



PCNSE

Panorama

Adding Bulk Firewalls

Step by Step Configuration Guide

Intellectual Property

*The Copyright in this work is vested in **Fortray Networks Limited** and the document is issued in confidence for the express purpose for which it is supplied. It must not be reproduced, in whole or in part, or be used for any other purpose without prior written consent being obtained from **Fortray Networks Limited**, and then only on the condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly therefrom shall be given orally or in writing or communicated in any manner whatsoever to any third party without the prior written consent of **Fortray Networks Limited**.*

© Copyright Fortray Networks Limited 2011-2020

Table of Contents

- 1. Fortray - Palo Alto - Version Control 4
- 2. Fortray - Palo Alto - Reference Document 4
- 3. Fortray - Palo Alto - Assumption 4
- 4. Fortray - Palo Alto - Network Topology..... 5
- 5. Fortray - Palo Alto - Notes About Task 6
- 6. Fortray - Palo Alto - Task: Adding Bulk Firewalls in Panorama 7
- 7. Fortray - Palo Alto - Configuration: Adding Bulk Firewalls in Panorama 8
 - 7.1. Step 1: Configuring Panorama Server on Each Firewall..... 8
 - 7.2. Step 2: Creating Palo Alto CVS File for Adding Bulk Firewalls..... 10
 - 7.3. Step 3: Adding Palo Alto Bulk Firewall to Panorama using CSV File 12
 - 7.4. Step 4: Committing Changes to Palo Alto Panorama..... 14
- 8. Fortray - Palo Alto - Verification..... 15
 - 8.1. Step 1: Verification using GUI 15

1. Fortray - Palo Alto - Version Control

Version	Date	Notes	Created By	Release
1.0	15/03/2018	Student Workbook for LAB	Mazhar Minhas	Draft
1.1	15/03/2018	Topology update	Mazhar Minhas	Initial Release
1.2	23/07/2020	Diagram and document redesign and Formatting	Farooq Zafar	Final Release

2. Fortray - Palo Alto - Reference Document

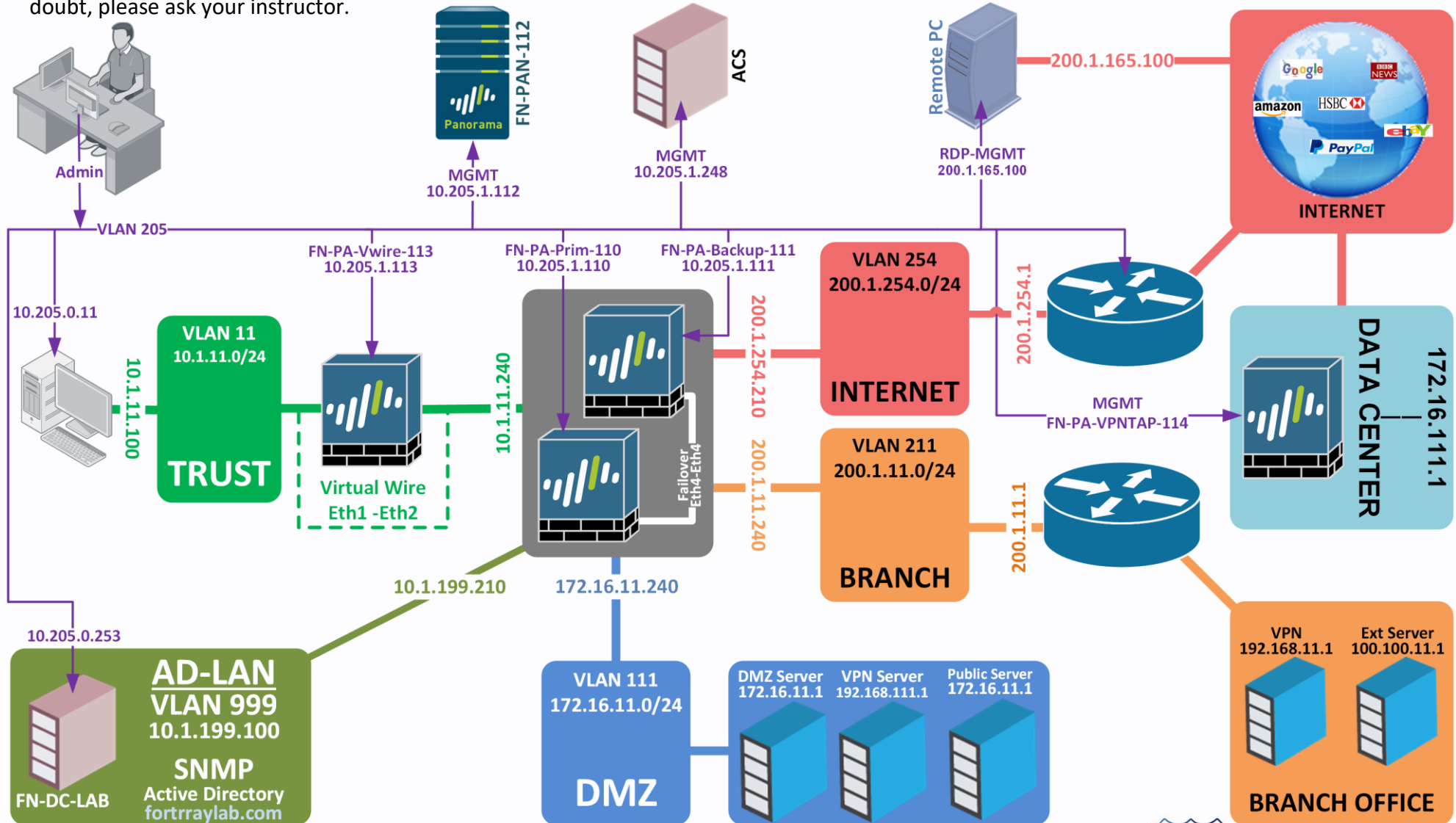
[Click for the Reference document](#)

