SafeNet IDPrime Virtual v2.3

RELEASE NOTES

Issue Date: February 2023

Build:
Server (Evaluation version): 2.3.0.450
Server (Full version): 2.3.0.448
Windows Client: 2.3.0.690
Document Part Number:007-000656-001 Rev D

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 v2.3 Release includes enhancements and bug fixes from previous version.

New Features and Enhancements

This release offers the following:

- Support for Oracle, and PostGreSQL database.
- Added support for log generation and proxy in JWT Generator utility.
- Updated Tenant Config Utility for usage commands
- Added support for onboard key generation using provisioning APIs.
- Added support for the following Identity providers (IDPs):
  - PingFederate
  - SAS PCE with Keycloak agent
  - Okta
- Availability of full version server image based on Alpine Linux distribution along with .Net 6 upgrade.
- Support for SoftHSM (evaluation version only).
- Added support for SKS mode on Luna 7.7 HSM.
- Enhancements done in IDPV server, client and credential provider for better error handling and logging.
- Added Self-Service Portal: A web application that enables download of certificates (credentials) on Android and iOS devices supported by partner mobile application. Self-Service Portal is currently available with evaluation package only.
- Added support for Remote Desktop applications (Devolutions, Royal TS, and Dameware).

Deployment Configuration

Deploy the following configuration setting for the latest release package:

Update in `idp-config.json`:

- `IdentityProvider` key is added in `idp-config.json` which signifies the name of the identity provider. Example: `IdentityProvider`: "`STA`".

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.

IDP	RedirectURL in idp-config.json	RedirectURL in IDP Server	
		Structure	**Example**
STA	https://<server-host>/oauth-callback	https://<server-host>/*	https://www.idpvserver.com/*
PingFed	https://<server-host>/oauth-callback	https://<server-host>/*	https://www.idpvserver.com/*
Okta	https://<server-host>/oauth-callback	https://<server-host>/oauth-callback	https://www.idpvserver.com/oauth-callback
		https://<server-host>/redirect	https://www.idpvserver.com/redirect
SAS PCE with Keycloak agent	https://<server-host>/oauth-callback	https://<server-host>/*	https://www.idpvserver.com/*

For details, refer to *SafeNet IDPrime Virtual Server-Client Integration Guide* , 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. Following 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** chapter in *SafeNet IDPrime Virtual Server-Client Product Documentation*.

4. 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** chapter in *SafeNet IDPrime Virtual Server-Client Product Documentation*.

5. `RefreshTokenExpirationDuration`: It is the expiration duration for the refresh access token. For PingFederate and Okta IDPs, 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 Guide*. For STA and SAS PCE with Keycloak agent IDP, this parameter from `idp-config.json` is ignored.

Advisory Notes

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

> `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 Integration Guide*.

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.

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 in hexadecimal (24 zeros in binary).

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’ chapter 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)
  - 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

> **NOTE** In case of full server build (Alpine based Docker image), the MSSQL prompts an error message. Refer to IDPV-5394 for more details.

Middleware

- SafeNet Authentication Client 10.8 R8 GA
- SafeNet Minidriver 10.8 R8 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.

Tokens

Following tokens are supported:

Smart Card Readers

- Gemalto Virtual Smart Card

Device Features Supported by IDPV

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

Features:	Device: SafeNet IDPrime Virtual
Number of Key	15 max
RSA Key Sizes	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

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
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 R8
- SafeNet Minidriver 10.8 R8 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.

To upgrade IDPV client, uninstall the current version then install the latest version.

> **NOTE** If you have IDPV server v2.0 installed, then it is recommended to uninstall the IDPrimeVirtualServer database instance before installing v2.1 or higher versions.

