PAN8 CYBERSECURITY ESSENTIALS

Lab 5: Managing Certificates

Document Version: 2018-07-02

Contents

Introduction

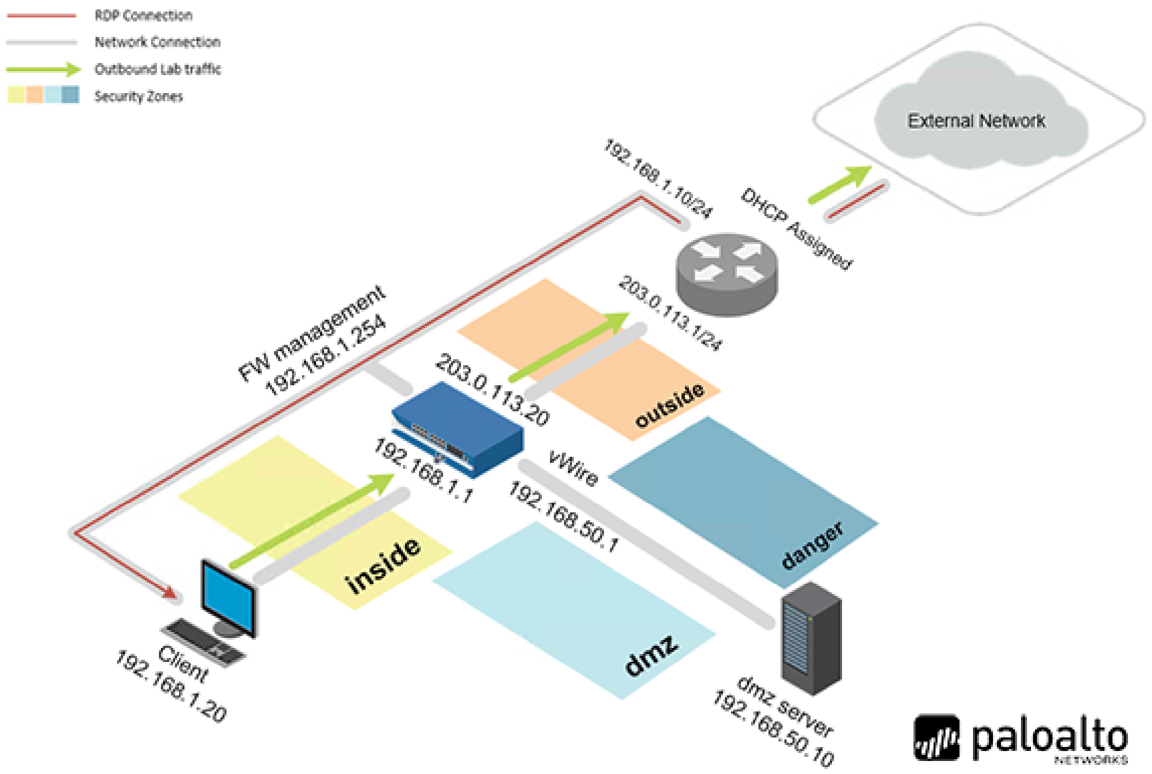
In this lab, you will generate a Self-Signed Root Certificate Authority (CA) certificate and replace the certificate for inbound management traffic. Then, you will import the root CA certificate on the Client machine.

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.

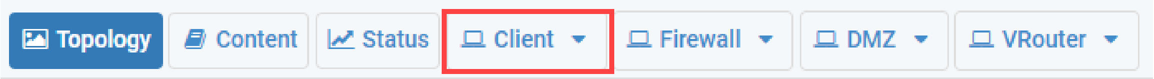
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	admin

5 Lab: Managing Certificates

5.0 Load Lab Configuration

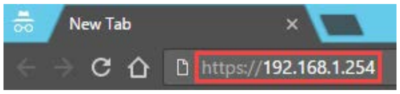
In this section, you will load the Firewall configuration file.

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

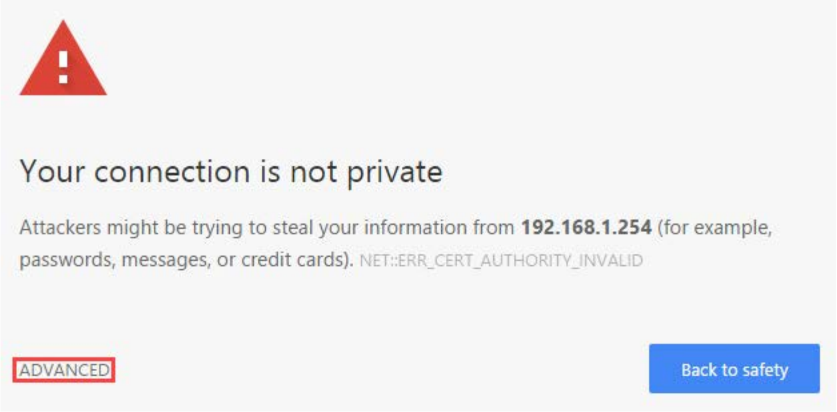


2. Login to the Client machine as username **lab-user**, password **`Pal0Alt0`**.
3. Double-click the **Google Chrome** icon located on the Desktop.

4. In the *Google Chrome* 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.

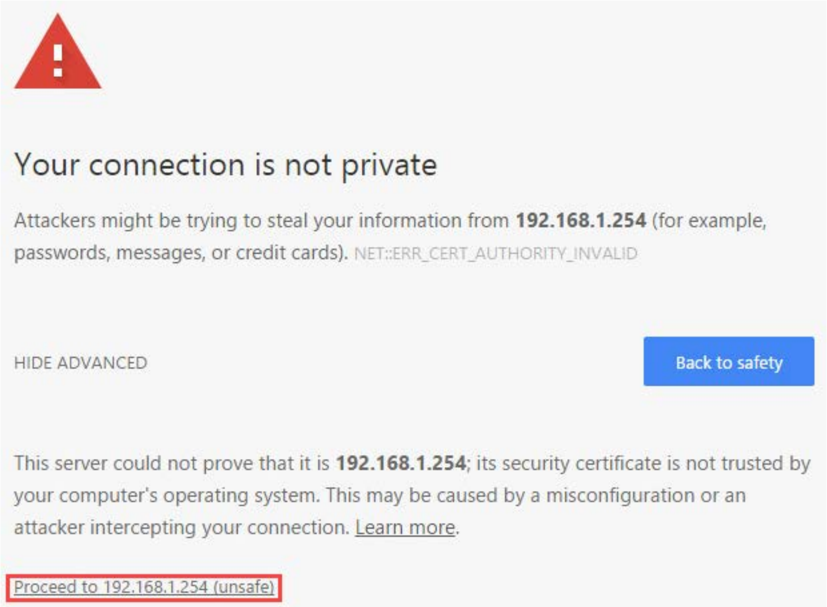


Your connection is not private

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)**.

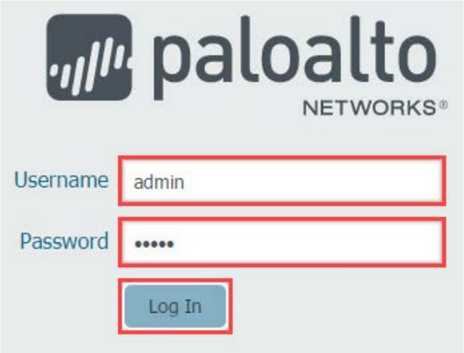


Your connection is not private

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.

