STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK VPN CLIENT EXCLUSIVE

DEPLOYMENT GUIDE

Version 7.5.006

Document last updated: February 26, 2024

Reference: sns-en-vpn_client_exclusive-deployment-guide-v7.5.006

Table of contents

1. Change log

Date	Description
February 26, 2024	New document

2. Getting started

Welcome to the SN VPN Client Exclusive v7.5.006 deployment guide.

This guide is intended for SN VPN Client Exclusive administrators. It contains all the information required to deploy the software, with licenses and VPN configurations.

A complementary document dedicated to the software's configuration, called "Administrator's Guide", is also available. Prior to proceeding with the deployment of the SN VPN Client Exclusive, carefully read the section entitled "Security recommendations" in the "Administrator's Guide".

In this document, Stormshield Network VPN Client Exclusive is referred to in its short form: SN VPN Client Exclusive. Some of the images used in this document are from the partner vendor's (TheGreenBow) software program. In your SN VPN Client Exclusive program, the graphics may vary but user experience is exactly the same.

3. Deploying the VPN Client

3.1 Introduction

The deployment of the software mostly relies on the fact that it can be installed silently, i.e. without any user interaction (prompts or warnings).

All the software configuration options can therefore be set during installation, either using initialization files or the set of MSI parameters and properties passed from the command line.

3.2 Customizing the software

In addition to using the software's **Configuration Panel** to generate VPN configurations to be deployed, you can customize the SN VPN Client Exclusive during installation and when you use it for the first time by any of the following three means:

- Using a set of parameters and properties passed to the MSI installer from the command line
- Using a software installation configuration file (`vpnsetup.ini`)
- • Using a PKCS#11 tokens or smart card initialization file (`vpnconf.ini`).

The configuration files must be stored in the following directories:

- `vpnsetup.ini` must be stored in the `C:\Windows` directory
- `vpnconf.ini` must be stored in the same directory where the SN VPN Client Exclusive is installed and running (`C:\Program Files\Stormshield\Network VPN Client Exclusive\` by default).

These various means of configuring the software during its installation allow you, for example, to prepare the deployment of the VPN Client on heterogeneous platforms equipped with different tokens or smart cards, but for which the certificates to be used have the same characteristics (e.g. the certificates to be used are of "authentication" type).

Other example: The VPN Client can be deployed on platforms equipped with tokens or smart cards that are unknown to it. The configuration file allows the VPN Client to recognize them.

3.3 Silent installation

A "silent" installation is an installation that is carried out without any user interaction, prompts, or warnings. The installation is carried out in an entirely transparent manner.

In this case, the installation parameters are configured using a set of MSI parameters and properties passed from the command line or the `vpnsetup.ini` software installation configuration file (see chapter vpnsetup.ini file).

To run the installation in silent mode, use the `/quiet` option in the command line.

1. Download the `NetworkVpnClientExclusive_Setup.msi` installation program from MyStormshield.
2. Run the Windows command prompt as an administrator and enter the following command line:

```
msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" /q
```

EXAMPLE

```
msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" /q
LICENSE=[license_number]
```

`[download_directory]` is the directory to which the installer was downloaded.

NOTE

For more command-line installation options, refer to chapter Parameters and properties of the MSI installer.

3.4 Deploying an update

Deploying a SN VPN Client Exclusive update is done in the exact same way as deploying a new installation.

When performing a silent update, the entire update process is silent (back up parameters, uninstall previous version, install new version, restore parameters).

NOTE

However, no version whatsoever of the Standard edition can be updated. This edition requires the prior version to be uninstalled. Moreover, the VPN configurations are not compatible.

3.5 Repairing

The repair function of the MSI installer is currently not supported.

3.6 Uninstalling the software

The software can be uninstalled from the **Programs and Features** tab in the Windows **Control Panel** or by right clicking the SN VPN Client Exclusive icon in the Windows **Start** menu and choosing **Uninstall**.

3.7 Order in which properties and files are taken into account

During installation, the properties passed in the command line have priority over equivalent values possibly present in the `vpnsetup.ini` file.

The `vpnconf.ini` file is taken into account each time the SN VPN Client Exclusive is started.

4. Deploying software activation

4.1 Introduction

SN VPN Client Exclusive software must be activated in order to be able to use it beyond the trial period.

By default, software activation is performed online on TheGreenBow's website.

When your pool of machines on which VPN clients are installed does not have an internet connection, you can activate the software on an activation server, called TheGreenBow Activation Server (TAS), installed in your premises.

The activation parameters can be configured to be automatically applied during the software installation and deployment process, either from the command line or in the `vpnsetup.ini` configuration file. These methods are described in the sections below.

4.2 Activating the software on the TheGreenBow website

Using activation parameters, the software's activation can be fully integrated in the deployment process. This allows for the activation process to be automated and performed in a manner that is entirely transparent for the end user (no interaction required).

In order for the activation to be executed automatically and in a manner that is transparent for the user, use the installer's command-line options: `AUTOACTIV` (which automates activation) and `NOACTIVWIN` (which hides the activation window), together with the `LICENSE` and `ACTIVMAIL` properties as described in section Activating the license.

Command line for automated and silent activation:

```
msiexec /i "[download_directory]/NetworkVpnClientExclusive_Setup.msi" /q
LICENSE=[license_number] ACTIVMAIL=[activation_email] NOACTIVWIN=1
AUTOACTIV=1
```

4.3 Activating the application on TAS

When activating the software using a TAS server ("TheGreenBow Activation Server", activation server installed on your infrastructure), we recommend that you specify the parameters of this server in the command line using the MSI properties `OSAURL`, `OSAPORT` and `OSACERT` (see chapter Using command line options).

Example of a command line for activation on a TAS server:

```
msiexec /i "[download_directory]/NetworkVpnClientExclusive_Setup.msi" /q
LICENSE=[license_number] ACTIVMAIL=[activation_email] NOACTIVWIN=1
AUTOACTIV=1 OSAURL=192.168.217.102/osace_activation.php OSAPORT=80
OSACERT="MIICGjCCAYOgAwIBAgIBADANBg [........]
muHf58kMO0jvhkyq24GryqptSaSJqVIA="
```

You can also use the `vpnsetup.ini` file together with the installer during installation (see chapter vpnsetup.ini file for further details on available parameters).

Example of a `vpnsetup.ini` file for activation on a TAS server:

```
[Activation]
OSAUrl=192.168.217.102/osace_activation.php
OSAPort=80
OSACert="MIICGjCCAYOgAwIBAgIBADANBg [........]
muHf58kMO0jvhkyq24GryqptSaSJqVIA="
```

NOTE
In order to avoid overloading the TAS server with a large number of simultaneous activation requests, as of version 7.4 of the SN VPN Client Exclusive, random attempts to activate the software are made starting from 90 days before the subscription expires and systematic attempts are made every time the software is started as of 30 days before the expiration date.

4.4 Activating "within the tunnel"

Activation on TheGreenBow's website or on TAS requires a connection to the internet or to the network on which the TAS is located. Users have 30 days (trial period) from the first time the SN VPN Client Exclusive is installed to connect to the internet, or to the network on which TAS is located, to activate the software.

