TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSO AGENT FOR WINDOWS - INSTALLATION AND DEPLOYMENT

Product concerned: SNS 4.x, SSO Agent 2.1 and 3.0 for Windows

Document last updated: February 13, 2024

Reference: sns-en-sso_agent_technical_note-v4

Table of contents

Getting started

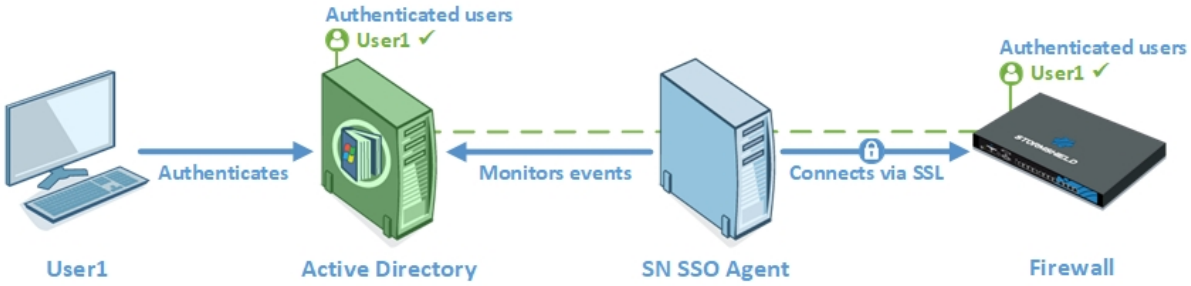
With SN SSO Agent for Windows, SN firewalls can authenticate transparently on Active Directory.

When a session is opened, i.e., when users log in to the Active Directory domain, they will automatically be authenticated on the firewall.

Principle

In the SSO method (*Single Sign-On*) users need to authenticate only once to access several services.

When a session is opened, the domain controller identifies a user on the Active Directory domain. SN SSO Agent will then collect the user's information by logging in remotely to the event viewer on the domain controller. SN SSO Agent then relays this information to the firewall through an SSL connection, which updates its table of authenticated users.



Multiple Active Directories

From version 3 of SN firewalls, up to five SSO agents, and therefore five Active Directory domains, can be managed on a firewall.

Whenever a firewall manages authentication on several domains (forest containing several domains linked by a trust relationship or several independent Active Directory domains), an SN SSO Agent must be dedicated to each authentication domain.

Requirements

You will need the following in order to use SN SSO Agent:

- A domain controller in Windows Server 2012 R2, 2016, 2019 or 2022,
- A user account listed in the Active Directory, that will be associated with the SN SSO Agent in question. This account must hold certain privileges, which will be requested during the installation of the agent on the client workstation. For more information, refer to the section Configuring access to Active Directory.
- An SNS firewall and SN SSO Agent for Windows running in a compatible version:

SN SSO Agent for Windows	Compatible SNS versions
2.1	3.x, 4.0 and 4.1
3.0	4.2 and higher

NOTE

SN SSO Agent for Windows can be installed on:

- A Windows client or server host belonging to the Active Directory domain,
- A domain controller, i.e., the server hosting the Active Directory.

However, we suggest that you install SN SSO Agent on a dedicated workstation instead of a domain controller.

Limitation

If a first session is locked but not shut down, when a second session is opened, it will replace the previous session. A user who logs in again to the first session will remain identified with the privileges assigned to the second session.

Users are therefore advised to shut down their sessions instead of locking them in case another user logs in to the same workstation.

Configuring access to Active Directory

Active Directory must authorize an account that allows SN SSO Agent **access to the event viewer** of the directory and grants permission to **open a session as a service**. This account must be configured before SN SSO Agent is installed.

To do so, you can either create a "privileged account" dedicated to SN SSO Agent, or grant permissions to an existing user. You are however advised against using the Administrator account on the Active Directory domain to prevent potential security issues.

NOTE
If several domain controllers manage the same domain, the account that SN SSO Agent uses must be a dedicated account belonging to the domain. The privileges described below must apply to all domain controllers so that all events occurring on the domain (logs that report users being denied access to read events) can be relayed.

If you wish to use the registry database disconnection detection method, this account must belong to the group **Administrator of the Active Directory server** or be defined as the **local administrator on monitored workstations**.

In this method, the opposite zone of the domain must also be configured on the DNS server to detect changes in IP addresses, e.g., when a DHCP address is renewed. Refer to the section Changing an IP address in **Specific cases** for more information.