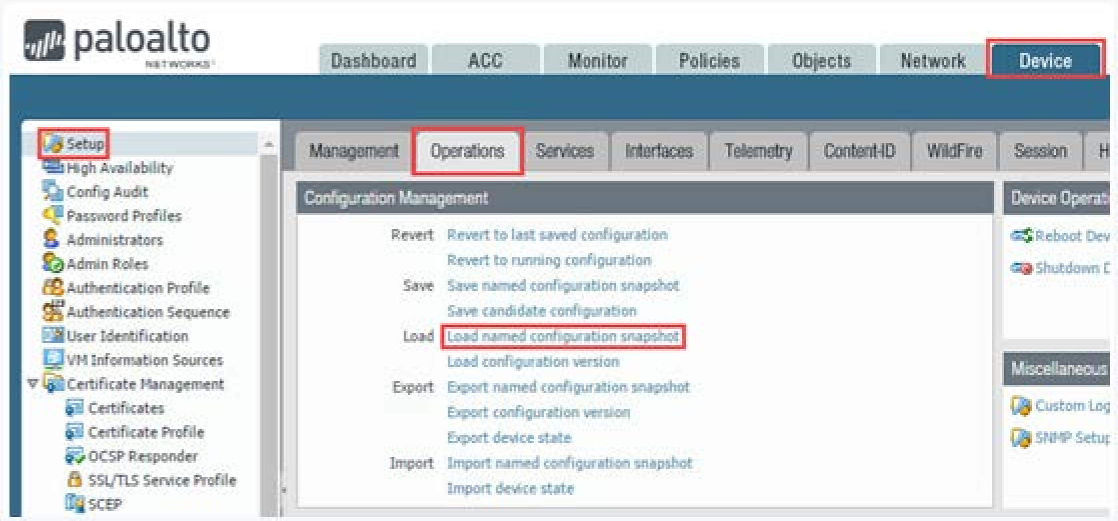
7. Login to the Firewall web interface as username **admin**, password **admin.**



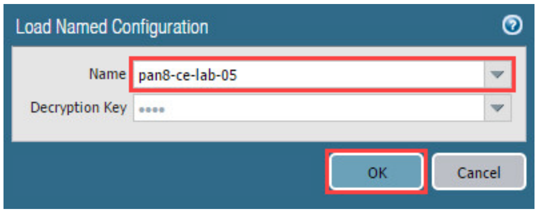
Username: admin

Password: •••••

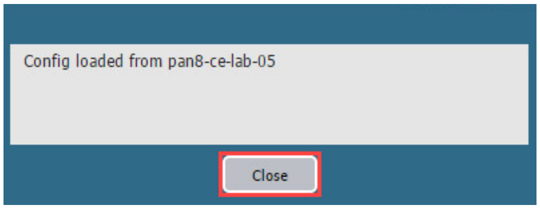
8. Navigate to **Device** > **Setup** > **Operations** > **Load named configuration snapshot**.



9. In the *Load Named Configuration* window, select **pan8-ce-lab-05** from the ***Name*** dropdown box and click **OK**.

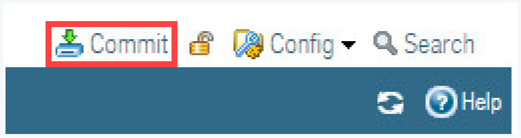


10. A message will confirm the configuration has loaded. Click **Close** to continue.

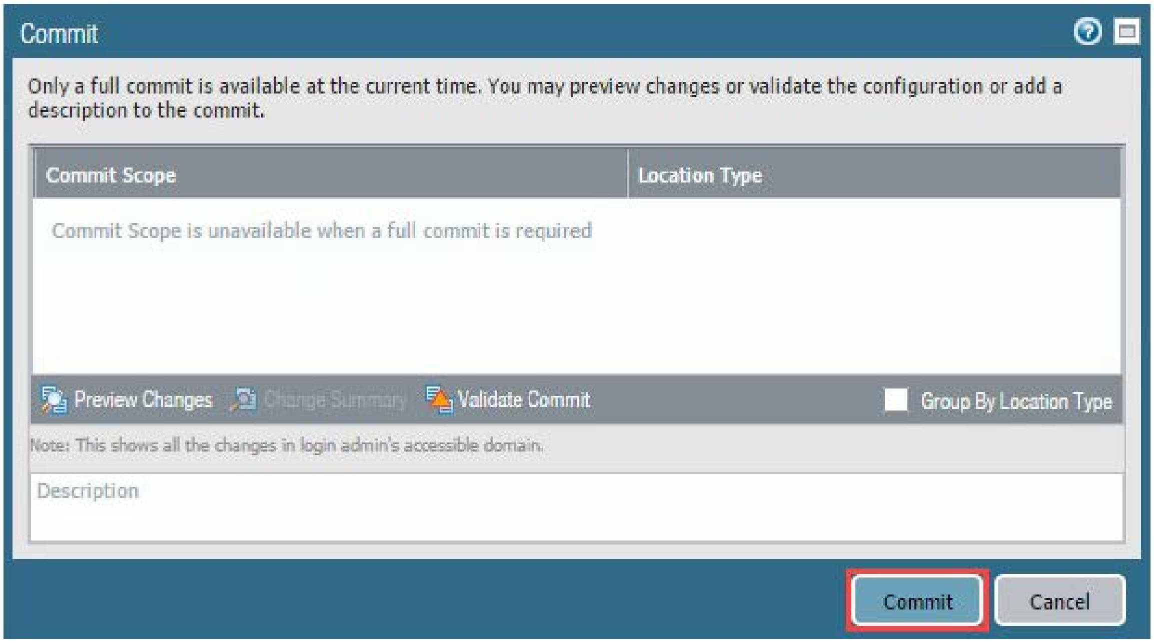


Config loaded from pan8-ce-lab-05

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



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

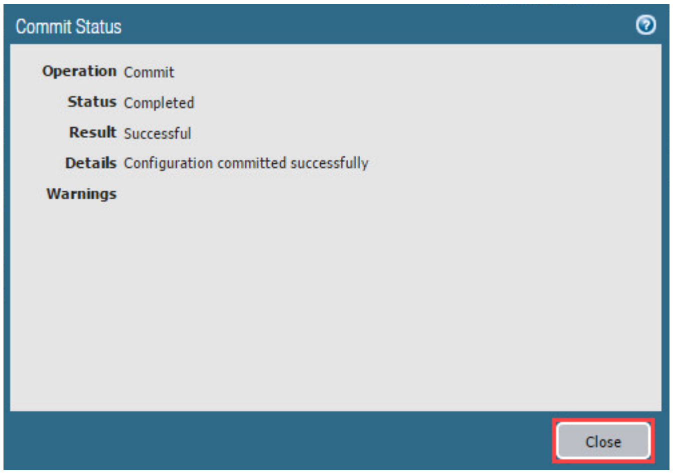


Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

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.

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



Commit Status

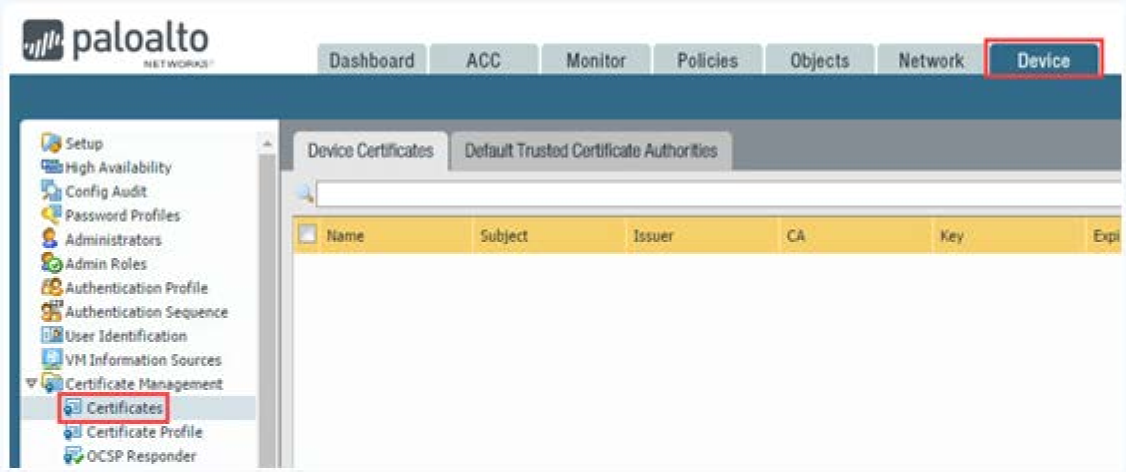
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

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.

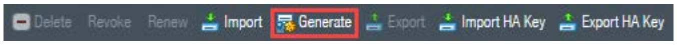
5.1 Generate Certificates

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.

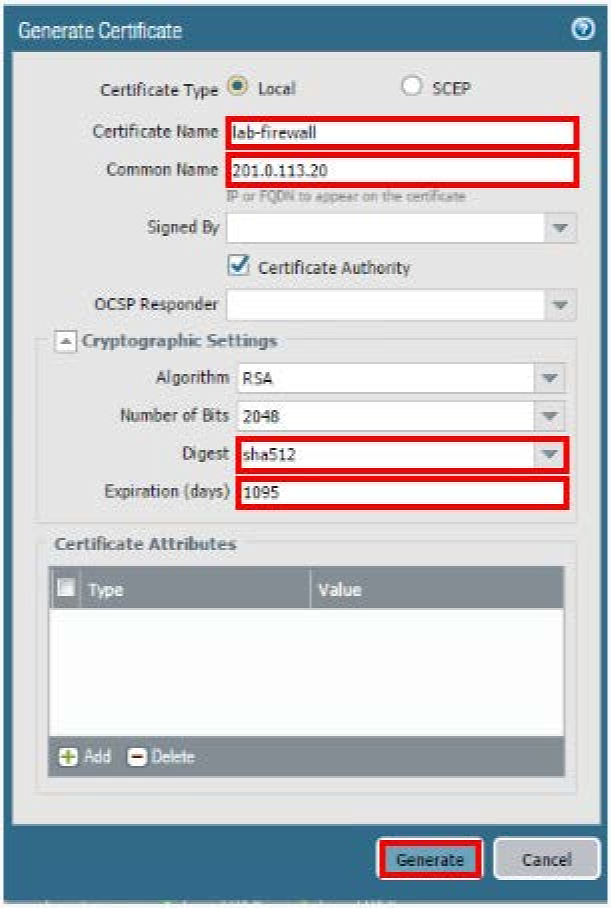
1. Navigate to **Device** > **Certificate Management > Certificates**.



