Palo Alto Networks

Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 10.2

Revision Date: February 6, 2023

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

1 Introduction

Palo Alto Networks Panorama management appliances provide centralized monitoring and management of Palo Alto Networks next-generation firewalls and WildFire appliances[1]. It provides a single location from which administrators can oversee all applications, users, and content traversing the whole network, and then use this knowledge to create application enablement policies that control and protect the network. Using Panorama for centralized policy and firewall management increases operational efficiency in managing and maintaining a network of firewalls.

This guidance only covers the Panorama physical and virtual appliance models. Palo Alto Networks next-generation firewalls and WildFire appliances were evaluated separately, and the documentation is provided in separate documents. Any information about them provided here is only for completeness.

The Palo Alto next-generation firewalls 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 WildFire appliance provides an on-premises WildFire private cloud, enabling the analysis of suspicious files in a sandbox environment without requiring the firewall to send files out of network. The WildFire appliance can be configured to host a WildFire private cloud where the firewall is configured to submit samples to the local WildFire appliance for analysis. The WildFire appliance sandboxes all files locally and analyzes them for malicious behaviors using the same engine the WildFire public cloud uses.

This document is a supplement to the Panorama Administrator's Guide, which is comprised 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 and meets all the required guidance assurance activities from the NDcPP.

[1] The firewalls and WildFire appliances are evaluated separately but are in the operational environment.

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 polices 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 Panorama (i.e., the TOE) for centralized management, logging, and reporting, you are required to register, activate, and retrieve the Panorama device management and support licenses. Every instance of Panorama requires valid licenses that entitle you to manage firewalls and obtain support. The firewall device management license enforces the maximum number of firewalls that Panorama can manage. This license is based on firewall serial numbers, not on the number of virtual systems on each firewall. The support license enables Panorama 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. The features below 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.
API request over HTTP	By default, the TOE supports API requests over HTTPS only. API requests over HTTP are disabled and cannot be enabled in the evaluated configuration.
Stateful inspection filtering, VPN gateway, IPS/IDS threat prevention, URL filtering (PAN-DB), Log forwarding, and Malware sandboxing	These features are provided by Palo Alto Networks firewalls and WildFire appliances and are not included in this evaluation. Only the secure TLS connections between the firewalls and WildFire to the TOE were evaluated.
Centralized Device Management	These features (e.g., Policy Template and Push, Device Group) were not evaluated. Only the secure TLS connections between the firewalls and WildFire to the TOE were evaluated.
OCSP Revocation Checking	In the evaluated configuration, CRLs are used for revocation checking.
Any features not associated with SFRs in claimed NDcPP	NDcPP forbids adding additional requirements to the Security Target (ST). If additional functionalities are mentioned in the ST, it is for completeness only.

Table 1: Scope of Evaluation

1.2 TOE References

Model	Description	Version
Physical	Palo Alto Networks Panorama M-200, M-300, M-600, and M-700 models	10.2.3-h2
Virtual	The Panorama 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 20.14: • Dell PowerEdge R740 Processor: Intel Xeon Gold 6248 (Cascade Lake microarchitecture) with Broadcom 57416 NIC • Memory: 128 GB RDIMM	10.2.3-h2

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 20.14.

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:

- Panorama Administrator's Guide Version 10.2, Last Revised: See Link Below

  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/panorama/10-2/panorama-admin/panorama-admin.pdf

- PAN-OS® and Panorama 10.2 API Guide, Last Revised: See Link Below

  https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-panorama-api/get-started-with-the-pan-os-rest-api/access-the-rest-api.html

- VM-Series 10.2 Deployment Guide, Last Revised: See Link Below

  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/vm-series/10-2/vm-series-deployment/vm-series-deployment.pdf

- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 10.2 [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,
- Palo Alto Networks firewalls and WildFire appliances
- Workstation
    - Web browsers - Chrome (version 94 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 92 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.VM_CONFIGURATION	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.	Administrators must configure VS and VMs to reduce the attack surface and enable protection features where applicable. Any unnecessary hardware, communication, or operation should be disabled and/or not used.

3 Before Installation You Must

Before you install your physical or virtual 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. Virtualization System (VS) hardware must be protected as well.
- [VM only] Ensure the system requirements (e.g., CPU cores, memory, disk capabilities, etc.) specified per VS are met.
- 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, or virtually separated via different virtual switches.
- 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.
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 management.
28270	TLS	TCP	Bidirectional	Logger Mode Only: Allows communication between log collectors in optional cluster deployment.

Table 4: Ports and Protocols

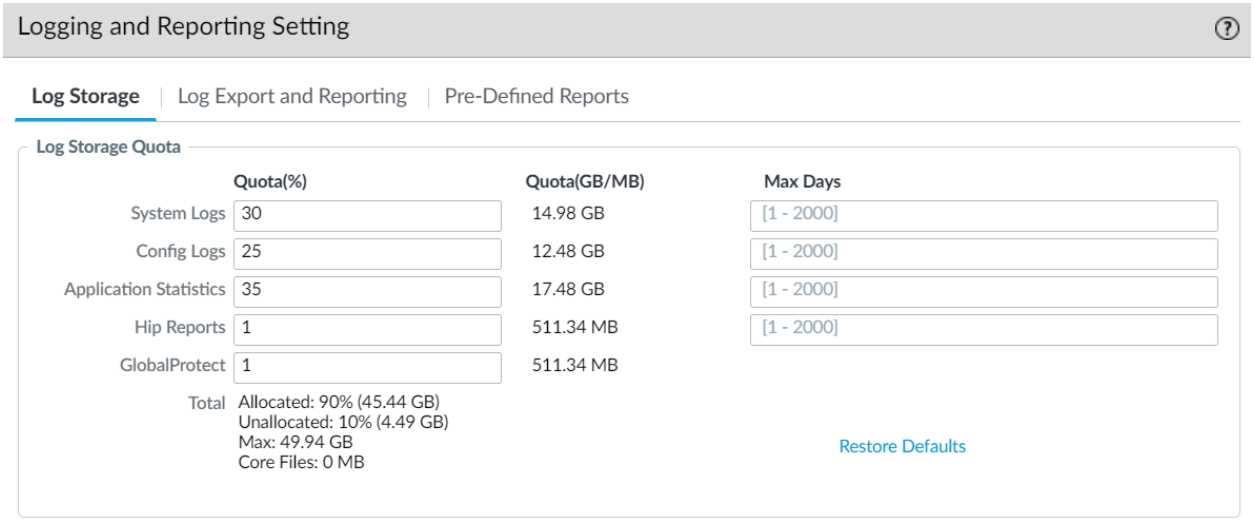
4 Required Auditable Events

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 consists of several logs, which are locally stored in the file system on the hard disk. The two 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.

The TOE generates an audit event for each user interaction with the web interface, API, and CLI command executed. 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 **Panorama > Setup > Logging and Reporting Settings >** click on "Gear" icon to edit **> Log Storage Tab**, and enter a percentage % per configuration or system logs). When the audit log is full, the oldest audit records are overwritten by the newest audit records.



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

SFR	Required Audit Event [Required Content]	Actual Audit Event - '*Description*' Only	Type
FAU_GEN.1	Start-up and shut-down of audit functions[2]	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 panorama certificate panorama* *{* *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 panorama certificate import <Name>* *Import <Name>* *{* *private-key ********;* *}* *Admin | delete | config panorama certificate panorama* *{* *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

[2] 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_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 while writing stream; tls_error='SSL routines: SSL3_WRITE_BYTES:sslhandshake failure'* *Syslog SSL error while 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.	**Failure** *Client authentication failed FIPS/CC cert validation failed Client IP: <Client IP address>:<Client Port> Server IP: <Server IP Address>:3978 Client cert CN: /CN=<Peer Device Name>* *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).]	<u>On UI (HTTPS):</u> *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>.* <u>On CLI (SSH):</u> *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).]	<u>On UI (HTTPS):</u> Password *User <Username> logged in via Web from <IP Address> using https* *failed authentication for user '<Username>'. Reason: Invalid username/password. From <IP Address>* Public-Key *Certificate validated for user '<Username>'. From: <Source IP>.*[3] *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>* <u>on CLI (SSH):</u> 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> - <Reason>* *<Reason> can be any of the following example: OCSP/CRL validation of the X.509v3 certificate failed or not configured.* *Client cert expired or revoked for peer <IP Address>* *Certificate unknown for peer <IP Address>*	System

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

	Identification of certificates added, replaced or removed as trust anchor[4] in the TOE's trust store	*Admin | request/upload | config panorama certificate panorama* *{* *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 panorama certificate import <Name>* *Import <Name>* *{* *private-key ********;* *}* *Admin | delete | config panorama certificate panorama* *{* *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

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

FMT_SMF.1	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 panorama log-settings syslog <Name> transport SSL* • 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 *deviceconfig setting management idle-timeout <Value>* • Configure the login banner *deviceconfig system login-banner <Banner>* • Configure X.509 certificate profiles. *config panorama certificate-profile <Unique Name>*	Config

		• Ability to manage the trusted public keys database. config mgt-config users <user>, , <user> {public key <public key mapping to user to be stored in database>} config mgt-config users <user>, , <user> {public key <public key mapping to user to be deleted in database>} • Manage the TOE trust store and designate X509v3 certificates as trust anchor *Admin | request/upload | config panorama certificate panorama* *{* *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 panorama certificate import <Name>* *Import <Name>* *{* *private-key ********;* *}* *Admin | delete | config panorama certificate panorama* *{* *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*	
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 TLS (device connection) **Initiation** *<Device Serial Number> connected* **Termination** *tls-session-disconnected: Device <Device Serial Number> disconnected from the server* **Failure** *Client authentication failed FIPS/CC cert validation failed Client IP: <Client IP address>:<Client Port> Server IP: <Server IP Address>:3978 Client cert CN: /CN=<Peer Device Name>* *SSL handshake failed - (NONE)*	System

FTP_TRP.1/ Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	<u>on UI (HTTPS)</u> **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)* <u>on CLI (SSH)</u> **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

Table 7: 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 user can use to perform administrative, management, and analysis tasks. User 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 92 or later)	JavaScript, cookies, Transport Layer Security (TLS) v1.2

Table 8: Web Browser Settings

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), or remotely over HTTPS. Note the TOE in Logger mode does not support GUI or API. The CLI is accessible via direct connection to the management port (physical or virtual) on the device (local access), 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 6.9.2.

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.

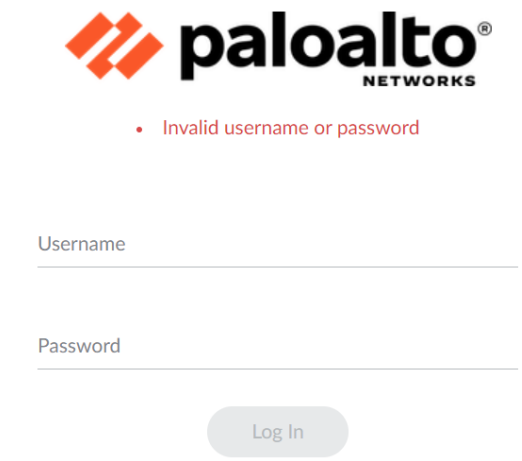
   The TOE login page appears.

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

3. Click **Log In**.

   The default start page appears if the authentication is successful.

   If authentication fails, the following error message is displayed:



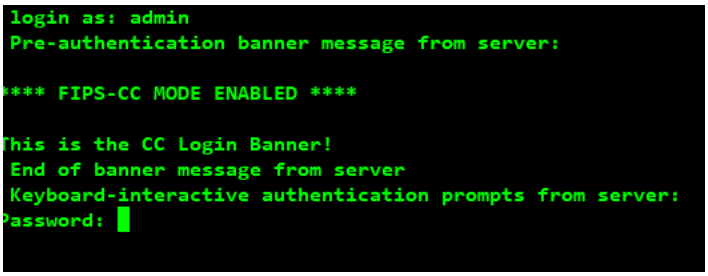
5.1.2 User Login to CLI Remotely

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.



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

   The command prompt appears if the authentication is successful.

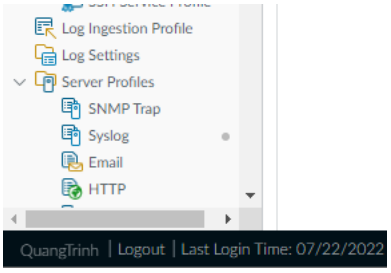
   If authentication fails, the following error message is displayed:

5.1.3 User Login to CLI Locally

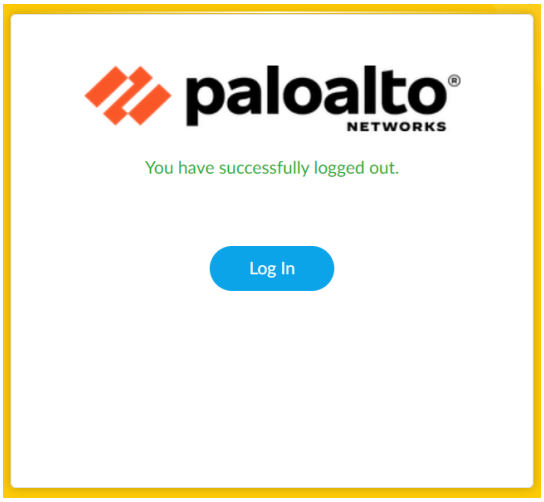
1. All localized TOE management will be done through the GUI/CLI/API via the direct RJ-45 Ethernet cable to the MGMT port (physical or virtual) using HTTPS or SSHv2. Use the IP Restriction feature (see section 6.1 for IP restrictions) to secure the appliance management access. Shell and local console access will be disabled in FIPS-CC mode.

