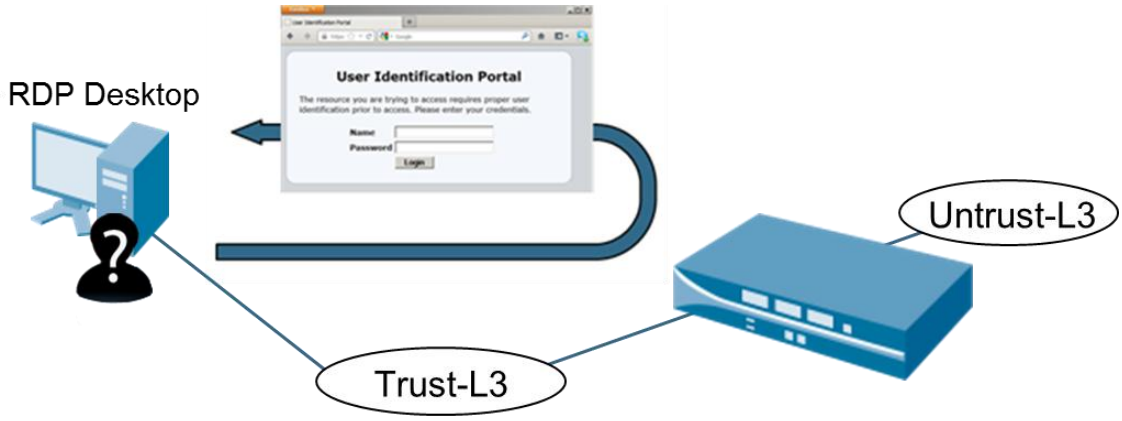
PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES

Lab 13: Advanced User-ID

Document Version: 2016-04-19

Contents

Introduction



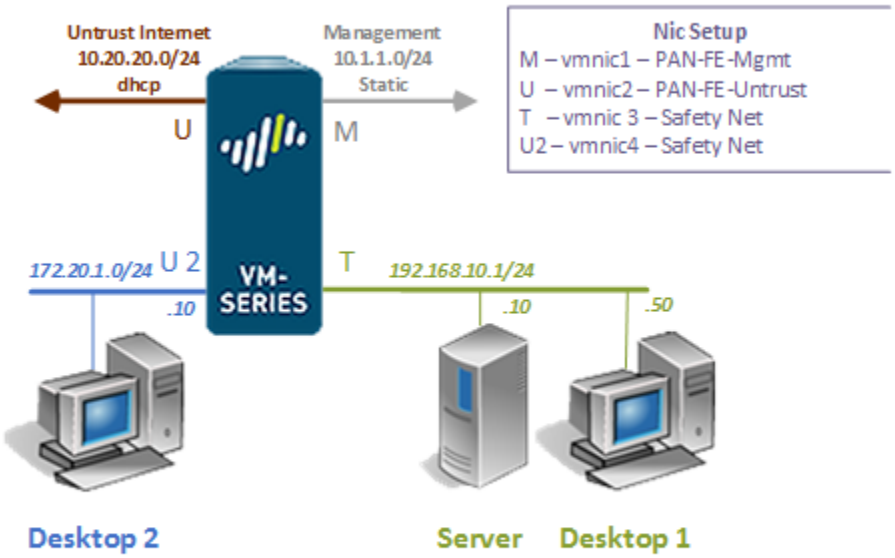
The company decides to allow Web traffic only for known users. Configure the environment to use captive portal based on these requirements. You are going to need to create user accounts, a new authentication profile and setup the captive portal.

Objective

In this lab, you will be utilizing Palo Alto technology to perform the following tasks:

1. Create local user database accounts
2. Create an Authentication Profile
3. Configure captive portal

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 Initial Firewall Configuration

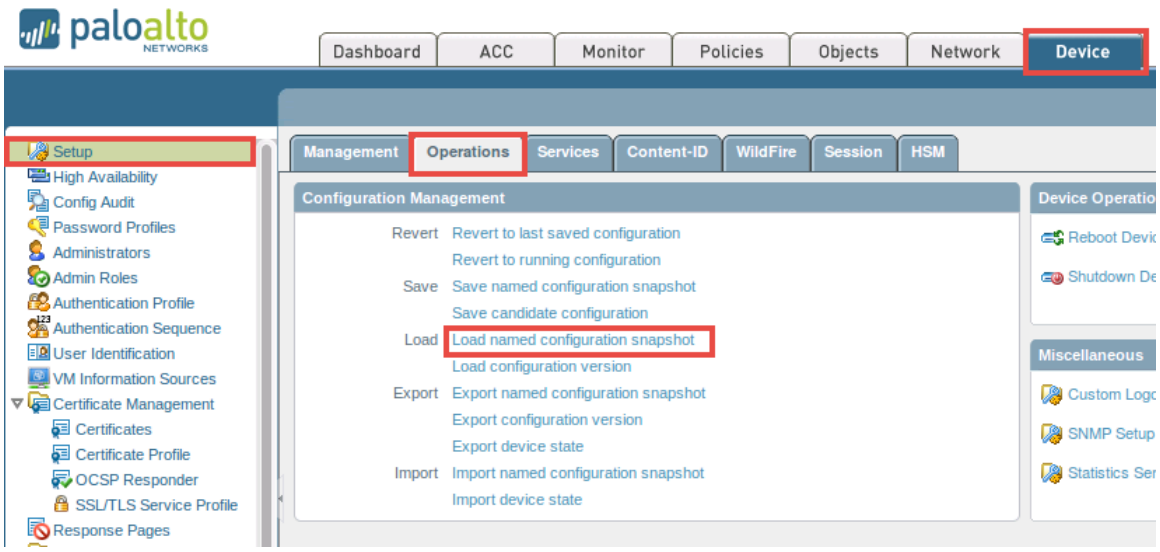
1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using `sysadmin` as the *username* and `Train1ng$` as the *password*. Click **Log In**.
3. Double-click on the **Firefox Web Browser** icon located on the *Desktop*.

