NETWORK SECURITY FUNDAMENTALS

Lab 5: Managing Certificates

Document Version: 2021-01-30

Contents

Introduction

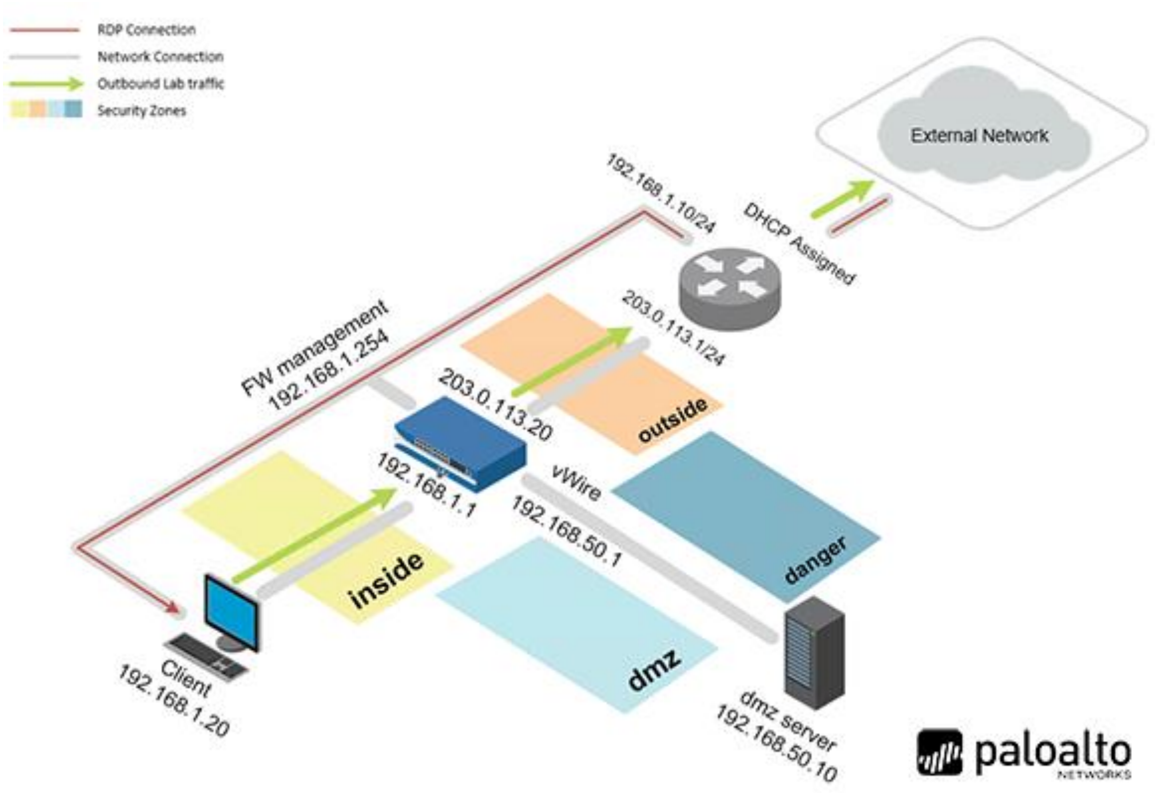
In this lab, you will generate a Self-Signed Root Certificate Authority (CA) certificate and replace the certificate for inbound management traffic. Then, you will import the root CA certificate on the Client machine.

Objective

In this lab, you will perform the following tasks:

- Generate Certificates
- Replace the Certificate for Inbound Management Traffic
- 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.

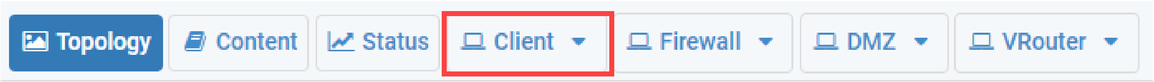
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

5 Managing Certificates

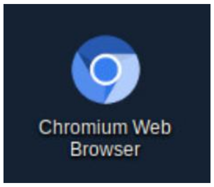
5.0 Load Lab Configuration

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

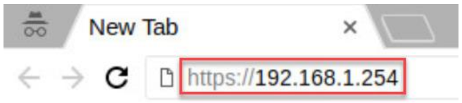
1. Click on the **Client** tab to access the Client PC.



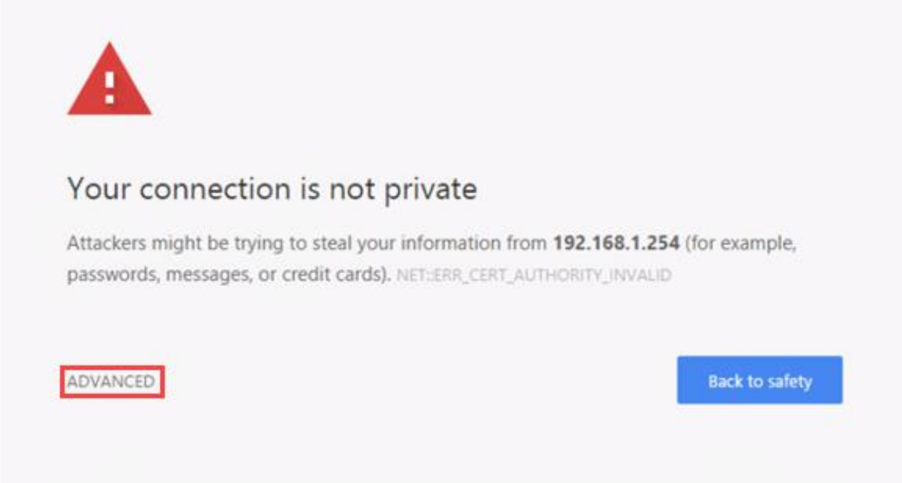
2. Log in to the Client PC as username `lab-user`, password `Train1ng$`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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.

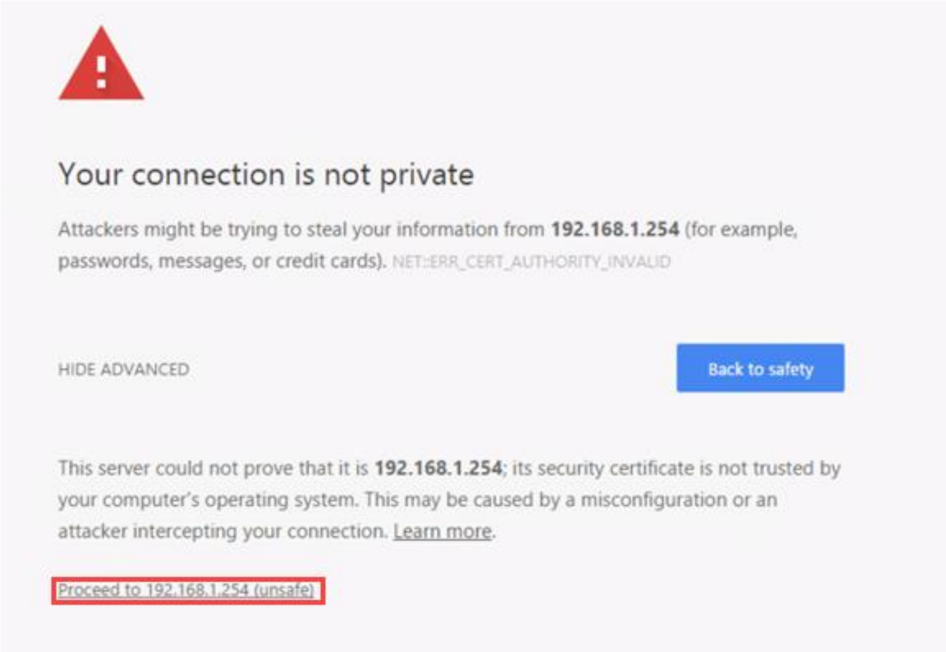


Your connection is not private

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)**.



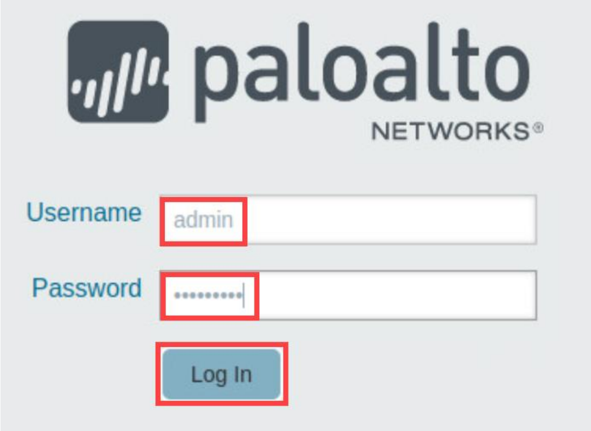
Your connection is not private

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.

Proceed to 192.168.1.254 (unsafe)

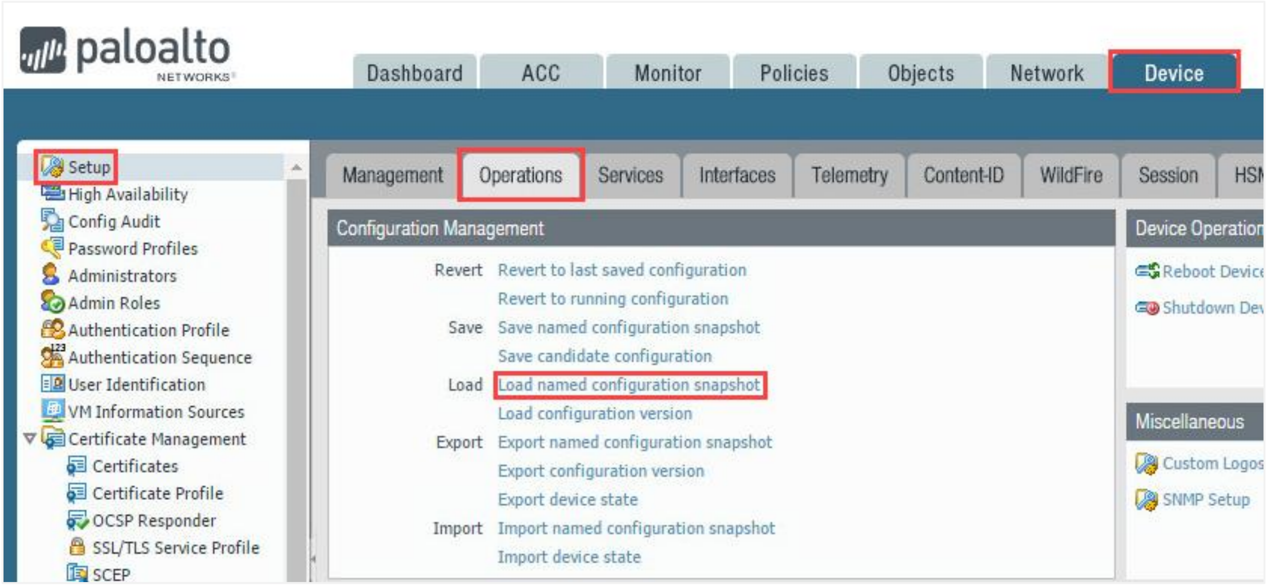
7. Log in to the Firewall web interface as username `admin`, password `Train1ng$`.



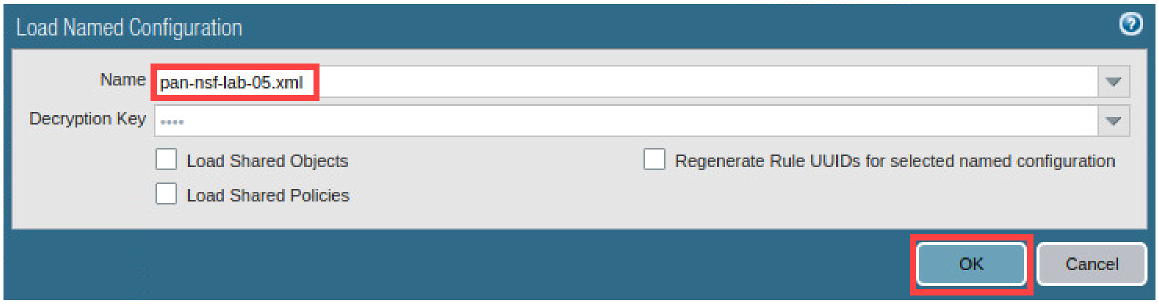
Username admin

Password •••••••••

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-nsf-lab-05.xml** from the *Name* dropdown box and click **OK**.

