STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSL VPN CLIENT

RELEASE NOTES

Version 3

Document last updated: May 30, 2024

Reference: sns-en-ssl_vpn_client_release_notes-v3.2.4

Table of contents

In the documentation, Stormshield Network SSL VPN Client is referred to in its short form: SN SSL VPN Client and Stormshield Network Security under the short form SNS.

This document is not exhaustive and minor changes may have been included in this version.

Change log

Date	Description
May 30, 2024	New document

New firewall behavior

This section lists the changes made to the automatic behavior of the SN SSL VPN Client when it is updated from the latest available version 2 to 3.2.4.

Changes introduced in version 3.2.3

Find out more

- Local "OpenVPN Administrators" group - The Windows user no longer needs to belong to the local "OpenVPN Administrators" group.
  The changes introduced in version 3.2.0 no longer apply.

Changes introduced in version 3.2.0

- Local "OpenVPN Administrators" group - The Windows user must now belong to the local "OpenVPN Administrators" group. Otherwise, SN SSL VPN Client will not be able to set up VPN tunnels.
  To check whether the user belongs to the group, execute the command `net localgroup "OpenVPN Administrators"` in the Windows command prompt. To manually add the user to the group, run `net localgroup "OpenVPN Administrators" "myuser" /add` (replace myuser with the relevant user).

  This requirement no longer applies from version 3.2.3.

Changes introduced in version 3.0.0

Find out more

- Compatibility - SN SSL VPN Client in version 3.0.0 is now a 64-bit service, so it is compatible only with 64-bit operating systems.

Resolved vulnerabilities in version 3.2.4

OpenVPN

A low severity vulnerability was fixed in OpenVPN.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2024-014.

Compatibility

For more information, refer to the section SSL VPN client in the *Product life cycle guide*.

> **NOTE**
> SN SSL VPN Client is not compatible with computers, smartphones and tablets equipped with ARM processors.

Multifactor authentication methods

This table lists the compatible multifactor authentication methods according to the version installed on the SNS firewall and the connection mode that the **SN SSL VPN Client** uses.

SNS versions	Connection mode used by the SN SSL VPN Client	Password + OTP	OTP only	Push mode	TOTP
4.7 or higher	All modes	✓	✓	✓	✓
4.3 LTSB	All modes	✓	✓	✓	✗
3.7 LTSB 3.11 LTSB	Automatic mode	✗	✗	✗	✗
	Manual mode	✓	✓	✗	✗

Known Issues

The up-to-date list of the known issues related to this SN VPN SSL Client version is available on the Stormshield **Knowledge base**. To connect to the Knowledge base, use your **MyStormshield** customer area identifiers.

Documentation resources

The technical documentation resources are available in the documentation base on the Stormshield technical documentation. We suggest that you rely on these resources for a better application of all features in this version.

Please refer to the Stormshield Knowledge base for specific technical information and to watch videos that the TAC (Technical Assistance Center) has created.

Downloading this version

Follow the steps below to download SN SSL VPN Client version 3.2.4.

1. Log in to your MyStormshield personal area.
2. Go to **Downloads** > **Downloads**.
3. Select **Stormshield Network Security** > **SSL VPN** from the suggested categories.
4. Depending on the language chosen and the Windows version used, click on the SN SSL VPN Client installation program (*.msi* file). The download will begin automatically.
5. Enter one of the following commands to check the integrity of the retrieved binary files:
   - Linux operating systems: *sha256sum < filename>*
   - Windows operating systems:: *CertUtil -hashfile <filename> SHA256*

   Next, compare the result with the hash indicated in MyStormshield. To view it, click on **Show** in the **SHA256** column of the file in question.

NOTE
This version can also be downloaded from the Stormshield SSL VPN website or from the captive portal of the SNS firewall that hosts the SSL VPN service. You must log in to MyStormshield to check the integrity of binary files.

Previous versions of SN SSL VPN Client 3

In this section, you will find the features, resolved vulnerabilities and fixes from previous versions of SN SSL VPN Client 3.

3.2.3			Bug Fixes
3.2.2			Bug Fixes
3.2.1		Resolved vulnerabilities	Bug Fixes
3.2.0	New features	Resolved vulnerabilities	Bug Fixes
3.1.1			Bug Fixes
3.1.0		Resolved vulnerabilities	Bug Fixes
3.0.1			Bug Fixes
3.0.0	New features	Resolved vulnerabilities	Bug Fixes

Version 3.2.3 bug fixes

Address book - OTP

Support reference 84763

The address book now takes into account multifactor authentication (OTP) when it connects to an address.

