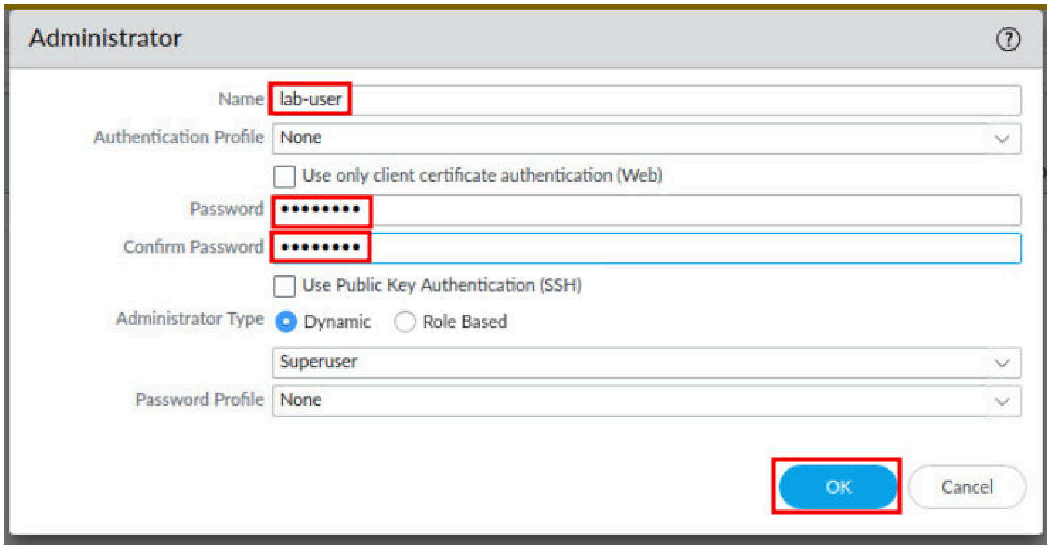
In this section, you will create a local user account, *lab-user*. This account will be used for authentication against the Firewall.

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



□	NAME	ROLE	AUTHENTICATI... PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)
□	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.


Administrator

Name: lab-user

Authentication Profile: None

□ Use only client certificate authentication (Web)

Password: ••••••••

Confirm Password: ••••••••

□ Use Public Key Authentication (SSH)

Administrator Type: ● Dynamic ○ Role Based

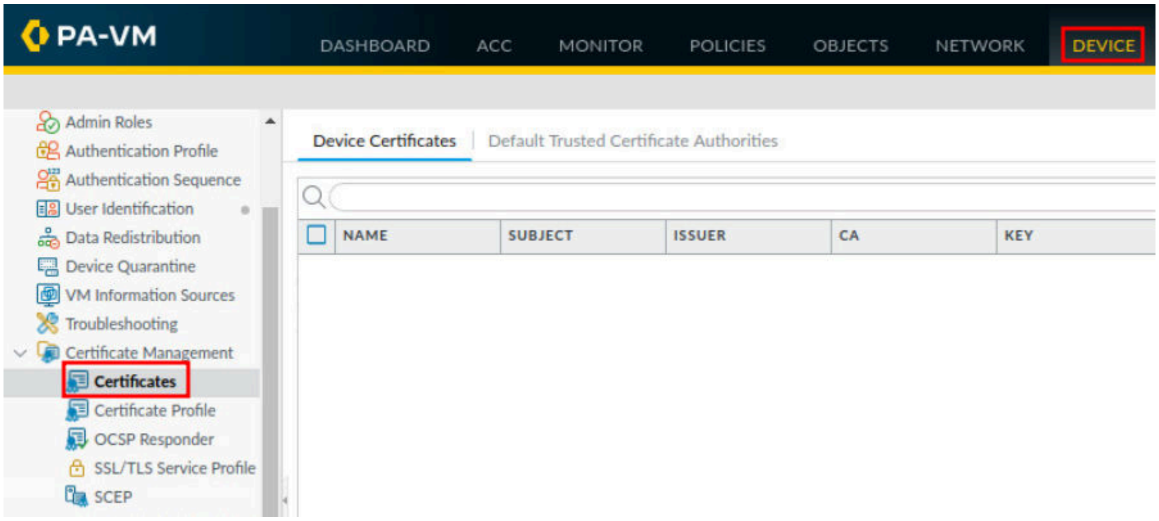
Superuser

Password Profile: None

1.2 Generate Certificates

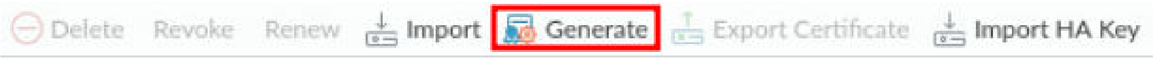
In this section, you will generate two certificates. The first is a self-signed Root Certificate Authority (CA) certificate, which is the top-most certificate in the certificate chain. The Firewall can use this certificate to automatically issue certificates for other uses. In this lab, you will use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

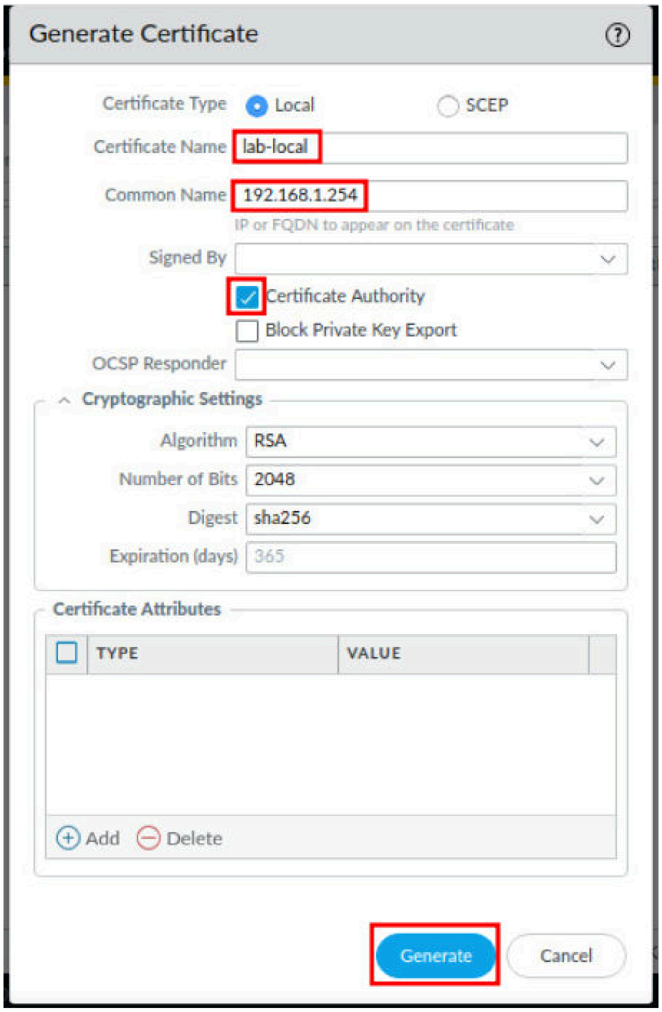


□	NAME	SUBJECT	ISSUER	CA	KEY

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.



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: lab-local

Common Name: 192.168.1.254

IP or FQDN to appear on the certificate

Signed By:

☑ Certificate Authority

□ Block Private Key Export

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

Digest: sha256

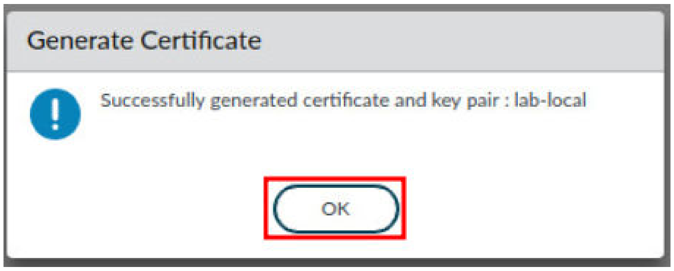
Expiration (days): 365

Certificate Attributes

□	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*.

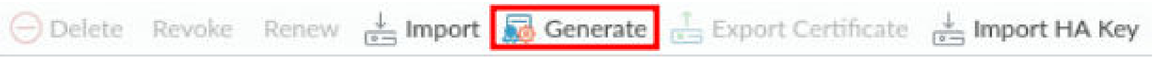
4. In the *Generate Certificate* window, click **OK** to continue.