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-4939	M	Import certificate issue in Luna 6 clone mode.
IDPV-1178	H	If a user is added to the IDPV whitelist then no validations can be done.
IDPV- 4680	H	When you login to *connect_on_behalf* with a user, the IDP tries to create a virtual card.
IDPV- 4663	H	IDPV behaves differently with intermittent issues.
IDPV- 4720	H	IDPV smart card ratification counter not decrementing for wrong User PIN during the Provisioning mode.
IDPV- 4275	H	SafeNet IDPrime Virtual is unable to connect with the "HttpError" message. (Customer ID: CS1313498)
IDPV- 4012	H	After the refresh token interval time-out, SAC stops displaying the token and IDPV tray menu icon shows in green color.
IDPV- 4201	M	Getting *smart card login failed* 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

Issue	Severity	Synopsis
IDPV- 4732	H	Multiple IDP windows opening at the same time.
IDPV-4988	M	For untrusted certificates errors are appearing twice.
IDPV-4997	M	Invalid/Wrong user notification error in case user is working offline without network.
IDPV-5012	C	CP does not connect and machine hangs on lock screen.
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-4963	M	Duplicate notification issue for delete token.
SAS-54719	M	When connecting the SafeNet IDPrime Virtual application through Credential Provider, the Credential Provider does not show a proper Keycloak-SASPCE login screen.
IDPV-4798	L	Error message is unclear when user istrying to login to offline bundle that has expired.

Known Issues

Issue	Severity	Synopsis
IDPV-5072	H	DPoD is not working on Alpine based docker.
IDPV-3334	H	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.
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**.

Issue	Severity	Synopsis
IDPV-4503	M	The quality error pop-up during the initialization if the Pin is not matching for preserver token settings.
IDPV-4504	M	Administrator pin retries get synchronized, but not the User Pin retries for the preserve token settings.
ASAC-15226	H	The User Pin retries counter does not decrease with a wrong password attempt of length less than four characters.
SAS-50616	L	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.
ASAC-14899	L	SafeNet Authentication Client (SAC) does not show a prompt while changing the Pin.
IDPV-4986	H	In case of incorrect IDP configuration, connection via Credential Provider do not generate any logs in the Event viewer.
IDPV-4980	H	CP- IDPV Credential Provider and systray remains connected even after offline bundle expires.
IDPV-4787	H	"Connect" doesn't create token for admin after "Connect on behalf" if Admin has no token already.
ASAC-15347	H	Machine hangs when the credential provider connects with etoken.cache containing huge data.
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.
IDPV-5266	M	SWS Sign API fails on Luna 6 HSM.
IDPV-5310	L	Certificate Signing Request (CSR) is generated with no Common Name (CN) value in the subject distinguished name field.
IDPV-5424	H	If you run Modify command from IDPV Client installer, momentarily two IDPV icons are displayed in the system tray.
IDPV-5423	M	If `RefreshTokenExpirationDuration` parameter in `idpconfiguration.json` 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-5394	H	Invariant culture error with MSSQL database in alpine based docker.

Issue	Severity	Synopsis
IDPV-5425	L	In the IDPV system tray, under the Connect on Behalf menu, some tokens are displayed inconsistently.
IDPV-5433	M	In case of invalid password in offline bundle, the displayed error message is vague.
IDPV-4510	M	Logout not working for Self-Service Portal with Ping Federate and Okta IDP.
IDPV-5444	M	Login does not work for the first time if JWT expires(offline mode).
IDPV-5553	H	In case of multiple certificates in a single `pfx` file, imported certificates are not visible in SAC.

Related Product Documentation

The following documentation is associated with this release:

PDF

- 007-000291-005_SafeNet IDPrime Virtual_ServerClient_2.3_Product_Documentation_Rev D
- 007-001593-001_SafeNet IDPrime Virtual_ServerClient_2.3_Integration_Guide_Rev C
- 007-000998-001_SafeNet IDPrime Virtual_ServerClient_2.3_Windows_SDK_Guide_RevC

HTML

- API Key Management API Guide
- Provisioning API Guide
- Signature Web Service Guide

We have attempted to make these documents 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).