Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About this Guide

This guide takes you through the configuration and maintenance of your Palo Alto Networks next-generation firewall. For additional information, refer to the following resources:

- For information on how to configure other components in the Palo Alto Networks Next-Generation Security Platform, go to the Technical Documentation portal: https://docs.paloaltonetworks.com or search the documentation.
- For access to the knowledge base and community forums, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/services/solution-assurance.
- For the most current PAN-OS and Panorama 7.1 release notes, go to https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-release-notes

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.
Certificate Management

The following topics describe the different keys and certificates that Palo Alto Networks® firewalls and Panorama use, and how to obtain and manage them:

- Keys and Certificates
- Certificate Revocation
- Certificate Deployment
- Set Up Verification for Certificate Revocation Status
- Configure the Master Key
- Obtain Certificates
- Export a Certificate and Private Key
- Configure a Certificate Profile
- Configure an SSL/TLS Service Profile
- Replace the Certificate for Inbound Management Traffic
- Configure the Key Size for SSL Forward Proxy Server Certificates
- Revoke and Renew Certificates
- Secure Keys with a Hardware Security Module
Keys and Certificates

To ensure trust between parties in a secure communication session, Palo Alto Networks firewalls and Panorama use digital certificates. Each certificate contains a cryptographic key to encrypt plaintext or decrypt cyphertext. Each certificate also includes a digital signature to authenticate the identity of the issuer. The issuer must be in the list of trusted certificate authorities (CAs) of the authenticating party. Optionally, the authenticating party verifies the issuer did not revoke the certificate (see Certificate Revocation).

Palo Alto Networks firewalls and Panorama use certificates in the following applications:

- **User authentication for Captive Portal, GlobalProtect™, Mobile Security Manager, and web interface access to a firewall or Panorama.**
- **Device authentication for GlobalProtect VPN (remote user-to-site or large scale).**
- **Device authentication for IPSec site-to-site VPN with Internet Key Exchange (IKE).**
- **Decrypting inbound and outbound SSL traffic.**

A firewall decrypts the traffic to apply policy rules, then re-encrypts it before forwarding the traffic to the final destination. For outbound traffic, the firewall acts as a forward proxy server, establishing an SSL/TLS connection to the destination server. To secure a connection between itself and the client, the firewall uses a signing certificate to automatically generate a copy of the destination server certificate.

The following table describes the keys and certificates that Palo Alto Networks firewalls and Panorama use. As a best practice, use different keys and certificates for each usage.

**Table: Palo Alto Networks Device Keys/Certificates**

<table>
<thead>
<tr>
<th>Key/Certificate Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Access</td>
<td>Secure access to firewall or Panorama administration interfaces (HTTPS access to the web interface) requires a server certificate for the MGT interface (or a designated interface on the dataplane if the firewall or Panorama does not use MGT) and, optionally, a certificate to authenticate the administrator.</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>In deployments where Captive Portal identifies users who access HTTPS resources, designate a server certificate for the Captive Portal interface. If you configure Captive Portal to use certificates (instead of, or in addition to, username/password credentials) for user identification, designate a user certificate also. For more information on Captive Portal, see Map IP Addresses to Usernames Using Captive Portal.</td>
</tr>
<tr>
<td>Forward Trust</td>
<td>For outbound SSL/TLS traffic, if a firewall acting as a forward proxy trusts the CA that signed the certificate of the destination server, the firewall uses the forward trust CA certificate to generate a copy of the destination server certificate to present to the client. To set the private key size, see Configure the Key Size for SSL Forward Proxy Server Certificates. For added security, store the key on a hardware security module (for details, see Secure Keys with a Hardware Security Module).</td>
</tr>
<tr>
<td>Forward Untrust</td>
<td>For outbound SSL/TLS traffic, if a firewall acting as a forward proxy does not trust the CA that signed the certificate of the destination server, the firewall uses the forward untrust CA certificate to generate a copy of the destination server certificate to present to the client.</td>
</tr>
<tr>
<td>SSL Inbound Inspection</td>
<td>The keys that decrypt inbound SSL/TLS traffic for inspection and policy enforcement. For this application, import onto the firewall a private key for each server that is subject to SSL/TLS inbound inspection. See Configure SSL Inbound Inspection.</td>
</tr>
</tbody>
</table>
## Certificate Management

### Key/Certificate Usage

<table>
<thead>
<tr>
<th>Key/Certificate Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Exclude Certificate</td>
<td>Certificates for servers to exclude from SSL/TLS decryption. For example, if you enable SSL decryption but your network includes servers for which the firewall should not decrypt traffic (for example, web services for your HR systems), import the corresponding certificates onto the firewall and configure them as SSL Exclude Certificates. See <a href="#">Configure Decryption Exceptions</a>.</td>
</tr>
<tr>
<td>GlobalProtect</td>
<td>All interaction among GlobalProtect components occurs over SSL/TLS connections. Therefore, as part of the GlobalProtect deployment, deploy server certificates for all GlobalProtect portals, gateways, and Mobile Security Managers. Optionally, deploy certificates for authenticating users also. Note that the GlobalProtect <a href="#">Large Scale VPN (LSVPN)</a> feature requires a CA signing certificate.</td>
</tr>
<tr>
<td>Site-to-Site VPNs (IKE)</td>
<td>In a site-to-site IPSec VPN deployment, peer devices use Internet Key Exchange (IKE) gateways to establish a secure channel. IKE gateways use certificates or preshared keys to authenticate the peers to each other. You configure and assign the certificates or keys when defining an IKE gateway on a firewall. See <a href="#">Site-to-Site VPN Overview</a>.</td>
</tr>
<tr>
<td>Master Key</td>
<td>The firewall uses a master key to encrypt all private keys and passwords. If your network requires a secure location for storing private keys, you can use an encryption (wrapping) key stored on a hardware security module (HSM) to encrypt the master key. For details, see <a href="#">Encrypt a Master Key Using an HSM</a>.</td>
</tr>
<tr>
<td>Secure Syslog</td>
<td>The certificate to enable secure connections between the firewall and a syslog server. See <a href="#">Syslog Field Descriptions</a>.</td>
</tr>
<tr>
<td>Trusted Root CA</td>
<td>The designation for a root certificate issued by a CA that the firewall trusts. The firewall can use a self-signed root CA certificate to automatically issue certificates for other applications (for example, <a href="#">SSL Forward Proxy</a>). Also, if a firewall must establish secure connections with other firewalls, the root CA that issues their certificates must be in the list of trusted root CAs on the firewall.</td>
</tr>
</tbody>
</table>
Certificate Revocation

Palo Alto Networks firewalls and Panorama use digital certificates to ensure trust between parties in a secure communication session. Configuring a firewall or Panorama to check the revocation status of certificates provides additional security. A party that presents a revoked certificate is not trustworthy. When a certificate is part of a chain, the firewall or Panorama checks the status of every certificate in the chain except the root CA certificate, for which it cannot verify revocation status.

Various circumstances can invalidate a certificate before the expiration date. Some examples are a change of name, change of association between subject and certificate authority (for example, an employee terminates employment), and compromise (known or suspected) of the private key. Under such circumstances, the certificate authority that issued the certificate must revoke it.

The firewall and Panorama support the following methods for verifying certificate revocation status. If you configure both methods, the firewall or Panorama first tries the OCSP method; if the OCSP server is unavailable, it uses the CRL method.

- **Certificate Revocation List (CRL)**
- **Online Certificate Status Protocol (OCSP)**

In PAN-OS, certificate revocation status verification is an optional feature. It is a best practice to enable it for certificate profiles, which define user and device authentication for Captive Portal, GlobalProtect, site-to-site IPSec VPN, and web interface access to the firewall or Panorama.

