



## **PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES**

### **Lab 1: Initial Configuration**

**Document Version: 2016-04-19**

Copyright © 2016 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

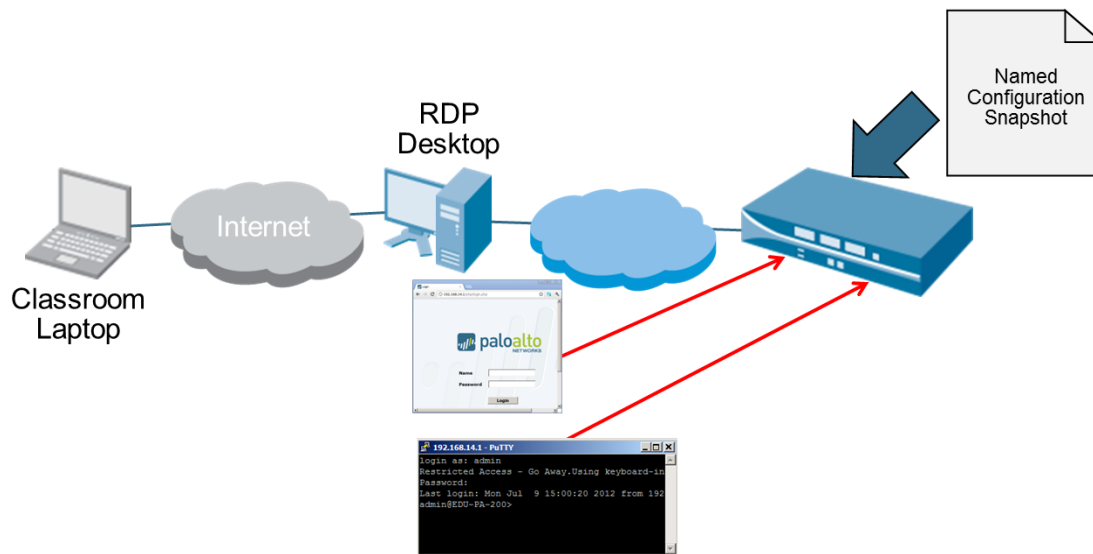
NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

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

## Contents

Introduction .....	3
Objective .....	4
Pod Topology .....	5
Lab Settings .....	6
1 Connect to Your Student Firewall .....	7
2 Clear the Logs.....	10
3 Add an Administrator Role .....	12
4 Add an Administrator Account .....	13
5 Test the ip-admin User.....	15
6 Take a Transaction Lock and Test the Lock.....	16

## Introduction



You have been tasked with integrating a new firewall into your environment:

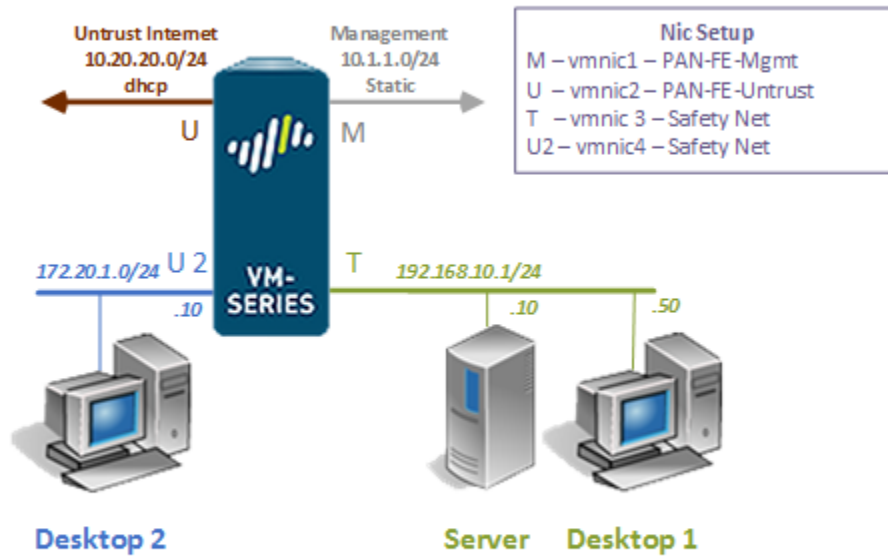
1. Check that the licenses are valid and that the software and dynamic updates are current.
2. Clear old log data so that you do not have to filter through old data when managing the firewall.
3. Set the date and time to your local time zone.
4. Apply a saved configuration to the firewall so that it is in a known state.
5. Create a new admin account.
6. Create a role for a policy administrator that allows access to all firewall functionality through the WebUI excluding the Monitor, Network, Privacy, and Device tabs. The account should have no access to the XML API or the CLI.
7. Create an account using this role.
8. Use the newly created account and your administrator account to test the locking features of the WebUI. Verify that you cannot create a new user with one account if the configuration is locked by the other. Be sure to remove the locks when you finish this exercise.

## Objective

In this lab, you will be using Palo Alto technology. You will be performing the following tasks:

1. Connecting to the Student PC
2. Verify connectivity between the student desktop and the student firewall
3. Clear the firewall logs
4. Apply a baseline configuration to build successive labs
5. Create a new admin account and test the configuration locks

## Pod 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)
Ubuntu Desktop 1	192.168.10.50	sysadmin	Train1ng\$
Ubuntu Server	192.168.10.10	sysadmin	Train1ng\$
Ubuntu Desktop 2	172.30.1.10	sysadmin	Train1ng\$
Palo Alto Firewall	192.168.10.1 172.30.1.1	admin	paloalto

## 1 Connect to Your Student Firewall

1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using **sysadmin** as the *username* and **Training\$** as the *password*. Click **Log In**.
3. Double-click on the **Firefox Web Browser** icon located on the *Desktop*.



