NETWORK SECURITY FUNDAMENTALS V2

Lab 5: Managing Certificates

Document Version: 2024-01-17

Contents

Introduction

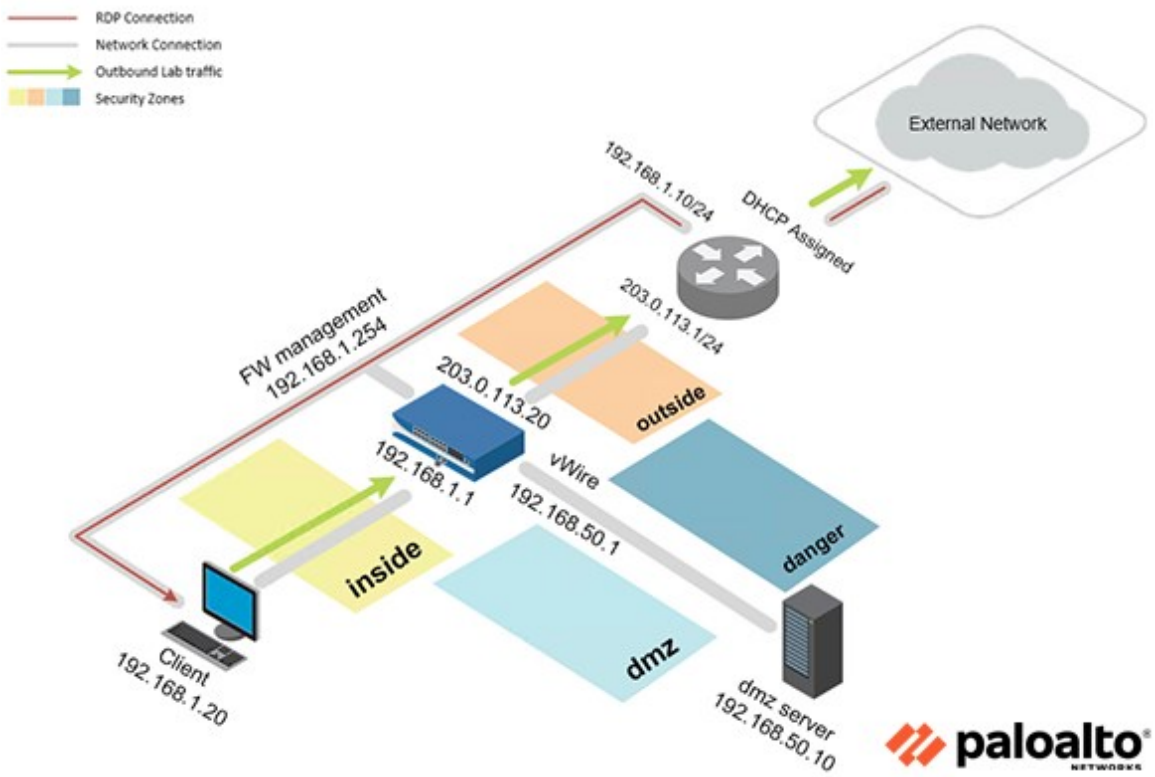
In this lab, you will generate a Self-Signed Root Certificate Authority (CA) certificate and replace the certificate for inbound management traffic. Then, you will import the root CA certificate on the Client machine.

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.

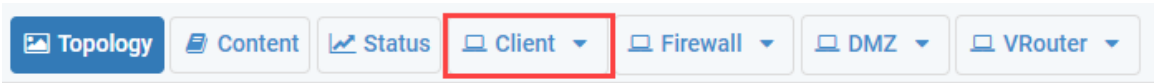
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Managing Certificates

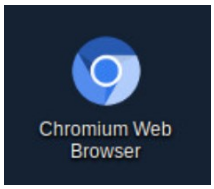
1.0 Load Lab Configuration

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

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

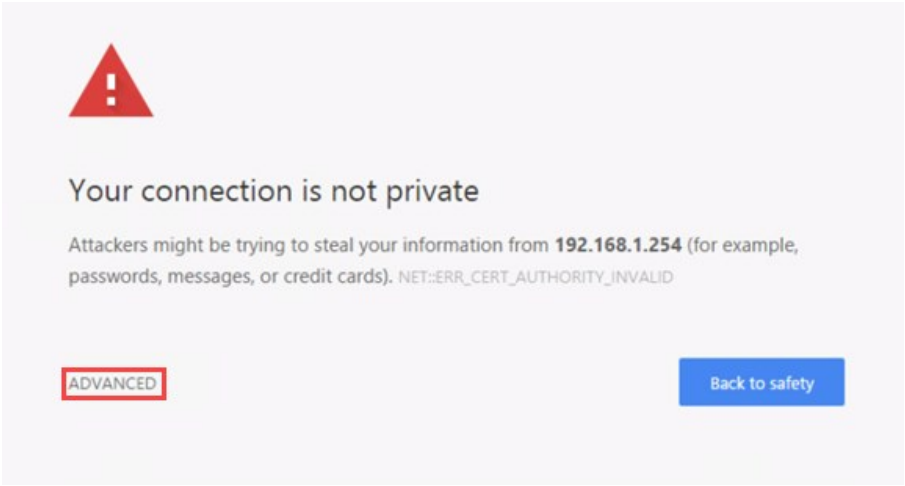


2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



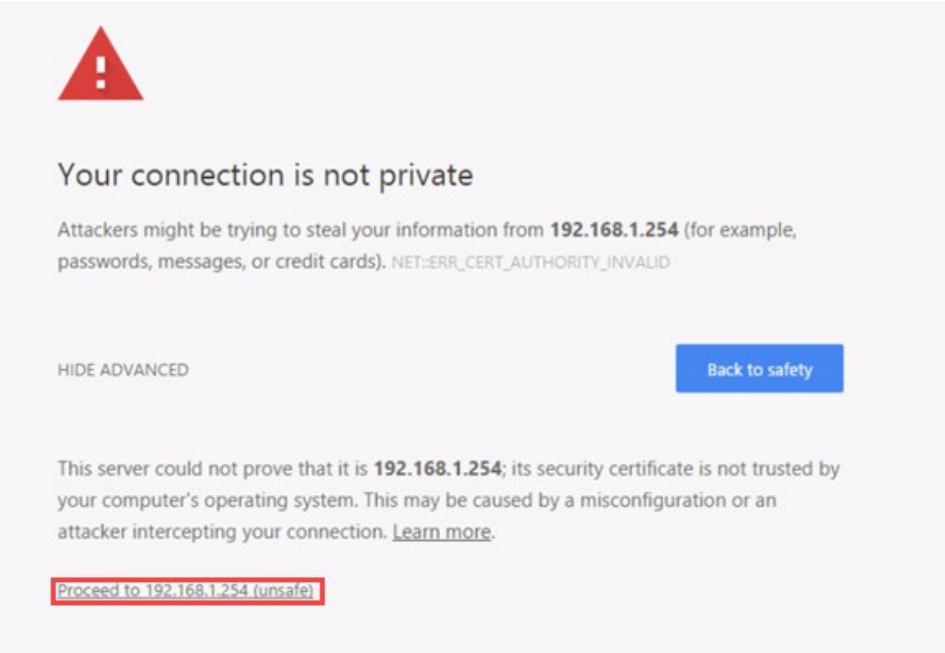
4. In the *Chromium address* field, type `https://192.168.1.254` and press **Enter**.

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



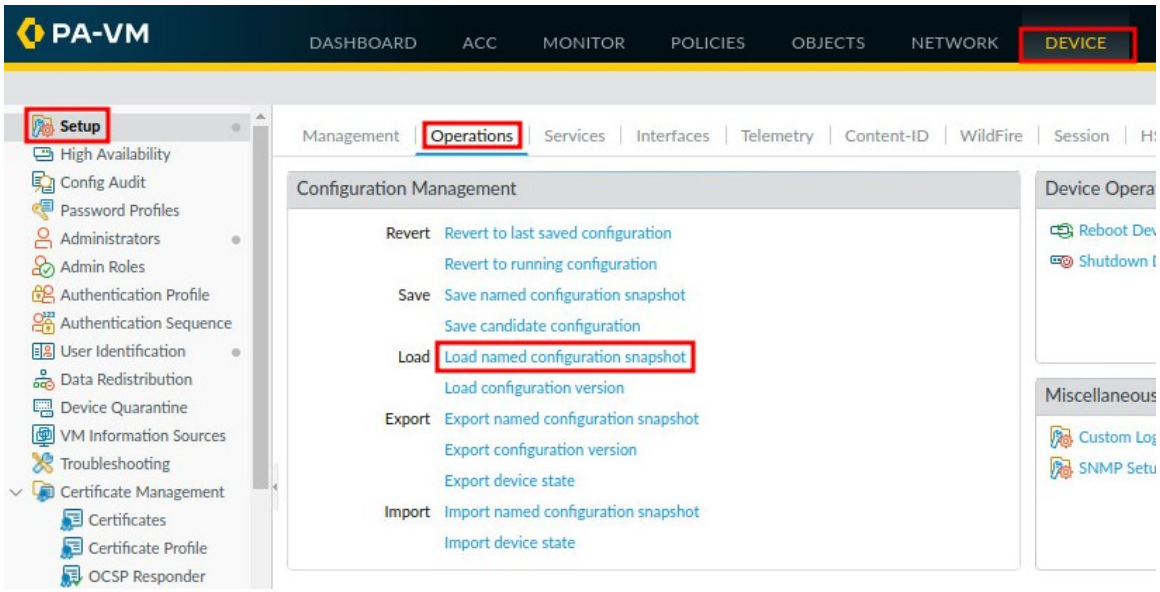
If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

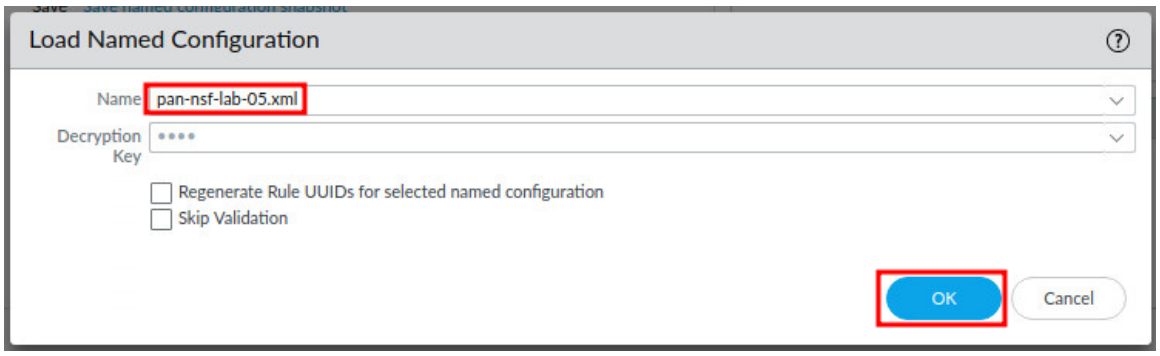


7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.