### Certificate Revocation List (CRL)

Each certificate authority (CA) periodically issues a certificate revocation list (CRL) to a public repository. The CRL identifies revoked certificates by serial number. After the CA revokes a certificate, the next CRL update will include the serial number of that certificate.

The Palo Alto Networks firewall downloads and caches the last-issued CRL for every CA listed in the trusted CA list of the firewall. Caching only applies to validated certificates; if a firewall never validated a certificate, the firewall cache does not store the CRL for the issuing CA. Also, the cache only stores a CRL until it expires.

The firewall supports CRLs only in Distinguished Encoding Rules (DER) format. If the firewall downloads a CRL in any other format—for example, Privacy Enhanced Mail (PEM) format—any revocation verification process that uses that CRL will fail when a user performs an activity that triggers the process (for example, sending outbound SSL data). The firewall will generate a system log for the verification failure. If the verification was for an SSL certificate, the firewall will also display the SSL Certificate Errors Notify response page to the user.

To use CRLs for verifying the revocation status of certificates used for the decryption of inbound and outbound SSL/TLS traffic, see [Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption](#).

To use CRLs for verifying the revocation status of certificates that authenticate users and devices, configure a certificate profile and assign it to the interfaces that are specific to the application: Captive Portal, GlobalProtect (remote user-to-site or large scale), site-to-site IPSec VPN, or web interface access to Palo Alto Networks firewalls or Panorama. For details, see [Configure Revocation Status Verification of Certificates](#).
Online Certificate Status Protocol (OCSP)

When establishing an SSL/TLS session, clients can use Online Certificate Status Protocol (OCSP) to check the revocation status of the authentication certificate. The authenticating client sends a request containing the serial number of the certificate to the OCSP responder (server). The responder searches the database of the certificate authority (CA) that issued the certificate and returns a response containing the status (good, revoked or unknown) to the client. The advantage of the OCSP method is that it can verify status in real-time, instead of depending on the issue frequency (hourly, daily, or weekly) of CRLs.

The Palo Alto Networks firewall downloads and caches OCSP status information for every CA listed in the trusted CA list of the firewall. Caching only applies to validated certificates; if a firewall never validated a certificate, the firewall cache does not store the OCSP information for the issuing CA. If your enterprise has its own public key infrastructure (PKI), you can configure the firewall as an OCSP responder (see Configure an OCSP Responder).

To use OCSP for verifying the revocation status of certificates when the firewall functions as an SSL forward proxy, perform the steps under Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption.

The following applications use certificates to authenticate users and/or devices: Captive Portal, GlobalProtect (remote user-to-site or large scale), site-to-site IPSec VPN, and web interface access to Palo Alto Networks firewalls or Panorama. To use OCSP for verifying the revocation status of the certificates:

- Configure an OCSP responder (if you are configuring the firewall as an OCSP responder).
- Enable the HTTP OCSP service on the firewall (if you are configuring the firewall as an OCSP responder).
- Create or obtain a certificate for each application.
- Configure a certificate profile for each application.
- Assign the certificate profile to the relevant application.

To cover situations where the OCSP responder is unavailable, configure CRL as a fall-back method. For details, see Configure Revocation Status Verification of Certificates.
Certificate Deployment

The basic approaches to deploy certificates for Palo Alto Networks firewalls or Panorama are:

- **Obtain certificates from a trusted third-party CA**—The benefit of obtaining a certificate from a trusted third-party certificate authority (CA) such as VeriSign or GoDaddy is that end clients will already trust the certificate because common browsers include root CA certificates from well-known CAs in their trusted root certificate stores. Therefore, for applications that require end clients to establish secure connections with the firewall or Panorama, purchase a certificate from a CA that the end clients trust to avoid having to pre-deploy root CA certificates to the end clients. (Some such applications are a GlobalProtect portal or GlobalProtect Mobile Security Manager.) However, note that most third-party CAs cannot issue signing certificates. Therefore, this type of certificate is not appropriate for applications (for example, SSL/TLS decryption and large-scale VPN) that require the firewall to issue certificates. See [Obtain a Certificate from an External CA](#).

- **Obtain certificates from an enterprise CA**—Enterprises that have their own internal CA can use it to issue certificates for firewall applications and import them onto the firewall. The benefit is that end clients probably already trust the enterprise CA. You can either generate the needed certificates and import them onto the firewall, or generate a certificate signing request (CSR) on the firewall and send it to the enterprise CA for signing. The benefit of this method is that the private key does not leave the firewall. An enterprise CA can also issue a signing certificate, which the firewall uses to automatically generate certificates (for example, for GlobalProtect large-scale VPN or sites requiring SSL/TLS decryption). See [Import a Certificate and Private Key](#).

- **Generate self-signed certificates**—You can [Create a Self-Signed Root CA Certificate](#) on the firewall and use it to automatically issue certificates for other firewall applications. Note that if you use this method to generate certificates for an application that requires an end client to trust the certificate, end users will see a certificate error because the root CA certificate is not in their trusted root certificate store. To prevent this, deploy the self-signed root CA certificate to all end user systems. You can deploy the certificates manually or use a centralized deployment method such as an Active Directory Group Policy Object (GPO).
Set Up Verification for Certificate Revocation Status

To verify the revocation status of certificates, the firewall uses Online Certificate Status Protocol (OCSP) and/or certificate revocation lists (CRLs). For details on these methods, see Certificate Revocation. If you configure both methods, the firewall first tries OCSP and only falls back to the CRL method if the OCSP responder is unavailable. If your enterprise has its own public key infrastructure (PKI), you can configure the firewall to function as the OCSP responder.

The following topics describe how to configure the firewall to verify certificate revocation status:

- Configure an OCSP Responder
- Configure Revocation Status Verification of Certificates
- Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption

Configure an OCSP Responder

To use Online Certificate Status Protocol (OCSP) for verifying the revocation status of certificates, you must configure the firewall to access an OCSP responder (server). The entity that manages the OCSP responder can be a third-party certificate authority (CA) or, if your enterprise has its own public key infrastructure (PKI), the firewall itself. For details on OCSP, see Certificate Revocation.

### Configure an OCSP Responder

**Step 1** Define an external OCSP responder or configure the firewall itself as an OCSP responder.

2. Enter a Name to identify the responder (up to 31 characters). The name is case-sensitive. It must be unique and use only letters, numbers, spaces, hyphens, and underscores.
3. If the firewall has more than one virtual system (vsys), select a Location (vsys or Shared) for the certificate.
4. In the Host Name field, enter the host name (recommended) or IP address of the OCSP responder. From this value, PAN-OS automatically derives a URL and adds it to the certificate being verified.
   
   If you configure the firewall itself as an OCSP responder, the host name must resolve to an IP address in the interface that the firewall uses for OCSP services.
5. Click OK.

**Step 2** If you want the firewall to use the management interface for the OCSP responder, enable OCSP communication on the firewall. Otherwise, continue to the next step to configure an alternate interface.

1. Select Device > Setup > Management.
2. In the Management Interface Settings section, edit to select the HTTP OCSP check box, then click OK.
Set Up Verification for Certificate Revocation Status

Configure Revocation Status Verification of Certificates

The firewall and Panorama use certificates to authenticate users and devices for such applications as Captive Portal, GlobalProtect, site-to-site IPSec VPN, and web interface access to the firewall/Panorama. To improve security, it is a best practice to configure the firewall or Panorama to verify the revocation status of certificates that it uses for device/user authentication.

Configure Revocation Status Verification of Certificates

Step 1 Configure a Certificate Profile for each application. Assign one or more root CA certificates to the profile and select how the firewall verifies certificate revocation status.