5.1.4 User Logout

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



2. The following message is displayed to the logged-out user. Close the web browser.



3. For CLI session, enter the **exit** command.
4. The session will close.

> **API HINT:** The equivalent API call is
>
> - 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 7.11 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.

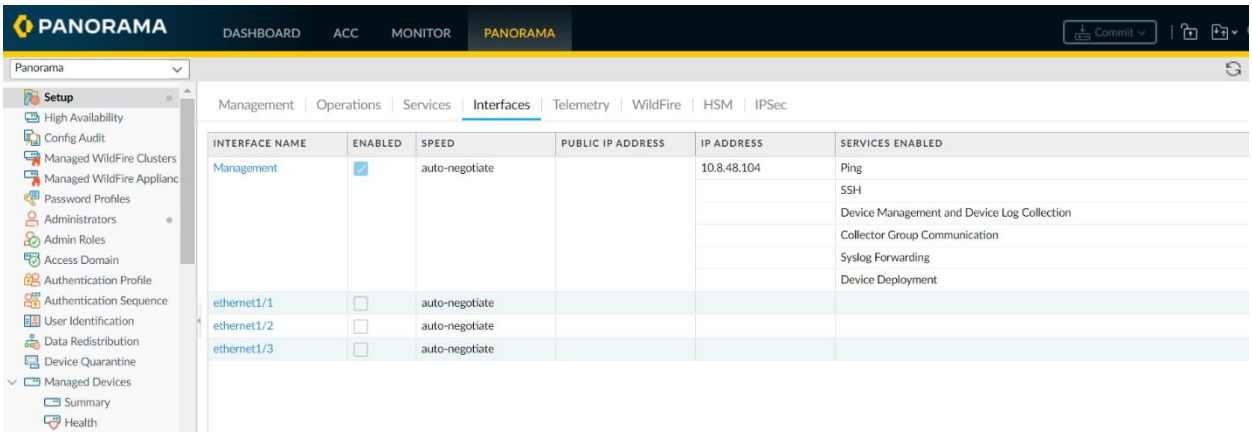
The TOE by default only supports SSH and HTTPS security protocols for management. Telnet and HTTP are not enabled for management and **must** not be enabled. The TOE is required to support only the cipher suites, version, and protocols claimed in the Security Target. HTTPS, SSH and TLS connection settings (TLS ciphersuites, SSH key exchange algorithms, key sizes, etc.) are configured 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 must 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.

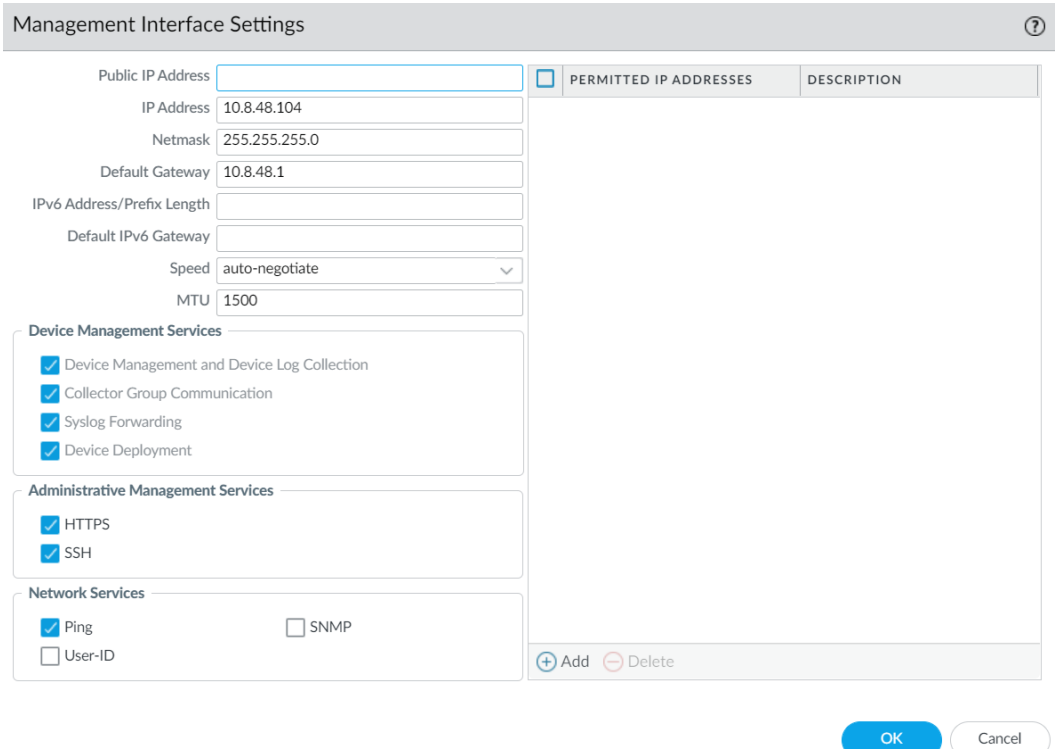
1. Login with Administrator Role.
2. Select **Panorama > Setup > Interfaces**.

   The Interfaces Tab page appears.

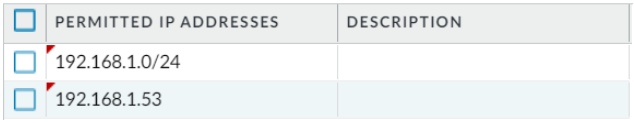


3. Click on the **Management** interface under the Interface Name column. The management interface is enabled by default.

   The Management Interface Settings page appears.



4. In the Permitted IP Address field, click **Add**.
    - Specify a single IPv4 or IPv6 address.
    - Specify a subnet.
    - Optionally, enter a description.

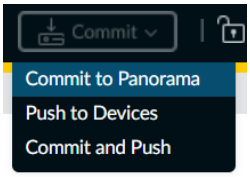


NOTE: In FIPS-CC mode, the management security protocols are restricted in HTTPS and SSH. The administrator cannot enable HTTP or telnet in FIPS-CC mode.

5. To delete an entry, select that row and click **Delete**.

Note: An empty list (default) specifies that access is available from any IP address.

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 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/IPv6 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 but the administrator may choose to restrict the MAC algorithms further.

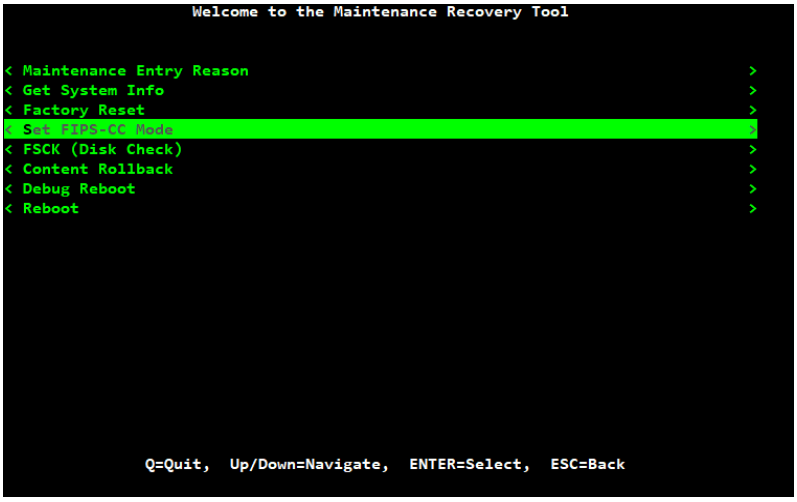
To enable FIPS-CC mode, first boot the TOE into the maintenance mode. From there, change the operational mode from normal mode to FIPS-CC mode.

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.

NOTE When the TOE is in maintenance mode, it is no longer in the evaluated configuration.

4. It will take approximately 2 to 3 minutes for the TOE to boot up into maintenance mode. During this time, the SSH and HTTPS management session will be disabled.

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.
7. Select **Enable FIPS-CC Mode** and press the Enter key.



8. When prompted, select **Reboot**.
9. After the TOE passed all the FIPS power-up self-tests and switch 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: Master key stored in an external HSM (part of operational environment) will not be zeroized. The HSM operator must zeroize the HSM directly.

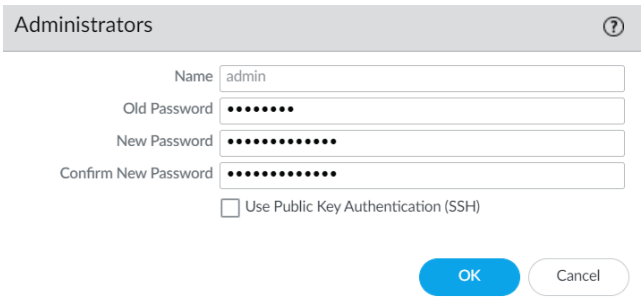
WARNING: Shell and local console access will be disabled. All further TOE management will be through the GUI/CLI locally via direct RJ-45 Ethernet cable and remotely using HTTPS/TLS or SSHv2 client.

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, this access will be disabled unless you are in maintenance mode.

6.3 Change Default Admin Password (Required)

NOTE: The default 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 administrator users.

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



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

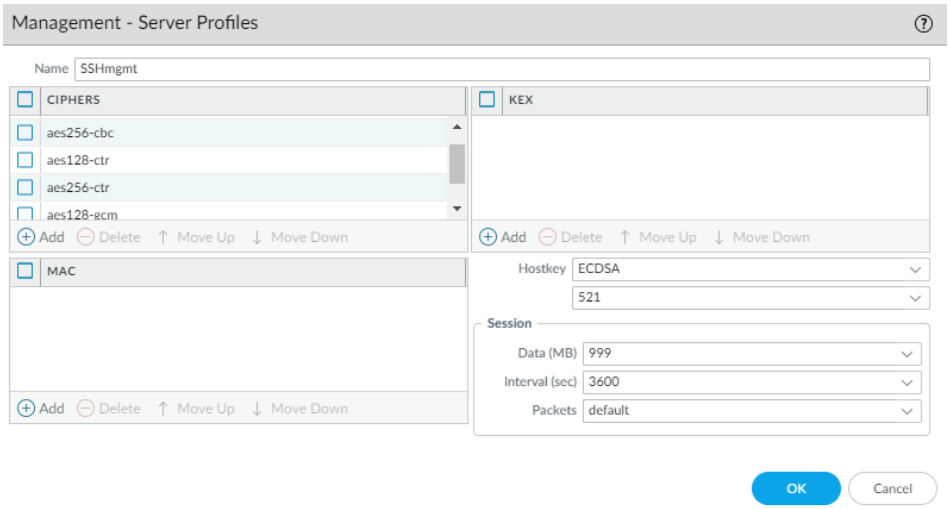
CLI HINT: The equivalent CLI command is **set password**.

6.4 Configure SSH Encryption Algorithms (Required)

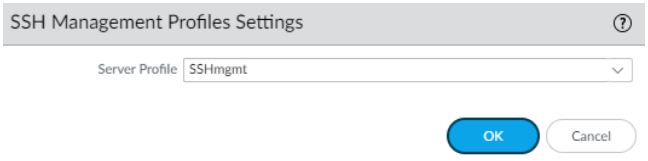
In FIPS-CC mode, the TOE supports all AES key sizes including 192 for CBC and CTR. The NDcPP does not allow this 192 bits key size for SSH. Use the following steps to configure 128 and 256 bits only:

Web UI

1. Login with Administrator Role.
2. Select **Panorama > 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.



5. Click **OK**.
6. Select **Panorama > 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**.



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.

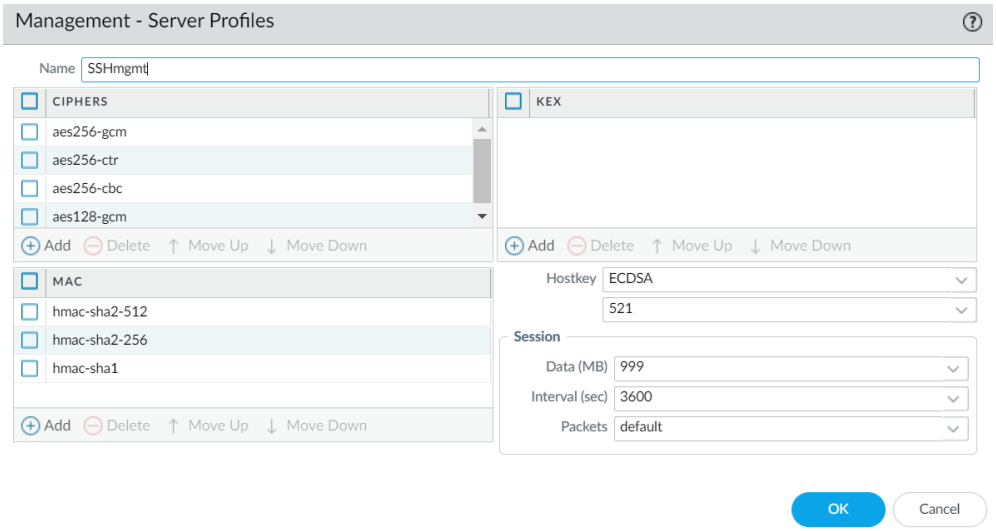
2. Enter configuration mode using **configure** command.
3. Enter the following commands:
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes128-cbc**
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes128-ctr**
    - **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 MAC Algorithms (Optional)

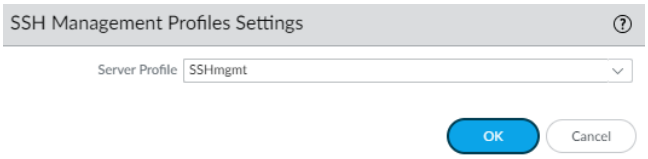
In FIPS-CC mode, the TOE is restricted to support the three HMAC algorithms below and only those algorithms. The administrators may further restrict the setting (for example, use only HMAC-SHA2-512).