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

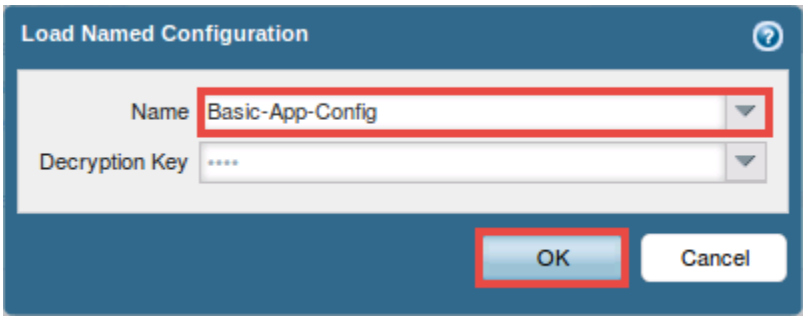
If you experience the "*Unable to connect*" message while attempting to connect to the specified IP above, please wait an additional 3-5 minutes for the PA VM to fully initialize and refresh the page to continue.

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

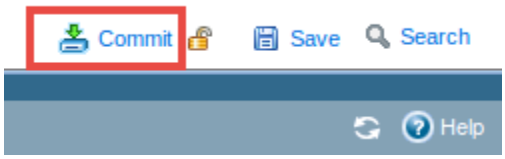
6. Using the *Palo Alto WebUI*, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



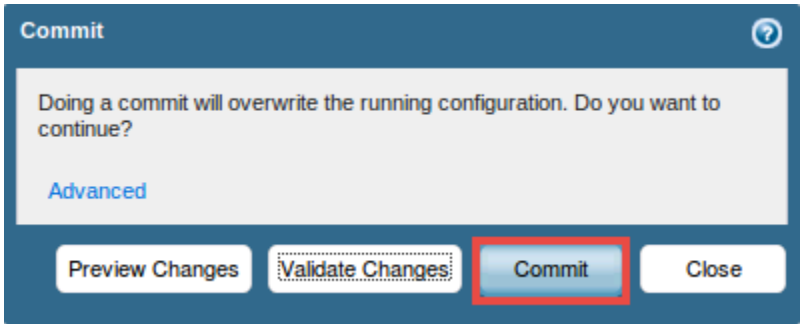
7. In the *Load Named Configuration* window, select **Basic-App-Config** from the *Name* drop-down box. Click **OK**.



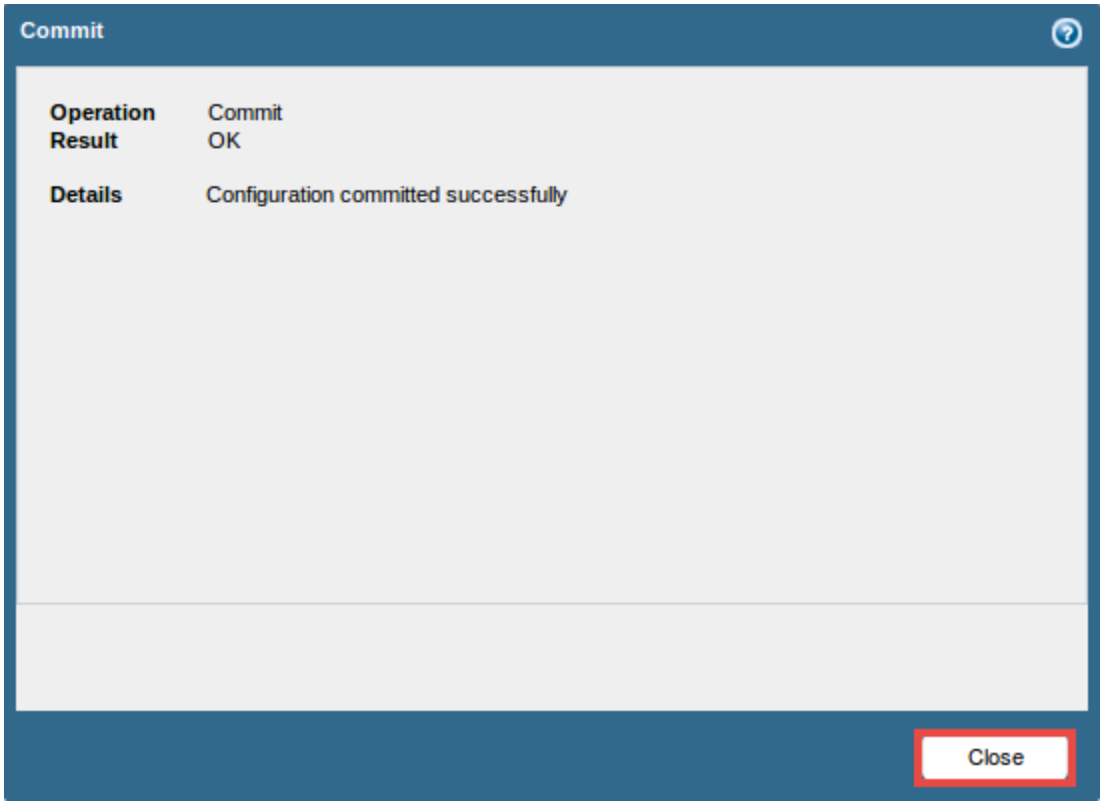
8. When prompted with the config loaded message, click on the **Close** button to continue.
9. Click on the **Commit** link located at the top-right of the *WebUI*.



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



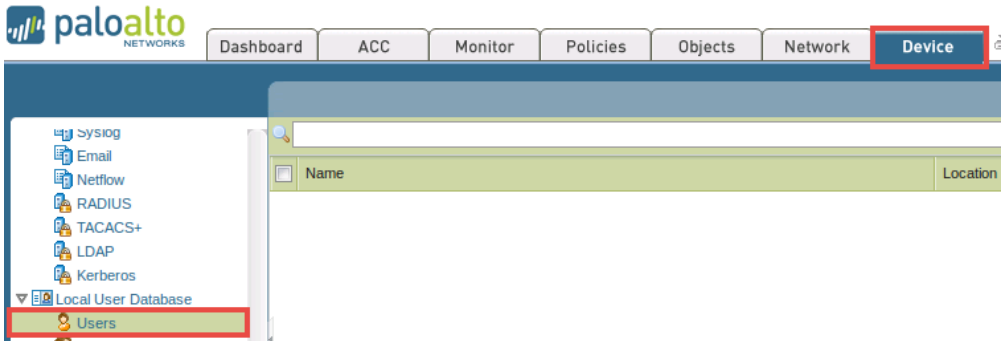
11. Once the operation successfully completes, click **Close** to continue.



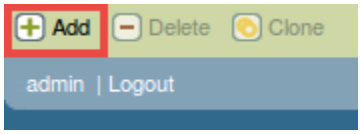
12. Leave the *WebUI* opened to continue with the next task.