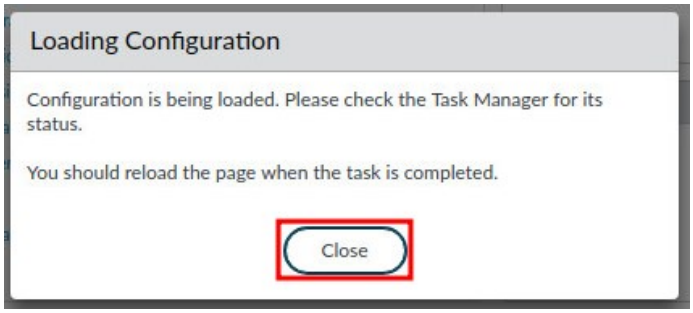
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



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

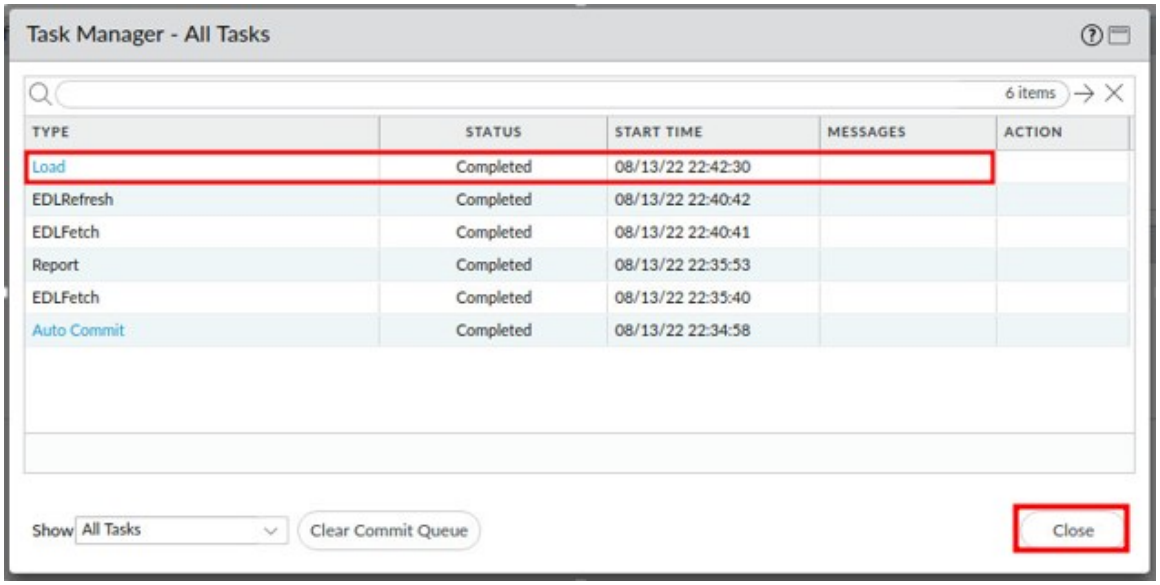


10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

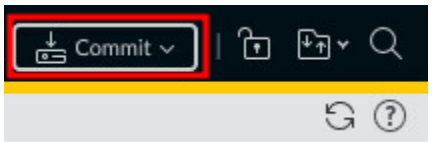


11. Click the **Tasks** icon located at the bottom-right of the web interface.

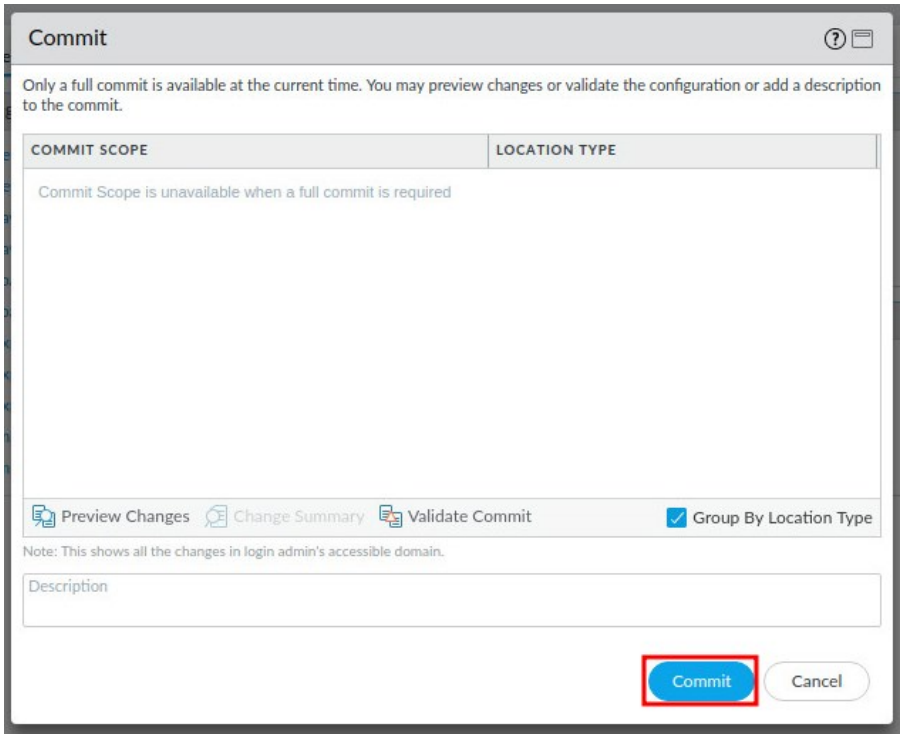
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**



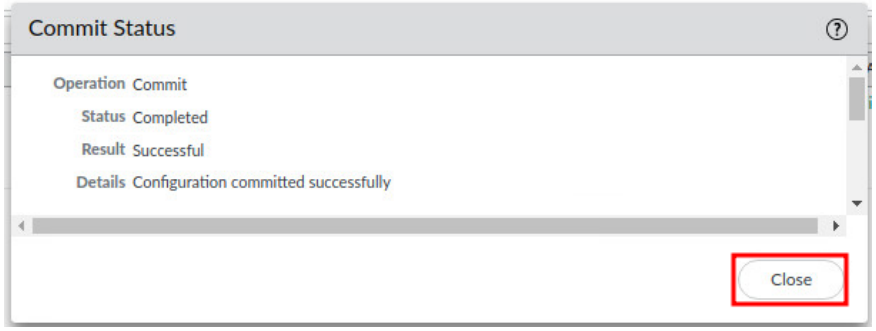
13. Click the **Commit** link located at the top-right of the web interface.



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



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

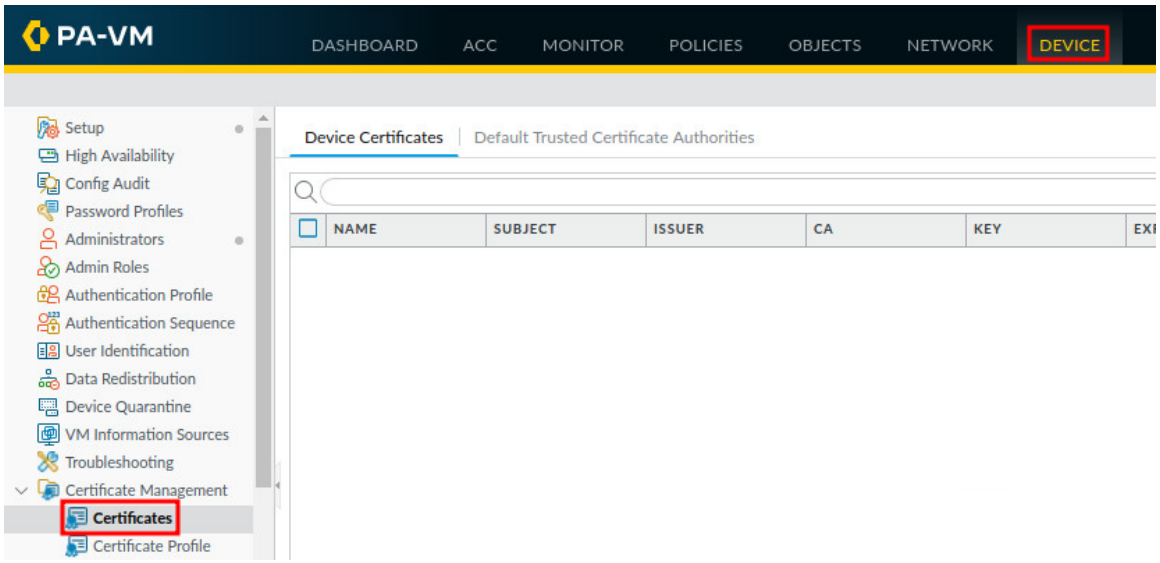


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

1.1 Generate Certificates

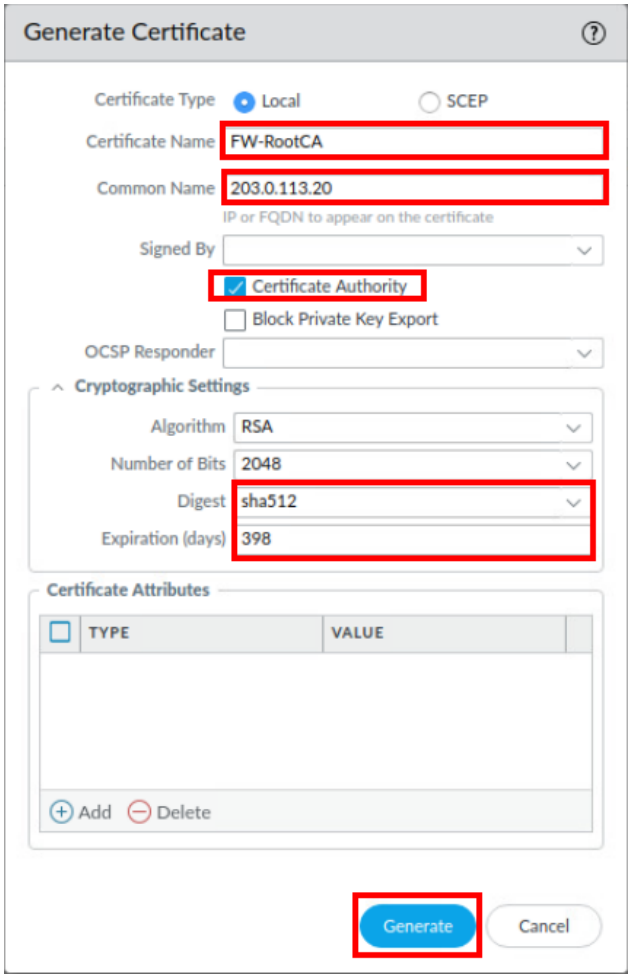
In this section, you will generate two certificates. The first is a self-signed Root Certificate Authority (CA) certificate, which is the top-most certificate in the certificate chain. The Firewall can use this certificate to automatically issue certificates for other uses. In this lab, you will use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



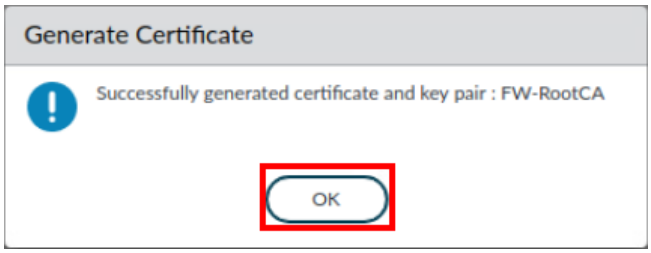
2. Click on the **Generate** button at the bottom-center of the center section.

3. In the *Generate Certificate* window, type `FW-RootCA` 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 `398` in the *Expiration (days)* field. Finally, click the **Generate** button.



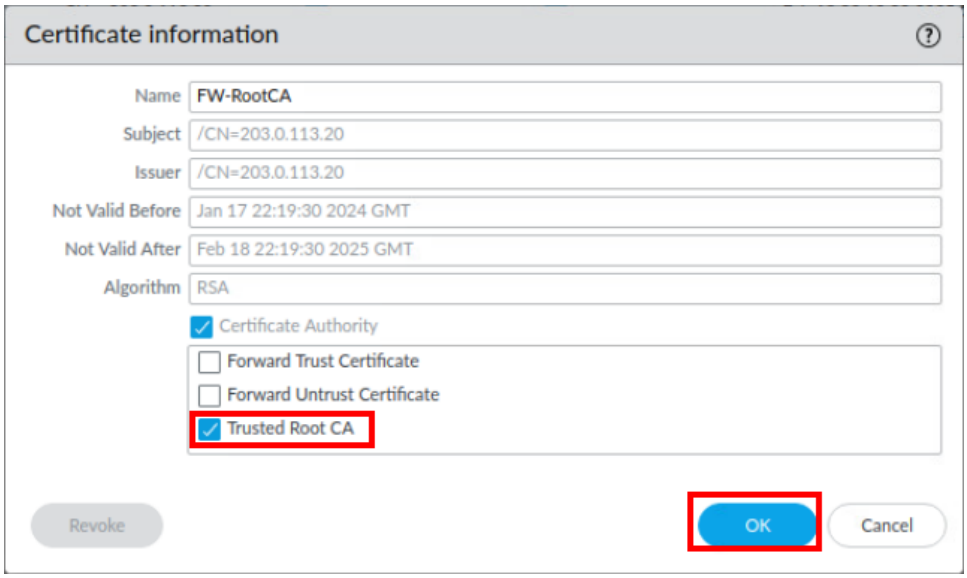
This will generate a certificate for the Firewall to act as a root Certificate Authority (CA). The IP address, **203.0.113.20**, used in the Common Name field is the Firewall's outside IP address. It is best practice that a digest algorithm of sha256 or higher is used for enhanced security. By increasing the default digest to **sha512**, you have created a much stronger certificate. The Expiration (days) value of **398** days represents the maximum certificate expiration time supported by modern web browsers.