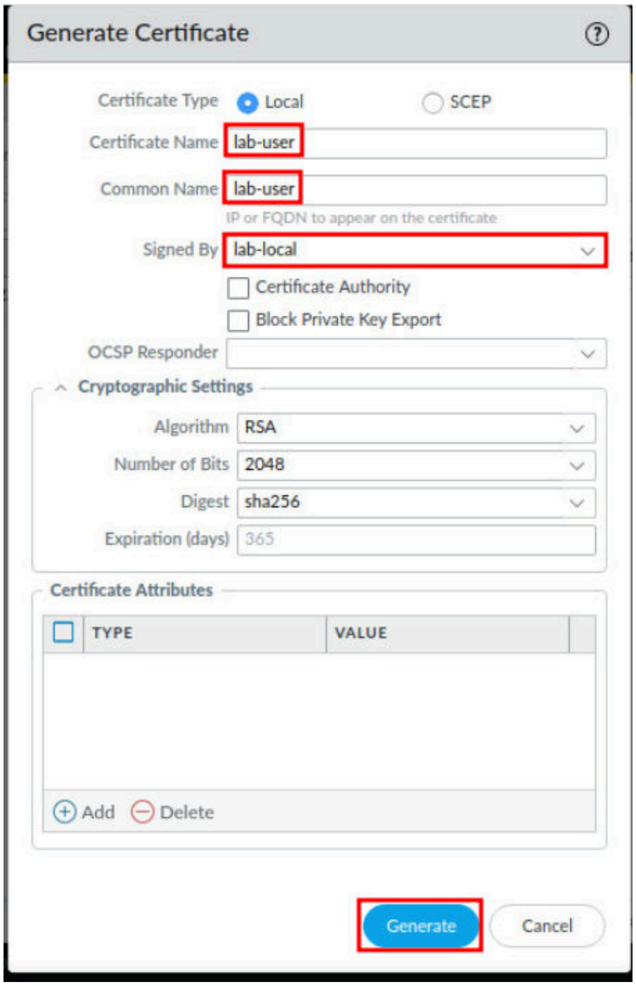
Generate Certificate

Successfully generated certificate and key pair : lab-local

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.



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: lab-user

Common Name: lab-user

IP or FQDN to appear on the certificate

Signed By: lab-local

□ Certificate Authority

□ Block Private Key Export

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

Digest: sha256

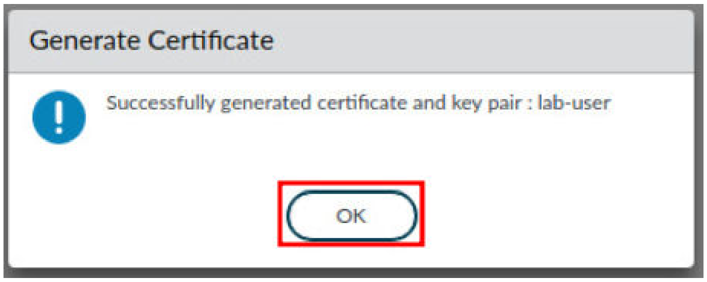
Expiration (days): 365

Certificate Attributes

□	TYPE	VALUE

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.



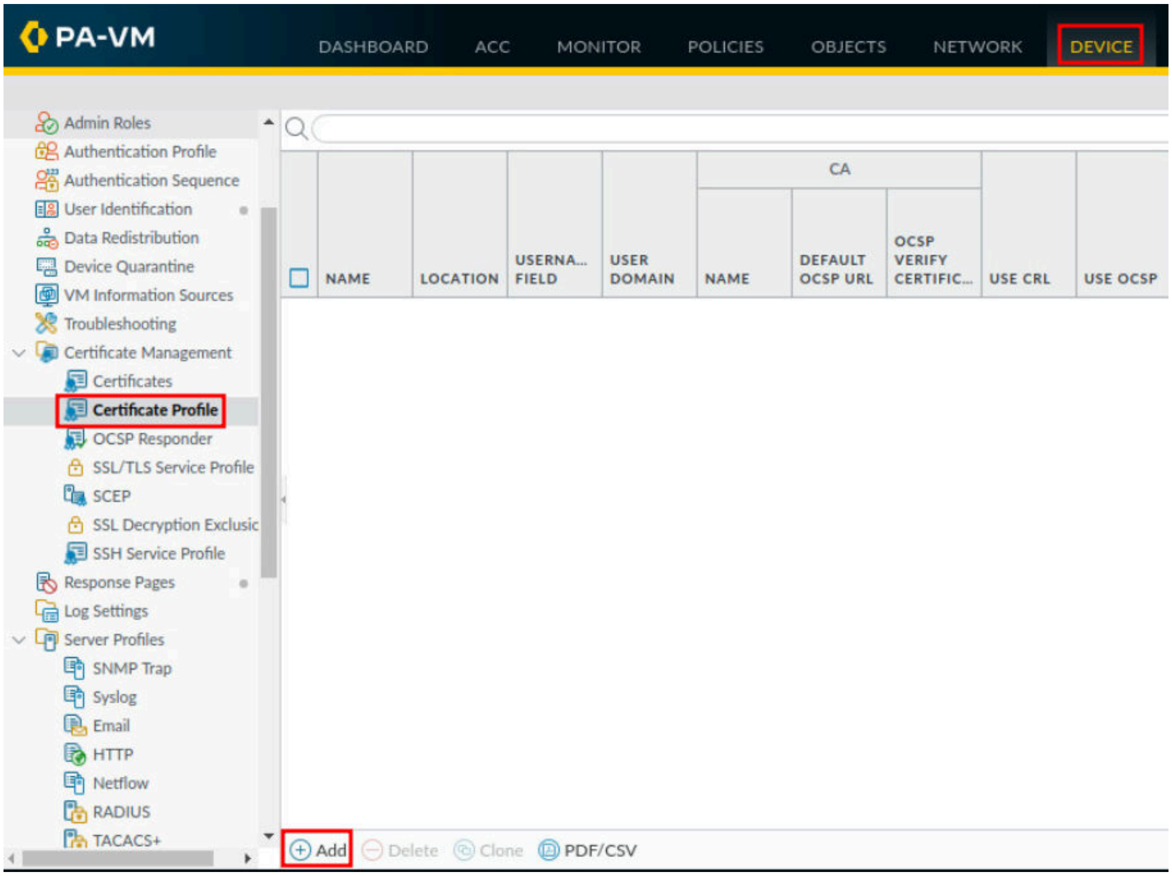
Generate Certificate

Successfully generated certificate and key pair : lab-user

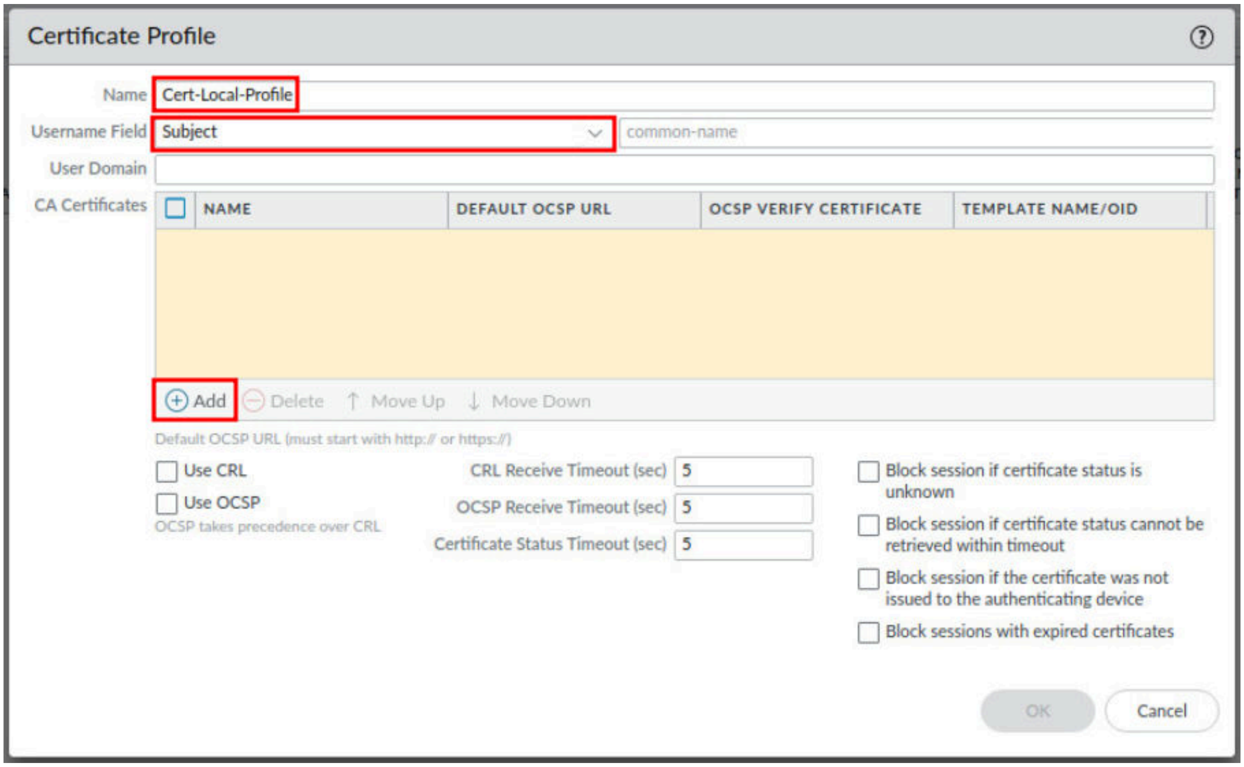
1.3 Create a Certificate Profile

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 *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.



