Trustway IP Protect

IP PROTECT CLIENT

Administrator's Guide

IP Protect Client

Administrator's Guide

June 2022

Table of contents

Preface

This guide is intended for administrators of IP Protect Client.

It contains all the information required to implement and configure the software so that secure VPN tunnels can be opened.

A complementary document dedicated to the software's deployment, called "Deployment Guide".

Software release

The minimal software release relative to this document is **7.0**.

Chapitre 1. Installing the software

1.1 Introduction

The IP Protect Client installation is done by executing the program provided by Trustway.

The default installation procedure, run by double-clicking the icon of the downloaded program, opens a window that allows you to customize the installation.

The installation of the software can be customized using a set of command-line options and VPN configuration files. These options and features are detailed in the document entitled "Deployment Guide".

Refer to section Installation procedure.

1.1.1 Installation conditions

The IP Protect Client is available for Windows 10 64-bit.

The minimum system requirements to install the software are as follows:

- Processor: 1 gigahertz (GHz) or faster processor
- RAM: 2 GB
- Hard disk space available: 40 MB

When the software is not installed from an administrator account, a window opens, prompting you for the username and password of an administrator account on the machine.

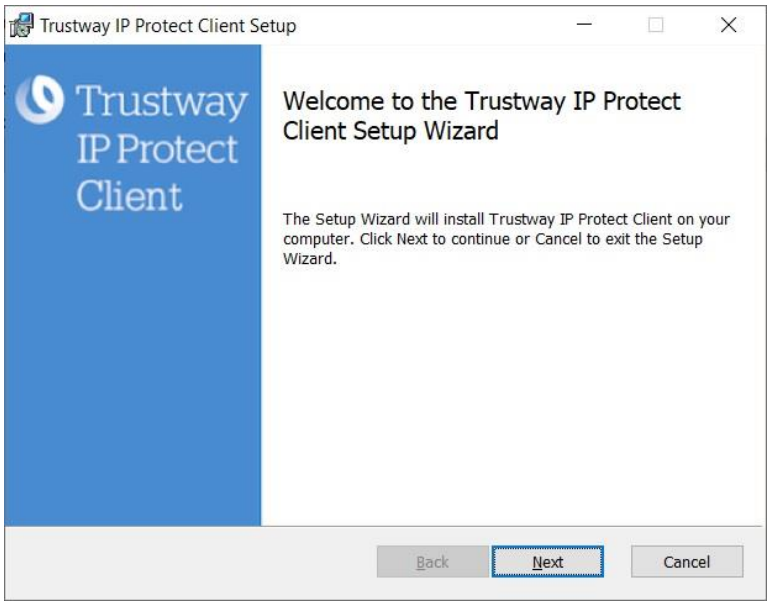
1.2 Installation procedure

The installation procedure is the same whether it is an initial installation or an update (see section Updating the software). When performing an update, the software settings, the existing VPN configuration[1], and the license are preserved.

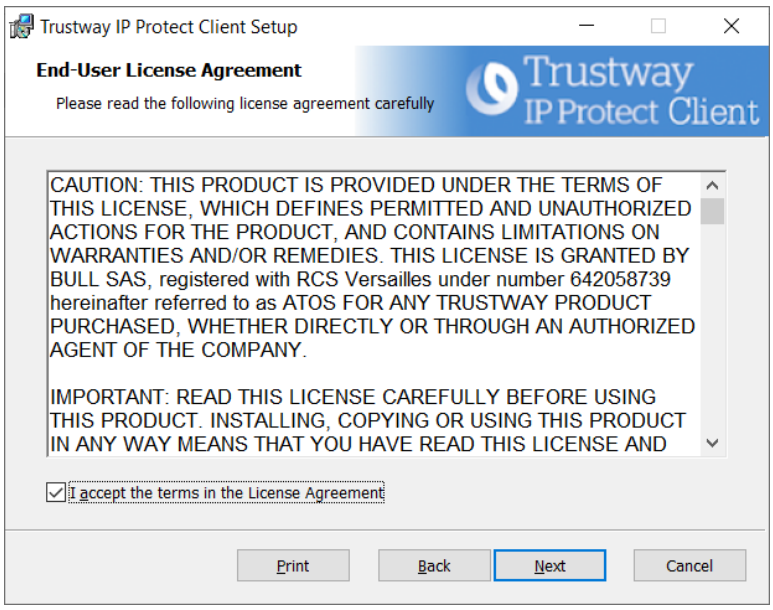
If you want to perform a silent installation, pass specific parameters during installation or perform a large-scale deployment, refer to the "Deployment Guide".

Double-click the installation program you downloaded. The following window is displayed:

[1] In some cases, see section Updating the VPN configuration.