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



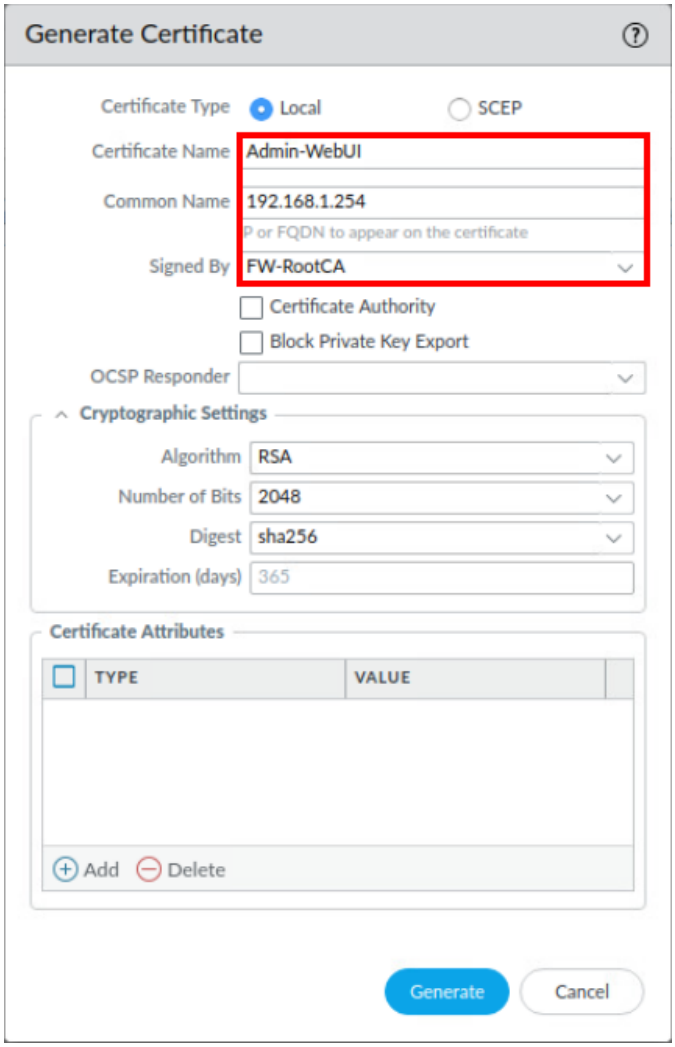
5. Click on the **FW-RootCA** certificate to edit.

6. In the *Certificate information* window, check the checkbox for **Trusted Root CA** and click **OK**.



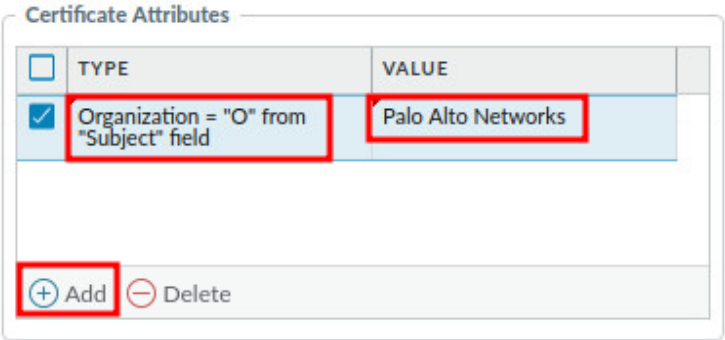
7. Click on the **Generate** button at the bottom-center of the center section.

8. In the *Generate Certificate* window, type `Admin-WebUI` in the *Certificate Name* field. Then, type `192.168.1.254` in the *Common Name* field. Next, select **FW-RootCA** in the *Signed By* dropdown. Continue to the next step to continue filling out information in the same window.

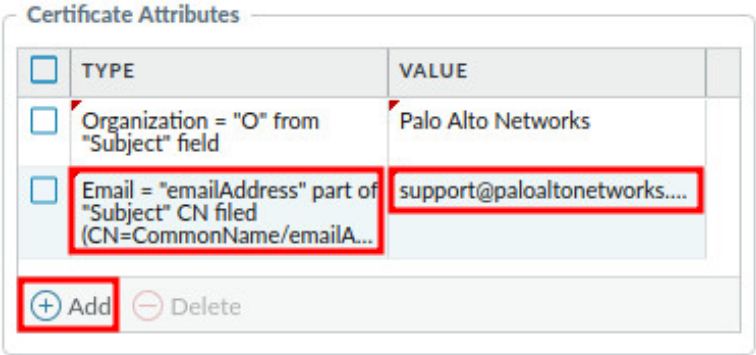


The IP address, **192.168.1.254**, used in the Common Name field is the Firewall's inside IP address. Notice you selected the previously created root CA certificate, **FW-RootCA**, to sign this certificate. Client certificates that are used when requesting firewall services that rely on TLSv1.2 (such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

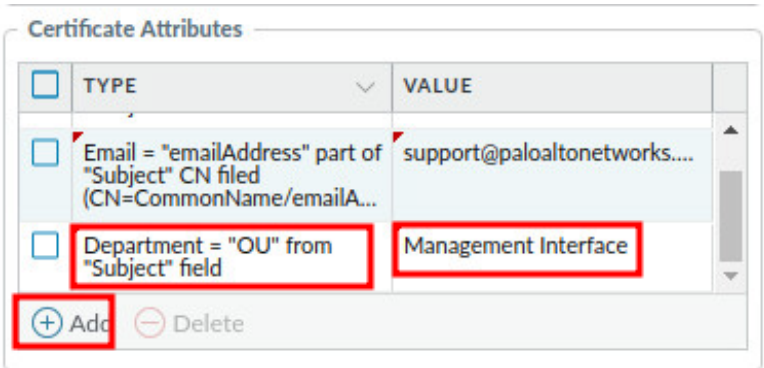
9. In the *Generate Certificate* window, click the **Add** button in the *Certificate Attributes* section. Then, select **Organization = "O" from …** in the *Type* column. Next, double-click the empty box in the *Value* column, type `Palo Alto Networks` and press **Enter**.



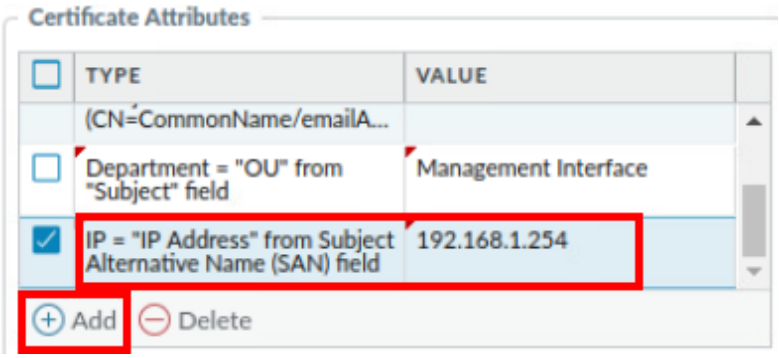
10. In the *Generate Certificate* window, click the **Add** button in the *Certificate Attributes* section. Then, select **Email = "emailAddress' pa…** in the *Type* column. Next, double-click the empty box in the *Value* column, type `support@paloaltonetworks.com` and press **Enter**.



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

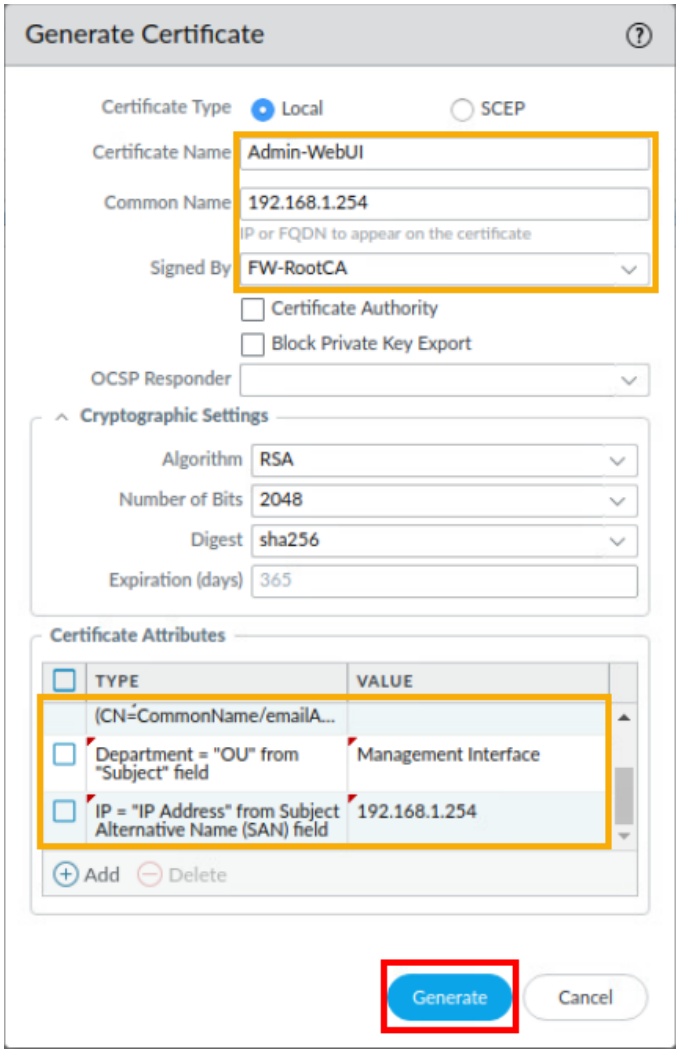


12. In the *Generate Certificate* window, click the **Add** button in the *Certificate Attributes* section. Then, select **IP = "IP Address" from …** in the *Type* column. Next, double-click the empty box in the *Value* column, type `192.168.1.254`, and press **Enter**.

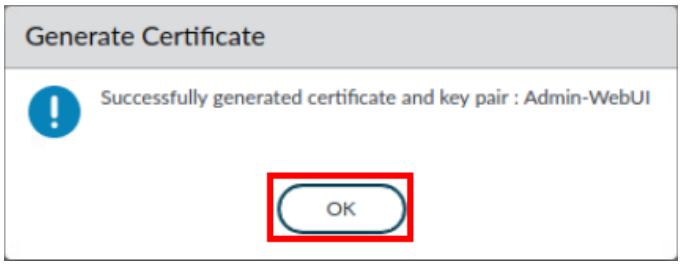


Certificate Attributes are used to uniquely identify the firewall and the service that will use the certificate.

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



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



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.