2 Create Local User Database Accounts

1. Using the *WebUI*, navigate to **Device > Local User Database > Users**.

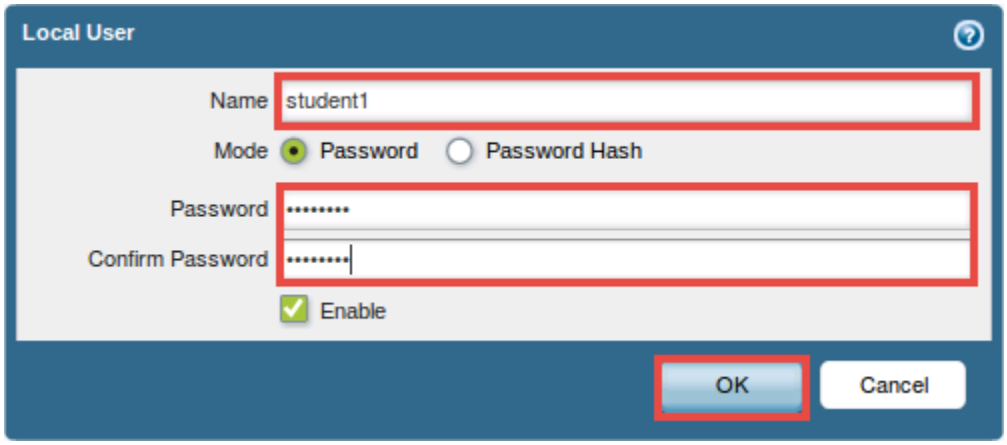


2. Click on **Add**, located near the bottom of the window, to create a new user.



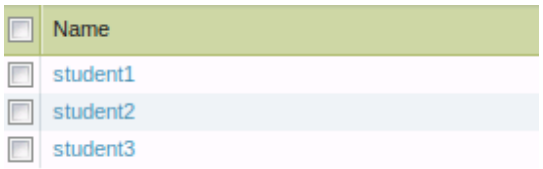
3. In the *Local User* window, use the information from the table below to make the appropriate user configurations.

Field	Data/Selection
Name	**student1**
Password	**paloalto**
Confirm Password	**paloalto**

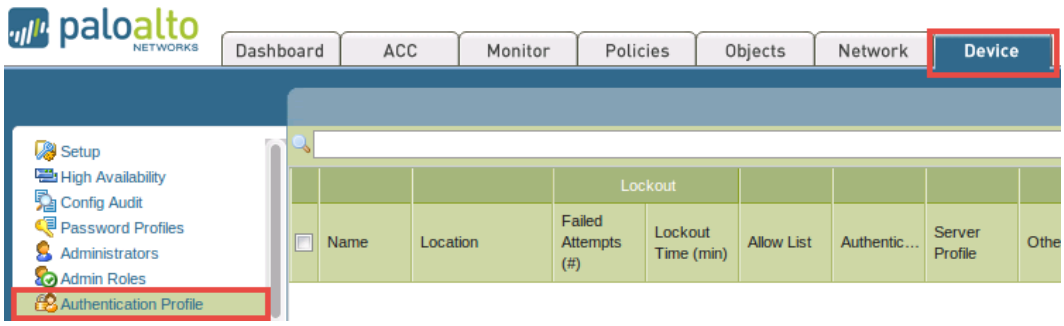


4. Click **OK** to save the user.

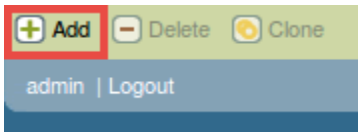
5. Repeat **Steps 2-4** to create two more users, **student2** and **student3**. Use the same password.



