

Palo Alto Networks (PAN)-OS

INTEGRATION GUIDE
SAFENET LUNA HSM



Document Information

Document Part Number	007-000441-001
Release Date	June 2019

Revision History

Revision	Date	Reason
A	June 2019	First Release

Trademarks, Copyrights, and Third-Party Software

© 2019 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- > The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE	5
Scope	5
Document Conventions.....	5
Command Syntax and Typeface Conventions	6
Support Contacts	7
Customer Support Portal	7
Telephone Support	7
Email Support	7
CHAPTER 1: Introduction	8
Third Party Application Details.....	8
Supported Platforms	8
Prerequisites	9
Setup the PAN-OS Virtual Appliance.....	9
Configure the SafeNet Luna HSM	9
CHAPTER 2: Integrating PAN-OS with a SafeNet Luna HSM	10
Setting up Connectivity with a SafeNet Luna HSM.....	10
Adding SafeNet Luna HSM server information to PAN-OS.....	10
Configuring PAN-OS to authenticate to the HSM.....	12
Registering PAN-OS as HSM client and assigning a partition on the HSM	12
Configuring PAN-OS to connect to the HSM partition	13
(For HA Only) Configuring PAN-OS to connect to the HA slot.....	13
Verifying PAN-OS connectivity and authentication with the HSM	14
Encrypting the Master Key	14
Rotating the Master Key used for Encryption	15
Storing Private Keys on the SafeNet Luna HSM	16
Generating the private key and certificate for decryption	16
Importing the certificate that corresponds to the HSM-stored key	17
(For Forward Trust certificates only) Enabling the certificate for use in SSL/TLS Forward Proxy	17
Verifying the certificate import	17

PREFACE

This document guides administrators through the steps for integrating Palo Alto Networks (PAN)-OS with a SafeNet Luna HSM.

Scope

This document outlines the steps to integrate PAN-OS with a SafeNet Luna HSM. The SafeNet Luna HSM is used to encrypt the Master Key and store the private keys that PAN-OS uses for SSL forward proxy and SSL inbound inspection.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Notes contain important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION! Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

****WARNING**** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury

Command Syntax and Typeface Conventions

Convention	Description
bold	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Window titles (On the Protect Document window, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italic</i>	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[a b c] [<a> <c>]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.
{ a b c } { <a> <c> }	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or [Gemalto Customer Support](#).

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.

CHAPTER 1: Introduction

Palo Alto Networks (PAN)-OS is a security-specific operating system which runs all Palo Alto Networks® next-generation firewalls that allows organizations to safely enable applications using App-ID, User-ID, Content-ID, GlobalProtect, and WildFire. It protects against all threats both known and unknown with Content-Id™ and Wildfire™. The SafeNet Luna HSM is used to encrypt the PAN-OS Master Key and store the private keys that PAN-OS uses for SSL forward proxy and SSL inbound inspection.

The benefits of integrating PAN-OS with a SafeNet Luna HSM include:

- > Full life cycle management of the keys.
- > Access to the HSM audit trail.
- > Significant performance improvements by off-loading cryptographic operations from servers.

Third Party Application Details

This integration guide uses the following third party applications:

- > PAN-OS

Supported Platforms

SafeNet Luna HSM: SafeNet Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. SafeNet Luna Network HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs. SafeNet Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

Third Party Details	SafeNet Appliance version	Firmware Version
PAN-OS VM Series 9.0.1	Appliance Version- 6.3.0-1048	6.27.0

Prerequisites

Before you proceed with the integration, complete the following:

Setup the PAN-OS Virtual Appliance

Use the appropriate virtual image file to deploy the virtual appliance on the VMware. Refer to the *Palo Alto Support Portal* and *Palo Alto Product Documentation* for further information.

When your virtual appliance is available on a VMware, perform the following steps:

1. Access the PAN-OS Web console through the IP address that was configured during deployment.

For example: <https://PAN-OS-Web_Interface_IP>.