3. Fortray - Palo Alto - Assumption

- ✓ We understand that delegate already understand L2/L3, Routing.
- ✓ The delegate already knows the "**Fortray Networks – Palo Alto Panorama**" physical and logical connection.
- ✓ The delegate already has a basis Troubleshooting skill, such as ping and trace.
- ✓ The delegate already has access to the "**Fortray Networks – Palo Alto Panorama**" *Spreadsheet encompassing the Basic Layer, 2, 3 and allocated subnet information. For more details refer to the "Student Folder".*
- ✓ This document is created to show an example for one topology only. The candidate needs to refer to his own topology and follow this step by step guide.
- ✓ We assume that delegate already has installed the VPN software and him/she have VPN user / Password. If any issue, contact our Technical team.
- ✓ Our VPN software is supported by PC, MAC, Android, and IOS devices.
- ✓ It's also assumed that delegate has access to PC/Laptop i5 with 4GB RAM.
- ✓ For optimal connectivity, we recommend at least 10MB internet connection.
- ✓ We assume that we already have INTERNAL, DMZ, OUTSIDE interfaces that are already configured.

4. Fortray - Palo Alto - Network Topology

The below network topology is just for information purpose only. Please refer to your student folder and your designated topology. If any doubt, please ask your instructor.








5. Fortray - Palo Alto - Notes About Task

Here we have Management Access details for Palo Alto firewalls and Panorama Installed in LAB.

Palo Alto Student Firewall Information								
Devcie Name	Role	Model	Version	PA-200 Serial no	MGMT IP	Default Credentials	New User	PASSWORD
FN-PA-PRIM-110	Primary	PA-200	8.1.0	001606067716	10.205.1.110	admin/admin	admin	Palo@123
FN-PA-BACK-111	Backup	PA-200	8.1.0	001606059502	10.205.1.111	admin/admin	admin	Palo@123
FN-Panorama-112	Panorama	VM	8.1.6		10.205.1.112	admin/admin	admin	Palo@123
PN-PA-VWVLAN-113	Virtual Wire + VLAN FW	PA-200	7.0.1	001606014209	10.205.1.113	admin/admin	admin	Palo@123
PN-PA-VPNTAP-114	VPN + TAP FW	PA-200	8.0.0	001606089665	10.205.1.114	admin/admin	admin	Palo@123

Workbook Shapes:

- ✓  Next Step Window
- ✓  Next Sub Steps Window
- ✓  Step Number
- ✓  Required Value
- ✓  Information / Verification



Please Do Not Change Password for admin account.

