



CYBERSECURITY FOUNDATION V2

Lab 4: Configuring Authentication

Document Version: **2022-12-22**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Configuring Authentication.....	6
1.0 Load Lab Configuration	6
1.1 Configure a Local User Account and Authentication Profile	11
1.2 Enable the Authentication Portal and Enable Web-Form based Logins	15
1.3 Create an Authentication Policy.....	19
1.4 Commit and Test Authentication Policy.....	22

Introduction

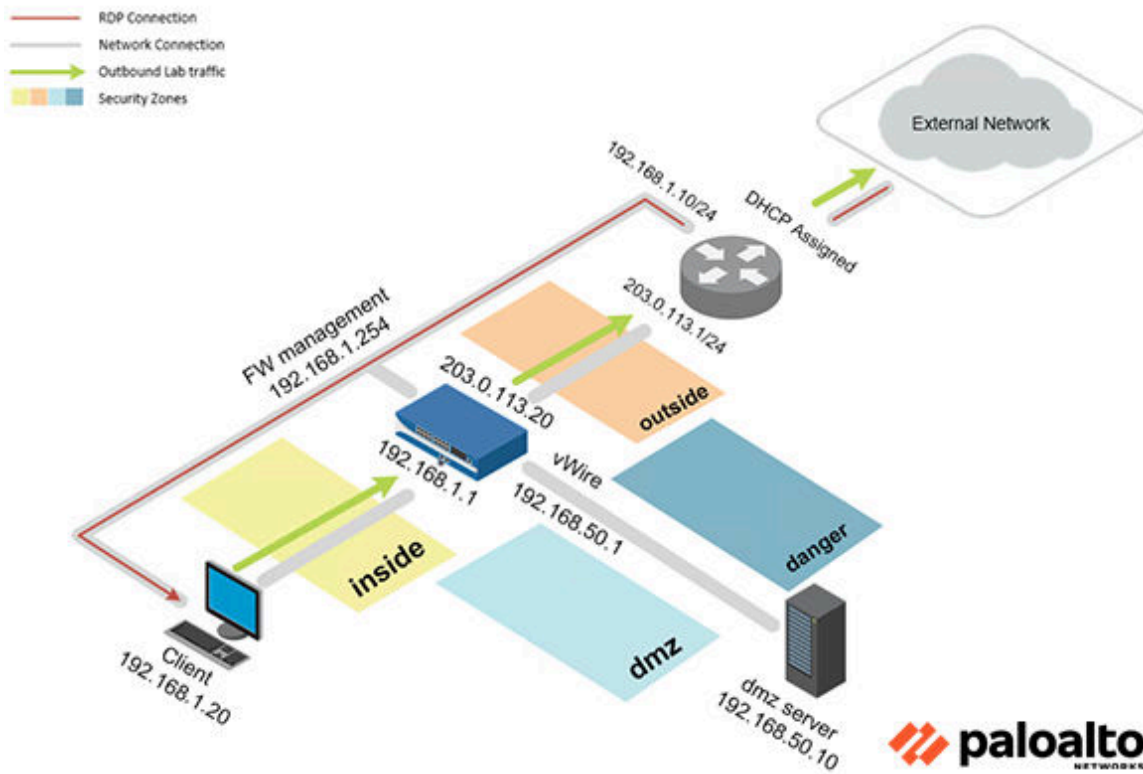
In this lab, you will configure the Firewall to use a Captive Portal to authenticate users by using a local user account and Authentication Policy.

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.

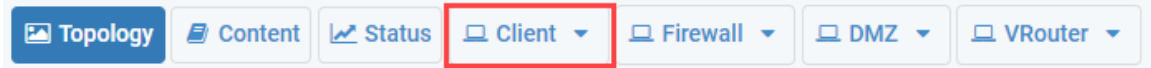
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Configuring Authentication

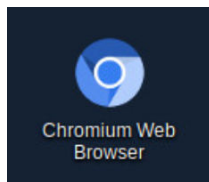
1.0 Load Lab Configuration

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

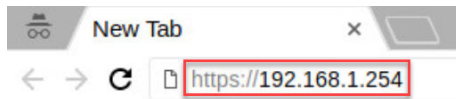
1. Click on the **Client** tab to access the Client PC.



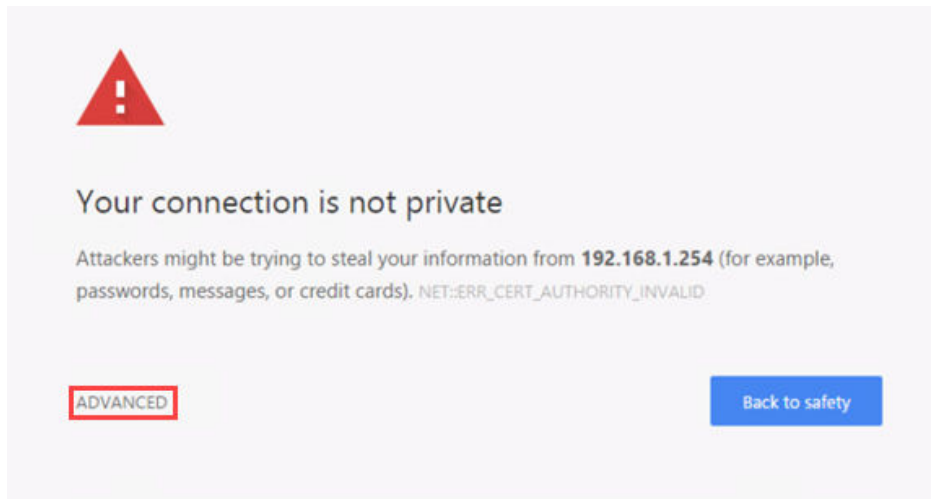
2. Log in to the Client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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

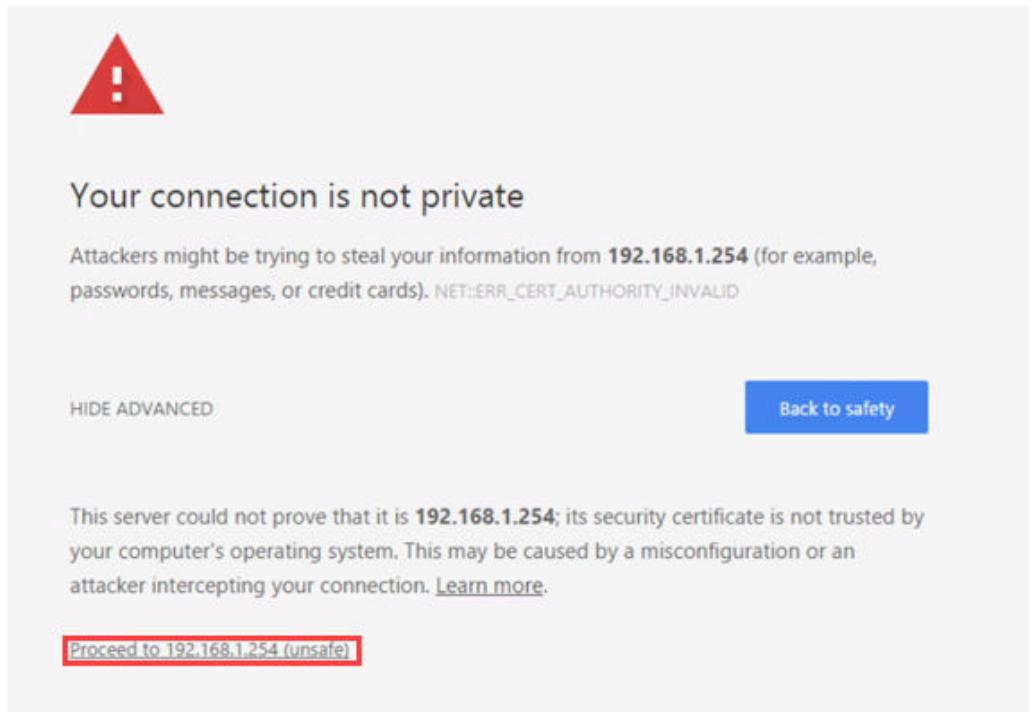


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

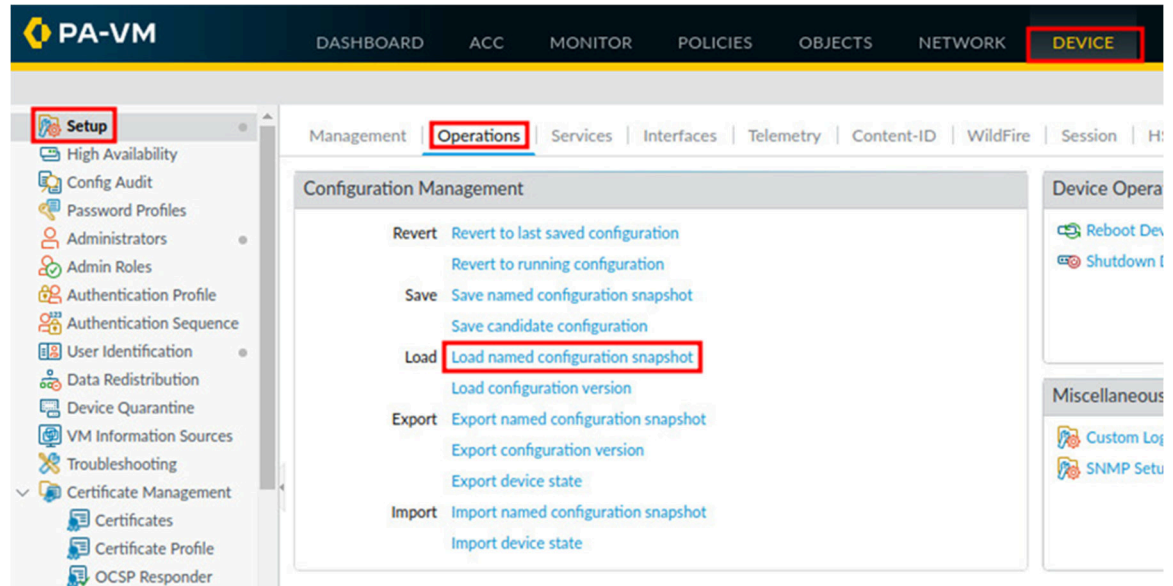
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



