



PALO ALTO NETWORKS - EDU 210

Lab 1: Initial Configuration

Document Version: 2017-09-28

Copyright © 2017 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC² is a registered trademark of EMC Corporation.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
1 Lab: Initial Configuration.....	6
1.0 Connect to Your Student Firewall	6
1.1 Apply a Baseline Configuration to the Firewall.....	6
1.2 Add an Admin Role Profile	8
1.3 Add an Administrator Account.....	10
1.4 Test the policy-admin User	11
1.5 Take a Commit Lock and Test the Lock	13
1.6 Verify the Update and DNS Servers	17
1.7 Schedule Dynamic Updates.....	18

Introduction

The long-awaited moment has arrived. Your new Palo Alto Networks Firewall appliance has arrived, and the networking team has put it in the racks and wired it up. It is now your job as the Security Engineer to configure and test the firewall.

You have decided that the first thing you would like to do is create a new admin account that can only work with certain features of the firewall. To setup these restrictions you are going to have to create an administrator role and then assign it to the new admin account you create.

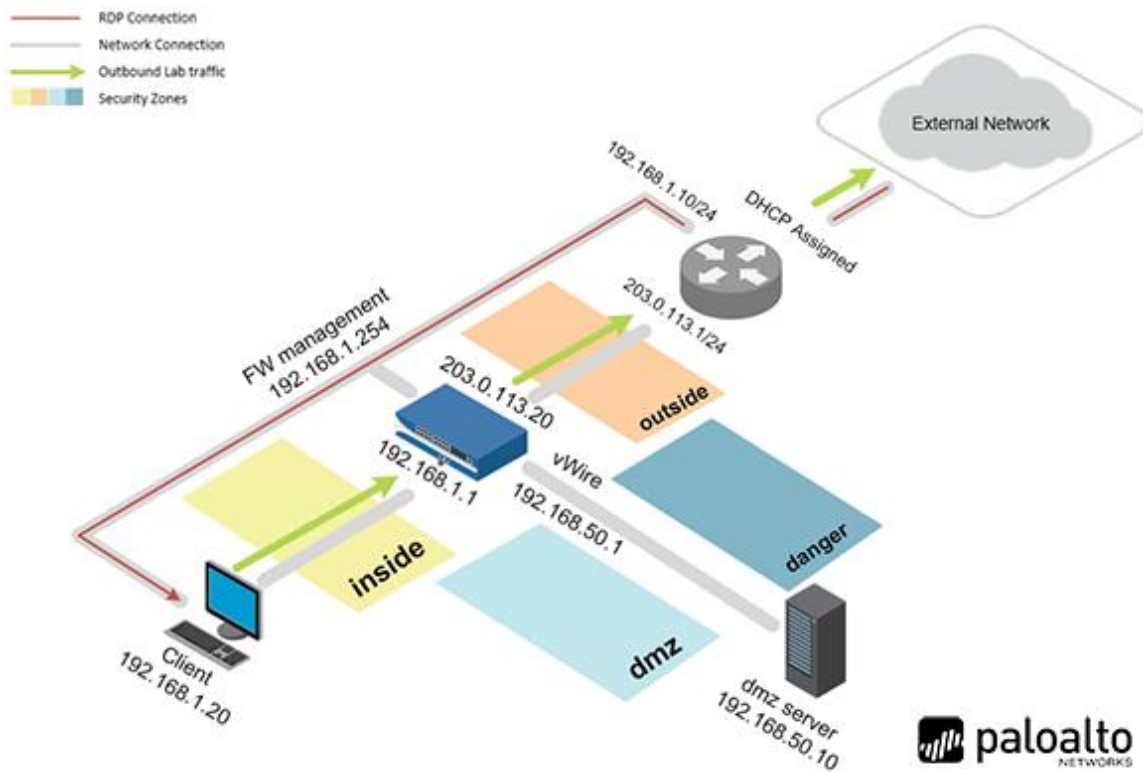
You also want to test the ability to prevent others from making or committing changes to the firewall while you are working. You have learned that this can be done with commit locks.

Finally, you need to make sure the firewall is updating with new signatures and updates on a regular basis, so you are going to configure the dynamic updates to do this for you.

Objectives

- Load a configuration.
- Create an administrator role.
- Create a new administrator and apply an administrator role.
- Observe the newly created role permissions via the CLI and WebUI.
- Create and test a commit lock.
- Configure DNS servers for the firewall.
- Schedule dynamic updates.

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 – Windows 2012 R2	192.168.1.20	lab-user	Pa10Alt0
Firewall – PA-VM	192.168.1.254	admin	admin