For details on the certificates that various applications use, see Keys and Certificates.

Step 2 Assign the certificate profiles to the relevant applications. The steps to assign a certificate profile depend on the application that requires it.

Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption

The firewall decrypts inbound and outbound SSL/TLS traffic to apply security rules and rules, then re-encrypts the traffic before forwarding it. (For details, see SSL Inbound Inspection and SSL Forward Proxy.) You can configure the firewall to verify the revocation status of certificates used for decryption as follows.

Enabling revocation status verification for SSL/TLS decryption certificates will add time to the process of establishing the session. The first attempt to access a site might fail if the verification does not finish before the session times out. For these reasons, verification is disabled by default.

Configure an OCSP Responder

Step 3 To use an alternate interface as the OCSP responder, add an Interface Management Profile to the interface used for OCSP services.

1. Select Network > Network Profiles > Interface Mgmt.
2. Click Add to create a new profile or click the name of an existing profile.
3. Select the HTTP OCSP check box and click OK.
4. Select Network > Interfaces and click the name of the interface that the firewall will use for OCSP services. The OCSP Host Name specified in Step 1 must resolve to an IP address in this interface.
5. Select Advanced > Other info and select the Interface Management Profile you configured.
6. Click OK and Commit.
Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Define the service-specific timeout intervals for revocation status requests.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select <strong>Device &gt; Setup &gt; Session</strong> and, in the Session Features section, select <strong>Decryption Certificate Revocation Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Perform one or both of the following steps, depending on whether the firewall will use <strong>Online Certificate Status Protocol (OCSP)</strong> or the <strong>Certificate Revocation List (CRL)</strong> method to verify the revocation status of certificates. If the firewall will use both, it first tries OCSP; if the OCSP responder is unavailable, the firewall then tries the CRL method.</td>
</tr>
<tr>
<td></td>
<td>• In the CRL section, select the <strong>Enable</strong> check box and enter the <strong>Receive Timeout</strong>. This is the interval (1-60 seconds) after which the firewall stops waiting for a response from the CRL service.</td>
</tr>
<tr>
<td></td>
<td>• In the OCSP section, select the <strong>Enable</strong> check box and enter the <strong>Receive Timeout</strong>. This is the interval (1-60 seconds) after which the firewall stops waiting for a response from the OCSP responder.</td>
</tr>
<tr>
<td></td>
<td>Depending on the <strong>Certificate Status Timeout</strong> value you specify in <strong>Step 2</strong>, the firewall might register a timeout before either or both of the <strong>Receive Timeout</strong> intervals pass.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Define the total timeout interval for revocation status requests.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enter the <strong>Certificate Status Timeout</strong>. This is the interval (1-60 seconds) after which the firewall stops waiting for a response from any certificate status service and applies the session-blocking logic you optionally define in <strong>Step 3</strong>. The <strong>Certificate Status Timeout</strong> relates to the OCSP/CRL <strong>Receive Timeout</strong> as follows:</td>
</tr>
<tr>
<td></td>
<td>• If you enable both OCSP and CRL—The firewall registers a request timeout after the lesser of two intervals passes: the <strong>Certificate Status Timeout</strong> value or the aggregate of the two <strong>Receive Timeout</strong> values.</td>
</tr>
<tr>
<td></td>
<td>• If you enable only OCSP—The firewall registers a request timeout after the lesser of two intervals passes: the <strong>Certificate Status Timeout</strong> value or the OCSP <strong>Receive Timeout</strong> value.</td>
</tr>
<tr>
<td></td>
<td>• If you enable only CRL—The firewall registers a request timeout after the lesser of two intervals passes: the <strong>Certificate Status Timeout</strong> value or the CRL <strong>Receive Timeout</strong> value.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Define the blocking behavior for <strong>unknown</strong> certificate status or a revocation status request timeout.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you want the firewall to block SSL/TLS sessions when the OCSP or CRL service returns a certificate revocation status of <strong>unknown</strong>, select the <strong>Block Session With Unknown Certificate Status</strong> check box. Otherwise, the firewall proceeds with the session.</td>
</tr>
<tr>
<td></td>
<td>If you want the firewall to block SSL/TLS sessions after it registers a request timeout, select the <strong>Block Session On Certificate Status Check Timeout</strong> check box. Otherwise, the firewall proceeds with the session.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Save and apply your entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click <strong>OK</strong> and <strong>Commit</strong>.</td>
</tr>
</tbody>
</table>
Configure the Master Key

Every firewall and Panorama management server has a default master key that encrypts all the private keys and passwords in the configuration to secure them (such as the private key used for SSL Forward Proxy Decryption).

In a high availability (HA) configuration, ensure both firewalls or Panorama management servers in the pair use the same master key. If the master keys differ, HA configuration synchronization will not work properly. Additionally, if you are using Panorama to manage your firewalls, you must use the same master key on Panorama and all managed firewalls so that Panorama can push configurations to the firewalls.

Be sure to store the master key in a safe location. You cannot recover the master key and the only way to restore the default master key is to Reset the Firewall to Factory Default Settings.

<table>
<thead>
<tr>
<th>Configure a Master Key</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> (HA only) Select Device &gt; High Availability &gt; General, edit the Setup and disable (clear) the Enable HA setting. Click OK and Commit your configuration changes.</td>
</tr>
<tr>
<td>This step is required before you can deploy a new master key to a firewall HA pair. If you do not disable HA before deploying a new master key, Panorama will lose connectivity to the primary firewall.</td>
</tr>
<tr>
<td><strong>Step 1</strong> Select Device &gt; Master Key and Diagnostics and edit the Master Key section.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Enter the Current Master Key if one exists.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Define a new New Master Key and then Confirm New Master Key. The key must contain exactly 16 characters.</td>
</tr>
<tr>
<td><strong>Step 4</strong> To specify the master key Life Time, enter the number of Days and/or Hours after which the key will expire. You must configure a new master key before the current key expires. If the master key expires, the firewall or Panorama automatically reboots in Maintenance mode. You must then Reset the Firewall to Factory Default Settings.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Enter a Time for Reminder that specifies the number of Days and Hours before the master key expires when the firewall generates an expiration alarm. The firewall automatically opens the System Alarms dialog to display the alarm. To ensure the expiration alarm displays, select Device &gt; Log Settings, edit the Alarm Settings, and Enable Alarms.</td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) Select whether to use an HSM to encrypt the master key. For details, see Encrypt a Master Key Using an HSM.</td>
</tr>
<tr>
<td><strong>Step 7</strong> Click OK and Commit.</td>
</tr>
<tr>
<td><strong>Step 8</strong> (HA only) Select Device &gt; High Availability &gt; General, edit the Setup and Enable HA. Click OK and Commit your configuration changes.</td>
</tr>
</tbody>
</table>
Obtain Certificates

- Create a Self-Signed Root CA Certificate
- Generate a Certificate
- Import a Certificate and Private Key
- Obtain a Certificate from an External CA

Create a Self-Signed Root CA Certificate

A self-signed root certificate authority (CA) certificate is the top-most certificate in a certificate chain. A firewall can use this certificate to automatically issue certificates for other uses. For example, the firewall issues certificates for SSL/TLS decryption and for satellites in a GlobalProtect large-scale VPN.

When establishing a secure connection with the firewall, the remote client must trust the root CA that issued the certificate. Otherwise, the client browser will display a warning that the certificate is invalid and might (depending on security settings) block the connection. To prevent this, after generating the self-signed root CA certificate, import it into the client systems.

On a Palo Alto Networks firewall or Panorama, you can generate self-signed certificates only if they are CA certificates.