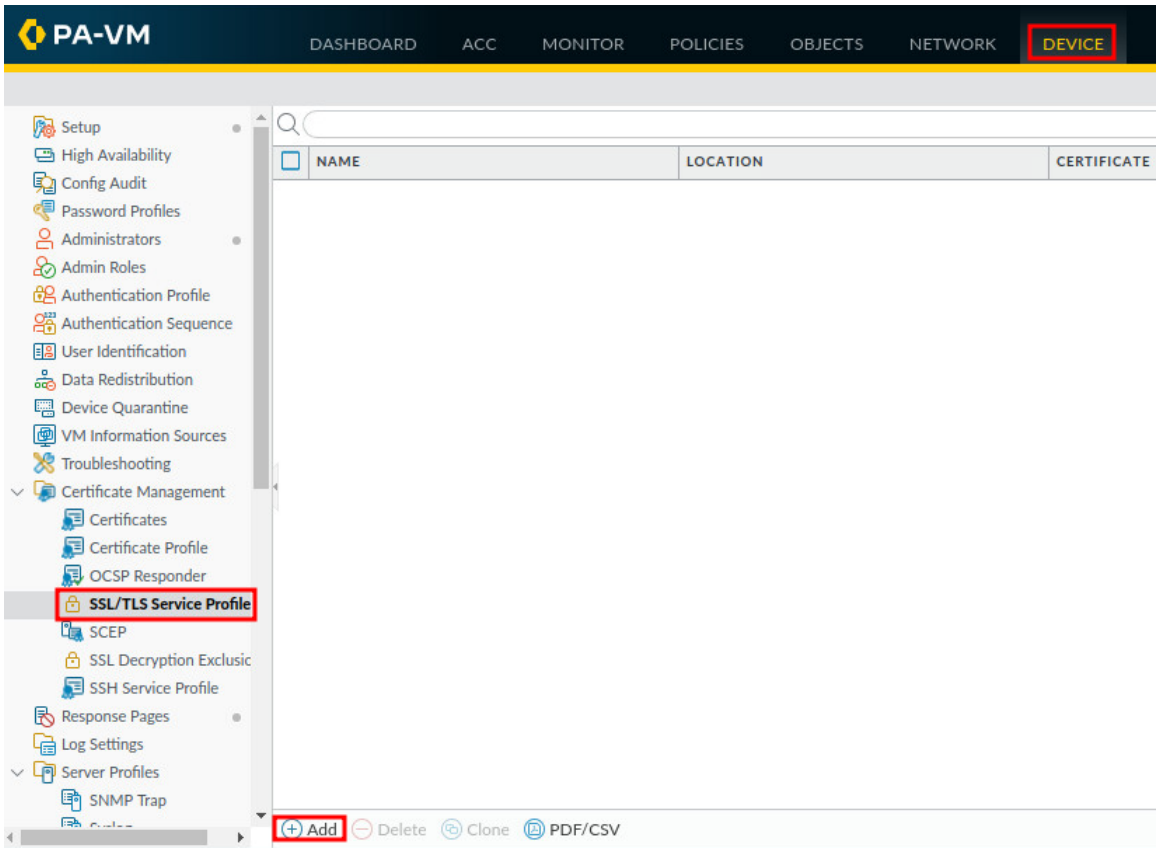
As a best practice, it is recommended you use different certificates for each usage.

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.

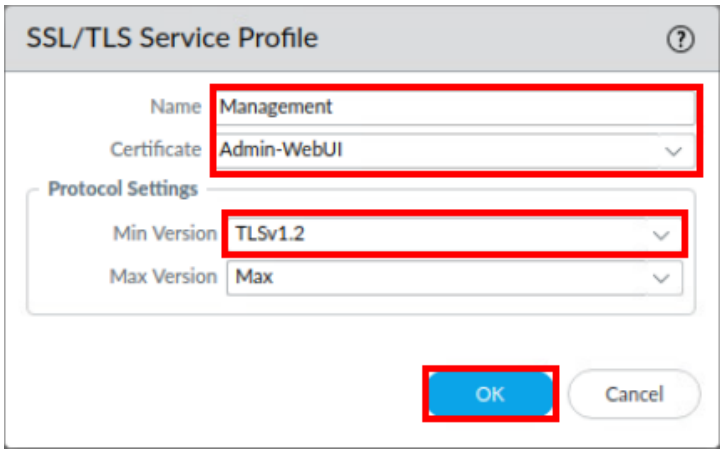
1.2 Replace the Certificate for Inbound Management Traffic

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 **Admin-WebUI** certificate you specifically created for this purpose. Then, you will apply the SSL/TLS Service Profile to inbound management traffic.

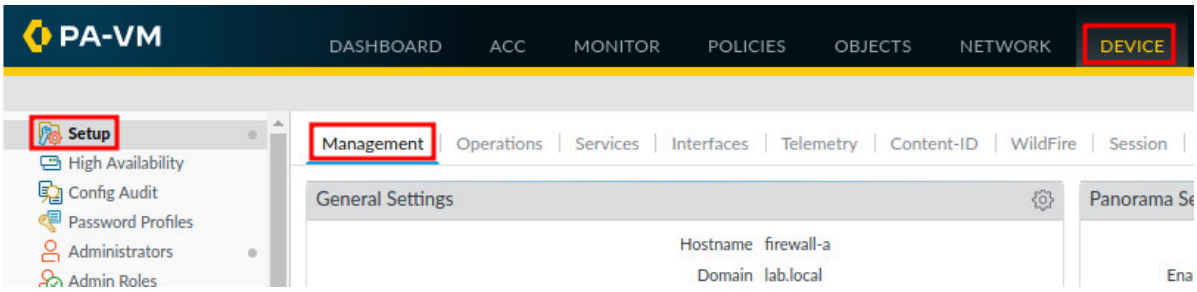
1. Navigate to **Device > Certificate Management > SSL/TLS Service Profile > Add.**



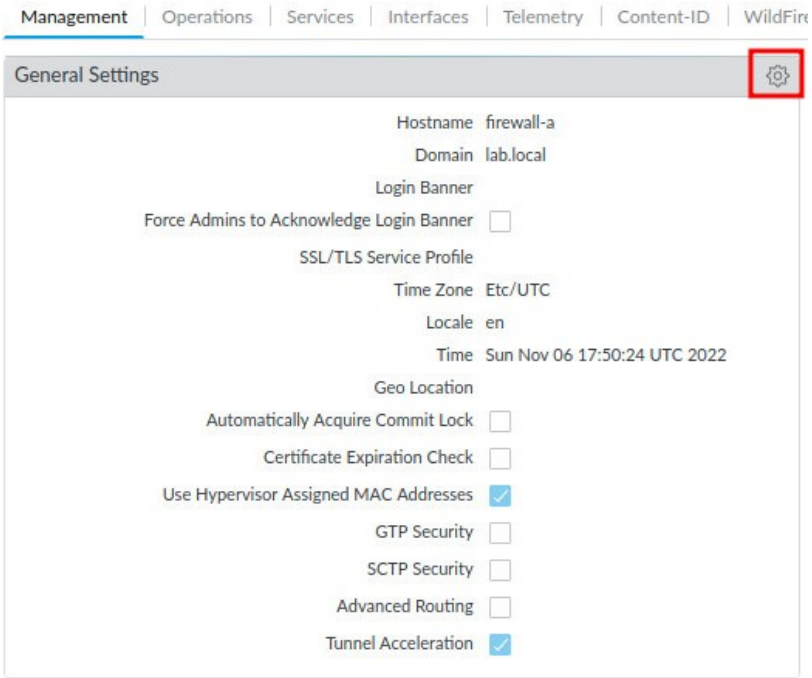
2. In the *SSL/TLS Service Profile* window, type `Management` in the *Name* field. Then, select **Admin-WebUI** from the *Certificate* dropdown. Next, select **TLSv1.2** from the *Min Version* dropdown. Finally, click the **OK** button.



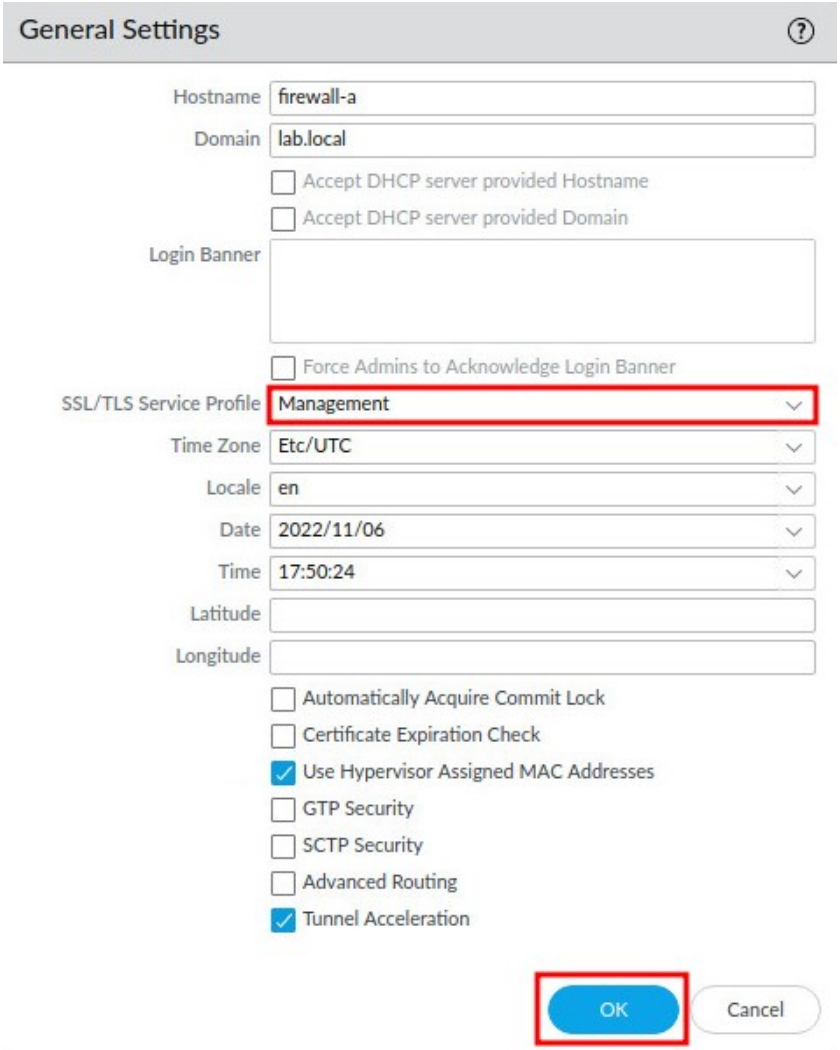
3. Navigate to **Device > Setup > Management.**



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



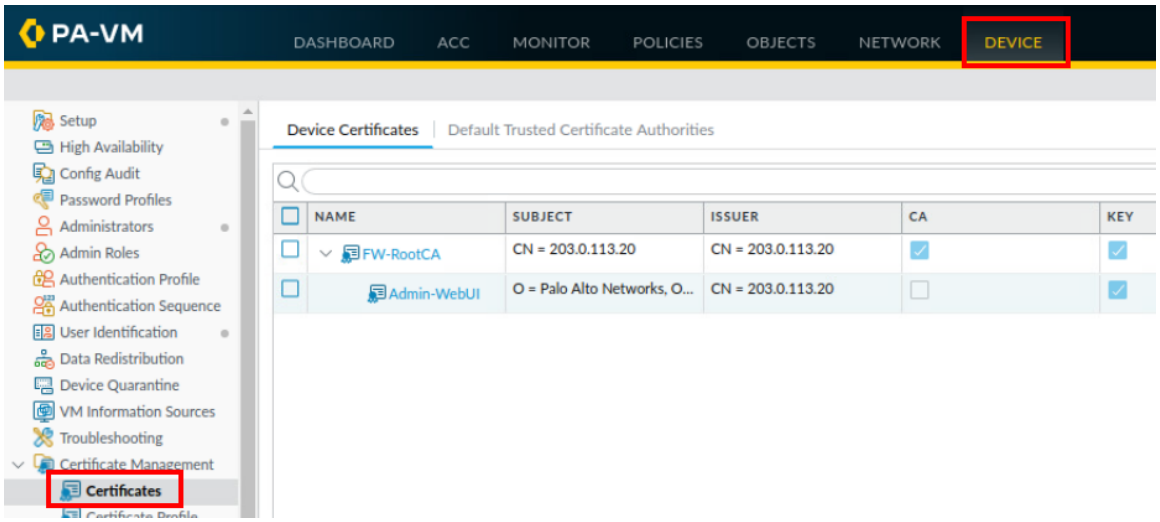
5. In the *General Settings* window, select **Management** from the *SSL/TLS Service Profile* dropdown. Then, click the **OK** button.