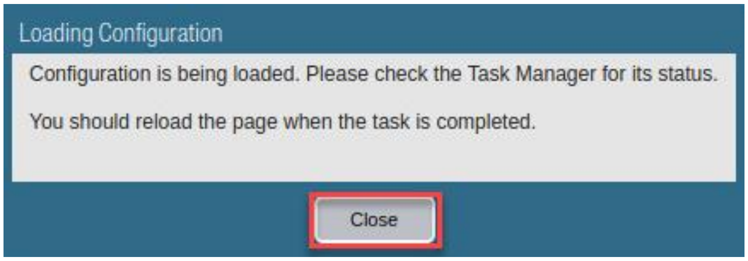

Load Named Configuration

Name pan-nsf-lab-05.xml

Decryption Key ••••

□ Load Shared Objects
□ Regenerate Rule UUIDs for selected named configuration
□ Load Shared Policies

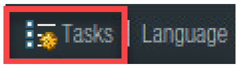
10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

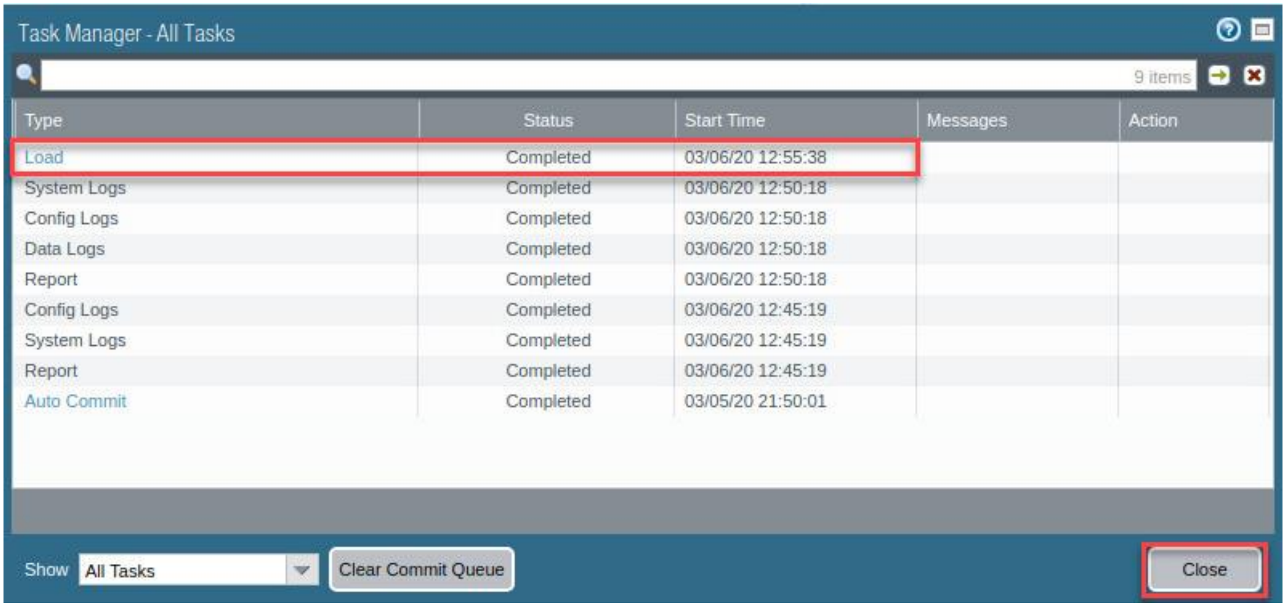
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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

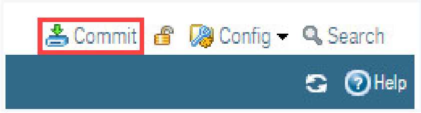


12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**

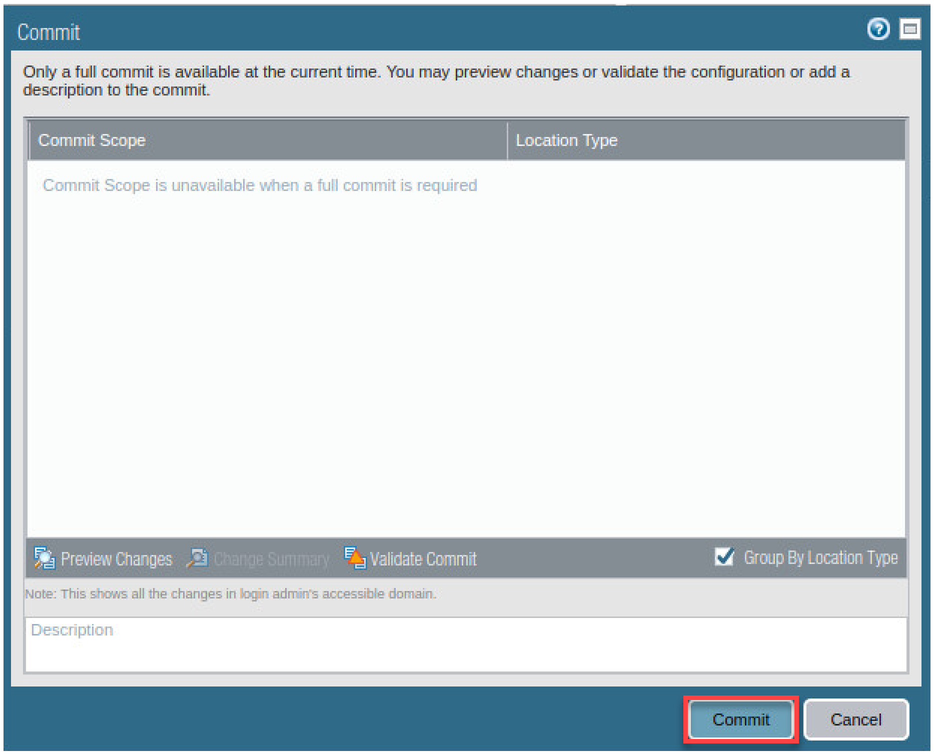


Type	Status	Start Time	Messages	Action
Load	Completed	03/06/20 12:55:38		
System Logs	Completed	03/06/20 12:50:18		
Config Logs	Completed	03/06/20 12:50:18		
Data Logs	Completed	03/06/20 12:50:18		
Report	Completed	03/06/20 12:50:18		
Config Logs	Completed	03/06/20 12:45:19		
System Logs	Completed	03/06/20 12:45:19		
Report	Completed	03/06/20 12:45:19		
Auto Commit	Completed	03/05/20 21:50:01		

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.

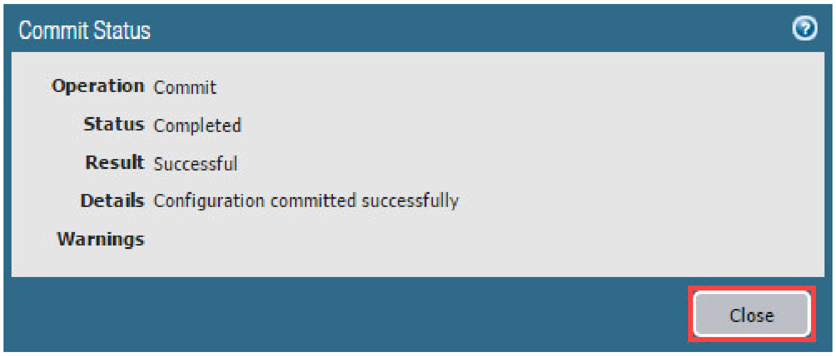


Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

Commit Scope	Location Type
Commit Scope is unavailable when a full commit is required	

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

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



Commit Status

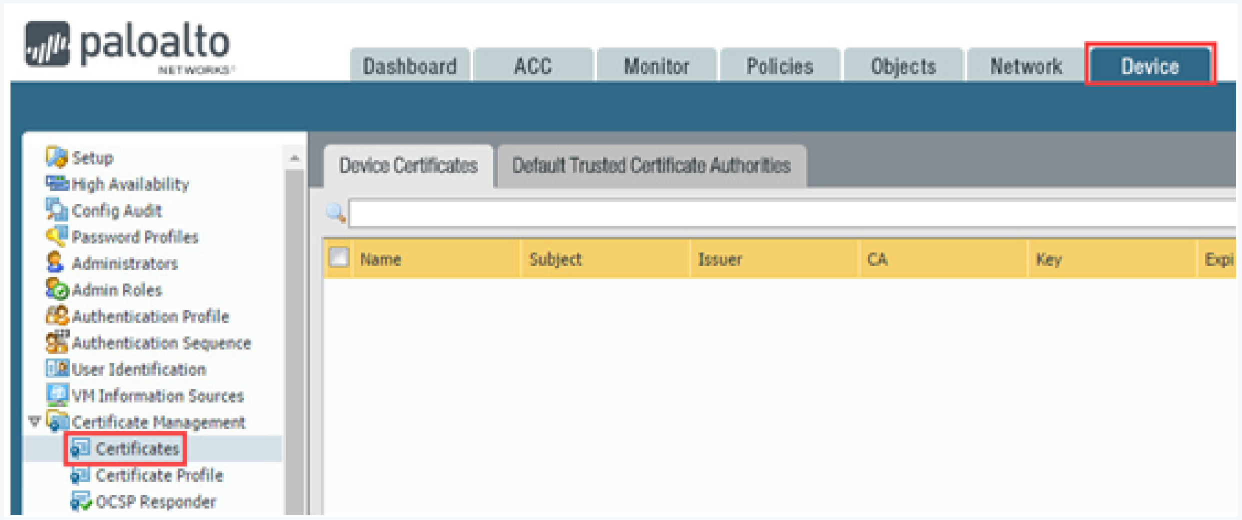
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

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.

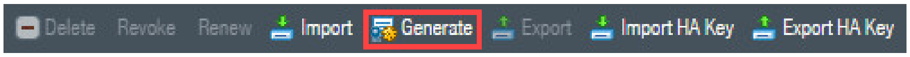
5.1 Generate Certificates

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 new certificate for the Firewall to use for Inbound Management Traffic, replacing the default certificate issued specifically for this lab environment.

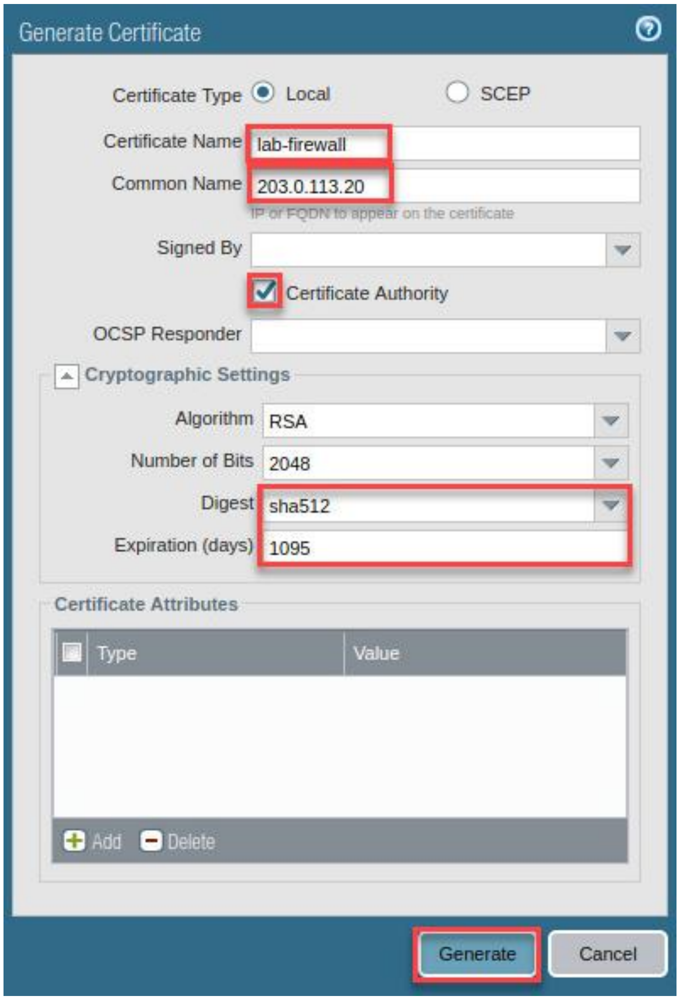
1. Navigate to **Device** > **Certificate Management > Certificates**.