Certificate Profile

Name: Cert-Local-Profile

Username Field: Subject — common-name

User Domain:

CA Certificates:

☐	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID

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

☐ Use CRL

☐ Use OCSP

OCSP takes precedence over CRL

CRL Receive Timeout (sec): 5

OCSP Receive Timeout (sec): 5

Certificate Status Timeout (sec): 5

☐ Block session if certificate status is unknown

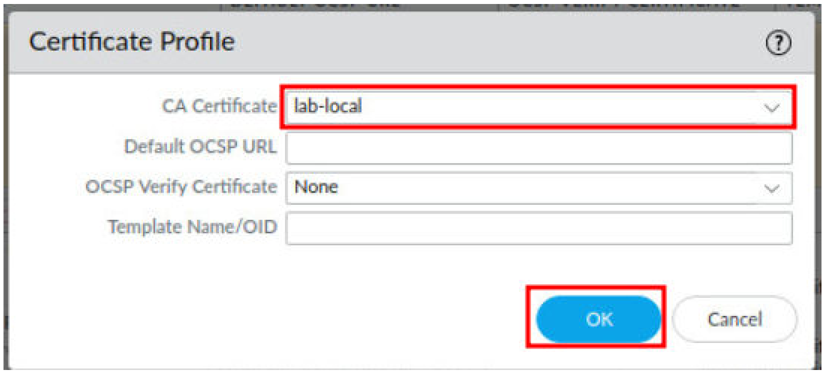
☐ Block session if certificate status cannot be retrieved within timeout

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

☐ Block sessions with expired certificates

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.



Certificate Profile

CA Certificate: lab-local

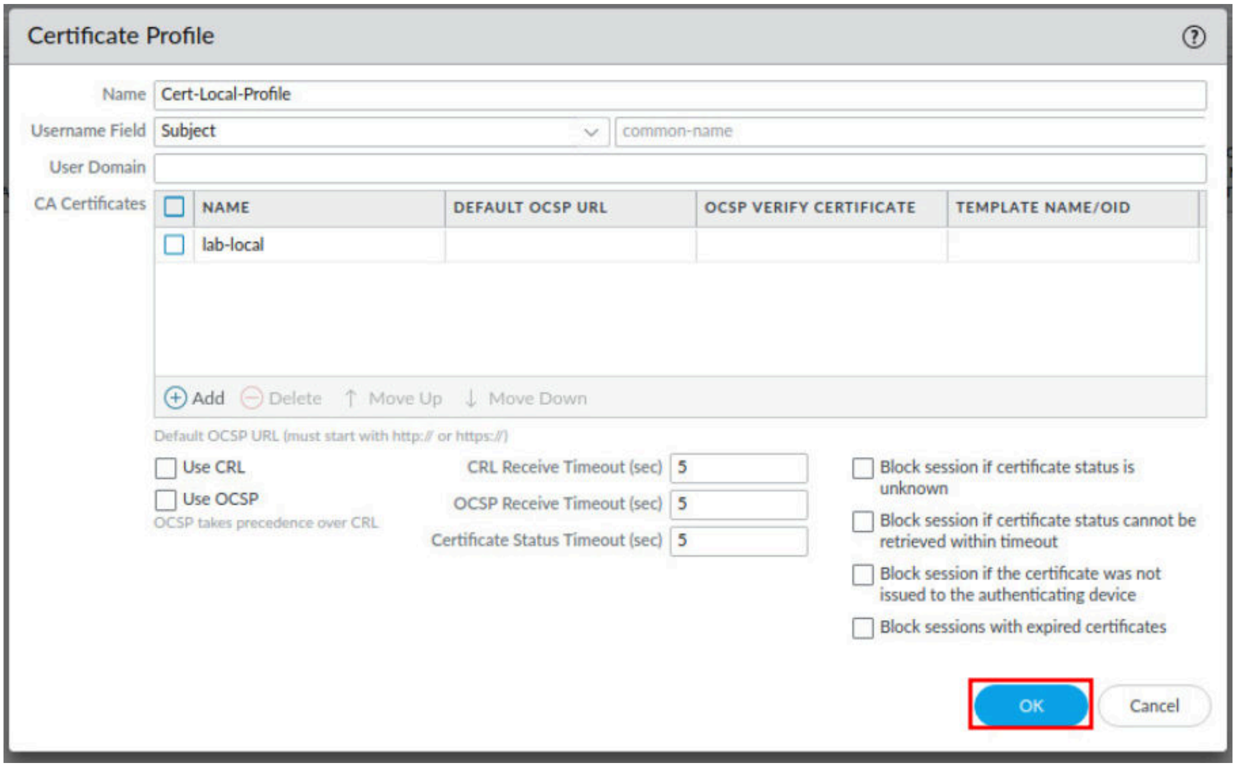
Default OCSP URL:

OCSP Verify Certificate: None

Template Name/OID:

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: Cert-Local-Profile

Username Field: Subject | common-name

User Domain:

CA Certificates:

□	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
□	lab-local			

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

□ Use CRL

□ Use OCSP

OCSP takes precedence over CRL

CRL Receive Timeout (sec): 5

OCSP Receive Timeout (sec): 5

Certificate Status Timeout (sec): 5

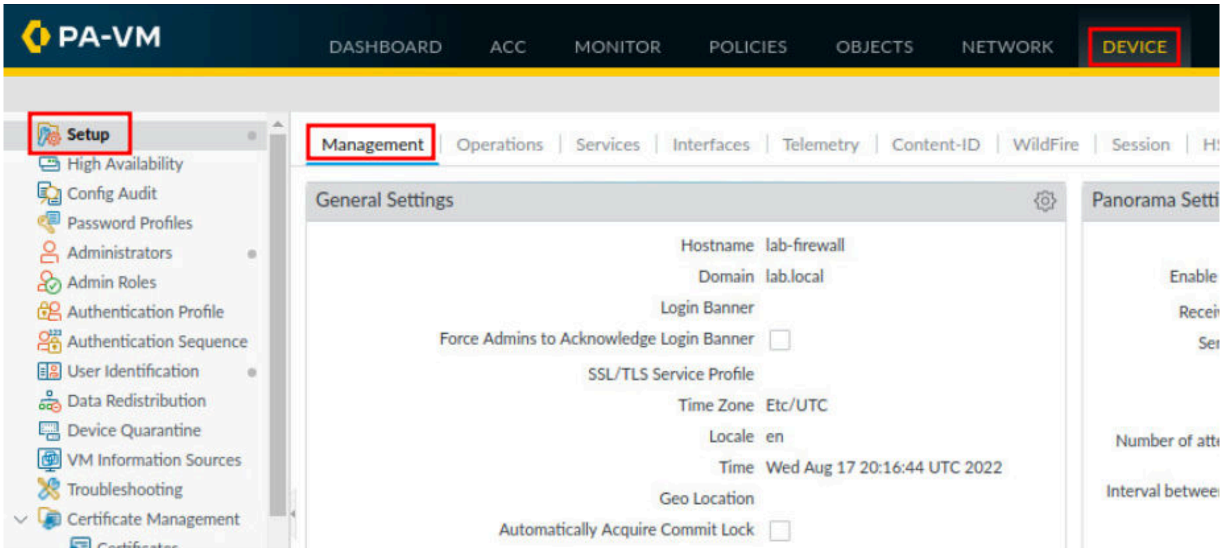
□ Block session if certificate status is unknown

□ 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

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



General Settings

Hostname: lab-firewall

Domain: lab.local

Login Banner:

Force Admins to Acknowledge Login Banner: □

SSL/TLS Service Profile:

Time Zone: Etc/UTC

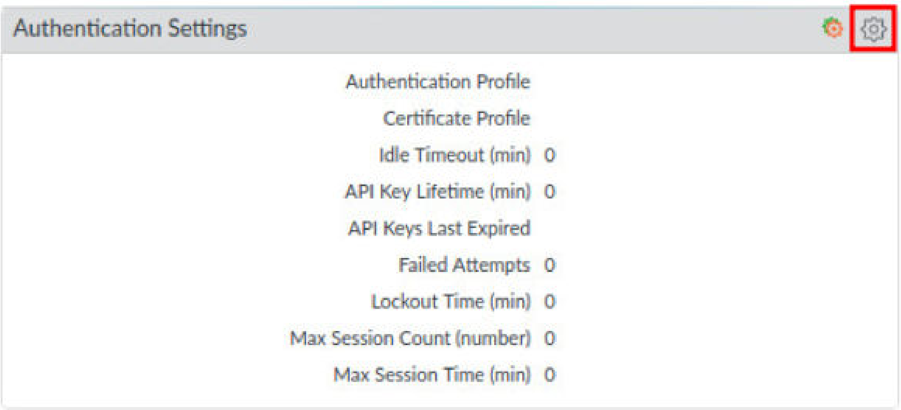
Locale: en

Time: Wed Aug 17 20:16:44 UTC 2022

Geo Location:

Automatically Acquire Commit Lock: □

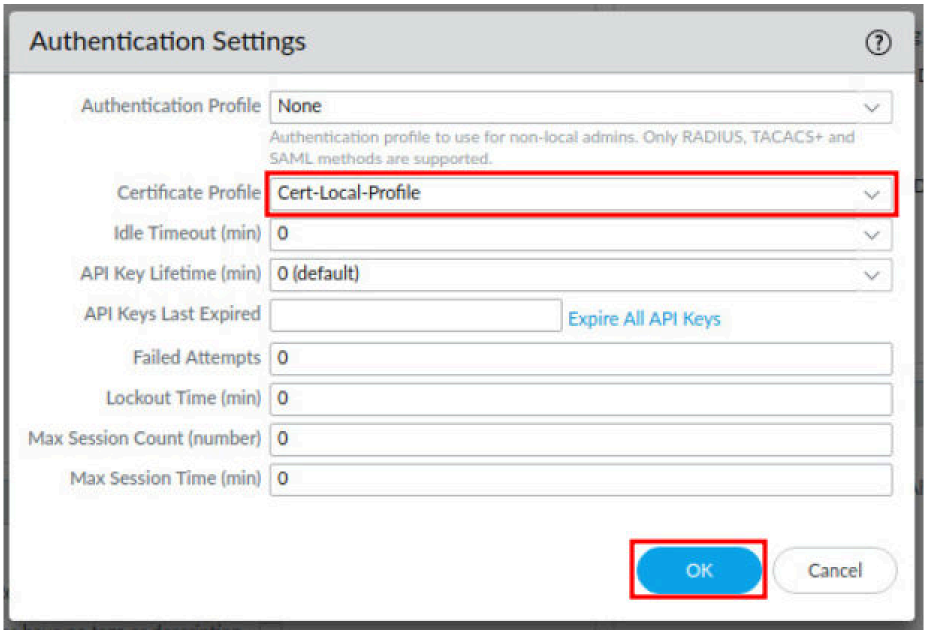
6. Click the **gear** icon on the *Authentication Settings* section, located in the center.



Authentication Settings

Authentication Profile	
Certificate Profile	
Idle Timeout (min)	0
API Key Lifetime (min)	0
API Keys Last Expired	
Failed Attempts	0
Lockout Time (min)	0
Max Session Count (number)	0
Max Session Time (min)	0

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



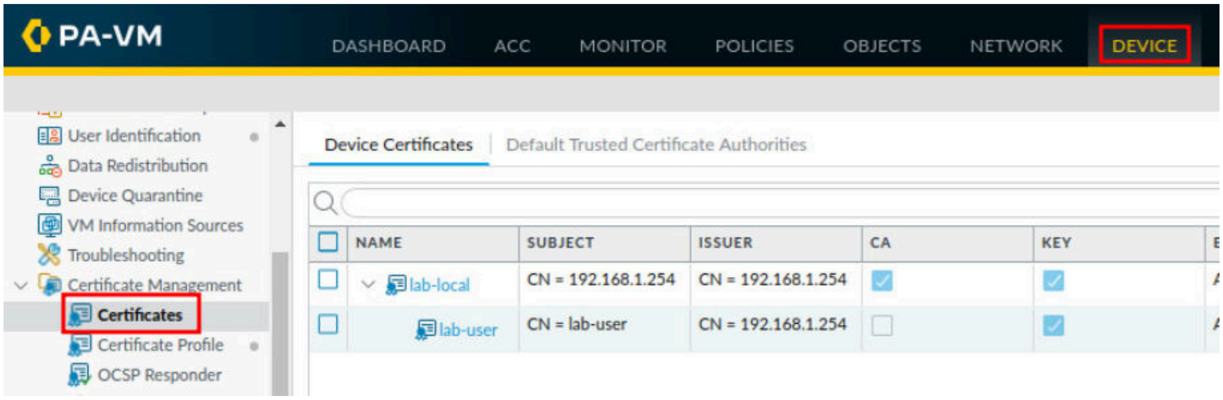
Authentication Settings

Authentication Profile	None Authentication profile to use for non-local admins. Only RADIUS, TACACS+ and SAML methods are supported.
Certificate Profile	Cert-Local-Profile
Idle Timeout (min)	0
API Key Lifetime (min)	0 (default)
API Keys Last Expired	Expire All API Keys
Failed Attempts	0
Lockout Time (min)	0
Max Session Count (number)	0
Max Session Time (min)	0

1.4 Export Certificate and Commit

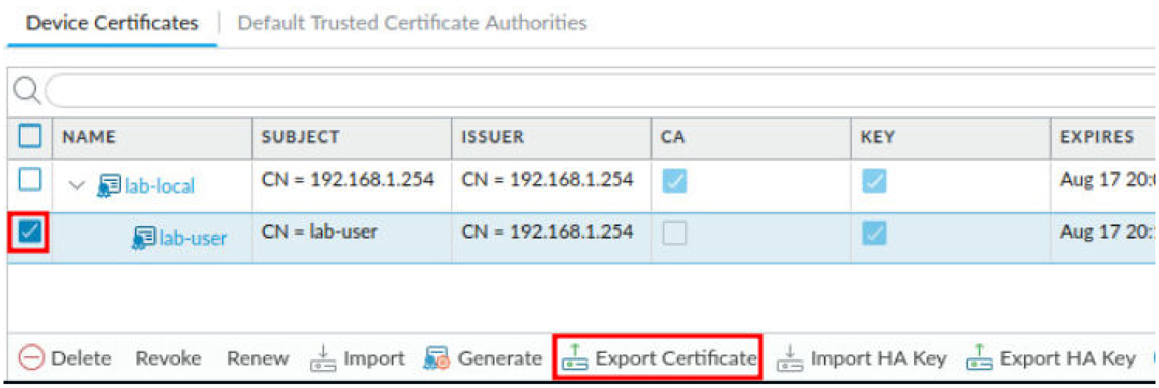
In this section, you will export the *lab-user* certificate you generated on the Firewall. Then, you will commit changes, causing the Firewall to start using certificates for authentication.

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



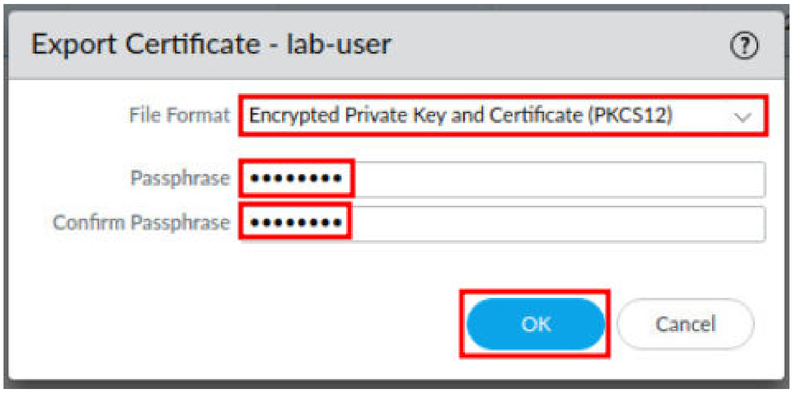
□	NAME	SUBJECT	ISSUER	CA	KEY
□	lab-local	CN = 192.168.1.254	CN = 192.168.1.254	☑	☑
□	lab-user	CN = lab-user	CN = 192.168.1.254	□	☑

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



□	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES
□	lab-local	CN = 192.168.1.254	CN = 192.168.1.254	☑	☑	Aug 17 20:
☑	lab-user	CN = lab-user	CN = 192.168.1.254	□	☑	Aug 17 20:

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.


Export Certificate - lab-user

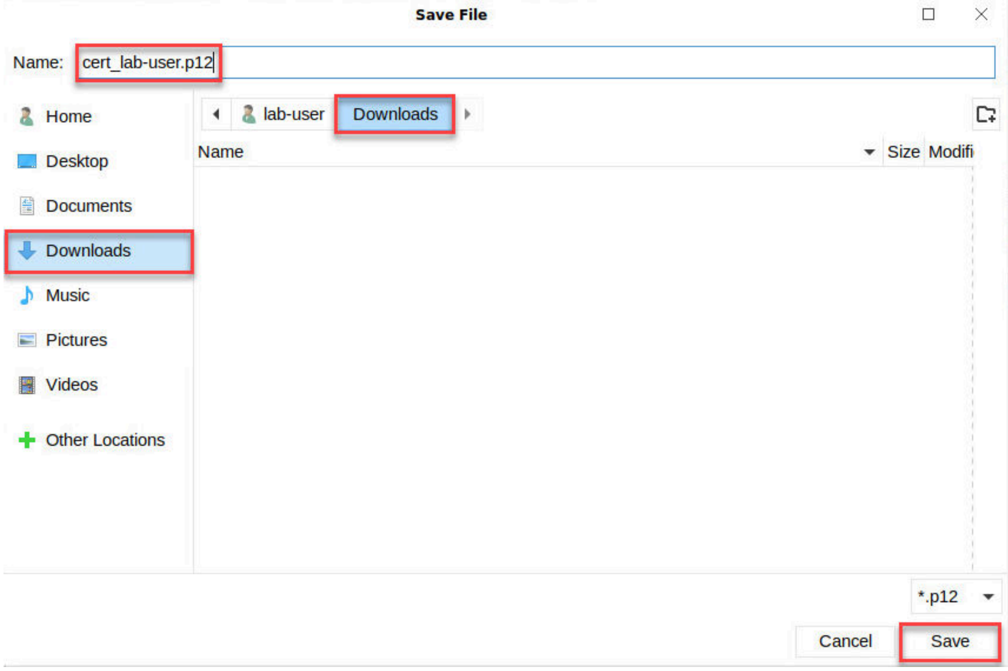
File Format: Encrypted Private Key and Certificate (PKCS12)

Passphrase: •••••••••

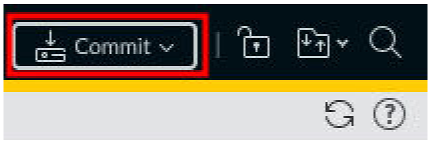
Confirm Passphrase: •••••••••

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.

