TECHNICAL NOTE

Stormshield Network SSO Agent

Installation and deployment

Document version: 1.2

Reference: snentno_SSO_Agent

Content

General information

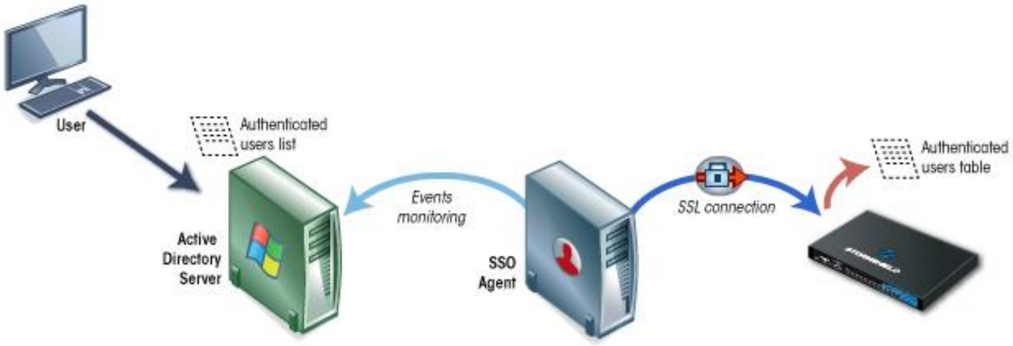
SN SSO Agent is a Windows service allowing Stormshield Network Firewalls to benefit transparently from authentication on a Windows Active Directory.

When a session is opened, meaning when a user logs on to the Windows domain, this user will automatically be authenticated on the firewall.

Principle

The SSO method (*Single Sign-On*) enables users to authenticate only once to access several services.

When a session is opened, a user will be identified on the Windows domain by the Active Directory domain controller. The SSO Agent will then collect this information by logging on remotely to the event viewer on the domain controller. The SSO Agent will then relay this information to the firewall via an SSL connection that will update the table of authenticated users.



Requirements

The following need to be installed in order to use the SSO Agent:

- A Windows Active Directory domain,
- SN SSO Agent,
- A Stormshield Network firewall.

The Stormshield Network SSO Agent service can be installed on a Windows workstation (client or server) belonging to the Active Directory domain or on a domain controller (server hosting the Active Directory). However, we suggest that you install the SSO Agent on a dedicated workstation instead of on the server hosting Active Directory.

During the installation on a workstation (client), you will be asked to enter information about a **User account** listed in the directory that will be associated with the SSO Agent.

NOTE

Before proceeding with the installation, this account must first be **registered in the directory** and have **certain privileges** (see following chapter).

The compatible Windows platforms are:

- Installation on a **server**: **Windows Server 2008 or 2008 R2, Windows Server 2011 and Windows Server 2012,**
- Installation on a **client workstation: Windows 7, Windows 7 SP1, Windows 8 and Windows 8.1**.

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

NOTE

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

Active Directory user account

Requirements

Active Directory must authorize an account allowing the SN SSO Agent to gain **access to the event viewer** of the directory and to obtain permissions to **open a session as a service**. This account has to be configured before the installation of the SSO agent.

To do so, you can either create a "privileged account" dedicated to the SSO agent, or grant privileges to an existing user. You are however advised against using the Administrator account of the AD domain in order to avoid potential security issues.

NOTE

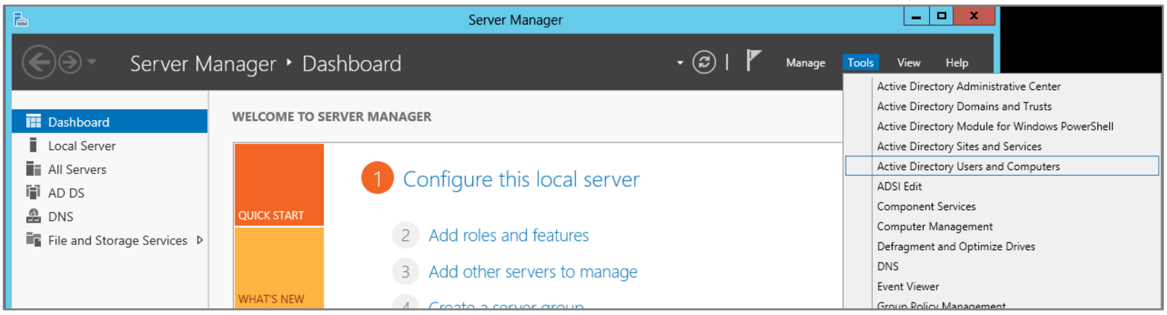
If several AD controllers manage the domain, the account that the SSO agent uses has to be a dedicated account belonging to the domain, as the privileges described hereafter must apply to all controllers, so that all events arising on the domain are relayed (generated logs will report the denial of access for reading events).

If you wish to use the registry database disconnection detection method (see chapter Detecting disconnections), this account has to belong to the group **Administrator of the Active Directory server** or be defined as the **local administrator on monitored workstations**. On the other hand, this method requires the configuration of the opposite zone of the domain on the DNS server in order to detect changes in IP addresses (in the event of a DHCP address renewal, for example). For further information, please refer to the chapter **Specific cases**, Changing an IP address.

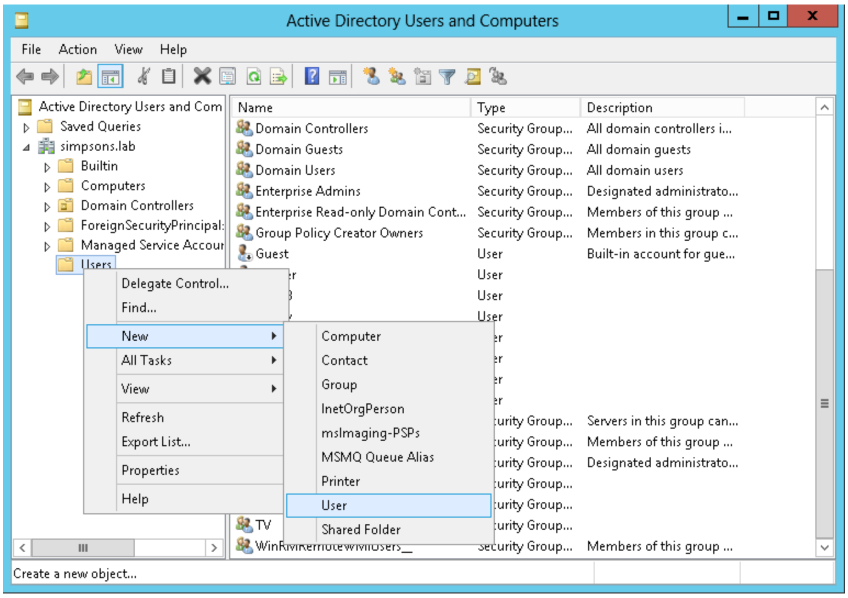
Account settings

Creating the account

Log on to your Active Directory Windows server. In the **Dashboard**, select **Tools** and click on **Active Directory Users and Computers**.