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: 201.0.113.20

IP or FQDN to appear on the certificate

Signed By:

☑ Certificate Authority

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

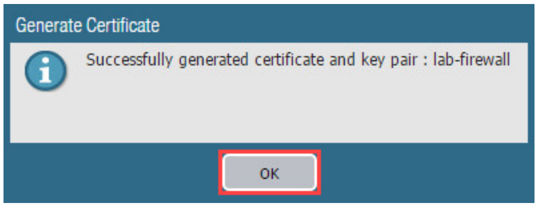
Digest: sha512

Expiration (days): 1095

Certificate Attributes

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).

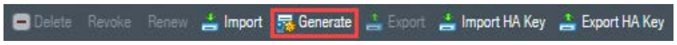
4. In the *Generate Certificate* window, click **OK** to continue.



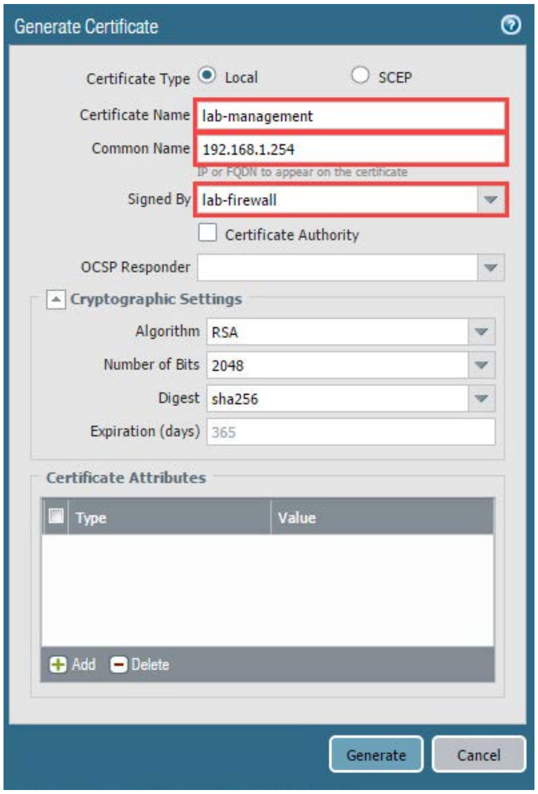
Generate Certificate

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.



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

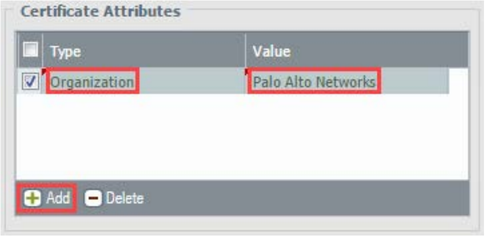
Expiration (days): 365

Certificate Attributes

Type	Value

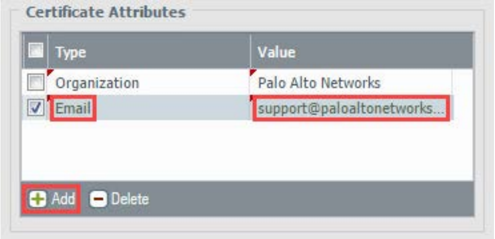
The IP address, **192.168.1.254**, used in the Common Name field is the Firewall's inside IP address. Notice you selected the previously created root CA certificate, **lab-firewall**, to sign this certificate. Client certificates that are used when requesting firewall services that rely on TLSv1.2 (such 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**.



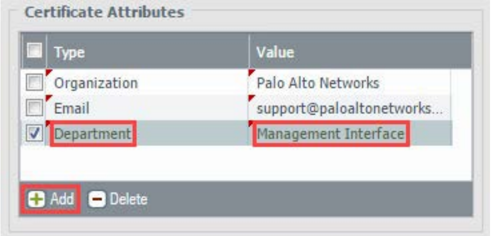
□	Type	Value
☑	Organization	Palo Alto Networks

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**.



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

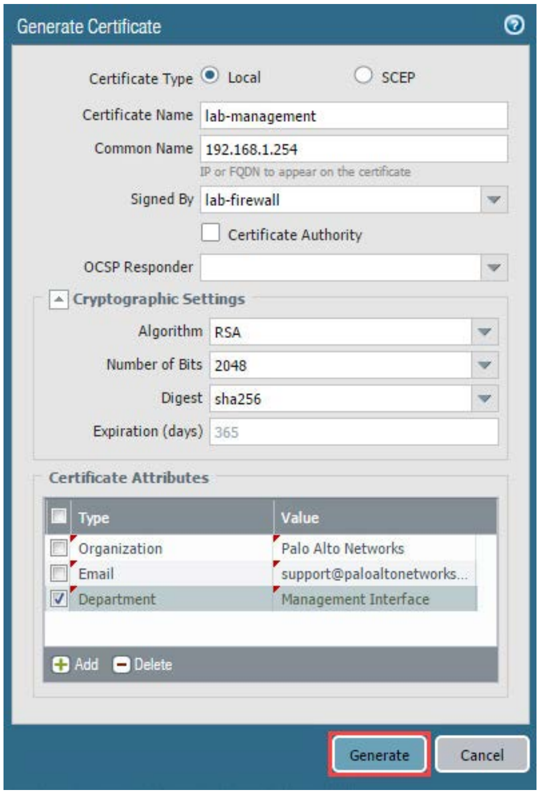
9. In the *Generate Certificate* window, click the **Add** button in the Certificate Attributes section. Then, select **Department** in the Type column. Next, double-click the empty box in the Value column, type **Management Interface** and press **Enter**.



□	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

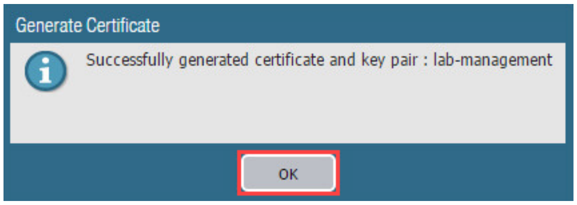
Digest: sha256

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.

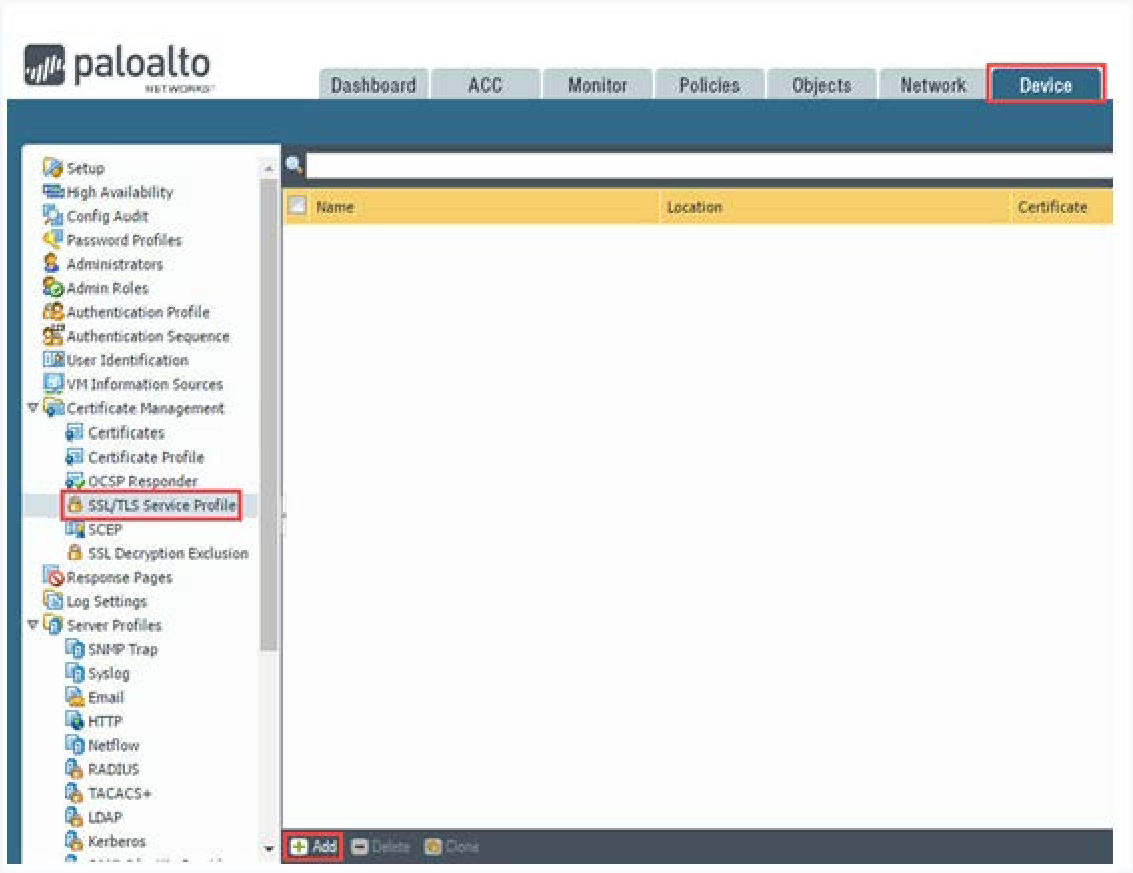
As a best practice, it is recommended you use different certificates for each usage.

