

# INITIAL CONFIGURATION



EDU-210 Version A  
PAN-OS® 9.0

## *GET STARTED RIGHT*

---

- Administrative controls
- Initial system access
- Configuration management
- Licensing and software updates
- Account administration
- Viewing and filtering logs

# Agenda



After you complete this module, you should be able to:

- Connect to the firewall and log in as admin
- Configure the network settings for the management interface port
- Describe the difference between the running config and the candidate config
- Configure dynamic firewall updates to update the applications and threats databases
- Create a local firewall administrative account
- Access the firewall logs



## **Administrative controls**

**Initial system access**

**Configuration management**

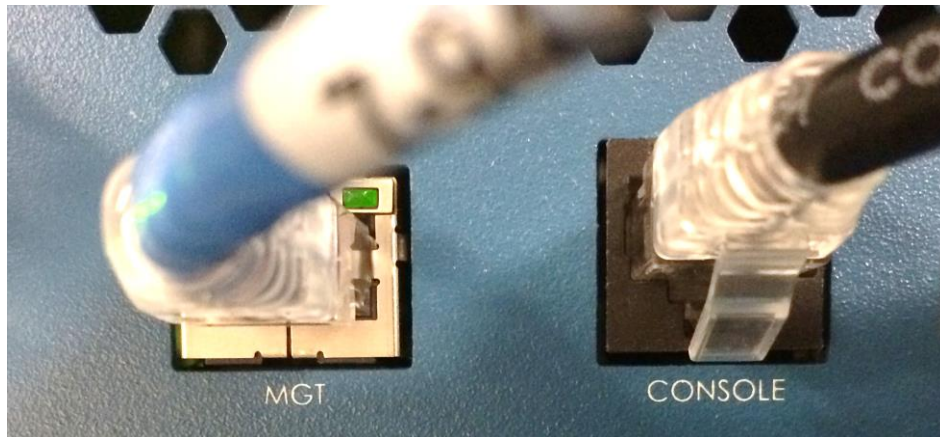
**Licensing and software updates**

**Account administration**

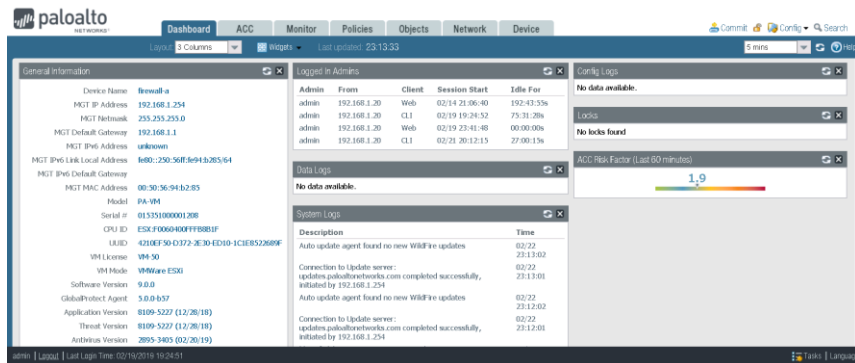
**Viewing and filtering logs**

# Initial Access to the Firewall

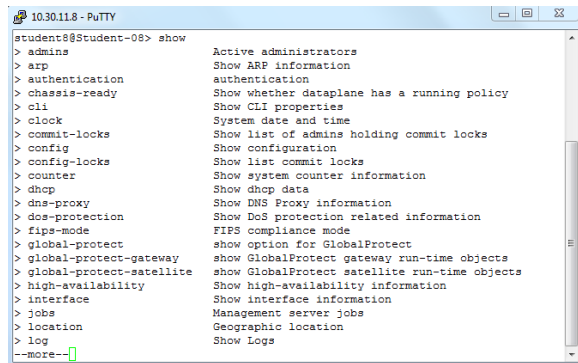
- Initial configuration must be performed using either:
  - Dedicated out-of-band management Ethernet interface (MGT)
  - Serial console connection
- Default MGT IP addressing:
  - Most firewall models: 192.168.1.1/24
  - VM-Series firewalls: DHCP client
- Default access:
  - Username: admin
  - Password: admin



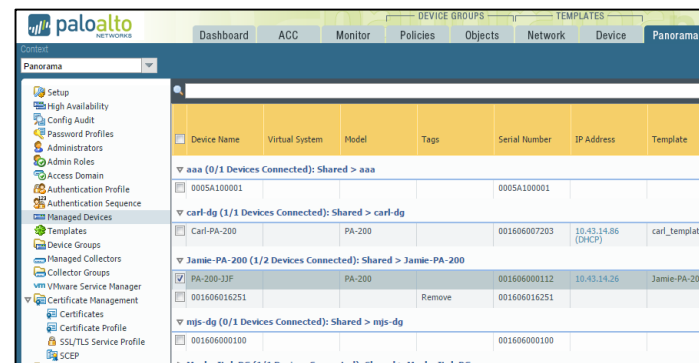
# Administrative Access



## Web Interface



## SSH/Console CLI



## Panorama

```
<response status="success" code="19">
  <result>
    <msg>
      <line>Commit job enqueued with jobid 17</line>
    </msg>
  </result>
</response>
```

## REST XML API

# Web Interface

The screenshot displays the Palo Alto Networks Web Interface. At the top, a navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. A 'Commit' button is visible next to the 'Device' tab. Below the navigation bar, the main content area is divided into several sections. On the left, the 'General Information' section displays details for a device named 'firewall-a', including its MGT IP Address (192.168.1.254), MGT Netmask (255.255.255.0), MGT Default Gateway (192.168.1.10), MGT IPv6 Address (unknown), MGT IPv6 Link Local Address (fe80::250:56ff:fe94:b285/64), MGT IPv6 Default Gateway, MGT MAC Address (00:50:56:94:b2:85), Model (PA-VM), and Serial # (015351000001208). In the center, the 'Logged In Admins' section shows a table of active administrators. To the right, the 'Locks' section indicates 'No locks found'. Below the 'Locks' section, the 'ACC Risk Factor (Last 60 minutes)' is displayed as a horizontal bar chart with a value of 4.0. At the bottom, the 'System Logs' section shows a table of system events. A 'Logout' button is located in the bottom left corner, and a 'Tasks' button is in the bottom right corner. A 'Help Portal' link is also visible in the top right corner. A 'Commit Configuration Changes' button is highlighted in the center of the interface.

**Functional Category Tabs**

**Commit Configuration Changes**

**Help Portal**

**Logout Button**

**Tasks Button**

Admin	From	Client	Time	Session
admin	192.168.1.20	Web	02/14 21:06:40	258:50:27s
admin	192.168.1.20	CLI	02/19 19:24:52	141:38:00s
admin	192.168.1.20	Web	02/19 23:41:48	00:00:00s
admin	192.168.1.20	CLI	02/21 20:12:15	93:06:47s

Description	Time
WildFire job started processing. Dequeue time=2019/02/25 17:20:04. Job Id=24234.	02/25 17:20:04
WildFire job enqueued. Enqueue time=2019/02/25 17:20:04. JobId=24234. .	02/25 17:20:04
Type: Full	

# Web Interface Editing Guidance

NAT Policy Rule

General Original Packet Translated Packet

Name

Description

Tags

Group Rules By Tag None

NAT Type ipv4

Audit Comment

Audit Comment Archive

OK Cancel

Red underline shows tabs where information is required.

Contextual Help

Yellow highlights indicate required fields.

OK button is unavailable if required information is missing or is invalid.



