CYBERSECURITY FOUNDATION V2

Lab 4: Configuring Authentication

Document Version: 2022-12-22

Contents

Introduction

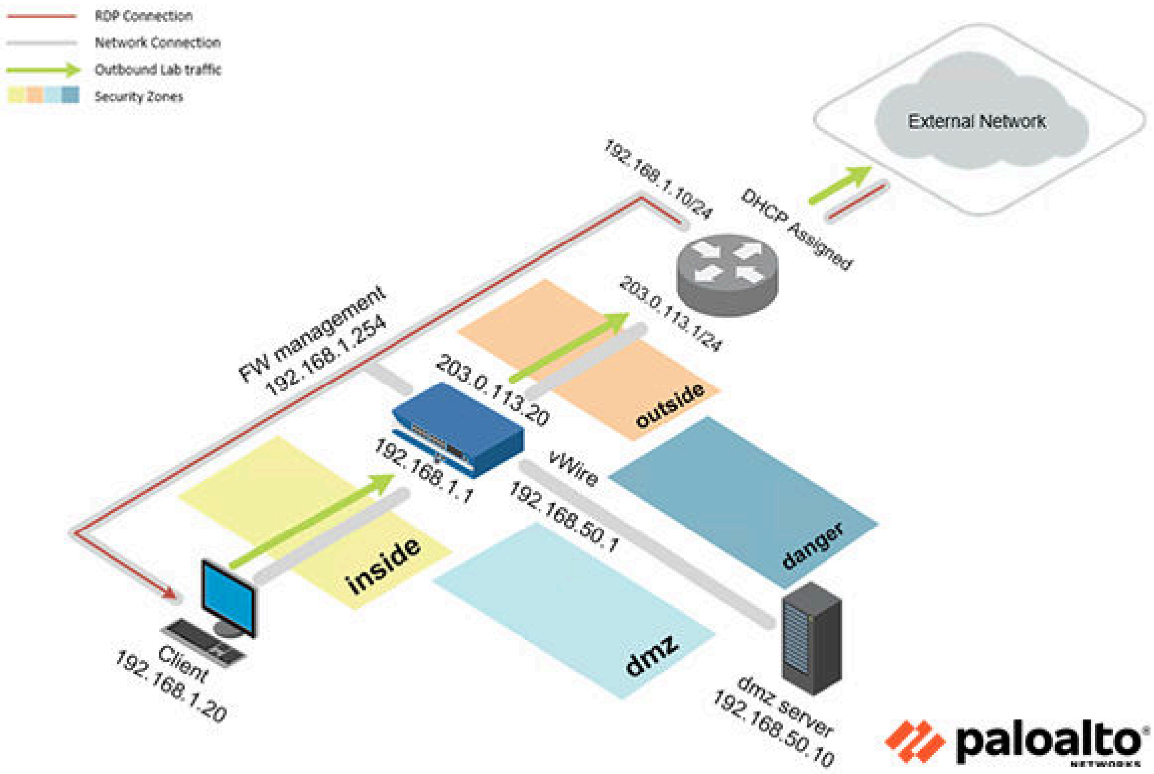
In this lab, you will configure the Firewall to use a Captive Portal to authenticate users by using a local user account and Authentication Policy.

Objective

In this lab, you will perform the following tasks:

- Configure a Local User Account and Authentication Profile
- Enable the Captive Portal and Enable Web-Form based Logins
- Create an Authentication Policy
- Commit and Test Authentication Policy

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.

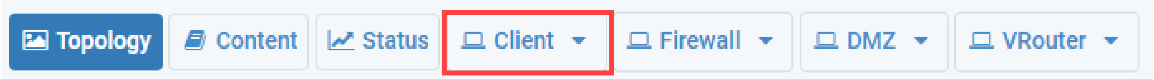
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Configuring Authentication

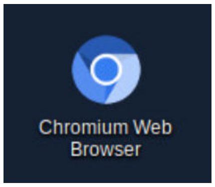
1.0 Load Lab Configuration

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

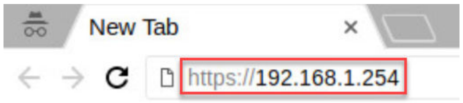
1. Click on the **Client** tab to access the Client PC.



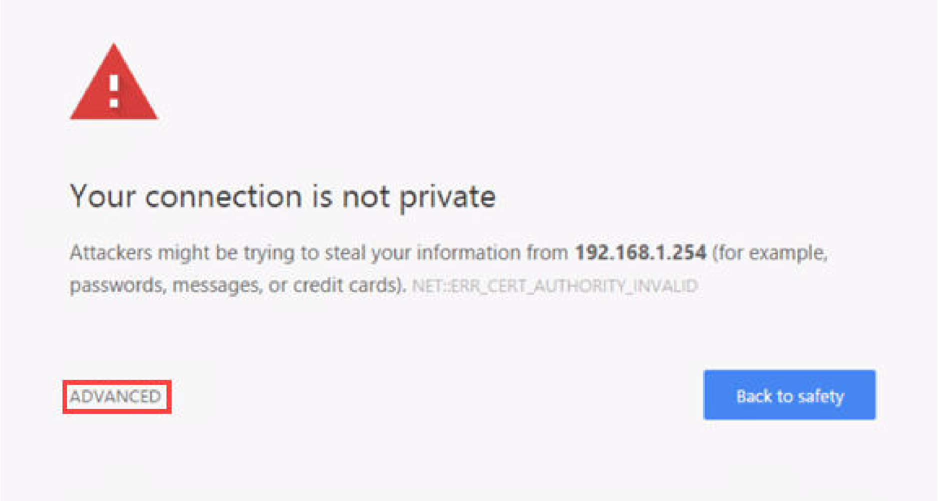
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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



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

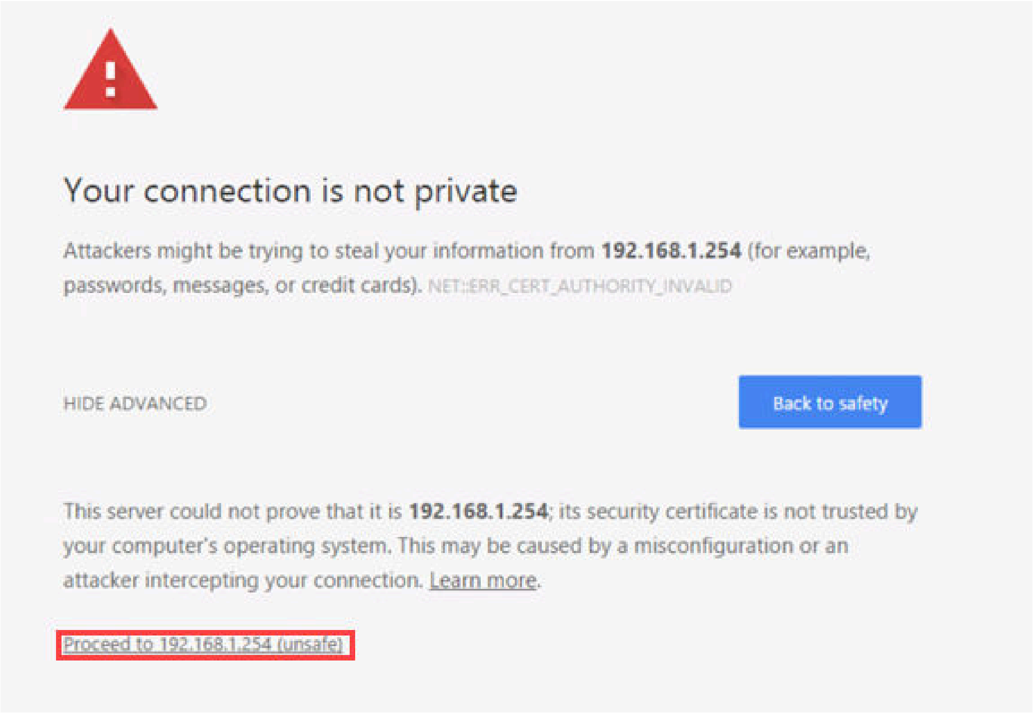


Your connection is not private

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

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

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

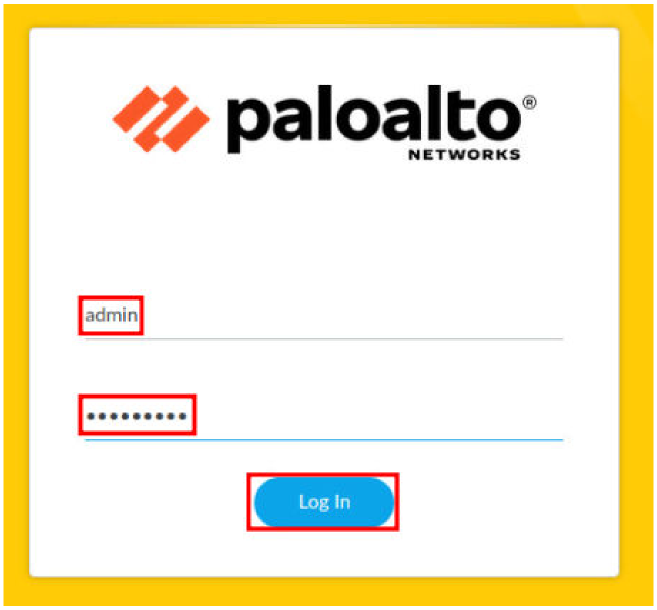


Your connection is not private

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

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

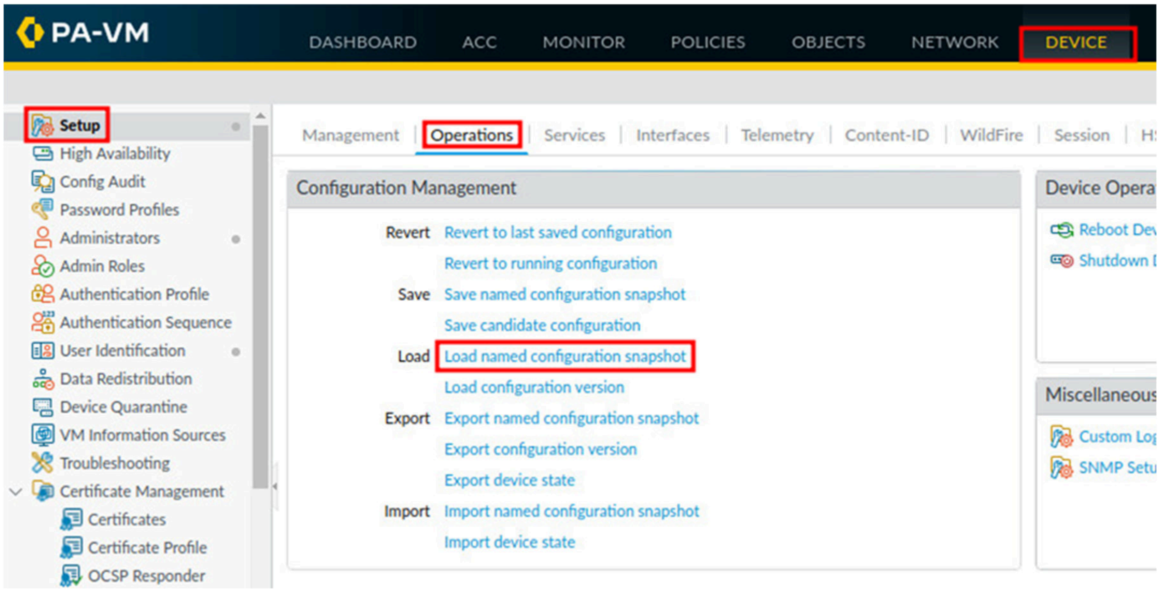
7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.