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.

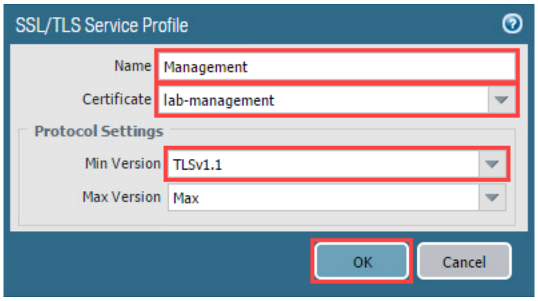
5.2 Replace the Certificate for Inbound Management Traffic

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 a 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.**



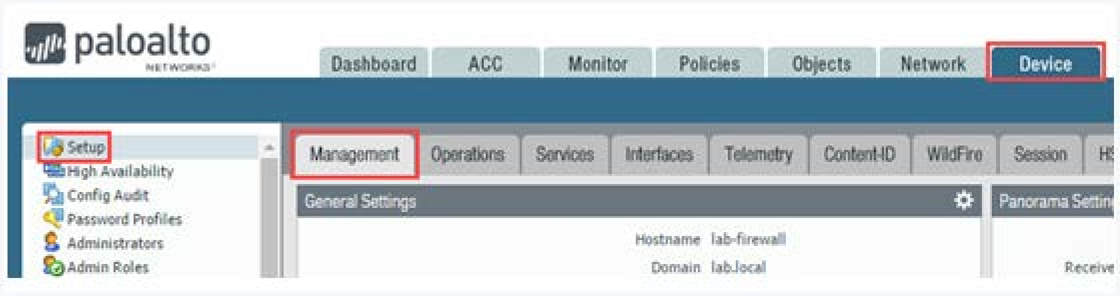
2. In the *SSL/TLS Service Profile* window, type **Management** in the Name field. Then, select **lab-management** from the Certificate dropdown. Next, select **TLSv1.1** from the Min Version dropdown. Finally, click the **OK** button.


SSL/TLS Service Profile

Name: Management
Certificate: lab-management

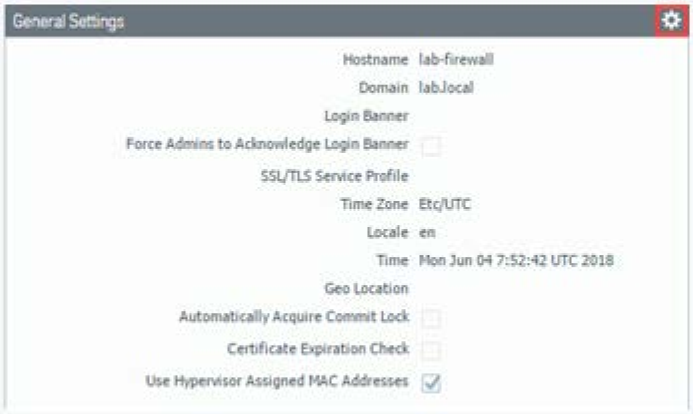
Protocol Settings
Min Version: TLSv1.1
Max Version: Max

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



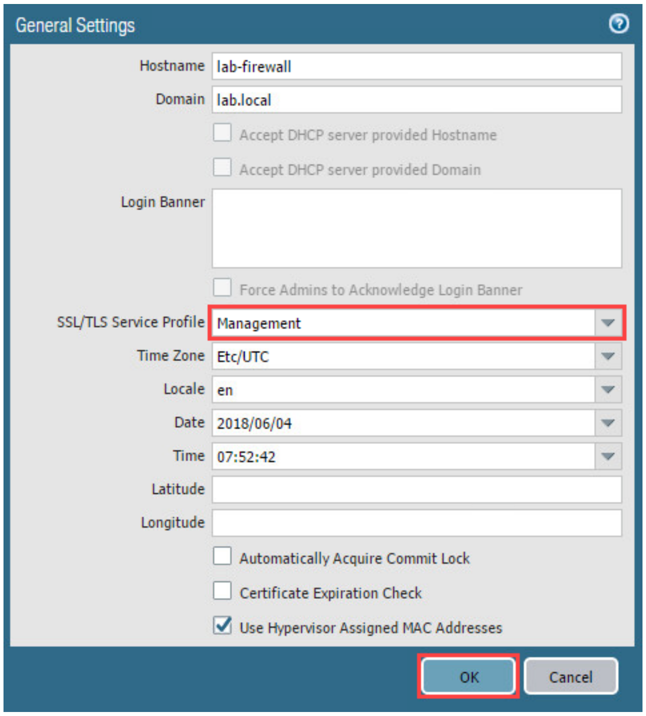
Hostname lab-firewall
Domain lab.local

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.

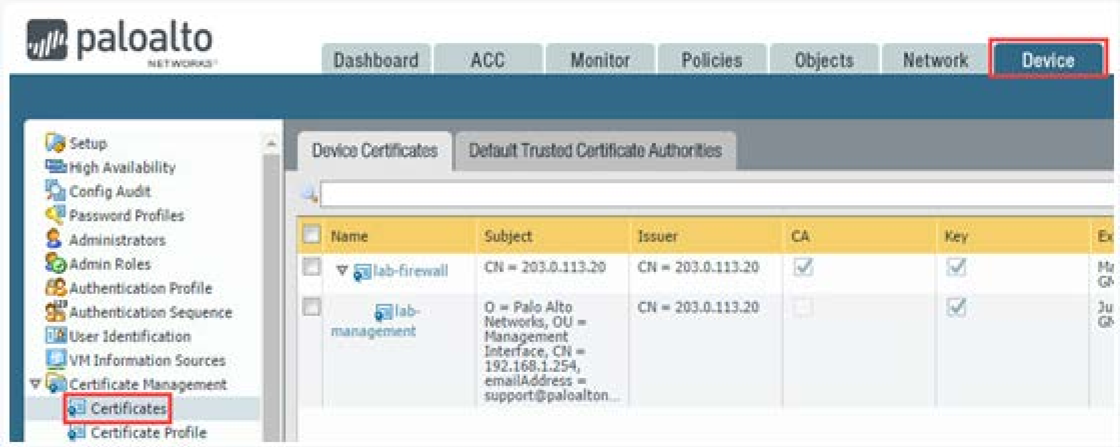


Hostname lab-firewall
Domain lab.local
□ Accept DHCP server provided Hostname
□ Accept DHCP server provided Domain
Login Banner
□ Force Admins to Acknowledge Login Banner
SSL/TLS Service Profile Management
Time Zone Etc/UTC
Locale en
Date 2018/06/04
Time 07:52:42
Latitude
Longitude
□ Automatically Acquire Commit Lock
□ Certificate Expiration Check
☑ Use Hypervisor Assigned MAC Addresses

5.3 Export Certificate and Commit

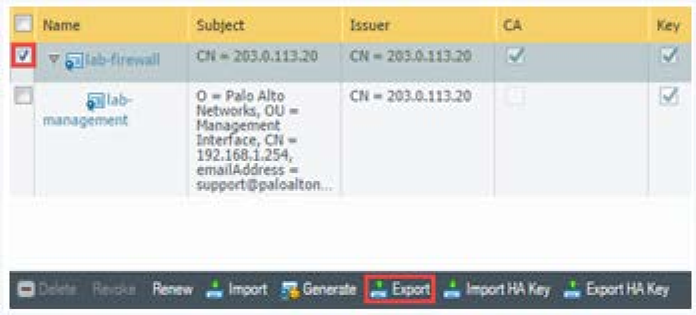
In this section, you will export the root CA certificate, **lab-firewall**. Then, you will commit your changes to the Firewall.