2. Configure PAN-OS to use a static IP address.

NOTE: Before the HSM and PAN-OS connect, the HSM authenticates PAN-OS based on its IP address. As a result, you must configure the PAN-OS to use a static IP address, not a dynamic address assigned through DHCP. Operations on the HSM stop working if the PAN-OS address changes during runtime.

Configure the SafeNet Luna HSM

Before you get started ensure that the HSM is setup, initialized, provisioned and ready for deployment.

The steps for configuring the connectivity between the PAN-OS environment and the SafeNet Luna HSM appliance are included as a procedure in the integration guide.

CHAPTER 2: Integrating PAN-OS with a SafeNet Luna HSM

To integrate PAN-OS with the SafeNet Luna HSM complete the following:

- > Setting up Connectivity with a SafeNet Luna HSM
- > Encrypting the Master Key
- > Rotating the Master Key used for Encryption
- > Storing Private Keys on the SafeNet Luna HSM

Setting up Connectivity with a SafeNet Luna HSM

To set up connectivity between the SafeNet Luna HSM and PAN-OS complete the following:

- > Adding SafeNet Luna HSM server Information to PAN-OS
- > Configuring PAN-OS to authenticate to the HSM
- > Registering PAN-OS as HSM client and assigning a partition on the HSM
- > Configuring PAN-OS to connect to the HSM partition
- > (For HA Only) Configuring PAN-OS to connect to the HA slot
- > Verifying PAN-OS connectivity and authentication with the HSM

Adding SafeNet Luna HSM server information to PAN-OS

Access the PAN-OS web interface and configure PAN-OS to use the SafeNet Luna HSM.

To add the SafeNet Luna HSM server information to PAN-OS

1. Log in to the PAN-OS web interface and select **Device**→**Setup**→**HSM**.
2. Edit the Hardware Security Module Provider settings and set the **Provider Configured** section to **SafeNet Network HSM**.
3. Add the HSM server. Repeat for each HSM server if completing a high-availability (HA) configuration.

NOTE: A high availability (HA) HSM configuration requires at least two servers. You can have a cluster of up to 16 HSM servers. All HSM servers in the cluster must run the same SafeNet version and must authenticate separately. You should use a SafeNet cluster only when you want to replicate the keys across the cluster. Alternatively, you can add up to 16 SafeNet HSM servers to function independently.

- a. Enter a **Module Name** (an ASCII string of up to 31 characters) for the HSM server.
- b. Enter an IPv4 address for the HSM **Server Address**.

4. If configuring HA, select **High Availability**, specify the **Auto Recovery Retry** value (maximum number of times the HSM client tries to recover its connection to an HSM server before failing over to an HSM HA peer server; range is 0 to 500; default is 0), and enter a **High Availability Group Name** (an ASCII string up to 31 characters long).

NOTE: If you configure two or more HSM servers, the best practice is to enable **High Availability**.

Module Name	Server Address
MySA1	10.164.74.107
MySA2	10.164.56.82

High Availability
 Auto Recovery Retry:
 High Availability Group Name:

5. Click **OK** and **Commit** your changes.
6. Click **Select HSM Client Version** and select version **6.3.0**.
7. Click **OK** and **Commit** your changes.
8. (Optional) If you don't want PAN-OS to connect through the management interface, you can configure a service route to connect to the HSM.

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

- a. Select **Device**→**Setup**→**Services** and click **Service Route Configuration**.
- b. **Customize** a service route. The **IPv4** tab is active by default.
- c. Click **HSM** in the **Service** column.
- d. Select a **Source Interface** for the HSM.
- e. Click **OK** and **Commit** your changes.

Configuring PAN-OS to authenticate to the HSM

Add the SafeNet Luna HSM admin credentials to PAN-OS to allow PAN-OS to access the HSM as a user.

To add the HSM admin credentials

1. Select **Device**→**Setup**→**HSM** and **Setup Hardware Security Module**.
2. Select the HSM **Server Name** configured in previous steps.
3. Enter the **Administrator Password** to authenticate the PAN-OS to the HSM. The **Administrator Password** is the HSM admin password.



4. Click **OK**.

The PAN-OS tries to authenticate to the HSM and displays a status message.



