STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

SN SSO AGENT FOR LINUX - INSTALLATION AND DEPLOYMENT

Product concerned: SNS 4.1 and higher, SSO Agent 2 and 3 for Linux

Document last update: May 4, 2021

Reference: sns-en-sso_agent_linux_technical_note-v4

Table of contents

Getting started

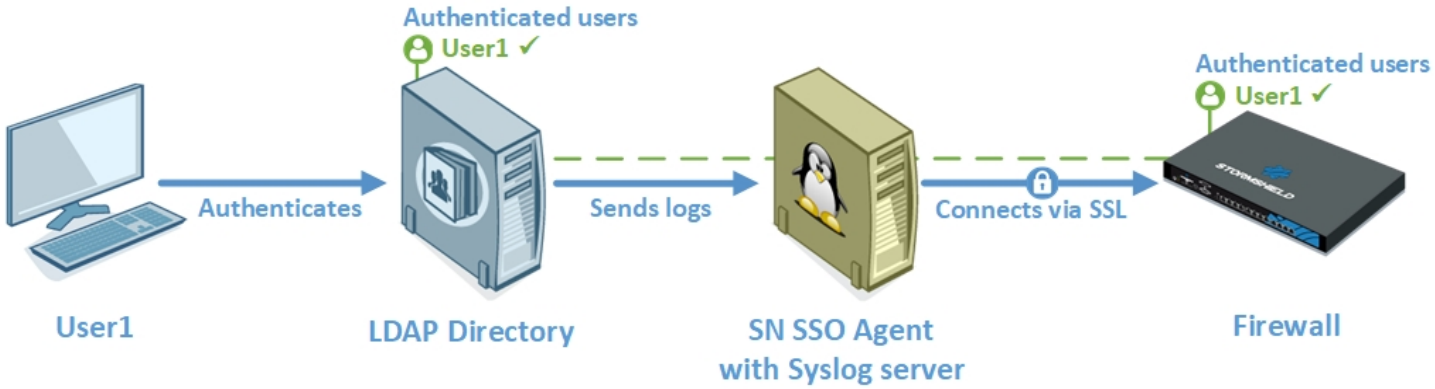
With SN SSO Agent for Linux, SN firewalls can authenticate transparently on non-Microsoft Active Directories such as Samba 4.

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

Introduction

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

When a session is opened and users authenticate on the authentication domain, these operations are logged. These logs are then sent in syslog format to the SN SSO Agent, which is equipped with a syslog server that filters the logs using regular expressions. SN SSO Agent then relays this information to the firewall through an SSL connection, which updates its table of authenticated users.



Requirements

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

- A machine running in Ubuntu 18.04 LTS to host SN SSO Agent,
- An SNS firewall and SN SSO Agent for Linux running in a compatible version:

SN SSO Agent for Linux	Compatible SNS versions
Version 2.1.0	Versions 3.10, 3.11 LTSB and 4.1
Version 3.0.1	Version 4.2 and higher

Recommendations

Securing communications with the syslog server

Communications between the LDAP directory and the SN SSO Agent syslog server must be in UDP. Since this protocol does not guarantee confidentiality or integrity, we recommend that you secure these communications to prevent potential security risks.

This can be done by physically segmenting the network, setting up a VLAN, or using IPSec, SSH or SSL tunnels. Alternatively, a TLS syslog server relay can also be placed between the hosts concerned.

Even though SN SSO Agent can be installed on the same machine as the LDAP directory, we recommend that you install them on separate machines.

Service restrictions

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 the LDAP directory

For the purposes of this technical note, we used a non-Microsoft Samba 4 LDAP directory installed on a workstation running in Ubuntu 18.04 LTS.

Configuring the directory to log authentication events

Edit the Samba 4 LDAP directory configuration file according to the usage context in your environment. The path to this file may vary depending on your installation.

In our example, the file is located at */usr/local/samba/etc/smb.conf* and contains the following configuration:

```
log level = 3
vfs object = full_audit
full_audit:success = connect
full_audit:failure = disconnect
full_audit:prefix = %u %I | %S
full_audit:facility = local5
```

Parameter	Details
log level	Defines which events to log. Level 3 makes it possible to keep logs of authentication events.
vfs object	Corresponds to the VFS module that Samba uses. In our example, we needed to use the *full_audit* module.
full_audit:success	Identifies the list of VFS operations that must be logged if they are successful. In our case, we added *connect* to log connection operations. The opposite parameter exists for operations that fail, and use *full_audit:failure*.
full_audit:prefix	Defines the format used to generate logs. Customize it with variables that reference specific elements, such as *%u*, which corresponds to the user name used. As these logs are sent to the SN SSO Agent syslog server, which analyzes them with regular expressions, define a format that is adapted to the elements that you want to send.
full_audit:facility	Associates an application system with the logs that you want to send to the SN SSO Agent syslog server.

