Palo Alto Networks

Common Criteria Evaluated Configuration Guide (CCECG) for Next-Generation Firewalls with PAN-OS 11.0

Revision Date: June 9, 2023

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

1 Introduction

The Palo Alto next-generation firewalls (NGFWs) are network firewall appliances and virtual appliances on specified hardware used to manage enterprise network traffic flow using function-specific processing for networking, security, and management. The next-generation firewalls let the administrator specify security policies based on an accurate identification of each application seeking access to the protected network. The next-generation firewall uses packet inspection and a library of applications to distinguish between applications that have the same protocol and port, and to identify potentially malicious applications that use non-standard ports. The next-generation firewall also supports the establishment of Virtual Private Network (VPN) connections to other next-generation firewalls or third-party security devices. The NGFWs also identify which applications are flowing across the network, irrespective of port, protocol, or TLS encryption.

GlobalProtect safeguards the mobile workforce by inspecting all traffic using the organization's next-generation firewalls that are deployed as internet gateways, whether at the perimeter, in the DMZ, or in the cloud. Laptops, smartphones and tablets with the GlobalProtect app automatically establish a secure TLS/IPsec VPN connection to the next-generation firewall with the best performance for a given location, thus providing the organization with full visibility of all network traffic, for applications, and across all ports and protocols. By eliminating the blind spots in mobile workforce traffic, the organization maintains a consistent view into applications.

This document is a supplement to the PAN-OS® Administrator's Guide, which is composed of the installation and administration documents identified in section 1.3 ("Documentation References"). This document supplements those manuals by specifying how to install, configure and operate this product in the Common Criteria evaluated configuration. This document is referred to as the operational user guide in the Network Device collaborative Protection Profile (NDcPP) v2.2e, PP-Module for Stateful Traffic Filter Firewalls (FW-Module) v1.4e, and PP-Module for VPN Gateways (VPNGW-Module) and meets all the required guidance assurance activities from these standards.

1.1 Common Criteria (CC) Evaluated Configuration

The following sections describe the scope of evaluation, required configuration, assumptions, and operational environment that the system must be in to ensure a secure deployment. To ensure the system is in the CC evaluated configuration, the administrators must do the following:

- Configure all the required settings and default policies as documented in this guide.
- Disable all the features that would violate the NDcPP requirements or would make the system vulnerable to attacks as documented in this guide.
- Ensure all the environmental assumptions in section 2 are met.
- Ensure that your operational environment is consistent with section 2.
- Follow the guidance in this document.

Accessing the shell should be limited to authorized administrators for pre-operational setup (for example, Security Technical Implementation Guide (STIG) or Security Requirements Guide (SRG) compliance testing), for troubleshooting, or regular maintenance. When FIPS-CC Mode is enabled, shell access will be permanently disabled (i.e., root access to the underlying hardened Linux shell).

Before you can begin using PAN-OS NGFW (i.e., the TOE) for application-level filtering, VPN, and IPS/IDS, you are required to register, activate, and retrieve the device support and licenses. Every instance of firewall requires valid licenses that entitle you to use the firewalls and obtain support. This license is based on firewall serial numbers, not on the number of virtual systems on each firewall. The support license enables the TOE software updates and dynamic content updates (for the latest Applications and Threats signatures, as an example).

Scope of Evaluation

The list below identifies features or protocols that are not evaluated or must be disabled, and the rationale why. Note that this does not mean the features cannot be used in the evaluated configuration (unless explicitly stated so). It means that the features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion. Evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target. In particular, only the following protocols implemented by the TOE have been tested, and only to the extent specified by the security functional requirements: TLS, HTTPS, SSH, IKE/IPsec. The features below and Normal mode are out of scope.

Feature	Description
Telnet and HTTP Management Protocols	Telnet and HTTP are disabled by default and cannot be enabled in the evaluated configuration. Telnet and HTTP are insecure protocols which allow for plaintext passwords to be transmitted. Use SSH and HTTPS only as the management protocols to manage the TOE.
External Authentication Servers	The NDcPP does not require external authentication servers.
Shell and Console Access	The shell and console access are only allowed for pre-operational installation, configuration, and post-operational maintenance and trouble shooting.
TLS and SSH Decryption Policies	The TLS and SSH decryption policies are not evaluated and therefore, these features are out of scope.
Anti-Virus, Anti-Spyware, Anti-Malware Security Policies	The Anti-Virus, Anti-Spyware, Anti-Malware security policies (i.e., profiles) are not evaluated and therefore, these features are out of scope.
File Blocking, DLP, and URL Filtering Security Policies	The File Blocking, DLP (Data Loss Prevention), and URL Filtering security policies/profiles are not evaluated and therefore, these features are out of scope.
API request over HTTP	By default, the TOE support API requests over HTTPS only. API request over HTTP is disabled and cannot be enabled in the evaluated configuration.
Any features not associated with SFRs in claimed [NDcPP], [FW-Module], and [VPNGW-Module]	NDcPP forbids adding additional requirements to the Security Target (ST). If additional functionalities or products are mentioned in the ST, it is for completeness only.

Table 1: Out of Scope Features

1.2 TOE References

Model	Description	Version
Physical	1. PA-220 Series a. PA-220R	11.0.1
	2. PA-400 Series a. PA-410 b. PA-415 c. PA-440 d. PA-445 e. PA-450 f. PA-460	
	3. PA-800 Series a. PA-820 b. PA-850	
	4. PA-1400 Series a. PA-1410 b. PA-1420	
	5. PA-3200 Series a. PA-3220 b. PA-3250 c. PA-3260	
	6. PA-3400 Series a. PA-3410 b. PA-3420 c. PA-3430 d. PA-3440	
	7. PA-5200 Series a. PA-5220 b. PA-5250 c. PA-5260 d. PA-5280	

Model	Description	Version
	8. PA-5400 Series a. PA-5410 b. PA-5420 c. PA-5430 d. PA-5440	
	9. PA-5450[1]	
	10. PA-7000 Series[2] a. PA-7050 b. PA-7080	

[1] PA-5450 firewall supports the following cards: PA-5400 MPC-A, PA-5400 NC-A, and PA-5400 DPC-A.

[2] Palo Alto Networks PA-7000 Series firewalls support different Network Processing Cards (NPC) and Switch Management Cards (SMC): PAN-PA-7050-SMC-B, PAN-PA-7080-SMC-B, PAN-PA-7000-LFC-A, PAN-PA-7000-100G-NPC-A-K2-EXP, PAN-PA-7000-100G-NPC-A-K2-SEC, and PAN-PA-7000-100G-NPC.

Model	Description	Version
Virtual	1. VM-Series a. VM-50 b. VM-100 c. VM-200 d. VM-300 e. VM-500 f. VM-700 g. VM-1000-HV The VM-Series virtual appliance must be the only guest running in the virtualized environment. Evaluation testing included the following: VMware ESXi 7.0: • Dell PowerEdge R740 Processor: Intel Xeon Gold 6248 (Cascade Lake microarchitecture) with Broadcom 57416 NIC • Memory: 128 GB RDIMM Hyper-V**, and KVM Ubuntu: • Dell PowerEdge R740 Processor: Intel Xeon Gold 6248 (Cascade Lake microarchitecture) with Broadcom 57416 NIC • Memory: 128 GB RDIMM	11.0.1

Table 2: TOE Reference

* - The TOE was tested and evaluated by the Common Criteria lab on ESXi version 7.0.

** - The TOE was tested on Microsoft Hyper-V Server 2019 and KVM on Ubuntu 20.04.

1.3 Documentation References

The Palo Alto Networks System documentation set includes online help and PDF files.

The following product guidance documents are provided online or by request:

- PAN-OS Administrator’s Guide Version 11.0, Last Revised: See Link Below

  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/pan-os-admin/pan-os-admin.pdf
- PAN-OS CLI Quick Start Version 11.0, Last Revised: See Link Below

  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/pan-os-cli-quick-start/pan-os-cli-quick-start.pdf
- PAN-OS Web Interface Help Version 11.0, Last Revised: See Link Below

  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/pan-os-web-interface-help/pan-os-web-interface-help.pdf
- VM-Series 11.0 Deployment Guide, Last Revised: See Link Below

  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/vm-series/11-0/vm-series-deployment/vm-series-deployment.pdf
- PAN-OS and Panorama API Usage Guide Version 11.0, Last Revised: See Link Below

  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/pan-os-panorama-api/pan-os-panorama-api.pdf
- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for PAN-OS 11.0 [This Document]

Online help can be accessed in two ways:

- By clicking on the Help icon ?
- Search for the feature

The most up-to-date versions of the documentation can be accessed on the Palo Alto Networks Support web site (https://support.paloaltonetworks.com) or Technical Documentation (https://docs.paloaltonetworks.com/).

2 Operational Environment

This section describes the non-TOE components in the environment and assumptions made about the environment.

2.1 Non-TOE Components

The operational environment includes the following:

- Syslog server,
- VPN gateway peer(s)
- Palo Alto Networks Global Protect (GP) application
- Workstation
  - Web browsers - Chrome (version 96 or later), Firefox (version 94.0.2 or later), Safari (version 12.0.3 or later on Mac, and version 5.1.7 or later on Windows and iOS), and Microsoft Edge (Release 942 or later) browser.
  - SSHv2 client

2.2 Environmental Security Objectives

The assumptions state the specific conditions that are expected to be met by the operational environment and/or administrators.

Table 3: Environment Security Objectives and Responsibility

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Administrators must ensure the system is installed and maintained within a secure physical location. This can include a secured building with key card access or within the physical control of an authorized administrator in a mobile environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	Administrators must not add any general-purpose computing capabilities (e.g., compilers or user applications) to the system.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	Administrators must configure the security devices that are managed by the TOE to secure the network.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	Administrators must be properly trained in the usage and proper operation of the system and all the enabled functionality. These administrators must follow the provided guidance.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must regularly update the system to address any known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must protect their access credentials where ever they may be.

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	Administrators must follow the proper electronic equipment disposal policy to ensure all sensitive information are wiped off the TOE prior to deactivation and removal from the network.
OE.CONNECTIONS	TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.	Administrators must deploy the firewalls in their networks such that they cannot be physically bypassed. All applicable traffic must flow through the TOE.

3 Before Installation You Must

Before you install your appliance in the evaluated configuration, Palo Alto Networks requires that the administrators **must** consider the following:

- Verify the delivery of Palo Alto Networks appliances from the trusted carrier and check the shipping containers for any sign of tampering. If tampering is found, please contact Support.
- Install the Palo Alto Networks appliances in a lockable rack within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the Palo Alto Networks appliances.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access. This management interface is physically separate from the data interface.
- Identify the specific management workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using the Permitted IP feature in the Management Interface Settings.
- Connect the management interface of managed devices to the same protected internal network as the TOE. This allows the administrators to securely control the device from the TOE and aggregate the event data generated on the managed device's network segment.
- By default, several ports are open to allow the TOE to take advantage of additional features and functionality. The following table lists these ports.

Ports	Description	Protocol	Direction	Open the port to ...
22	SSH	TCP	Bidirectional	Allow a secure remote connection to the appliance.
161, 162	SNMP	UDP	Bidirectional (161); Outbound (162)	Provide access if you enabled SNMP polling (inbound) and SNMP traps (outbound).
443	HTTPS	TCP	Bidirectional	Allow a secure remote connection to the appliance. **Required**
514 6514	SYSLOG SYSLOG over TLS	UDP TCP	Outbound Outbound	Send logs to a remote syslog server. The remote syslog server must allow port 6514 (configurable) to be opened.
3978 28443	TLS	TCP	Bidirectional	Allow for device communication

Table 4: Ports and Protocols

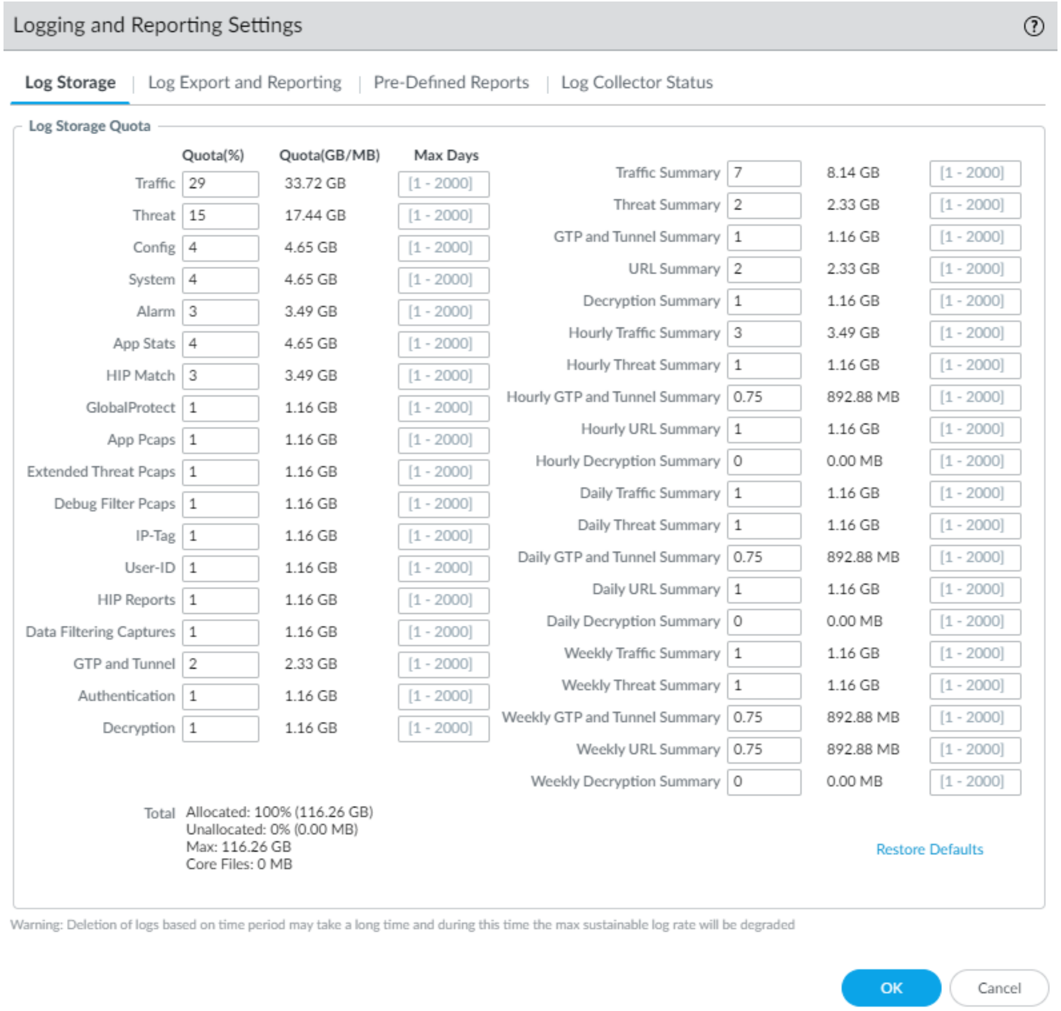
4 Required Auditable Events

This section lists and describes the audit events generated by the TOE to meet the NDcPP auditing requirements. In addition, this section describes the format, syntax, and content of these audit logs.

The audit trail generated by the TOE consist of several logs, which are locally stored in the file system on the hard disk. The four main logs are the following:

- Configuration logs — Record events such as when an administrator configures the security policies, and when an administrator configures which events are audited.
- System logs — Record user login and logout, system, and session information.
- Traffic logs — Record the traffic flow events and information.
- Threat logs — Record the detection and blocking of threats.

The TOE generates an audit event for each user interaction or API call with the web interface, and CLI command executed. API calls are supported over HTTPS to the web interface only. Each audit event includes at least a timestamp, the username of the user whose action generated the event, a source IP, and message describing the event. The common fields are described in the tables below. The TOE has an internal log database that can be used to store and review audit records locally. However, the internal log database only stores a limited number of entries in the database based on the disk space (to configure the log size, go to **Device > Setup > Logging and Reporting Settings >** click on “Gear” ⚙ icon to edit **> Log Storage Tab**, and enter a percentage % per traffic, threat, configuration, or system logs). When the audit log is full, the oldest audit records are overwritten by the newest audit records. If the log size is reduced and there are more existing logs than can be stored when committed, the TOE will remove the logs in the order of oldest first.



Logging and Reporting Settings

Log Storage | Log Export and Reporting | Pre-Defined Reports | Log Collector Status

Log Storage Quota

	Quota(%)	Quota(GB/MB)	Max Days
Traffic	29	33.72 GB	[1 - 2000]
Threat	15	17.44 GB	[1 - 2000]
Config	4	4.65 GB	[1 - 2000]
System	4	4.65 GB	[1 - 2000]
Alarm	3	3.49 GB	[1 - 2000]
App Stats	4	4.65 GB	[1 - 2000]
HIP Match	3	3.49 GB	[1 - 2000]
GlobalProtect	1	1.16 GB	[1 - 2000]
App Pcaps	1	1.16 GB	[1 - 2000]
Extended Threat Pcaps	1	1.16 GB	[1 - 2000]
Debug Filter Pcaps	1	1.16 GB	[1 - 2000]
IP-Tag	1	1.16 GB	[1 - 2000]
User-ID	1	1.16 GB	[1 - 2000]
HIP Reports	1	1.16 GB	[1 - 2000]
Data Filtering Captures	1	1.16 GB	[1 - 2000]
GTP and Tunnel	2	2.33 GB	[1 - 2000]
Authentication	1	1.16 GB	[1 - 2000]
Decryption	1	1.16 GB	[1 - 2000]

Traffic Summary	7	8.14 GB	[1 - 2000]
Threat Summary	2	2.33 GB	[1 - 2000]
GTP and Tunnel Summary	1	1.16 GB	[1 - 2000]
URL Summary	2	2.33 GB	[1 - 2000]
Decryption Summary	1	1.16 GB	[1 - 2000]
Hourly Traffic Summary	3	3.49 GB	[1 - 2000]
Hourly Threat Summary	1	1.16 GB	[1 - 2000]
Hourly GTP and Tunnel Summary	0.75	892.88 MB	[1 - 2000]
Hourly URL Summary	1	1.16 GB	[1 - 2000]
Hourly Decryption Summary	0	0.00 MB	[1 - 2000]
Daily Traffic Summary	1	1.16 GB	[1 - 2000]
Daily Threat Summary	1	1.16 GB	[1 - 2000]
Daily GTP and Tunnel Summary	0.75	892.88 MB	[1 - 2000]
Daily URL Summary	1	1.16 GB	[1 - 2000]
Daily Decryption Summary	0	0.00 MB	[1 - 2000]
Weekly Traffic Summary	1	1.16 GB	[1 - 2000]
Weekly Threat Summary	1	1.16 GB	[1 - 2000]
Weekly GTP and Tunnel Summary	0.75	892.88 MB	[1 - 2000]
Weekly URL Summary	0.75	892.88 MB	[1 - 2000]
Weekly Decryption Summary	0	0.00 MB	[1 - 2000]

Total Allocated: 100% (116.26 GB)
Unallocated: 0% (0.00 MB)
Max: 116.26 GB
Core Files: 0 MB

Warning: Deletion of logs based on time period may take a long time and during this time the max sustainable log rate will be degraded

Configuration Log (**Monitor > Logs > Configuration**)

Field	Description
Generate Time	Time and date that the appliance generated the audit record.
Administrator	Username of the user that triggered the audit event.
Host	IP address of the host used by the user.
Client	Web or CLI
Command	The command executed such as view, set, or commit.
Result	The result of the command.
Configuration Path	If applicable, the configuration path of the command. For the CLI, it is the actual command executed.
Full Path	If applicable, the full configuration path of the command.
Before Change	If applicable, the old configuration values or settings.
After Change	The new configuration values or settings.
Sequence Number	The sequence number of the command.
Device SN	The device serial number that the command executed on.
Device Name	The device name that the command executed on.

Table 5: Configuration Log

Syslog (**Monitor > Logs > System**)

Field	Description
Generate Time	Time and date that the appliance generated the audit record.
Type	The event type such as general, tls, ssh, auth, etc.
Severity	The severity of the event.
Event	The high-level identification of the event.
Object	If applicable, the object accessed or modified as part of the event.
Description	The detailed description of the event. This may include IP address, result of event, etc.
Device SN	The device serial number that the event occurred on.
Device Name	The device name that the event occurred on.

Table 6: System Log

Traffic and Threat (**Monitor > Logs > Traffic** and **Monitor > Logs > Threat**)

Field	Description
Receive Time	Time and date that the appliance generated the audit record.
Type	Specifies type of log; values are traffic, threat, config, system and hip-match.
From Zone	Zone the session was sourced from ('Source Zone').
To Zone	Zone the session was destined to ('Destination Zone').
Source	Original session source IP address.
Destination	Original session destination IP address
Source Port	Source port utilized by the session.
Destination Port	Destination port utilized by the session.
Application	Application associated with the session.
IP Protocol	IP protocol associated with the session.
Action	Action taken for the session; possible values are: • Allow—session was allowed by policy • Deny—session was denied by policy • Drop—session was dropped silently • Drop ICMP—session was silently dropped with an ICMP unreachable message to the host or application • Reset both—session was terminated and a TCP reset is sent to both the sides of the connection • Reset client—session was terminated and a TCP reset is sent to the client • Reset server—session was terminated and a TCP reset is sent to the server
Rule	Rule identifier (ID)
Session End Reason	Reason for session termination (e.g., aged-out, tcp-fin, policy-deny, threat)

Table 7: Traffic and Threat Logs

SFR	Required Audit Event [Required Content]	Actual Audit Event - '*Description*' Only	Type
FAU_GEN.1	Start-up and shut-down of audit functions[3]	Startup *The system is starting up.* Shutdown *System restart requested by <Username>* *The system is shutting down due to CLI Initiated.*	System
FAU_GEN.1	Administrator login and logout [Username]	See FIA_UIA	System
FAU_GEN.1	Changes to TSF data related to configuration changes [What has changed]	See FMT_SMF	Config
FAU_GEN.1	Generating/import of, changing, deleting of cryptographic keys [Unique key name or reference]	*Admin | request/upload | config shared certificate device* *{* *certificate* *{* *RSA 3072 CC keys* *{* *subject-hash ebcd3885; issuer-hash ebcd3885; not-valid-before "May 9 22:30:59 2018 GMT"; issuer "/CN=Root CA"; not-valid-after "May 9 22:30:59 2019 GMT"; common-name "Root CA"; expiry-epoch 1557441059; ca yes; subject "/CN=Root CA"; public-key…* *Admin | Upload | config device certificate import <Name>* *Import <Name>* *{* *private-key ********;* *}* *Admin | delete | config shared certificate device* *{* *certificate* *{* *RSA 3072 CC keys* *{* *subject-hash ebcd3885; issuer-hash ebcd3885; not-valid-before "May 9 22:30:59 2018 GMT"; issuer "/CN=Root CA"; not-valid-after "May 9 22:30:59 2019 GMT"; common-name "Root CA"; expiry-epoch 1557441059; ca yes; subject "/CN=Root CA"; public-key…*	Config

FAU_GEN.1	Resetting passwords
	
	[Username]
		On UI (HTTPS):
		Password changed for user <Username>
		
		On CLI (SSH):
		Password changed for user <Username>
			System

[3] The audit function cannot be disabled. To stop the audit function, you must shutdown the whole system.

		On UI (HTTPS):
		Admin | Web | config mgt-config users <Username> <Username>
		{
		*phash ********;*
		}
		On CLI (SSH):
		Admin | CLI | config mgt-config users <Username> <Username>
		{
		*phash ********;*
		}
			Config

FCS_HTTPS_EXT.1	Failure to establish an HTTPS session. Reason for failure.	**Failure** *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, unknown state, unknown protocol* *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, unknown state, no shared cipher* *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, unknown state, handshake failure* *SSL handshake failed - (NONE)*	System
FCS_IPSEC_EXT.1	Session Establishment with peer Entire packet contents of packets transmitted/received during session establishment	*11/15/2019 6:27 vpn ikev2-nego-child-start branchgw IKEv2 child SA negotiation is started as initiator, rekey. Initiated SA: <Source IP>[500]-<Destination IP>[500] message id:0x00000000.*	Traffic
	Failure to establish an IPsec SA. Reason for failure.	*11/15/2019 6:34 vpn ikev2-nego-fail-cert, PA-7080, general, critical, IKEv2 certificate authentication failed, peer certification revocation status couldn't be checked due to request timeout.* *11/15/2019 6:54 vpn ikev2-nego-fail-cert, PA-7080, general, critical, IKEv2 certificate authentication failed, peer certification revocation status couldn't be checked due to status is unknown.* *11/15/2019 6:54 vpn ikev2-nego-fail-common, PA-7080, general, informational, IKEv2 SA negotiation is failed, received notify type AUTHENTICATION_FAILED.*	System
FCS_SSHS_EXT.1	Failure to establish a SSH session. Reason for failure.	**Failure** *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching mac found: client <Client Cipher> server <Server Cipher>* *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching cipher found: client <Client Cipher> server <Server Cipher>* *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching key exchange method found. client <Client Cipher> server <Server Cipher>*	System

FCS_TLSC_EXT.1 FCS_TLSC_EXT.2	Failure to establish a TLS session. Reason for failure.	**Failure (to other device)** *client: <Client IP Address>:<Port Number> server: <Server IP Address>:<Port Number>, unknown state, unknown protocol* **Failure (to syslog server)** *Syslog SSL error whle writing stream; tls_error='SSL routines: SSL3_WRITE_BYTES:sslhandshake failure'* *Syslog SSL error whle writing stream; tls_error='SSL routine:SSL3_GET_SERVER_CERTIFICATE: certificate verify failed'*	System
FCS_TLSS_EXT.1 FCS_TLSS_EXT.2	Failure to establish a TLS session. Reason for failure.	*Tls-x509-eku-client-auth-failed, client <Client IP Address>:<Port Number>, server: <Server IP Address>:<Port Number> at 0 depth lookup: Failed Validation of the X.509v3 certificate: ClientAuth purpose in extendedKeyUsage field* *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, unknown state, unknown protocol* *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, unknown state, no shared cipher* *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, unknown state, handshake failure* *SSL handshake failed - (NONE)*	System
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded. [Origin of the attempt (e.g., IP address).]	On UI (HTTPS): *failed authentication for user <Username>. Reason: User is in locked users list. From <IP Address>.* *failed authentication for user <Username>. Reason: Invalid username/password. From <IP Address>.* On CLI (SSH): *Failed keyboard-interactive/pam for <username> from <ip.addr> port <port> ssh2* *ssh: euid 0 user <Username>: LOGIN_EXCEED_MAXTRIES* *Admin <Username> account has been restored – lockout timer expired*	System

FIA_UIA_EXT.1 FIA_UAU_EXT.2	All use of the identification and authentication mechanism. [Origin of the attempt (e.g., IP address).]	On UI (HTTPS): Password *User <Username> logged in via Web from <IP Address> using htttps* *failed authentication for user '<Username>'. Reason: Invalid username/password. From <IP Address>* Public-Key *Certificate validated for user ‘<Username>’. From: <Source IP>.*[4] *failed authentication for user '<Username>'. Reason: Invalid Authentication profile not found for the user. From <IP Address>* *User <Username> logged out via Web from <IP Address>* on CLI (SSH): Password *User <Username> logged in via CLI from <IP Address>* *Failed password for <Username> from <IP Address> port <Port Number> ssh2* Public-Key *Accepted publickey for <Username> from <IP Address> port <Source Port> ssh2: RSA <fingerprint>* *ssh: euid 0 user <Username>: CONNECTION_ABANDON* *User <Username> logged out via CLI from <IP Address>*	System
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate and reason for failure.	*Src Host/IP : <IP/hostname> Dst Host/IP: <IP/hostname> - OCSP/CRL validation of the X.509v3 certificate failed or not configured.*	System

[4] If mutual authentication is configured for the HTTPS web UI.

	Identification of certificates added, replaced or removed as trust anchor[5] in the TOE's trust store	*Admin | request/upload | config shared certificate device* *{* *certificate* *{* *RSA 3072 CC keys* *{* *subject-hash ebcd3885; issuer-hash ebcd3885; not-valid-before "May 9 22:30:59 2018 GMT"; issuer "/CN=Root CA"; not-valid-after "May 9 22:30:59 2019 GMT"; common-name "Root CA"; expiry-epoch 1557441059; ca yes; subject "/CN=Root CA"; public-key…* *Admin | Upload | config shared certificate import <Name> Import <Name>* *{* *private-key* ********; *}* *Admin | delete | config shared certificate device* *{* *certificate* *{* *RSA 3072 CC keys* *{* *subject-hash ebcd3885; issuer-hash ebcd3885; not-valid-before "May 9 22:30:59 2018 GMT"; issuer "/CN=Root CA"; not-valid-after "May 9 22:30:59 2019 GMT"; common-name "Root CA"; expiry-epoch 1557441059; ca yes; subject "/CN=Root CA"; public-key…*	Config
FMT_MOF.1 /ManualUpdate	Any attempt to initiate a manual update	*Installed cms software version <Software Version>*	System

[5] Importing CA certificate(s) or generating CA certificate(s) internally will implicitly set them as trust anchor.

FMT_SMF.1 FMT_SMF.1 /FFW FMT_SMF.1 /VPN	All management activities of TSF data	All user actions, security relevant or not, are logged in the configuration logs. • Start and reboot TOE Startup *The system is starting up.* Reboot/Shutdown *System restart requested by <Username>* *The system is shutting down due to CLI Initiated.* • Set time See FPT_STM_EXT.1 • Configure communication with external syslog *config shared log-settings syslog <Name>* • Ability to configure audit behavior Syslog over TLS *config shared log-settings syslog <Name> transport SSL* Syslog over IPsec *deviceconfig system route <Interface> <Address>* • Configure the authentication failure parameters for FIA_AFL.1 *deviceconfig setting management failed attempt <Value>* • Delete log file *log type <type> cleared by user <Username>* • Configure behavior of authentication failure lockout mechanism *deviceconfig setting management lockout-time <Value>* • Enable and configure TLS/HTTPS/SSH In FIPS-CC mode, these protocols are enabled by default and cannot be disabled. HTTP and telnet are disabled permanently. • Configure thresholds for SSH rekeying *deviceconfig system ssh session-rekey mgmt <Value>* • Create a local user *config mgt-config users <Username>* • Configure local authentication *config mgt-config users <Username> client-certificate-only yes* *config mgt-config users <Username> phash* • Initiate and verify software updates *Installed cms software version <Software Version>* • Configure time interval of session inactivity	Config

<table>
<tr><td></td><td></td><td><i>deviceconfig setting management idle-timeout <Value></i>
• Configure the login banner
<i>deviceconfig system login-banner <Banner></i>
• Configure the firewall rules
<i>vsys vsys1 rulebase security rules <Name></i>
• Configure the lifetime for IPsec SAs
<i>network ike crypto-profiles ipsec-crypto-profiles <Name></i>
• Configure the reference identifier for the peer
<i>network ike crypto-profiles ike-crypto-profiles <Name></i>
• Configure X.509 certificate profiles.
<i>config shared certificate-profile <Unique Name></i>
• Manage the TOE trust store and designate X509v3 certificates as trust anchor (also configure the cryptographic functionality)
<i>Admin | request/upload | config shared certificate device
{
certificate
{
RSA 3072 CC keys
{
subject-hash ebcd3885; issuer-hash ebcd3885; not-valid-before "May 9 22:30:59 2018 GMT"; issuer "/CN=Root CA"; not-valid-after "May 9 22:30:59 2019 GMT"; common-name "Root CA"; expiry-epoch 1557441059; ca yes; subject "/CN=Root CA"; public-key…</i>

<i>Admin | Upload | config shared certificate import <Name>
Import <Name>
{
private-key ********;
}</i>

<i>Admin | delete | config shared certificate device
{
certificate
{
RSA 3072 CC keys
{
subject-hash ebcd3885; issuer-hash ebcd3885; not-valid-before "May 9 22:30:59 2018 GMT"; issuer "/CN=Root CA"; not-valid-after "May 9 22:30:59 2019 GMT"; common-name "Root CA"; expiry-epoch 1557441059; ca yes; subject "/CN=Root CA"; public-key</i>
• Ability to start and stop[6] services
<i>FIPS-CC Mode Enabled Successfully</i>
<i>System { dns-setting { servers { primary <DNS IPAddress>; }</i>

<u>All administrative actions</u></td><td></td></tr>
</table>

[6] To disable FIPS-CC mode requires a factory reset of the appliance which will zeroize all public/private keys, CSPs, configuration data and audit logs.