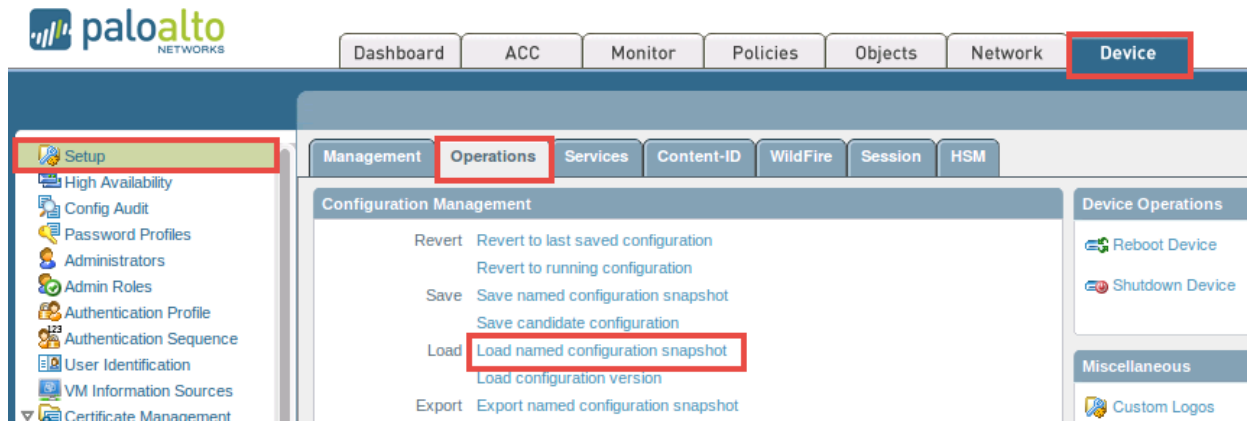
4. In the address field, type **https://192.168.10.1** and press **Enter**.

If you experience the “Unable to connect” message while attempting to connect to the specified IP above, please wait an additional 3-5 minutes for the PA VM to fully initialize and refresh the page to continue.

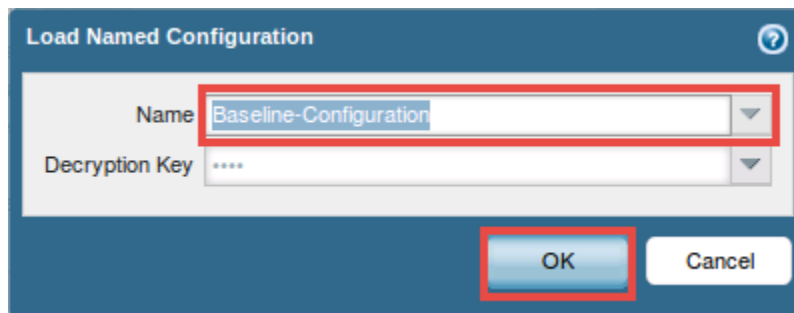
5. Login with the *username* **admin** and *password* **paloalto** on the firewall web interface.



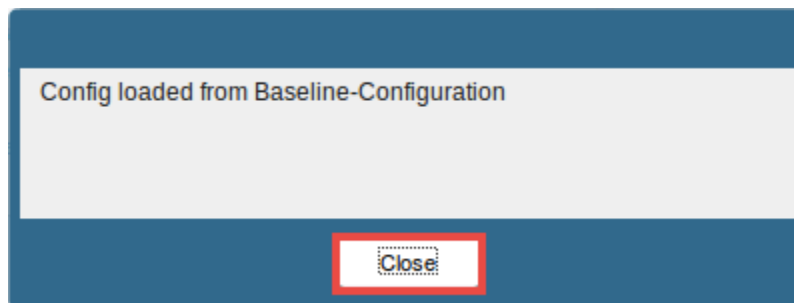
6. Using the *Palo Alto WebUI*, navigate to **Device > Setup > Operations** and click on the **Load named configuration snapshot** link.



7. In the *Load Named Configuration* window, choose **Baseline-Configuration** for the *Name* drop-down box and click **OK** to continue.



