

---

# PAN-OS: Integration Guide

---

THALES LUNA HSM

## Document Information

<b>Document Part Number</b>	007-000441-001
<b>Revision</b>	C
<b>Release Date</b>	13 May 2021

## Trademarks, Copyrights, and Third-Party Software

Copyright © 2021 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group 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.

# CONTENTS

Overview .....	4
Certified Platforms .....	4
Prerequisites .....	5
Set up PAN-OS virtual appliance.....	5
Configure Luna HSM .....	5
Integrating PAN-OS with a Luna HSM.....	6
Set up connectivity with Luna HSM .....	6
Encrypt Master Key.....	11
Rotate the master key used for encryption .....	12
Store private keys on Luna HSM .....	13
Contacting Customer Support.....	15
Customer Support Portal .....	15
Telephone Support .....	15
Email Support .....	15

## Overview

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

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 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 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.

## Certified Platforms

This integration is certified with Luna HSM on the following platforms:

Third Party Details	Thales Luna Client
PAN-OS VM Series 10.0.2	7.2.0
PAN-OS VM Series 9.0.1	6.3.0

**Luna HSM:** 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. Luna Network HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

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

## Prerequisites

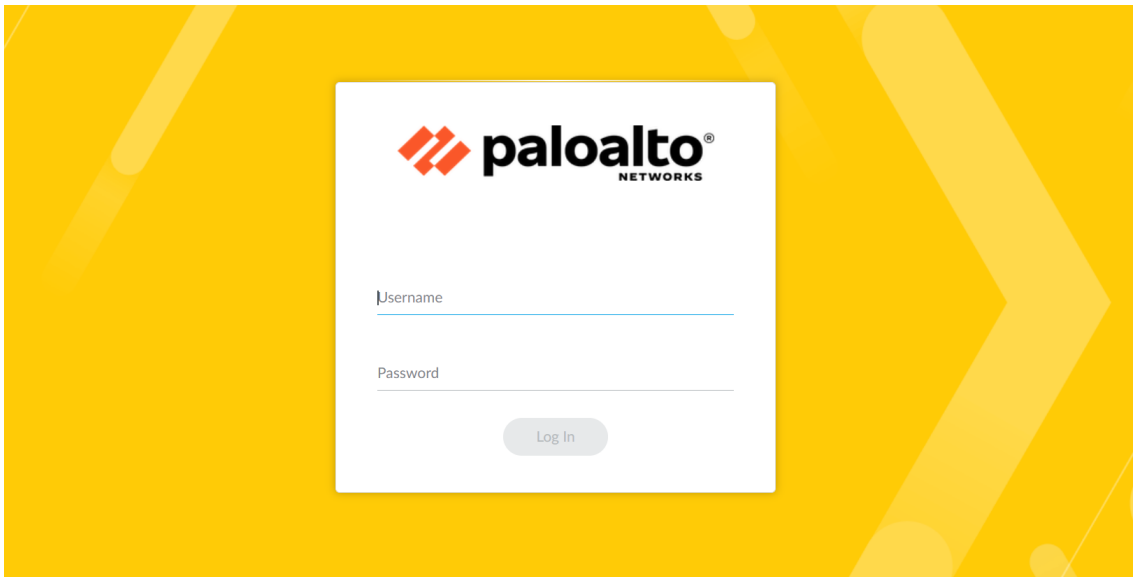
Before you proceed with the integration, complete the following tasks:

- > [Set up PAN-OS Virtual Appliance](#)
- > [Configure Luna HSM](#)

### Set up 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. Apply the license for PAN-OS.

**NOTE:** You must apply the license on PAN-OS for HSM feature to work. Refer <https://docs.paloaltonetworks.com/pan-os> for more details on licenses and subscriptions.

3. 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 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 Luna HSM appliance are included in the [Integrating PAN-OS with a Luna HSM](#) section.