Activation can be performed manually by opening the **About** window of the SN VPN Client Exclusive (refer to the SN VPN Client Exclusive "Administrator's Guide").

If the `AUTOACTIV` property is set to 1, the SN VPN Client Exclusive will attempt to activate automatically every time:

1. The VPN Client is started
2. A tunnel is opened

NOTE
As of version 7.4 of the SN VPN Client Exclusive, if the software has not been activated within 30 days of installation or if the license has expired, a tunnel can still be mounted in order to proceed with activation on a TAS server. If activation is successful, the tunnel remains open. Otherwise, it will be closed automatically.

4.5 Identifying activations

When you deploy the software, we recommend that you identify the workstations on which activation has been performed. This will allow for easy activation/deactivation of the installed licenses.

Workstation identification is achieved by using the **Activation email** field during the installation process, e.g. to enter the name of the activated workstation.

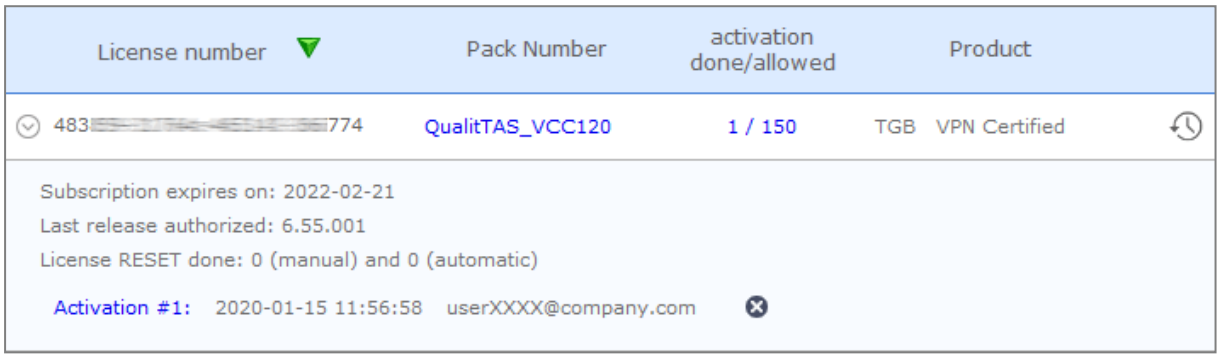
Installation script for the Windows command prompt with the identifier of an activated workstation:

```
msiexec /i "[download_directory]/NetworkVpnClientExclusive_Setup.msi" /q
LICENSE=[license_number] ACTIVMAIL=%ComputerName%@company.com
NOACTIVWIN=1 AUTOACTIV=1
```

Installation script for Microsoft PowerShell with the identifier of an activated workstation:

```
msiexec /i "[download_directory]/NetworkVpnClientExclusive_Setup.msi" /q
LICENSE=[license_number] ACTIVMAIL=$env:computername@company.com
NOACTIVWIN=1 AUTOACTIV=1
```

The operating system automatically enters the `%ComputerName%` or `$env:ComputerName` environment variable during installation. The activation process will then automatically use the environment variable, which will ultimately be displayed in the pages showing available activations on the activation server on TheGreenBow's website or on your TAS.



IMPORTANT

The value of the `ACTIVMAIL` property must always be formatted according to the email address syntax, i.e. it must always contain the characters "@" and "." (dot). Activation will fail if this is not the case.

5. Deploying VPN configurations

5.1 Integrity of a VPN configuration

Protecting the integrity of a VPN configuration when it is exported and checking its integrity when it is imported is a function that can be enabled using the `SIGNFILE` property. This property is disabled by default.

Example of a command line to enable signing and checking the integrity of a configuration file:

```
msiexec /i "[download_directory]/NetworkVpnClientExclusive_Setup.msi" /q
SIGNFILE=1
```

A preconfigured VPN configuration can be included with the installation of the SN VPN Client Exclusive. This configuration will be automatically imported and applied during software installation. It will therefore be immediately operational for the end user, as of the first time the VPN Client is started.

The steps to create such an installation are as follows:

1. From the SN VPN Client Exclusive's **Configuration Panel**, create the VPN configuration for the target workstation.
2. Export the VPN configuration (**Configuration** > **Export** menu item, refer to the SN VPN Client Exclusive "Administrator's Guide") and protect it with a password, if desired.
3. Transfer the installation program and the VPN configuration to the target workstation.
4. Run the installation of the SN VPN Client Exclusive by specifying the `TGBCONF_PATH` and `TGBCONF_PASSWORD` properties (if the configuration is password protected, refer to section VPN Configuration). When the installation is complete, the VPN Client will have been installed with the imported VPN configuration applied.

EXAMPLE

```
msiexec /i "[download_directory]/NetworkVpnClientExclusive_Setup.msi" /q
TGBCONF_PATH=C:\Users\Admin\conf.tgb TGBCONF_PASSWORD=[password]
```

From a deployment security perspective, this method relies on the integrity check function in VPN configurations, if it is enabled. If this is the case, the function ensures that the configuration imported during installation has not been corrupted.

5.2 Deploying a VPN configuration update

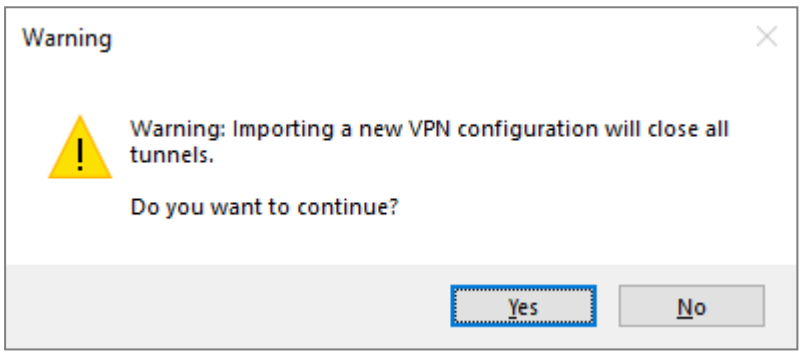
Once the SN VPN Client Exclusive is installed, you can update its VPN configuration using the function to import a configuration file from the command line.

To import a configuration from the command line, proceed as follows:

1. Create the VPN configuration for the target workstation.
2. Export the configuration (**Configuration** > **Export** menu item, refer to the SN VPN Client Exclusive "Administrator Guide"). It can be encrypted with a password.
3. 3. Transfer the VPN configuration to the workstation to be updated.
4. On the target workstation, run `vpnconf.exe` in command line and, where appropriate, specify the password used to protect the exported configuration (refer to the `/add`, `/replace` and `/pwd` options described in detail in section Importing).
5. If one or several tunnels are open, the following warning window will appear:

NOTE
If you want to perform a silent update of the configuration (without warning window), when one or several tunnels are open, use the command-line options to close and then open them again (see chapter Using command line options).

IMPORTANT
If access to the **Configuration Panel** is restricted to administrators, the command line interpreter (cmd, PowerShell, etc.) must be run as administrator to be able to use the import or export commands: `/import`, `/importonce`, `/add`, `/replace`, `/export`, `/exportonce`.