For further information, refer to official Samba configuration documentation and official Samba documentation on the "full_audit" VFS module.

After the configuration is modified, run this command so that the daemon will reload its configuration and apply it:

```
smbcontrol all reload-config
```

Sending logs

The Samba 4 LDAP directory depends on a syslog client that allows it to send logs in syslog format to the SN SSO Agent syslog server.

In the folder */etc/rsyslog.d/*, create a file and name it "00-samba.conf". Add the desired configuration to it in the following format:

```
facility.syslogseverity @ip:port
```

In our example, we used the following configuration:

```
local5.notice @172.30.227.74:3514
```

Parameter	Details
facility	Defines the application system for which the syslog client captures logs. In our example, it corresponds to the *full_audit:facility* parameter entered in the Samba 4 LDAP directory configuration.
syslogseverity	Corresponds to the severity of the syslogs. Since the application system (facility) is entered, it determines which logs will be sent to the SN SSO Agent syslog server.
@	Specifies that UDP mode is used to send logs. Communications with the SN SSO Agent syslog server must be in UDP.
ip:port	Corresponds to the IP address of the SN SSO Agent to which logs will be sent, and the port number that the syslog server will listen on. We recommend that you use a port higher than or equal to 1024. To use a port lower than 1024, SN SSO Agent must restart with administrator privileges (sudo).

For more information, refer to official syslog documentation.

After the configuration is added, run this command so that the rsyslog daemon will restart:

```
sudo service syslog restart
```

Installing SN SSO Agent

Downloading SN SSO Agent

1. Log in to your MyStormshield personal area.
2. Go to **Downloads**,
3. Under **Stormshield Network Security** > **SSO Agent**, download the SN SSO Agent archive for Linux and copy it to the machine on which you want to install it.

Configuring SN SSO Agent

1. On the target machine, decompress the archive in the folder of your choice. Access to this folder must be restricted for security reasons.
2. Open the SN SSO Agent configuration file "config.ini".
3. Edit the following parameters:

Parameter	Detail
VerboseLevel	Defines how much information will be logged. Enter *low* if this parameter is used in production. Use *high* for the installation phase.
SSLKey	Sets the password that allows the SN SSO Agent to communicate with your firewall. To ensure that this password is complex, we recommend that you use a combination of lowercase, uppercase and special characters, with a minimum required length. Memorize this password, as you will need to enter it in the configuration of your firewall.

Starting SN SSO Agent

Use the following command to start SN SSO Agent:

```
./stormshieldssoagent
```

Manipulate the command to start SN SSO Agent with administrator privileges (sudo) if it needs to use a syslog port lower than 1024.

You can also configure SN SSO Agent to start automatically on the machine. To do so, we recommend that you create a specific service that makes it possible to launch SN SSO Agent automatically during the startup process. There are several solutions, such as via *Systemd* or */etc/init.d*.

Configuring the SN firewall

The configuration of the firewall involves several necessary operations:

- Creating network objects,
- Adding the LDAP directory,
- Adding an authentication method,
- Defining an authentication policy.

Creating network objects

Several network objects must be created:

- A Host object for the device that hosts the LDAP directory,
- A Host object for the device that hosts SN SSO Agent,
- A Port object that represents the listening port on the SN SSO Agent syslog server, except when you use the default port (UDP port 514) that is already represented by an object.

Creating host objects

1. Log in to the firewall's administration interface: https://*firewall_IP_address*/admin,
2. Go to **Configuration** > **Objects** > **Network objects**.
3. Click on **Add**.
4. In the wizard, ensure that you are in the **Host** tab.
5. Enter the name of the SN SSO Agent or LDAP directory in the **Object name** field.
6. Enter the IPv4 address of the host in question. 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).
7. The host's MAC address is not required, so enter it only if your configuration requires it.

If you have several SN SSO Agents or LDAP directories, create host objects for each of them.