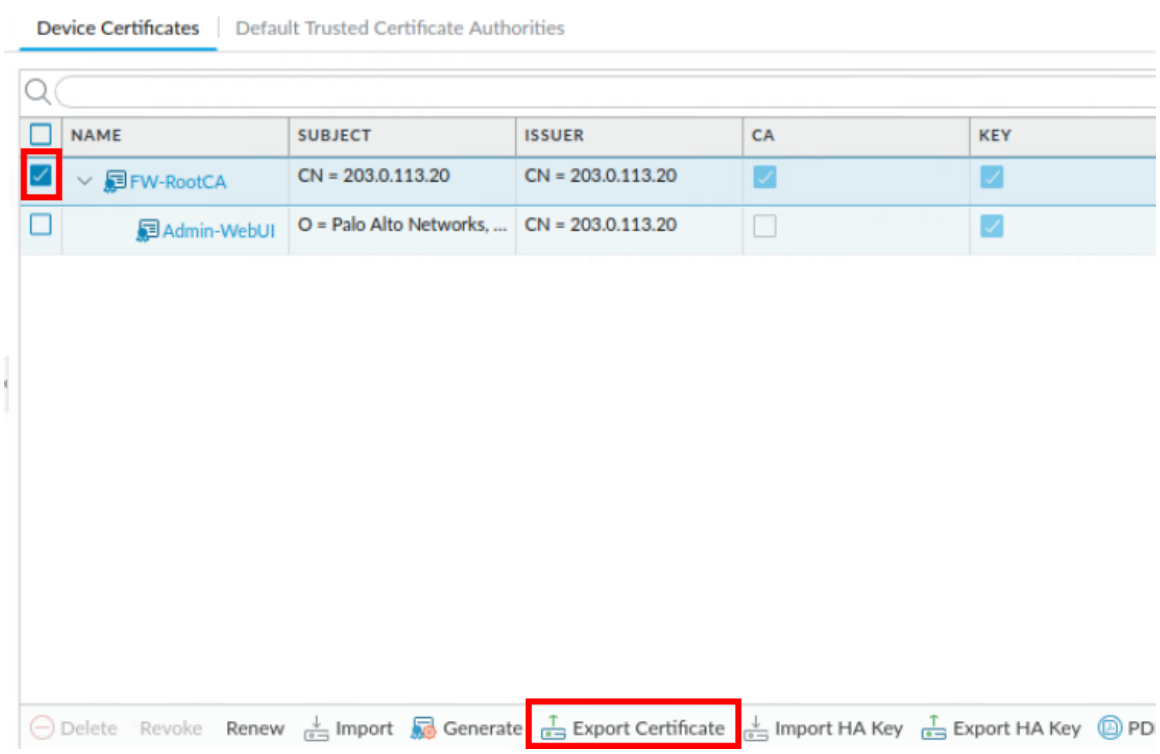
1.3 Export Certificate and Commit

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

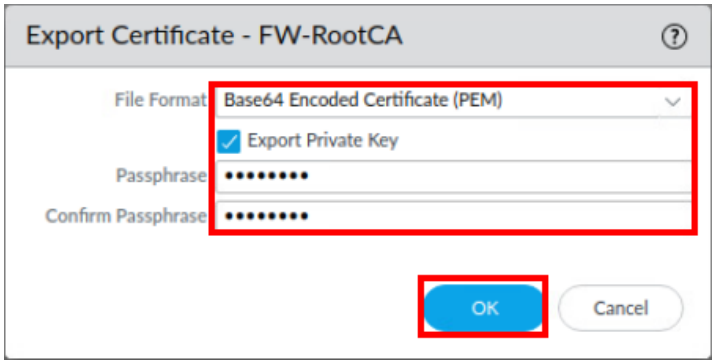
1. Navigate to **Device > Certificate Management > Certificates**.



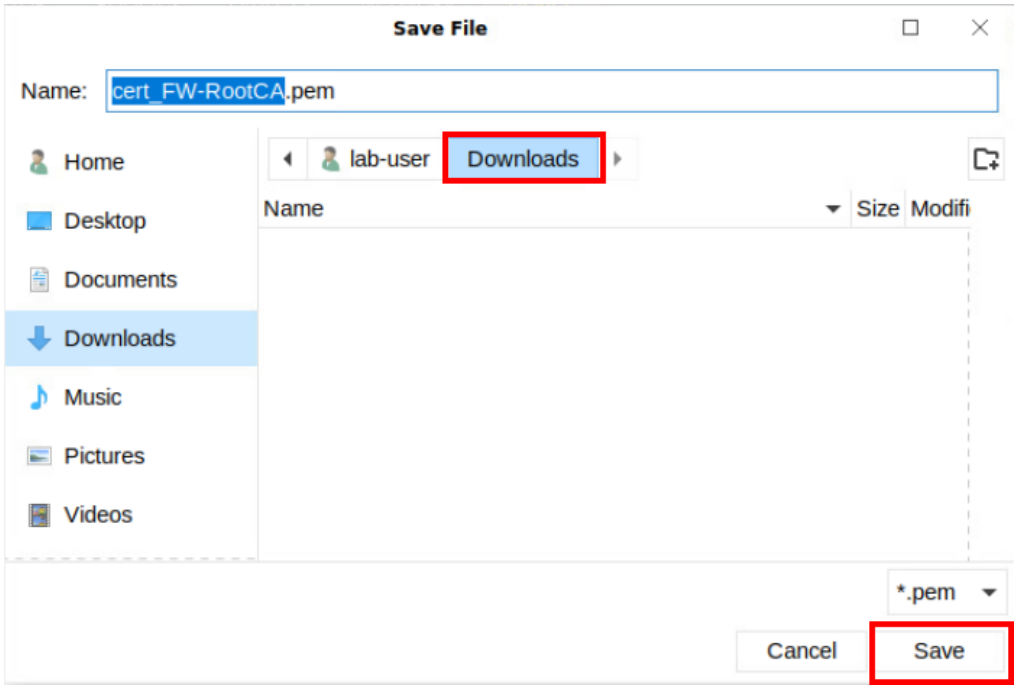
2. Click the checkbox for **FW-RootCA**. Then, click on the **Export Certificate** button at the bottom.



3. In the *Export Certificate – FW-RootCA* 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.

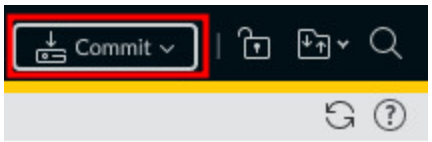


4. In the *Save File* window, make sure **cert_FW-RootCA.pem** is located in the *Name* field, verify that *cert_FW-RootCA* is going to the **Downloads** folder. Then, click the **Save** button.

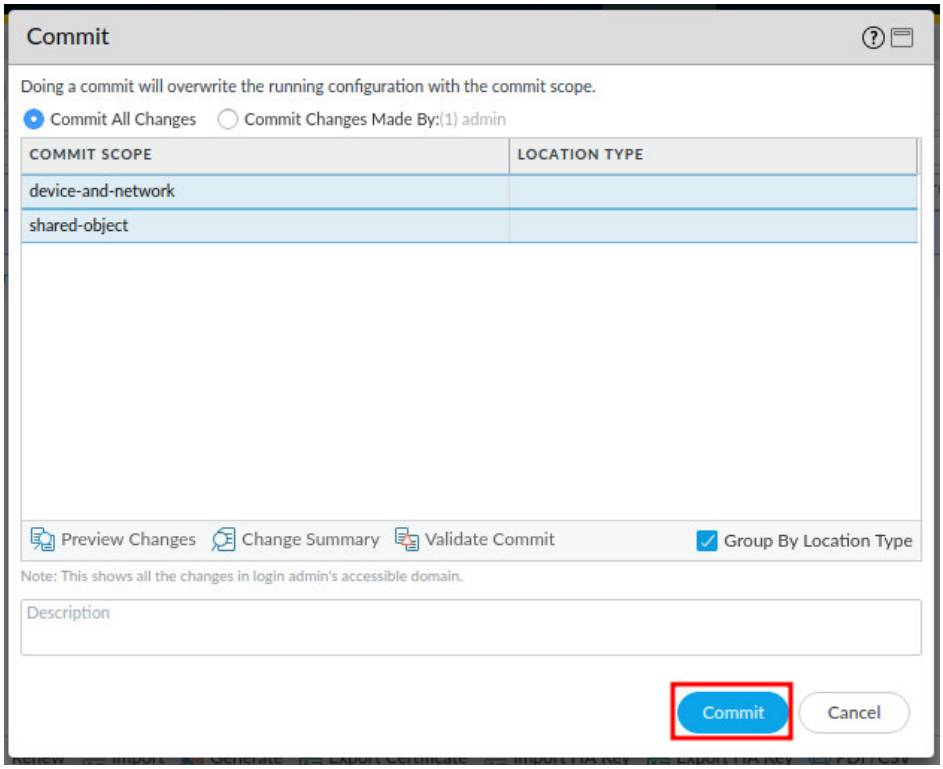


By using the **Base64 Encoded Certificate (PEM) File Format**, this generates a certificate signing request to accept SSL certificates.

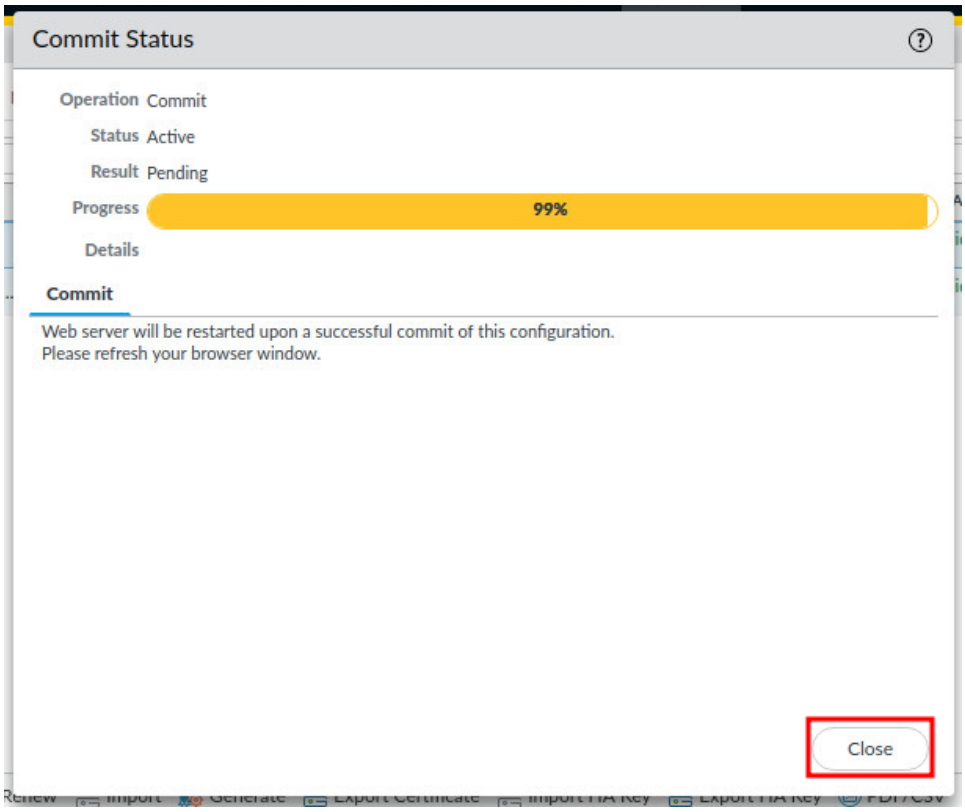
5. Click the **Commit** link located at the top-right of the web interface.



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



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%.

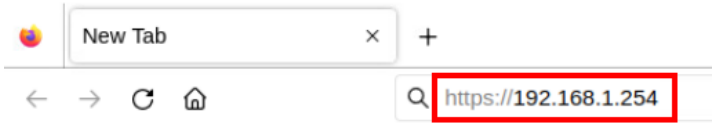
8. Click the **X** in the upper-right to close *Chromium*.