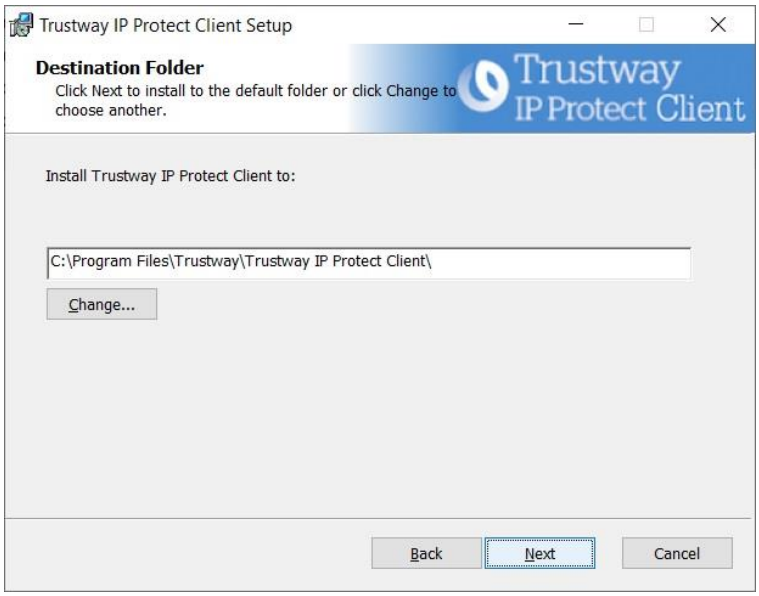
Click **Next**. The following window is displayed:



Read the End User License Agreement (EULA) carefully. If you accept all the terms of the agreement, select the **I accept the terms of the license agreement** checkbox, and then click **Next**. Otherwise, you will not be able to continue installing the IP Protect Client.
Carefully read the information about what's new and the note about how the existing VPN configuration will be converted during an update.

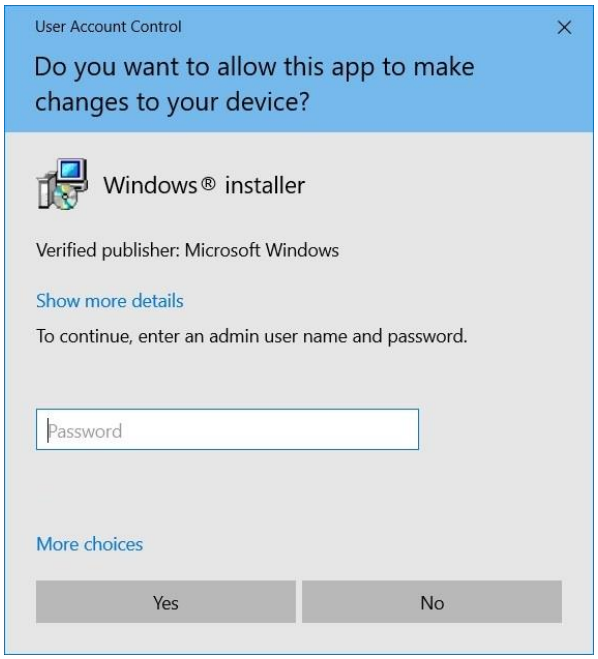
⚠ Once the installation is complete, you will not be able to revert to an earlier version of the software without manual intervention. If in doubt, back up your VPN configuration to a separate folder or to a removable storage medium.

The following window is displayed:



If you want to install IP Protect Client in a specific directory, click **Change…** and select the desired directory. Otherwise, you can keep the default directory. Then, click **Next**. The following window is displayed:

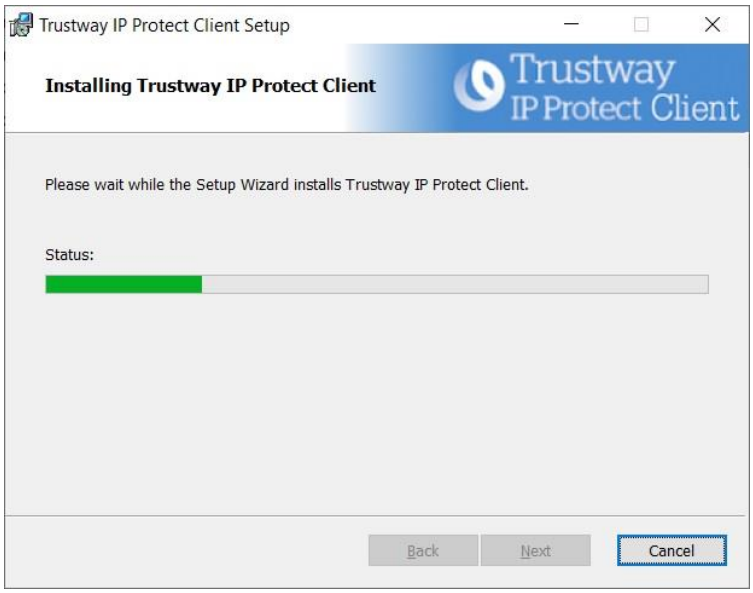
The program is ready to install. If you want to go back to check or change your installation settings, click **Back**. Otherwise, click **Install**. If you are installing from an account that does not have administrator rights, the following window is displayed :