8. Click **Close** when prompted that the configuration has been loaded successfully.

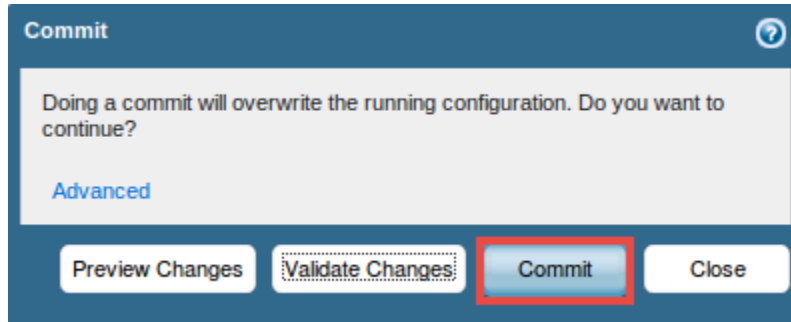


9. Click on the **Commit** link located at the top-right of the *WebUI*.

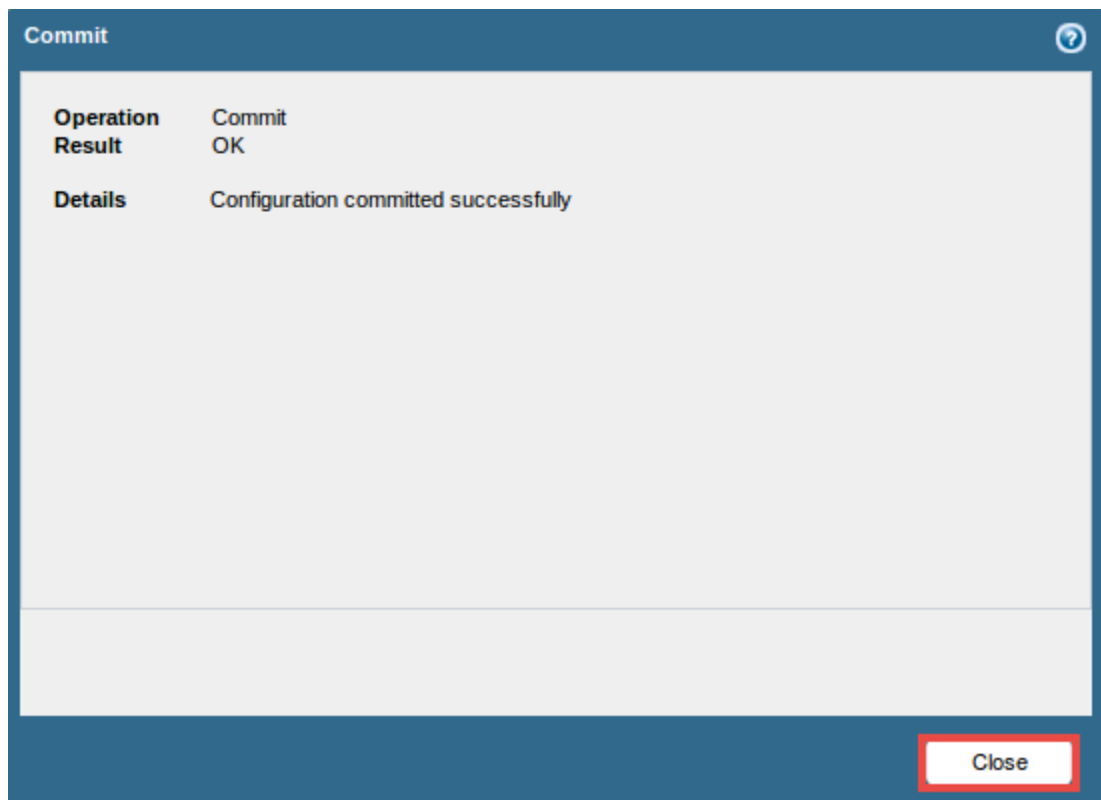




10. In the *Commit* window, click **Commit** to proceed with committing the changes.



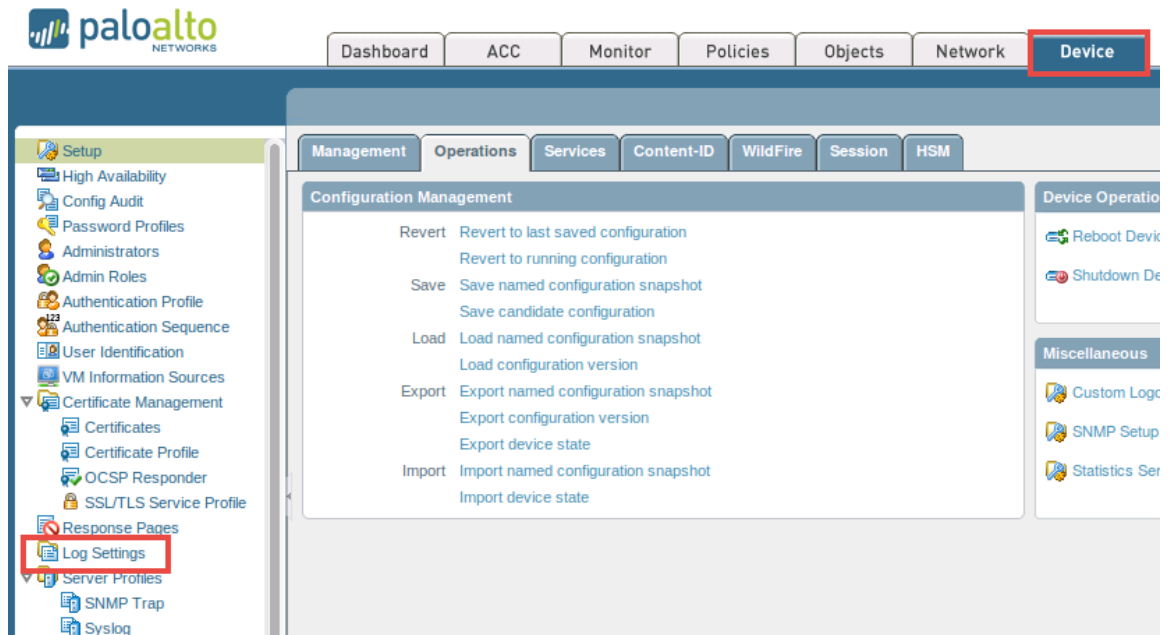
11. Once the operation successfully completes, click **Close** to continue.



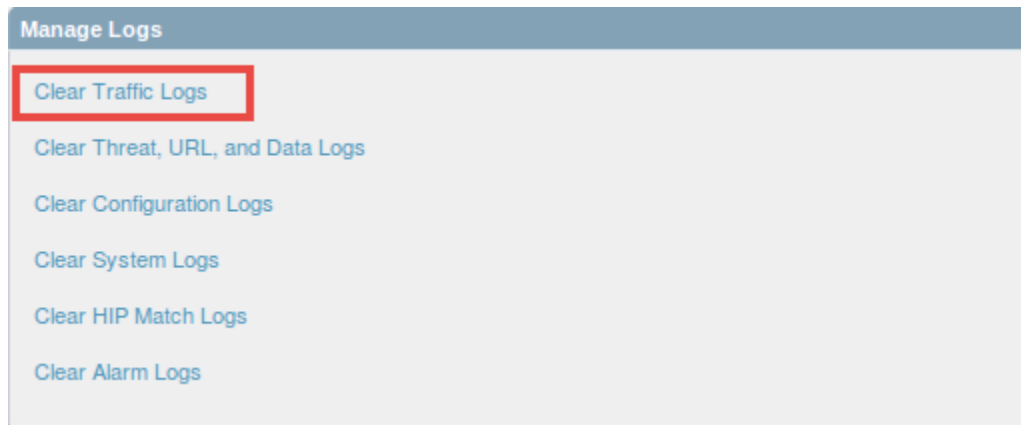
12. Leave the *Palo Alto WebUI* open for the next task.