For further details on command-line options, refer to chapter Using command line options.

6. Deploying the software with tokens or smart cards

6.1 Introduction

The SN VPN Client Exclusive supports a great number of tokens and smart cards that can be used for strong multi-factor authentication (MFA) using one of the following APIs: CNG (default) or PKCS#11.

> **NOTE**
> The list of tokens and smart cards compatible with the SN VPN Client Exclusive is available on TheGreenBow's website at: https://www.thegreenbow.com/en/support/integration-guides/compatible-vpn-tokens/.

6.1.1 CNG

CNG stands for "Cryptography API: Next Generation". It is an API to access cryptographic tokens and smart cards, currently provided by Microsoft. The SN VPN Client Exclusive uses it by default, and it does not require any additional configuration.

6.1.2 PKCS#11

PKCS#11 is an API to access cryptographic tokens and smart cards that has been standardized by RSA Labs. Most tokens and smart cards are compatible with PKCS#11. For the SN VPN Client Exclusive to be able to use the PKCS#11 API, a middleware provided by the manufacturer of the token or smart card must first be installed on the target computer.

To force the SN VPN Client Exclusive to use the PKCS#11 API instead of the CNG API, use the **Force PKCS#11 API usage** option (refer to the section entitled "PKI Options" in the SN VPN Client Exclusive "Administrator's Guide") or the MSI property PKCS11ONLY when installing the software (see section PKCS11ONLY).

The SN VPN Client Exclusive supports PKCS#11-compatible tokens or smart cards from leading manufacturers (Gemalto, IN Groupe, Neowave, Feitian, Yubico, etc.) without any additional configuration.

The tokens and smart cards compatible with the SN VPN Client Exclusive are the ones listed on TheGreenBow's website at: https://www.thegreenbow.com/en/support/integration-guides/compatible-vpn-tokens/ and for which the **PKCS11** box is checked.

For tokens or smart cards that are not recognized as standard by the SN VPN Client Exclusive, the software allows you to specify their characteristics in a PKCS#11 initialization file called `vpnconf.ini`, described below.

6.2 vpnconf.ini file

To enable the SN VPN Client Exclusive to support tokens or smart cards that are not recognized as standard, you must create a `vpnconf.ini` file in the VPN Client's installation directory (`C:\Program Files\Stormshield\Network VPN Client Exclusive\` by default). You can create the file using a standard text editor (e.g. Notepad).

The parameters to be specified in the `vpnconf.ini` file are broken down into several sections:

- A series of (optional) `ATR` sections used to define the attributes of tokens or smart cards that are not recognized as standard by the software
- An (optional) `ROAMING` section to specify the token or smart card to be used when initializing the software

6.2.1 ATR sections

ATR stands for "Answer To Reset". It is an identifier that the token or smart card returns upon receiving a reset command. This identifier is related to the manufacturer and model of the token or smart card.

Each ATR section describes the required characteristics to access a token or smart card, or a family of tokens or smart cards that are not yet known to the software.

The parameters to be specified in the ATR section are detailed in the following table:

Parameter	Meaning
`[ATR#]`	ATR of the token or smart card to be added
`mask`	Mask to be used with this ATR. Details regarding ATRs and ATR masks are provided by the manufacturers of tokens or smart cards. If in doubt, you can configure a mask containing only FF. The lengths of the ATR and the mask must be identical. The mask line can thus be as follows: mask=FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF
`scname`	Name of the token or smart card (strictly descriptive field)
`manufacturer`	Name of the manufacturer (strictly descriptive field)
`pkcs11dllname`	Name of the PKCS#11 DLL
`dllpath`	Path to the PKCS#11 DLL. The path is the complete path. It must also contain the DLL name. At least one of the two parameters dllpath or registry must be defined.
`registry`	Name of the key in the registry specifying the path to the middleware. At least one of the two parameters dllpath or registry must be defined

EXAMPLE

```
[3B:0F:52:4E:42:4F:24:00:23:00:00:00:00:00:00:00:01]
mask="FF:FF:FF:FF:FF:FF:FF:00:FF:00:00:FF:FF:00:00:00:FF"
scname="Card Name"
manufacturer="Company Name"
pkcs11dllname="mdlw.dll"
dllpath="C:\path\to\middleware\mdlw.dll"
```

6.2.2 ROAMING section

The ROAMING section is used to specify the token or smart card reader to be used when the option **Use the token or SC reader specified in the VPN Config.** is selected (refer to the section entitled "PKI Options" in the SN VPN Client Exclusive "Administrator's Guide") or when the software has been installed with the `SMARTCARDROAMING` property set to 2 or 3 (see section SMARTCARDROAMING).

The parameters to be specified in the ROAMING section are detailed in the following table:

Parameter	Meaning
`SmartCardReader`	Name of the smart card reader or token to use
`SmartCardMiddleware`	DLL file used to communicate with the token or smart card
`SmartCardMiddlewareType`	Type of middleware. PKCS#11 is the only value possible for the `SmartCardMiddlewareType` parameter.
`SmartCardMiddelwarePath`	Path to the middleware including the middleware name. At least one of the two parameters `SmartCardMiddlewarePath` or `SmartCardMiddlewareRegistry` must be defined.
`SmartCardMiddlewareRegistry`	Name of the key in the registry specifying the path to the middleware. At least one of the two parameters `SmartCardMiddlewarePath` or `SmartCardMiddlewareRegistry` must be defined.

NOTE

The parameters for accessing the Windows registry must comply with the following syntax: PRIMARY_KEY:path\\to\\specific\\key:value

EXAMPLE

```
[ROAMING]
SmartCardReader="Card Name"
SmartCardMiddleware="mdlw.dll"
SmartCardMiddlewareType="PKCS#11"
SmartCardMiddlewareRegistry="HKEY_LOCAL_
MACHINE:SOFTWARE\\Vendor\\Prod\\CK:PKCS#11DLL"
```

7. Using command line options

7.1 Introduction

The SN VPN Client Exclusive offers a set of command-line options as standard that can be used in scripts or batch files. These options are used to perform various tasks, such as opening or closing a VPN tunnel, importing or exporting a VPN configuration, etc.

The syntax of these command-line options always remains the same:

```
"[installation_directory]\vpnconf.exe" [/option[:value]]
```

- `[installation_directory]` is the directory in which the `vpnconf.exe` executable file is located (i.e. the SN VPN Client Exclusive installation directory).
- If the value contains blank spaces (e.g. a directory name), it must be placed between quotation marks.
- All available options are explained below.

IMPORTANT
The `vpnconf.exe` command line cannot be run when the SN VPN Client Exclusive is started in TrustedConnect mode. You must quit the **TrustedConnect Panel** to use the command-line options, and then restart it.

The value `TunnelName` used with options `/open`, `/status`, and `/close` consists of the following (replace the name of the IKEAuth, ChildSA, or TLS with the name you defined in your configuration):

	TunnelName
IKEv2	IKEAuth-ChildSA
SSL	TLS

IMPORTANT
The tunnel name is case sensitive. If the name contains spaces, it must be placed between quotation marks.

7.2 Difference between import, importonce, add, and replace

The `/import` option is used to import a VPN configuration and simultaneously start the SN VPN Client Exclusive, if it is not already running.