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



3. In the *Generate Certificate* window, type `lab-firewall` in the *Certificate Name* field. Then, type `203.0.113.20` in the *Common Name* field. Next, click the **Certificate Authority** checkbox. Then, select **sha512** in the *Digest* dropdown. Next, type `1095` in the *Expiration (days)* field. Finally, click the **Generate** button.


Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: lab-firewall

Common Name: 203.0.113.20

IP or FQDN to appear on the certificate

Signed By:

☑ Certificate Authority

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

Digest: sha512

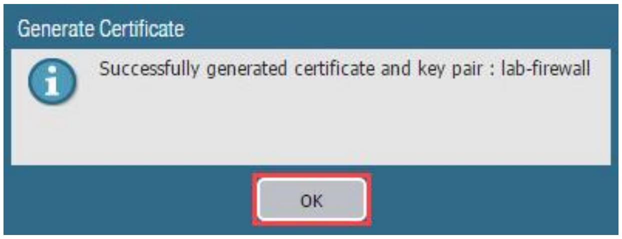
Expiration (days): 1095

Certificate Attributes

□	Type	Value

This will generate a certificate for the Firewall to act as a root Certificate Authority (CA). The IP address, **203.0.113.20**, used in the Common Name field is the Firewall's outside IP address. It is best practice that a digest algorithm of sha256 or higher is used for enhanced security. By increasing the default digest to **sha512**, you have created a much stronger certificate. The Expiration (days) field is equivalent to 3 years (365 days x 3 years = 1,095 days).

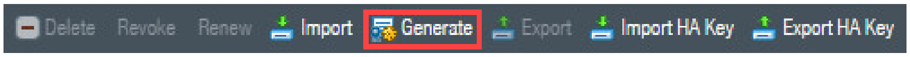
4. In the *Generate Certificate* window, click **OK** to continue.



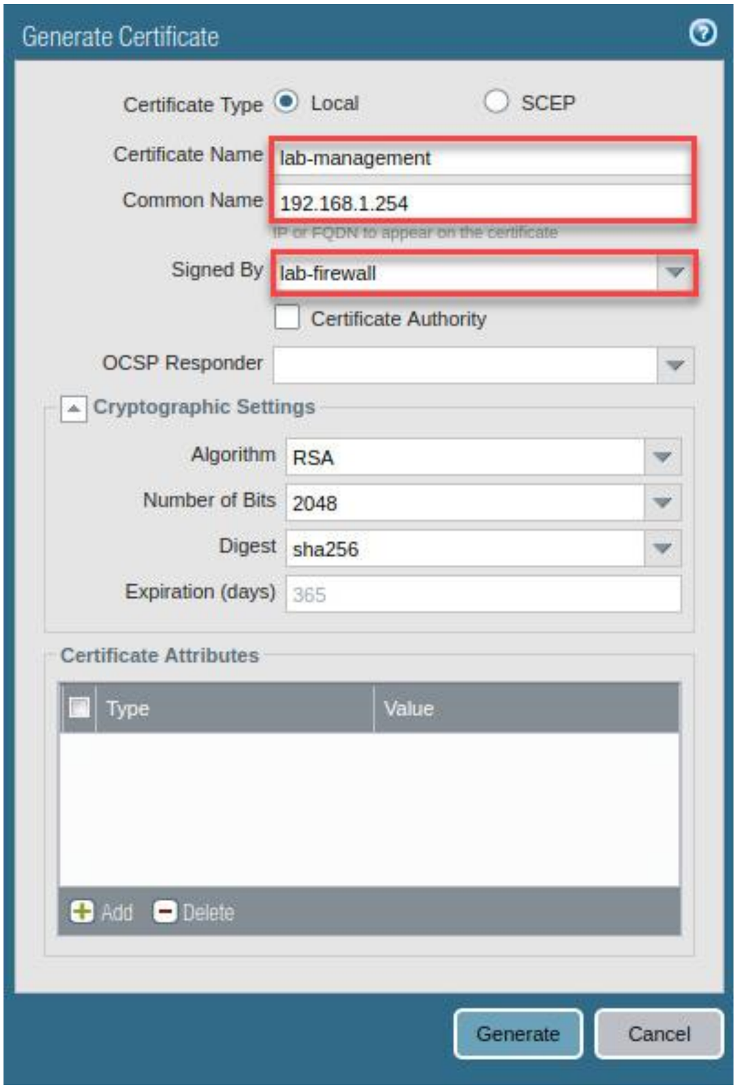
Generate Certificate

Successfully generated certificate and key pair : lab-firewall

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



6. In the *Generate Certificate* window, type `lab-management` in the *Certificate Name* field. Then, type `192.168.1.254` in the *Common Name* field. Next, select **lab-firewall** in the *Signed By* dropdown. Continue to step 7.



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: lab-management

Common Name: 192.168.1.254

IP or FQDN to appear on the certificate

Signed By: lab-firewall

□ Certificate Authority

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

Digest: sha256

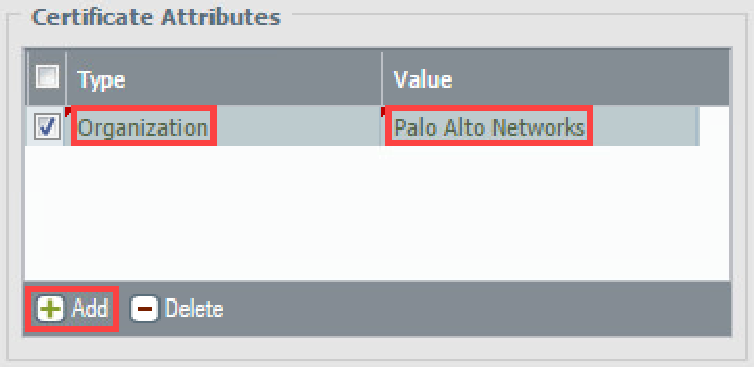
Expiration (days): 365

Certificate Attributes

□	Type	Value

> The IP address, **192.168.1.254**, used in the Common Name field is the Firewall's inside IP address. Notice you selected the previously created root CA certificate, **lab-firewall**, to sign this certificate. Client certificates that are used when requesting firewall services that rely on TLSv1.2 (such as administrator access to the web interface) cannot have sha512 as a digest algorithm, therefore you will leave the default **sha256**.

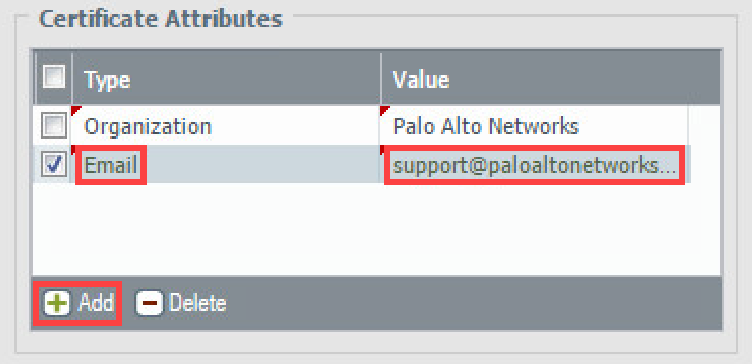
7. In the *Generate Certificate* window, click the **Add** button in the *Certificate Attributes* section. Then, select **Organization** in the *Type* column. Next, double-click the empty box in the *Value* column, type `Palo Alto Networks` and press **Enter**.



Certificate Attributes

□	Type	Value
☑	Organization	Palo Alto Networks

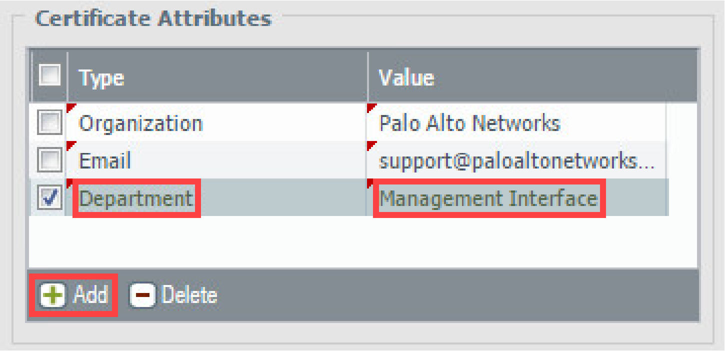
8. In the *Generate Certificate* window, click the **Add** button in the *Certificate Attributes* section. Then, select **Email** in the *Type* column. Next, double-click the empty box in the *Value* column, type `support@paloaltonetworks.com` and press **Enter**.



Certificate Attributes

□	Type	Value
□	Organization	Palo Alto Networks
☑	Email	support@paloaltonetworks...

9. In the *Generate Certificate* window, click the **Add** button in the *Certificate Attributes* section. Then, select **Department** in the *Type* column. Next, double-click the empty box in the *Value* column, type **`Management Interface`**, and press **Enter**.

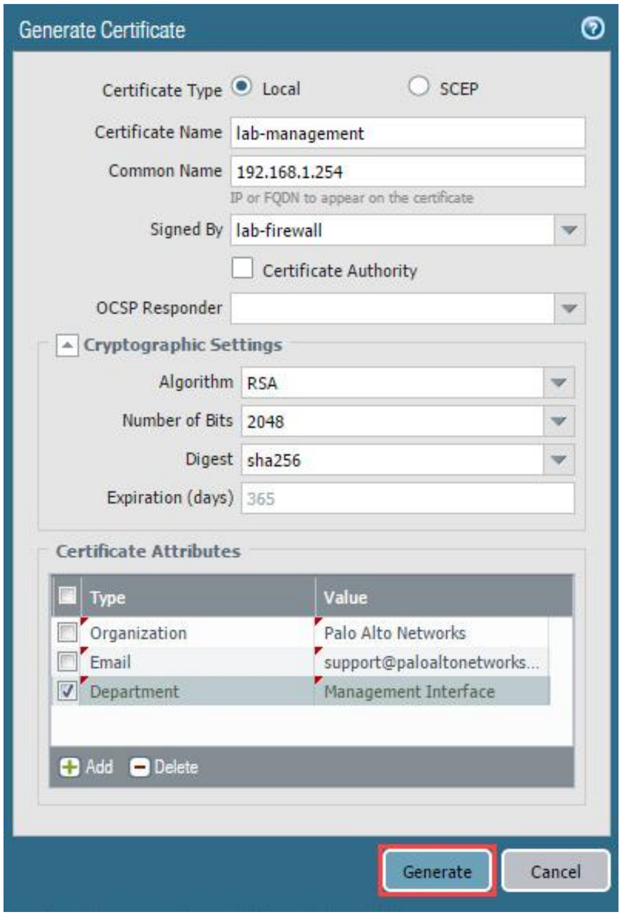


Certificate Attributes

☐	Type	Value
☐	Organization	Palo Alto Networks
☐	Email	support@paloaltonetworks...
☑	Department	Management Interface

Certificate Attributes are used to uniquely identify the firewall and the service that will use the certificate.