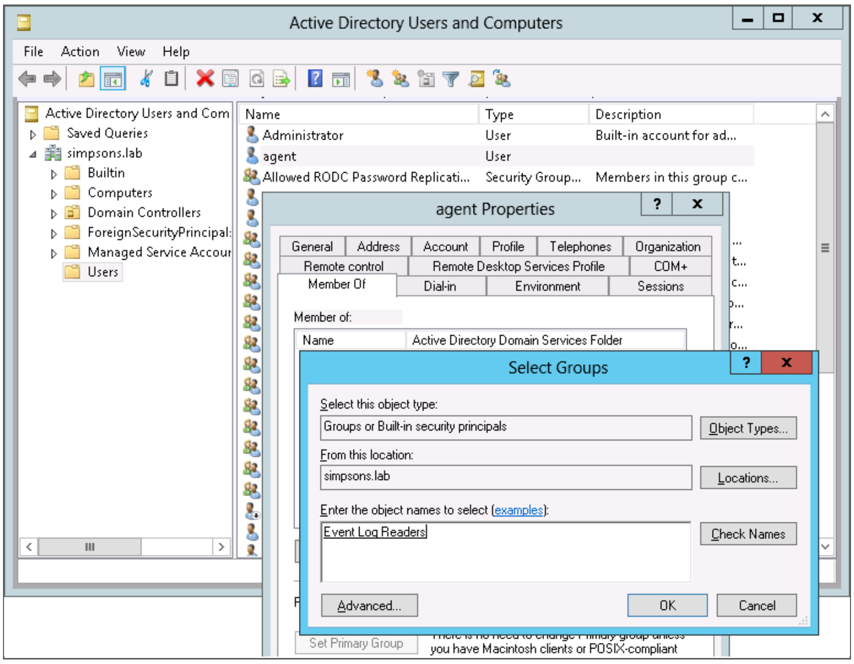

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management

To create a new user, right-click on the **Users** folder and select **New**, then **User**. Fill in the fields relating to the account (names, login and password).



Reading privileges on the event viewer

This account has to belong to the group that has **reading privileges on the directory's event viewer**. Open the folder **Users** to add it to the group.


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
simpsons.lab
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
agent Properties
General Address Account Profile Telephones Organization
Remote control Remote Desktop Services Profile COM+
Member Of Dial-in Environment Sessions
Member of:
Set Primary Group
Select Groups
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel

Name	Type	Description
Administrator	User	Built-in account for ad...
agent	User	
Allowed RODC Password Replicati...	Security Group...	Members in this group c...

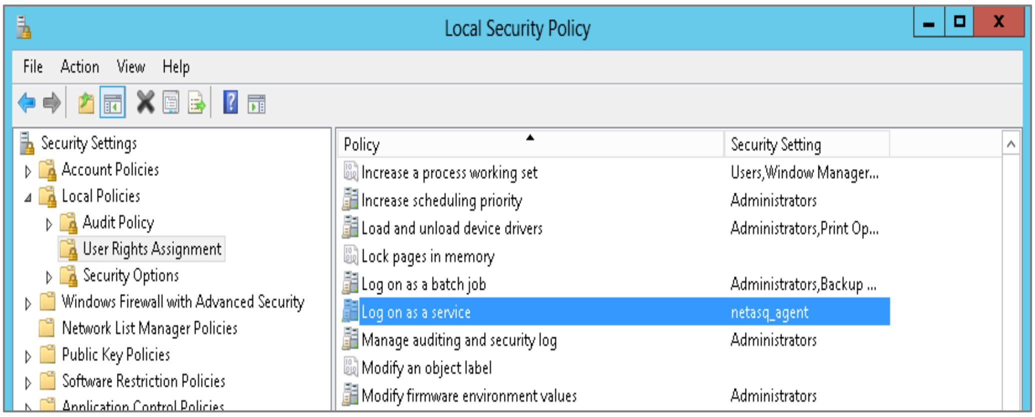
Select this object type:
Groups or Built-in security principals

From this location:
simpsons.lab

Enter the object names to select (examples):
Event Log Readers

1. Double-click on the account **chosen** from the list,
2. Click on the tab **Member of,**
3. Click on **Add,**
4. Click on **Advanced,**
5. Click on **Find now,**
6. Double-click on Read on event viewer,
7. Click on **OK,**
8. Click on **Apply.**

Privileges to open a session as a service



Policy	Security Setting
Increase a process working set	Users,Window Manager...
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators,Print Op...
Lock pages in memory	
Log on as a batch job	Administrators,Backup ...
Log on as a service	netasq_agent
Manage auditing and security log	Administrators
Modify an object label	
Modify firmware environment values	Administrators

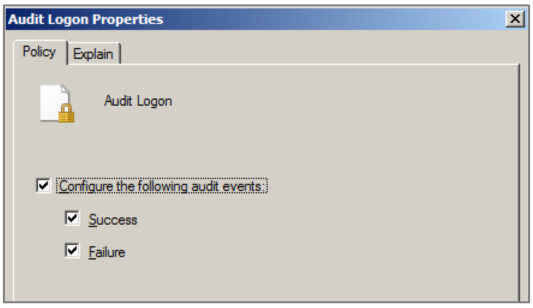
1. In the control panel, click on **Local security policy,**
2. In **Local policies**, select the folder **User Rights Assignment,**
3. Double-click on **Log on as a service** and add the dedicated account.

Saving opened sessions in the Event Viewer

In order to generate session opening logs (corresponding to ID 4624 in the Event Viewer) on which SSO agent relies to detect a new authentication, check that the audit logon policy has been enabled.

In Windows Server 2008: **Start** > **Administrative tools** > **Local Security Policy** > **Advanced Audit Policy Configuration** > **System Audit Policies – Local Group Policy Object** > **Logon/Logoff** > **Audit Logon.**

In Windows Server 2012: **Server Manager** > **Tools** > **Local Security Policy** > **Advanced Audit Policy Configuration** > **System Audit Policies – Local Group Policy Object** > **Logon/Logoff** > **Audit Logon.**


Audit Logon Properties

Policy | Explain

Audit Logon

☑ Configure the following audit events:

☑ Success

☑ Failure

All 3 checkboxes in the *Policy* tab have to be selected.

Installing the Stormshield Network SSO Agent

Installation wizard

You can install the SN SSO Agent on a workstation belonging to the Windows domain or on your Active Directory server. The installation wizard allows configuring the parameters of the SSO agent on the workstation.

NOTE

If you are not logged on as the administrator, right-click on the icon of the SSO agent and click on **Execute as administrator**.

Type of workstation

Specify the account selected for this service and whether you wish to install the SSO agent on a domain controller (server hosting AD) or on a machine belonging to the Active Directory domain.

- You are currently on the server hosting Active Directory and wish to use the **local system account**.
- You wish to use a **dedicated account** on the server hosting Active Directory or on a host on the domain.

User account associated with the SSO agent

Enter the information about the **dedicated account** on the domain controller, defined in the previous chapter (Active Directory user account).

Enter the name of this account in the format **Domain\User** or **User@Domain** (Example: *mycompany\ssoagent*). Enter the password and confirm it.