		<Admin> set vsys vsys1 rulebase security rules <VPN rule name> [<zone/interface>] *<Admin> move vsys vsys1 rulebase security rules <VPN rule name>*	
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	*Installed cms software version <Software Version>*	System
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1) [For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).]	*System time changed from <Old Date> <Old Time> to <New Date> <New Time> by <Username> from host <IP Address>*	System

FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	on UI (HTTPS):
		Session for user <Username> logged out via Web from <IP Address> timed out
		on CLI (SSH):
		Session for user <Username> via CLI from <IP Address> timed out
			System

FTA_SSL.3	The termination of a remote session by the session locking mechanism.	on UI (HTTPS):
		Session for user <Username> logged out via Web from <IP Address> timed out
		on CLI (SSH):
		Session for user <Username> via CLI from <IP Address> timed out
			System

FTA_SSL.4	The termination of an interactive session.	on UI (HTTPS):
		User <Username> logged out via Web from <IP Address>
		on CLI (SSH):
		User <Username> logged out via CLI from <IP Address>
			System

FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions [Identification of the initiator and target of failed trusted channels establishment attempt.]	on TLS (syslog) **Initiation** *Syslog connection established to server['AF_INET.<IP>:<port>.']* **Termination** *Syslog connection broken to server['AF_INET.<IP>:<port>.']* **Failure** *Syslog connection failed to server['AF_INET.<IP>:<port>.']* On VPN connection **Initiation** *11/15/2019 6:27 vpn ikev2-nego-child-start branchgw IKEv2 child SA negotiation is started as initiator, rekey. Initiated SA: <Source IP>[500]-<Destination IP>[500] message id:0x00000000.* **Termination** *11/15/2019 6:27 ikev2-nego-ike-dpd-dn, <IPsec peer>, IKEv2 IKE SA is down determined by DPD* **Failure** *11/10/2019 01:54:51 vpn critical ikev2-nego-failcert IKEv2 certificate authentication failed. Peer certificate revocation status couldn't be checked due to end-entity certificate 'CN=20.1.1.20, O=Internet Widgits Pty Ltd, ST=Some State, C=AU*	System

FTP_TRP.1/ Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	on UI (HTTPS) **Initiation** *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, SSL Negotiation finished successfully* **Termination** *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, close notify* **Failure** *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, unknown state, unknown protocol* *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, unknown state, no shared cipher* *client: <Client IP Address>:<Port Number> server: <Server IP Address>:443, unknown state, handshake failure* *SSL handshake failed - (NONE)* on CLI (SSH) **Initiation** *ssh: session open from <Source IP Address> to <IP Address> for uid <ID> user <Username> on tty* **Termination** *ssh: session close from <Source IP Address> to <IP Address> for uid <ID> user <Username> on tty* **Failure** *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching mac found: client <Client Cipher> server <Server Cipher>* *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching cipher found: client <Client Cipher> server <Server Cipher>* *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching key exchange method found. client <Client Cipher> server <Server Cipher>*	System

FFW_RUL_EXT.1	Application of rules configured with the 'log' operation Additional Audit Record Contents: Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface	*11/10/2019 1:08 10108000519 TRAFFIC end <Source IP> <Destination IP> VPNRule ike vsys1 ISP ISP ethernet3/2 ethernet3/2 1 500 500 0 0 0x19 udp allow 8198 6734 1464 37 11/10/2017 0:50 452 any 0 6.48E+18 0x0 United States United States 0 33 4 agedout aged-out 0 0 0 0 PA-7050 from-policy*	Traffic
FFW_RUL_EXT.2	Dynamical definition of rule, Establishment of a session	*9/25/2019 15:36 10108000519 TRAFFIC end 1 <Source IP> <Destination IP> rule2 **ftp** vsys1 untrust trust ethernet3/6 ethernet3/5 570425425 1 54425 21 0 0 0x1c tcp allow 2506 1018 1488 31 6 any 0 6.46871E+18 0x0 United States United States 0 16 15 tcp-fin 0 0 0 0 PA-7050 from-policy 0 0 N/A*	Traffic
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation Additional Audit Record Contents: Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface	*11/10/2019 1:08 10108000519 TRAFFIC end <Source IP> <Destination IP> VPNRule ike vsys1 ISP ISP ethernet3/2 ethernet3/2 1 500 500 0 0 0x19 udp allow 8198 6734 1464 37 11/10/2017 0:50 452 any 0 6.48E+18 0x0 United States United States 0 33 4 aged-out aged-out 0 0 0 0 PA-7050 from-policy*	Traffic
	Indication of packets dropped due to too much network traffic Additional Audit Record Contents: TOE interface that is unable to process packets	*9/25/2019 18:45 10108000519 THREAT flood 0.0.0.0 0.0.0.0 not-applicable vsys1 untrust untrust 1 0 0 0 0 0x2000 tcp drop TCP Flood(8501) any critical client-to-server 6.4699E+18 0x0 0.0.0.0-0.255.255.255 0.0.0.0-0.255.255.255 0 0 0 0 0 0 0 0 PA-7050 0 0 N/A flood AppThreat-0-0 0x0*	Threat

Table 8: Required Auditable Events

The auditable administrative actions are identified in the above table for FMT_SMF.1.

5 Identification and Authentication

This section and subsequent sections describe the required guidance assurance activities as specified in the NDcPP. Before any configuration can be performed on the TOE, the user must login. Other than viewing the login banner and pinging (i.e., ICMP echo request and reply) the TOE, no other action is provided to the users until they are successfully logged in. After that, the actions available will be based on the role and privileges assigned to that user.

5.1 Logging into the TOE

5.1.1 User Login to Web Interface

The TOE has a web interface that users can use to perform administrative, management, and analysis tasks. Users can access the web interface by logging into the appliance using a web browser. The following table lists web browser compatibility.

Browser	Required Enabled Options and Settings
Chrome (version 96 or later)	JavaScript, cookies, Transport Layer Security (TLS) v1.2
Firefox (version 94.0.2 or later)	JavaScript, cookies, Transport Layer Security (TLS) v1.2
Safari (version 12.0.3 or later on Mac, and version 5.1.7 or later on Windows and iOS)	JavaScript, cookies, Transport Layer Security (TLS) v1.2
Microsoft Edge (Release 942 or later)	JavaScript, cookies, Transport Layer Security (TLS) v1.2

Table 9: Web Browser Requirements

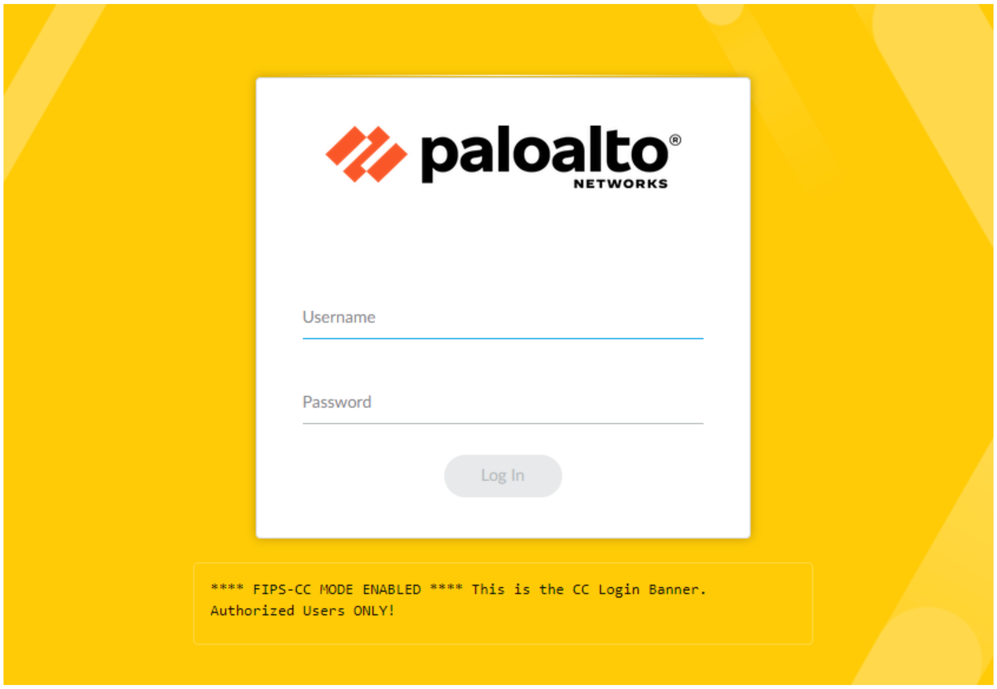
In addition, a CLI is provided to manage the TOE. This interface provides the equivalent operations provided by the web interface. For ease of use, it is highly recommended that the users use the web interface over the CLI. For automation purposes, it is highly recommended that the users use the CLI or API over the web interface.

The TOE provides a GUI management interface and CLI/API to support security management of the TOE. The GUI or API is accessible via direct connection to the management port on the device (local access) over HTTPS, or remotely over HTTPS or HTTPS over IPsec. The CLI is accessible via direct connection to the management port on the device (local access) over SSHv2, or remotely over SSHv2.

If you are the first user to log into the appliance after it is installed, you must log in using the predefined, factory-default administrative (**admin**) user account and default password. By default, your session automatically logs out after 60 minutes of inactivity. To configure certificate-based authentication, please see section 6.8.2.

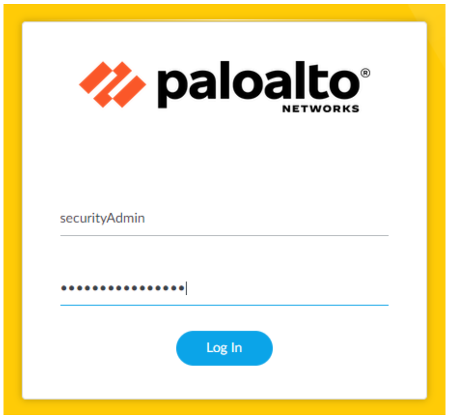
1. Direct the web browser to https://hostname/, where hostname corresponds to the host name of the TOE. You can also use the IP address of the TOE.

   The TOE login page appears.



```
**** FIPS-CC MODE ENABLED **** This is the CC Login Banner.
Authorized Users ONLY!
```

2. In the **Username** and **Password** fields, type your username and password.



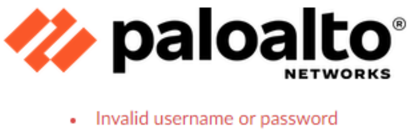
securityAdmin

••••••••••••••••

3. Click **Log In**.

   The default start page appears if the authentication is successful.

   If authentication fails, the following error message is displayed:



- Invalid username or password

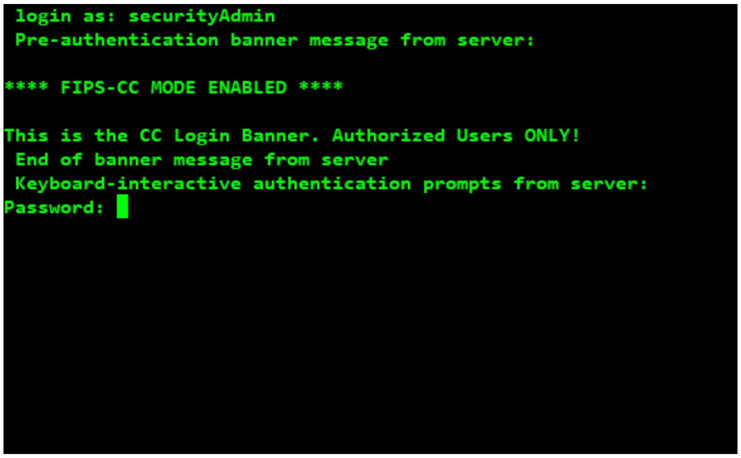
5.1.2 User Login to CLI Remotely

1. Direct an SSHv2 connection to the appliance at ***hostname***, where hostname corresponds to the host name of the appliance. You can also use the IP address of the appliance.

   The **login in:** command prompt appears.

2. Type your username and press **Enter**.

   The login banner and **Password:** prompt appear.



```
 login as: securityAdmin
 Pre-authentication banner message from server:

**** FIPS-CC MODE ENABLED ****

This is the CC Login Banner. Authorized Users ONLY!
 End of banner message from server
 Keyboard-interactive authentication prompts from server:
Password: 
```

3. Type your password and press **Enter**.

   The command prompt appears if the authentication is successful.

   If authentication fails, the following error message is displayed:

```
Access denied
```

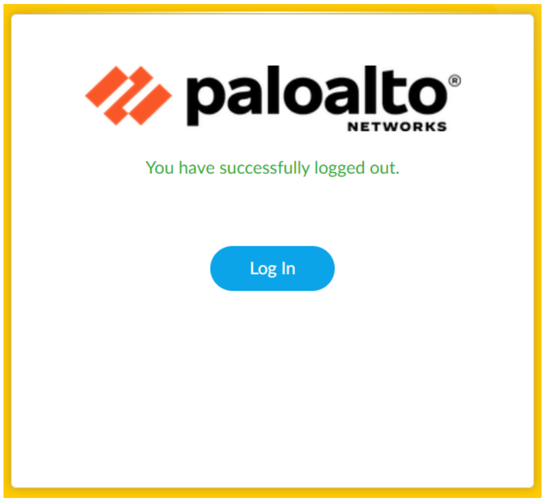
5.1.3 User Login to CLI Locally

All localized TOE management will be done through the GUI/CLI/API via the direct RJ-45 Ethernet cable to the MGMT port using HTTPS or SSHv2. Use the IP Restriction feature (see section 6.1 for IP restrictions) to secure the appliance management access.

NOTE: Shell and local console access will be disabled in FIPS-CC mode.

5.1.4 User Logout

1. For web session, from the lower left corner, click **Logout**.



You have successfully logged out.

2. Close the web browser.
3. For CLI session, enter the **exit** command.
4. The session will close.

API HINT: The equivalent XML API calls are

- https://<TOE>/api/?type=op&cmd=<exit></exit>&key=<APIkey>

6 Evaluated Configuration

This section describes the required steps to put the TOE in the CC evaluated configuration.

The delivered TOE may not have the correct evaluated version identified in section 1.2. Execute the **show system info** command to verify the version. If the version does not match, please proceed to section 7.12 to upgrade the TOE to the evaluated version. In addition, the following configuration actions **must** be taken:

- The administrator **must** enable FIPS-CC mode.
- The administrator **must** change the default password on the TOE.
- The administrator **must** restrict all cryptographic mechanisms to NDcPP-Approved algorithms and key sizes.
- The administrator **must** enable CC-specific logging to enable verbose logging level that meets the NDcPP audit requirements.

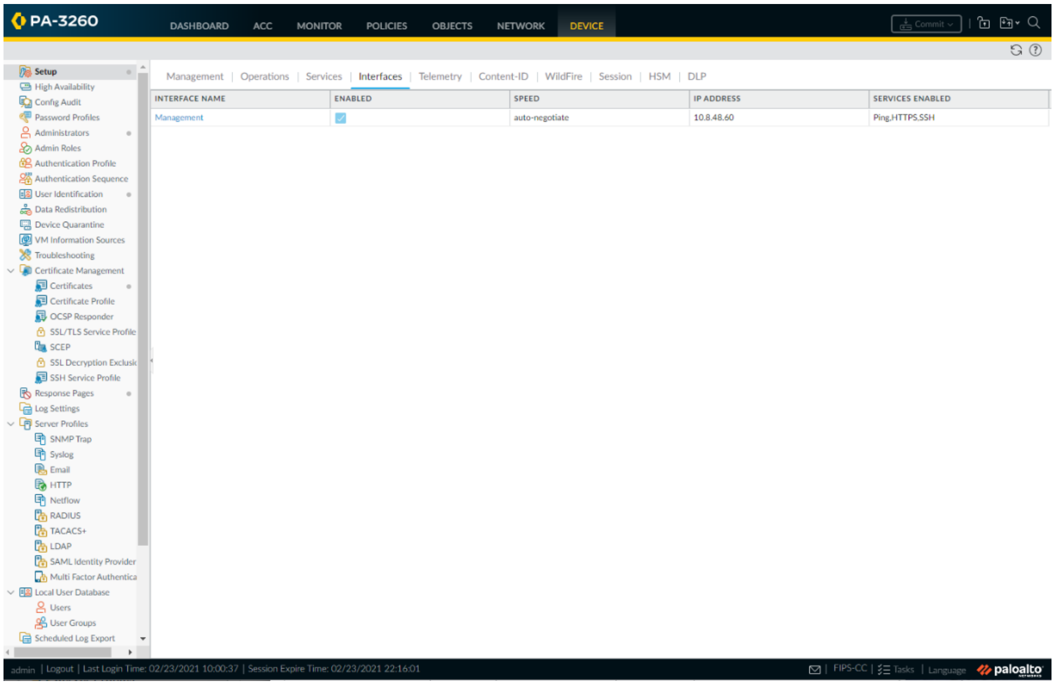
The TOE by default only supports SSH, HTTPS, and HTTPS over IPsec security protocols for management. Telnet and HTTP are not enabled for management and **must** not be enabled. The TOE is required to support only the cipher suites, version, algorithms, and protocols claimed in the Security Target. HTTPS, IKE/IPsec, SSH and TLS connection settings (TLS ciphersuites, IKE/IPsec algorithms, SSH key exchange algorithms, key sizes, etc.) are configured or restricted automatically when FIPS-CC mode is enabled. For the remaining settings such as SSH encryption and rekey, please follow the guide in sections 6.4 and 6.5. While not required by the NDcPP, the administrator should configure the Permitted IP feature to restrict which computers can access the TOE and from specific IP addresses.

6.1 Restrict Management Access (Required)

By default, port 443 (HTTPS), which is used to access the web interface or API, and port 22 (SSH), which is used to access the command line, are enabled for any IP address. To configure the permitted IP (also known as Whitelist), go to the management general settings.

1. Login with Administrator Role.
2. Select **Device> Setup > Management > Interfaces**.

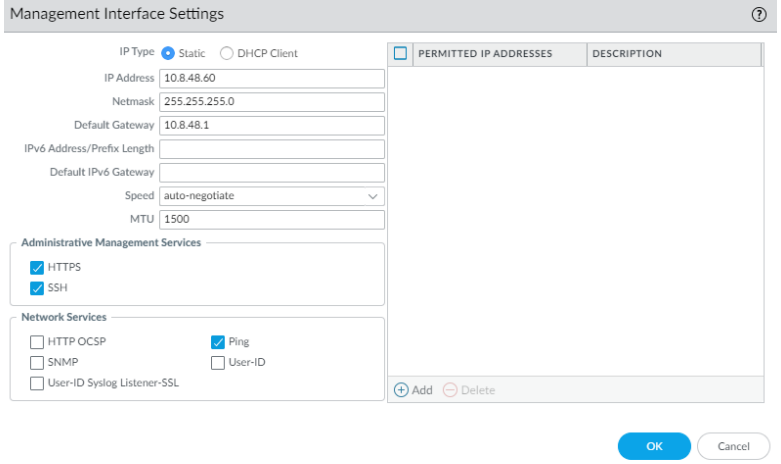
   The Interfaces Tab page appears.



INTERFACE NAME	ENABLED	SPEED	IP ADDRESS	SERVICES ENABLED
Management	☑	auto-negotiate	10.8.48.60	Ping,HTTPS,SSH

3. Click on the **Management** interface under the Interface Name column. The management interface is enabled by default.

   The Management Interface Settings page appears.



Management Interface Settings

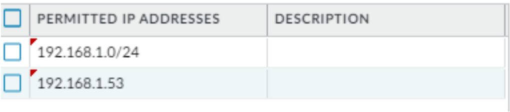
IP Type ● Static ○ DHCP Client
IP Address 10.8.48.60
Netmask 255.255.255.0
Default Gateway 10.8.48.1
IPv6 Address/Prefix Length
Default IPv6 Gateway
Speed auto-negotiate
MTU 1500

Administrative Management Services
☑ HTTPS
☑ SSH

Network Services
□ HTTP OCSP ☑ Ping
□ SNMP □ User-ID
□ User-ID Syslog Listener-SSL

□ PERMITTED IP ADDRESSES	DESCRIPTION

4. In the Permitted IP Address field, click **Add**. An empty list (default) specifies that access is available from any IP address.
    - Specify a single IPv4 or IPv6 address.
    - Specify a subnet.
    - Optionally, enter a description.



□	PERMITTED IP ADDRESSES	DESCRIPTION
□	192.168.1.0/24	
□	192.168.1.53	

NOTE: In FIPS-CC mode, the management security protocols are restricted to HTTPS, HTTPS over IPsec, and SSH. The administrator cannot enable HTTP or telnet in FIPS-CC mode.

5. To delete an entry, select that row and click **Delete**.
6. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

CLI HINT: The equivalent CLI commands are **set deviceconfig system permitted-ip <IP/Netmask>** and **delete deviceconfig system permitted-ip <IP/Netmask>**.

API HINT: The equivalent XML API calls are (need to edit the value and API key)

- **https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system/permitted-ip&element=<entry name='1.1.1.1'></entry>&key=<APIkey>**
- **https://<TOE>/api/?type=config&action=delete&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system/permitted-ip&element=<entry name='1.1.1.1'></entry>&key=<APIkey>**

6.2 Enable FIPS-CC Mode (Required)

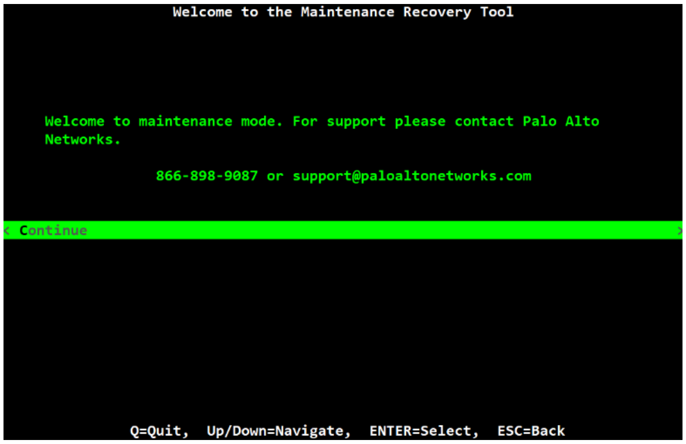
The administrator must enable FIPS-CC mode to automatically restrict the TLS version and cipher suites (including elliptical curves) to the Approved ones claimed in the Security Target (ST). There are additional features such as enabling the FIPS power-up self-tests, enabling FIPS mode, disabling non-Approved RNG, setting Approved DRBG to AES-CTR, restricting SSH key exchange algorithms, and enforcing other TLS required checks such as the ones specified in section 6 of RFC 6125 plus IPv4 addresses in the SAN or CN. When FIPS-CC mode is enabled, all key destruction activities occur in the manner specified by FCS_CKM.4. To be in the evaluated configuration, the administrator must enable FIPS-CC Mode.

NOTE: The administrator must still configure the SSH encryption algorithms and rekeying interval. No other SSH settings are required.

NOTE: The TLS ciphersuites are negotiated based on the public key algorithm (RSA vs ECDSA) in the TLS certificate and the TLS version(s) supported in the SSL/TLS Service Profile (TLSv1.1 [SHA-1 only] vs TLSv1.2 [SHA-256 and SHA-384]).

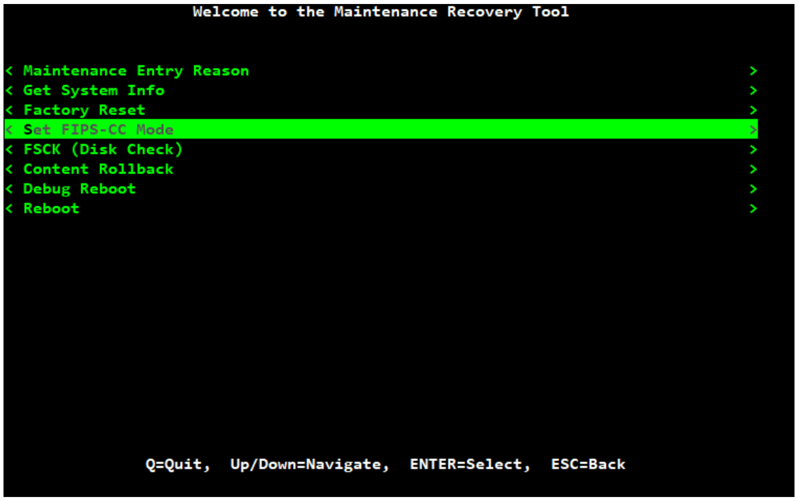
To enable FIPS-CC mode, first boot the TOE into the maintenance mode. From there, change the operational mode from normal mode to FIPS-CC mode.

1. Using SSH, login with Administrator Role.
2. Enter the following command: **debug system maintenance-mode**
3. Type **y** to confirm. The SSH session will disconnect.
4. It will take approximately 2 to 3 minutes for the TOE to boot up into maintenance mode. During this time, the HTTPS, HTTPS over IPsec, and SSH management sessions will be disabled.



```
                    Welcome to the Maintenance Recovery Tool



     Welcome to maintenance mode. For support please contact Palo Alto
     Networks.

                  866-898-9087 or support@paloaltonetworks.com

< Continue                                                                  >




               Q=Quit,  Up/Down=Navigate,  ENTER=Select,  ESC=Back
```

5. Using the local console, select **Continue** and press the Enter key.
6. Using the down arrow, select **Set FIPS-CC Mode** and press the Enter key.



```
                    Welcome to the Maintenance Recovery Tool

< Maintenance Entry Reason                                                  >
< Get System Info                                                           >
< Factory Reset                                                             >
< Set FIPS-CC Mode                                                          >
< FSCK (Disk Check)                                                         >
< Content Rollback                                                          >
< Debug Reboot                                                              >
< Reboot                                                                    >

               Q=Quit,  Up/Down=Navigate,  ENTER=Select,  ESC=Back
```

7. Select **Enable FIPS-CC Mode** and press the Enter key.
8. When prompted, select **Reboot**.
9. After the TOE passes all the FIPS power-up self-tests and switches to FIPS-CC mode, the administrator will see the following status: *FIPS-CC mode enabled successfully*.

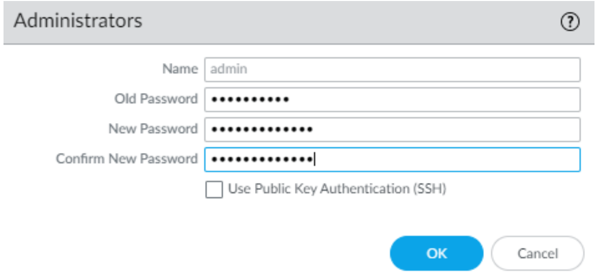
> **WARNING:** Enabling FIPS-CC Mode will completely zeroize the TOE, and all configurations and logs will be erased permanently.
>
> **WARNING:** Shell and local console access will be disabled. All further TOE management will be through the GUI/CLI locally via direct RJ-45 Ethernet cable and remotely using HTTPS/TLS/IPsec or SSHv2 client.

The shell and local console access are only allowed for pre-operational installation, configuration, and post-operational maintenance and trouble shooting. Once FIPS-CC mode is enabled, these access interfaces will be disabled unless you are in maintenance mode.

6.3 Change Default Admin Password (Required)

NOTE: The default predefined administrator password (admin/paloalto) must be changed on the first log in on a device. The new password must be a minimum of eight characters and include three out of four character types (lowercase, uppercase, number or special character). This change does not affect other user-defined administrator users.

1. Login as **admin** with the default password **paloalto**.
2. Select **Device > Administrators**.
3. Click on the **admin** user.
4. Enter the old password.
5. Enter the new password twice.



Administrators

Name admin

Old Password ••••••••••

New Password •••••••••••••

Confirm New Password •••••••••••••

□ Use Public Key Authentication (SSH)

6. Click **OK**.
7. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

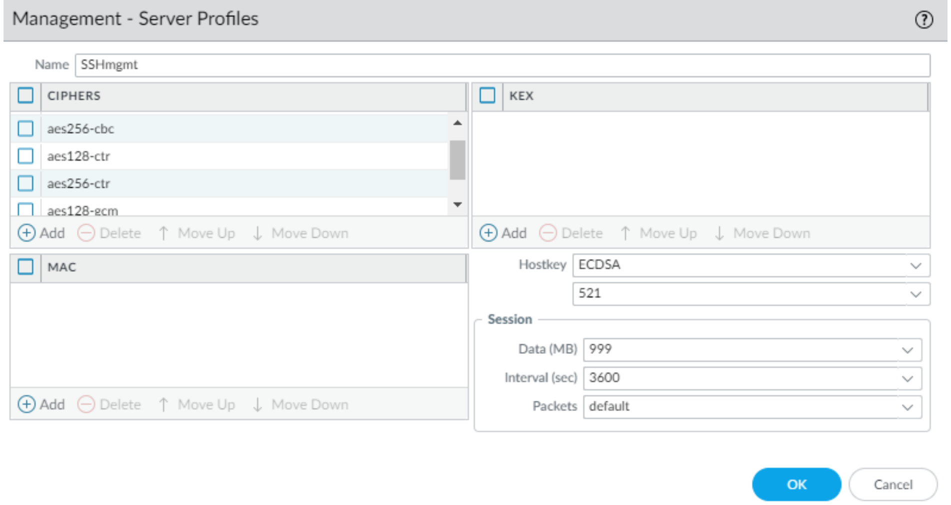
CLI HINT: The equivalent CLI command is **set password**.

6.4 Configure SSH Encryption Algorithms (Required)

In FIPS-CC mode, the TOE supports all AES key sizes including 192 for CBC and CTR. The NDcPP does not allow this 192 bits key size for SSH. Use the following steps to configure 128 and 256 bits only:

Web UI

1. Login with Administrator Role.
2. Select **Device** > **Certificate Management** > **SSH Service Profile** > **Management – Server Profiles** > **Add**.
3. Enter a **Name**.
4. Under **CIPHERS**, add AES algorithms with key sizes of 128 and 256 bits.



Management - Server Profiles

Name: SSHmgmt

CIPHERS:
- aes256-cbc
- aes128-ctr
- aes256-ctr
- aes128-gcm

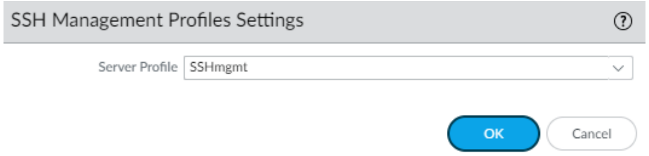
KEX

MAC

Hostkey: ECDSA, 521

Session
- Data (MB): 999
- Interval (sec): 3600
- Packets: default

5. Click **OK**.
6. Select **Device** > **Management** > **SSH Management Profiles Settings**. Click on the edit gear ⚙ icon.
7. Under the **Server Profile** drop-down list, select the SSH Server Profile you created above. Click **OK**.



SSH Management Profiles Settings

Server Profile: SSHmgmt

8. **Commit** to save the changes.
9. On the CLI, enter **run set ssh service-restart mgmt** to restart the SSH server.
10. Type **y** to confirm.

CLI

1. Using SSH, login with Administrator Role.

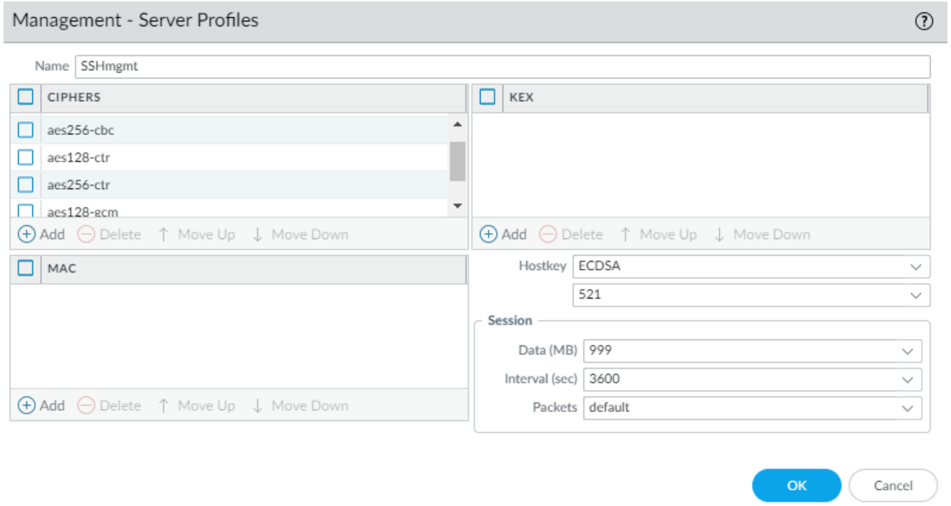
2. Enter configuration mode using **configure** command.
3. Enter the following commands:
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes128-cbc**
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes128-ctr**
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes128-gcm**
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes256-cbc**
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes256-ctr**
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes256-gcm**
4. Enter **set deviceconfig system ssh mgmt server-profiles <Profile_Name>** to apply the profile to the management interface.
5. Enter **commit** to save the changes.
6. Enter **run set ssh service-restart mgmt** to restart the SSH server.
7. Type **y** to confirm.

6.5 Configure SSH Rekey Interval (Required)

When FIPS-CC mode is enabled, the SSH rekeying will occur approximately at 1 hour of time or after 1 GB of data has been transmitted, whichever occurs first. To change the SSH rekeying interval, please follow the instructions below.

Web UI

1. Login with Administrator Role.
2. Select **Device > Certificate Management > SSH Service Profile > Management – Server Profiles > Add**.
3. Enter a **Name**.
4. Under **Session**, configure the **Data (MB)** to a value less than 1 GB and **Interval (sec)** to a value less than 1 hour.



Management - Server Profiles

Name: SSHmgmt

□	CIPHERS
□	aes256-cbc
□	aes128-ctr
□	aes256-ctr
□	aes128-gcm

□ KEX

□ MAC

Hostkey: ECDSA

521

Session

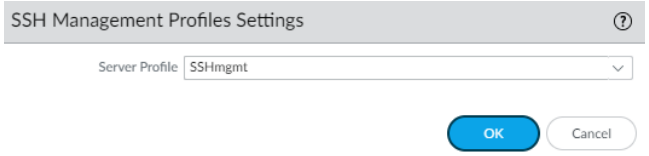
Data (MB): 999

Interval (sec): 3600

Packets: default

⊕ Add ⊖ Delete ↑ Move Up ↓ Move Down
⊕ Add ⊖ Delete ↑ Move Up ↓ Move Down
⊕ Add ⊖ Delete ↑ Move Up ↓ Move Down
OK
Cancel

5. Click **OK**.
6. Select **Device > Management > SSH Management Profiles Settings**. Click on the edit gear ⚙ icon.
7. Under the **Server Profile** drop-down list, select the SSH Server Profile you created above. Click **OK**.



SSH Management Profiles Settings

Server Profile: SSHmgmt

8. **Commit** to save the changes.
9. On the CLI, enter **run set ssh service-restart mgmt** to restart the SSH server.
10. Type **y** to confirm.

CLI

1. Using SSH, login with Administrator Role.
2. Enter configuration mode using **configure** command.
3. Enter the following commands:
   - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> session-rekey interval <10-3600 seconds>**
   - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> session-rekey data <10-4000 MB>**

WARNING: The data limit must be 1024 MB or less in the evaluated configuration.

4. Enter **set deviceconfig system ssh mgmt server-profiles <Profile_Name>** to apply the profile to the management interface.
5. Enter **commit** to save the changes.
6. Enter **run set ssh service-restart mgmt** to restart the SSH server.
7. Type **y** to confirm.

6.6 Configure SSH Public-Key Authentication (Recommended)

Perform the following steps on a remote workstation:

1. Log in as a privileged user.
2. Generate the SSH keypair.

Note: Currently, only RSA keypair is supported and only generate RSA 2048 bits or higher.

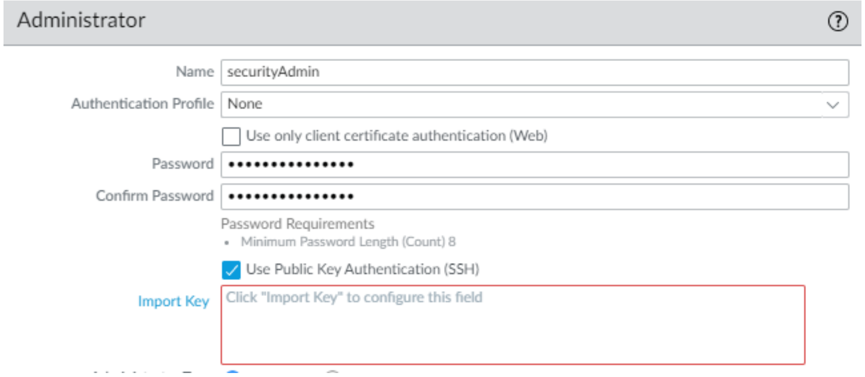
3. Enter **ssh-keygen -t rsa -b 3072**
4. Enter an optional passphrase, if desired.

> **NOTE:** ECDSA keypair is not supported at the moment.

On the TOE UI:

1. Login with Administrator Role.
2. Select **Device > Administrators**. Click on the user you want to configure SSH public-key authentication for. In the example below, ‘admin2’ is the chosen user.