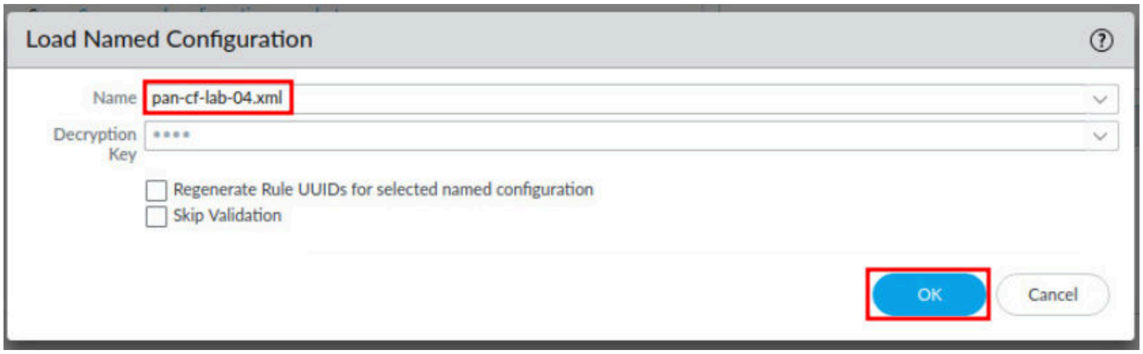
admin

•••••••••

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



9. In the *Load Named Configuration* window, select **pan-cf-lab-04.xml** from the *Name* dropdown box and click **OK**.


Load Named Configuration

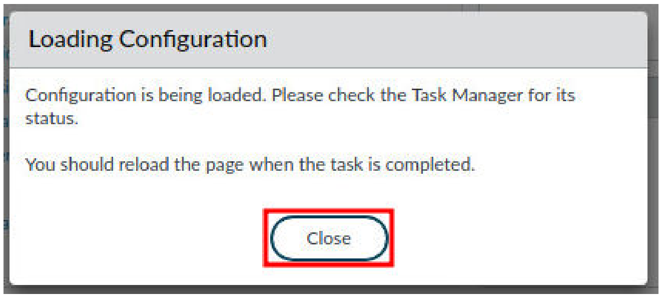
Name: pan-cf-lab-04.xml

Decryption Key: ••••

☐ Regenerate Rule UUIDs for selected named configuration

☐ Skip Validation

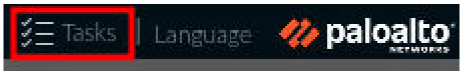
10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

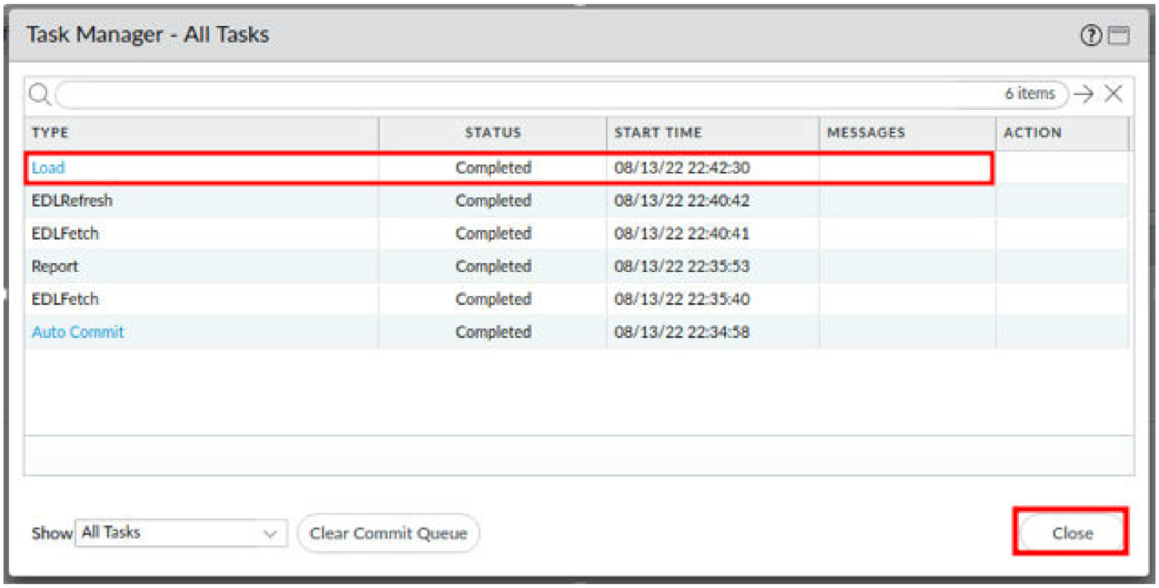
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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



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



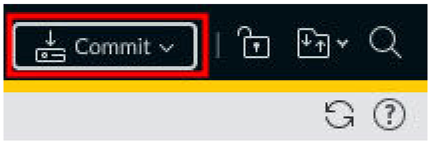
Task Manager - All Tasks

6 items

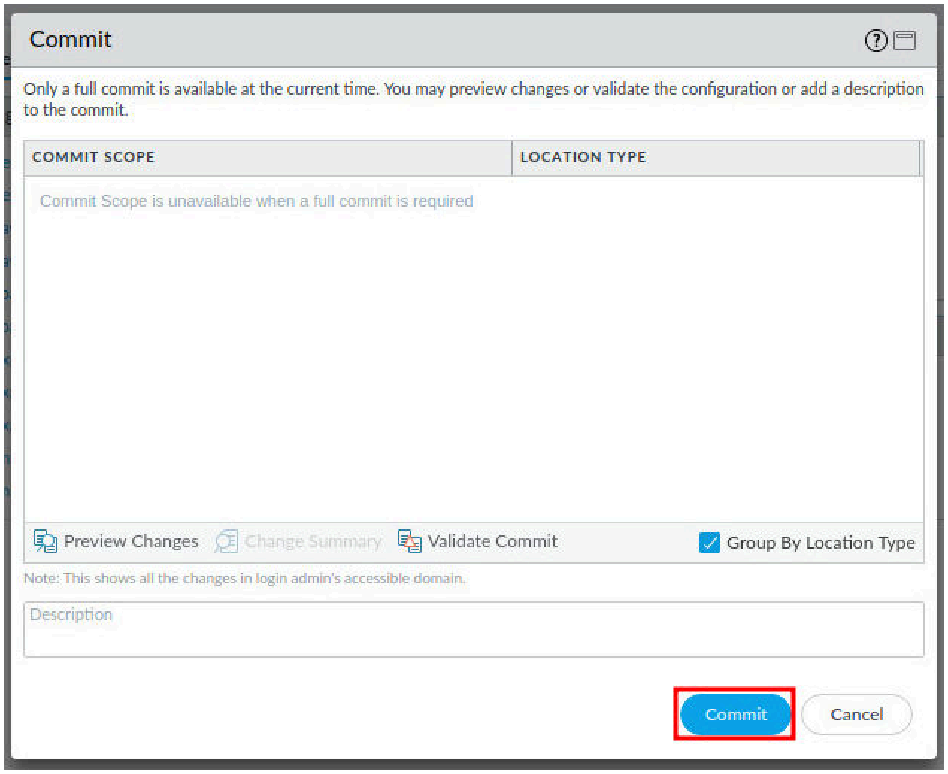
TYPE	STATUS	START TIME	MESSAGES	ACTION
Load	Completed	08/13/22 22:42:30		
EDLRefresh	Completed	08/13/22 22:40:42		
EDLFetch	Completed	08/13/22 22:40:41		
Report	Completed	08/13/22 22:35:53		
EDLFetch	Completed	08/13/22 22:35:40		
Auto Commit	Completed	08/13/22 22:34:58		

Show All Tasks

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



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



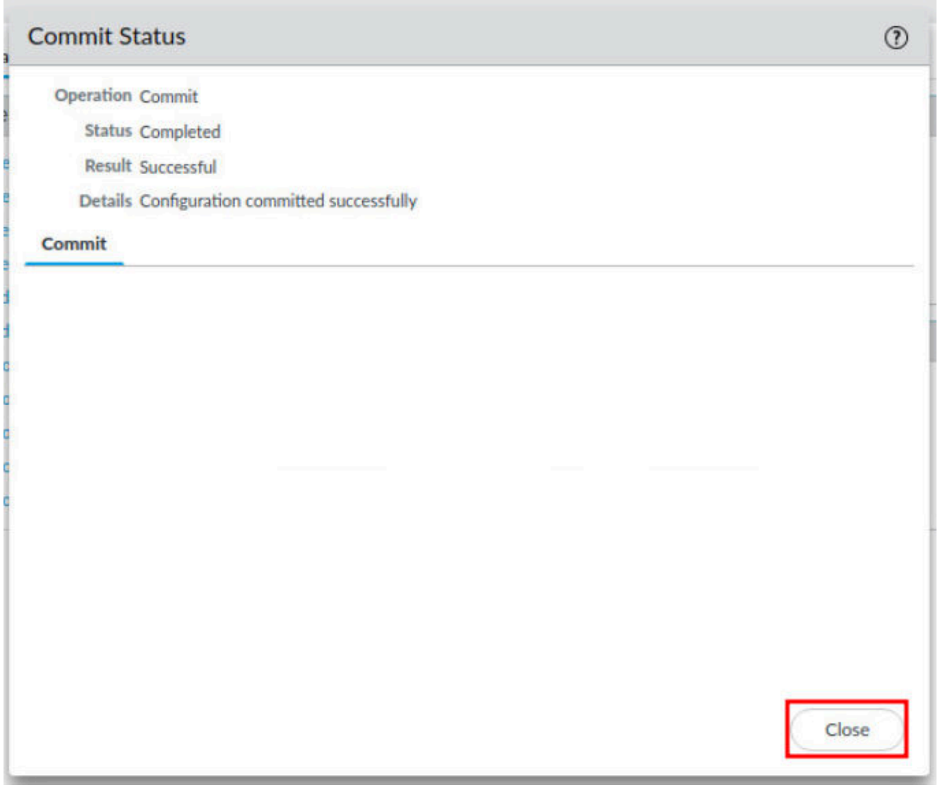
Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