Web UI

11. Login with Administrator Role.
12. Select **Panorama > Certificate Management > SSH Service Profile > Management – Server Profiles > Add**.
13. Enter a **Name**.
14. Under **MAC**, add HMAC algorithms with hash sizes of 160, 256, and/or 512 bits.



15. Click **OK**.
16. Select **Panorama > Management > SSH Management Profiles Settings**. Click on the edit gear icon.
17. Under the **Server Profile** drop-down list, select the SSH Server Profile you created above. Click **OK**.



18. **Commit** to save the changes.
19. On the CLI, enter **run set ssh service-restart mgmt** to restart the SSH server.
20. Type **y** to confirm.

CLI

8. Using SSH, login with Administrator Role.

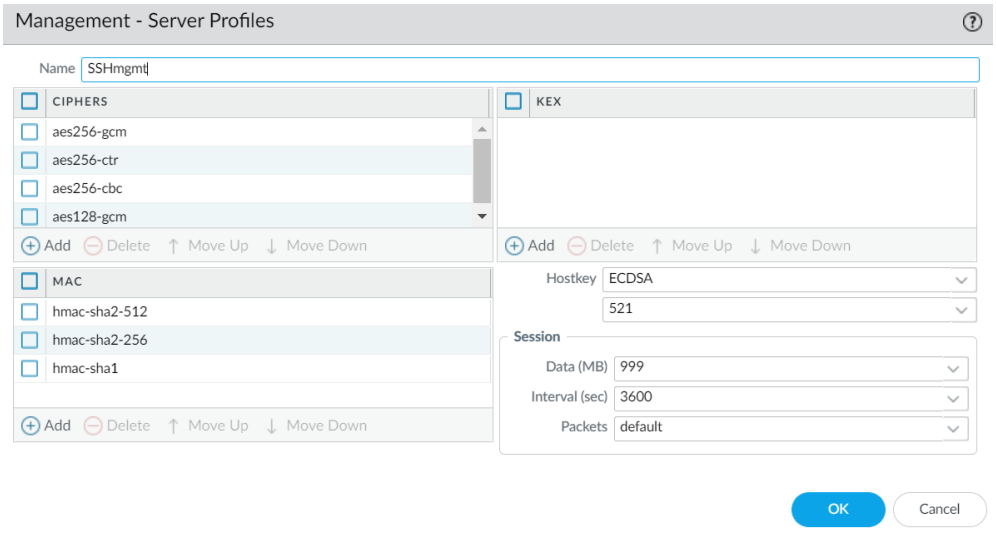
9. Enter configuration mode using **configure** command.
10. Enter the following commands:
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> mac hmac-sha2-512**
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> mac hmac-sha2-256**
    - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> mac hmac-sha1**
11. Enter **set deviceconfig system ssh mgmt server-profiles <Profile_Name>** to apply the profile to the management interface.
12. Enter **commit** to save the changes.
13. Enter **run set ssh service-restart mgmt** to restart the SSH server.
14. Type **y** to confirm.

6.6 Configure SSH Rekey Interval (Required)

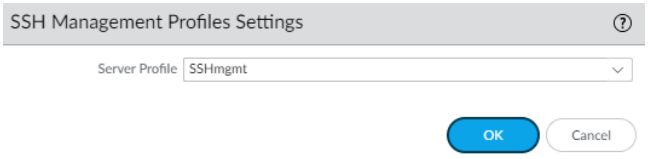
When FIPS-CC mode is enabled, the SSH rekeying will occur approximately at 1 hour of time or after 1 GB of data has been transmitted, whichever occurs first. To change the SSH rekeying interval, please follow the instructions below.

Web UI

1. Login with Administrator Role.
2. Select **Panorama > 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.



5. Click **OK**.
6. Select **Panorama > 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**.



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.

6.7 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.

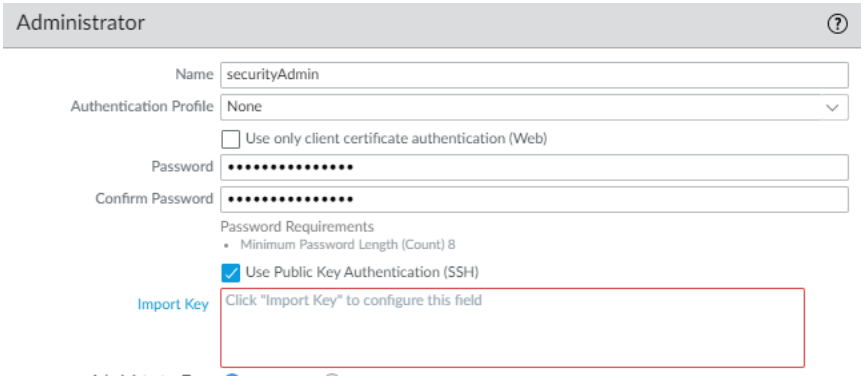
3. Enter **ssh-keygen -t rsa -b 3072**
4. Enter an optional passphrase, if desired.

WARNING: ECDSA keypair is not supported at the moment.

On the TOE UI:

1. Login with Administrator Role.
2. Select **Panorama > 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



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 (**Commit to Panorama**).

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.

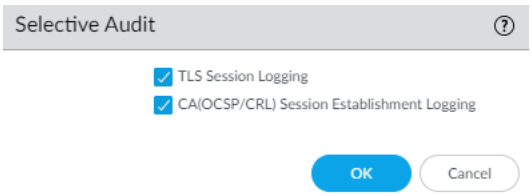
NOTE: The passphrase is different from the password. The passphrase, if set above, is used to protect the SSH private key and will be prompted each time the private key is accessed.

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>**

6.8 Configure Auditing Settings (Required)

On the TOE UI:

1. Login with Administrator Role.
2. Select **Panorama > Log Settings**.
3. Scroll down to the Selective Audit section.
4. Click on the gear setting.
5. Check both **TLS Session Logging** and **CA(OCSP/CRL) Session Establishment Logging** checkboxes.



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 (**Commit to Panorama**).

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

API HINT: The equivalent 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-tls-session-logging>&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>

NOTE: The TLS connection from Panorama to the Palo Alto Networks Firewalls must have CRL configured if the **CA(OCSP/CRL) Session Establishment Logging** checkbox is checked. Otherwise, the TLS connection will fail.

6.9 Secure Connection Settings

6.9.1 Syslog Server Connection Settings (Required)

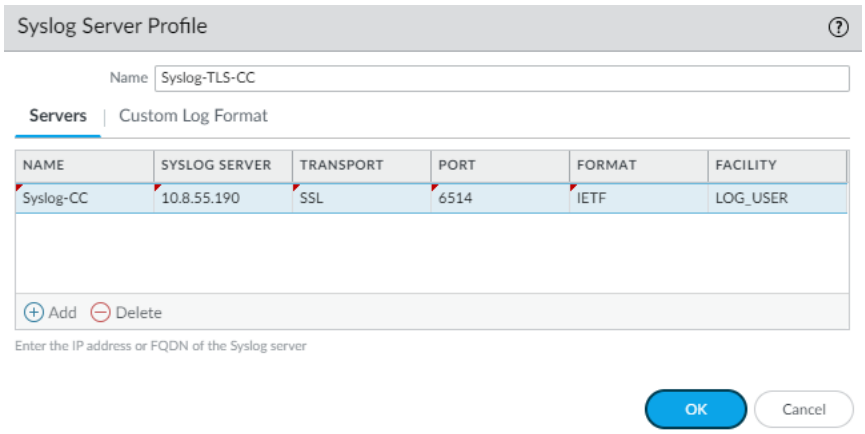
The TOE can be configured to forward generated audit records to an external syslog server in real-time. When configured, the TOE automatically converts the audit records to syslog format before forwarding them to the external syslog server. Audit records are converted and forwarded to the external syslog 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 meets 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 CRL revocation information.

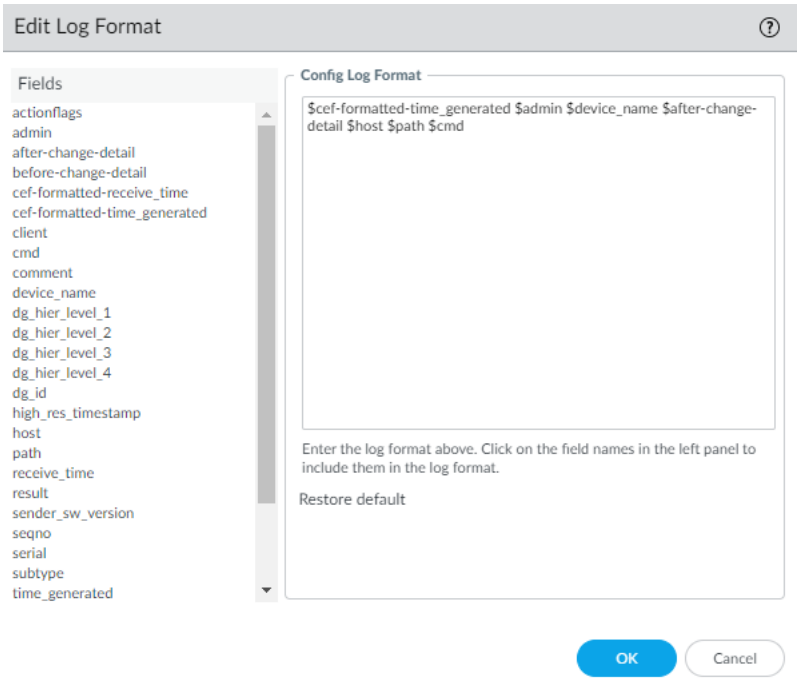
Configure a Syslog Server Profile:

1. Login with Administrator Role.
2. Select **Panorama > 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**

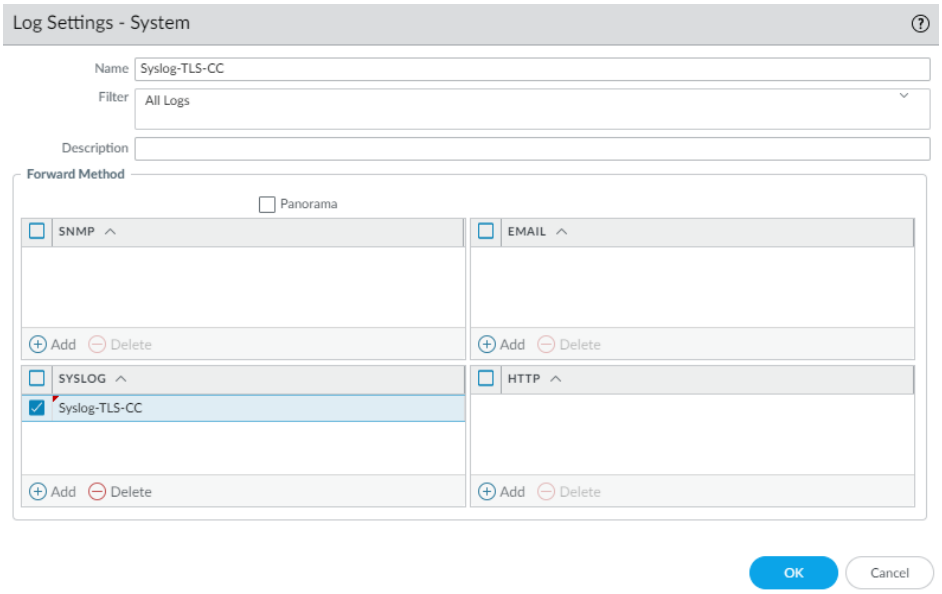


NOTE: For the configuration logs, the default log format has the minimal level of details. Edit the log format to include more details if necessary.

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.



7. Click **OK** to exit.
8. Click **OK** to save the changes.
9. Select **Panorama > 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.



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 panorama 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 **Panorama > 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.