**Administrative controls**

**Initial system access**

**Configuration management**

**Licensing and software updates**

**Account administration**

**Viewing and filtering logs**



# Reset to Factory Configuration

- From CLI with known admin user password:
  - > **request system private-data-reset**
    - Erases all logs
    - Resets all settings, including IP addressing, which causes loss of connectivity
    - Saves a default configuration after the MGT IP address is changed
- Without known admin user password:
  - From the console port, type maint during bootup
  - Choose **Reset to Factory Default**



# MGT Interface Configuration: Web Interface

Device > Setup > Interfaces > Management

Management Interface Settings

IP Type ☒ Static ☐ DHCP Client

IP Address

Netmask

Default Gateway

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed

MTU

**Administrative Management Services**

☐ HTTP ☒ HTTPS

☐ Telnet ☒ SSH

**Network Services**

☐ HTTP OCSP ☒ Ping

☐ SNMP ☐ User-ID

☐ User-ID Syslog Listener-SSL ☐ User-ID Syslog Listener-UDP

Permitted IP Addresses	Description
------------------------	-------------

+ Add - Delete

Minimum configuration requires IP address, netmask, and default gateway.

Restrict administrative access to specific IP addresses

# Configure General Settings

- Configure hostname and domain name:
  - Each defaults to the firewall model name
- The Accept DHCP... options are available only if MGT is configured by DHCP.
- Configure a security message in the **Login Banner** (optional).
- **Latitude** and **Longitude** are used to place the firewall on maps on the ACC tab.

## Device > Setup > Management

General Settings

Hostname:

Domain:

☐ Accept DHCP server provided Hostname

☐ Accept DHCP server provided Domain

Login Banner:

☐ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile:

Time Zone:

Locale:

Date:

Time:

Latitude:

Longitude:

☐ Automatically Acquire Commit Lock

☐ Certificate Expiration Check

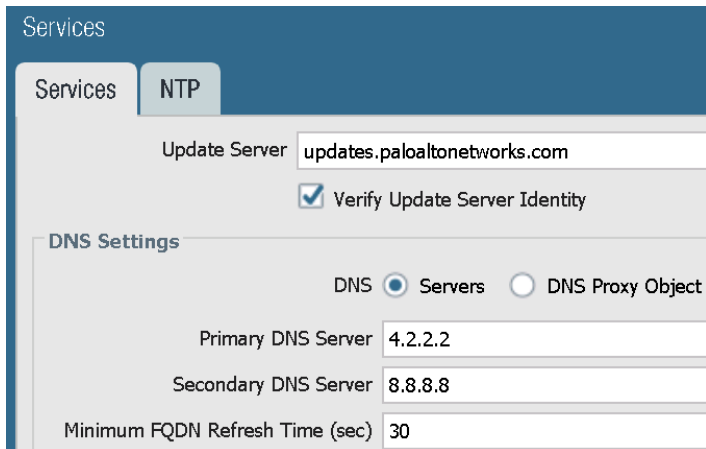
☒ Use Hypervisor Assigned MAC Addresses

☐ GTP Security

☐ SCTP Security

# Configure DNS and NTP Servers

## Device > Setup > Services



The screenshot shows the 'Services' configuration page with the 'NTP' tab selected. The 'Update Server' field is set to 'updates.paloaltonetworks.com' and the 'Verify Update Server Identity' checkbox is checked. Under the 'DNS Settings' section, the 'DNS' radio button is selected with 'Servers' as the option. The 'Primary DNS Server' is '4.2.2.2' and the 'Secondary DNS Server' is '8.8.8.8'. The 'Minimum FQDN Refresh Time (sec)' is set to '30'.

Services

Services NTP

Update Server updates.paloaltonetworks.com

☒ Verify Update Server Identity

DNS Settings

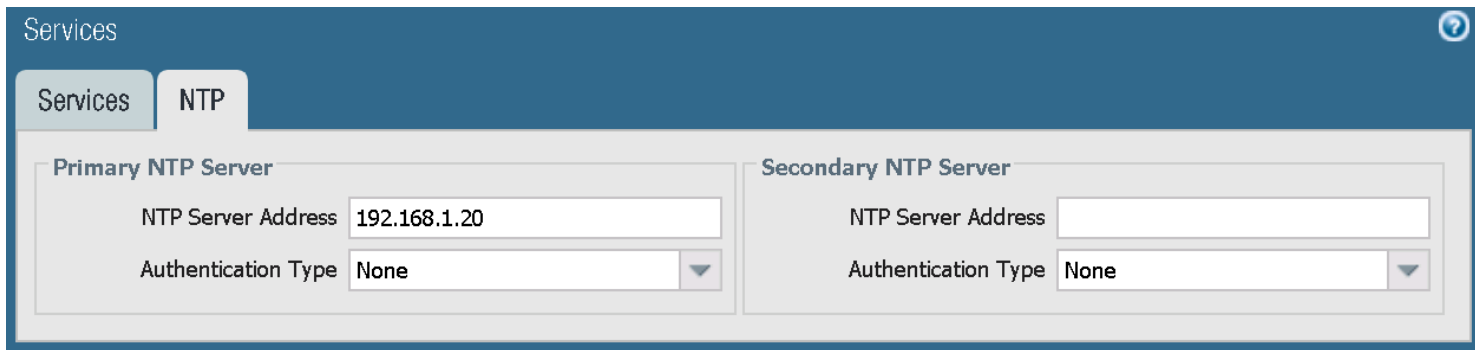
DNS ☒ Servers ☐ DNS Proxy Object

Primary DNS Server 4.2.2.2

Secondary DNS Server 8.8.8.8

Minimum FQDN Refresh Time (sec) 30

- DNS server configuration is required to reach update servers.
- NTP client configuration is optional but is recommended.



The screenshot shows the 'Services' configuration page with the 'NTP' tab selected. It displays two sections: 'Primary NTP Server' and 'Secondary NTP Server'. The 'Primary NTP Server' has an 'NTP Server Address' of '192.168.1.20' and an 'Authentication Type' of 'None'. The 'Secondary NTP Server' has empty fields for both 'NTP Server Address' and 'Authentication Type'.

Services

Services NTP

Primary NTP Server

NTP Server Address 192.168.1.20

Authentication Type None

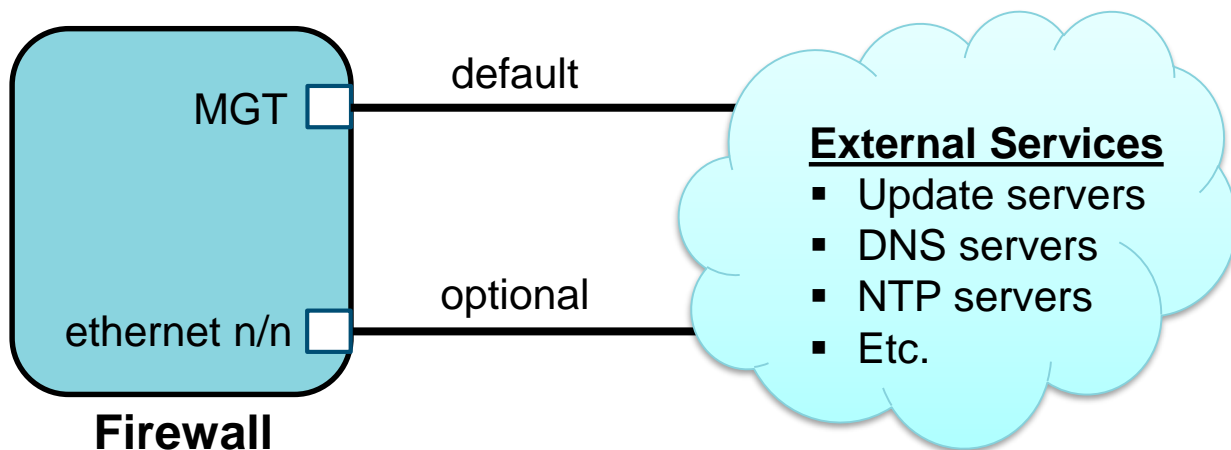
Secondary NTP Server

NTP Server Address

Authentication Type None

# Service Routes

- By default the MGT port is used to access external services.
- Configure an in-band port to access external services (optional).