Installing the SSO agent on a workstation that is a member of the domain

To run the SSO agent on a workstation that is a member of the AD domain, 3 rules must be enabled in the firewall on this workstation:

- Remote management of event logs (NP-Entry),
- Remote management of event logs (RPC),
- Remote management of event logs (RPC-EMAP),

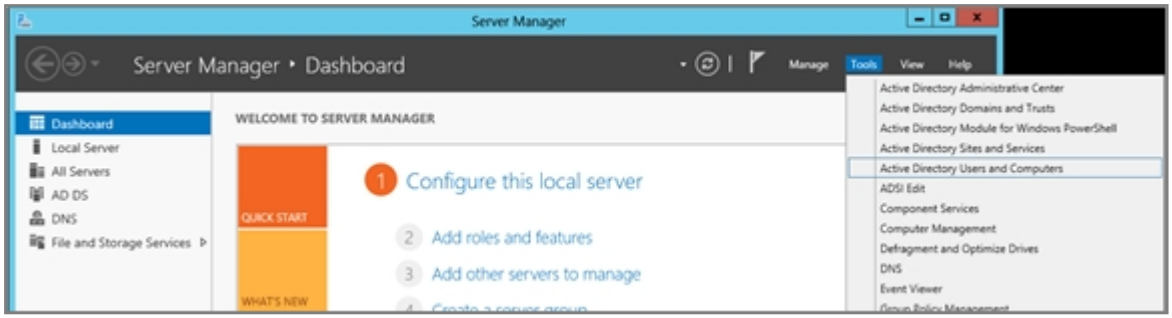
This operation is described in the section Installing SN SSO Agent.

Configuring the user account

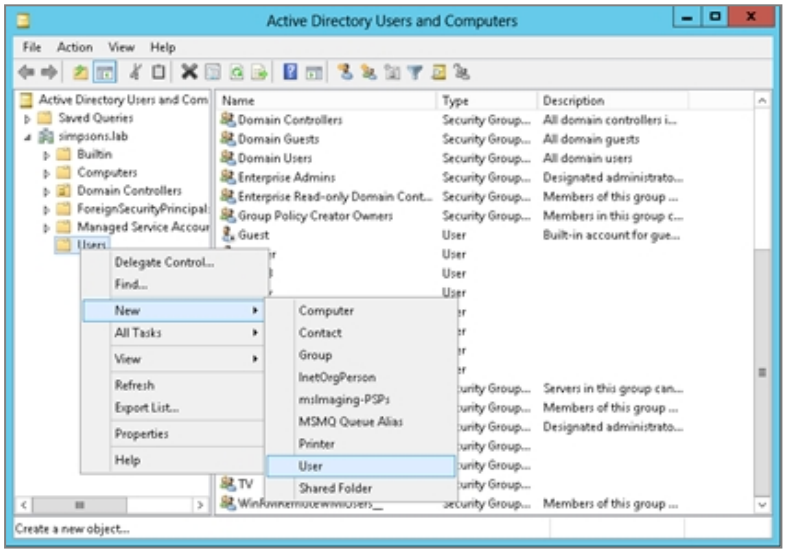
To configure the Active Directory user account for SN SSO Agent, follow the three steps below:

Create an account

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



3. Right-click on the **Users** folder and select **New**, then **User**. Fill in the fields relating to the account (names, login and password).

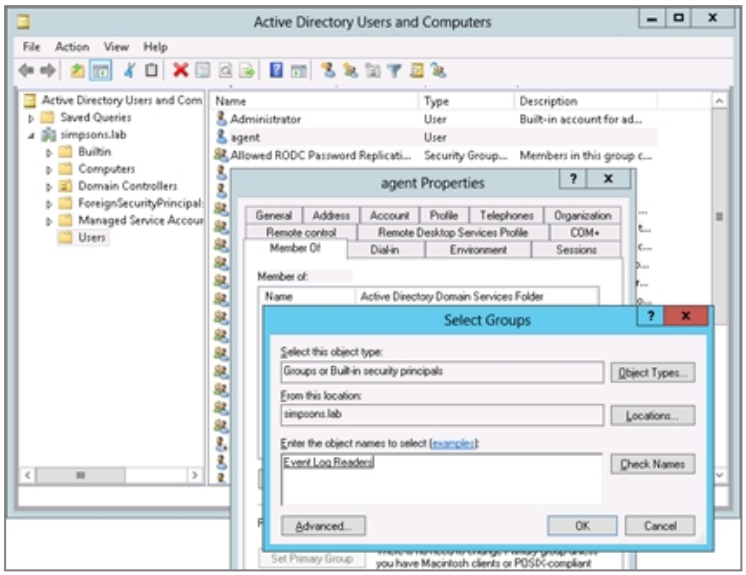


Assign the “Read on event viewer” privilege to the account

This account must belong to the group that has **read privileges on the event viewer** on Active Directory.

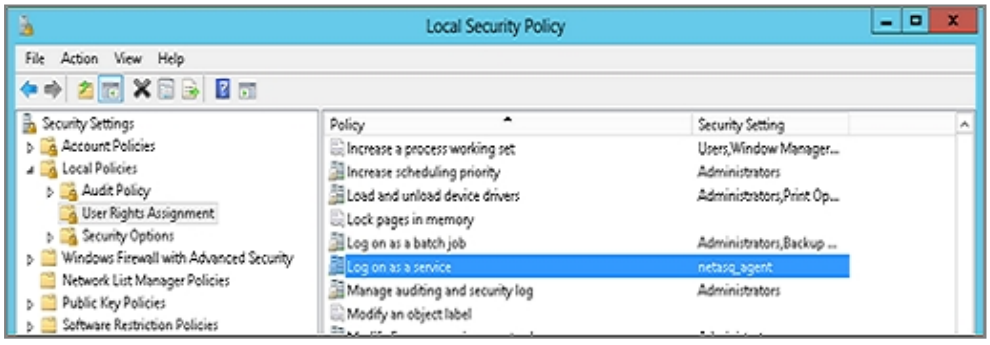
1. Open the **Users** folder and double-click on the **account chosen** from the list,
2. Click on the tab *Member of,*
3. Click on **Add**,
4. Click on **Advanced,**