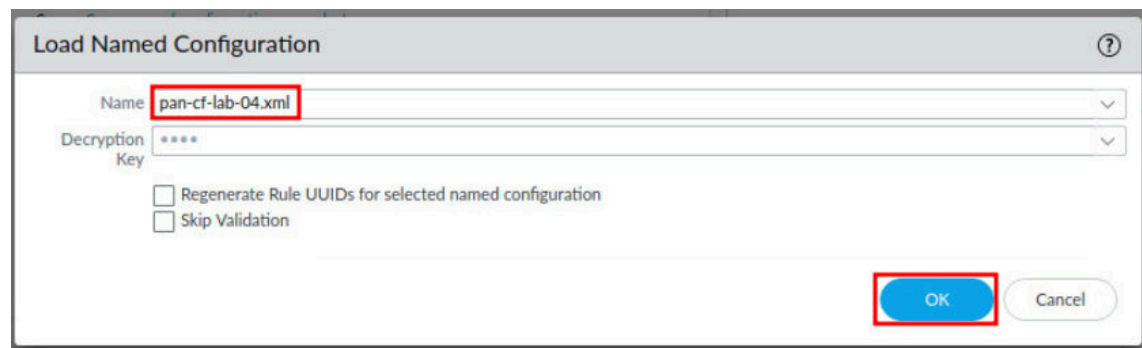
7. Log in to the Firewall web interface as username admin, password Pal0Alt0!.



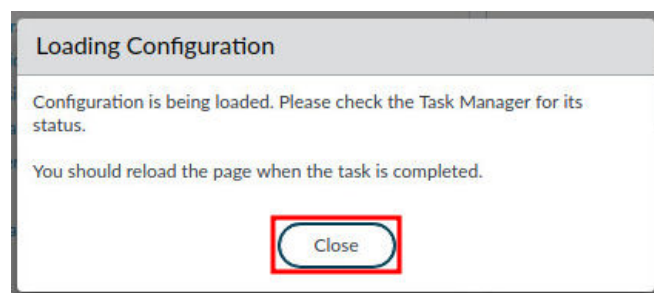
- In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named configuration snapshot underneath the *Configuration Management* section.



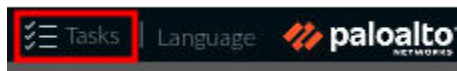
- In the *Load Named Configuration* window, select **pan-cf-lab-04.xml** from the *Name* dropdown box and click **OK**.



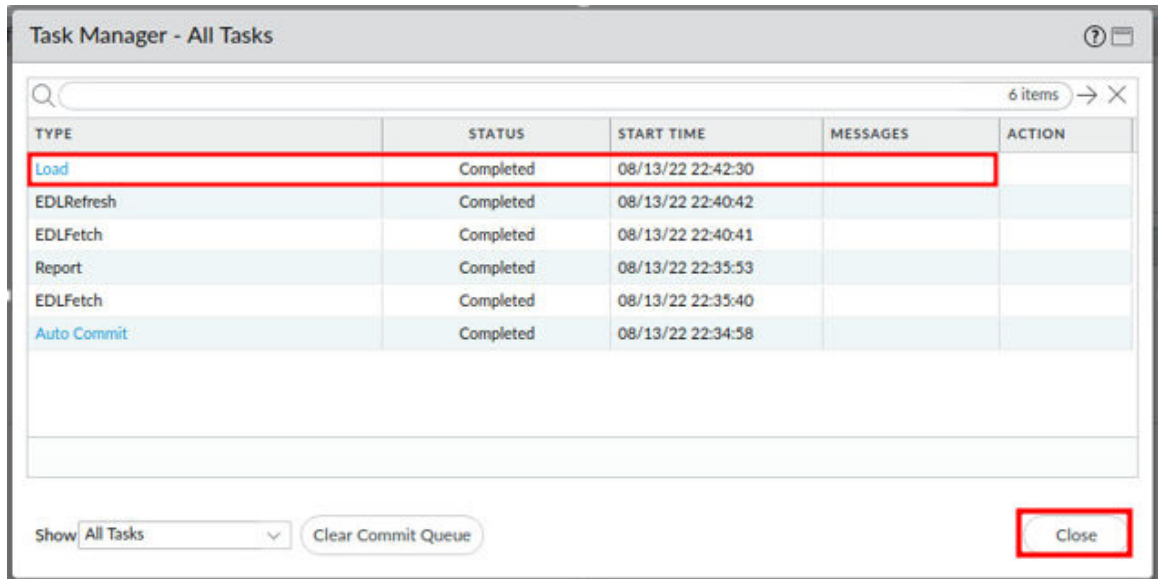
- In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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



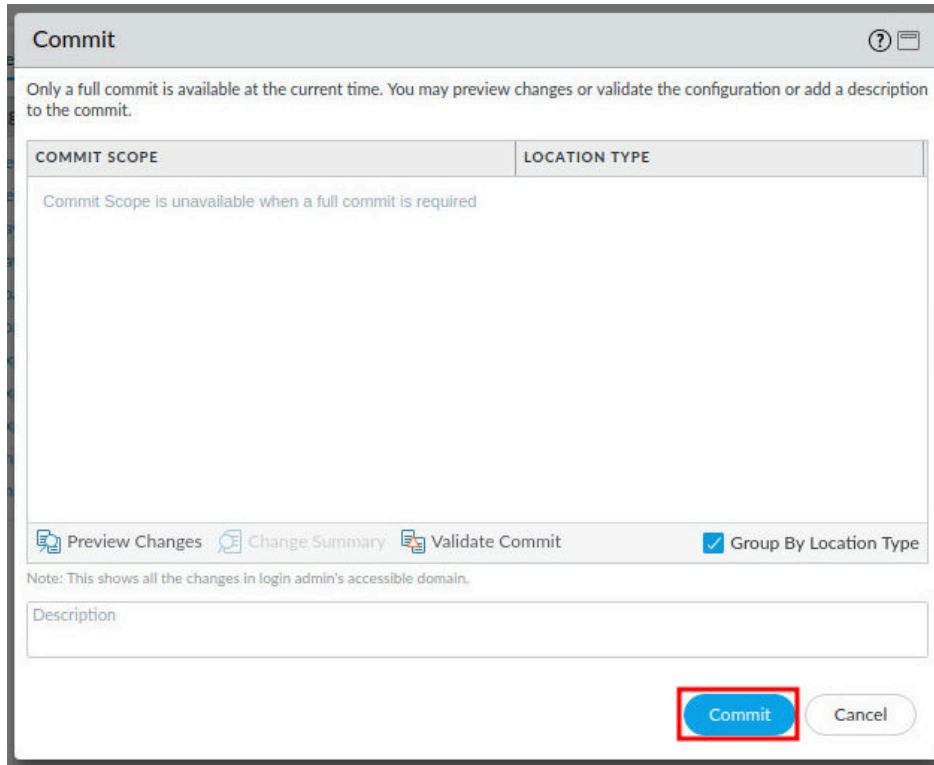
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



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

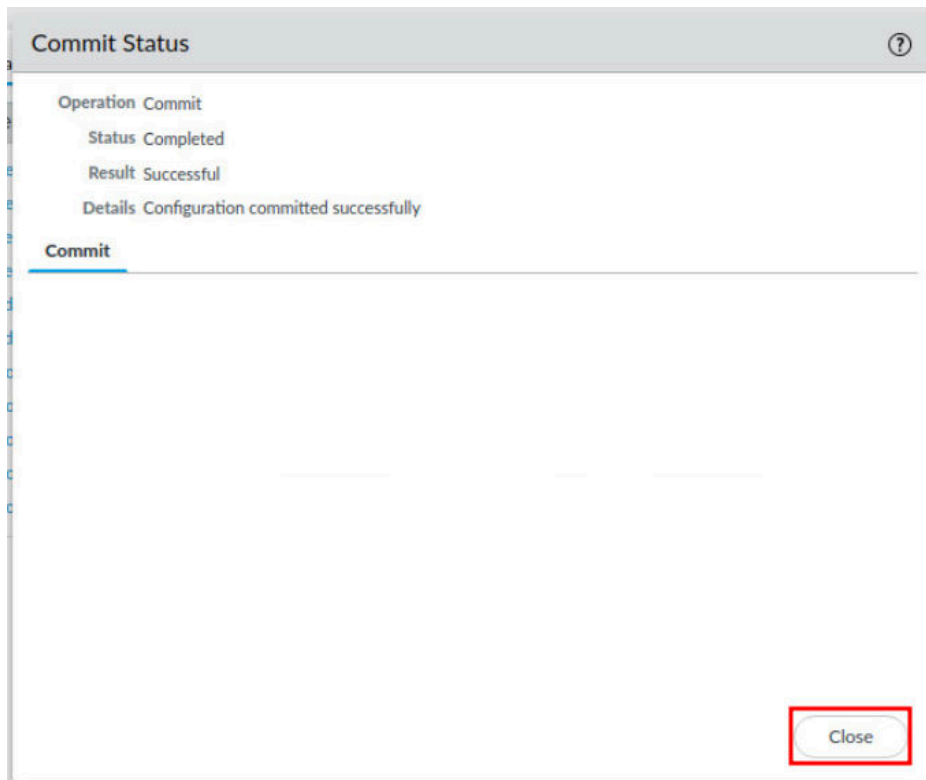


14. In the *Commit* window, click **Commit** to proceed with committing the changes.



The screenshot shows the 'Commit' window. At the top, it says '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.' Below this is a table with two columns: 'COMMIT SCOPE' and 'LOCATION TYPE'. The 'COMMIT SCOPE' column contains the text 'Commit Scope is unavailable when a full commit is required'. Below the table are three buttons: 'Preview Changes', 'Change Summary', and 'Validate Commit'. To the right of these buttons is a checkbox labeled 'Group By Location Type' which is checked. Below the buttons is a text area labeled 'Description'. At the bottom right, there are two buttons: 'Commit' (highlighted with a red box) and 'Cancel'.

