STORMSHIELD NETWORK SECURITY
STORMSHIELD NETWORK SSO AGENT

RELEASE NOTES VERSION 1

English version

June 30, 2017

Table of contents

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

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

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

Stormshield Network SSO Agent 1.6 bug fixes

Authentication field modified

Support reference 64843 - 64342

As the default value of an authentication field returned by Microsoft Active Directory servers had been modified, authentication via the SSO agent would fail. The agent has been modified to recognize the new value of this field.

Compatibility

The following platforms are compatible with Stormshield Network SSO Agent 1.6:

Stormshield Network Firewall	System requirements
Versions 1.x, 2.x and 3.x	Windows Server 2012
Netasq 9.1.x	Windows Server 2011
	Windows Server 2008 or 2008 R2
	Windows 10
	Windows 8 and 8.1
	Windows 7 and 7 SP1

The SSO agent is a 32-bit service, compatible with 64-bit operating systems.

NOTE

If NETASQ SSO Agent was previously installed, the service must be uninstalled before beginning the installation of Stormshield Network SSO Agent.

Explanations on usage

In SNS firmware versions 1 and 2, the SN SSO agent does not support the management of multiple Microsoft domains, containing as a result various directories. As the firewall manages a sole directory, the firewall will not be able to retrieve user groups from the directories. Furthermore, conflicts between accounts may arise if there are common identifiers.

For further information, please refer to the Technical note ***Stormshield Network SSO Agent - Installation and deployment***.

Identification by SSO agent can be cancelled on the firewall if the user of the workstation uses a different login on the domain. This second identification is relayed by the domain controller which replaces the initial session.

These case figures occur in particular for the following types of access:

- Logging on to an intranet with the kerberos and/or ntlm method(s),
- Mounting of shared remote resources (files, printers) via the SMB protocol,
- RDP Terminal Services connection on a remote server.

Documentation

The following technical documentation is available in PDF in the documentation base in the client area. 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 Knowledge base for specific technical information and to watch videos that the TAC (Technical Assistance Center) has created.

Hashes

In order to check the integrity of Stormshield Network SSO Agent binary files, enter one of the following commands and compare the result with the hashes indicated in the MyStormshield client area, under Downloads > SNS > Software:

- Linux operating system: `sha1sum filename`
- Windows operating system: `CertUtil -hashfile filename SHA1`

Replace `filename` with the name of the file you want to check.

Contributions from previous versions of Stormshield Network SSO Agent 1

In this section, you will find the new features, resolved vulnerabilities and fixes from previous versions of Stormshield Network SSO Agent 1.

1.5			Bug fixes
1.4	Features		Bug fixes
1.3		Resolved vulnerabilities	
1.2		Resolved vulnerabilities	
1.1	Features		Bug fixes
Explanations on usage			

Bug fixes for Stormshield Network SSO Agent 1.5

Domains names

Support reference 58993

The SSO agent duplicated the names of the authenticated users when there were differences in the domain name case.

This issue caused the communication between the SSO agent and the firewall to be interrupted, and issued a “Bad ack” message in the logs. It has been fixed.

New features for Stormshield Network SSO Agent 1.4

Support reference 56146

Compatibility with SNS v3 firmware

On firewalls in firmware version 3 and up, the SN SSO agent sends the Microsoft Active Directory domain name of the host on which it has been installed. For firewalls in lower firmware versions, the agent will send the host's Netbios name.

Bug fixes for Stormshield Network SSO Agent 1.4

Support reference 54016

Character encoding

The SSO agent would send the results of its requests to the firewall over a Microsoft Active Directory using ISO encoding. As SNS firewalls use UTF-8 encoding, doing so would cause authentication anomalies for users and groups containing special characters. This issue has been fixed and the agent now uses UTF-8 encoding.

Resolved vulnerabilities for Stormshield Network SSO Agent 1.3

SSL and TLS security flaw

A vulnerability that could cause a Denial of Service attack (CVE-2015-0286) has been resolved with the upgrade of the OpenSSL cryptographic library in version 1.0.1m.

Resolved vulnerabilities for Stormshield Network SSO Agent 1.2

SSL and TLS security flaw

Vulnerabilities that can cause Man in the Middle (MITM) attacks or Denials of Service have been resolved following the upgrade of the OpenSSL cryptographic library to version 1.0.1j. The list of

these vulnerabilities is as follows:

- SRTP Memory Leak (CVE-2014-3513),
- Session Ticket Memory Leak (CVE-2014-3567),
- SSL 3.0 Fallback,
- Build option no-ssl3 is incomplete (CVE-2014-3568).

New features for Stormshield Network SSO Agent 1.1

Transparent authentication on a Microsoft domain

This new authentication method will allow users from a Microsoft domain to authenticate seamlessly.

Stormshield Network SSO Agent, when installed on an Active Directory server or on a workstation in the domain, retrieves information about connections on the domain and sends them to the firewall. Users identified on the domain will automatically be authenticated by the firewall.

Logging off, done via the *Probe* method (ping or registry database), deletes authenticated users when logging off from the machine or when the session is shut down.

The Stormshield Network SSO Agent now supports IPv6 for communication with Active Directory servers and Stormshield Firewalls.

Bug fixes for Stormshield Network SSO Agent 1.1

Support reference 46352 - 47065

Logging off

The *Probe* method (registry database) that detects users logging off has been enhanced.

Contact

To contact our Stormshield Technical Assistance Center (TAC):

- https://mystormshield.eu/
  All requests to the TAC 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, please use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu/.

STORMSHIELD