1 Lab: Initial Configuration

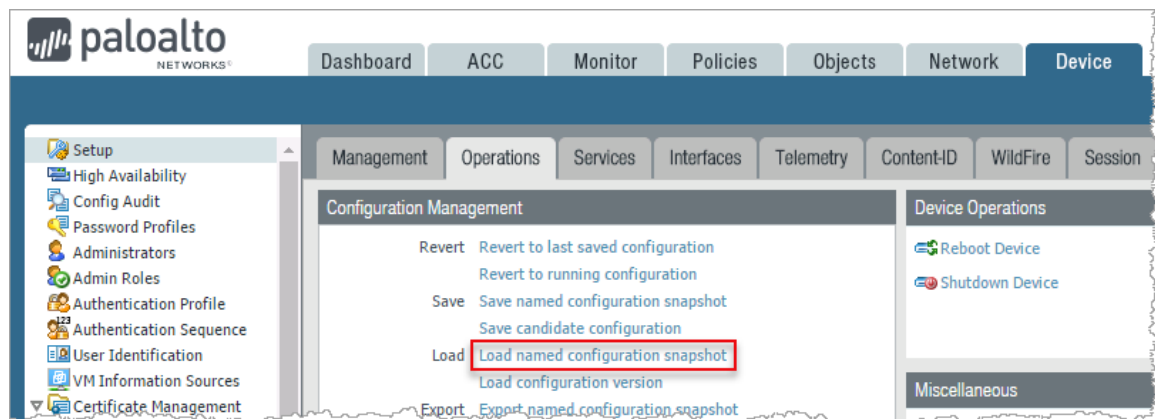
1.0 Connect to Your Student Firewall

1. Launch a browser and connect to `https://192.168.1.254`.
2. Log in to the Palo Alto Networks firewall using the following:

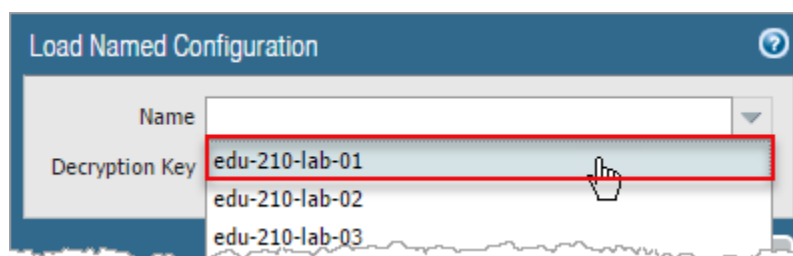
Parameter	Value
Name	admin
Password	admin

1.1 Apply a Baseline Configuration to the Firewall

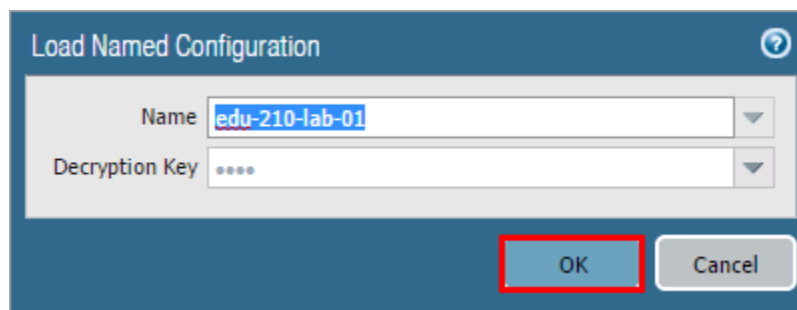
1. In the Palo Alto Networks firewall WebUI, select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



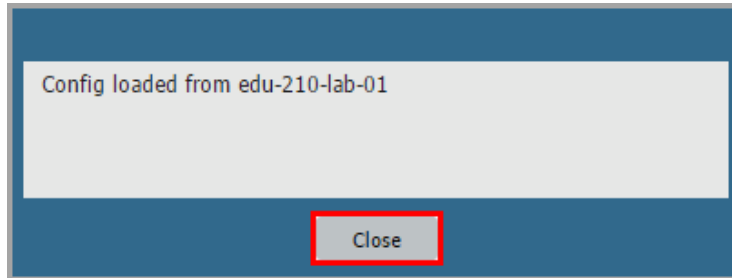
3. Click the drop-down list next to the Name text box and select **edu-210-lab-01**.



4. Click **OK**.



5. After some time, a confirmation that the configuration has been loaded appears. Click **Close**.

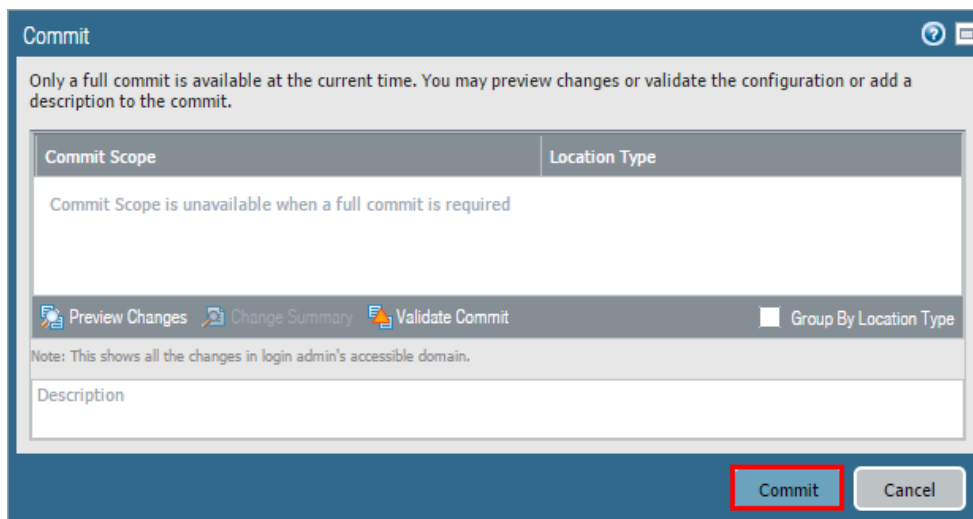


The following instructions are the steps to execute a “**Commit All**” as you will perform many times throughout these labs.