Selecting the SSL encryption key

The **pre-shared key** allows encrypting communications between the SSO agent and the Stormshield Network Firewall. This key (password) must also be indicated to the firewall. Therefore, keep it in order to enter it during the configuration of the authentication method on the firewall (see following chapter).

If this is not the first installation, the SSO agent will detect the existing pre-shared key. For a reinstallation after changes have been made to the workstation, an upgrade of the SSO agent or other changes, you are advised to keep the pre-shared key.

NOTE

During an upgrade of the SSO agent, you are advised against uninstalling the earlier version of the service. This would require rebooting the machine, which may not necessarily be easy on a server. Upgrading the SSO agent does not require prior uninstallation.

Confirming settings

To change the settings that you have configured, click on **Previous**.

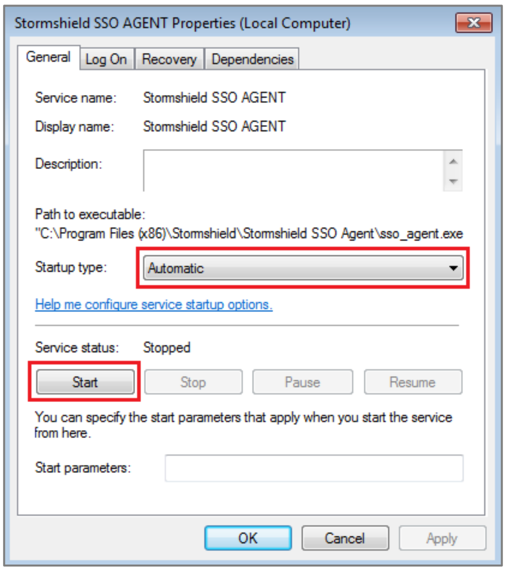
If the installation was successful, click on **Finish.**

Starting the service

Start the **Stormshield Network SSO Agent** service in the Windows services. To access these services, type **Services** in the search field, and press **Enter**. Double-click on the **Stormshield Network SSO AGENT** service.

In the **General** tab, check that the service has been configured in **Automatic** mode when Windows is starting up.

In the section **Service status**, click on **Start**.



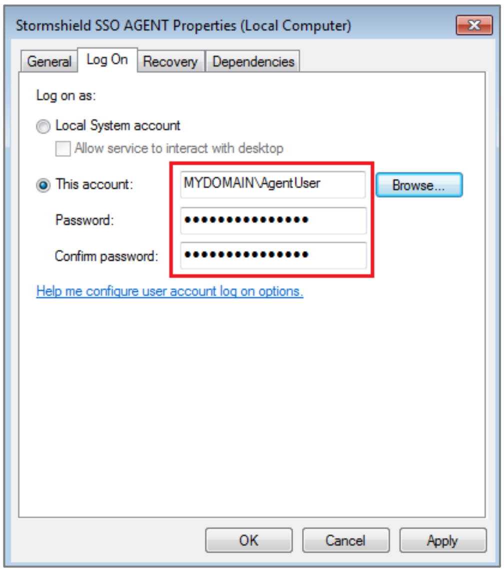
Stormshield SSO AGENT Properties (Local Computer)

Service name: Stormshield SSO AGENT
Display name: Stormshield SSO AGENT
Description:
Path to executable:
"C:\Program Files (x86)\Stormshield\Stormshield SSO Agent\sso_agent.exe
Startup type: Automatic
Help me configure service startup options.
Service status: Stopped
You can specify the start parameters that apply when you start the service from here.
Start parameters:

SSO agent installed on a host on the domain

When the SSO agent has been installed on a host other than the domain controller, the login and password for the **Active Directory user account** have to be entered in the **Log On** tab.

Please be reminded that this account must have reading privileges on the Event Viewer and open a session as a service (cf. chapter **Active Directory user account**).



Stormshield SSO AGENT Properties (Local Computer)

Log on as:
○ Local System account
□ Allow service to interact with desktop
● This account: MYDOMAIN\AgentUser
Password: •••••••••••••••
Confirm password: •••••••••••••••
Help me configure user account log on options.

Configuring the Stormshield Network Firewall

To configure the SSO agent, log on to the Firewall via a web browser to the address: **https://*IPaddress_of the firewall*/admin**

Objects

You need to create **Network objects** corresponding to the machine hosting the **SSO agent** and to the **Active Directory domain controllers**, if you have several of them.

To create these objects, click on the module **Network objects** (**Objects** menu).

Next, click on **Add**. Select **Machine** and enter the name of the SSO agent or the domain controller. Specify whether this machine has been configured in **dynamic** (DHCP changes the IP address upon each connection) or **static** (fixed IP address) DNS resolution. The machine's MAC address is not required.

Configuring the directory

It is possible to use the service of the SSO agent without **Active Directory** configured on the Firewall. However, you are strongly advised to configure this directory (menu **User** > **Directory configuration**). This would allow searching for users and groups, especially in the authentication rules and building a security policy based on these groups and users.

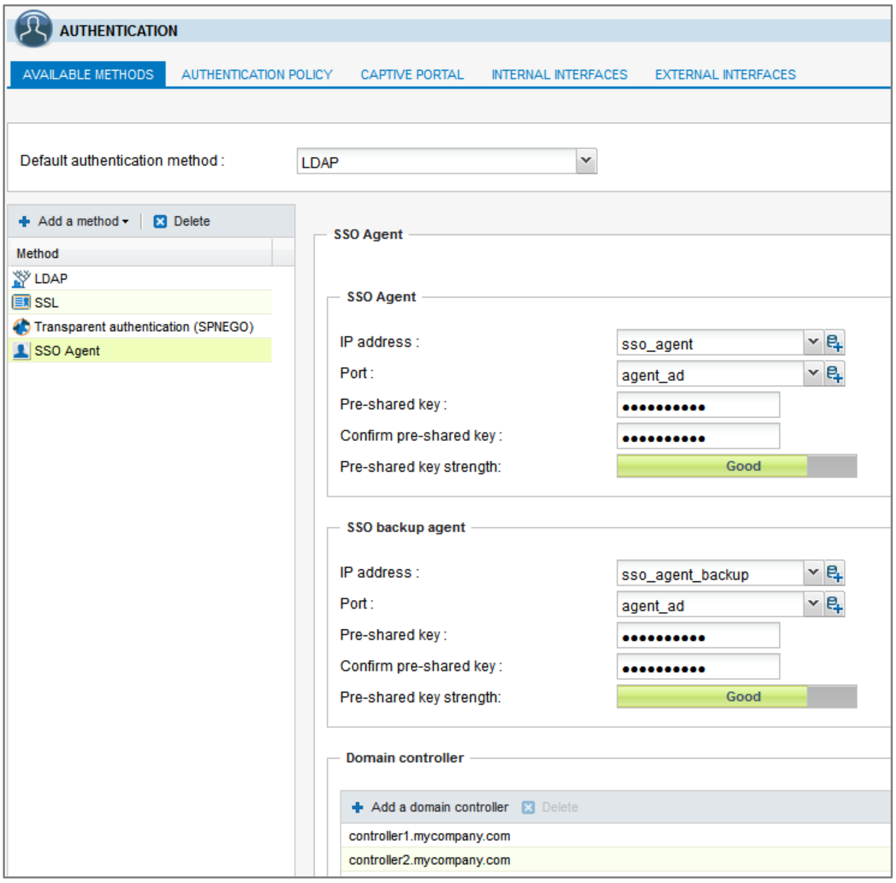
The *SSO Agent* method also offers an advanced option that defines a *User group update frequency* that can only function with the configured directory.

