TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

SN TS AGENT - INSTALLATION AND DEPLOYMENT

Product concerned: SNS 4.7 and higher versions, SN TS Agent 1.0.2 and higher versions

Document last updated: October 30, 2023

Reference: sns-en-SN_TS_Agent_installation_and_deployment_technical_note

Table of contents

Change log

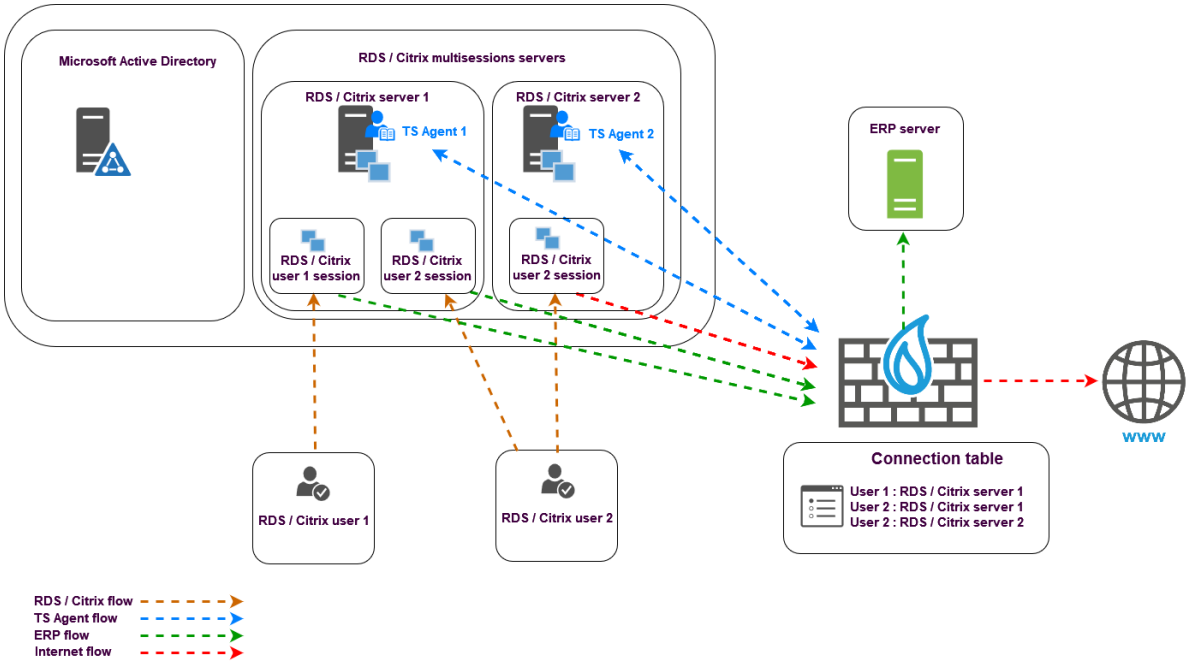
Date	Description
October 30, 2023	New document

Getting started

The SN TS Agent transparent authentication method is intended for multi-user authentication in VDIs (Virtual Desktop Infrastructures).

This method relies on exchanges between a dedicated service on the SNS firewall (TSD service) and TS agents deployed on Citrix Virtual Apps and Desktops or Microsoft Remote Desktop Services (RDS).

Every user that authenticates with the server's IP address is identified by the firewall with a dedicated source network port range (network ports higher than 1024) that the SN TS Agent assigns.



NOTE

Further on in this document:

- Citrix Virtual Apps and Desktops servers will be referred to as "Citrix servers",
- Microsoft Remote Desktop Services servers will be referred to as "RDS servers",
- SN TS Agent can also be referred to as "TS Agent" in reference to its name in the SNS web administration interface.

Click on the links below for more information on:

- Microsoft (Remote Desktop Services),
- Citrix Virtual Apps and Desktops.

Compatibility and limitations

Compatibility

Stormshield Network Firewall

4.7 and later versions

Operating systems

Windows Server 2016, 2019 and 2022

Server components

Citrix Virtual Apps and Desktop 7 LTSR (2203) Microsoft Remote Desktop Services (RDS)

Specifications

Maximum number of TS Agents for an SNS firewall:	100
Maximum number of users per TS Agent:	20 to 50 (values recommended by Citrix and Microsoft for a multi-session server).
Maximum number of port ranges per user:	20 (by default: 2)
Number of ports per range:	50 to 1000 (by default: 200)

Limitations and explanations on usage

- Transparent authentication will not function on the TS Agent if ports (PAT) or addresses (NAT) are translated between the TS Agent and the SNS firewall,
- Users authenticated via the TS Agent cannot be disconnected via the pop-up menu in user monitoring.
  A user can only be forced to disconnect with the command *sfctl -a* from the firewall's console, and the TSD service on the firewall must be restarted so that the user in question can authenticate again.

Configuring the TS Agent authentication method on the firewall

Go to **Configuration > Users > Authentication> Available methods** tab.

The TS Agent method appears directly in the list of authentication methods enabled (left side of the screen).

Creating TS Agents

In the **TS agent list** on the right side of the screen:

1. Click on **Add**.
2. As for the status (ON/OFF switch), you are advised to leave the TS agent inactive (OFF) to avoid generating unnecessary alarms and logs.
   It will be enabled when the agent is deployed on the RDS/Citrix server.
3. In the **TS agent name** field, indicate the name you want to give this agent (e.g., *RDS-1-TS-AGENT*).
4. In the **TS server** field, select or create the object corresponding to the RDS/Citrix server on which the TS agent will be installed (e.g., RDS-1-SERVER).
5. In the **Port** field, select or create the object corresponding to the dialogue port between the firewall and the TS agent..
   The object *agent_ts* (TCP/1303) is suggested by default.

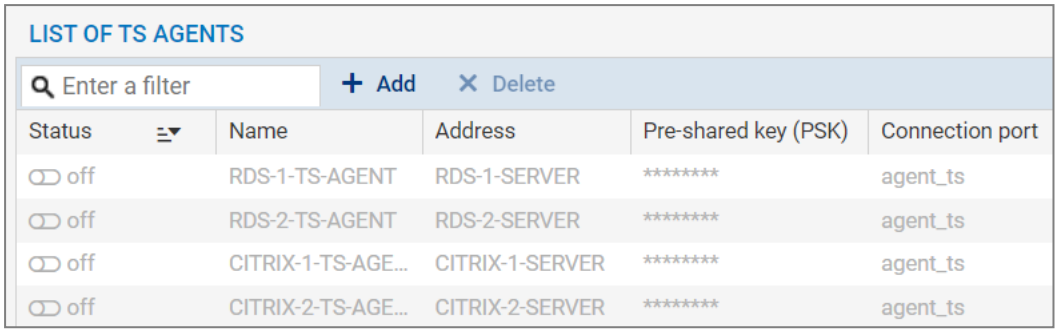
   > **NOTE**
   > If you select any port other than the default port, it must also be changed on the corresponding TS Agent (see Identifying/editing SN TS Agent operating settings).

6. Enter and confirm the **Pre-shared key** used during the exchanges between the Firewall and the TS agent.
   This pre-shared key must meet the minimum entropy set on the firewall (**Configuration** > **General configuration** tab, **Password policy** section).

   > **NOTE**
   > This key can be changed later.
   > You must also change the pre-shared key on the TS Agent in question, through the Windows registry key of the server on which this TS Agent is installed (see Identifying/editing SN TS Agent operating settings).

7. Confirm by clicking on **Apply**.
   The TS agent is added to the **TS agent list**.

Repeat steps 1 to 7 for each TS Agent to be created on the firewall (maximum 100 TS Agents per firewall).



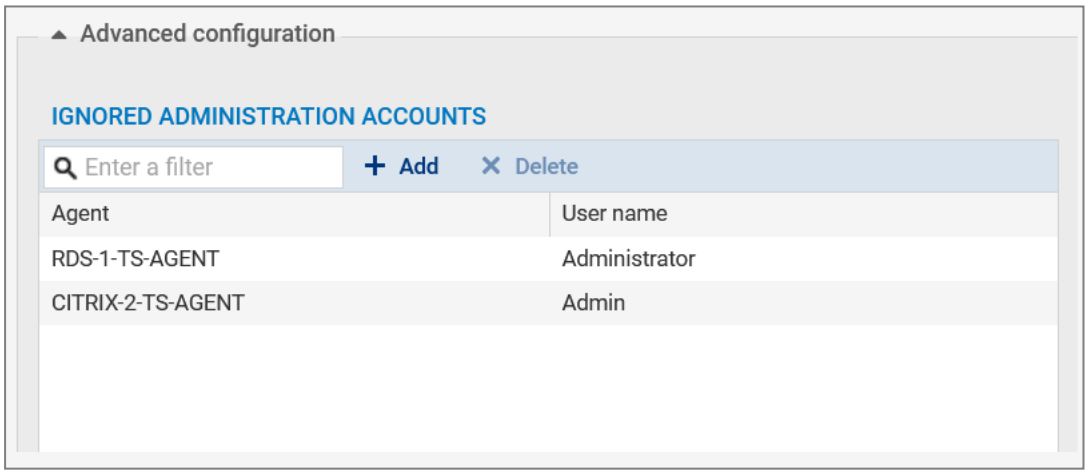
Excluding administration accounts (optional)

For each TS agent configured, administration accounts can be excluded from the TS Agent authentication mechanism.

In this case, even when traffic initiated by the selected administrator accounts matches filter rules that allow the TS Agent method, the firewall will block such traffic.

To add an administration account to ignore:

1. Expand the **Advanced properties** section,
2. In the **Ignored administration accounts** grid, click on **Add**,
3. Select a TS Agent configured earlier,
4. Enter the name of the administration account to ignore.



Adding the TS Agent authentication method to the authentication policy

NOTE
The external Microsoft Active Directory LDAP, to which the users who must be authenticated via the TS Agent belong, must be defined beforehand on the firewall.
More information on configuring directories on an SNS firewall.

Go to **Configuration** > **Users** > **Authentication**> **Authentication policy** tab, then:

1. Click on **New rule** and select **Standard rule**.
2. In the **Users** menu, select a user or user group allowed to use the TS Agent method.

3. In the **Source** menu, add the network interfaces on which the RDS/Citrix servers or objects/groups representing the networks or RDS/Citrix servers are connected (e.g., RDS1-SERVER).
4. In the **Authentication** methods menu, add the TS Agent method.

IMPORTANT
The TS Agent method cannot be combined with another authentication method in the same authentication rule.

5. Confirm the creation of the authentication rule by clicking on **OK**.
   The rule will be added to the authentication policy but will not be enabled by default.
6. In the authentication rule grid, double click on the status of the rule to enable it.

Status	Source	Methods (assess by order)	One-time password
Enabled	RDS-USERS@documentation.org RDS-2-SERVER RDS-1-SERVER	1 TS agent	N/A
Enabled	CITRIX-USERS@documentation.org CITRIX-2-SERVER CITRIX-1-SERVER	1 TS agent	N/A
Enabled	Any user@documentation.org in	1 LDAP	☐

During authentication, rules will be scanned in the order of their appearance in the list.
As such, you are advised to organize them using the **Up** and **Down** buttons when necessary.

Installing or updating SN TS Agent

Downloading SN TS Agent (*msi* package)

1. Log in to your MyStormshield personal area.
2. Go to **Downloads > Downloads**.
3. Select **Stormshield Network Security > TS agent** from the suggested categories.
4. Click on the TS Agent installation program (*msi* file). The download will begin automatically.
5. Enter one of the following commands to check the integrity of retrieved binary files:
   - Linux operating systems: *sha256sum < filename>*
   - Windows operating systems: *CertUtil -hashfile <filename> SHA256*

   Next, compare the result with the hash indicated in MyStormshield. To view it, click on **Show** in the **SHA256** column of the file in question.

Installing or manually updating SN TS agent on an RDS or Citrix server

Manually installing SN TS Agent

> **NOTE**
> The server must be restarted after SN TS Agent is installed to apply the new driver installed. You will be asked to restart when the installation of the agent is complete.

To install SN TS Agent on an RDS or Citrix server:

1. Open an administrator session on the server on which you wish to install SN TS Agent.
2. On this server, upload the SN TS Agent *.msi* installation file downloaded earlier.
3. Double-click on the *.msi* file to run the installation.
4. Click on **Run** then on **Next**.
5. Follow the steps in the installation program:

- In the **Account type** window, select the account used to run this service (**Local system account** or **Account dedicated to the service**).
- In the **Encryption key** window, enter and confirm the pre-shared key defined on the firewall for this TS Agent instance (see Creating TS agents in Configuring the TS Agent authentication method on the firewall).

> **NOTE**
> If the agent is being reinstalled, you can select the checkbox **Use existing configuration** to keep the pre-shared key and any custom values in settings from the previous version of SN TS Agent installed on the server.

- In the **Ready to install Stormshield TS Agent** window, select the checkbox **Restart now** if you wish to restart the server once SN TS Agent is installed.

IMPORTANT
If you have not chosen to restart the server immediately, remember to schedule it in order to use SN TS Agent.

Manually updating SN TS Agent

NOTE
The server must be restarted after SN TS Agent is updated to apply the new driver installed. You will be asked to restart when the installation of the agent is complete.

To update SN TS Agent on an RDS or Citrix server:

1. Open an administrator session on the server on which you wish to update SN TS Agent.
2. On this server, upload the *.msi* installation file of the new version of SN TS Agent.
3. Double-click on the *.msi* file to run the update.
4. Click on **Next**.
5. Follow the steps in the installation program:

- In the **Account type** window, select the account used to run this service (**Local system account** or **Account dedicated to the service**).
- In the **Encryption key** window, select the checkbox **Use existing configuration** to keep the pre-shared key and any custom values in settings from the version of SN TS Agent already installed on the server.
- In the **Ready to install Stormshield TS Agent** window, select the checkbox **Restart now** if you wish to restart the server once SN TS Agent is installed.

IMPORTANT
If you have not chosen to restart the server immediately, remember to schedule it in order to use SN TS Agent.

Installing SN TS agent on an RDS or Citrix server via a Microsoft GPO

Installing SN TS agent via a Microsoft GPO

NOTE
In a Microsoft Active Directory environment, SN TS Agent can be automatically deployed via a GPO (group policy object).

Copy the SN TS Agent installation program (*msi* file) in a shared folder that can be accessed by the Microsoft Active Directory domain controller and the RDS/Citrix servers.

Creating the *mst* package containing the arguments required for deploying SN TS Agent via a GPO

When deploying SN TS Agent, two operations must be performed:

- Specify the pre-shared key (PSK) required for communication between SN TS Agent and the SNS firewall,
- Restart the server when the installation of SN TS Agent is complete.

The agent can only be installed through an *mst* package, in which the two properties for these operations will be specified:

- PKEY_VALUE, specifying the pre-shared key ,
- REBOOT, set to "Force".

> **NOTE**
> A third-party solution must be used to define the *mst* package. The procedure described below uses the Microsoft *Orca* tool available in the components of the Microsoft Windows Installer software development kit (SDK).

On a machine equipped with the Microsoft *Orca* tool (administrator workstation, Microsoft Active Directory controller, etc.) and which can access the shared folder containing the SN TS Agent installation program (*msi* file):

1. Right-click on the SN TS Agent *msi* package and select **Edit with Orca**.
2. Click on **Transform** > **New transform** and select the TS Agent *msi* package.
3. Select the **Property** table.
4. Right-click and choose **Add Row**.
5. In the **Property** field, type *PKEY_VALUE*.
6. In the **Value** field in the *PKEY_VALUE* property, indicate the value of the pre-shared key.
7. Confirm by clicking on **OK**.
8. Repeat steps 4 to 7 with the following values:

- **Property**: *REBOOT*,
- **Value**: *Force*.

9. Click on **Transform** > **Generate Transform**.
10. Choose a name for the *mst* package (e.g., SN_TS_AGENT.mst) and save it in the same folder as the SN TS Agent *msi* installation package.
11. Close the *Orca* editor by clicking on **File** > **Exit**.

Creating the GPO to deploy SN TS Agent *msi* and *mst* packages

On the Microsoft Active Directory domain controller on which the GPO is to be created:

1. Run the server manager.
2. In the upper menu bar, click on **Tools,** then on **Group Policy Management**.
3. In the list on the left, right-click on the Microsoft Active Directory domain name and select **Create a GPO in this domain, and Link it here...**
4. Name the GPO and confirm by clicking on **OK** (e.g., *SN TS Agent*).
5. In the list on the left, right-click on the name of the GPO that you have just created, and select **Edit**.
   The GPO editing window opens.
6. In the menu to the left of the GPO, expand the menu **Computer Configuration** > **Policies** > **Software Settings**.
7. Right-click on **Software installation** and select **New** > **Package**. Select the SN TS Agent *msi* installation package.

8. Select **Advanced** mode and click on **OK**.
   The GPO editing window opens.
9. If you wish to do so, you can rename this installation instance (*e.g., Stormshield TS Agent 1.0.0*).
10. In the **Changes** tab, click on **Add...**, select the *mst* package created earlier (*SN_TS_AGENT.mst* in the example) and click on **Open**.
    The *mst* package selected is now associated with the SN TS Agent installation GPO.
11. Confirm by clicking on **OK**.

The TS Agent installation package is now ready to be deployed on machines in the Microsoft Active Directory domain.

The GPO will apply the next time the machines in question are restarted (RDS/Citrix servers).

Updating SN TS Agent via a Microsoft GPO

On the Microsoft Active Directory domain controller:

1. Run the server manager.
2. In the upper menu bar, click on **Tools,** then on **Group Policy Management**.
3. In the list on the left, right-click on the name of the GPO in question and select **Edit**.
   The GPO editing window opens.
4. In the menu to the left of the GPO, expand the menu **Computer Configuration** > **Policies** > **Software Settings**.
5. Right-click on **Software installation** and select **New** > **Package**. Select the new SN TS Agent *msi* installation package.
6. Select **Advanced** mode and click on **OK**.
   The GPO editing window opens.
7. If you wish to do so, you can rename this installation instance (*e.g., Stormshield TS Agent 1.0.2*).
8. In the **Changes** tab, click on **Add...**, select the *mst* package created earlier (*SN_TS_AGENT.mst* in the example) and click on **Open**.
   The *mst* package selected is now associated with the SN TS Agent update installation GPO.
9. In the **Upgrades** tab, the installation instance of the previous Stormshield TS Agent package (named *Stormshield TS Agent 1.0.0* in the example) is shown with the caption **Upgrade**. Select it and click on **Remove**. This property must be edited in order for SN TS Agent to be upgraded properly.
10. Click on **Add...**, select the update package, then select the option **Uninstall the existing package, then install the upgrade package**.
11. Click on **OK** to confirm.
    In the **Upgrades** tab, the Stormshield TS Agent 1.0.0 installation instance is now associated with the **Replace** operation.
12. Click on **OK** to confirm.

The TS Agent update package is now ready to be deployed on machines in the Microsoft Active Directory domain.

The GPO will apply the next time the machines in question are restarted (RDS/Citrix servers).

Identifying/editing SN TS Agent operating settings

Version 1.0 of SN TS Agent does not have a configuration interface: SN TS Agent operating settings can be looked up in the registry base of the server on which it is installed.

To look up/edit these settings:

1. Open an administrator session on the server on which SN TS Agent is installed.
2. Open the server's registry base.
3. Go to:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StormshieldRdsDrv\Parameters.

The settings of the TS Agent's driver are as follows:

Parameter	Description
ExhaustedPortAction	Action performed by the TS agent when no other ports are available for a new connection. The possible values are: • **Pass**: the connection is allowed and has been assigned a port from the range [EphemeralPortMin-EphemeralPortMax]. • **Block**: the connection has been blocked. • Default value: **Block**:
PortsPerRange	Number of ports included in each port range assigned to a user: • Minimum: 50, • Maximum: 1000, • Default value: 200.
RangePerUser	Number of port ranges assigned to a user: • Minimum: 1, • Maximum: 20, • Default value: 2.
ReservedSystemPorts	Ports included in the range [TotalPortsRangeLow-TotalPortsRangeHigh] that must be reserved for the operation of the system. These ports cannot be assigned to a user. They are strings in "aaaa-bbbb" format. Several strings can be defined. **EXAMPLE** • 1025-1025: to exclude port 1025, • 1025-1358: to exclude the port range [1025-1358].
TcpTimedWaitDelay	Time (in seconds) between the closure of a connection and when the associated port is available again: • Minimum: 30, • Maximum: 300, • Default value: 240.

TotalPortsRangeLow	Lower limit of the port range assigned to a user. • Minimum: 1024, • Default value: 1024.
TotalPortsRangeHigh	Higher limit of the port range assigned to a user. • Maximum: 49151, • Default value: 49151.
MaximumNumberRequests	Number of requests that can be processed simultaneously in the driver. This value must be adjusted according to the memory capacity on the server. • Minimum: 1, • Maximum: 65535, • Default value: 512. **NOTE** A value of 0 disables the limit on the number of simultaneous requests. You are strongly advised against disabling this limit, as it may cause overconsumption of memory on the RDS/Citrix server.

4. Go to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\stormshield-rds-service\Parameters.

The settings of the TS Agent service are as follows:

Parameter	Description
PSK	Pre-shared key for exchanges with the SNS firewall. This key is entered when SN TS Agent is installed. **NOTE** This registry key must be changed if the pre-shared key is changed on the SNS firewall.
EphemeralPortMin	Lower limit of the range of additional ports that can be assigned to a user when the **ExhaustedPortAction** setting is set to **pass**: • Minimum: 49152, • Maximum: 65535, • Default value: 49152.
EphemeralPortMax	Higher limit of the range of additional ports that can be assigned to a user when the **ExhaustedPortAction** setting is set to **pass**: • Minimum: 49152, • Maximum: 65535, • Default value: 65535.

LogLevel	Log verbosity for communications between the agent and the firewall. These logs can be looked up in the event viewer of the server on which the agent is installed: • Minimum: 1 (errors only), • Maximum: 3 (errors, information and debug). • Default value: 2 (errors and information).
ServerPort	Communication port with the SNS firewall. This port is TCP/1303 by default and corresponds to the predefined network object *agent_ts* on the SNS firewall. **NOTE** This registry key must be changed if the connection port declared on the SNS firewall is different from the object *agent_ts* (TCP/1303).
SNS Timeout	Duration in seconds before the TS Agent considers the firewall unreachable. Once this duration expires, the TS Agent ends the communication with the firewall. It will then save all information regarding authenticated users and forwards it to the firewall when it manages to restore the connection with the TS Agent. The possible values are: • Minimum: 0, • Maximum: 60, • Default value: 2.

NOTE
If any changes are made to these registry keys, the server must be restarted to apply the changes.

Enabling TS Agents and configuring the filter policy

Enabling TS Agents

On the firewall, go to **Configuration** > **Users** > **Authentication**> **Available methods** tab:

1. In the **TS agent list** found on the right side of the screen, double-click on the status of every TS agent that you wish to enable, to change it from *off* to *on*.
2. Click on **Apply** to apply the change to the configuration.

Creating filter rules

You must create rules so that users authenticated via the TS Agent method can access the various resources allowed. These rules can apply to user groups or individual users.

It is also important to prepare "exception" rules allowing RDS/Citrix servers to access security updates (Microsoft Windows and antivirus updates, for example) without the need for prior authentication.

A set of rules meeting these criteria may look like this:

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
Access to security update resources for RDS and Citrix servers without authentication (contains 1 rules, from 1 to 1)							
	on	pass	RDS-1-SERVER RDS-2-SERVER CITRIX-1-SERVER CITRIX-2-SERVER	Any Web services and IP reputations Microsoft public IPs windowsupdate Microsoft Azure	http https		IPS
Access to production server for groups of users authentified by TS Agent (contains 2 rules, from 2 to 3)							
	on	pass	RDS-USERS	ERP-SERVER	http https		IPS
	on	pass	CITRIX-USERS	ERP-SERVER	http https		IPS
Access to production server for unique user authentified by TS Agent (contains 1 rules, from 4 to 4)							
	on	pass	john.doe	ERP-SERVER	http https		IPS
Access to Internet for unique user authentified by TS Agent (contains 2 rules, from 5 to 6)							
	on	pass	john.doe	Internet	https		IPS

Creating an exception rule regarding server updates

In the module **Configuration > Security policy > Filter - NAT**:

1. Select the security policy to modify.
2. Go the rule under which you want to create a new filter rule.
   You can move this rule later using the arrows found in the action bar.
3. Click on **New rule** and select **Single rule**.
4. Double-click in the **Action** column in this new rule.
   The editing window of the rule opens.
5. Click on the **General** menu on the left.
6. In the **Status** field, set the value to *On*.
   You can add a comment if you wish.
7. Click on the **Action** menu on the left.
8. In the **General** tab, select *pass* for the **Action** field.
9. Click on the **Source** menu on the left.

10. In the **General** tab, in the **Source hosts** field, select the servers or server groups allowed to access security update services (the servers *RDS-1-SERVER*, *RDS-2-SERVER*, *CITRIX-1-SERVER* and *CITRIX-2-SERVER* in this example).
11. Click on the **Destination** menu on the left.
12. In the **General** tab, in the **Web services and IP reputations** field, select the objects *Microsoft public IPs*, *Windows update* and *Microsoft Azure*.
13. Click on the **Port - Protocol** menu on the left.
14. In the **Destination port** field, select the *http* and *https* objects.
15. Confirm the creation of the filter rule by clicking on **OK**.

Creating a rule applying to a user group or individual user authenticated via the TS Agent method

In the module **Configuration > Security policy > Filter - NAT**:

1. Select the security policy to modify.
2. Go the rule under which you want to create a new filter rule.
   You can move this rule later using the arrows found in the action bar.
3. Click on **New rule** and select **Single rule**.
4. Double-click in the **Action** column in this new rule.
   The editing window of the rule opens.
5. Click on the **General** menu on the left.
6. In the **Status** field, set the value to *On*.
   You can add a comment if you wish.
7. Click on the **Action** menu on the left.
8. In the **General** tab, select *pass* for the **Action** field.
9. Click on the **Source** menu on the left.
10. In the **General** tab, in the **User** field, select the user or user group authenticated via the TS Agent method (user group *RDS-USERS@documentation.org* or CITRIX-USERS@documentation.org or individual user john.doe@documentation.org in this example).

> **NOTE**
> A single user or a single user group can be selected in such rules.
> In this case, you must create as many rules as the number of user groups or individual users authenticated via the TS Agent method, and allowed to access the same resources.

11. Click on the **Destination** menu on the left.
12. In the **General** tab, in the **Destination hosts** field, select the hosts that will be accessible to users authenticated via the TS Agent method (host *ERP-SERVER* in this example).
13. Click on the **Port - Protocol** menu on the left.
14. In the **Destination port** field, select the objects corresponding to the ports to be allowed (objects *http* and *https* in this example).
15. Confirm the creation of the filter rule by clicking on **OK**.

Repeat the process to create the other filter rules that will apply to users authenticated via the TS Agent method.

When a firewall is placed between users that must authenticate via the TS Agent and RDS/Citrix servers

In this case, you must create a rule on this firewall to allow the networks of the users in question to reach:

- RDS servers on port TCP/3389 (object *microsoft-ts* on an SNS firewall),
- Citrix servers on port 1494 corresponding to the Citrix ICA protocol (object *citrix* on an SNS firewall).

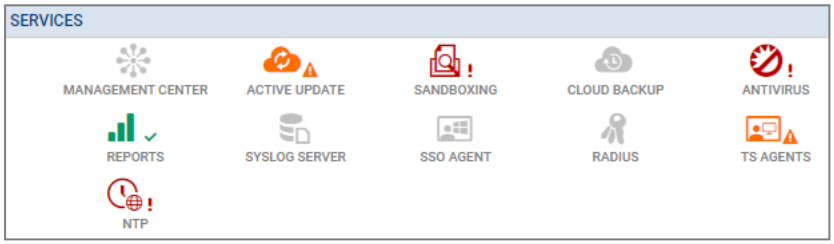
Monitoring authentication and TS Agents on the firewall

Various events can be viewed in the firewall's web administration interface.

Monitoring agent status

Monitoring dashboard

Agents' statuses can be viewed in the **Monitoring** tab > **Dashboard** > **Services** widget:



Depending on the status of TS Agents, the colors and symbols of the icons change:

- **Gray** icon without a symbol: all TS Agents configured on the firewall are inactive.
- Green icon and ✔ symbol: communication with all configured active TS Agents is optimal.
- Orange icon and ⚠ symbol: communication with at least one of the configured active TS Agents has encountered an issue. Scrolling over the icon will show a tooltip that explains the reason for this status.
- Red icon and ! symbol: communication with all TS Agents has been disconnected. Scrolling over the icon will show a tooltip that explains the reason for this status.

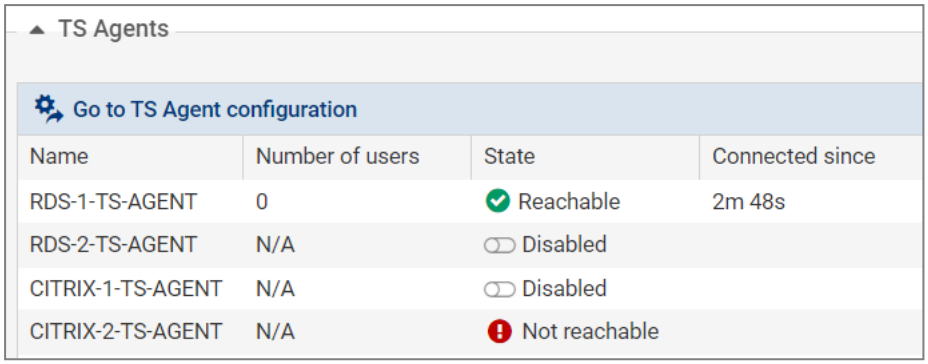
Double-clicking on the TS Agents icon will redirect you to the TS Agents widget in the System monitoring module.

System monitoring

Details on the status of each TS Agent can also be viewed via the **Monitoring** tab > **System monitoring** module > **TS Agents** widget.

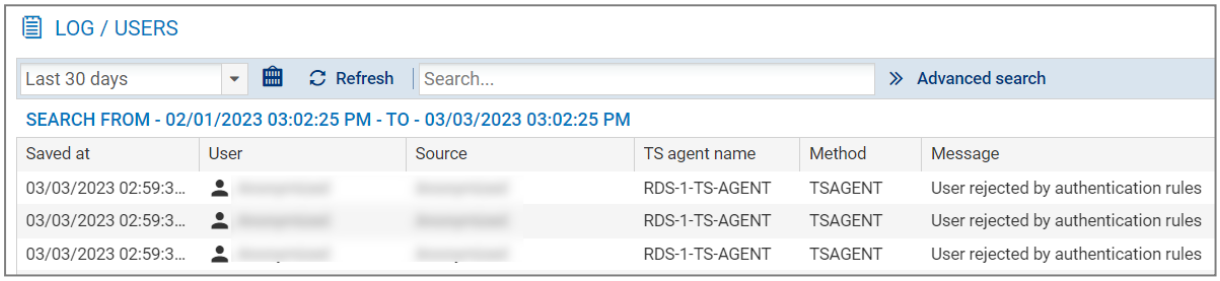
This grid presents the following information for each TS agent configured on the firewall. including agents that have not been enabled:

- The name of the TS Agent,
- The number of users connected via this TS Agent,
- The status of the TS Agent (**Reachable**, **Unreachable** or **Disabled**),
- Time lapsed since the connection between the firewall and the TS Agent.



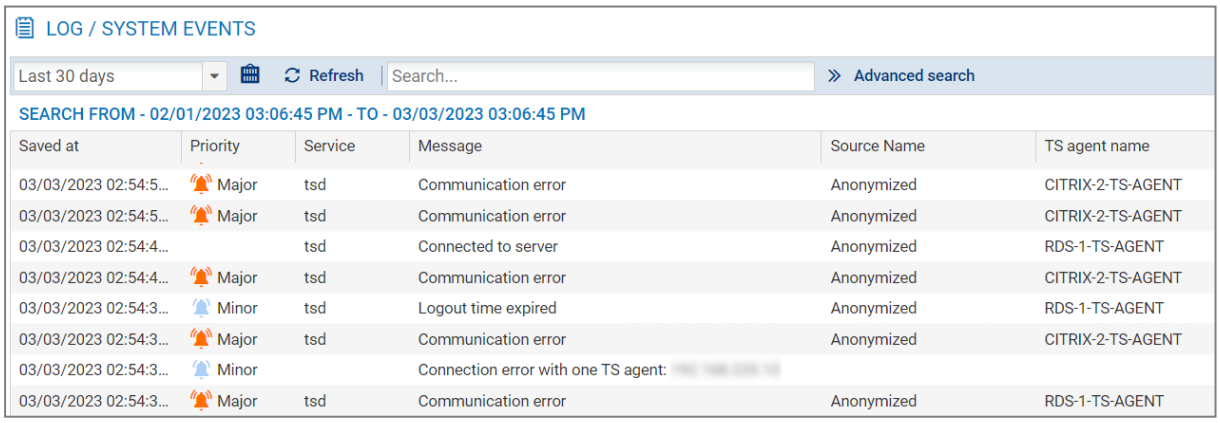
Viewing authentication logs

Look up successful or unsuccessful authentications in **Monitoring > Audit logs > Users**:



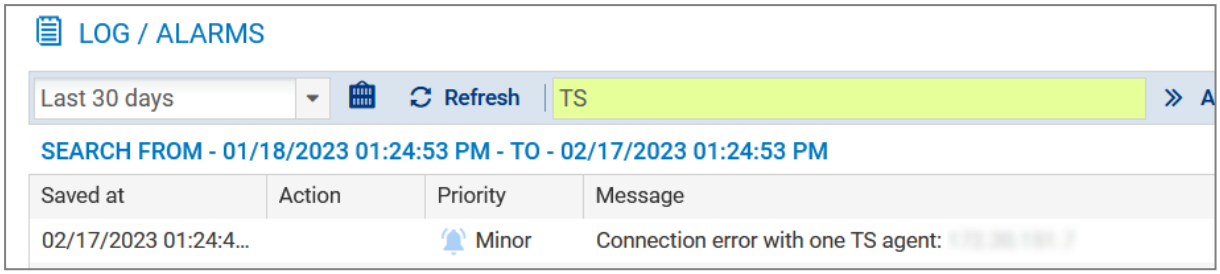
Viewing system logs

Look up events regarding communication between the firewall (TSD service) and TS Agents in **Monitoring > Audit logs > System events**:



Viewing alarms

Look up events regarding communication between the firewall and TS Agents in **Monitoring > Audit logs > Alarms**:


LOG / ALARMS
Last 30 days
Refresh
TS
SEARCH FROM - 01/18/2023 01:24:53 PM - TO - 02/17/2023 01:24:53 PM
Saved at
Action
Priority
Message
02/17/2023 01:24:4...
Minor
Connection error with one TS agent:

Monitoring the TS Agent on the server

Changing the TS Agent's log level on the RDS/Citrix server

If necessary, on the server on which the TS Agent is deployed:

1. Open the server's registry base.
2. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\stormshield-rds-service\Parameters.
3. Change the value of the **LogLevel** key and confirm by clicking on **OK**.
4. Restart the server (recommended) or, only if no users are connected to the server, restart the *stormshield-rds-service* service from the **Microsoft Server Manager**.

Viewing the TS Agent's logs on the RDS/Citrix server

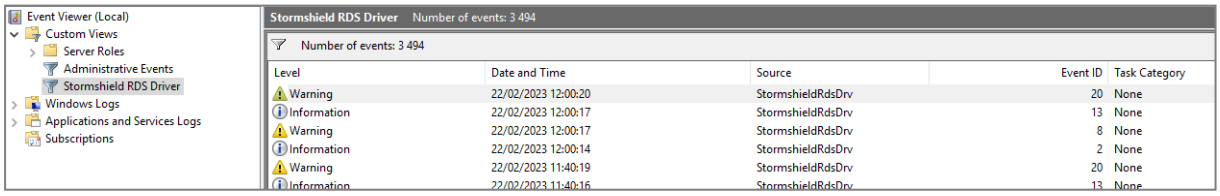
On the server on which the TS Agent is deployed:

1. Open the **Event Viewer**.
2. In the **Applications and services logs** menu, select **Stormshield RDS Service**.
The list of events that occurred for the Stormshield RDS Service appears.

Viewing the logs of the RDS agent's driver

On the server on which the TS Agent is deployed:

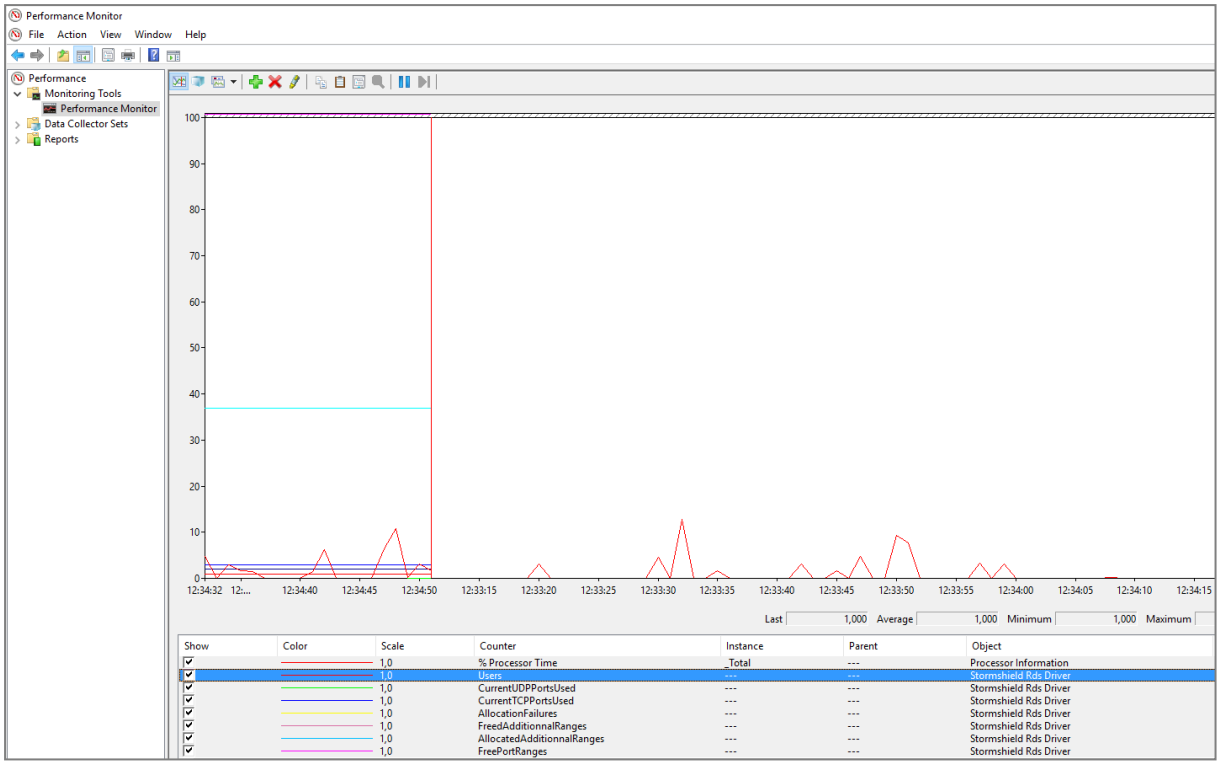
1. Open the **Event Viewer**.
2. Right-click on the **Custom views** and select **Create a custom view**.
3. Select **By source**.
4. In the **Source** list, select **StormshieldRdsDrv** and click on **OK**.
5. Name your filter (e.g., *Stormshield RDS Driver*) and click on **OK**.
This new view is added to the list of **Custom views**.



Viewing the performance of the TS Agent's driver in the Windows performance monitor

On the server on which the TS Agent is deployed:

1. Open the **Performance Monitor**.
2. Click on **Monitoring tools** > **Performance Monitor**.
3. Click on the green cross in the window on the right.
4. In the list of **Counters**, select **Stormshield Rds Driver**.
5. Click on **Add** and confirm by clicking on **OK**.


Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
Reports
100
90
80
70
60
50
40
30
20
10
0
12:34:32 12:...
12:34:40
12:34:45
12:34:50
12:33:15
12:33:20
12:33:25
12:33:30
12:33:35
12:33:40
12:33:45
12:33:50
12:33:55
12:34:00
12:34:05
12:34:10
12:34:15
Last 1,000 Average 1,000 Minimum 1,000 Maximum
Show Color Scale Counter Instance Parent Object
1,0 % Processor Time _Total --- Processor Information
1,0 Users --- --- Stormshield Rds Driver
1,0 CurrentUDPPortsUsed --- --- Stormshield Rds Driver
1,0 CurrentTCPPortsUsed --- --- Stormshield Rds Driver
1,0 AllocationFailures --- --- Stormshield Rds Driver
1,0 FreedAdditionnalRanges --- --- Stormshield Rds Driver
1,0 AllocatedAdditionnalRanges --- --- Stormshield Rds Driver
1,0 FreePortRanges --- --- Stormshield Rds Driver

Diagnosing and troubleshooting the most frequently encountered issues

Identifying ports assigned to a user

From the web administration interface

In **Monitoring > Monitoring > Users**, scrolling over the line corresponding to a user connected via the TS agent method will show a tool tip with the ports assigned to this user.

From the firewall's console

The command `sfctl -s user -H name=<username> -v` lists the ports assigned by the TS Agent to a particular user.

EXAMPLE

```
VMSNSX01B2085A9&gt;sfctl -s user -H name=john.doe -v
User (ASQ):
username            domain              addr                      ports       timeout cookhash    authmethod  flags
john.doe            documentation.org   fe80::dd80:7fa:4148:c2ae  1424-1623   85870   0           TSAGENT     (0x0000)
Memberof: TS-USERS
john.doe            documentation.org   TS-SERVER-1               1424-1623   85870   0           TSAGENT     (0x0000)
Memberof: TS-USERS
```

The Microsoft Active Directory server sends the TS Agent the NetBIOS name on the domain instead of the FQDN

The Microsoft Active Directory server may sometimes send the TS Agent the NetBIOS name on the domain instead of the FQDN (e.g., MYDOMAIN instead of mydomain.org).

To allow the firewall to associate the reference Active Directory, it is possible to link the NetBIOS name to the FQDN on the domain using the CLI/Serverd command sequence:

```
CONFIG AUTH NETBIOS FQDN ADD NETBIOS=<netbiosname> FQDN=<fqdn>
CONFIG AUTH ACTIVATE.
```

EXAMPLE

```
CONFIG AUTH NETBIOS FQDN ADD NETBIOS=documentation
FQDN=documentation.org
CONFIG AUTH ACTIVATE
```

NOTE

Up to 5 NETBIOS/FQDN links can be declared on the same firewall.

More information about the command **CONFIG AUTH NETBIOS FQDN**.

Further reading

Additional information and answers to questions you may have relating to the TS Agent are available in the Stormshield knowledge base (authentication required).

STORMSHIELD

documentation@stormshield.eu