STORMSHIELD

STORMSHIELD NETWORK SECURITY
STORMSHIELD NETWORK SSL VPN CLIENT

RELEASE NOTES
Version 3

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.

Compatibility

The following platforms are compatible with SN SSL VPN Client 3.1.1.

Stormshield Network Firewall

3.x and 4.x

Operating systems

Windows 8.1 - 64 bits
Windows 10 - 64 bits (up to date)
Windows 11 - 64 bits

> **ℹ 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 version	Connection mode used by the SN SSL VPN Client	Password + OTP	OTP only	Push mode	TOTP
4.5 or higher	All modes	✅	✅	✅	✅
4.3 and 4.4	All modes	✅	✅	✅	❌
3.x, 4.2 or below	Automatic mode	❌	❌	❌	❌
	Manual mode	✅	✅	❌	❌

The SN SSL VPN Client's connection modes are: Automatic mode and manual mode. Do note that the address book (with Automatic mode) does not allow multifactor authentication.

Version 3.1.1 bug fixes

System

Installing SN SSL VPN Client

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.

Recommendations

Installing SN SSL VPN Client

When SN SSL VPN Client has been installed through msi package, you must uninstall it before installing the new version.

Documentation

The following technical documentation resources are available on the Stormshield Technical Documentation website or on Stormshield Institute website. We suggest that you rely on these resources for a better application of all features in this version.

Guides

- Stormshield Network Firewall - User and configuration manual

Technical notes

- Configuring and using SSL VPN on SNS firewalls

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

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 3.1.1 version of SN SSL VPN Client:

1. Log in to MyStormshield with your personal identifiers.
2. In the left panel, select **Downloads**.
3. In the right panel, select the relevant product and version.

Checking the integrity of the binary files

To check the integrity of SN SSL VPN Client binary files:

1. Enter one of the following commands and replace `filename` by the name of the file you want to check:
   - Linux operating system: `sha256sum filename`
   - Windows operating system: `CertUtil -hashfile filename SHA256`
2. Compare with hashes provided on MyStormshield personal area, section **Downloads**.

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.

3.1.0		Resolved vulnerabilities	Bug Fixes
3.0.1			Bug Fixes
3.0.0	New features	Resolved vulnerabilities	Bug Fixes

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.

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** > **Report an incident / Follow up on an incident**.

- +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.

Copyright © Stormshield 2023. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.