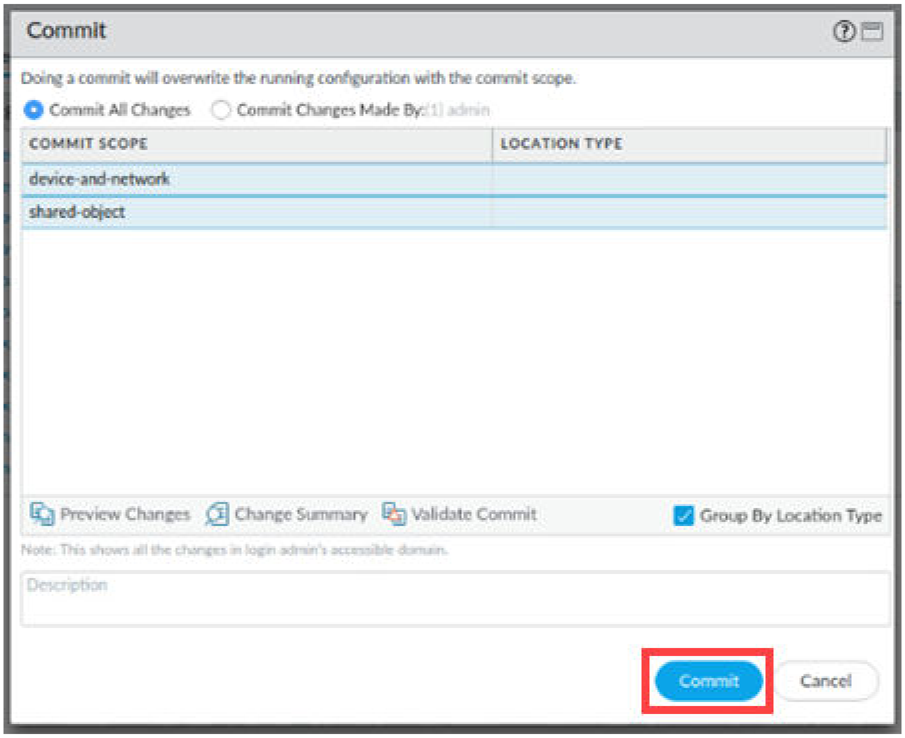
4. In the *Save File* window pop-up, verify the name of ***cert_lab-user.p12*** is correct in the *Name* field, verify the ***.p12*** file is being saved in the ***Downloads*** folder, and click **Save**.



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.



Commit

Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

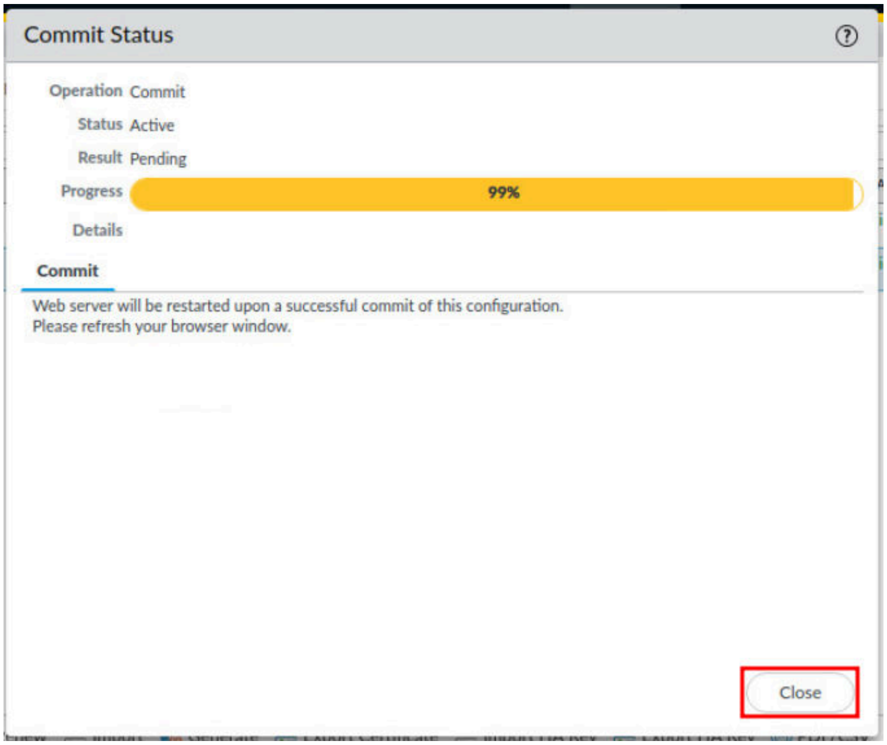
COMMIT SCOPE	LOCATION TYPE
device-and-network	
shared-object	

☑ Group By Location Type

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

Description

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



Commit Status

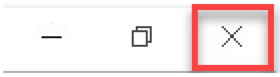
Operation Commit
Status Active
Result Pending
Progress 99%
Details

Commit

Web server will be restarted upon a successful commit of this configuration.
Please refresh your browser window.

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%.

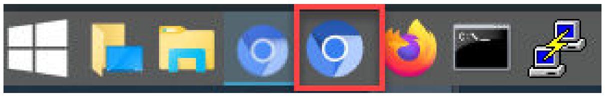
8. Click the **X** in the upper-right to close the *Chromium Web Browser*.



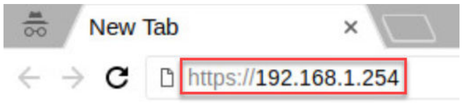
1.5 Test Connectivity and Import Certificate on the Client

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.

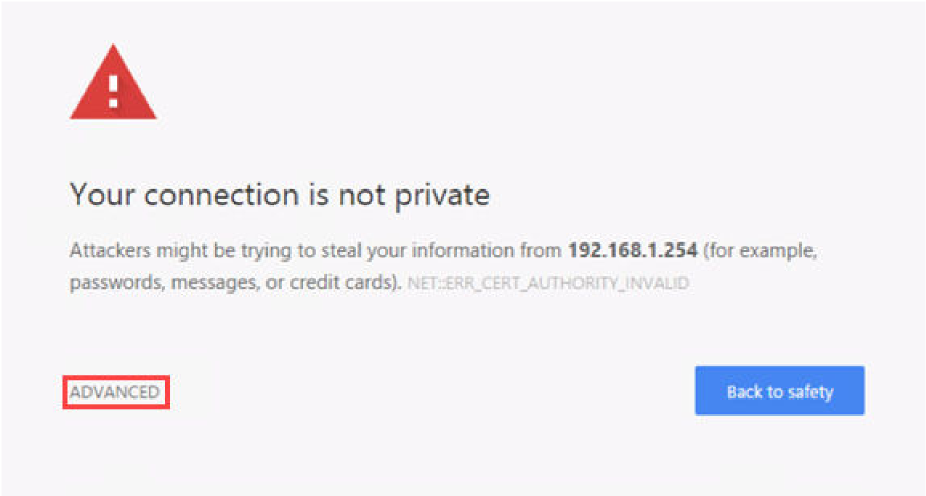
1. Open **Chromium** from the taskbar.



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.

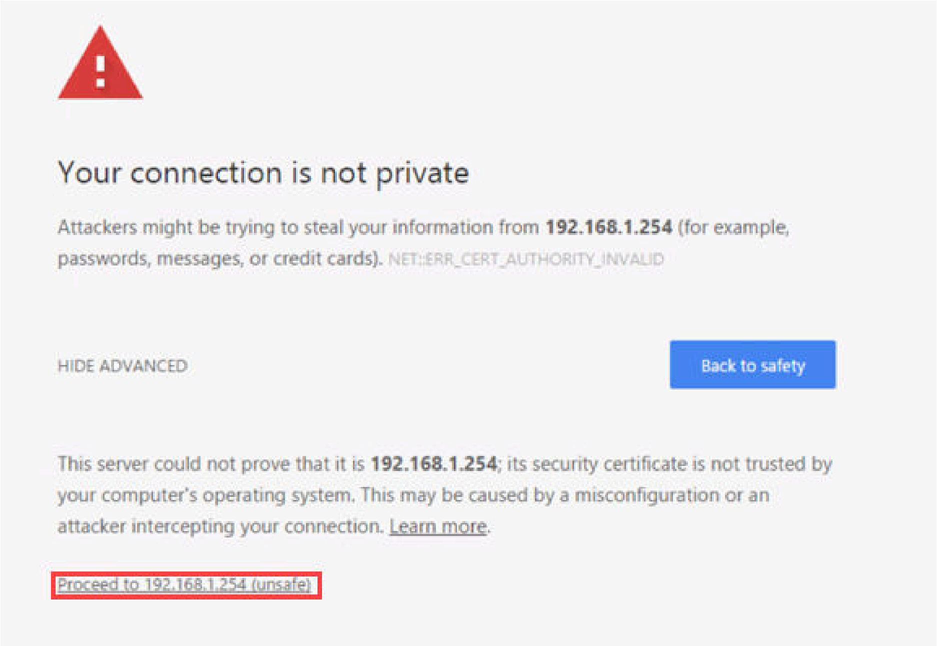


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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).**