More information on configuring and using the SN SSL VPN Client.

Installation

Local Windows "OpenVPN Administrators" group

Support reference 85105

In some cases, the Windows user was not added to the local "OpenVPN Administrators" group when the installation of the SN SSL VPN Client was complete, preventing the user from setting up VPN tunnels. To fix this issue, the Windows user now no longer needs to belong to the local "OpenVPN Administrators" group.

Windows environment variables

Support references 85167 - 85168

The installation of the SN SSL VPN Client would fail whenever the value of the Windows environment variable "*Path*" was changed. This issue, which generated the errors "*pnputil.exe failed with return code 9009*" and "*GENERATE_OVPN_AUTH*", has been fixed. The SN SSL VPN Client installation mechanism now uses the Windows environment variable "*SystemRoot*" instead of "*Path*".

Do note that the installation of the SN SSL VPN Client will fail if the value of the "*SystemRoot*" variable is changed and no longer matches the Windows installation folder (e.g., *C:\Windows*).

Version 3.2.2 bug fixes

NOTE
In some cases, the installation of the SN SSL VPN Client in Windows 10 or 11 may fail. If you are affected by this issue, contact Stormshield support (support refer 84756).

Installation

Installation on Windows user profiles that contain spaces

Support reference 85042

An issue that prevented the SN SSL VPN Client from being installed, due to a space in the profile of the Windows user, has been fixed. This issue occurred particularly when the settings for short name behavior (8dot3 name) were disabled in Windows.

Deployment via GPO

Support reference 85010

An issue made the deployment of the SN SSL VPN Client difficult via GPO if an earlier version had been installed manually on the user's workstation.

This issue has been fixed for future deployments: if a version equal to or higher than 3.2.2 has been installed manually on the workstation, a version higher than the original will be deployed normally via GPO.

If a version older than version 3.2.2 has been installed manually on the workstation, a version equal to or higher than 3.2.2 will be deployed via GPO, but the user's workstation must be restarted.

Multifactor authentication - OTP

Execution of an opening script

Support reference 84754

Users needed to authenticate a second time in order to open the VPN tunnel when both of these elements were configured:

- OTP authentication,
- A script created via the Windows notepad, which had to be run when the SSL VPN connection started.

This issue has been fixed.

System

Shutdown of the VPN tunnel

Support reference 85070

When CPU consumption reached 100% on the Windows workstation for 2 seconds, SN SSL VPN Client considered that Windows was no longer responding, and would then shut down the VPN tunnel.

To reduce the frequency of these shutdowns, the duration has been increased from 2 to 60 seconds, and can be configured individually by user in the following Windows registry key: **HKEY_CURRENT_USER\SOFTWARE\Stormshield\STORMSHIELD SSL VPN CLIENT\living_timeout**.

Resolved vulnerabilities in version 3.2.1

OpenSSL

A moderate severity vulnerability was fixed in OpenSSL.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-011.

Version 3.2.1 bug fixes

Multifactor authentication - OTP

Support reference 85005

An issue that prevented authentication with an OTP has been fixed. This regression appeared in SN SSL VPN Client version 3.2.0.

.bat scripts run by SN SSL VPN Client

Interruption of the VPN tunnel after running an opening script

Support reference 85009

When SN SSL VPN Client ran a script while the VPN tunnel was being set up with the SNS firewall, the tunnel would be interrupted if the execution of the script lasted two seconds or more. This issue, which generated the error "*The SSL VPN was disconnected when Windows was in sleep or hibernate mode, so you must log in again*." has been fixed.

Removal of opening and closing scripts

Support reference 85013

Scripts run by SN SSL VPN Client when opening or closing the VPN tunnel with the SNS firewall were not deleted from the Windows workstation when they were removed from the SNS firewall's SSL VPN configuration. As such, these scripts would continue to run. This issue has been fixed.

New features and enhancements in version 3.2.0

Installation

From version 3.2 of the SN SSL VPN Client onwards, the client can be installed on a host without the need to uninstall the original version, as long as the original is equal to or higher than version 2.9.

Resolved vulnerabilities in version 3.2.0

System

A high severity vulnerability was fixed in the SN SSL VPN Client.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-028/.