The `/importonce` option is used to import a VPN configuration without starting the SN VPN Client Exclusive.

When the SN VPN Client Exclusive is already running, both options simply import the VPN configuration.

When the existing VPN configuration (prior to import) of the SN VPN Client Exclusive is not empty, both options will display a pop-up asking the user whether to “Add or replace”, i.e. add the new VPN configuration or replace the old configuration with the new one.

The `/add` and `/replace` options are used to prevent showing the user prompt: the `/add` option will always add the VPN configuration, the `/replace` option will always replace the old configuration with the new one.

Option	Prompt to "Add or replace"	Starts VPN Client if not already running
`/import`	Yes	Yes
`/importonce`	Yes	No
`/add`	No: adds the VPN configuration	No
`/replace`	No: replaces the VPN configuration	No

If access to the **Configuration Panel** is restricted to administrators, the command line interpreter (cmd, PowerShell, etc.) must be run as administrator to be able to use the import or export commands: `/import`, `/importonce`, `/add`, `/replace`, `/export`, `/exportonce`.

7.3 Importing

7.3.1 /import

Syntax:	`"[installation_directory]\vpnconf.exe" /import:[ConfigFileName]`
Usage:	This option is used to import a VPN configuration when the SN VPN Client Exclusive is started. This option can be used to start the SN VPN Client Exclusive with a specific VPN configuration. If the VPN Client is already running, this option will import and update the VPN configuration without stopping the software. A window is displayed prompting you to decide whether the configuration should be added or replaced. If a tunnel is open when you import a configuration, it is closed and no tunnel will be opened automatically. `[ConfigFileName]` is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after.
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /import:"C:\Users\Admin\Documents\mavpnconf.tgb"`

NOTE
If the imported VPN configuration is password-protected, you must use the `/import` option together with the `/pwd` option (see below).

NOTE
If the current VPN configuration is not empty, the software will display a window prompting the user to decide whether to add the imported VPN configuration or replace the existing configuration with the one being imported. To prevent this window from being displayed, use the `/add` or `/replace` options (see below).

7.3.2 /importonce

Syntax:	`"[installation_directory]\vpnconf.exe" /importonce:[ConfigFileName]`
Usage:	Same behavior as the `/import` option, but without starting the VPN Client. `[ConfigFileName]` is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after.
Return code:	Refer to the note on return codes below. 0: Command has been executed successfully 1: File not found 2: Error in file signature 3: Wrong password (the configuration is protected) 4: A password is required and could not be obtained (password prompt window canceled)
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /importonce:"C:\Users\admin\Documents\mavpnconf.tgb"`

NOTE
If the VPN configuration is empty, both the `/import` and `/importonce` options will not prompt the user for anything and will "add" the VPN configuration.

NOTE
If the current VPN configuration is not empty, the software will display a window prompting the user to decide whether to add the imported VPN configuration or replace the existing configuration with the one being imported. To prevent this window from being displayed, use the `/add` or `/replace` options (see below).

NOTE
The `/importonce` command is preemptive and will pause the rest of the command line until it has been successfully completed.
An error code will be returned in the `ERRORLEVEL` environment variable (see return codes below).
If `/importonce` is not specified with a password, but a password is required, a dialog box opens.

NOTE
If the user cancels the Add/Replace prompt, a return code set to 1 will be written in `ERRORLEVEL` (users are not supposed to use `/importonce` in a script if the execution should be silent).

7.3.3 /add

Syntax:	`"[installation_directory]\vpnconf.exe" /add:[ConfigFileName]`
Usage:	Used to add a VPN configuration. `[ConfigFileName]` is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after.
Return code:	Refer to the note on return codes below. 0: Command has been executed successfully 1: File not found 2: Error in file signature 3: Wrong password (the configuration is protected) 4: A password is required and could not be obtained (password prompt window canceled)
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /add:"C:\Users\Admin\Documents\mavpnconf.tgb"`

NOTE
If the imported VPN configuration is password-protected, then `/add` must be used with the `/pwd` option (see below).

NOTE
The `/add` command is preemptive and will pause the rest of the command line until it has been successfully completed.
An error code will be returned in the `ERRORLEVEL` variable (see return codes below).
If `/add` is not specified with a password, but a password is required, a dialog box will open.

7.3.4 /replace

Syntax:	`"[installation_directory]\vpnconf.exe" /replace:[ConfigFileName]`
Usage:	Used to add a VPN configuration. `[ConfigFileName]` is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after.
Return code:	Refer to the note on return codes below. 0: Command has been executed successfully 1: File not found 2: Error in file signature 3: Wrong password (the configuration is protected) 4: A password is required and could not be obtained (password prompt window canceled)
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /replace:"C:\Users\Admin\Documents\mavpnconf.tgb"`

NOTE
If the imported VPN configuration is password-protected, then `/replace` must be used with the `/pwd` option (see below).

NOTE
The `/replace` command is preemptive and will pause the rest of the command line until it has been successfully completed.
An error code will be returned in the `ERRORLEVEL` variable (see return codes below).
If `/replace` is not specified with a password, but a password is required, a dialog box will open.

7.3.5 /pwd

Syntax:	`"[installation_directory]\vpnconf.exe" /pwd:[password]`
Usage:	Used to specify a password for importing and exporting VPN configurations. This option is used with the following options: `/import`, `/importonce`, `/add`, `/replace`, `/export`, `/exportonce`. In the command line, the `/pwd` option must be specified after the import or export options. When exporting the configuration file, the password must be greater than or equal to 16 characters in length.
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /import:"C:\Users\Admin\Documents\mavpnconf.tgb" /pwd:monmdp`

TIP
From a security standpoint, we recommend using the `/importonce`, `/add` and `/replace` options for maintenance tasks (and not `/import`), since they quit the software immediately after their execution.

7.4 Exporting

7.4.1 /export

Syntax:	`"[installation_directory]\vpnconf.exe" /export:[ConfigFileName]`
Usage:	Used to export a VPN configuration when you start the VPN Client software. If the software is already running, the `/export` option will export the VPN configuration without stopping it. `[ConfigFileName]` is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after. `/export` can be used with `/pwd` in order to export a VPN configuration and protect it with a password.
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /export:"C:\Users\Admin\Documents\mavpnconf.tgb" /pwd:gq1aRe7fr8TGB2!5`

7.4.2 /exportonce

Syntax:	`"[installation_directory]\vpnconf.exe" /exportonce:[ConfigFileName]`
Usage:	Same behavior as the `/export` option, but without starting the VPN Client. If the software is already running, the `/exportonce` option will export the VPN configuration without stopping it. `[ConfigFileName]` is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after. `/exportonce` can be used with `/pwd` in order to export a VPN configuration and protect it with a password.
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /exportonce:"C:\Users\Admin\Documents\mavpnconf.tgb" /pwd:gq1aRe7fr8TGB2!5`

7.5 Opening/closing a VPN tunnel

The `/stop`, `/closeall`, and `/status` options can only be executed if the SN VPN Client Exclusive is already running and not started in TrustedConnect mode.