# Configuring Service Routes

## Device > Setup > Services > Service Route Configuration

The screenshot shows the 'Service Route Configuration' window in the Palo Alto Networks management console. The 'Customize' radio button is selected. Under the 'IPv4' tab, a table lists various services and their source configurations. The 'NTP' service is selected, and a 'Set Selected Service Routes' button is visible at the bottom left. A modal dialog titled 'Service Route Source' is open, showing the configuration for the selected service. The 'Source Interface' is set to 'ethernet1/1' and the 'Source Address' is set to '203.0.113.20/24'. An arrow points from the 'Set Selected Service Routes' button to the modal dialog.

Service Route Configuration

☐ Use Management Interface for all ☒ Customize

IPv4 IPv6 Destination

Service	Source Interface	Source Address
<input type="checkbox"/> AutoFocus	Use default	Use default
<input type="checkbox"/> CRL Status	Use default	Use default
<input type="checkbox"/> Panorama pushed updates	Use default	Use default
<input type="checkbox"/> DNS	Use default	Use default
<input type="checkbox"/> External Dynamic Lists	Use default	Use default
<input type="checkbox"/> Email	Use default	Use default
<input type="checkbox"/> HSM	Use default	Use default
<input type="checkbox"/> HTTP	Use default	Use default
<input type="checkbox"/> Kerberos	Use default	Use default
<input type="checkbox"/> LDAP	Use default	Use default
<input type="checkbox"/> MDM	Use default	Use default
<input type="checkbox"/> Multi-Factor Authentication	Use default	Use default
<input type="checkbox"/> Netflow	Use default	Use default
<input checked="" type="checkbox"/> NTP	Use default	Use default

Set Selected Service Routes

Service Route Source

Source Interface: ethernet1/1

Source Address: 203.0.113.20/24

OK Cancel



**Administrative controls**

**Initial system access**

**Configuration management**

**Licensing and software updates**

**Account administration**

**Viewing and filtering logs**

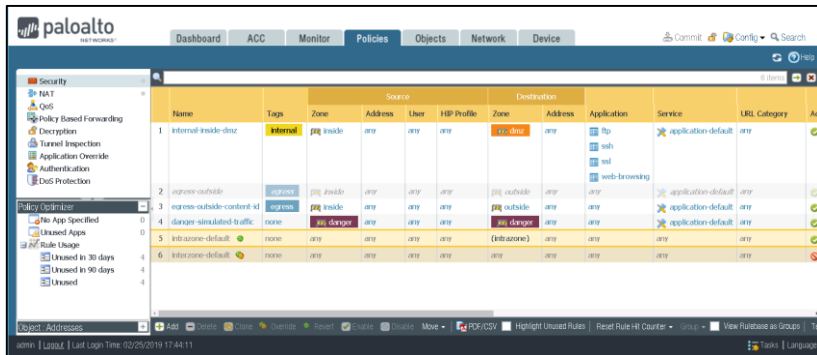
# Configuration Types

## Candidate Configuration

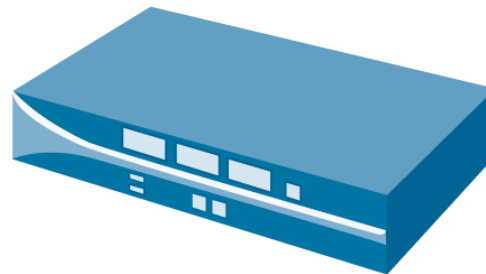
- Configuration changes made but not committed