☑ Group By Location Type

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

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



Operation Commit

Status Completed

Result Successful

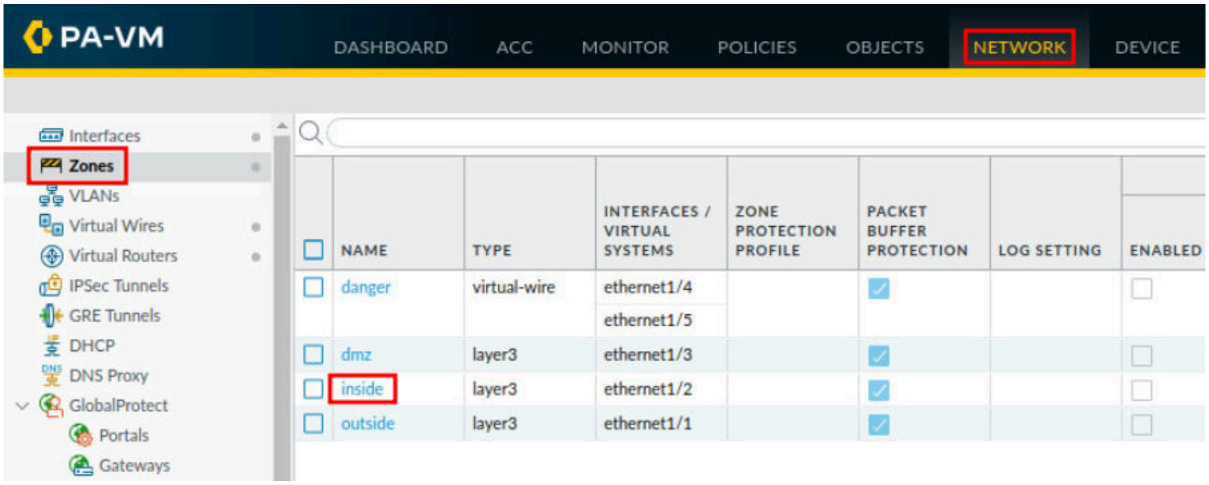
Details Configuration committed successfully

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 Configure a Local User Account and Authentication Profile

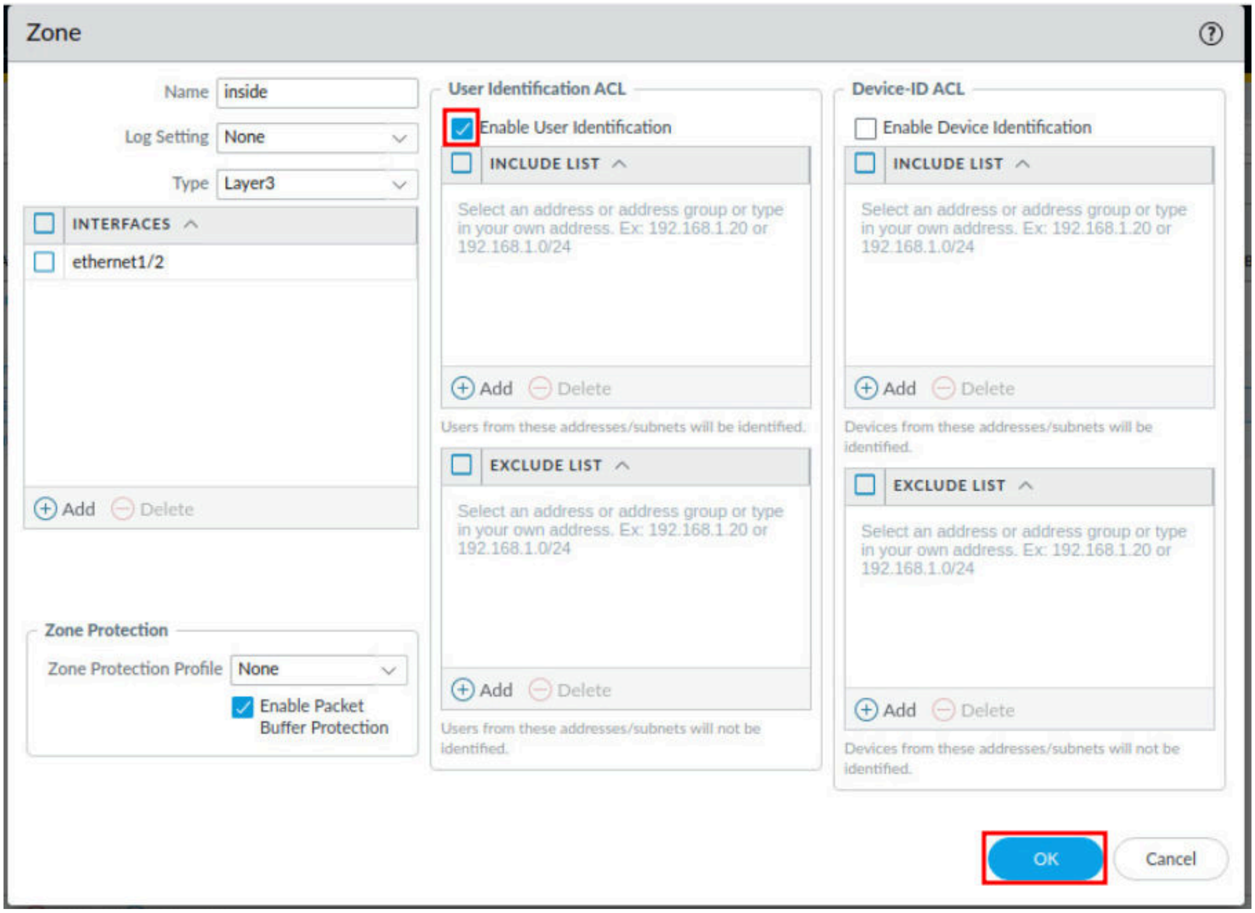
In this section, you will configure a local user account. Then, you will create a local authentication profile, which will later be assigned to a security policy.

1. Navigate to **Network > Zones**, and click on the **inside** zone**.**



□	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED
□	danger	virtual-wire	ethernet1/4 ethernet1/5		☑		□
□	dmz	layer3	ethernet1/3		☑		□
□	inside	layer3	ethernet1/2		☑		□
□	outside	layer3	ethernet1/1		☑		□

2. In the *Zone* window, click the **Enable User Identification** checkbox under the *User Identification ACL*. Then, click the **OK** button.



Zone

Name: inside

Log Setting: None

Type: Layer3

□ INTERFACES

□ ethernet1/2

Zone Protection

Zone Protection Profile: None

☑ Enable Packet Buffer Protection

User Identification ACL

☑ Enable User Identification

□ INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

□ EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

Device-ID ACL

□ Enable Device Identification

□ INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Devices from these addresses/subnets will be identified.

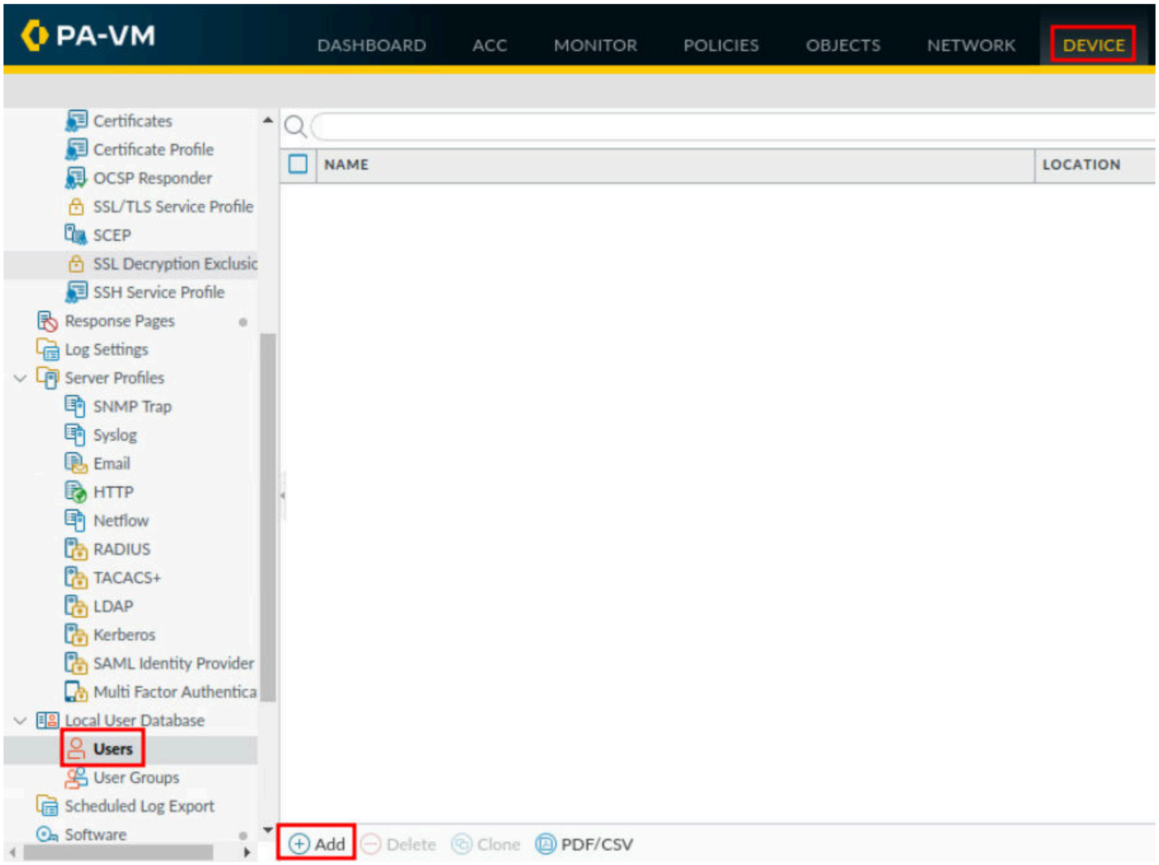
□ EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

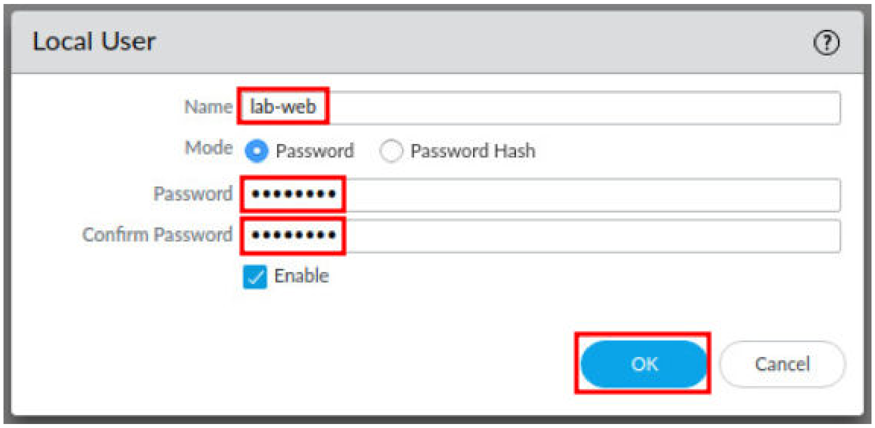
Devices from these addresses/subnets will not be identified.

This will enable the inside zone to use a Username for authentication.

3. Navigate to **Device > Local User Database > Users > Add**. You may need to scroll down on the left pane.



4. In the *Local User* window, type `lab-web` in the *Name* field. Then, type `Pal0Alt0` in the *Password* and *Confirm Password* fields. Finally, click the **OK** button.


