

# SafeNet IDPrime Virtual v2.4.1

## RELEASE NOTES

**Issue Date:** August 2023

**Build:**

Server (Evaluation version): 2.4.1.24

Server (Full version): 2.4.1.23

Windows Client: 2.4.1.26

SSP version: 2.4.1.3

**Document Part Number:**007-000656-001 Rev J

### Contents

<b>Product Description</b> .....	<b>3</b>
Release Description .....	3
New Features and Enhancements .....	3
Deployment Configuration .....	3
Setup Configuration .....	4
Advisory Notes .....	5
Licensing .....	6
Localization Support .....	6
Default Password .....	6
Password Recommendations .....	6
Compatibility Information .....	6
Operating Systems .....	6
Minimum System Requirements .....	7
Database Servers .....	7
Middleware .....	7
Tools and Software .....	7
Virtual Smart Card Features .....	8
Execution of Third-Party Security Tools .....	8
Compatibility with Third-Party Applications .....	8
Compatibility with Thales Applications .....	9
Installation and Upgrade Information .....	9
Installation .....	9
Upgrade .....	9
<b>Resolved and Known Issues</b> .....	<b>10</b>

---

Resolved Issues .....	10
Known Issues .....	12
<b>Related Product Documentation .....</b>	<b>16</b>
<b>Support Contacts .....</b>	<b>17</b>

# Product Description

SafeNet IDPrime Virtual (IDPV) is a PKI-based software authenticator that uses latest innovation in software-based smart token technology to combine the strong two-factor security of a smart card. It is cost effective and convenient for the software authentication. IDPV emulates the functionality of physical smart cards used for authentication, email, data encryption, and digital signing to enable the use cases such as VDI, BYOD, backup, and mobility on any device. It secures user private key on HSM with user authentication from OIDC compatible Identity providers (IDPs).

## Release Description

SafeNet IDPrime Virtual v2.4.1 Release includes latest enhancements and bug fixes from the previous version.

## New Features and Enhancements

This release offers the following:

- > Added support for Microsoft Azure Identity Provider integration. Refer to the [integration](#) section for more details.
- > Removal of -b (thumbprint) parameter in SetupTenant utility command. Refer to [setup configuration section](#) for more details.
- > IdpScope parameter is added in the `idp-configuration.json` file. This mandatory parameter must match the scope value present in the Identity Provider settings for successful authentication.

## Deployment Configuration

Deploy the following configuration setting for the latest release package:

### Update in `idp-config.json`:

- IdpScope key is added in `idp-config.json` which signifies the token permission and determines the token behavior. Example: "IdpScope": "openid".

**NOTE** Earlier, the IdpScope field was set to 'openid' by default, but now it is IDP specific. IdpScope should be identical in `idpconfig.json` and IDP configuration. Refer to the table below for the IdpScope values corresponding to the respective IDP.

STA	"openid"
SAS PCE	"idpvscope openid offline_access"
Keycloak	"idpvscope openid offline_access"
OKTA	"idpvscope openid offline_access"

PingID	"idpvscope openid offline_access"
AZURE	"openid offline_access api://idpv/idpvscope", or "openid offline_access https://<sub-domain>.<domain.com>/idpvscope"

### For the deployment of IDPV Server with IDPV Client only, update the RedirectURL as below:

- Update in `idp-config.json`:  
The IDP configuration should contain `idpRedirectUrl` as `<Server Host>/redirect`. For example: `https://www.idpvserver.com/redirect`
- Update IDP server configuration:  
The IDP configuration value should match the `idpRedirectUrl` parameter configured in the `idp-config.json` (exact match or pattern match).

### For the deployment of IDPV Server along with IDPV Client and Self-Service Portal, update the RedirectURL as below:

- Update in `idp-config.json`:  
The IDP configuration should contain `idpRedirectUrl` as `<Server Host>/oauth-callback`. For example: `https://www.idpvserver.com/oauth-callback`
- Update IDP server configuration:  
The IDP server configuration should be set as per following combinations for different IDPs to support IDPV Client and Self-Service Portal both.  
For more details, refer to the [Self-Service](#) section.

For details, refer to [SafeNet IDPrime Virtual Server-Client Integration Documentation](#), for the Valid Redirect URL setting for the selected IDP configuration.