5. Click **OK**.

Registering PAN-OS as HSM client and assigning a partition on the HSM

Register PAN-OS as the HSM client and assign a partition to it.

NOTE: If the HSM has an existing PAN-OS with the same <PAN-OS_client_name> already registered, you must remove the duplicate registration by running the **client delete - client <PAN-OS_client_name>** command before trying to register the new client.

To register the PAN-OS as HSM client and assign a partition on the HSM

1. Log in to the HSM as the admin user.
2. Register PAN-OS:

```
# client register -c <PAN-OS_client_name> -ip <PAN-OS_IP>
```


3. Assign a partition to PAN-OS.

```
# client assignpartition -c <PAN-OS_client_name> -p <partition-name>
```

Configuring PAN-OS to connect to the HSM partition

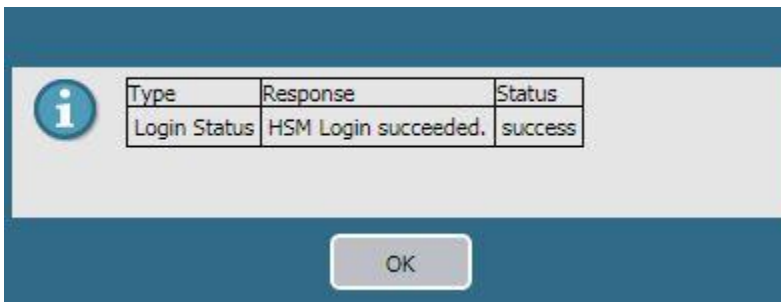
Add the partition password to authenticate the PAN-OS to the HSM partition.

To configure PAN-OS to connect to the HSM partition

1. Select **Device**→**Setup**→**HSM** and refresh () the display.
2. Open the **Setup HSM Partition** (Hardware Security Operations settings).
3. Enter the **Partition Password** to authenticate the PAN-OS to the partition on the HSM. The **Partition Password** is the Crypto Officer password.



4. Click **OK**.



(For HA Only) Configuring PAN-OS to connect to the HA slot

Repeat the previous authentication, registration, and partition connection steps to add another 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.

Add the HA slots to PAN-OS using the available PAN-OS CLI commands.

To configure PAN-OS to connect to the HA slot

1. Log in to PAN-OS CLI.
2. Create the HA group.

```
# request hsm ha create-ha-group password
```

3. Synchronize the members of the HA group.

```
# request hsm ha synchronize password
```

4. Replace the HSM servers in the HA group.

```
# request hsm ha replace-server password
```

Verifying PAN-OS connectivity and authentication with the HSM

Verify the connectivity of PAN-OS and the HSM partition using the PAN-OS web interface.

To Verify PAN-OS connectivity and authentication with the HSM

1. Select **Device**→**Setup**→**HSM** and check the authentication and connection **Status**.

- **Green:** The PAN-OS is successfully authenticated and connected to the HSM.
- **Red:** The PAN-OS failed to authenticate to the HSM or network connectivity to the HSM is unavailable.

2. View the following columns in **Hardware Security Module Status** to determine the authentication status:

- **Serial Number:** The serial number of the HSM partition. This value is only available if PAN-OS successfully authenticated to the HSM.
- **Partition:** The partition name on the HSM that is assigned to PAN-OS.
- **Module State:** The current state of the HSM connection. This value is always **Authenticated** if the Hardware Security Module Status displays the HSM.

The screenshot displays the 'Hardware Security Module Provider' configuration page. The 'Provider Configured' is 'SafeNet Network HSM'. 'High Availability' is checked, with 'High Availability Group Name' set to 'MyHA1' and 'Firewall Source Address' set to '10.164.78.99'. 'Master Key Secured by HSM' is unchecked. The 'Status' is shown as a green circle. To the right, the 'Hardware Security Operations' menu includes options like 'Setup Hardware Security Module', 'Setup HSM Partition', 'Show Detailed Information', 'Export Support File', 'Reset HSM Connection', and 'Select HSM Client Version'. Below this, the 'Hardware Security Module Status' table is visible.