Authentication

Available methods tab

In the **Authentication** module (**User** menu), you will configure the *SSO Agent* method. After these settings have been defined, click on **Apply** to save your settings.

In the tab **Available methods,** click on **Add a method** and select *SSO Agent* in the drop-down menu. Please enter the information about the main SSO agent and a backup SSO Agent (optional).



AUTHENTICATION

Default authentication method : LDAP

Method
- LDAP
- SSL
- Transparent authentication (SPNEGO)
- SSO Agent

SSO Agent

SSO Agent

IP address :	sso_agent
Port :	agent_ad
Pre-shared key :	••••••••••
Confirm pre-shared key :	••••••••••
Pre-shared key strength:	Good

SSO backup agent

IP address :	sso_agent_backup
Port :	agent_ad
Pre-shared key :	••••••••••
Confirm pre-shared key :	••••••••••
Pre-shared key strength:	Good

Domain controller

controller1.mycompany.com
controller2.mycompany.com

SSO Agent

From the drop-down menu, select the network object that corresponds to the host on which the SSO agent has been installed.

Enter the **pre-shared key** (password) defined during the installation of the SSO agent (see the chapter Selecting the SSL encryption key). This key is used for encrypting in SSL exchanges between the SSO agent and the firewall.

The strength of the pre-shared key indicates this password's level of security. You are strongly advised to use uppercase letters and special characters.

The port "agent_ad" is selected by default, corresponding to port 1301. The protocol used is TCP.

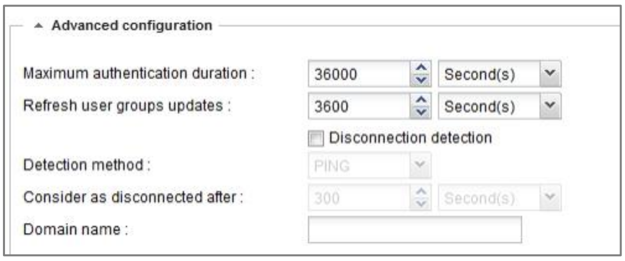
Domain controller

You need to add all the controllers that control the domain. These must be saved beforehand in the firewall's Objects database.

REMINDER

If several AD controllers manage the domain, the account that the SSO agent uses has to be a dedicated account belonging to the domain, with the privileges described in the chapter Active Directory user account. These privileges apply to all controllers, so that all events arising on the domain are relayed.

Advanced properties



▲ Advanced configuration

Maximum authentication duration : 36000 Second(s)

Refresh user groups updates : 3600 Second(s)

□ Disconnection detection

Detection method : PING

Consider as disconnected after : 300 Second(s)

Domain name :

Maximum authentication duration

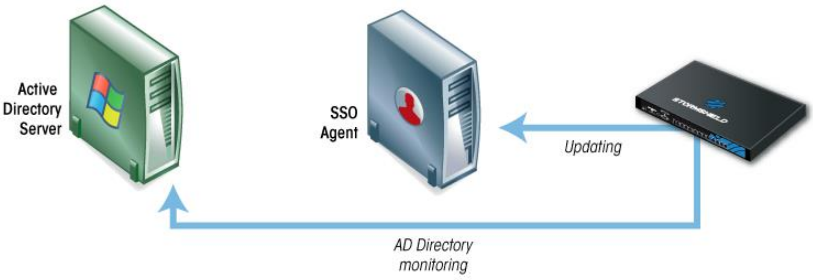
Define a maximum duration of an authenticated user's session. After this duration has been exceeded, the firewall will delete the user associated with this IP address from its table of authenticated users, logging the user out of the firewall.

This limit is to be defined in seconds or minutes and is set by default to 36000 sec. (or 10 hours).

User group update frequency

Only if the AD has been configured on the firewall (**Directory configuration**), the firewall will check for possible changes to the **LDAP directory groups**. The firewall will update its directory configuration, and then send back this information to the SSO agent.

This duration defined in seconds, minutes or hours, is set by default to 3600 sec. (1 h).



Detecting disconnections

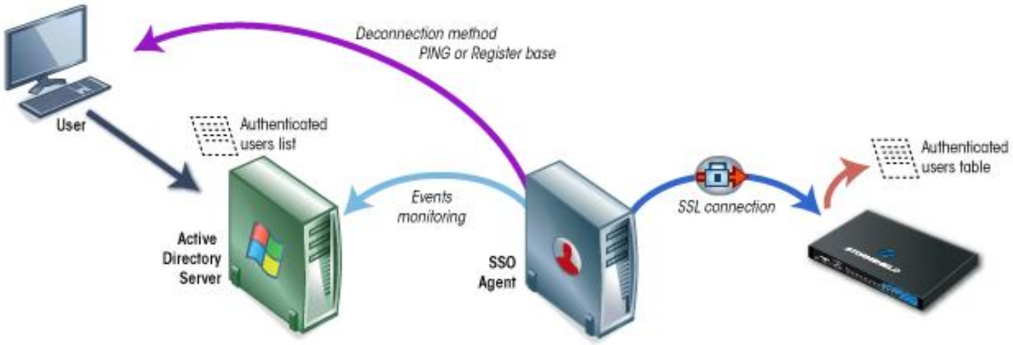
Enabling the disconnection method allows deleting authenticated users when logging out a machine or shutting down a session. This test of machines connected to the firewall is conducted either by pinging or by the registry database.

If this method is not enabled, the user will be unauthenticated only after the set authentication period, even when the session has been shut down.

NOTE

Machines on the domain must allow responses to ping tests (parameters of the *Windows firewall* on the machines).

On the other hand, if the SSO passes through a firewall in order to access machines on the domain, rules have to be created to allow the SSO agent to test the workstations in the firewall's filter policy.



Pinging

The SSO agent tests the accessibility of all the machines authenticated on the firewall every 60 seconds by default. When a response *host unreachable* is not received or there is no response from an IP address after a defined period has lapsed, the SSO agent will send a disconnection request to the firewall, which will then delete the user associated with the IP address from its table of authenticated users, thereby logging the user out of the firewall.