5. In the search field, enter "Log readers",
   The group will be added to the *Member of* list.



Assign the “Open a session as a service” privilege to the account

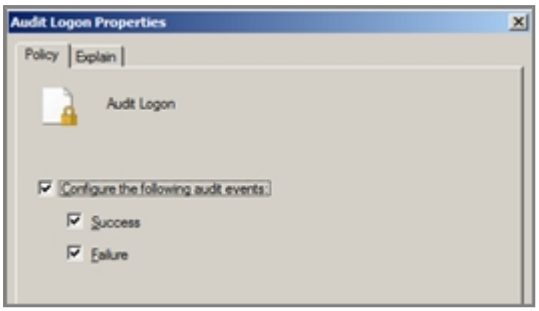
1. In the control panel, click on **Local security policy,**
2. In **Local policies**, select the folder **User Rights Assignment,**
3. Double-click on **Log on as a service** and add the dedicated account.



Saving opened sessions in the Event Viewer

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

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.**



All three checkboxes in the *Policy* tab must be selected.

Installing the SN SSO Agent

You can install SN SSO Agent for Windows on a host that belongs to the Active Directory domain or on your domain controller. The installation wizard helps you to configure the parameters of the SN SSO Agent on the workstation.

NOTE
In a Microsoft Active Directory environment, SN SSO Agent version 3.x can be automatically deployed via a GPO (group policy object). The agent can therefore be installed silently (transparent for the user), with the necessary administration privileges whenever a mobile client passes through the corporate network.

If you are installing the SSO agent on a workstation that is a member of the domain

1. Run **Windows Defender with advanced security features**,
2. Click on the menu on the left **Incoming traffic rules**: the list of rules appears,
3. Using the [Ctrl] key and mouse, select the 3 following rules:
   - Remote management of event logs (NP-Entry),
   - Remote management of event logs (RPC),
   - Remote management of event logs (RPC-EMAP),
4. In the **Actions** panel on the right side of the screen, click on **Enable rule**.
5. Quit **Windows Defender with advanced security features**.

Opening the installation wizard

1. Retrieve the SN SSO Agent for Windows installation program in your MyStormshield area, through **Downloads** > **Stormshield Network Security** > **SSO Agent**.
2. Run the program on the selected host. If you are not logged in as the administrator, right-click on the SN SSO Agent icon and click on **Run as administrator**. The installation wizard will run;

Type of workstation

Specify the account selected for this service and whether you wish to install SN SSO Agent on a domain controller or on a machine belonging to the Active Directory domain.

- You are on the domain controller and wish to use the local system account.
- You wish to specify an account dedicated to the service.

User account associated with SN SSO Agent

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

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

Selecting the SSL encryption key

The **pre-shared key** makes it possible to encrypt communications between SN SSO Agent and the SN 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.

If this is not the first installation, SN SSO Agent will detect the existing pre-shared key. If you are reinstalling SN SSO Agent after it was upgraded, or after changes were made to the workstation, you are advised to keep the pre-shared key.

NOTE
If SN SSO Agent is installed on a workstation in a version lower than 1.4, you must uninstall it before installing the new version. The workstation must be restarted to finalize the uninstallation. Run this operation at the most convenient time in your schedule.

Confirming settings

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

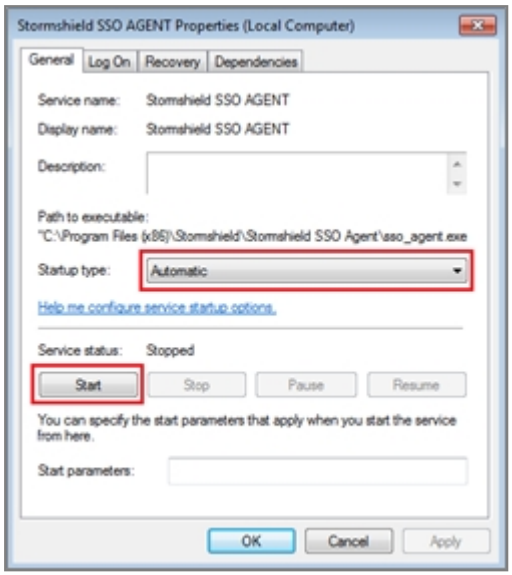
If the installation was successful, click on **Finish.**

Starting the Windows service

As soon as SN SSO Agent is installed, start the **Stormshield SSO Agent** service in Windows services:

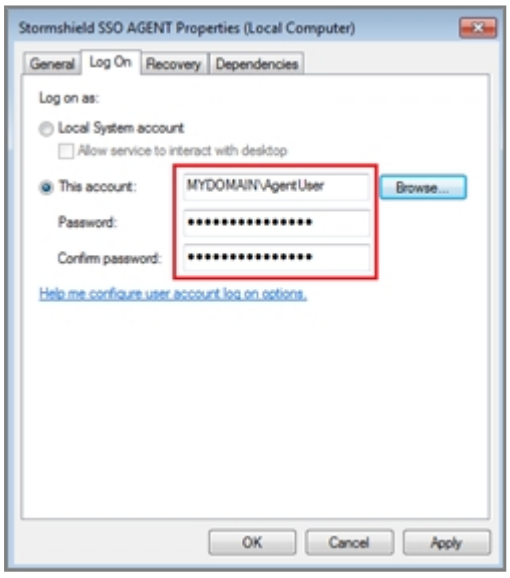
1. Type **Services** in the search field.
2. Confirm by pressing **Enter**.
3. Double-click on the service **Stormshield SSO AGENT**.
4. In the **General** tab, check that the service has been configured in **Automatic** mode when Windows is starting up.