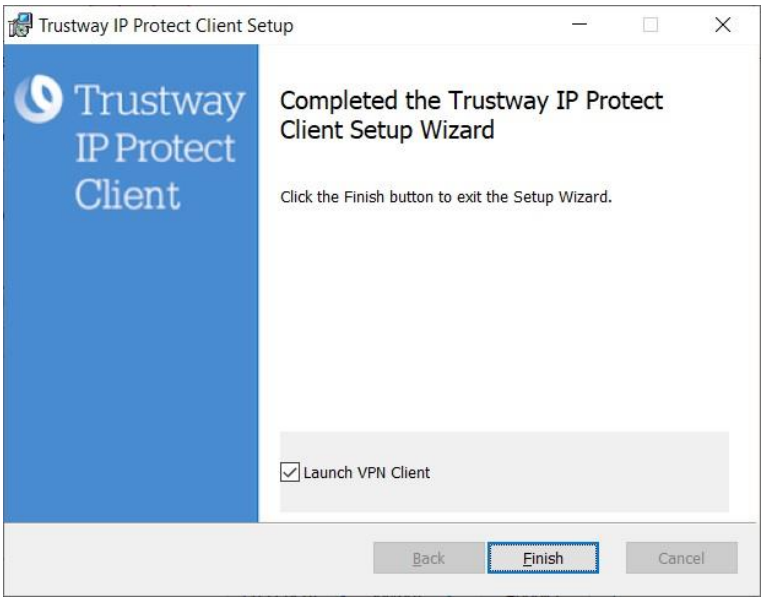
To proceed with the installation, you must enter an administrator name and password to allow the installation program to make changes to your computer. Otherwise, the software will not be installed.

If you are installing from an administrator account, you do not need to enter a password. Simply confirm that you allow the app to make changes to your device.

Installation begins and the following window is displayed :

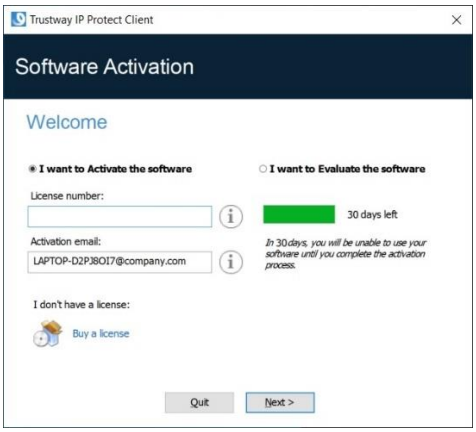


Wait for the installation of IP Protect Client including all its components to complete. If installation has succeeded, the following window is displayed:



If you do not want to launch IP Protect Client immediately, uncheck the corresponding box. To exit the setup wizard, click **Finish.** If you want to launch it immediately, keep the box checked[2]. To exit the setup wizard, click **Finish**.

Otherwise, the activation screen is displayed:



IP Protect Client is now installed on your workstation.

If you already own a license for IP Protect Client:

- Select **I want to Activate the software**,
- Enter the license number and activation email
- Then, click **Next >**

[2] In the case of an update, if the software has been activated, then the activation screen will not appear unlike the case of a first installation.

For further details on the activation procedure, refer to section Activating the software:

- Select **I want to Evaluate the software**,
- Then, click **Next >**.

You will then be able to use the software for a 30-day trial period. For further details on the trial period, refer to Trial period.

If you do not have a license and want to buy one, contact the Trustway commercial team.

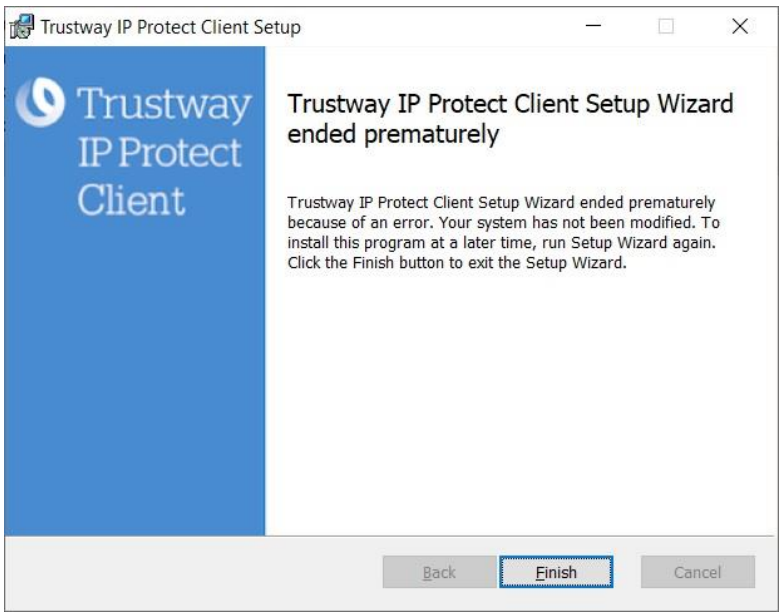
For further details on the activation procedure, refer to section Activating the software.