6. Fortray - Palo Alto - Task: Adding Bulk Firewalls in Panorama

Fortray Network Management noticed that the configuration on Palo Alto Firewalls is taking too long, Security engineer has to configure each Palo Alto Firewall Separately.



Fortray Network Security Team suggested to add all firewalls in Panorama and Managed all of them under one platform. In this task we will learn how to add Palo Alto Bulk Firewalls in Panorama.

Summary of the Configuration Steps:

- Configuring Panorama Server on Required Firewalls
- Creating Palo Alto CVS File for Adding Bulk Firewalls
- Adding Palo Alto Bulk Firewall to Panorama using CSV File
- Committing Changes to Palo Alto Panorama
- Verification

7. Fortray - Palo Alto - Configuration: Adding Bulk Firewalls in Panorama

In this section, we will add Palo Alto Bulk Firewalls in Panorama using CSV file.

7.1. Step 1: Configuring Panorama Server on Each Firewall

We need to add Panorama Server address in each firewall, which needs to be added in Panorama. In this section, we will add Panorama Server address in FN-PA-BACK-111 and PN-PA-VPNTAP-114. Login to **FN-PA-BACK-111** Firewall using Web GUI and follow these steps:

1. Click on **Device**
2. Click on **Setup**
3. Click on **Management**
4. Click on **Setting icon** of Panorama Settings.
5. Enter IP Address of Panorama Server in First Text Box
6. Click **OK** to complete.
7. **Commit**

The screenshot displays the Palo Alto Networks Web GUI. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The 'Device' tab is selected. The left sidebar shows a navigation menu with categories like Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, VM Information Sources, Certificate Management, Certificates, Certificate Profile, OCSP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusion, Response Pages, Log Settings, Server Profiles, SNMP Trap, and Syslog. The main content area shows the 'Panorama Settings' configuration page for device 'FN-PA-BACK-111'. A modal dialog box is open, allowing the user to enter the Panorama Server IP address (10.205.1.112) and other settings like timeouts and retry counts. The 'OK' button is highlighted.

Login to **PN-PA-VPNTAP-114** Firewall using Web GUI and follow these steps:

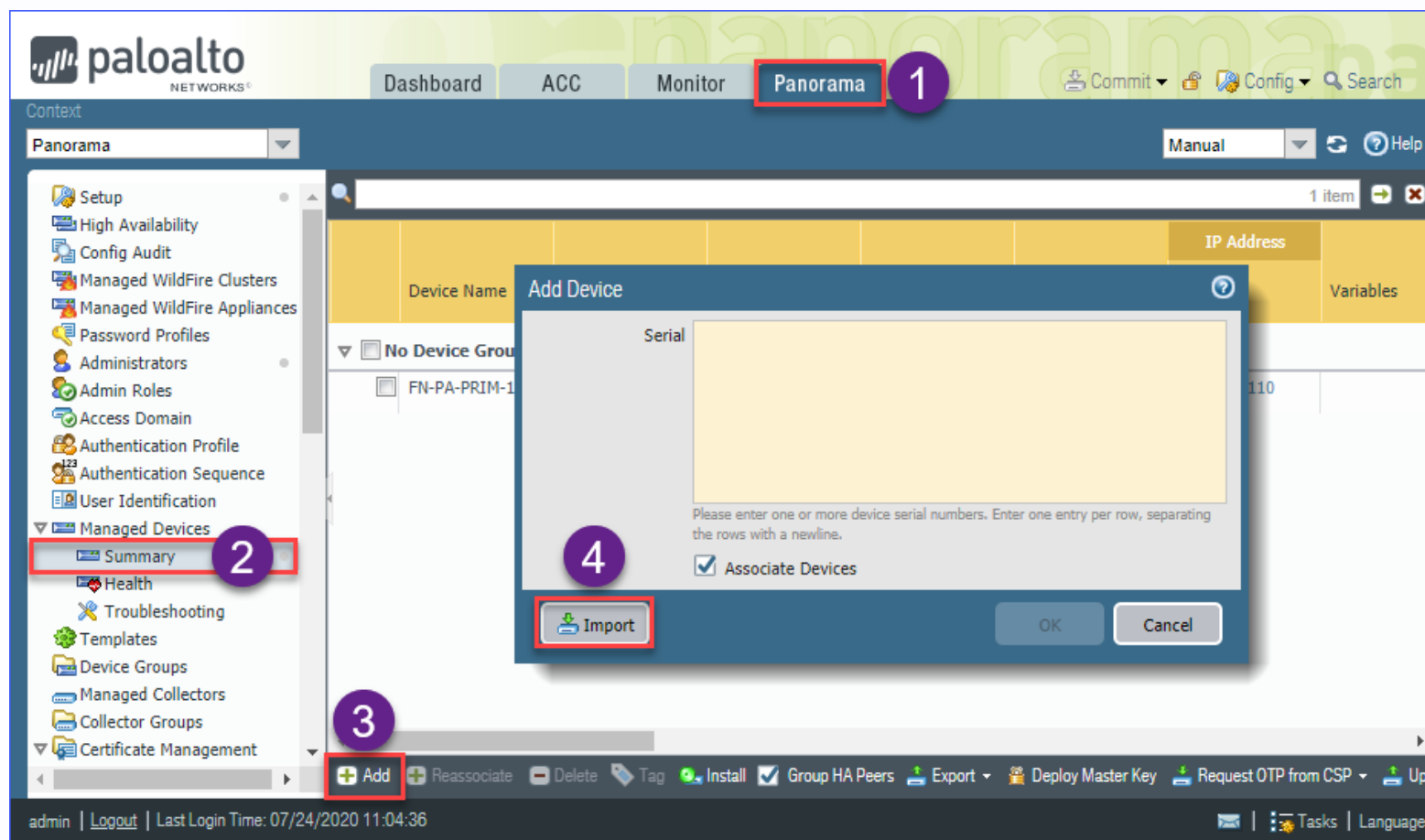
1. Click on **Device**
2. Click on **Setup**
3. Click on **Management**
4. Click on **Setting icon** of Panorama Settings.
5. Enter IP Address of Panorama Server in First Text Box
6. Click **OK** to complete.
7. **Commit**