6. Using the *WebUI*, navigate to **Device > Authentication Profile**.

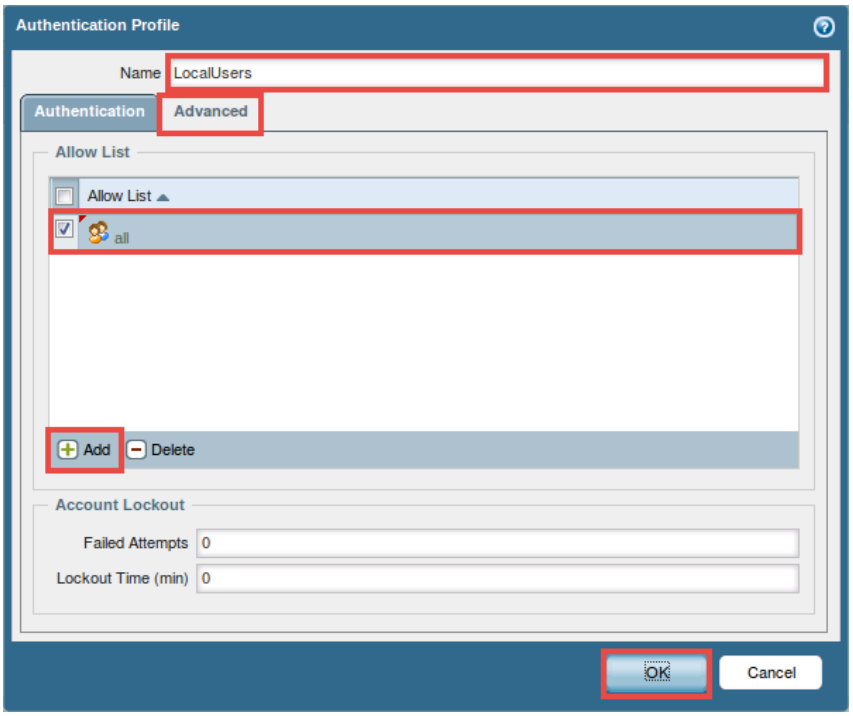


7. Click on **Add**, located near the bottom of the window, to create the authentication profile.



8. In the *Authentication Profile* window, type `LocalUsers` in the *Name* field.

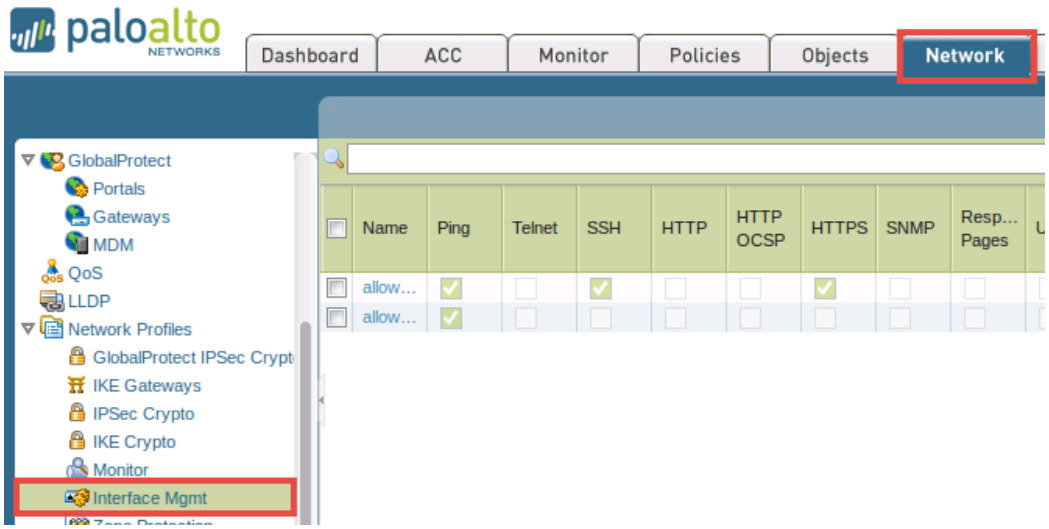
9. In the *Authentication Profile* window, click on the **Advanced** tab followed by clicking on the **Add** button. Select **all** from the menu.



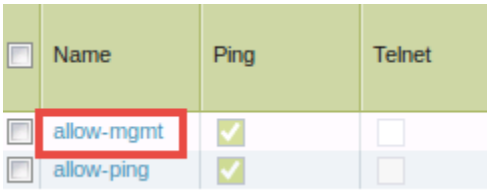
10. Click **OK** to save the configurations.
11. Leave the *WebUI* opened to continue with the next task.

3 Prepare the Firewall for Captive Portal

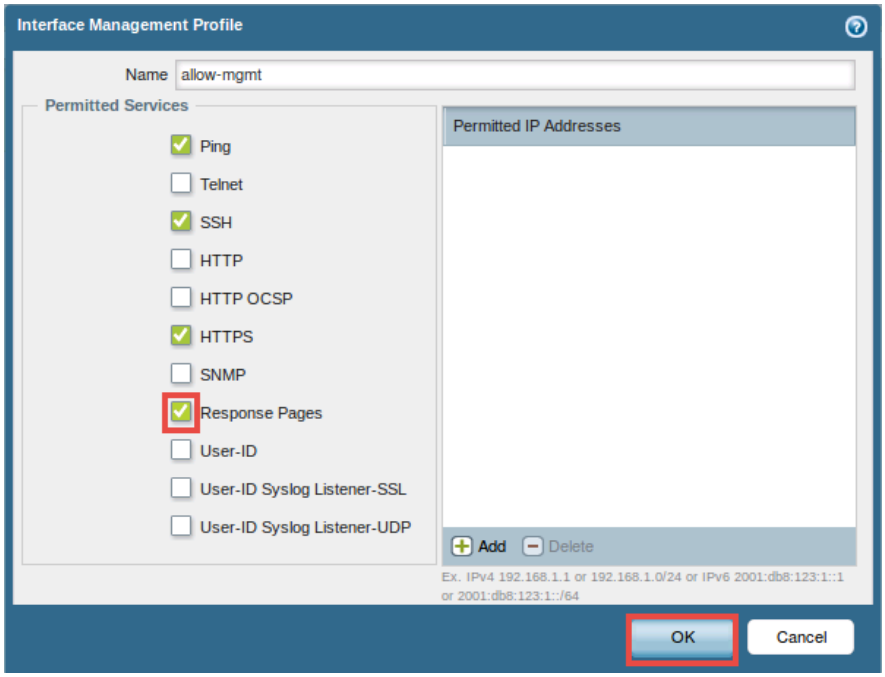
1. Using the *WebUI*, navigate to **Network > Network Profiles > Interface Mgmt**.



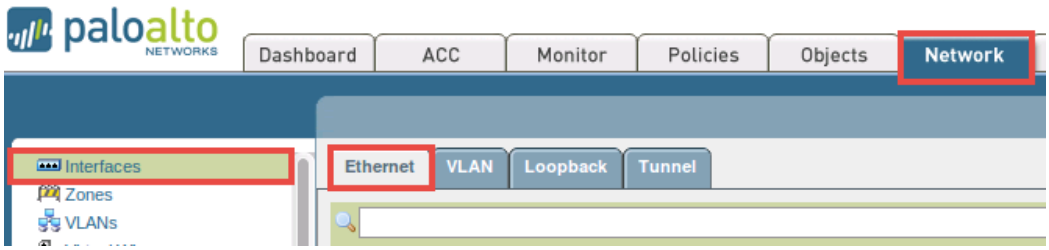
2. Click on **allow-mgmt** from the list, underneath the *Name* column.



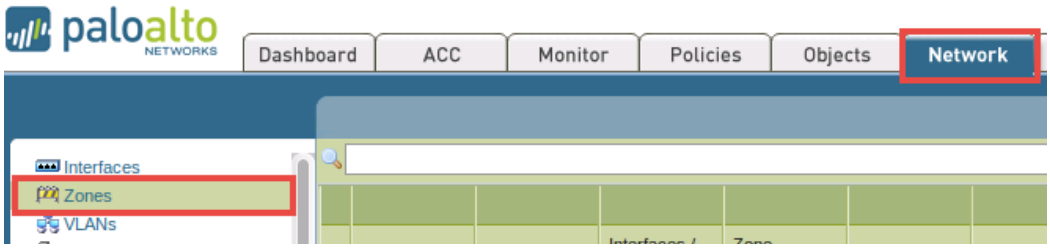
3. In the *Interface Management Profile* window, check the box for **Response Pages**.



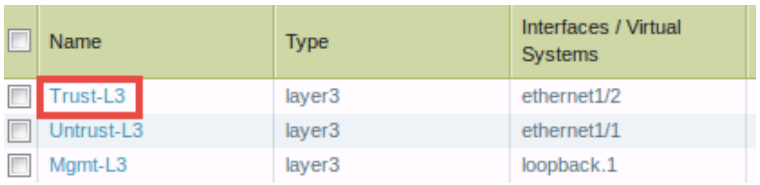
4. Click **OK** to save changes.
5. Using the *WebUI*, navigate to **Network > Interfaces > Ethernet**.



6. Verify that *ethernet1/2* is assigned to the **allow-mgmt** profile, underneath the *Management Profile* column.
7. Using the *WebUI*, navigate to **Network > Zones**.