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



If SN SSO Agent was installed on a workstation other than the domain controller, the login and password for the **Active Directory user account** must be entered in the **Log On** tab.

Reminder: this account must have “read” and “open a session as a service” privileges on the Event Viewer. For more information, refer to the section Configuring access to Active Directory.



Configuring the SN firewall

To configure SN SSO Agent on your SN firewall, log in to the firewall's web administration interface at: https://*firewall_IP_address*/admin.

Creating network objects

You need to create **Network objects** corresponding to the workstations that host **SN SSO Agent** and **domain controllers**, if you have several.

1. Go to **Configuration** > **Objects** > **Network objects**.
2. Click on **Add**.
3. In the wizard, ensure that you are in the **Host** tab.
4. Enter the name of the SN SSO Agent or domain controller in the **Object name** field.
5. Enter the IPv4 address of the host. We recommend that you use **static** DNS resolution (fixed IP address). However, depending on your configuration, you can use dynamic resolution (DHCP, which changes the IP address on every connection).
6. The host's MAC address is not required, so enter it only if your configuration requires it.

Configuring Active Directories

You will need to configure Active Directories corresponding to the various SSO agents (maximum five) specified in the authentication methods that the firewall manages. This configuration makes it possible to search for users and groups, especially in the authentication rules and when building a security policy based on these groups and users.

Active Directories can be configured in **Configuration** > **User** > **Directory configuration**.

Configuring the authentication method and policy

Configuring the authentication method

1. Go to **Configuration** > **Users** > **Authentication**, *Available methods* tab.
2. Click on **Add a method** or **Enable a method** (according to the version installed on the SNS firewall).
3. Select **SSO Agent** from the drop-down list.
4. In the section on the right, in the **Domain name** field, select the Active Directory domain associated with SN SSO Agent from the drop-down list.
5. Continue with the configuration section by section according to the parameters below.