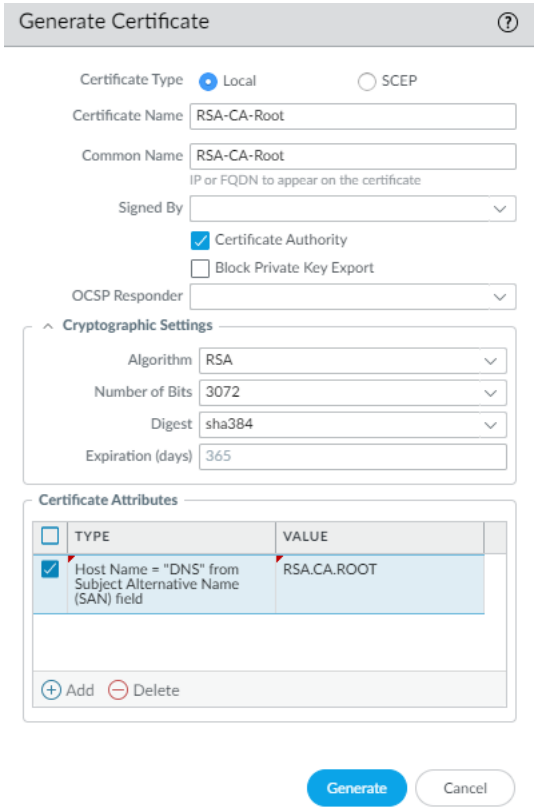
d) Select **key size** the **Number of Bits** field.

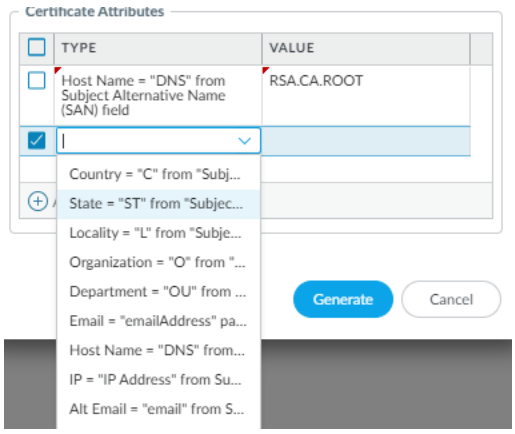
Note: RSA supports 2048, 3072, and 4096 bits. ECDSA supports 256 and 384 bits.

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

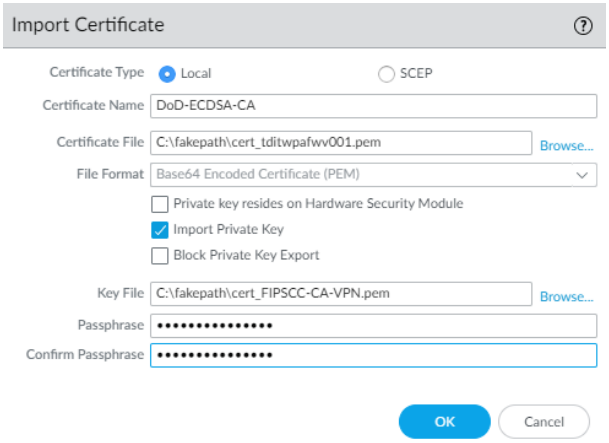
Note: The size supports SHA256, SHA384, and SHA512.

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.

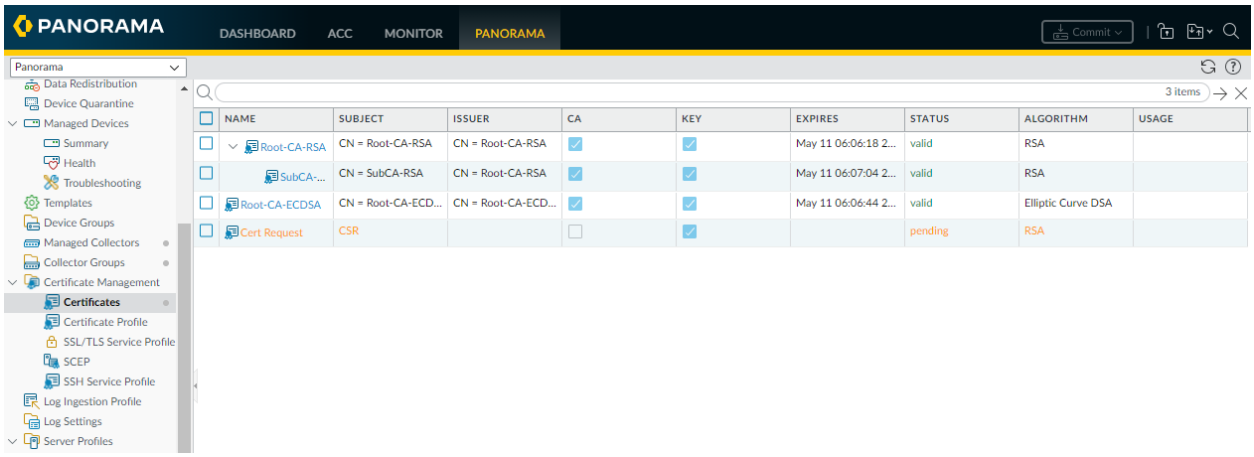




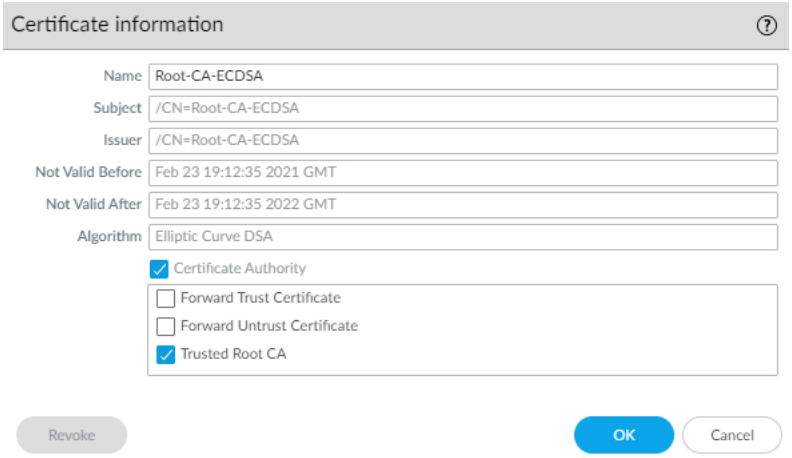
4. To import external CA Certificates, do the following steps:
    a) Click **Import**. The Import Certificate page appears.
    b) Enter **Certificate Name**. Do not include space if possible.
    c) Click **Browse…** to look for and select the CA file (PEM).
    d) Check the **Import private key** 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.



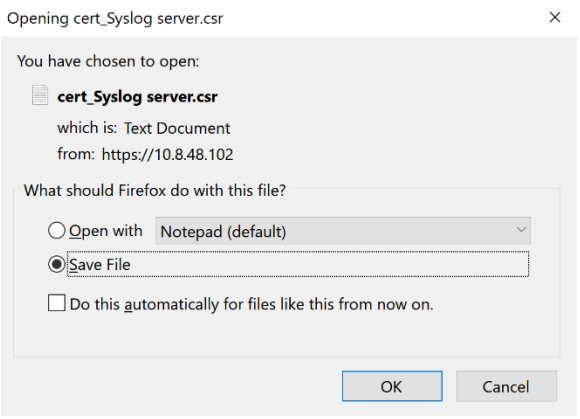
5. Click **OK** to save the changes.
6. In the screenshot below, there are two internally generated CAs, one CSR, and one imported external CAs.



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).



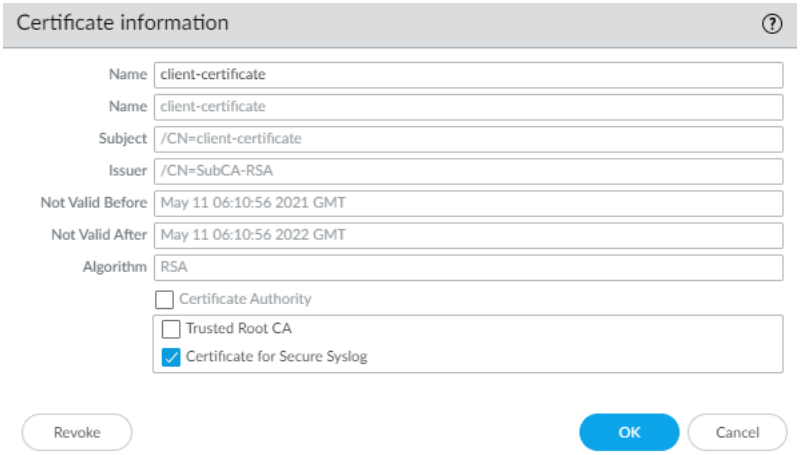
8. Click **OK** to save the changes.
9. To export any certificate or CSR, click on the certificate or CSR you want to export, and select **Export Certificate**. For example, if you want to export the syslog server CSR, it will prompt you to save the file.



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 associate 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.

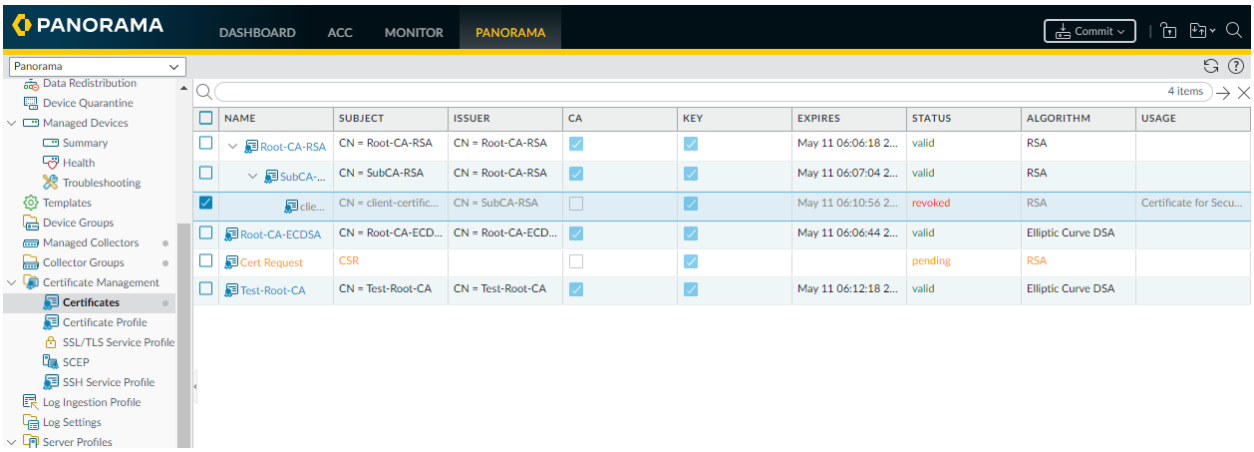


> **NOTE:** Only one client certificate can be designated as the certificate for the secure syslog connection.

> **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).



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 panorama 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_Panorama {
        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/Panorama_messages");   # The remote syslog file location can be configured here
};

log {
  source(s_Panorama); 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 Revoked'
  - Certificate is revoked[5].

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.
- 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)
- 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.

[5] To clear CRL cache, type **debug sslmgr delete crl all**.

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:

- 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_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_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_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
- 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

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.

6.9.2 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 administrator accounts that are local to Panorama. 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 a certificate to log in. Section 7.3 presents the configuration information.

NOTE: Export the client certificate in PKCS12 format to import into Chrome.

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 as the ones described the previous section.

Configure a Certificate Profile:

1. Login with Administrator Role.
2. Select **Panorama > 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. To enable CRL, **must** check the **Use CRL** checkbox to use Certificate Revocation List (CRL) to verify the revocation status of the certificates.

6. 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) **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.

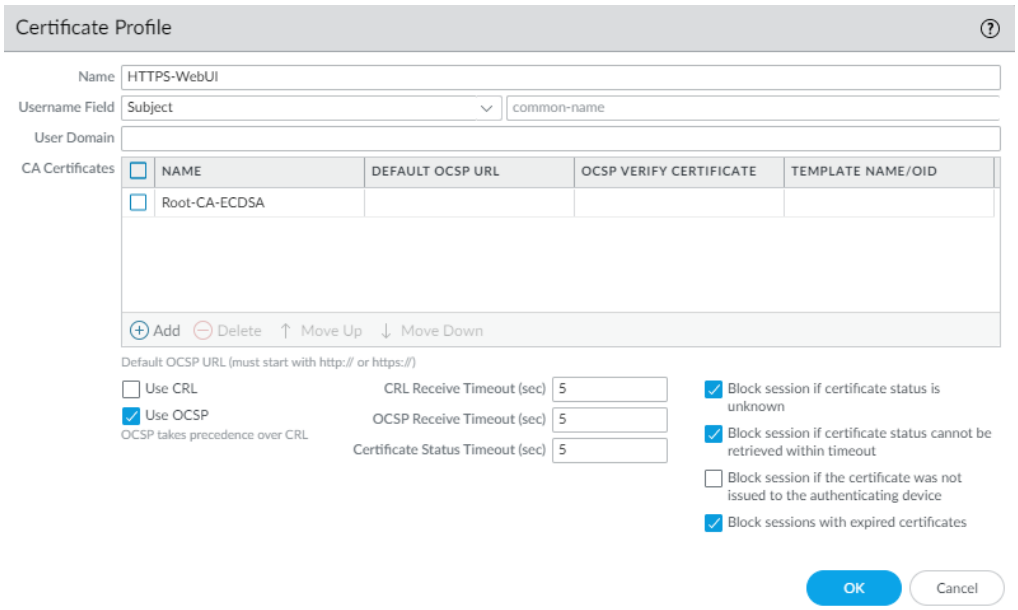
7. Check the appropriate session blocking logic checkbox.

a) **Block session if certificate status is unknown** – Select this option if you want the TOE to block sessions when the 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 a 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.