You are now ready to use the software. You can continue with the following steps:

- To start using the IP Protect Client immediately, refer to section Getting started with the software.
- To use the **Configuration Wizard** to quickly create a VPN connection, refer to section Configuration Wizard.
- To import an IP Protect Client configuration compatible with this version of the software, refer to section Importing a VPN configuration.
- For a detailed presentation of the available interfaces, refer to sections Connection Panel, Configuration Panel and TrustedConnect Panel.
- For a comprehensive explanation of all VPN tunnel configuration options, refer to section Configuring a VPN tunnel.
- To uninstall IP Protect Client, refer to section Getting started with the software.

1.3 Canceling installation

If you cancel the setup wizard before clicking the “Install” button, the following window is displayed:

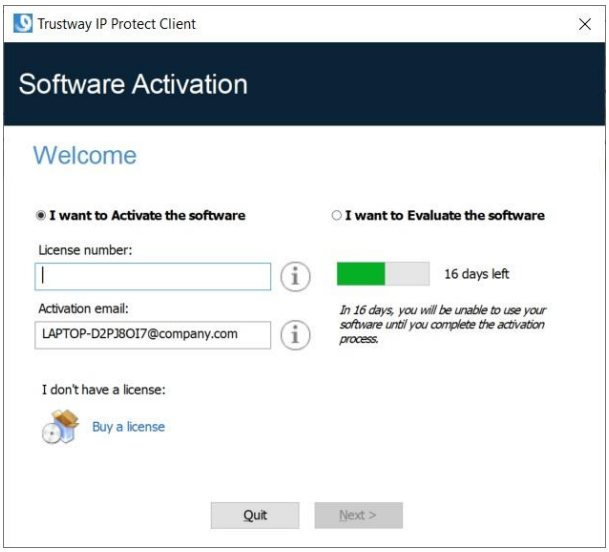


Your system has not been modified and you can resume installation at a later time.

1.4 Trial period

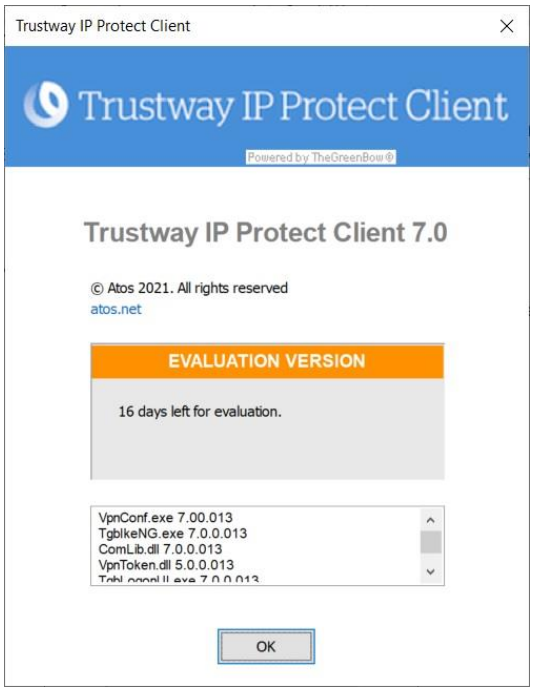
The first time the software is installed on a workstation, if no license key is provided to the installer, IP Protect Client will enter a 30-day trial period. During this trial period, IP Protect Client is fully operational, and all functions are unlocked.

The activation window will be displayed every time the software is started during the trial period. It shows the number of days remaining in the trial period.

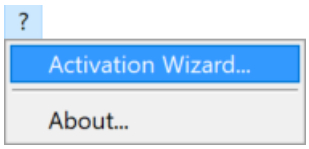


Select **I want to Evaluate the software**, then click **Next >** to run the software.

During the trial period, the **About…** window will display the number of days remaining until the trial ends.