   The Administrator page appears



Administrator

Name	securityAdmin
Authentication Profile	None
	☐ Use only client certificate authentication (Web)
Password	•••••••••••••••
Confirm Password	•••••••••••••••
	Password Requirements • Minimum Password Length (Count) 8
	☑ Use Public Key Authentication (SSH)
Import Key	Click "Import Key" to configure this field

3. Check the **Use Public Key Authentication (SSH)** checkbox.
4. Click **Import Key** to import the SSH public key (e.g., id_rsa.pub). This is the public key part of the SSH keypair generated above.
5. Click **Browse…** to find the text file with the public key.

> **NOTE:** Copy the public key into a non-rich text file. The UI will auto format it into Base64.

6. Click **OK** to save the changes. Click **OK** again to save the changes.
7. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

CLI HINT: The equivalent CLI commands are **set mgt-config users <Username> public-key <Value>** and **delete mgt-config users <Username> public-key <Value>**. The **<Value>** must be Base64 encoded (e.g., linux$: base64 id_rsa.pub).

On the same remote workstation:

1. Log into the remote machine as a privileged user.
2. Attempt to log in as ‘admin2’ using the SSH public-key authentication.
    a. Enter **ssh admin2@<IP Address>**
    b. Verify access is allowed without entering the password.

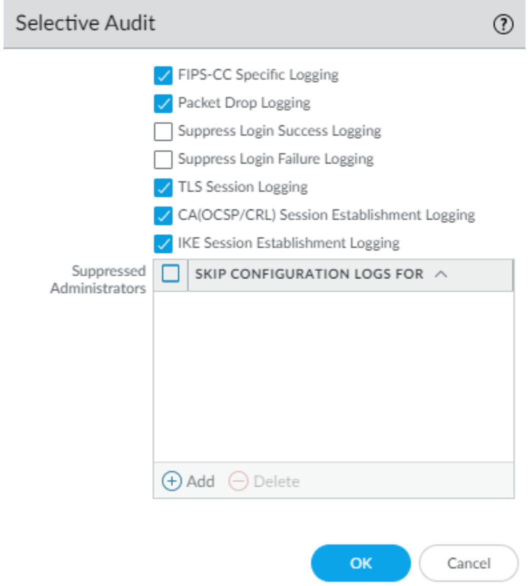
NOTE: The passphrase is different from the password. The passphrase, if set above, is used to protect the SSH private key and will be prompted each time the private key is accessed.

NOTE: If StrictHostKeyChecking is enabled on the SSH client, the user may need to add the SSH server (TOE) host key to the known hosts. Use this command if prompted to do so: **ssh-keygen -f "/home/user/.ssh/known_hosts" -R <IP Address>**

6.7 Configure Auditing Settings (Required)

On the TOE UI:

1. Login with Administrator Role.
2. Select **Device > Log Settings**.
3. Scroll down to the Selective Audit section.
4. Click on the ⚙ gear setting.
5. Check the **FIPS-CC Specific Logging**, **Packet Drop Logging**, **TLS Session Logging**, **CA(OCSP/CRL) Session Establishment Logging** and **IKE Session Establishment Logging** checkboxes.



Selective Audit

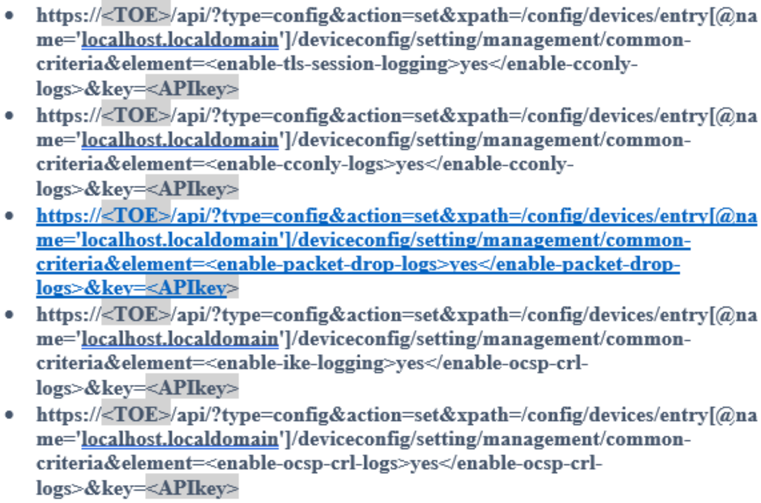
☑ FIPS-CC Specific Logging
☑ Packet Drop Logging
☐ Suppress Login Success Logging
☐ Suppress Login Failure Logging
☑ TLS Session Logging
☑ CA(OCSP/CRL) Session Establishment Logging
☑ IKE Session Establishment Logging

Suppressed Administrators: ☐ SKIP CONFIGURATION LOGS FOR

6. Click **OK** to save the changes.
7. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

CLI HINT: The equivalent CLI commands are **set deviceconfig setting management common-criteria enable-tls-session-logging yes, set deviceconfig setting management common-criteria enable-cconly-logs yes, set deviceconfig setting management common-criteria enable-packet-drop yes, set deviceconfig setting management common-criteria enable-ike-logging yes** and **set deviceconfig setting management common-criteria enable-ocsp-crl-logs yes**.

API HINT: The equivalent XML API calls are (need to edit the value and API key)



- https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management/common-criteria&element=<enable-tls-session-logging>yes</enable-cconly-logs>&key=<APIkey>
- https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management/common-criteria&element=<enable-cconly-logs>yes</enable-cconly-logs>&key=<APIkey>
- https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management/common-criteria&element=<enable-packet-drop-logs>yes</enable-packet-drop-logs>&key=<APIkey>
- https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management/common-criteria&element=<enable-ike-logging>yes</enable-ocsp-crl-logs>&key=<APIkey>
- https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management/common-criteria&element=<enable-ocsp-crl-logs>yes</enable-ocsp-crl-logs>&key=<APIkey>

6.8 Secure Connection Settings

6.8.1 Syslog Server Connection Settings (Required)

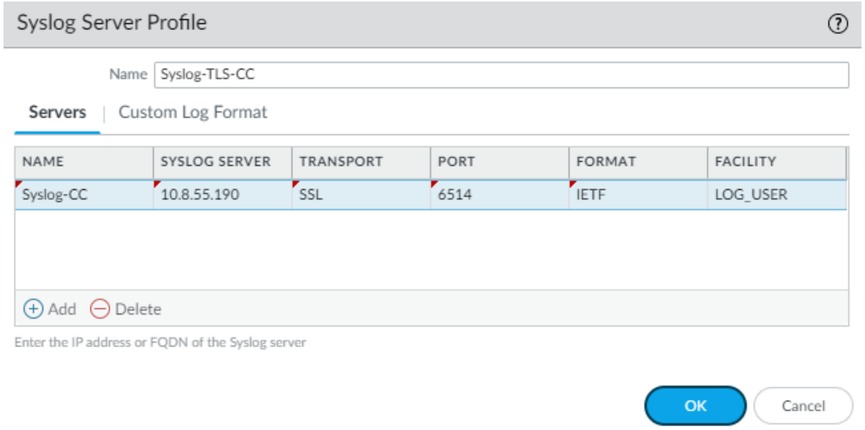
The TOE can be configured to forward generated audit records to an external syslog server in real-time. When configured, the TOE automatically converts the audit records to syslog format before forwarding them to the external syslog server. Audit records are converted and forwarded to the external syslog as they are locally written to the log files. The TOE automatically attempts to re-connect to the external syslog server should the TLSv1.2 channel be broken.

Syslog over TLS connection fails if the syslog server certificate does not meet any of the following criteria:

- The server certificate has been revoked or modified.
- The server certificate is not signed by the CA with cA flag set to TRUE.
- The server certificate is not signed by a trusted CA in the certificate chain.
- The server certificate Common Name (CN) or Subject Alternative Name (SAN) has FQDN (hostname) or IP address that does not match the configured hostname or IP address (i.e., expected reference identifier). SAN takes priority over CN.
- The server certificate must have either OCSP or CRL revocation information but **not** both.

Configure a Syslog Server Profile:

1. Login with Administrator Role.
2. Select **Device > Server Profiles > Syslog**.
3. Click **Add** and enter a **Name** for the profile.
4. On the **Servers** tab, click **Add**, and enter the following information:
   a) Name: **<Syslog Server Name>**
   b) Syslog Server: **<IP Address or Hostname>**
   c) Transport: **SSL**
   d) Port: **<Port>**
   Note: The default port is 6514.
   e) Format: **IETF**
   f) Facility: **LOG_USER**



Syslog Server Profile

Name Syslog-TLS-CC

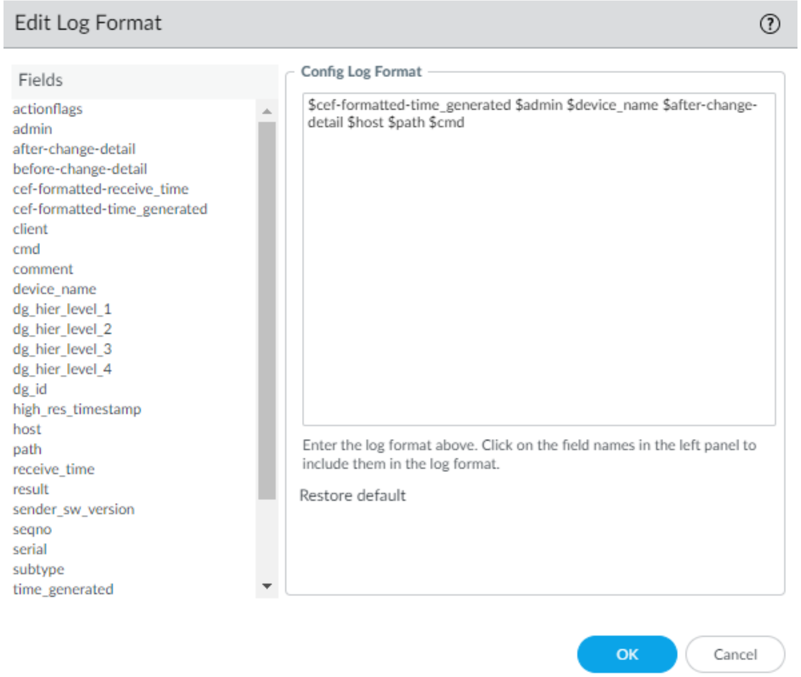
Servers | Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
Syslog-CC	10.8.55.190	SSL	6514	IETF	LOG_USER

Enter the IP address or FQDN of the Syslog server

NOTE: For the configuration logs, the default log format has the minimal level of details. Edit the log format to include more details if necessary.

5. Click on the **Custom Log Format** tab.
6. Click on **Config** in the log type column. Choose the fields of the config log you want to send the syslog server. For example, $after-change-detail field will show the TSF values that were changed.



Edit Log Format

Fields

actionflags
admin
after-change-detail
before-change-detail
cef-formatted-receive_time
cef-formatted-time_generated
client
cmd
comment
device_name
dg_hier_level_1
dg_hier_level_2
dg_hier_level_3
dg_hier_level_4
dg_id
high_res_timestamp
host
path
receive_time
result
sender_sw_version
seqno
serial
subtype
time_generated

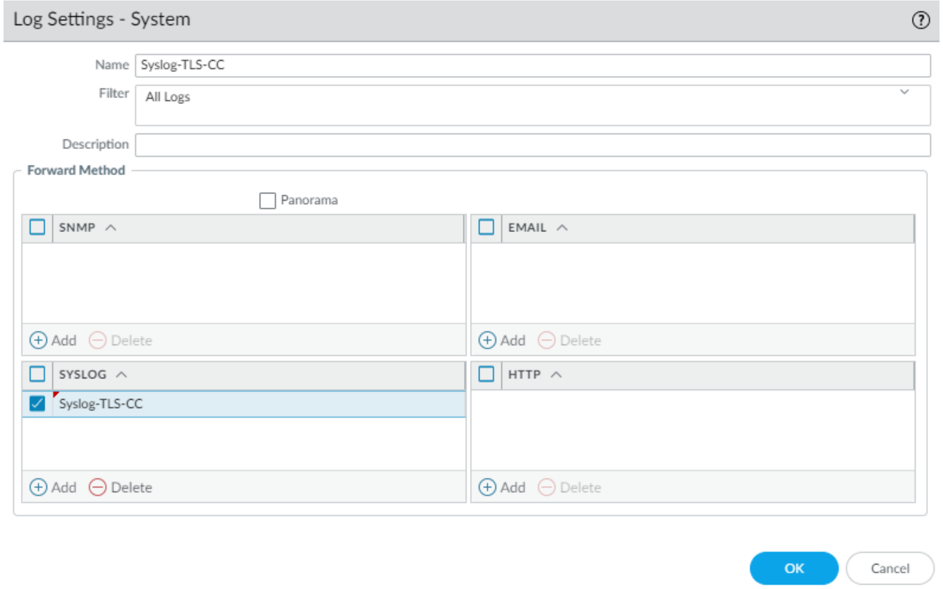
Config Log Format

$cef-formatted-time_generated $admin $device_name $after-change-detail $host $path $cmd

Enter the log format above. Click on the field names in the left panel to include them in the log format.

7. Click **OK** to exit.
8. Click **OK** to save the changes.
9. Select **Device > Log Settings**.
10. Enter **Name**.

11. On the **System** panel, click **Add**. On the **Syslog** panel, click **Add**. Select the syslog server profile created above via the drop-down list.



Log Settings - System

Name: Syslog-TLS-CC

Filter: All Logs

Description:

Forward Method

□ Panorama

☑ Syslog-TLS-CC

12. Click **OK** to save the changes.

13. On the **Configuration** panel, click **Add**. On the **Syslog** panel, click **Add**. Select the syslog server profile created above via the drop-down list.

14. Click **OK** to save the changes.

15. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

CLI HINT: The equivalent CLI commands are: **configure** and **set shared log-settings syslog <Name> server <Name> transport <UDP | TCP | SSL> port <1-65535> format <BSD | IETF> format config "$cef-formatted-time_generated $device_name $admin $cmd $path $after-change-detail $host"**.

Generate or Import the X.509v3 Certificates:

1. Login with Administrator Role.
2. Select **Device > Certificate Management > Certificates.**
3. To generate CA Certificates internally, do the following steps:
    a) Click **Generate**. The Generate Certificate page appears.
    b) Enter **Certificate Name** and **Common Name**.
        i. To generate an internal self-signed CA certificate, leave the **Signed By field** blank and check the **Certificate Authority** checkbox.

ii. To generate an internal subordinate CA, select a CA certificate in the drop-down list for the **Signed By** field and check the **Certificate Authority** checkbox.

iii. To generate a Certificate Signing Request (CSR), select the **External Authority (CSR)** in the drop-down list for **Signed By** field. Check the **Certificate Authority** checkbox only if this is a CSR for a CA certificate. If this CSR is for a leaf certificate, do not check the **Certificate Authority** checkbox.

c) Select **RSA** or **Elliptic Curve DSA** in the **Algorithm** field.

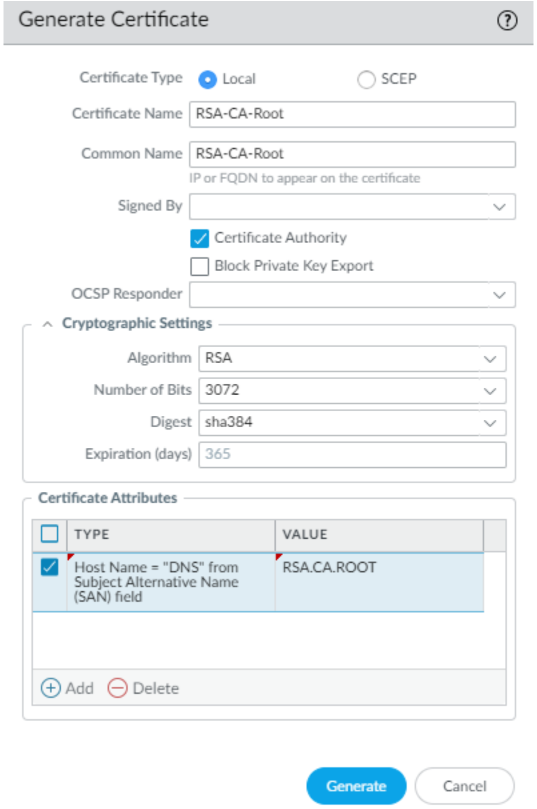
d) Select **key size** the **Number of Bits** field.

Note: RSA supports 2048, 3072, and 4096 bits. ECDSA supports 256 and 384 bits.

e) Select **SHA size** in the **Digest** field.

Note: The size supports SHA256, SHA384, and SHA512.

f) Optionally, enter additional certificate attributes such as SAN, Country, State, Locality, etc. using the **Add**. SAN is configured via Host Name and Organization Unit is configured via Department.



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name RSA-CA-Root

Common Name RSA-CA-Root

IP or FQDN to appear on the certificate

Signed By

☑ Certificate Authority

□ Block Private Key Export

OCSP Responder

Cryptographic Settings

Algorithm RSA

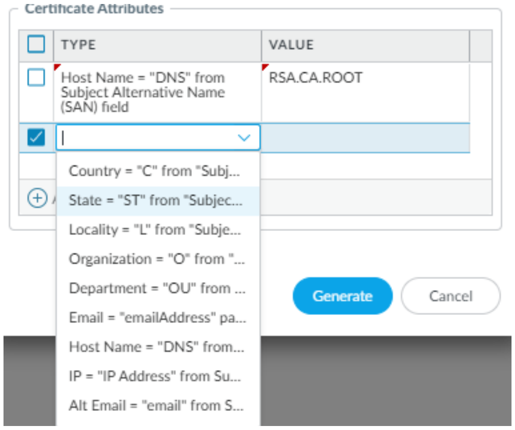
Number of Bits 3072

Digest sha384

Expiration (days) 365

Certificate Attributes

□	TYPE	VALUE
☑	Host Name = "DNS" from Subject Alternative Name (SAN) field	RSA.CA.ROOT

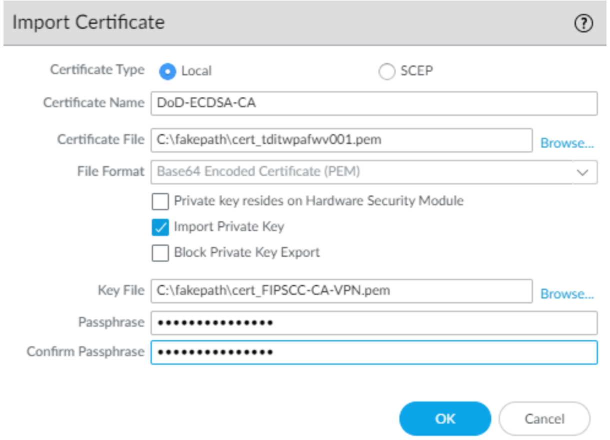


Certificate Attributes

☐	TYPE	VALUE
☐	Host Name = "DNS" from Subject Alternative Name (SAN) field	RSA.CA.ROOT
☑		

Country = "C" from "Subj...
State = "ST" from "Subjec...
Locality = "L" from "Subje...
Organization = "O" from "...
Department = "OU" from ...
Email = "emailAddress" pa...
Host Name = "DNS" from...
IP = "IP Address" from Su...
Alt Email = "email" from S...
Generate
Cancel

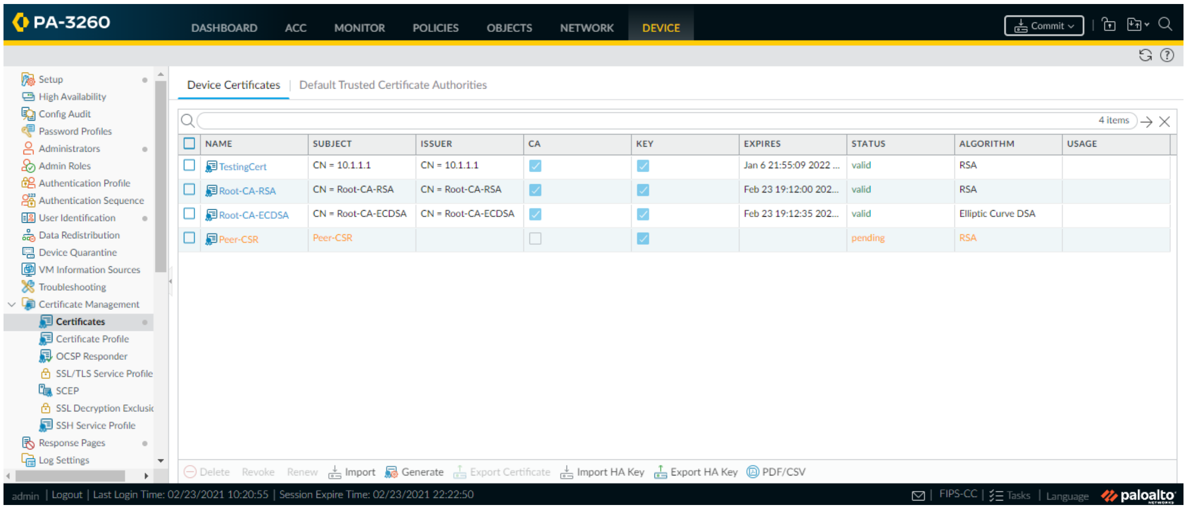
4. To import external CA Certificates, do the following steps:
   a) Click **Import**. The Import Certificate page appears.
   b) Enter **Certificate Name**. Do not include space if possible.
   c) Click **Browse…** to look for and select the CA file (PEM).
   d) Check the **Import private key** checkbox.
   e) Click **Browse…** to look for and select the CA Key file (PEM).
   f) If a passphrase is used to protect the private key, enter it in the **Passphrase** and **Confirm Passphrase** fields.



Import Certificate

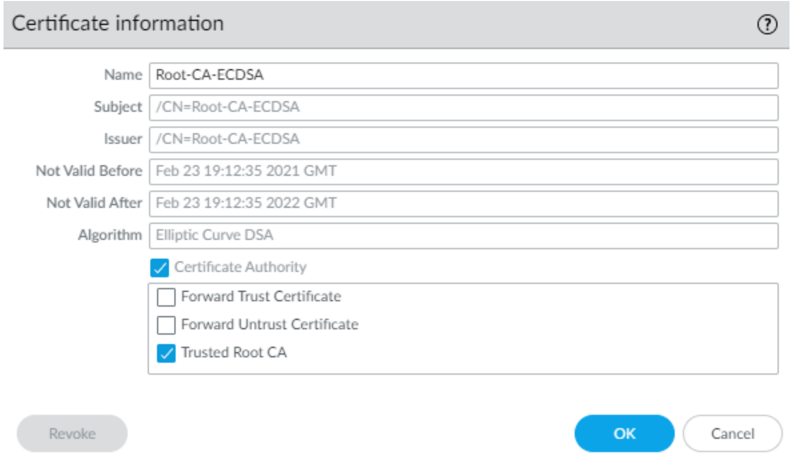
Certificate Type	● Local ○ SCEP
Certificate Name	DoD-ECDSA-CA
Certificate File	C:\fakepath\cert_tditwpafwv001.pem
File Format	Base64 Encoded Certificate (PEM)
	☐ Private key resides on Hardware Security Module
	☑ Import Private Key
	☐ Block Private Key Export
Key File	C:\fakepath\cert_FIPSCC-CA-VPN.pem
Passphrase	•••••••••••••••
Confirm Passphrase	•••••••••••••••

5. Click **OK** to save the changes.
6. In the screenshot below, there are two internally generated CAs, one CSR, and one imported external CAs.



☐	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
☐	TestingCert	CN = 10.1.1.1	CN = 10.1.1.1	☑	☑	Jan 6 21:55:09 2022 ...	valid	RSA	
☐	Root-CA-RSA	CN = Root-CA-RSA	CN = Root-CA-RSA	☑	☑	Feb 23 19:12:00 202...	valid	RSA	
☐	Root-CA-ECDSA	CN = Root-CA-ECDSA	CN = Root-CA-ECDSA	☑	☑	Feb 23 19:12:35 202...	valid	Elliptic Curve DSA	
☐	Peer-CSR	Peer-CSR		☐	☑		pending	RSA	

7. To add the CA certificate to the trust anchor, click on that CA certificate and check the **Trusted Root CA** checkbox. The CA certificate can be a root CA (best practice) or a non-root CA (not recommended).

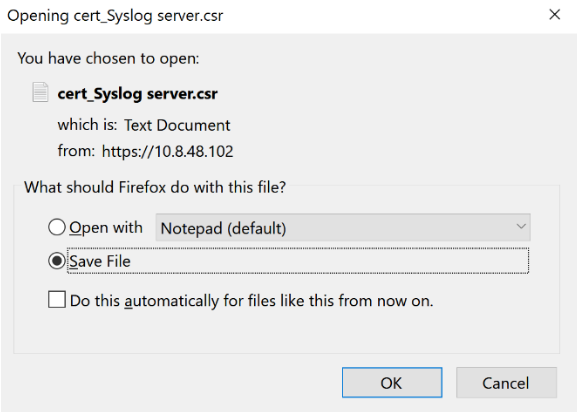


Name	Root-CA-ECDSA
Subject	/CN=Root-CA-ECDSA
Issuer	/CN=Root-CA-ECDSA
Not Valid Before	Feb 23 19:12:35 2021 GMT
Not Valid After	Feb 23 19:12:35 2022 GMT
Algorithm	Elliptic Curve DSA

☑ Certificate Authority
☐ Forward Trust Certificate
☐ Forward Untrust Certificate
☑ Trusted Root CA

8. Click **OK** to save the changes.

9. To export any certificate or CSR, click on the certificate or CSR you want to export, and select **Export Certificate**. For example, if you want to export the syslog server CSR, it will prompt you to save the file.



Opening cert_Syslog server.csr

You have chosen to open:

cert_Syslog server.csr

which is: Text Document

from: https://10.8.48.102

What should Firefox do with this file?

○ Open with Notepad (default)

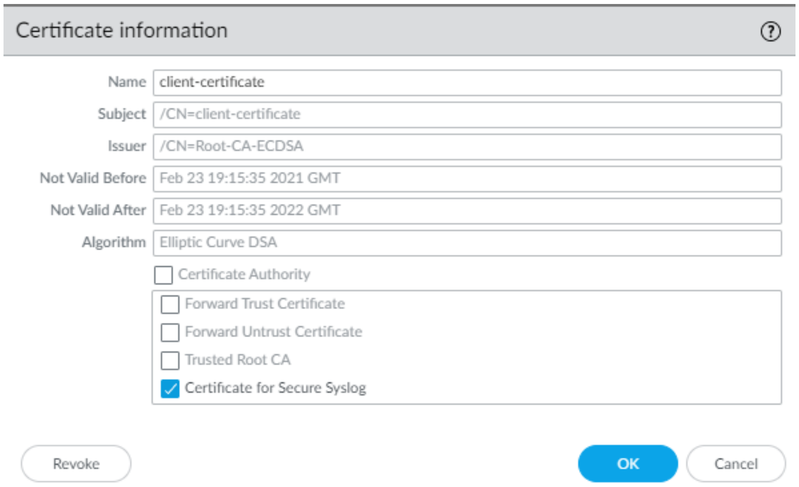
● Save File

□ Do this automatically for files like this from now on.

10. Click **OK** to download the file.
11. Take the CSR to an external CA to sign and issue a new syslog server certificate. This certificate is then installed on the external syslog server.

> **NOTE:** If the signed certificate is being imported to replace the CSR, it must have the same name in order for the TOE to associated it with the CSR.

12. (Optional) If TLS mutual authentication is required for the syslog connection, you must generate a TLS X.509v3 client certificate or import a X.509v3 client certificate. Check the **Certificate for Secure Syslog** checkbox to indicate this client certificate is used for the syslog connection. To revoke an internally generated client certificate, click the **Revoke** button.



Certificate information

Name	client-certificate
Subject	/CN=client-certificate
Issuer	/CN=Root-CA-ECDSA
Not Valid Before	Feb 23 19:15:35 2021 GMT
Not Valid After	Feb 23 19:15:35 2022 GMT
Algorithm	Elliptic Curve DSA

□ Certificate Authority

□ Forward Trust Certificate

□ Forward Untrust Certificate

□ Trusted Root CA

☑ Certificate for Secure Syslog

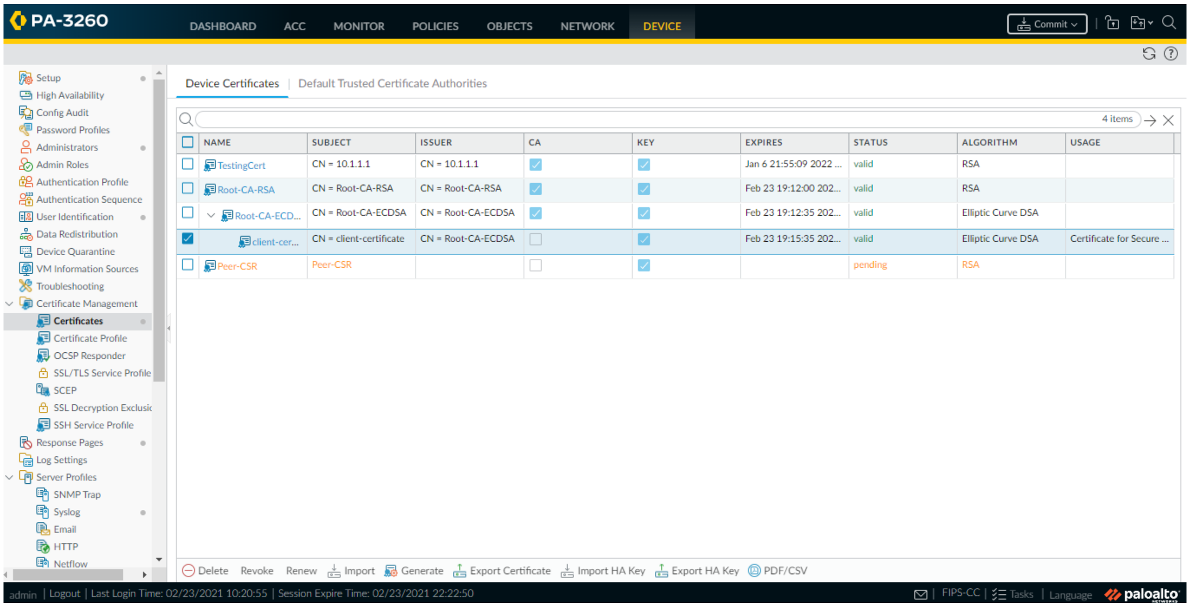
> **NOTE:** Only one client certificate can be designated as the certificate for the secure syslog connection.

> **WARNING:** Once the internal certificate has been revoked, it cannot be undone.

WARNING: If the certificate was generated from an internal CSR and signed by an external CA, you must import the external CA or CA(s) first before you can import the signed certificate (e.g., client certificate). Do not forget to commit after importing the CA. Otherwise, you will get this error message: "Import of <Name> failed. Certificate chain cannot be validated, required CAs not found". Root CA and Intermediate CA certificates cannot have spaces in their names.

WARNING: Do not import CA that has been expired or revoked. Do not import CA with duplicate Common Name (CN) with an existing CA. Delete the old CA first. The TOE will use the first CA with the matching CN from the signed certificate (Issuer field) which may not be the CA you want to use to validate the chain.

13. The **Status** column will indicate the status of the certificates (e.g., valid, pending, revoked). The **Usage** column will provide information about the certificate purpose (e.g., trusted anchor, secure syslog connection).



☐	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
☐	TestingCert	CN = 10.1.1.1	CN = 10.1.1.1	☑	☑	Jan 6 21:55:09 2022 ...	valid	RSA	
☐	Root-CA-RSA	CN = Root-CA-RSA	CN = Root-CA-RSA	☑	☑	Feb 23 19:12:00 202...	valid	RSA	
☐	Root-CA-ECD...	CN = Root-CA-ECDSA	CN = Root-CA-ECDSA	☑	☑	Feb 23 19:12:35 202...	valid	Elliptic Curve DSA	
☑	client-cer...	CN = client-certificate	CN = Root-CA-ECDSA	☐	☑	Feb 23 19:15:35 202...	valid	Elliptic Curve DSA	Certificate for Secure ...
☐	Peer-CSR	Peer-CSR		☐	☑		pending	RSA	

14. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

15. Reboot the TOE (or **request restart system**).

CLI HINT: The equivalent CLI command to generate certificate: **request certificate generate ca <yes | no> digest <sha256 | sha384 | sha512> algorithm <RSA | ECDSA> [<rsa-nbits 2048 | 3072> | <ecdsa-nbits 256 | 384>] certificate-name <Name of certificate object> name <IP or FQDN to appear on the certificate> passphrase <Pass-phrase for encrypting private key>**

CLI HINT: The equivalent CLI command to generate CSR: **request certificate generate signed-by external country-code <Country> state <State or Province> locality <Locality> organization <Organization> organization-unit <Department> hostname <SAN DNS> digest <sha256 | sha384 | sha512> algorithm <RSA | ECDSA> [<rsa-nbits 2048 | 3072> | <ecdsa-nbits 256 |**

384>] certificate-name <Name of certificate object> name <IP or FQDN to appear on the certificate>

CLI HINT: The equivalent CLI command to delete certificate: **#delete shared certificate <certificate object name>**

CLI HINT: The equivalent CLI commands to export or import certificate: **scp export certificate format pem certificate-name <Name of certificate object> to <username@ip_address>:<path>\<filename>**, and **scp import certificate format pem certificate-name <Name of certificate object> from <username@ip_address>:<path>\<filename>**.

Configure the external Syslog-ng Server:

1. Login as authorized administrator.
2. Install or use syslog-ng with version 3.7 or later (recommended).
3. Edit the syslog-ng configuration file by adding the following highlighted section below.
   vi /etc/syslog-ng/syslog-ng.conf

   If the config file is in a different location, search for with **find / -name syslog-ng.conf**
   # This command assumes you have root privilege or can sudo to root.

```
source s_Device {
            syslog(ip(0.0.0.0) port(6514)  # This port can be changed but must match the port configured in the TOE.
            transport("tls")
            tls(
              # Location of the private key of syslog server certificate.
              key-file(“/etc/ssl/Server.Key.pem”)  # Make sure the private key is not encrypted.
              # Location of the syslog server certificate.
              cert-file(“/etc/ssl/Server.Cert.pem”)  # Make sure the server cert has the correct EKU.

              ### The next line is needed if authentication mutual is required.
              ca-dir(“/etc/ssl”) # Location of the CA certificates and symbolic links. See below
                   ###   openssl x509 -noout -hash -in <CA certificate>
                   ###    ln -s <CA certificate> <Hash Output>.0
                   ###   This is the CA that signed the client certificate and other CA(s) in the chain.
                   ###   All CA certs must have basic constraints CA flag set to TRUE

              cipher-suite(AES128-SHA) # e.g., TLS Ciphersuite to be supported by the server
              ssl-options(no-sslv2, no-sslv3, no-tlsv1)  # TLS Version NOT supported by the server
                                                        # The TOE only supports TLSv1.2
              peer-verify(optional-trusted)  # required-trusted for mutual auth, optional-trusted for no mutual auth
            )
         );
};
```

```
destination d_Local {
    file("/var/log/Device_messages");   # The remote syslog file location can be configured here
};

log {
    source(s_Device); destination(d_Local);
};
```

4. Restart the syslog-ng server and make sure there is no error message.
   systemctl restart syslog-ng.service # This command may be different on different OS.