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



The screenshot shows the 'Commit Status' window. It displays the following information: 'Operation Commit', 'Status Completed', 'Result Successful', and 'Details Configuration committed successfully'. Below this information is a tab labeled 'Commit'. At the bottom right, there is a button labeled 'Close' (highlighted with a red box).

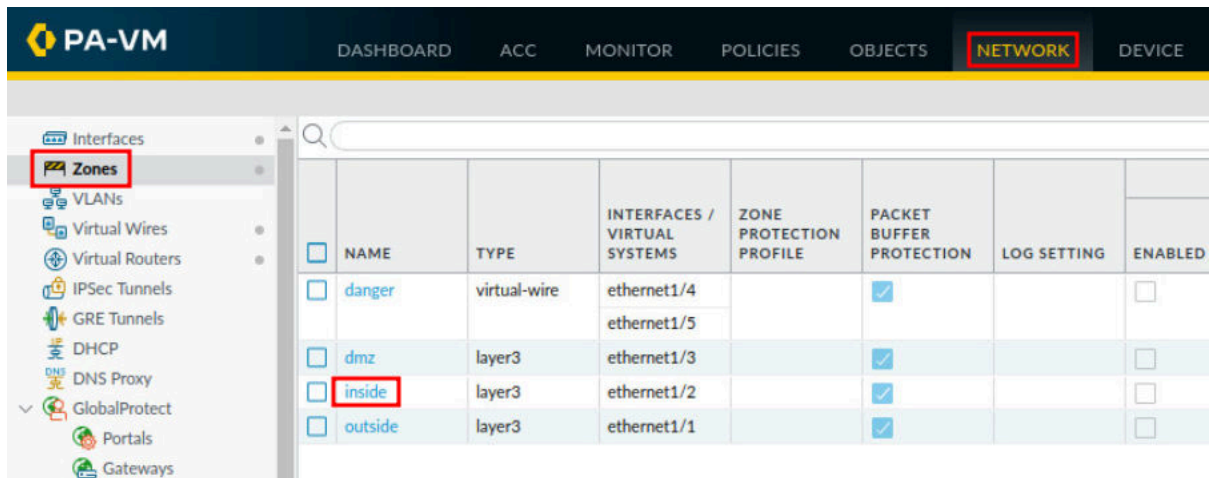


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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.

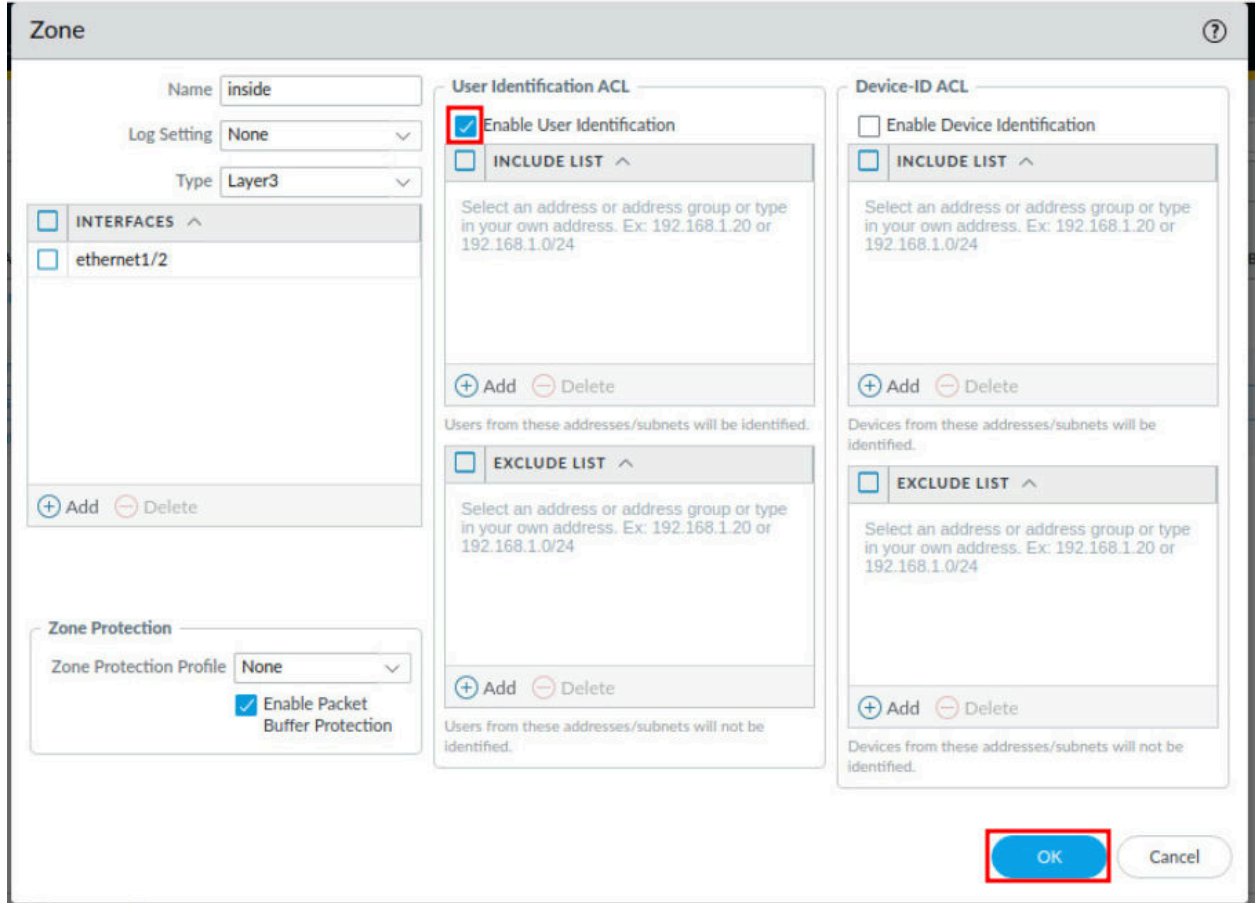
1. Navigate to **Network > Zones**, and click on the **inside** zone.



The screenshot shows the PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK' (highlighted with a red box), and 'DEVICE'. The left sidebar shows a tree view of configuration options, with 'Zones' highlighted under the 'Interfaces' section. The main content area displays a table of configured zones.

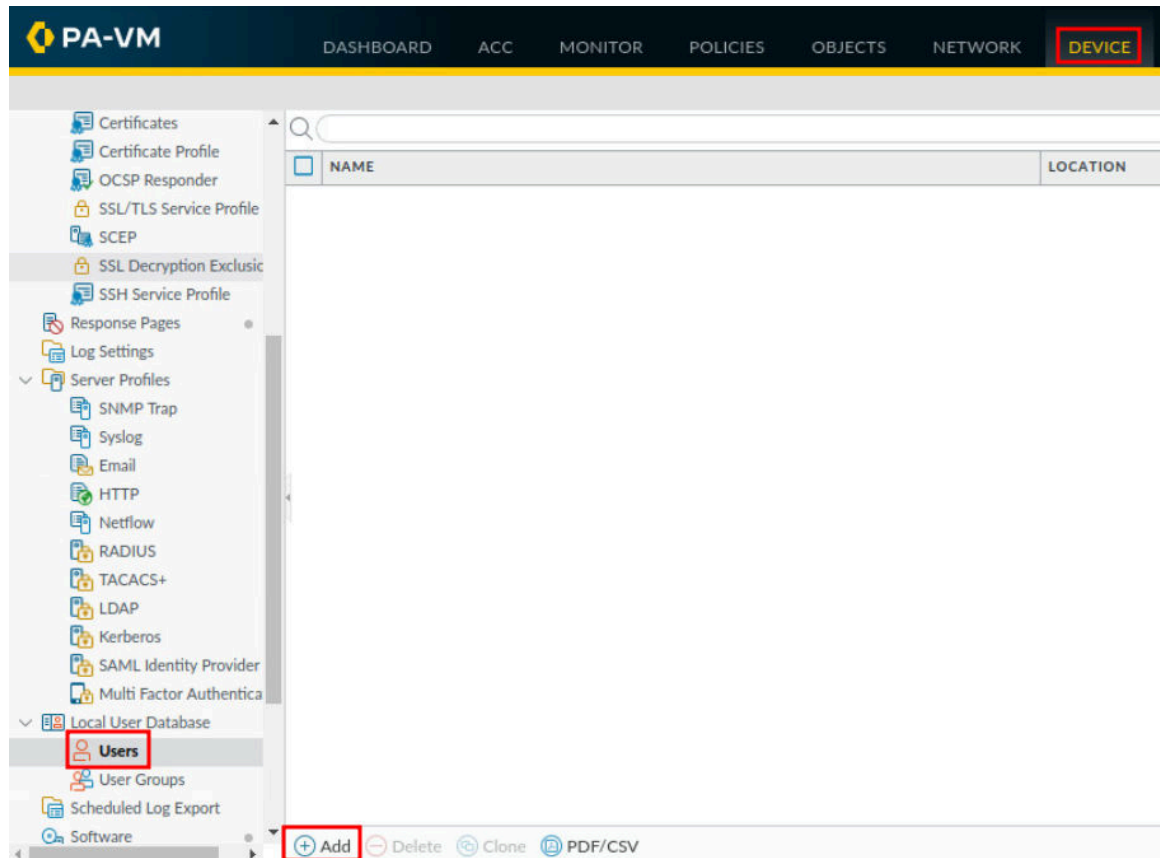
	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED
<input type="checkbox"/>	danger	virtual-wire	ethernet1/4 ethernet1/5		<input checked="" type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	dmz	layer3	ethernet1/3		<input checked="" type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	inside	layer3	ethernet1/2		<input checked="" type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	outside	layer3	ethernet1/1		<input checked="" type="checkbox"/>		<input type="checkbox"/>

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

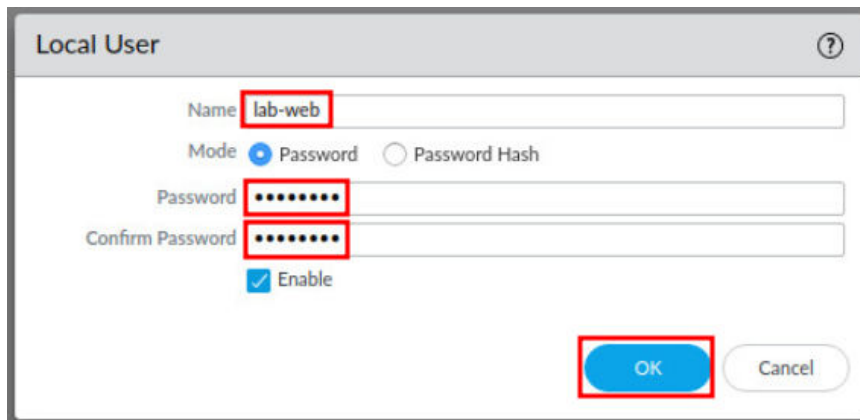


This will enable the inside zone to use a Username for authentication.