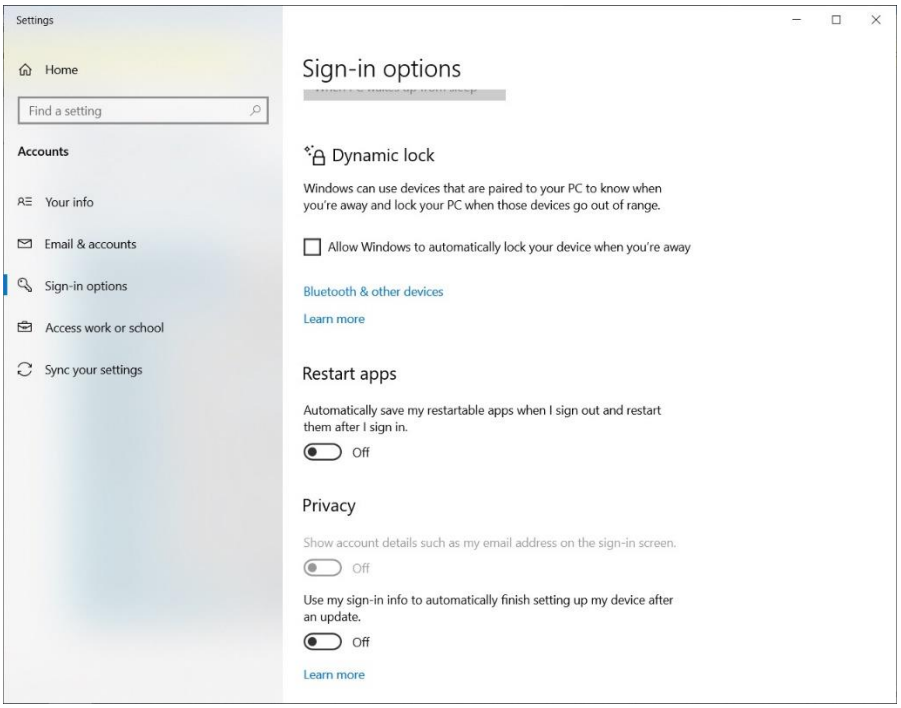


During the trial period, the activation window can be accessed at any time using the **?** > **Activation Wizard** menu item in the main interface (**Configuration Panel**).



1.5 Configuring Windows

Once you have completed installation, make sure the Windows privacy option **Use my sign-in info to automatically finish setting up my device after an update or restart**, found under the **Sign-in options** in the Windows 10 **Settings**, is disabled, as shown in the screenshot below:


Settings
Home
Find a setting
Accounts
Your info
Email & accounts
Sign-in options
Access work or school
Sync your settings
Sign-in options
Dynamic lock
Windows can use devices that are paired to your PC to know when you're away and lock your PC when those devices go out of range.
Allow Windows to automatically lock your device when you're away
Bluetooth & other devices
Learn more
Restart apps
Automatically save my restartable apps when I sign out and restart them after I sign in.
Off
Privacy
Show account details such as my email address on the sign-in screen.
Off
Use my sign-in info to automatically finish setting up my device after an update.
Off
Learn more

Chapitre 2. Activating the software

If the software has not been activated during its silent installation (refer to the "Deployment Guide"), IP Protect Client must be activated to continue to work beyond the trial period.

The activation procedure can be accessed every time the software is launched or using the **?** > **Activation Wizard** menu item in the main interface.

2.1 Step 1

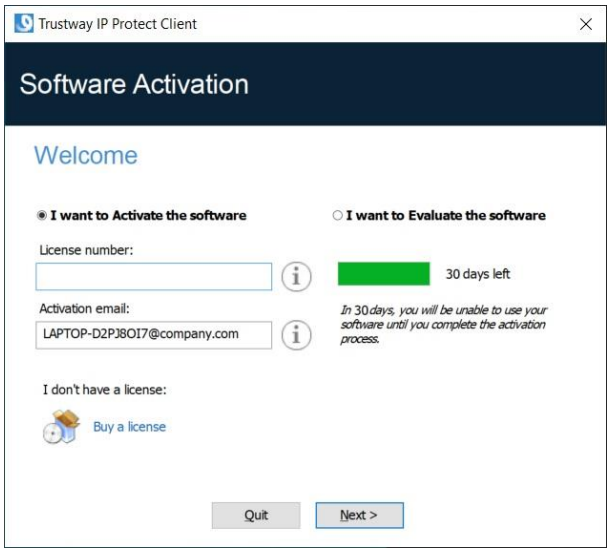
If you do not have a license and want to buy one, contact the Trustway commercial team.

In the **License number** field, enter the license number you received by email.

The license number can be copy-pasted directly from the purchase confirmation email into this field.

The license number consists of the characters [0..9] and [A..F], possibly grouped 6 by 6 and separated by hyphens.

In the **Activation email** field, enter the email address used to identify your activation. This information is used for recovering the activation information if it is lost.



The **Activation email** field is filled by default with the username of the workstation on which the software is installed (as follows: `username@company.com`). This allows administrators of a "master" software license to individually identify all activated workstations. It allows them to manage software activations and deactivations in a deterministic way.