5. Use netstat to make sure the syslog-ng is listening.
   netstat -an | grep 6514

6. Make sure port 6514 is opened by the local firewall to allow the connection.

This section provides TLS troubleshooting tips. Use this command to view the debug syslog on the TOE (**tail follow yes mp-log syslog-ng.log**). The following are common reasons why the TLS connection fails and how to fix it:

- ClientHello but no ServerHello from Server
  - Make sure the private key (unencrypted) and server certificate are in the right directory and are accessible (e.g., permission to read).
- 'Unknown ca'
  - On the TOE, make sure the server certificate is signed and issued by valid CA chain with one of the CA certificates (i.e., Root CA) specified as the trust anchor.
  - If mutual authentication is configured, make sure the CA certificates are in the right directory with the correct name and symbolic links.
  - For syslog connection, the syslog server cannot be signed by the Root CA. At minimum, the syslog server certificate must be signed and issued by an Intermediate CA.
  - Reboot the TOE.
- 'Unknown certificate'
  - Make sure the revocation status is accessible.
  - CRL should be in PEM format.
  - If you change the server certificate and/or key on the syslog-ng server, make sure to restart the syslog server.
  - Certificate has explicit EC parameters.
- 'Certificate revoked'
  - Certificate is revoked[7].
- 'Certificate verify failed'
  - Certificate has invalid Key Usage (KU) or Extended Key Usage (EKU) field value.

[7] To clear CRL or OCSP cache, type **debug sslmgr delete crl all** or **debug sslmgr delete ocsp all**.

This section provides CC X509v3 certificate checks when FIPS-CC mode is enabled.

- CAs must have CA flag set to TRUE.
- CAs must have CRLsign in the Key Usage field and OSCP Responder must have OCSPsigning in the Extended Key Usage field.
- Server certificate must have CA flag set to FALSE.
- Server certificate must have ServerAuth in the Extended Key Usage field. (for client certificate, ClientAuth instead of ServerAuth)
- Server certificate must have digitalSignature in the Key Usage field.
- Certificate must have proper CDP (for CRL) and/or AIA (for OCSP) reference but not both references in one certificate.
- Certificate must have proper CN and SAN format that complies with section 6 of RFC 6125.
- Certificate names must not have space in them. For example, “Root CA” should be Root-CA, Root.CA or Root_CA.
- Certificate must not be expired or modified.
- The syslog server must be restarted and TOE must be rebooted.

The administrator is responsible for maintaining the physical connection between the TOE and external syslog server. If the connection is unintentionally broken, the administrator should perform the following steps to diagnose and fix the problem:

- Check the physical network cables.
- Check that the syslog server is still running.
- Reconfigure the Log Settings.
- If all else fail, reboot the TOE and/or syslog server.

The TOE, as a TLS client for the syslog over TLS connection, can support the following TLS ciphersuites:

(Certificate with RSA as digital signature algorithm)

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

(Certificate with ECDSA as digital signature algorithm)

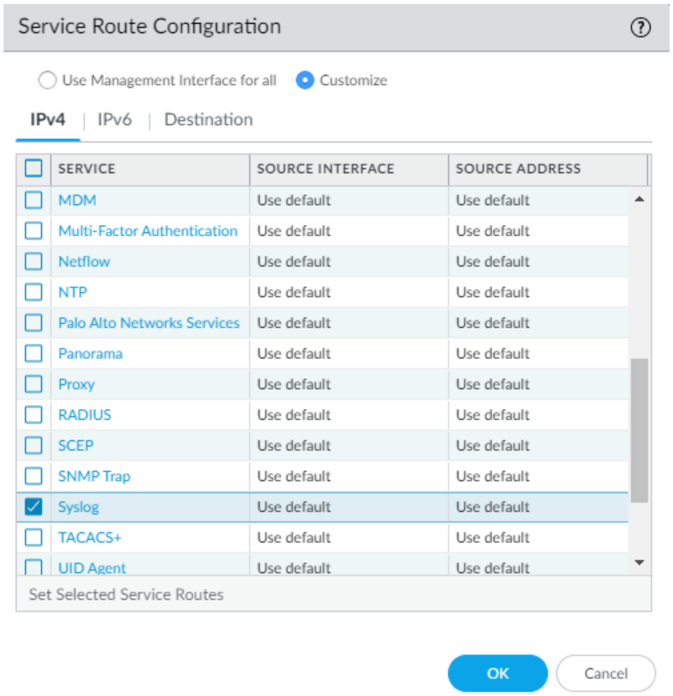
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

The same ciphersuites are supported regardless if mutual authentication is configured or not. By default, it is not configured. For all TLS_ECDHE_* ciphersuites, secp256r1, secp384r1, and secp521r1 will be offered in the Supported Elliptic Curves (Supported Groups) extension in the TLS ClientHello. The ciphersuites listed above are all supported in FIPS-CC mode.

The syslog or management data can also be tunneled over IPsec to its final destination. This is tunneled over the IKE/IPsec implementation in the Data Plane (DP). Configure the IKE/IPsec tunnel as instructed in section 7.11 below. Then configure a service route to route syslog and/or management traffic from the Management Plane (MP) to the DP IKE/IPsec interface.

Configure a Service Route:

1. Login with Administrator Role.
2. Select **Device > Setup > Services**.
3. Click **Service Route Configuration**.
4. Select **Customize**.
5. Select **Syslog**. You can configure the source interface and address. The source interface should be the MGT and the management IP address. If you want to tunnel HTTPS management data, select **HTTP**.



Service Route Configuration

○ Use Management Interface for all ● Customize

IPv4 | IPv6 | Destination

□	SERVICE	SOURCE INTERFACE	SOURCE ADDRESS
□	MDM	Use default	Use default
□	Multi-Factor Authentication	Use default	Use default
□	Netflow	Use default	Use default
□	NTP	Use default	Use default
□	Palo Alto Networks Services	Use default	Use default
□	Panorama	Use default	Use default
□	Proxy	Use default	Use default
□	RADIUS	Use default	Use default
□	SCEP	Use default	Use default
□	SNMP Trap	Use default	Use default
☑	Syslog	Use default	Use default
□	TACACS+	Use default	Use default
□	UID Agent	Use default	Use default

Set Selected Service Routes

6. Click on the **Destination** tab and configure the destination information.
7. Click **OK** to save the changes.
8. **Commit** the changes.

6.8.2 Certificate-Based Authentication for Web UI (Optional)

As a more secure alternative to password-based authentication to the TOE web UI, you can configure certificate-based authentication (for example, CAC or Common Access Card) for administrator accounts that are local to the TOE. Certificate-based authentication involves the exchange and verification of a digital signature instead of a password.

Configuring certificate-based authentication for any administrator disables the username/password logins for all administrators on the TOE and all administrators thereafter require the certificate to log in. Section 7.3 presents the configuration information.

> **NOTE:** Export the client certificate in PKCS12 format to import into Google Chrome. For smart card, export the client certificate to the supported format.

Generate or Import the Certificates:

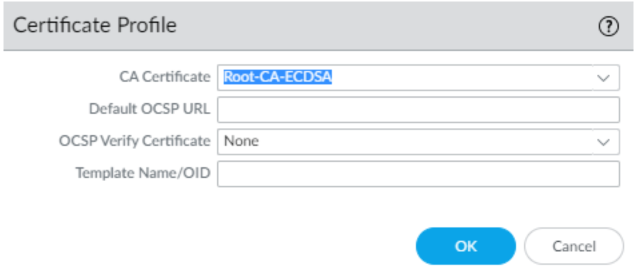
1. Login with Administrator Role.
2. Generate a CA certificate on the TOE. You will use this CA certificate to sign the client certificate of each administrator. You can
    a) Create a self-signed root CA certificate.
    b) Alternatively, you can import a certificate from your enterprise CA.
3. These steps are the same to the ones described the previous section.

Configure a Certificate Profile:

1. Login with Administrator Role.
2. Select **Device > Certificate Management > Certificate Profile** and click **Add**.
3. Enter a **Name** for the certificate profile and set the **Username Field** to **Subject**.
4. Select **Add** in the **CA Certificates** section and select the CA certificate you just created or imported above.

> **NOTE:** If you configure an intermediate CA as part of the certificate profile, you must include the root CA as well.

5. Optionally, if the TOE uses Online Certificate Status Protocol (OCSP) to verify certificate revocation status, configure the following fields to override the default setting in the certificate.
    a) Enter the default OCSP responder URL in the **Default OCSP URL** field.
    b) By default, the TOE uses the certificate selected in the **CA Certificate** field to validate the OCSP response. To use a different certificate for validation, select it in the **OCSP Verify CA Certificate** field.



CA Certificate: Root-CA-ECDSA

Default OCSP URL:

OCSP Verify Certificate: None

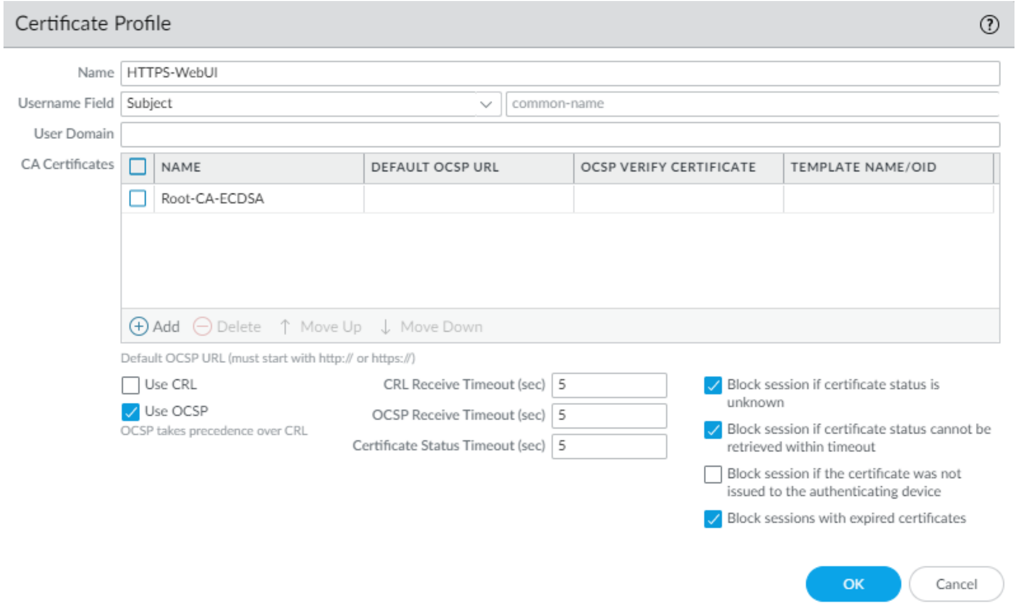
Template Name/OID:

c) Click **OK** to save the changes.

6. To enable CRL, you **must** check the **Use CRL** checkbox to use Certificate Revocation List (CRL) to verify the revocation status of the certificates.
7. To enable OCSP, you **must** check the **Use OCSP** checkbox to use Online Certificate Status Protocol (OCSP) to verify the revocation status of the certificates.

> **NOTE:** If you select both OCSP and CRL, the TOE first tries OCSP and only falls back to the CRL method if the OCSP responder is unavailable.

8. Set the timeout values or use the default values.
    a) **CRL Receive Timeout** – Specify the interval (1 – 60 seconds) after which the TOE stops waiting for a response from the CRL service.
    b) **OCSP Receive Timeout** – Specify the interval (1 – 60 seconds) after which the TOE stops waiting for a response from the OCSP responder.
    c) **Certificate Status Timeout** – Specify the interval (1 – 60 seconds) after which the TOE stops waiting for a response from any certificate status service and applies any session blocking login you define.
9. Check the appropriate session blocking logic checkbox.
    a) **Block session if certificate status is unknown** – Select this option if you want the TOE to block sessions when the OCSP or CRL service returns a certificate revocation status of unknown. Otherwise, the TOE proceeds with the sessions.
    b) **Block sessions if certificate status cannot be retrieved within timeout** – Select this option if you want the TOE to block sessions after it registers an OCSP or CRL request timeout. Otherwise, the TOE proceeds with the sessions.
    c) **Block sessions if certificate was not issued to the authentication device** – (GlobalProtect Only) Select this option if you want the TOE to block sessions when the serial number attribute in the subject of the client certificate does not match the host ID that the GlobalProtect app reports for the endpoint.
    d) **Block sessions with expired certificates** – Select this option if you want the TOE to block sessions with expired certificates.



Certificate Profile

Name: HTTPS-WebUI

Username Field: Subject | common-name

User Domain:

CA Certificates

☐	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
☐	Root-CA-ECDSA			

Default OCSP URL (must start with http:// or https://)

☐ Use CRL

☑ Use OCSP

OCSP takes precedence over CRL

CRL Receive Timeout (sec): 5

OCSP Receive Timeout (sec): 5

Certificate Status Timeout (sec): 5

☑ Block session if certificate status is unknown

☑ Block session if certificate status cannot be retrieved within timeout

☐ Block session if the certificate was not issued to the authenticating device

☑ Block sessions with expired certificates

10. Click **OK** to save the changes.

11. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

> **WARNING:** Should check **Block session if certificate status is unknown**, **Block session if certificate status cannot be restrieved within timeout**, and **Block sessions with expired certificates**.

> **CLI HINT:** The equivalent CLI commands are: **configure** and **set shared certificate-profile <Name> <Options>**. You configure the value one-by-one. For example,

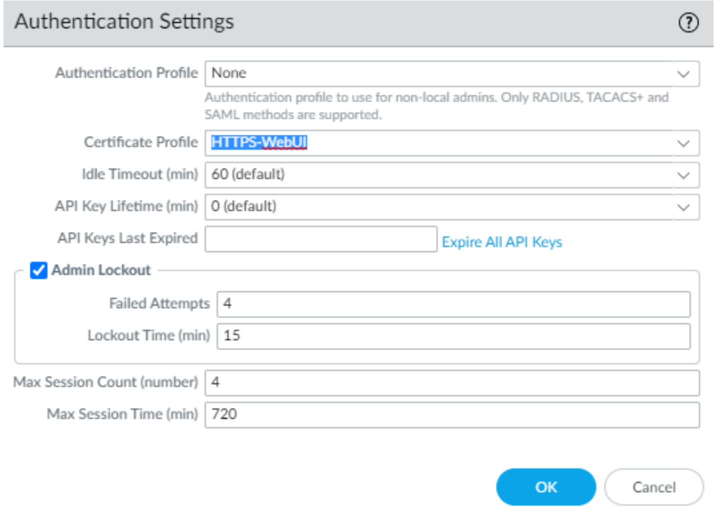
```
configure
#set shared certificate-profile <Profile Name> CA <CA Name>
#set shared certificate-profile <Profile Name> block-expired-cert yes
#set shared certificate-profile <Profile Name> block-unknown-cert yes
#set shared certificate-profile <Profile Name> block-timeout-cert-timeout yes
#set shared certificate-profile <Profile Name> use-ocsp yes
#commit
```

```
admin@PA-5250# set shared certificate-profile HTTPS-WebUI
+ block-expired-cert          whether to block a session if cert. status is expired
+ block-timeout-cert          whether to block a session if cert. status can't be retrieved within
timeout
```

```
+ block-unauthenticated-cert   whether to block session if the certificate was not issued to the
authenticating device
+ block-unknown-cert          whether to block a session if cert. status is unknown
+ cert-status-timeout         set cert status query timeout value in seconds
+ crl-receive-timeout         set CRL receive timeout value in seconds
+ domain                      alphanumeric string [ 0-9a-zA-Z._-]
+ ocsp-exclude-nonce          whether to exclude nonce extension for OCSP requests
+ ocsp-receive-timeout        set OCSP receive timeout value in seconds
+ use-crl                     use-crl
+ use-ocsp                    use-ocsp
> CA                          CA
> username-field              username-field
```

Configure the Web UI to use Certificate Profile for Authentication:

1. Login with Administrator Role.
2. Select **Device > Setup > Management** and edit the **Authentication Settings**.
3. Select the **Certificate Profile** you just created and click **OK**.



Authentication Settings

Authentication Profile: None

Authentication profile to use for non-local admins. Only RADIUS, TACACS+ and SAML methods are supported.

Certificate Profile: HTTPS-WebUI

Idle Timeout (min): 60 (default)

API Key Lifetime (min): 0 (default)

API Keys Last Expired:

☑ Admin Lockout

Failed Attempts: 4

Lockout Time (min): 15

Max Session Count (number): 4

Max Session Time (min): 720

> **CLI HINT:** The equivalent CLI commands are: **configure** and **set deviceconfig system certificate-profile <Profile Name>**.

4. Configure the user accounts to use client certificate authentication.
5. Select **Device > Administrators** and click on the user.
6. Check the **Use only client certificate authentication (Web)** checkbox.

7. Generate a client certificate for each administrator.
8. Export the client certificates.
9. Import the client certificate into the client system (i.e., web browser) of each administrator who will access the web interface. You can also import the client certificate to a smart card or CAC.
10. Commit the changes on the TOE. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.
11. Verify that administrators can access the web interface.
12. Open the TOE IP address in a web browser on the computer that has the client certificate.
13. When prompted. Select the certificate you imported and click **OK**. If you are using a CAC, please insert it into the card reader. The browser displays a certificate warning.
14. Add the certificate to the browser exception list.
15. Click **Login**. The web interface will appear without prompting you for a username or password.

WARNING: If you made a mistake above (e.g., forgot to export the client certificates) and have now lost access to the web UI, log into the CLI as administrator and execute these commands:

a) **configure**
b) **delete deviceconfig system certificate-profile**
c) **commit**

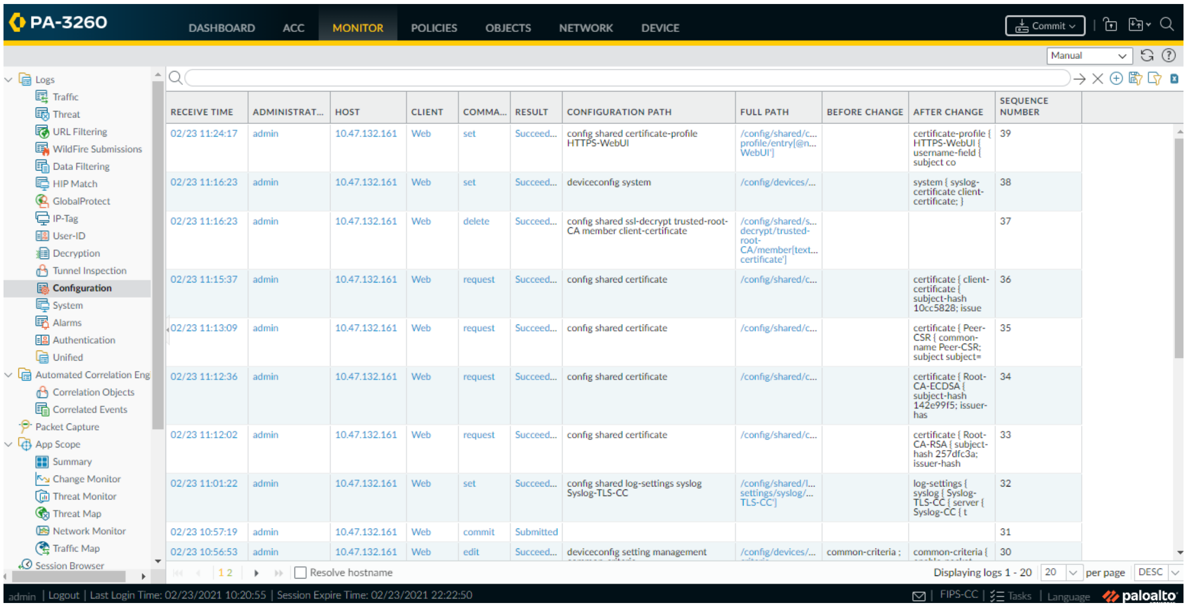
7 Management Activity

This section describes the management functions provided by the TOE to the authorized administrators.

7.1 Manage Audit Log

The TOE generates and stores read-only auditing information for user activity. The logs are presented in a standard event view that allows an administrator to view, sort, and filter audit log messages based on any item in the audit columns. Administrators can delete and report on audit information and can view detailed reports of the changes that users make.

1. Login with Administrator Role.
2. Select **Monitor > Logs > Configuration**.

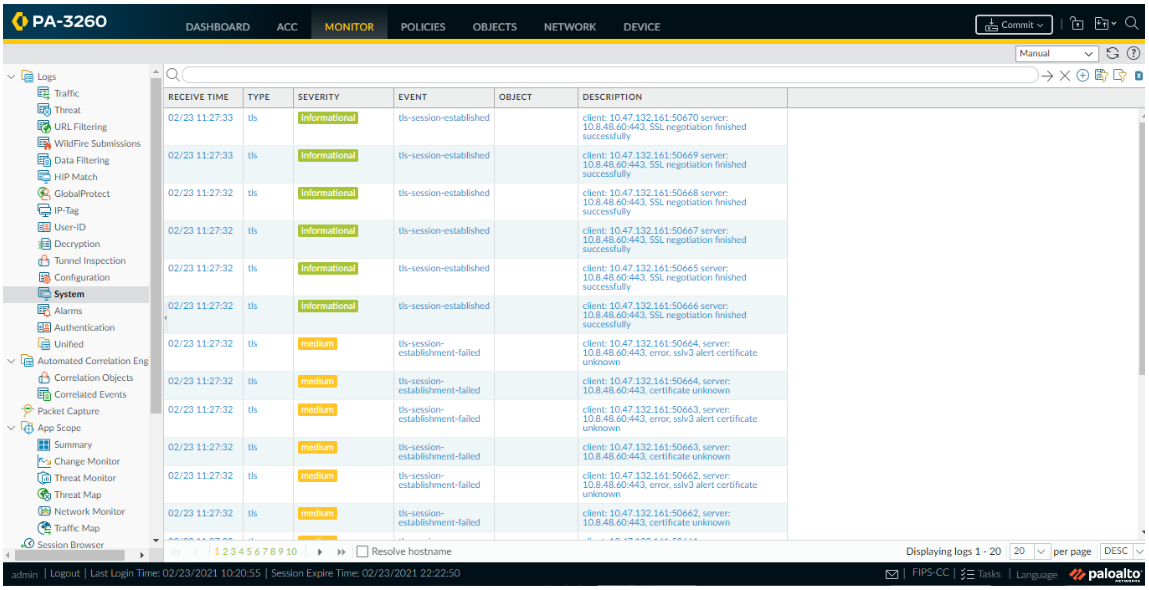


RECEIVE TIME	ADMINISTRAT...	HOST	CLIENT	COMMA...	RESULT	CONFIGURATION PATH	FULL PATH	BEFORE CHANGE	AFTER CHANGE	SEQUENCE NUMBER
02/23 11:24:17	admin	10.47.132.161	Web	set	Succeed...	config shared certificate-profile HTTPS-WebUI	/config/shared/c... profile/entry[@n... WebUI']		certificate-profile { HTTPS-WebUI { username-field { subject co	39
02/23 11:16:23	admin	10.47.132.161	Web	set	Succeed...	deviceconfig system	/config/devices/...		system { syslog-certificate client-certificate; }	38
02/23 11:16:23	admin	10.47.132.161	Web	delete	Succeed...	config shared ssl-decrypt trusted-root-CA member client-certificate	/config/shared/s... decrypt/trusted-root-CA/member[text... certificate']			37
02/23 11:15:37	admin	10.47.132.161	Web	request	Succeed...	config shared certificate	/config/shared/c...		certificate { client-certificate { subject-hash 10cc5828; issue	36
02/23 11:13:09	admin	10.47.132.161	Web	request	Succeed...	config shared certificate	/config/shared/c...		certificate { Peer-CSR { common-name Peer-CSR; subject subject=	35
02/23 11:12:36	admin	10.47.132.161	Web	request	Succeed...	config shared certificate	/config/shared/c...		certificate { Root-CA-ECDSA { subject-hash 142e99f5; issuer-has	34
02/23 11:12:02	admin	10.47.132.161	Web	request	Succeed...	config shared certificate	/config/shared/c...		certificate { Root-CA-RSA { subject-hash 257dfc3a; issuer-hash	33
02/23 11:01:22	admin	10.47.132.161	Web	set	Succeed...	config shared log-settings syslog Syslog-TLS-CC	/config/shared/l... settings/syslog/... TLS-CC']		log-settings { syslog { Syslog-TLS-CC { server { Syslog-CC { t	32
02/23 10:57:19	admin	10.47.132.161	Web	commit	Submitted					31
02/23 10:56:53	admin	10.47.132.161	Web	edit	Succeed...	deviceconfig setting management	/config/devices/...	common-criteria ;	common-criteria {	30

1 2 □ Resolve hostname Displaying logs 1 - 20 20 per page DESC

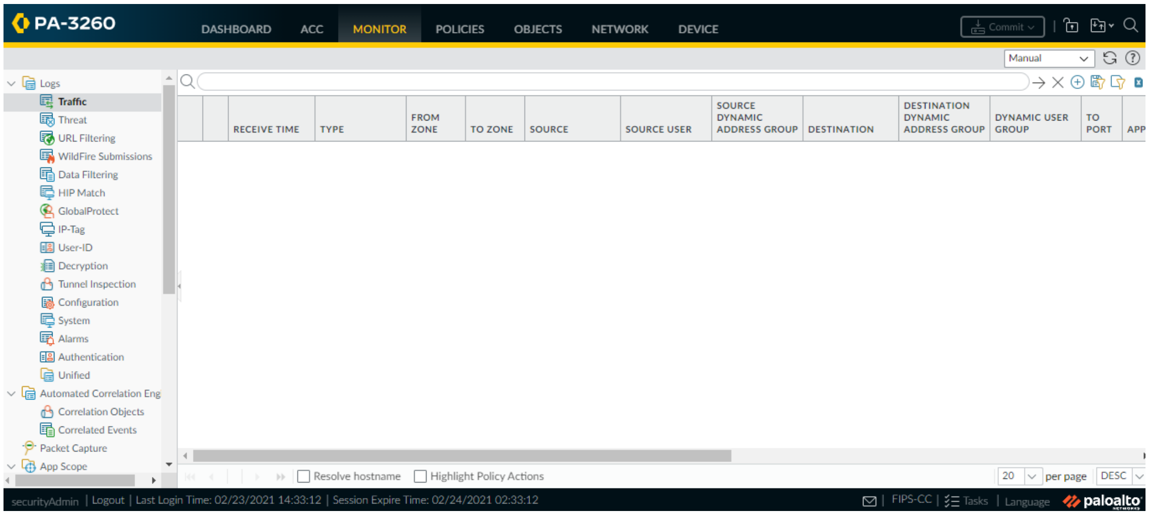
admin | Logout | Last Login Time: 02/23/2021 10:20:55 | Session Expire Time: 02/23/2021 22:22:50

3. Select **Monitor > Logs > System**.



RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
02/23 11:27:33	tls	informational	tls-session-established		client: 10.47.132.161:50670 server: 10.8.48.60:443, SSL negotiation finished successfully
02/23 11:27:33	tls	informational	tls-session-established		client: 10.47.132.161:50669 server: 10.8.48.60:443, SSL negotiation finished successfully
02/23 11:27:32	tls	informational	tls-session-established		client: 10.47.132.161:50668 server: 10.8.48.60:443, SSL negotiation finished successfully
02/23 11:27:32	tls	informational	tls-session-established		client: 10.47.132.161:50667 server: 10.8.48.60:443, SSL negotiation finished successfully
02/23 11:27:32	tls	informational	tls-session-established		client: 10.47.132.161:50665 server: 10.8.48.60:443, SSL negotiation finished successfully
02/23 11:27:32	tls	informational	tls-session-established		client: 10.47.132.161:50666 server: 10.8.48.60:443, SSL negotiation finished successfully
02/23 11:27:32	tls	medium	tls-session-establishment-failed		client: 10.47.132.161:50664, server: 10.8.48.60:443, error, sslv3 alert certificate unknown
02/23 11:27:32	tls	medium	tls-session-establishment-failed		client: 10.47.132.161:50664, server: 10.8.48.60:443, certificate unknown
02/23 11:27:32	tls	medium	tls-session-establishment-failed		client: 10.47.132.161:50663, server: 10.8.48.60:443, error, sslv3 alert certificate unknown
02/23 11:27:32	tls	medium	tls-session-establishment-failed		client: 10.47.132.161:50663, server: 10.8.48.60:443, certificate unknown
02/23 11:27:32	tls	medium	tls-session-establishment-failed		client: 10.47.132.161:50662, server: 10.8.48.60:443, error, sslv3 alert certificate unknown
02/23 11:27:32	tls	medium	tls-session-establishment-failed		client: 10.47.132.161:50662, server: 10.8.48.60:443, certificate unknown

4. Select **Monitor > Logs > Traffic** or **Monitor > Logs > Threat**.



	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APP

5. The equivalent CLI commands are **show log config**, **show log system**, **show log traffic**, and **show log threat**.

CLI HINT: To view the latest logs, use this command: **show log system direction equal backward**.

CLI HINT: To export the logs and view them externally, use this command: **scp export log system to <User>@<SSH IP Address>:<Filename> start-time equal <YYYY>/<MM>/<DD>@<hh>:<mm>:<ss> end-time equal <YYYY>/<MM>/<DD>@<hh>:<mm>:<ss>**.

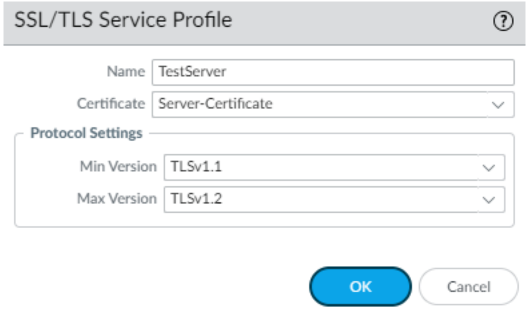
7.2 Configure Custom HTTPS or TLS Server Certificate

Use the following procedures to configure the TLS server (TOE) to use a custom certificate instead of the predefined certificate. We highly recommend you deploy a custom certificate on the TOE by generating a server certificate internally or obtaining a server certificate from your enterprise CA or a trusted third-party CA.

Configure the HTTPS Server Certificate for Web Management

1. Login with Administrator Role.
2. Select **Device > Certificate Management > Certificates**.
3. You can deploy a certificate on the TOE by generating a server certificate or obtaining a server certificate from your enterprise CA or a trusted third-party CA.
4. Configure an SSL/TLS service profile.
5. Select **Device > Certificate Management > SSL/TLS Service Profile**.
6. Click **Add**. Enter a **Name**, select a certificate in the **Certificate** field (NOTE: Must be a server certificate), and configure the TLS minimum and maximum version.

> **WARNING:** The minimum TLS version must be TLSv1.1 or higher.



SSL/TLS Service Profile

Name: TestServer

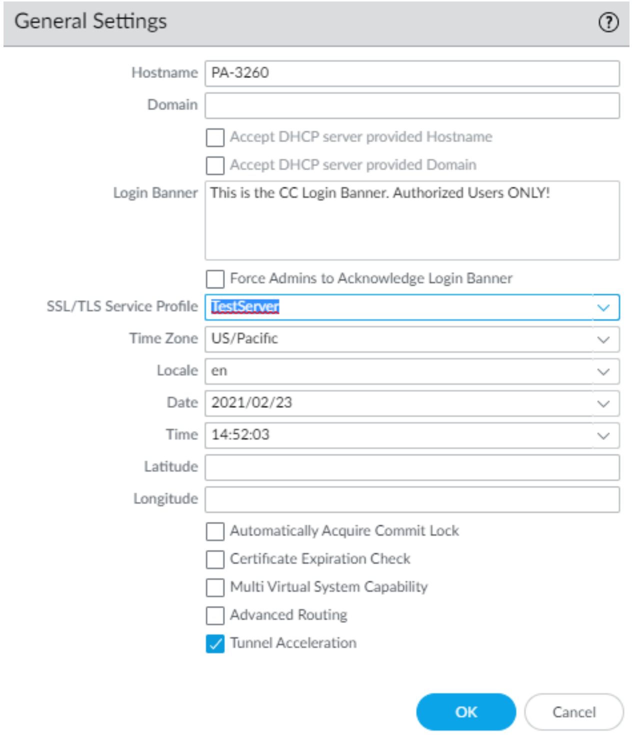
Certificate: Server-Certificate

Protocol Settings

Min Version: TLSv1.1

Max Version: TLSv1.2

7. Configure web server on the TOE to present the custom server certificate.
8. Select **Device > Setup > Management** and **Edit** the **General Settings**.
9. In the **SSL/TLS Service Profile** field, select the SSL/TLS service profile created above.



General Settings

Hostname: PA-3260

Domain:

☐ Accept DHCP server provided Hostname

☐ Accept DHCP server provided Domain

Login Banner: This is the CC Login Banner. Authorized Users ONLY!

☐ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: TestServer

Time Zone: US/Pacific

Locale: en

Date: 2021/02/23

Time: 14:52:03

Latitude:

Longitude:

☐ Automatically Acquire Commit Lock

☐ Certificate Expiration Check

☐ Multi Virtual System Capability

☐ Advanced Routing

☑ Tunnel Acceleration

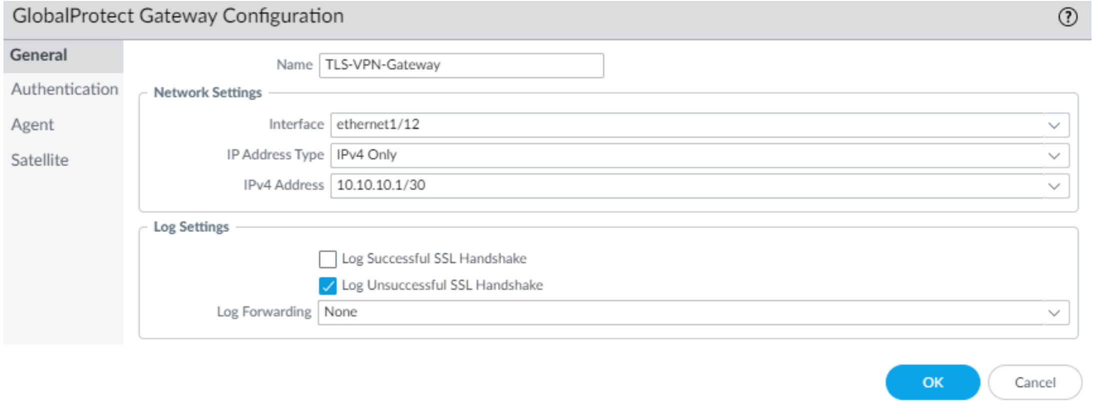
10. Click **OK** to save the changes.

11. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

> **CLI HINT:** The equivalent CLI commands are **configure**, **set shared ssl-tls-service-profile <Name> protocol-settings [min-version | max-version] <tls1-0 | tls1-1 | tls1-2 | max>**, and **set deviceconfig system ssl-tls-service-profile <Profile Name>**.

Configure the TLS Server Certificate for Gateway (for GlobalProtect VPN Client)

1. Login with Administrator Role.
2. Select **Network > GlobalProtect > Gateways** and then **Add** a gateway.
3. Enter a **Name** for the gateway. The name cannot contain spaces.
4. Select an **Interface**.
5. Specify the **IP Address Type** and **IP Address** for the gateway.



GlobalProtect Gateway Configuration

Name: TLS-VPN-Gateway

Network Settings

Interface: ethernet1/12

IP Address Type: IPv4 Only

IPv4 Address: 10.10.10.1/30

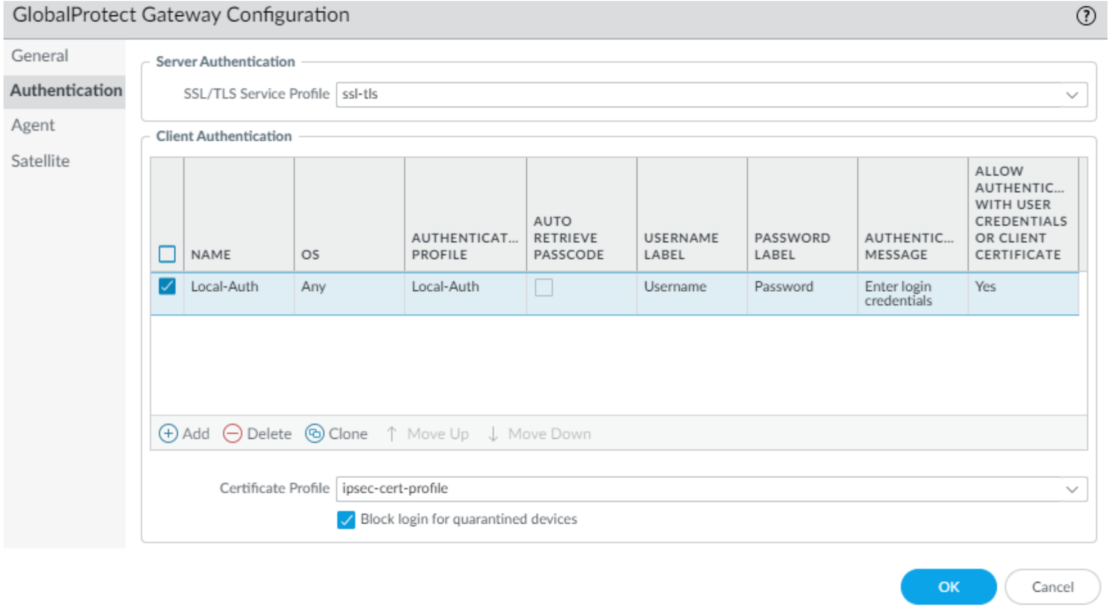
Log Settings

□ Log Successful SSL Handshake

☑ Log Unsuccessful SSL Handshake

Log Forwarding: None

6. In the **Authentication** tab, select an **SSL/TLS Service Profile**. Configure the client authentication method (user credentials or client certificate). To validate the client certificate, specify the **Certificate Profile**.



GlobalProtect Gateway Configuration

Server Authentication

SSL/TLS Service Profile: ssl-tls

Client Authentication

□	NAME	OS	AUTHENTICAT... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTIC... MESSAGE	ALLOW AUTHENTIC... WITH USER CREDENTIALS OR CLIENT CERTIFICATE
☑	Local-Auth	Any	Local-Auth	□	Username	Password	Enter login credentials	Yes

Certificate Profile: ipsec-cert-profile

☑ Block login for quarantined devices

7. Click **OK** to save the changes.
8. Commit the changes.

When an ECDSA server certificate is configured, the following TLS ciphersuites are supported:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 (TLSv1.1 and TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 (TLSv1.1 and TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2 only)

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)

When an RSA server certificate is configured, the following TLS ciphersuites are supported:

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 (TLSv1.1 and TLSv1.2)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 (TLSv1.1 and TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2 only)

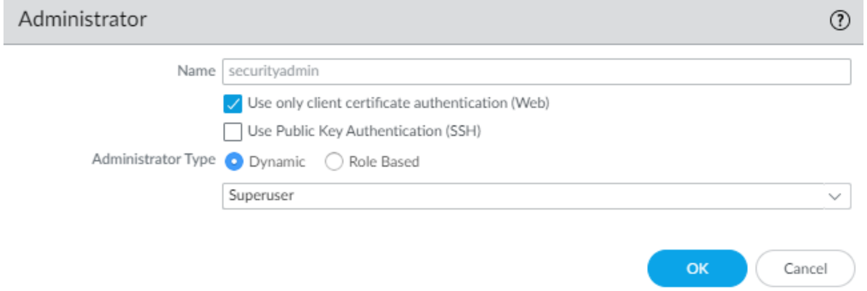
The key establishment parameters specified in FCS_TLSS_EXT.1.3 are automatically derived from the negotiated TLS ciphersuite. The same ciphersuites are supported regardless if mutual authentication is configured or not. The supported ciphersuites are implemented based on the server certificate (RSA vs ECDSA) configured. Note that secp521r1 is not supported for TLS server.

WARNING: The algorithms must match if mutual authentication is configured. For example, if the server certificate (TOE) is RSA-based and the client certificate (user) is ECDSA-based, the connection will fail.

7.3 Configure HTTPS or TLS Client Certificate Authentication

Use the following procedures to configure the TLS web server (TOE) to authenticate client users by their x509v3 certificates (i.e., Mutual Authentication). You can deploy the client certificate on the web browser by generating the certificate internally or obtaining the certificate from your enterprise CA or a trusted third-party CA. The TOE automatically compares the distinguished name (DN) or Subject Alternative Name (SAN) contained in the client certificate to the expected identifier for the peer (e.g., username) and will not establish a trusted channel if they do not match.

1. Login with Administrator Role.
2. Select **Device > Administrators**.
3. Create a user and check **Use only client certificate authentication (Web)** checkbox.
4. Click **OK**.



Administrator

Name: securityadmin

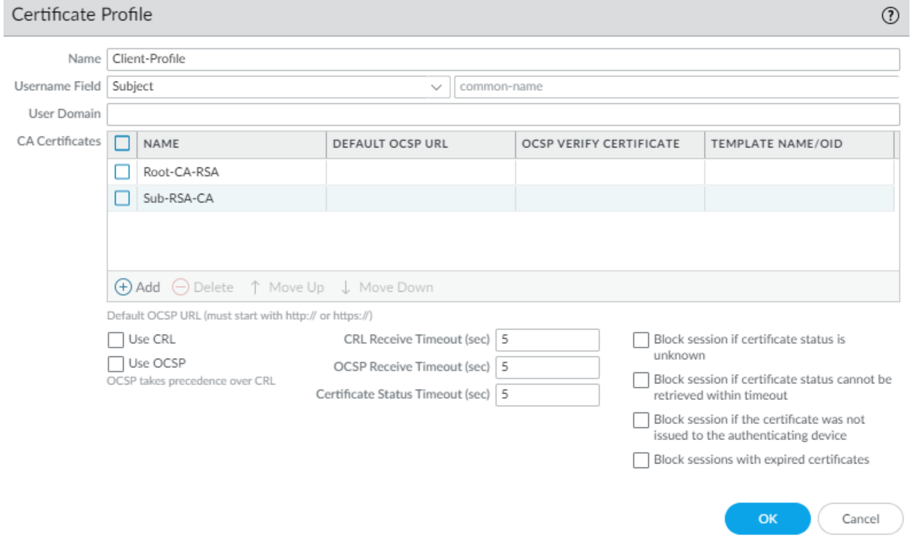
☑ Use only client certificate authentication (Web)

□ Use Public Key Authentication (SSH)

Administrator Type: ● Dynamic ○ Role Based

Superuser

5. Create a Root CA and Intermediate CA (internally or externally). Import the CA(s) and private keys into the TOE, if generated externally. This will set the CA certificates in the Trust Anchor.
6. Create a client certificate profile. The **Username** field should be set to **Subject**. In the **CA Certificates** field, add the CA(s) that will validate the client certificate. Optionally, configure the revocation methods.



Certificate Profile

Name: Client-Profile

Username Field: Subject | common-name

User Domain:

CA Certificates:

□ NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
□ Root-CA-RSA			
□ Sub-RSA-CA			

Default OCSP URL (must start with http:// or https://)

□ Use CRL

□ Use OCSP

OCSP takes precedence over CRL

CRL Receive Timeout (sec): 5

OCSP Receive Timeout (sec): 5

Certificate Status Timeout (sec): 5

□ Block session if certificate status is unknown

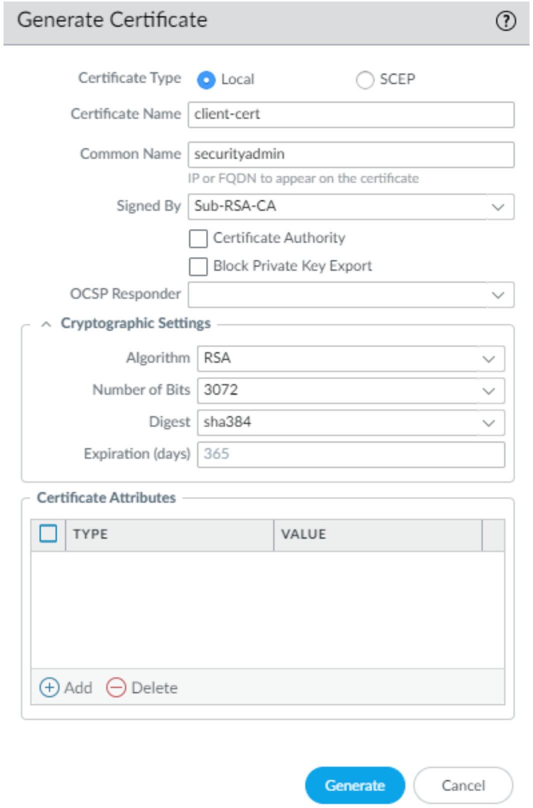
□ Block session if certificate status cannot be retrieved within timeout

□ Block session if the certificate was not issued to the authenticating device

□ Block sessions with expired certificates

WARNING: Should check **Block session if certificate status is unknown**, **Block session if certificate status cannot be retrieved within timeout**, and **Block sessions with expired certificates**.

7. Create a client certificate.
8. To create a client certificate, **Device > Certificate Management > Certificate > Generate**.



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: client-cert

Common Name: securityadmin

IP or FQDN to appear on the certificate

Signed By: Sub-RSA-CA

□ Certificate Authority

□ Block Private Key Export

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 3072

Digest: sha384

Expiration (days): 365

Certificate Attributes

□	TYPE	VALUE

WARNING: Make sure **Common Name** field matches the name (i.e., username) in step 4. IP address or email address is not supported. The username must match the username stored in the local database.

9. If the client certificate is generated and signed internally, export the client certificate and private key (PEM format). For example, copy the certificate into client.pem and key into client.key.

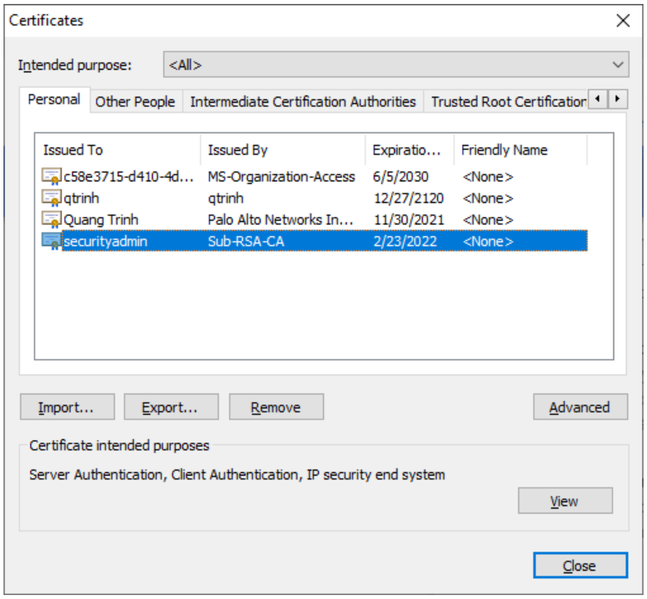
WARNING: The exported private key will always be encrypted. Please decrypt the key before converting to PKCS12. For example, for encrypted RSA key

openssl rsa -in client.key -out decrypted-client.key

Enter pass phrase for key.pem:

10. Change the client certificate PEM format to PKCS12 (see command below) before

importing the client certificate into Chrome (Settings > Privacy & Security > Security > Manage Certificates > Import…) or Firefox (Options > Privacy & Security > Certificates > View Certificates… > Import…).



Intended purpose: <All>

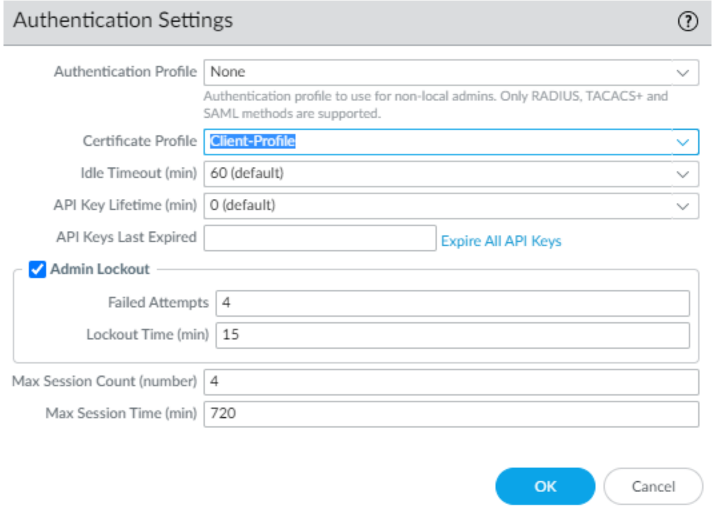
Issued To	Issued By	Expiratio…	Friendly Name
c58e3715-d410-4d…	MS-Organization-Access	6/5/2030	<None>
qtrinh	qtrinh	12/27/2120	<None>
Quang Trinh	Palo Alto Networks In…	11/30/2021	<None>
securityadmin	Sub-RSA-CA	2/23/2022	<None>

Certificate intended purposes

Server Authentication, Client Authentication, IP security end system

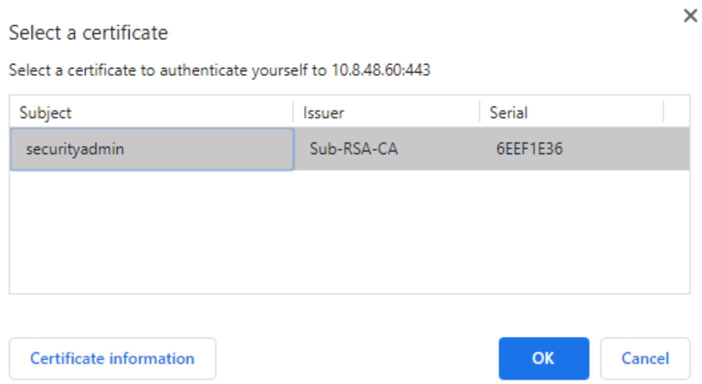
```
openssl pkcs12 -export -clcerts -in client.pem -inkey decrypted-client.key -out client.p12
```

11. Set the new client certificate profile for the **Certificate Profile** in Authentication settings.
12. **Device > Setup > Management > Authentication Settings**.



Authentication Profile	None Authentication profile to use for non-local admins. Only RADIUS, TACACS+ and SAML methods are supported.
Certificate Profile	Client-Profile
Idle Timeout (min)	60 (default)
API Key Lifetime (min)	0 (default)
API Keys Last Expired	
☑ Admin Lockout	
Failed Attempts	4
Lockout Time (min)	15
Max Session Count (number)	4
Max Session Time (min)	720

13. Click **OK** and **Commit**.
14. Verify on the web browser with the imported client certificate that password authentication is not required. The web browser will ask for the client certificate for authentication.

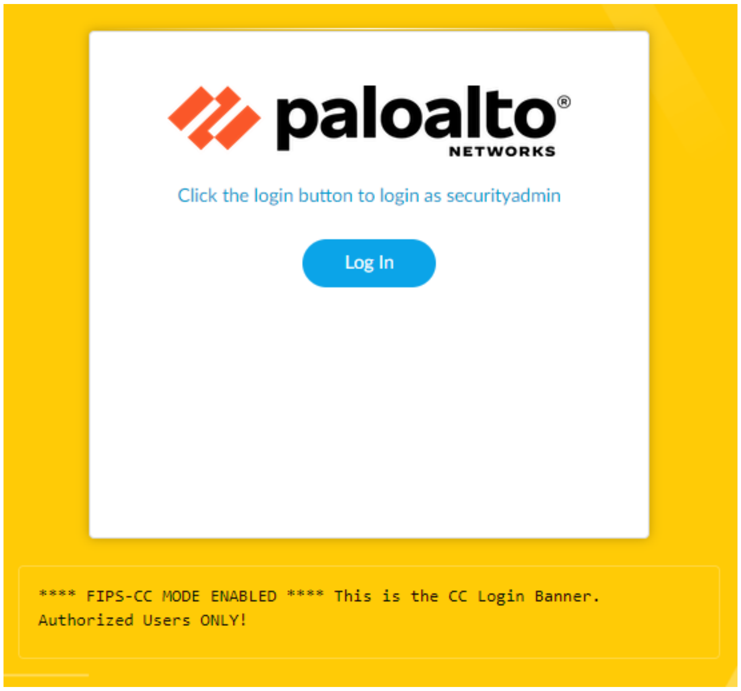


Select a certificate

Select a certificate to authenticate yourself to 10.8.48.60:443

Subject	Issuer	Serial
securityadmin	Sub-RSA-CA	6EEF1E36

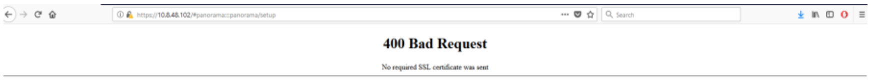
15. Click **Log In**, if asked.



Click the login button to login as securityadmin

```
**** FIPS-CC MODE ENABLED **** This is the CC Login Banner.
Authorized Users ONLY!
```

16. On a web browser without the client certificate imported, verify access is denied.



400 Bad Request

No required SSL certificate was sent

WARNING: In case the X509 public key authentication fails and you can’t access the Web UI due to certificate error/failure, SSH into the TOE and **delete deviceconfig system certificate-profile** and **commit**.

CLI HINT: The equivalent CLI commands are: **configure, set shared certificate-profile <Name> username-field subject common-name, set shared certificate-profile <Name> CA <CA-Names>, set deviceconfig system certificate-profile <Name>**.

Use the following procedures to configure the firewall (TOE) to authenticate GlobalProtect by their x509v3 certificates (i.e., Mutual Authentication). You can deploy the client certificate on the platform by generating the certificate internally or obtaining the certificate from your enterprise CA or a trusted third-party CA.

Generate the Client Certificate for GlobalProtect or User-ID Agent.

1. Login with Administrator Role.
2. Create the root CA certificate for using client certificate to GP or UIA clients.
3. Select **Device > Certificate Management > Certificates > Device Certificates** and then click **Generate**.
4. Enter a **Certificate Name**. The name cannot contain any spaces.
5. Enter the IP Address or FQDN that will appear on the certificate in the **Common Name** field.
6. Select your root CA from the **Signed By** drop-down.
7. Select an **OCSP Responder** to verify the revocation status of certificates.
8. Configure the **Cryptographic Settings** for the certificate, including the encryption **Algorithm**, key length **(Number of bits)**, **Digest** algorithm, and **Expiration** (in days) for the certificate.
9. In the **Certificate Attribute** area, **Add** and define the attributes that uniquely identify the endpoints as belonging to your organization. Keep in mind that if you add a **Host Name** attribute (which populates the SAN field of the certificate), it must be the same as the **Common Name** value you defined.
10. Click **OK** to generate the certificate.

Deploy the Client Certificate on the Platform with GlobalProtect or User-ID Agent (UIA)

1. Login with Administrator Role on the Windows platform.
2. From the command prompt, enter **mmc**.
3. Select **File > Add/Remove Snap-in**.
4. From the list of **Available snap-ins**, select **Certificates**, and then **Add** and select one of the following certificate snap-ins, depending on what type of certificate you are importing.

   a. Computer account
   b. My user account

5. From the **Console Root**, expand **Certificates**, and then select **Personal**.
6. In the **Actions** column, select **Personal > More Actions > All Tasks > Import** and follow the steps in the Certificate Import Wizard to import the PKCS file you received from the CA.
7. **Browse** to and select the .p12 certificate file to import (select **Personal Information Exchange** as the file type to browse for) and enter the **Password** that you used to encrypt the private key.
8. Verify that the certificate has been added to the certificate store.

If you use an external root CA or third-party CA to generate the client certificate, you must import that root CA certificate into the TOE.

Import the root CA certificate used to issue the client certificate into the TOE.

1. Login with Administrator Role.
2. Download the root CA certificate (Base64 format) used to issue the client certificate.
3. Select **Device > Certificate Management > Certificates > Device Certificates** and then click **Import**.
4. Set the **Certificate Type** to **Local** (default).
5. Enter a **Certificate Name** that identifies the certificate.
6. **Browse** to the select the **Certificate File** you download from the CA.
7. Set the **File Format** to **Base64 Encoded Certificate (PEM)**, and then click **OK**.
8. On the **Device Certificates** tab, select the certificate you just imported to open the Certificate Information.
9. Select **Trusted Root CA** and then click **OK**.

7.4 Role-Based Access Control (RBAC)

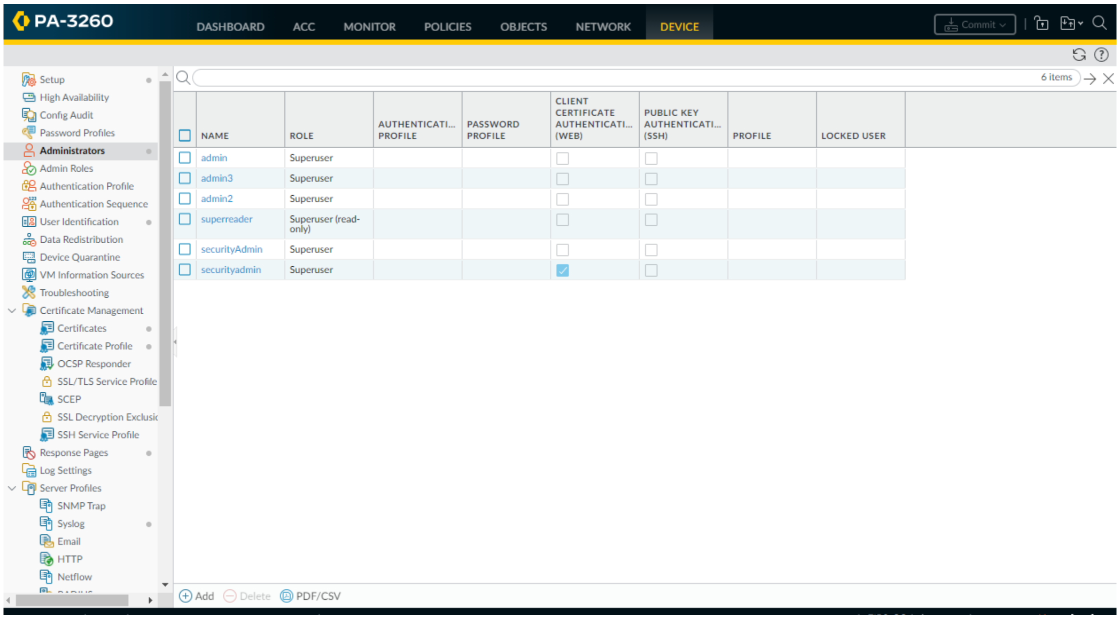
RBAC enables you to define the privileges and responsibilities of administrative users. Every administrator must have a user account that specifies a role and authentication method. By default, every TOE appliance (PA-Series or VM-Series) has a predefined administrative account (**admin**) that provides full read-write access (superuser access) to all. In the evaluated configuration, it is recommended that the users use the **admin** account to create separate accounts with different roles, with privileges based on the security requirements of your organization, and only use those accounts. The **admin** account should only be used as an emergency account.

7.4.1 View Administrator Account

From the Administrators page, you can view, edit, and delete existing accounts.

1. Login with Administrator Role.
2. Select **Device > Administrators**.

   The Administrators page appears.



□	NAME	ROLE	AUTHENTICATI... PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)	PROFILE	LOCKED USER
□	admin	Superuser			□	□		
□	admin3	Superuser			□	□		
□	admin2	Superuser			□	□		
□	superreader	Superuser (read-only)			□	□		
□	securityAdmin	Superuser			□	□		
□	securityadmin	Superuser			☑	□		

> **CLI HINT:** The equivalent CLI commands are **configure** and **show mgt-config users**.

7.4.2 Adding New Accounts

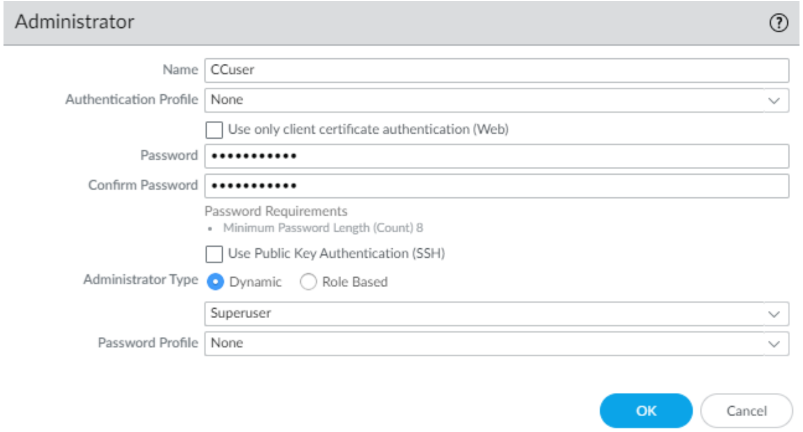
When you create a new user account, you can control which parts of the system the account can access. You can set the authentication method (password vs public-key), authentication profile (e.g., using authentication server), administrator type (e.g., dynamic, custom role), and administrator role (e.g., superuser, superuser (Read-Only), Device administrator).

1. Login with Administrator Role.

3. Select **Device > Administrators**.
2. Click **Add**.
3. Click **Name**. The username can be up to 15 characters long. The name is case-sensitive, must be unique, and can contain only letters, numbers, hyphens, and underscores.
4. Select an **Authentication Profile** or sequence to authenticate this administrator.
5. Check the **Use only client certificate authentication (Web)** for web interface access. If you select this option, a username (Name) and Password are not required.
6. Enter **Password/Confirm Password**.
7. Check the **Use Public Key Authentication (SSH)** for SSH interface access.

> **NOTE:** If public key authentication fails, the TOE will failback to password authentication.

8. In the **Administrator Type** field, select the type.
   - **Dynamic** – Roles that provide access to the TOE and managed devices. When new features are added, The TOE automatically updates the definitions of dynamic roles; you never need to manually update them.
   - **Role-Based** – Configurable custom roles.
9. In the **Admin Role** field, select the role.
   - **Superuser** – Full read-write access to Device.
   - **Superuser (Read Only)** – Read-only access to Device.
   - **Device administrator** – Full access to Device except for the following actions:
     i. Create, modify, or delete user and roles.
     ii. Export, validate, revert, save, load, or import a configuration (**Device > Setup > Operations**).
     iii. Configure a **Scheduled Config Export** in the **Device** tab.
10. Select a **Password Profile**.


Administrator

Name: CCuser

Authentication Profile: None

□ Use only client certificate authentication (Web)

Password: •••••••••••

Confirm Password: •••••••••••

Password Requirements
• Minimum Password Length (Count) 8

□ Use Public Key Authentication (SSH)

Administrator Type: ● Dynamic ○ Role Based

Superuser

Password Profile: None

c

11. Click **OK** to save the changes.
12. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

> CLI HINT: The equivalent CLI commands are **configure** and **show mgt-config users <Username> <Options>**. See below for list of options.

```
admin@PA-TOE# set mgt-config users admin2
+ authentication-profile    authentication-profile
+ client-certificate-only   Is client certificate authentication enough?
+ password-profile          password-profile
+ public-key                Public RSA
> permissions               permissions
> phash                     phash
> preferences               preferences
  password                  password
  <Enter>                   Finish input
```

7.4.3 Deleting or Modifying Accounts

The administrator can modify or delete user accounts from the system at any time, with the exception of the **admin** account, which cannot be deleted.

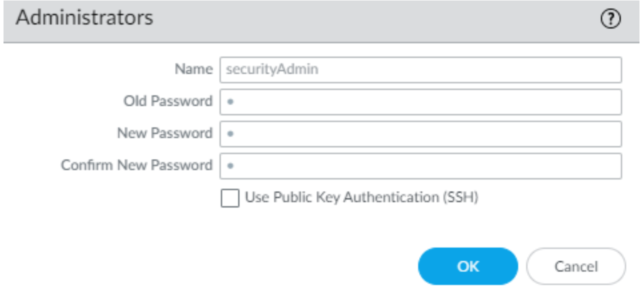
1. Login with Administrator Role.
2. Select **Device > Administrators**.
3. To delete a user, select the user you want to delete. Click on the checkbox next to the user or users to delete multiple accounts.
4. Click **Delete**.
5. Click **Yes** to confirm. Commit the changes.
6. The user account is deleted.
7. To modify a user, select the user link you want to modify under Name column.
8. Edit the user settings and click **OK**.
9. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

> CLI HINT: The equivalent CLI commands are **configure** and **delete mgt-config users <Username>**. Use **set mgt-config users <Username>** to modify an existing user.

7.4.4 Change User Password

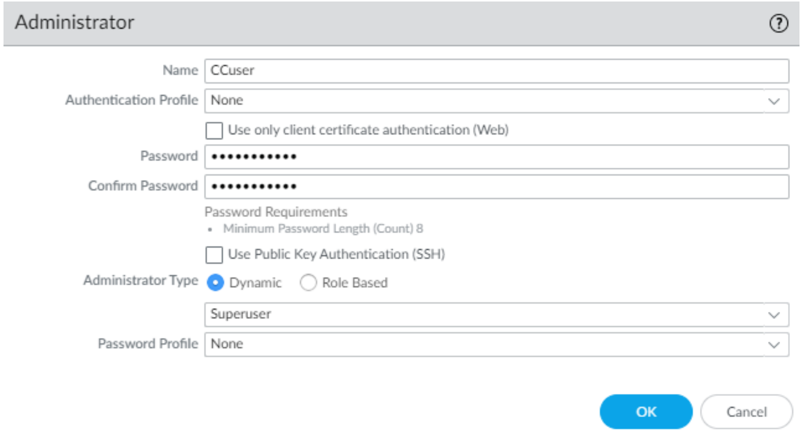
All user accounts are protected with a password by default. Any user can change their own password but only a user with Administrator role (i.e., superuser) can change another user's password.

1. Login with Administrator Role.
2. Select **Device > Administrators**.
3. To modify your own password, select the user link.
4. Enter the **Old Password**, **New Password**, and **Confirm New Password** and click **OK**.



Name	securityAdmin
Old Password	•
New Password	•
Confirm New Password	•
	□ Use Public Key Authentication (SSH)

5. To modify another user's password, select that user link.
6. Enter the **Password** and **Confirm Password** and click **OK**.



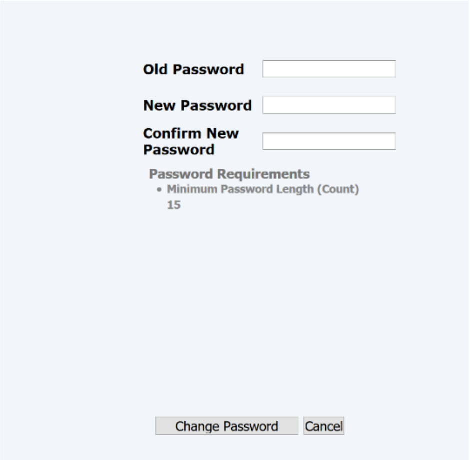
Name	CCuser
Authentication Profile	None
	□ Use only client certificate authentication (Web)
Password	•••••••••••
Confirm Password	•••••••••••
	Password Requirements • Minimum Password Length (Count) 8
	□ Use Public Key Authentication (SSH)
Administrator Type	● Dynamic ○ Role Based
	Superuser
Password Profile	None

7. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

CLI HINT: The equivalent CLI commands are **configure** and **set mgt-config users <Username> password**.

CLI HINT: To change own password: **set password**.

NOTE: When configured to change password on first login, the following page will appear.



Password Requirements

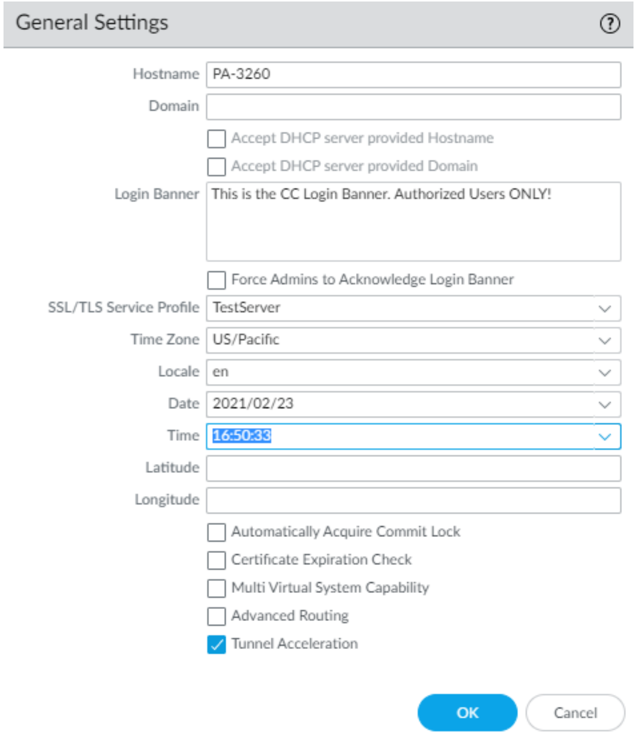
- Minimum Password Length (Count)
  15

7.5 Configure System Time

The administrator can configure time manually.

7.5.1 Configure Time Manually

1. Login with Administrator Role.
2. Select **Device > Setup > Management > General Settings**. The General Setting page appears.