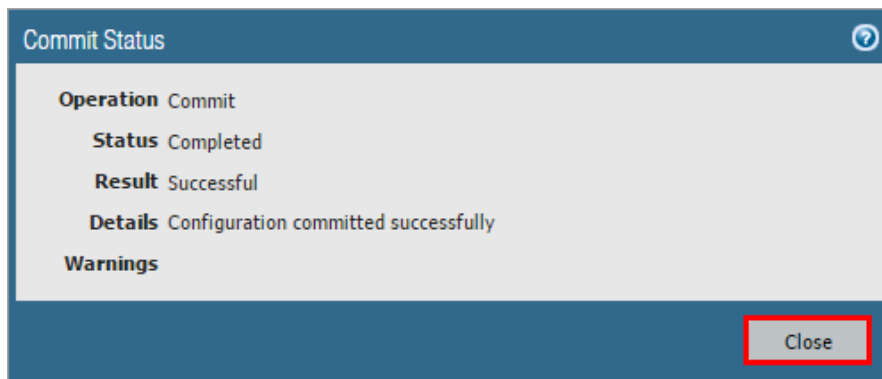
6. Click the **Commit** link at the top right of the WebUI.



7. Click **Commit** and wait until the commit process is complete.



8. Click **Close** to continue.



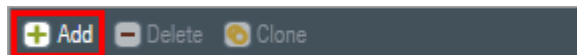
Note: Continue if warned about a full commit.

1.2 Add an Admin Role Profile

1. Select **Device > Admin Roles**.




2. Click **Add** in the lower-left corner of the panel to create a new administrator role:







3. In the Admin Role Profile wizard enter the following:

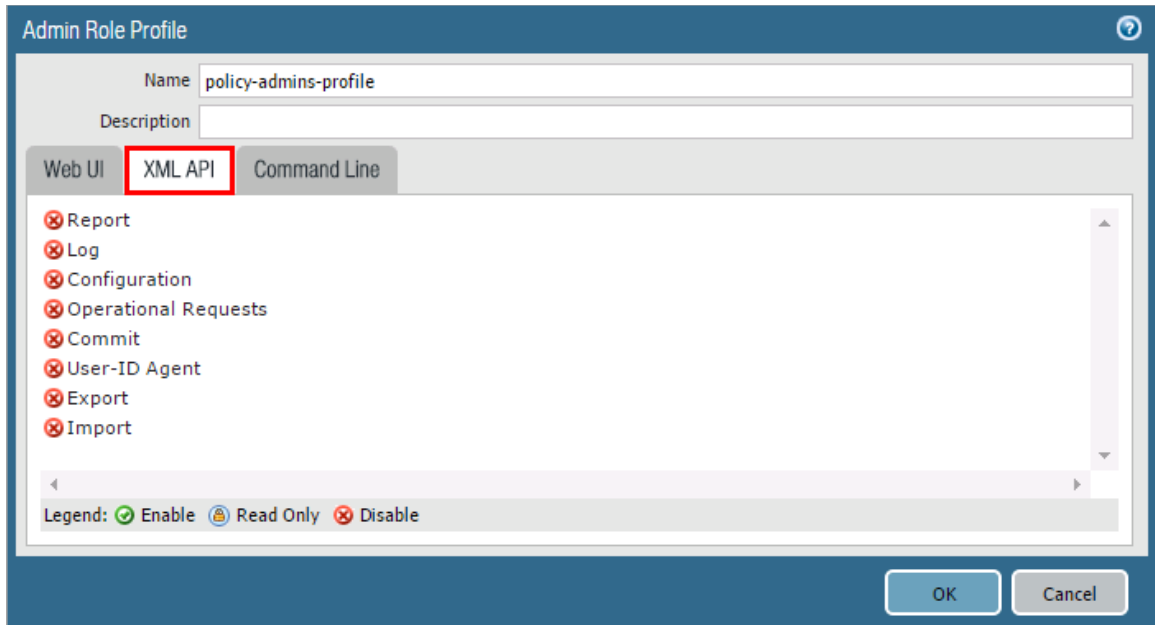


4. Type `policy-admins-profile` in the **Name** textbox.

5. Under the **Web UI** tab, click the  icon to disable the following:

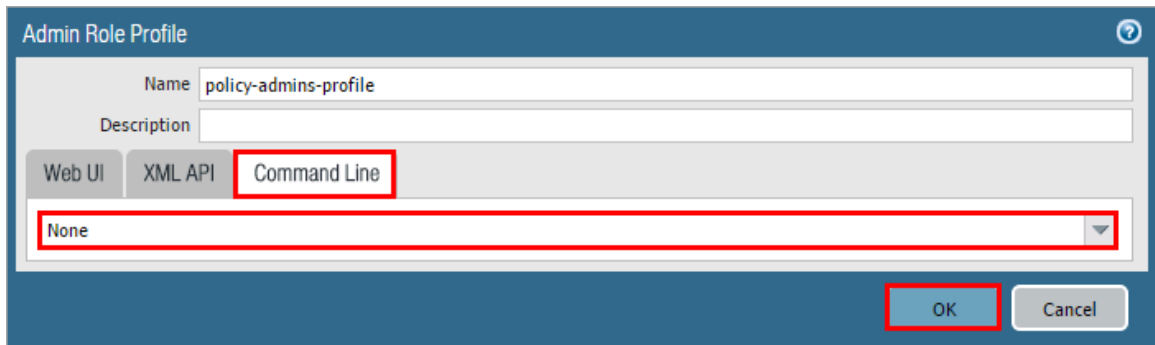
Parameter	Value
Monitor	
Network	
Device	
Privacy	

6. Click the **XML API** tab and verify that all items are  disabled.



The screenshot shows the 'Admin Role Profile' dialog box for the profile 'policy-admins-profile'. The 'XML API' tab is selected and highlighted with a red box. The list of XML API functions includes Report, Log, Configuration, Operational Requests, Commit, User-ID Agent, Export, and Import, all of which are preceded by a red 'X' icon indicating they are disabled. A legend at the bottom indicates that a green checkmark means 'Enable', a blue lock means 'Read Only', and a red 'X' means 'Disable'. The 'OK' button is also highlighted with a red box.