Registry database method

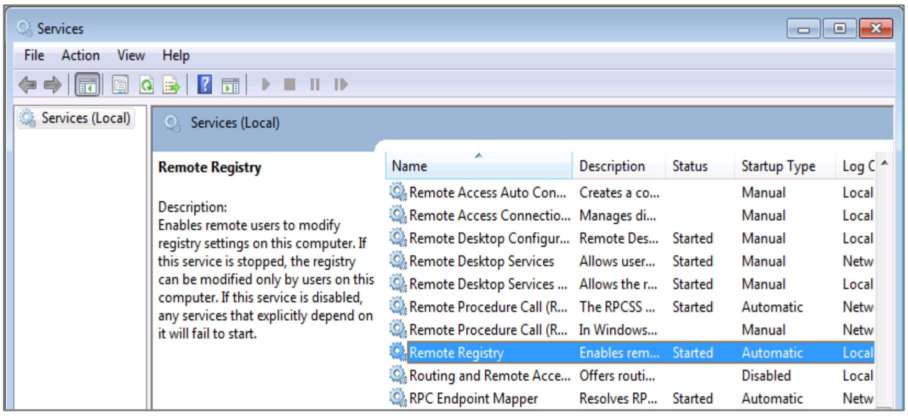
This method allows detecting, for example, a session that has been shut down on a machine that is still running. The **Registry database (RD)** is a database used by the Windows operating system to store the configuration information of the system and the installed software.

If a positive response to a ping is received, the SSO agent will log on remotely to the machine and check the list of users with an open session on a machine in the registry database. This allows updating the table of authenticated users.

NOTE

For this method, the account associated with the SSO agent must have **administration privileges on all machines authenticated on the firewall**; this account must belong to the group **Administrator of the Active Directory server** or be defined as a **local administrator on monitored machines** (see the chapter Active Directory user account).

On the other hand, the **Remote registry** service has to be enabled on these machines. To do so, go to **Services** in Windows, select the service **Remote registry** then click on **Start**. The status of this service also has to be changed from **Manual** to **Automatic**.

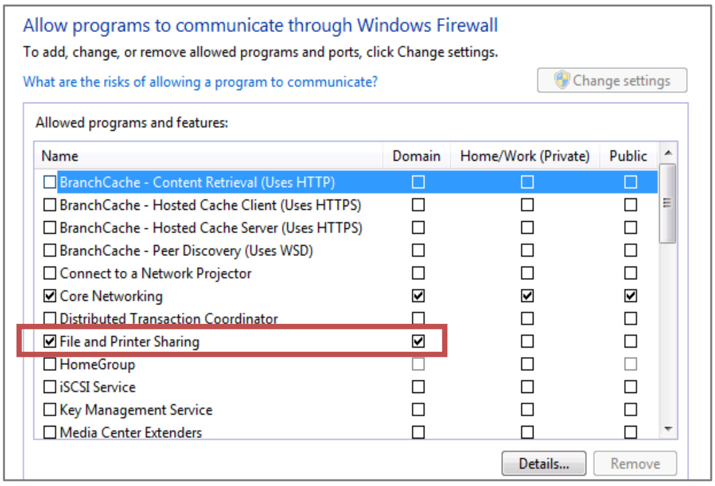


Remote Registry

Description:
Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log C
Remote Access Auto Con...	Creates a co...		Manual	Local
Remote Access Connectio...	Manages di...		Manual	Local
Remote Desktop Configur...	Remote Des...	Started	Manual	Local
Remote Desktop Services	Allows user...	Started	Manual	Netw
Remote Desktop Services ...	Allows the r...	Started	Manual	Local
Remote Procedure Call (R...	The RPCSS ...	Started	Automatic	Netw
Remote Procedure Call (R...	In Windows...		Manual	Netw
Remote Registry	Enables rem...	Started	Automatic	Local
Routing and Remote Acce...	Offers routi...		Disabled	Local
RPC Endpoint Mapper	Resolves RP...	Started	Automatic	Netw

Lastly, ports 139 and 445 (Windows ports) & ICMP have to be open. Follow the path *Control panel* > *System and security* > *System* > *Windows firewall* and click on *Allow programs to communicate through Windows firewall*, then select *File and printer sharing.*



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Domain	Home/Work (Private)	Public
□ BranchCache - Content Retrieval (Uses HTTP)	□	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□	□
□ Connect to a Network Projector	□	□	□
☑ Core Networking	☑	☑	☑
□ Distributed Transaction Coordinator	□	□	□
☑ File and Printer Sharing	☑	□	□
□ HomeGroup	□	□	□
□ iSCSI Service	□	□	□
□ Key Management Service	□	□	□
□ Media Center Extenders	□	□	□

REMINDER

On the other hand, this method requires the configuration of the opposite zone of the domain on the DNS server in order to detect changes in IP addresses (in the event of a DHCP address renewal, for example). For further information, please refer to the chapter **Specific cases**, **Changing an IP address**.

Consider offline

If a machine does not respond to a ping after this duration, it will be considered offline. The firewall will then delete the user associated with the machine from its table of authenticated users. This duration is defined in seconds, minutes or hours and is set by default to 5 minutes.

Domain name (NETBIOS)

If this field has not been filled in, the SSO agent will take into account all events on domains that trust each other (Windows trust relationships). Conversely, if a domain has been entered, authentication will only be possible for events relating to this domain.

Authentication rules tab

Rules allowing traffic dedicated to the **SSO agent** method have to be defined. In the tab **Authentication rules**, select **Standard rule** (**New rule** menu) in order to launch the rule creation wizard.

Step 1: User authentication

Select the user or group concerned or leave the default value as "Any".

Step 2: Authentication source

Click **Add an object** in order to target the source of the traffic to which the rule applies. This may be the object corresponding to these internal networks (e.g.: *network_internals*).

IMPORTANT

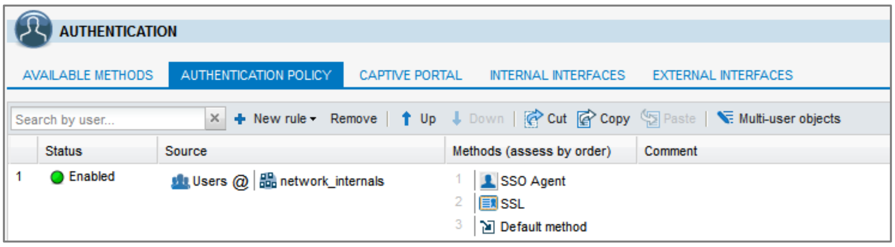
The Stormshield Network SSO Agent authentication method is based on authentication events collected by Windows domain controllers. As these do not indicate the source of the traffic, the authentication policy cannot be specified with interfaces.

Step 3: Order of evaluation

Click on **Authorize a method** and select from the drop-down list the authentication methods to be applied to the traffic to which the rule applies.

The *Default method* selected corresponds to the method chosen in the tab **Available methods**.

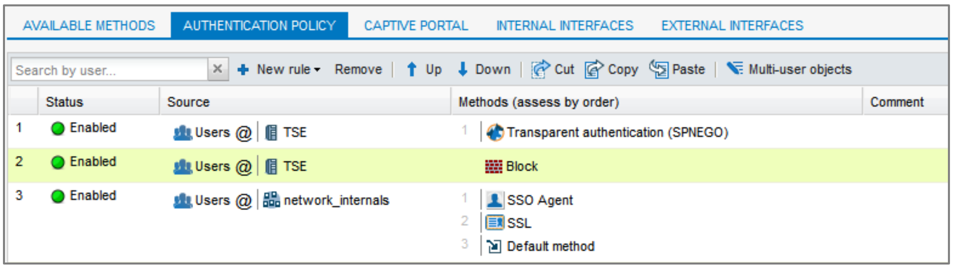
Authentication methods are **evaluated in the order in the list** and from top to bottom. As the *SSO Agent* method is transparent, it is by definition always applied as a priority. Click on **Finish,** then on **Apply**.