Generate a Self-signed Root CA Certificate

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates.</td>
</tr>
<tr>
<td>2</td>
<td>If the firewall has more than one virtual system (vsys), select a Location (vsys or Shared) for the certificate.</td>
</tr>
<tr>
<td>3</td>
<td>Click Generate.</td>
</tr>
<tr>
<td>4</td>
<td>Enter a Certificate Name, such as GlobalProtect_CA. The name is case-sensitive and can have up to 63 characters on the firewall or up to 31 characters on Panorama. It must be unique and use only letters, numbers, hyphens, and underscores.</td>
</tr>
<tr>
<td>5</td>
<td>In the Common Name field, enter the FQDN (recommended) or IP address of the interface where you will configure the service that will use this certificate.</td>
</tr>
<tr>
<td>6</td>
<td>If the firewall has more than one vsys and you want the certificate to be available to every vsys, select the Shared check box.</td>
</tr>
<tr>
<td>7</td>
<td>Leave the Signed By field blank to designate the certificate as self-signed.</td>
</tr>
<tr>
<td>8</td>
<td>(Required) Select the Certificate Authority check box.</td>
</tr>
<tr>
<td>9</td>
<td>Leave the OCSP Responder field blank; revocation status verification doesn't apply to root CA certificates.</td>
</tr>
<tr>
<td>10</td>
<td>Click Generate and Commit.</td>
</tr>
</tbody>
</table>
Obtain Certificates
Certificate Management

Generate a Certificate

Palo Alto Networks firewalls and Panorama use certificates to authenticate clients, servers, users, and devices in several applications, including SSL/TLS decryption, Captive Portal, GlobalProtect, site-to-site IPSec VPN, and web interface access to the firewall/Panorama. Generate certificates for each usage: for details, see Keys and Certificates.

To generate a certificate, you must first Create a Self-Signed Root CA Certificate or import one (Import a Certificate and Private Key) to sign it. To use Online Certificate Status Protocol (OCSP) for verifying certificate revocation status, Configure an OCSP Responder before generating the certificate.

Generate a Certificate

Step 1 Select Device > Certificate Management > Certificates > Device Certificates.

Step 2 If the firewall has more than one virtual system (vsys), select a Location (vsys or Shared) for the certificate.

Step 3 Click Generate.

Step 4 Select Local (default) as the Certificate Type unless you want to deploy SCEP certificates to GlobalProtect clients.

Step 5 Enter a Certificate Name. The name is case-sensitive and can have up to 63 characters on the firewall or up to 31 characters on Panorama. It must be unique and use only letters, numbers, hyphens, and underscores.

Step 6 In the Common Name field, enter the FQDN (recommended) or IP address of the interface where you will configure the service that will use this certificate.

Step 7 If the firewall has more than one vsys and you want the certificate to be available to every vsys, select the Shared check box.

Step 8 In the Signed By field, select the root CA certificate that will issue the certificate.

Step 9 (Optional) Select an OCSP Responder.

Step 10 For the key generation Algorithm, select RSA (default) or Elliptical Curve DSA (ECDSA). ECDSA is recommended for client browsers and operating systems that support it.

Firewalls that run PAN-OS 6.1 and earlier releases will delete any ECDSA certificates that you push from Panorama™, and any RSA certificates signed by an ECDSA certificate authority (CA) will be invalid on those firewalls.

Step 11 Select the Number of Bits to define the certificate key length. Higher numbers are more secure but require more processing time.

Step 12 Select the Digest algorithm. From most to least secure, the options are: sha512, sha384, sha256 (default), sha1, and md5.

Client certificates that are used when requesting firewall services that rely on TLSv1.2 (such as administrator access to the web interface) cannot have sha384 (in releases before PAN-OS 7.1.8) or sha512 as a digest algorithm. The client certificates must use a lower digest algorithm or you must limit the Max Version to TLSv1.1 when you Configure an SSL/TLS Service Profile for the firewall services.

Step 13 For the Expiration, enter the number of days (default is 365) for which the certificate is valid.

Step 14 (Optional) Add the Certificate Attributes to uniquely identify the firewall and the service that will use the certificate.

If you add a Host Name (DNS name) attribute, it is a best practice for it to match the Common Name. The host name populates the Subject Alternative Name field of the certificate.
Obtain Certificates

Certificate Management

Import a Certificate and Private Key

If your enterprise has its own public key infrastructure (PKI), you can import a certificate and private key into the firewall from your enterprise certificate authority (CA). Enterprise CA certificates (unlike most certificates purchased from a trusted, third-party CA) can automatically issue CA certificates for applications such as SSL/TLS decryption or large-scale VPN.

On a Palo Alto Networks firewall or Panorama, you can import self-signed certificates only if they are CA certificates.

Instead of importing a self-signed root CA certificate into all the client systems, it is a best practice to import a certificate from the enterprise CA because the clients will already have a trust relationship with the enterprise CA, which simplifies the deployment.

If the certificate you will import is part of a certificate chain, it is a best practice to import the entire chain.

Import a Certificate and Private Key

Step 1 From the enterprise CA, export the certificate and private key that the firewall will use for authentication. When exporting a private key, you must enter a passphrase to encrypt the key for transport. Ensure the management system can access the certificate and key files. When importing the key onto the firewall, you must enter the same passphrase to decrypt it.

Step 2 Select Device > Certificate Management > Certificates > Device Certificates.

Step 3 If the firewall has more than one virtual system (vsys), select a Location (vsys or Shared) for the certificate.

Step 4 Click Import and enter a Certificate Name. The name is case-sensitive and can have up to 63 characters on the firewall or up to 31 characters on Panorama. It must be unique and use only letters, numbers, hyphens, and underscores.

Step 5 To make the certificate available to all virtual systems, select the Shared check box. This check box appears only if the firewall supports multiple virtual systems.

Step 6 Enter the path and name of the Certificate File received from the CA, or Browse to find the file.
Obtain a Certificate from an External CA

The advantage of obtaining a certificate from an external certificate authority (CA) is that the private key does not leave the firewall. To obtain a certificate from an external CA, generate a certificate signing request (CSR) and submit it to the CA. After the CA issues a certificate with the specified attributes, import it onto the firewall. The CA can be a well-known, public CA or an enterprise CA.

To use Online Certificate Status Protocol (OCSP) for verifying the revocation status of the certificate, **Configure an OCSP Responder before** generating the CSR.

---

**Obtain Certificates**

**Certificate Management**

**Import a Certificate and Private Key**

**Step 7** Select a File Format:

- **Encrypted Private Key and Certificate (PKCS12)**—This is the default and most common format, in which the key and certificate are in a single container (Certificate File). If a hardware security module (HSM) will store the private key for this certificate, select the **Private key resides on Hardware Security Module** check box.

- **Base64 Encoded Certificate (PEM)**—You must import the key separately from the certificate. If a hardware security module (HSM) stores the private key for this certificate, select the **Private key resides on Hardware Security Module** check box and skip the next step. Otherwise, select the **Import Private Key** check box, enter the **Key File** or **Browse** to it, then continue to the next step.