7. Click the **Command Line** tab and verify that the selection is none then click **OK** to continue.



The screenshot shows the 'Admin Role Profile' dialog box with the 'Command Line' tab selected and highlighted with a red box. The dropdown menu for the Command Line tab shows 'None' as the selected option, which is also highlighted with a red box. The 'OK' button is highlighted with a red box.

1.3 Add an Administrator Account

1. Select **Device > Administrators**.

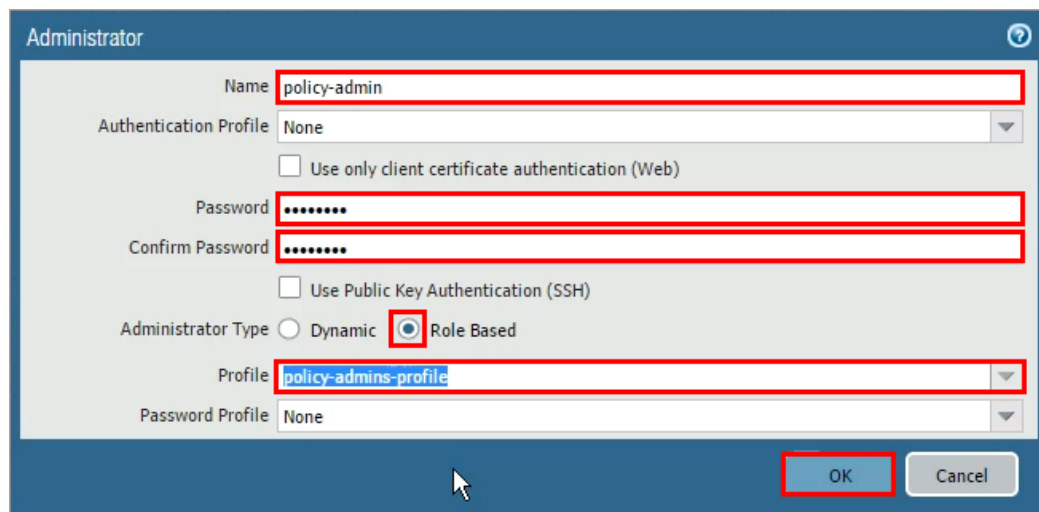


2. Click **Add** in the lower-left corner of the panel to open the Administrator configuration window.



3. Configure the following:

Parameter	Value
Name	policy-admin
Authentication Profile	None
Password	paloalto
Administrator Type	<input checked="" type="radio"/> Role Based
Profile	policy-admins-profile
Password Profile	None



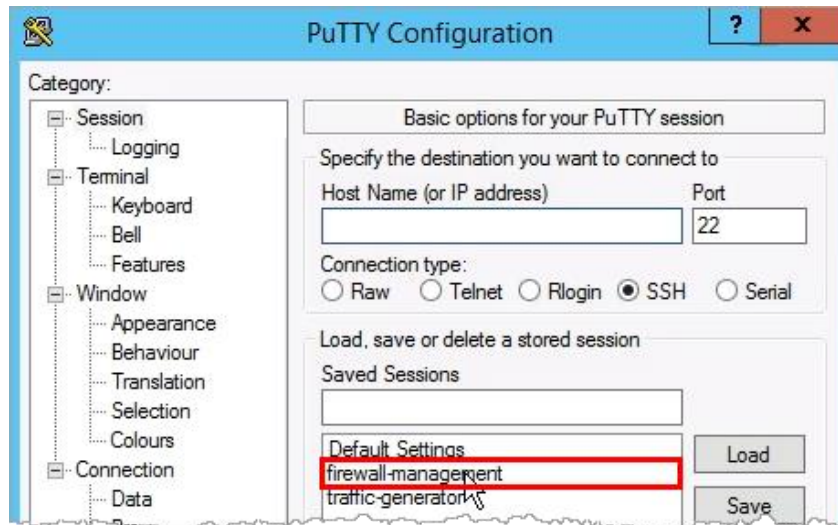
4. Click OK.
5. **Commit** all changes.

1.4 Test the policy-admin User

1. Open **PuTTY** from the Windows desktop.



2. Double-click **firewall-management**:



3. Log in using the following information:

Parameter	Value
Name	admin
Password	admin

The role assigned to this account is allowed CLI access, so the connection should succeed.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Mon Jul 10 11:00:21 2017 from 192.168.1.20
Number of failed attempts since last successful login: 0