10. In the *Generate Certificate* window, review the settings. Then, click the **Generate** button.



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: lab-management

Common Name: 192.168.1.254

IP or FQDN to appear on the certificate

Signed By: lab-firewall

☐ Certificate Authority

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

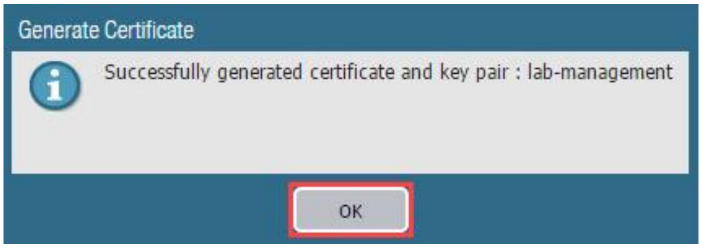
Digest: sha256

Expiration (days): 365

Certificate Attributes

☐	Type	Value
☐	Organization	Palo Alto Networks
☐	Email	support@paloaltonetworks...
☑	Department	Management Interface

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



Generate Certificate

Successfully generated certificate and key pair : lab-management

Palo Alto Networks Firewalls use certificates in the following applications:

- User authentication for Captive Portal, GlobalProtect™, Mobile Security Manager, and web interface access to a firewall or Panorama.
- Device authentication for GlobalProtect VPN (remote user-to-site or large scale).
- Device authentication for IPSec site-to-site VPN with Internet Key Exchange (IKE).
- Decrypting inbound and outbound SSL traffic.

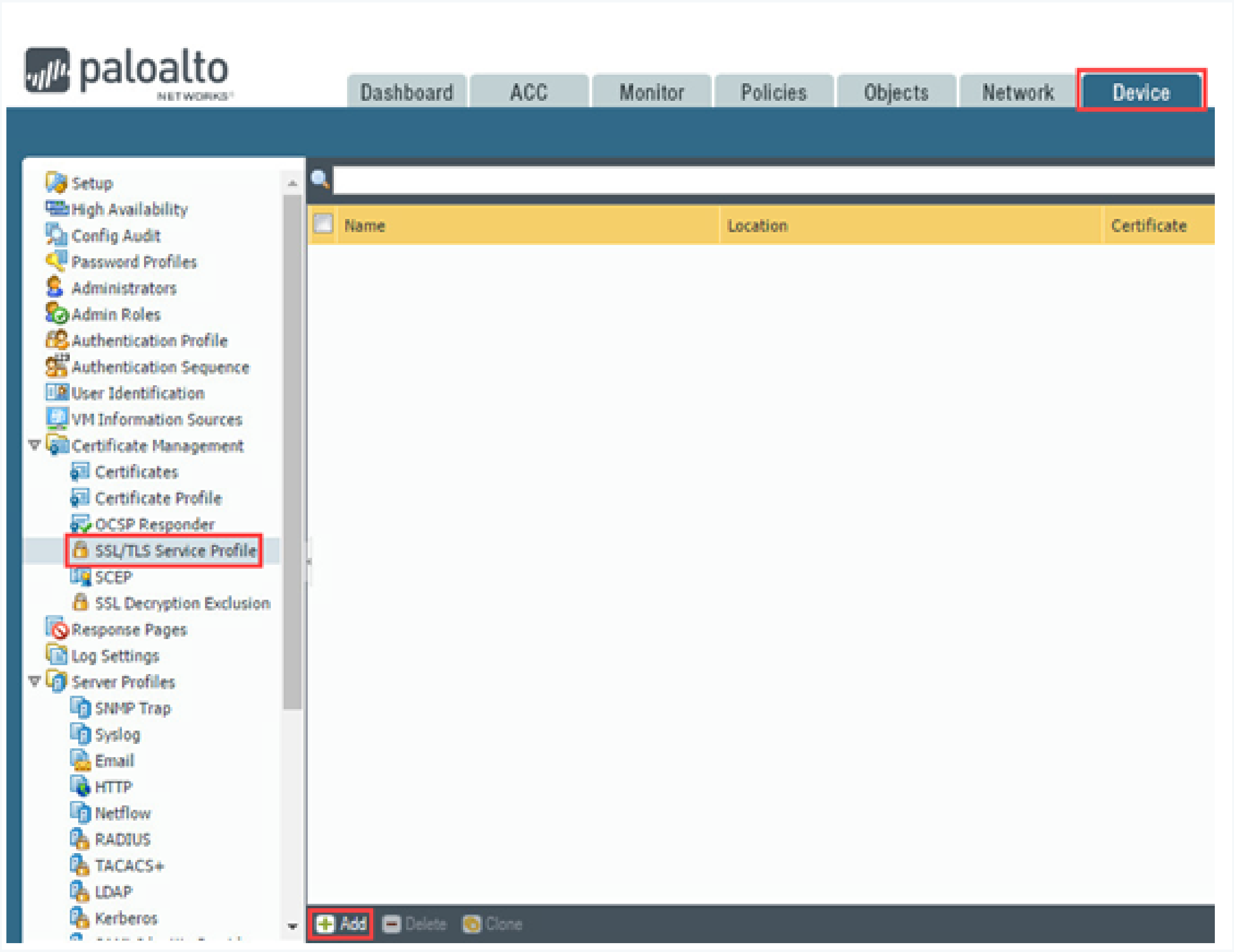
As a best practice, it is recommended you use different certificates for each usage.

In a real-world scenario, you can simplify your certificate deployment by using a certificate that the client systems already trust. It is recommended that you import a certificate and private key from your enterprise certificate authority (CA) or obtain a certificate from an external CA. The trusted root certificate store of the client systems is likely to already have the associated root CA certificate that ensures trust. This prevents you from having to create a root CA certificate and install it on every client system to prevent a certificate error.

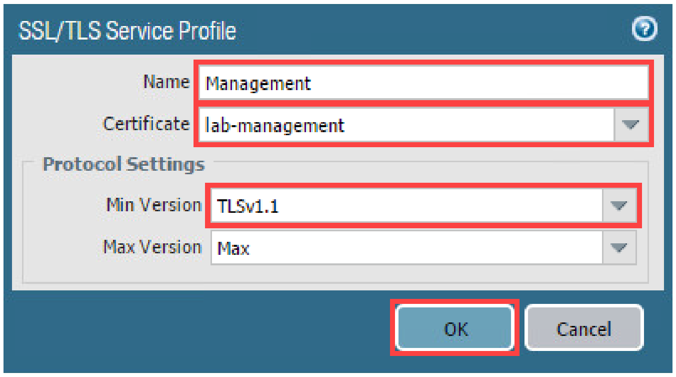
5.2 Replace the Certificate for Inbound Management Traffic

In this section, you will replace the certificate for inbound management traffic. When you boot the Firewall for the first time, it automatically generates a default certificate that enables HTTPS access to the web interface over the management (MGT) interface. To improve the security of inbound management traffic, you will configure an SSL/TLS Service Profile to replace the default certificate with the **lab-management** certificate you specifically created for this purpose. Then, you will apply the SSL/TLS Service Profile to inbound management traffic.

1. Navigate to **Device > Certificate Management > SSL/TLS Service Profile > Add.**



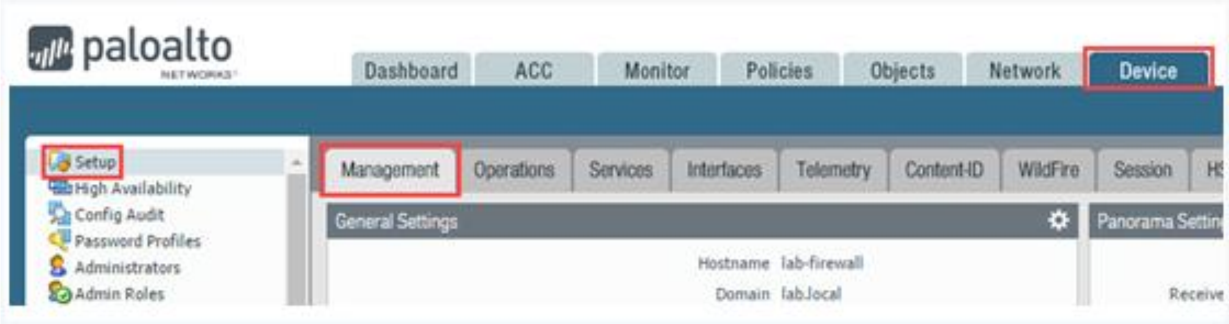
2. In the *SSL/TLS Service Profile* window, type `Management` in the *Name* field. Then, select **lab-management** from the *Certificate* dropdown. Next, select **TLSv1.1** from the *Min Version* dropdown. Finally, click the **OK** button.



Name: Management
Certificate: lab-management

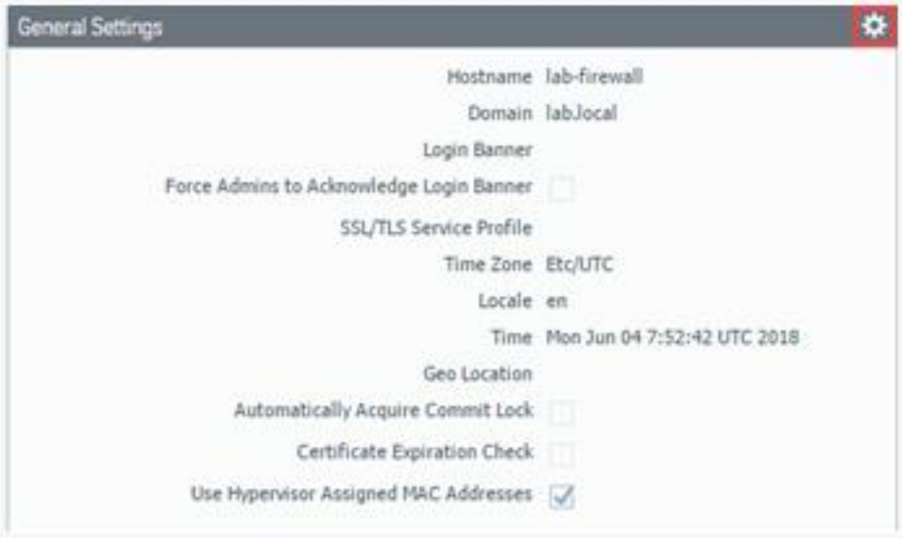
Protocol Settings
Min Version: TLSv1.1
Max Version: Max

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



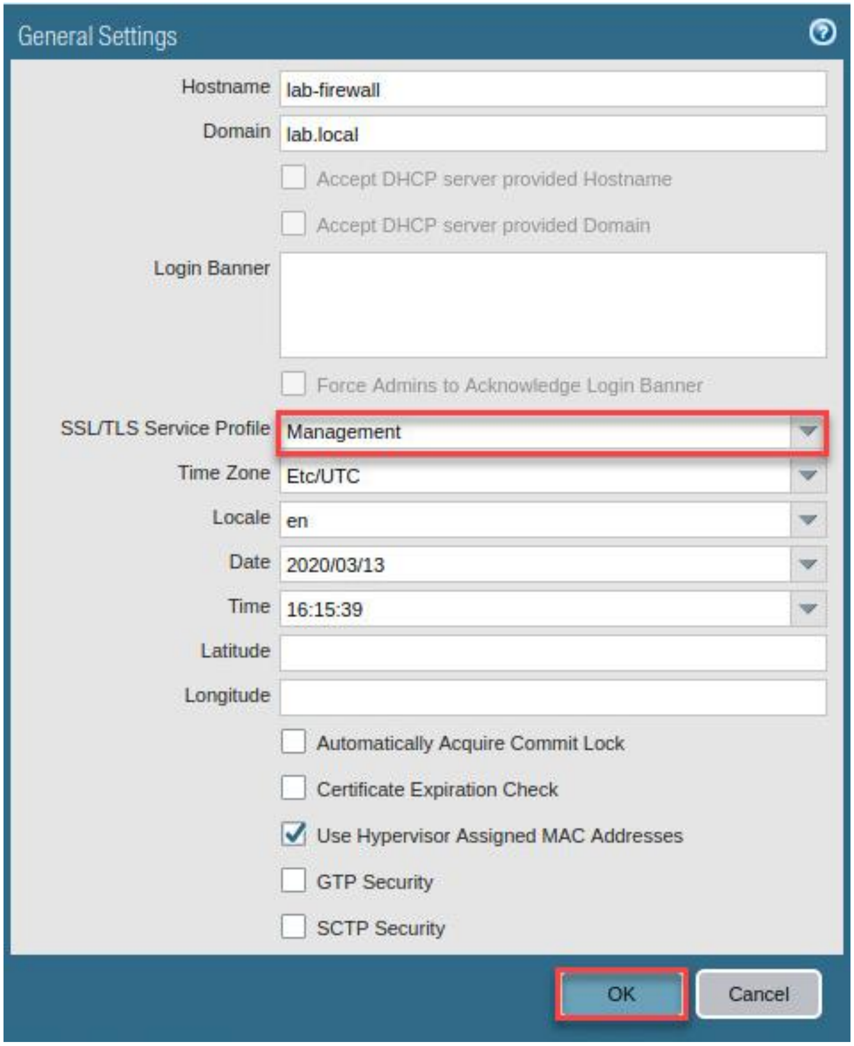
Hostname: lab-firewall
Domain: lab.local