---

**Step 8** Enter and re-enter (confirm) the **Passphrase** used to encrypt the private key.

---

**Step 9** Click **OK**. The Device Certificates page displays the imported certificate.
## Obtain a Certificate from an External CA

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Request the certificate from an external CA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>If the firewall has more than one virtual system (vsys), select a <strong>Location</strong> (vsys or <strong>Shared</strong>) for the certificate.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Generate</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter a <strong>Certificate Name</strong>. The name is case-sensitive and can have up to 63 characters on the firewall or up to 31 characters on Panorama. It must be unique and use only letters, numbers, hyphens, and underscores.</td>
</tr>
<tr>
<td>5.</td>
<td>In the <strong>Common Name</strong> field, enter the FQDN (recommended) or IP address of the interface where you will configure the service that will use this certificate.</td>
</tr>
<tr>
<td>6.</td>
<td>If the firewall has more than one vsys and you want the certificate to be available to every vsys, select the <strong>Shared</strong> check box.</td>
</tr>
<tr>
<td>7.</td>
<td>In the <strong>Signed By</strong> field, select <strong>External Authority (CSR)</strong>.</td>
</tr>
<tr>
<td>8.</td>
<td>If applicable, select an <strong>OCSP Responder</strong>.</td>
</tr>
<tr>
<td>9.</td>
<td><strong>(Optional)</strong> Add the <strong>Certificate Attributes</strong> to uniquely identify the firewall and the service that will use the certificate. If you add a <strong>Host Name</strong> attribute, it is a best practice for it to match the <strong>Common Name</strong> (this is mandatory for GlobalProtect). The host name populates the Subject Alternative Name field of the certificate.</td>
</tr>
<tr>
<td>10.</td>
<td>Click <strong>Generate</strong>. The Device Certificates tab displays the CSR with a Status of <strong>pending</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Submit the CSR to the CA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the CSR and click <strong>Export</strong> to save the .csr file to a local computer.</td>
</tr>
<tr>
<td>2.</td>
<td>Upload the .csr file to the CA.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Import the certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>After the CA sends a signed certificate in response to the CSR, return to the <strong>Device Certificates</strong> tab and click <strong>Import</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter the <strong>Certificate Name</strong> used to generate the CSR.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter the path and name of the PEM <strong>Certificate File</strong> that the CA sent, or <strong>Browse</strong> to it.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK</strong>. The <strong>Device Certificates</strong> tab displays the certificate with a Status of <strong>valid</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Configure the certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click the certificate <strong>Name</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the check boxes that correspond to the intended use of the certificate on the firewall. For example, if the firewall will use this certificate to secure forwarding of syslogs to an external syslog server, select the <strong>Certificate for Secure Syslog</strong> check box.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>OK</strong> and <strong>Commit</strong>.</td>
</tr>
</tbody>
</table>
Export a Certificate and Private Key

Palo Alto Networks recommends that you use your enterprise public key infrastructure (PKI) to distribute a certificate and private key in your organization. However, if necessary, you can also export a certificate and private key from the firewall or Panorama. You can use an exported certificate and private key in the following cases:

- Configure Certificate-Based Administrator Authentication to the Web Interface
- GlobalProtect agent/app authentication to portals and gateways
- SSL Forward Proxy decryption
- Obtain a Certificate from an External CA

### Export a Certificate and Private Key

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates.</strong></td>
</tr>
<tr>
<td>2</td>
<td>If the firewall has more than one virtual system (vsys), select a <strong>Location</strong> (a specific vsys or <strong>Shared</strong>) for the certificate.</td>
</tr>
</tbody>
</table>
| 3    | Select the certificate, click **Export**, and select a **File Format**:  
  - **Base64 Encoded Certificate (PEM)**—This is the default format. It is the most common and has the broadest support on the Internet. If you want the exported file to include the private key, select the **Export Private Key** check box.  
  - **Encrypted Private Key and Certificate (PKCS12)**—This format is more secure than PEM but is not as common or as broadly supported. The exported file will automatically include the private key.  
  - **Binary Encoded Certificate (DER)**—More operating system types support this format than the others. You can export only the certificate, not the key: ignore the **Export Private Key** check box and passphrase fields. |
| 4    | Enter a **Passphrase** and **Confirm Passphrase** to encrypt the private key if the **File Format** is PKCS12 or if it is PEM and you selected the **Export Private Key** check box. You will use this passphrase when importing the certificate and key into client systems. |
| 5    | Click **OK** and save the certificate/key file to your computer. |
Configure a Certificate Profile

Certificate profiles define user and device authentication for Captive Portal, GlobalProtect, site-to-site IPSec VPN, Mobile Security Manager, and web interface access to Palo Alto Networks firewalls or Panorama. The profiles specify which certificates to use, how to verify certificate revocation status, and how that status constrains access. Configure a certificate profile for each application.

It is a best practice to enable Online Certificate Status Protocol (OCSP) and/or Certificate Revocation List (CRL) status verification for certificate profiles. For details on these methods, see Certificate Revocation.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Obtain the certificate authority (CA) certificates you will assign.</th>
<th>Perform one of the following steps to obtain the CA certificates you will assign to the profile. You must assign at least one.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Generate a Certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Export a certificate from your enterprise CA and then import it onto the firewall (see Step 3).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Identify the certificate profile.</th>
<th>1. Select Device &gt; Certificate Management &gt; Certificates Profile and click Add.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. Enter a Name to identify the profile. The name is case-sensitive, must be unique and can use up to 63 characters on the firewall or up to 31 characters on Panorama that include only letters, numbers, spaces, hyphens, and underscores.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. If the firewall has more than one virtual system (vsys), select a Location (vsys or Shared) for the certificate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Assign one or more certificates.</th>
<th>Perform the following steps for each CA certificate:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1. In the CA Certificates table, click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select a CA Certificate. Alternatively, to import a certificate, click Import, enter a Certificate Name, Browse to the Certificate File you exported from your enterprise CA, and click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. (Optional) If the firewall uses OCSP to verify certificate revocation status, configure the following fields to override the default behavior. For most deployments, these fields do not apply.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• By default, the firewall uses the Authority Information Access (AIA) information from the certificate. To override the AIA information, enter a Default OCSP URL (starting with http:// or https://).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• By default, the firewall uses the certificate selected in the CA Certificate field to validate OCSP responses. To use a different certificate for validation, select it in the OCSP Verify CA Certificate field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click OK. The CA Certificates table displays the assigned certificate.</td>
</tr>
</tbody>
</table>
Step 4 Define the methods for verifying certificate revocation status and the associated blocking behavior.

1. Select **Use CRL** and/or **Use OCSP**. If you select both, the firewall first tries OCSP and falls back to the CRL method only if the OCSP responder is unavailable.

2. Depending on the verification method, enter the **CRL Receive Timeout** and/or **OCSP Receive Timeout**. These are the intervals (1-60 seconds) after which the firewall stops waiting for a response from the CRL/OCSP service.

3. Enter the **Certificate Status Timeout**. This is the interval (1-60 seconds) after which the firewall stops waiting for a response from any certificate status service and applies any session-blocking logic you define. The Certificate Status Timeout relates to the OCSP/CRL Receive Timeout as follows:
   - If you enable both OCSP and CRL—The firewall registers a request timeout after the lesser of two intervals passes: the Certificate Status Timeout value or the aggregate of the two Receive Timeout values.
   - If you enable only OCSP—The firewall registers a request timeout after the lesser of two intervals passes: the Certificate Status Timeout value or the OCSP Receive Timeout value.
   - If you enable only CRL—The firewall registers a request timeout after the lesser of two intervals passes: the Certificate Status Timeout value or the CRL Receive Timeout value.

4. If you want the firewall to block sessions when the OCSP or CRL service returns a certificate revocation status of **unknown**, select the Block session if certificate status is unknown check box. Otherwise, the firewall proceeds with the session.

5. If you want the firewall to block sessions after it registers an OCSP or CRL request timeout, select the Block session if certificate status cannot be retrieved within timeout check box. Otherwise, the firewall proceeds with the session.

6. (GlobalProtect only) If you want the firewall to block sessions when the serial number attribute in the subject of the client certificate does not match the host ID that the GlobalProtect agent reports for the client endpoint, select Block sessions if the certificate was not issued to the authenticating device.