Creating the port object

1. Log in to the firewall's administration interface: https://*firewall_IP_address*/admin,
2. Go to **Configuration** > **Objects** > **Network objects**.
3. Click on **Add**.
4. In the wizard, ensure that you are in the **Port** tab.
5. Give the object a name.
6. Enter the port number on which you want the syslog server to listen.
7. Set UDP as the protocol.

If you have several SN SSO Agents, and therefore several syslog servers, create a port object for each listening port that you need in your configuration.

Adding the LDAP directory

By adding your LDAP directory, you will be able to search for your users and groups straight from the firewall. You can then define authentication policies involving these users and groups on your LDAP directory.

To add the LDAP directory on the firewall:

1. Log in to the firewall's administration interface: https://*firewall_IP_address*/admin,
2. Go to **Configuration** > **Users** > **Directory configuration**.
3. If directories have not yet been configured on the firewall, the wizard will appear automatically. If you have configured directories elsewhere, click on **Add a directory**.
4. Select "Connect to an external LDAP directory" in the wizard.
5. Enter the login information for the directory. For more information, refer to the SNS user guide.

Repeat these steps to add several directories. You can configure up to four non-Microsoft LDAP directories and/or Active Directories in addition to the internal directory.

Adding authentication methods

The *SSO Agent* authentication method must be configured on your firewall so that users can authenticate on an authentication domain. You can configure up to five SSO Agent authentication methods.

1. Log in to the firewall's administration interface: https://*firewall_IP_address*/admin,
2. Go to **Configuration** > **Users** > **Authentication**, *Available methods* tab.
3. Click on **Add a method** and select **SSO Agent** in the drop-down menu.
4. In the section on the right, select the relevant authentication domain from the drop-down list in the **Domain name** field.
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:

Field	Details
IP address	Select from the list the host object that corresponds to the SN SSO Agent created earlier.
Port	Leave the object *agent_ad* selected by default.
Pre-shared key	Enter the SSLKey defined when SN SSO Agent was installed. This key is used to encrypt exchanges between SN SSO Agent and the firewall in SSL. The strength of the pre-shared key indicates the password's level of security.

"Domain controller" section

Add all the LDAP directories that control the authentication domain concerned. They must be saved beforehand in the firewall's **Network objects** database. For more information, refer to the section Creating network objects.

"Advanced properties" section

Mode: since SN SSO Agent is installed on a Linux machine, select **Syslog server mode**.

Syslog server configuration:

Field	Details
Listening IP address	Select from the list the host object associated with the machine that hosts SN SSO Agent and its syslog server.
Listening port	Select from the list the port object representing the listening port on the syslog server. The object *syslog* is selected by default (UDP port 514)
IP address search	Regular expression that will be used to search for IP addresses in logs hosted on the syslog server. For this technical note, we used: `([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s`
User search	Regular expression that will be used to search for user names in logs hosted on the syslog server. For this technical note, we used: `DOMAINNAME\\([a-zA-Z0-9\.]*)\s` Replace "DOMAINNAME" with the authentication domain used. Remember to protect special characters, if you are using any.
Message search	Regular expression that will be used to search for connection messages in logs hosted on the syslog server. For this technical note, we used: `connect|ok` Ensure that the format of this regular expression is correct so that you do not include unnecessary results in the search.

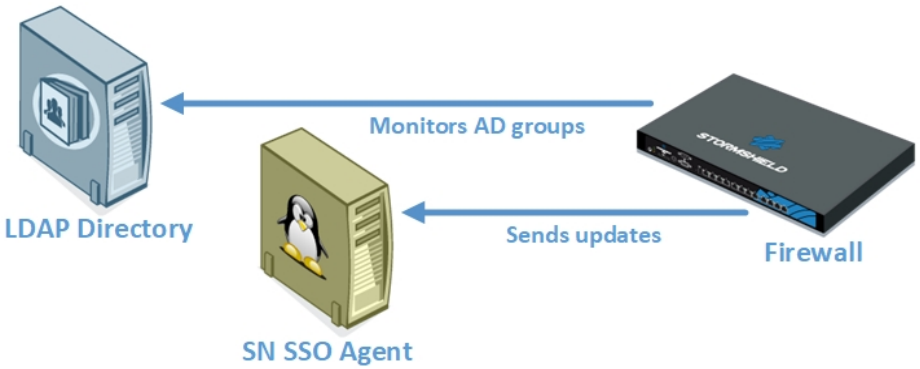
For more information on these elements, refer to the SNS user guide.

