



STORMSHIELD NETWORK SECURITY

STORMSHIELD SSO AGENT

NOTES DE VERSION

VERSION 1

Édition française

11/08/15



Compatibilité logicielle

Firmware du Firewall

Stormshield Network 1.x et 2.x

Netasq 9.1.x

Pré-requis système

Windows Server 2008 ou 2008 R2

Windows Server 2011

Windows Server 2012

Windows 7 ou 7 SP1

Windows 8 ou 8.1

L'Agent SSO est un service 32 bits, compatibles avec les versions Windows 64bits.

NOTE

Si NETASQ SSO a été installé au préalable, il est impératif de désinstaller le service avant de procéder à l'installation de Stormshield Network SSO Agent.

Version

Cette note contient le descriptif des principales modifications apportées aux différentes versions d'une même version majeure. Il est recommandé d'appliquer la dernière version afin de bénéficier des nouveautés et correctifs les plus récents.

1.3	Vulnérabilités résolues	
1.2	Vulnérabilités résolues	
1.1	Fonctionnalités	Correctifs
Précisions sur les cas d'utilisation		



1.3 Vulnérabilités résolues

Faible de sécurité SSL et TLS

Une vulnérabilité pouvant entraîner une attaque de type Déni de Service ([CVE-2015-0286](#)) a été résolue par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1m.

1.2 Vulnérabilités résolues

Failles de sécurité SSL et TLS

Des vulnérabilités pouvant entraîner une attaque de type Man In The Middle (MITM) ou un Déni De Service ont été résolues par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1j. En voici la liste :

- 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](#)).

1.1 Fonctionnalités

Authentification transparente sur un domaine Microsoft

Cette nouvelle méthode d'authentification va permettre d'authentifier de manière transparente les utilisateurs d'un domaine Microsoft.

Stormshield Network SSO Agent installé sur un serveur Active Directory ou sur un poste du domaine, récupère les informations de connexions sur le domaine et les transfère au Firewall Stormshield Network. Un utilisateur identifié sur le domaine sera automatiquement authentifié par le Firewall.

La déconnexion permettant de supprimer les utilisateurs authentifiés lors d'une déconnexion de la machine ou d'une fermeture de session, s'effectue par méthode *Probe* (PING ou Base de registre).

Stormshield Network SSO Agent supporte désormais IPv6 pour la communication avec les serveurs Active Directory et les Firewalls Stormshield.

1.1 Correctifs

Référence support 46352 - 47065

Déconnexion

La méthode *Probe* (Base de registre) de détection des déconnexions d'utilisateurs a été améliorée.



Précisions sur les cas d'utilisation

La gestion de domaines Microsoft multiples, comportant ainsi des annuaires différents, n'est pas supportée par SN SSO Agent. Le Firewall gère un annuaire unique, les groupes utilisateurs de différents annuaires ne pourront être récupérés. D'autre part, des possibles conflits entre comptes peuvent survenir en cas d'identifiants communs.

Pour plus d'information, consultez la Note technique ***Stormshield Network SSO Agent - Installation et déploiement***.

Si un utilisateur identifié par l'agent SSO utilise un autre identifiant du domaine sur son poste de travail, cela peut annuler son identification sur le firewall. En effet, cette seconde identification est relayée par le contrôleur du domaine qui remplace la session initiale. Ces cas se présentent notamment pour les accès suivants :

- Connexion sur un intranet avec la méthode *kerberos* et/ou *ntlm*,
- Montage de ressources partagées distantes (fichiers, imprimantes) via le protocole SMB,
- Connexion RDP Terminal Services sur un serveur distant.



STORMSHIELD