## Integrating PAN-OS with a Luna HSM

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

- > [Set up connectivity with a Luna HSM](#)
- > [Encrypt the master key](#)
- > [Rotate the master key used for encryption](#)
- > [Store private keys on the Luna HSM](#)

### Set up connectivity with Luna HSM

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

- > [Add Luna HSM server information to PAN-OS](#)
- > [Configure PAN-OS to authenticate to the HSM](#)
- > [Register PAN-OS as HSM client and assign a partition](#)
- > [Configure PAN-OS to connect to the HSM partition](#)
- > [Configure PAN-OS to connect to the HA slot \(for HA only\)](#)
- > [Verify PAN-OS connectivity and authentication with the HSM](#)

### Add Luna HSM server information to PAN-OS

Access the PAN-OS web interface and configure PAN-OS to use the Luna HSM. To add the 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 Luna HSM version and must authenticate separately. You should use a Luna HSM cluster only when you want to replicate the keys across the cluster. Alternatively, you can add up to 16 Luna 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**.

- 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).

Hardware Security Module Details

Provider Configured: SafeNet Network HSM

MODULE NAME	SERVER ADDRESS
LunaHSM1	10.164.75.32
LunaHSM2	10.164.75.30

+ Add - Delete

High Availability

Auto Recovery Retry: 3

High Availability Group Name: myha

OK Cancel

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

- Click **OK** and **Commit** your changes.
- Click **Select HSM Client Version** and select version.

**NOTE:** If you are using PAN-OS 10.x it is recommended to use HSM Client Version as 7.2.0. If you are using PAN-OS 9.x it is recommended to use HSM Client Version as 6.3.0.

- Click **OK** and **Commit** your changes.
- (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.

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

## Configure PAN-OS to authenticate to Luna HSM

Add the 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**.
3. Select HSM Authentication as **Automatic** or **Manual**.
4. If HSM Authentication is **Automatic** then perform the following tasks:
  - a. Enter the **Administrator Password** to authenticate the PAN-OS to the HSM. The **Administrator Password** is the HSM admin password.

- b. Click **OK**. The PAN-OS tries to authenticate to the HSM and displays a status message.

Type	Response	Status
Authentication Status	HSM authentication server name LunaHSM1 authentication success. Please register client on HSM server and login.	success

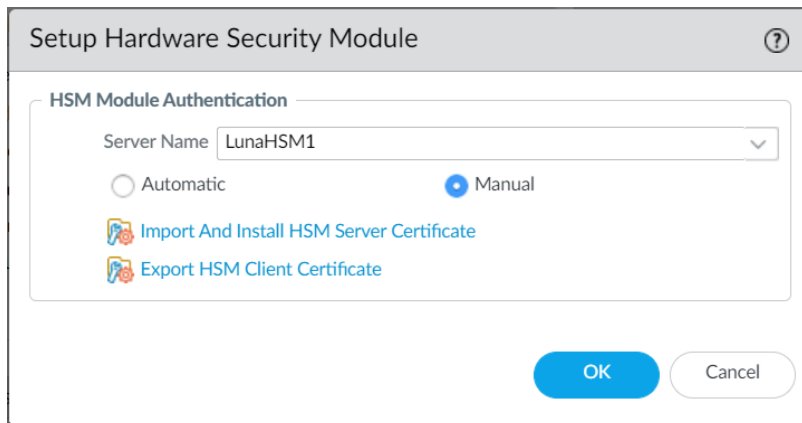
- c. Click **OK**.
5. If HSM Authentication is **Manual** then perform the following tasks:
  - a. Use any Linux or Windows machine to copy server.pem file from Luna HSM. For example:
 

```
# scp admin@10.164.75.32:server.pem /home
```