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

Refresh user groups updates: for every LDAP directory configured, the firewall will check for any changes to the **LDAP directory groups**. The firewall then updates the configuration of its directory, and sends back this information to SN SSO Agent.

This limit is defined in minutes or hours, and is set by default to 1 hour.

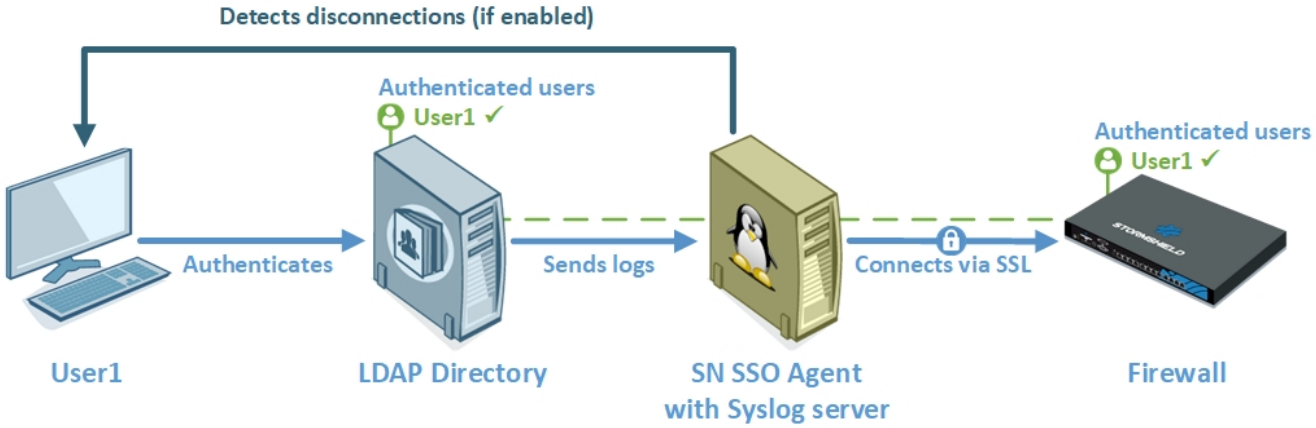


Disconnection detection: enable the disconnection method so that authenticated users can be deleted when a host is disconnected or when a session is shut down. If this method is not

enabled, the user will be logged out when the maximum authentication period expires, even when the session has been shut down.

SN SSO Agent tests the accessibility of all hosts authenticated on the firewall by pinging them every 60 seconds. To ensure the success of these tests:

- Workstations on the authentication domain must allow responses to pings (ICMP requests). The Windows firewall may block such requests in some cases.
- A rule in the firewall's filter policy must allow SN SSO Agent to test hosts on the authentication domain if the agent must access it through the firewall.



Consider offline after: if a host does not respond within the time frame set in the "Disconnection detection" test conducted every 60 seconds, SN SSO Agent will consider this host offline. The agent will then send a disconnection request to the firewall, which will delete the user from its table of authenticated users, logging the user out of the firewall.

This duration defined in seconds or minutes is set by default to 5 minutes.

Enable DNS host lookup: enable this setting if the hosts connected to the firewall have several IP addresses or their addresses change regularly. This setting may be useful, for example, if your users often switch from an Ethernet configuration to a Wi-Fi connection.

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. To ensure the success of these tests:

- A **Reverse lookup zone** (right-click on the folder) must be added to the settings of the DNS server for the authentication domain,
- A rule in the firewall's filter policy must allow SN SSO Agent to test hosts on the authentication domain if the agent must access it through the firewall.

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

This mechanism was set up because the LDAP directory 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 session.

The pre-defined list of "Ignored Administrator accounts" allows SN SSO Agent to ignore their authentication. Edit it if necessary.

Defining an authentication policy

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

1. Log in to the firewall's administration interface: https://*firewall_IP_address*/admin,
2. Go to **Configuration** > **Users** > **Authentication**, *Authentication policy* tab.
3. Click on **New rule** and 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@domain*.
5. In the **Source** tab, click on **Add an object** and select the source of the traffic to which the rule applies. This object can be the one that corresponds to internal networks (*network_internals*).
   Interfaces cannot be specified as criteria for the SSO Agent authentication method, as it is based on authentication events gathered by LDAP directories. Since these events do not indicate the source of the traffic, interfaces may not always be specified in the authentication policy.
6. In the **Authentication methods** tab, click on **Authorize 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**, from top to bottom. As the SSO Agent method is transparent, it always has priority.
   The default method can be changed below the table containing the rules of the authentication policy
7. Click on **OK,** then on **Apply**.