Local User

Name: lab-web

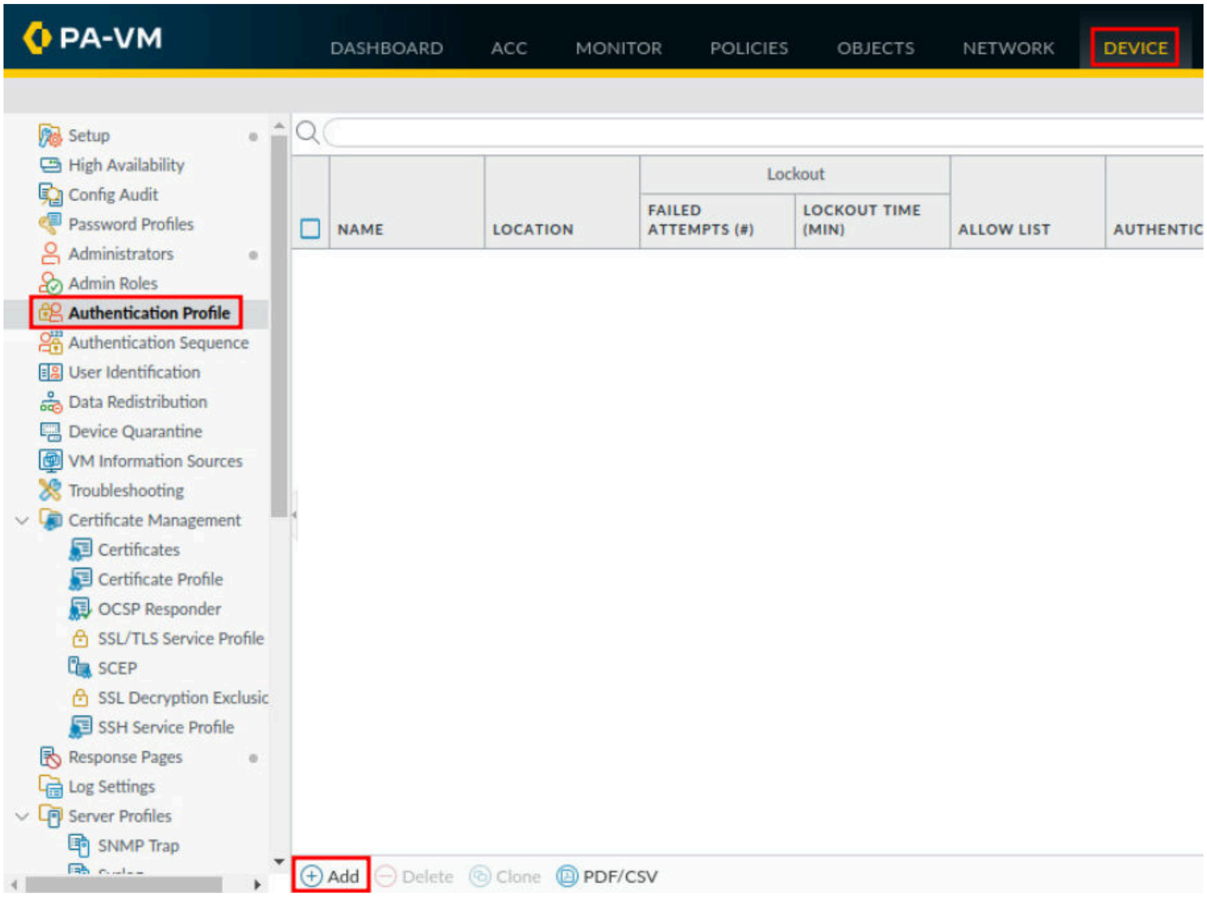
Mode: ● Password ○ Password Hash

Password: ••••••••

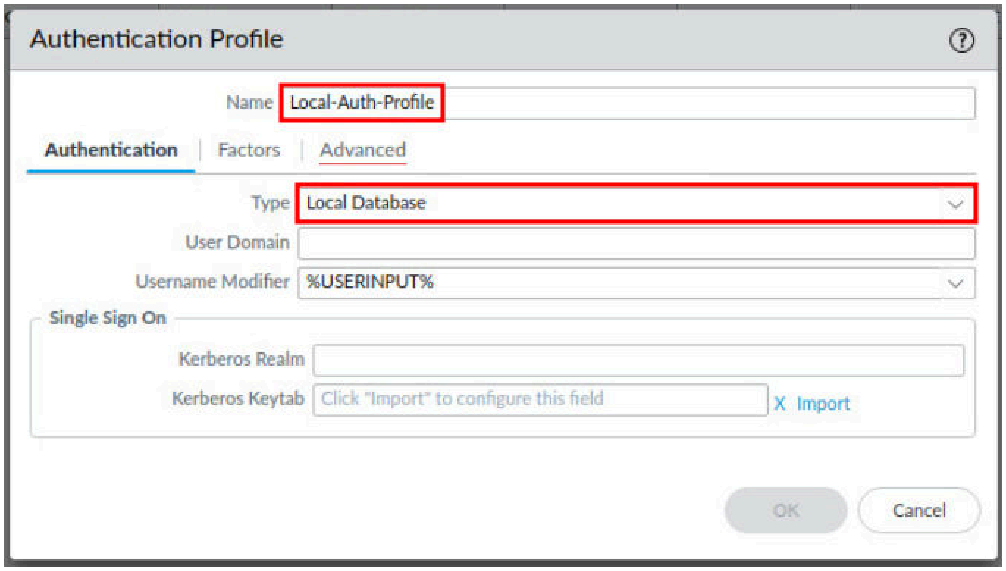
Confirm Password: ••••••••

☑ Enable

5. Navigate to **Device > Authentication Profile > Add**. You may need to scroll up on the left pane.



6. In the *Authentication Profile* window, type `Local-Auth-Profile` in the *Name* field. Then, select **Local Database** from the *Type* dropdown.


Authentication Profile

Name: Local-Auth-Profile

Authentication | Factors | Advanced

Type: Local Database

User Domain:

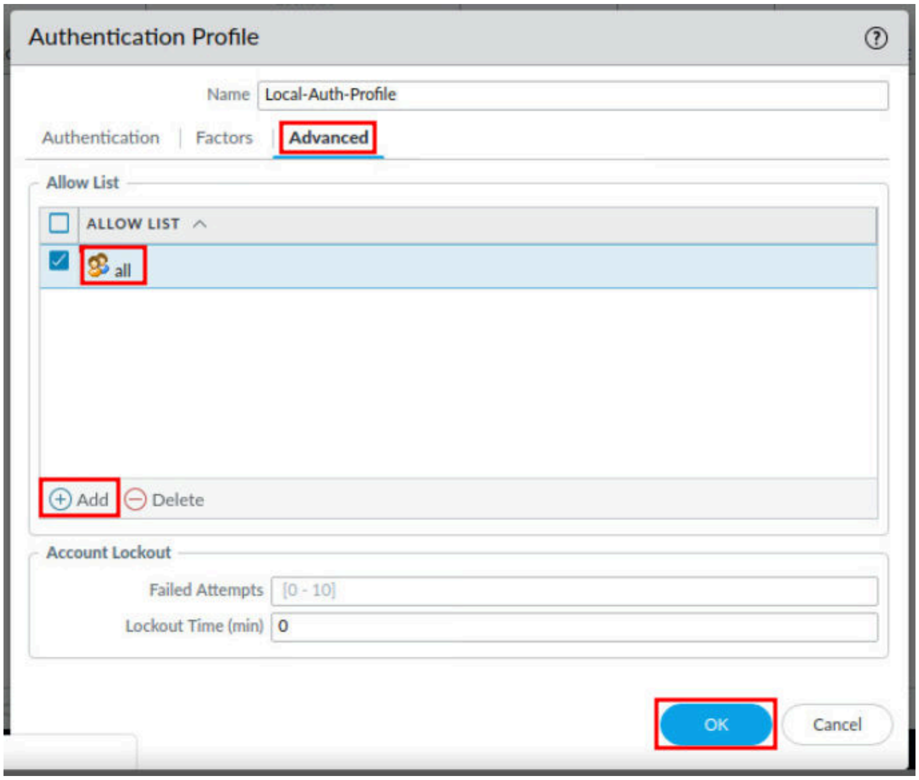
Username Modifier: %USERINPUT%

Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field

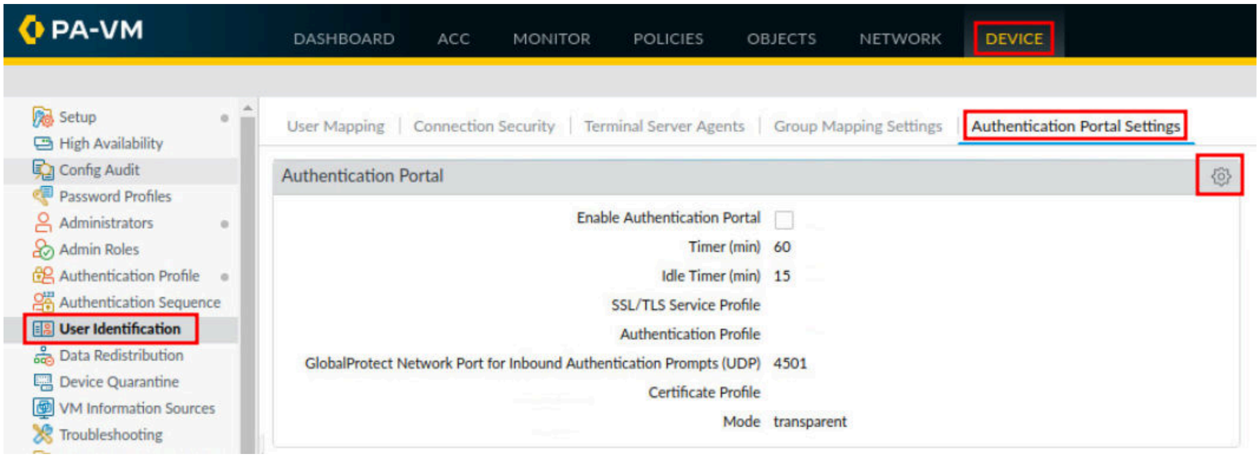
7. In the *Authentication Profile* window, click on the **Advanced** tab. Then, click on the **Add** button. Next, select **all** from the dropdown in the *Allow List* column. Finally, click the **OK** button.



1.2 Enable the Authentication Portal and Enable Web-Form based Logins

In this section, you will enable a captive portal. In that captive portal, you will use a web-form for login.

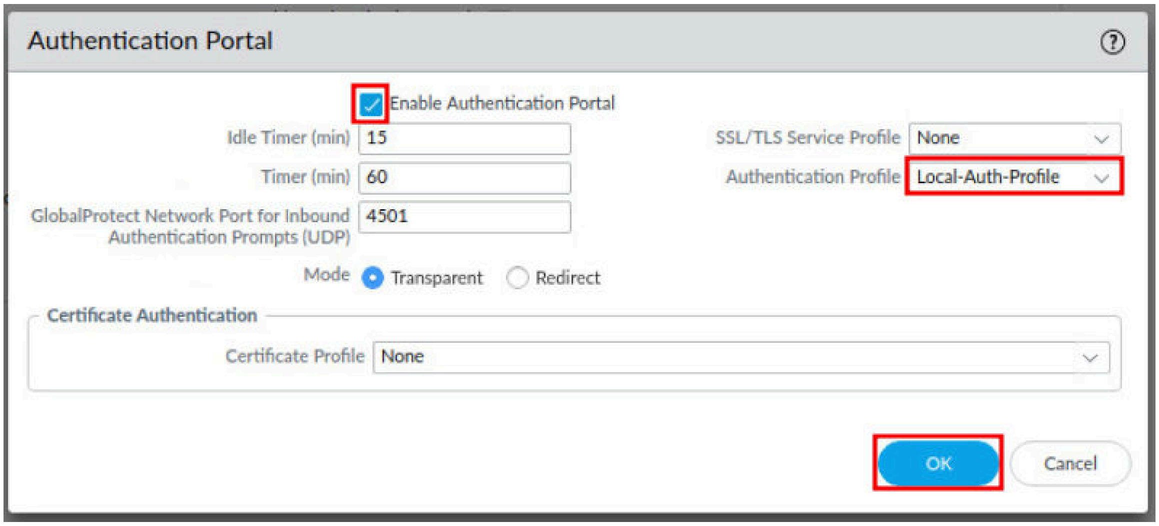
1. Navigate to **Device > User Identification > Authentication Portal Settings**, and click on the **gear** icon.