Serial No	Partition	Module State
1233061544413	arif	Authenticated

Encrypting the Master Key

The Master Key encrypts all private keys and passwords on the PAN-OS. You can encrypt the master key using an encryption key that is stored on SafeNet Luna HSM. PAN-OS then requests the HSM to decrypt the master key whenever it is required to decrypt a password or private key on the PAN-OS.

The HSM encrypts the master key using a wrapping key.

NOTE: PAN-OS configured in FIPS/CC mode do not support master key encryption using an HSM.

If you have not previously encrypted the master key on a PAN-OS, use the following procedure to encrypt it.

Return to this procedure anytime you need to encrypt a key for the first time, or if you define a new master key and you want to encrypt it.

To encrypt the Master Key

1. Select **Device**→**Master Key and Diagnostics**.
2. Specify the key that is currently used to encrypt all of the private keys and passwords on the PAN-OS in the **Master Key** field.
3. If changing the Master Key, enter the new Master Key and confirm.
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**.

Rotating the Master Key used for Encryption

As a best practice, we recommend periodically refreshing the Master Key encryption by rotating the wrapping key that encrypts it. The wrapping key resides on the HSM.

To refresh the Master Key Encryption

1. Log in to the PAN-OS CLI.
2. 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.

Storing Private Keys on the SafeNet Luna HSM

For additional security, you can use an HSM to secure the private keys used for PAN-OS SSL/TLS decryption. PAN-OS uses the HSM for SSL/TLS decryption for the following features:

- > **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 PAN-OS 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.

If you use the DHE or ECDHE key exchange algorithms to enable perfect forward secrecy (PFS) support for SSL decryption, you can use an HSM to store the private keys for SSL Inbound Inspection. You can also use an HSM to store ECDSA keys used for SSL Forward Proxy or SSL Inbound Inspection decryption.

This section contains the following topics:

- > [Generating the private key and certificate for decryption](#)
- > [Importing the certificate that corresponds to the HSM-stored key](#)
- > (For Forward Trust certificates only) [Enabling the certificate for use in SSL/TLS Forward Proxy](#)
- > [Verifying the certificate import](#)

Generating the private key and certificate for decryption

For the purpose of this demonstration the SafeNet Luna HSM client is installed on a separate OS (Linux/Windows) with an NTLS connection to PAN-OS.

Access the partition used by PAN-OS and generate a key pair and self-signed certificate using the **cmu** utility.

To generate a key pair and certificate

1. Create key pair using **cmu**.

```
# ./cmu gen -modulusBits=2048 -publicExp=65537 -sign=T -verify=T
```

2. Run **cmu list** to list the key.

```
# ./cmu list
```

3. Create a self-signed certificate.

```
# ./cmu selfSign -C=CA -O=thales -startDate=20190101 -endDate=20250101 -
CN="test.thales.com"
```

4. Run **cmu list** to verify that the certificate was generated successfully.

```
# ./cmu list
```

5. Export the certificate.

```
# ./cmu export
```

Copy the certificate to the system from where you are using the PAN-OS web console

Importing the certificate that corresponds to the HSM-stored key

Import the copied certificate into PAN-OS using PAN-OS web interface.

To import the certificate that corresponds to the HSM-stored key

1. Select **Device**→**Certificate Management**→**Certificates**→**Device Certificates** and click **Import**.
2. Enter the **Certificate Name**.
3. **Browse** to the **Certificate File** on the HSM.
4. Select a **File Format**.
5. Select **Private Key resides on Hardware Security Module**.
6. Click **OK** and **Commit** your changes.

(For Forward Trust certificates only) Enabling the certificate for use in SSL/TLS Forward Proxy

If using SSL/TLS Forward Proxy then enable the certificate.

To enable the certificate for use in SSL/TLS Forward Proxy

1. Open the certificate you imported for editing.
2. Select **Forward Trust Certificate**.
3. Click **OK** and **Commit** your changes.

Verifying the certificate import

Verify that the certificate has been successfully imported onto PAN-OS.

To verify the certificate import

Locate the certificate you imported 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.

This completes the integration of SafeNet Luna HSM with Palo Alto Networks-OS.