## 2 Clear the Logs

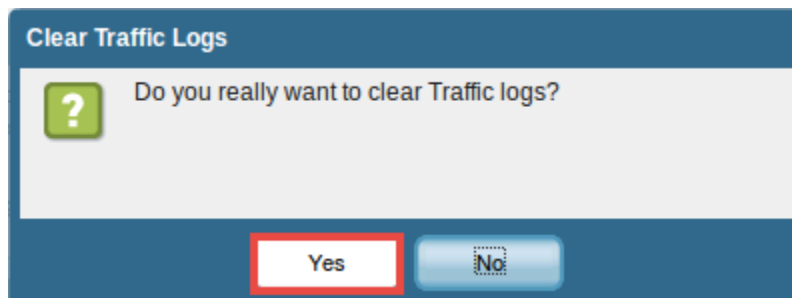
1. Using the *Palo Alto WebUI*, navigate to **Device > Log Settings**.



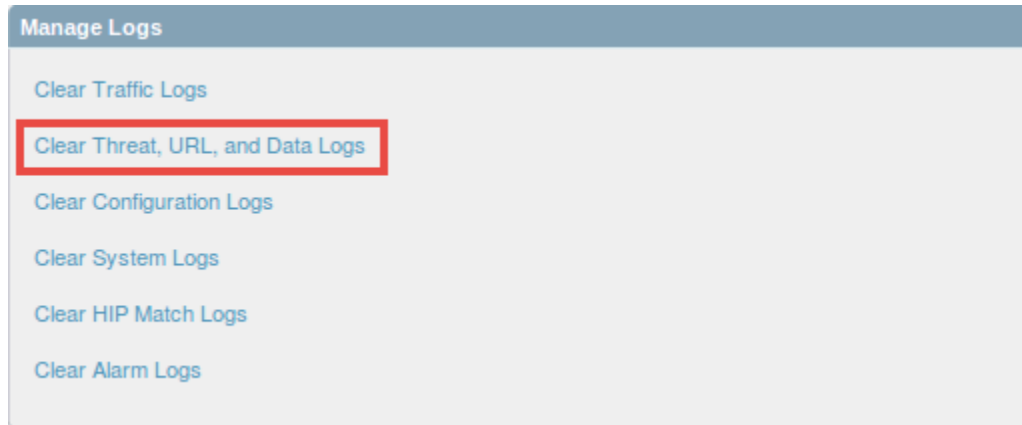
2. Under the *Manage Logs* section in the middle pane, click **Clear Traffic Logs**.



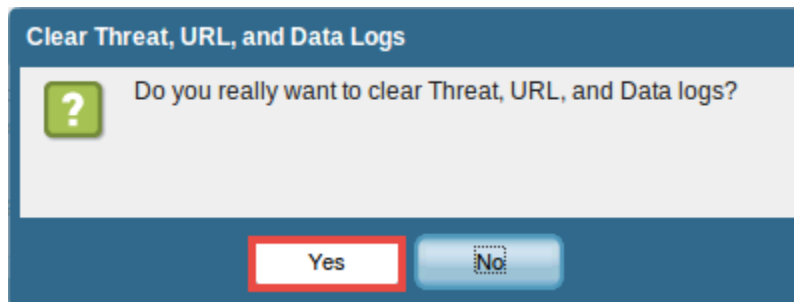
3. In the *Clear Traffic Logs* window, click **Yes**.



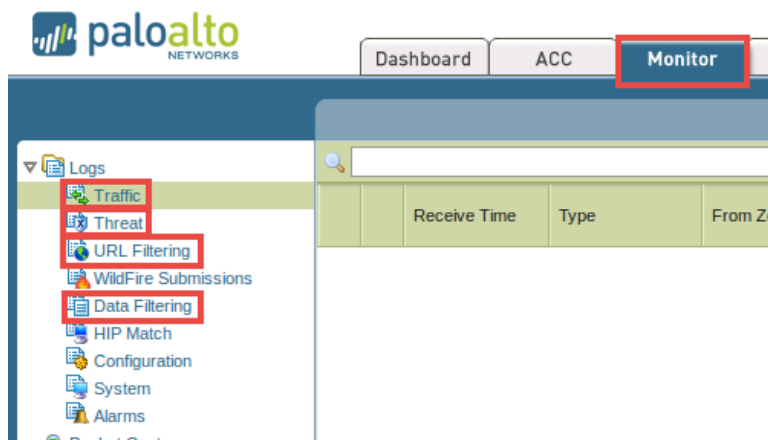
4. When prompted with a successful message indicating that the traffic logs have been deleted, click **OK** to continue.
5. While on the same page, underneath the *Manage Logs* section, click **Clear Threat, URL, and Data Logs**.