2.2 Step 2

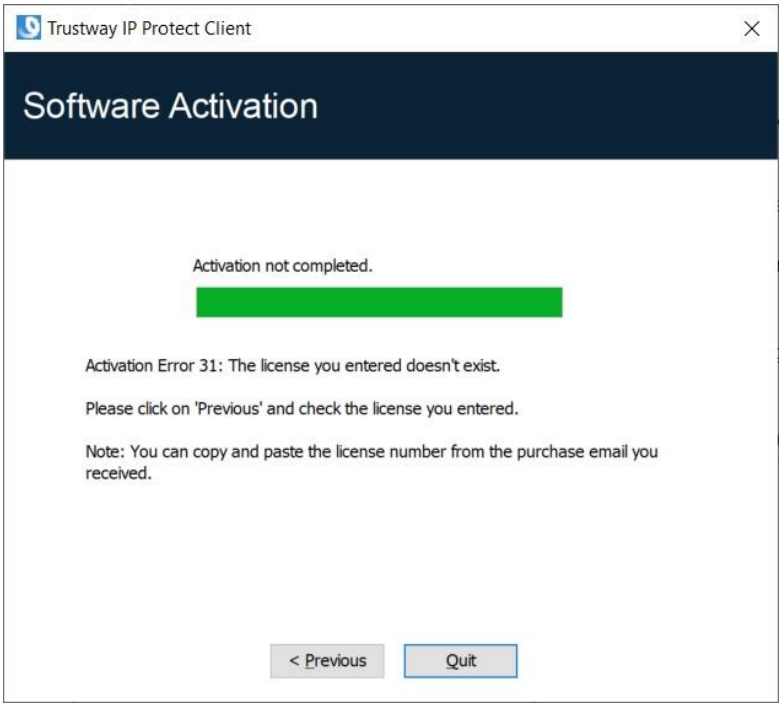
Click **Next >**. The online activation process will run automatically.

Once the activation has been carried out successfully, click **Run** to run the software.

The software activation is linked to the workstation on which the software has been installed. Consequently, a license number allowing a single activation cannot be reused on another workstation once it is activated.
Conversely, a license number activation can be canceled by simply uninstalling the software.

2.3 Activation errors

Software activation may fail for various reasons. The error is always displayed in the activation window.

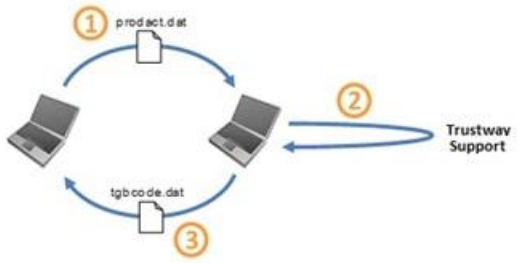


The most common activation errors are :

No.	Meaning	Troubleshooting
31	Wrong license number	Check license number.
33	The license number is already activated on a different workstation	Uninstall the software on the workstation with the activated license or contact the Trustway commercial team.
53, 54	Communication with the activation server is impossible	Ensure that the workstation is connected to the internet. Check that communication is not blocked by a firewall or proxy. Configure the firewall to let the communication through or the proxy to reroute it properly.

2.4 Manual activation

When activation fails because of a communication issue with the activation server, the software can be activated manually. The procedure is as follows:



① `prodact.dat file`	Retrieve the `prodact.dat` file from the **Documents** directory in Windows on the workstation that you want to activate.[3]
② ActivationF	Provide this file to Trustway support who will provide the tgbcode file in return.

[3] The `prodact.dat` file is a text file that contains the workstation information used for the activation. If this file cannot be found in the **Documents** directory, carry out the software activation steps on the workstation. This will generate the file even if activation fails.

③ `Tgbcode file`

Copy the `tgbcode` file to the **Documents** Windows directory on the workstation that you want to activate. Start the software; it will be activated.

2.5 License and activated software

Once the software is activated, the license and email used for activation can be viewed in the **About…** window of the software.

Chapitre 3. Updating the software

3.1 Update procedure

Updating the IP Protect Client allows you to upgrade to a newer version of the software while preserving the settings, the VPN configuration, and the license. It is performed in the same way as a normal installation (see section Installation procedure) except in the following two cases:

1. If the license of the installed product is not compatible with IP Protect Client, updating will not be possible.

   In this case, you will need to uninstall the previous version of the software before you install the new one.

2. If access to the **Configuration Panel** is protected by a password on the version that is already installed, the update cannot be performed using the graphical interface of the installation program.

   You can either delete the password protecting access to the **Configuration Panel**, then proceed with the update, or perform the update in the command line using the `TGBCONF_ADMINPASSWORD` property (refer to the "Deployment Guide").