Step 5 Save and apply your entries. Click **OK** and **Commit**.
Configure an SSL/TLS Service Profile

Palo Alto Networks firewalls and Panorama use SSL/TLS service profiles to specify a certificate and the allowed protocol versions for SSL/TLS services. The firewall and Panorama use SSL/TLS for Captive Portal, GlobalProtect portals and gateways, inbound traffic on the management (MGT) interface, the URL Admin Override feature, and the User-ID™ syslog listening service. By defining the protocol versions, you can use a profile to restrict the cipher suites that are available for securing communication with the clients requesting the services. This improves network security by enabling the firewall or Panorama to avoid SSL/TLS versions that have known weaknesses. If a service request involves a protocol version that is outside the specified range, the firewall or Panorama downgrades or upgrades the connection to a supported version.

In the client systems that request firewall services, the certificate trust list (CTL) must include the certificate authority (CA) certificate that issued the certificate specified in the SSL/TLS service profile. Otherwise, users will see a certificate error when requesting firewall services. Most third-party CA certificates are present by default in client browsers. If an enterprise or firewall-generated CA certificate is the issuer, you must deploy that CA certificate to the CTL in client browsers.

Configure an SSL/TLS Service Profile

Step 1  For each desired service, generate or import a certificate on the firewall (see Obtain Certificates).
Use only signed certificates, not CA certificates, in SSL/TLS service profiles.

Step 2  Select Device > Certificate Management > SSL/TLS Service Profile.

Step 3  If the firewall has more than one virtual system (vsys), select the Location (vsys or Shared) where the profile is available.

Step 4  Click Add and enter a Name to identify the profile.

Step 5  Select the Certificate you just obtained.

Step 6  Define the range of protocols that the service can use:
• For the Min Version, select the earliest allowed TLS version: TLSv1.0 (default), TLSv1.1, or TLSv1.2.
• For the Max Version, select the latest allowed TLS version: TLSv1.0, TLSv1.1, TLSv1.2, or Max (latest available version). The default is Max.

Client certificates that are used when requesting firewall services that rely on TLSv1.2 cannot have SHA384 (in releases before PAN-OS 7.1.8) or SHA512 as a digest algorithm. The client certificates must use a lower digest algorithm or you must limit the Max Version to TLSv1.1 for the firewall service.

Step 7  Click OK and Commit.
Replace the Certificate for Inbound Management Traffic

When you first boot up the firewall or Panorama, it automatically generates a default certificate that enables HTTPS access to the web interface and XML API over the management (MGT) interface and (on the firewall only) over any other interface that supports HTTPS management traffic (for details, see Use Interface Management Profiles to Restrict Access). To improve the security of inbound management traffic, replace the default certificate with a new certificate issued specifically for your organization.

You cannot view, modify, or delete the default certificate.

Securing management traffic also involves configuring how administrators authenticate to the firewall or to Panorama.

Step 1 Obtain the certificate that will authenticate the firewall or Panorama to the client systems of administrators.

You can simplify your Certificate Deployment by using a certificate that the client systems already trust. Therefore, we recommend that you Import a Certificate and Private Key from your enterprise certificate authority (CA) or Obtain a Certificate from an External CA; the trusted root certificate store of the client systems is likely to already have the associated root CA certificate that ensures trust.

If you Generate a Certificate on the firewall or Panorama, administrators will see a certificate error because the root CA certificate is not in the trusted root certificate store of client systems. To prevent this, deploy the self-signed root CA certificate to all client systems.

Regardless of how you obtain the certificate, we recommend a Digest algorithm of sha256 or higher for enhanced security.

Step 2 Configure an SSL/TLS Service Profile.

Select the Certificate you just obtained.

For enhanced security, we recommend that you set the Min Version (earliest allowed TLS version) to TLSv1.1 for inbound management traffic. We also recommend that you use a different SSL/TLS Service Profile for each firewall or Panorama service instead of reusing this profile for all services.

Step 3 Apply the SSL/TLS Service Profile to inbound management traffic.

2. Select the SSL/TLS Service Profile you just configured.
3. Click OK and Commit.
Configure the Key Size for SSL Forward Proxy Server Certificates

When responding to a client in an SSL Forward Proxy session, the firewall creates a copy of the certificate that the destination server presents and uses the copy to establish a connection with the client. By default, the firewall generates certificates with the same key size as the certificate that the destination server presented. However, you can change the key size for the firewall-generated certificate as follows:

**Configure the Key Size for SSL Forward Proxy Server Certificates**

**Step 1** Select Device > Setup > Session and, in the Decryption Settings section, click SSL Forward Proxy Settings.

**Step 2** Select a Key Size:

- **Defined by destination host**—The firewall determines the key size for the certificates it generates to establish SSL proxy sessions with clients based on the key size of the destination server certificate. If the destination server uses a 1024-bit RSA key, the firewall generates a certificate with that key size and an SHA-1 hashing algorithm. If the destination server uses a key size larger than 1,024 bits (for example, 2,048 bits or 4,096 bits), the firewall generates a certificate that uses a 2,048-bit RSA key and SHA-256 algorithm. This is the default setting.

- **1024-bit RSA**—The firewall generates certificates that use a 1,024-bit RSA key and SHA-1 hashing algorithm regardless of the key size of the destination server certificates. As of December 31, 2013, public certificate authorities (CAs) and popular browsers have limited support for X.509 certificates that use keys of fewer than 2,048 bits. In the future, depending on security settings, when presented with such keys the browser might warn the user or block the SSL/TLS session entirely.

- **2048-bit RSA**—The firewall generates certificates that use a 2,048-bit RSA key and SHA-256 hashing algorithm regardless of the key size of the destination server certificates. Public CAs and popular browsers support 2,048-bit keys, which provide better security than the 1,024-bit keys.

- **Changing the key size setting clears the current certificate cache.**

**Step 3** Click OK and Commit.
Revoke and Renew Certificates

Revoke a Certificate

Various circumstances can invalidate a certificate before the expiration date. Some examples are a change of name, change of association between subject and certificate authority (for example, an employee terminates employment), and compromise (known or suspected) of the private key. Under such circumstances, the certificate authority (CA) that issued the certificate must revoke it. The following task describes how to revoke a certificate for which the firewall is the CA.

**Revoke a Certificate**

**Step 1** Select Device > Certificate Management > Certificates > Device Certificates.

**Step 2** If the firewall supports multiple virtual systems, the tab displays a **Location** drop-down. Select the virtual system to which the certificate belongs.

**Step 3** Select the certificate to revoke.

**Step 4** Click **Revoke**. PAN-OS immediately sets the status of the certificate to revoked and adds the serial number to the Online Certificate Status Protocol (OCSP) responder cache or certificate revocation list (CRL). You need not perform a commit.

Renew a Certificate

If a certificate expires, or soon will, you can reset the validity period. If an external certificate authority (CA) signed the certificate and the firewall uses the Online Certificate Status Protocol (OCSP) to verify certificate revocation status, the firewall uses the OCSP responder information to update the certificate status (see Configure an OCSP Responder). If the firewall is the CA that issued the certificate, the firewall replaces it with a new certificate that has a different serial number but the same attributes as the old certificate.

**Renew a Certificate**

**Step 1** Select Device > Certificate Management > Certificates > Device Certificates.

**Step 2** If the firewall has more than one virtual system (vsys), select a **Location** (vsys or Shared) for the certificate.