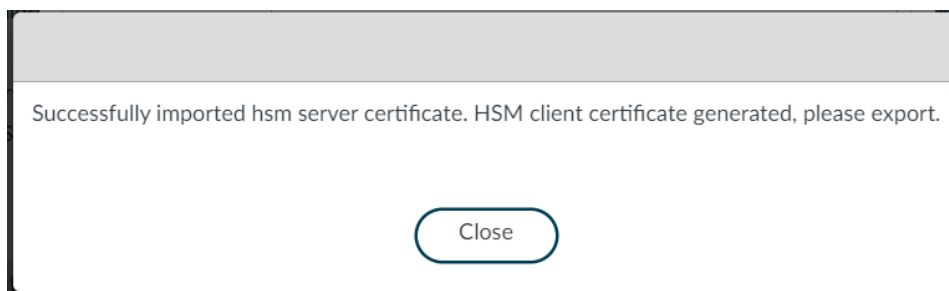
 Provide HSM Admin password when prompted.



- b. Click on Import Select Server And Install HSM Server Certificate.



- c. Click on **Browse** and select the server.pem file that you have copied in step a.  
 d. Click **OK**. HSM Certificate will be uploaded to PAN-OS.



- e. Click **Close**  
 f. Click on **Export HSM Client Certificate**. Client certificate file will be downloaded.  
 g. Copy client certificate to HSM using Linux or Windows machine.

```
# scp /home/10.164.76.45.pem admin@10.164.75.32:
```

Provide HSM Admin password when prompted.  
 Here, 10.164.76.45.pem is the client certificate.

### Register PAN-OS as HSM client and assign a partition

Register PAN-OS as the Luna HSM client and assign a partition to it. To register the PAN-OS as Luna HSM client and assign a partition on Luna HSM:

1. Log in to Luna 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.

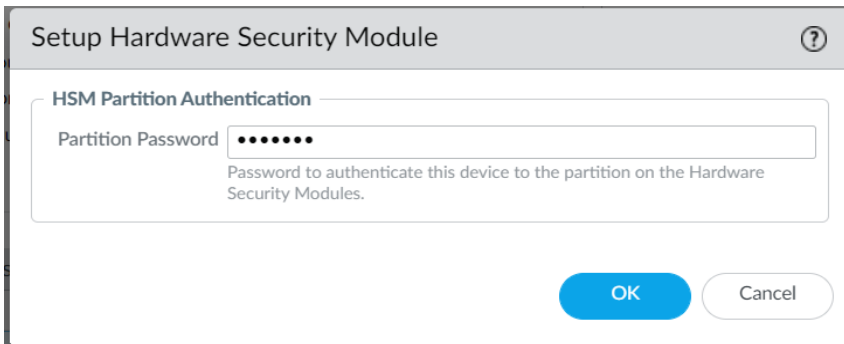
```
# client assignpartition -c < PAN-OS_client_name> -p <partition-name>
```

**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.

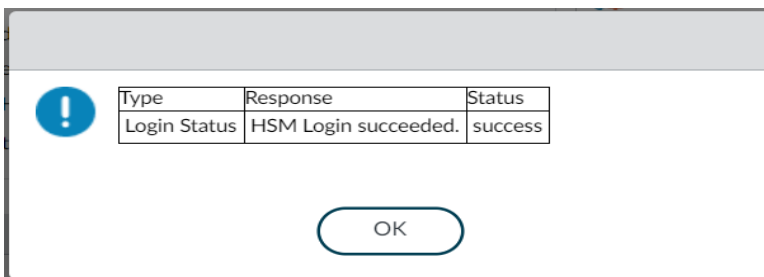
### Configure PAN-OS to connect to Luna HSM partition

Add the partition password to authenticate the PAN-OS to the Luna HSM partition. To configure PAN-OS to connect to the Luna 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. Click **OK**.



4. Click **OK**.



Type	Response	Status
Login Status	HSM Login succeeded.	success

### Configure PAN-OS to connect to the HA slot (for HA Only)

Repeat the previous authentication, registration, and partition connection steps to add another Luna HSM to the existing HA group. If you remove a Luna HSM from your configuration, repeat the previous partition connection step to remove the deleted Luna HSM from the HA group.