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



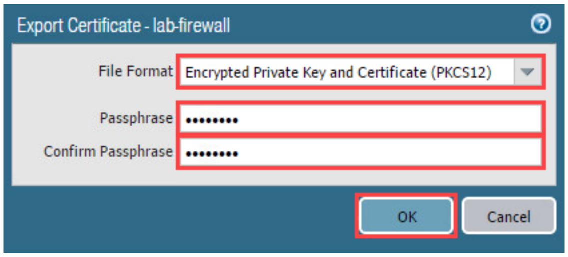
□	Name	Subject	Issuer	CA	Key	Ex
□	lab-firewall	CN = 203.0.113.20	CN = 203.0.113.20	✓	✓	Ma GM
□	lab-management	O = Palo Alto Networks, OU = Management Interface, CN = 192.168.1.254, emailAddress = support@paloalton...	CN = 203.0.113.20	□	✓	Ju GM

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



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

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



Export Certificate - lab-firewall

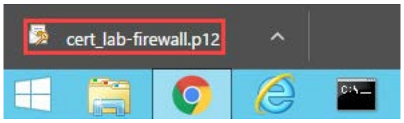
File Format: Encrypted Private Key and Certificate (PKCS12)

Passphrase: ••••••••

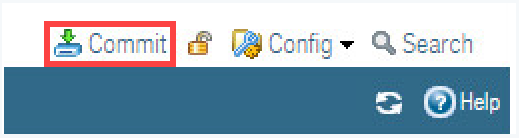
Confirm Passphrase: ••••••••

> 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.

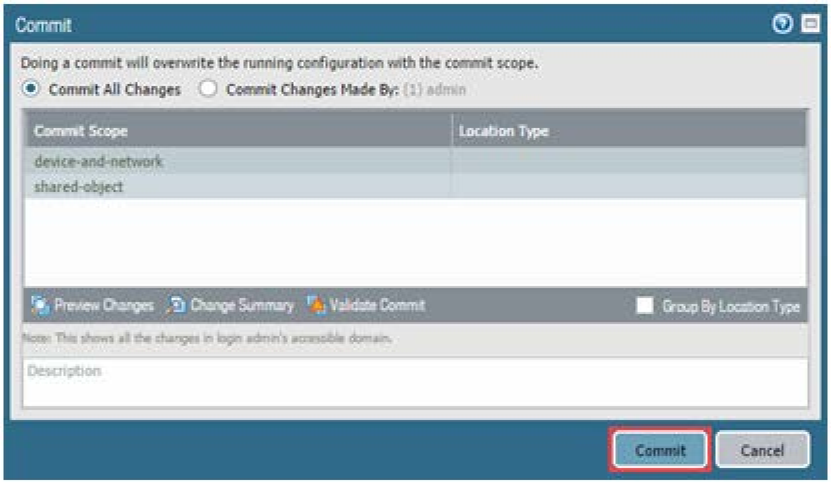
4. The **cert_lab-firewall.p12** file will download to the Client machine's Downloads folder.



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.



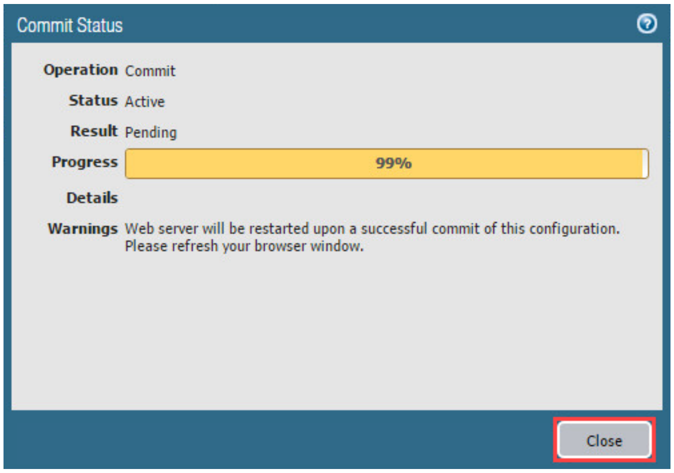
Doing a commit will overwrite the running configuration with the commit scope.

● 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.

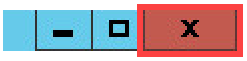
7. When the commit operation reaches 99%, click **Close** to continue.



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 Google Chrome.

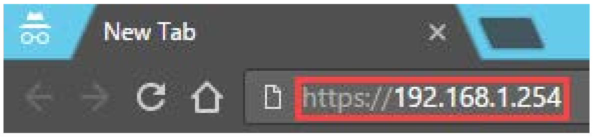


5.4 Test Connectivity and Import Certificate on the Client

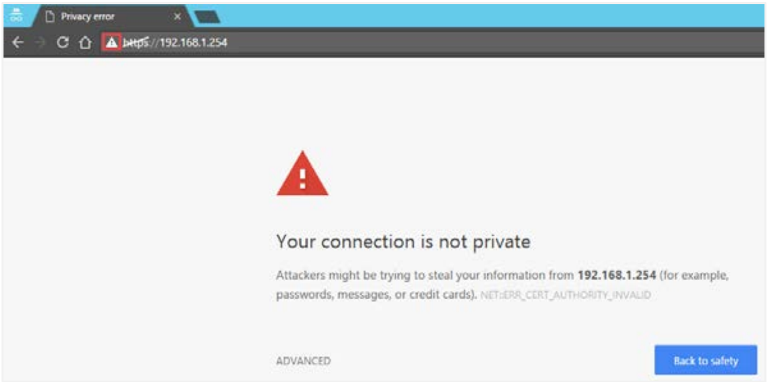
In this section, you will test connectivity to the Firewall. When establishing a secure connection with the Firewall, the client must trust the root CA that issued the certificate. Otherwise, the client browser will display a warning that the certificate is invalid and might (depending on security settings)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

1. Double-click the **Google Chrome** icon located on the Desktop.

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



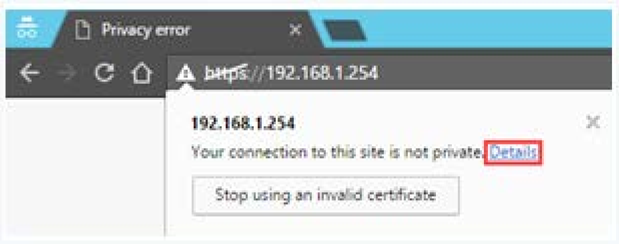
3. You will see a *"Your connection is not private"* message. This is because the Client cannot verify the certificate from the Firewall. To view the certificate, click the **!** icon (triangle exclamation) in the address bar.



Your connection is not private

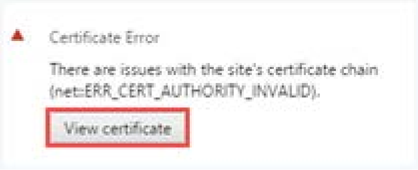
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

4. In the popup, click the **Details** link.



Privacy error
https://192.168.1.254
192.168.1.254
Your connection to this site is not private. Details
Stop using an invalid certificate

5. In the *Developer Tools* pane on the right, click on **View certificate** under the Certificate Error section.

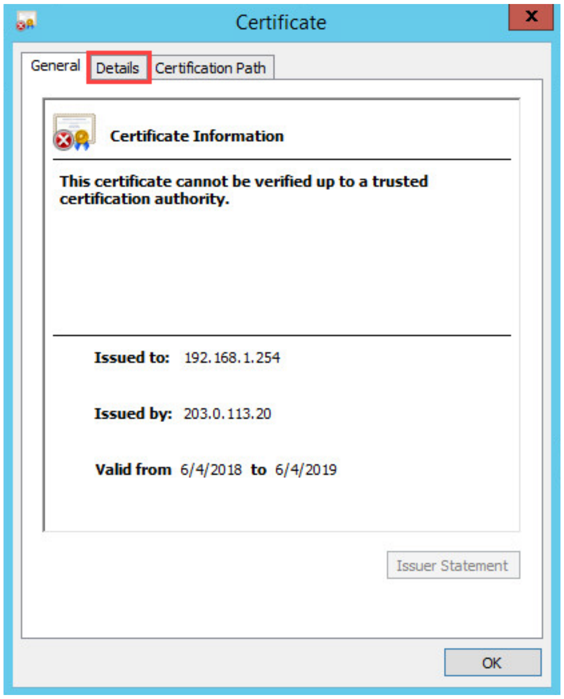


Certificate Error

There are issues with the site's certificate chain (net::ERR_CERT_AUTHORITY_INVALID).

