



STORMSHIELD



STORMSHIELD NETWORK SECURITY
STORMSHIELD NETWORK SSL VPN CLIENT

RELEASE NOTES

Version 4

Document last updated: September 24, 2024

Reference: [sns-en-ssl_vpn_client_release_notes-v4.0.7-EA](#)



Table of contents

Change log	3
New SN SSL VPN Client behavior	4
Version 4.0.7 EA bug fixes	5
Compatibility	6
Known issues	7
Limitations and explanations on usage	8
Documentation resources	9
Downloading this version	10
Previous versions of SN SSL VPN Client 4	11
Contact	22

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
September 24, 2024	New document



New SN SSL VPN Client 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 3 to 4.0.7 EA.

Changes introduced in version 4.0.5 EA

- Address book - The address book format has been changed to increase security on the SN SSL VPN Client. The address book is automatically updated when it is opened with SN SSL VPN Client in version 4.0.5 EA. For more information, refer to the entry *Downgrading to an earlier version* in the section [Limitations and explanations on usage](#).
- Compatibility - SN SSL VPN Client is no longer compatible with Windows 8.1.
- Certificates:
 - As the SHA-1 and MD5 algorithms make it possible to sign certificates that are obsolete, they will no longer be supported in a later version of SN SSL VPN Client. It is essential for administrators to update their certificates immediately. Refer to the procedure in the article on [How can I regenerate the sslvpn-full-default-authority?](#) in the Stormshield knowledge base.
 - The SN SSL VPN Client installation folder in version 4 has been changed. During the initial connection, some users will need to indicate once again that the SNS firewall certificate has to be trusted.



Version 4.0.7 EA bug fixes

Connection

When the password contains a special character as &, the connection to SN SSL VPN Client v4 was impossible in automatic mode. This issue has been fixed.



Compatibility

For more information, refer to the section [SSL VPN client](#) in the *Product life cycle guide*.

For more information on the compatibility of authentication methods and SN SSL VPN Client features, refer to the section [Specific characteristics of Stormshield SSL VPN clients](#) in the technical note *Configuring and using the SSL VPN on SNS firewalls*.



Known issues

The updated list of known issues relating to this version of SN SSL VPN Client can be found in the Stormshield [Knowledge base](#). To log in to the Knowledge base, use the same credentials as for your [MyStormshield](#) client area.

Multi-account installation

SN SSL VPN Client must not be launched on several user profiles simultaneously.

If users lock their sessions without shutting down their VPN tunnel, the tunnel in question will remain up, allowing other users to use the same tunnel from another session. We recommend that users who share a Windows workstation with other users ensure that they shut down their sessions.

For more information, refer to the Stormshield knowledge base article [SSLVPN should close VPN connection when locking computer](#).



Limitations and explanations on usage

Multi-account installation

SN SSL VPN Client must not be launched on several profiles simultaneously. We recommend that users who share a Windows workstation with other users ensure that they shut down their sessions. Otherwise, the workstation will need to be restarted so that other users can set up tunnels.

Downgrading to an earlier version

Downgrading to an earlier version of SN SSL VPN Client is not supported.

The address book saved on the workstation can no longer be accessed if the update is towards a major version lower than the original version (e.g. downgrading from a 4.x version to a 3.x version).

Error message "Could not purge the log file of the OpenVPN process"

In the SN SSL VPN Client connection window, the error message "Could not purge the log file of the OpenVPN process" may appear if you click repeatedly on OK. Wait several seconds before clicking again on OK in order to log in.

Displaying the icon in the Windows 11 system tray

In Windows 11, ensure that the display of the SN SSL VPN Client icon has been enabled in the Windows system tray (in **Taskbar settings** > **Other system tray icons** > **Hidden icon menu**). If this is not the case, none of the features will be accessible, as they require access to the icon of the application in order to open its menu.



Documentation resources

Technical documentation resources are available on the [Stormshield technical documentation](#) website. We recommend that you rely on these resources to get the best results from 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 4.0.7 EA.

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. Click on the SN SSL VPN Client installation program (*.msi* or *.exe* 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.

i 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 4

In this section, you will find new features, resolved vulnerabilities and fixes from previous versions of SN SSL VPN Client 4.

4.0.6 EA		Bug fixes
4.0.5 EA	New features	Bug fixes
4.0.4		Version not published
4.0.3		Version not published
4.0.2		Version not published
4.0.1		Version not published
4.0.0		Version not published



Version 4.0.6 EA bug fixes

Compatibility

SN SSL VPN Client v4 is compatible again with SNS firewalls version 4.3. This regression appeared in version 4.0.5 EA



New features and enhancements in version 4.0.5 EA

Compliance verification (ZTNA)

SN SSL VPN Client is compatible with the feature that verifies the compliance of client workstations, which can now be configured on SNS firewalls in from version 4.8 onwards.