Enable Authentication Portal	□
Timer (min)	60
Idle Timer (min)	15
SSL/TLS Service Profile	
Authentication Profile	
GlobalProtect Network Port for Inbound Authentication Prompts (UDP)	4501
Certificate Profile	
Mode	transparent

Authentication Portal may also be identified as Captive Portal, which was the name used in versions prior to PAN-OS 10.

2. In the *Authentication Portal* window, click the **Enable Authentication Portal** checkbox. Then, select **Local-Auth-Profile** from the *Authentication Profile* dropdown. Finally, click the **OK** button.



Authentication Portal

☑ Enable Authentication Portal

Idle Timer (min): 15

Timer (min): 60

GlobalProtect Network Port for Inbound Authentication Prompts (UDP): 4501

Mode: ● Transparent ○ Redirect

SSL/TLS Service Profile: None

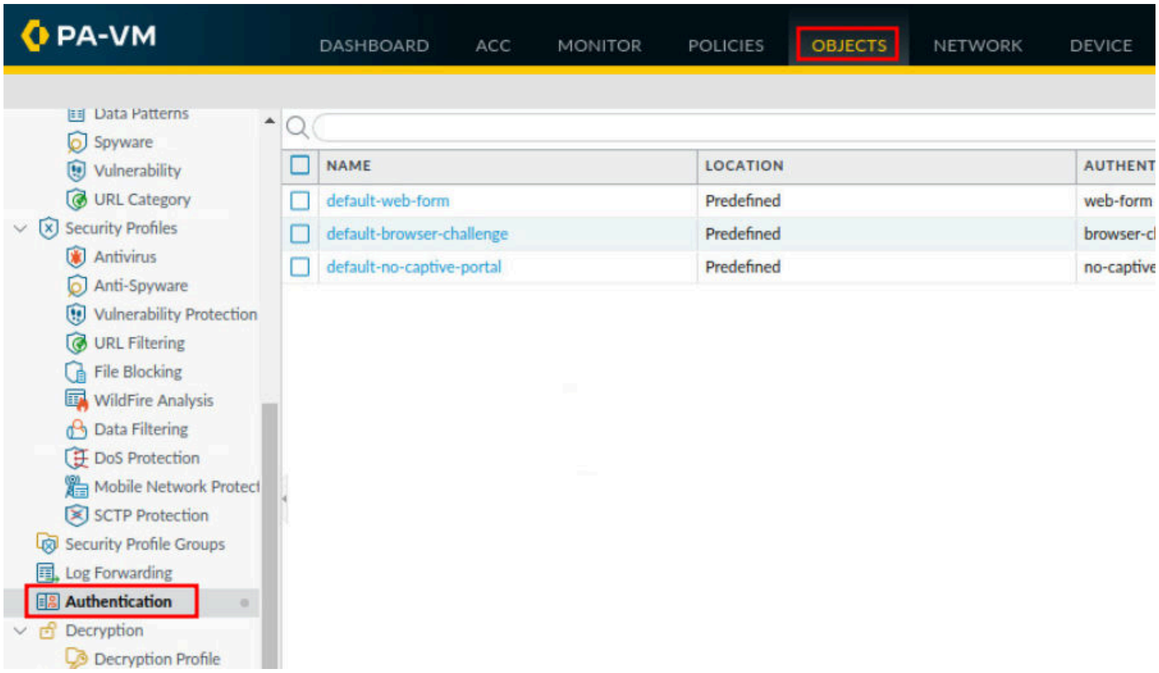
Authentication Profile: Local-Auth-Profile

Certificate Authentication

Certificate Profile: None

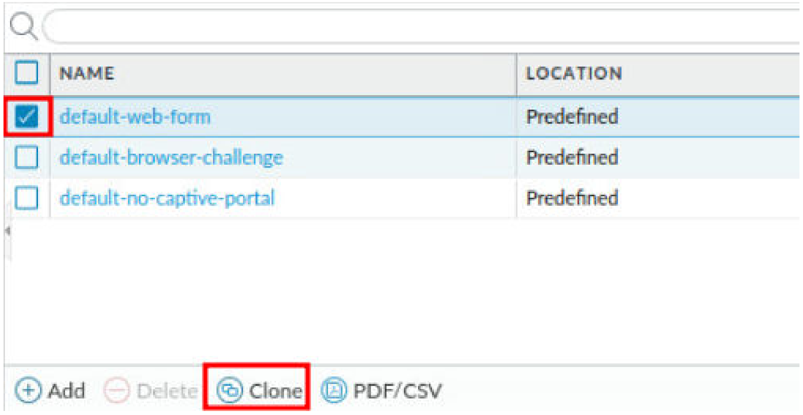
This will turn on the Authentication Portal for web-form logins and associate it with the **Local-Auth-Profile** you created earlier.

3. Navigate to **Objects > Authentication**. You may need to scroll down on the left pane.



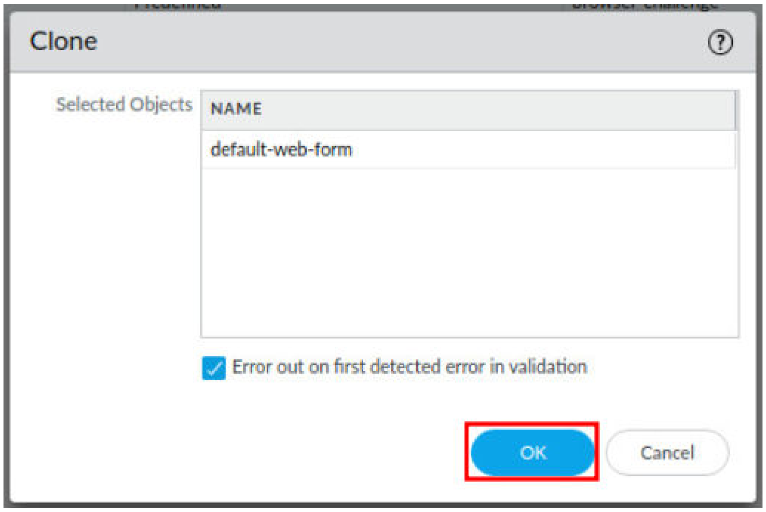
☐	NAME	LOCATION	AUTHENT
☐	default-web-form	Predefined	web-form
☐	default-browser-challenge	Predefined	browser-cl
☐	default-no-captive-portal	Predefined	no-captive

4. Click the checkbox beside the **default-web-form** and click **Clone**.



☐	NAME	LOCATION
☑	default-web-form	Predefined
☐	default-browser-challenge	Predefined
☐	default-no-captive-portal	Predefined

5. In the *Clone* window, click the **OK** button to confirm the clone.

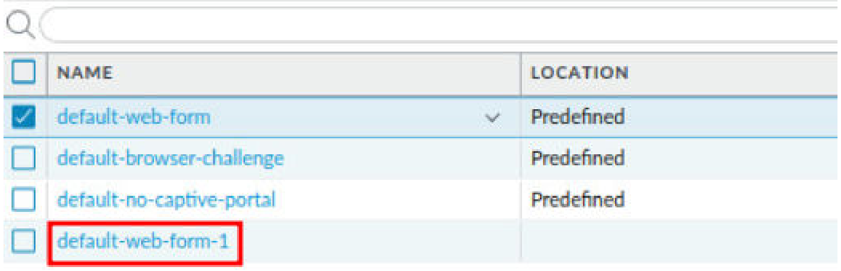


Selected Objects

NAME
default-web-form

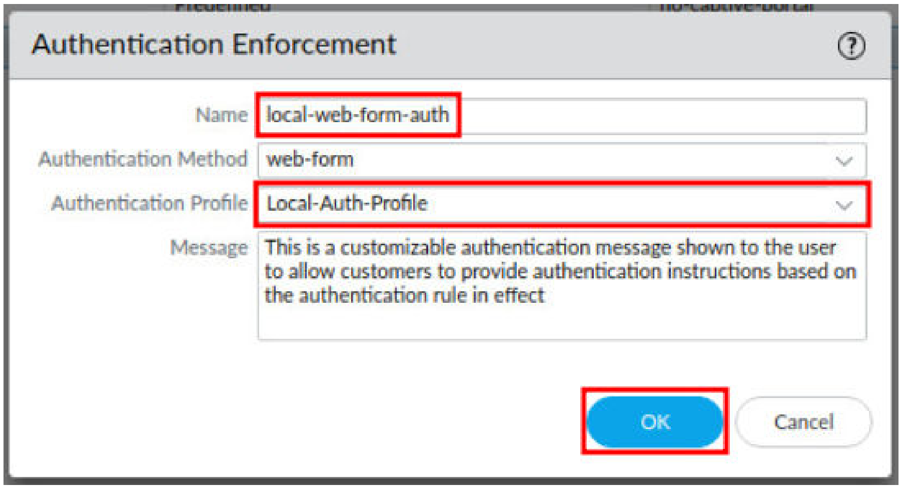
☑ Error out on first detected error in validation

6. You will notice a new entry named default-web-form-1 has been created; click on **default-web-form-1**.



☐	NAME	LOCATION
☑	default-web-form	Predefined
☐	default-browser-challenge	Predefined
☐	default-no-captive-portal	Predefined
☐	default-web-form-1	

7. In the *Authentication Enforcement* window, type `local-web-form-auth` in the *Name* field. Then, select **Local-Auth-Profile** in the *Authentication Profile* dropdown. Next, click the **OK** button.