	Status	Source	Methods (assess by order)	Comment
1	● Enabled	Users @ network_internals	1 SSO Agent 2 SSL 3 Default method	

REMARK

The SSO Agent method does not support multi-user objects (several authenticated users on the same IP address). However, such objects can be contained on a network, a range or a group defined as the source of a rule using the SSO Agent method. To avoid having multiple logs on the denial of authentication via the SSO agent, you are advised to add two rules dedicated to these objects in front of the rules that use the SSO Agent method: the first rule specifies the method used by the multi-user object followed by a second rule that will "block" the authentication of this object in order to block any other authentication attempts (see image below).



	Status	Source	Methods (assess by order)	Comment
1	Enabled	Users @ TSE	1 Transparent authentication (SPNEGO)	
2	Enabled	Users @ TSE	Block	
3	Enabled	Users @ network_internals	1 SSO Agent 2 SSL 3 Default method	

Ignored administration accounts

In the firewall’s factory configuration, there is a list of users for whom authentication is ignored. These accounts list the usual logins dedicated to the administrator (*Administrator* and *Default administrator*).

This mechanism has been set up as the domain controller considers the execution of a service or an application (**Execute as administrator** feature, for example) an authentication. As the SSO Agent restricts authentication by IP address, this type of authentication may potentially replace the authentication of the user with an open Windows session. The pre-set list of “Ignored Administrator accounts” allows the SSO agent to not take into account their authentication.

This list of administration accounts can be modified from the **Advanced properties** menu in the *SSO Agent* authentication method.

To make this list, refer also to the chapter **Specific cases**, paragraph Other accounts on the domain.

Advanced settings of the SSO agent on the machine

Logs

Logs record communications between the SSO agent and Stormshield Network Firewalls. Connection information about Active Directory users is collected when the SSO agent sends this information to the firewall.

Access

The SSO agent installs *logs* on the installation host in the following folder:

C:\Program Files (x86) \Stormshield\ Stormshield SSO Agent\log\ssoagent.log

To access this folder, follow the path **Stormshield** > **Stormshield SSO Agent** > **open log folder**.

Then double-click on the file **ssoagent**.

Log files

The log file **ssoagent.log** contains the following information: **the date and time of the connection, name of the connected user, IP address** of the machine, **SID** (security ID of the connected user).

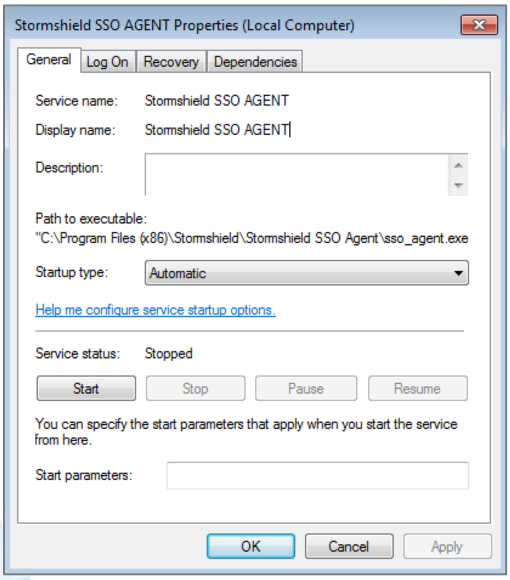
The maximum size of a file is 1Mb. The folder can contain a maximum of 100Mb, or 100 log files. When the folder reaches the maximum capacity, the oldest log file will be erased.

Stormshield Network SSO Agent Service

Check that the **Stormshield SSO Agent** service is running in Windows services.

For client workstations, the user must have **Administrator privileges** on the machine to modify **Services.**

To access Windows services, enter **Services** in the search field, and press **Enter**. Double-click on the service **Stormshield SSO AGENT**.



Stormshield SSO AGENT Properties (Local Computer)

Service name: Stormshield SSO AGENT

Display name: Stormshield SSO AGENT

Description:

Path to executable:
"C:\Program Files (x86)\Stormshield\Stormshield SSO Agent\sso_agent.exe

Startup type: Automatic

Help me configure service startup options.

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

General tab

Check that the service has been configured in **Automatic** mode when Windows is starting.

If the status of the service is **Stopped,** click on the **Start** button.

Log on tab

To prevent the service from shutting down without authorization, you can associate the user account of the service with it.

Example: Domain\user & password on the domain.

Recovery tab

This allows configuring the service of the SSO agent if it has stopped; by default, no changes are necessary.

Dependencies tab

The SN SSO Agent service does not depend on any other service; by default, no changes are necessary.

Configuring the Windows firewall

In the event of a failure when configuring the *firewall* during installation, check that port 1301 (default port) is open in its configuration.

Specific cases

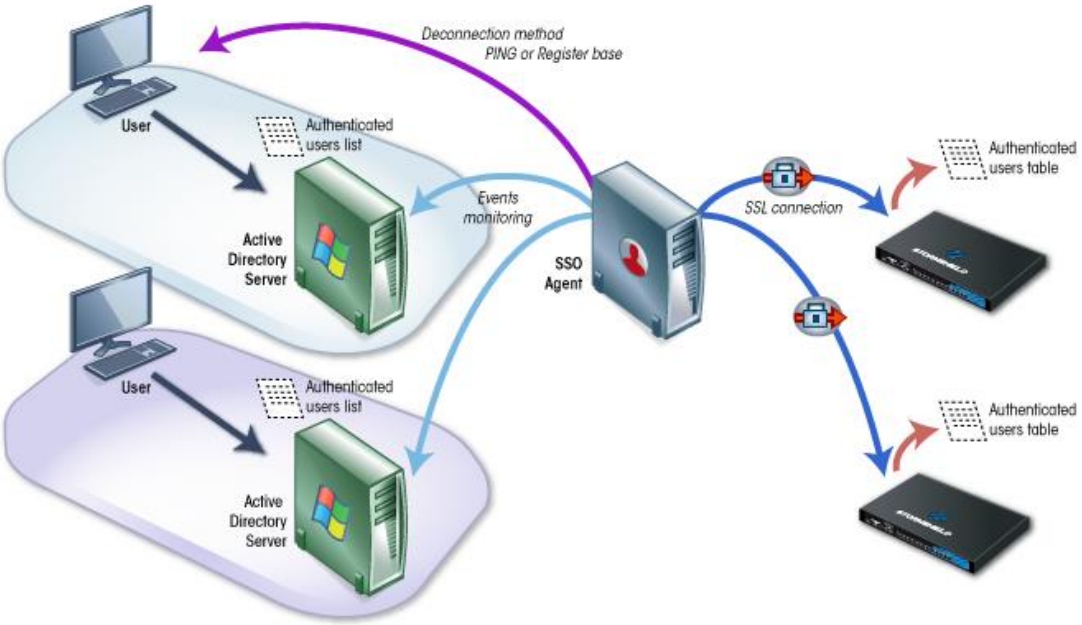
Multiple UTM firewalls

Several firewalls managing the same domain can log on to the same SSO Agent.