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

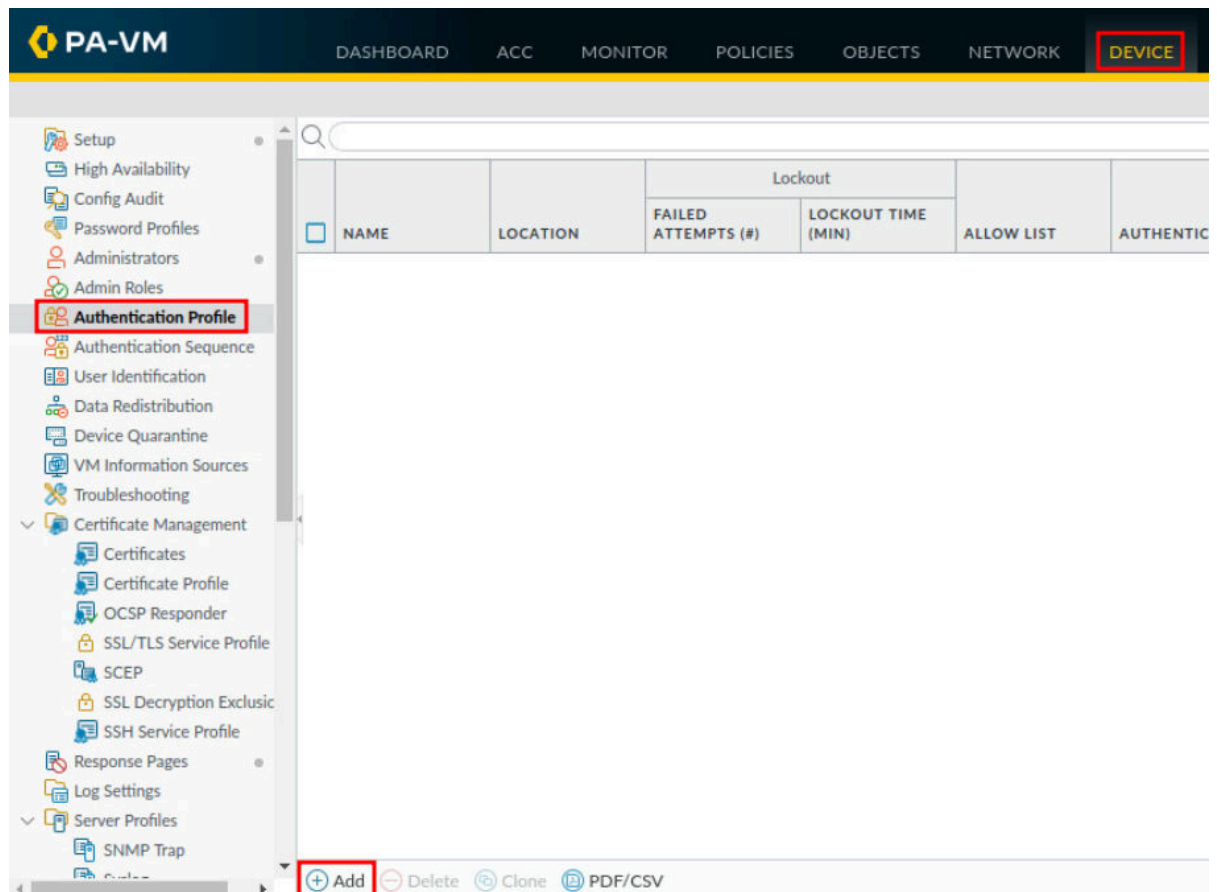


4. In the *Local User* window, type `lab-web` in the *Name* field. Then, type `Pa10A1t0` in the *Password* and *Confirm Password* fields. Finally, click the **OK** button.

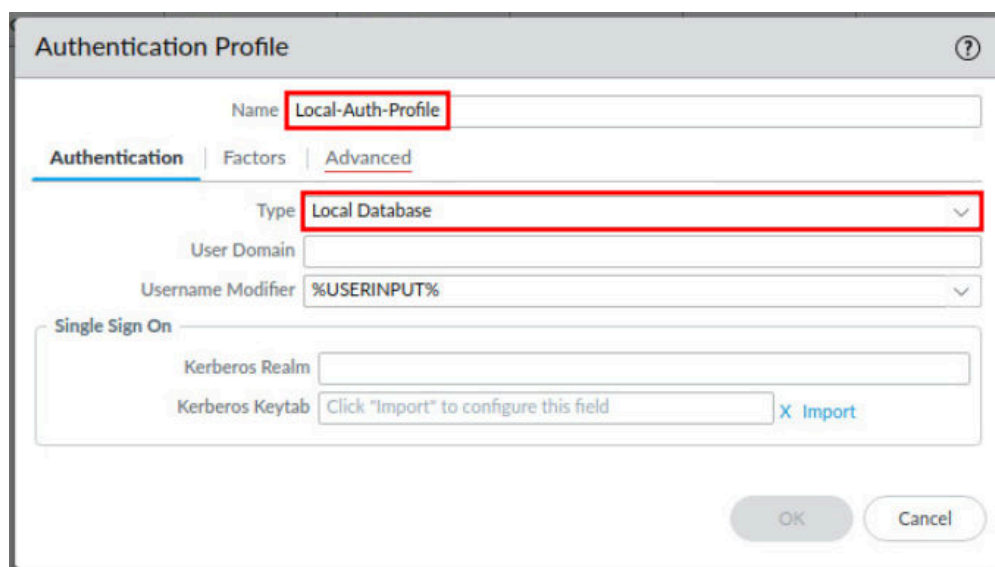


The screenshot shows the 'Local User' configuration window. The 'Name' field contains 'lab-web' (highlighted with a red box). The 'Mode' is set to 'Password' (selected with a radio button). The 'Password' and 'Confirm Password' fields both contain masked text (highlighted with red boxes). The 'Enable' checkbox is checked. The 'OK' button is highlighted with a red box, and the 'Cancel' button is also visible.

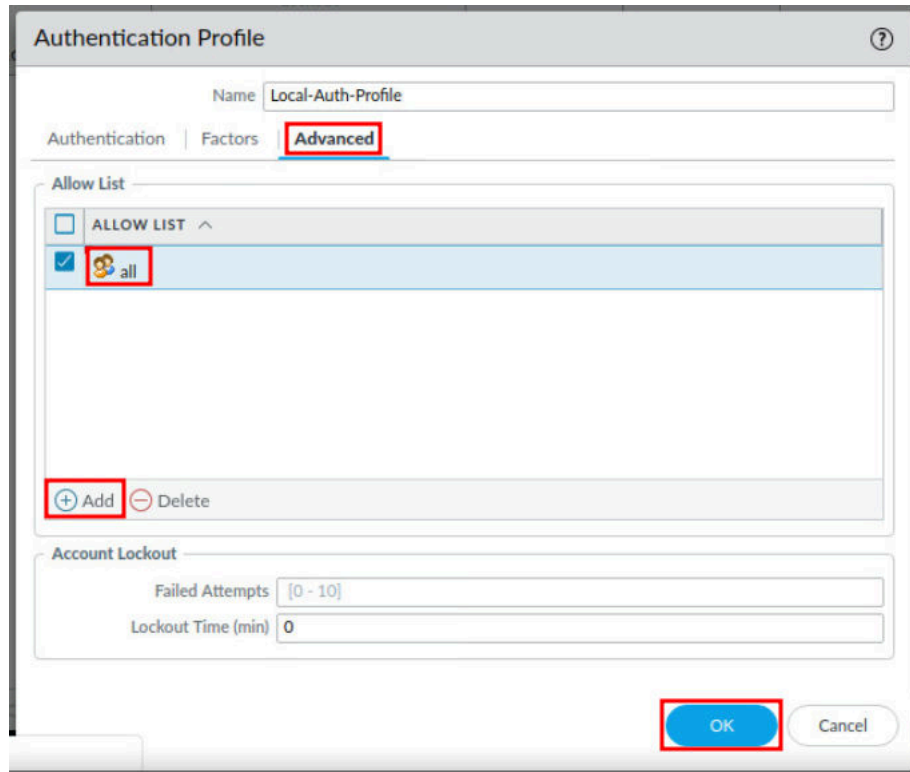
5. Navigate to **Device > Authentication Profile > Add**. You may need to scroll up on the left pane.



