

# SafeNet IDPrime Virtual 2.6.1

## RELEASE NOTES

**Issue Date:** April 2024

**Build:**

Server (Full version): 2.6.0.22

Windows Client: 2.6.1.6

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

---

### Contents

<b>Product Description</b> .....	<b>2</b>
Release Description .....	2
Bug Fixes .....	2
Advisory Notes .....	2
Licensing .....	3
Localization Support .....	3
Default Password .....	3
Password Recommendations .....	3
Compatibility Information .....	4
Operating Systems .....	4
Minimum System Requirements .....	4
Database Servers .....	4
Middleware .....	4
Tools and Software .....	4
Virtual Smart Card Features .....	5
Execution of Third-Party Security Tools .....	5
Compatibility with Third-Party Applications .....	6
Compatibility with Thales Applications .....	6
Installation and Upgrade Information .....	6
Installation .....	6
Upgrade .....	7
<b>Known Issues</b> .....	<b>8</b>
<b>Related Product Documentation</b> .....	<b>11</b>
<b>Support Contacts</b> .....	<b>12</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 2.6.1 includes bug fixes from the previous version.

---

## Bug Fixes

---

This release provides the following bug fixes:

- > **IDPV-8370:** Outlook detects an offline token after the machine reboot.
- > **IDPV-8865:** Offline bundle is expired after the system restart when the server is not reachable.
- > **IDPV-8819:** When resuming after being offline for long hours, IDPV client remains connected using a new refresh token.
- > **IDPV-8934:** Offline bundle expiry is extended after the system restart when the server is reachable.
- > **IDPV-8931:** Warning notification message is changed to "Cannot go offline."
- > **IDPV-8927:** Bundle expiry time is extended after service restart.
- > **IDPV-8932:** If a user has a valid offline bundle, the user can switch to offline mode irrespective of the state of the server.

---

## Advisory Notes

---

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

- > 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`.
- > `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](#).

- > It is suggested not to use the installer upgrade option for the latest IDPV2.6.1 client installer. Instead, perform a fresh installation. Also, IDPV client v2.6 must be installed together with SAC v10.9.
- > Credential Provider should not be installed with IDPV client v2.6.1.
- > To avoid unforeseen issues, do not enable offline usage for current users of IDPV Client v2.4.1.
- > Working of sign and verify in offline mode for SHA384 and SHA512 -PSS mechanisms will depend on the client machine TPM.
- > Simultaneous write operations from different IDPV Client machines is not support for IDPV virtual tokens.
- > Any enrollment of smart cards done on IDPV Server 2.6.1 require IDPV Client 2.6.1 to make them usable.

## 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
- > Windows 11

## 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 11.2.2
- > MSSQL 16.0.1000.6
- > PostgreSQL 14.2
- > Oracle Database Enterprise and Express Edition 21.3.0.0.0

## Middleware

- > SafeNet Authentication Client 10.9 GA
- > SafeNet Minidriver 10.9 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 and Signature Schemes	<ul style="list-style-type: none"> <li>• SHA-2 512-bit</li> <li>• CKM_SHA1_RSA_PKCS_PSS</li> <li>• CKM_SHA256_RSA_PKCS_PSS</li> <li>• CKM_SHA384_RSA_PKCS_PSS</li> <li>• CKM_SHA512_RSA_PKCS_PSS</li> </ul>
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, RSA PSS

## Execution of Third-Party Security Tools

- > Aqua Trivy 0.34.0
- > Anchore Grype 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 7.0.3.01400
Identity Access Management (IAM) Identity Management (IDM)	vSEC:CMS	vSEC:CMS 6.9
Certificate Authority (CA)	Microsoft (Local CA)	For All Windows platforms
Browsers	Mozilla	Firefox 123 or higher
	Microsoft	Edge (Chromium) 121.0.2277.112 or higher
	Google	Chrome 122.0.6261 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) 10.9 GA
- > SafeNet Minidriver 10.9 GA

## Installation and Upgrade Information

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

### 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.

**CAUTION!** Before deleting the exiting docker container, ensure to create a backup of the IDPV server database. Click [here](#) for instructions on backing up the database.

**CAUTION!** Upgrade on IDPV Client is not supported currently. Uninstall current version before reinstalling the latest version.

For more Installation and Upgrade details, refer to [SafeNet IDPrime Virtual Server-Client Product Documentation](#).

# Known Issues

This section lists the known issues that exist in this release. The following table defines the severity of the issues listed in this section.

Severity	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.

Below are the known issues that exist in this release.

Issue	Severity	Synopsis
ASAC-16178	M	<b>Summary:</b> SAC tool pin validity setting is not functioning as expected with IDPV tokens. <b>Workaround:</b> None
IDPV-8123	M	<b>Summary:</b> Bundle Expiry is upgraded after the IDPV client upgrade. <b>Workaround:</b> None
IDPV-8132	L	<b>Summary:</b> Negative memory space is left when more certs(size) are uploaded. <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-7889	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
SAS-50616	L	<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. <b>Workaround:</b> None



Issue	Severity	Synopsis
IDPV-3333	L	<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>
ASAC-15236	L	<p><b>Summary:</b> In case of preserve token settings, user PINs do not synchronize, whereas admin PINs are synchronized.</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-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>
ASAC-16734	L	<p><b>Summary:</b> Friendly name doesn't appear when certificate is imported via Import API.</p> <p><b>Workaround:</b> None</p>
IDPV-8603	M	<p><b>Summary:</b> Old IDPV Client Windows SDK does not work with latest IDPV Client and Server.</p> <p><b>Workaround:</b> None</p>
IDPV-8673	M	<p><b>Summary:</b> Unable to uninstall IDPV Client after upgrading it with the Credential Provider component.</p> <p><b>Workaround:</b> None</p>

Issue	Severity	Synopsis
IDPV-8681	M	<b>Summary:</b> IDPV Client upgrade fails to go to online. <b>Workaround:</b> None
IDPV-8683	L	<b>Summary:</b> The Token PIN window takes some time to display the incorrect password error. <b>Workaround:</b> None
IDPV-8691	L	<b>Summary:</b> Currently, the upgrade of the <b>Microsoft.Web.Webview2</b> version is categorized as Low vulnerability. <b>Workaround:</b> None
IDPV-8749	L	<b>Summary:</b> No warning is displayed when tenant is created with <b>-f</b> as <b>false</b> . <b>Workaround:</b> None
IDPV-8751	L	<b>Summary:</b> On swagger <code>isAutoOfflineBundleDownloadEnabled</code> is showing incorrect value in <b>GetTenantDetails</b> . <b>Workaround:</b> None
IDPV-8752	L	<b>Summary:</b> Token PIN prompt is getting displayed for blocked tokens. <b>Workaround:</b> None
IDPV-8822	M	<b>Summary:</b> The IDPV Server container image uses the latest version of the Alpine container base image (v3.19), which includes the latest version of BusyBox and is subject to certain vulnerabilities (CVE-2023-42363, 42364, 42365, 42366). <b>Workaround:</b> Since there is currently no available fix for the issue, it is recommended to restrict user access to the running container. The aim is to prevent malicious users from accessing the running container and executing commands mentioned in the vulnerability, in order to mitigate the risk of potential attacks.
IDPV-8761	L	<b>Summary:</b> Upon entering the token PIN, exiting the System try, and restarting the IDPV client prevents the completion of the offline process, leaving the user in Online mode. <b>Workaround:</b> None
IDPV-8626	H	<b>Summary:</b> Virtual smart card is automatically switching to the offline mode. <b>Workaround:</b> None
IDPV-8945	L	<b>Summary:</b> User needs to update the registry and then restart the services when internet is not available. <b>Workaround:</b> None

---

# 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](#)).