## Running Configuration

- Configuration settings currently active on the firewall



Commit





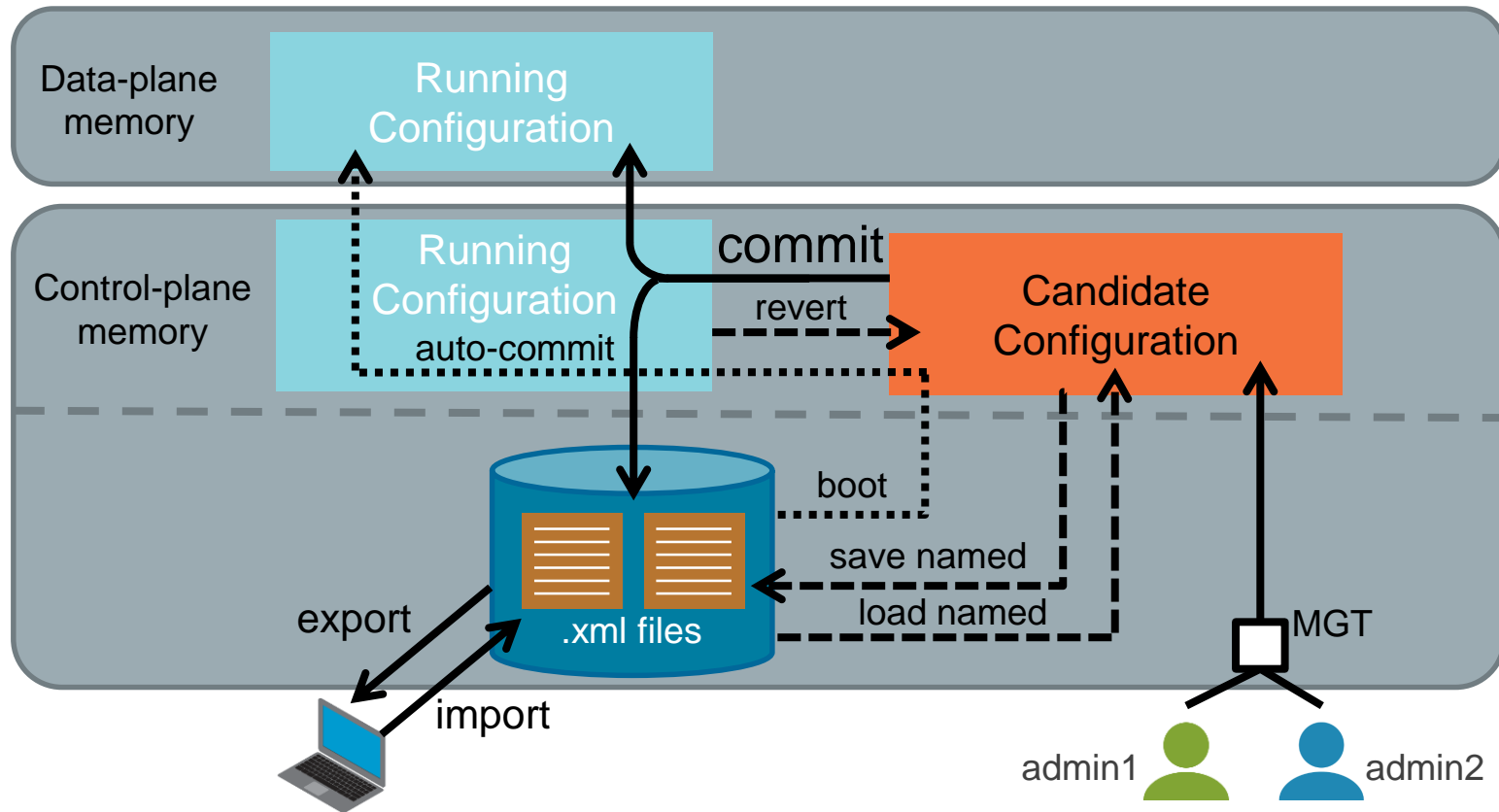
# Global Configuration Management

## Device > Setup > Operations

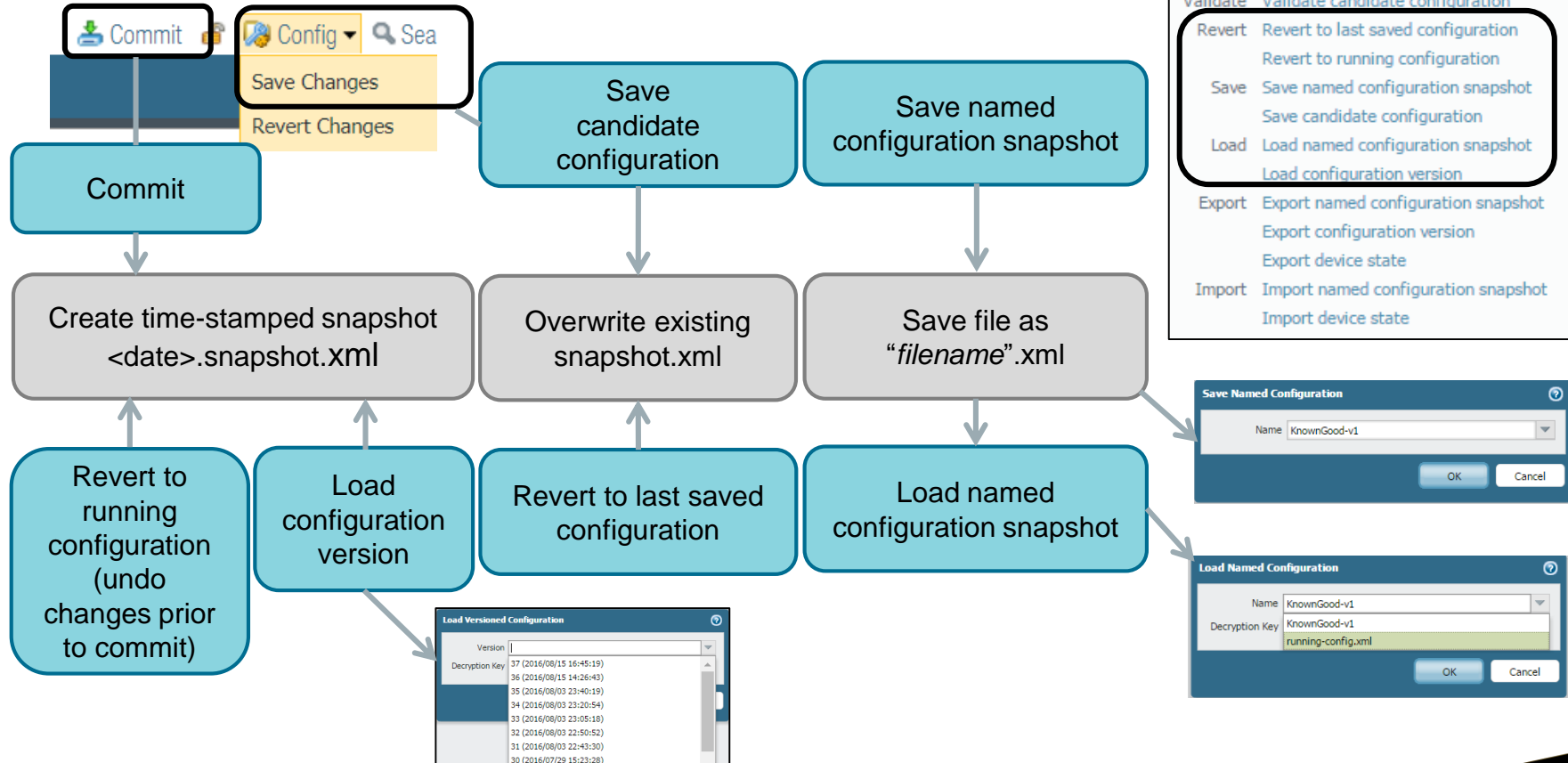
Configuration Management	
Revert	Revert to last saved configuration
	Revert to running configuration
Save	Save named configuration snapshot
	Save candidate configuration
Load	Load named configuration snapshot
	Load configuration version
Export	Export named configuration snapshot
	Export configuration version
	Export device state
Import	Import named configuration snapshot
	Import device state

- These operations are global in scope and not per-admin.
- **Revert**, **Save**, and **Load** operations all manage configurations local to the firewall.
- **Export** operations export configurations from the firewall to the host running the web interface.
- **Import** operations import configurations from the firewall to the host running the web interface.

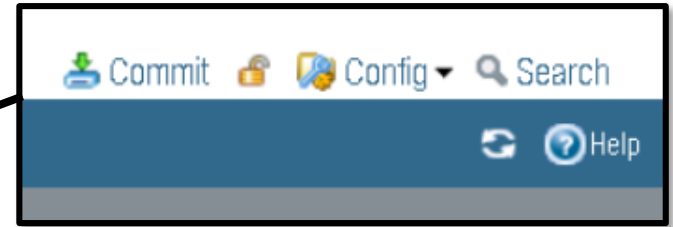
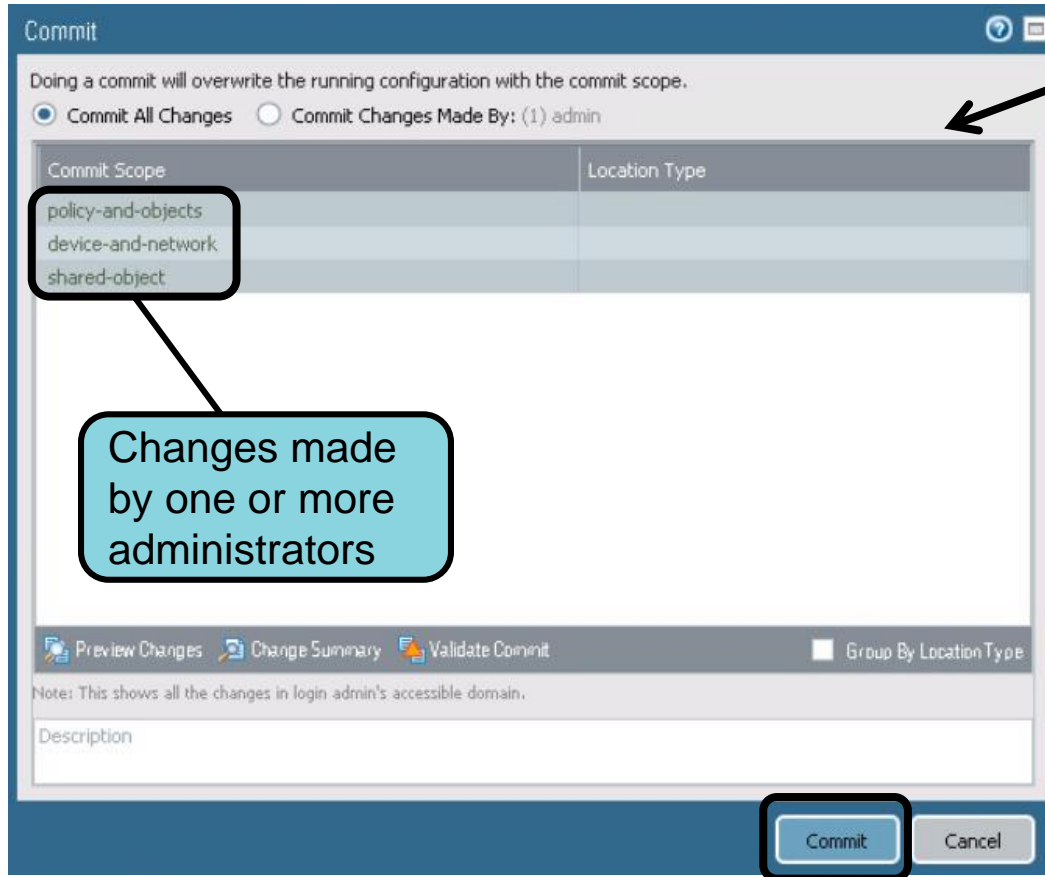
# Configuration Operations



# Configuration Operations



# Admin-Level Commit



- View and commit all administrators' changes:
  - Requires proper permissions
- View and commit only selected administrator changes

# Performing a Per-Admin Commit

The diagram illustrates the process of performing a per-admin commit in Palo Alto Networks. It shows two states of the 'Commit' dialog box and an 'Admin Scope Selection' panel.

**Commit Dialog Box (Top):**

- Doing a commit will overwrite the running configuration with the commit scope.
- ☐ Commit All Changes
- ☒ Commit Changes Made By: (1) admin
- Commit Scope: device-and-network
- Location Type: (empty)
- Include in Commit: ☒

**Admin Scope Selection Panel:**

- Name: admin
- Name: ZoneAdmin

**Commit Dialog Box (Bottom):**

- Doing a commit will overwrite the running configuration with the commit scope.
- ☐ Commit All Changes
- ☒ Commit Changes Made By: (2) admin, ZoneAdmin
- Commit Scope: policy-and-objects
- Commit Scope: device-and-network
- Location Type: (empty)
- Include in Commit: ☒

**Annotations:**

- admin user changes (points to 'admin' in the top dialog)
- ZoneAdmin user changes (points to 'ZoneAdmin' in the bottom dialog)
- admin user changes (points to 'device-and-network' in the bottom dialog)

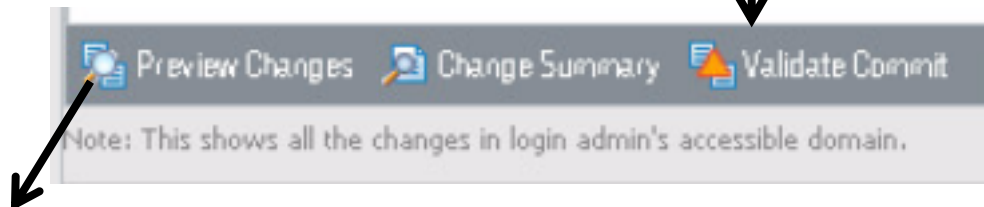
# Admin-Level Save and Revert



- Save changes in progress without committing:
  - Per-admin or all changes
- Revert changes to previous saved configuration:
  - Per-admin or all changes

# Preview and Validate Changes

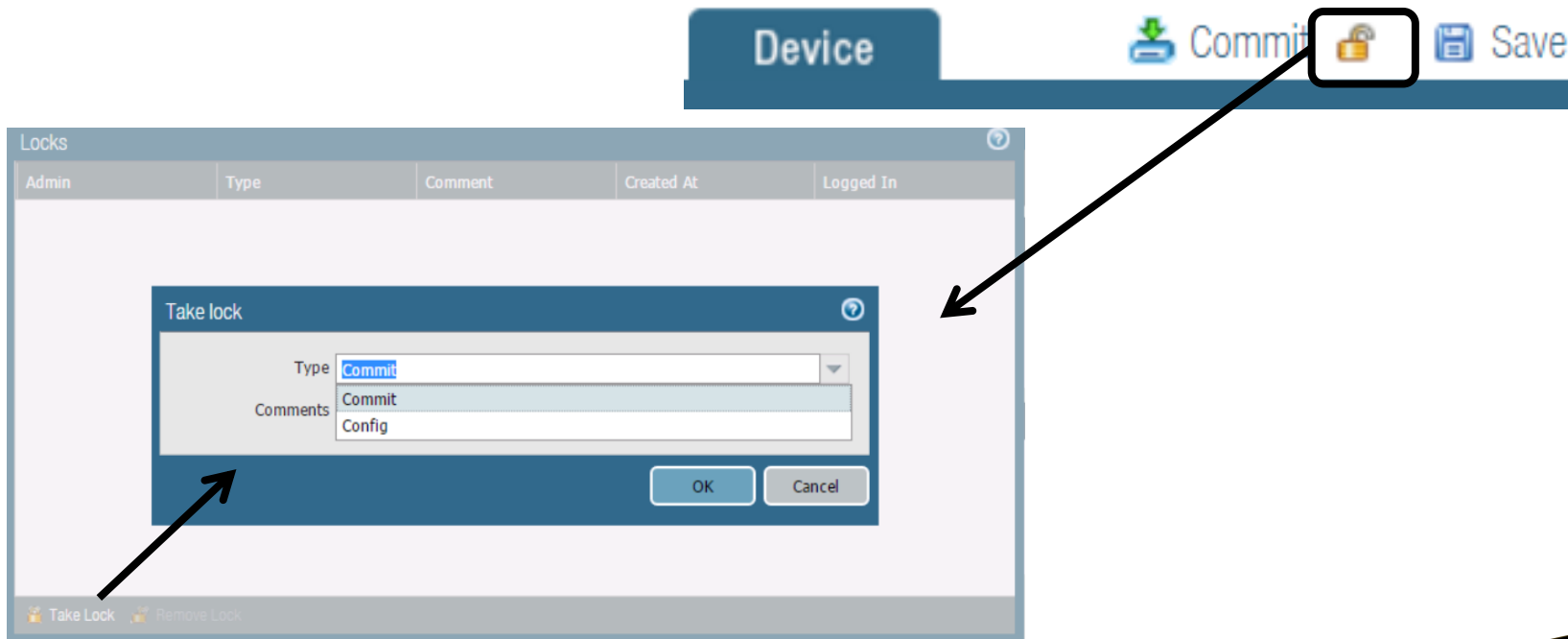
- **Preview Changes** compares the candidate configuration to the running configuration.
- **Change Summary** lists the individual settings for which you are committing changes.
- **Validate Commit** shows any error messages that would appear during a commit.



Device Config Audit (FW-07)			
Wed Nov 2 16:53:54 PDT 2016			
Legend: <span>Added</span> <span>Modified</span> <span>Deleted</span>			
Local Device Changes			
	Running Configuration		Candidate Configuration
404	}	404	}
405	timezone US/Pacific;	405	timezone US/Pacific;
406	service {	406	service {
407	disable-telnet yes;	407	disable-telnet yes;
408	disable-http yes;	408	disable-http yes;
		409	disable-userid-service no;
409	}	410	}
410	hostname FW-07;	411	hostname FW-07;
411	default-gateway 10.5.5.60;	412	default-gateway 10.5.5.60;
412	ntp-servers;	413	ntp-servers;
413	dns-setting {	414	dns-setting {

# Transaction Locks for Multiple Admins

- Commit lock: Blocks other admins from committing the candidate configuration
- Config lock: Blocks other admins from changing the candidate configuration







Administrative controls

Initial system access

Configuration management

**Licensing and software updates**

Account administration

Viewing and filtering logs

# Activate the Firewall

Step	Hardware Firewall	VM-Based Firewall
<b>Register with Palo Alto Networks Support</b>	Use serial number from <b>Dashboard</b>	Use emailed auth codes and purchase/order number
<b>Activate licenses at Device &gt; Licenses</b>	Retrieve license keys from license server	Activate feature using authorization code
<b>Verify update and DNS servers</b>	Use correct update and DNS server in <b>Device &gt; Setup &gt; Services</b>	
<b>Manage content updates</b>	Get latest application and threat signatures and URL filtering database	
<b>Install software updates</b>	Verify OS version and install recommended version	

# Dynamic Updates

## Device > Dynamic Updates



Version ▲	File Name	Features	Type	Size	Release Date	Download...	Currently Installed	Action	Documentation	
<b>▼ Antivirus</b> <b>Last checked:</b> 2019/02/25 01:02:02 UTC <b>Schedule:</b> <b>Every day at 01:02 (Download and Install)</b>										
2895-3405	panup-all-antivirus-2895-3405		Full	83 MB	2019/02/20 12:00:54 UTC	✓ previously				
2896-3406	panup-all-antivirus-2896-3406		Full	83 MB	2019/02/21 12:04:45 UTC					
2897-3407	panup-all-antivirus-2897-3407		Full	84 MB	2019/02/22 12:02:54 UTC					
2898-3408	panup-all-antivirus-2898-3408		Full	85 MB	2019/02/23 12:00:17 UTC	✓				
2899-3409	panup-all-antivirus-2899-3409		Full	85 MB	2019/02/24 12:02:17 UTC	✓		Install	Release Notes	<input checked="" type="checkbox"/>
<b>▼ Applications and Threats</b> <b>Last checked:</b> 2019/02/20 01:05:11 UTC <b>Schedule:</b> <b>Every Wednesday at 01:05 (Download only)</b>										
748-4315	panupv2-all-contents-748-4315	Apps, Threats	Full	35 MB	2017/11/08 00:49:47 UTC			Download	Release Notes	
8109-5227	panupv2-all-contents-8109-5227	Apps, Threats	Full	44 MB	2018/12/28 00:48:11 UTC		✓	Review Policies Review Apps	Release Notes	
8116-5267	panupv2-all-contents-8116-5267	Apps, Threats	Full	44 MB	2019/01/24 00:09:25 UTC			Download	Release Notes	
8117-5272	panupv2-all-contents-8117-5272	Apps, Threats	Full	44 MB	2019/01/26 02:59:18 UTC			Download	Release Notes	
8118-5277	panupv2-all-contents-8118-5277	Apps, Threats	Full	44 MB	2019/01/29 22:04:16 UTC			Download	Release Notes	
8119-5282	panupv2-all-contents-8119-5282	Apps, Threats	Full	44 MB	2019/02/01 18:50:00 UTC			Download	Release Notes	
8120-5288	panupv2-all-contents-8120-5288	Apps, Threats	Full	44 MB	2019/02/06 01:31:22 UTC			Download	Release Notes	
Check Now     Upload     Install From File										

Schedule checking for new content, and automatic download or download and install.

# PAN-OS Software Updates

## Device > Software

Version	Size	Release Date	Available	Currently Installed	Action	
9.0.0-b7	756 MB	2018/09/21 23:11:43	Downloaded	✓	Reinstall	<a href="#">Release Notes</a>
8.1.3	464 MB	2018/08/13 11:13:02			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.2	461 MB	2018/06/13 05:56:35			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.1	460 MB	2018/05/01 07:49:33			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.0	663 MB	2018/03/01 20:10:59			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.0-b50	667 MB	2018/02/09 13:51:32			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.0-b41	654 MB	2018/01/16 07:33:00			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.0-b34	653 MB	2017/12/21 13:44:52			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.0-b33	653 MB	2017/12/08 13:14:51			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.0-b28	653 MB	2017/11/16 20:32:14			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.0-b17	652 MB	2017/10/26 13:49:52			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.1.0-b8	651 MB	2017/10/08 19:01:26			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.0.12	433 MB	2018/08/09 15:16:58			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.0.11-h1	433 MB	2018/07/05 22:03:46			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.0.10	431 MB	2018/05/14 21:49:45			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.0.9	431 MB	2018/04/03 19:17:53			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.0.8	431 MB	2018/02/11 09:42:06			<a href="#">Download</a>	<a href="#">Release Notes</a>
8.0.7	431 MB	2017/12/28 10:26:05			<a href="#">Download</a>	<a href="#">Release Notes</a>

 Check Now  Upload

1. **Check Now** to list new software.
2. **Download** from update server or **Upload** from local machine.
3. **Install** software.



**Administrative controls**

**Initial system access**

**Configuration management**

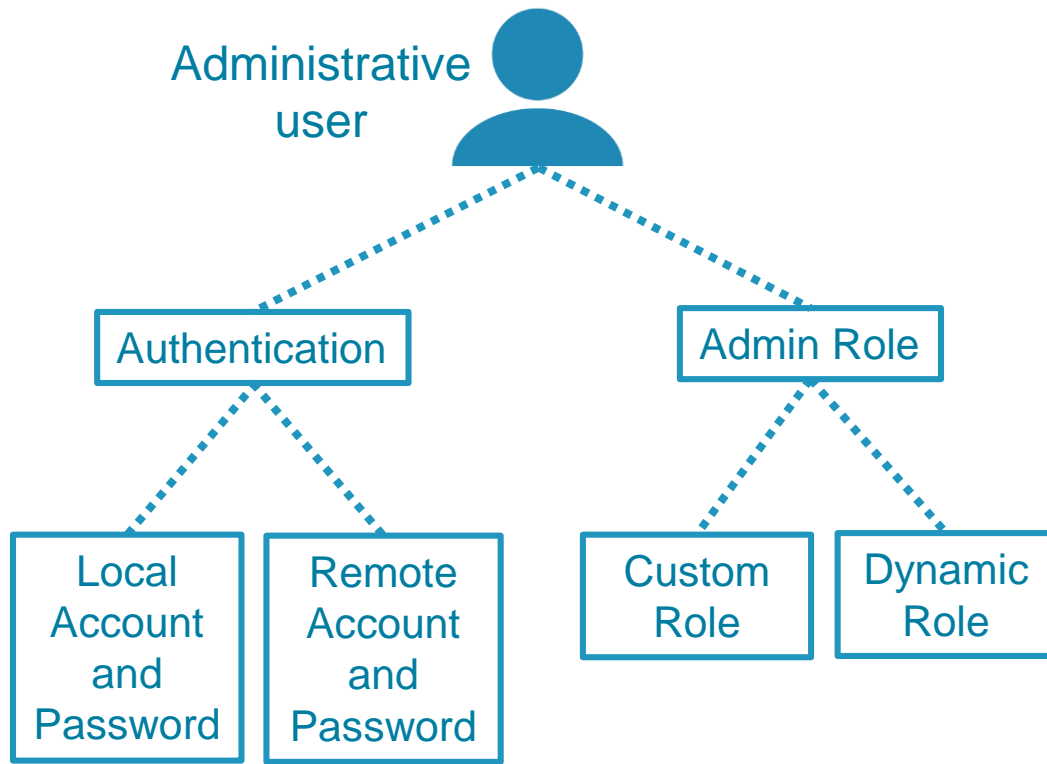
**Licensing and software updates**

**Account administration**

**Viewing and filtering logs**

# Administrator Account and Role Repositories

- Firewall can authenticate locally or remotely defined administrators.
- Each administrative account is assigned a role with specific privileges.
- Administrator actions are logged in the Configuration and System logs:
  - **Monitor > Logs**



# Creating an Administrator Role

- Roles define administrative privileges on the firewall.
- Two types:
  - Dynamic: Predefined permission sets:
    - superuser
    - superuser (read only)
    - device administrator
    - device administrator (read only)
  - Role Based: Custom permission sets

## Device > Admin Roles > Add

Admin Role Profile

Name: policy-admin-role

Description: Policy Administrators

Web UI XML/REST API Command Line

- ☒ Dashboard
- ☒ ACC
- ☒ Monitor
- ☒ Logs
  - ☒ Traffic
  - ☒ Threat
  - ☒ URL Filtering
  - ☒ WildFire Submissions
  - ☒ Data Filtering
  - ☒ HIP Match
  - ☒ IP-Tag
  - ☒ User-ID
  - ☒ Tunnel Inspection
  - ☒ Configuration
  - ☒ System

Legend: ☒ Enable ☐ Read Only ☒ Disable

Admin Role Profile

Name: policy-admin-role

Description: Policy Administrators

Web UI XML/REST API Command Line

- ☒ Report
- ☒ Log
- ☒ Configuration
- ☒ Operational Requests
- ☒ Commit
- ☒ User-ID Agent
- ☒ Export
- ☒ Import

Legend: ☒ Enable ☐ Read Only ☒ Disable

Admin Role Profile

Name: policy-admin-role

Description: Policy Administrators

Web UI XML/REST API Command Line

None

None

superuser

superreader

deviceadmin

devicereader

## Creating a Role Based Role

# Creating a Local Administrator Account

## Device > Administrators > Add

Administrator ?

Name

Authentication Profile

☐ Use only client certificate authentication (Web)

Password

Confirm Password

☐ Use Public Key Authentication (SSH)

Administrator Type ☒ Dynamic ☐ Role Based

Password Profile

Administrator Type: ☐ Dynamic ☒ Role Based

Profile:

Password Profile:

Superuser

Superuser (read-only)

Device administrator

Device administrator (read-only)



# Creating a Non-Local Administrator Account

## Device > Administrators > Add

Administrator

Name

Authentication Profile PAN-AD

☐ Use only client certificate authentication (Web)

☐ Use Public Key Authentication (SSH)


Administrator Type ☒ Dynamic ☐ Role Based

Superuser

None

PAN-AD

PAN-Radius

New  Authentication Profile

Password  
maintained in  
external service

# Firewall Authentication of Non-Local Passwords

## Server Profile:

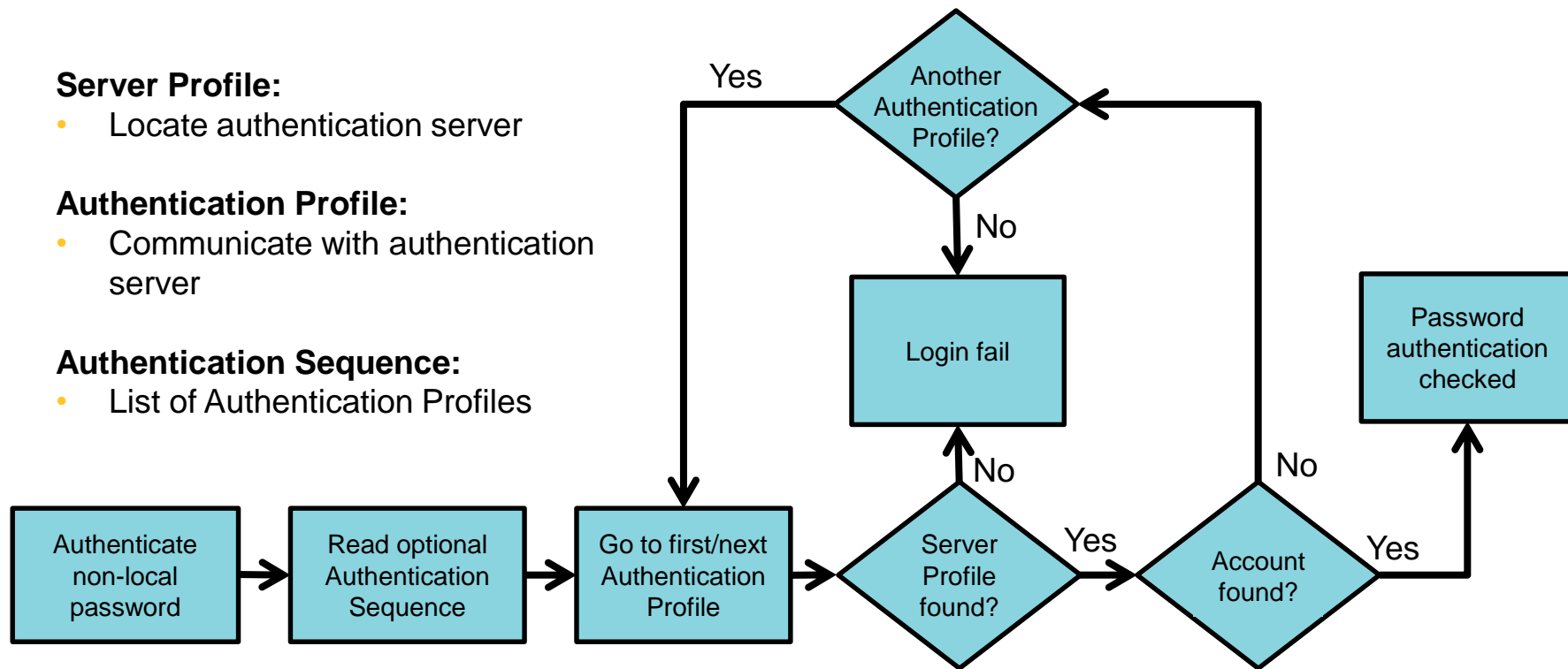
- Locate authentication server

## Authentication Profile:

- Communicate with authentication server

## Authentication Sequence:

- List of Authentication Profiles



# Configuring Server Profiles

## Device > Server Profiles

**Log Settings**

- Server Profiles
  - SNMP Trap
  - Syslog
  - Email
  - HTTP
  - Netflow
  - RADIUS
  - TACACS+
  - LDAP
  - Kerberos

Name	Location	Servers	Others
PAN-AD		Name: AD-DC-01 LDAP Server: 192.168.1.20 Port: 389	Type: active-directory Base: DC=example,DC=local Bind DN: ad-service-user@example.com

### LDAP Server Profile

Profile Name: PAN-AD

☐ Administrator Use Only

#### Server List

Name	LDAP Server	Port
AD-DC-01	192.168.1.20	389

+ Add - Delete

Enter the IP address or FQDN of the LDAP server

#### Server Settings

Type: active-directory

Base DN: DC=example,DC=local

Bind DN: ad-service-user@example.local

Password: .....

Confirm Password: .....

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

☐ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

# Configuring Authentication Profiles

## Device > Authentication Profiles

The screenshot shows the Palo Alto Networks configuration interface for Authentication Profiles. On the left is a navigation pane with the following items: Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile (selected), Authentication Sequence, User Identification, VM Information Sources, Certificate Management, and Certificates. The main area displays a table of authentication profiles. The table has columns: Name, Location, Lockout (Failed Attempts (#) and Lockout Time (min)), Allow List, Authentication..., Server Profile, Others, and Locked Users. Two profiles are listed: PAN-AD and PAN-Radius. The PAN-AD profile has a location of 'PAN-Training-AD' and a password expiration message of 'Login Attr: sAMAccount... Password Exp Msg: 7 days'. The PAN-Radius profile has a location of 'PAN-Radius'. At the bottom of the table are buttons for Add, Delete, and Clone.

Name	Location	Lockout		Allow List	Authentication...	Server Profile	Others	Locked Users
		Failed Attempts (#)	Lockout Time (min)					
PAN-AD		0 (default)	0 (default)	all	LDAP	PAN-Training-AD	Login Attr: sAMAccount... Password Exp Msg: 7 days	none
PAN-Radius		0 (default)	0 (default)	all	RADIUS	PAN-Radius		none

Buttons: Add, Delete, Clone

# Configuring an Authentication Sequence

Device > Authentication Sequence > Add

The screenshot displays the Palo Alto Networks configuration interface. On the left, a navigation pane shows the hierarchy: Administrators, Admin Roles, Authentication Profile, Authentication Sequence (selected), User Identification, VM Information Sources, and Certificate Management. The main area shows a table with columns: Name, Location, and Profile List. A row is selected with the name 'Two Auth Systems' and profile list 'PAN-AD, PAN-Radius'. A callout box points to this row with the text 'Check Active Directory, then RADIUS'. Below the table, the 'Authentication Sequence' configuration window is open, showing the name 'Two Auth Systems' and the 'Authentication Sequence Settings' section with the checkbox 'Use domain to determine authentication profile' checked. Under 'Authentication Profiles', 'PAN-AD' and 'PAN-Radius' are listed. At the bottom of the window are buttons for Add, Delete, Move Up, and Move Down.

Name	Location	Profile List
Two Auth Systems		PAN-AD PAN-Radius

Check Active Directory, then RADIUS

Authentication Sequence

Name: Two Auth Systems

Authentication Sequence Settings

☒ Use domain to determine authentication profile

Authentication Profiles

- PAN-AD
- PAN-Radius

Buttons: Add, Delete, Move Up, Move Down

**Administrative controls**

**Initial system access**

**Configuration management**

**Licensing and software updates**

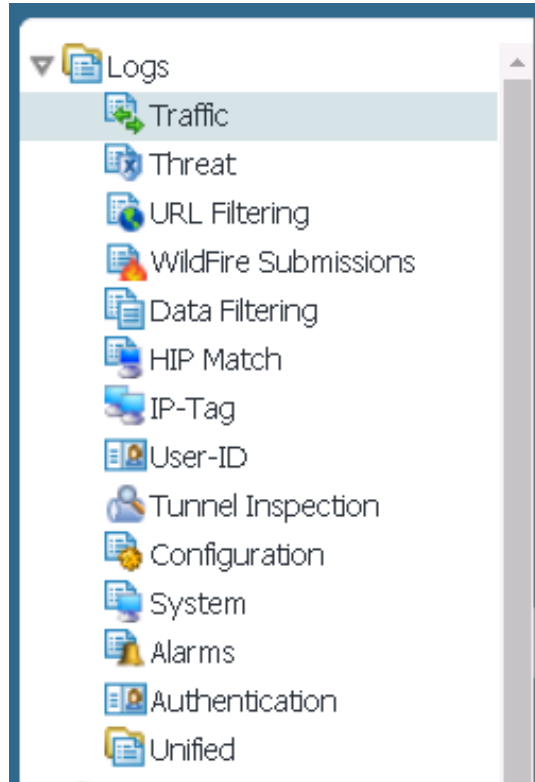
**Account administration**



**Viewing and filtering logs**

# Accessing Firewall Logs

## Monitor > Logs



- Each firewall maintains multiple log types.

# Constructing a Log Filter

- Click any link in the log listing to add that item as a log filter option.

Monitor > Logs > Traffic



The screenshot shows the Palo Alto Networks traffic log interface. At the top, a search bar contains the query `( addr.src in 10.0.0.101 ) and ( app eq ntp )`. To the right of the search bar are three buttons: a green arrow (labeled "Runs a query using the filter"), a red X (labeled "Clears the existing filter"), and a green plus sign. Below the search bar is a table with columns: Receive Time, From Zone, To Zone, Source, Destination, To Port, Application, Action, and Rule. The table contains five rows of log entries, all showing traffic from 10.0.0.101 to various Internet destinations on port 123, with the application set to ntp and action set to allow. Two arrows point from the search bar to the first two columns of the table: one from the search bar to the "From Zone" column and another from the search bar to the "Source" column.

	Receive Time	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
	10/23 09:32:03	LAN10	Internet	10.0.0.101	159.203.158.197	123	ntp	allow	LAN10-to-Internet
	10/23 09:30:25	LAN10	Internet	10.0.0.101	148.167.132.200	123	ntp	allow	LAN10-to-Internet
	10/23 09:30:17	LAN10	Internet	10.0.0.101	69.195.159.158	123	ntp	allow	LAN10-to-Internet
	10/23 09:30:04	LAN10	Internet	10.0.0.101	207.171.178.6	123	ntp	allow	LAN10-to-Internet
	10/23 09:29:53	LAN10	Internet	10.0.0.101	209.115.181.107	123	ntp	allow	LAN10-to-Internet



# Add Log Filter

Monitor > Logs > Traffic

Download log  
in CSV format.

The screenshot shows the Palo Alto Networks traffic log interface. A modal dialog titled "Add Log Filter" is open, displaying a filter rule: `( addr.src in 192.168.1.20 ) and ( addr.dst in 74.217.90.199 )`. The dialog includes a table for building the filter:

Connector	Attribute	Operator	Value
and	Chunks	in	74.217.90.199
or	Chunks Received	not in	
	Chunks Sent		
	Count		
	Destination Address		
	Destination Country		
	Destination Interface		
	Destination Port		

There is a "Negate" checkbox at the bottom left of the filter table. At the bottom right of the dialog are "Add", "Apply", and "Close" buttons. In the background, a table of log entries is visible with columns: Receive Time, URL Category, Type, Decrypted, From Zone, To Zone, Source, Sour... User, Destination, To Port, Application, Action, and Rule. A callout box points to a download icon in the top right corner of the log table, with the text "Download log in CSV format."

# Module Summary



Now that you have completed this module, you should be able to:

- Connect to the firewall and log in as admin
- Configure the network settings for the management interface port
- Describe the difference between the running config and the candidate config
- Configure dynamic firewall updates to update the applications and threats databases
- Create a local firewall administrative account
- Access the firewall logs

# Questions?



## Initial Configuration Lab (Pages 11-23 in the Lab Guide)

- Load a firewall lab configuration file
- Create an admin role
- Create an administrator account
- Manage commit locks
- Manage external firewall services
- Schedule dynamic updates

PROTECTION. DELIVERED.



This page intentionally left blank