## Setup Configuration

IDPV setup configuration is updated in the latest release package:

### 1. Commands for accessing IDPV server is updated:

```
docker exec -it <idpvserver_container_name> sh
```

### 2. Command for Setuptenant utility is updated:

For example to list all tenants:

```
setuptenant list -l true
```

### 3. The `-b` (Thumbprint) parameter is removed from the SetupTenant utility command. So, accordingly the create and update commands in SetupTenant will be executed without `-b` parameter. Refer to the latest create command syntax below:

```
setuptenant create -i Config/azure-test.json -p Config/policy-configuration.json  
-a <client_secret> -k <true or false> -u <true or false> -c <IDPV> -n <tenant_  
name>
```

Example command:

```
setuptenant create -i Config/idp-configuration.json -p Config/policy-  
configuration.json -a XWN8Q~xoPkcwjsNJ-6QiED2nIQjoNsdVs.Vriad_ -k true -u false  
-c IDPV -n "Azure-test"
```

4. Following sample value is added in the `appsettings.yml` under `WebServerConfig` for the deployment of self-service portal:

```
SelfServicePortalUrl: 'https://10.164.42.253:3001/'
```

For more information, refer **Running IDPV Server and Setting up Tenant** section in **SafeNet IDPrime Virtual Server** section in [SafeNet IDPrime Virtual Server-Client Product Documentation](#).

5. For the creation of Signature Web Services (SWS) tenant, the configuration should be provided in a separate json file.  
For more information, refer to **Setting up Signature Web Service** and **swsconfig.json parameters** section in **Signature Web Service** section in [SafeNet IDPrime Virtual Server-Client Product Documentation](#).
6. `RefreshTokenExpirationDuration`: It is the expiration duration for the refresh access token. For PingFederate and Okta IDP, this parameter should be included in `idp-config.json` and this value can be fetched from IDP Server. For more information, refer to **Setting up Refresh Token** section in [SafeNet IDPrime Virtual Server Client Integration Documentation](#). For STA and SAS PCE with Keycloak agent IDP, this parameter from `idp-config.json` is ignored.
7. For Azure IDP, the recommended value for `RefreshTokenExpirationDuration` should be less than 24 hours. Refer to [Microsoft guidelines](#) and [Known issues](#) section for more details.

**CAUTION!** Maximum value for `RefreshTokenExpirationDuration` parameter is 24 days (34560 minutes).

## Advisory Notes

Before deploying this release, note the following high-level requirements and limitations:

- > [KeySecure](#) and [PingOne](#) are validated with 2.4 release build only.
- > If you are installing IDPV Client with `adm` and `adml` files from the release package, you need to manually provide the registry settings like `Proxy` and `DisableNotification`.
- > IDPV Client versions prior to 2.4.1. release are compatible with latest IDPV Server versions until the tenant is updated using `UpdateTenant` utility command.
- > `appsetting.yml`:
  - `appsetting.yml` should be carefully updated before running the server Docker container as it contains sensitive information like `DatabaseProvider`, `HSMProvider`, HSM partition serial number, and more.
- > `idp-config.json`:
  - Be cautious before assigning groups and values in `idp-config.json` as any other change requires updating/ creating a new tenant.
- > Identity Providers (IDPs) need to be configured distinctively for different IDPs. To know about the newly supported IDPs, refer to [SafeNet IDPrime Virtual Server Client Integration Documentation](#).

After deploying this release, take note of the following step:

- > In case of Keysecure HSM , certificate signing request only supports RSA SHA 1 (1.2.840.113549.1.1.5) algorithm as `signAlgorithm`.
- > If you want to use `-u` functionality for tenant, after upgrading the server, upgrade the tenant as well and restart the server immediately to view the changes, else it will be refreshed based on the time configured in `appsettings.json` file (default value is 24 hours).

- > When IDPV Client is upgraded from version 2.3 to any higher version through installer, this might result in deletion of offline bundle.

## Licensing

---

SafeNet IDPrime Virtual users can opt between the evaluation and full version software licenses. The evaluation version is free but limits users to create 50 tokens. Users must purchase the full version to create unlimited tokens.

## Localization Support

---

Operating System is localization based. Therefore, it is automatically managed.