Note the issue listed: **net::ERR_CERT_AUTHORITY_INVALID**.

6. In the *Certificate* window, click the **Details** tab.



Certificate Information

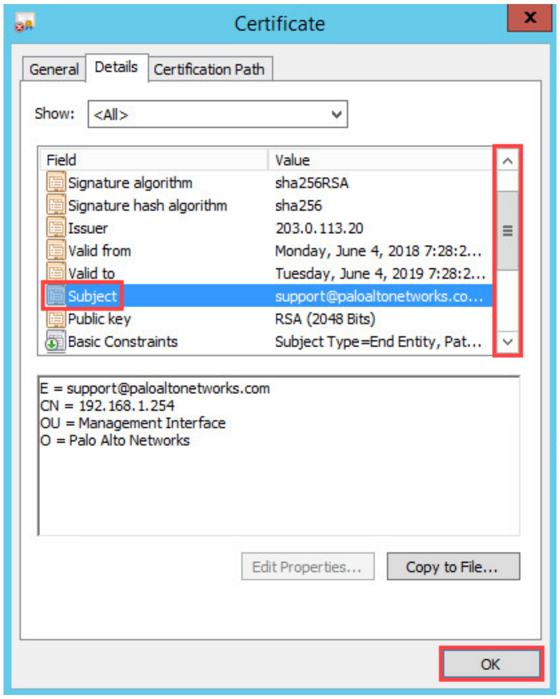
This certificate cannot be verified up to a trusted certification authority.

Issued to: 192.168.1.254

Issued by: 203.0.113.20

Valid from 6/4/2018 to 6/4/2019

7. Scroll down using the scroll bar on the right. Then, review then information. Next, click the **Subject** field. Finally, click the **OK** button.

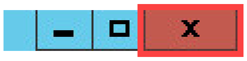


Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	203.0.113.20
Valid from	Monday, June 4, 2018 7:28:2...
Valid to	Tuesday, June 4, 2019 7:28:2...
Subject	support@paloaltonetworks.co...
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity, Pat...

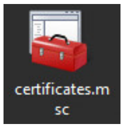
E = support@paloaltonetworks.com
CN = 192.168.1.254
OU = Management Interface
O = Palo Alto Networks

Notice the details match the **lab-management** certificate you created earlier in section 5.1. The sha256 algorithm is being used. The certificate was issued by **203.0.113.20**, which is the common-name of the root CA certificate, **lab-firewall**, you created. The Valid from and Valid to fields indicate the certificate is valid for 365 days. In the center, you will see the certificate attributes you set when you generated the certificate. The Public key is using RSA (2048 Bits).

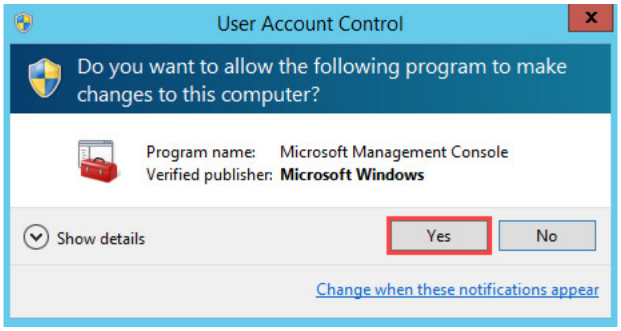
8. Click the **X** in the upper-right to close Google Chrome.



9. To install the **lab-firewall** certificate, double-click **certificates.msc** on the Desktop. This launches the Client's Certificate Manager snap-in for the Management Console.



10. In the *User Account Control* window, click the **Yes** button.

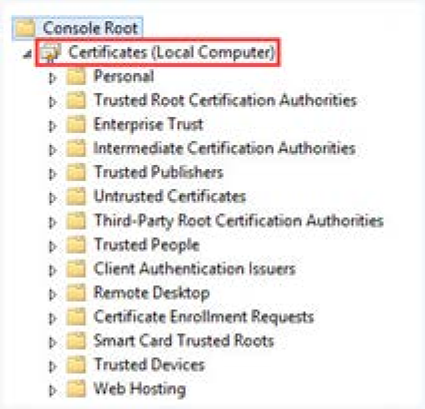


User Account Control

Do you want to allow the following program to make changes to this computer?

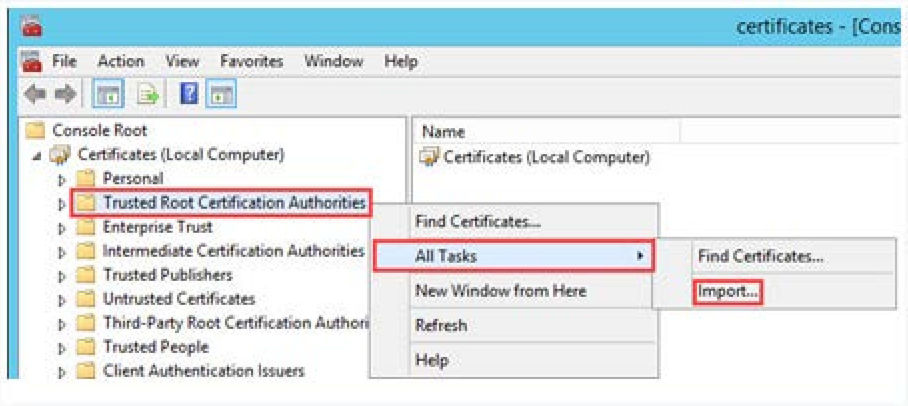
Program name: Microsoft Management Console
Verified publisher: **Microsoft Windows**

11. In the *certificates – [Console Root]* window, click **Certificates (Local Computer)** in the left side pane, to expand the section.

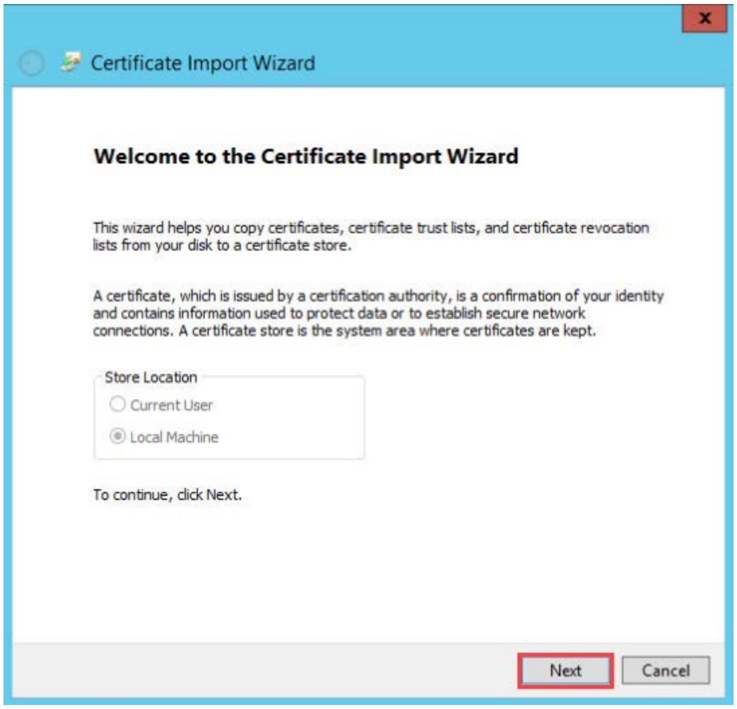


Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Web Hosting

12. In the *certificates – [Console Root]* window, right-click the **Trusted Root Certification Authorities** folder. Then, click on **All Tasks > Import…**



13. In the *Certificate Import Wizard* window, click the **Next** button.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