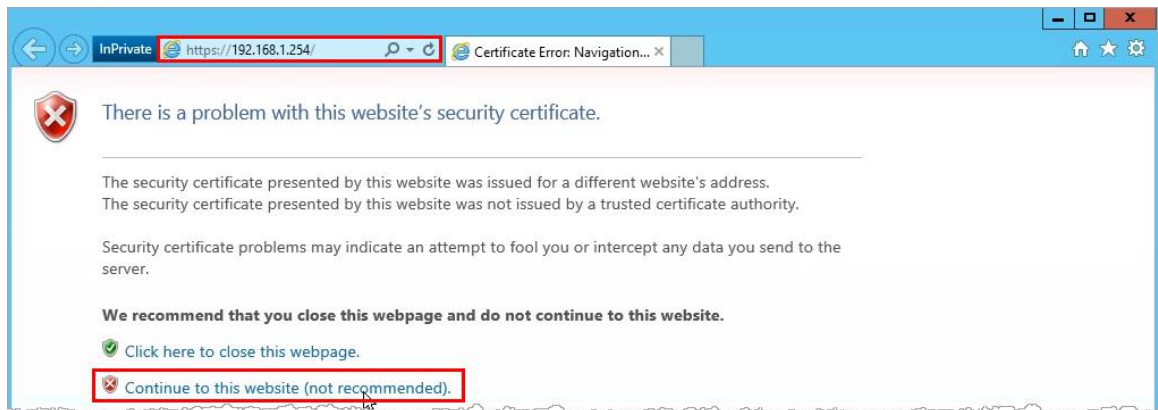
admin@lab-firewall> █
```

4. Close the **PuTTY** window and then open **PuTTY** again.
5. Open an SSH connection to **firewall-management**.
6. Log in using the following information (*the window will **close** if authentication is **successful***):

Parameter	Value
Name	policy-admin
Password	paloalto