The screenshot displays the Palo Alto Networks Web GUI. The top navigation bar shows 'Device' selected. The left navigation menu has 'Setup' selected. The main content area shows 'Management' selected, and the 'Panorama Settings' dialog box is open. The 'Panorama Servers' section has the IP address '10.205.1.112' entered in the first text box. The 'OK' button is highlighted.

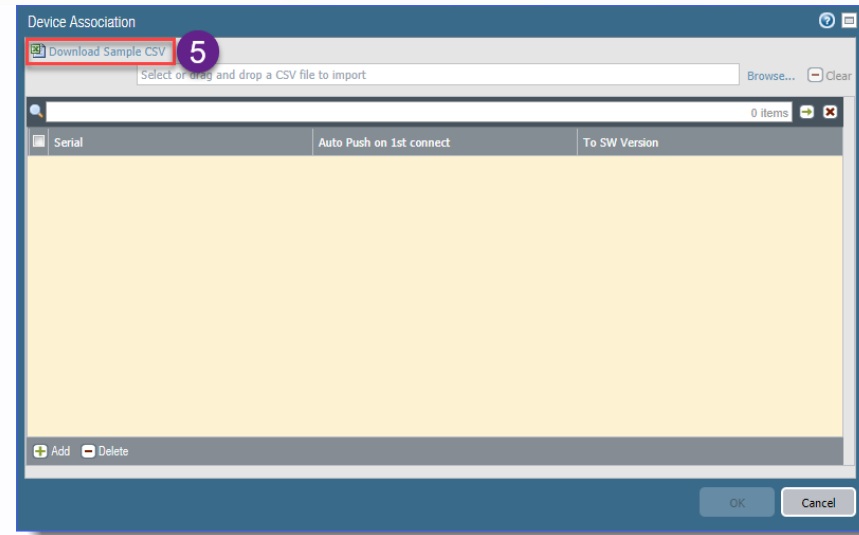
7.2. Step 2: Creating Palo Alto CVS File for Adding Bulk Firewalls

To create CVS file, we can download sample file by Login to Panorama and following these steps:

1. Click on **Panorama**
2. Click on **Managed Devices > Summary**
3. Click on **Add**
4. In new windows, Click on **Import**



5. Click on **Download Sample CSV**



6. Open CSV File in MS Excel or Notepad

	A	B	C	D	E	F
1	serial	device-group	template	collector-group	log-collector	auto-push-on-first-connect
2	AA11	devicegroup1	templatestack1	cg1	lc1-srno;lc2-srno	TRUE
3	BB22	devicegroup2	templatestack2	cg2	lc3-srno;lc4-srno	TRUE
4						
5						

7. Delete all Fields except required fields and adding a field **to-sw-version** which is required to add firewall. Fill all values in CSV File and Save the File.