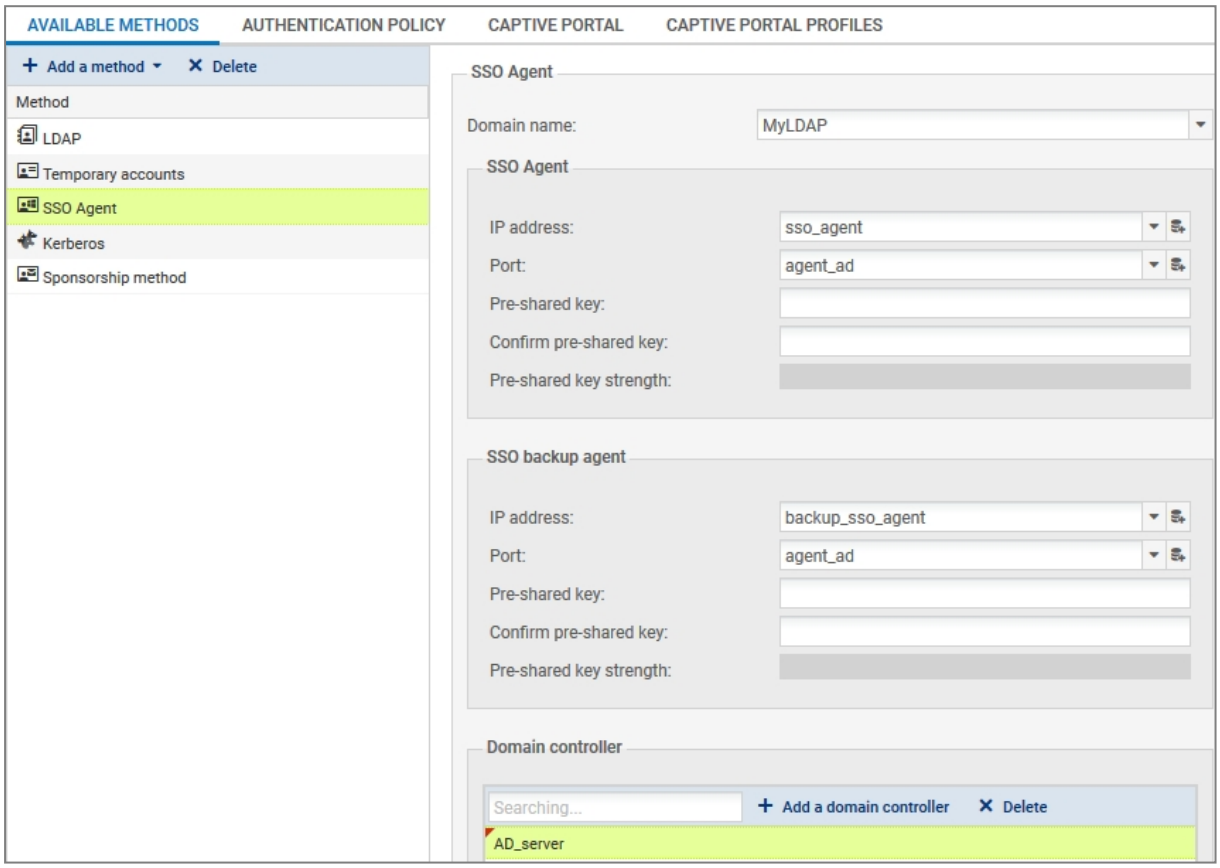
"SSO Agent" section

Enter the information about the main SN SSO Agent:

- **IP address**: from the drop-down menu, select the **network object** that corresponds to the host on which SN SSO Agent is installed.
- **Port**: the port "agent_ad" is selected by default, corresponding to port 1301. The protocol used is TCP.

- **Pre-shared key** (password): enter the key defined during the installation of SN SSO Agent. This key is used to encrypt exchanges between SN SSO Agent and the firewall in SSL. The strength of the pre-shared key indicates this password's level of security. You are strongly advised to use uppercase and special characters.

You can also specify this information for a backup SN SSO Agent (optional).



"Domain controller" section

You will need to add all the domain controllers that control the Active Directory domain. They must be saved beforehand in the firewall's **Network objects** database.

If several domain controllers manage the domain, the account that SN SSO Agent uses must be a dedicated account belonging to the domain, with the privileges described in the chapter Configuring access to Active Directory. These privileges must apply to all domain controllers so that all events occurring on the domain can be relayed.

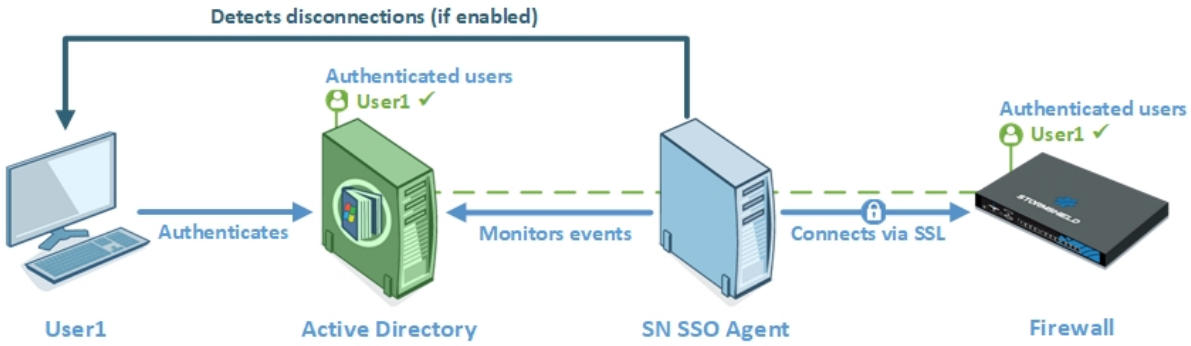
"Advanced properties" section - Microsoft Active Directory mode

Maximum authentication duration: define the maximum duration of an authenticated user's session. After this duration is 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 minutes or hours, and is set by default to 10 hours.

Refresh user groups updates: for each Active Directory configured on the firewall (**Directory configuration**), the firewall will check for any changes to the **LDAP directory groups**. It then updates its directory configuration, and sends back this information to SN SSO Agent.
This limit is to be defined in minutes or hours, and is set by default to 1 hour.

Disconnection detection: by enabling the disconnection method, authenticated users can be deleted when a host is logged out or when a session is shut down. If this method is not enabled, the user will be unauthenticated after the set authentication period, even when the session has been shut down.

To test which hosts are logged in to the firewall, you can either **ping** them or look up the **registry database**.



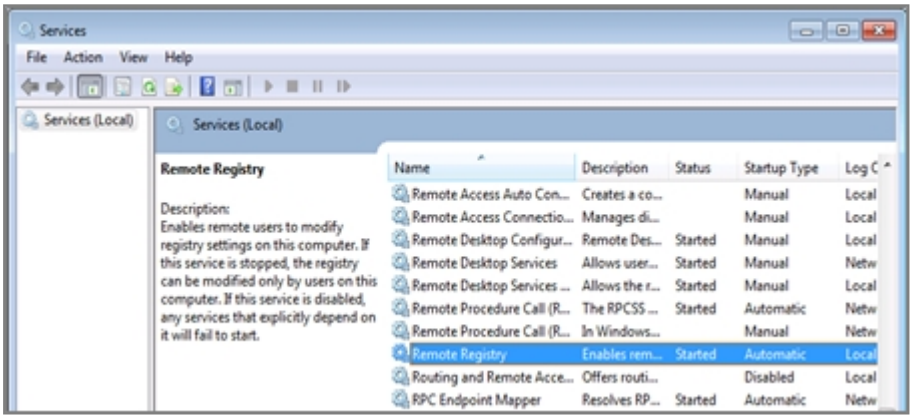
- **PING**: SN SSO Agent tests the accessibility of all hosts authenticated on the firewall every 60 seconds by default.
  If it gets a *host unreachable* response or no response is received from an IP address after the period defined below, SN SSO Agent will send a logoff request to the firewall. The firewall will then will delete the user associated with this IP address from its table of authenticated users, logging the user out of the firewall.