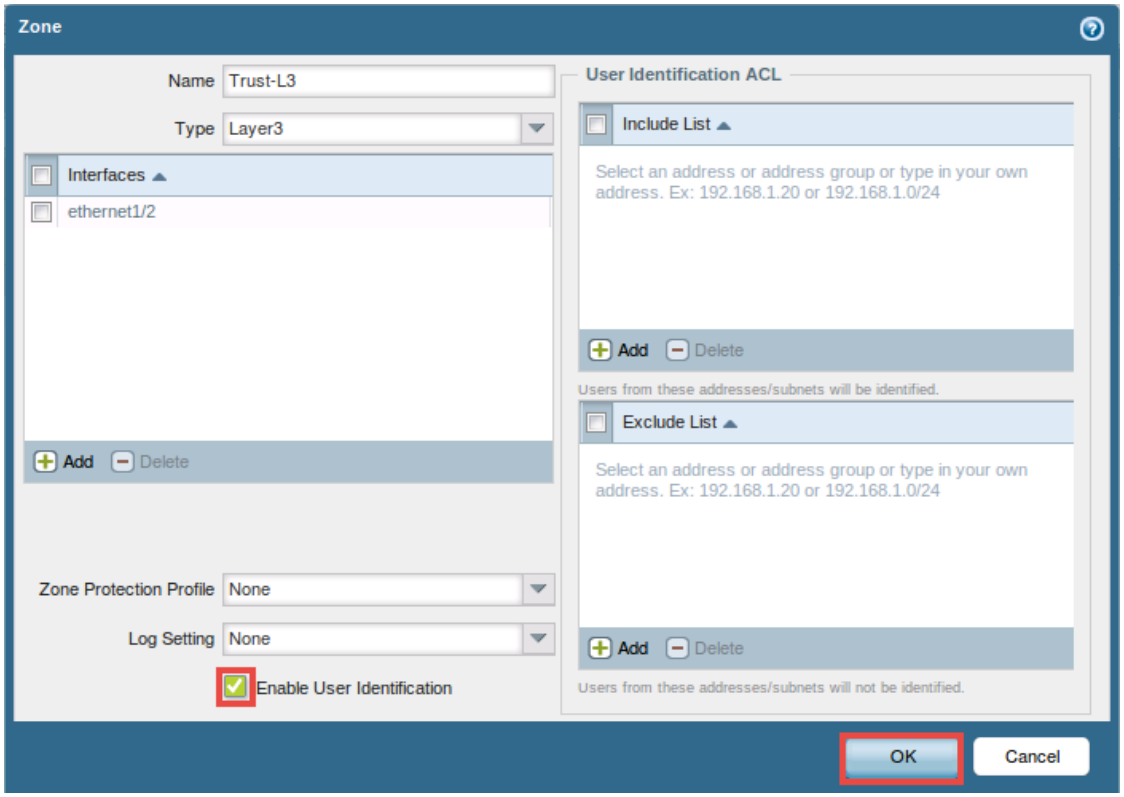


8. Click on **Trust-L3** link, underneath the *Name* column.



Name	Type	Interfaces / Virtual Systems
Trust-L3	layer3	ethernet1/2
Untrust-L3	layer3	ethernet1/1
Mgmt-L3	layer3	loopback.1

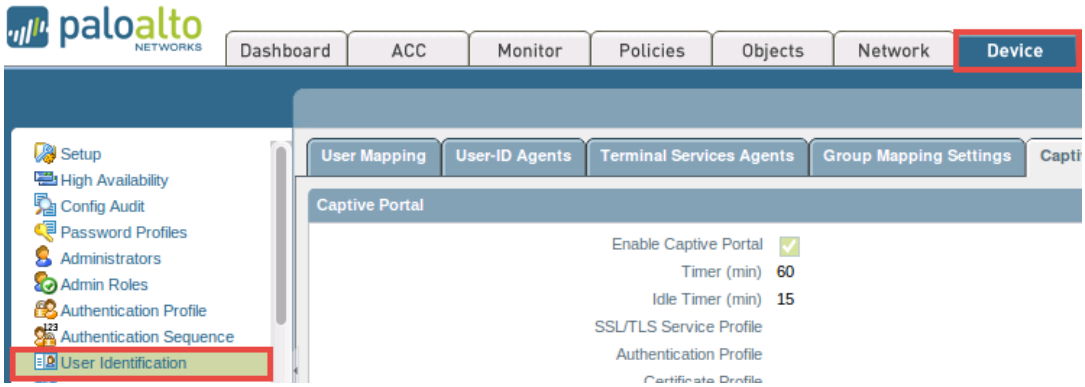
9. In the *Zone* window, check the box for **Enable User Identification**.



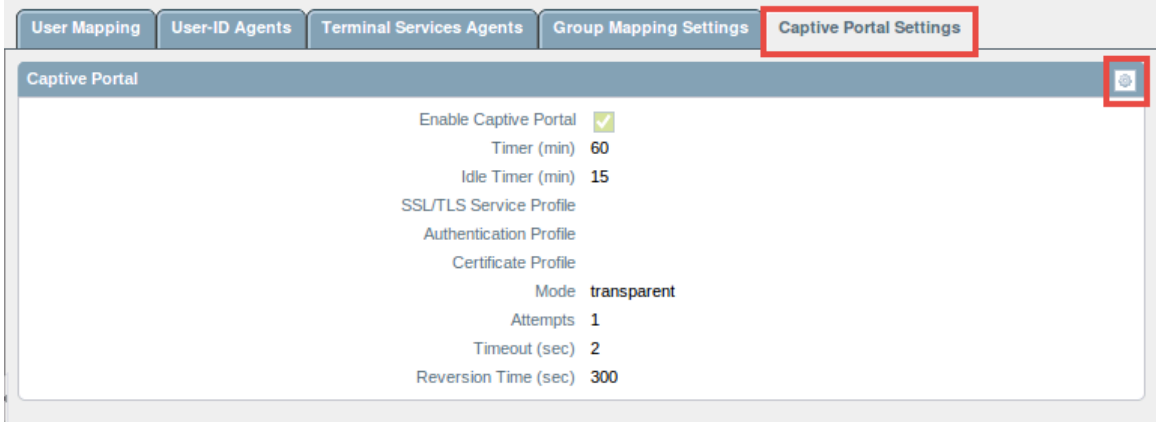
10. Click **OK** to save changes.
11. Leave the *WebUI* opened to continue with the next task.