Authentication Enforcement

Name: local-web-form-auth

Authentication Method: web-form

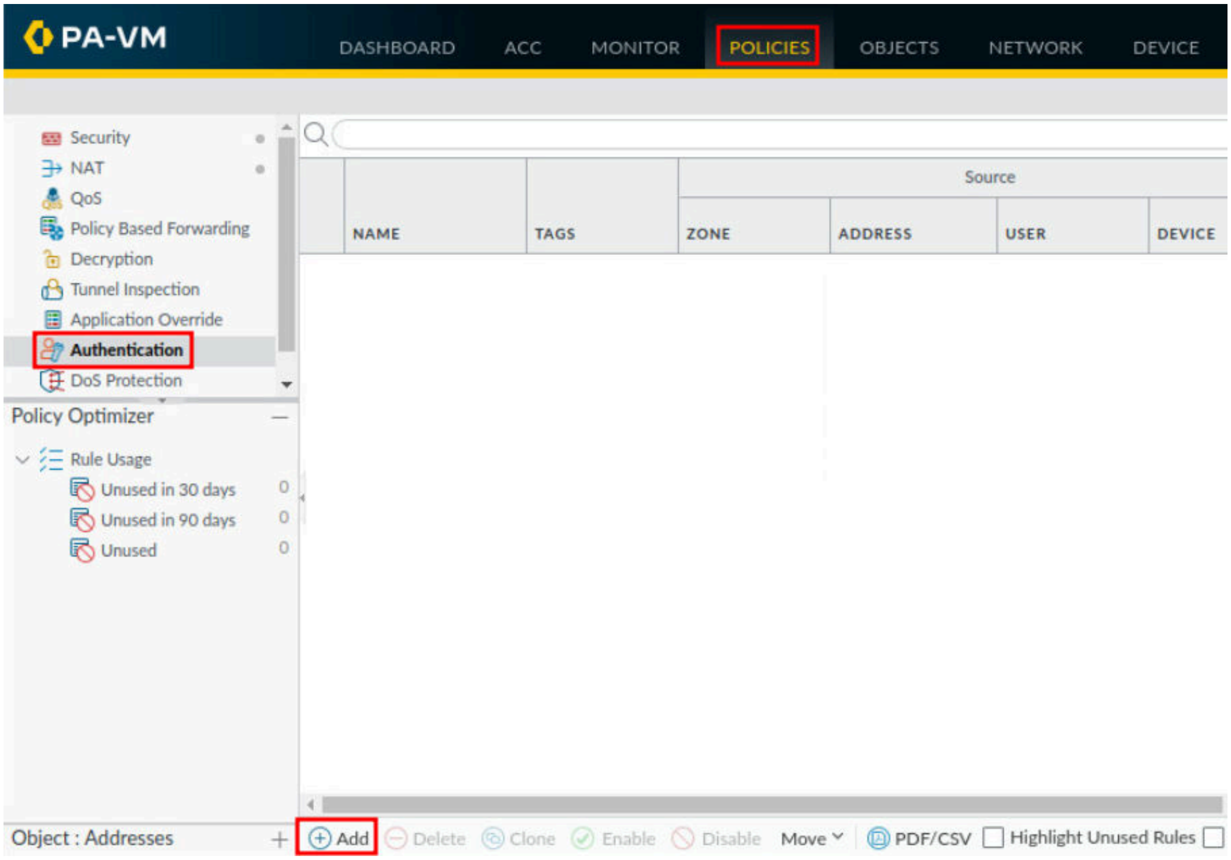
Authentication Profile: Local-Auth-Profile

Message: This is a customizable authentication message shown to the user to allow customers to provide authentication instructions based on the authentication rule in effect

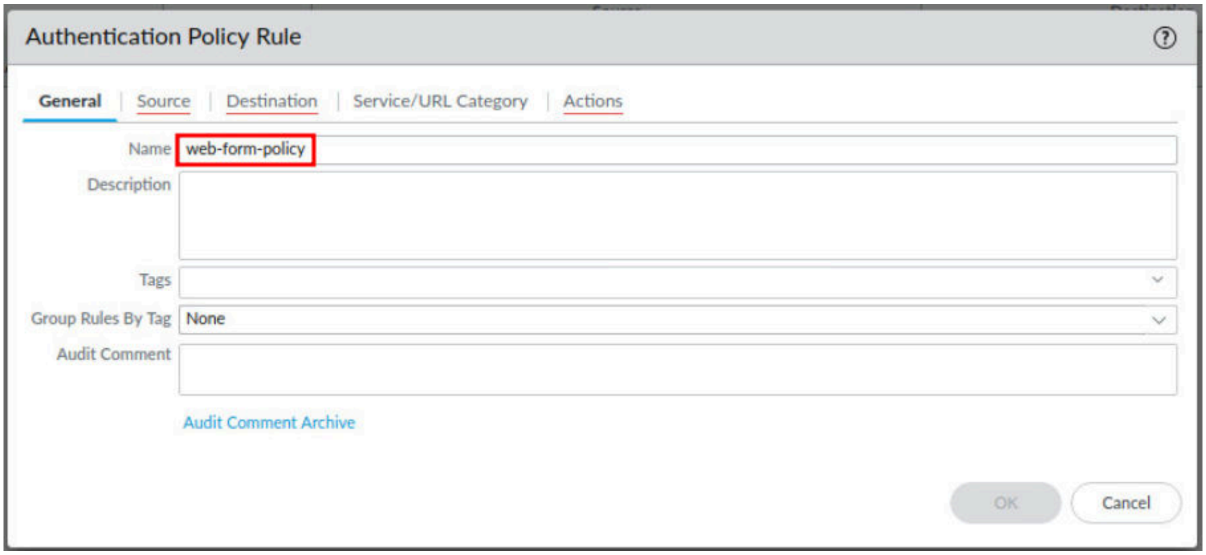
1.3 Create an Authentication Policy

In this section, you will enable a captive portal. A captive portal redirects web requests that match the authentication policy and forces the user to use a login to continue. This is typically seen in corporate guest networks, hotels, and Wi-Fi hotspots. In this captive portal, you will use a web-form for login.

1. Navigate to **Policies > Authentication > Add**.



2. In the *Authentication Policy Rule* window, type `web-form-policy` in the *Name* field.



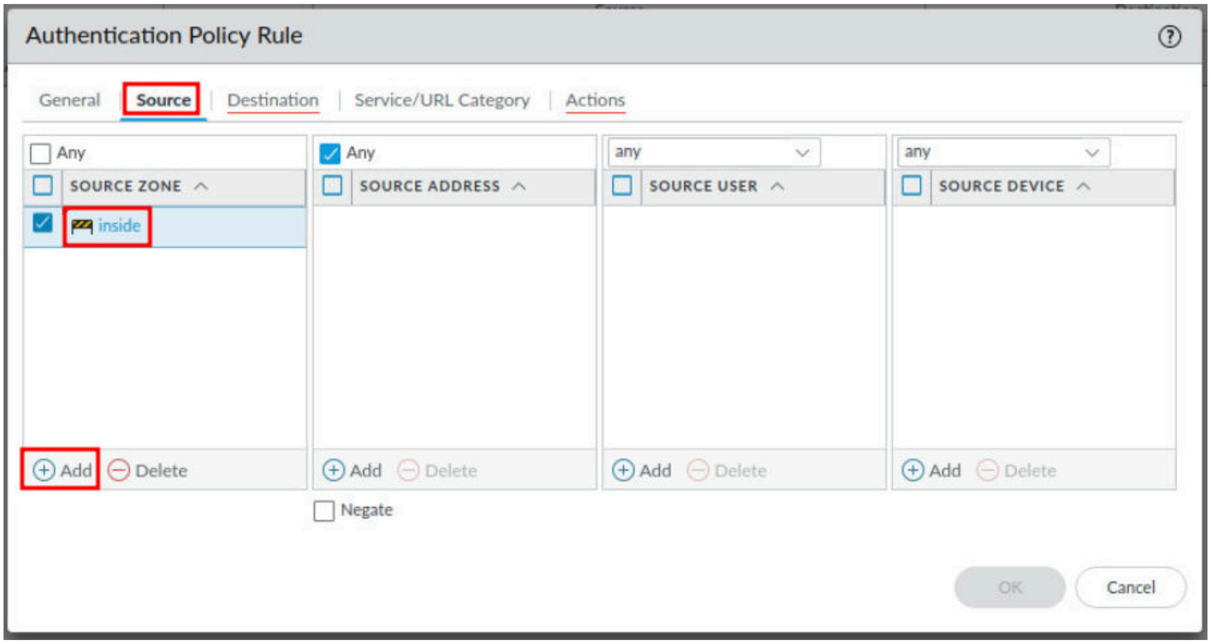
Authentication Policy Rule

General | Source | Destination | Service/URL Category | Actions

Name: web-form-policy
Description:
Tags:
Group Rules By Tag: None
Audit Comment:

Audit Comment Archive
OK
Cancel

3. In the *Authentication Policy Rule* window, click on the **Source** tab. Then, click the **Add** button in the *Source Zone* section. Next, select **inside**.

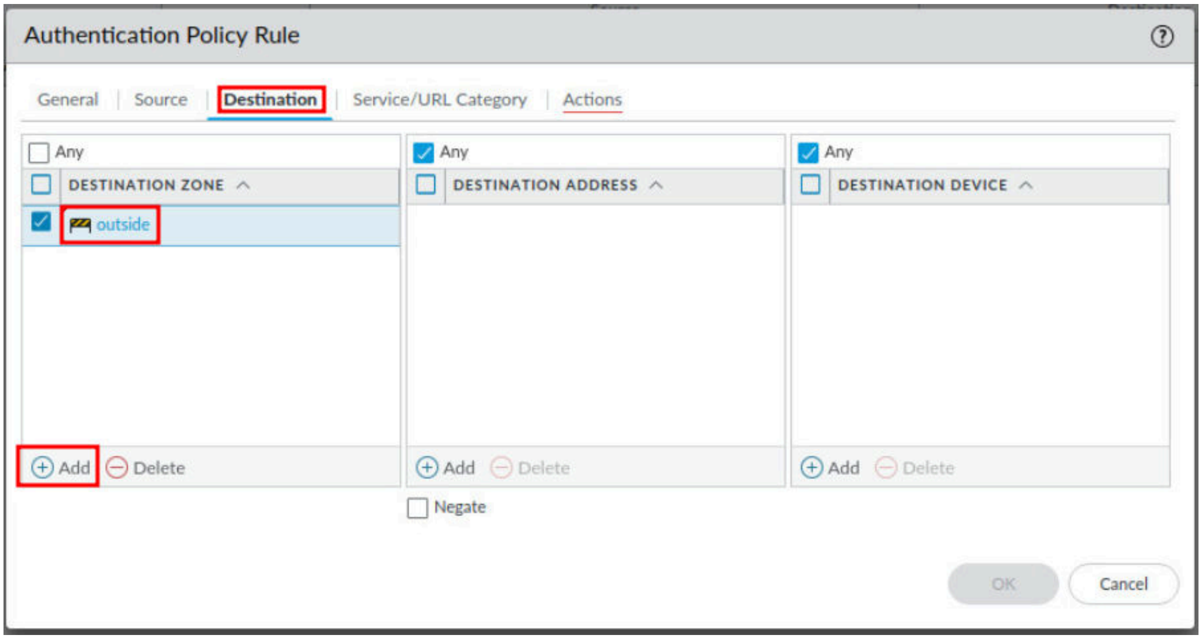


Authentication Policy Rule

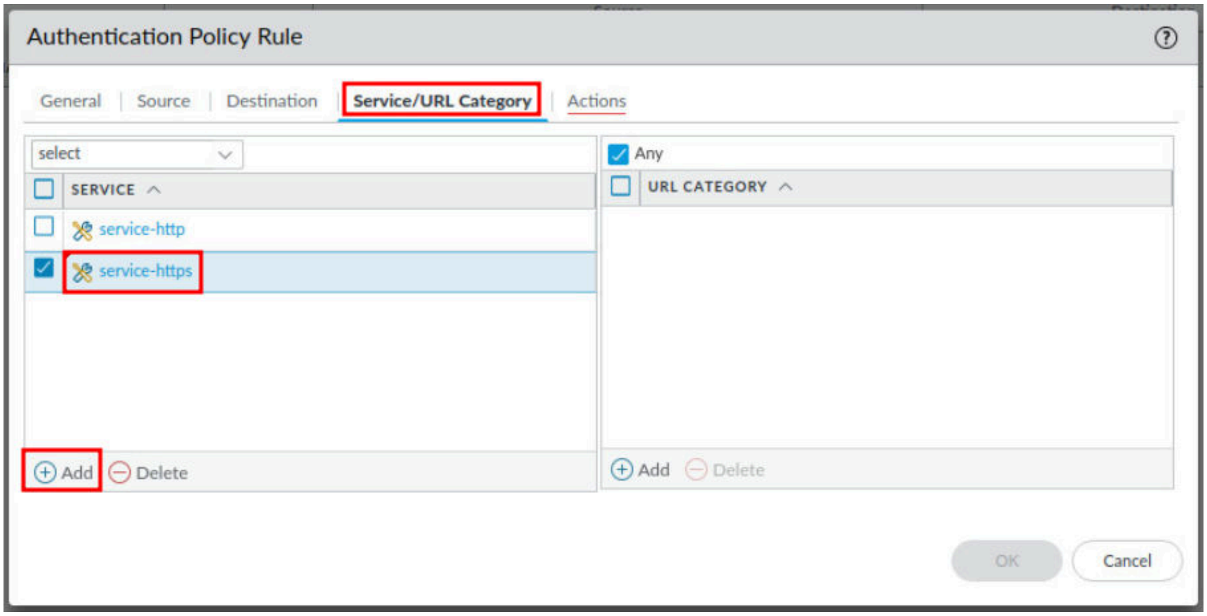
General | Source | Destination | Service/URL Category | Actions