	A	B	C	D
1	serial	auto-push-on-first-connect	to-sw-version	
2	001606059502	TRUE	8.1.0	
3	001606089665	TRUE	8.0.0	
4				
5				

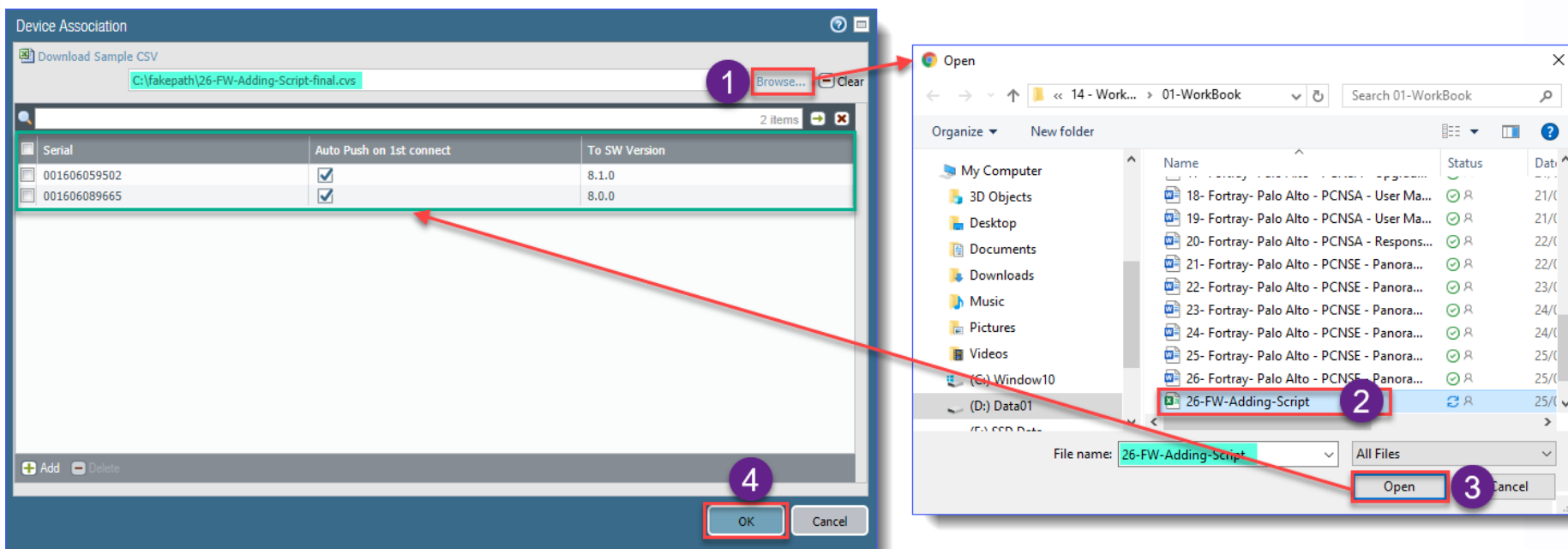


1. As MS Excel Remove leading Zeroes, format serial column as text.
2. Fill Firewall software Version in to-sw-version column.

7.3. Step 3: Adding Palo Alto Bulk Firewall to Panorama using CSV File

To add bulk Firewalls in Panorama using CSV Files, we need to follow these steps:

1. Click **Browse**
2. Select Saved CSV file in Previous File
3. Click **Open**, this will add list of Firewalls in this step
4. Click **OK**



After Pressing **OK** Button, all firewalls will be added in Panorama and status will be **Disconnected**.