4. Click the **gear** icon on the *General Settings* section, located in the center.



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: Mon Jun 04 7:52:42 UTC 2018
Geo Location
Automatically Acquire Commit Lock: □
Certificate Expiration Check: □
Use Hypervisor Assigned MAC Addresses: ☑

5. In the *General Settings* window, select **Management** from the *SSL/TLS Service Profile* dropdown. Then, click the **OK** button.



General Settings

Hostname: lab-firewall

Domain: lab.local

□ Accept DHCP server provided Hostname

□ Accept DHCP server provided Domain

Login Banner:

□ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: Management

Time Zone: Etc/UTC

Locale: en

Date: 2020/03/13

Time: 16:15:39

Latitude:

Longitude:

□ Automatically Acquire Commit Lock

□ Certificate Expiration Check

☑ Use Hypervisor Assigned MAC Addresses

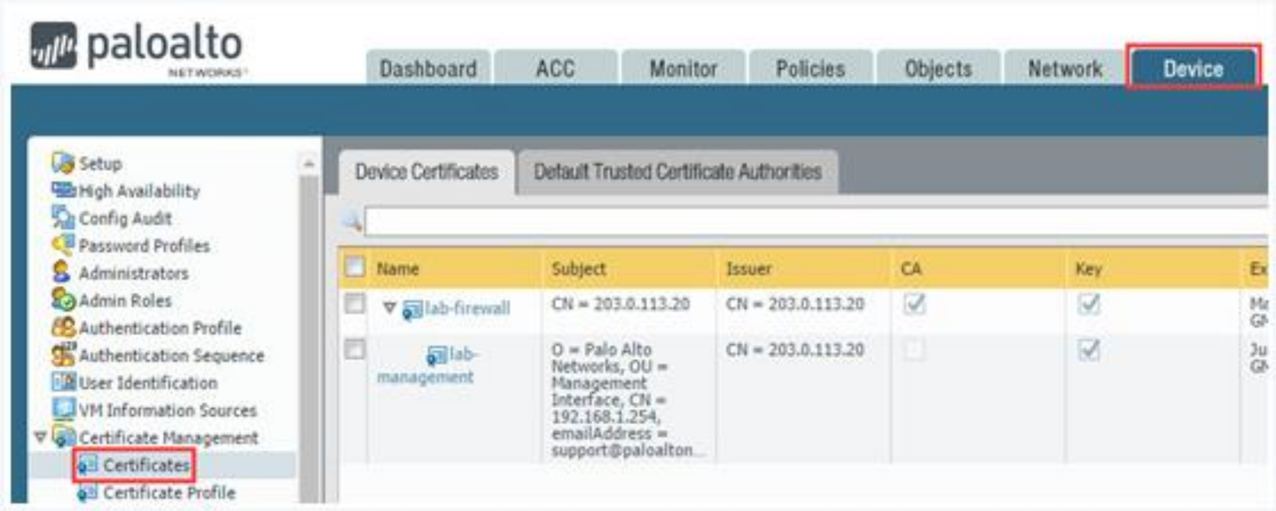
□ GTP Security

□ SCTP Security

5.3 Export Certificate and Commit

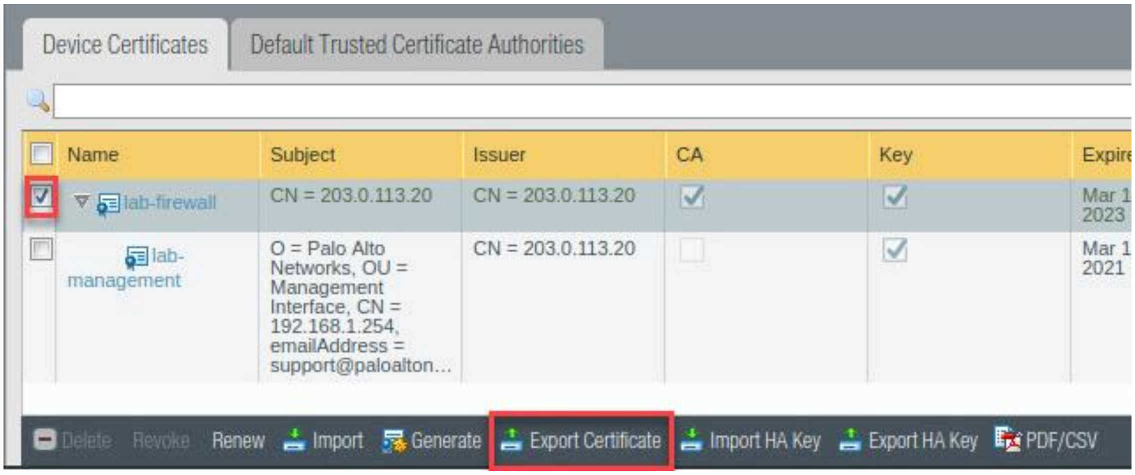
In this section, you will export the **lab-firewall** certificate. Then, you will commit your changes to the Firewall.

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



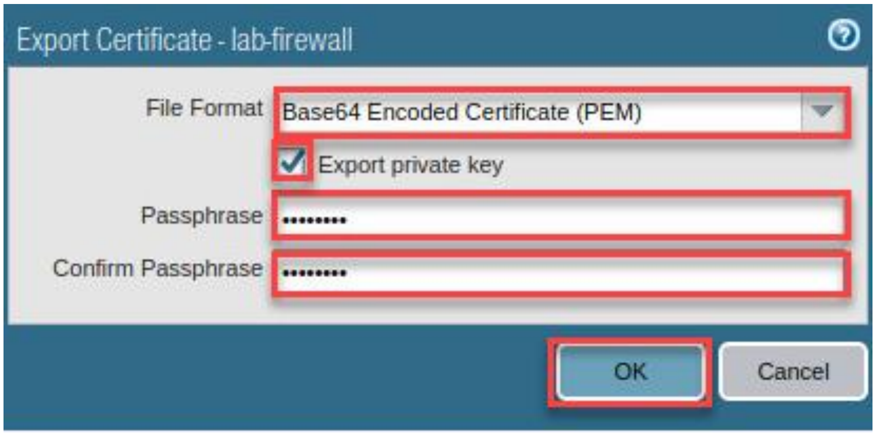
□	Name	Subject	Issuer	CA	Key	Ex
□	lab-firewall	CN = 203.0.113.20	CN = 203.0.113.20	☑	☑	Ma GM
□	lab-management	O = Palo Alto Networks, OU = Management Interface, CN = 192.168.1.254, emailAddress = support@paloalton...	CN = 203.0.113.20	□	☑	Ju GM

2. Click the checkbox for **lab-firewall**. Then, click on the **Export Certificate** button at the bottom.



□	Name	Subject	Issuer	CA	Key	Expire
☑	lab-firewall	CN = 203.0.113.20	CN = 203.0.113.20	☑	☑	Mar 1 2023
□	lab-management	O = Palo Alto Networks, OU = Management Interface, CN = 192.168.1.254, emailAddress = support@paloalton...	CN = 203.0.113.20	□	☑	Mar 1 2021

3. In the *Export Certificate - lab-firewall* window, select **Base64 Encoded Certificate (PEM)** in the *File Format* dropdown. Check **Export private key**. Then, type `paloalto` for the *Passphrase* and *Confirm Passphrase* fields, and then click on the **OK** button.



Export Certificate - lab-firewall

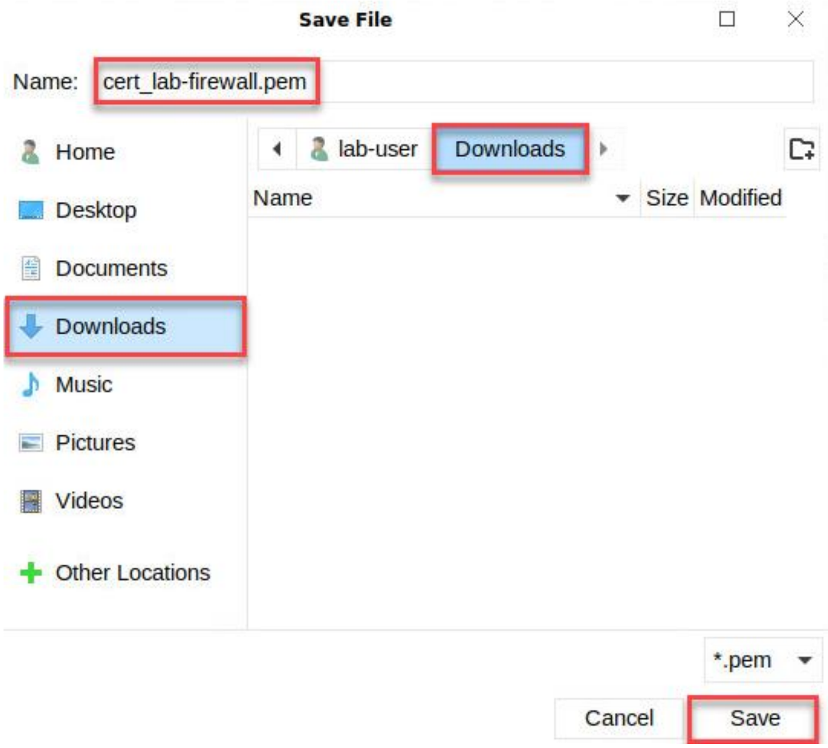
File Format: Base64 Encoded Certificate (PEM)

☑ Export private key

Passphrase: ••••••••

Confirm Passphrase: ••••••••

4. In the *Save File* window, make sure **cert_lab-firewall.pem** is located in the *Name* field, verify that *cert_lab-firewall* is going to the **Downloads** folder. Then, click the **Save** button.

