Stormshield Network SSO Agent

RELEASE NOTE V1

Software compatibility

Firewall firmware

Stormshield Network 1.x

Netasq 9.1.x

System requirements

Windows Server 2003 SP3

Windows Server 2008 R2

Windows Server 2012

Windows 7 SP1

Windows 8

The SSO agent is a 32-bit service, compatible with 64-bit Windows versions.

> **ⓘ NOTE**
>
> If you have installed the NETASQ SSO Agent earlier, you must uninstall this service before proceeding with the installation of the Stormshield Network SSO Agent.

Version

This release note contains the description of the main modifications made to the various versions of the same major version. You are advised to apply the latest version in order to benefit from the most recent developments and bug fixes.

1.1	Features	Bug fixes
Explanations on usage		

1.1 Features

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.

1.1 Bug fixes

Logging off

Support reference 46352 - 47065

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

Explanations on usage

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.