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



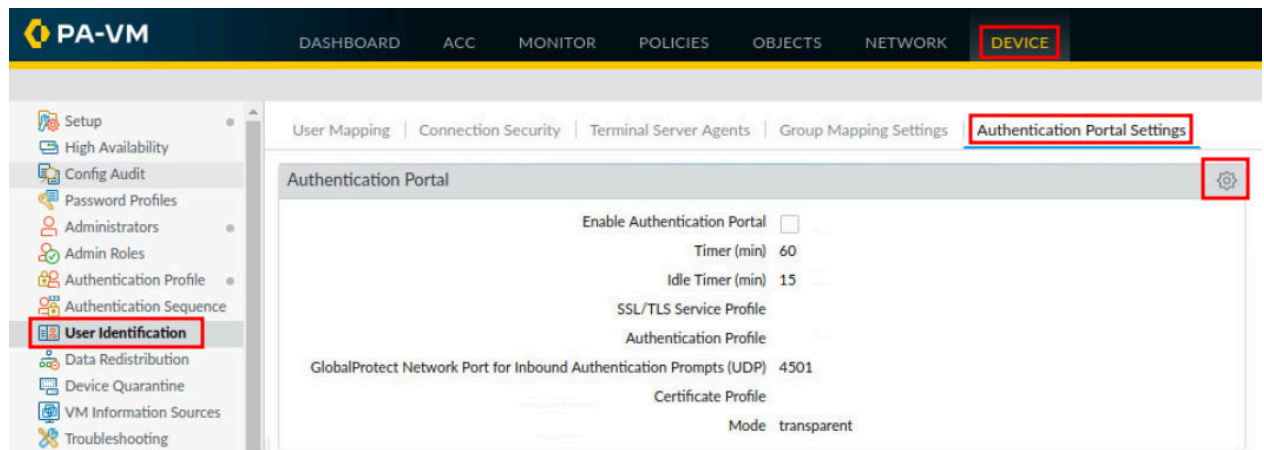
7. In the *Authentication Profile* window, click on the **Advanced** tab. Then, click on the **Add** button. Next, select **all** from the dropdown in the *Allow List* column. Finally, click the **OK** button.



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.

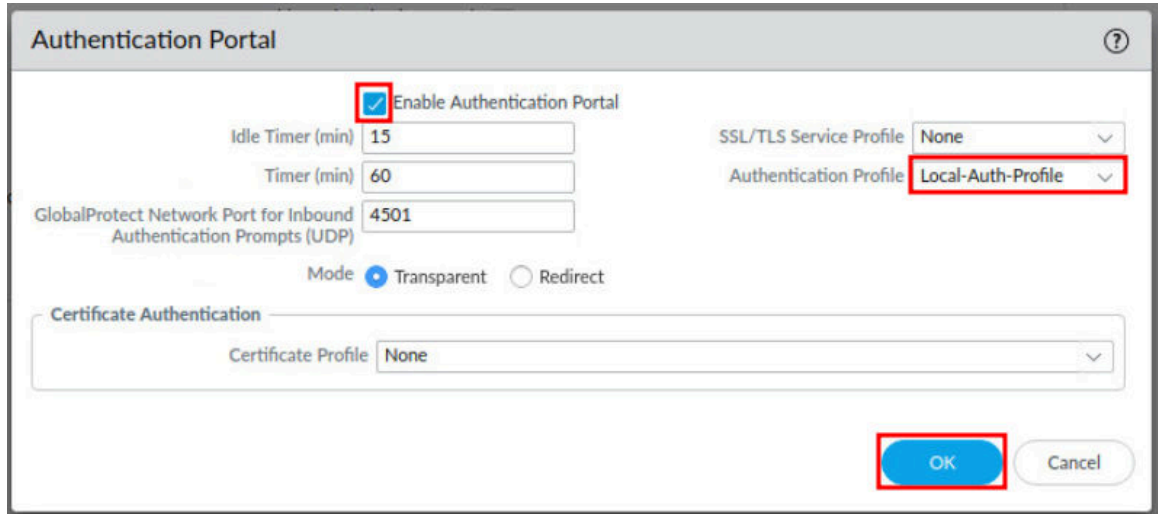
1. Navigate to **Device > User Identification > Authentication Portal Settings**, and click on the **gear** icon.





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

SSL/TLS Service Profile None

Authentication Profile Local-Auth-Profile

Mode ☒ Transparent ☐ Redirect

Certificate Authentication

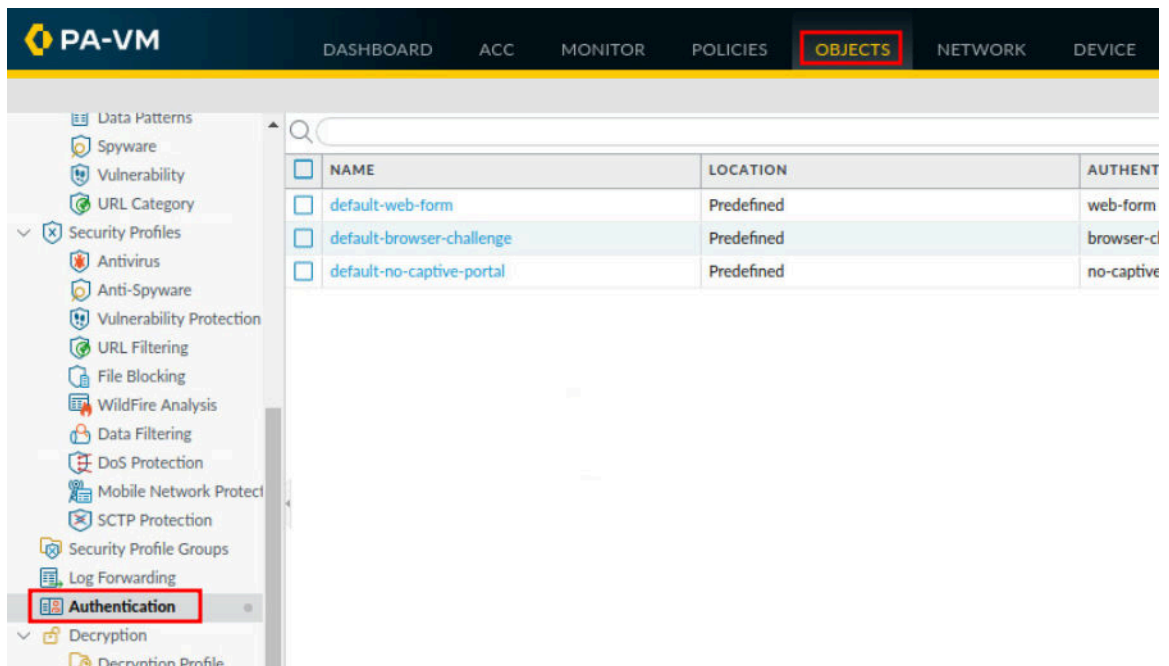
Certificate Profile None

OK Cancel



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.



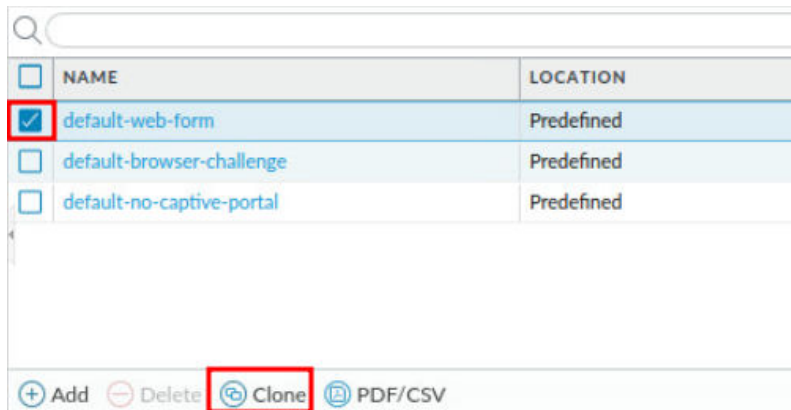
PA-VM DASHBOARD ACC MONITOR POLICIES **OBJECTS** NETWORK DEVICE

Search: []

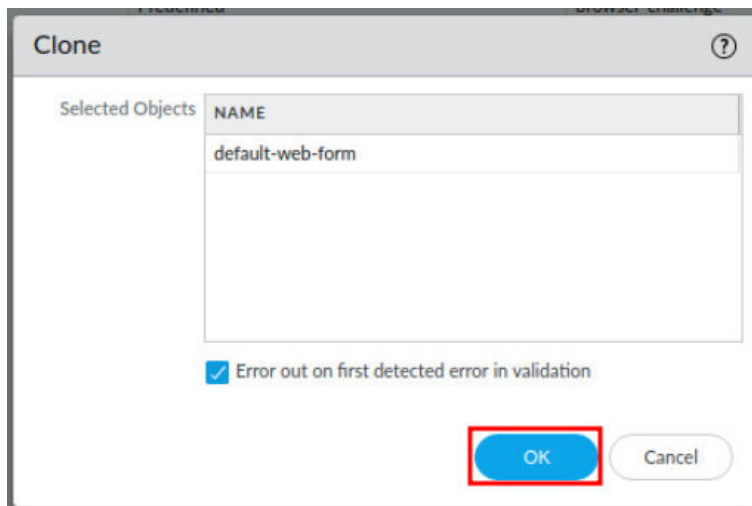
	NAME	LOCATION	AUTHENT
<input type="checkbox"/>	default-web-form	Predefined	web-form
<input type="checkbox"/>	default-browser-challenge	Predefined	browser-cl
<input type="checkbox"/>	default-no-captive-portal	Predefined	no-captive

Left sidebar items: Data Patterns, Spyware, Vulnerability, URL Category, Security Profiles (Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, WildFire Analysis, Data Filtering, DoS Protection, Mobile Network Protection, SCTP Protection), Security Profile Groups, Log Forwarding, **Authentication**, Decryption, Decryption Profile.

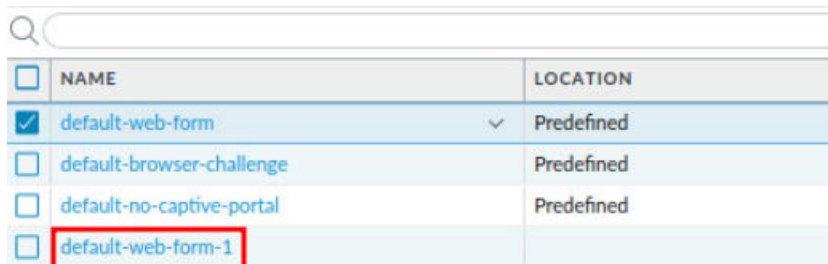
4. Click the checkbox beside the **default-web-form** and click **Clone**.