4 Configure Captive Portal

1. Using the *WebUI*, navigate to **Device > User Identification**.

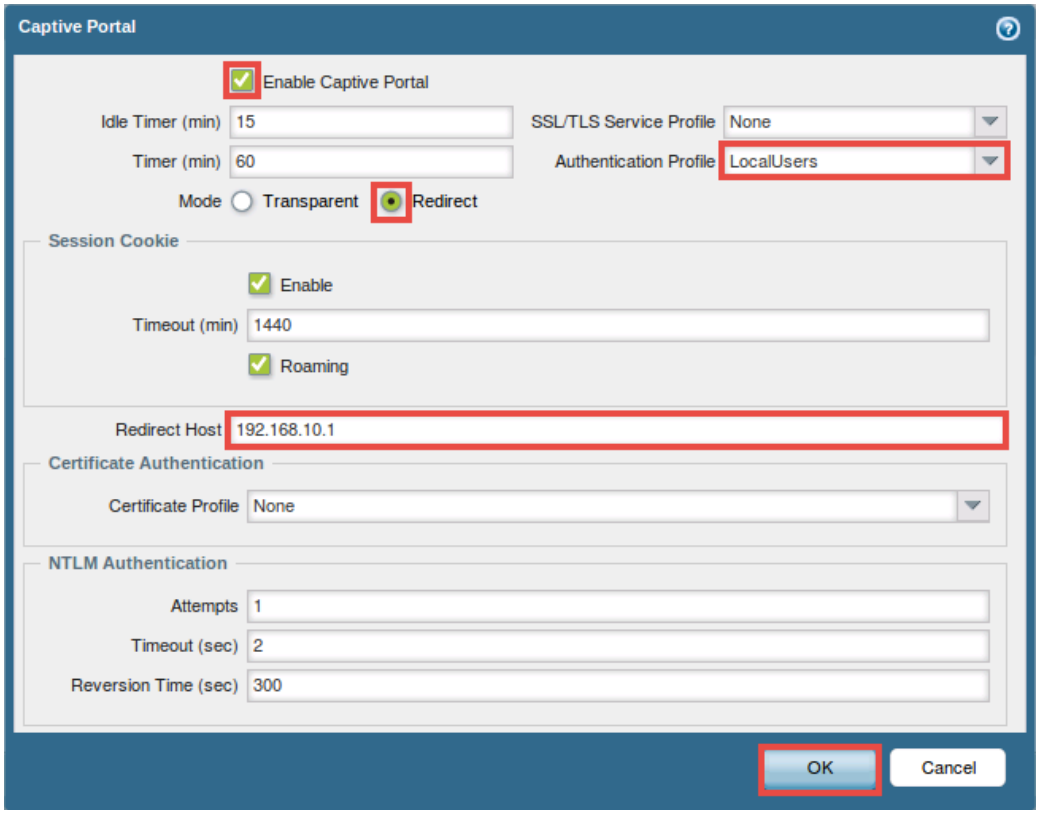


2. Click on the **Captive Portal Settings** tab.
3. Click on the **gear icon** in the upper right corner of the *Captive Portal* panel to configure a new captive portal.

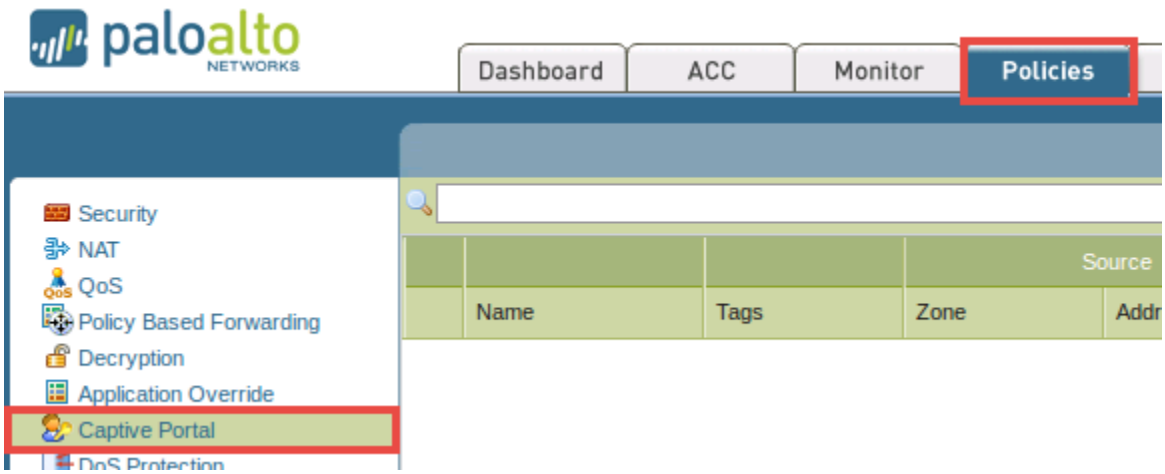


4. In the *Captive Portal* window, use the information from the table below to make the appropriate configurations.

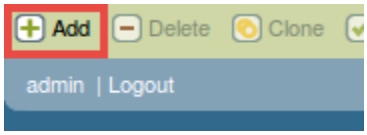
Field	Data/Selection
Enable Captive Portal	Check the box
Authentication Profile	Select **LocalUsers**
Mode	Select **Redirect**
Redirect Host	Enter **192.168.10.1**



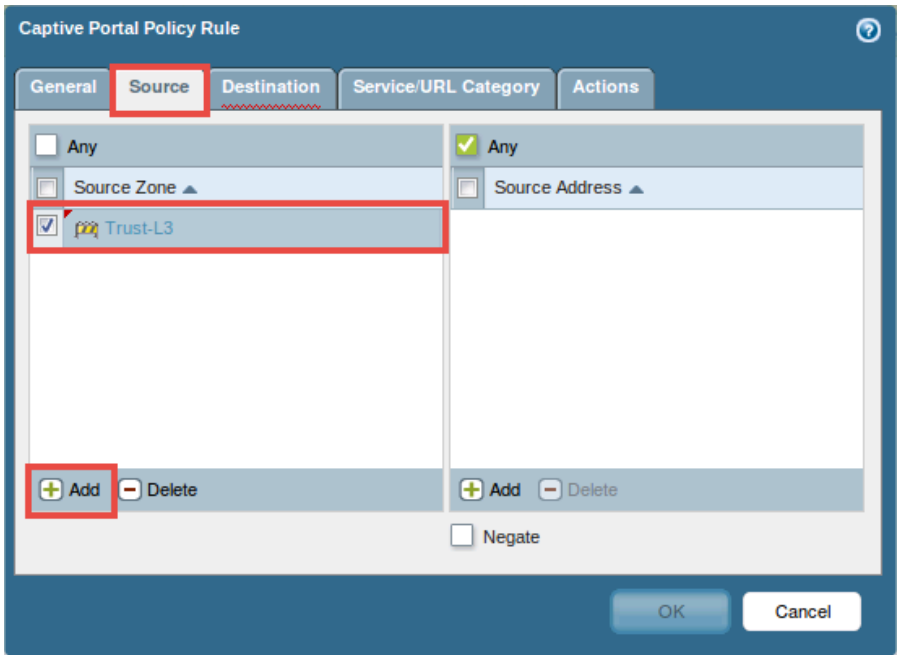
5. Click **OK** to save the configurations.
6. Using the *WebUI*, navigate to **Policies > Captive Portal**.