6. In the *Clear Threat, URL and Data Logs* window, click **Yes**.



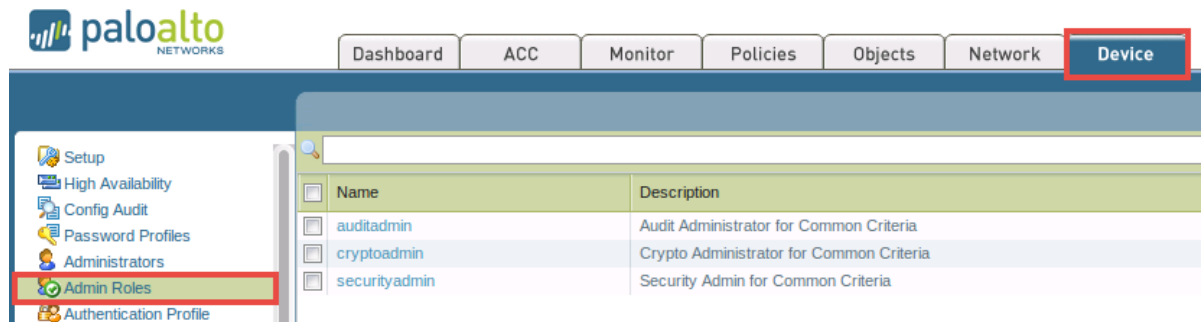
7. When prompted with a successful message indicating that the threat logs have been deleted, click **OK** to continue.
8. Navigate to **Monitor > Logs** and confirm that **Traffic, Threat, URL, and Data Filtering Logs** are empty.



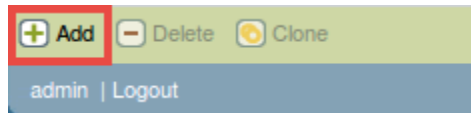
9. Leave the *Palo Alto WebUI* open for the next task.

### 3 Add an Administrator Role

1. Using the *Palo Alto WebUI*, navigate to **Device > Admin Roles**.



2. Click on **Add** located near the bottom of the web browser window to create a new administrator role.



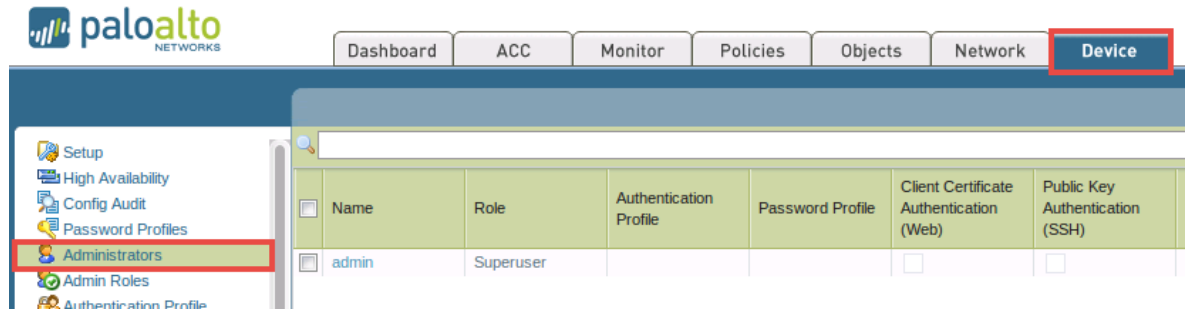
3. In the *Admin Role Profile* window, fill out the form using the information found in the table below:

Field	Data/Selection
Name	Enter <b>Policy Admins</b>
WebUI tab	<p>Click these major categories to disable them:</p> <ul style="list-style-type: none"> <li>• <b>Monitor</b></li> <li>• <b>Network</b></li> <li>• <b>Device</b></li> <li>• <b>Privacy</b></li> </ul> <p>The remaining major categories, <b>Dashboard</b>, <b>ACC</b>, <b>Policies</b>, <b>Objects</b>, <b>Validate</b>, <b>Commit</b>, and <b>Global</b> should remain enabled</p>
XML API tab	Verify that all the categories are disabled
Command Line tab	Keep the default of <b>None</b>

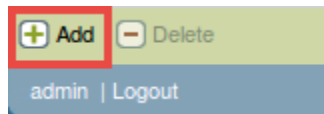
4. Click **OK** to continue.
5. Leave the *Palo Alto WebUI* open for the next task.

## 4 Add an Administrator Account

1. Using the *Palo Alto WebUI*, navigate to **Device > Administrators**.

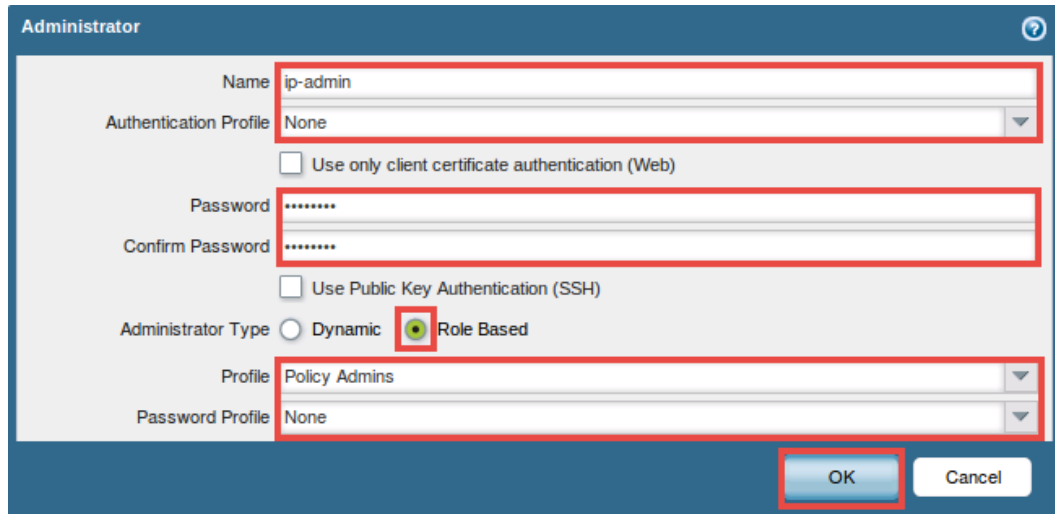


2. Click on **Add** located near the bottom of the web browser window to create a new administrator account.



3. In the *Administrator* window, configure a new administrator account by filling out the form using the information found in the table below:

Field	Data/Selection
Name	Enter <b>ip-admin</b>
Authentication Profile	Select <b>None</b>
Password/Confirm Password	Enter <b>paloalto</b>
Administrator Type	Select <b>Role Based</b>
Profile	Select <b>Policy Admins</b>
Password Profile	Select <b>None</b>



The image shows the 'Administrator' configuration window in the Palo Alto WebUI. The window has a blue header with the title 'Administrator' and a help icon. The main area contains several fields and options:

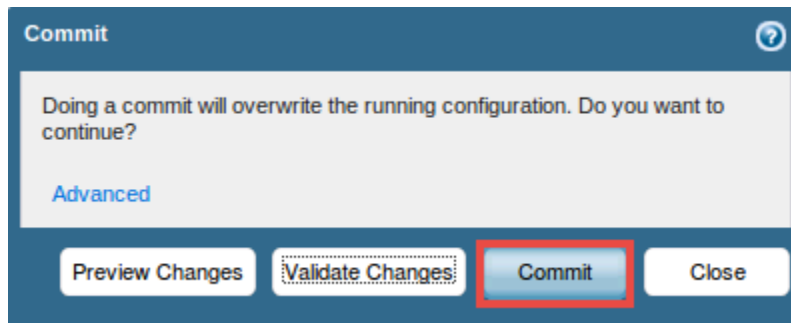
- Name:** A text field containing 'ip-admin'.
- Authentication Profile:** A dropdown menu set to 'None'.
- Use only client certificate authentication (Web):** An unchecked checkbox.
- Password:** A text field with masked characters (dots).
- Confirm Password:** A text field with masked characters (dots).
- Use Public Key Authentication (SSH):** An unchecked checkbox.
- Administrator Type:** Two radio buttons: 'Dynamic' (unchecked) and 'Role Based' (checked).
- Profile:** A dropdown menu set to 'Policy Admins'.
- Password Profile:** A dropdown menu set to 'None'.

At the bottom right, there are two buttons: 'OK' and 'Cancel'. The 'OK' button is highlighted with a red box.

4. Click **OK** to continue.
5. Click on the **Commit** link located at the top-right of the *WebUI*.



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



The image shows the 'Commit' confirmation window in the Palo Alto WebUI. The window has a blue header with the title 'Commit' and a help icon. The main area contains a message: 'Doing a commit will overwrite the running configuration. Do you want to continue?'. Below the message is a link labeled 'Advanced'. At the bottom, there are four buttons: 'Preview Changes', 'Validate Changes', 'Commit', and 'Close'. The 'Commit' button is highlighted with a red box.

7. Once the operation successfully completes, click **Close** to continue.
8. Minimize the *Palo Alto WebUI* for the next task.

## 5 Test the ip-admin User

1. While on the *Desktop 1* VM, open a new terminal window by clicking on the **Terminal** icon located in the lower-left corner.



2. Using the terminal, open an SSH connection to the firewall by typing the command below followed by pressing the **Enter** key.

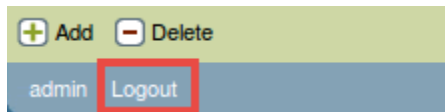
```
ssh ip-admin@192.168.10.1
```

3. When prompted for a password, enter `pa1oa1to`. Press **Enter**.

```
sysadmin@lubuntu:~$ ssh ip-admin@192.168.10.1
Password:
Connection to 192.168.10.1 closed.
sysadmin@lubuntu:~$
```

Notice the system responds with a “connection closed”. This is because the *ip-admin* is configured with no CLI access.

4. Navigate back to the **Firefox** web browser.
5. Click on **Logout** located near the bottom of the window.



6. Log into the *WebUI* using `ip-admin` as the *username* and `pa1oa1to` as the *password*. Click **Login**.
7. Explore the available functionality of the *WebUI*. Stay logged in as *ip-admin* and continue to the next task.

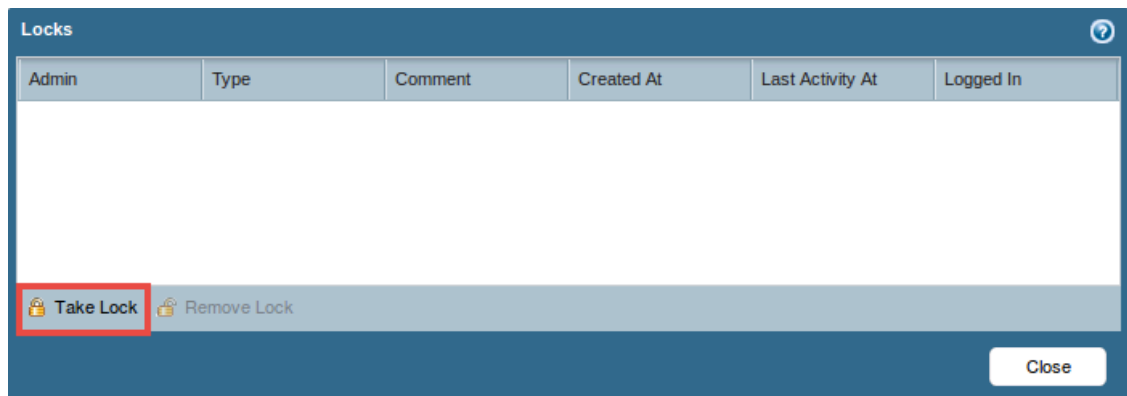
Notice that several tabs and functions are excluded from the interface. Also notice that there are tabs missing or not available to the *ip-admin* user when compared to the admin user. This is due to disabling the categories in the “Policy Admin” admin role that was created earlier.