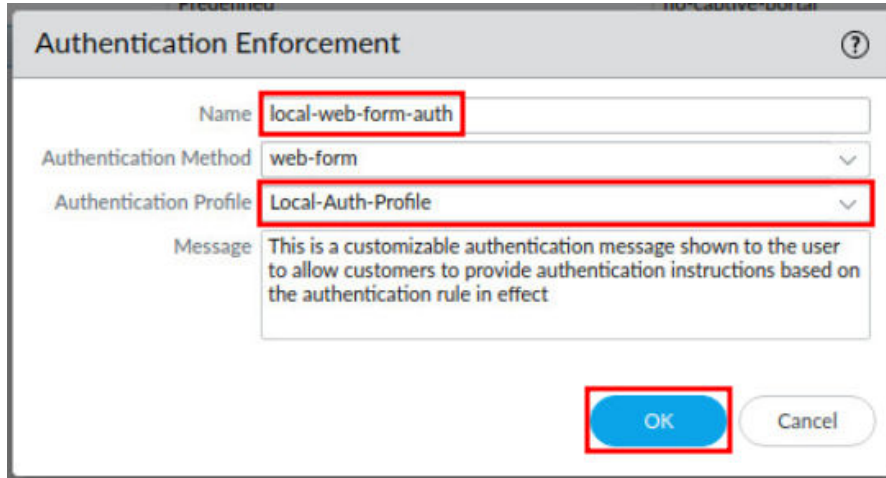
5. In the *Clone* window, click the **OK** button to confirm the clone.



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

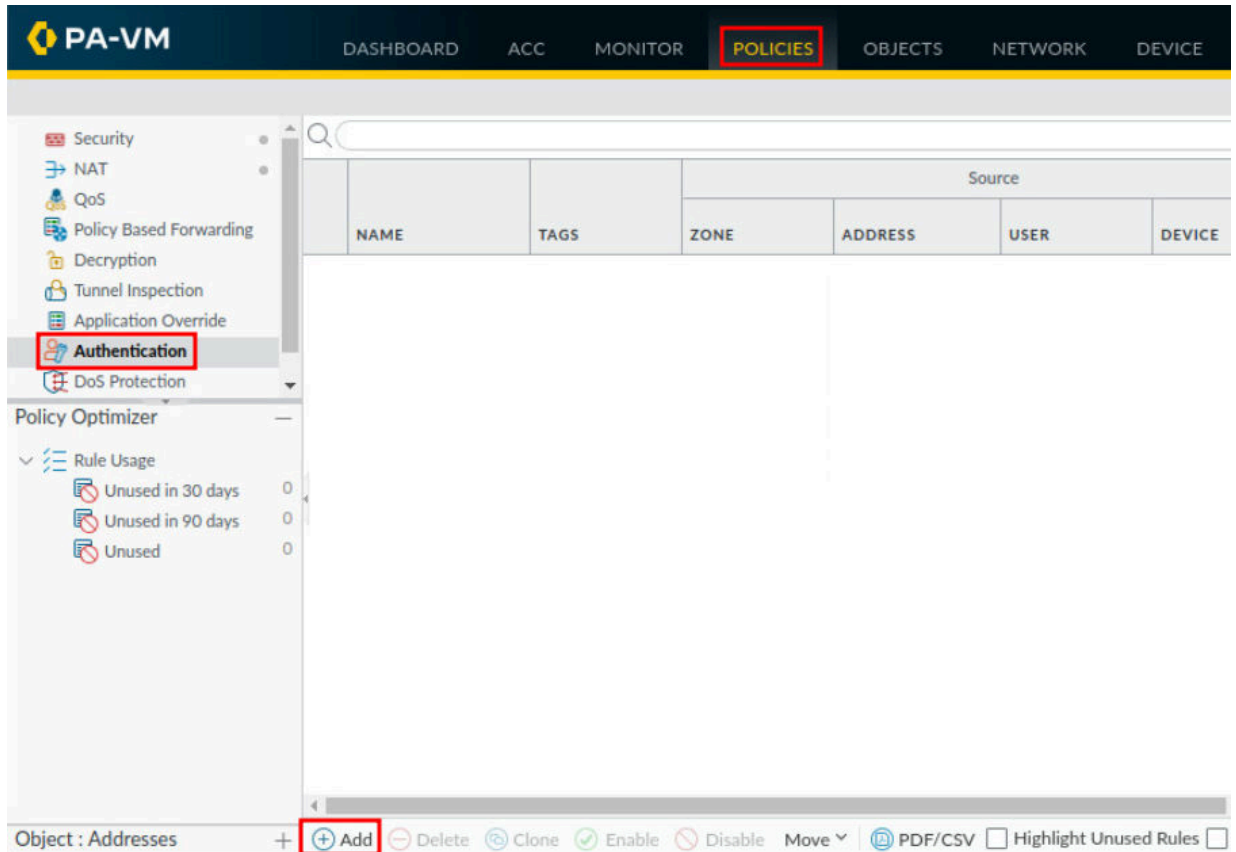


The screenshot shows the 'Authentication Enforcement' configuration window. The 'Name' field is set to 'local-web-form-auth'. The 'Authentication Method' is set to 'web-form'. The 'Authentication Profile' dropdown is set to 'Local-Auth-Profile'. The 'Message' field contains the text: 'This is a customizable authentication message shown to the user to allow customers to provide authentication instructions based on the authentication rule in effect'. The 'OK' button is highlighted with a red box.

1.3 Create an Authentication Policy

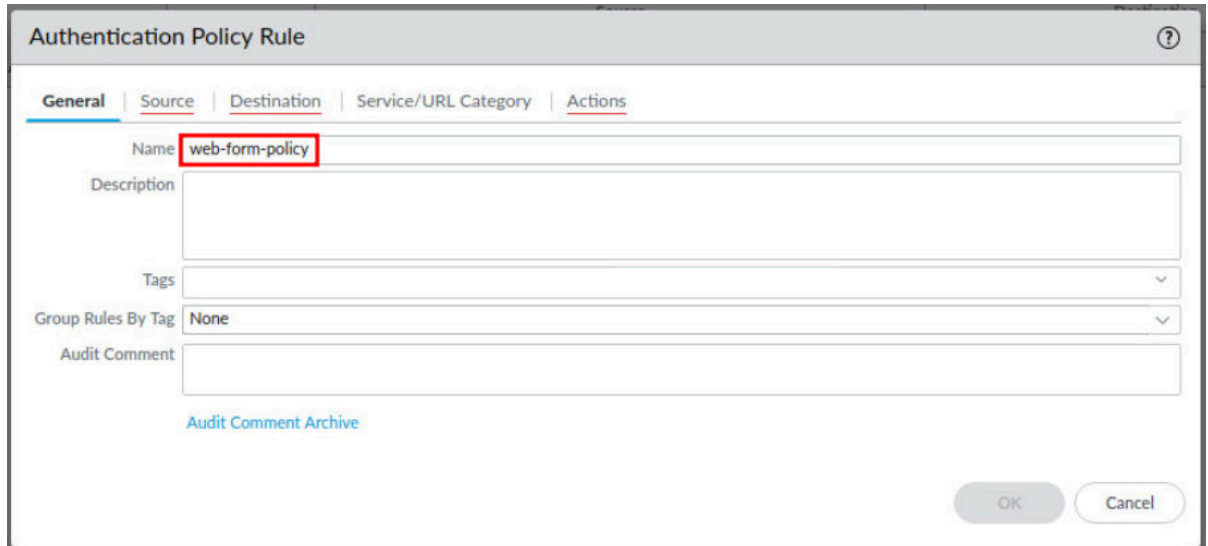
In this section, you will enable a captive portal. A captive portal redirects web requests that match the authentication policy and forces the user to use a login to continue. This is typically seen in corporate guest networks, hotels, and Wi-Fi hotspots. In this captive portal, you will use a web-form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

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



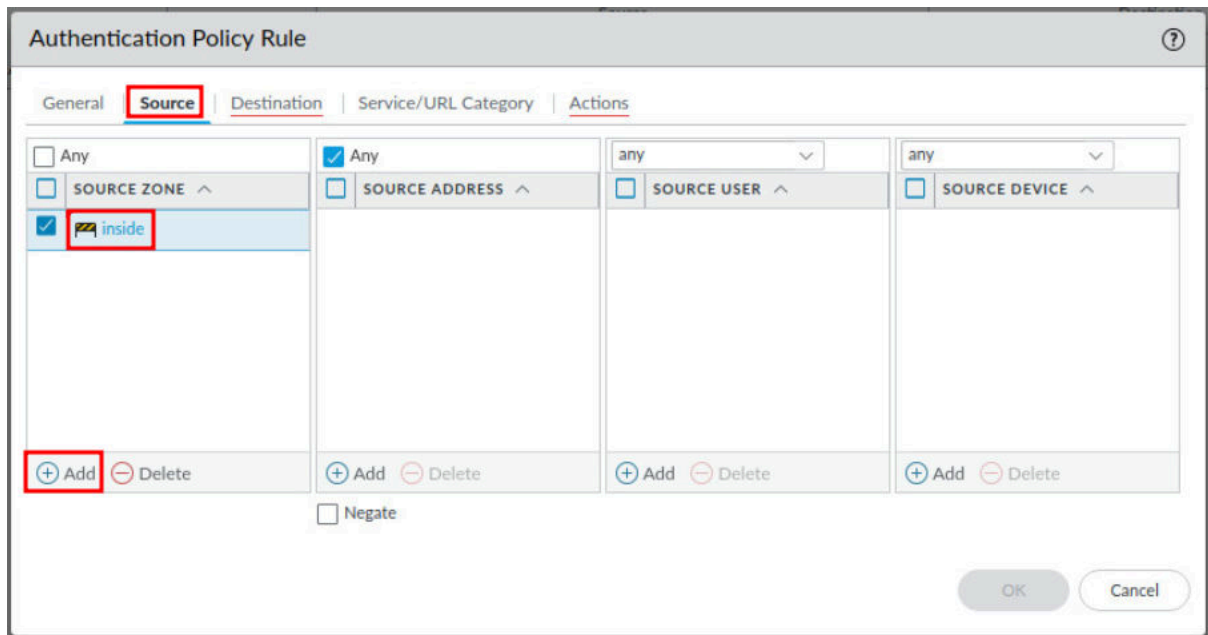
The screenshot shows the PA-VM web interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, **POLICIES** (highlighted with a red box), OBJECTS, NETWORK, and DEVICE. On the left sidebar, the 'Authentication' option is highlighted with a red box. The main content area displays a table with columns: NAME, TAGS, ZONE, ADDRESS, USER, and DEVICE. Below the table, there is a 'Policy Optimizer' section showing rule usage statistics. At the bottom, the 'Object : Addresses' is selected, and the '+ Add' button is highlighted with a red box. Other buttons like Delete, Clone, Enable, Disable, Move, PDF/CSV, and Highlight Unused Rules are also visible.