General Settings

Hostname: PA-3260

Domain:

☐ Accept DHCP server provided Hostname

☐ Accept DHCP server provided Domain

Login Banner: This is the CC Login Banner. Authorized Users ONLY!

☐ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: TestServer

Time Zone: US/Pacific

Locale: en

Date: 2021/02/23

Time: 16:50:33

Latitude:

Longitude:

☐ Automatically Acquire Commit Lock

☐ Certificate Expiration Check

☐ Multi Virtual System Capability

☐ Advanced Routing

☑ Tunnel Acceleration

3. Select the **Time Zone** for the TOE.
4. Configure the **Date** for the TOE.
5. Configure the **Time** for the TOE.
6. Edit the user settings and click **OK**.
7. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

> **CLI HINT:** The equivalent CLI commands are **set clock date <YYYY/MM/DD> time <hh:mm:ss>** and **set deviceconfig system timezone <Timezone>**.

> **API HINT:** The equivalent XML API call is (need to edit the value and API key)

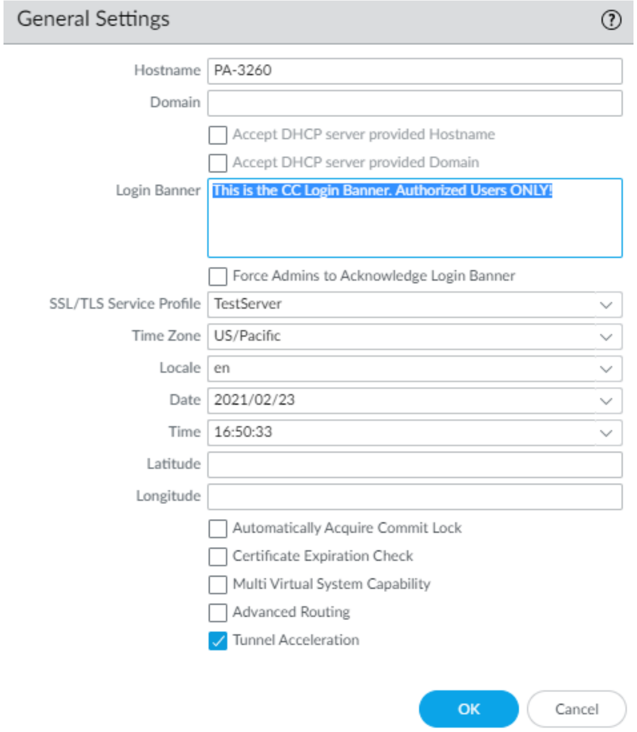
- **https://<TOE>/api/?type=op&cmd=<set><clock><date>2019/06/27</date><time>17:35:00</time></clock></set>&key=<APIkey>**

> **NOTE:** For PAN-OS VM on Hyper-V, please disable “Time Synchronization” setting in Hyper-V to allow time change on the VM.

7.6 Configure Login Banner

The administrator can create a custom login banner that appears when users log into the appliance using SSH and on the login page of the web interface.

1. Login with Administrator Role.
2. Select **Device > Setup > Management > General Settings**. The General Setting page appears.



General Settings

Hostname	PA-3260
Domain	
	□ Accept DHCP server provided Hostname
	□ Accept DHCP server provided Domain
Login Banner	This is the CC Login Banner. Authorized Users ONLY!
	□ Force Admins to Acknowledge Login Banner
SSL/TLS Service Profile	TestServer
Time Zone	US/Pacific
Locale	en
Date	2021/02/23
Time	16:50:33
Latitude	
Longitude	
	□ Automatically Acquire Commit Lock
	□ Certificate Expiration Check
	□ Multi Virtual System Capability
	□ Advanced Routing
	☑ Tunnel Acceleration

3. Configure the **Login Banner** for the TOE.
4. Edit the user settings and click **OK**.
5. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

> **CLI HINT:** The equivalent CLI commands are **configure** and **set deviceconfig system login-banner <Value>**.

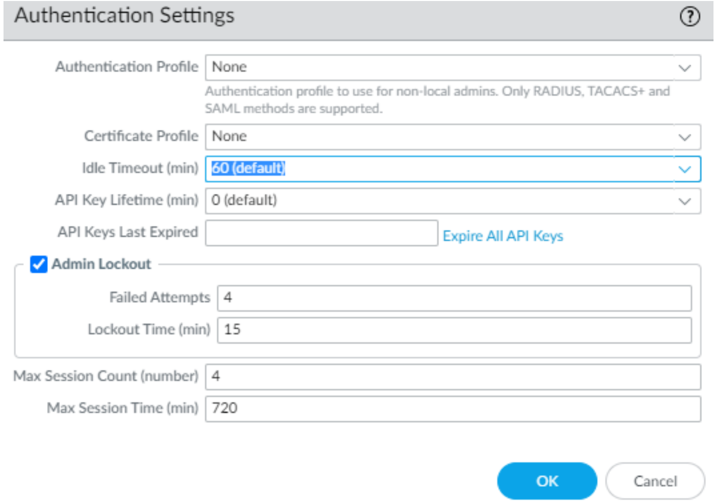
> **API HINT:** The equivalent XML API call is (need to edit the value and API key)

- **https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system&element=<login-banner>CC-Login-Banner</login-banner>&key=<APIkey>**

7.7 Configure Idle Timeout and Lockout

The administrator can configure the idle session timeout for both UI and CLI sessions (local or remote) and apply to all users including the predefined 'Admin' user. By default, the idle timeout value is 60 minutes. The administrator can also configure lockout feature to prevent someone from trying to brute-force the password. This only applies to password-based authentication, not public key-based authentication. It is required that an administrator be created, or the default admin uses SSH public key-based authentication for additional security and prevention against permanent lockout.

1. Login with Administrator Role.
2. Select **Device > Setup > Management > Authentication Settings**. The Authentication Setting page appears.



Authentication Settings

Authentication Profile	None Authentication profile to use for non-local admins. Only RADIUS, TACACS+ and SAML methods are supported.
Certificate Profile	None
Idle Timeout (min)	60 (default)
API Key Lifetime (min)	0 (default)
API Keys Last Expired	
☑ Admin Lockout	
Failed Attempts	4
Lockout Time (min)	15
Max Session Count (number)	4
Max Session Time (min)	720

3. Configure the **Idle Timeout (min)** for the TOE. The value can be 1-1,440 minutes with a default value of 60. A value of 0 means never timeout.

NOTE: Both manual and automatic refreshing of web interface pages (such as the Dashboard, Monitor, and System Alarms dialog) reset the **Idle Timeout** counter. To enable the TOE to enforce the timeout when you are on a page that supports automatic refreshing, set the refresh interval to **Manual** or to a value higher than the **Idle Timeout**. You can also disable Auto Refresh in the **ACC** tab.

4. Configure the number of **Failed Attempts**. Enter the number of failed login attempts (range is 1 to 10) that the TOE allows for the web interface and CLI before locking out the administrator account. A value of 0 specifies unlimited login attempts.

WARNING: In the evaluated configuration, you must not enter 0. This will disable the lockout feature.

5. Configure the **Lockout Time (min)** interval. Enter the number of minutes (range is 1 to 60) for which the TOE locks out an administrator from access to the web interface and CLI after reaching the **Failed Attempts** limit. A value of 0 means the lockout applies until another administrator manually unlocks the account.

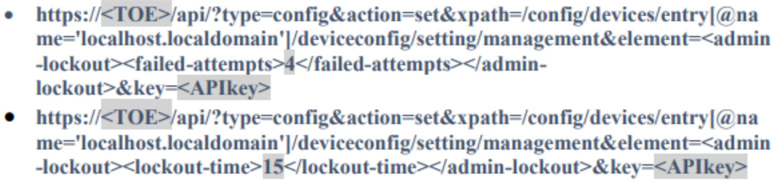
WARNING: In the evaluated configuration, you must not enter 0.

6. Click **OK**.
7. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

CLI HINT: The equivalent CLI commands are **configure** and **set deviceconfig setting management idle-timeout <0-1440>**.

CLI HINT: The equivalent CLI commands are **configure** and **set deviceconfig setting management admin-lockout failed-attempt <0-10>** and **set deviceconfig setting management admin-lockout lockout-time <0-60>**.

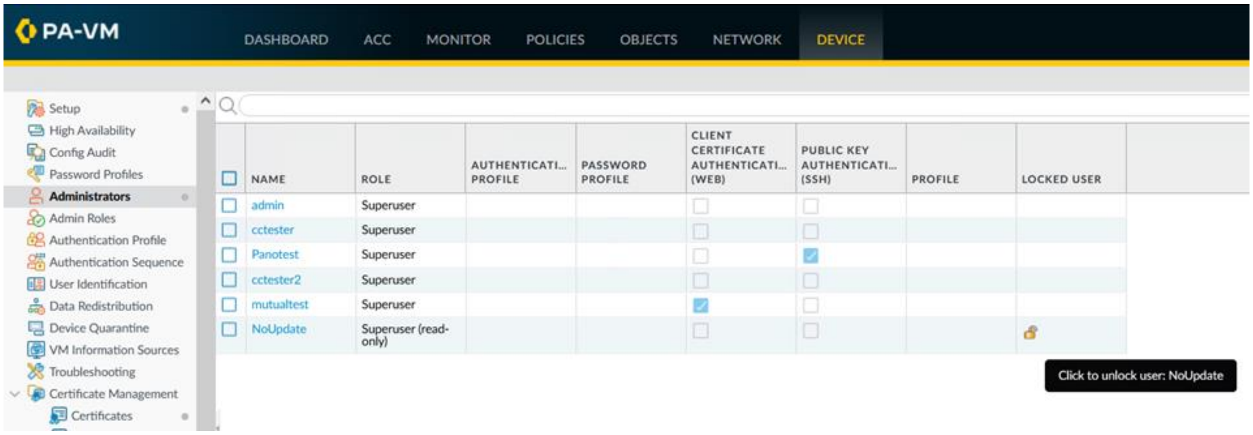
API HINT: The equivalent XML API calls are (need to edit the value and API key)



- **https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management&element=<admin-lockout><failed-attempts>4</failed-attempts></admin-lockout>&key=<APIkey>**
- **https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management&element=<admin-lockout><lockout-time>15</lockout-time></admin-lockout>&key=<APIkey>**

7.7.1 Unlock User

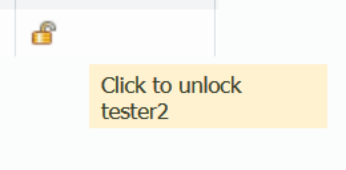
1. Login with Administrator Role.
2. Select **Device > Administrators**. The Administrators page appears.



□	NAME	ROLE	AUTHENTICATI... PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)	PROFILE	LOCKED USER
□	admin	Superuser			□	□		
□	cctester	Superuser			□	□		
□	Panotest	Superuser			□	☑		
□	cctester2	Superuser			□	□		
□	mutualtest	Superuser			☑	□		
□	NoUpdate	Superuser (read-only)			□	□		🔒

Click to unlock user: NoUpdate

3. The locked user has 🔒 in the **Locked User** column.
4. Click on that icon to unlock the user.



Click to unlock tester2

5. No commit is needed.

> **CLI HINT:** The equivalent CLI command is **request authentication unlock-admin user <username>**.

> **API HINT:** The equivalent XML API call is (need to edit the value and API key)

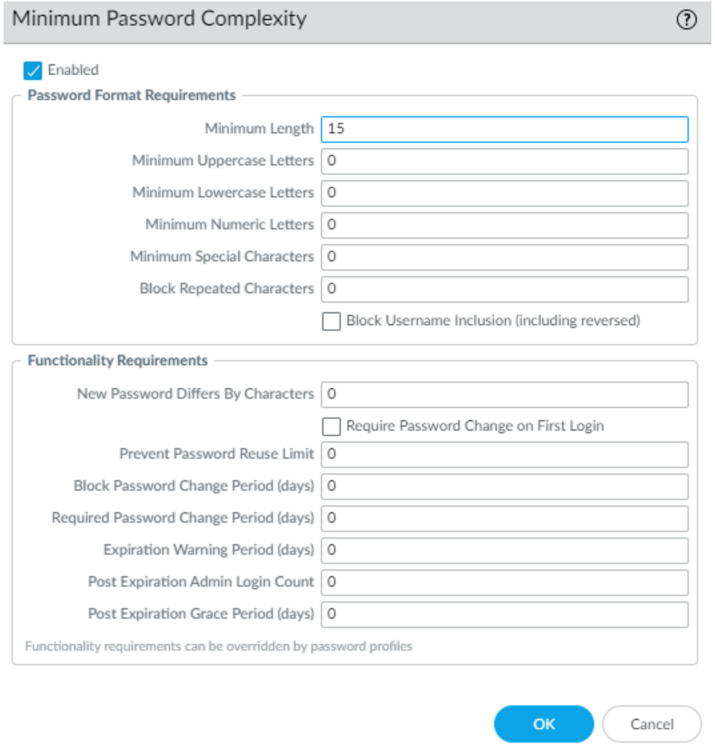
- **https://<TOE>/api/?type=op&cmd=<request><authentication><unlock-admin><user>username</user></unlock-admin></authentication></request>&key=<APIkey>**

7.8 Configure Minimum Password Length

The administrator can create password complexity rules to force users to create only strong, non-guessable passwords. Strong passwords are harder to brute-force or guess. This section will only cover minimum password length, but the administrator is recommended to configure additional password settings in the evaluated configuration (for example, password minimum length should be 12 or greater, and password should have at least one uppercase, one lowercase, one number, and one special character). Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, “)”, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “\”, “[“, “]”, “_”, “`”, “{”, “}”, and “~”.

NOTE: For the default Admin user, the password must be composed of at least one lower case, one upper case, and one number or special character. This is the default settings and can only be configured stronger, not weaker. The minimum password length for the default Admin user is lower bounded to 8 and can only be configured higher, not lower.

1. Login with Administrator Role.
2. Select **Device > Setup > Management > Minimum Password Complexity**. The Minimum Password Complexity page appears.



Minimum Password Complexity

☑ Enabled

Password Format Requirements

Minimum Length: 15
Minimum Uppercase Letters: 0
Minimum Lowercase Letters: 0
Minimum Numeric Letters: 0
Minimum Special Characters: 0
Block Repeated Characters: 0
□ Block Username Inclusion (including reversed)

Functionality Requirements

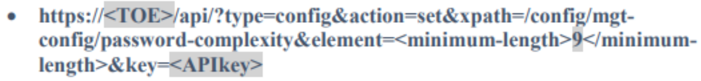
New Password Differs By Characters: 0
□ Require Password Change on First Login
Prevent Password Reuse Limit: 0
Block Password Change Period (days): 0
Required Password Change Period (days): 0
Expiration Warning Period (days): 0
Post Expiration Admin Login Count: 0
Post Expiration Grace Period (days): 0

Functionality requirements can be overridden by password profiles

3. Check the **Enabled**.
4. Enter a value in the **Minimum Length** field. The range is from 8 to 15 characters.
5. Click **OK**.
6. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

CLI HINT: The equivalent CLI commands are **configure** and **set mgt-config password-complexity minimum-length <8-15>**. Per user basis, use **set mgt-config users <User> password-complexity minimum-length <8-15>**.

API HINT: The equivalent XML API call is (need to edit the value and API key)



- **https://<TOE>/api/?type=config&action=set&xpath=/config/mgt-config/password-complexity&element=<minimum-length>9</minimum-length>&key=<APIkey>**

7.9 Configure Device DNS or SNMP Service

The administrator can configure DNS Service on the TOE. By default, the DNS service is disabled.

1. Login with Administrator Role.
2. Select **Device > Setup > Services**. The Services page appears.
3. In the settings, you can configure two DNS servers. One primary and one secondary.
4. Click on the configure icon.
5. Enter the DNS IP address or hostname in the **Primary DNS Server** field.
6. Optionally, you can provide a secondary DNS server.
7. Click **OK**.
8. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

1. Login with Administrator Role.
2. Select **Device > Setup > Operations > SNMP Setup**. The SNMP Setup page appears.
3. In the settings, you can configure the SNMP version.
4. If Version 3 is selected, you can configure the Authentication password and Privacy password along with the Authentication and Privacy protocols.

9. Click **OK**.
10. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

7.10 Configure Stateful Inspection Filtering

The TOE uses policies to enforce rules and specify actions to be taken by the TOE. Security policy rules are used to determine whether to block or allow a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service. When an administrator creates a security policy rule, the administrator can specify if the TOE will log traffic matching the rule. The administrator does this as follows.

1. Login with Administrator Role.
2. Select Policies > Security. Configure a security policy (firewall) rule.
3. Click Add and enter a Name for the rule. The following example creates a rule to deny all traffic arriving on port 22 and to log packets matching the rule:

Name: **deny-port22**

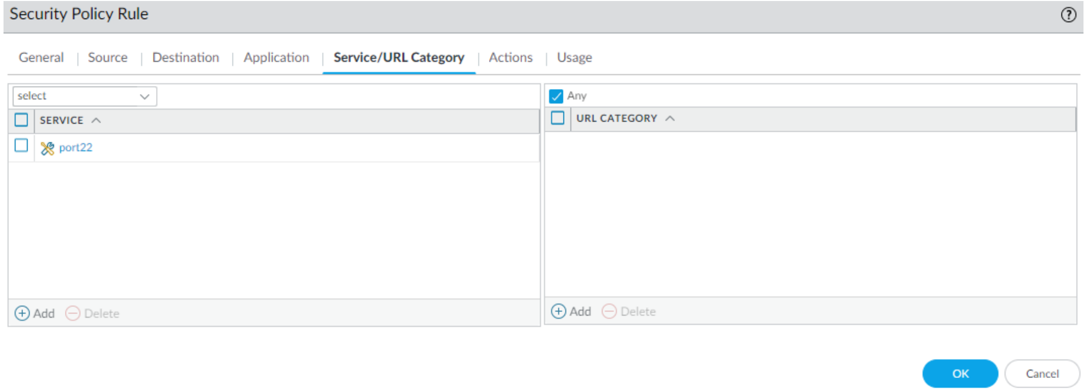
Select **any** for all options except **Service/URL Category** tab

In the **Service/URL Category** tab:

Above **Service** panel choose **select** in the drop down.

Under **Service** click **Add**

Select **port22**



Security Policy Rule

General | Source | Destination | Application | **Service/URL Category** | Actions | Usage

select

□ SERVICE

□ port22

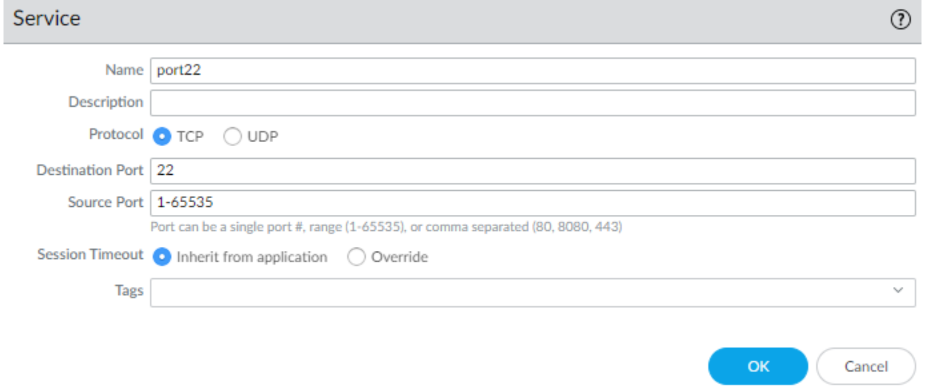
⊕ Add ⊖ Delete

☑ Any

□ URL CATEGORY

⊕ Add ⊖ Delete

OK Cancel



Service

Name: port22

Description:

Protocol: ● TCP ○ UDP

Destination Port: 22

Source Port: 1-65535

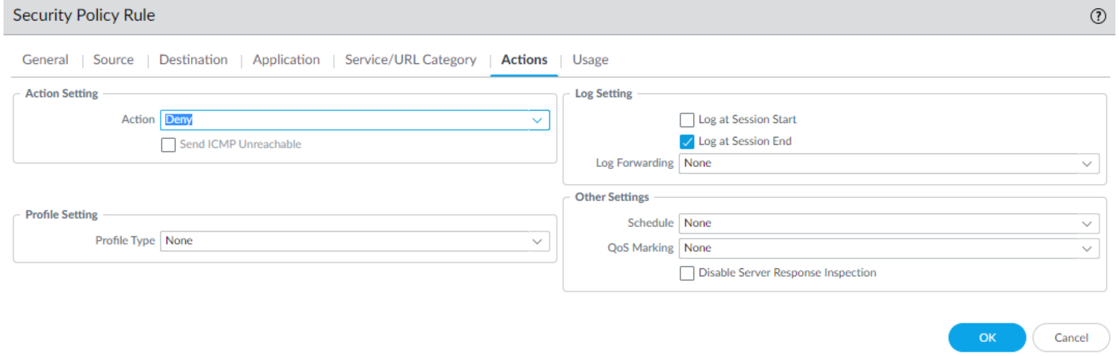
Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)

Session Timeout: ● Inherit from application ○ Override

Tags:

OK Cancel

4. Click on the **Actions** tab.
5. Set **Action Setting > Action** to **Deny** to deny SSH traffic.
6. Set **Log Setting** to **Log at Session End**.



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions** | Usage

Action Setting

Action: Deny

□ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

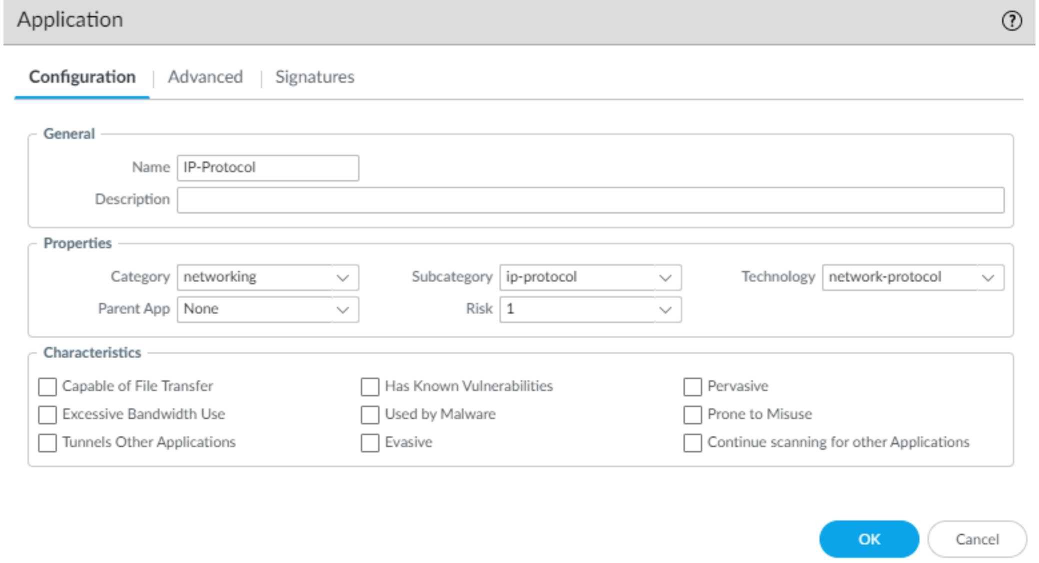
QoS Marking: None

□ Disable Server Response Inspection

OK Cancel

7. Click **OK**.

8. Click **Commit**.
9. The administrator can also filter traffic based on IP Protocol and ICMP type/code.
10. Create an application object via **Objects > Applications** and click on **Add**.
11. Assign a **Name** and configure the **Properties**.



Application

Configuration | Advanced | Signatures

General

Name: IP-Protocol

Description:

Properties

Category: networking | Subcategory: ip-protocol | Technology: network-protocol

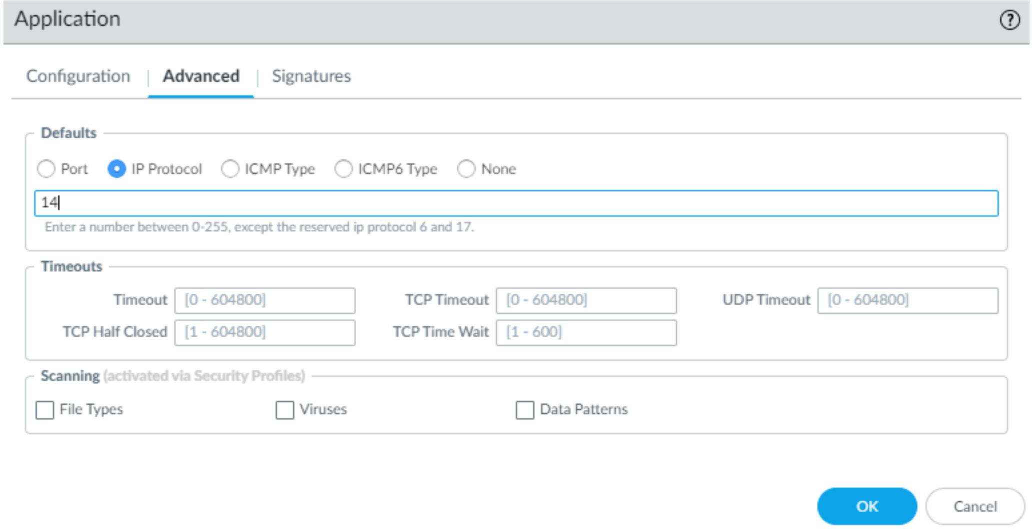
Parent App: None | Risk: 1

Characteristics

□ Capable of File Transfer □ Has Known Vulnerabilities □ Pervasive
□ Excessive Bandwidth Use □ Used by Malware □ Prone to Misuse
□ Tunnels Other Applications □ Evasive □ Continue scanning for other Applications

OK Cancel

12. On the **Advanced** tab, configure the **Defaults**.



Application

Configuration | Advanced | Signatures

Defaults

○ Port ● IP Protocol ○ ICMP Type ○ ICMP6 Type ○ None

14

Enter a number between 0-255, except the reserved ip protocol 6 and 17.

Timeouts

Timeout: [0 - 604800] | TCP Timeout: [0 - 604800] | UDP Timeout: [0 - 604800]

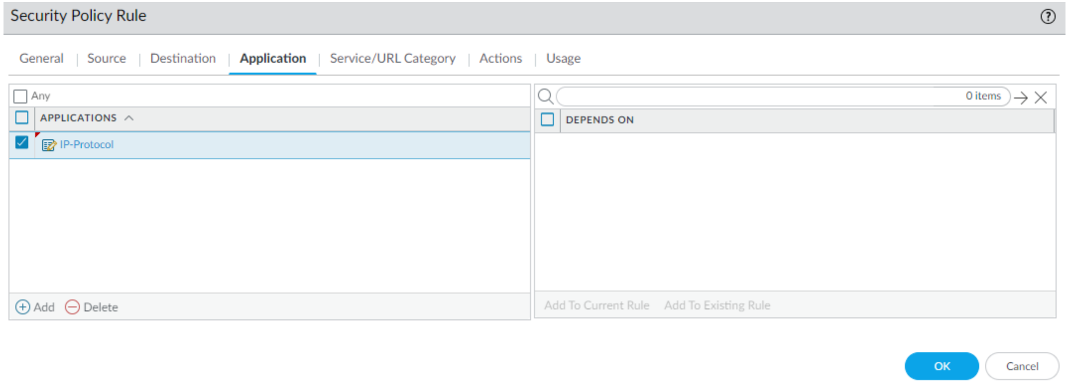
TCP Half Closed: [1 - 604800] | TCP Time Wait: [1 - 600]

Scanning (activated via Security Profiles)

□ File Types □ Viruses □ Data Patterns

OK Cancel

13. Click **OK** to create the object.
14. In the security rule, click on the **Application** tab.
15. Click **Add** and select your application object.

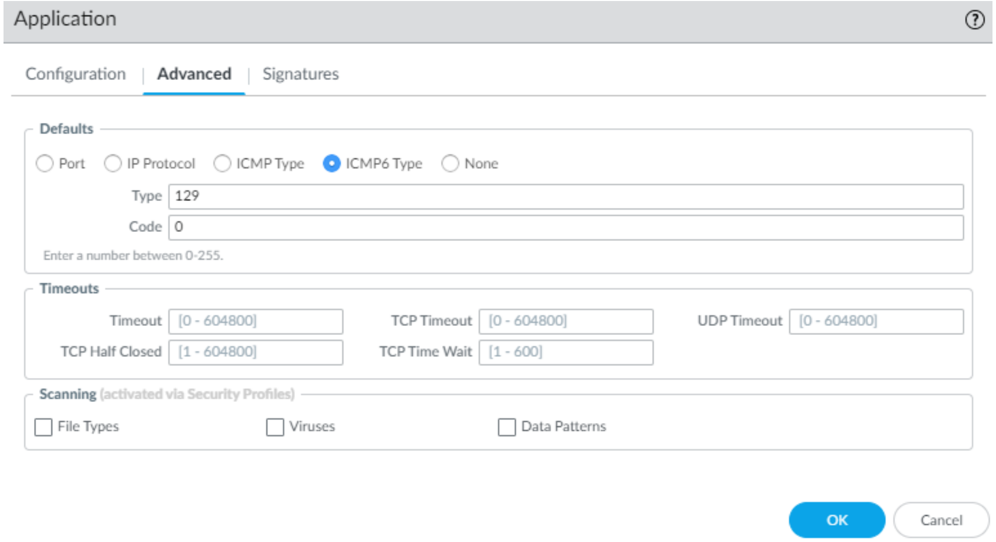

Security Policy Rule
General | Source | Destination | Application | Service/URL Category | Actions | Usage
0 items
Add To Current Rule
Add To Existing Rule
Add
Delete
OK
Cancel

□ Any

□ APPLICATIONS
☑ IP-Protocol

□ DEPENDS ON

16. Repeat the steps for ICMPv4 and ICMPv6 type/code.



Defaults

○ Port ○ IP Protocol ○ ICMP Type ● ICMP6 Type ○ None

Type 129

Code 0

Enter a number between 0-255.

Timeouts

Timeout [0 - 604800] TCP Timeout [0 - 604800] UDP Timeout [0 - 604800]

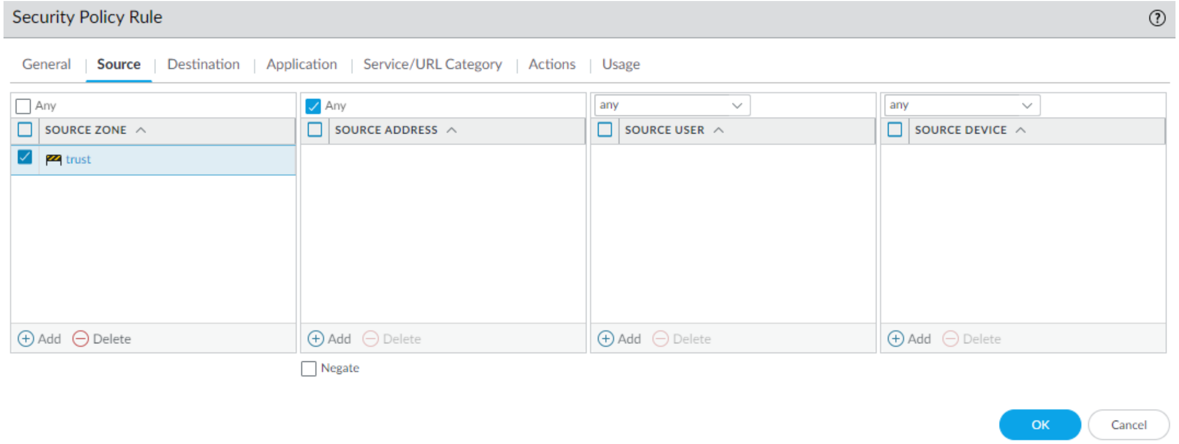
TCP Half Closed [1 - 604800] TCP Time Wait [1 - 600]

Scanning (activated via Security Profiles)

□ File Types □ Viruses □ Data Patterns

17. Click **OK**.
18. Click **Commit**.

The security rule can be assigned to security zones (source or destination). Each zone is tied to a physical interface (e.g., ethernet1/1, ethernet2/1). The administrator can assign security rules to a distinct interface by configuring the source and destination zones. For example, let's configure physical ethernet1/1 interface as Trusted Zone and ethernet2/1 interface as Untrusted Zone. The administrator can create a security rule that allow certain traffic from Trusted Zone to Untrusted Zone and the rule will only apply to traffic traveling from ethernet1/1 to ethernet2/1. Vice versa, the administrator can create a more restrictive security rule from Untrusted Zone to Trusted Zone.



Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions | Usage

☐ Any

☐ SOURCE ZONE

☑ trust

☑ Any

☐ SOURCE ADDRESS

☐ Negate

any

☐ SOURCE USER

any

☐ SOURCE DEVICE

The TOE can be configured to perform stateful traffic filtering on the following protocols and associated attributes:

- Internet Control Message Protocol version 4 (ICMPv4), as defined in RFC 792
  - o Type
  - o Code
- Internet Control Message Protocol version 6 (ICMPv6), as defined in RFC 4443
  - o Type
  - o Code
- Internet Protocol (IPv4), as defined in RFC 791
  - o Source address
  - o Destination address
  - o Transport layer protocol [0-255[8]]
- Internet Protocol version 6 (IPv6), as defined in RFC 2460
  - o Source address
  - o Destination address
  - o Transport layer protocol [0-255]
- Transmission Control Protocol (TCP), as defined in RFC 793
  - o Source port
  - o Destination port
- User Datagram Protocol (UDP), as defined in RFC 768
  - o Source port
  - o Destination port.

The TOE group interfaces into security zones. Each zone identifies one or more interfaces on the firewall. Separate zones must be created for each type of interface (Layer 2, Layer 3, or virtual wire), and each interface must be assigned to a zone before it can process traffic.

On the TOE, security policies are used to determine whether to block or allow a session, based on traffic attributes such as the source and destination security zone, the source and destination

[8] Enter a number between 0-255, except the reserved IP/IPv6 protocols 6 and 17.

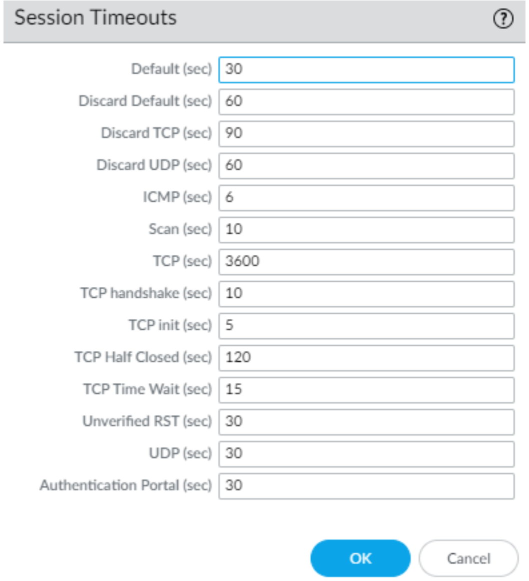
IP address, and the source and destination port (service). A security policy rule also includes the following attributes that determine what the TOE does with the network packet:

- Action—can be ‘allow’ or ‘deny’
- Profiles—specifies any checking to be performed by the security profiles such as IPsec crypto Security and IKE Network Security. These profiles allow/require the network traffic to be PROTECTed.)
- Options—specifies the following additional processing options for network packets matching the rule:
    - o Log Setting—generate log entries in the local traffic log
    - o Schedule—limits the days and times when the rule is in effect (e.g., an ‘allow’ rule might be active only during normal business hours)
    - o QoS Marking—change the Quality of Service (QoS) marking on packets matching the rule
    - o Disable Server Response Inspection—disables packet inspection from the server to the client, which may be useful under heavy server load conditions.