Several moderate severity were fixed in the SN SSL VPN Client.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2022-028/,
- https://advisories.stormshield.eu/2022-029/.

Version 3.2.0 bug fixes

Using the client on a Windows user profile with special characters

Support reference 84668

The SN SSL VPN Client now runs correctly when it is installed on a Windows user profile with a user name that contains special characters (é, ç, ę, ć, etc.). Previously, this issue would generate the error "*Failed to extract the configuration file*".

Quitting sleep or hibernate mode on a Windows workstation

Support reference 84499

If the VPN was not disconnected and the Windows workstation went into sleep or hibernate mode, the routes included in the SSL VPN configuration and installed on the workstation were not deleted. This could prevent the VPN tunnel from functioning after it quits sleep or hibernate mode.

This issue has been fixed and the VPN tunnel is now automatically disconnected after it quits sleep or hibernate mode. The user is informed of this with a notification.

Version 3.1.1 bug fixes

System

Installing SN SSL VPN Client

Support reference 84687

SN SSL VPN Client version 3.1.0 could not be installed if the TAP network driver was already present on the system. This issue has been fixed. The issue would generate the "*There is a problem with the Windows Installer package.*" error.

Uninstalling SN SSL VPN Client

It is now possible to uninstall SN SSL VPN Client version 3.1.0 if the TAP network driver is no longer present on the system.

Resolved vulnerabilities in version 3.1.0

System

A high severity vulnerability was fixed in SN SSL VPN Client.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-004/.

Version 3.1.0 bug fixes

System

Setting up tunnels

Support reference 82807

An issue, which prevented SSL VPN tunnels from being set up when proxy settings were configured in Internet Explorer properties, has been fixed. This regression appeared in SN SSL VPN Client version 2.9.1.

Version 3.0.1 bug fixes

System

Automatic mode - Entering a custom port

Support reference 84329

In automatic mode, SN SSL VPN Client now correctly applies custom ports entered for the captive portal (other than default port 443).

Missing *auth_management.txt* file after installing SN SSL VPN Client

Support reference 84348

In some configurations, even after the installation of SN SSL VPN Client has ended, the *auth_management.txt* file would not be installed on the system, therefore preventing SN SSL VPN Client from running. This issue has been fixed.

New features and enhancements in version 3.0.0

Compatibility

SN SSL VPN Client in version 3.0.0 is now a 64-bit service, so it is compatible only with 64-bit operating systems.

Multifactor authentication - OTP

Users can now specify that they use multifactor authentication by selecting a new option in the SN SSL VPN Client connection window in version 3.0.0. After selecting this option, the user can enter an OTP in a separate field.

This additional field allows SN SSL VPN Client to support the following multifactor authentication methods:

- **Password + OTP**: to use this method, select the **Use multifactor authentication** checkbox and fill in the **Password** and **OTP code** fields.
- **OTP only**: to use this method, select the **Use multifactor authentication** checkbox, leave the **Password** field empty and fill in the **OTP code** field.
- **Push mode**: to use this method, select the **Use multifactor authentication** checkbox and leave the **Password** and **OTP code** fields empty.

For more information on the compatibility of multifactor authentication methods according to the version installed on the SNS firewall and the connection mode used by SN SSL VPN Client, refer to to the section on Compatibility.

More information about how to configure and use SSL VPN on SNS firewalls.

Resolved vulnerabilities in version 3.0.0

System

A moderate severity vulnerability was fixed in SN SSL VPN Client.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-019/.

Version 3.0.0 bug fixes

System

Disconnecting the tunnel when the session shuts down

Support references 81985 - 82934 - 83152

When users closed then reopened their Windows session without restarting their machine, SN SSL VPN Client would not disconnect the tunnel when the Windows session was shut down. The tunnel would therefore remain up when the Windows session was reopened even though the SN SSL VPN Client icon in the taskbar indicated otherwise. This issue has been fixed.

Deployment with Microsoft Intune

Support reference 82577

SN SSL VPN Client in version 2.9 no longer functioned after it was deployed with Microsoft Intune. This issue has been fixed.

Contact

To contact our Technical Assistance Center (TAC) Stormshield:

- https://mystormshield.eu/

All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under **Technical support > Manage cases**.

- +33 (0) 9 69 329 129

In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu.

All images in this document are for representational purposes only, actual products may differ.