□ Any	☑ Any	any	any
□ SOURCE ZONE	□ SOURCE ADDRESS	□ SOURCE USER	□ SOURCE DEVICE
☑ inside			

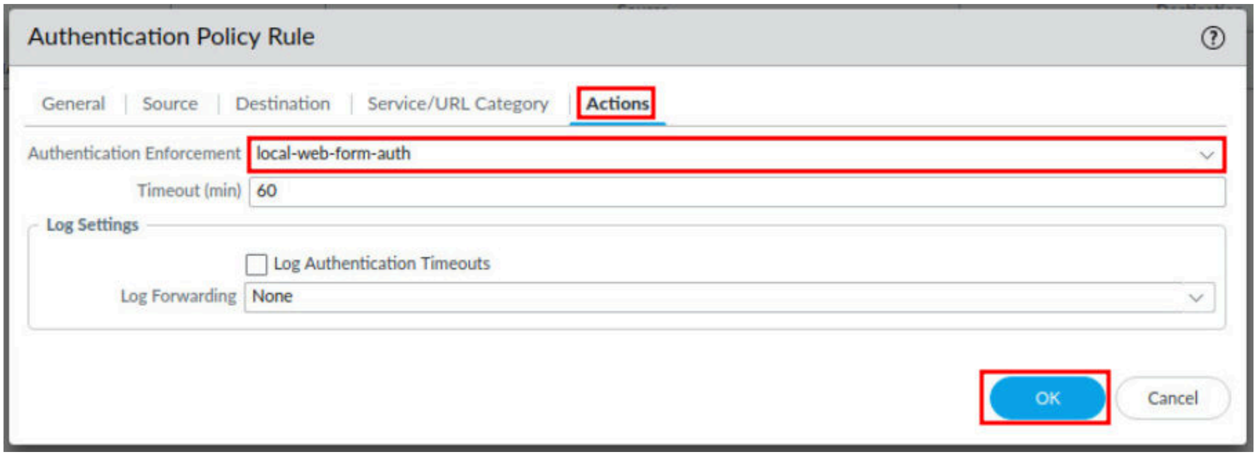
4. In the *Authentication Policy Rule* window, click on the **Destination** tab. Then, click the **Add** button in the *Destination Zone* section. Next, select **outside**.



5. In the *Authentication Policy Rule* window, click on the **Service/URL Category** tab. Then, click on the **Add** button in the *Service* section. Next, select **service-https**.



6. In the *Authentication Policy Rule* window, click on the **Actions** tab. Then, select **local-web-form-auth** from the *Authentication Enforcement* dropdown. Then, click the **OK** button.



Authentication Policy Rule

Authentication Enforcement: local-web-form-auth

Timeout (min): 60

Log Settings

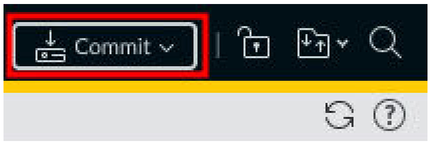
☐ Log Authentication Timeouts

Log Forwarding: None

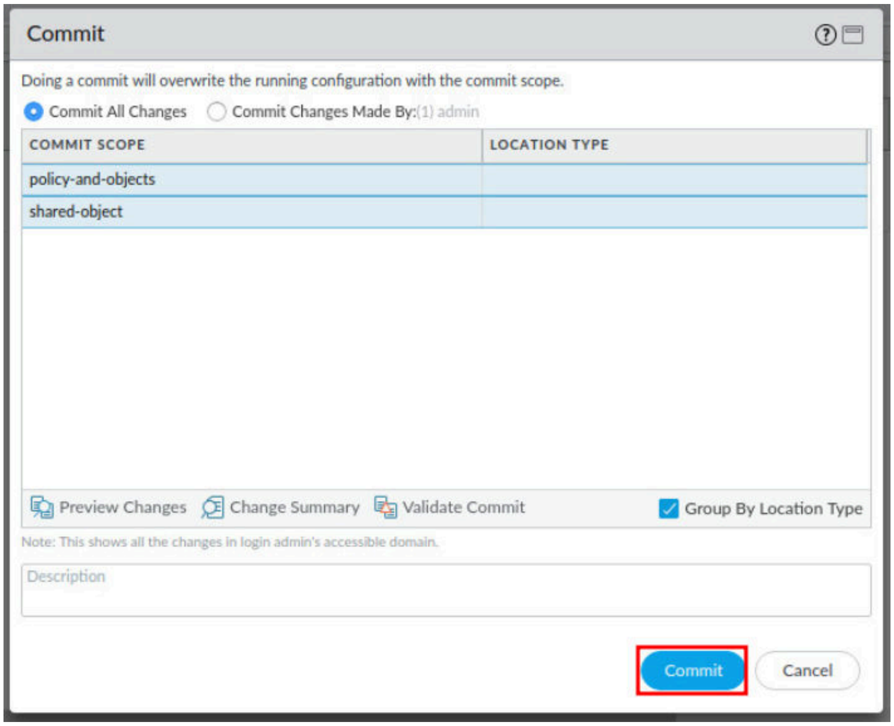
1.4 Commit and Test Authentication Policy

In this section, you will commit your changes and test the authentication policy with the captive portal.

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



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



Commit

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

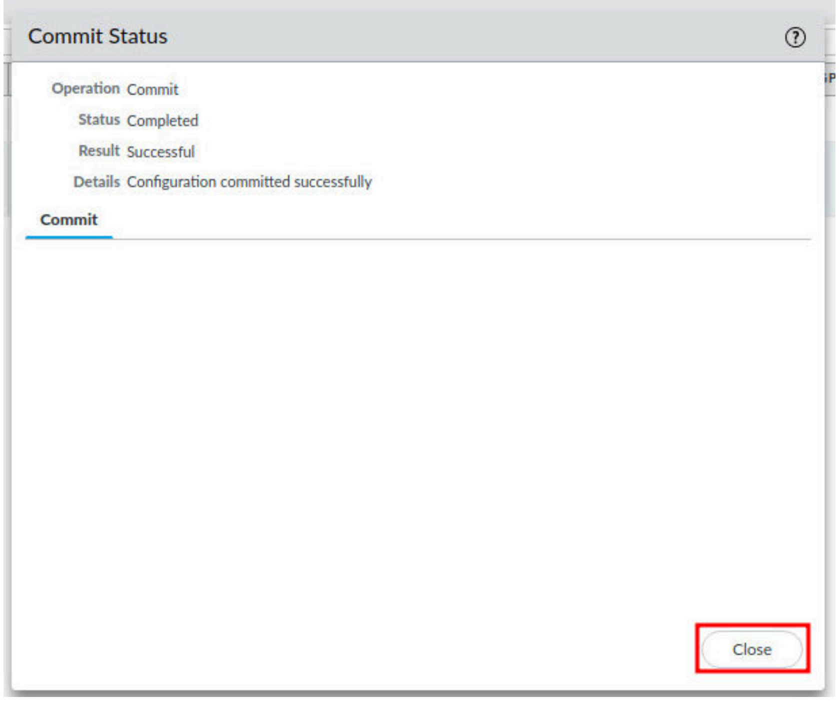
● Commit All Changes ○ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
policy-and-objects	
shared-object	

☑ Group By Location Type

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

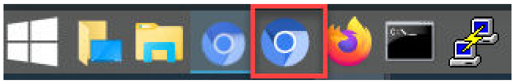
3. When the commit operation successfully completes, click **Close** to continue.



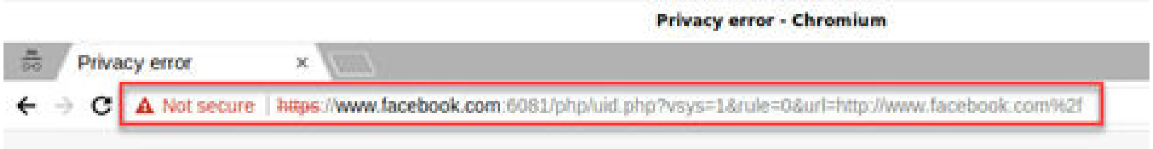
Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

4. Open a second **Chromium Web Browser** from the taskbar.

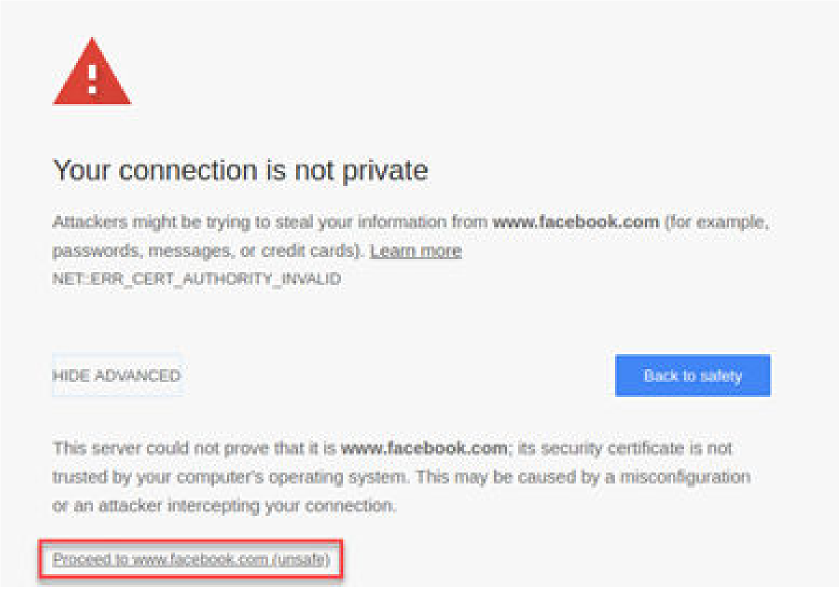


5. In the *Chromium* address field, type `http://www.facebook.com` and press **Enter.**



Not secure | https://www.facebook.com:6081/php/uid.php?vsys=1&rule=0&url=http://www.facebook.com%2f

6. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** Link, and then click **Proceed to www.facebook.com (unsafe).**



Your connection is not private

Attackers might be trying to steal your information from **www.facebook.com** (for example, passwords, messages, or credit cards). Learn more

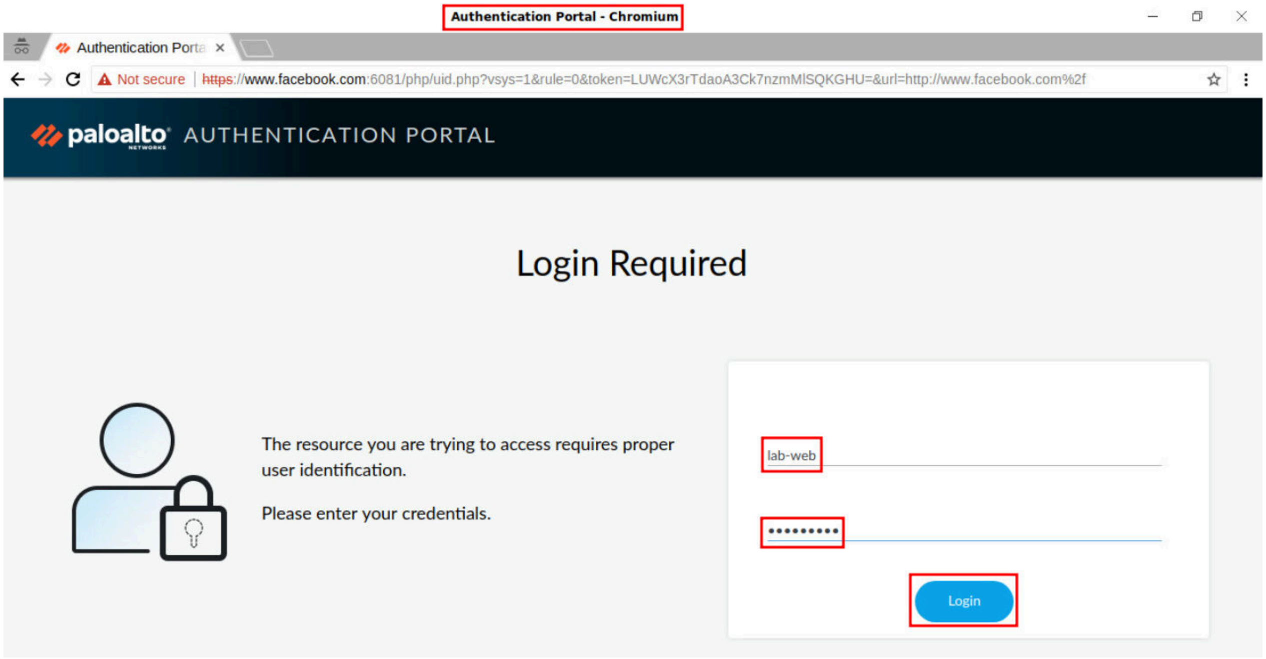
NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **www.facebook.com**; 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.

Proceed to www.facebook.com (unsafe)

You are seeing this error because the Firewall is intercepting traffic coming from the inside zone to the outside zone. The Firewall serves as a man-in-the-middle until authenticated.

7. You will see a web-form login, type `lab-web` as the username. Then, type `Pal0Alt0` as the password. Finally, click the **Login** button.



Authentication Portal - Chromium

https://www.facebook.com:6081/php/uid.php?vsys=1&rule=0&token=LUWcX3rTdaoA3Ck7nzmMlSQKGHU=&url=http://www.facebook.com%2f

paloalto AUTHENTICATION PORTAL

Login Required

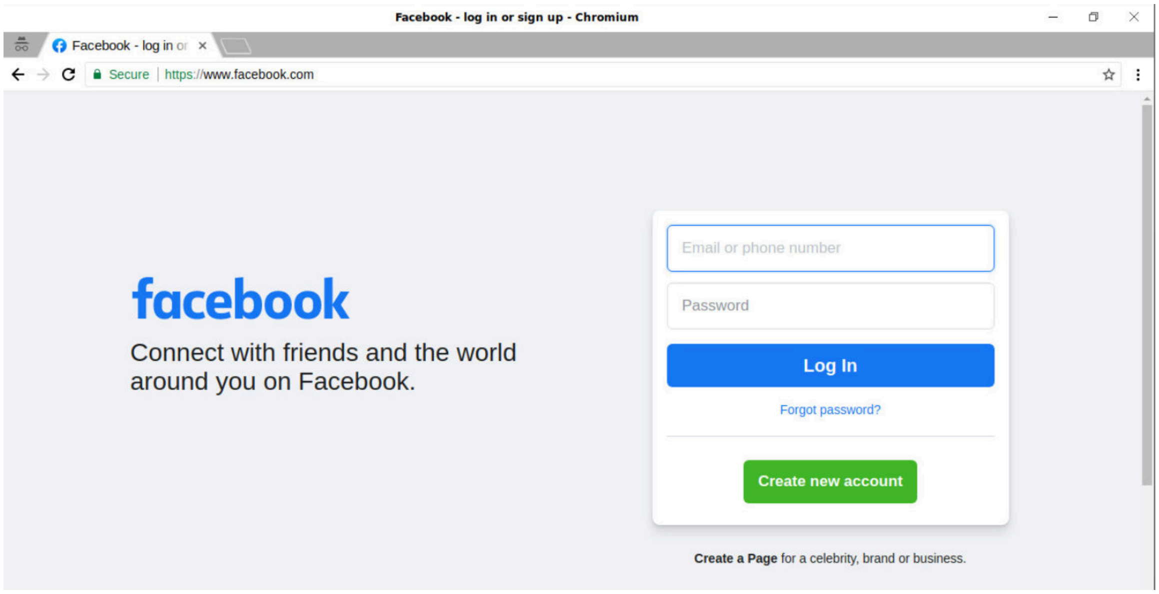
The resource you are trying to access requires proper user identification.

Please enter your credentials.

lab-web

•••••••••

8. You will then see Facebook after you successfully authenticate to the Firewall as **lab-web**.



Facebook - log in or sign up - Chromium

Secure | https://www.facebook.com

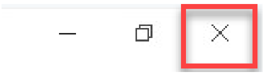
facebook

Connect with friends and the world around you on Facebook.

Create a Page for a celebrity, brand or business.

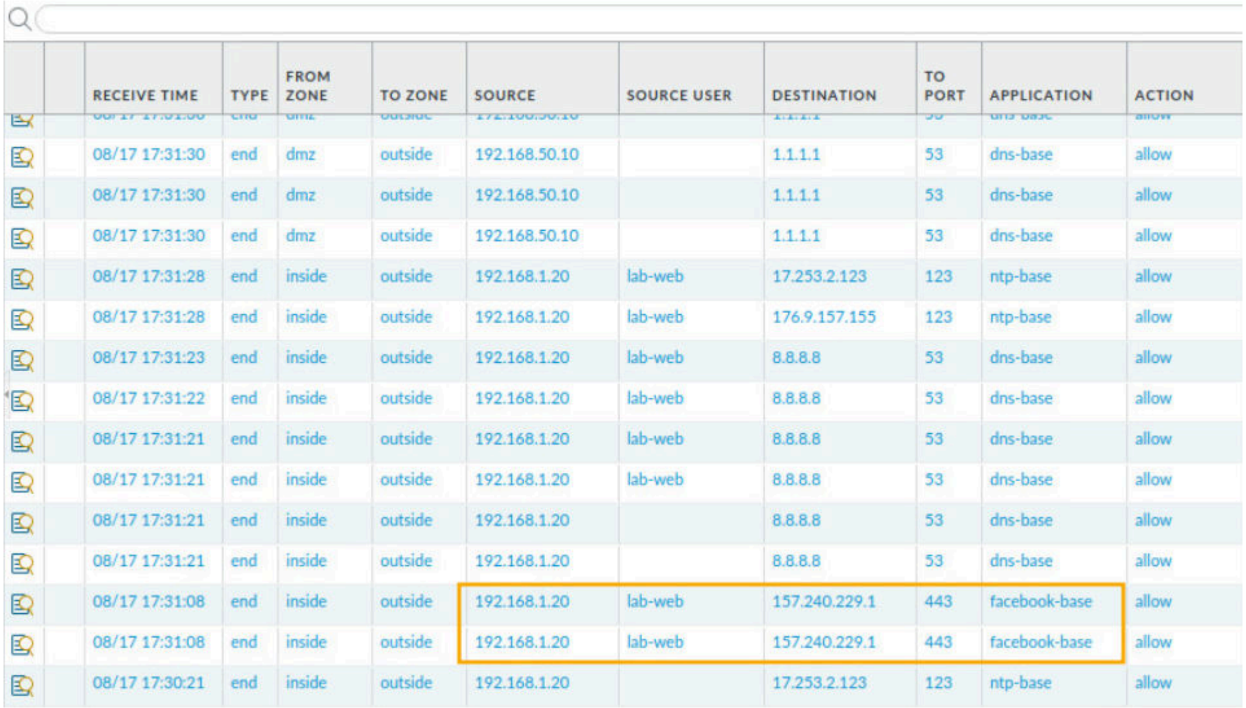
If the tab does not immediately load the Facebook page, wait and try again, or open a new tab in Chromium and enter `http://www.facebook.com` in the address bar, then press **Enter**.

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



10. Navigate to **Monitor > Logs > Traffic**.

11. In the logs, you will see that the entries to **facebook-base** are associated with the **lab-web** user. You may need to manually refresh logs or check additional pages at the bottom.



		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION
		08/17 17:31:30	end	dmz	outside	192.168.50.10		1.1.1.1	53	dns-base	allow
		08/17 17:31:30	end	dmz	outside	192.168.50.10		1.1.1.1	53	dns-base	allow
		08/17 17:31:30	end	dmz	outside	192.168.50.10		1.1.1.1	53	dns-base	allow
		08/17 17:31:28	end	inside	outside	192.168.1.20	lab-web	17.253.2.123	123	ntp-base	allow
		08/17 17:31:28	end	inside	outside	192.168.1.20	lab-web	176.9.157.155	123	ntp-base	allow
		08/17 17:31:23	end	inside	outside	192.168.1.20	lab-web	8.8.8.8	53	dns-base	allow
		08/17 17:31:22	end	inside	outside	192.168.1.20	lab-web	8.8.8.8	53	dns-base	allow
		08/17 17:31:21	end	inside	outside	192.168.1.20	lab-web	8.8.8.8	53	dns-base	allow
		08/17 17:31:21	end	inside	outside	192.168.1.20	lab-web	8.8.8.8	53	dns-base	allow
		08/17 17:31:21	end	inside	outside	192.168.1.20		8.8.8.8	53	dns-base	allow
		08/17 17:31:21	end	inside	outside	192.168.1.20		8.8.8.8	53	dns-base	allow
		08/17 17:31:08	end	inside	outside	192.168.1.20	lab-web	157.240.229.1	443	facebook-base	allow
		08/17 17:31:08	end	inside	outside	192.168.1.20	lab-web	157.240.229.1	443	facebook-base	allow
		08/17 17:30:21	end	inside	outside	192.168.1.20		17.253.2.123	123	ntp-base	allow

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