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



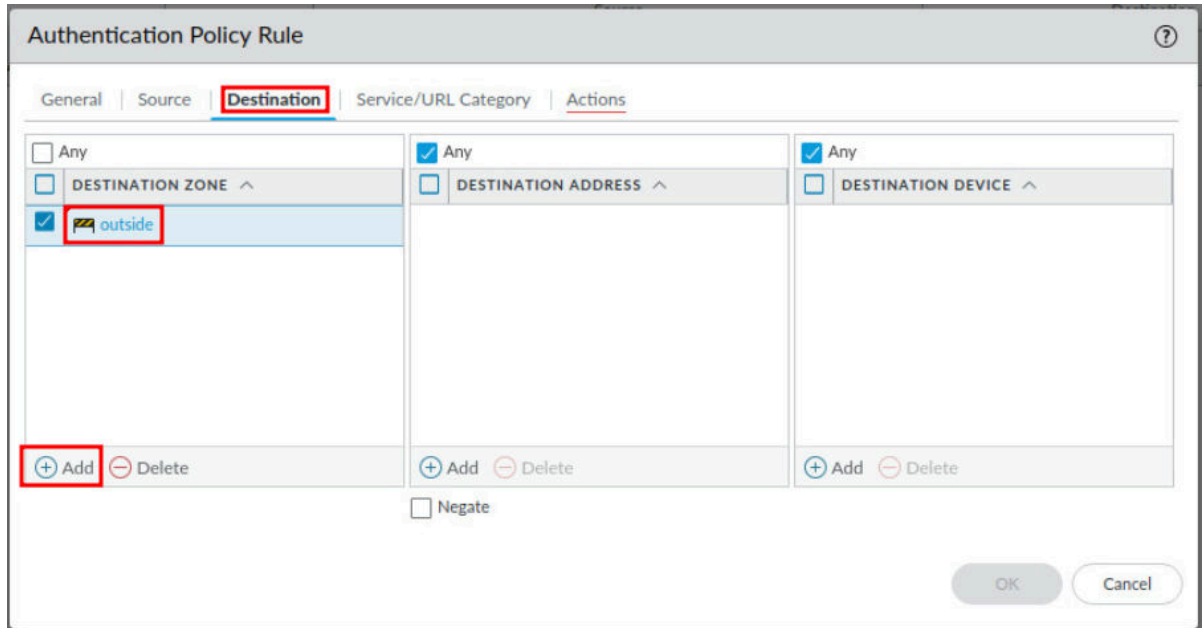
The screenshot shows the 'Authentication Policy Rule' window with the 'General' tab selected. The 'Name' field contains 'web-form-policy' and is highlighted with a red box. Other fields include 'Description', 'Tags', 'Group Rules By Tag' (set to 'None'), and 'Audit Comment'. There is a link for 'Audit Comment Archive' and 'OK'/'Cancel' buttons at the bottom right.

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**.



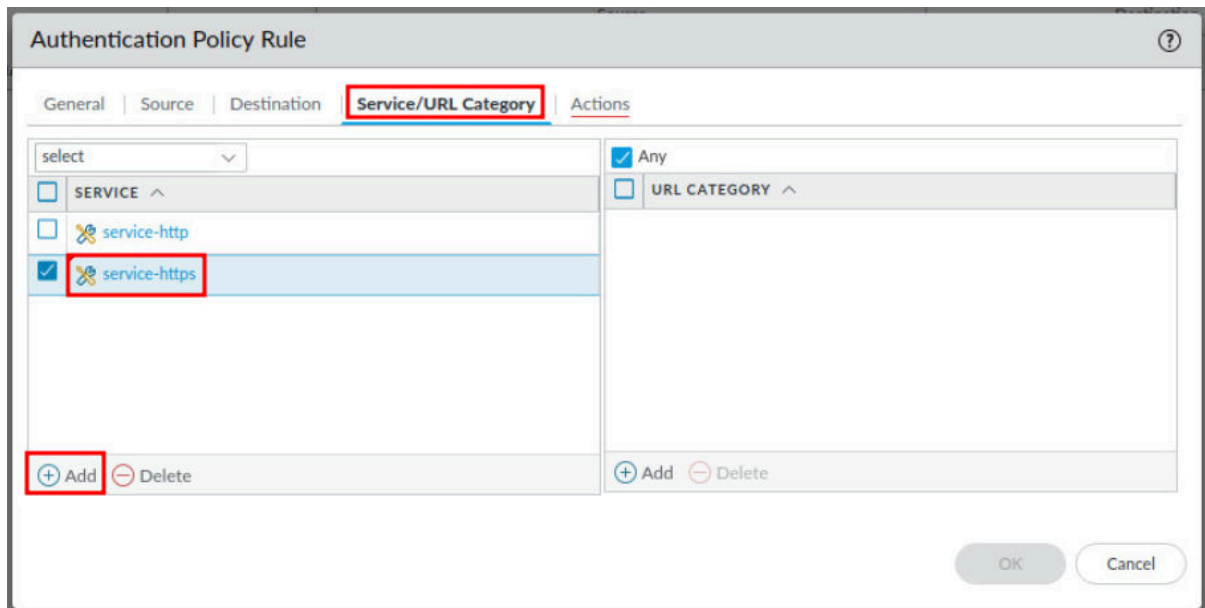
The screenshot shows the 'Authentication Policy Rule' window with the 'Source' tab selected. The 'Source' tab is highlighted with a red box. The 'Source Zone' section has a list with 'Any' and 'inside'. The 'inside' entry is selected and highlighted with a red box. Below the list are 'Add' and 'Delete' buttons, with the 'Add' button highlighted by a red box. There are also 'Add' and 'Delete' buttons for 'Source Address', 'Source User', and 'Source Device'. A 'Negate' checkbox is at the bottom. 'OK'/'Cancel' buttons are at the bottom right.

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**.



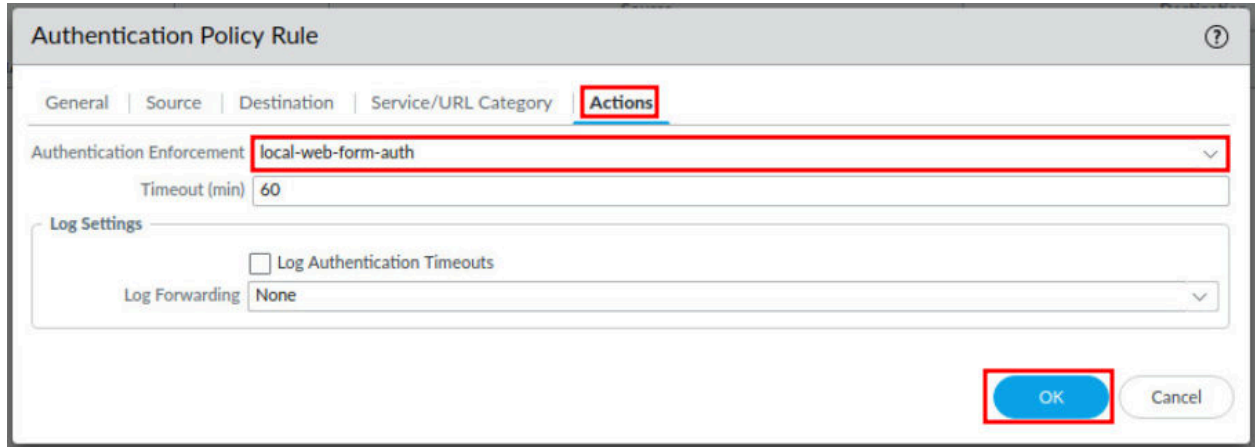
The screenshot shows the 'Authentication Policy Rule' window with the 'Destination' tab selected. The 'Destination Zone' section has a list with 'Any' and 'outside'. The 'outside' option is selected and highlighted. The 'Add' button is circled in red. The 'Destination Address' and 'Destination Device' sections are empty. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

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**.



The screenshot shows the 'Authentication Policy Rule' window with the 'Service/URL Category' tab selected. The 'Service' section has a list with 'Any', 'service-http', and 'service-https'. The 'service-https' option is selected and highlighted. The 'Add' button is circled in red. The 'URL Category' section is empty. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

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.



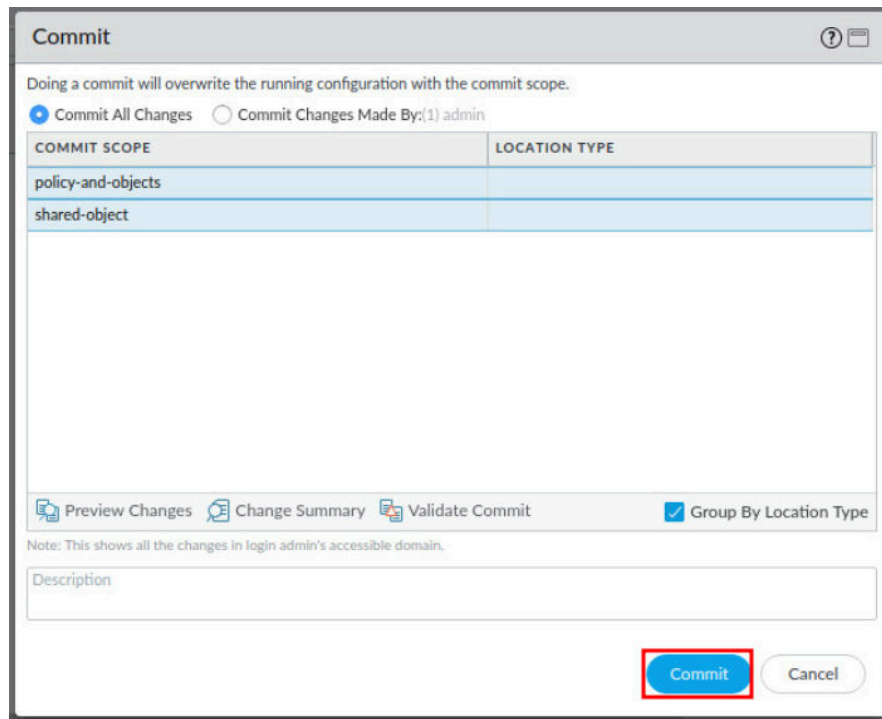
1.4 Commit and Test Authentication Policy