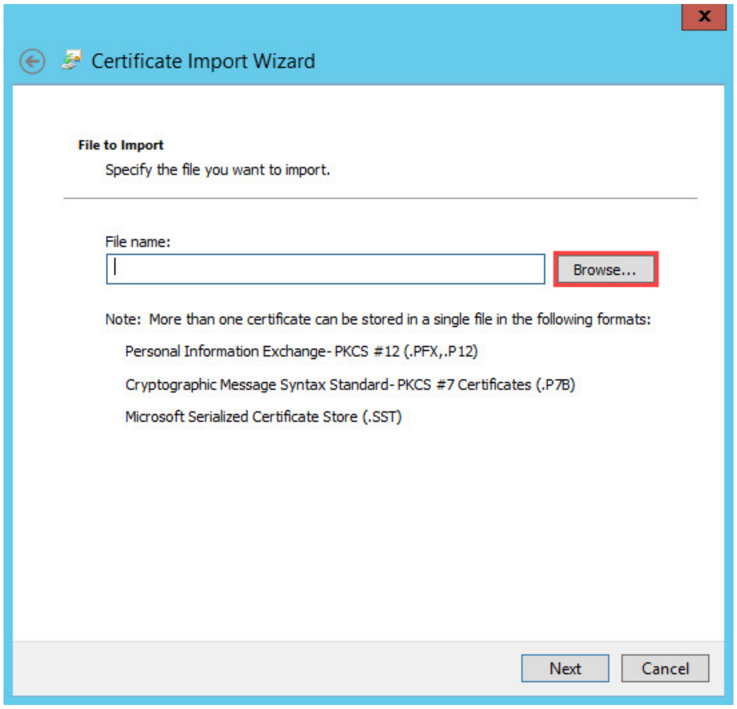
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

14. In the *Certificate Import Wizard* window, click the **Browse…** button.



Certificate Import Wizard

File to Import
Specify the file you want to import.

File name:

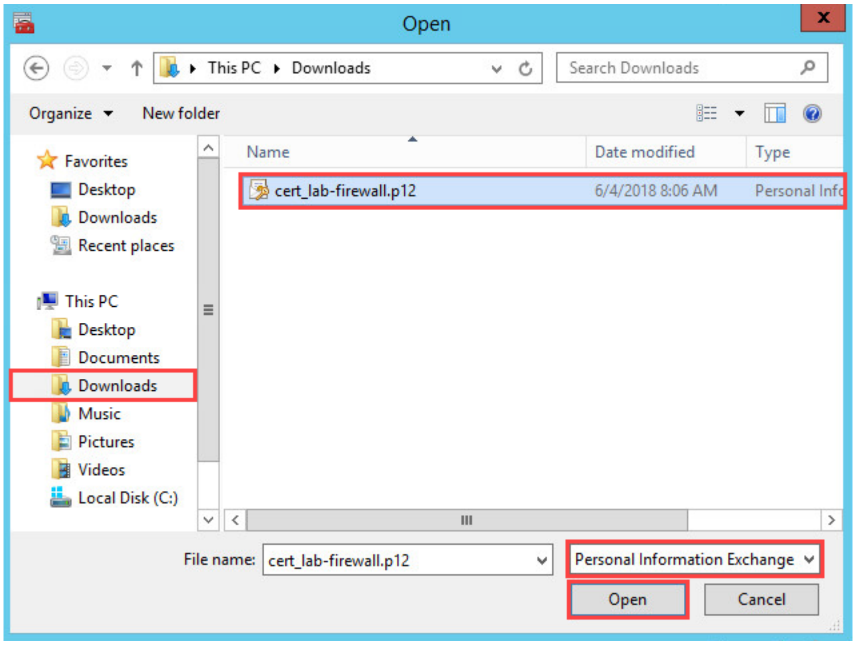
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

15. In the *Open* window, click on **Downloads** folder on the left. Then, select **Personal Information Exchange (*.pfx;*.p12)** from the File Type dropdown in the lower-right. Next, select the **cert_lab-firewall.p12** file. Finally, click the **Open** button.

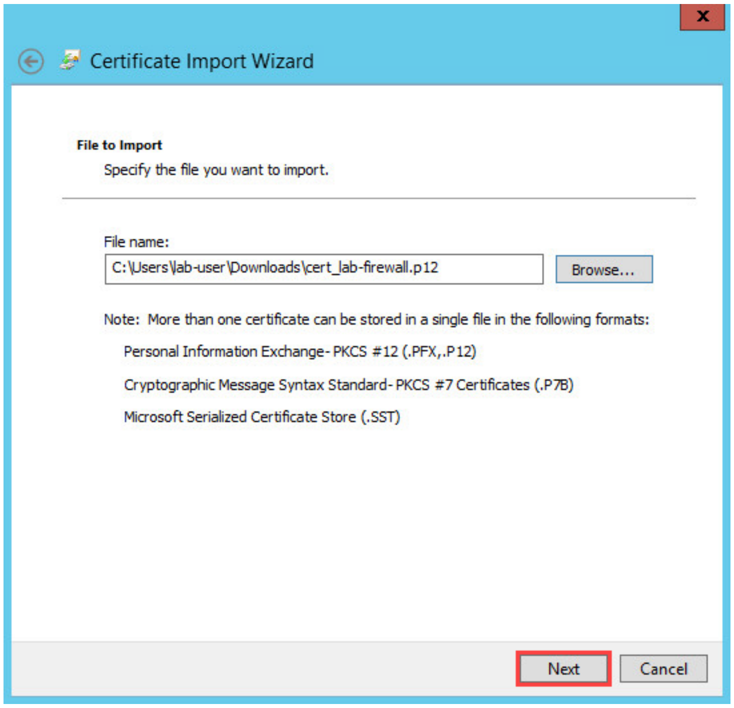


cert_lab-firewall.p12 6/4/2018 8:06 AM Personal Info

File name: cert_lab-firewall.p12

Personal Information Exchange

16. In the *Certificate Import Wizard* window, click the **Next** button.



File to Import

Specify the file you want to import.

File name:

C:\Users\lab-user\Downloads\cert_lab-firewall.p12

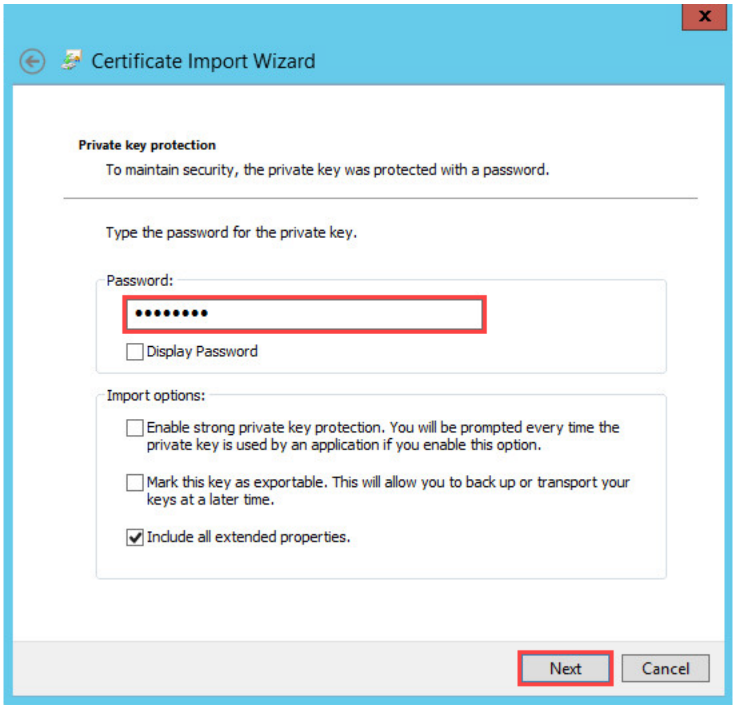
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

17. In the *Certificate Import Wizard* window, type **paloalto**. This is the passphrase you entered when you exported the certificate from the Firewall. Then, click the **Next** button.



Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: ••••••••

□ Display Password

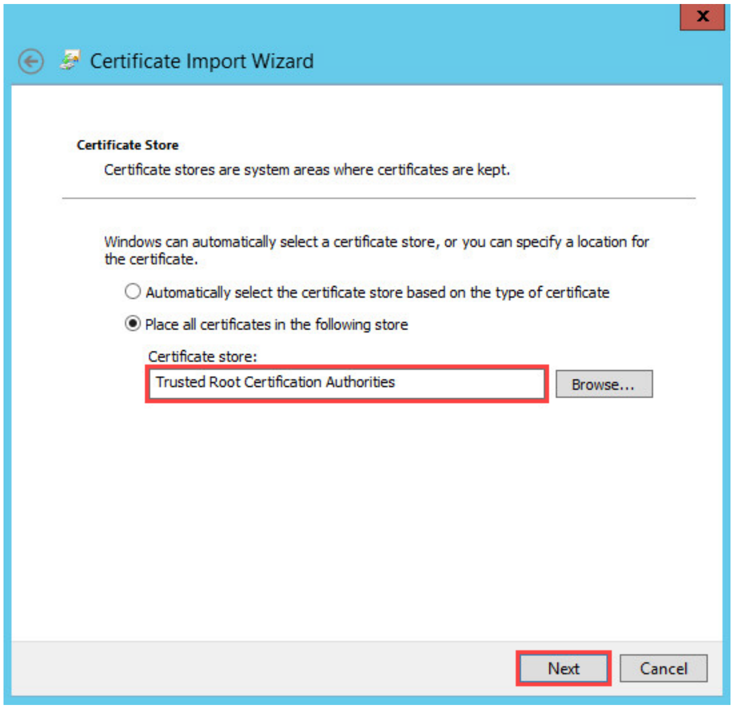
Import options:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

18. In the *Certificate Import Wizard* window, leave the default **Trusted Root Certification Authorities**, in the Certificate Store field. Then, click the **Next** button.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

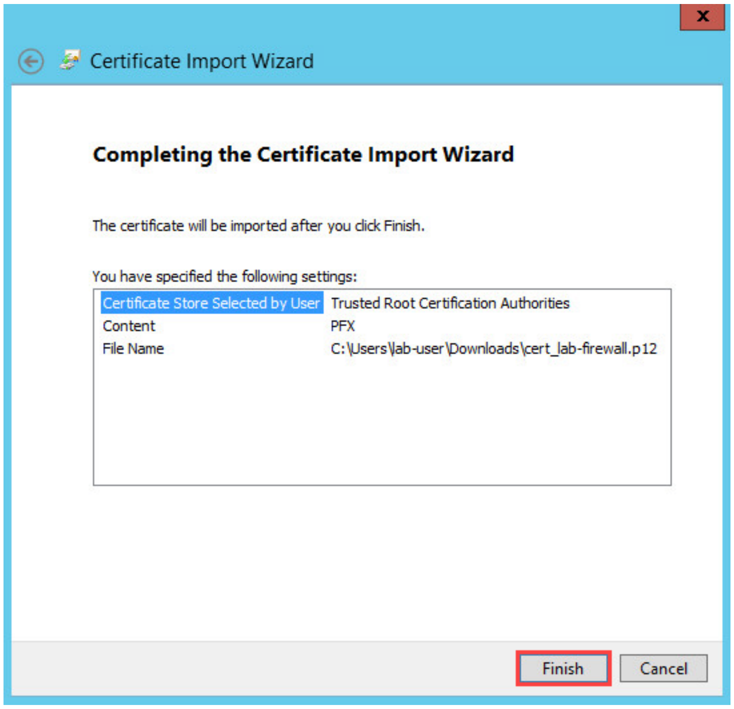
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

19. In the *Certificate Import Wizard* window, click the **Finish** Button.



Certificate Import Wizard

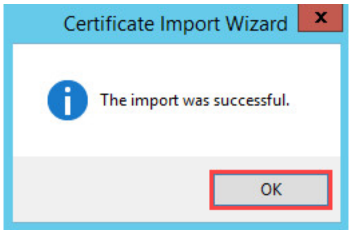
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	PFX
File Name	C:\Users\lab-user\Downloads\cert_lab-firewall.p12

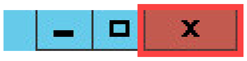
20. In the *Certificate Import Wizard* window, click the **OK** button.



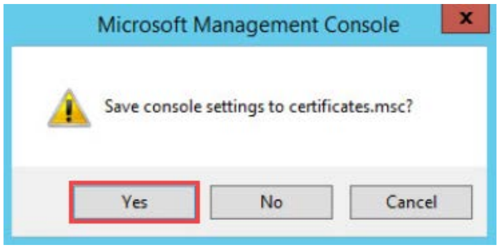
Certificate Import Wizard

The import was successful.

21. Click the **X** in the upper-right to close the Certificate Manager.



22. In the *Microsoft Management Console* window, click the **Yes** button to save console settings.

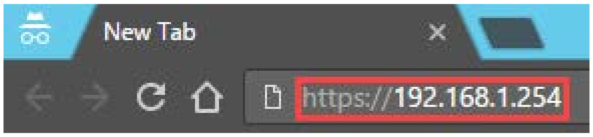


Microsoft Management Console

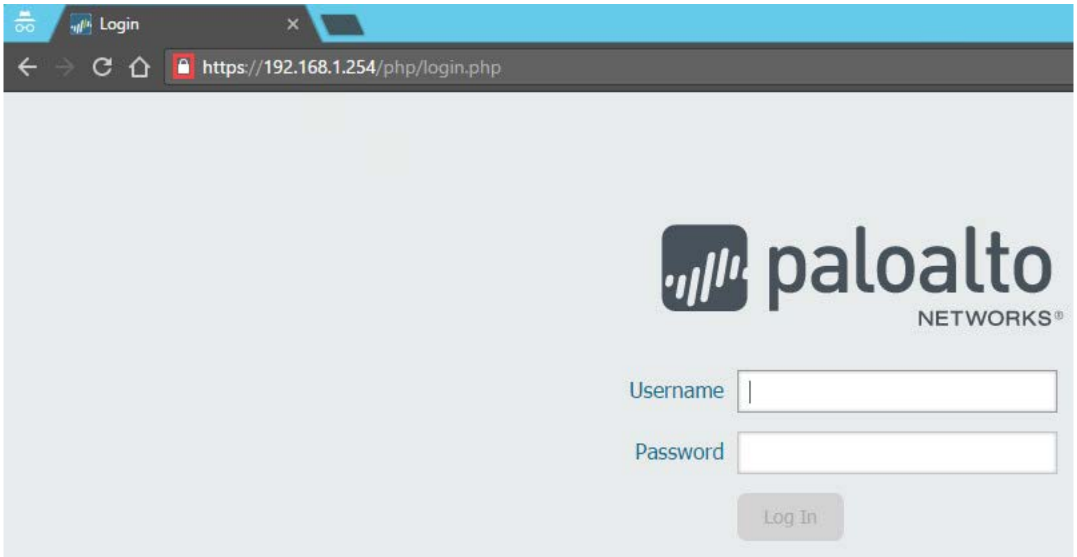
Save console settings to certificates.msc?

23. Double-click the **Google Chrome** icon located on the Desktop.

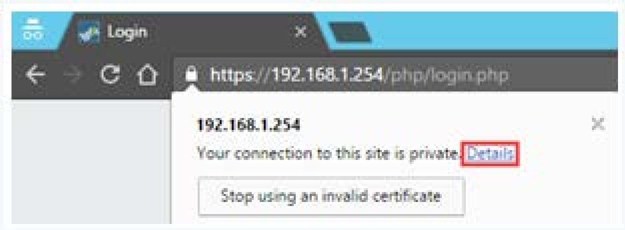
24. In the *Google Chrome* address bar, type **https://192.168.1.254** and press **Enter**.



25. 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.



26. In the popup, click the **Details** link.

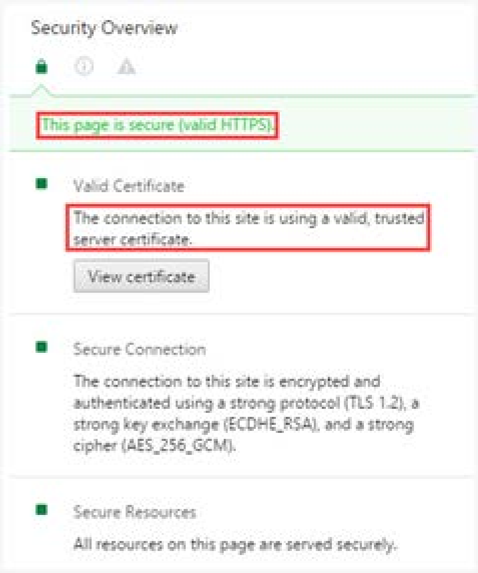


192.168.1.254

Your connection to this site is private. Details

Stop using an invalid certificate

27. In the *Developer Tools* pane on the right, notice the message "*This page is secure (valid HTTPS)*". Below, under the Valid Certificate section, you will see the message "*The connection to this site is using a valid, trusted server certificate.*"



Security Overview

This page is secure (valid HTTPS).

Valid Certificate

The connection to this site is using a valid, trusted server certificate.

Secure Connection

The connection to this site is encrypted and authenticated using a strong protocol (TLS 1.2), a strong key exchange (ECDHE_RSA), and a strong cipher (AES_256_GCM).

Secure Resources

All resources on this page are served securely.