```
login as: policy-admin
Using keyboard-interactive authentication.
Password: █
```

- Open a *different* browser (not a tab) in private/incognito mode and browse to `https://192.168.1.254`. A Certificate Warning might appear.



Click through the Certificate Warning. The Palo Alto Networks firewall login page opens.

- Log in using the following information (this action must be done in a different browser):

Parameter	Value
Name	policy-admin
Password	paloalto



- Close** the Welcome window if one is presented.
- Explore the available functionality of the WebUI. Notice that several tabs and functions are excluded from the interface because of the Admin Role assigned to this user account.

1.5 Take a Commit Lock and Test the Lock

The web interface supports multiple concurrent administrator sessions by enabling an administrator to lock the candidate or running configuration so that other administrators cannot change the configuration until the lock is removed.

1. From the WebUI where you are logged in as *policy-admin*, click the **transaction lock** icon to the right of the Commit link.



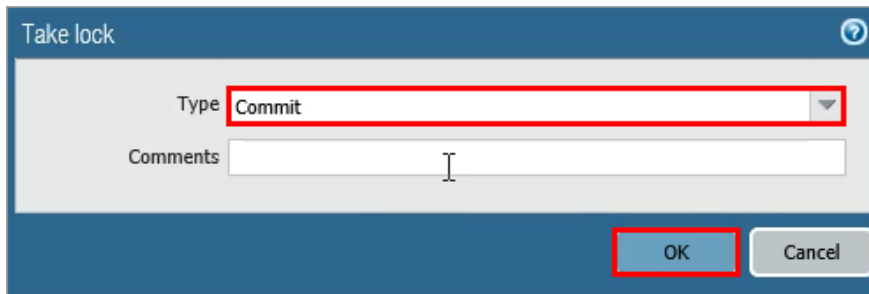
The **Locks** window opens.

2. Click **Take Lock**.



A **Take lock** window opens.

3. Set the Type to **Commit**, and click **OK**. The policy-admin lock is listed in the Locks window.



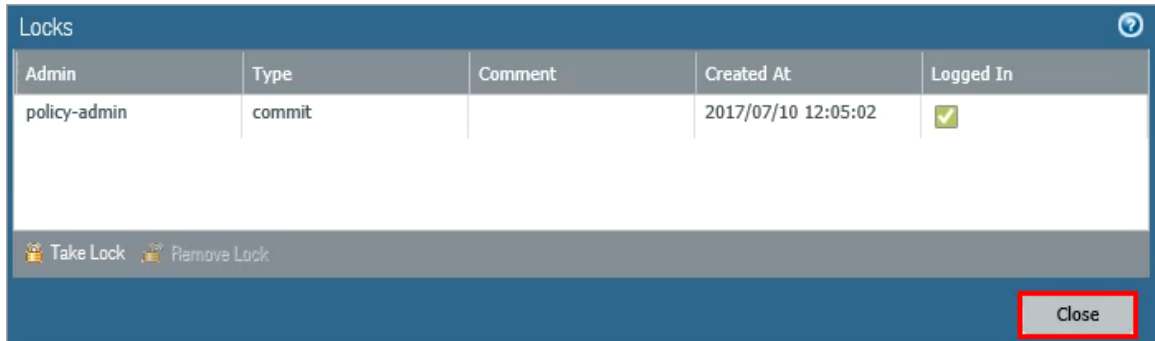
Take lock

Type: **Commit**

Comments:

OK Cancel

4. Click **Close** to close the Locks window.



Admin	Type	Comment	Created At	Logged In
policy-admin	commit		2017/07/10 12:05:02	✓

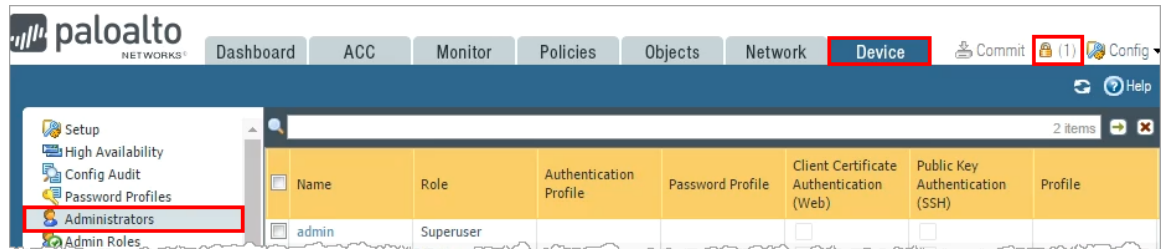
Take Lock Remove Lock

Close

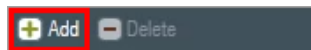
5. Click the **Logout** button on the bottom-left corner of the WebUI:



6. Close the policy-admin browser window.
7. Return to the WebUI where you are logged in as admin.
8. Click the **Device > Administrators** link. The WebUI refreshes. Notice the lock icon in the upper-right corner of the WebUI.

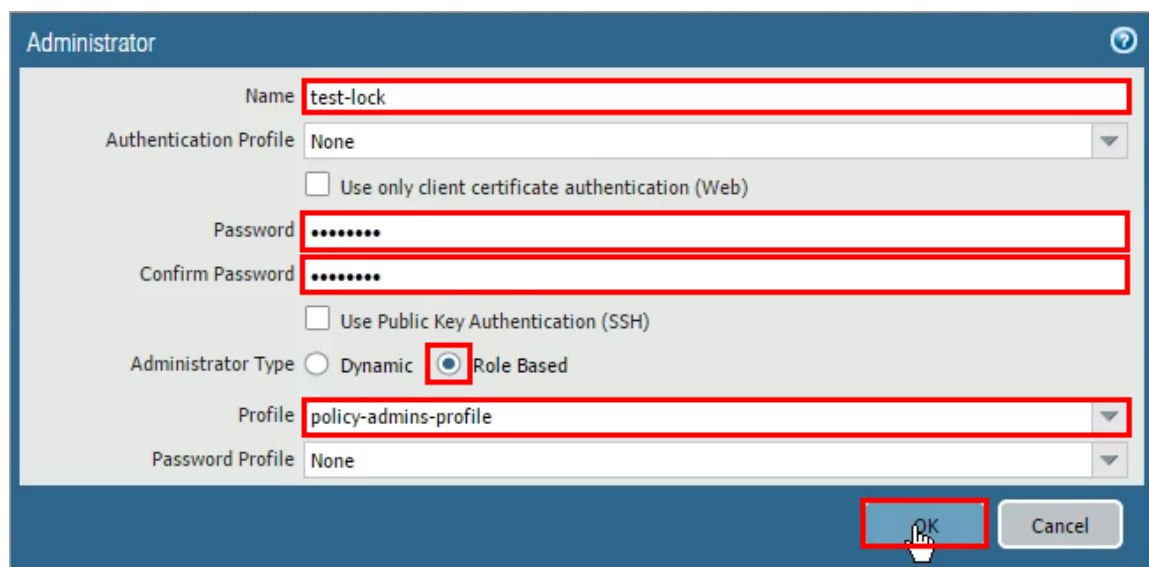


9. Click **Add** to add another administrator account.



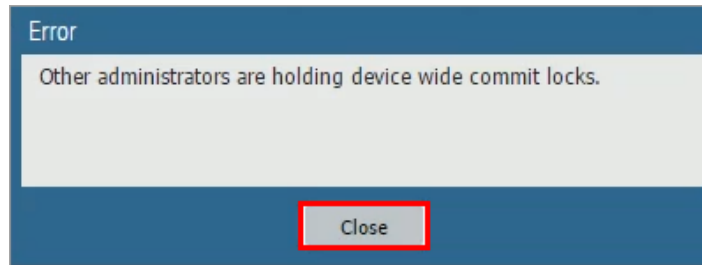
10. Configure the following:

Parameter	Value
Name	test-lock
Authentication Profile	None