**Step 3** Select a certificate to renew and click **Renew**.

**Step 4** Enter a **New Expiration Interval** (in days).

**Step 5** Click **OK** and **Commit**.
Secure Keys with a Hardware Security Module

A hardware security module (HSM) is a physical device that manages digital keys. An HSM provides secure storage and generation of digital keys. It provides both logical and physical protection of these materials from non-authorized use and potential adversaries.

HSM clients integrated with Palo Alto Networks firewalls or Panorama enable enhanced security for the private keys used in SSL/TLS decryption (both SSL forward proxy and SSL inbound inspection). In addition, you can use the HSM to encrypt master keys.

The following topics describe how to integrate an HSM with your firewall or Panorama:

- Set up Connectivity with an HSM
- Encrypt a Master Key Using an HSM
- Store Private Keys on an HSM
- Manage the HSM Deployment

Set up Connectivity with an HSM

HSM clients are integrated with PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, and VM-Series firewalls and with the Panorama management server (virtual appliance and M-Series appliances) for use with the following HSM vendors.

- **SafeNet Network**—The supported client versions depend on the PAN-OS release:
  - PAN-OS 7.1 releases and earlier releases (also PAN-OS 8.0 releases)—SafeNet Network client version 5.2.1.
  - PAN-OS 7.1.10 and later PAN-OS 7.1 releases (also PAN-OS 8.0.2 and later PAN-OS 8.0 releases)—SafeNet Network client version 5.2.1, 5.4.2, and 6.2.2. On the firewall or Panorama, use the request hsm client-version CLI command to select the version that is compatible with your SafeNet HSM server.

- **Thales nShield Connect**—All PAN-OS releases support client version 11.62.

The HSM server version must be compatible with these client versions. Refer to the HSM vendor documentation for the client-server version compatibility matrix.

- Set Up Connectivity with a SafeNet Network HSM
- Set Up Connectivity with a Thales nShield Connect HSM

Set Up Connectivity with a SafeNet Network HSM

To set up connectivity between the Palo Alto Networks firewall (HSM client) and a SafeNet Network HSM server, you must specify the IP address of the server, enter a password for authenticating the firewall to the server, and register the firewall with the server. Before starting the configuration, make sure you created a partition for the firewall on the HSM server. To ensure the SafeNet Network client version on the firewall is compatible with your SafeNet Network server, see Set up Connectivity with an HSM.
Before the HSM and firewall connect, the HSM authenticates the firewall based on the firewall IP address. Therefore, you must configure the firewall to use a static IP address, not a dynamic address assigned through DHCP. Operations on the HSM would stop working if the firewall IP address changed during runtime.

Set up Connectivity with a SafeNet Network HSM

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Define connection settings for each SafeNet Network HSM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to the firewall web interface and select Device &gt; Setup &gt; HSM.</td>
</tr>
<tr>
<td>2.</td>
<td>Edit the Hardware Security Module Provider section and set the Provider Configured to SafeNet Network HSM.</td>
</tr>
<tr>
<td>3.</td>
<td>Add each HSM server as follows. A high availability (HA) HSM configuration requires two servers.</td>
</tr>
<tr>
<td></td>
<td>a. Enter a Module Name for the HSM server. This can be any ASCII string of up to 31 characters.</td>
</tr>
<tr>
<td></td>
<td>b. Enter an IPv4 address for the HSM Server Address.</td>
</tr>
<tr>
<td>4.</td>
<td>(HA only) Select High Availability, specify the Auto Recovery Retry value, and enter a High Availability Group Name.</td>
</tr>
<tr>
<td></td>
<td>If two HSM servers are configured, the best practice is to enable High Availability. Otherwise the second HSM server is not used.</td>
</tr>
<tr>
<td>5.</td>
<td>Click OK and Commit.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>(Optional) Configure a service route to connect to the HSM if you don't want the firewall to connect through the Management interface (default).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you configure a service route for the HSM, running the clear session all CLI command clears all existing HSM sessions, bringing all HSM states down and then up again. During the several seconds required for the HSM to recover, all SSL/TLS operations will fail.</td>
</tr>
<tr>
<td></td>
<td>1. Select Device &gt; Setup &gt; Services and click Service Route Configuration.</td>
</tr>
<tr>
<td></td>
<td>2. Customize a service route. The IPv4 tab is active by default.</td>
</tr>
<tr>
<td></td>
<td>3. Click HSM in the Service column.</td>
</tr>
<tr>
<td></td>
<td>4. Select a Source Interface for the HSM.</td>
</tr>
<tr>
<td></td>
<td>5. Click OK and Commit.</td>
</tr>
</tbody>
</table>
### Set up Connectivity with a SafeNet Network HSM (Continued)

**Step 3** Configure the firewall to authenticate to the HSM.
1. Select **Device > Setup > HSM** and **Setup Hardware Security Module**.
2. Select the HSM **Server Name**.
3. Enter the **Administrator Password** to authenticate the firewall to the HSM.
4. Click **OK**.
   - The firewall tries to authenticate to the HSM and displays a status message.
5. Click **OK**.

**Step 4** Register the firewall as an HSM client with the HSM server and assign the firewall to a partition on the HSM server.

1. Log in to the HSM from a remote system.
2. Register the firewall using the `client register -c <cl-name> -ip <fw-ip-addr>` command, where `<cl-name>` is a name that you assign to the firewall for use on the HSM and `<fw-ip-addr>` is the firewall IP address. The IP address must be static, not assigned through DHCP.
3. Assign a partition to the firewall using the `client assignpartition -c <cl-name> -p <partition-name>` command, where `<cl-name>` is the name assigned to the firewall in the `client register` command and `<partition-name>` is the name of a previously configured partition that you want to assign to the firewall.

**Step 5** Configure the firewall to connect to the HSM partition.
1. Select **Device > Setup > HSM** and click the Refresh 🔄 icon.
2. **Setup HSM Partition** in the Hardware Security Operations section.
3. Enter the **Partition Password** to authenticate the firewall to the partition on the HSM.
4. Click **OK**.

**Step 6** (HA only) Configure an additional HSM for HA.

- Repeat the previous authentication, registration, and partition connection steps to add an additional HSM to the existing HA group.
- If you remove an HSM from your configuration, repeat the previous partition connection step to remove the deleted HSM from the HA group.
Secure Keys with a Hardware Security Module

Certificate Management

Set up Connectivity with a Thales nShield Connect HSM

You must set up a remote filesystem (RFS) as a hub to synchronize key data for all the firewalls (HSM clients) in your organization that use the Thales nShield Connect HSM. To ensure the Thales nShield Connect client version on your firewalls is compatible with your Thales nShield Connect server, see Set up Connectivity with an HSM.

Before the HSM and firewalls connect, the HSM authenticates the firewalls based on their IP addresses. Therefore, you must configure the firewalls to use static IP addresses, not dynamic addresses assigned through DHCP. Operations on the HSM would stop working if the firewall IP addresses changed during runtime.

HSM configurations are not synchronized between high availability (HA) firewall peers. Consequently, you must configure the HSM separately on each peer. In active/passive HA deployments, you must manually perform one failover to individually configure and authenticate each HA peer to the HSM. After this initial manual failover, user interaction is not required for the failover function.

Set up Connectivity with a Thales nShield Connect HSM

Step 1  Define connection settings for each Thales nShield Connect HSM.

1. Log in to the firewall web interface and select Device > Setup > HSM.
2. Edit the Hardware Security Module Provider section and set the Provider Configured to Thales nShield Connect.
3. Add each HSM server as follows. A high availability (HA) HSM configuration requires two servers.
   a. Enter a Module Name for the server. This can be any ASCII string of up to 31 characters.
   b. Enter an IPv4 address for the HSM Server Address.
4. Enter an IPv4 address for the Remote Filesystem Address.
5. Click OK and Commit.
## Set up Connectivity with a Thales nShield Connect HSM (Continued)

### Step 2 (Optional)
Configure a service route to connect to the HSM if you don’t want the firewall to connect through the Management interface (default).

