TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

INSTALLING AND DEPLOYING THE TS AGENT

Product concerned: SNS 4.7 and higher versions, SN TS Agent 1.0

Document last updated: March 18, 2025

Reference: sns-en-SN_TS_Agent_installation_and_deployment_technical_note

Table of contents

Change log

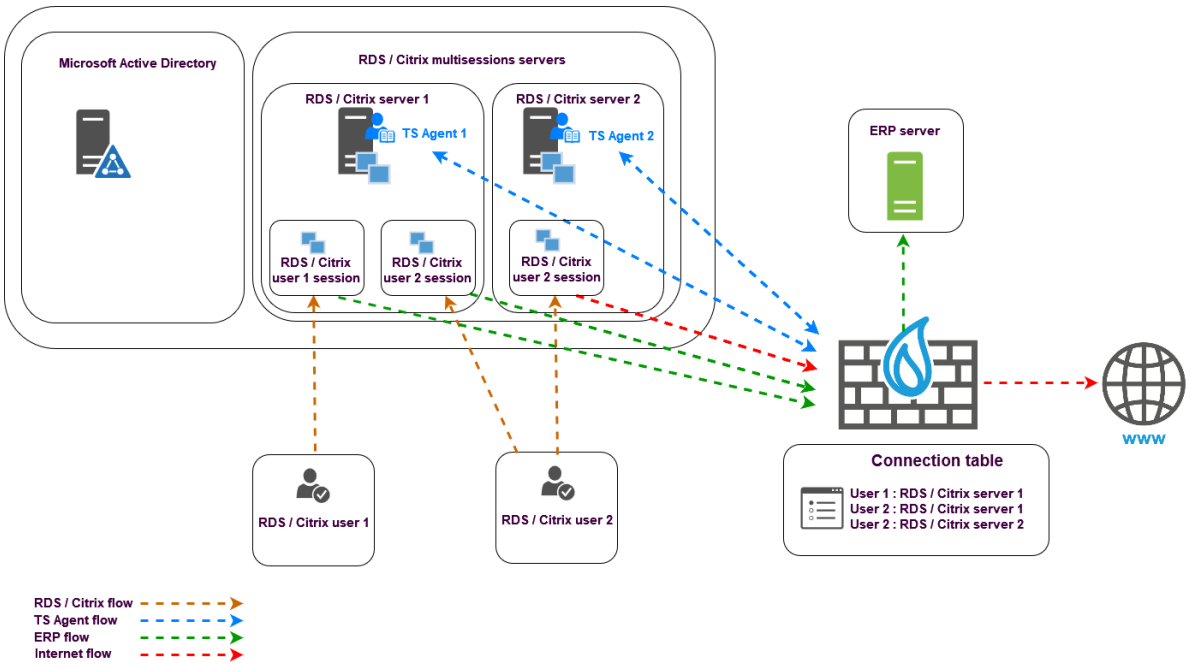
Date	Description
March 18, 2025	• Addition of three limitations and explanations on usage in the section "Specifications and limitations" • Addition of explanations regarding the selection of the port and pre-shared key in the section "Configuring the TS Agent authentication method on the firewall > Creating TS Agents" • Content relating to the installation and update of the TS Agent now has its own separate section in the document • Addition of the procedure for updating the TS Agent from a 1.0.3 or lower version in the section "Updating the TS Agent" • Changes to procedures to install and manually update the TS Agent with regard to restarting the server and the configuration of ports that are reserved for system operations in the section "Installing or updating the TS Agent" • Addition of the **ReservedPortAction** parameter, and changes to the description of the parameters **ExhaustedPortAction**, **PortsPerRange**, **RangePerUser**, **ReservedSystemPorts**, **TcpTimedWaitDelay**, **TotalPortsRangeLow**, **TotalPortsRangeHigh**, **EphemeralPortMin** and **EphemeralPortMax** in the section "Identifying/editing TS Agent operating settings" • Content relating to the monitoring of users who have connected through TS Agents now has its own separate section in the document • Changes to the procedure for looking up the TS Agent's driver logs in the section "Monitoring the TS Agent on the RDS/Citrix server" • Addition of the scenario in which the RDS/Citrix server restarts while users are connected in the "Troubleshooting" section • Addition of the appendix "Using script to configure ports that are reserved for system operations"
October 30, 2023	• New document

Getting started

The 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 that the TS Agent assigns.



NOTE

In this document:

- Citrix Virtual Apps and Desktops servers are referred to as "Citrix servers",
- Microsoft Remote Desktop Services servers are referred to as "RDS servers",
- SN TS Agent is now "TS Agent".

Click on the links below for more information on:

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

Specifications and limitations

Compatibility

For more information, refer to section TS Agent in the *Network Security & Tools Product Life Cycle guide*.

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 (2 by default)
Number of ports per range	50 to 1000 (200 by default)

Limitations and explanations on usage

Port (PAT) or address (NAT) translation

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.

Receiving a domain name in NETBIOS format

When the TS Agent receives a domain name in NetBIOS format, you must map this name to the Active Directory domain name in FQDN format. For more information, please refer to the section Troubleshooting.

TS Agent operating parameters

The TS Agent's operating parameters (listening port, port range, pre-shared key, etc.) can be looked up in the registry base of the server on which it is installed. For further information, refer to the section Identifying/editing TS Agent operating settings,

Disconnecting users who were authenticated via the TS Agent

Users authenticated via the TS Agent cannot be disconnected via the pop-up menu in user monitoring.
A user can be forced to disconnect only 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.

Prohibited characters in LDAP directory user IDs

```
" <tab> & ~ | = * < > ! ( ) \ $ % ? ' ` <space>
```

IMPORTANT
In external directories such as Microsoft Active Directory, user IDs must comply with the above criteria **as well as** the criteria imposed by Microsoft.

Configuring the TS Agent authentication method on the SNS firewall

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

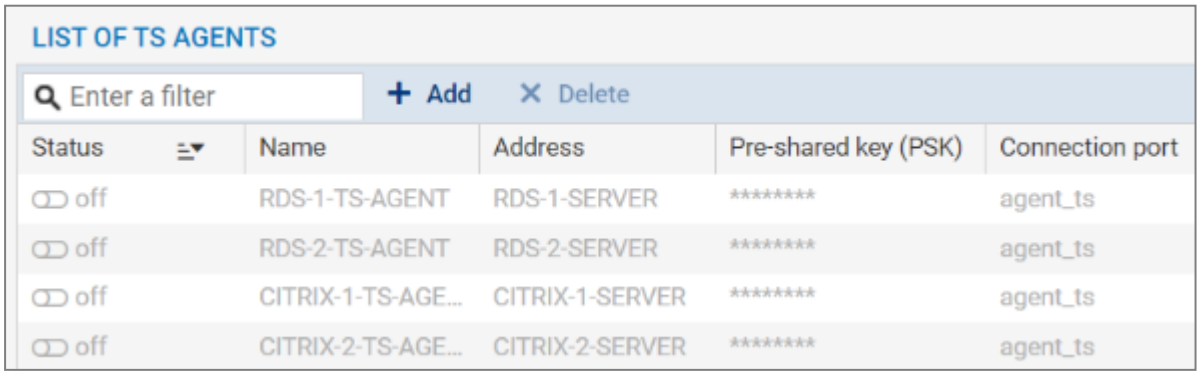
The TS Agent method appears directly in the list of enabled authentication methods to the left of the screen. Click on the TS Agent method to view its details.

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. The object *agent_ts* (TCP/1303) is suggested by default in the **Port** field. This port is also entered in the TS Agent's default configuration.
   You can select or create another object corresponding to the dialogue port between the firewall and the TS Agent. You will then need to edit the corresponding **ServerPort** parameter on the TS Agent to enter the new selected port (see the section Identifying/editing TS Agent operating settings).
6. Enter and confirm the **Pre-shared key** used during the exchanges between the Firewall and the TS Agent. It must meet the minimum entropy set on the firewall (**Configuration** > **General configuration** tab, **Password policy** section). This key can be changed later.
   You will also need to enter this key in the settings of the TS Agent in question:
   - Either during its installation (see the section Installing or updating the TS Agent),
   - Or after editing the **PSK** parameter (see the section Identifying/editing 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).



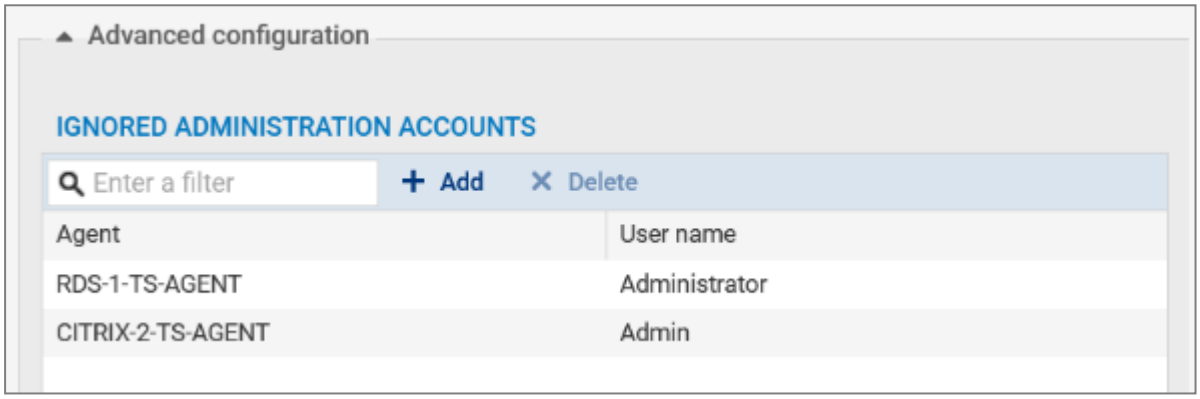
Excluding administration accounts (optional)

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 that is 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., RDS-1-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 the TS Agent

This section explains how to install or update the TS Agent, either manually or through a Microsoft GPO.

Downloading the TS Agent installation program (*MSI* package)

Start by downloading the TS Agent installation program (*MSI* package).

1. Log in to your MyStormshield 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 the TS Agent

This section explains how to install the TS Agent, either manually or through a Microsoft GPO.

Installing the TS Agent manually

1. Open an administrator session on the server on which the TS Agent will be installed.
2. Upload the *.msi* installation file that was downloaded earlier.
3. Double-click on the file to run the installation.
4. Click on **Run** then on **Next**.
5. 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**).
6. 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).

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

7. In the **Ready to install Stormshield TS Agent** window, click on **Install**.
8. The server has to be restarted to finalize the installation of the TS Agent. If you do not restart the server immediately, remember to schedule it in order to use the TS Agent.

> **NOTE**
> Before restarting the server, you can run a script, which analyzes any ports that may be in conflict with the TS Agent, and which adds them to its settings to reserve them for system

operations. As such, these ports cannot be assigned to any user. This script can be used later, but the server will need to be restarted again. For further information, refer to the section Appendix: Using script to configure ports that are reserved for system operations

Installing the TS Agent through a Microsoft GPO

In a Microsoft Active Directory environment, the TS Agent can be automatically deployed through a GPO (Group Policy Objects). This deployment is a two-step process.

Creating an *MST* package containing the arguments required for deploying the TS Agent

An *MST* package must first be created to include the following arguments required for deploying the TS Agent:

- *PKEY_VALUE*, which specifies the pre-shared key (PSK) required for communication between the TS Agent the and the firewall,
- *REBOOT*, set to *Force* to restart the server at the end of the installation.

A third-party tool has to be used to create 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).

1. Copy the TS Agent installation program (*.msi* file) downloaded earlier in a shared folder that can be accessed by the Microsoft Active Directory domain controller and the RDS/Citrix servers.
2. On a machine equipped with the Microsoft *Orca* tool (administrator workstation, Microsoft Active Directory controller, etc.) and which can access the shared folder, right-click on the TS Agent's *MSI* package, and select **Edit with Orca**.
3. Click on **Transform** > **New transform** and select the TS Agent's *msi* package.
4. Select the **Property** table.
5. To specify the pre-shared key required for communication between the TS Agent and the SNS firewall:
   1. Right-click and choose **Add Row**.
   2. In the **Property** field, enter *PKEY_VALUE*.
   3. In the **Value** field, indicate the value of the pre-shared key.
   4. Click on **OK**.
6. To restart the server when the installation of the TS Agent is complete:
   1. Right-click and choose **Add Row**.
   2. In the **Property** field, enter *REBOOT*.
   3. In the **Value** field, enter *Force*.
   4. Click on **OK**.
7. Click on **Transform** > **Generate Transform**.
8. Choose a name for the *MST* package and save it in the same folder as the TS Agent *MSI* installation package.
9. Close the *Orca* editor by clicking on **File** > **Exit**.

Creating the GPO to deploy the TS Agent *MSI* and *MST* packages

As soon as the *MST* package is created, you can create the GPO to deploy the 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., *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 TS Agent *MSI* installation package.
8. Select **Advanced** mode and click on **OK**.
   The GPO editing window opens.
9. Rename this installation instance if necessary, by adding the TS Agent version number, for example.
10. In the **Changes** tab, click on **Add**. , select the *MST* package that was created earlier and click on **Open**. The *MST* package selected is now associated with the 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 the TS Agent

This section explains how to update the TS Agent, either manually or through a Microsoft GPO.

Updating the TS Agent from version 1.0.3 or lower

Before updating the TS Agent to version 1.0.5 or higher, you need to fully uninstall 1.0.3 or other lower versions with a script provided by Stormshield.

IMPORTANT
Even if you have used the TS Agent uninstall program in version 1.0.3 or lower, you must follow this procedure to fully uninstall the version.

1. In your MyStormshield personal area, go to **Downloads > Downloads.**
2. Select **Stormshield Network Security > TS Agent** from the suggested categories.
3. Click on the uninstall script (*.ps1* file) to download it.
4. Copy the script on each RDS or Citrix server on which a TS Agent has been installed.
5. Run the script as an administrator.
6. When the script is being executed, errors may appear if files from the previous installation have already been deleted.

Updating the TS Agent manually

1. Open an administrator session on the server on which the TS Agent will be updated.
2. Upload the *.msi* installation file of the new version that was downloaded earlier.
3. Double-click on this file to run the update.
4. Click on **Next**.
5. 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**).
6. 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 TS Agent that is already installed on the server.
7. In the **Ready to install Stormshield TS Agent** window, click on **Install**.
8. The server has to be restarted to finalize the installation of the new TS Agent version. If you do not restart the server immediately, remember to schedule it in order to apply the new driver that was installed.

NOTE
Before restarting the server, you can run a script, which analyzes any ports that may be in conflict with the TS Agent, and which adds them to its settings to reserve them for system operations. As such, these ports cannot be assigned to any user. This script can be used later, but the server will need to be restarted again. For further information, refer to the section Appendix: Using script to configure ports that are reserved for system operations

Updating the TS Agent through a Microsoft GPO

In a Microsoft Active Directory environment, the TS Agent update can be automatically deployed through a GPO (Group Policy Objects). This deployment is a two-step process.

Creating an *MST* package containing the arguments required for deploying the new version of the TS Agent

An *MST* package must first be created to include the following arguments required for deploying the new version of the TS Agent:

- *PKEY_VALUE*, which specifies the pre-shared key (PSK) required for communication between the TS Agent the and the firewall,
- *REBOOT*, set to *Force* to restart the server at the end of the installation.

A third-party tool has to be used to create 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).

1. Copy the 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.
2. On a machine equipped with the Microsoft *Orca* tool (administrator workstation, Microsoft Active Directory controller, etc.) and which can access the shared folder, right-click on the TS Agent's *MSI* package, and select **Edit with Orca**.
3. Click on **Transform** > **New transform** and select the TS Agent's *msi* package.
4. Select the **Property** table.

5. To specify the pre-shared key required for communication between the TS Agent and the SNS firewall:
   1. Right-click and choose **Add Row**.
   2. In the **Property** field, enter *PKEY_VALUE*.
   3. In the **Value** field, indicate the value of the pre-shared key.
   4. Click on **OK**.
6. To restart the server when the installation of the TS Agent is complete:
   1. Right-click and choose **Add Row**.
   2. In the **Property** field, enter *REBOOT*.
   3. In the **Value** field, enter *Force*.
   4. Click on **OK**.
7. Click on **Transform** > **Generate Transform**.
8. Choose a name for the *MST* package and save it in the same folder as the TS Agent *MSI* installation package.
9. Close the *Orca* editor by clicking on **File** > **Exit**.

Editing the GPO to deploy TS Agent *MSI* and *MST* packages

As soon as the *MST* package is created, you can edit the GPO to deploy TS Agent *MSI* and *MST* packages.

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 TS Agent *MSI* installation package.
6. Select **Advanced** mode and click on **OK**.
   The GPO editing window opens.
7. Rename this installation instance if necessary, by adding the TS Agent version number, for example.
8. In the **Changes** tab, click on **Add...**, select the *mst* package that was created earlier and click on **Open**. The selected *MST* package is now associated with the TS Agent's update installation GPO.
9. In the **Upgrades** tab, the installation instance of the previous TS Agent package is shown with the caption **Upgrade**. Select it and click on **Remove**. This property must be edited in order for the 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. Confirm by clicking on **OK**.
    In the **Upgrades** tab, the installation instance of the previous TS Agent package is now associated with the **Replace** operation.
12. Confirm by clicking on **OK**.

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 TS Agent operating settings

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

To look up/edit these TS Agent settings:

1. Open an administrator session on the server on which the TS Agent is installed.
2. Open the server's registry base (*regedit*).

In the registry base, you will find the TS Agent driver settings, and the TS Agent service settings. These settings have different locations.

TS Agent driver settings

IMPORTANT
If any changes are made to registry keys on the TS Agent's driver, the server must be restarted to apply the changes.

Location in the registry base:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StormshieldRdsDrv\Parameters

Parameter	Description/Prescribed values
ExhaustedPortAction	Action that the TS Agent applies when users no longer have any available ports in their port ranges for new connections. • **pass** (by default): the TS Agent accepts the connection, and a port from the range [**EphemeralPortMin-EphemeralPortMax**] is assigned to the user. These connections are anonymous to the firewall. Its filter policy must allow anonymous network connections with source ports that are higher than or equal to the value of the **EphemeralPortMin** parameter. Otherwise, the firewall will block such connections. • **block**: the TS Agent blocks the connection.
ReservedPortAction	Action that the TS Agent applies when an application attempts to use a port from the port range that is reserved for users [**TotalPortsRangeLow-TotalPortsRangeHigh**]. • **block** (by default): the TS Agent blocks the connection, unless this port is in the port ranges that have been assigned to the user in question. If a connection is blocked, an event will be generated in the Windows **Event Viewer**: Process [...] has been blocked because it tried to use a port [...] which is reserved by the driver. • **pass**: the TS Agent accepts the connection. Changing this parameter to "*pass*" is considered advanced configuration, as this may cause issues with the assignment of ports on the host.

Parameter	Description/Prescribed values
PortsPerRange	Number of ports included in each port range assigned to each user (200 by default). • Minimum: 50, • Maximum: 1000. If the default value is unsuitable, for example, if some applications require a large number of ports in order to function, you can change the value. This will ensure that users will not run out of available ports, but reduces the maximum number of users on the TS Agent.
RangePerUser	Number of port ranges assigned to a user (2 by default). • Minimum: 1, • Maximum: 20. If the default value is unsuitable, for example, if some applications require a large number of ports in order to function, you can change the value. This will ensure that users will not run out of available ports, but reduces the maximum number of users on the TS Agent.
ReservedSystemPorts	List of ports included in the range [**TotalPortsRangeLow-TotalPortsRangeHigh**] that must be reserved for the operation of the system. These ports cannot be assigned to any user. Several strings can be defined, by following the "[aaaaa-bbbbb]" format. For example: • To reserve port 20025: [20025-20025] • To reserve the port range [20025-20358]: [20025-20358] The following ports are reserved by default: [1303-1303] [3389-3389] [5353-5353] [5355-5355] You can run a script that analyzes any ports that may be in conflict with the TS Agent, and which adds them to this setting. For further information, refer to the section Appendix: Using script to configure ports that are reserved for system operations **NOTE** When a port is added to this list, the entire port range (**PortsPerRange** setting) that contains this port will be reserved.
TcpTimedWaitDelay	Time in seconds between the closure of a connection and when the associated port is available again (120 by default). • Minimum: 30, • Maximum: 300. The value must match the one used by the Windows server under the registry key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip** (120 by default). Ensure that you use the same value for both parameters.

Parameter	Description/Prescribed values
TotalPortsRangeLow	Lower limit of the port range that is reserved for users (20000 by default). • Minimum: 1024. If you bring down this value, ensure that the ports in the new range are not being used by other applications. You can reserve ports for the operation of the system with the parameter **ReservedSystemPorts**.
TotalPortsRangeHigh	Higher limit of the port range that is reserved for users (49151 by default). • Maximum: 65535. If you raise this value, ensure that no dynamic Windows port ranges overlap the new port range that is reserved for users. Use the following command to check whether this is the case: `netsh int <ipv4|ipv6> show dynamicport <tcp|udp>` **NOTE** The TS Agent's driver manages only one port range.
MaximumNumberRequests	Number of requests that can be processed simultaneously by the driver (512 by default). Adjust this value according to the memory capacity on the server. • Minimum: 1, • Maximum: 65535. 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.

TS Agent service settings

IMPORTANT
If any changes are made to registry keys on the TS Agent's service, the "*Stormshield-rds-service*" service has to be restarted to apply the changes.

Location in the registry base:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\stormshield-rds-service\Parameters

Parameter	Description
PSK	Pre-shared key for exchanges with the firewall. This key is entered when the TS Agent is installed. **NOTE** Edit this value if the pre-shared key is changed on the firewall.

Parameter	Description
EphemeralPortMin	Lower limit of the range of additional ports that can be assigned to users (49152 by default). This limit is used when users no longer have any available ports in their port ranges (**ExhaustedPortAction** parameter set to "*pass*"). • Minimum: 1, • Maximum: 65535. If you edit this value, ensure that the port range [**EphemeralPortMin-EphemeralPortMax**] covers all dynamic Windows port ranges. Use the following command to check whether this is the case: `netsh int <ipv4|ipv6> show dynamicport <tcp|udp>` **NOTE** The TS Agent's service sends only one port range to the driver.
EphemeralPortMax	Higher limit of the range of additional ports that can be assigned to users (65535 by default). This limit is used when users no longer have any available ports in their port ranges (**ExhaustedPortAction** parameter set to "*pass*"). • Minimum: 1, • Maximum: 65535. If you edit this value, ensure that the port range [**EphemeralPortMin-EphemeralPortMax**] covers all dynamic Windows port ranges. Use the following command to check whether this is the case: `netsh int <ipv4|ipv6> show dynamicport <tcp|udp>` **NOTE** The TS Agent's service sends only one port range to the driver.
LogLevel	Log level *(verbose)* for communications between the TS Agent and the firewall. These logs can be looked up in the Windows **Event Viewer** of the server on which the TS Agent is installed. • Level 1: errors only, • Level 2: errors and information (by default), • Level 3: errors, information and debug.
ServerPort	Communication port with the firewall (TCP/1303 by default). The default port corresponds to the predefined network object *agent_ts* on the firewall. **NOTE** Edit this value if the connection port declared on the firewall is different from the object *agent_ts* (TCP/1303).
SNS Timeout	Waiting time in seconds before the TS Agent considers the firewall unreachable (2 by default). 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. • Minimum: 0, • Maximum: 60.

Enabling TS Agents and configuring the filter policy

This section explains how to enable TS Agents and configure the filter policy on the SNS firewall.

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

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**.

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.

Rule 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:

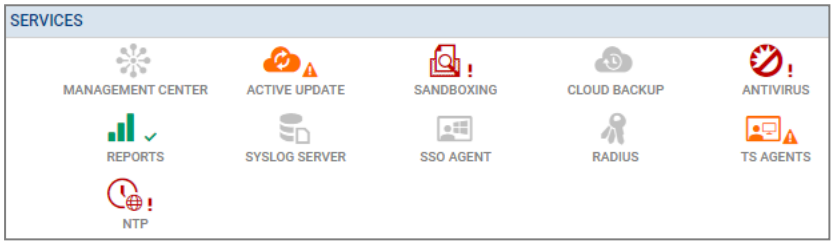
- RDS servers on port TCP/3389 (object *microsoft-ts* on an SNS firewall),
- Citrix servers on port 1494 corresponding to the Citrix ICA protocol (object *citrix* on an SNS firewall).

Monitoring the status of communications between TS Agents and the SNS firewall

Various events can be viewed in the firewall's web administration interface, to monitor the status of communications between TS Agents and the SNS firewall.

From the Dashboard module

TS Agents' statuses can be viewed in the **Monitoring** tab > **Dashboard** module > **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.

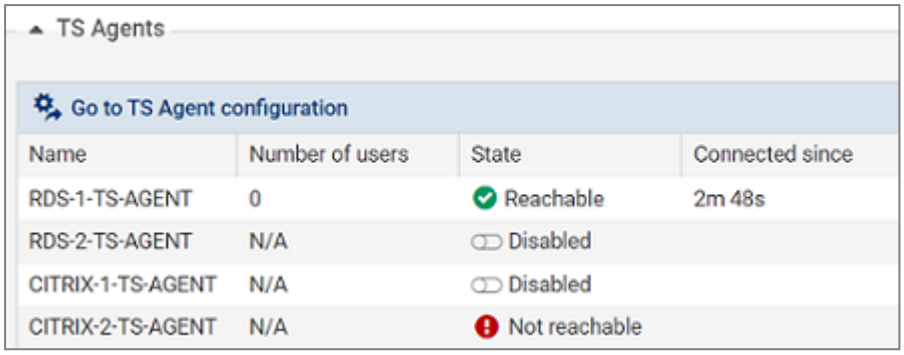
Double-clicking on the TS Agents icon will redirect you to the **TS Agents** widget in the **System monitoring** module.

From the System monitoring module

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:

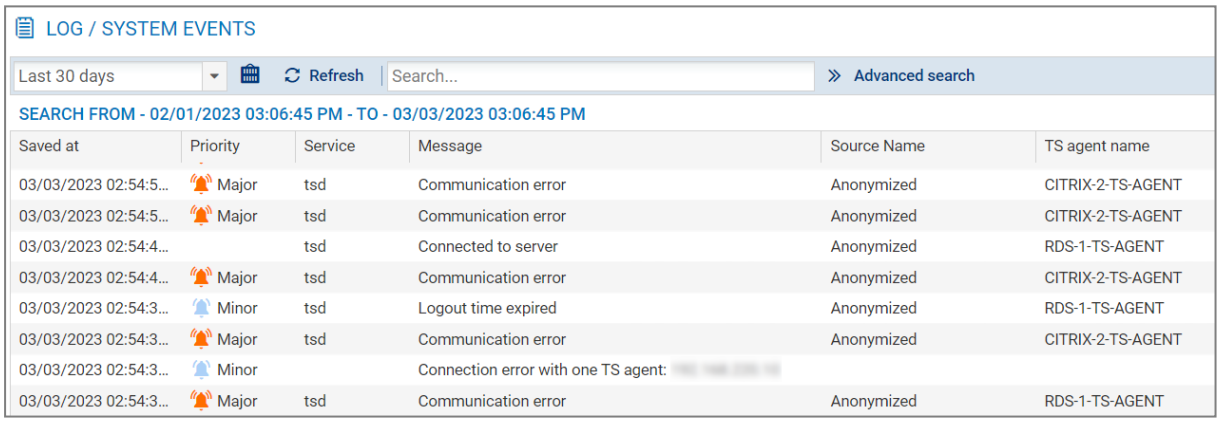
- The name of the TS Agent,
- The number of users connected via this TS Agent,
- The status of the TS Agent (**Reachable**, **Unreachable** or **Disabled**),
- Time lapsed since the connection between the firewall and the TS Agent.



From the Logs - Audit logs module

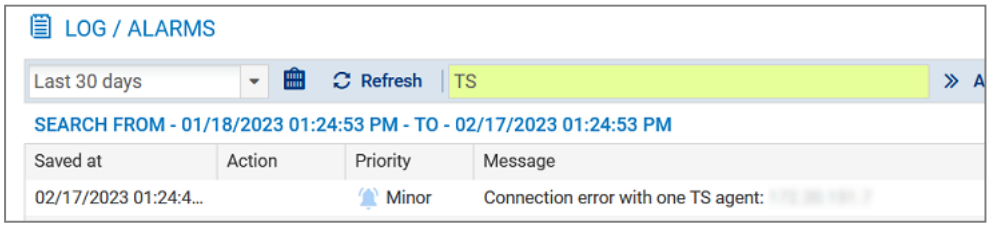
System events

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



Alarms

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



Monitoring the TS Agent on the RDS/Citrix server

This section explains how to monitor TS Agents (performance and logs) that are installed on an RDS/Citrix server.

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

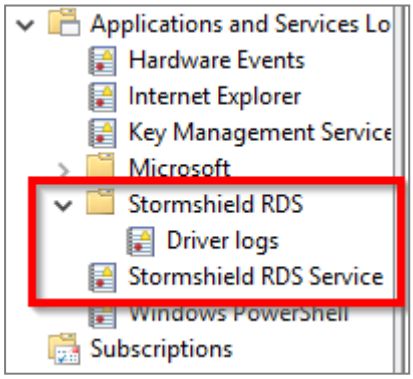
If necessary, on the server on which the TS Agent is deployed:

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 logs of the TS Agent's driver and service

On the RDS/Citrix server on which the TS Agent is deployed:

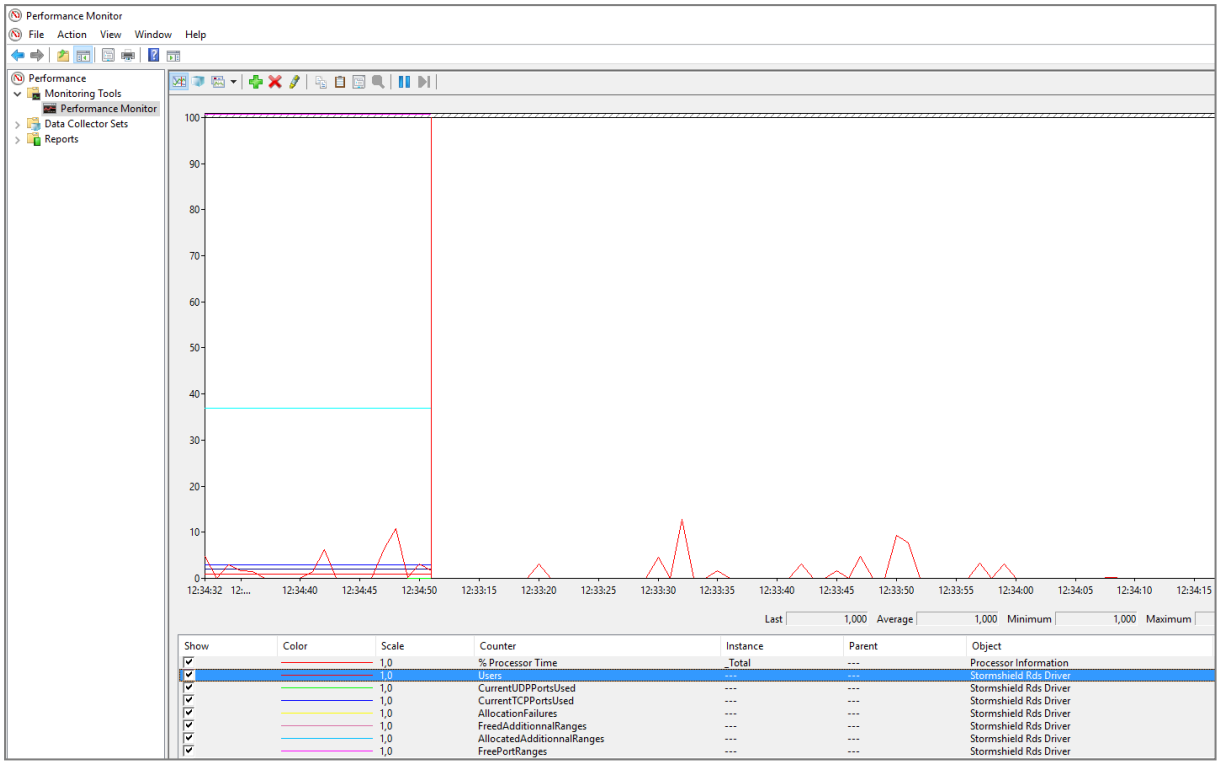
1. Open the **Event Viewer**.
2. In the **Applications and services logs** menu, select:
   - **Stormshield RDS Service** to show the list of events that occurred for the Stormshield RDS Service,
   - **Stormshield RDS > Driver logs** to show the list of events that occurred for the the TS Agent's driver.



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**.

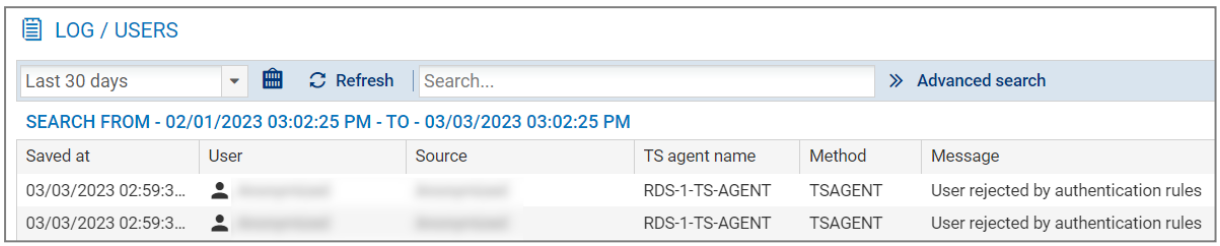

Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
Reports
100
90
80
70
60
50
40
30
20
10
0
12:34:32 12:...
12:34:40
12:34:45
12:34:50
12:33:15
12:33:20
12:33:25
12:33:30
12:33:35
12:33:40
12:33:45
12:33:50
12:33:55
12:34:00
12:34:05
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

Monitoring users connected through TS Agents

This section explains how to monitor users who have connected through TS Agents (authentication logs, and ports assigned to users).

Viewing authentication logs

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



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.

```
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    21424-21623   85870   0           TSAGENT     (0x0000)
Memberof: TS-USERS
john.doe            documentation.org   TS-SERVER-1                 21424-21623   85870   0           TSAGENT     (0x0000)
Memberof: TS-USERS
```

Troubleshooting

This section lists several issues that are frequently encountered when using the TS Agent. If the issue you encounter cannot be found in this section, we recommend that you refer to the Stormshield knowledge base.

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

- *Situation*: 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.tld).
- Solution To allow the firewall to associate the reference Active Directory, you need to map the NETBIOS name to the FQDN on the domain.
  Up to 5 NETBIOS/FQDN links can be declared on the same firewall, by 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=STORMSHIELD FQDN=stormshield.eu
CONFIG AUTH ACTIVATE
```

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

Users are unable to log back in after restarting the RDS/Citrix server

- *Situation*: Restarting the RDS/Citrix server while users are connected through the TS Agent method may prevent such users from logging back in later.
- Solution Restart the RDS/Citrix server again to fix this issue.

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).

Appendix: Using script to configure ports that are reserved for system operations

This appendix explains how to use the script to configure ports that have been reserved for system operations (**AddRangeReservedSystemPorts.ps1**).

This script can be used:

- Immediately after the installation of the TS Agent, ideally before restarting the server,
- Later to adjust the TS Agent's parameters, for example, in the installation of new applications, or when there are connection issues.

Operating principle of the script

This script, which is provided by Stormshield, analyzes any ports that may be in conflict with the TS Agent, and adds them to the parameter **ReservedSystemPorts** on the TS Agent to reserve them for system operations. As such, these ports cannot be assigned to any user.

The script analyzes ports in several ways:

- By analyzing the host's network status (such as an improved *netstat*),
- By analyzing events on the TS Agent in the **Event Viewer**, in order to identify any port conflicts (event ID 32781). This analysis is run by default over a month (the exact number of days varies by month).

Requirements for using the script

- Permissions to run Windows PowerShell as an administrator.
- Permissions to run local scripts on the host.
  This execution policy can be edited with these commands:

```
Set-ExecutionPolicy unrestricted
Set-ExecutionPolicy remotesigned
```

Downloading the script

1. In your MyStormshield personal area, go to **Downloads > Downloads.**
2. Select **Stormshield Network Security > TS Agent** from the suggested categories.
3. Click on the script **AddRangeReservedSystemPorts.ps1** to download it.
4. Copy the script on each RDS or Citrix server on which a TS Agent has been installed.

Using the script

1. In Windows PowerShell, run the command:

```
.\AddRangeReservedSystemPorts.ps1
```

2. Take note of the script output:
   - The listed ports may be in conflict with the TS Agent,
   - *Pre-configured* ports are from the TS Agent's default configuration.

3. Indicate with a "**yes**" or "**no**" whether you want the script to modify the TS Agent's **ReservedSystemPorts** parameter in the registry base, by adding the ports found.
4. Indicate with a "**yes**" or "**no**" whether you want to immediately restart the server. New ports that are reserved for the operation of the system will only be taken into account after the server is restarted. If you do not restart the server immediately, remember to schedule it in order to apply changes.

Possible options

The script can be used with the following options:

```
.\AddRangeReservedSystemPorts.ps1 -Options
```

Option	Description
-PauseAtExit	Forces the script to wait until the user presses a key before ending, and applies every time. This option is useful for viewing the script output when it is called up by another script or program.
-Force	Edits the TS Agent's **ReservedSystemPorts** parameter in the registry base without asking for confirmation.
-HistoryDepth <days>	Sets a period in number of days to analyze TS Agent events in the **Event Viewer**, By default, the analysis is run over a month (the exact number of days varies by month). This option is not compatible with the **-FullLog** option.
-FullLog	Analyzes the full available history of TS Agent events in the **Event Viewer**, This option is not compatible with the **-HistoryDepth** option.
-AutoRestart	Automatically restarts the server without asking for confirmation, on the condition that the script is correctly executed. This option is useful in immediately finding out which new ports are reserved for the operation of the system. This option is not compatible with the **-NoRestart** option.
-NoRestart	Determines that the server must not be restarted, thereby preventing the display of confirmation requests to restart when executing the script. This option is not compatible with the **-AutoRestart** option.
-Verbose	Displays additional messages when executing the script. This option is helpful when obtaining technical assistance, such as with Stormshield technical support.
-DryRun	Shows only the output of the script analysis. No actions will be initiated with this option. This option is often used with the **-Verbose** option. This option is useful for running scripts without administrator privileges.

documentation@stormshield.eu