8. Click **OK** to save the changes.
9. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option (**Commit to Panorama**).

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

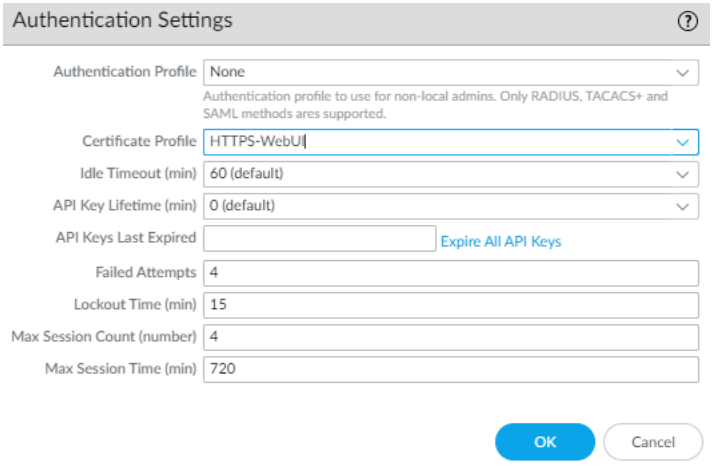
CLI HINT: The equivalent CLI commands are: **configure** and **set panorama certificate-profile <Name> <Options>**. You configure the value one-by-one. For example,

```
configure
#set panorama certificate-profile HTTPS-WebUI CA RSA_CA_Root
#set panorama certificate-profile HTTPS-WebUI block-expired-cert yes
#set panorama certificate-profile HTTPS-WebUI block-unknown-cert yes
#set panorama certificate-profile HTTPS-WebUI block-timeout-cert-timeout yes
#commit


admin@M-700# set panorama 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._-]
+ use-crl
> CA
> username-field
```

Configure the Web UI to use Certificate Profile for Authentication:

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



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 **Panorama > 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.
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**. 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 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**

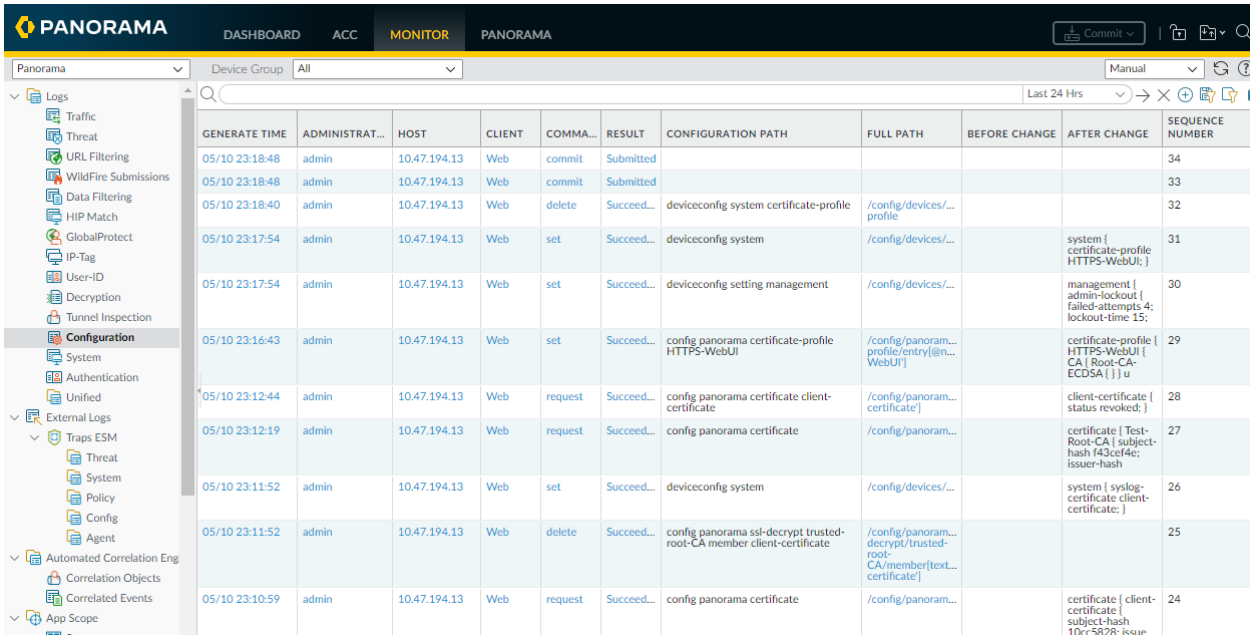
7 Management Activity

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

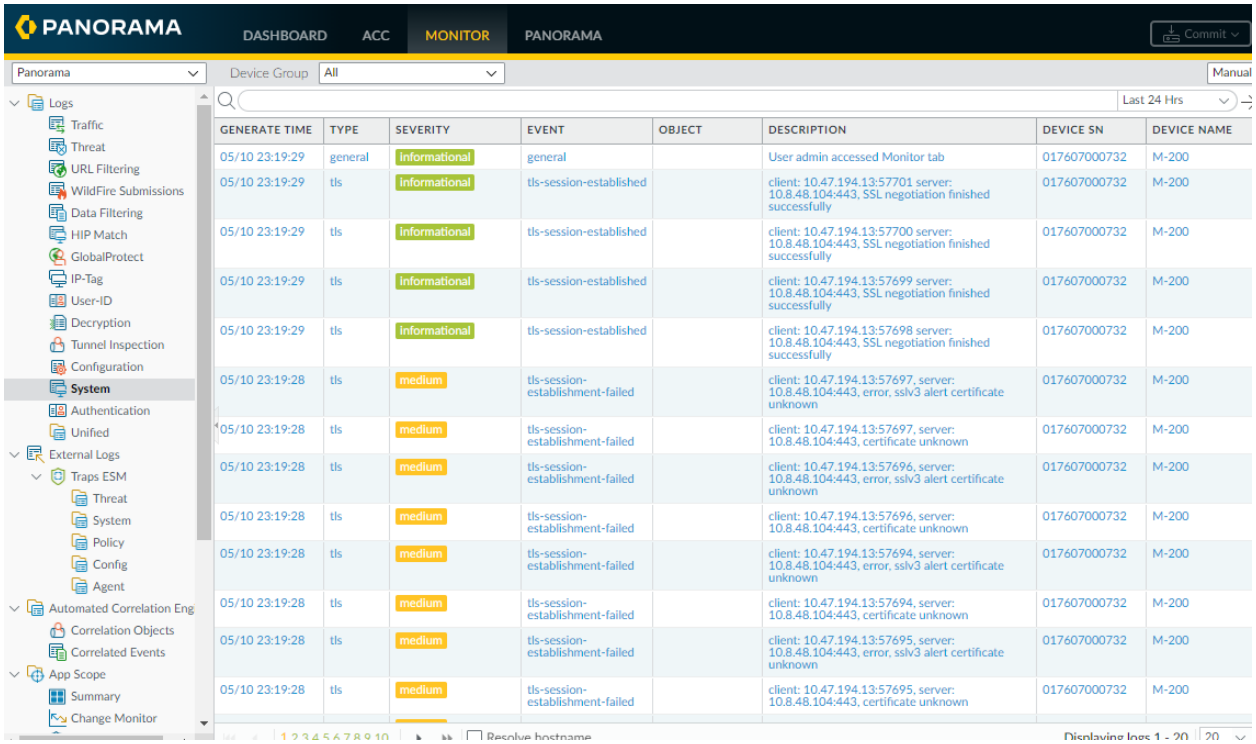
7.1 Manage Audit Log

The TOE generates and stores read-only auditing information for user activity. The logs are presented in a standard event view that allows administrator to view, sort, and filter audit log messages based on any item in the audit columns. Administrator 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**.



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



4. The equivalent CLI commands are **show log config** and **show log system**.

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

CLI HINT: To view the detailed configuration logs, use this command: **show log config csv-output equal yes**.

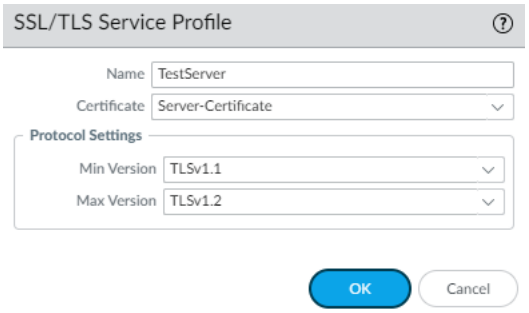
CLI HINT: To export the logs and view them externally, use this command: **scp export log system to <User>@<SSH IP Address>:<Filename> start-time equal <YYYY>/<MM>/<DD>@<hh>:<mm>:<ss> end-time equal <YYYY>/<MM>/<DD>@<hh>:<mm>:<ss>**.

7.2 Configure Custom HTTPS or TLS Server Certificate

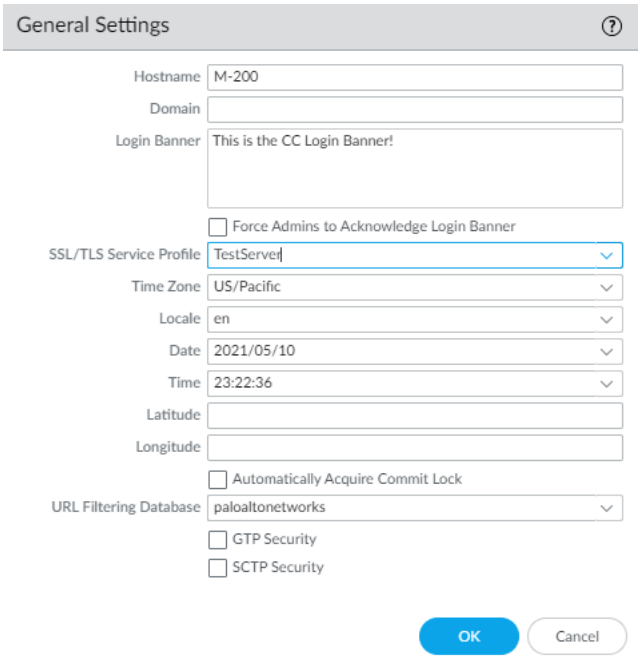
Use the following procedures to configure the TLS server (TOE) to use custom certificate instead of the predefined certificate. You can deploy the custom certificate on the TOE by generating a server certificate internally or obtaining a server certificate from your enterprise CA or a trusted third-party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

1. Login with Administrator Role.
2. Select **Panorama > 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 **Panorama > 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.



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



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 (**Commit to Panorama**).

CLI HINT: The equivalent CLI commands are **configure**, **set panorama 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>**.

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

- 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 a 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)

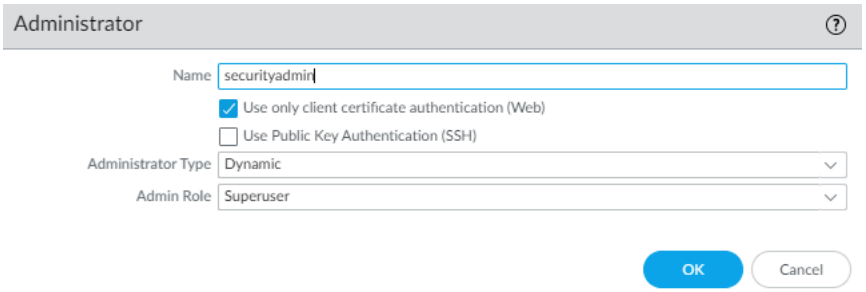
The key establishment parameters specified in FCS_TLSS_EXT.1.3 are automatically derived from the negotiated TLS ciphersuite. The same ciphersuites are supported regardless if mutual authentication is configured or not. The supported ciphersuites are implemented based on the server certificate (RSA vs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

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.

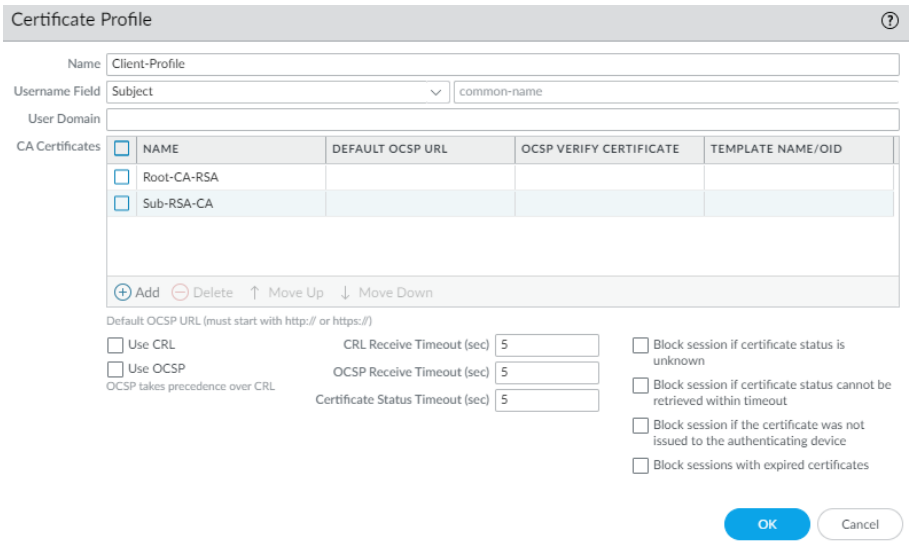
7.3 Configure HTTPS or TLS Client Certificate Authentication

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. Create a user and check **Use only client certificate authentication (Web)** checkbox.
3. Click **OK**.