*If you configure a service route for the HSM, running the `clear session all` CLI command clears all existing HSM sessions, bringing all HSM states down and then up again. During the several seconds required for the HSM to recover, all SSL/TLS operations will fail.*

1. Select `Device > Setup > Services` and click `Service Route Configuration`.
2. Customize the service route. The IPv4 tab is active by default.
3. Click `HSM` in the Service column.
4. Select a `Source Interface` for HSM.
5. Click `OK` and `Commit`.

### Step 3
Register the firewall as an HSM client with the HSM server.

This step briefly describes the procedure for using the front panel interface of the Thales nShield Connect HSM. For more details, refer to the Thales documentation.

1. Log in to the front panel display of the Thales nShield Connect HSM unit.
2. Use the right-hand navigation button to select `System > System configuration > Client config > New client`.
3. Enter the firewall IP address.
4. Select `System > System configuration > Client config > Remote file system` and enter the IP address of the client computer where you set up the RFS.

### Step 4
Configure the RFS to accept connections from the firewall.

1. Log in to the RFS from a Linux client.
2. Obtain the electronic serial number (ESN) and the hash of the \( K_{NETI} \) key, which authenticates the HSM to clients, by running the `anonkneti <ip-address>` command, where `<ip-address>` is the IP address of the HSM.
   
   The following is an example:
   ```
   anonkneti 192.0.2.1
   B1E2-2D4C-E6A2 5a2e5107e70d525615a903f6391ad72b1c03352c
   ```
   
   In this example, `B1E2-2D4C-E6A2` is the ESN and `5a2e5107e70d525615a903f6391ad72b1c03352c` is the hash of the \( K_{NETI} \) key.
3. Use the following command from a superuser account to set up the RFS:
   ```
   rfs-setup --force <ip-address> <ESN> <hash-Kneti-key>
   ```
   The `<ip-address>` is the HSM IP address, `<ESN>` is the electronic serial number, and `<hash-Kneti-key>` is the hash of the \( K_{NETI} \) key.
   
   The following example uses the values obtained in this procedure:
   ```
   rfs-setup --force 192.0.2.1 B1E2-2D4C-E6A2 5a2e5107e70d525615a903f6391ad72b1c03352c
   ```
4. Use the following command to permit HSM client submissions on the RFS:
   ```
   rfs-setup --gang-client --write-noauth <FW-IPaddress>
   ```
   where `<FW-IPaddress>` is the firewall IP address.
Secure Keys with a Hardware Security Module

Encrypt a Master Key Using an HSM

A master key encrypts all private keys and passwords on the firewall and Panorama. If you have security requirements to store your private keys in a secure location, you can encrypt the master key using an encryption key that is stored on an HSM. The firewall or Panorama then requests the HSM to decrypt the master key whenever it is required to decrypt a password or private key on the firewall. Typically, the HSM is in a highly secure location that is separate from the firewall or Panorama for greater security.

The HSM encrypts the master key using a wrapping key. To maintain security, you must occasionally change (refresh) this wrapping key.

Firewalls configured in FIPS/CC mode do not support master key encryption using an HSM.

The following topics describe how to encrypt the master key initially and how to refresh the master key encryption:

- Encrypt the Master Key
- Refresh the Master Key Encryption
Encrypt the Master Key

If you have not previously encrypted the master key on a firewall, use the following procedure to encrypt it. Use this procedure for first time encryption of a key, or if you define a new master key and you want to encrypt it. If you want to refresh the encryption on a previously encrypted key, see Refresh the Master Key Encryption.

### Encrypt a Master Key Using an HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Device &gt; Master Key and Diagnostics</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Specify the key that is currently used to encrypt all of the private keys and passwords on the firewall in the <strong>Master Key</strong> field.</td>
</tr>
<tr>
<td>3</td>
<td>If changing the master key, enter the new master key and confirm.</td>
</tr>
</tbody>
</table>
| 4    | Select the **HSM** check box.  
  * **Life Time**—The number of days and hours after which the master key expires (range 1-730 days).  
  * **Time for Reminder**—The number of days and hours before expiration when the user is notified of the impending expiration (range 1–365 days).  |
| 5    | Click **OK**. |
Secure Keys with a Hardware Security Module

Certificate Management

Refresh the Master Key Encryption

As a best practice, periodically refresh the master key encryption by rotating the wrapping key that encrypts it. The frequency of the rotation depends on your application. The wrapping key resides on your HSM. The following command is the same for SafeNet Network and Thales nShield Connect HSMs.

Refresh the Master Key Encryption

Step 1 Use the following CLI command to rotate the wrapping key for the master key on an HSM:

> request hsm mkey-wrapping-key-rotation

If the master key is encrypted on the HSM, the CLI command will generate a new wrapping key on the HSM and encrypt the master key with the new wrapping key.

If the master key is not encrypted on the HSM, the CLI command will generate new wrapping key on the HSM for future use.

The old wrapping key is not deleted by this command.

Store Private Keys on an HSM

For added security, you can use an HSM to secure the private keys used in SSL/TLS decryption for:

- **SSL Forward Proxy**—The HSM can store the private key of the Forward Trust certificate that signs certificates in SSL/TLS forward proxy operations. The firewall will then send the certificates that it generates during such operations to the HSM for signing before forwarding the certificates to the client.

- **SSL Inbound Inspection**—The HSM can store the private keys for the internal servers for which you are performing SSL/TLS inbound inspection.

Store Private Keys on an HSM

Step 1 On the HSM, import or generate the certificate and private key used in your decryption deployment.

For instructions on importing or generating a certificate and private key on the HSM, refer to your HSM documentation.

Step 2 (Thales nShield Connect only) Synchronize the key data from the Thales nShield remote file system to the firewall.

Synchronization with the SafeNet Network HSM is automatic.

Step 3 Import the certificate that corresponds to the HSM-stored key onto the firewall.

1. Access the firewall web interface and select Device > Setup > HSM.
3. Select Device > Certificate Management > Certificates > Device Certificates and click Import.
4. Enter the Certificate Name.
5. Browse to the Certificate File on the HSM.
7. Select Private Key resides on Hardware Security Module.
8. Click OK and Commit.
Certificate Management

Secure Keys with a Hardware Security Module

Store Private Keys on an HSM (Continued)

| Step 4  (Forward Trust certificates only) | 1. Open the certificate you imported in Step 3 for editing.  
| Enable the certificate for use in SSL/TLS Forward Proxy. | 2. Select Forward Trust Certificate.  
| | 3. Click OK and Commit.  
| Step 5 | Verify that you successfully imported the certificate onto the firewall. | Locate the certificate you imported in Step 3 and check the icon in the Key column:  
| | | • Lock icon—The private key for the certificate is on the HSM.  
| | | • Error icon—The private key is not on the HSM or the HSM is not properly authenticated or connected.  

Manage the HSM Deployment

Manage HSM

- View the HSM configuration settings.  
Select Device > Setup > HSM.

- Display detailed HSM information.  
Select Show Detailed Information from the Hardware Security Operations section. Information regarding the HSM servers, HSM HA status, and HSM hardware is displayed.

- Export Support file.  
Select Export Support File from the Hardware Security Operations section. A test file is created to help customer support when addressing a problem with an HSM configuration on the firewall.

- Reset HSM configuration.  
Select Reset HSM Configuration from the Hardware Security Operations section. Selecting this option removes all HSM connections. All authentication procedures must be repeated after using this option.