  Hosts on the domain must allow responses to ping tests (parameters of the Windows firewall on workstations). On the other hand, if SN SSO Agent passes through a firewall to access hosts on the domain, rules have to be created to allow SN SSO Agent to test the workstations in the firewall's filter policy.

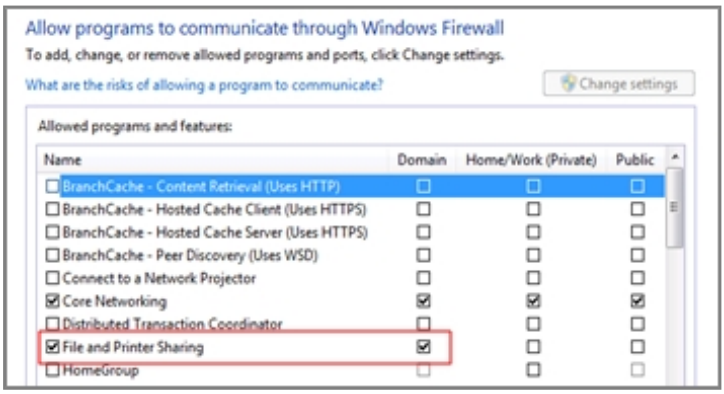
- **Registry database**: this method makes it possible to detect, for example, a closed session on a host that is still running. If a positive response to the ping is received, SN SSO Agent will log in remotely to the host and check in the **Registry database** the list of users with a session open on the host. This allows the registry database to update its table of authenticated users.

  To set up the **Registry database** method, you must meet the following conditions:

  - The account associated with SN SSO Agent must have **administration privileges on all hosts 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 Configuring access to Active Directory).
  - The **Remote registry** service has to be enabled on these hosts. To do so, go to **Services** in Windows, select the service **Remote registry** then click on **Start**. The status of this service must also be changed from **Manual** to **Automatic**.



  - 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**.



  - This method requires the configuration of the opposite zone of the domain on the DNS server in order to detect changes in IP addresses (if a DHCP address is renewed, for example). Refer to the section Changing an IP address in **Specific cases** for more information.

Consider as disconnected after: if a host does not respond to the ping after this period, it will be considered disconnected. The firewall will then delete the user associated with this host from its table of authenticated users. This duration defined in seconds or minutes is set by default to 5 minutes.

Ignored administration accounts: in the firewall's factory configuration, there is a list of users whose authentication is ignored. These accounts list the usual logins dedicated to the administrator (*Administrator* and *Administrateur* by default).

This mechanism was set up because the domain controller treats the execution of a service or an application (*Run as administrator* feature, for example) as an authentication. As SN 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 SN SSO Agent to ignore their authentication. Edit it if necessary.

Configuring the authentication policy

To allow traffic dedicated to the **SSO Agent** authentication method that was configured, you must define rules in the **Authentication policy**.

Adding a new standard rule

1. Go to **Configuration** > **Users** > **Authentication**, *Authentication policy* tab.
2. Click on **New rule**.
3. Select **Standard rule** to run the wizard.
4. Under the **User** tab, in the *User or group* field: select the user or group concerned or leave the default value Any user@*selected domain*.
5. In the **Source** tab: click **Add an object** 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*).

   The **SSO agent** authentication method is based on authentication events collected by domain controllers. Since these events do not indicate the source of the traffic, interfaces cannot be specified in the authentication policy.
6. In the **Authentication methods** tab: click on **Enable a method** and select from the drop-down list the authentication methods to apply to the traffic affected by the rule.
   They are evaluated **in the order in which they appear on the list** and from top to bottom. As the **SSO agent** method is transparent, it is by definition always applied as a priority.
   The **Default method** can be modified below the table containing the rules of the authentication policy
7. Click on **OK,** then on **Apply**.

The **SSO Agent** method does not support multi-user objects, i.e., several authenticated users on the same IP address. However, such objects can be contained in a network, address range or a group defined as the source of a rule that uses the **SSO Agent** method.

To avoid having multiple logs regarding SN SSO Agent being denied for users on an address declared as a multi-user address, 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.

Checking the operation of SN SSO Agent

To check whether SN SSO Agent is correctly installed and configured, you can:

- Look up logs on the host machine,
- Look up logs in the firewall's administration interface,
- Check the status of the Stormshield SSO Agent service,
- Check the configuration of the Windows firewall.

Looking up logs on the host machine

Logs record communications between SN SSO Agent and SN firewalls. Connection information about Active Directory users is collected when SN SSO Agent sends this information to the firewall.