All traffic passing through the TOE is matched against a session and each session is matched against a security policy. When a session match occurs, the security policy is applied to bi-directional traffic (client to server and server to client) in that session. For traffic that doesn’t match any defined rules, the default rules apply. The default rules allow all intrazone (within the same zone) traffic and deny all interzone (between different zones, e.g., ‘trust’ and ‘untrust’) traffic. Typically, intrazone traffic is considered to be trusted. However, both intrazone and interzone traffic can be configured to deny all traffic if there is no rule match by clicking on the security policy and clicking on the Override button on the bottom on the Policy ->Security screen. In the evaluated configuration, the default deny all rule for interzone traffic must not be modified. Each rule can be configured to generate a log record when the traffic matches the defined rule using the ‘policy->Security->options’ selection. The logging option can be configured to log at the start of a session, or at the end of a session or both.

Security policies are evaluated left to right and from top to bottom. A packet is matched against the first rule that meets the defined criteria; after a match is triggered the subsequent rules are not evaluated. The administrator can order the rules anyway they want but here is a recommendation. The more specific rules must precede more generic ones in order to enforce the best match criteria. Traffic that matches a rule generates a log entry at the end of the session in the traffic log (by default), if configured for that rule. The logging options are configurable for each rule and can for example be configured to log at the start of a session instead of, or in addition to, logging at the end of a session.

The TOE can remove existing traffic flows from the set of established traffic flows based on the session inactivity timeout and completion of the expected information flow. The timeout period due to inactivity is administrator configurable from 1 – 6044800 seconds (**Device > Session > Session Timeouts**). Session removal becomes effective before the next packet that might match the session is processed.



Session Timeouts

Default (sec)	30
Discard Default (sec)	60
Discard TCP (sec)	90
Discard UDP (sec)	60
ICMP (sec)	6
Scan (sec)	10
TCP (sec)	3600
TCP handshake (sec)	10
TCP init (sec)	5
TCP Half Closed (sec)	120
TCP Time Wait (sec)	15
Unverified RST (sec)	30
UDP (sec)	30
Authentication Portal (sec)	30

Traffic is dropped if the source address of the incoming traffic corresponds to the IP address of an external broadcast network or loopback network; if the incoming traffic is received from the external network but has a source address that correspond to the internal network; or if traffic is received from the internal network but has a source address that correspond to the external network. The TOE rejects packets where the source address is equal to the address of the network interface where the network packet was received. Access or service requests are also rejected when the presumed source identity specifies a broadcast identity or a loopback identifier. Security rules to block, permit or log are applied to multicast traffic. The TOE rejects and logs packets where the source address of the network packet is defined as being on a multicast network. The TOE discards and logs strict source routing, loose source routing, and record route packets. The TOE blocks IPv4 packets with the shared address space address range 100.64.0.0/10 as specified in RFC 6598, and link-local addresses[9] in the source or destination address. In addition, requests in which the information received contains the set of host network identifiers by which information is to travel from the source subject to the destination subject are rejected.

The TOE drops the following traffic:

- Invalid fragments;
- Fragmented packets which cannot be re-assembled completely;
- Network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4; and

[9] IPv4 link-local addresses are assigned to address block 169.254.0.0/16 and IPv6 link-local addresses are assigned the address block fe80::/10.

- Network packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6.

The TOE blocks the following IPv6 traffic:

- block both inbound and outbound IPv6 Site Local Unicast addresses (FEC0::/10)
- block IPv6 Jumbo Payload datagrams (Option Type 194).
- drop all inbound and outbound IPv6 packets containing a Hop-by-Hop header with option type values intended for Destination Options
- block RFC 6598 "Carrier Grade NAT" IP address block of 100.64.0.0/10
- drop all inbound IPv6 packets for which the layer 4 protocol and ports (undetermined transport) cannot be located.
- drop all inbound IPv6 packets with a Type 0 Routing header
- drop all inbound IPv6 packets with a Type 1 or Types 3 through 255 Routing Header.
- drop all inbound IPv6 packets containing undefined header extensions/protocol values.
- drop fragmented IPv6 packets when any fragment overlaps another.
- drop all inbound IPv6 packets containing more than one Fragmentation Header within an IP header chain.
- drop all inbound and outbound IPv6 packets containing a Hop-by-Hop header with option type values intended for Destination Options.
- block IPv6 multicast addresses (FF00::/8) as a source address

The TOE creates dynamic rules, maintaining the session states to support processing the FTP network protocol traffic for TCP data sessions in accordance with the FTP protocol as specified in RFC 959 using the FTP App-ID. The TOE uses App-ID, the traffic classification technology, to identify traffic on the network. Logging can be enabled in the security policy rule configured to control the FTP traffic.

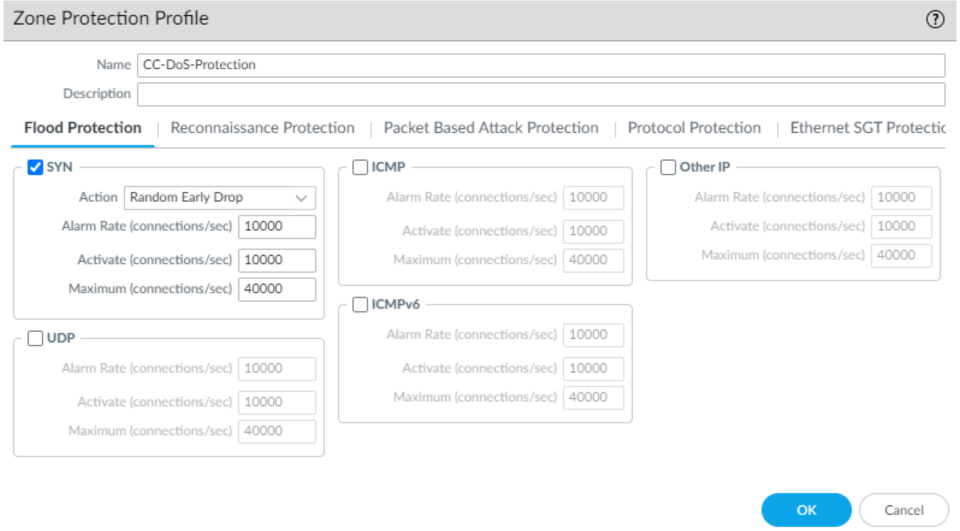
7.10.1 Zone Protection Profile

Zone protection profile defends the system from session, resource-based, and flood attacks. A DoS attack overloads the network with large amounts of unwanted traffic in an attempt to disrupt services. A Zone protection profile with flood protection configured defends against

SYN, ICMP, IMCPv6, UDP, and other IP flood attacks. For each flood type, the administrator can set three thresholds for new connection per second (CPS) entering the zone and can set DROP action for SYN floods. By default, this feature is not enabled. When it is enabled, the default value is 10,000 connections per second. If the CPS is set too low, the TOE may start dropping legit half-open TCP connections (per zone). If the CPS is set too high, the TOE resources may be exhausted before the protection is activated.

- Alarm Rate – The new CPS threshold to trigger an alarm.
- Activate – The new CPS threshold to activate the flood protection mechanism and begin dropping new connections.
- Maximum – The max percentage of TOE capacity taking into account other features that consume TOE resources.

1. Login with Administrator Role.
2. Select Network > Zone Protection. Click Add.
3. Enter a name for the zone protection profile.
4. On the Flood Protection tab, click on the type of floods.
5. Enter the values for Alarm Rate, Activate, and Maximum.


Zone Protection Profile
?

Name CC-DoS-Protection

Description

Flood Protection | Reconnaissance Protection | Packet Based Attack Protection | Protocol Protection | Ethernet SGT Protectic

☑ SYN

Action Random Early Drop

Alarm Rate (connections/sec) 10000

Activate (connections/sec) 10000

Maximum (connections/sec) 40000

□ UDP

Alarm Rate (connections/sec) 10000

Activate (connections/sec) 10000

Maximum (connections/sec) 40000

□ ICMP

Alarm Rate (connections/sec) 10000

Activate (connections/sec) 10000

Maximum (connections/sec) 40000

□ ICMPv6

Alarm Rate (connections/sec) 10000

Activate (connections/sec) 10000

Maximum (connections/sec) 40000

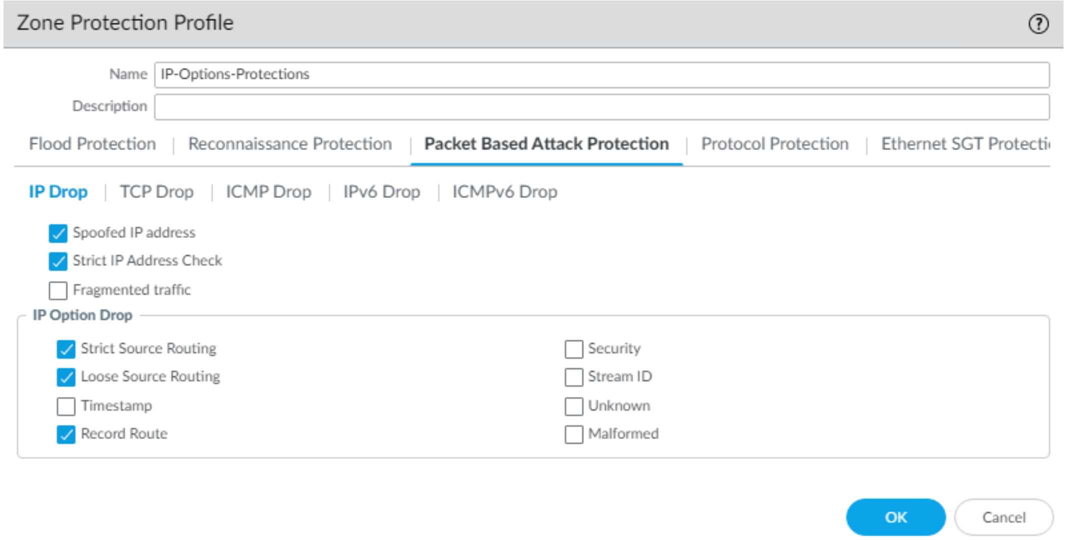
□ Other IP

Alarm Rate (connections/sec) 10000

Activate (connections/sec) 10000

Maximum (connections/sec) 40000

6. On the Packet Based Attack Protection tab, click on the IP Drop.



Name: IP-Options-Protections

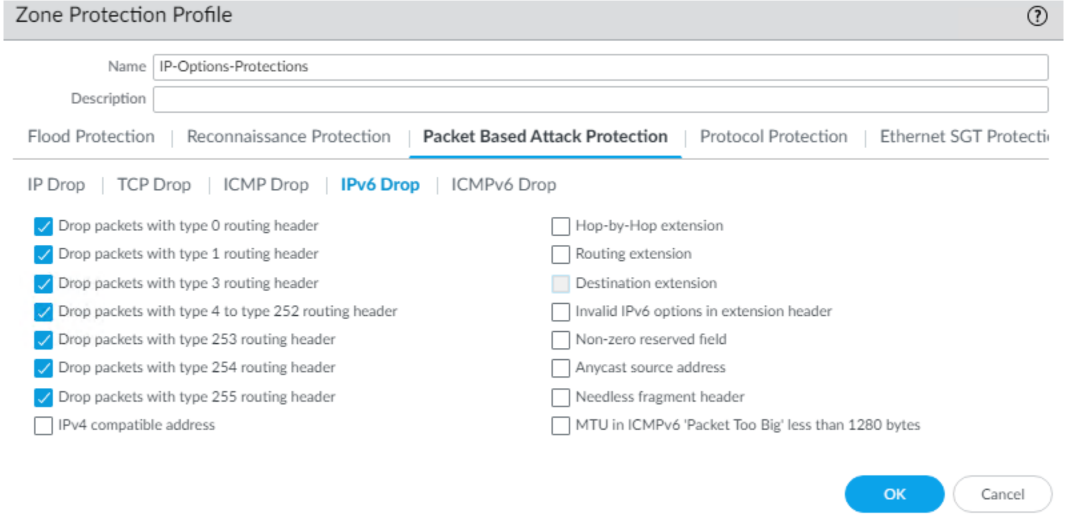
Description:

☑ Spoofed IP address
☑ Strict IP Address Check
☐ Fragmented traffic

IP Option Drop

☑ Strict Source Routing
☑ Loose Source Routing
☐ Timestamp
☑ Record Route
☐ Security
☐ Stream ID
☐ Unknown
☐ Malformed

7. Configure as shown above.
8. Click on the IPv6 Drop.

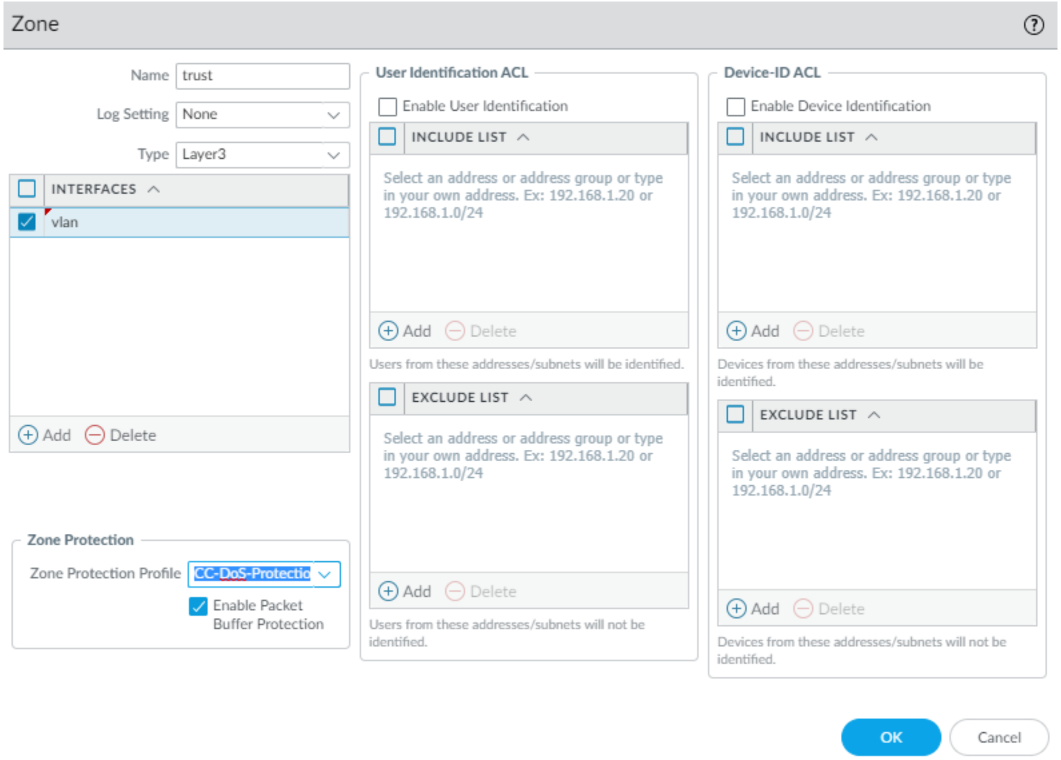


Name: IP-Options-Protections

Description:

☑ Drop packets with type 0 routing header
☑ Drop packets with type 1 routing header
☑ Drop packets with type 3 routing header
☑ Drop packets with type 4 to type 252 routing header
☑ Drop packets with type 253 routing header
☑ Drop packets with type 254 routing header
☑ Drop packets with type 255 routing header
☐ IPv4 compatible address
☐ Hop-by-Hop extension
☐ Routing extension
☐ Destination extension
☐ Invalid IPv6 options in extension header
☐ Non-zero reserved field
☐ Anycast source address
☐ Needless fragment header
☐ MTU in ICMPv6 'Packet Too Big' less than 1280 bytes

9. Configure as shown above.
10. Click OK to create the profile object.
11. Now associate that profile object with a security zone.
12. Select Network > Zones. Create a new zone or modifying an existing zone.
13. Go to the Zone Protection and set it to the object created above.


Zone
User Identification ACL
☐ Enable User Identification
☐ INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
⊕ Add ⊖ Delete
Users from these addresses/subnets will be identified.
☐ EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
⊕ Add ⊖ Delete
Users from these addresses/subnets will not be identified.
Device-ID ACL
☐ Enable Device Identification
☐ INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
⊕ Add ⊖ Delete
Devices from these addresses/subnets will be identified.
☐ EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
⊕ Add ⊖ Delete
Devices from these addresses/subnets will not be identified.
⊕ Add ⊖ Delete
OK
Cancel

Name: trust
Log Setting: None
Type: Layer3

☐ INTERFACES
☑ vlan

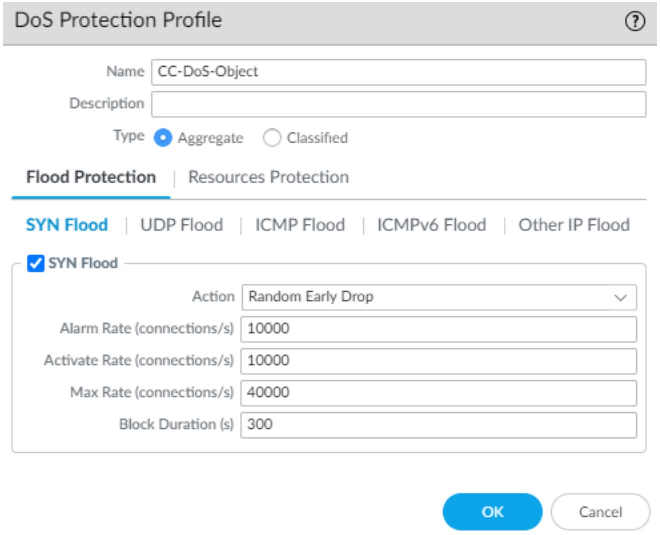
Zone Protection
Zone Protection Profile: CC-DoS-Protectio
☑ Enable Packet Buffer Protection

14. Click **OK**.
15. **Commit** the changes.

7.10.2 Denial of Service (DoS) Protection Profile

The DoS protection profiles, and DoS protection policy rules combine to protect specific groups of critical resources and individual critical resources against session floods such as TCP SYN floods. Compared to the Zone protection profiles, which protect entire zones from flood attacks, DoS protection provides granular defense for specific systems and targets such as web servers and database servers. By default, this feature is not enabled. When it is enabled, the default value is 10,000 connections per second. If the CPS is set too low, the TOE may start dropping legit half-open TCP connections (per destination). If the CPS is set too high, the TOE resources may be exhausted before the protection is activated.

1. Login with Administrator Role.
2. Select **Object** > **Security Profiles** > **DoS Protection**. Click **Add**.
3. Configure the same values but also specify the block duration.


DoS Protection Profile

Name: CC-DoS-Object

Description:

Type: ● Aggregate ○ Classified

Flood Protection | Resources Protection

SYN Flood | UDP Flood | ICMP Flood | ICMPv6 Flood | Other IP Flood

☑ SYN Flood

Action: Random Early Drop

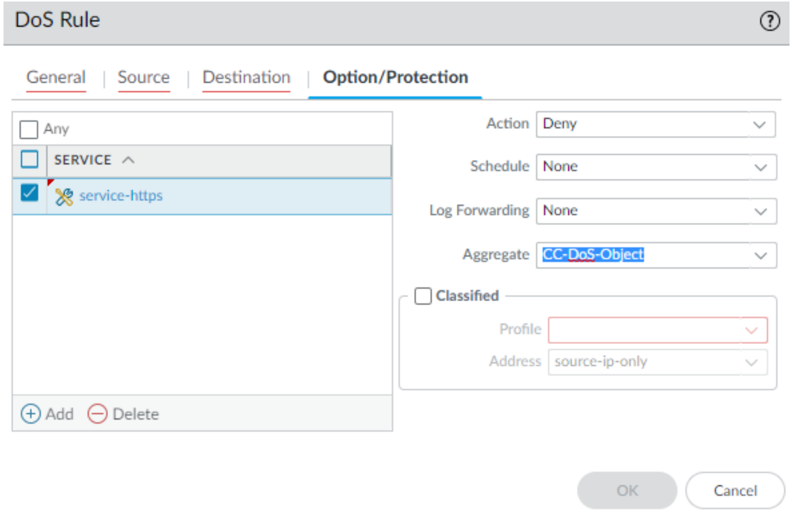
Alarm Rate (connections/s): 10000

Activate Rate (connections/s): 10000

Max Rate (connections/s): 40000

Block Duration (s): 300

4. Click **OK**.
5. Go to **Policies > Dos Protection**. Click **Add.**
6. On the **General** tab, enter a name and description.
7. Specify the source and destination zones and/or IP addresses.
8. On the **Option/Protection** tab, specify the service (e.g., web server or service-http/service-https) and select the profile created above in the **Aggregate**.


DoS Rule

General | Source | Destination | Option/Protection

□ Any

□ SERVICE

☑ service-https

Action: Deny

Schedule: None

Log Forwarding: None

Aggregate: CC-DoS-Object

□ Classified

Profile:

Address: source-ip-only

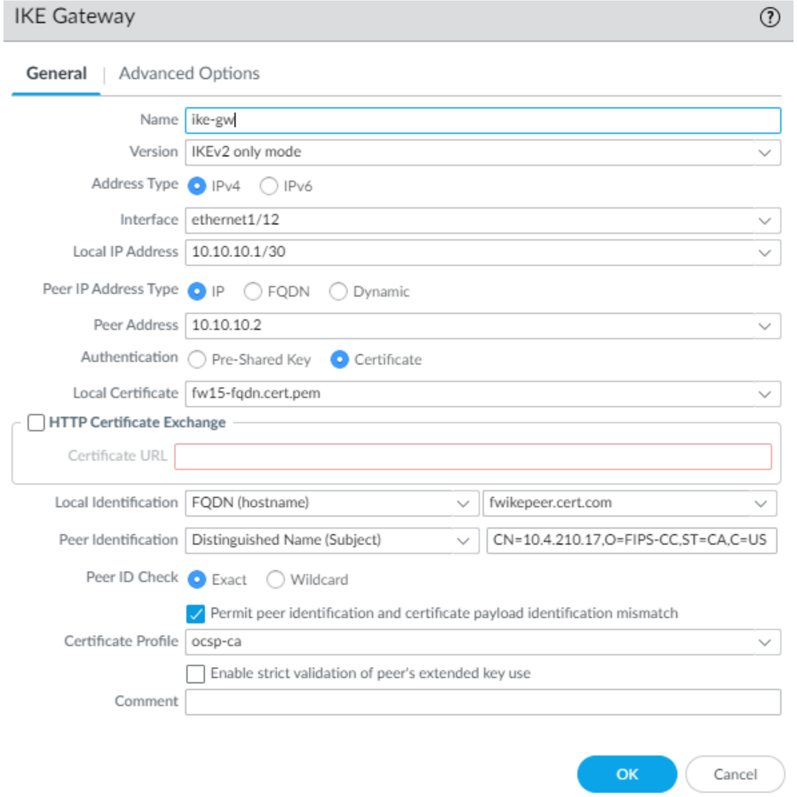
9. Click **OK**.
10. **Commit** the changes.

7.11 Configure IKE/IPsec VPN Gateway

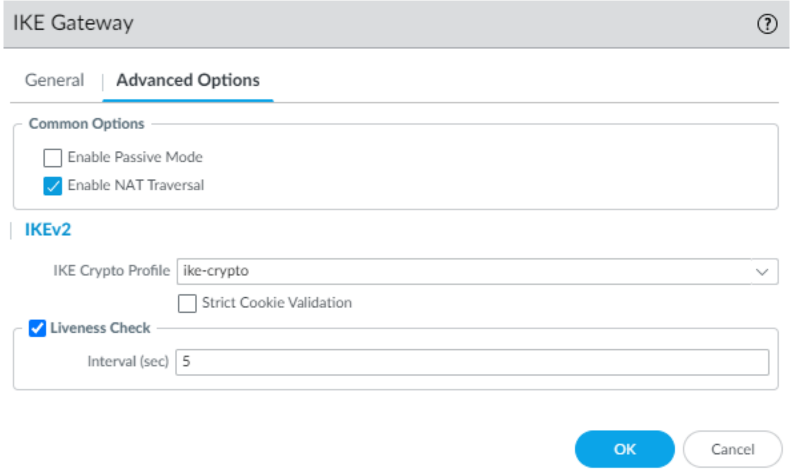
The administrator can configure the TOE as an IKE/IPsec VPN gateway and specify **IKEv1 only mode**, **IKEv2 only mode**, or **IKEv2 preferred mode**. The gateway begins its negotiation with its peer in the mode specified here. If the administrator selects **IKEv2 preferred mode**, the two peers will use IKEv2 if the remote peer supports it; otherwise, they will use IKEv1.

WARNING: If you specify **IKEv1 mode only** or **IKEv2 preferred mode**, you must specify main for the **Exchange Mode** (done on the **Network > IKE Gateways > Advanced Options** tab). Aggressive mode is not allowed in the evaluated configuration.

NAT traversal (NAT-T) must be enabled on both gateways if NAT is occurring on a device that sits between the two gateways. Select the **Advanced Options** tab and select **Enable NAT Traversal**.



Name: ike-gw
Version: IKEv2 only mode
Address Type: ● IPv4 ○ IPv6
Interface: ethernet1/12
Local IP Address: 10.10.10.1/30
Peer IP Address Type: ● IP ○ FQDN ○ Dynamic
Peer Address: 10.10.10.2
Authentication: ○ Pre-Shared Key ● Certificate
Local Certificate: fw15-fqdn.cert.pem
□ HTTP Certificate Exchange
Certificate URL:
Local Identification: FQDN (hostname) fwikepeer.cert.com
Peer Identification: Distinguished Name (Subject) CN=10.4.210.17,O=FIPS-CC,ST=CA,C=US
Peer ID Check: ● Exact ○ Wildcard
☑ Permit peer identification and certificate payload identification mismatch
Certificate Profile: ocsp-ca
□ Enable strict validation of peer's extended key use
Comment:



Common Options

□ Enable Passive Mode

☑ Enable NAT Traversal

IKEv2

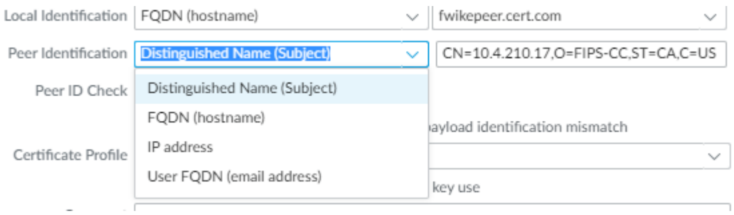
IKE Crypto Profile: ike-crypto

□ Strict Cookie Validation

☑ Liveness Check

Interval (sec): 5

A trusted channel is established only if the presented identifier in the peer certificate matches the configured reference identifier, and the peer certificate is signed by a trusted anchor CA specified in the **Certificate Profile**. Local identification defines the format and identification of the local gateway. The **Local Certificate** identifies the local gateway certificate (RSA-based or ECDSA-based) that will be presented to the IKE peer. Select the **Local Identification** type from the following: **Distinguished Name (Subject)**, **FQDN (hostname)**, **IP address**, and enter the value. Peer identification defines the format and identification of the peer gateway. Select the **Peer Identification** type from the following: **Distinguished Name (Subject)**, **FQDN (hostname)**, **IP address**, and enter the value.


Distinguished Name (Subject)
FQDN (hostname)
IP address
User FQDN (email address)
ayload identification mismatch
key use

Local Identification: FQDN (hostname) | fwikepeer.cert.com

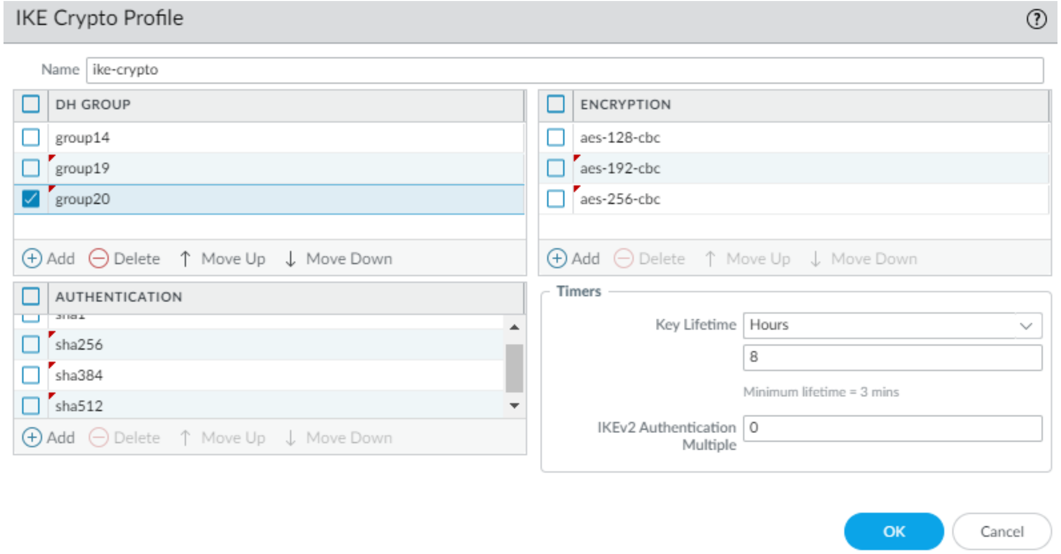
Peer Identification: Distinguished Name (Subject) | CN=10.4.210.17,O=FIPS-CC,ST=CA,C=US

Peer ID Check

Certificate Profile

When configuring an IKE cryptographic profile:

- Only the following Diffie-Hellman (DH) groups are to be used: **group14**; **group19**; **group20**.
- Only the following authentication algorithms are to be used: **sha1**; **sha256**; **sha384**; **sha512**.
- Only the following encryption algorithms are to be used: **aes-128-cbc**; **aes-192-cbc**; **aes-256-cbc**.



IKE Crypto Profile

Name: ike-crypto

□ DH GROUP
□ group14
□ group19
☑ group20

□ ENCRYPTION
□ aes-128-cbc
□ aes-192-cbc
□ aes-256-cbc

□ AUTHENTICATION
□ sha1
□ sha256
□ sha384
□ sha512

Timers

Key Lifetime: Hours

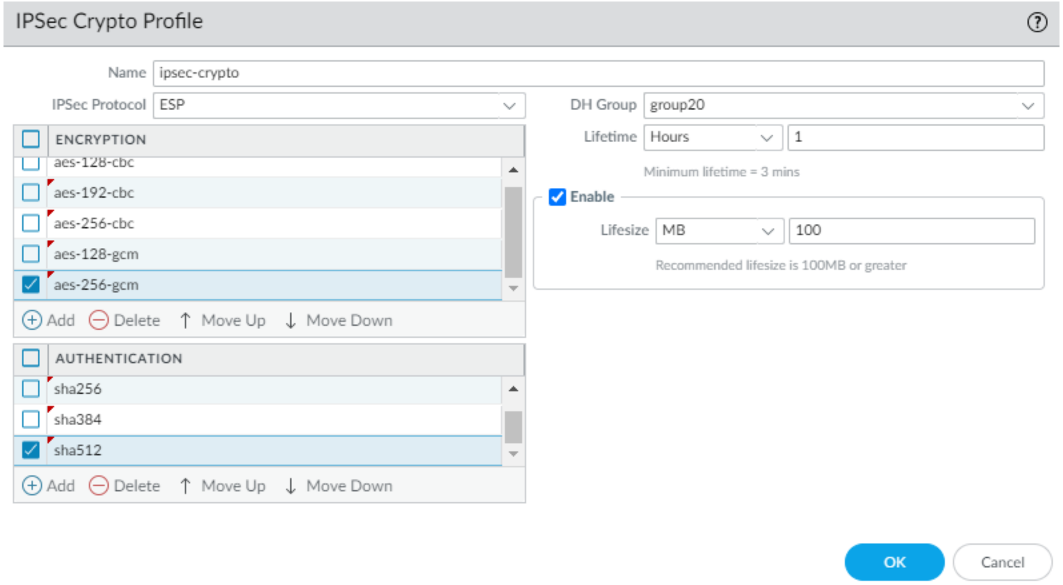
8

Minimum lifetime = 3 mins

IKEv2 Authentication Multiple: 0

When configuring an IPsec cryptographic profile:

- Select ESP (Encapsulating Security Payload) as the IPsec Protocol. Do not use AH (Authentication Header).
- Only the following encryption algorithms are to be used: **aes-128-cbc**; **aes-192-cbc**; **aes-256-cbc**; **aes128-gcm**; **aes-256-gcm**. Do not specify aes-128-ccm.
- Only the following authentication algorithms are to be used: **sha1**; **sha256**; **sha384**; **sha512**.
- Only the following Diffie-Hellman (DH) groups are to be used: **group14**; **group19**; **group20**.



IPSec Crypto Profile

Name: ipsec-crypto

IPSec Protocol: ESP

□	ENCRYPTION
□	aes-128-cbc
□	aes-192-cbc
□	aes-256-cbc
□	aes-128-gcm
☑	aes-256-gcm

□	AUTHENTICATION
□	sha256
□	sha384
☑	sha512

DH Group: group20

Lifetime: Hours 1

Minimum lifetime = 3 mins

☑ Enable

Lifesize: MB 100

Recommended lifesize is 100MB or greater

Note also, when configuring and selecting IKE and IPsec cryptographic profiles, that the key strength of the encryption algorithm specified in the IPsec profile is not to be greater than the key strength of the encryption algorithm specified in the IKE profile. For example, if the configured IKE profile specifies **aes-128-cbc**, then the configured IPsec profile must not specify **aes-256-cbc** or **aes-256-gcm**.