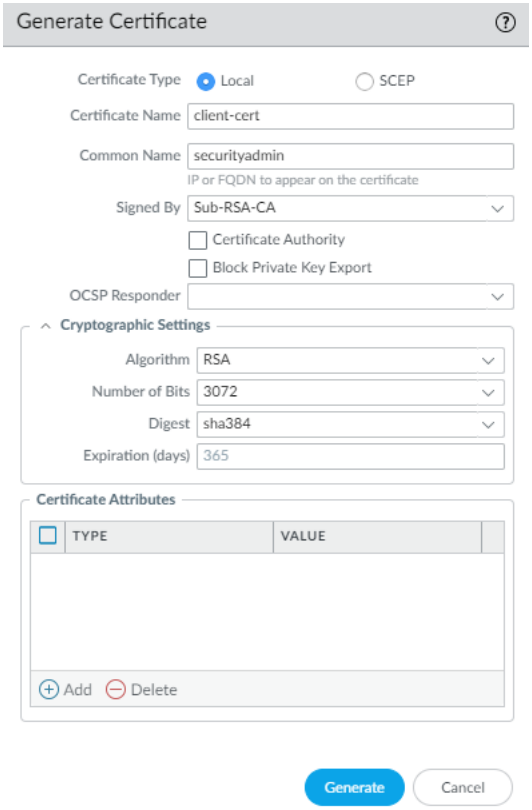


4. Create a Root CA and Intermediate CA (internally or externally). Import the CA(s) and private keys into the TOE, if generated externally. This will set the CA certificates in the Trust Anchor.
5. Create a client certificate profile. The **Username** field should be set to **Subject**. In the **CA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



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**.

6. Create a client certificate.
7. To create a client certificate, **Panorama > Certificate Management > Certificate > Generate**.



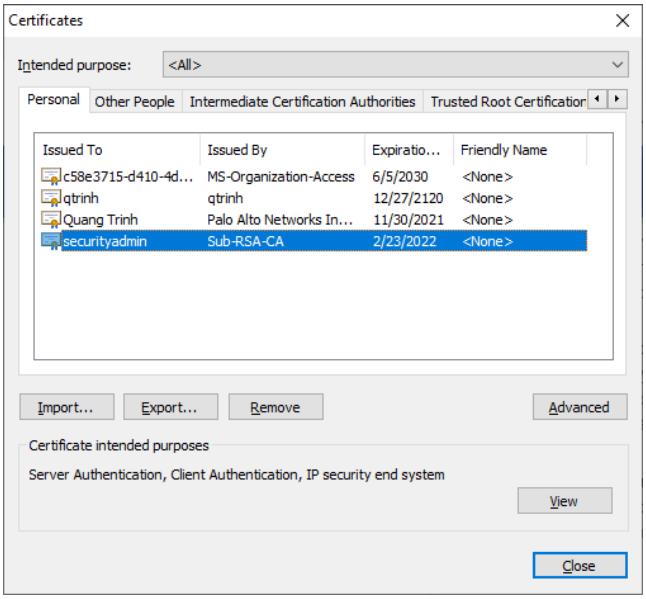
WARNING: Make sure **Common Name** field matches the name (i.e., username) in step 3. IP address or email address is not supported, and should not be used in the evaluated configuration. The username must match the username stored in the local database.

8. 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.

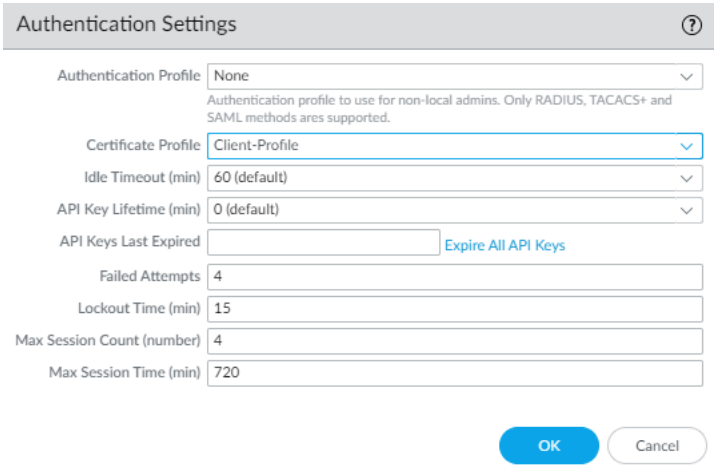
9. Change the client certificate PEM format to PKCS12 (see command below) before importing the client certificate into Chrome (Settings > Advanced > Privacy & Security > Manage Certificates > Import…) or Firefox (Options > Privacy & Security > Certificates > View Certificates… > Import…). You can also store the client certificate on a Common

Access Card (CAC) and configure the web browser to retrieve the client certificate from the CAC.

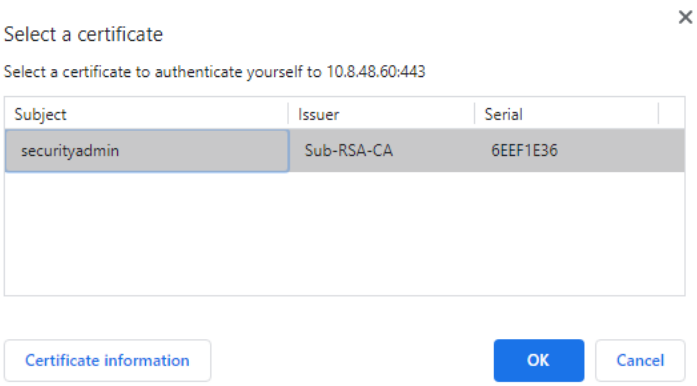


openssl pkcs12 -export -clcerts -in client.pem -inkey client.key -out client.p12

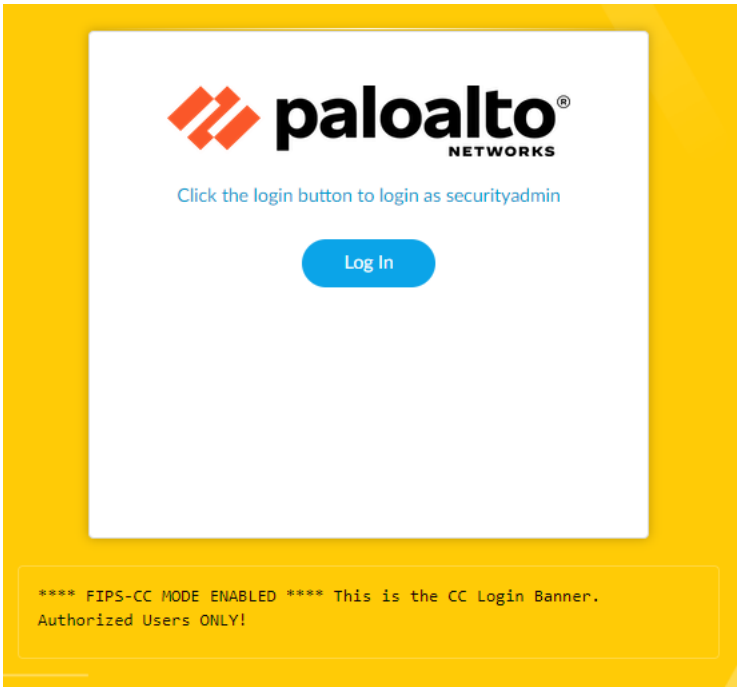
10. Set the new client certificate profile for the **Certificate Profile** in Authentication settings.
11. **Panorama > Setup > Management > Authentication Settings**.



12. Click **OK** and **Commit**.
13. 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.



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



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

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 panorama certificate-profile <Name> username-field subject common-name, set panorama certificate-profile <Name> CA <CA-Names>, set panorama certificate-profile <Name> <Options specified in section 6.9.2>, set deviceconfig system certificate-profile <Name>**.

7.4 Role-Based Access Control (RBAC)

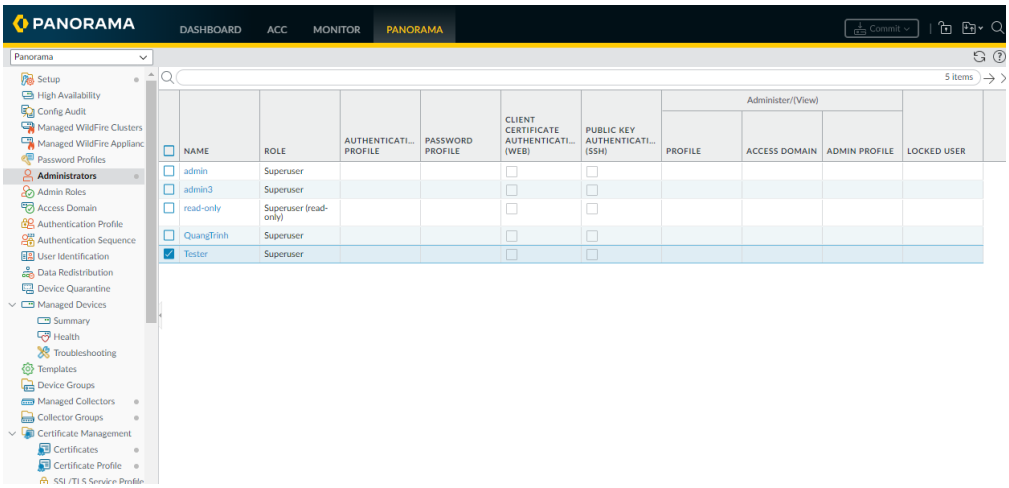
RBAC enables you to define the privileges and responsibilities of administrative users. Every administrator must have a user account that specifies a role and authentication method. By default, every TOE appliance (M-Series or virtual appliance) has a predefined administrative account (**admin**) that 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, 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 **Panorama > Administrators**.

   The Administrators page appears.



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

7.4.2 Adding New Accounts

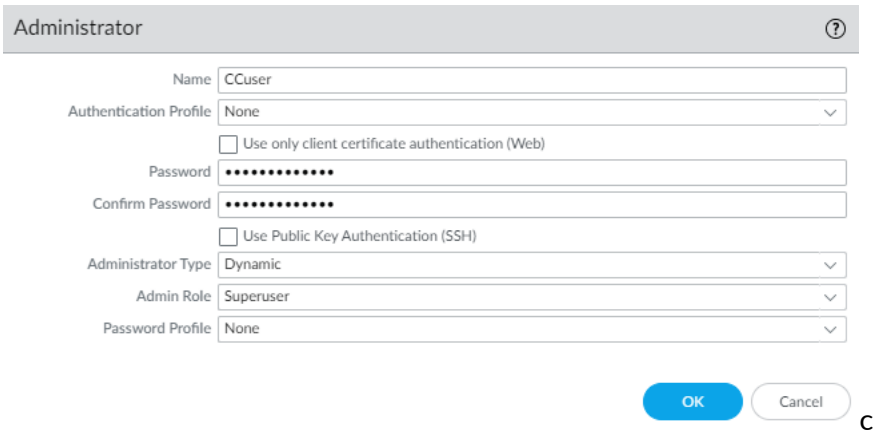
When you create a new user account, you can control which parts of the system the account can access. You can set the authentication method (password vs public-key), authentication profile (e.g., using authentication server), administrator type (e.g., dynamic, custom role), and administrator role (e.g.,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

1. Login with Administrator Role.
3. Select **Panorama > 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.
    - **Custom Panorama Admin** – Configurable roles that have read-write access, read-only access, or no access to TOE features.
    - **Device Group and Template Admin** – Configurable roles that have read-write access, read-only access, or no access to features for the device groups and templates that are assigned to the access domains you select for this administrator.
9. In the **Admin Role** field, select the role.
    - **Superuser** – Full read-write access to Panorama and all device groups, templates, and managed devices.
    - **Superuser (Read Only)** – Read-only access to Panorama and all device groups, templates, and managed devices.
    - **Panorama administrator** – Full access to Panorama 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 **Panorama** tab.
10. Select a **Password Profile**.



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@M-700# set mgt-config users admin2

+ authentication-profile

+ client-certificate-only Is client certificate authentication enough?

+ 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 **Panorama > 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**.