However, a firewall cannot log on to several SSO Agents, apart from the backup agent.

Multiple domains (different directories)

A firewall and an SSO Agent are required per domain, as a firewall can only manage one domain.



Trusting

Trust Relationship allows establishing a list of “trusted” domains.

In an Active directory forest including sub-domains (for example *nestaq.int* and its sub-domain *lab.nestaq.int*), approval relationships allow using logins on a domain to access resources on another domain.

Even if the SSO agent is connected only to the controllers of a single domain, it can then receive authentication events from another domain.

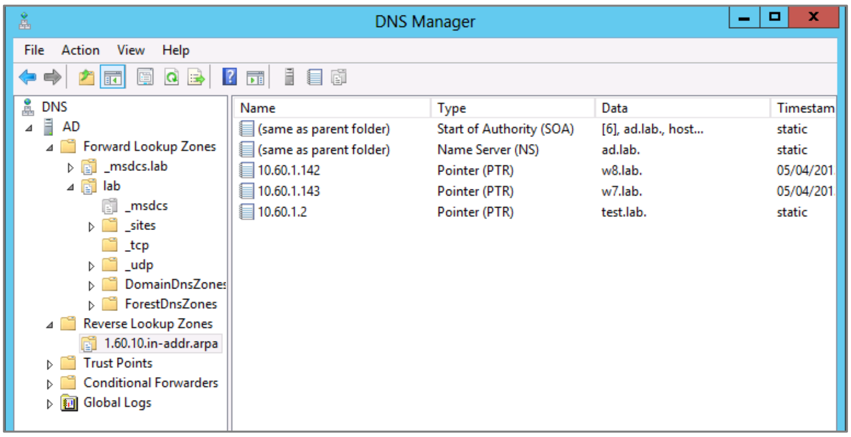
It is not advisable to let the SSO agent retrieve events from another domain, to avoid conflicts of networks or identical logins.

As the firewall manages only one Active Directory, known groups and users will therefore only be those belonging to the configured domain. As a result, even if the same login exists on different domains, the policy applied will be the policy of the user references in the firewall’s known directory.

To conclude, it is recommended in this case to restrict authentication to the domain (*Domain name* field in *Advanced properties*).

Changing an IP address

Periodically, the agent will perform DNS requests (PTR) to check that machines have not changed their IP addresses. If there is a new IP address, the information will be sent to the firewall. For this, in the settings of your DNS server, add a **Reverse lookup zone** (right-click on the folder) for machines on the domain.



Name	Type	Data	Timestam
(same as parent folder)	Start of Authority (SOA)	[6], ad.lab., host...	static
(same as parent folder)	Name Server (NS)	ad.lab.	static
10.60.1.142	Pointer (PTR)	w8.lab.	05/04/201
10.60.1.143	Pointer (PTR)	w7.lab.	05/04/201
10.60.1.2	Pointer (PTR)	test.lab.	static

Other accounts on the domain

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 cases occur especially for the following types of access:

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

Checking the SN SSO Agent service

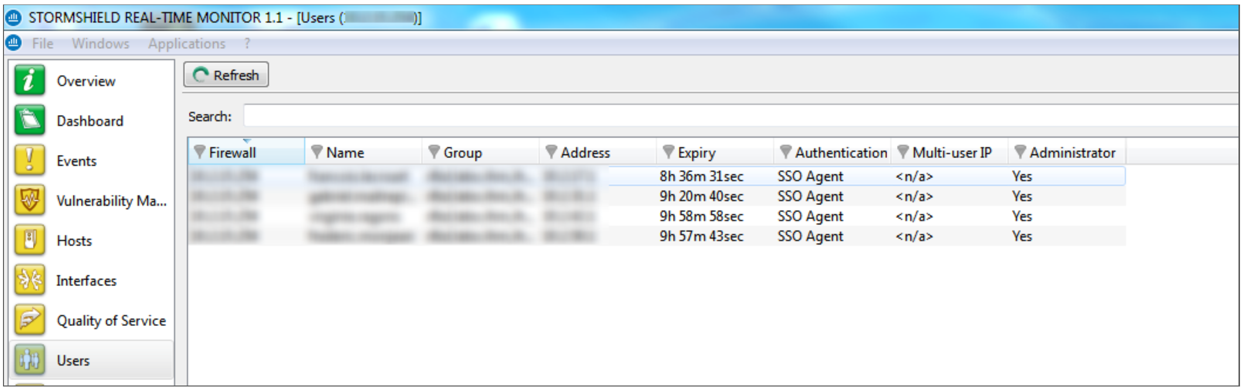
To ensure that the SSO agent has been correctly installed and configured, you can check the status of the service using **Stormshield Network Administration Suite** software programs or via *System Logs* on the machine hosting the SSO agent.

Download the **SN Administration Suite** tools from your client or partner area or at the address:

http://gui.stormshield.eu/last-version

Stormshield Network Real-time Monitor

Launch SN Real-time Monitor and log on to your firewall through the program. Go to the **Users** module. Information about connections via the SSO agent is displayed by user.

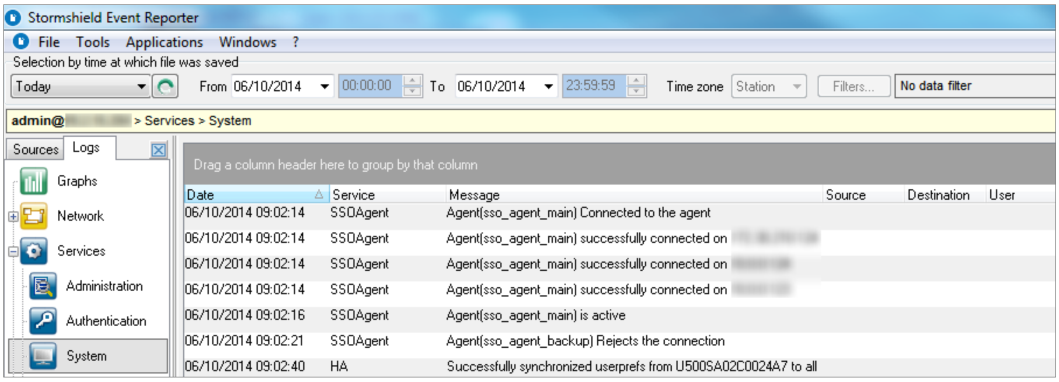


Firewall	Name	Group	Address	Expiry	Authentication	Multi-user IP	Administrator
[redacted]	[redacted]	[redacted]	[redacted]	8h 36m 31sec	SSO Agent	<n/a>	Yes
[redacted]	[redacted]	[redacted]	[redacted]	9h 20m 40sec	SSO Agent	<n/a>	Yes
[redacted]	[redacted]	[redacted]	[redacted]	9h 58m 58sec	SSO Agent	<n/a>	Yes
[redacted]	[redacted]	[redacted]	[redacted]	9h 57m 43sec	SSO Agent	<n/a>	Yes

If none of your users are connected via the SSO Agent method, go on to the next chapters.

