STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSO AGENT

RELEASE NOTES

Version 2

Table of contents

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

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

New features in SN SSO Agent 2.0

Authentication

New SN SSO Agent for Linux
A new Linux-based SN SSO Agent supports directories that run on non-Windows systems, such as Samba 4. It can be configured in the **Authentication** module in the web administration interface, and detected through logs exported via Syslog. Exported logs can be filtered by regular expressions configured in the interface.

ℹ NOTE
SNS 4.0.x firewalls are not compatible with the Linux-based SN SSO Agent.

SN SSO Agent 2.0 bug fixes

System

Microsoft Active Directory

Support reference 74708
A vulnerability to memory leaks that occurred during a connection error to the Microsoft Active Directory has been fixed.

Compatibility

The following platforms are compatible with SN SSO Agent 2.0.0:

Windows systems

Stormshield Network Firewall	Active Directories
Versions 3.x and 4.x	Windows Server 2016
	Windows Server 2012 ou 2012 R2

SN SSO Agent is a 32-bit service, compatible with 64-bit operating systems.

> ℹ️ **NOTE**
>
> If NETASQ SSO Agent or SN SSO Agent prior to version 1.4 was previously installed, the service must be uninstalled before beginning the installation of SN SSO Agent.

Linux systems

Stormshield Network Firewall	Operating system
Versions 3.10 and higher	Ubuntu 18.04 LTS

The Linux-based SN SSO Agent is a service compatible only with 64-bit operating systems.

> ℹ️ **NOTE**
>
> SNS 4.0.x firewalls are not compatible with the Linux-based SN SSO Agent.

Explanations on usage

Authentication

If a user known to the SSO agent uses another login from the same domain, the firewall may cancel the identification of this user. The second identification is relayed by the domain controller, which replaces the initial session. Such cases occur especially for the following types of access:

- Login to an intranet using the *kerberos* and/or *ntlm* method,
- Mounting of shared remote resources, e.g., files and printers, via the SMB protocol,
- Login to RDP Terminal Services on a remote server.

Syslog

Communications with the syslog server must be in UDP. Since this protocol does not guarantee confidentiality or integrity, we recommend that you secure communications between non-Windows directories, such as Samba 4, and the syslog server to prevent potential security risks that include IP address spoofing, or the injection of unauthorized syslog messages to the firewall.

Secure these communications by physically segmenting the network, setting up a VLAN, or using IPSec, SSH or SSL tunnels. Alternatively, a TLS syslog server relay can also be placed between the hosts concerned.

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.

User guide

- Stormshield Network Firewall - User and configuration manual

Technical note

- Stormshield Network SSO Agent - Installation and deployment

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

Checking the integrity of the binary files

To check the integrity of Stormshield Network Security 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 customer area, section Downloads.

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 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.