## 6 Take a Transaction Lock and Test the Lock

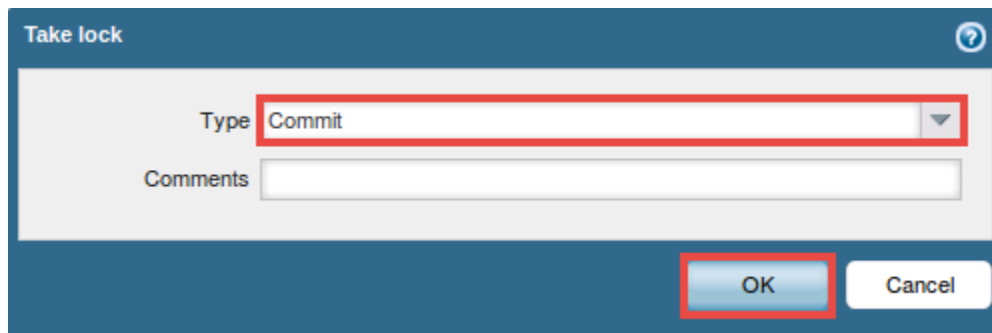
1. Using the *WebUI*, while logged in as *ip-admin*, click on the **Transaction Lock** icon located to the right of the *Commit* icon.



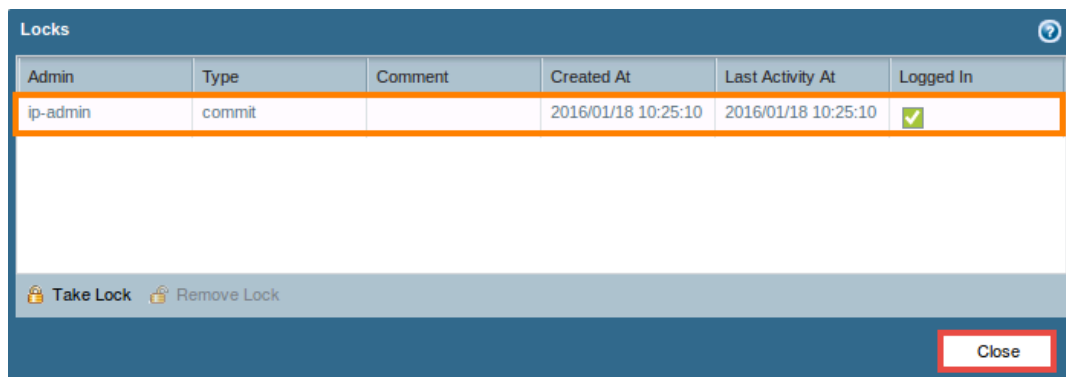
2. In the *Locks* window, click on the **Take Lock** icon.



3. In the *Take lock* window, set *Type* to **Commit** and then click **OK**.



4. Verify that the *ip-admin* lock is listed in the *Locks* window. Click **Close**.

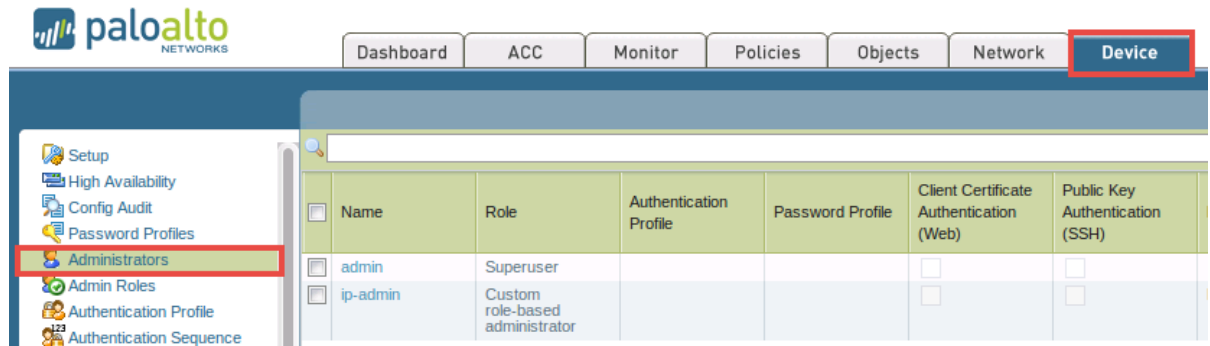




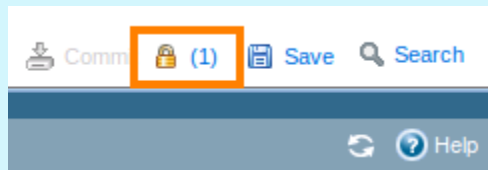
- Click on **Logout** located near the bottom of the window.



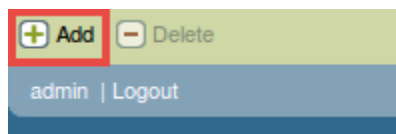
- Log back into the *WebUI* using **admin** as the *username* and **paloalto** as the *password*. Click **Login**.
- Navigate to **Device > Administrators**.



Notice the lock in the upper-right corner of the *WebUI*.