The `/open` and `/close` options can be executed even if the SN VPN Client Exclusive is not already running. In this case, the software is started and does not quit, but no return code is output to find out the result of the execution.

7.5.1 /stop

Syntax:	`"[installation_directory]\vpnconf.exe" /stop`
Usage:	Closes all VPN tunnels currently open and quits the VPN Client software.
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /stop`

7.5.2 /open

Syntax:	`"[installation_directory]\vpnconf.exe" /open:[TunnelName]`
Usage:	Used to open a VPN tunnel from the command line.
Return code:	0: Tunnel is still closed 2: Tunnel is now open Other: See the list of return codes below.

Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /open:TgbTest-TgbTest`
	`@echo return_code = %ERRORLEVEL%`
	`Pause`

7.5.3 /status

Syntax:	`"[installation_directory]\vpnconf.exe" /status:[TunnelName]`
Usage:	Used to get the status of a VPN tunnel from the command line.
Return code:	0: VPN tunnel is closed 1: VPN tunnel is being opened 2: VPN tunnel is open 3: VPN tunnel is being closed 4: Error while opening a VPN tunnel Other: See the list of return codes below.

Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /status:TgbTest-TgbTest`
	`@echo return_code = %ERRORLEVEL%`
	`Pause`

7.5.4 /close

Syntax:	`"[installation_directory]\vpnconf.exe" /close:[TunnelName]`
Usage:	Used to close a VPN tunnel from the command line.
Return code:	0: VPN tunnel is closed Other: See the list of return codes below.
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /close:TgbTest-TgbTest`

7.5.5 /closeall

Syntax:	`"[installation_directory]\vpnconf.exe" /closeall`
Usage:	Used to close all currently open VPN tunnels.
Return code:	0: All VPN tunnels are closed Other: See the list of return codes below.
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /closeall`

7.6 Restarting

The `/resetike` option can only be executed if the SN VPN Client Exclusive is already running and not started in TrustedConnect mode.

7.6.1 /resetike

Syntax:	`"[installation_directory]\vpnconf.exe" /resetike`
Usage:	Used to restart the IKE service from the command line.
Return code:	0: IKE service has restarted Other: See the list of return codes below.
Example:	`"C:\Program Files\Stormshield\Network VPN Client Exclusive\vpnconf.exe" /resetike`

7.7 Return codes

The command-line options (`/open`, `/close`, `/status`, `/closeall`, `/resetike`) may return the following codes:

-1:	Cannot execute the command: the VPN Client is not running yet.
100 to 499:	Internal error (contact support).
500:	The specified VPN tunnel does not exist (case sensitive!).
501 to 999:	Internal error (contact support).
1000 to 1999:	Other issue while accessing the VPN tunnel.
1089:	No reply from gateway.
1090:	The gateway refuses to authenticate the client (IKE_AUTH Failed).

8. Parameters and properties of the MSI installer

8.1 Introduction

The installer of the SN VPN Client Exclusive is in Microsoft Installer (MSI) format. It can be configured using command-line parameters and so-called properties.

To install the SN VPN Client Exclusive, we recommend starting the `MSIEXEC` command line from an admin shell with the `/i` option, `/q` or `/quiet` option as well as any other suitable properties for your deployment.

EXAMPLE

```
msiexec /i [path_to_installer] /q
```

Syntax rules: Options that call for a specific value must be entered without any blank spaces between the option and the value assigned to it. Values that contain blank spaces, such as directory names, must be placed between quotation marks.

For further details on how `msiexec` works and available installation options, refer to the Microsoft documentation: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec.

8.2 Passing command-line parameters to MSI

8.2.1 /i

Syntax:	`msiexec /i [path_to_installer]`
Usage:	Installs or updates the SN VPN Client Exclusive software
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi"`

8.2.2 /x

Syntax:	`msiexec /x [path_to_installer]`
Usage:	Uninstalls the SN VPN Client Exclusive software
Example:	`msiexec /x "[download_directory]\NetworkVpnClientExclusive_Setup.msi"`

8.2.3 /q

Syntax:	`msiexec /q` or `/quiet`
Usage:	Configures the installation or uninstallation in silent mode (no messages or warnings to the user)
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" /q`

8.2.4 /L*V!

Syntax:	`msiexec /L*V! <path_to_log_file>`
Usage:	Enables logging and includes a detailed output in the output log file by specifying the location and name of the output log file.
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi " /L*V! "C:\install.log"`

8.3 Installing the software

> **NOTE**
> `"C:\Program Files\Stormshield\Network VPN Client Exclusive\"` is the default installation directory.

8.3.1 APPLICATIONROOTDIRECTORY

Syntax:	`APPLICATIONROOTDIRECTORY=[installation_directory]`
Usage:	`[installation_directory]` is the directory where the VPN Client software is to be installed. Quotation marks are required before and after `[installation_directory]`, if the directory name contains blank spaces.
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi " APPLICATIONROOTDIRECTORY="C:\my directory\vpn"`

8.3.2 TGBCONF_ADMINPASSWORD

Syntax:	`TGBCONF_ADMINPASSWORD=[password]`
Usage:	Administrator password used to protect access to the **Configuration Panel** in version 6.8 and earlier, where appropriate. Used to update an earlier version in which the **Configuration Panel** was password protected.
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" TGBCONF_ADMINPASSWORD=Tgb@dM1Npwd!`

8.3.3 NOAUTORUN

Syntax:	`NOAUTORUN=1`
Usage:	This property is used to not start the SN VPN Client Exclusive (regardless of the mode: **Connection Panel, TrustedConnect**) when Windows is started. Default value 0 (automatic startup).

8.4 VPN Configuration

8.4.1 TGBCONF_PATH

Syntax:	`TGBCONF_PATH=[path_to_conf_file]`
Usage:	Full path to the VPN configuration file to be used for this installation.

8.4.2 TGBCONF_PASSWORD

Syntax:	`TGBCONF_PASSWORD=[password]`
Usage:	Password used to protect the VPN configuration entered as a parameter using the `TGBCONF_PATH` property.

8.5 TheGreenBow Activation Server

Properties determine the characteristics of TheGreenBow Activation Server (TAS, an activation server optionally installed on the user's infrastructure).

These properties include the following: server address, access port, and activation authentication certificate.

Since the values of these properties are required for specific configurations, they are generally provided by TheGreenBow.