Password	paloalto
Administrator Type	<input checked="" type="radio"/> Role Based
Profile	policy-admins-profile
Password Profile	None



11. Click **OK**. The new test-lock user is listed.

12. **Commit** all changes. Although you could add a new administrator account, you are not allowed to commit the changes because of the Commit lock set by the policy-admin user:

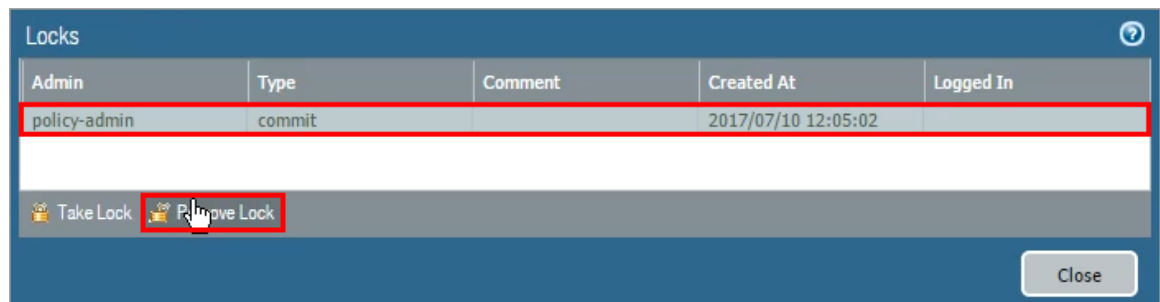


Click **Close**.

13. Click the **transaction lock** icon in the upper-right corner:

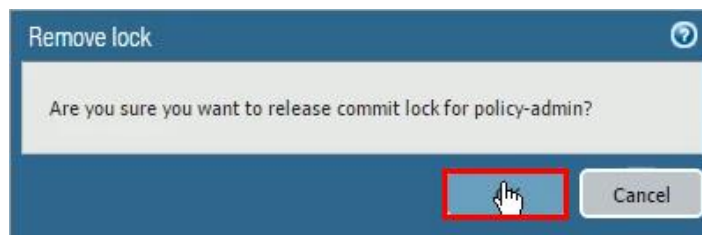


14. Select the **policy-admin** lock and click **Remove Lock**:

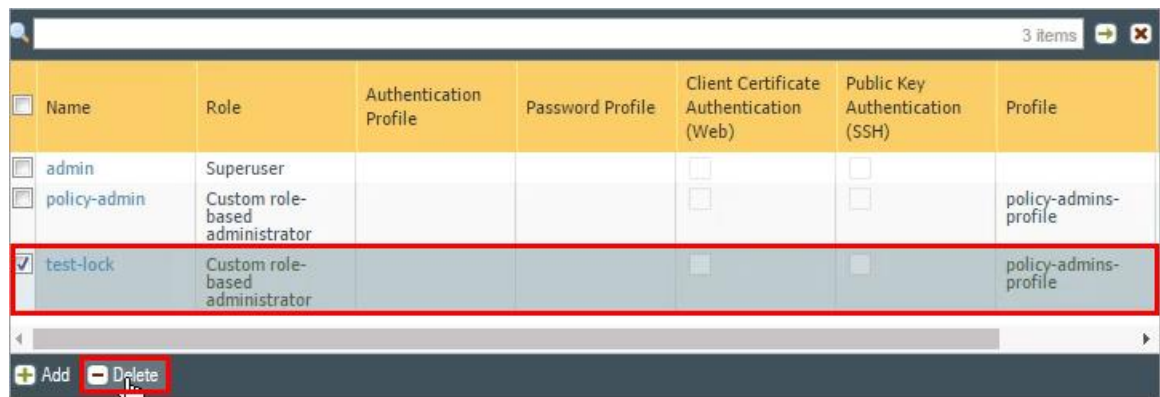


Note: The user that took the lock or any superuser can remove a lock.

15. Click **OK** and the lock is removed from the list.



16. Click **Close**.
17. **Commit** all changes. You can now commit the changes.
18. Select the test-lock user and then click **Delete** to delete the test-lock user.



	Name	Role	Authentication Profile	Password Profile	Client Certificate Authentication (Web)	Public Key Authentication (SSH)	Profile
<input type="checkbox"/>	admin	Superuser			<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	policy-admin	Custom role-based administrator			<input type="checkbox"/>	<input type="checkbox"/>	policy-admins-profile
<input checked="" type="checkbox"/>	test-lock	Custom role-based administrator			<input type="checkbox"/>	<input type="checkbox"/>	policy-admins-profile

Add Delete

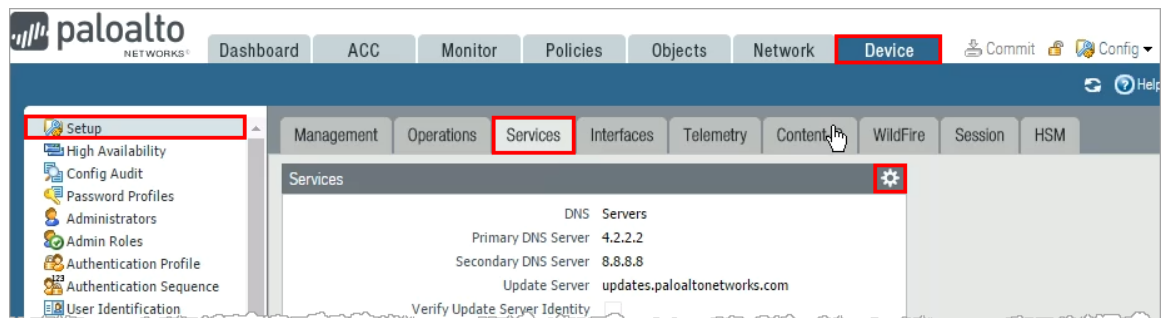
19. Click **Yes** to confirm the deletion.

20. **Commit** all changes.

1.6 Verify the Update and DNS Servers

The DNS server configuration settings are used for all DNS queries that the firewall initiates in support of FQDN address objects, logging, and firewall management.

1. Select **Device > Setup > Services**.
2. Open the Services window by clicking the **icon** in the upper-right corner of the Services panel:

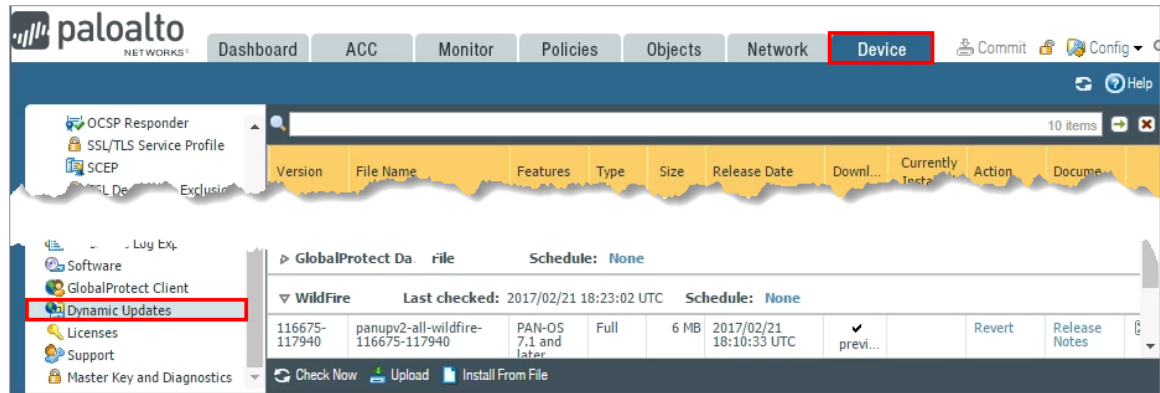


3. Verify that **4.2.2.2** is the Primary DNS Server and that **8.8.8.8** is the Secondary DNS Server.
4. Verify that **updates.paloaltonetworks.com** is the Update Server.
5. Click **OK**.

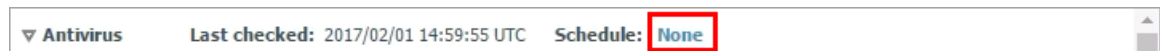