Repeat the steps above to add several rules.

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

To prevent multiple logs from being generated when SN SSO Agent is denied for users on an address declared as a multi-user address, we recommend that you add two rules dedicated to such objects in front of the rules that use the SSO Agent method:

- The first rule specifies the authentication method used by the multi-user object,
- The next rule blocks any other authentication method for multi-user objects.

Checking service operation

By checking the operation of the service, you will be able to ensure that SN SSO Agent was correctly installed and configured, and that the configuration of firewall is also accurate.

There are several ways in which you can check service operation:

- Reading SN SSO Agent logs,
- Reading logs in the firewall's administration interface.

Reading SN SSO Agent logs

Logs capture communications between SN SSO Agent and your firewall, and may contain the following information:

- The SN SSO Agent's connection to the firewall. If the connection fails, an error message will appear.
- Rules from the authentication policy applied to users,
- Sessions opened by users – date and time of sessions, name of the user concerned, IP address of the machine used, etc.
- Logouts from workstations associated with users.

To access logs, identify the folder on which SN SSO Agent was installed on the machine, then look up the files in the folder */log/*, e.g., "stormshieldssoagent.log".

Files must not exceed 1 MB each. The folder can contain a maximum of 100 MB. When the folder reaches its capacity, the oldest log files will be erased. These files make it possible to debug the service, and you will be asked to provide them when you request assistance from our Technical Assistance Center.

The image below is an extract from a log file that contains information about an agent connecting to the firewall.

Reading logs on the firewall

The firewall on which the SSO Agent authentication method has been configured allows you to read the logs of authenticated users and of connections between SN SSO Agent and the firewall.

User authentication

1. Log in to the firewall's administration interface: https://*firewall_IP_address*/admin,
2. Go to **Monitoring** > **Monitoring** > **Users**.
3. Filter the results by authentication method.

For more information, refer to the SNS user guide and the technical note Complying with regulations on personal data.

Connection between SN SSO Agent and the firewall

1. Log in to the firewall's administration interface: https://*firewall_IP_address*/admin,
2. Go to **Monitoring** > **Audit logs** > **System events**.
3. In the window, display data according to the desired period.

For more information, refer to the SNS user guide.

Specific cases

In this section, we cover cases other than the setup of a single firewall in a single authentication domain with a single SN SSO Agent.

Multiple firewalls managing the same authentication domain

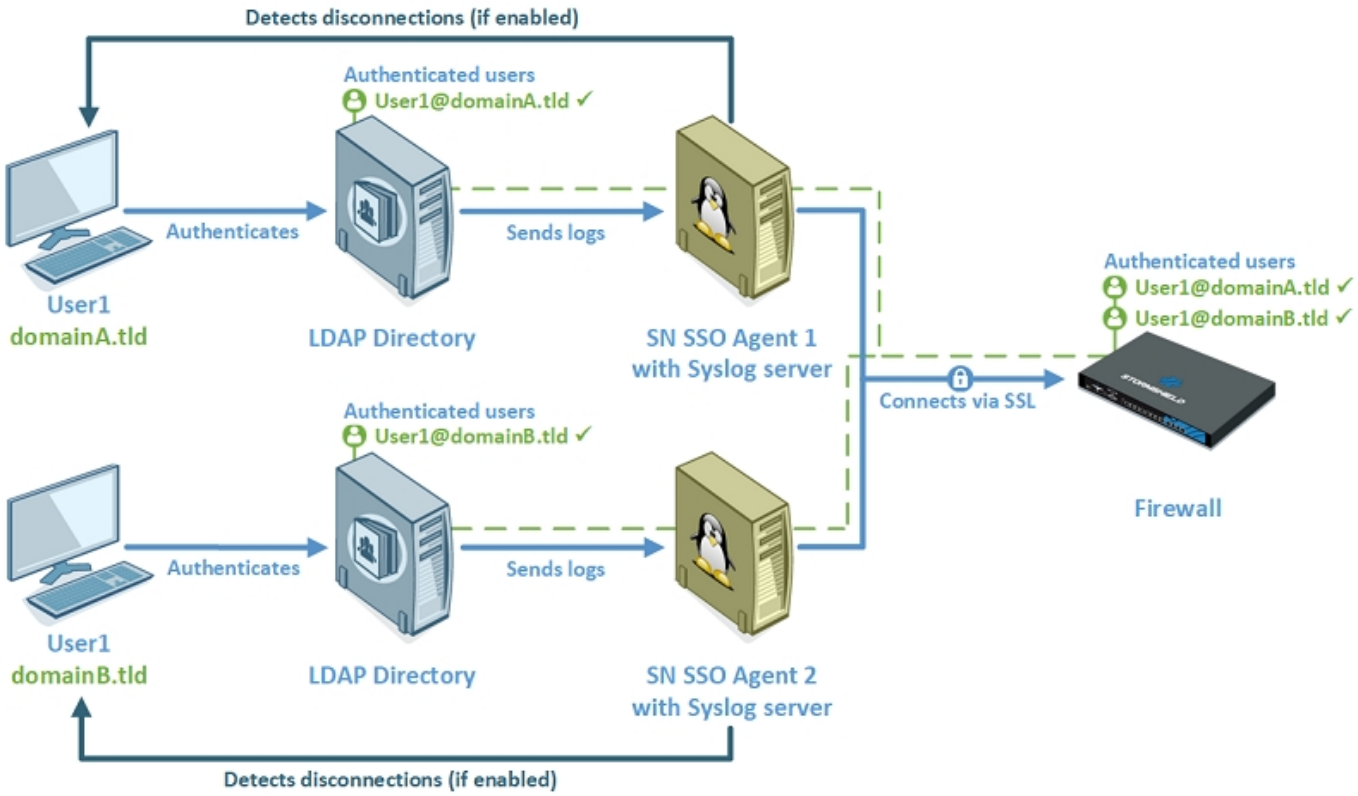
Several firewalls managing the same authentication domain can log in to the same SN SSO Agent.

Single firewall managing several authentication domains

Whenever a firewall manages several authentication domains, regardless of whether they are non-Microsoft LDAP directories and/or Active Directories, an SN SSO Agent must be dedicated to each domain. Each firewall can manage up to five SN SSO Agents, therefore up to five different authentication domains.

For more information on installation with a Microsoft Active Directory type of authentication domain, refer to the technical note Stormshield Network SSO Agent pour Windows.

The following illustration shows a firewall managing two authentication domains that are non-Microsoft LDAP directories.



Resolving issues

Check the points below to resolve malfunctions.

SN SSO Agent cannot connect to the firewall

- Check the **SSL encryption key** (SSLKey) , known as the **pre-shared key**.
  It is entered in the SN SSO Agent configuration (config.ini file) and in the configuration of the SSO Agent authentication method.
- Ensure that **port 1301**, or the port that you have customized, is not blocked by a firewall or located on the machine that hosts SN SSO Agent.
  For this machine, check that messages can be sent correctly through this port with the command:
  ```
  tcpdump port 1301
  ```
- Check logs from the firewall administration interface in **Monitoring** > **Audit logs** > **System events**.

No users are authenticating on the firewall

- Check logs from the firewall administration interface in **Monitoring** > **Audit logs** > **Users**.
- Ensure that there are no rules in the authentication policy blocking users who attempt to authenticate.
  Try to add in the first position (right at the top) in your authentication policy a rule that uses the following elements:
  - For the **User** field: “All”,
  - For the **Source** field: "Any",
  - For the **Authentication methods** field: the SSO Agent method concerned.
- Using the following command, check whether the messages that the SN SSO Agent syslog server sends to the firewall go through the port defined in the configuration as expected.
  ```
  tcpdump port 3514
  ```
- Ensure that the correct information regarding the syslog server is entered in the SSO Agent authentication method configured on the firewall.
- Ensure that the regular expressions configured in your firewall and used by the SN SSO Agent syslog server make it possible to retrieve the authentication events that are required for the service to run. If necessary, check your regular expressions (*RegEx*) on websites that provide such a service.

The SN SSO Agent syslog server is not retrieving events from the LDAP directory

- Ensure that the configuration of your LDAP directory is accurate. For more information, see the section Configuring the LDAP directory.
- Check whether the LDAP directory correctly logs authentication events. In our example, we used the following command to check it on a Samba 4 server. The access path may have been modified in the configuration of the server (file smb.conf).
  ```
  tail -f /var/log/messages.log
  ```

- Check the configuration of the syslog client installed on the same machine as your LDAP directory (file 00-samba.conf). Try to modify its configuration so that it sends all logs regardless of their severity and associated application system. Follow the format below by keeping "*.*" :

```
*.* @ip:port
```

documentation@stormshield.eu