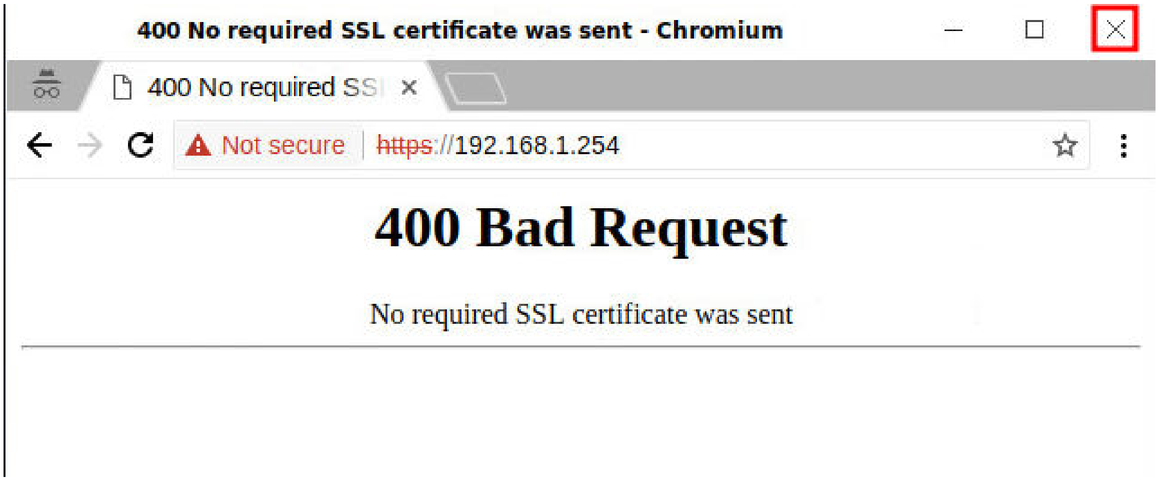
Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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

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.*

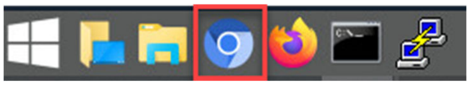


400 Bad Request

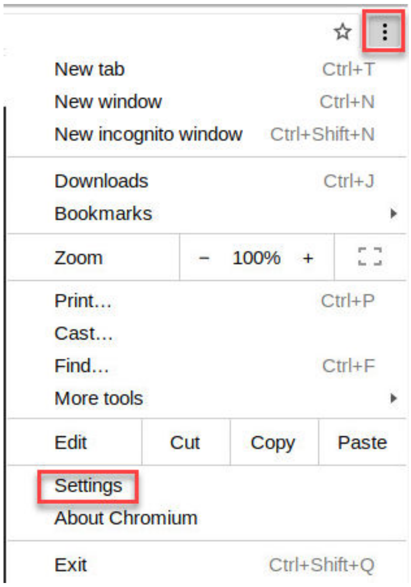
No required SSL certificate was sent

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.

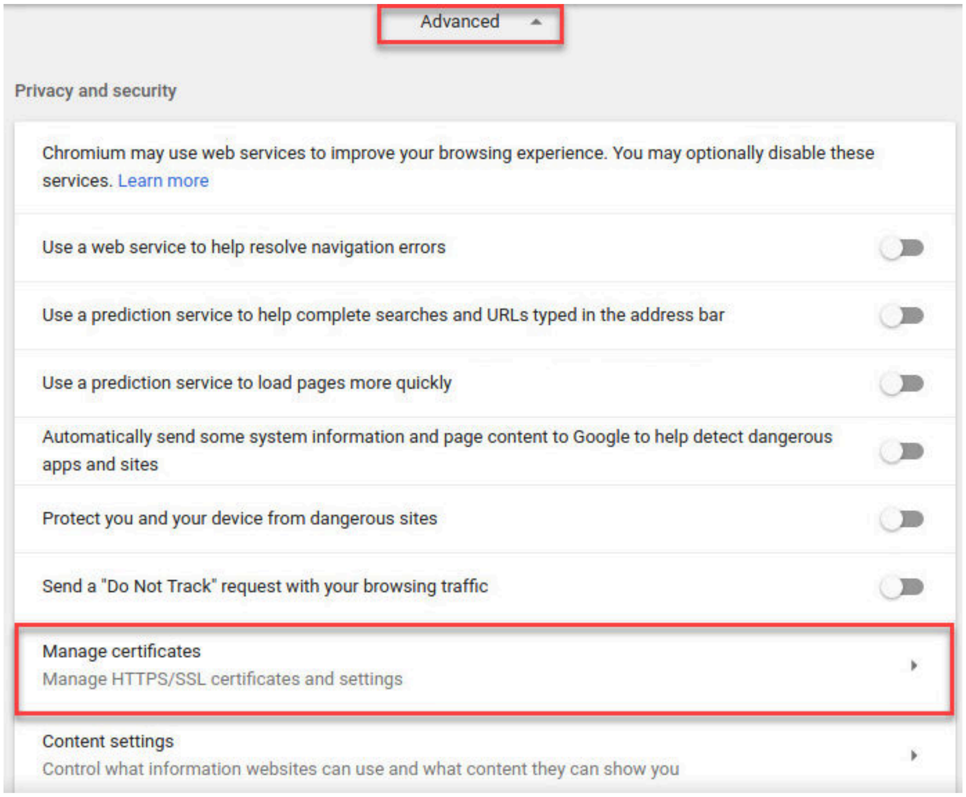
6. To install the *lab-user* certificate, open **Chromium** from the taskbar.



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**.



Privacy and security

Chromium may use web services to improve your browsing experience. You may optionally disable these services. Learn more

Use a web service to help resolve navigation errors

Use a prediction service to help complete searches and URLs typed in the address bar

Use a prediction service to load pages more quickly

Automatically send some system information and page content to Google to help detect dangerous apps and sites

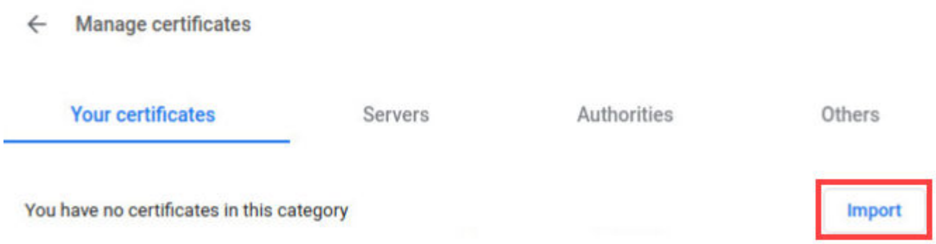
Protect you and your device from dangerous sites

Send a "Do Not Track" request with your browsing traffic

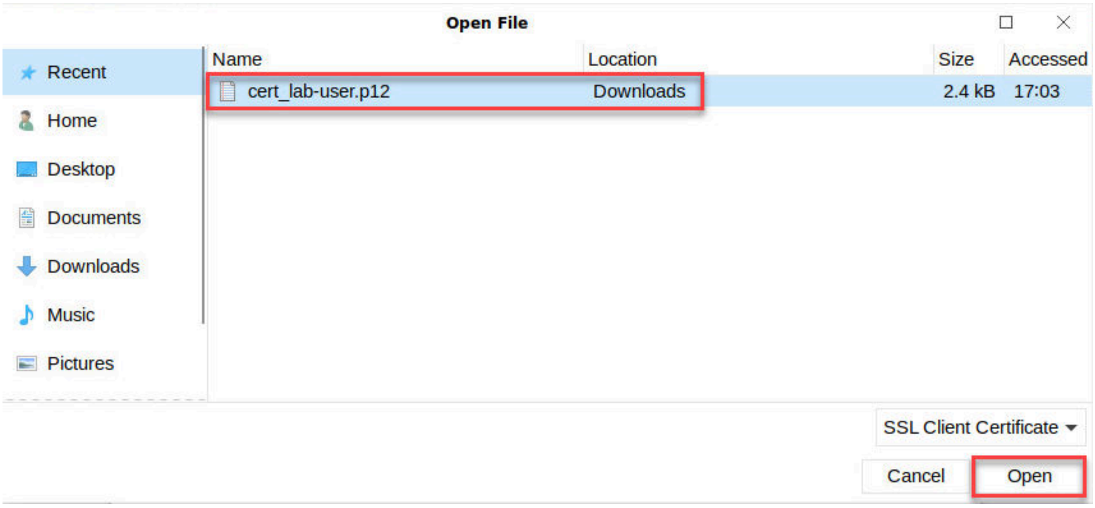
Manage certificates
Manage HTTPS/SSL certificates and settings

Content settings
Control what information websites can use and what content they can show you

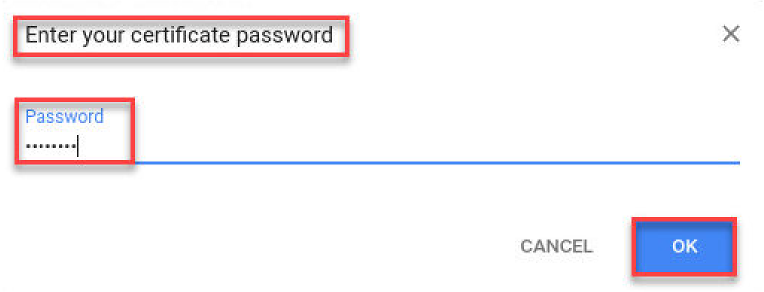
9. In the *Manage Certificates* window, click **Import**.