1.7 Schedule Dynamic Updates

Palo Alto Networks regularly posts updates for application detection, threat protection, and GlobalProtect data files through dynamic updates.

1. Select **Device > Dynamic Updates**.



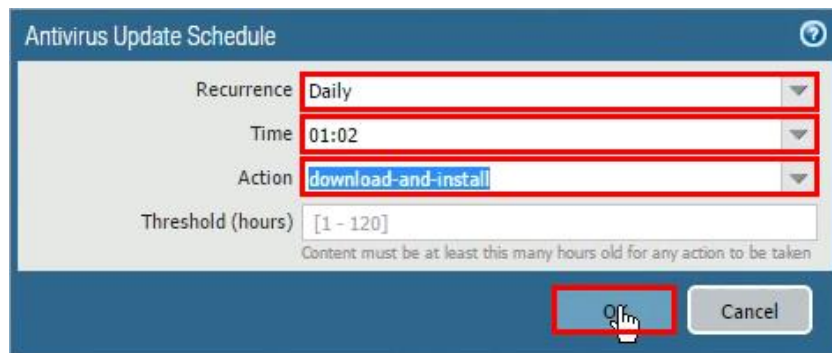
2. Locate and click the hyperlink on the far right of **Antivirus**:



The scheduling window opens. Antivirus signatures are released daily.

3. Configure the following:

Parameter	Value
Recurrence	Daily
Time	01:02
Action	download-and-install



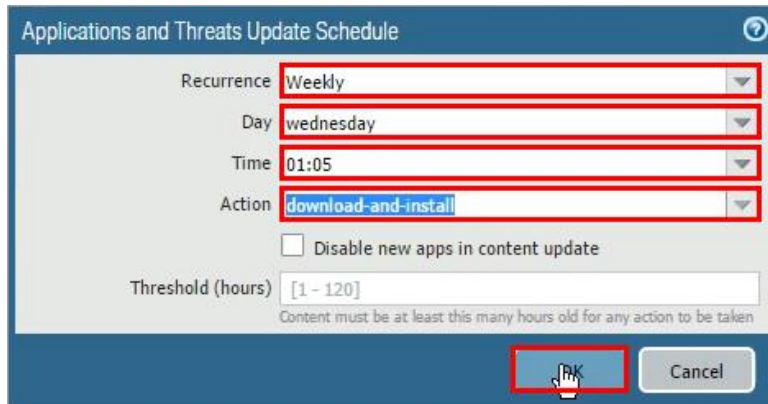
Then click **OK**.

4. Locate and click the hyperlink on the far right of **Application and Threats**. The scheduling window opens. Application and Threat signatures are released weekly.

▼ Applications and Threats Last checked: 2017/02/01 15:00:47 UTC Schedule: **Every Wednesday at 01:02 (Download only)**

5. Configure the following:

Parameter	Value
Recurrence	Weekly
Day	wednesday
Time	01:05
Action	download-and-install



The dialog box titled "Applications and Threats Update Schedule" contains the following settings: Recurrence is set to "Weekly", Day is set to "wednesday", Time is set to "01:05", and Action is set to "download-and-install". There is an unchecked checkbox for "Disable new apps in content update" and a "Threshold (hours)" field set to "[1 - 120]" with a note below it stating "Content must be at least this many hours old for any action to be taken". The "OK" button is highlighted with a red box and a mouse cursor.

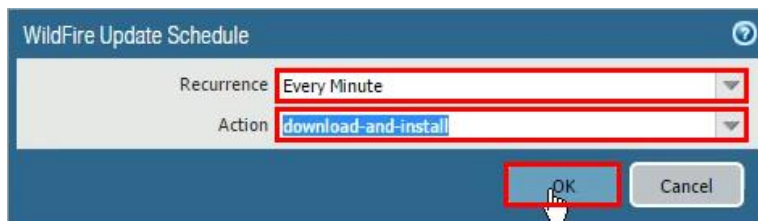
Click **OK**.

6. Locate and click the hyperlink on the far right of **WildFire**. The scheduling window opens. WildFire signatures can be available within five minutes.

▼ WildFire Last checked: 2017/02/21 18:23:02 UTC Schedule: **None**

7. Configure the following:

Parameter	Value
Recurrence	Every Minute
Action	download-and-install



The dialog box titled "WildFire Update Schedule" contains the following settings: Recurrence is set to "Every Minute" and Action is set to "download-and-install". The "OK" button is highlighted with a red box and a mouse cursor.

8. Click **OK**.
9. **Commit** all changes.

Stop. This is the end of the Initial Configuration lab.