The currently supported languages are:

- > English (default)
- > Spanish
- > German
- > French
- > Hindi and Hebrew as experimental

This list is expandable based on Qt cross-platform development solution and its internationalization support.

## Default Password

---

Virtual IDPrime cards are supplied with the following default token password: "000000" (6 zeros) and the Administrator Password must be entered using 48 zeros.

## Password Recommendations

We strongly recommend changing all device passwords upon receipt of a token/ smart card as follows:

- > User PIN should include at least 8 characters of different types.
- > PIN character types should include upper case, lower case, numbers, and special characters.  
For more information, refer to the 'Security Recommendations' section in [SafeNet IDPrime Virtual Server-Client Product Documentation](#).

## Compatibility Information

---

### Operating Systems

Following operating systems are supported:

#### Server Operating Systems

- > Red Hat Enterprise Linux (RHEL) Server 9
- > Ubuntu 22.04
- > CentOS-7

## Client Operating Systems

- > Windows 10 (2004 or higher)
  - Microsoft Trusted Platform Module (TPM 2.0) for Offline Mode
- > Linux
  - Red Hat Enterprise 8.3
  - Ubuntu 20.04
  - CentOS 8.3

## Minimum System Requirements

- > Linux Kernel 3.10 (or higher) (included with the operating systems listed above)
- > 16 GB RAM (for server performance that matches your requirements, contact Thales team)
- > 256 GB HDD
- > Minimum 64 GB of space for the /var directory before Docker is installed

## Database Servers

- > MySQL 8.0.29
- > MariaDB 10.10.2
- > MSSQL 16.0.1000.6
- > PostgreSQL 14.2
- > Oracle Database Enterprise and Express Edition 21.3.0.0.0

## Middleware

- > SafeNet Authentication Client 10.8 R9 GA
- > SafeNet Minidriver 10.8 R9 GA

## Tools and Software

- > Docker 17.03.1 (or higher)
- > LUNA Network HSM 6/7.3/7.7
- > Kubernetes v1.13.0 (or higher)
- > Support for Evaluation version only
  - SoftHSM 2.6.1
  - DPoD 7.3
  - Keysecure
- > KeySecure 450v
  - Software Version 8.4.2
  - P11 connector version 8.8.0
  - ProtectApp connector version 8.12

**NOTE** SafeNet IDPrime Virtual is tested with the provided versions of the software.

## Virtual Smart Card Features

Below table specifies the various features that are supported by IDPV:

Features:	Device: SafeNet IDPrime Virtual
Number of Keys	15 max
RSA Key Size	2048 bit
RSA Padding	PKCS#1 v1.5
Hash	SHA-2 512-bit
Supported APIs	PKCS#11 V2.20, PKCS#15, MS CryptoAPI and CNG(CSP,KSP), PC/SC
Supported cryptographic algorithms	3DES, SHA-256, RSA upto 2048

## Execution of Third-Party Security Tools

- > Aqua Trivy 0.34.0
- > Aqua Gype 0.53.1
- > Open Collective Dockle 0.1.16
- > Anchore Syft 0.62.1
- > Cisco ClamAV 2.6.5

## Compatibility with Third-Party Applications

Following third-party applications are supported:

Solution Type	Vendor	Product Version
Virtual Desktop Infrastructure (VDI)	VMware VSphere	vSphere 6.7
Identity Access Management (IAM) Identity Management (IDM)	vSEC:CMS	vSEC:CMS 6.4
Certificate Authority (CA)	Microsoft (Local CA)	For All Windows platforms



Solution Type	Vendor	Product Version
Browsers	Mozilla	Firefox 105 or higher
	Microsoft	Edge (Chromium) 104.0.1293.70 or higher
	Google	Chrome 105.0.5195.127 or higher
Remote Desktop Applications	Devolutions	2022.1.23.0
	Royal TS	6.1.50425.0
	Dameware	12.2.2.12

## Compatibility with Thales Applications

Virtual IDPrime cards can be used with the following products:

- > SafeNet Authentication Service Private Cloud Edition (SAS PCE) with Keycloak / SafeNet Trusted Access (STA)
- > SafeNet Authentication Client (SAC) 10.8 R9
- > SafeNet Minidriver 10.8 R9 GA

## Installation and Upgrade Information

**NOTE** Local administrator rights are required to install or upgrade IDPV.

### Installation

SafeNet IDPrime Virtual (IDPV) server must be installed on the supported Linux machines. IDPV client must be installed on each computer on which IDPrime Virtual Smart Cards are to be used.