8.5.1 OSAURL

Syntax:	`OSAURL=[TAS_URL]`
Usage:	This property is used to define the URL for TAS. It must be defined together with the `OSAPORT` property and, where appropriate, with the `OSACERT` property.
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" OSAUrl=192.168.217.102/osace_activation.php`

8.5.2 OSAPORT

Syntax:	`OSAPORT=[TAS_port]`
Usage:	This property is used to define the port for TAS and must be combined with the `OSAURL` property.
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" OSAPort=80`

8.5.3 OSACERT

Syntax:	`OSACERT=[certificate_contents]`
Usage:	This property is required when the TAS activation server is used. It is used to decrypt the activation key received from the TAS server. Its content is available on TheGreenBow's website in the **Private partner area** under the heading **Public key (certificate)**.
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" OSACert="MIICGjCCAYOgAwIBAgIBADANBg [........] muHf58kMO0jvhkyq24GryqptSaSJqVIA="`

8.6 Activating the license

8.6.1 ACTIVMAIL

Syntax:	`ACTIVMAIL=[activation_email]`
Usage:	This property is used to configure the e-mail address used to activate the software.
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" ACTIVMAIL=salesgroup@company.com`

8.6.2 AUTOACTIV

Syntax:	`AUTOACTIV=1`
Usage:	This property is used to configure the software so that it is automatically activated. If the value is set to 1, the SN VPN Client Exclusive will attempt to activate automatically every time: 1. The VPN Client is started 2. A tunnel is opened
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" AUTOACTIV=1`

8.6.3 LICENSE

Syntax:	`LICENSE=[license_number]`
Usage:	This property is used to configure the license number used to activate the software.
Example:	`msiexec /i "[download_directory]\NetworkVpnClientExclusive_Setup.msi" LICENSE=1234567890ABCDEF12345678`

8.6.4 NOACTIVWIN

Syntax:	`NOACTIVWIN=1`
Usage:	This property is used to prevent the activation window from being displayed. It can be combined with the `AUTOACTIV=1` property to deploy a non-activated software on the target user workstations and to automate its activation in an entirely transparent manner for the users. Please bear in mind that the activation window will ultimately be displayed to the user at the end of the trial period if no activation has been carried out by that date. However, in this case, users can still mount a tunnel in order to proceed with activation.

8.7 TrustedConnect Panel

Properties related to the **TrustedConnect Panel** are described below.

8.7.1 USEDIALERBYDEFAULT

Syntax:	`USEDIALERBYDEFAULT=1`
Usage:	The **TrustedConnect Panel** is used as user interface when this property is set to 1. The **TrustedConnect Panel** start automatically upon Windows logon, unless the `NOAUTORUN` property is set to 1.

8.7.2 DIALERMINIMIZE

Syntax:	`DIALERMINIMIZE=5000`
Usage:	This property is used to configure the time delay before the **TrustedConnect Panel** is minimized, when the workstation has been detected as being connected to the trusted network (either physically or through the VPN tunnel). This time delay is configured in milliseconds. If the value is set to 0, the feature is disabled: the **TrustedConnect Panel** is no longer automatically minimized. If no time delay is configured, the default time delay is 2000 ms (2 seconds).

8.7.3 DIALERDEFS

Syntax:	`DIALERDEFS=01000000`
Usage:	This property is used to configure the type of minimization when the minimization time delay is configured: the **TrustedConnect Panel** can be minimized to the taskbar or to the notification area (systray or system tray). To minimize the **TrustedConnect Panel** to the taskbar, enter the value `01000000`. If the property is not specified, the **TrustedConnect Panel** is minimized to the notification area (systray) by default. Reminder: The time delay and minimization type only apply to automatic minimization of the **TrustedConnect Panel** when a connection to the trusted network is detected.

8.7.4 VPNLOGPURGE

Syntax:	`VPNLOGPURGE=3`
Usage:	This property is used to configure the number of days log files are kept. The value is expressed in number of days. The default value is 10 days. If the value is set to 0, the purging of log files is disabled.

8.7.5 TOKENOUTHANDLE

Syntax:	`TOKENOUTHANDLE=30`
Usage:	This property is used to configure the behavior of the VPN Client when the token is removed or the smart card is removed from the reader while a VPN tunnel is open. The following three modes are available for this event: • Mode A: The tunnel is closed immediately as soon as the token/smart card is removed (default behavior). • Mode B: The tunnel remains open for the configured time period (only available with the **TrustedConnect Panel**). • Mode C: The tunnel remains open indefinitely. Note: In mode C, if the token or smart card is required to open the VPN tunnel, the next renegotiation will fail. By default, if nothing has been configured, mode A is enabled. • `TOKENOUTHANDLE=0`: tunnel is not closed when the token/smart card is removed (mode C) • `TOKENOUTHANDLE=N`: with the **TrustedConnect Panel**, time in seconds before the tunnel is closed once the token/smart card is removed (mode B). With the **Connection Panel**, the tunnel remains open indefinitely (mode C).

8.7.6 BTNBEHAVIORTC

Syntax:	`BTNBEHAVIORTC=1`
Usage:	This property is used to disable the disconnect button when a connection is established (TND check, opening a tunnel, etc.) to prevent users from activating this button once the tunnel is mounted: • 0 or undefined: The button can be activated even after the connection has been established. • 1: The disconnect button is disabled and the tunnel cannot be closed as soon as it is being opened.

8.7.7 MENUITEMTC

Syntax:	`MENUITEMTC=[0..3F]`
Usage:	This property is used to determine which items appear in the taskbar menu. The value assigned to the `MENUITEMTC` property is a bit field, in which every bit represents one item of the taskbar menu: • 1 (1st bit): **Quit** • 2 (2nd bit): **Restart** • 4 (3rd bit): **Logs** • 8 (4th bit): **About** • 16 (5th bit): **Language** • 32 (6th bit): **Console** By default, all the menu items are displayed: value = 0 (0x3F hex). **EXAMPLE** `MENUITEMTC=3` Will only display the **Restart** and **Quit** items. • 0: The taskbar menu is not displayed • 1: Displays **Quit** • 2: Displays **Restart** • 3: Displays **Restart** and **Quit** • 4: Displays **Logs** • 5: Displays **Logs** and **Quit** • 6: Displays **Restart** and **Logs** • 7: Displays **Restart**, **Logs** and **Quit** • Etc.

8.7.8 DIALERBEHAVIOR

Syntax:	`DIALERBEHAVIOR=010000`
Usage:	This property is used to add the following three options to the **TrustedConnect Panel**: • A button to disable trusted network detection (TND) so that users may open a tunnel even if a trusted network has been detected • Enable multiconnection mode so that users can choose the active connection by clicking the connection name in the **TrustedConnect Panel**'s title banner • Enable an on-the-fly compliance check to change the TrustedConnect Panel's state according to the compliance level, without needing to stop or restart the tunnel One, two, or all three options can be enabled at the same time. • 000000 or undefined: None of the three options is enabled. No tunnel can be mounted when a trusted network has been detected and users cannot choose the connection by clicking in the title banner. • 010000: The option used to disable the TND function is shown in the **TrustedConnect Panel**'s status bar. When the TND function is disabled, users can mount a tunnel even if the trusted network has been detected. When the TND function is enabled again, users can no longer mount a tunnel when the trusted network has been detected (default behavior). • 000100: Enables multiconnection mode so that users can choose the active connection by clicking the connection name in the **TrustedConnect Panel**'s title banner after having closed any open tunnel. Users cannot change active connections while a connection is open or being initialized or closed. • 000001: Enables the on-the-fly compliance check to automatically switch the TrustedConnect Panel to: ◦ An error state when the compliance level is no longer satisfactory ◦ The standard tunnel when the compliance level becomes satisfactory ◦ The remediation tunnel when the compliance level allows it • 010100: Enables the first two options. • 000101: Enables the last two options. • 010001: Enables the first and the last option. • 010101: Enables all three options.