3.2 Updating the VPN configuration

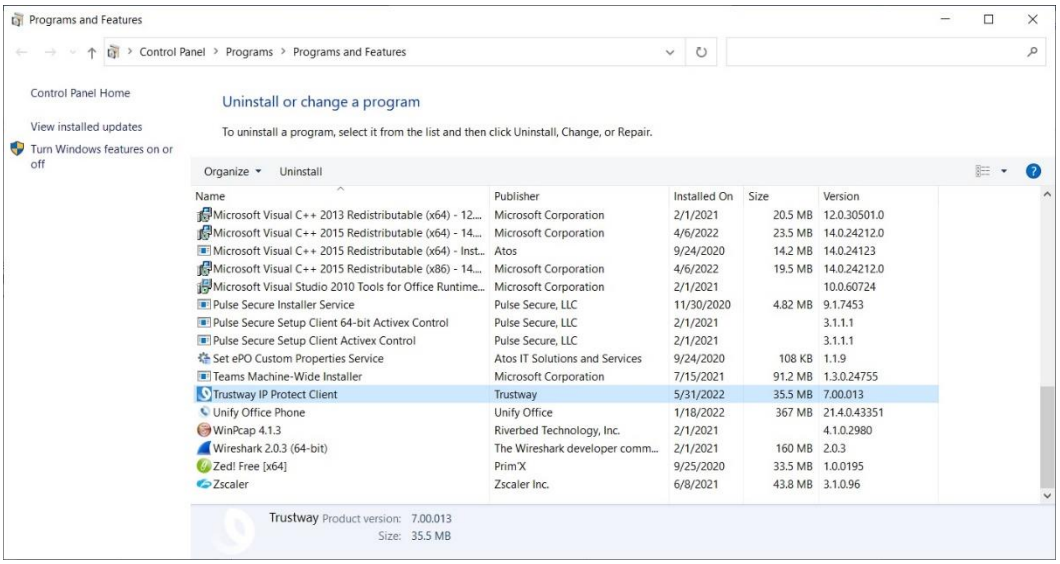
During an update, the VPN configuration is backed up and restored, except in the case mentioned below.

If access to the Control Panel is locked by a password, this password is requested during the update, to authorize the restoration of the VPN configuration.

Chapitre 4. Uninstalling the software

To uninstall IP Protect Client, proceed as follows:

1. Open the Windows **Control Panel**.
2. Select **Uninstall a program**.
3. Select **Trustway IP Protect** in the list of programs.
4. Click **Uninstall** and follow the instructions to uninstall the program.



OR

1. Open the Windows **Start** menu.
2. Right-click the **Trustway IP Protect Client** program, then select **Uninstall**.

3. The Windows **Control Panel** is displayed. Select **Trustway IP Protect Client** in the list of programs.
4. Click **Uninstall** and follow the instructions to uninstall the program.

Administrator privileges are required to install or uninstall the program on the workstation.

Chapitre 5. Getting started with the software

5.1 Introduction

The IP Protect Client graphical interface allows you to perform the following actions:

- Configure the software (startup mode, language, access control, etc.,
- Manage VPN tunnel configurations, certificates, imports, exports, etc,
- Use VPN tunnels (open, close, identify incidents, etc.),
- Switch to TrustedConnect mode (automatically open a tunnel when no trusted network is detected).

The graphical interface includes the following elements:

- The Connection Panel (list of VPN tunnels to open) ;
- The Configuration Panel, which can be displayed from the Connection Panel or using the icon in the taskbar and consists of the following items :
  - A set of menus for VPN configuration and software management;
  - The VPN tunnel tree ;
  - VPN tunnel configuration tabs;
  - A status bar ;
- The TrustedConnect Panel to use the Always-On and TND features (specific executable file) ;
- An icon on the taskbar and the associated menu, which is different for the TrustedConnect Panel and for the Connection/Configuration Panel.

5.2 Starting the software

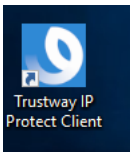
Once the installation or update is complete, if you have not unchecked the **Launch VPN Client** box and you have not activated the software, the activation window is displayed (see section Activating the software). When the software has been activated or if you choose to try it out, IP Protect Client will start minimized and the Trustway IP Protect Client icon will appear in the taskbar. The taskbar icon is described in detail in the paragraph entitled Taskbar icon below.

If you have unchecked the **Launch VPN Client** checkbox at the end of the installation or update procedure, or if you want to use the test tunnel after having installed or updated the software, to start IP Protect Client, you can either double-click the corresponding desktop icon or open the Windows **Start** menu and then select the program in the list.

Starting IP Protect Client using the shortcut on the desktop

During the installation of the software, a shortcut to run the application is created on the Windows desktop.

IP Protect Client can be started directly by double-clicking on this icon.



IP Protect Client will start minimized and the Trustway IP Protect Client icon will appear in the taskbar (see paragraph entitled Taskbar icon below).

Starting IP Protect Client using the Windows Start menu

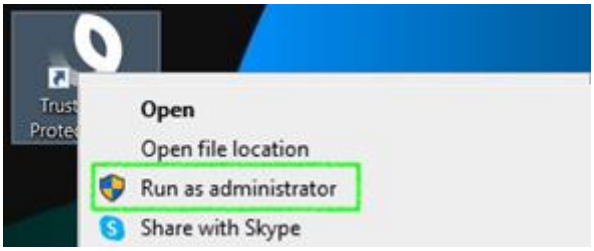
Once the installation is complete, you can start IP Protect Client by clicking the program name in the Windows **Start** menu.