Stormshield Network Event Reporter

Via SN Event Reporter, log on to your firewall and click on the **Logs** tab. Go to the **Services** section and click on the **System** module. Events relating to the SSO agent are listed in the corresponding Service.

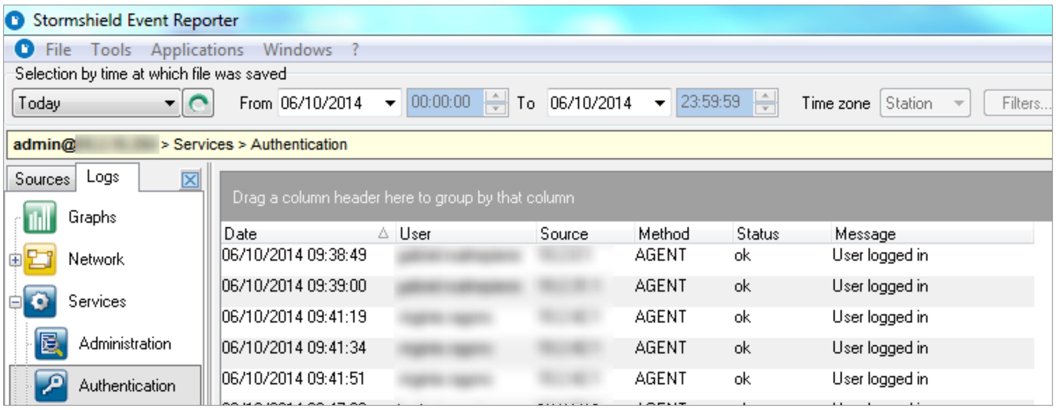


Selection by time at which file was saved: Today; From 06/10/2014 00:00:00 To 06/10/2014 23:59:59; Time zone Station; No data filter

admin@[redacted] > Services > System

Date	Service	Message	Source	Destination	User
06/10/2014 09:02:14	SSOAgent	Agent(sso_agent_main) Connected to the agent			
06/10/2014 09:02:14	SSOAgent	Agent(sso_agent_main) successfully connected on [redacted]			
06/10/2014 09:02:14	SSOAgent	Agent(sso_agent_main) successfully connected on [redacted]			
06/10/2014 09:02:14	SSOAgent	Agent(sso_agent_main) successfully connected on [redacted]			
06/10/2014 09:02:16	SSOAgent	Agent(sso_agent_main) is active			
06/10/2014 09:02:21	SSOAgent	Agent(sso_agent_backup) Rejects the connection			
06/10/2014 09:02:40	HA	Successfully synchronized userprefs from U500SA02C0024A7 to all			

The **Authentication** module sets out the details of the connected users.


Stormshield Event Reporter
File Tools Applications Windows ?
Selection by time at which file was saved
Today
From 06/10/2014 00:00:00 To 06/10/2014 23:59:59
Time zone Station
Filters...
admin@[redacted] > Services > Authentication
Sources Logs
Graphs
Network
Services
Administration
Authentication
Drag a column header here to group by that column

Date	User	Source	Method	Status	Message
06/10/2014 09:38:49	[redacted]	[redacted]	AGENT	ok	User logged in
06/10/2014 09:39:00	[redacted]	[redacted]	AGENT	ok	User logged in
06/10/2014 09:41:19	[redacted]	[redacted]	AGENT	ok	User logged in
06/10/2014 09:41:34	[redacted]	[redacted]	AGENT	ok	User logged in
06/10/2014 09:41:51	[redacted]	[redacted]	AGENT	ok	User logged in

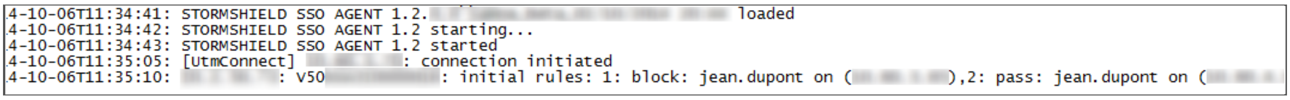
Logs – SSO Agent

On the machine where the SSO agent has been installed, look up the log files in the following folder: **C:\Program Files (x86)\Stormshield\ Stormshield SSO AGENT\log**

Check that the log file **ssoagent** contains the following information:

1. The connection to the firewall,
2. The authentication rules that apply to users,
3. Opening of sessions of authenticated users sent to the firewall,
4. Logouts of machines associated with users.

The image below displays information about the connection to the firewall in the log file.



```
4-10-06T11:34:41: STORMSHIELD SSO AGENT 1.2.[redacted] loaded
4-10-06T11:34:42: STORMSHIELD SSO AGENT 1.2 starting...
4-10-06T11:34:43: STORMSHIELD SSO AGENT 1.2 started
4-10-06T11:35:05: [UtmConnect] [redacted]: connection initiated
4-10-06T11:35:10: [redacted]: V50[redacted]: initial rules: 1: block: jean.dupont on ([redacted]),2: pass: jean.dupont on ([redacted]
```

If the connection of the SSO agent to the firewall fails, an error message will be returned. This file, which allows debugging the service, is necessary during technical assistance.

Frequently encountered problems

The following points list some of the most frequently encountered problems. Checking these elements may help in the resolution of a probable malfunction.

The SSO agent cannot log on to the firewall

1. Check the SSL encryption key i.e. pre-shared key (password),
2. Check that **port 1301** has not been blocked by a firewall or on the machine hosting the SSO agent,
3. Check the logs in the "System" log file (fichier */log/l_system*) of the firewall via the Stormshield Network Administration tools (chapter Checking the SN SSO Agent service).

The SSO agent cannot log on to the domain controller

1. Check that the account associated with the SSO agent has **reading privileges on the event viewer** in Active Directory,
2. Check that **ports 139 and 445** have not been blocked by a firewall or on the machine hosting the SSO agent.

No authentication on the firewall

If there are no authenticated users on the firewall according to the Stormshield Network Administration Suite or the log files, you are advised to test the authentication method using an authentication rule with *Any* as the **User** value and as the **Source**.

Machines do not respond to the ping (users unauthenticated from the firewall)

If the SSO agent is unable to test a machine by pinging it, the firewall will automatically delete the login from its table of authenticated users. This is visible in the logs of the SSO agent (chapter Checking the SN SSO Agent service).

Check that ICMP is allowed on machines in the domain (configuration of the *Windows firewall*).

Could not connect to the registry database

If the SSO agent is unable to access a machine, it will be visible in the logs of the SSO agent (chapter Checking the SN SSO Agent service)

Check that ICMP has been allowed and that **ports 139 and 445** are open on the machines in the domain (configuration of the *Windows firewall*). Also check that the remote registry is running in Windows services and that the account used by the SSO agent has administration privileges on these machines.

Change of IP address not detected

Changes to IP addresses have been detected by DNS requests. Check that the DNS servers have been configured for machines in the domain.

If the machines are configured in DHCP, the DHCP server must update the entries in the DNS servers. It is therefore necessary to check that the Reverse lookup zone has indeed been created (see the specific case **Changing an IP address**).