[More information on the SNS firewall compliance verification.](#)

Installation

Multi-account installation

SN SSL VPN Client can now be installed on several user profiles on the same Windows workstation. Individual users have their own address books and own logs.

However, SN SSL VPN Client must not be launched on several profiles simultaneously. We recommend that users who share a Windows workstation with other users ensure that they shut down their sessions. Otherwise, the workstation will need to be restarted so that other users can set up tunnels.

Do note that:

- The installation always requires local administrator privileges on the workstation or the user must enter the login and password of an administrator account,
- The SN SSL VPN Client installation folder in version 4 has been changed. During the initial connection, some users will need to indicate once again that the SNS firewall certificate has to be trusted.

Configuring settings

During installation, you can now define the following settings:

- The IP address or FQDN of the SNS firewall,
- Whether the VPN configuration must be retrieved in automatic mode,
- Whether multifactor authentication has to be used,
- Whether the Windows session user in question must be used as the ID.

Installation package

A single SN SSL VPN Client installation program now groups all languages and Windows versions supported. The administrator can still download an .msi package for an installation through a policy deployment tool.

Updated certificates

As the SHA-1 and MD5 algorithms make it possible to sign certificates that are obsolete, they will no longer be supported in a later version of SN SSL VPN Client. It is essential for administrators to update their certificates immediately. Refer to the procedure in the article on [How can I regenerate the sslvpn-full-default-authority?](#) in the Stormshield knowledge base.



For greater security, support for these algorithms can now be disabled by deleting the value "insecure_compat", or by setting it to 0 in the registry key:

HKLM\SYSTEM\CurrentControlSet\Services\StormshieldSSLVPNService\Parameters



Version 4.0.5 EA bug fixes

Certificates - Security

Previously, if:

- SN SSL VPN Client used a root authority certificate that was found in the Windows store,
- The SN SSL VPN Client file used the certificate name indicated in the captive portal's certificate,

A certificate error message would appear in loop. This issue has been fixed.

Timeout of HTTPS requests

Previously, if:

- The tunnel was established for the first time or the configuration was modified,
- The user used a RADIUS authentication,

Then the timeout of HTTPS requests was too short to allow the user to authenticate using a third-party application (multifactor authentication). Now, there are three parameters for setting the timeout in the registry key

HKLM\SYSTEM\CurrentControlSet\Services\StormshieldSSLVPNService\Parameters:

- `https_connect_timeout`: defines the timeout for the connection to SNS. The default value is 30 seconds.
- `https_recvsend_timeout`: defines the timeout for the emission and reception of an answer, including a RADIUS authentication. The default value is 30 seconds. This parameter must be added to the registry key to change the default value.
- `https_resolve_timeout`: defines the timeout for a FQDN address resolution. The default value is 0 second. This parameter must be added to the registry key to change the default value.

If the value of a parameter is 0 second, then there is no timeout.

Address book

Saving after an import

The **Save** button, which used to be grayed out after importing an address book, is now available. This regression appeared in SN SSL VPN Client version 3.2.3.

Missing translation

The contents of the OTP column have been translated.

Wrong tab sequence

In the window allowing new entries to be added to the address book, the order in which fields are tabbed has been changed.




OTP authentication

Support reference 84809

Where:

- SN SSL VPN Client is configured in automatic mode with multifactor authentication,
- Changes relating to the SSL VPN have been made on the SNS side and the SSL VPN service has been restarted.

Previously, VPN tunnels would be shut down and SN SSL VPN Client would attempt to reconnect these tunnels without applying the changes to the configuration. This issue has been fixed and SN SSL VPN Client will now request two OTPs in such a situation.

 For more information on automatic mode, refer to the section [Specific characteristics of Stormshield SSL VPN clients](#) in the technical note *Configuring and using the SSL VPN on SNS firewalls*.

Update

Following an update, now only the latest version of SN SSL VPN Client will be kept. Previously, the former version was also kept.

Logs

Previously, some characters in log error messages would not be correctly displayed. This issue has been fixed.



Version 4.0.4 not published

Version 4.0.4 is not available to the public.



Version 4.0.3 not published

Version 4.0.3 is not available to the public.



Version 4.0.2 not published

Version 4.0.2 is not available to the public.



Version 4.0.1 not published

Version 4.0.1 is not available to the public.



Version 4.0.0 not published

Version 4.0.0 is not available to the public.



Contact

To contact our Stormshield Technical Assistance Center (TAC):

- <https://mystormshield.eu/>

All requests to technical support must be submitted through the incident manager in the **MyStormshield** client area, under **Technical support > Ticket management**.

- +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 **MyStormshield**.



STORMSHIELD

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

Copyright © Stormshield 2024. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.