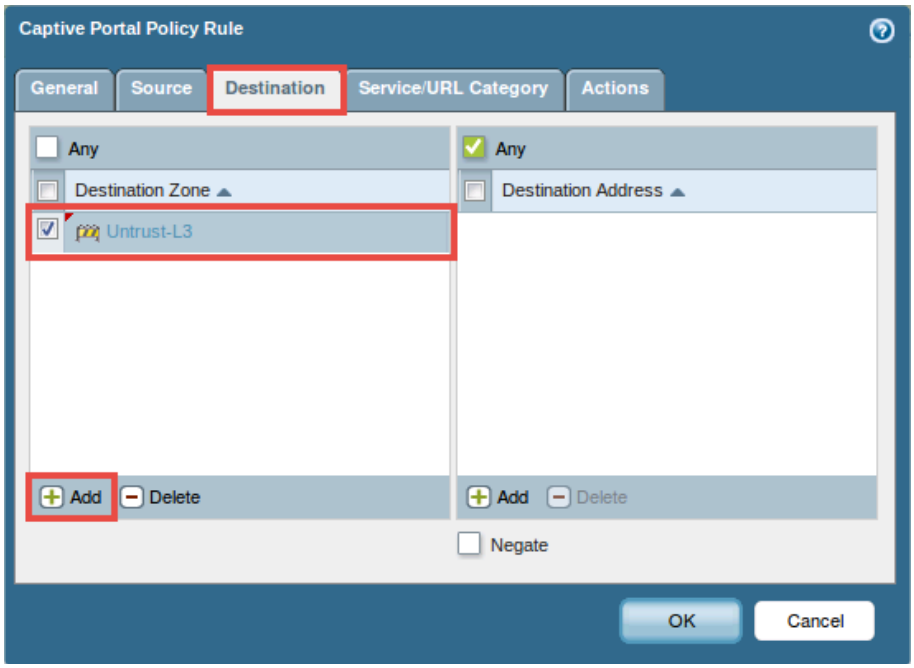
7. Click on **Add**, located near the bottom of the window, to create a new captive policy.



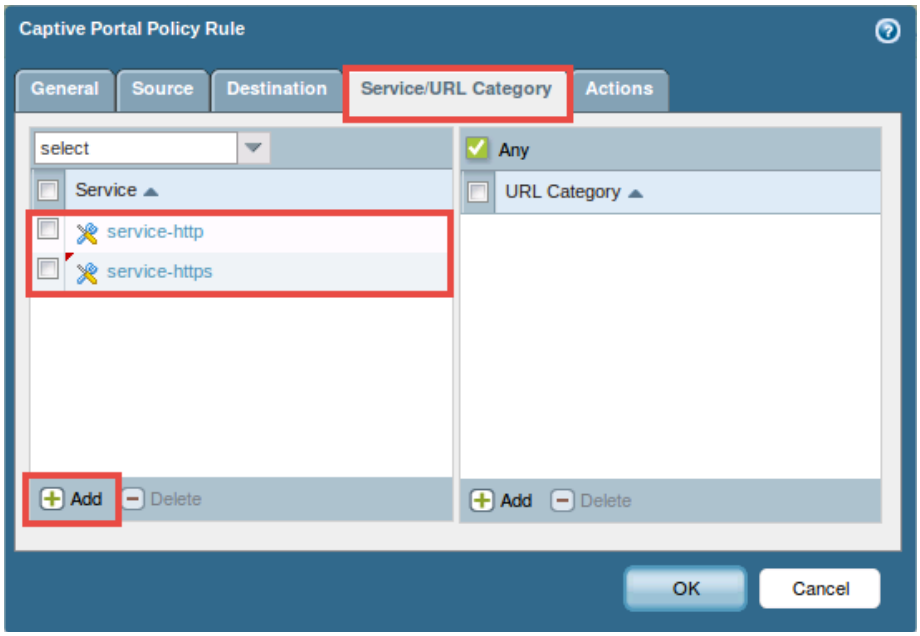
8. In the *Captive Portal Policy Rule* window, click on the **General** tab and enter `CP-Policy-1` into the *Name* field.
9. In the *Captive Portal Policy Rule* window, click on the **Source** tab and click **Add**, in the *Source Zone* pane followed by selecting the **Trust-L3** zone.



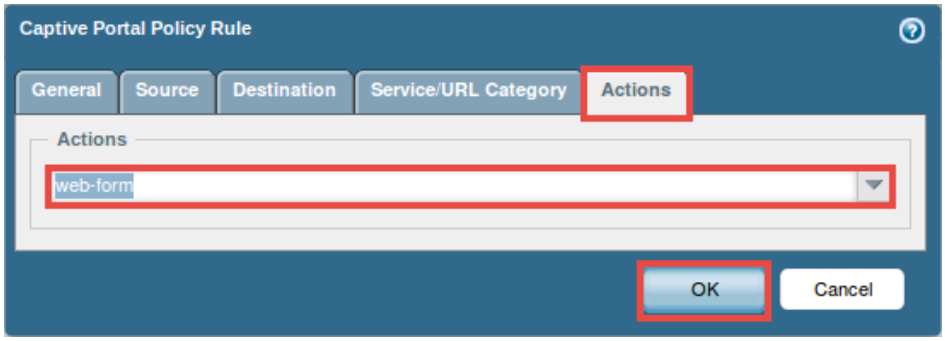
10. In the *Captive Portal Policy Rule* window, click on the **Destination** tab and click **Add**, in the *Destination Zone* pane followed by selecting the **Untrust-L3** zone.