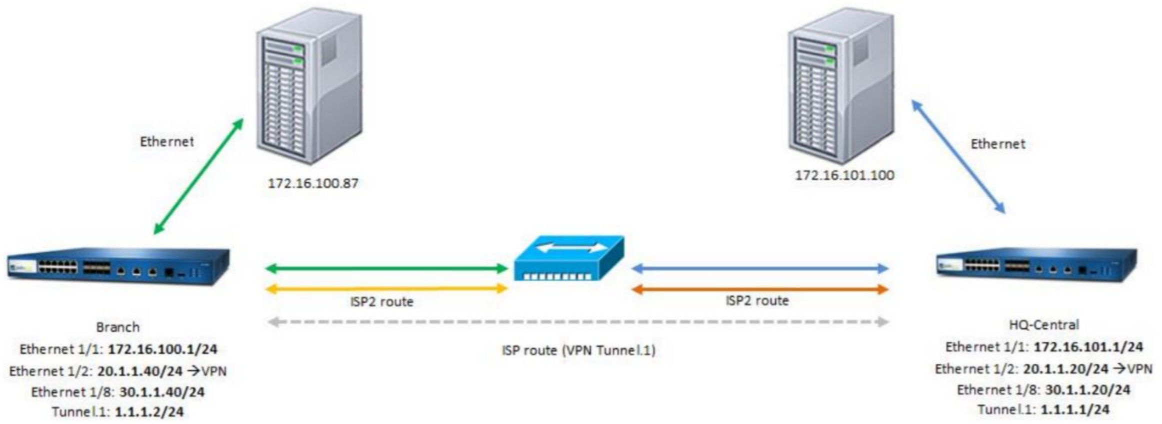
The Phase 1 lifetime is configured in the IKE profile and can be specified in seconds, minutes, hours, or days. The supported range is 3 minutes to 365 days, with a default of 8 hours. The Phase 2 lifetime is configured in the IPsec profile and can be specified in terms both of time (in seconds, minutes, hours, or days—the supported range is 3 minutes to 365 days) (denoted as **Lifetime**), and volume of data (denoted as **Lifesize**).

The administrator may choose to allow a successful IKE SA even when the peer identification does not match the peer identification in the certificate by selecting **Permit peer identification and certificate payload identification mismatch**. This selection is not permitted in the evaluated configuration.

7.11.1 Policy-Based Forwarding

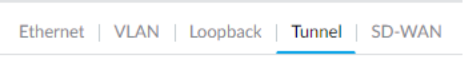
The Policy-Based Forwarding (PBF) provides information on configuring rules consistent with the definition of an IPsec Security Policy Database (SPD) as specified in RFC 4301 (i.e., rules that contain operations that DISCARD, BYPASS, and PROTECT network packets).

The following example shows how to set up connections between peer VPN devices and configure Policy-Based Forwarding and security policy rules for DISCARD, BYPASS and PROTECT processing. It uses the following setup:


Ethernet
172.16.100.87
172.16.101.100
Ethernet
ISP2 route
ISP2 route
Branch
Ethernet 1/1: **172.16.100.1/24**
Ethernet 1/2: **20.1.1.40/24** →VPN
Ethernet 1/8: **30.1.1.40/24**
Tunnel.1: **1.1.1.2/24**
ISP route (VPN Tunnel.1)
HQ-Central
Ethernet 1/1: **172.16.101.1/24**
Ethernet 1/2: **20.1.1.20/24** →VPN
Ethernet 1/8: **30.1.1.20/24**
Tunnel.1: **1.1.1.1/24**

(1) Configure Zones, Ports, and Interfaces on the Branch Firewall:

1. Login with Administrator Role.
2. Select **Network > Zones**. Click **Add**.
   - Enter the zone name in the **Name** field. In example above, ISP2.
   - Select **Type** as **Layer 3**.
3. Click **OK**.
4. Select **Network > Interfaces**. Click **ethernet1/8**.
5. Select **Interface Type** as **Layer 3**.
6. On the **Config** tab
   - set **Assign Interface To – Virtual Router** = **branch-router** (created in step 13)
   - Set **Assign Interface To – Zones** = **ISP2** (or the zone you created in step 2).
7. On the **IPv4** tab
   - Select **Static** as the **Type**.
   - Click **Add**.
   - Type **30.1.1.40/24** as in example above.
8. Click **OK**.
9. On the **Tunnel** tab (part of the **Network > Interfaces** page)



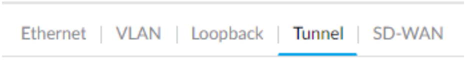
10. Click **Add**. Should be named **tunnel.<1-9999>**.
11. On the **IPv4** tab
    - Select **Static** as the **Type**.
    - Click **Add**.
    - Type **1.1.1.2/24** as in example above.
12. Click **OK**.
13. Select **Network > Virtual Routers**. Click **Add**.
    - Enter the name in the **Name** field. In example above, branch-router.
    - Click on the side **Static Routes** tab. Click **Add**.
    - Enter the name in the **Name** field. For example, ISP2-PBF
    - Enter the **Destination** field. For example, 172.16.100.0/24.
    - Enter the **Interface** field. For example, ethernet1/8.
    - Select **Next Hop** as **None**.
    - Enter **11** (as different than IPsec route) for **Metric**.

- Click **OK**.

14. Click **OK**.

(2) Configure Zones, Ports, and Interfaces on the HQ-Central Firewall:

1. Login with Administrator Role.
2. Select **Network > Zones**. Click **Add**.
   - Enter the zone name in the **Name** field. In example above, ISP2.
   - Select **Type** as **Layer 3**.
3. Click **OK**.
4. Select **Network > Interfaces**. Click **ethernet1/8**.
5. Select **Layer 3** as **Interface Type**.
6. On the **Config** tab
   - set **Assign Interface To – Virtual Router** = **central-router** (created in step 13)
   - Set **Assign Interface To – Zones** = **ISP2** (or the zone you created in step 2).
7. On the **IPv4** tab
   - Select **Static** as the **Type**.
   - Click **Add**.
   - Type **30.1.1.20/24** as in example above.
8. Click **OK**.
9. On the **Tunnel** tab (part of the **Network > Interfaces** page)



10. Click **Add**. Should be named **tunnel.<1-9999>**.
11. On the **IPv4** tab
    - Select **Static** as the **Type**.
    - Click **Add**.
    - Type **1.1.1.1/24** as in example above.
12. Click **OK**.
13. Select **Network > Virtual Routers**. Click **Add**.
    - Enter the name in the **Name** field. In example above, central-router.
    - Click on the side **Static Routes** tab. Click **Add**.
    - Enter the name in the **Name** field. For example, ISP2-PBF

- Enter the **Destination** field. For example, 172.16.101.0/24.
- Enter the **Interface** field. For example, ethernet1/8.
- Select **Next Hop** as **None**.
- Enter **11** (as different than IPsec route) for **Metric**.
- Click **OK**.

14. Click **OK**.

(3) Configure PBF Rules for ISP2 on the Branch Firewall:

1. Login with Administrator Role.
2. Select **Policies > Policy Based Forwarding**. Click **Add**.
   - Enter the rule name in the **Name** field. In example above, ISP2-PBF.
   - On **Source** tab, select **Interface** as **Type**.
     i. In the **Interface** window, click **Add**.
     ii. Select **ethernet1/1** as in example above.
     iii. In the **Source Address** window, Click **Add**.
     iv. Enter **172.16.100.87** as in example above.
     v. Select **any** for **Source User** window.
   - On **Destination/Application/Service** tab
     i. In the **Destination Address** window, click **Add**.
     ii. Enter **172.16.101.100** as in example above.
     iii. Leave default **any** for both Applications and Service
   - On **Forwarding** tab
     i. Select **Forward** as the **Action**. This should be the default action.
     ii. Select **ethernet1/8** as the **Egress Interface** as shown in example.
     iii. Enter **30.1.1.20** as Next Hop (IP address of peer device alternative interface).
3. Click **OK**.
4. Create a policy rule for ISP-IPSEC.
   - Click **Add**.
   - On the **General** tab, enter a name in **Name** field. For example, ISP-IPSEC.
   - On the **Source** tab, select **Interface** as **Type**.
     i. In the **Interface** window, click **Add**.

    ii. Select **ethernet1/1** as in example above.
    iii. In the **Source Address** window, Click **Add**.
    iv. Enter **172.16.100.87** as in example above.
    v. Select **any** for **Source User** window.

- On **Destination/Application/Service** tab
    i. In the **Destination Address** window, click **Add**.
    ii. Enter **172.16.101.100** as in example above.
    iii. Leave default **any** for both Applications and Service
- On **Forwarding** tab
    i. Select **Forward** as the **Action**. This should be the default action.
    ii. Select **tunnel.1** as the **Egress Interface** as shown in example.
    iii. Enter **1.1.1.1** as Next Hop (IP address of peer device alternative interface).

5. Click **OK**.

(4) Configure PBF Rules for ISP2 on HQ-Central Firewall:

1. Login with Administrator Role.
2. Select **Policies > Policy Based Forwarding**. Click **Add**.
    - Enter the rule name in the **Name** field. In example above, ISP2-PBF.
    - On **Source** tab, select **Interface** as **Type**.
        i. In the **Interface** window, click **Add**.
        ii. Select **ethernet1/1** as in example above.
        iii. In the **Source Address** window, Click **Add**.
        iv. Enter **172.16.101.100** as in example above.
        v. Select **any** for **Source User** window.
    - On **Destination/Application/Service** tab
        i. In the **Destination Address** window, click **Add**.
        ii. Enter **172.16.100.87** as in example above.
        iii. Leave default **any** for both Applications and Service
    - On **Forwarding** tab
        i. Select **Forward** as the **Action**. This should be the default action.
        ii. Select **ethernet1/8** as the **Egress Interface** as shown in example.

    iii. Enter **30.1.1.40** as Next Hop (IP address of peer device alternative interface).

3. Click **OK**.
4. Create a policy rule for ISP-IPSEC.
    - Click **Add**.
    - On the **General** tab, enter a name in **Name** field. For example, ISP-IPSEC.
    - On the **Source** tab, select **Interface** as **Type**.
        i. In the **Interface** window, click **Add**.
        ii. Select **ethernet1/1** as in example above.
        iii. In the **Source Address** window, Click **Add**.
        iv. Enter **172.16.101.100** as in example above.
        v. Select **any** for **Source User** window.
    - On **Destination/Application/Service** tab
        i. In the **Destination Address** window, click **Add**.
        ii. Enter **172.16.100.87** as in example above.
        iii. Leave default **any** for both Applications and Service
    - On **Forwarding** tab
        i. Select **Forward** as the **Action**. This should be the default action.
        ii. Select **tunnel.1** as the **Egress Interface** as shown in example.
        iii. Enter **1.1.1.2** as Next Hop (IP address of peer device alternative interface).
5. Click **OK**.

(5) Configure a Security Policy on the Branch Firewall to allow Traffic:

1. Login with Administrator Role.
2. Select **Policies > Security**. Click **Add**.
    - On the **General** tab, enter a name in **Name** field. For example, PBF_rule_Allow.
    - On the **Source Zone** tab, add **ISP2** and **Branch**.
    - On the **Destination Zone** tab, add **ISP2** and **Branch**.
    - On the **Application** tab, select **any** as the **Applications**.
    - On the **Service/URL Category** tab, select **any** as the **Service** and **URL Category**.
    - On the **Action** tab, select **Allow** as the **Action**.
3. Click **OK**.

(6) Configure a Security Policy on the HQ-Central Firewall to allow Traffic:

1. Login with Administrator Role.
2. Select **Policies > Security**. Click **Add**.
   - On the **General** tab, enter a name in **Name** field. For example, PBF_rule_Allow.
   - On the **Source Zone** tab, add **ISP2** and **Central**.
   - On the **Destination Zone** tab, add **ISP2** and **Central**.
   - On the **Application** tab, select **any** as the **Applications**.
   - On the **Service/URL Category** tab, select **any** as the **Service** and **URL Category**.
   - On the **Action** tab, select **Allow** as the **Action**.
3. Click **OK**.

This configuration will cause packets that match the PBFrule security policy to be forwarded to the VPN peer without going through the IPsec tunnel, effectively acting as a BYPASS rule, while packets that match the VPNrule security policy will be forwarded to the VPN peer via the IPsec tunnel, effectively acting as a PROTECT rule.

1. Login with Administrator Role.
2. Select **Policies > Security**. Click **Add**.
   - On the **General** tab, enter a name in **Name** field. For example, PBF_rule_Allow.
   - On the **Source Zone** tab, add **ISP2** and **Branch**.
   - On the **Destination Zone** tab, add **ISP2** and **Branch**.
   - On the **Application** tab, select **any** as the **Applications**.
   - On the **Service/URL Category** tab, select **any** as the **Service** and **URL Category**.
   - On the **Action** tab, select **Allow** as the **Action**.
3. Click **OK**.

To configure a DISCARD rule, create a security policy to deny traffic through the interfaces.

1. Login with Administrator Role.
2. Select **Policies > Security**. Click **Add**.
   - On the **General** tab, enter a name in **Name** field. For example, Deny-All.
   - On the **Source Zone** tab, check **any** checkbox.
   - On the **Destination Zone** tab, check **any** checkbox.

- On the **Application** tab, select **any** as the **Applications**.
- On the **Service/URL Category** tab, select **any** as the **Service** and **URL Category**.
- On the **Action** tab, select **Deny** as the **Action**.

3. Click **OK**.

7.12 Verify and Update System Software

The administrator must verify the TOE version is the evaluated version 11.0.1. The TOE version is verified using the **show system info** command. If the delivered version is not version 11.0.1 please follow the commands:

- **request system software check**
- **request system software download version 11.0.1**
- **request system software install version 11.0.1**

The TOE supports system software download and update process (**Device > Software**). For direct download, the TOE must be connected to the Internet. If the TOE is not connected to the Internet, the software updates must be acquired through a different means and uploaded to the TOE. All software updates are digitally signed by Palo Alto Networks. The TOE will verify all digital signature prior to installation. If the verification fails, the TOE will not install the system updates. Please confirm the system updates are authentic by downloading the images from updates.paloaltonetworks.com only.

1. Login with Administrator Role.
2. View the TOE software version.
    - UI: **Dashboard > General Information**
    - CLI: **show system info | match sw-version**
    - API: See below
3. Select **Device > Setup > Services**. Click on the ⚙ gear setting.
4. Make sure the TOE is connected to the correct updates.paloaltonetworks.com (Internet connection required!).
5. Select **Device > Software**.
6. Click **Check Now**.
7. If the TOE is connected to the updates.paloaltonetworks.com, find the version you want to download and click **Download** under the Action column.
8. If the TOE is not connected to the Internet, click **Upload** to upload the system update. You must first download it from https://support.paloaltonetworks.com/. Browse to the directory where the downloaded system image is stored on the local computer. Select the system image you want to upload and upload it to the TOE.
9. Click **Install** to install the system update under the Action column.

> **WARNING:** You MUST reboot the system! The installation cannot complete until the system is rebooted.

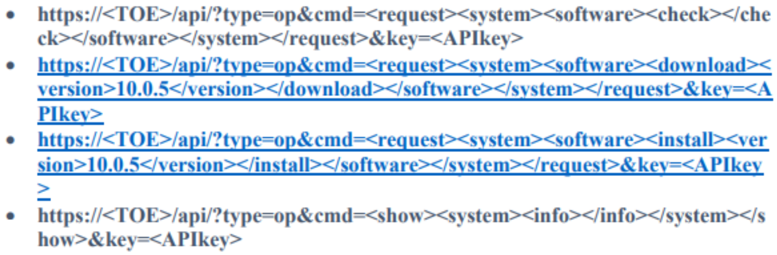
10. Login with Administrator Role.

11. Verify the updated TOE software version.

- UI: **Dashboard > General Information**
- CLI: **show system info | match sw-version**

CLI HINT: The equivalent CLI commands are **request system software check**, **request system software download version <Version Number>** and **request system software install version <Version Number>**.

API HINT: The equivalent XML API calls are (replace version as needed)



- **https://<TOE>/api/?type=op&cmd=<request><system><software><check></check></software></system></request>&key=<APIkey>**
- **https://<TOE>/api/?type=op&cmd=<request><system><software><download><version>10.0.5</version></download></software></system></request>&key=<APIkey>**
- **https://<TOE>/api/?type=op&cmd=<request><system><software><install><version>10.0.5</version></install></software></system></request>&key=<APIkey>**
- **https://<TOE>/api/?type=op&cmd=<show><system><info></info></system></show>&key=<APIkey>**

7.13 XML and REST API

The Application Programming Interface (API) allows administrators to manage the TOE through a third-party service, application, or script. The TOE supports two types of API: REST API and XML API.

- The XML API uses a tree of XML nodes to map TOE functionality. To make an API request, you must specify the XPath (XML Path Language) to the XML node that corresponds to a specific setting or action. XPath allows you to navigate through the hierarchical XML tree structure for the TOE.
- The administrator can use the REST API to Create, Update, Rename, Delete (CRUD) Objects and Policies on the TOE; the administrator can access the REST API directly on the TOE to perform these operation on policies and objects from a central location and push them to the managed TOEs.

Use your administrative username and password to generate an API key to authenticate API calls. Granular roles allow you to grant API access to specific functionality including reports, logs, and operational mode commands.

7.13.1 Structure of XML API Request

A PAN-OS XML API request typically comprises a number of parameters, as shown in the example below:

```
https://<TOE>/api/?type=<type>&action=<action>&xpath=<xpath>&key=<APIkey>
```

- API key (key=): The API key allows you to authenticate yourself to the API when making requests.
- Request type (type=): Because the XML API allows you to perform a wide array of requests, you must first specify the type of request you want, ranging from configuration to operation, importing to exporting, and from reports to user ID.
- Action (action=): When the request type is config (configuration) or op (operational mode command), you must also specify an associated action, such as edit, delete, or move.
- XML and XPath elements (xpath= or cmd=): When using configuration or operational mode commands on the TOE, you include only the XML or the XPath that specifies the XML node.

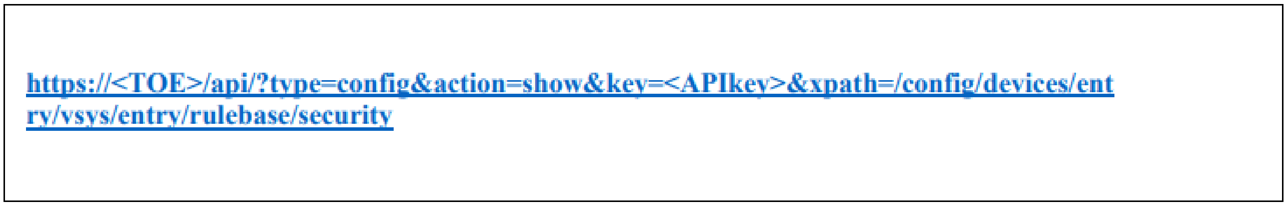
To make requests to the PAN-OS XML API, you can use the GET and POST methods.

7.13.2 API Authentication and Security

To use the API (XML or REST), you must enable API access for your administrators and get your API key. By default, the TOE supports API requests over HTTPS. To enforce key rotation set an API key lifetime; the administrator can also revoke all API keys to protect from accidental exposure.

7.13.3 API XML and XPath

The XML API uses XML for both requests and responses. When making requests, construct an HTTPS GET or POST request with the correct type and action along with the correct XPath. Here is an example API request:



https://<TOE>/api/?type=config&action=show&key=<APIkey>&xpath=/config/devices/entry/vsys/entry/rulebase/security

Replace variables such as <TOE> and <APIkey> with the IP address or hostname of the TOE and API key, respectively.

When making configuration requests (**type=config**), the administrator can use XPath, a syntax for selecting nodes from within an XML document. Use the XPath to isolate and modify portions of your configuration. The XML configuration within PAN-OS uses four different types of nodes as shown here:

```
<users>
        <entry name="admin">
                <permissions>
                        <role-based>
                                <superuser>yes</superuser>
                        </role-based>
                </permissions>
        </entry>
        <entry name="guest">
                <permissions>
                        <role-based>
                                <custom>
                                        <profile>NewUser</profile>
                                </custom>
                        </role-based>
                </permissions>
        </entry>
</users>
```

- Root nodes are top-level nodes with no parent. Requesting the root node returns all child elements.
- Element nodes represent containers of information. Element nodes can contain other element nodes or simply act as a container of information. Example: **<permissions></permissions>**
- Attribute nodes are nodes that contain name/value pairs. Example: **<entry name="admin"></entry>**
- Text nodes contain plain text. Example: **<superuser>yes</superuser>**

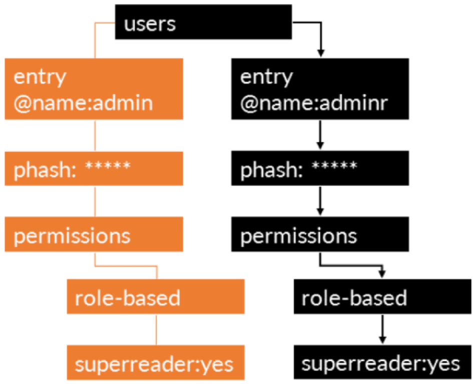
7.13.4 XPath Node Selection

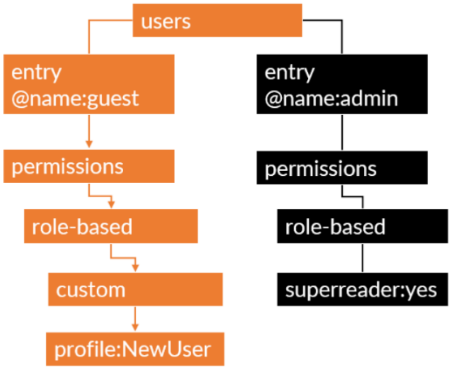
There are various ways to specify the XPath for an XML node in an API request. The simplest is to use the location path of the resource. For example, to select all users within your management configuration, use the following path:

/config/mgt-config/users

Another method for selecting the XPath for an XML node is to select the specific node, such as the **superuser** or **NewUser** node within the node shown above. Use XPath syntax similar to the following to drill-down and select a specific node:

XML Node	XPath Syntax

 users
entry
@name:admin
entry
@name:adminr
phash: *****
phash: *****
permissions
permissions
role-based
role-based
superreader:yes
superreader:yes
	`/config/mgt-config/users/`
	`entry/permissions/role-based/`
	`superuser[text()='yes']`

 users
entry
@name:guest
entry
@name:admin
permissions
permissions
role-based
role-based
custom
superreader:yes
profile:NewUser
	`/config/mgt-config/users/entry/`
	`permissions/role-based/custom/`
	`profile[text()='NewUser']`

7.13.5 Enable API Access

The API supports the following types of Administrators and Admin roles:

- Dynamic roles: Superuser, Superuser (readonly), Device admin, Device admin (readonly), Vsys admin, Vsys admin (readonly)
- Role-based Admins: Device, Vsys.

Admin Role profiles enable or disable features on the management interfaces of the TOE, XML API, web interface, and CLI.

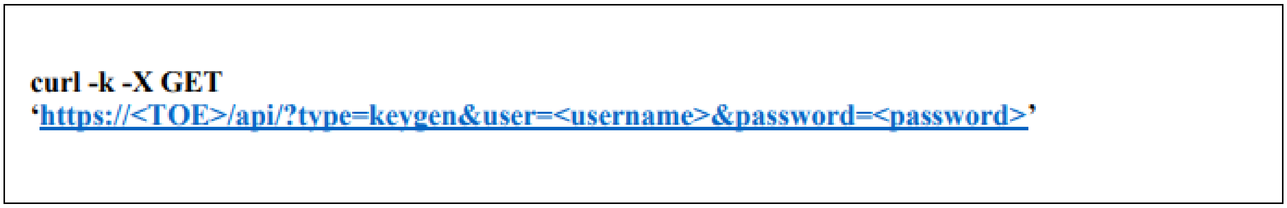
NOTE: As a best practice, set up a separate admin account for XML API access.

1. Login with Administrator Role.
2. Go to **Device > Admin Roles** and select or create an admin role.
3. Select features available to the admin role.
4. Select the **XML API** tab.
5. Enable or disable XML API features from the list, such as **Report**, **Log**, and **Configuration**.
6. Select **OK** to confirm your change.
7. Assign the admin role to an administrator account.

7.13.6 Get Your API Key

To use the API, you must generate the API key required for authenticating API calls.

Then, when you use this API key in your request, you can either provide the URL encoded API key in the request URL or use the custom *X-PAN-KEY: <key>* parameter to add the key as a name-value pair in the HTTP header.



```
curl -k -X GET
‘https://<TOE>/api/?type=keygen&user=<username>&password=<password>’
```

A successful API call returns status="success" along with the API key within the key element:

```
<response status="success">

<result>

<key>gJlQWE56987nBxIqyfa62sZeRtYuIo2BgzEA9UOnlZBhU</key>

</result>

</response>
```

A failure API call is shown below.

```
<response status = 'error' code = '403'><result><msg>Invalid Credential</msg></result></response>
```

You can revoke all currently valid API keys, in the event one or more keys are compromised. To change an API key associated with an administrator account, change the password associated with the administrator account. API keys that were generated before you expired all keys, or a key that was created using the previous credentials will no longer be valid.

Example 1 of using the API key, make a cURL call to get system information, which returns the IP address, hostname, and model of the TOE.

```
curl -k
'https://<TOE>/api/?type=op&cmd=<show><system><info></info></system></show>&key=<APIkey>'
```

Example 2 of using the API key, make a cURL call to make a commit.

```
curl -k 'https://<TOE>/api/?type=commit&cmd=<commit></commit>&key=<APIkey>'
```

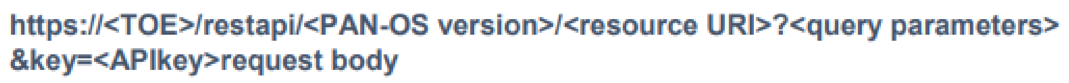
NOTE: When you make your API calls, as an alternative to providing the URL encoded API key in the request URL, you can use the custom X-PAN-KEY: <key> parameter to add the key as a name value pair in the HTTP header. For example, **curl -H "XPAN-KEY:**

LU234T02234565s2Z1FtZWFyWXJOSTdk1234565234565=" -k 'https://<TOE>/api/?type=op&cmd=<show><system><info></info></system></show>'

NOTE: Curl requires a backward slash to encode some special character such as a square bracket. For example, **curl -k -X GET 'https://10.8.48.106/api/?type=config&action=set&xpath=/config/devices/entry\[@name='localhost.localdomain'\]/deviceconfig/system/ssh/ciphers/mgmt&element=<aes256-cbc></aes256-cbc>&key=... '**

7.13.7 Structure of REST API Request

The PAN-OS REST API URL format includes a base path and the URI for the endpoint.



https://<TOE>/restapi/<PAN-OS version>/<resource URI>?<query parameters>
&key=<APIkey>request body

The base path includes the FQDN or IP address of the TOE and the version. The resource URI is the path for the resource or endpoint you want to work with, and it corresponds with the resources you can access on the web interface.

- Base path and the resource URI for the endpoint.
- Query parameters. Every request includes query parameters that are passed to the API endpoint using query strings. The query parameters are appended to the URL with a ? that indicates the start of the query string. The query parameters appear after the ?, the parameter are concatenated with other parameters using the ampersand & symbol.

For example, use REST API to create security policy (firewall) rule

```
curl -X POST \
'https://10.1.1.4/restapi/11.0.1/Policies/SecurityRules?
location=vsys&vsys=vsys1&name=rule-example1' \
-H 'X-PAN-KEY: LUFRPT=' \
-d '{
    "entry": [
        {
            "@name": "rule-example1",
            "@location": "vsys",
            "@vsys": "vsys1",
            "to": {
                "member": [
                "any"
                ]
            },
            "from": {
```

```
"member": [
    "zone-edge1"
    ]
},
"source-user": {
    "member": [
        "any"
    ]
},
"application": {
    "member": [
        "email-collaboration-apps"
    ]
},
"service": {
    "member": [
        "application-default"
    ]
},
"hip-profiles": {
    "member": [
        "any"
    ]
},
"action": "allow",
    "category": {
        "member": [
            "any"
        ]
},
                "source": {
                        "member": [
                                "any"
                        ]
                },
                "destination": {
                        "member": [
                                "any"
                        ]
                }
        }
      ]
}’
```

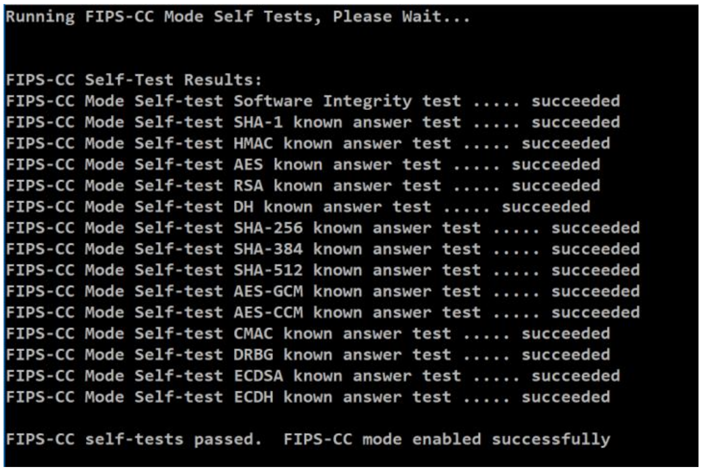
7.14 Self-Tests

The TOE performs a suite of FIPS self-tests during power-up and on demand (via reboot). If any of the self-test fails, the TOE will enter maintenance mode (i.e., no longer in the evaluated configuration). The TOE enters an error state and outputs an error indicator. The TOE doesn't perform any cryptographic operations while in the error state. All data output from the TOE is inhibited when an error state exists. If this occurs, please re-boot the appliance. If the self-tests continue to fail, please contact Palo Alto Networks Support (e-mail support@paloaltonetworks.com or call them at 866-898-9087).

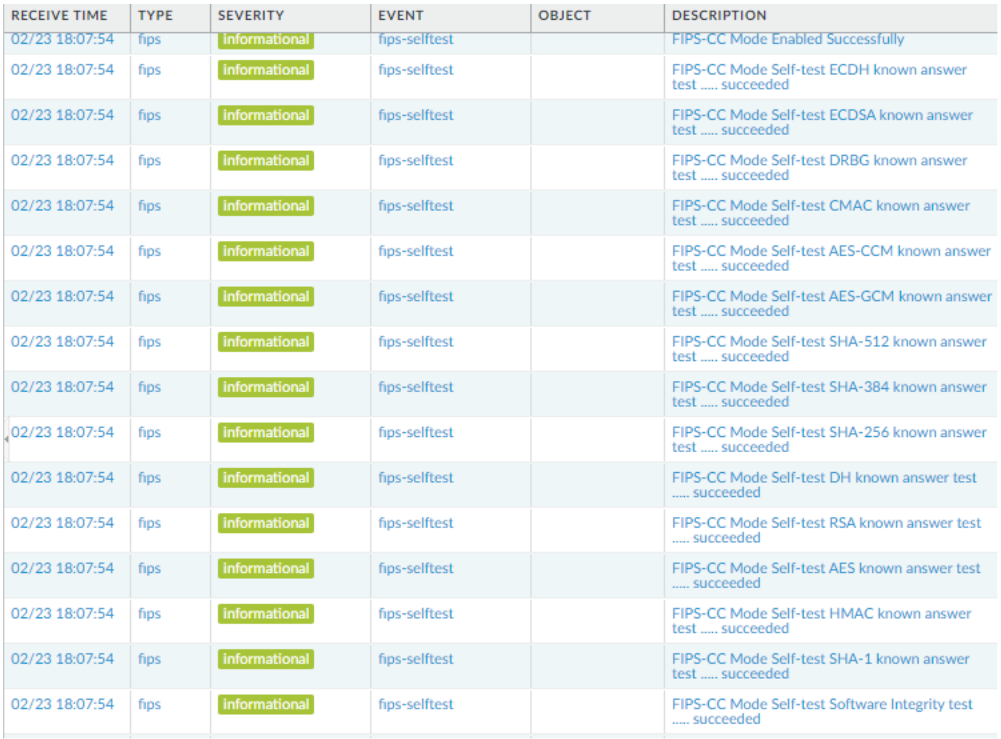
The following possible failures can be detected during the self-test are:

- Firmware Integrity failure [power-up | schedule]
- Known Answer Test (KAT) failures [power-up | schedule]
- Entropy Health Test [power-up | schedule]

The actual output of the FIPS power-up self-tests can only be viewed in the system logs.



```
Running FIPS-CC Mode Self Tests, Please Wait...


FIPS-CC Self-Test Results:
FIPS-CC Mode Self-test Software Integrity test ..... succeeded
FIPS-CC Mode Self-test SHA-1 known answer test ..... succeeded
FIPS-CC Mode Self-test HMAC known answer test ..... succeeded
FIPS-CC Mode Self-test AES known answer test ..... succeeded
FIPS-CC Mode Self-test RSA known answer test ..... succeeded
FIPS-CC Mode Self-test DH known answer test ..... succeeded
FIPS-CC Mode Self-test SHA-256 known answer test ..... succeeded
FIPS-CC Mode Self-test SHA-384 known answer test ..... succeeded
FIPS-CC Mode Self-test SHA-512 known answer test ..... succeeded
FIPS-CC Mode Self-test AES-GCM known answer test ..... succeeded
FIPS-CC Mode Self-test AES-CCM known answer test ..... succeeded
FIPS-CC Mode Self-test CMAC known answer test ..... succeeded
FIPS-CC Mode Self-test DRBG known answer test ..... succeeded
FIPS-CC Mode Self-test ECDSA known answer test ..... succeeded
FIPS-CC Mode Self-test ECDH known answer test ..... succeeded

FIPS-CC self-tests passed.  FIPS-CC mode enabled successfully
```



RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Enabled Successfully
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test ECDH known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test ECDSA known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test DRBG known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test CMAC known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test AES-CCM known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test AES-GCM known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test SHA-512 known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test SHA-384 known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test SHA-256 known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test DH known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test RSA known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test AES known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test HMAC known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test SHA-1 known answer test ..... succeeded
02/23 18:07:54	fips	informational	fips-selftest		FIPS-CC Mode Self-test Software Integrity test ..... succeeded

The FIPS power-up self-tests that are executed are provided below:

- AES Encrypt Known Answer Test
- AES Decrypt Known Answer Test
- AES GCM Encrypt Known Answer Test
- AES GCM Decrypt Known Answer Test
- AES CCM Encrypt Known Answer Test
- AES CCM Decrypt Known Answer Test
- RSA Sign Known Answer Test
- RSA Verify Known Answer Test
- RSA Encrypt/Decrypt Known Answer Test
- ECDSA Sign Known Answer Test
- ECDSA Verify Known Answer Test
- HMAC-SHA-1 Known Answer Test
- HMAC-SHA-256 Known Answer Test
- HMAC-SHA-384 Known Answer Test
- HMAC-SHA-512 Known Answer Test
- SHA-1 Known Answer Test
- SHA-256 Known Answer Test
- SHA-384 Known Answer Test
- SHA-512 Known Answer Test
- DRBG SP800-90A Known Answer Tests
- SP 800-90A Section 11.3 Health Tests
- DH Known Answer Test
- ECDH Known Answer Test
- SP 800-135 KDF Known Answer Tests

- Firmware Integrity Test – verified with HMAC-SHA-256 and ECDSA P-256. If the calculated result does not equal the previously generated result, the software/firmware test shall fail.