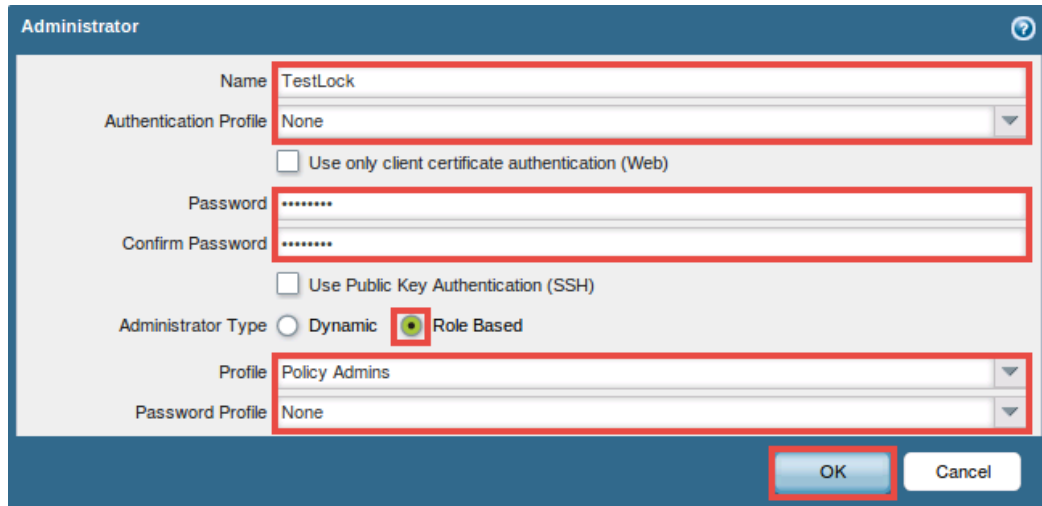


- Click on **Add**, located near the bottom of the window, to add another user.



9. In the *Administrator* window, configure a new administrator account by filling out the form using the information from the table below:

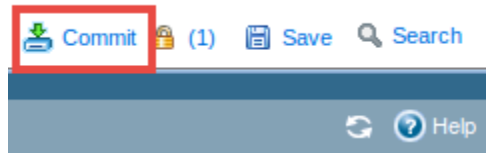
Field	Data/Selection
<i>Name</i>	Enter <b>TestLock</b>
<i>Authentication Profile</i>	Select <b>None</b>
<i>Password/Confirm Password</i>	Enter <b>paloalto</b>
<i>Administrator Type</i>	Select <b>Role Based</b>
<i>Profile</i>	Select <b>Policy Admins</b>
<i>Password Profile</i>	Select <b>None</b>



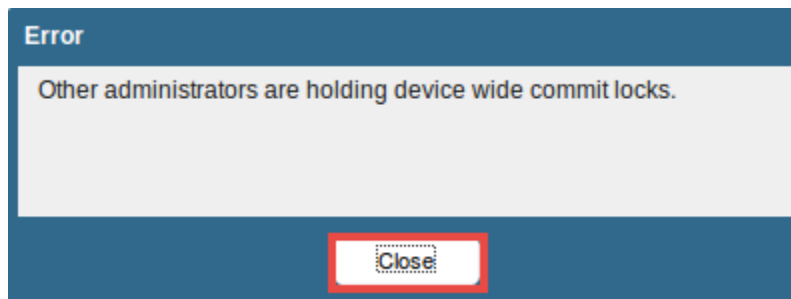
10. Click **OK**.  
 11. Verify that the new user is listed.

	Name	Role	Authentication Profile	Password Profile	Client Certificate Authentication (Web)	Public Key Authentication (SSH)	Profile	Locked User
<input type="checkbox"/>	admin	Superuser			<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	ip-admin	Custom role-based administrator			<input type="checkbox"/>	<input type="checkbox"/>	Policy Admins	
<input checked="" type="checkbox"/>	TestLock	Custom role-based administrator			<input type="checkbox"/>	<input type="checkbox"/>	Policy Admins	

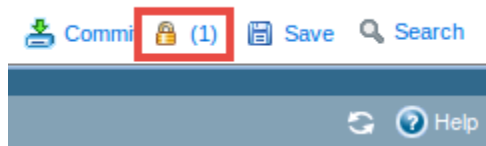
12. Click on **Commit**, located in the upper-right corner of the screen to commit the changes.



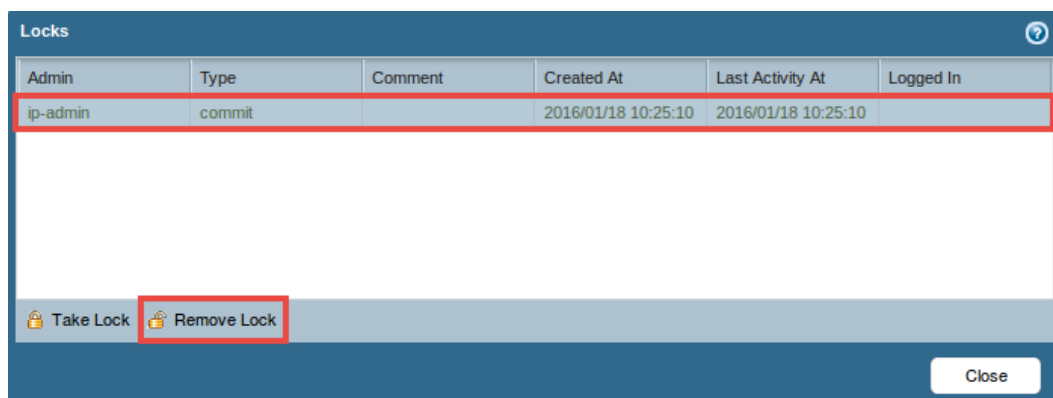
13. In the *Commit* window, click the **Commit** button.
14. Notice an *Error* message appears. The commit function has been disabled for this user because of the lock set by the *ip-admin* user. Click **Close** to continue.



15. Click on the **Lock** icon in the upper-right corner, next to *Commit*.



16. In the *Locks* window, select **ip-admin** from the list and click **Remove Lock**.



17. When prompted to remove the lock for *ip-admin*, click **OK** to continue.
18. In the *Locks* window, click **Close**.
19. Notice the lock is now removed. You can now click on the commit button and you may perform a commit as you have done previously in the lab. Close the **Desktop 1** PC viewer.