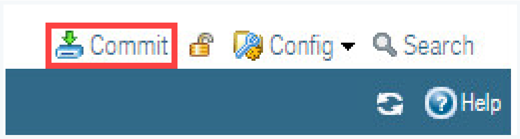


Save File

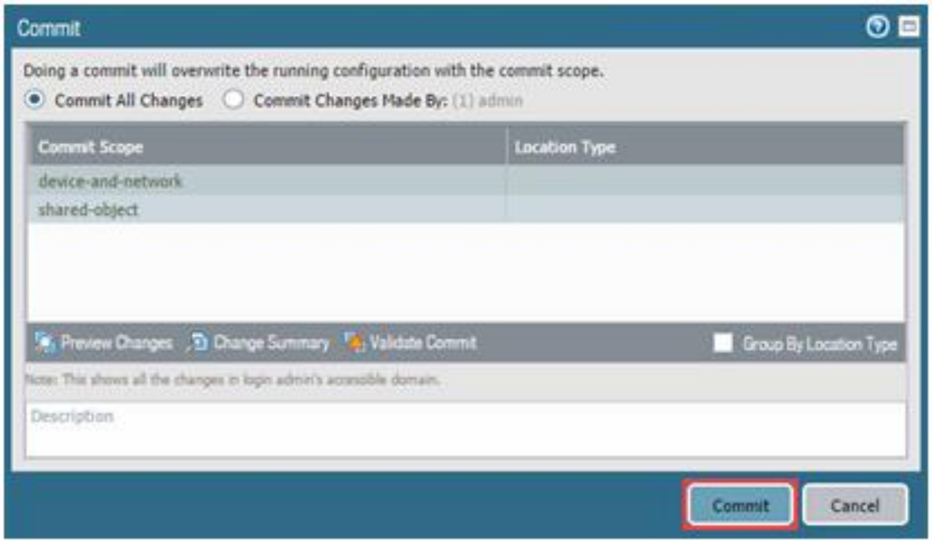
Name: cert_lab-firewall.pem

By using the **Base64 Encoded Certificate (PEM) File Format**, this generates a certificate signing request to accept SSL certificates.

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.



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

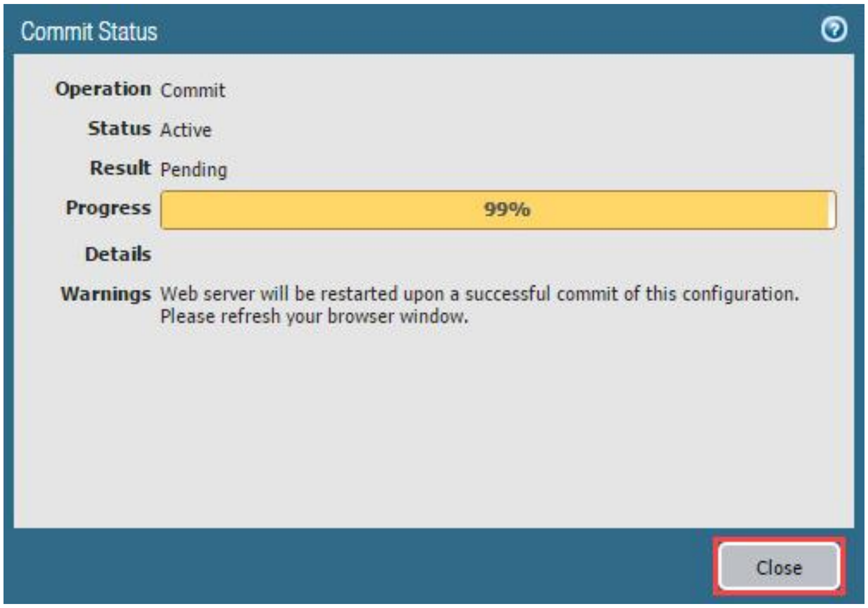
● Commit All Changes ○ Commit Changes Made By: (1) admin

Commit Scope	Location Type
device-and-network	
shared-object	

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

Description

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



Operation Commit

Status Active

Result Pending

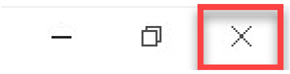
Progress 99%

Details

Warnings 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%.

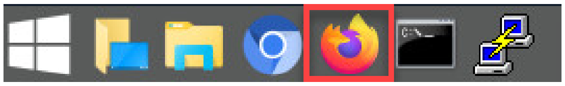
8. Click the **X** in the upper-right to close *Chromium*.



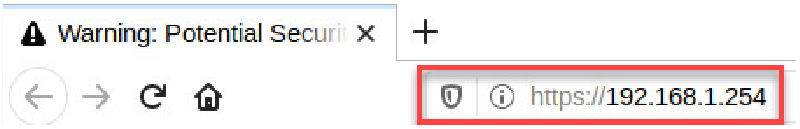
5.4 Test Connectivity and Import Certificate on the Client

In this section, you will test the connectivity to the Firewall. When establishing a secure connection with the Firewall, the Client must trust the root CA that issued the certificate. Otherwise, the Client browser will display a warning that the certificate is invalid and might (depending on security settings) block the connection. To prevent this, you will import the lab-firewall certificate on the Client, creating a trust relationship between the Firewall and the Client machine. Then, you will test connectivity again.

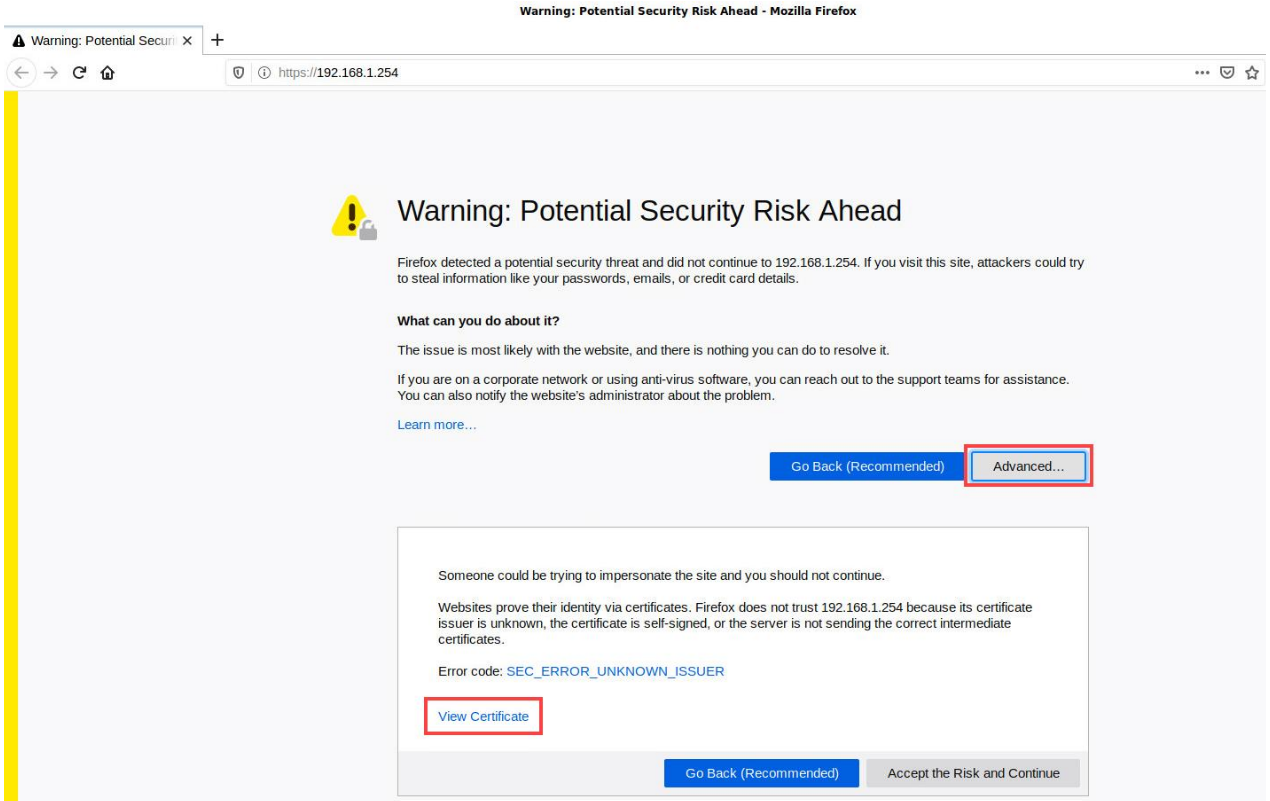
1. Open **Firefox** from the taskbar.



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



3. You will see a "*Warning: Potential Security Risk Ahead*" message. This is because the Client cannot verify the certificate from the Firewall. To view the certificate, click the **Advanced** button, scroll to the bottom of the security window, and select **View Certificate**.


Warning: Potential Security Risk Ahead - Mozilla Firefox
Warning: Potential Securi
https://192.168.1.254
Learn more…
Go Back (Recommended)
Advanced…
View Certificate
Go Back (Recommended)
Accept the Risk and Continue

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.1.254. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

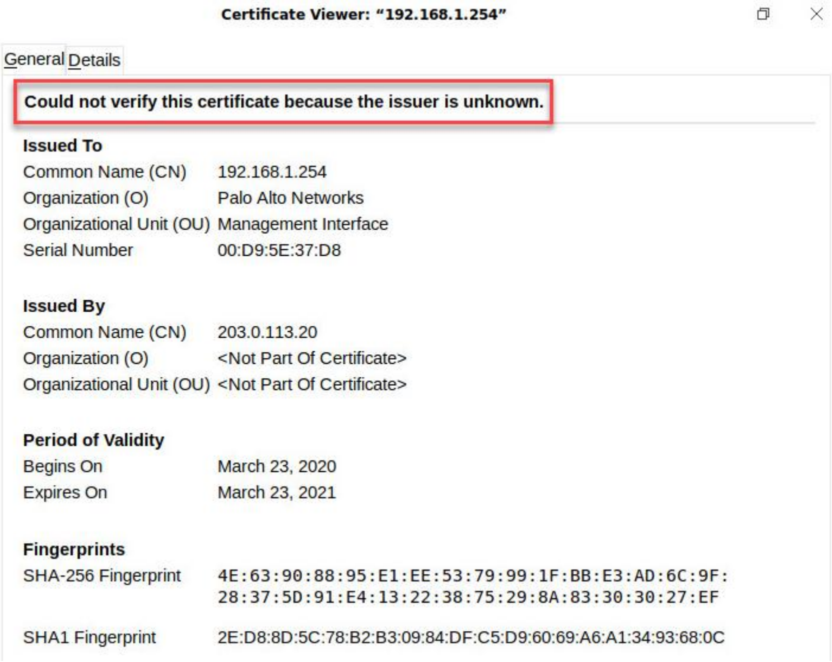
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 192.168.1.254 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

4. In the *Certificate Viewer: "192.168.1.254"* window, note that the certificate *Could not verify this certificate because the issuer is unknown*.



Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	192.168.1.254
Organization (O)	Palo Alto Networks
Organizational Unit (OU)	Management Interface
Serial Number	00:D9:5E:37:D8

Issued By

Common Name (CN)	203.0.113.20
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

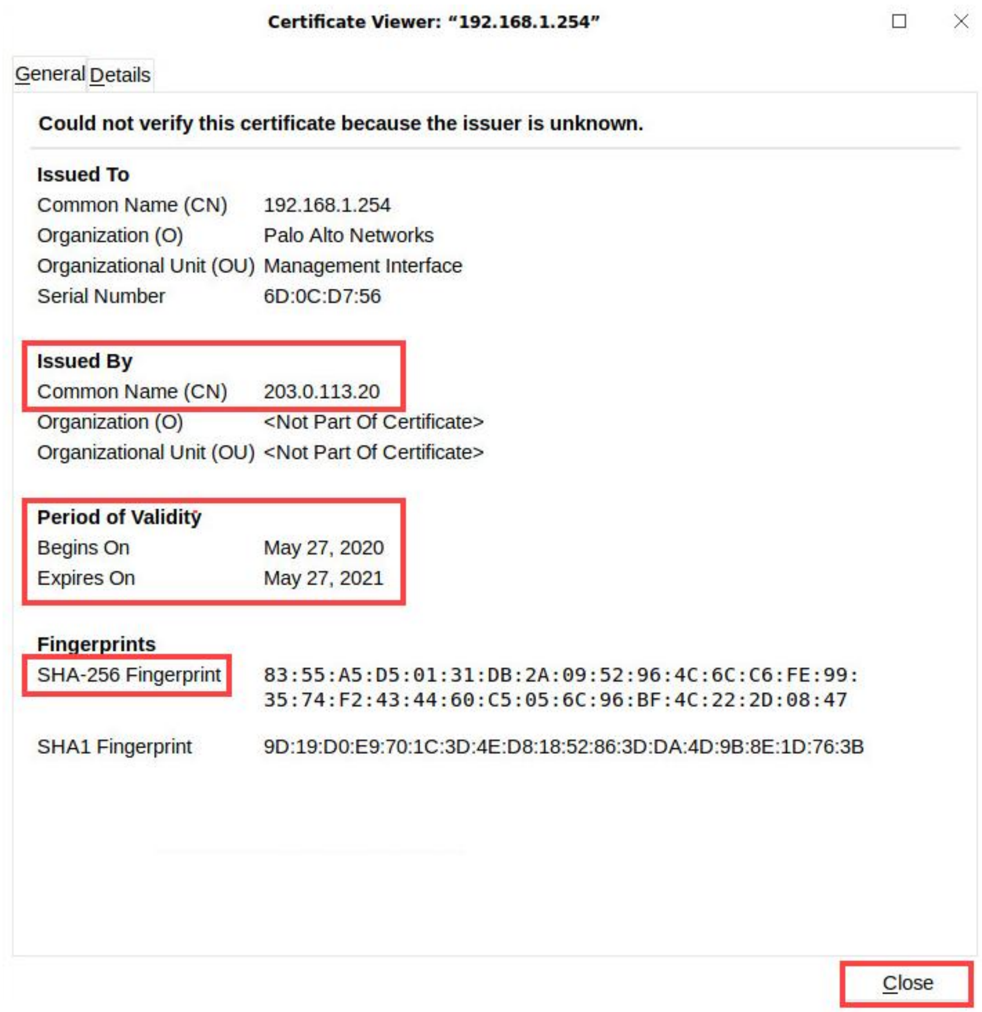
Period of Validity

Begins On	March 23, 2020
Expires On	March 23, 2021

Fingerprints

SHA-256 Fingerprint	4E:63:90:88:95:E1:EE:53:79:99:1F:BB:E3:AD:6C:9F: 28:37:5D:91:E4:13:22:38:75:29:8A:83:30:30:27:EF
SHA1 Fingerprint	2E:D8:8D:5C:78:B2:B3:09:84:DF:C5:D9:60:69:A6:A1:34:93:68:0C

5. In the *Certificate Viewer: 192.168.1.254 window*, View the content on the *General* tab under the *Certificate Error* section. Lastly, click **Close**.



Certificate Viewer: "192.168.1.254"

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	192.168.1.254
Organization (O)	Palo Alto Networks
Organizational Unit (OU)	Management Interface
Serial Number	6D:0C:D7:56

Issued By

Common Name (CN)	203.0.113.20
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Period of Validity

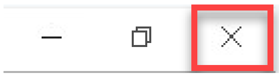
Begins On	May 27, 2020
Expires On	May 27, 2021

Fingerprints

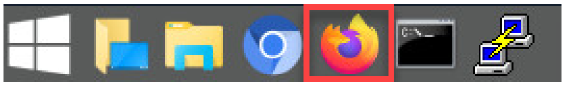
SHA-256 Fingerprint	83:55:A5:D5:01:31:DB:2A:09:52:96:4C:6C:C6:FE:99: 35:74:F2:43:44:60:C5:05:6C:96:BF:4C:22:2D:08:47
SHA1 Fingerprint	9D:19:D0:E9:70:1C:3D:4E:D8:18:52:86:3D:DA:4D:9B:8E:1D:76:3B

Notice on the general tab it matches the **lab-management** certificate you created earlier in section 5.1. The sha256 algorithm is being used in the Fingerprints. The certificate was issued by **203.0.113.20**, which is the common-name of the root CA certificate, **lab-firewall**, you created. The Validity Period indicates the certificate is valid for 365 days. The Issued To indicates the common name of **192.168.1.254** which is the management interface of the firewall. The Organization is **Palo Alto Networks**.

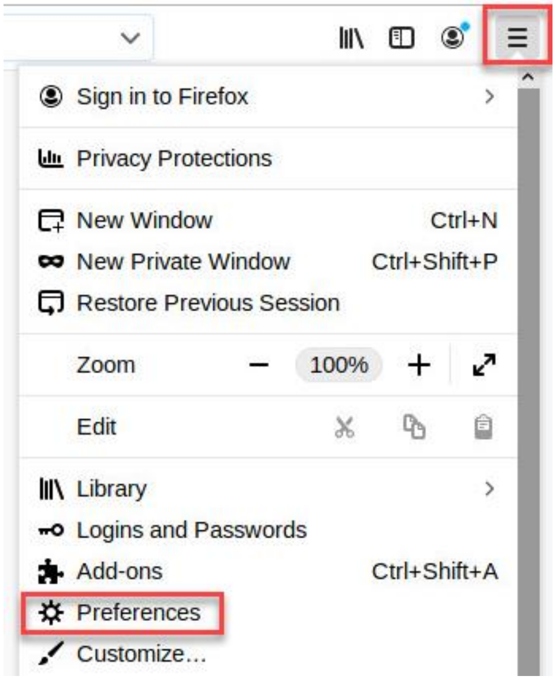
6. Click the **X** in the upper-right to close *Firefox*.



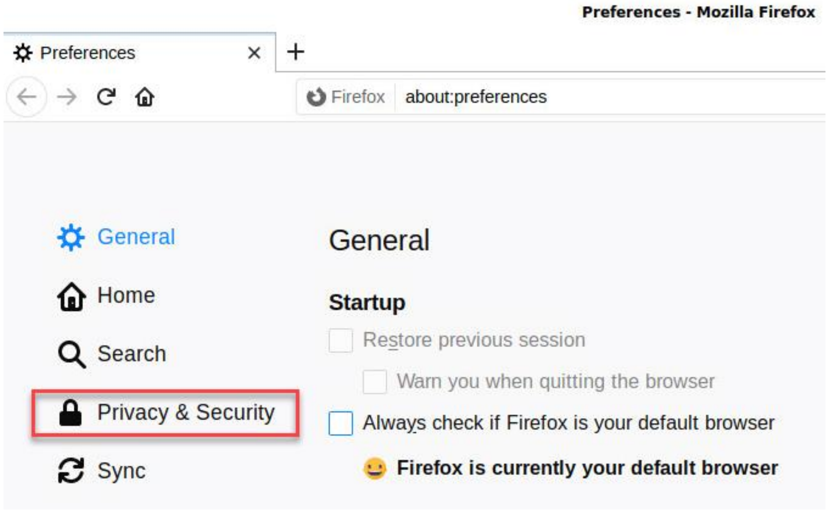
7. To install the **lab-firewall** certificate, open **Firefox** from the taskbar.



8. Click on the **3-bar menu** icon in *Firefox* and click **Preferences**.



9. In the *Preferences* window, click on **Privacy & Security.**



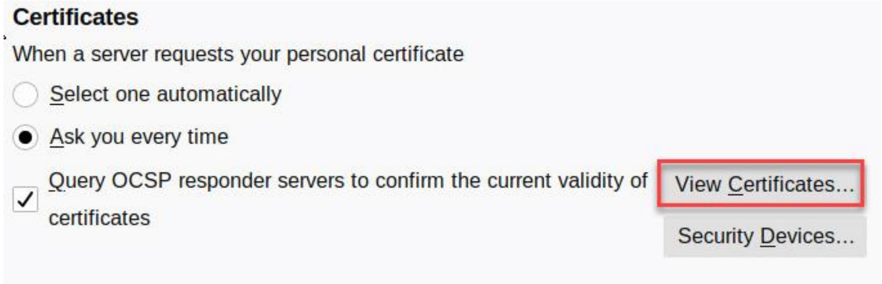
□ Restore previous session

□ Warn you when quitting the browser

□ Always check if Firefox is your default browser

Firefox is currently your default browser

10. Scroll down to the *Certificates* options and click on **View Certificates...**



Certificates

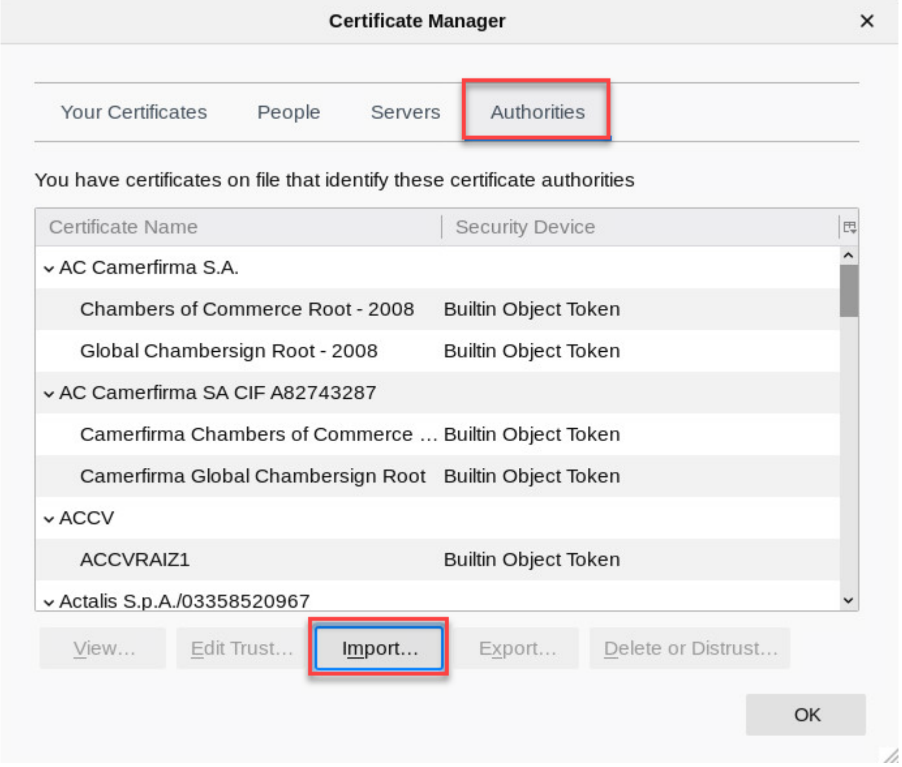
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

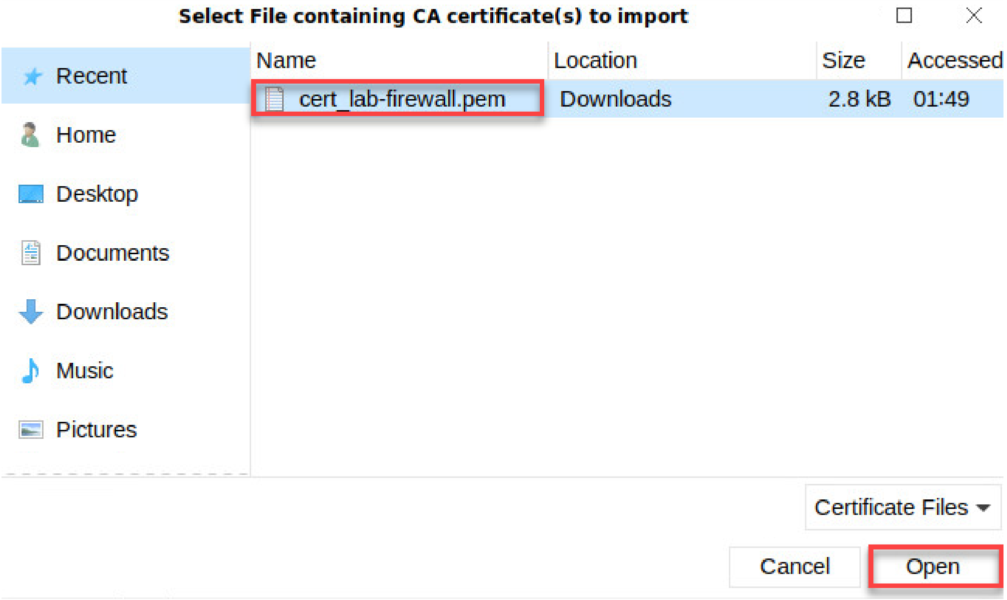
11. In the *Certificate Manager* window, click on **Authorities** and lastly click **Import...**