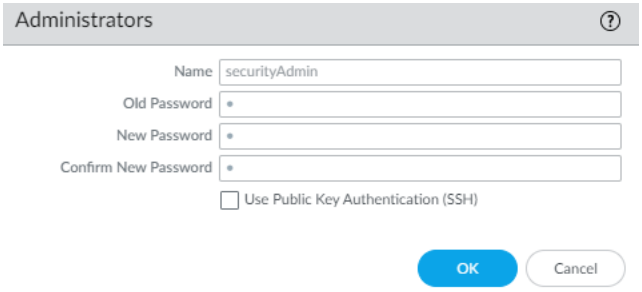
5. Click **Yes** to confirm. Commit the changes.
6. The user account is deleted.
7. To modify a user, select the user link you want to modify under Name column.
8. Edit the user settings and click **OK**.
9. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select 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.

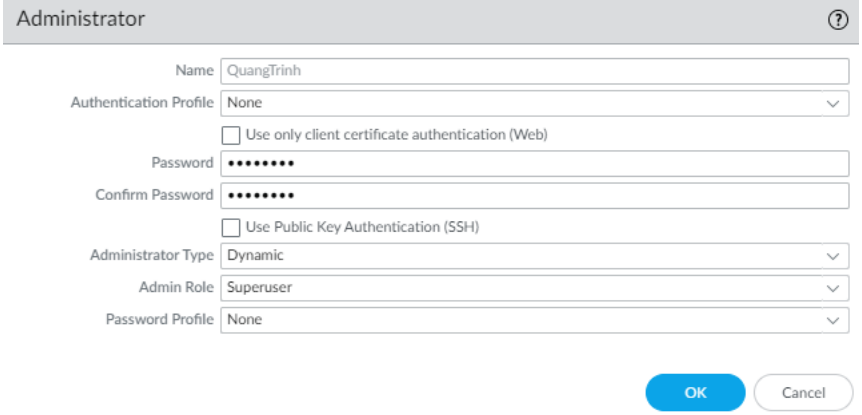
7.4.4 Change User Password

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

1. Login with Administrator Role.
2. Select **Panorama > 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**.



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

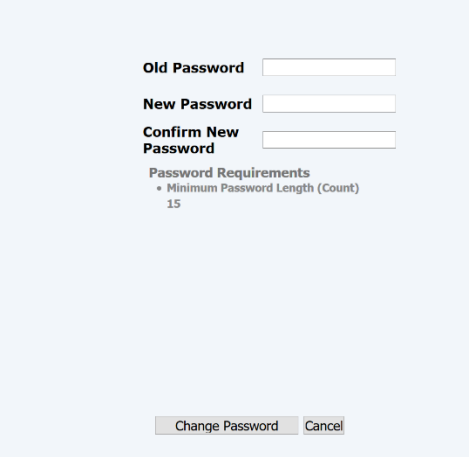


7. Commit the changes. In the upper right corner, click on the **Commit** drop-down, and select the appropriate option.

CLI HINT: The equivalent CLI commands are **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.

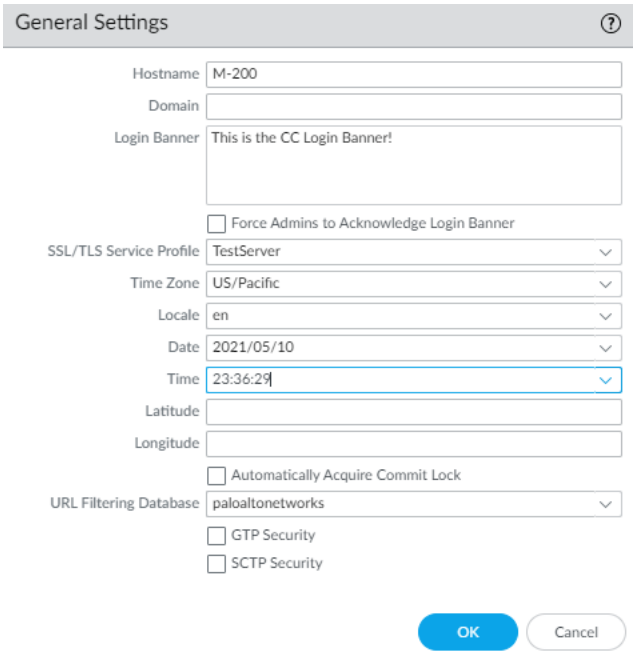


7.5 Configure System Time

The administrator can configure time manually.

7.5.1 Configure Time Manually

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



3. Select the **Time Zone** for the TOE.
4. Configure the **Date** for the TOE.
5. Configure the **Time** for the TOE.
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 **set clock date <YYYY/MM/DD> time <hh:mm:ss>** and **set deviceconfig system timezone <Timezone>**.

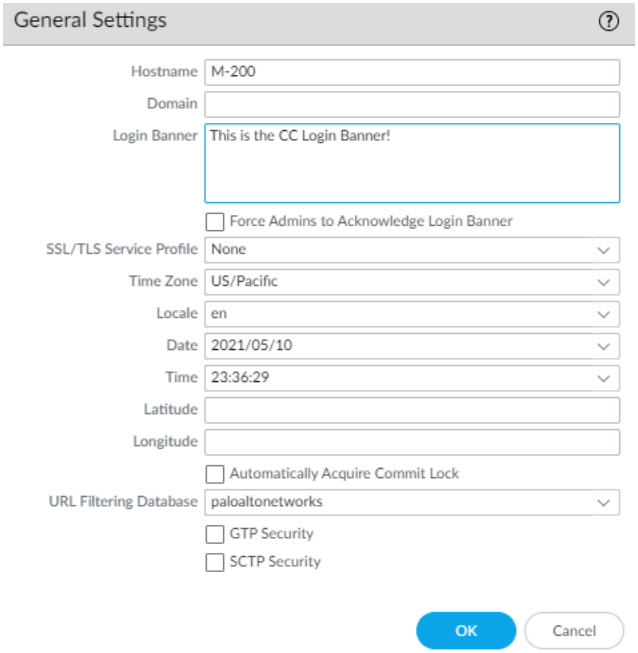
> **API HINT:** The equivalent API call is (need to edit the value and API key)
>
> - **https://<TOE>/api/?type=op&cmd=<set><clock><date>2019/06/27</date><time>17:35:00</time></clock></set>&key=<APIkey>**

NOTE: For Panorama 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 **Panorama > Setup > Management > General Settings**. The General Setting page appears.



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.

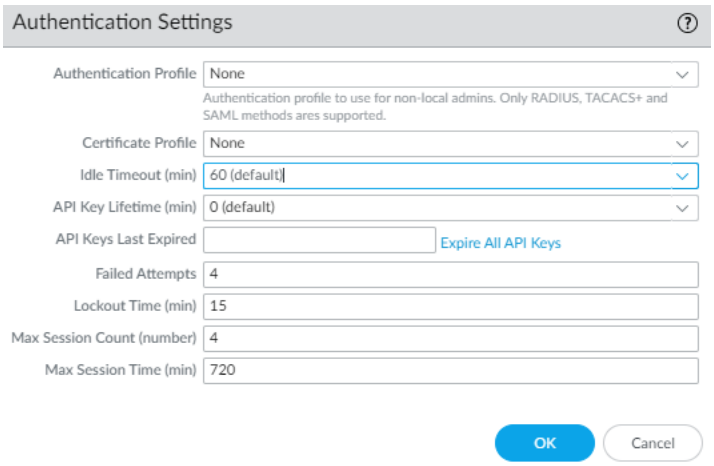
> **CLI HINT:** The equivalent CLI commands are **configure** and **set deviceconfig system login-banner <Value>**.

> **API HINT:** The equivalent 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. When the idle timeout value is exceeded, the idle session will be terminated. 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 **Panorama > Setup > Management > Authentication Settings**. The Authentication Setting page appears.



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 0 to 10) that the TOE allows for the web interface and CLI before locking out the administrator account. A value of 0 (default) specifies unlimited login attempts. In the evaluated configuration, this value must not be set to 0.

> **NOTE:** If you set the **Failed Attempts** to a value other than 0 but leave the **Lockout Time** at 0, the user is locked out until another administrator manually unlocks the account.

5. Configure the **Lockout Time** interval. Enter the number of minutes (range is 0 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 (default) means the lockout applies until another administrator manually unlocks the account.

NOTE: If you set the **Lockout Time** to a value other than 0 but leave the **Failed Attempts** at 0, the **Lockout Time** is ignored, and the user is never locked out.

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>**.

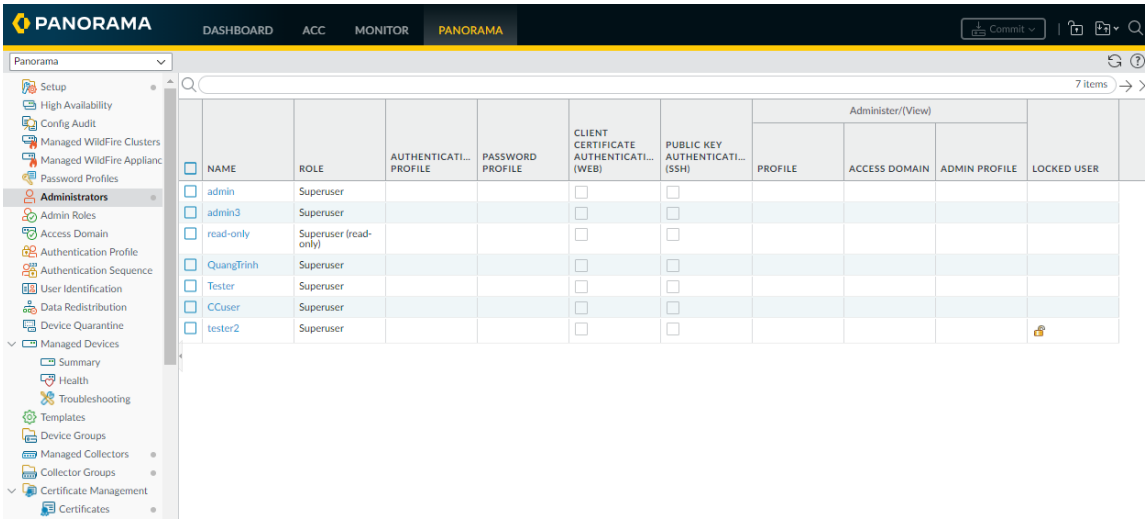
CLI HINT: The equivalent CLI commands are **configure** and **set deviceconfig setting management admin-lockout failed-attempt <0-10>** and **set deviceconfig setting management admin-lockout lockout-time <0-60>**. In the evaluated configuration, these values must not be set to 0.

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

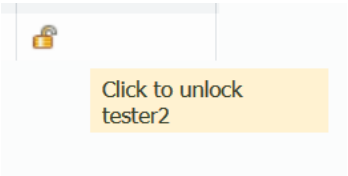
- **https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management&element=<admin-lockout><failed-attempts>4</failed-attempts></admin-lockout>&key=<APIkey>**
- **https://<TOE>/api/?type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management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

7.7.1 Unlock User

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



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



5. No commit is needed.

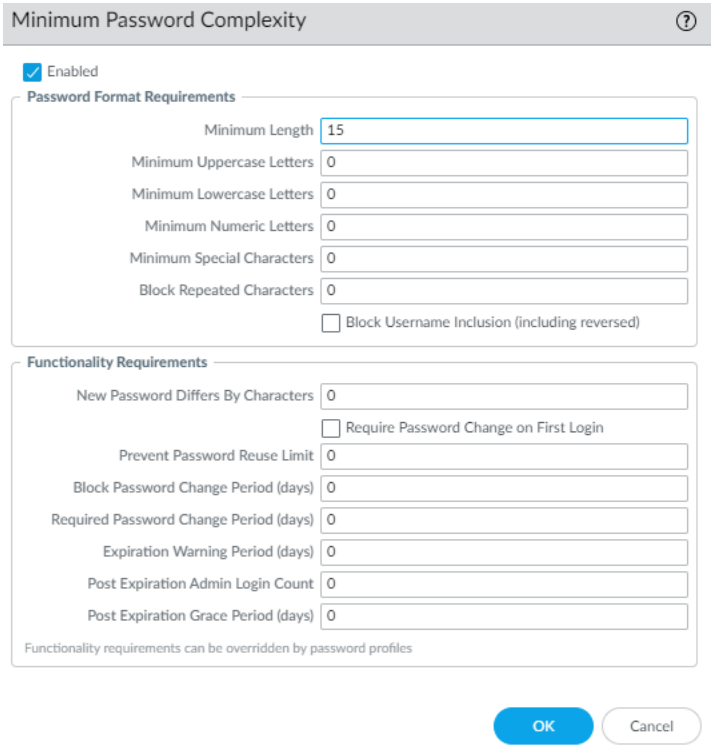
> **CLI HINT:** The equivalent CLI command is **request authentication unlock-admin user <username>**.

> **API HINT:** The equivalent 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).

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



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 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 Managed Device

To use the TOE to manage other devices (such as NGFW, WildFire, etc.) the administrator will need to enable a secure connection between the TOE and device. This connection requires you enter the TOE IP address on each device that will be managed, and to enter the serial number of each device on the TOE. The device uses the TOE server IP address to set up a TLS connection to register with TOE. The TOE and the device authenticate each other using X509v3 certificates and the TLS connections for configuration management and log collection. Mutual authentication is required for all TLS connections between TOE and devices, and all data (security-relevant or not) are protected via TLS.

NOTE: The CC evaluation only covers the secure connections between the TOE and managed devices. The effective management of those devices is out of scope.

