STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSL VPN CLIENT

RELEASE NOTES

Version 4

Document last updated: December 13, 2024

Reference: sns-en-ssl_vpn_client_release_notes-v4.0.9

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
December 13, 2024	"Early Adopter" (EA) label removed from 4.0.9 version
November 13, 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 4.0.9.

Changes introduced in version 4.0.5 EA

- Address book - The address book format has been changed to increase security on SN SSL VPN Client version 4. This new format is not compatible with lower versions. For more information, refer to the section Limitations and explanations on usage in the technical note *Configuring and using the SSL VPN on SNS firewalls*.
- 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 4.0.9 bug fixes

System

Communication with the OpenVPN process

The mechanism that verifies the port used by the Stormshield SSL VPN client to communicate with the OpenVPN process has been enhanced. Errors such as “Could not reserve the port to communicate with the OpenVPN process” and “Could not purge the log file of the OpenVPN process” no longer appear unexpectedly.

Now, when the port verification fails, the message “Connection to the OpenVPN process is not secure” appears.

Multi-account installation

Enhancements have been applied to multi-account installations. Now, when a VPN tunnel is set up in a locked session, the tunnel will automatically be disconnected when other users open their own sessions.

There is no longer any need to ask individual users sharing a workstation to close their sessions after use. Each user can therefore set up his or her own tunnel, but only one tunnel can be set up at a time on the workstation.

Access to logs

When no connection attempts have been made, and no logs have been generated, clicking on the **Logs** pop-up menu now correctly redirects the user to the log destination folder.

Connection

Connecting to the SNS firewall - TCP or UDP port blocked

When the connection to the SNS firewall does not succeed because the TCP or UDP port has been blocked on it, the Stormshield SSL VPN client will no longer wrongly attempt to connect continuously. Now the message “Unable to connect to SSL VPN: the maximum number of connection attempts has been reached” appears after five connection attempts.

Connecting to the SNS firewall in version 4.3 - Customized certificate

Support reference 84992

Users can now set up a VPN tunnel with a customized certificate when the firewall is in SNS version 4.3. This regression appeared in version 4.0.5 EA.

Filling in the OTP - Push mode field

The **OTP** field no longer needs to be filled in, making it possible once again to connect through push notifications (**Push mode**). This regression appeared in version 4.0.5 EA.

Manual mode

Displaying profiles in the pop-up menu

Address book entries from the Stormshield SSL VPN client are no longer wrongly displayed in the **Manual mode** pop-up menu.

Adding or deleting profiles when a VPN tunnel has been set up

Profiles can no longer be added or deleted in the **Manual mode** pop-up menu once a VPN tunnel has been set up. Previously, remaining items from profiles would persist when such profiles were deleted after a VPN tunnel had been set up.

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.

Limitations and explanations on usage

For more information, refer to the section Limitations and explanations on usage in the technical note *Configuring and using the SSL VPN on SNS firewalls*.

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 that the TAC (Technical Assistance Center) has created.

Downloading this version

Follow the steps below to download SN SSL VPN Client version 4.0.9.

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.

> **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 v4

In this section, you will find new features, resolved vulnerabilities and fixes from previous versions of SN SSL VPN Client v4.

4.0.8 EA	Version not published		
4.0.7 EA			Bug fixes
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 4.0.8 EA not published

Version 4.0.8 EA is not available to the public.

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.

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** > **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 MyStormshield.

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