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce …	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	

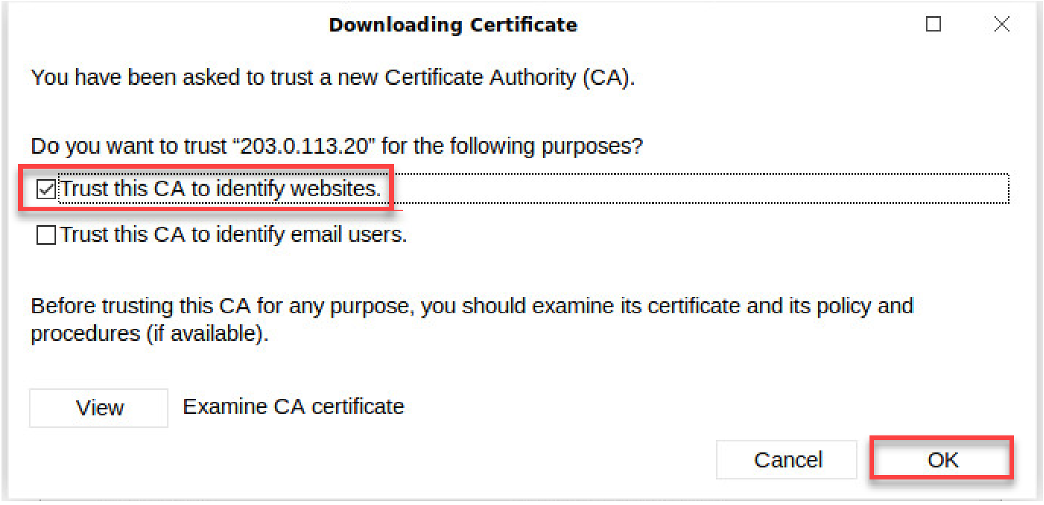
12. In the *Select File containing CA certificate(s) to import* window, make sure **cert_lab-firewall.pem** is selected. Then, click the **Open** button.



Select File containing CA certificate(s) to import

Name	Location	Size	Accessed
cert_lab-firewall.pem	Downloads	2.8 kB	01:49

13. In the *Downloading Certificate* window, select **Trust this CA to identify websites**. Click **OK**.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

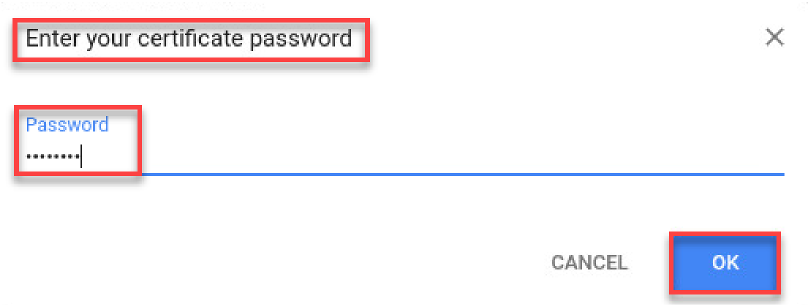
Do you want to trust "203.0.113.20" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

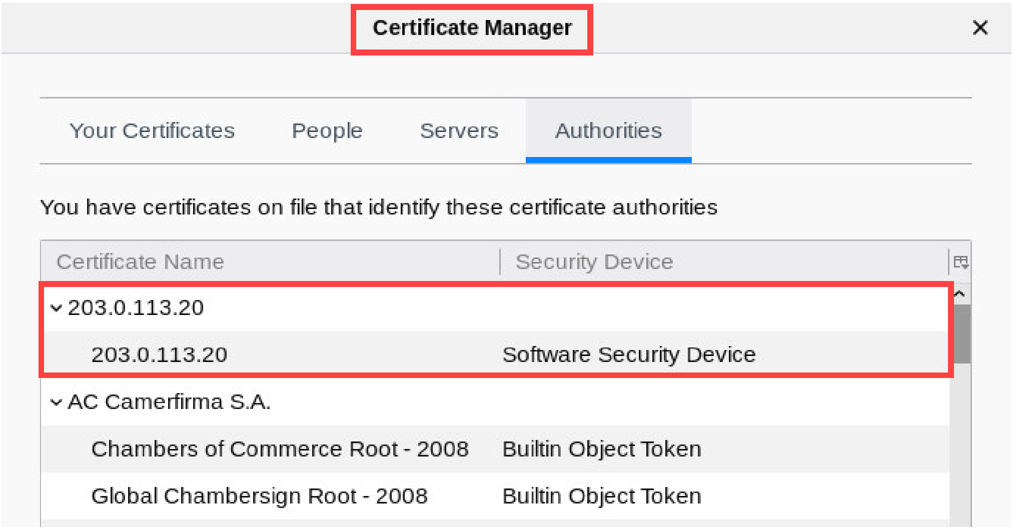
14. If the Enter *your certificate password* window pops up, enter `paloalto` and click **OK**.



Enter your certificate password

Password: ••••••••

15. In the *Certificate Manager* window, verify the **lab-firewall** certificate has imported.



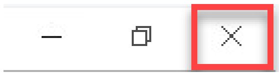
Certificate Manager

You have certificates on file that identify these certificate authorities

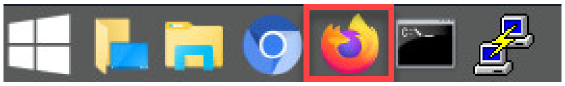
Certificate Name	Security Device
203.0.113.20	
203.0.113.20	Software Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token

Notice that the common-name of org-203.0.113.20 is showing. This is the common name of the firewall created in a previous step.

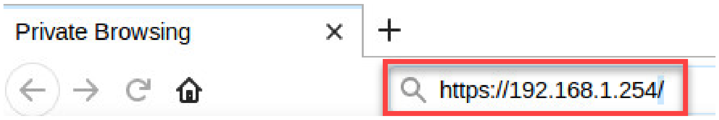
16. Click on the **X** in the upper-right to close *Firefox*.



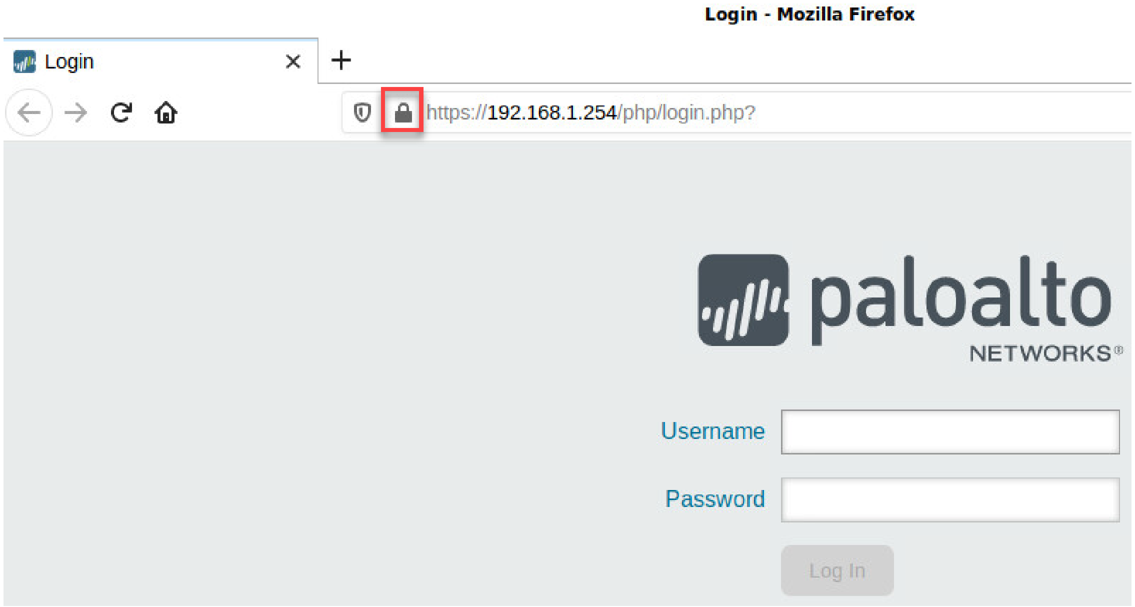
17. Open **Firefox** from the taskbar.



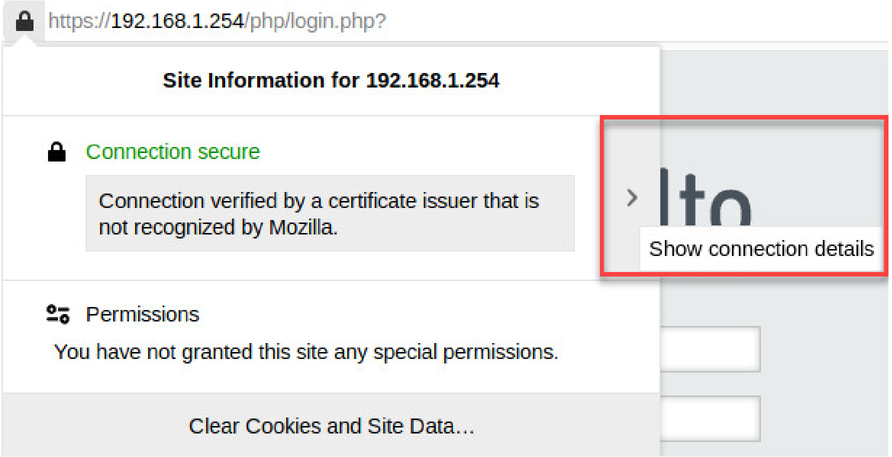
18. In the *Firefox address* field, type `https://192.168.1.254` and press **Enter.**



19. Now you will see the login prompt from the Firewall. Notice the ! icon in the address bar from before is now showing a secured padlock icon. Click on the **padlock icon**.



20. In the *Site Information for 192.168.1.254* popup, click the **Show Connection Details** link.


https://192.168.1.254/php/login.php?
Site Information for 192.168.1.254
Connection secure

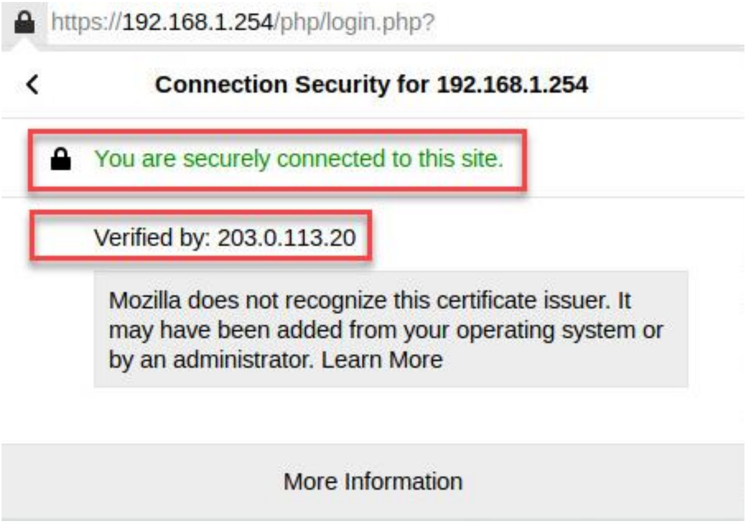
Connection verified by a certificate issuer that is not recognized by Mozilla.

Show connection details
Permissions

You have not granted this site any special permissions.

Clear Cookies and Site Data…

21. In the *Connection Security for 192.168.1.254* window, notice the message "*You are securely connected to this site*". Below, you will see it has also been "*Verified by: 203.0.113.20*".



https://192.168.1.254/php/login.php?

Connection Security for 192.168.1.254

You are securely connected to this site.

Verified by: 203.0.113.20

Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

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