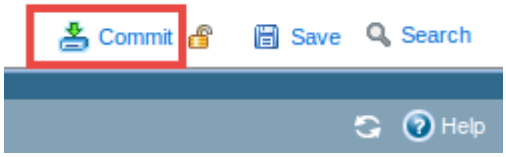
11. In the *Captive Portal Policy Rule* window, click on the **Service/URL Category** tab and click **Add**, in the *Service* pane followed by selecting **service-https** from the list. Verify that both *service-http* and *service-https* are both added in the *Service* pane.



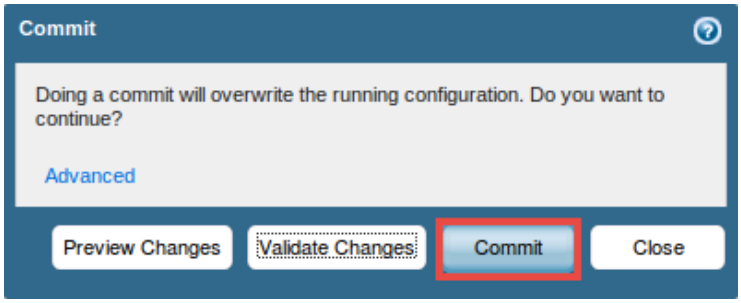
12. In the *Captive Portal Policy Rule* window, click on the **Actions** tab and select **web-form** from the *Actions* drop-down menu.



13. Click **OK** to save the configurations.
14. Click on the **Commit** link located at the top-right of the *WebUI*.



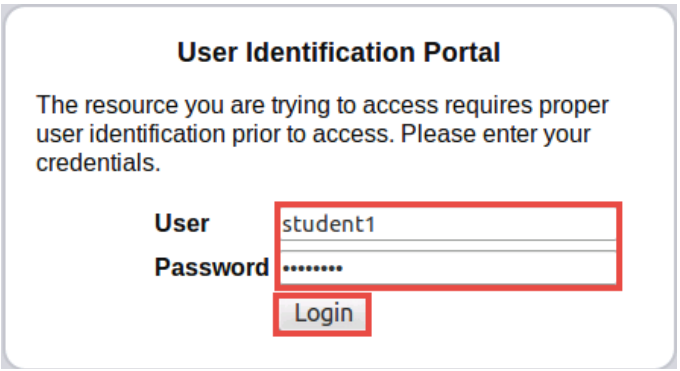
15. In the *Commit* window, click **Commit** to proceed with committing the changes.



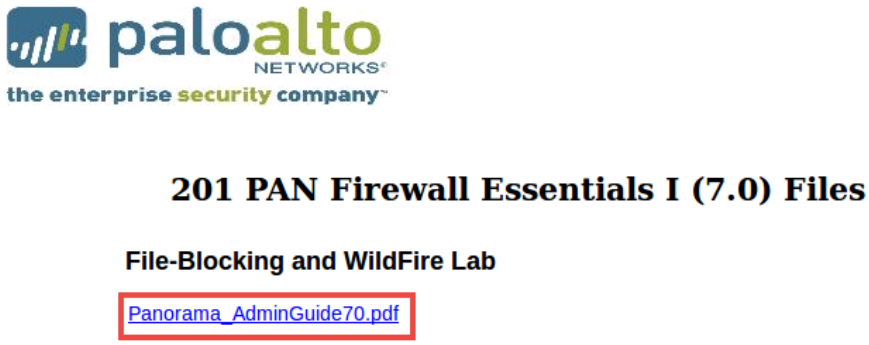
16. Once the operation successfully completes, click **Close** to continue.
17. Leave the *Firefox* web browser opened to continue with the next task.

5 Test Captive Portal

1. Using the *Firefox* web browser, open a **new tab**.
2. Type `http://www.panedufiles.com` into the address bar followed by pressing the **Enter** key.
3. Notice you are prompted with a *User Identification Portal*. Enter `student1` as the user and `paloalto` for the password. Click **Login**.



4. Once logged into the system, generate some traffic by clicking on the **Panorama_AdminGuide70.pdf** link, continuing with the download process saving the PDF to the *Downloads* directory.



5. Once downloaded, open a new terminal by clicking on the **LXTerminal** icon in the bottom pane.

6. In the terminal window, enter the command below.

```
ssh admin@192.168.10.1
```


7. When prompted for a password, enter **`paloalto`** followed by pressing the **Enter** key.

```
sysadmin@lubuntu:~$ ssh admin@192.168.10.1
Password:
Last login: Thu Mar  3 09:55:54 2016 from 10.20.20.253
Welcome admin.
admin@PA-VM>
```

8. Verify that the user identity was recorded by captive portal by entering the command below.

```
show user ip-user-mapping all
```

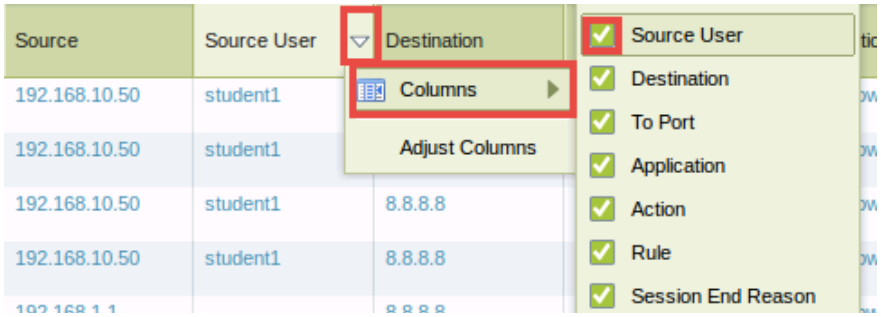
```
admin@PA-VM> show user ip-user-mapping all

IP              Vsys   From    User                            IdleTimeout(s) M
axTimeout(s)
--------------- ------ ------- ------------------------------- -------------- -
------------
192.168.10.50   vsys1  CP      student1                        896            3
171
Total: 1 users
```

9. Type **`exit`** to log out of the terminal.

```
admin@PA-VM> exit
Connection to 192.168.10.1 closed.
sysadmin@lubuntu:~$
```

10. Change focus to the **WebUI**.
11. Using the *WebUI*, navigate to **Monitor > Logs > Traffic**.

12. In the traffic logs output, verify that the **Source User** column is visible. If it isn't, hover the mouse over any column header and click the **downward arrow** icon. Make sure **Source User** is checked.



13. Notice that the source user, in this case *student1*, is identified for the web-browsing traffic generated from *Desktop 1*.
14. Close the **Desktop 1** PC viewer.