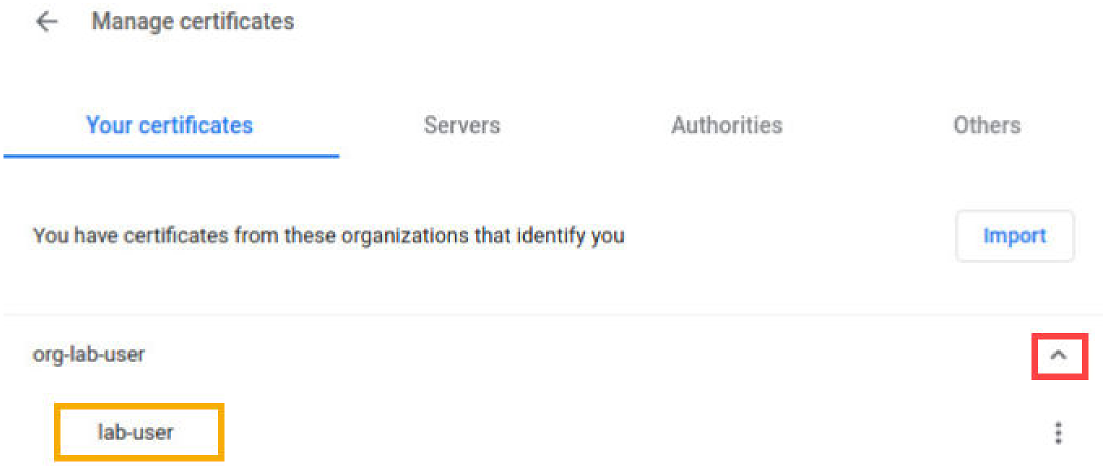
10. In the *Open File* window, select **cert_lab-user.p12** and then click the **Open** button.



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.



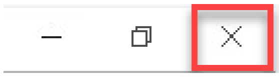
Manage certificates

You have certificates from these organizations that identify you

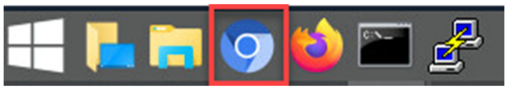
org-lab-user

lab-user

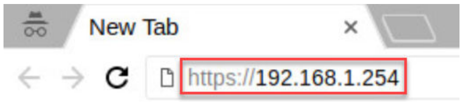
13. Click the **X** in the upper-right to close *Chromium*.



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

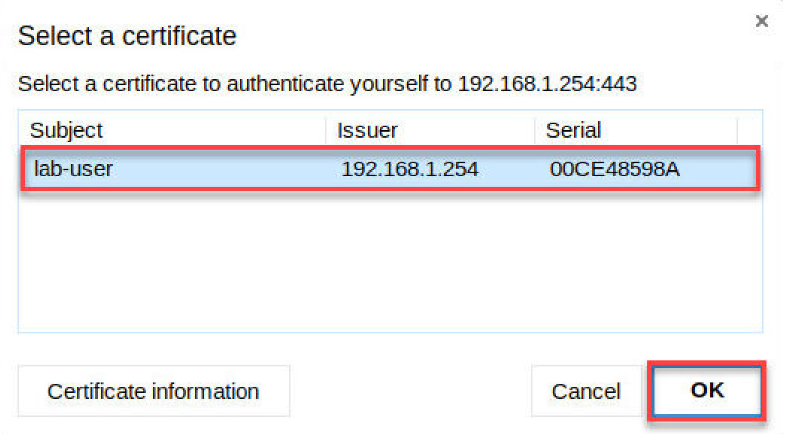


15. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter.**



https://192.168.1.254

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

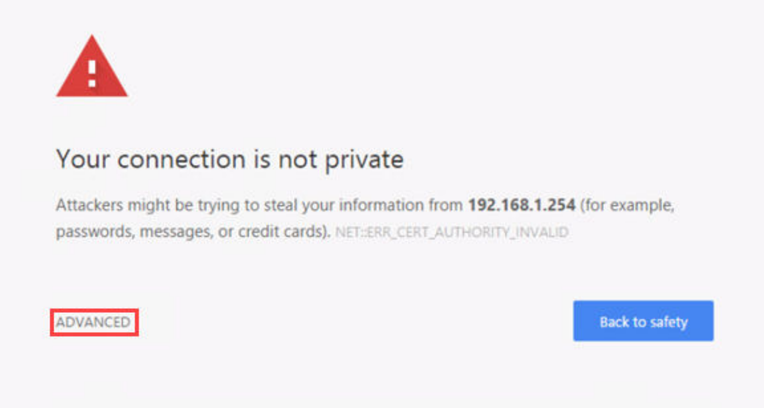


Select a certificate

Select a certificate to authenticate yourself to 192.168.1.254:443

Subject	Issuer	Serial
lab-user	192.168.1.254	00CE48598A

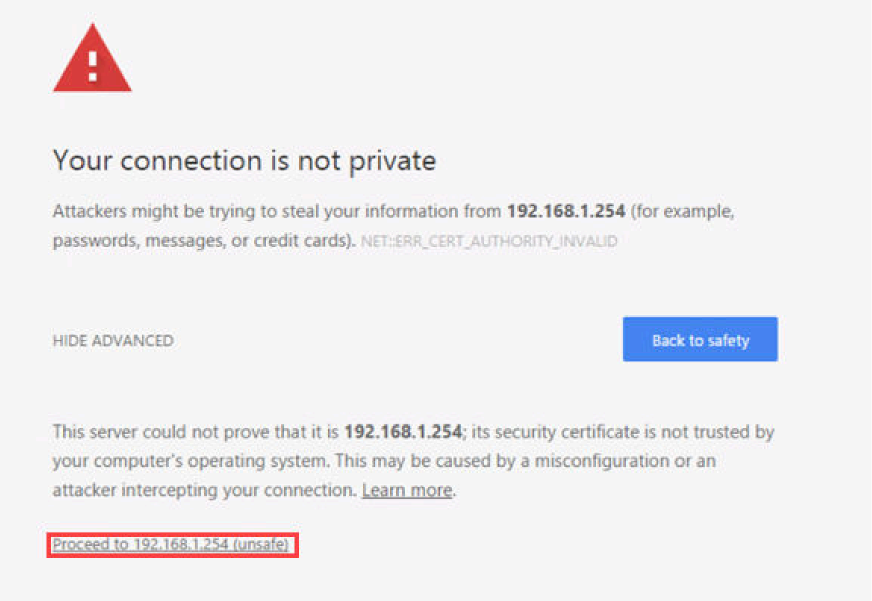
17. You will see a “*Your connection is not private”* message. Click on the **ADVANCED** link**)**.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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



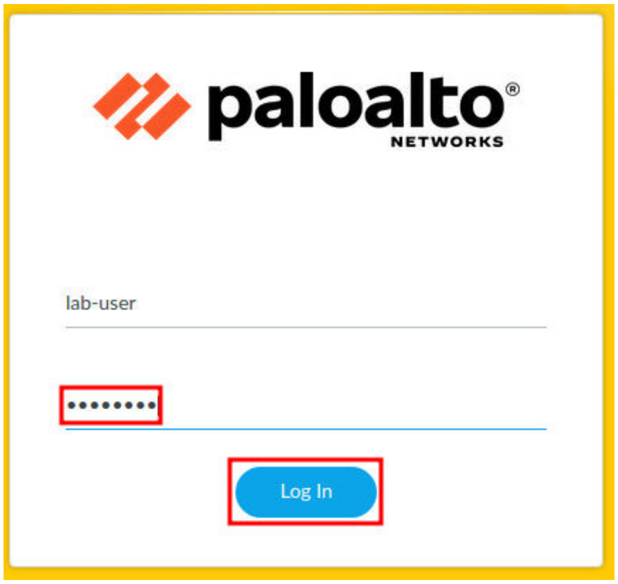
Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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

Proceed to 192.168.1.254 (unsafe)

19. The Firewall login window will be displayed. Type `Pal0Alt0` for the *Password* field. Then, click the **Log In** button.