### Upgrade

To upgrade IDPV server from any supported previous version to the latest version, you need the latest version delivery package, which contains the Docker image file. For using the latest version of IDPV server, existing running container should be removed and new image should be used.

For more Installation and Upgrade details, refer to *SafeNet IDPrime Virtual Server-Client Product Documentation*.

## Resolved and Known Issues

This section lists the issues that have been resolved and known to exist in this release. The following table defines the severity of the issues listed in this section.

Priority	Classification	Definition
C	Critical	No reasonable workaround exists.
H	High	Reasonable workaround exists.
M	Medium	Medium level priority problems.
L	Low	Lowest level priority problems.

## Resolved Issues

Issue	Severity	Synopsis
IDPV-5394	H	Invariant culture error with MSSQL database in alpine based docker.
IDPV-6755	H	Different group formats are not supported on Azure IDP.
IDPV-6838	M	IDPV Client incorrectly shows connected sign(green) and Connect stays enabled.
IDPV-6822	M	Only one application per Azure tenant is supported currently.
IDPV-6817	M	Upgrade from 2.4.0.66 to 2.4.1.4 server is not successful if Tenant keys are deleted in HSM.
IDPV-6745	M	IDPV Client throws error when re-connecting
IDPV-5845	H	Signed only certificates not supported via CSR API.
IDPV-5675	M	After IDPV Client upgrade, the Windows displays a system restart prompt.
IDPV-5266	M	SWS Sign API fails on Luna 6 HSM.
ASAC-15347	H	Machine hangs when the credential provider connects with etoken.cache containing huge data.
IDPV-4980	H	CP- IDPV Credential Provider and systray remains connected even after offline bundle expires.
IDPV-5654	M	In generic case of IDP configuration IDPV client is not working as expected in certain scenarios.

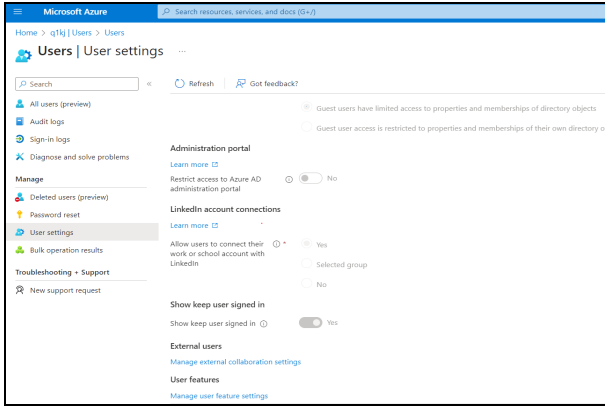
Issue	Severity	Synopsis
IDPV-5423	M	If <code>RefreshTokenExpirationDuration</code> parameter in <code>idpconfiguration.json</code> has more value than the value defined in the IDP server, then IDPV Client shows two IDP windows after the refresh token has expired.
IDPV-5671	H	"Connect" doesn't create token for admin after "Connect on behalf" if Admin has no token already.
IDPV-5743	M	In specific scenario connected via non-admin user in Connect on Behalf , exit doesn't clear the JWT in first go.
IDPV-5741	H	Self-Service portal shows error message "Something went wrong" after importing certificate from SAC.
IDPV-5723	M	Same name is displayed multiple times in IDPV Client when entered from <b>Connect On Behalf</b> pop-up.
IDPV-5772	H	GetKeyAPI doesn't show correct OBKG status.
IDPV-5553	H	In case of multiple pfx in a p12 file, certificate is not visible in SAC.
IDPV-4663	H	IDPV behaves differently with intermittent issues.
IDPV-4201	M	Getting <i>smart card login failed</i> error notifications during smartcard issuance or revocation with vSEC:CMS in a STA OIDC integration.
IDPV-4873	H	IDPV Client systray showing connected even after JWT expiry.
IDPV-4970	H	CSR formatting improvement in the Certificate Signing Request API response
IDPV-4903	H	IDPV Client not working on the VMs hosted in Citrix environment
IDPV-4732	H	Multiple IDP windows opening at the same time.
IDPV-4988	M	For untrusted certificates errors are appearing twice.
IDPV-5100	M	Multiple balloon messages appear when the user is working in offline mode.
IDPV-5132	H	Import certificate and CSR failing on Luna 7.7 SKS tenant
IDPV-4798	L	Error message is unclear when user is trying to login to offline bundle that has expired.
IDPV-5252	M	Setup Tenant command in server docker container does not automatically pick IDP thumbprint value automatically even when IDP server url is reachable.