For PAN-OS 9.x you need to perform these additional steps 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
```

## Verify PAN-OS connectivity and authentication with Luna 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 Luna 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 shows the PAN-OS web interface with the 'HSM' tab selected. The 'Hardware Security Module Details' section displays the following configuration:

- Provider Configured: SafeNet Network HSM
- High Availability:
- High Availability Group Name: myha
- Firewall Source Address: 10.164.76.45
- HSM Client Version on Firewall: 7.2.0
- Master Key Secured by HSM:
- Status: ●

The 'Hardware Security Operations' section contains the following links:

- Set Up Hardware Security Module
- Setup HSM Partition
- Show Detailed Information
- Export Support File
- Reset HSM Connection
- Select HSM Client Version

The 'Hardware Security Module Status' table is shown below:

SERIAL NO	PARTITION	MODULE STATE
1280780175982	lunapartition1	Authenticated
1289637052004	lunapartition2	Authenticated

## Encrypt Master Key

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

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 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. If you have not previously encrypted the master key on a PAN-OS, use the following procedure 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. If changing the Master Key, enter the new Master Key and confirm.
3. Select the **Stored on HSM** check box and enter values for:
  - **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).

4. Click **OK**.

**Master Key**

Master Key

Current Master Key

Stored on HSM

New Master Key

Confirm New Master Key

Lifetime  Days  Hours  
Ranges from 1 hour to 18250 days.

Time for Reminder  Days  Hours  
Ranges from 1 hour to 365 days.

You must configure a new master key before the current key expires. If the master key expires, the firewall automatically reboots in Maintenance mode. You must then reset the firewall to Factory Default Settings.

Auto Renew Master Key

Auto Renew With Same Master Key  Days  Hours  
Ranges from 1 hour to 730 days.

**OK** **Cancel**

**NOTE:** 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.

**NOTE:** If Master Key is not synced between the members of the HA slot then run `request hsm ha synchronize password` from PAN-OS CLI.

## Rotate 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 or rotate 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
```

```
admin@PA-VM> request hsm mkey-wrapping-key-rotation
```

```
Mkey wrapping key rotation succeeded. New key handle 39.
admin@PA-VM> █
```

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 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:

- > [Generate private key and certificate for decryption](#)
- > [Import the certificate that corresponds to the HSM-stored key](#)
- > [Enable the certificate for use in SSL/TLS Forward Proxy \(for forward trust certificates only\)](#)
- > [Verify the certificate import](#)

### Generate private key and certificate for decryption

For the purpose of this demonstration the 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
```

Provide partition password when prompted.

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

```
# ./cmu list
```

Provide partition password when prompted.

3. Create a self-signed certificate.

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

Provide partition password when prompted.

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

```
# ./cmu list
```

Provide partition password when prompted.

5. Export the certificate.

```
# ./cmu export
```

Provide partition password when prompted.

Also provide the filename for the certificate.

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

### Import the certificate that corresponds to 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:

- Select **Device**→**Certificate Management**→**Certificates**→**Device Certificates** and click **Import**.
- Select Certificate Type as **Local**.
- Enter the **Certificate Name**.
- Browse** to the **Certificate File** on the HSM.
- Select a **File Format**.
- Select **Private Key resides on Hardware Security Module**.
- Click **OK** and **Commit** your changes.

### Enable the certificate for use in SSL/TLS Forward Proxy (for forward trust certificates only)

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

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

### Verify the certificate import

Verify that the certificate has been successfully imported onto PAN-OS. To verify the certificate import:

- Locate the certificate you imported.
- 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 Luna HSM with Palo Alto Networks-OS.

---

## Contacting Customer Support

---

If you encounter a problem during this integration, refer to the documentation. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#). Thales 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 Thales 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.thalesgroup.com>, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository 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 Thales 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.DIS@thalesgroup.com](mailto:technical.support.DIS@thalesgroup.com).