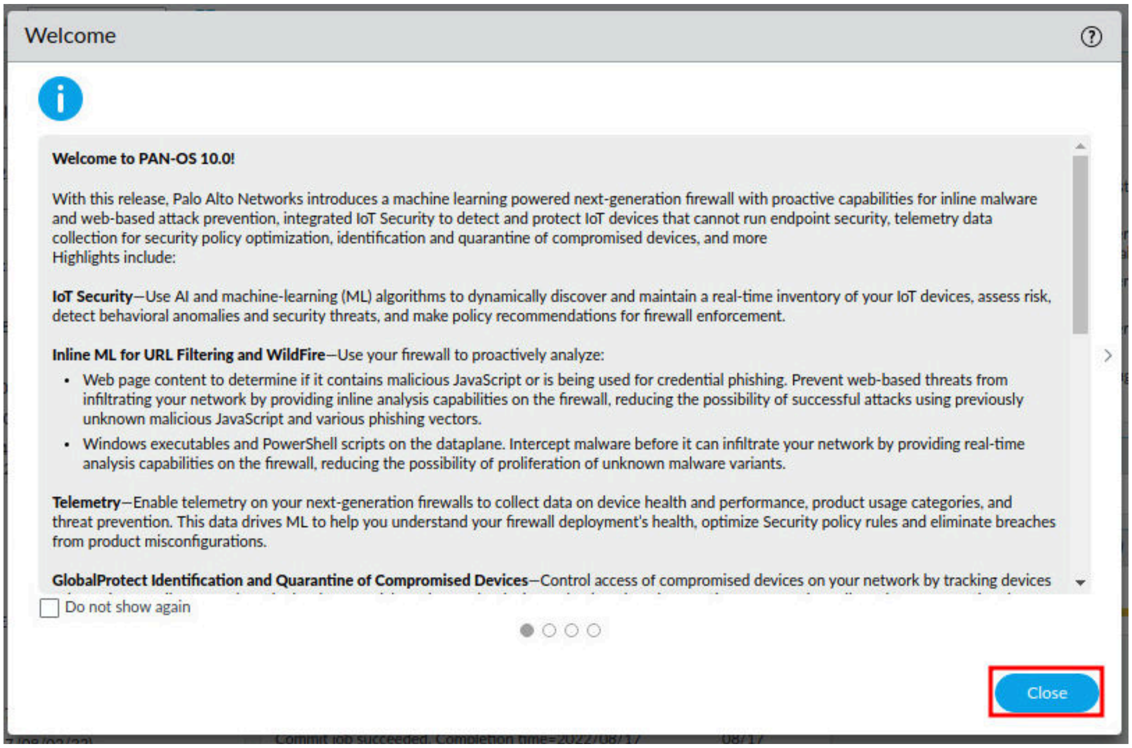


lab-user

••••••••

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.



Welcome

Welcome to PAN-OS 10.0!

With this release, Palo Alto Networks introduces a machine learning powered next-generation firewall with proactive capabilities for inline malware and web-based attack prevention, integrated IoT Security to detect and protect IoT devices that cannot run endpoint security, telemetry data collection for security policy optimization, identification and quarantine of compromised devices, and more
Highlights include:

IoT Security—Use AI and machine-learning (ML) algorithms to dynamically discover and maintain a real-time inventory of your IoT devices, assess risk, detect behavioral anomalies and security threats, and make policy recommendations for firewall enforcement.

Inline ML for URL Filtering and WildFire—Use your firewall to proactively analyze:

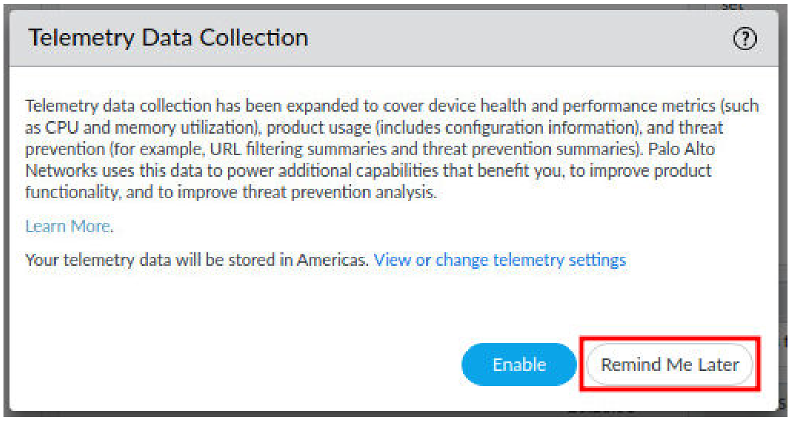
- Web page content to determine if it contains malicious JavaScript or is being used for credential phishing. Prevent web-based threats from infiltrating your network by providing inline analysis capabilities on the firewall, reducing the possibility of successful attacks using previously unknown malicious JavaScript and various phishing vectors.
- Windows executables and PowerShell scripts on the dataplane. Intercept malware before it can infiltrate your network by providing real-time analysis capabilities on the firewall, reducing the possibility of proliferation of unknown malware variants.

Telemetry—Enable telemetry on your next-generation firewalls to collect data on device health and performance, product usage categories, and threat prevention. This data drives ML to help you understand your firewall deployment's health, optimize Security policy rules and eliminate breaches from product misconfigurations.

GlobalProtect Identification and Quarantine of Compromised Devices—Control access of compromised devices on your network by tracking devices

☐ Do not show again

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



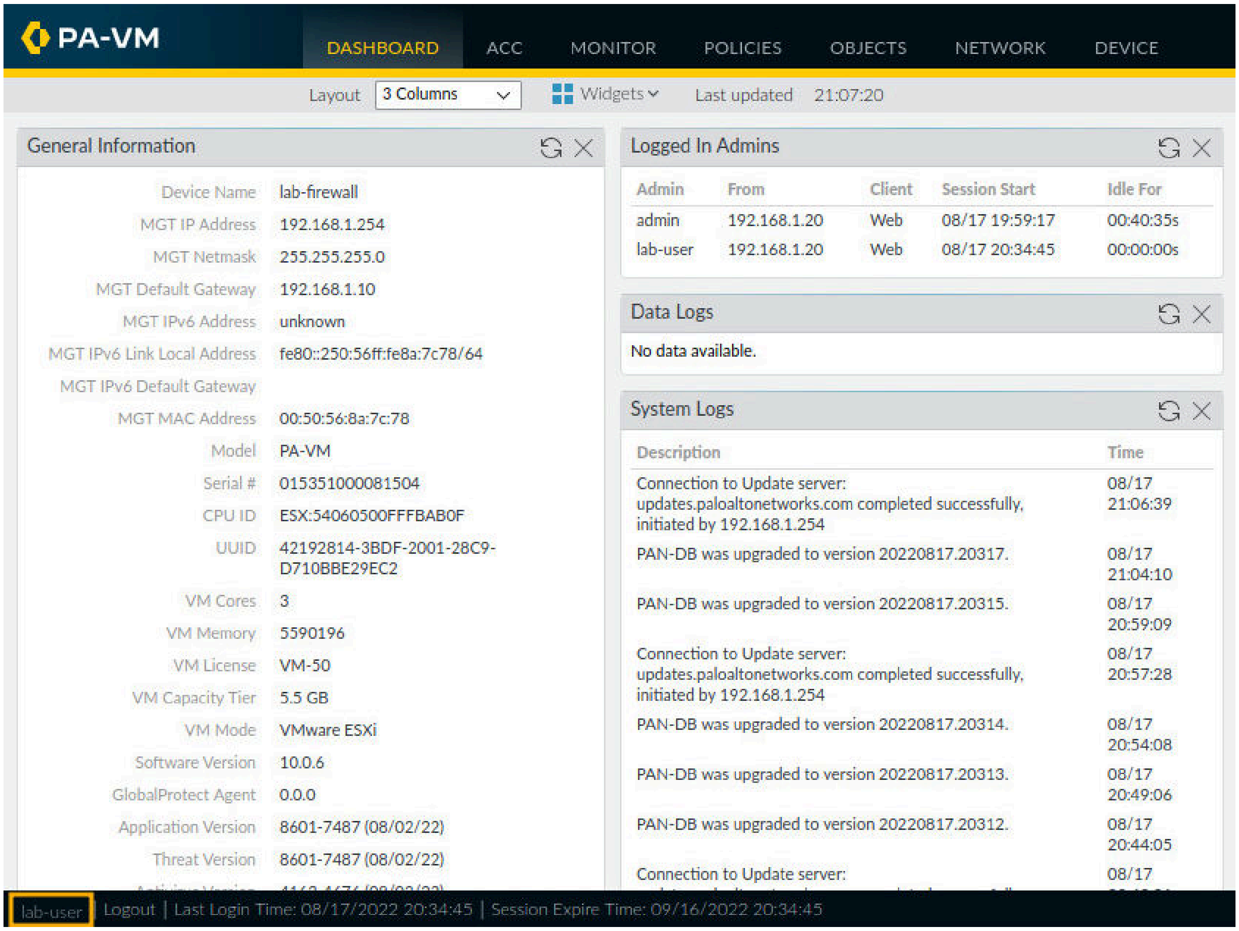
Telemetry Data Collection

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

Learn More.

Your telemetry data will be stored in Americas. View or change telemetry settings

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



Layout 3 Columns Last updated 21:07:20

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:54060500FFFBABOF
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.