Issue	Severity	Synopsis
IDPV-5310	L	Certificate Signing Request (CSR ) is generated with no Common Name (CN) value in the subject distinguished name field.
IDPV-5444	M	Login does not work for the first time if JWT expires(offline mode).

## Known Issues

Issue	Severity	Synopsis
IDPV-7187	M	<b>Summary:</b> Integrated browser used in IDPV Client is using browser version IE7, browser upgrade is required in IDPV Client. <b>Workaround:</b> None
IDPV-7207	L	<b>Summary:</b> Incorrect message on swagger interface in case of Generate CSR response-UI Issue. <b>Workaround:</b> None
IDPV-7202	H	<b>Summary:</b> IDPrime virtual server API gives 200 response without response body , in case the database connection fails. <b>Workaround:</b> <ol style="list-style-type: none"> <li>1. Check the Database container is running fine or not.</li> <li>2. If not, restart the DB container and then IDPV server.</li> </ol>
IDPV-5828	H	<b>Summary:</b> IDPV Linux Client 2.2.1 is not working with current redirect URL implementation in IDPV Server 2.4. <b>Workaround:</b> None
IDPV-6448	L	<b>Summary:</b> In Domain joined machine, IDP window is opening up again in the first instance and not on subsequent activities. <b>Workaround:</b> None
IDPV-5746	L	<b>Summary:</b> In Provisioning APIs , Import pfx certificate in case of wrong cert and wrong password is getting 500 error. <b>Workaround:</b> None
IDPV-4510	L	<b>Summary:</b> Logout not working for Self-Service Portal with Ping Federate and Okta IDP. <b>Workaround:</b> None
IDPV-5433	M	<b>Summary:</b> In case of invalid password in offline bundle, the displayed error message is vague. <b>Workaround:</b> None
IDPV-4986	M	<b>Summary:</b> In case of incorrect IDP configuration, connection via Credential Provider do not generate any logs in the Event viewer. <b>Workaround:</b> None

Issue	Severity	Synopsis
SAS-50616	L	<p><b>Summary:</b> If a user clicks <b>Back to Application</b> on the STA window, which is displayed when a user clicks <b>LOGIN</b> multiple times after entering the login credentials shows an error message.</p> <p><b>Workaround:</b> None</p>
ASAC-15226	H	<p><b>Summary:</b> The User Pin retries counter does not decrease with a wrong password attempt of length less than four characters.</p> <p><b>Workaround:</b> None</p>
IDPV-4504	H	<p><b>Summary:</b> Administrator pin retries get synchronized, but not the User Pin retries for the preserve token settings.</p> <p><b>Workaround:</b> None</p>
IDPV-4503	L	<p><b>Summary:</b> The quality error pop-up during the initialization if the Pin is not matching for preserver token settings.</p> <p><b>Workaround:</b> None</p>
IDPV-4078	M	<p><b>Summary:</b> When connecting the SafeNet IDPrime Virtual application through Credential Provider, the <b>'User Account Control'</b> window blocks the <i>'SafeNet Trusted Access'</i> login window. User Account Control window gets hang and requires to restart the machine.</p> <p><b>Workaround:</b> Disable User Account Control (UAC)</p> <ol style="list-style-type: none"> <li>1. On the Windows taskbar, select <b>Start &gt; Control Panel</b>.</li> <li>2. Click <b>User Accounts</b>, and then click <b>Change User Account Control settings</b>.</li> <li>3. Enter the admin credentials.</li> <li>4. Drag the slider one-step down to <b>Notify me only when apps try to make changes to my computer (default)</b>.</li> <li>5. Click <b>OK</b>.</li> </ol>
IDPV-3334	H	<p><b>Summary:</b> If the user tries multiple incorrect Pin in Offline Mode and then restarts the service in online mode, the User Pin retries do not synchronize with the IDPV server.</p> <p><b>Workaround:</b> None</p>
IDPV-5072	H	<p><b>Summary:</b> DPoD is not working on Alpine based docker.</p> <p><b>Workaround:</b> None</p>
IDPV-6323	M	<p><b>Summary:</b> When only using server side API to generate and update key pair, keys are not visible in SAC and other supporting tools.</p> <p><b>Workaround:</b> None</p>
IDPV-6118	M	<p><b>Summary:</b> For Okta IDP, the redirect URL is opening in Internet Explorer.</p> <p><b>Workaround:</b> None</p>

Issue	Severity	Synopsis
IDPV-5424	L	<p><b>Summary:</b> Momentarily, there are two IDPV icon visible in system tray.</p> <p><b>Workaround:</b> None</p>
IDPV-7193	L	<p><b>Summary:</b> SSP loops back to the start of enrollment page</p> <p><b>Workaround:</b> None</p>
IDPV-6819	M	<p><b>Summary:</b> Azure IDP - Once Stay signed in selected, there is no option to provide another user of Azure IDP.</p> <p><b>Workaround:</b> The KMSI setting is managed in the User settings of Azure Active Directory (Azure AD).</p> <ol style="list-style-type: none"> <li>1. Sign in to the Azure portal.</li> <li>2. Navigate to <b>Azure Active Directory &gt; Users &gt; User settings</b>.</li> <li>3. Disable the <b>Stay Signed</b> feature in <b>User Settings</b>, by setting the <b>Show keep user signed in</b> toggle to <b>No</b>.</li> </ol> <p>Refer the below screenshot to disable Stay Signed functionality.</p>  <p>The screenshot shows the 'User settings' page in the Microsoft Azure portal. The 'Show keep user signed in' toggle is currently set to 'No'. Other settings visible include 'Administration portal', 'LinkedIn account connections', and 'External users'.</p>
IDPV-6827	M	<p><b>Summary:</b> Refresh token behavior conflicting with Windows system level cookies in Azure IDPV Client.</p> <p><b>Workaround:</b> Recommended value for <code>RefreshTokenExpirationDuration</code> for Azure IDP is 24 hours. Any value more than this can create inconsistent behavior in IDPV Client.</p> <p><b>Workaround:</b> None</p>
IDPV-6589	H	<p><b>Summary:</b> MFA setup is not supported through IDPV client login window.</p> <p><b>Workaround:</b> MFA should be pre-enabled with Microsoft authenticator only.</p> <p><b>Workaround:</b> None</p>
IDPV-5983	M	<p><b>Summary:</b> Provisioning API (Update Cert) is allowing the same certificate to be uploaded multiple times.</p> <p><b>Workaround:</b> None</p>

Issue	Severity	Synopsis
IDPV-6850	H	<p><b>Summary:</b> JWT signing key rotation is not handled.</p> <p>Workaround: Obtain a jwt and find the key id used for signing. Note down the corresponding modulus and exponent. Replace the KeyID, IdpPublicKeyModulus, IdpPublicKeyExponent in idp-configutation.json file.</p> <p>Commands:</p> <ul style="list-style-type: none"> <li>a) <code>docker exec -it &lt;idpv_container_name&gt; sh</code></li> <li>b) <code>setuptenant update -t &lt;tenant_id&gt; -i Config/idp-configuration.json</code></li> </ul> <p>Restart IDPV server docker container:  <code>docker restart &lt;idpv_container_name&gt;</code></p> <p><b>Workaround:</b> None</p>
IDPV-6591	L	<p><b>Summary:</b> IDPV Client is redirecting after authentication if redirect URL is configured for SSP.</p> <p><b>Workaround:</b> None.</p>
IDPV-5710	L	<p><b>Summary:</b> Friendly name doesn't appear when certificate is imported via Import API.</p> <p><b>Workaround:</b> None</p>

---

# Related Product Documentation

---

The following documentation is associated with this release:

---

## ThalesDocs

[IDPV Documentation Homepage](#)

We have attempted to make the documentation complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.



---

# Support Contacts

---

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. 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 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

The support portal also lists telephone numbers for voice contact ([Contact Us](#)).