8.7.9 RESTARTGUITC

Syntax:	`RESTARTGUITC=1`
Usage:	This property is used to automatically restart the **TrustedConnect Panel** when it is quit or if it has crashed: • 0 or undefined: The **TrustedConnect Panel** is not restarted automatically after it has stopped (default behavior). • 1: The **TrustedConnect Panel** is automatically restarted after it has stopped.

8.8 Tokens and smart cards

8.8.1 SMARTCARDROAMING

Syntax:	`SMARTCARDROAMING=1`
Usage:	This property specifies the smart card reader or token to be used: • Undefined: Smart card reader or token configured in the VPN configuration The subject of the certificate is in the VPN configuration. • 1: Smart card reader or token configured in the VPN configuration The subject of the certificate in the VPN configuration is not taken into account. • 2: Smart card reader or token configured in the `vpnconf.ini` file The subject of the certificate is in the VPN configuration. • 3: Smart card reader or token configured in the `vpnconf.ini` file The subject of the certificate in the VPN configuration is not taken into account. • 4: 1st token or smart card inserted The subject of the certificate is in the VPN configuration. • 5: 1st token or smart card inserted The subject of the certificate in the VPN configuration is not taken into account.

8.8.2 PKCS11ONLY

Syntax:	`PKCS11ONLY=1`
Usage:	This property specifies the smart card or token access mode: • Undefined: The CNG mode (Cryptography API: Next Generation) is used (default value) • 1: Forces use of PKCS#11 mode

8.8.3 KEYUSAGE

IMPORTANT
We recommended that you no longer use this MSI property and instead use the dynamic parameter `user_cert_keyusage`. Its function is identical to that of the MSI property, but it is more granular since it applies to a specific tunnel rather than to all tunnels. Refer to the SN VPN Client Exclusive "Administrator's Guide" for further details.

Syntax:	`KEYUSAGE=1`
Usage:	This property is used to select a certificate based on its "key usage" field: • 0 or undefined: Certificate is not selected based on "key usage" field. • 1: Certificate is selected based on "key usage" field whose attribute `digitalSignature=1`. • 2: Certificate is selected based on "key usage" field whose attribute `digitalSignature=1` and `keyEncipherment=1`.

NOTE
When the value of the `KEYUSAGE` property is set to 2, the **Only authentication certificate** check

box on the **PKI Options** tab is grayed out, refer to the SN VPN Client Exclusive "Administrator's Guide".

8.8.4 NOCACERTREQ

Syntax:	`NOCACERTREQ=1`
Usage:	This property configures the VPN Client to manage various client/gateway certification authorities (CAs). It must be specified if the client and gateway certificates come from different CAs (this can also be done using the software interface).

8.8.5 PKICHECK

Syntax:	`PKICHECK=1`
Usage:	This property is used to specify the way in which the VPN gateway certificate is checked: • 0 or undefined: The VPN gateway certificate is not checked. • 1: The following characteristics of the VPN gateway certificate are checked: validity date, certificate chain, signature, and CRL of each certificate in the certificate chain. • 2: The following characteristics of the VPN gateway certificate are checked: validity date, certificate chain, signature of each certificate in the certificate chain (not the CRLs)—default value. • 3: Same as 1.

8.8.6 X509DIRECTORYSTRING

Syntax:	`X509DIRECTORYSTRING=14`
Usage:	This property specifies the expected identifier for the Remote ID: • Undefined: Expected identifier type: `teletexString` • 14: Expected identifier type: `teletexString` • 13: Expected identifier type: `printableString` • 1C: Expected identifier type: `universalString` • 0C: Expected identifier type: `utf8String` • 1E: Expected identifier type: `bmpString`

NOTE
As of version 6.8 of the software, it is no longer necessary to prefix the characters "0x" to the value of the `X509DirectoryString` property.

8.8.7 DNPATTERN

IMPORTANT
We recommended that you no longer use this MSI property and instead use the dynamic parameter `user_cert_dnpattern`. Its function is identical to that of the MSI property, but it is

more granular since it applies to a specific tunnel rather than to all tunnels. Refer to the "Administrator's Guide" for further details.

Syntax:	`DNPATTERN=[text]`
Usage:	This property is used to specify the certificate to be used: when specified, the SN VPN Client Exclusive searches for the certificate whose subject contains the `[text]` pattern on the token, smart card or in the Windows certificate store. If this property is not specified, the VPN Client searches for the first certificate that meets the other characteristics configured.

8.8.8 NOPINCODE

Syntax:	`NOPINCODE=1`
Usage:	This property is used to prevent a PIN code from being requested for tokens that do not require it. For example, this is the case with Ercom's microSD.

8.9 General settings

8.9.1 MENUITEM

Syntax:	`MENUITEM=[0..1F]`
Usage:	This property is used to determine which items appear in the taskbar menu. The value assigned to the `MENUITEM` property is a bit field, in which every bit represents one item of the taskbar menu: • 1 (1st bit): **Quit** • 2 (2nd bit): **Connection Panel** • 4 (3rd bit): **Console** • 16 (5th bit): **Configuration Panel** By default, all the menu items are displayed: value = 31 (1F hex). **EXAMPLE** `MENUITEM=3` Will only display the **Connection Panel** and **Quit** items. • 0: The taskbar menu is not displayed • 1: Displays **Quit** • 2: Displays **Connection Panel** • 3: Displays **Connection Panel** and **Quit** • 4: Displays **Console** • 5: Displays **Console** and **Quit** • 6: Displays **Connection Panel** and **Console** • 7: Displays **Connection Panel**, **Console** and **Quit** • Etc.

8.9.2 RESTRICTCONFADMIN

Syntax:	`RESTRICTCONFADMIN=0`
Usage:	This property is used to restrict access to the **Configuration Panel** to administrators only. By default, only administrators can access the **Configuration Panel**.

8.9.3 NOSPLITTUNNELING

Syntax:	`NOSPLITTUNNELING=1`
Usage:	This property disables the default route of the physical interface when the tunnel is established. Only applies to tunnels configured with “All traffic through the tunnel”.

8.9.4 NOSPLITDNS

Syntax:	`NOSPLITDNS=1`
Usage:	This property ensures that the DNSs of the virtual interface also apply to the physical interface when the tunnel is established. Only applies to tunnels configured with “All traffic through the tunnel”.

8.9.5 ROUTINGMODE

Syntax:	`ROUTINGMODE=1`
Usage:	This property is used to prevent local traffic coming from the physical interface from going through the tunnel. Only the traffic coming from the virtual interface will be allowed through.

8.9.6 FORCELOCALTRAFICTOTUNNEL

Syntax:	`FORCELOCALTRAFICTOTUNNEL=1`
Usage:	In “all through tunnel” mode, this property is used to route the local traffic coming from the physical interface through the tunnel. If this property is not included (default setting), the mode will not be enabled. • 0 or undefined: Mode disabled • 1: Mode enabled

8.9.7 IKESTART

Syntax:	`IKESTART=1`
Usage:	This property is used to start the IKE service independently of the software’s interface. If this property is not included (default setting), the mode will not be enabled. • Undefined: The mode is not enabled • 1: The mode is enabled • Other value: The mode is not enabled

8.9.8 SIGNFILE

Syntax:	`SIGNFILE=1`
Usage:	This property is used to force the integrity hash check for the VPN configuration file. The default value is 0 (i.e. disabled).