1.4 Test Connectivity and Import Certificate on the Client

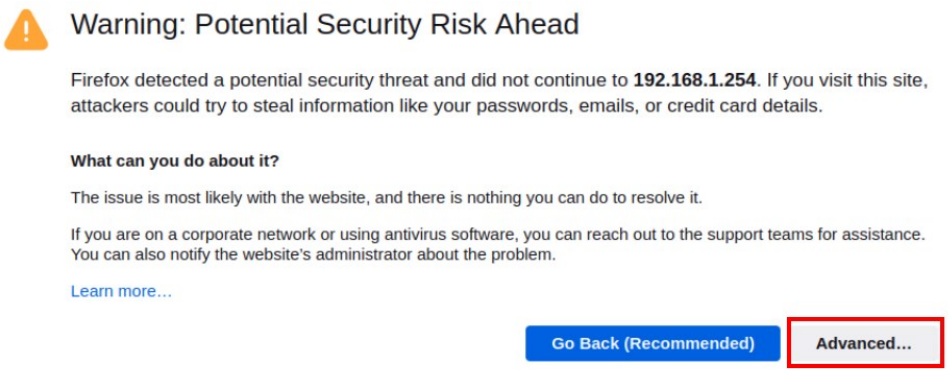
In this section, you will test the connectivity to the Firewall. When establishing a secure connection with the Firewall, the Client must trust the root CA that issued the certificate. Otherwise, the Client browser will display a warning that the certificate is invalid and might (depending on security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

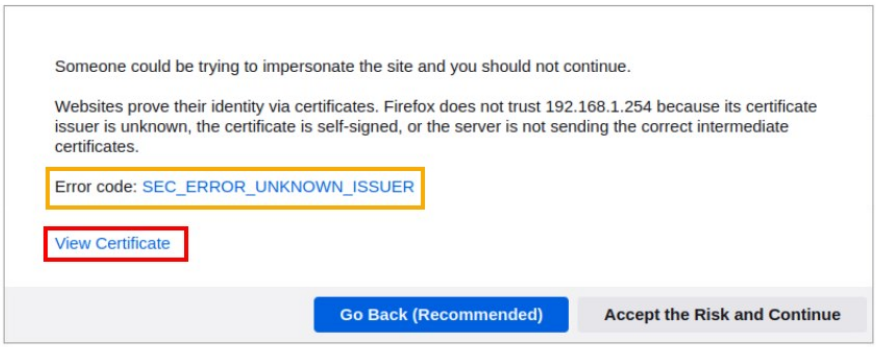
1. Open **Firefox** from the taskbar.

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. Notice the error code displays information relating to the certificate not being able to be verified due to an unknown issuer. To view the certificate, click the **Advanced** button, scroll to the bottom of the security window, and select **View Certificate**.





4. In the *Certificate for 192.168.1.254* tab, view the contents of the certificate.

Certificate

192.168.1.254 | 203.0.113.20

Subject Name

Organization	Palo Alto Networks
Organizational Unit	Management Interface
Common Name	192.168.1.254
Email Address	support@paloaltonetworks.com

Issuer Name

Common Name	203.0.113.20

Validity

Not Before	Wed, 17 Jan 2024 22:28:22 GMT
Not After	Thu, 16 Jan 2025 22:28:22 GMT

Subject Alt Names

IP Address	192.168.1.254

Subject Alt Names

IP Address	192.168.1.254

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	BE:94:F6:37:36:E7:83:D6:7D:0F:83:33:2D:F3:CB:A2:E4:B1:19:5B:A7:39:FB:...

Miscellaneous

Serial Number	6E:E0:B0:9A
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

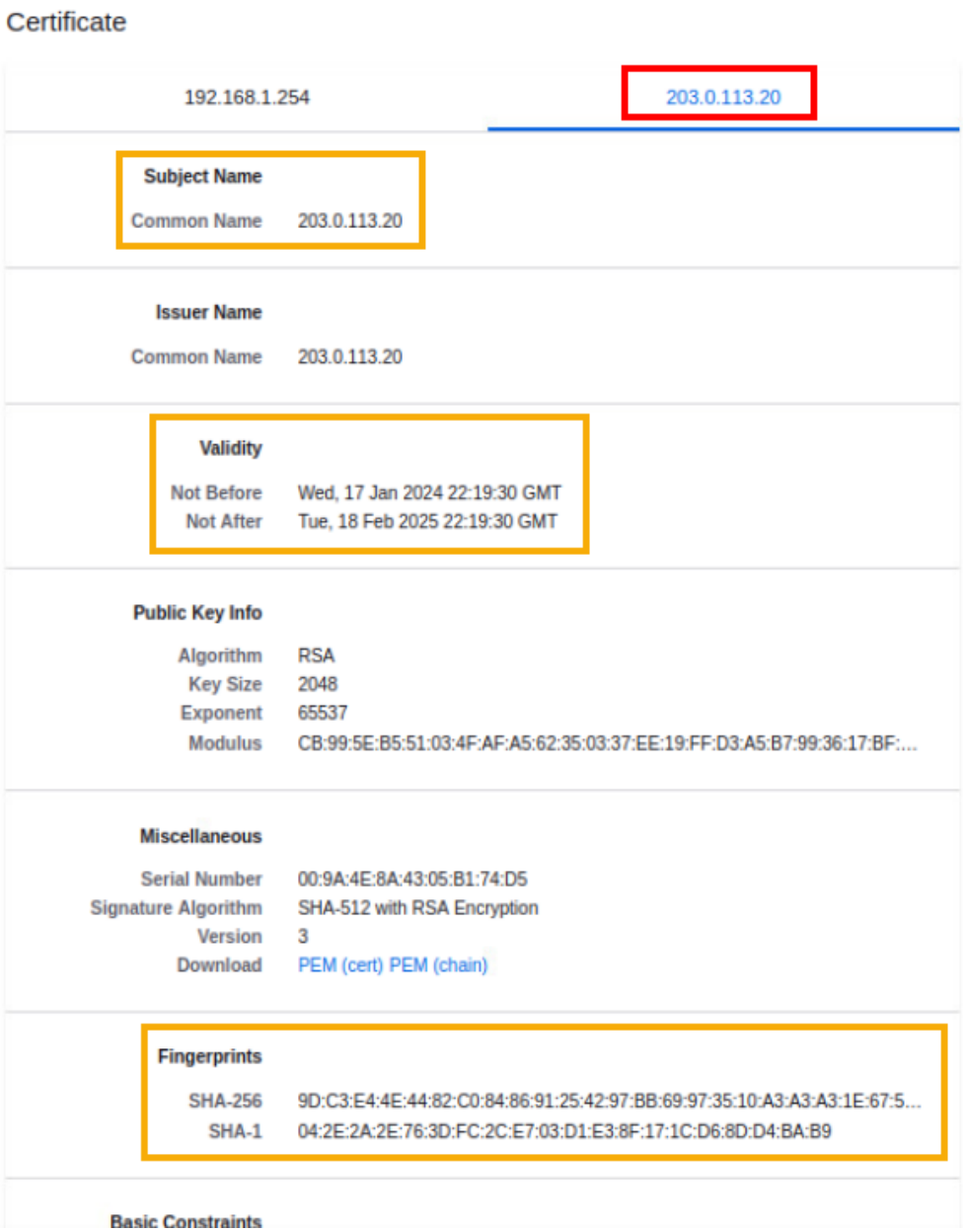
Fingerprints

SHA-256	25:64:D0:58:AB:D2:EF:A4:92:34:44:1D:3C:04:F2:D0:A5:85:1C:70:66:F3:CF:...
SHA-1	66:5E:84:0C:67:BE:EB:0E:4A:B8:98:F4:49:95:BE:00:81:CC:90:66

Basic Constraints

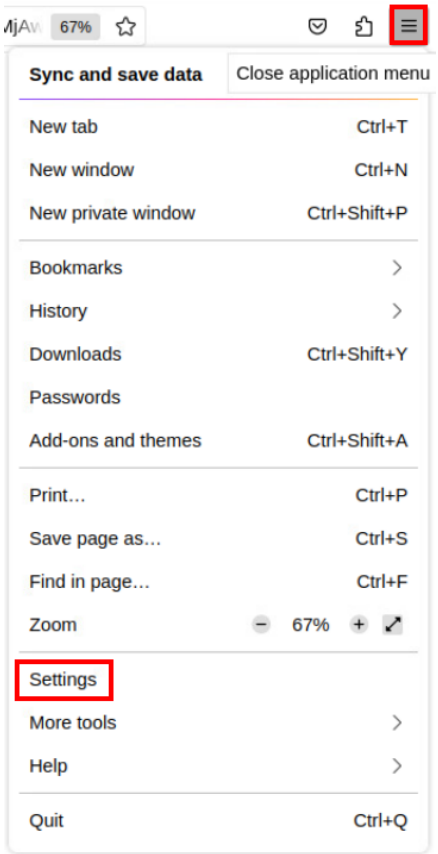
Certificate Authority	No

5. Click on the **203.0.113.20** tab near the top to view additional contents of the certificate.

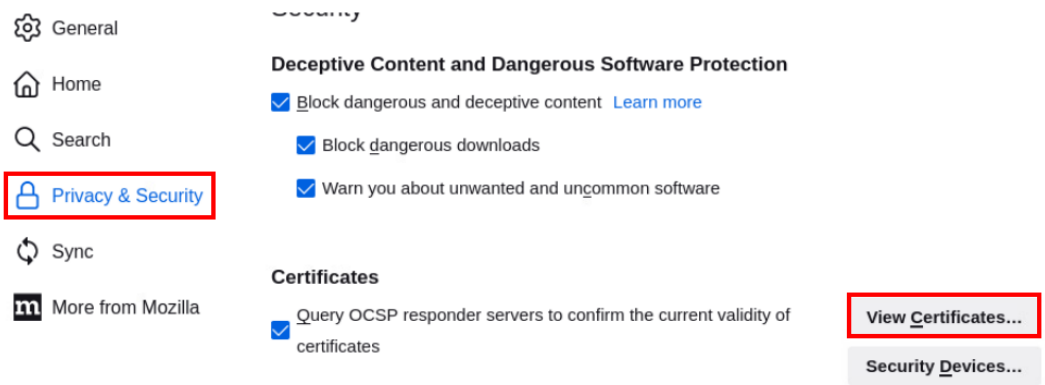


Notice on the general tab it matches the **Admin-WebUI** certificate you created earlier in section 5.1. The sha256 algorithm is being used in the fingerprints. The certificate was issued by **203.0.113.20**, which is the common-name of the root CA certificate, **FW-RootCA**, you created. The Validity Period indicates the certificate is valid for 398 days. The Organization is **Palo Alto Networks**.

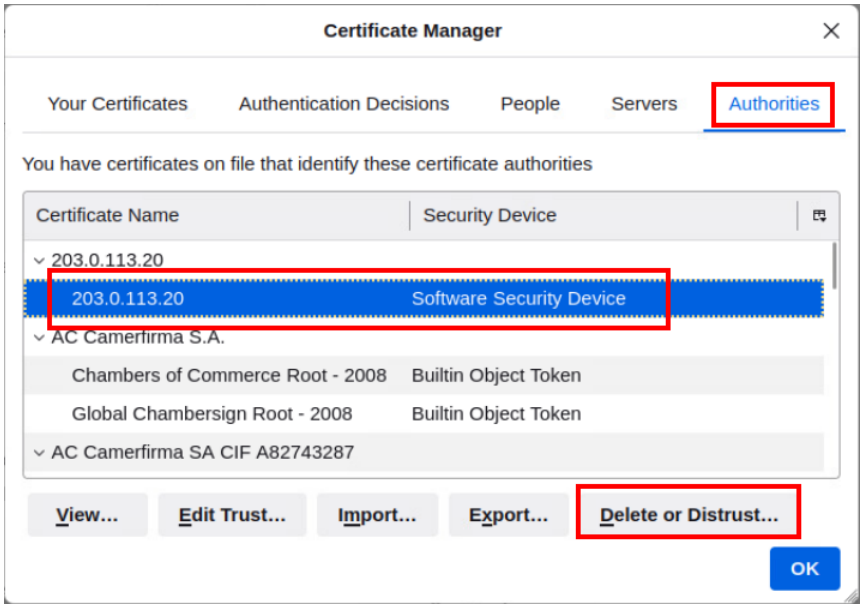
6. Before importing certificates, let's make sure to clear the *Firefox* browser of any old, outstanding certificates that may be cached on the system. Click on the **3-bar** menu icon and click **Settings**.