Device Name	Virtual System	Model	Tags	Serial Number	IP Address		Variables	Template	Device State	Device C
					IPv4					
No Device Group Assigned (1/3 Devices Connected)										
<input type="checkbox"/> 001606059502				001606059502					Disconnected	
<input type="checkbox"/> FN-PA-PRIM-110		PA-200	Head-office-FW	001606067716	10.205.1.110				Connected	
<input type="checkbox"/> 001606089665				001606089665					Disconnected	

7.4. Step 4: Committing Changes to Palo Alto Panorama

Commit Changes to Panorama.

The screenshot displays the Palo Alto Networks Panorama web interface. The 'Panorama' tab is active, and the 'Commit' button in the top right corner is highlighted with a red box and the number '1'. A dropdown menu is open, showing 'Commit to Panorama' (highlighted with a red box and the number '2'), 'Push to Devices', and 'Commit and Push'. A 'Commit Status' dialog box is centered on the screen, showing the following details:

- Operation:** Commit
- Status:** Active
- Result:** Pending
- Progress:** 3% (indicated by a progress bar)
- Details:** (Empty)
- Warnings:** (Empty)

The dialog box has 'Cancel' and 'Close' buttons at the bottom. The background interface shows a sidebar with navigation options like Setup, High Availability, Config Audit, and Managed Devices. The main content area shows a table with columns for Template, Device State, and Device Certificate. The status bar at the bottom indicates the URL 'https://10.205.1.112/?#', the time '07/24/2020 02:37:13', and various system icons.

8. Fortray - Palo Alto - Verification

In this section, we will verify added Firewall's status.

8.1. Step 1: Verification using GUI

Click on **Panorama > Managed Devices > Summary**. Here, we can see newly added firewalls and their details.

The screenshot shows the Palo Alto Panorama GUI. The left sidebar contains a navigation menu with 'Managed Devices' expanded to 'Summary'. The main content area displays a table of managed devices. A red note box is overlaid on the table with the text: 'Note: If we don't see firewall's status as connected here, refresh current page.'

Device Name	Virtual System	Model	Tags	Serial Number	IP Address		Template	Device State	Device
					IPV4	Variables			
No Device Group Assigned (3/3 Devices Connected)									
<input checked="" type="checkbox"/> FN-PA-BACK-111		PA-200		001606059502	10.205.1.111			Connected	
<input type="checkbox"/> FN-PA-PRIM-110		PA-200	Head-office-FW	001606067716	10.205.1.110			Connected	
<input checked="" type="checkbox"/> FN-PA-VPNTAP-114		PA-200		001606089665	10.205.1.114			Connected	

Now, click on **Panorama > Device Deployment > Licenses**. Here we can see complete license detail of newly added firewall.

The screenshot shows the Palo Alto Networks Panorama interface. The navigation menu on the left has 'Licenses' highlighted with a red box and a purple circle containing the number 3. The main content area shows a table of license details for three devices. The table has the following columns: Device, Virtual System, Threat Prevention, URL, Support, GlobalProtect Gateway, GlobalProtect Portal, WildFire, VM-Series Capacity, AutoFocus, Logging Service, Decrypting Port Mirror, Decrypting Broker, DNS Security, and SD-WAN. The table contains three rows of data:

Device	Virtual System	Threat Prevention	URL	Support	GlobalProtect Gateway	GlobalProtect Portal	WildFire	VM-Series Capacity	AutoFocus	Logging Service	Decrypting Port Mirror	Decrypting Broker	DNS Security	SD-WAN
FN-PA-BACK-111	⊗	⚠ License Expired Expires: 4/4/2019	⚠ BrightClick License Expired Expires: 12/16/2018 ⚠ PaloAlto Networks License Expired Expires: 4/4/2019	⚠ License Expired Expires: 4/4/2019	⚠ License Expired Expires: 4/4/2019	✔	⚠ License Expired Expires: 4/4/2019	⊗	⊗	⊗	⊗	⊗	⊗	⊗
FN-PA-PRIM-110	⊗	✔ Expires: 9/13/20...	✔ PaloAlto Networks Expires: 9/13/2021	✔ Expires: 9/13/20...	✔ Expires: 9/13/20...	✔	✔ Expires: 9/13/20...	⊗	⊗	⊗	⊗	⊗	⊗	⊗
FN-PA-VPNTAP-114														

Thanks, and Good Luck