SN SSO Agent creates log files on the host in the following folder:

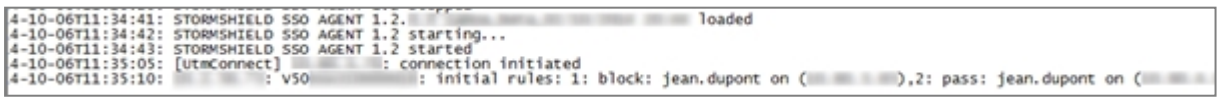
C:\Program Files (x86) \Stormshield\ Stormshield SSO Agent\log

NOTE
Files must not exceed 1 MB. The folder can contain a maximum of 100 MB, or 100 log files. When the folder reaches the maximum capacity, the oldest log file will be erased.
This file, which makes it possible to debug the service, is necessary when you obtain technical assistance from our Technical Assistance Center.

Double-click on a log file to open it, e.g. **stormshieldssoagent.log**. It may contain the following information:

- SN SSO Agent logging in to the firewall. If the connection fails, an error message will appear.
- Rules from the authentication policy applied to users,
- Sessions opened by users. These logs contain:
  - The date and time of the session,
  - The name of the user concerned,
  - The IP address of the host used.
- Logouts from hosts associated with users.

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



Looking up logs on the firewall

You can look up logs on users who authenticate on the firewall on which SN SSO Agent was configured.

1. Log in to the web administration interface of the firewall.
2. Go to **Monitoring** > **Audit logs** > **Users**.
3. In the window, display data according to the desired period.

Checking the Stormshield SSO Agent service

Check the status and properties of the **Stormshield SSO Agent** services in Microsoft Windows services.

Checking the status of the Stormshield SSO Agent service

On a Microsoft Windows Server host

1. Open the **Administration tools** menu.
2. Double-click on the **Services** icon to display the list of services.
3. Check that the status of the Stormshield SSO Agent service is "Running" and that the startup type is "Automatic".

On a Microsoft Windows client workstation

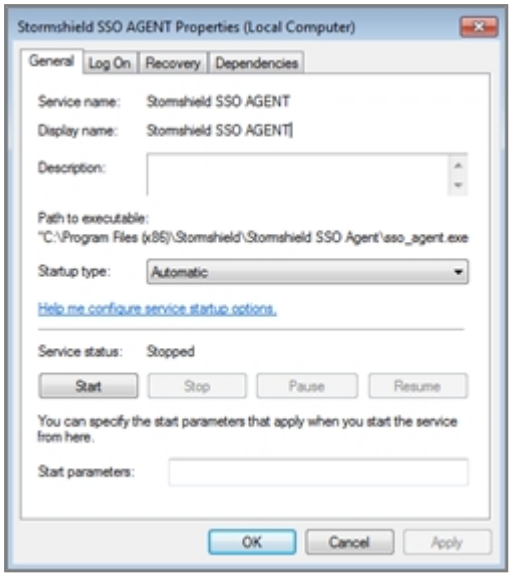
1. Type “services” in the search field.
2. Click on the **Services** icon suggested. The list of services appears.
3. Check that the status of the Stormshield SSO Agent service is "Running" and that the startup type is "Automatic". The user must have **Administrator privileges** on the machine to modify **Services.**

Checking the properties of the Stormshield SSO Agent service

Double-click on the **Stormshield SSO Agent** service to display the service’s properties.

Based on the information below and what you notice, change the properties of the service where necessary.

- **General** tab: check that the service was configured in **Automatic** mode when Windows starts. If the status of the service is **Stopped,** click on the **Start** button.
- **Connection** tab: to prevent the service from shutting down without authorization, you can associate the service with the user account of the service. Example: Domain\user and password on the domain.
- **Recovery** tab: enables the configuration of the SN SSO Agent service if it is shut down. By default, no changes are necessary.
- **Dependencies** tab: the **Stormshield SSO Agent** service does not depend on any other service. By default, no changes are necessary.



Checking the Windows firewall configuration

If a configuration failure occurs during the installation of the firewall, check that port 1301 (default port) is open in its configuration.

Specific cases

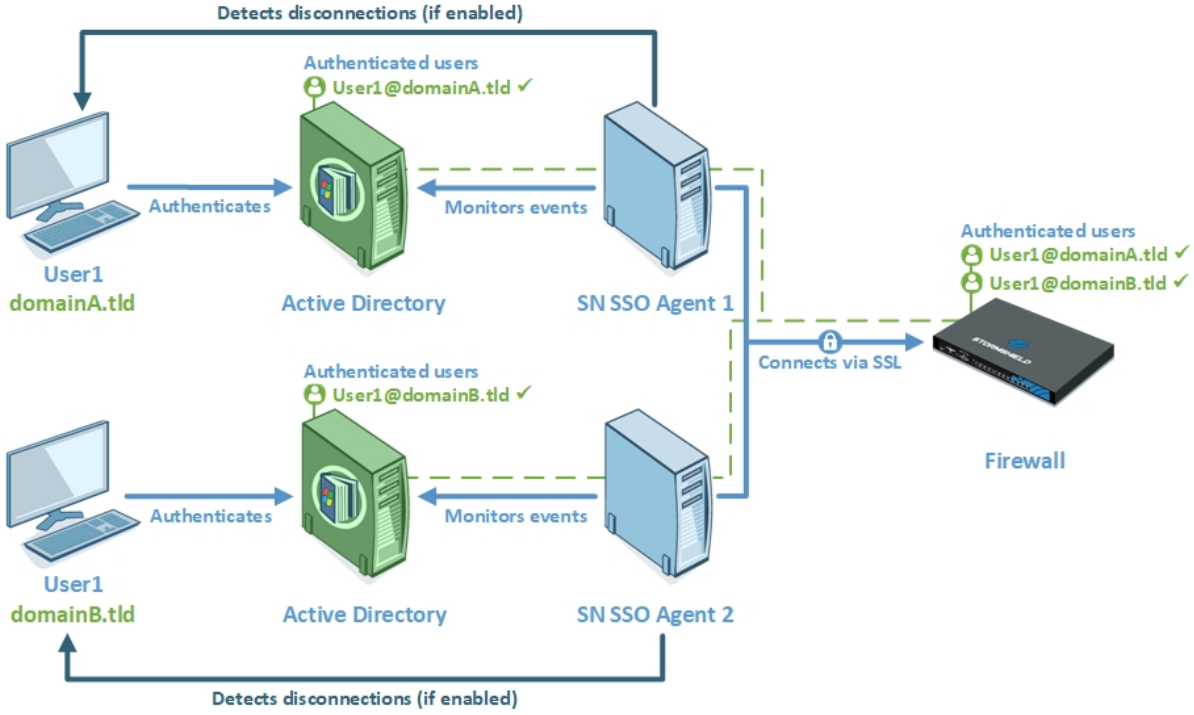
In this section, we cover cases other than the setup of a single firewall in a single Active Directory domain.