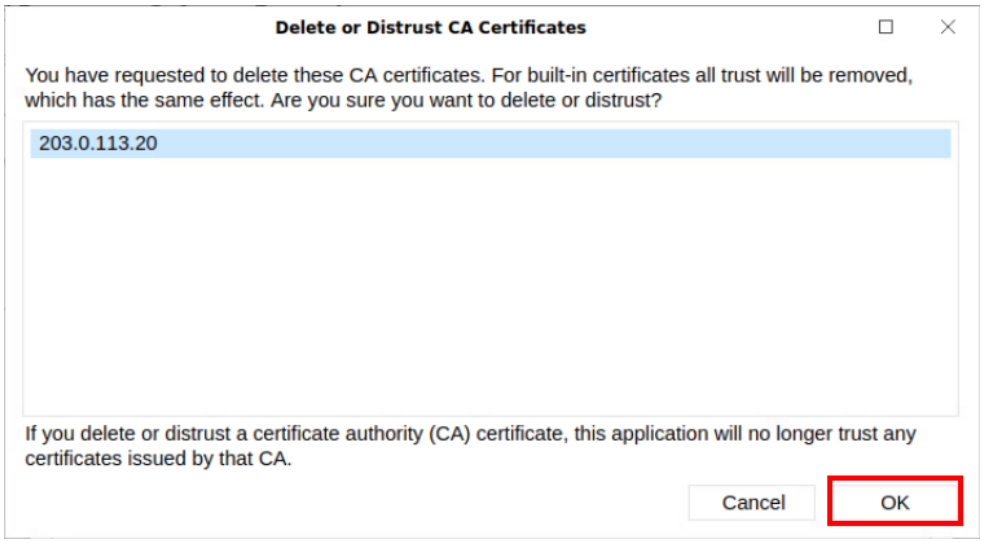
7. Click on **Privacy & Security** from the menu on the left and then scroll down to click on the **View Certificates** button.



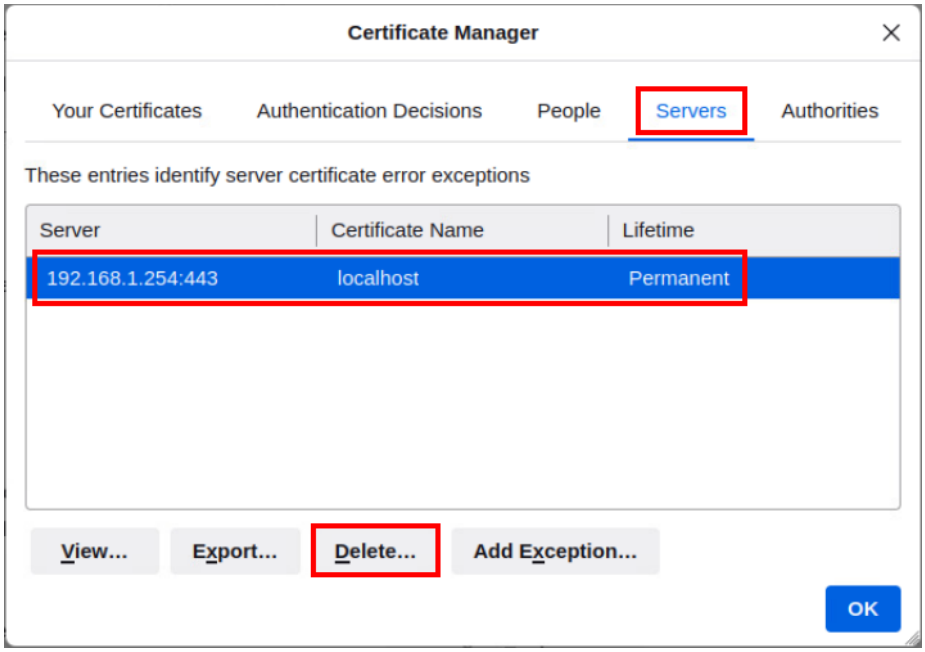
8. In the *Certificate Manager* window, view the **Authorities** tab and select the **203.0.113.20** entry. Click the **Delete or Distrust** button.



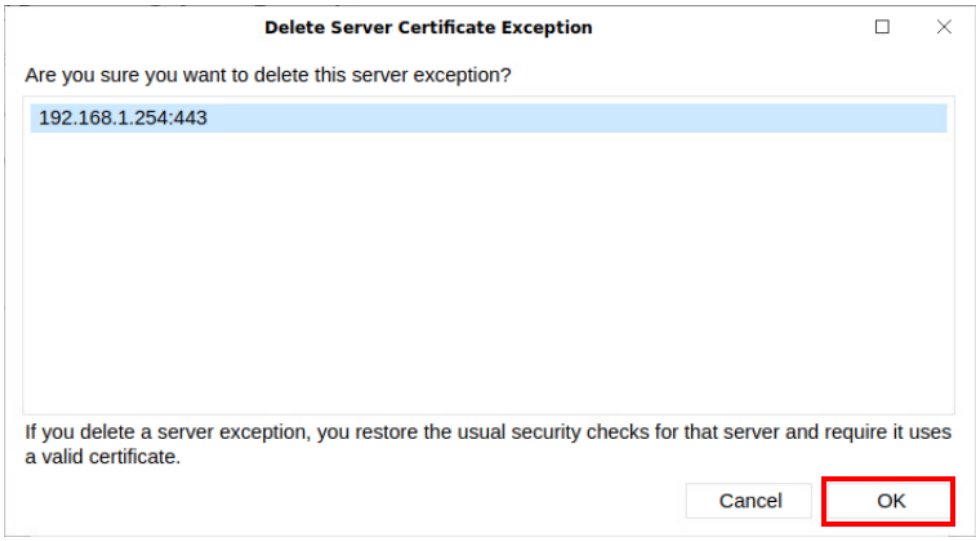
9. Confirm the deletion by clicking **OK**.



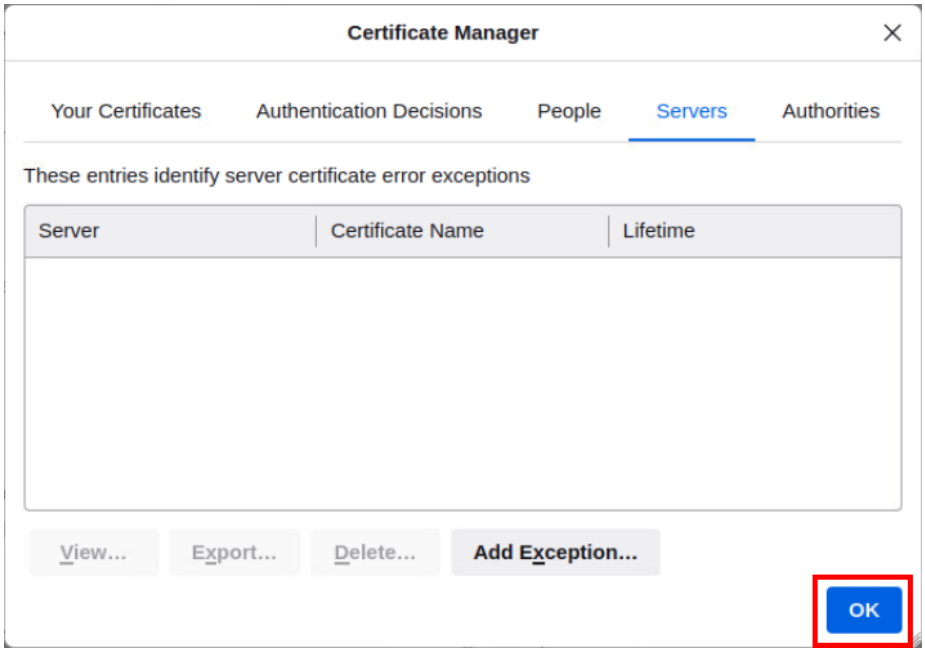
10. Back in the *Certificate Manager* window, confirm the entry is removed. Click on the **Servers** tab. Select the **192.168.1.254:443** entry and click the **Delete** button.



11. Confirm the deletion by clicking **OK**.



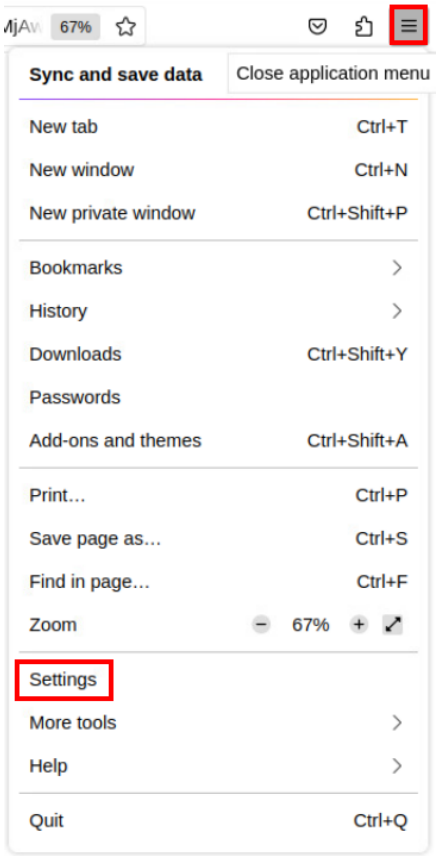
12. Back in the *Certificate Manager* window, confirm the entry is deleted and click **OK**.



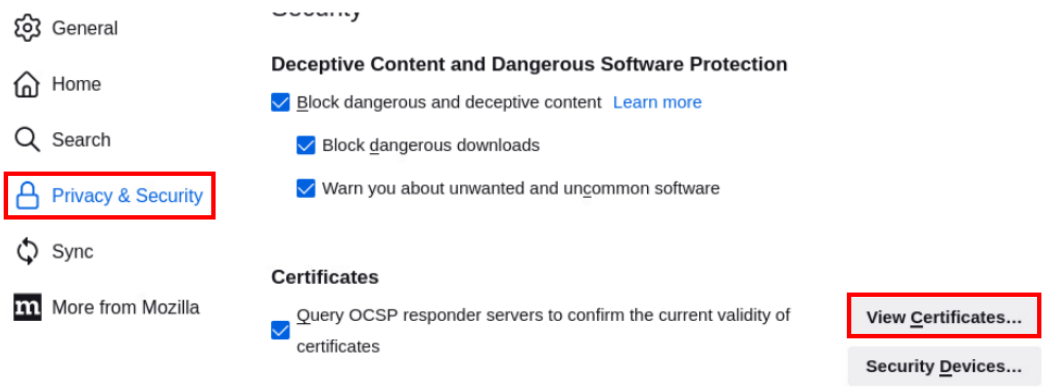
13. Click the **X** in the upper-right to close *Firefox*.

14. To import the **FW-RootCA** certificate, open **Firefox** from the taskbar.

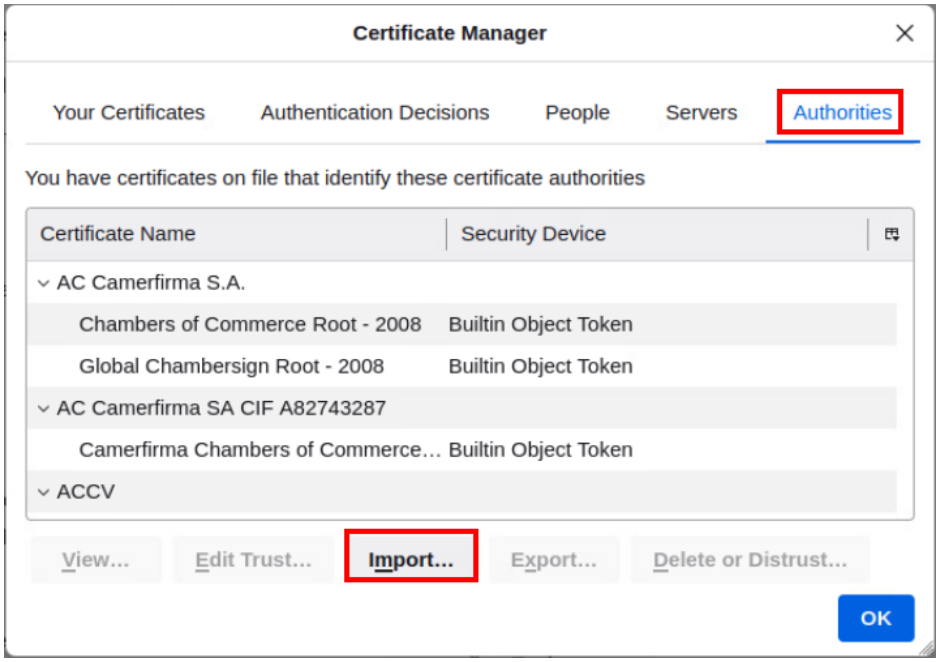
15. Click on the **3-bar** menu icon and click **Settings**.



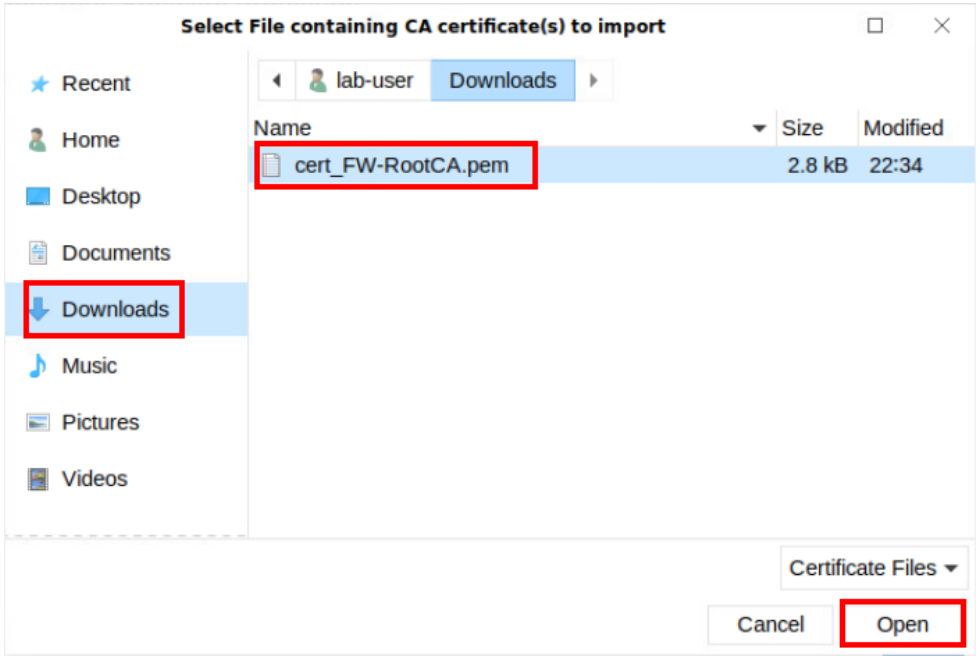
16. Click on **Privacy & Security** from the menu on the left and then scroll down to click on the **View Certificates** button.



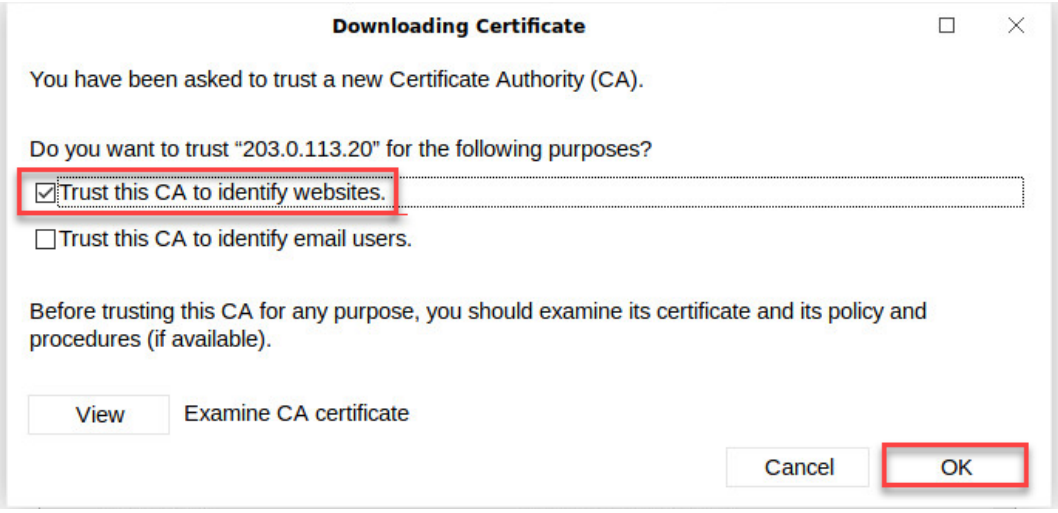
17. In the *Certificate Manager* window, click on the **Authorities** tab followed by clicking the **Import** button.



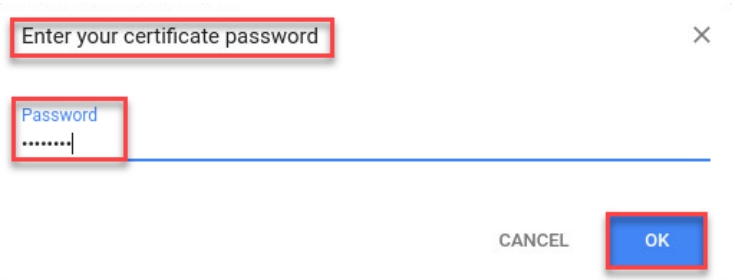
18. In the *Select File containing CA certificate(s) to import* window, navigate to the **Downloads** folder and select the **cert_FW-RootCA.pem** file. Click the **Open** button.



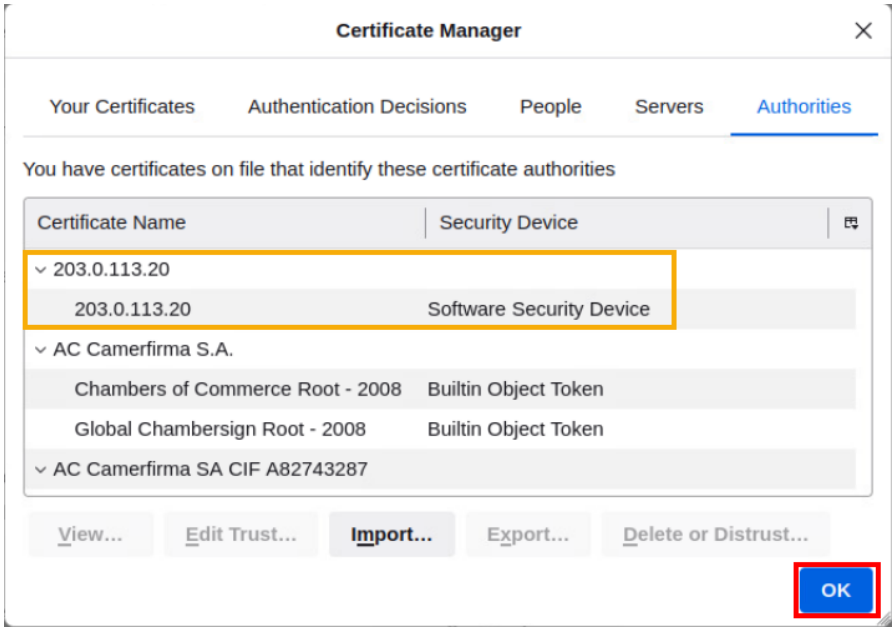
19. In the *Downloading Certificate* window, check the checkbox for **Trust this CA to identify websites**. Click **OK**.



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



21. In the *Certificate Manager* window, verify the **FW-RootCA** certificate has been imported. Click **OK**.

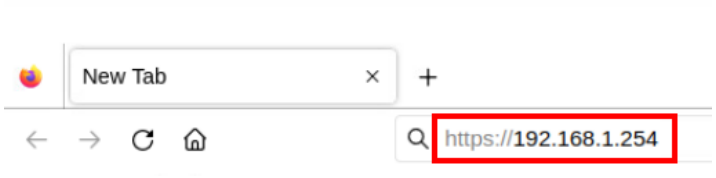


Notice that the common name of *203.0.113.20* is shown. This is the common name of the firewall.

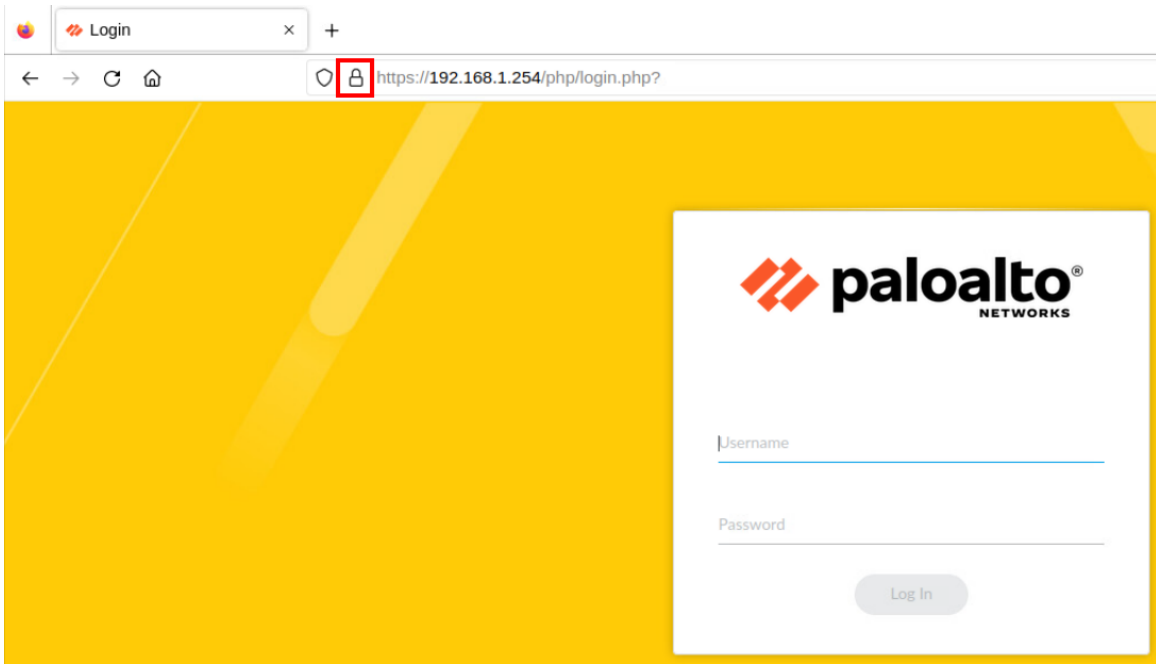
22. Click on the **X** in the upper-right to close *Firefox* so that it can reload properly.

23. Open **Firefox** from the taskbar.

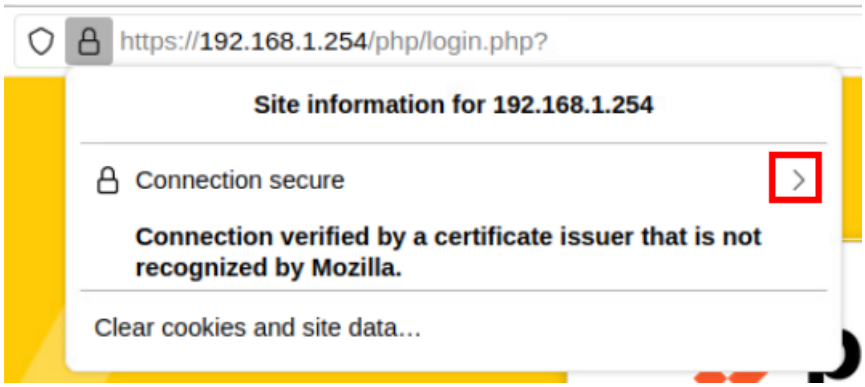
24. In the *Firefox address* field, type `https://192.168.1.254` and press **Enter.**



25. Notice that the login prompt to the firewall immediately appears this time. Also, take notice of the secured padlock icon in the address bar, signaling a secure connection. Click on the **padlock icon**.



26. In the *Site Information for 192.168.1.254* popup, click the **right arrow** to show more information.



27. 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*".

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