8.9.9 GINABEHAVES

Syntax:	`GINABEHAVES=1`
Usage:	In its default behavior, the GINA mode displays a panel on the Windows logon screen that allows you to open one or more tunnels before logging on to Windows. However, this panel will not be displayed on the lock screen when the user has locked the session. This property is used to make the GINA mode panel visible on the lock screen. The default value is 0.

8.9.10 NESTEDTUNNEL

Syntax:	`NESTEDTUNNEL=1`
Usage:	This property is used to nest two tunnels. To be used when you want a second tunnel to use the connection provided by a first tunnel. In this case, the gateway of the second tunnel will only be accessible on the remote network of the first tunnel. The default value is 0 (i.e. disabled).

8.10 Logs

8.10.1 SYSTEMLOGOUTPUT

Syntax:	`SYSTEMLOGOUTPUT=7`
Usage:	This property is used to select the output of administrator logs. The outputs can be combined, e.g. use the value 7 to combine the 3 outputs. • 0: No system logs • 1: Log files • 2: Syslog server • 4: Windows event observer

8.10.2 SYSTEMLOGSYSLOGSERVER

Syntax:	`SYSTEMLOSERVER=syslogserver.company.com`
Usage:	This property is used to specify the machine's IP address or name to syslog servers.

8.10.3 SYSTEMLOGSYSLOGPORT

Syntax:	`SYSTEMLOGSYSLOGPORT=5514`
Usage:	This property is used to specify the port of the machine for syslog servers. The default port is 514.

9. vpnsetup.ini file

9.1 Introduction

The `vpnsetup.ini` file is used to configure the installation of the SN VPN Client Exclusive from a file, rather than passing command-line properties to MSI.

IMPORTANT
Due to Microsoft MSI installer constraints, as opposed to previous versions of the software, the `vpnsetup.ini` file may no longer be located in the same directory as the installer, but should be in the `C:\Windows` folder.

The `vpnsetup.ini` file is used to define the following parameters:

- Software activation parameters
- Parameters of the **TrustedConnect Panel**
- PKI parameters for token, smart card, and certificate management
- General operating parameters
- System log parameters
- Other parameters

The names of the parameters for the `vpnsetup.ini` file are identical to those of the MSI installer's properties (see chapter Parameters and properties of the MSI installer), the only difference being that they are not case-sensitive (no difference is made between lowercase and uppercase characters).

It can be edited using a standard text editor (e.g. Notepad). Just like any other `ini` file, it is organized into sections. The parameters must be entered in the appropriate section, as specified below.

NOTE
The MSI installer's installation and VPN configuration properties, `APPLICATIONROOTDIRECTORY`, `TGBCONF_ADMINPASSWORD`, `NOAUTORUN`, `TGBCONF_PATH`, and `TGBCONF_PASSWORD` have no equivalent in the `vpnsetup.ini` file.

9.2 [Activation] section

The `[Activation]` section uses the following parameters:

- `OSAUrl` (see section OSAURL)
- `OSAPort` (see section OSAPORT)
- `OSACert` (see section OSACERT)
- `ActivMail` (see section ACTIVMAIL)
- `AutoActiv` (see section AUTOACTIV)
- `License` (see section LICENSE)
- `NoActivWin` (see section NOACTIVWIN)

9.3 [Dialer] section

The `[Dialer]` section uses the following parameters:

- `UseDialerByDefault` (see section USEDIALERBYDEFAULT)
- `DialerMinimize` (see section DIALERMINIMIZE)
- `DialerDefs` (see section DIALERDEFS)
- `VpnLogPurge` (see section VPNLOGPURGE)
- `TokenOutHandle` (see section TOKENOUTHANDLE)
- `DialerBehavior` (see section DIALERBEHAVIOR)
- `GinaBehaves` (see section GINABEHAVES)

9.4 [PKIOptions] section

The parameters defined in the `[PKIOptions]` section are used to specify how the software should use smart cards, tokens, and certificates:

- `SmartcardRoaming` (see section SMARTCARDROAMING)
- `PKCS11Only` (see section PKCS11ONLY)
- `KeyUsage` (see section KEYUSAGE)
- `NoCACertReq` (see section NOCACERTREQ)
- `PKICheck` (see section PKICHECK)
- `X509DirectoryString` (see section X509DIRECTORYSTRING)
- `DnPattern` (see section DNPATTERN)

9.5 [AddRegKey] section

The `[AddRegKey]` section is used to define the general operating parameters:

- `BtnBehaviorTC` (see section BTNBEHAVIORTC)
- `MenuItemTC` (see section MENUITEMTC)
- `RestartGuiTC` (see section RESTARTGUITC)
- `NoPinCode` (see section NOPINCODE)
- `MenuItem` (see section MENUITEM)
- `RestrictConfAdmin` (see section RESTRICTCONFADMIN)
- `NoSplitTunneling` (see section NOSPLITTUNNELING)
- `NoSplitDNS` (see section NOSPLITDNS)
- `ForceLocalTraficToTunnel` (see section FORCELOCALTRAFICTOTUNNEL)
- `IkeStart` (see section IKESTART)
- `NestedTunnel` (see section NESTEDTUNNEL)

9.6 [Config] section

The `[Config]` section uses the following parameter:

- `SignFile` (see section SIGNFILE)

9.7 [Logs] section

The `[Logs]` section is used to define options for system logs. This section uses the following parameters:

- `SystemLogOutput` (see section SYSTEMLOGOUTPUT)
- `SystemLogSyslogServer` (see section SYSTEMLOGSYSLOGSERVER)
- `SystemLogSyslogPort` (see section SYSTEMLOGSYSLOGPORT)

9.8 [VirtMDriver] section

The `[VirtMDriver]` section uses the following parameter:

- `RoutingMode` (see section ROUTINGMODE)

9.9 Sample vpnsetup.ini file

```
[Activation]
OSAUrl=192.168.217.102/osace_activation.php
OSAPort=80
OSACert="ABCDE...."
activmail=john.doe@company.com
AutoActiv=1
License=123456-123456-123456
NoActivWin=1

[Dialer]
UseDialerByDefault=1
DialerMinimize=5000
DialerDefs=01000000
VPNLogPurge=3
TokenOutHandle=30
GinaBehaves=1
DialerBehavior=1

[PKIOptions]
PKICheck=1
SmartcardRoaming=1
NoCACertReq=0
KeyUsage=1
PKCS11Only=1
X509DirectoryString=14
DnPattern=company

[AddRegKey]
BtnBehaviorTC=1
MenuItemTC=3
RestartGuiTC=1
NoPinCode=1
MenuItem=4
RestrictConfAdmin=1
NoSplitTunneling=1
NoSplitDNS=1
ForceLocalTraficToTunnel=1
```

```
IkeStart=1
NestedTunnel=1

[Config]
SignFile=1

[VirtMDriver]
RoutingMode=1

[Logs]
SystemLogOutput=7
SystemLogSyslogServer=syslogserver.company.com
SystemLogSyslogPort=5514
```

All images in this document are for representational purposes only, actual products may differ.