# STORMSHIELD

# STORMSHIELD NETWORK SECURITY
STORMSHIELD NETWORK SSL VPN CLIENT

# RELEASE NOTES
Version 3

Document last updated: May 12, 2022

Reference: sns-en-ssl_vpn_client_release_notes-v3.0.1

# 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.

# 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.

# Compatibility

The following platforms are compatible with SN SSL VPN Client 3.0.1.

## Stormshield Network Firewall

2.x, 3.x and 4.x

## Operating systems

Windows 8.1 - 64 bits
Windows 10 - 64 bits
Windows 11 - 64 bits

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

## Multi-factor authentication methods

This table provides a summary of the compatible multi-factor authentication methods according to the version installed on the SNS firewall and the connection mode that **SN SSL VPN Client** uses.

| SNS version | SN SSL VPN Client connection mode | Compatible multi-factor authentication methods |
|---|---|---|
| 4.3 and higher versions | Automatic mode | • Password + one-time password<br>• One-time password only<br>• Push mode |
| | Sites mode (manual) | |
| 3.x, 4.2 and lower versions | Automatic mode | • Not compatible |
| | Sites mode (manual) | • Password + one-time password<br>• One-time password only |

# Recommendations

## Installation

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

- SSL VPN tunnels

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 3.0.1 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.

| 3.0.0 | New features | Resolved vulnerabilities | Bug Fixes |

# 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. It is therefore compatible only with 64-bit operating systems.

## Multi-factor authentication - OTP

Users can now specify that they use multi-factor authentication, by selecting a new option in the SN SSL VPN Client connection window in version 3.0.0. After selecting the option, users can then enter a one-time password (OTP) in a specific field.

The addition of this option allows SN SSL VPN Client to support the following multi-factor authentication methods:

- **Password + one-time password**: to use this method, the checkbox specifying the use of multi-factor authentication must be selected and the **Password** and **OTP** fields must be filled in,

- **One-time password only**: to use this method, the checkbox specifying the use of multi-factor authentication must be selected, the **Password** field must be left empty and **OTP** field must be filled in,

- **Push Mode**: to use this method, the checkbox specifying the use of multi-factor authentication must be selected and the **Password** and **OTP** fields must be left empty.

For more information on the compatibility of multi-factor authentication methods according to the version installed on the SNS firewall and the connection mode that SN SSL VPN Client uses, refer 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.*