Prepare the TOE, and each device as follows:

Repeat this step for each device the TOE will manage.

1. Perform initial configuration on the device so that it is accessible and can communicate with the TOE over the network.
2. Add the TOE IP address to the device.
    a. Select **Device > Setup > Management** and edit the Panorama Settings.
    b. Enter the Panorama IP address in the first field.
    c. (Optional) If you have set up a High Availability pair in Panorama, enter the IP address of the secondary Panorama in the second field.
    d. Click **OK**.
    e. Select **Commit** and **Commit** your changes.

Add the device to the TOE.

1. Select **Panorama > Managed Devices** and click **Add**.

2. Enter the serial number for each device (one entry per line) that you want to manage centrally using the TOE, and then click **OK**. The Managed Devices page displays the new device.

3. (Optional) Add a **Tag**. Tags make it easier for you to find a device from a large list; they help you to dynamically filter and refine the list of devices that display. For example, if you add a tag called branch office, you can filter for all branch office firewalls across your network.

    1. Select the check box beside the device and click **Tag**.

    2. Click **Add**, enter a string of up to 31 characters (no empty spaces), and click **OK**.

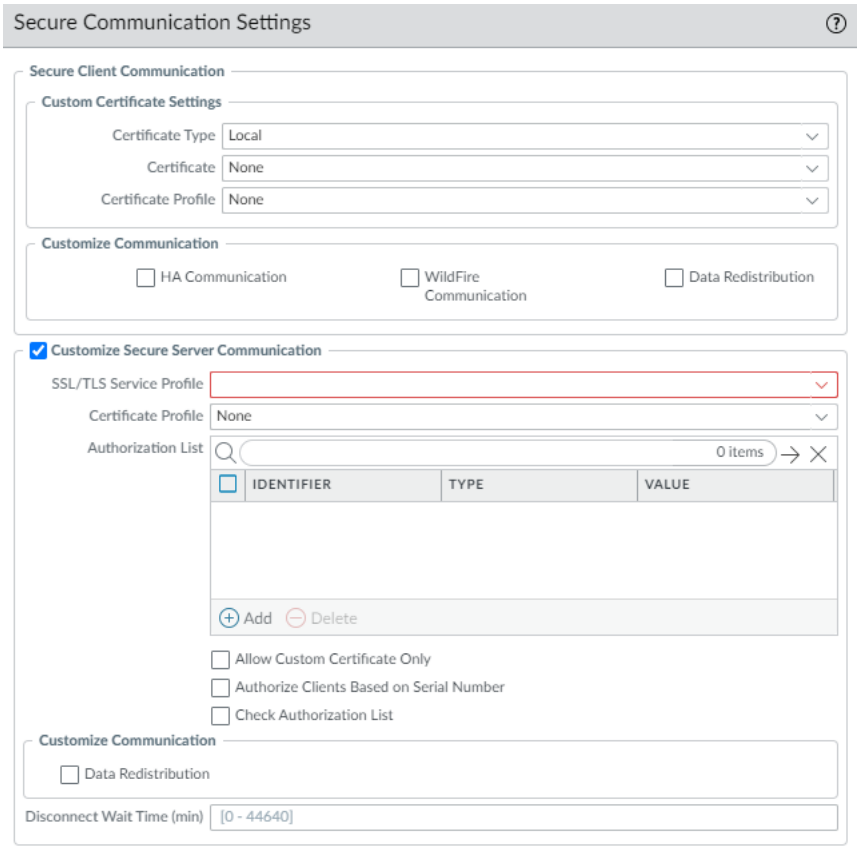
4. If your deployment is using custom certificates for authentication between Panorama and managed devices, deploy the custom client device certificate.

5. Select **Commit > Commit to Panorama** and **Commit** your changes.

CLI HINT: The equivalent CLI commands are **configure** and **set deviceconfig system panorama-server <IP address or FQDN>**.

WARNING: To secure the communication between the TOE and managed devices, you must configure the **Secure Communication Settings**.

1. Login with Administrator Role.
2. Select **Panorama > Setup > Management > Secure Communication Settings**. Click on the gear setting. The Secure Communication Settings page appears.



3. When communicating with another TOE peer (HA) or WildFire appliance, select **Local** as the **Certificate Type**. The default is **Predefined** which means no custom device certificate is configured and the TOE will use the default predefined certificate for those devices.
4. Select **Certificate** - Select the local device certificate you generated or imported. This certificate can be unique to the firewall (based on a hash of the serial number of that firewall) or it can be a common device certificate used by all firewalls that connect to Panorama.

5. Select **Certificate Profile -** Select the Certificate Profile from the drop-down. The Certificate Profile defines the CA certificate for verifying client certificates and how to verify certificate revocation status.
6. Optionally, configure the **Customize Communication**. Otherwise, when the TOE is communicating with the managed firewalls, the TOE is always the TLS server.
7. To customize the secure connection, check the **Customize Secure Server Communication** checkbox.
8. Select an **SSL/TLS Service Profile** from the drop-down. This profile defines the certificate and supported SSL/TLS versions that the managed firewall can use to communicate with TOE.
9. Select a **Certificate Profile** from the drop-down. This certificate profile defines certificate revocation-checking behavior and the root CA used to authenticate the certificate chain presented by the peer.
10. **Authorization List—Add** and configure a new authorization profile using the following fields to set the criteria for authorizing client devices that can connect to the TOE. The Authorization List supports a maximum of 16 profile entries.
    - **Identifier**—Select **Subject** or **Subject Alt. Name** as the authorization identifier.
    - **Type**—If you selected **Subject Alt. Name** as the Identifier, then select **IP**, **hostname**, or **e-mail** as the identifier type. If you selected **Subject**, then you must use **common name** as the identifier type.
    - **Value**—Enter the identifier value.
11. Check the appropriate checkboxes.
    - **Allow Custom Certificate Only**— When checked, the TOE accepts only custom certificates for authentication with managed devices.

    NOTE: This checkbox must be checked if the certificate and TLS version range from the SSL/TLS Service Profile are to be utilized.

    - **Authorized Clients Based on Serial Number**—When checked, the TOE authorizes client devices based on a hash of the device serial number.
    - **Check Authorization List**—When checked the TOE checks client device identities against the authorization list. A device must match only one criterion on the list to be authorized. If no match is found, the device is not authorized.
12. **Disconnect Wait Time (min)**—The amount of time (in minutes) that the TOE waits before terminating the current connection with its managed devices.
13. Click **OK**.
14. Select **Commit** and **Commit** your changes.

> **CLI HINT:** The equivalent CLI commands are **set deviceconfig setting management secure-conn-server certificate-profile <name of profile> disable-pre-defined-cert <yes | no> ssl-tls-service-profile <name of profile> check-authorization-list <yes | no> authorization-list <name of list> identifier <subject or subject-alt-name> <common-name | email, hostname, ip> <value>** and **set deviceconfig setting management secure-conn-client certificate-profile <name of profile> disable-pre-defined-cert <yes | no> ssl-tls-service-profile <name of profile> check-authorization-list <yes | no> authorization-list <name of list> identifier <subject or subject-alt-name> <common-name | email, hostname, ip> <value>**.

The TOE (as a TLS server) connection to firewall or Wildfire (mutual authentication required) supports the following TLSv1.1 and TLSv1.2 ciphersuites:

- 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_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
- 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

The administrator is responsible for maintaining the physical connection between the TOE and external trusted devices. 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 external trusted device is still running.
- Re-register the device with the TOE.
- If all else fails, reboot the TOE and/or external trusted device.

7.10 Configure System Mode

The administrator can change the system mode. Regardless of which system mode is deployed, the TOE must also be configured to run in the Common Criteria mode of operation (FIPS-CC mode).

1. Login with Administrator Role.
2. Enter the following commands:
    - **request system system-mode <system mode>**
3. Type 'Y' to confirm.

WARNING: The system must be rebooted for the system mode to change.

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

- **https://<TOE>/api/?type=op&cmd=<request><system><system-mode>system </system-mode></system></request>&key=<APIkey>**

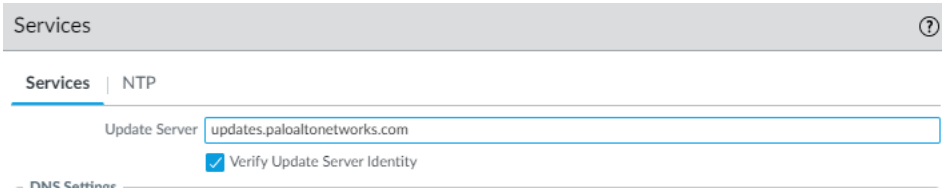
7.11 Verify and Update System Software

The administrator must verify the TOE version is the evaluated version 10.2.3-h2. The TOE version is verified using the **show system info** command. If the delivered version is not version 10.2.3-h2, please follow the commands:

- **request system software check**
- **request system software download version 10.2.3-h2**
- **request system software install version 10.2.3-h2**

The TOE supports system software download and update process (**Panorama > 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 signatures 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 **Panorama > Setup > Services**. Click on the gear setting.
4. Make sure the TOE is connected to the correct Update Server updates.paloaltonetworks.com (Internet connection required!).



5. Select **Panorama > Software**.
6. Click **Check Now**.
7. If the TOE is connected to the Update Server (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 API calls are

- **curl -X GET 'https://<TOE>/api/?type=op&cmd=<request><system><software><check></check></software></system></request>&key=<APIkey>'**
- **curl -X GET 'https://<TOE>/api/?type=op&cmd=<request><system><software><download><version>9.0.9</version></download></software></system></request>&key=<APIkey>'**
- **curl -X GET 'https://<TOE>/api/?type=op&cmd=<request><system><software><install><version>9.0.9</version></install></software></system></request>&key=<APIkey>'**

7.12 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 firewall or Panorama 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 firewall or use Panorama to perform these operation on policies and objects from a central location and push them to the managed firewalls.

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.

7.12.1 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 firewall, 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.

7.12.2 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 firewall and Panorama support 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.

7.12.3 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/ent
ry/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>
```

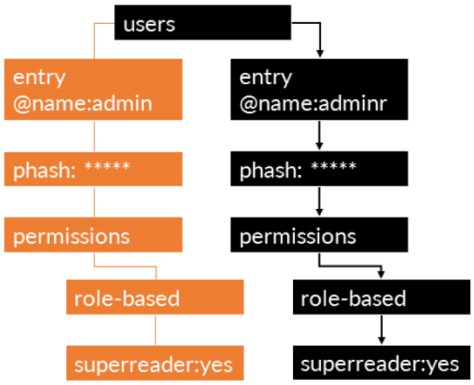
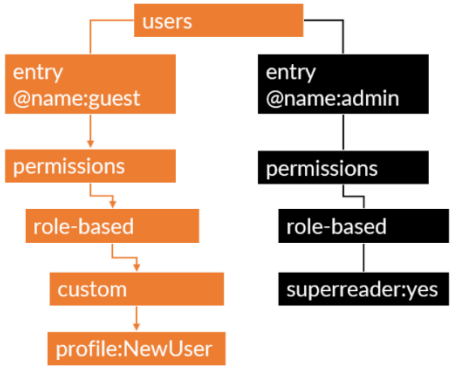
- Root nodes are top-level nodes with no parent. Requesting the root node returns all child elements.
- Element nodes represent containers of information. Element nodes can contain other element nodes or simply act as a container of information. Example: **<permissions></permissions>**
- Attribute nodes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

7.12.4 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
	`/config/mgt-config/users/ entry/permissions/role-based/ superuser[text()='yes']`
	`/config/mgt-config/users/entry/ permissions/role-based/custom/ profile[text()='NewUser']`

7.12.5 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, Panorama.

Admin Role profiles enable or disable features on the management interfaces of the firewall or Panorama, 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.

7.12.6 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>&ke
y=<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=... '

7.12.7 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 firewall rule

```
curl -X POST \
'https://10.1.1.4/restapi/10.2.3/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"
                ]
            }
        }
    ]
}'
```

7.13 Self-Tests

The TOE performs a suite of FIPS self-tests during power-up, at scheduled intervals, and during operational state. If any 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:

- Software Integrity failure [power-up | schedule]
- Known Answer Test (KAT) failures [power-up | schedule]
- Pairwise Consistency failures [during operational]
- RNG Continuous failures [during operational]
- Entropy Continuous failures [during operational]

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

GENERATE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION	DEVICE SN	DEVICE NAME
05/11 10:37:05	general	high	system-start		The system is starting up.	017607000732	M-200
05/11 10:36:11	hw	informational	ps-inserted		Power Supply #2 (right) inserted	017607000732	M-200
05/11 10:36:08	port	informational	link-change	MGT	Port MGT: Up 1Gb/s Full duplex	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Enabled Successfully	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test ECDH known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test ECDSA known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test DRBG known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test CMAC known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test AES-CCM known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test AES-GCM known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test SHA-512 known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test SHA-384 known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test SHA-256 known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test DH known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test RSA known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test AES known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test HMAC known answer test ..... succeeded	017607000732	M-200
05/11 10:36:04	fips	informational	fips-selftest		FIPS-CC Mode Self-test SHA-1 known answer test ..... succeeded	017607000732	M-200

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.