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

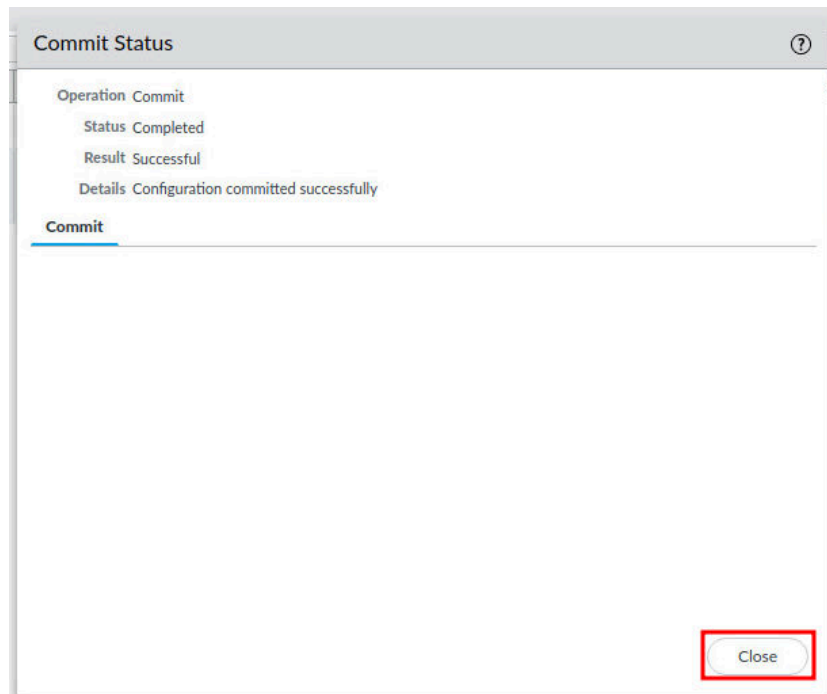
1. Click the **Commit** link located at the top-right of the web interface.



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



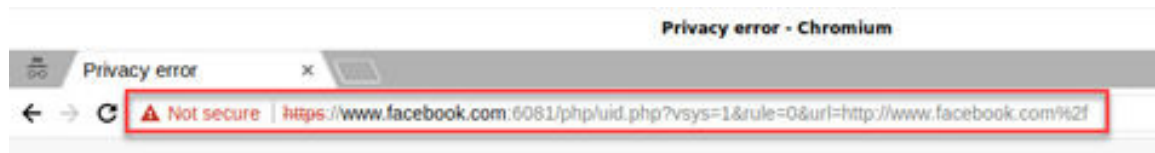
3. When the commit operation successfully completes, click **Close** to continue.



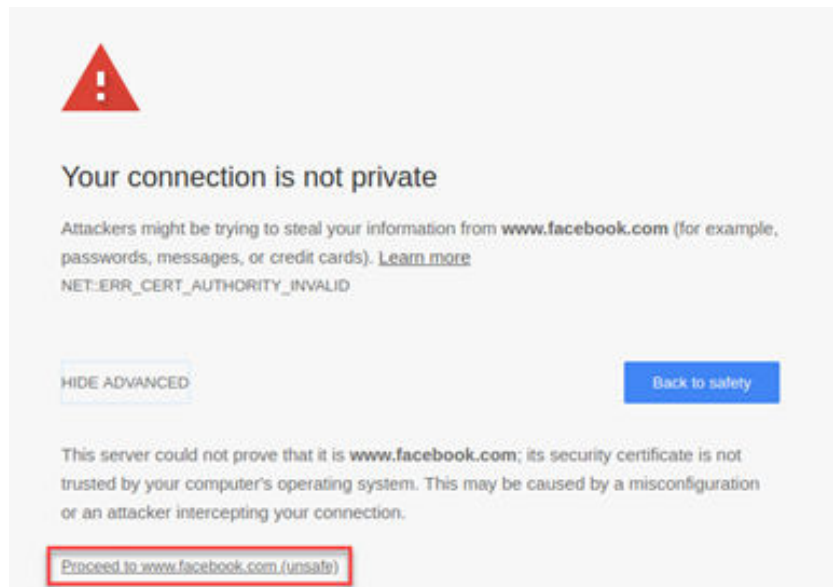
4. Open a second **Chromium Web Browser** from the taskbar.



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

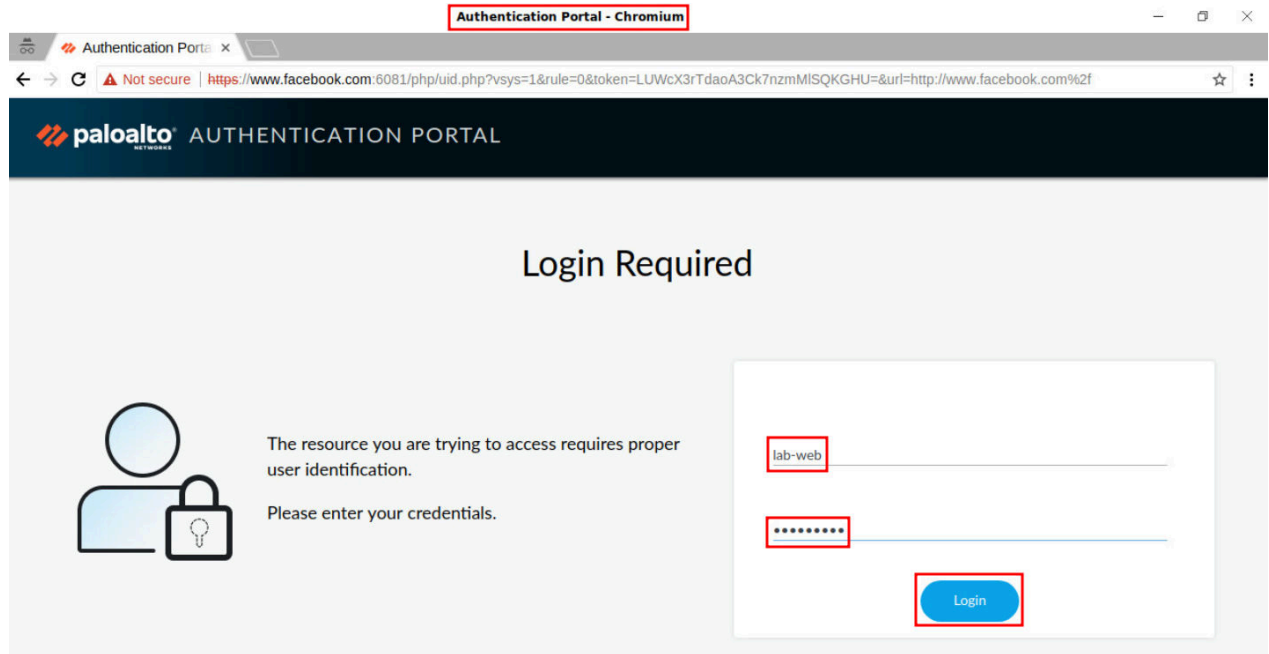


6. You will see a “Your connection is not private” message. Click on the **ADVANCED** Link, and then click **Proceed to www.facebook.com (unsafe)**.

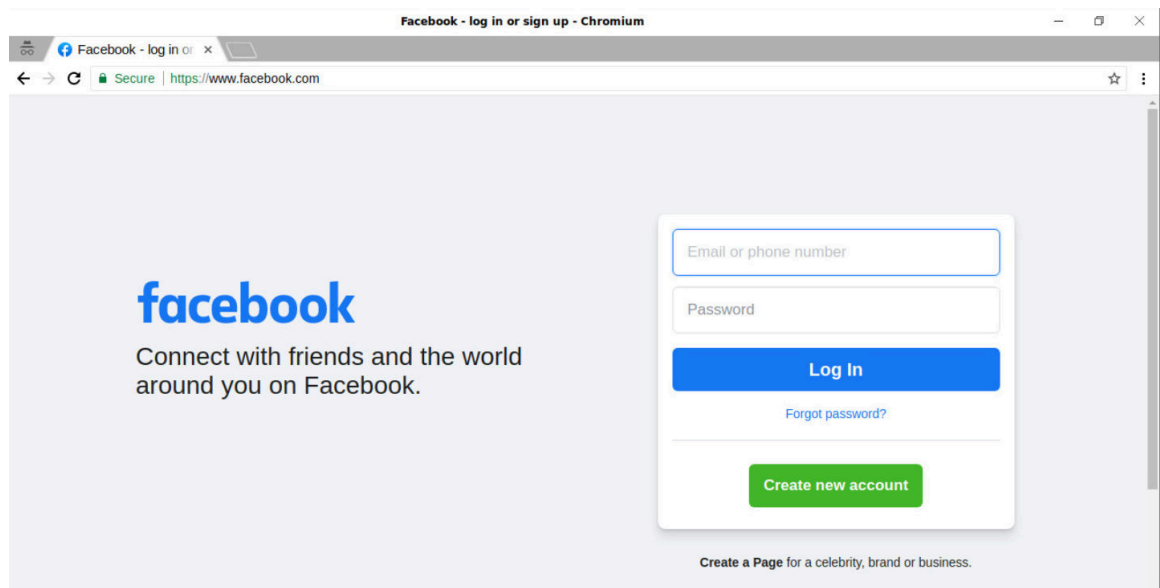


You are seeing this error because the Firewall is intercepting traffic coming from the inside zone to the outside zone. The Firewall serves as a man-in-the-middle until authenticated.

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.

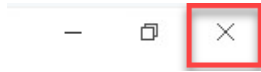


8. You will then see Facebook after you successfully authenticate to the Firewall as lab-web.

















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.