Multiple firewalls

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

Multiple domains (different directories)

A firewall can manage up to five different domains. If multiple directories are used, an SN SSO Agent is required for each domain.



Trusting domains

By approving domains, a list of “trusted” domains can be established.

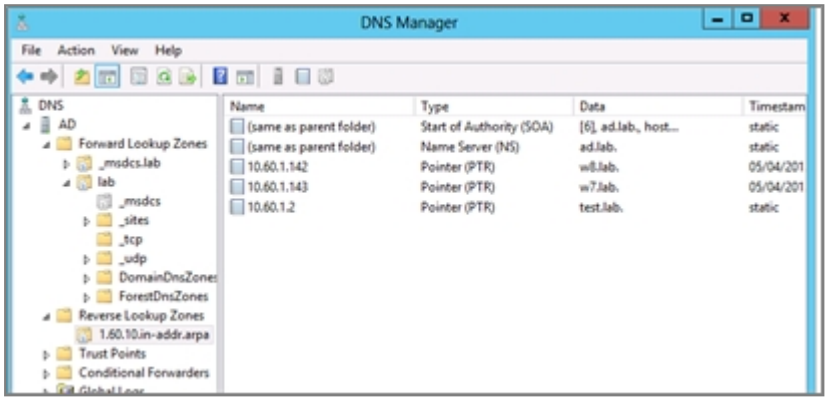
In an Active Directory forest including sub-domains (for example company.int and its sub-domain lab.company.int), approval relationships make it possible to use logins on a domain to access resources on another domain.

As is the case with multiple directories, one SN SSO Agent needs to be dedicated to each domain (or sub-domain) that is part of the trust relationship.

Changing IP addresses

Periodically, SN SSO 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.

In the settings of your DNS server, add a **Reverse lookup zone** (right-click on the folder) for hosts on the domain.



Frequently encountered issues

The following points list some of the most frequently encountered problems. Check these points to resolve malfunctions.

Symptom:

SN SSO Agent cannot log in to the firewall

Solutions:

- Check the **SSL encryption key** i.e. **pre-shared key** (password),
- Check that **port 1301** is not blocked by a firewall or on the machine hosting SN SSO Agent,
- Check logs from the firewall administration interface in **Monitoring** > **Audit logs** > **Users**. For more information, refer to the section Looking up logs on the firewall.

Symptom:

SN SSO Agent cannot log in to the domain controller

Solutions:

- Check that the account associated with SN SSO Agent has **read privileges on the event viewer** in Active Directory,
- Check that **ports 139 and 445** are not blocked by a firewall or on the machine hosting SN SSO Agent.

Symptom:

No authentication on the firewall

Solution

If there are no authenticated users on the firewall based on what was reported in log files, you are advised to test the authentication method using an authentication rule with *Any* as the **User** value and as the **Source**.

Symptom:

Hosts do not respond to the ping (users de-authenticated from the firewall).

Solution

If SN SSO Agent is unable to test a host by pinging it, the firewall will automatically delete the login from its table of authenticated users. This action is logged in SN SSO Agent logs. For more information, refer to the section Looking up logs on the host machine.

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

Symptom:

Could not connect to the registry database.

Solutions:

If SN SSO Agent is unable to access a machine, it will be logged in SN SSO Agent logs. For more information, refer to the section Looking up logs on the host machine.

- **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 SN SSO Agent has administration privileges on these machines.

Symptom:

Change of IP address not detected.

Solutions:

Changes to IP addresses have been detected by DNS requests:

- Check that the DNS servers have been configured for hosts in the domain.

If the hosts are configured in DHCP, the DHCP server must update the entries in the DNS servers.

- Check that the reverse lookup zone was created. For more information, refer to the section Changing IP addresses in **Specific cases**.

Further reading

Additional information and responses to questions you may have about the SSO Agent are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu