SafeNet IDPrime Virtual 2.6

RELEASE NOTES

Issue Date: April 2024

Build:
Server (Full version): 2.6.0.22
Windows Client: 2.6.0.75
Document Part Number: 007-000656-001 Rev P

Contents

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 includes new features and bug fixes from the previous version.

New Features and Enhancements

This release introduces the following features and resolved some major bug fixes:

- The System tray now features the **Go Offline** option that enables users to switch to offline mode. Users can now go offline when they click **Go Offline** in System tray. For this feature to work, a user must have only one active token and all other prerequisites must be met.
- A new flag **isAutoOfflineBundleDownloadEnabled** (**-o**) is added for enabling the offline usage of the smart card when the smart card is connected. The prerequisites for offline mode remain unchanged from previous releases. If **Auto offline download** setting is enabled, the offline bundle is automatically downloaded in background when the user click **Connect** in the System tray, and then the user gets a PIN prompt if the user's offline bundle is not present. For more information, refer to the tenant related configuration.
- When using the IDPV Client, users or /admins will not be able to see their virtual cards for which the enrollment is not completed by the administrator.
- Security improvements in white listing of applications that can use virtual smart cards, which requires to configure AllowedList registry parameter present at **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Thales\SafeNet IDPrime Virtual\ClientProcess** location.
- IDPV Client embedded browser upgraded to **Microsoft Edge WebView2**.
- For enhanced documentation user experience, the client administrator and end user workflows have been segregated in the IDPV documentation on Thalesdocs.
- IDPrime Virtual Card now supports CBA (Certificate Based Authentication) using TLS 1.3 RSA-PSS mechanism with selected hash mechanisms provided below:
  - CKM_SHA1_RSA_PKCS_PSS
  - CKM_SHA256_RSA_PKCS_PSS
  - CKM_SHA384_RSA_PKCS_PSS
  - CKM_SHA512_RSA_PKCS_PSS
  - Applications (usage)
    - TLS v1.3 based authentication of websites.

  - Validation is done with websites, Self Service portal of Azure IdP and Thales STA IdP self and Sign & Verify using PKCS11Explorer, Cryptokimanager tool, etc,.

Advisory Notes

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

- If you are installing IDPV Client with admx 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 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.
- 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 require IDPV Client 2.6 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	• SHA-2 512-bit • CKM_SHA1_RSA_PKCS_PSS • CKM_SHA256_RSA_PKCS_PSS • CKM_SHA384_RSA_PKCS_PSS • CKM_SHA512_RSA_PKCS_PSS
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*.

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-6827	M	Refresh token behavior conflicting with Windows system level cookies in Azure IDPV Client.
IDPV-7911	H	MSSQL database is not working after migration.
IDPV-8004	H	When the client undergoes an upgrade, the offline bundle expiry is updated. Once the expiry period of the bundle ends, the user is unable to go online.
IDPV-6579	M	Only the Import API code is updated as it was having scope for code optimization.
IDPV-7207	L	Incorrect message on swagger interface in case of Generate CSR response-UI Issue.
IDPV-7202	H	IDPrime virtual server API gives 200 response without response body, in case the database connection fails.
IDPV-5746	L	In Provisioning APIs, Import pfx certificate in case of wrong cert and wrong password is getting 500 error.
IDPV-6118	M	For Okta IDP, the redirect URL is opening in Internet Explorer.
IDPV-5983	M	Provisioning API (Import Cert) is allowing the same certificate to be uploaded multiple times.
IDPV-6850	H	JWT signing key rotation is not handled.

Issue	Severity	Synopsis
IDPV-8166	H	For IDPV Windows Client, upgrade from version 2.5 to version 2.6 is not functioning as expected.
IDPV-7965	L	The Azure redirect authentication URL opens intermittently during Azure IdP authentication. However, there is no impact on the functionality due to this issue.
IDPV-6448	L	In Domain joined machine, IDP window is opening up again in the first instance and not on subsequent activities.
IDPV-6591	L	IDPV Client is redirecting after authentication if redirect URL is configured for SSP.
IDPV-7926	M	Data is not synchronized across multiple machines that are used by a user.
IDPV-7187	M	Integrated browser used in IDPV Client is using browser version IE7, browser upgrade is required in IDPV Client.
IDPV-4503	L	The quality error pop-up during the initialization if the Pin is not matching for preserver token settings.
IDPV-6589	H	MFA setup is not supported through IDPV client login window.
IDPV-8743	M	Upon entering an incorrect token PIN, balloon error notifications will be displayed, depending on the number of attempts made.
IDPV-8369	H	Outlook can use offline virtual smart card even after the token is expired.
IDPV-8341	H	When the user clicks **Go To Online** after the offline token is expired, the refresh token is expired before the timeout period.
IDPV-8624	H	The offline feature is not user-friendly for the Smart card offline usage.

Known Issues

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

Issue	Severity	Synopsis
IDPV-4510	L	**Summary**: Logout not working for Self-Service Portal with Ping Federate and Okta IDP. **Workaround**: None
IDPV-5433	M	**Summary**: In case of invalid password in offline bundle, the displayed error message is vague. **Workaround**: None
IDPV-7889	M	**Summary**: In case of incorrect IDP configuration, connection via Credential Provider do not generate any logs in the Event viewer. **Workaround**: None
SAS-50616	L	**Summary**: If a user clicks **Back to Application** on the STA window, which is displayed when a user clicks **LOGIN** multiple times after entering the login credentials shows an error message. **Workaround**: None
IDPV-3333	L	**Summary**: The User PIN retries counter does not decrease with a wrong password attempt of length less than four characters. **Workaround**: None
ASAC-15236	L	**Summary**: In case of preserve token settings, user PINs do not synchronize, whereas admin PINs are synchronized. **Workaround**: None
IDPV-4078	M	**Summary:** When connecting the SafeNet IDPrime Virtual application through Credential Provider, the '**User Account Control**' window blocks the '*SafeNet Trusted Access*' login window. User Account Control window gets hang and requires to restart the machine. **Workaround:** Disable User Account Control (UAC) 1. On the Windows taskbar, select **Start** > **Control Panel**. 2. Click **User Accounts**, and then click **Change User Account Control settings**. 3. Enter the admin credentials. 4. Drag the slider one-step down to **Notify me only when apps try to make changes to my computer (default)**. 5. Click **OK**.
IDPV-3334	H	**Summary**: 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. **Workaround**: None
IDPV-5072	H	**Summary**: DPoD is not working on Alpine based docker. **Workaround**: None

Issue	Severity	Synopsis
IDPV-5424	L	**Summary**: Momentarily, there are two IDPV icon visible in system tray. **Workaround**: None
IDPV-7193	L	**Summary**: SSP loops back to the start of enrollment page **Workaround**: None
ASAC-16734	L	**Summary**: Friendly name doesn't appear when certificate is imported via Import API. **Workaround**: None
IDPV-8603	M	**Summary**: Old IDPV Client Windows SDK does not work with latest IDPV Client and Server. **Workaround**: None
IDPV-8673	M	**Summary**: Unable to uninstall IDPV Client after upgrading it with the Credential Provider component. **Workaround**: None
IDPV-8681	M	**Summary**: IDPV Client upgrade fails to go to online. **Workaround**: None
IDPV-8683	L	**Summary**: The Token PIN window takes some time to display the incorrect password error. **Workaround**: None
IDPV-8691	L	**Summary**: Currently, the upgrade of the **Microsoft.Web.Webview2** version is categorized as Low vulnerability. **Workaround**: None
IDPV-8749	L	**Summary**: No warning is displayed when tenant is created with **-f** as **false**. **Workaround**: None
IDPV-8751	L	**Summary**: On swagger `isAutoOfflineBundleDownloadEnabled` is showing incorrect value in **GetTenantDetails**. **Workaround**: None
IDPV-8752	L	**Summary**: Token PIN prompt is getting displayed for blocked tokens. **Workaround**: None
IDPV-8822	M	**Summary**: 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). **Workaround**: 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.

Issue	Severity	Synopsis
IDPV-8761	L	**Summary**: 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. **Workaround**: None
IDPV-8819	L	**Summary**: When resuming after being offline for long hours, the user gets disconnected after a while (3 to 5 minutes). **Workaround**: None
IDPV-8865	H	**Summary**: Offline bundle is not expired even after service restart when server is not reachable. **Workaround**: None
IDPV-8370	H	**Summary**: Offline bundle is not expired even after service restart when server is not reachable. **Workaround**: None
IDPV-8626	H	**Summary**: Virtual smart card is automatically switching to the offline mode. **Workaround**: 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).