IP Protect Client will start minimized and the Trustway IP Protect Client icon will appear in the taskbar (see paragraph entitled Taskbar icon below).

Running IP Protect Client as administrator

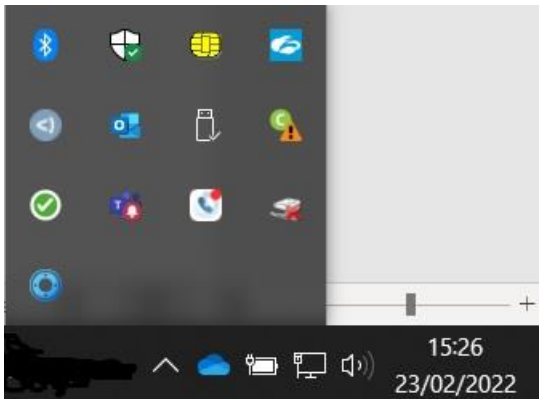
By default, access to IP Protect Client's **Configuration Panel** is restricted to Windows administrators only.

To start IP Protect Client in administrator mode and be able to access the **Configuration Panel**, right-click the **Trustway IP Protect Client** icon and then select **Run as administrator**.



Taskbar icon

Under normal operating conditions, the taskbar icon shows the status of the IP Protect Client **Connection Panel**/**Configuration Panel**.



The color of the icon changes when a VPN tunnel is open:

 Blue icon: no VPN tunnel open

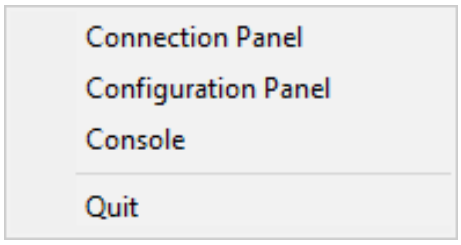
 Green icon: at least one VPN tunnel is open

tooltip for the icon always shows the software status:

- **VPN Tunnel opened** if one or several tunnels are open.
- **Trustway IP Protect Client** when IP Protect Client is running, but no tunnels are open.

Left-clicking the icon opens the **Connection Panel**.

Right-clicking the IP Protect Client icon in the taskbar opens the contextual menu associated with the icon:



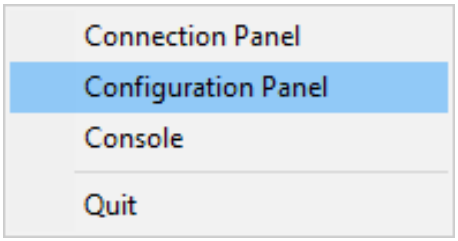
The administrator can limit the options displayed in the menu (see section Showing options in systray menu). The contextual menu contains the following items :

- Connection Panel**: opens the** Connection Panel**.**
- Configuration Panel**: opens the** Configuration Panel (if IP Protect Client has been run with administrator privileges)).
- Console**: opens the VPN traces window.**
- Quit**: closes all open VPN tunnels and quits the software.**

If the software has not been run as administrator and the **Restrict access to Configuration Panel to administrator** has not been disabled, when the user selects the **Configuration Panel** option, a message is displayed indicating that the software must be run as administrator to access the **Configuration Panel** (see paragraph Running IP Protect Client as administrator above)..

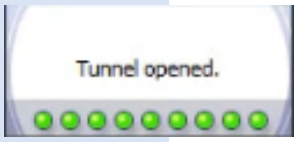
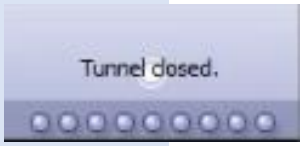
5.3 Configuring a VPN tunnel

To open the **Configuration Panel**, you must first have started IP Protect Client as administrator (see paragraph Starting IP Protect Client as administrator above). If this is not the case, quit and restart IP Protect Client as administrator. If it is, right-click the taskbar icon (see the paragraph entitled Taskbar icon above), and then select the **Configuration Panel** menu item. The **Configuration Panel** is described in section Configuration Panel.

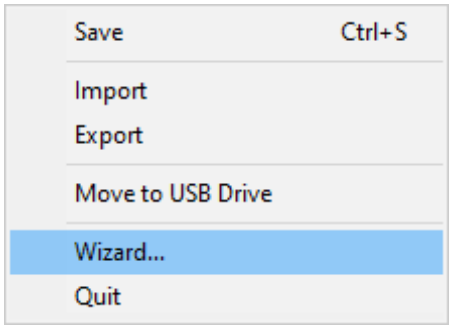


When the **Restrict access to Configuration Panel to administrator** option is disabled (see section When the **Don't show the systray sliding popup** option is disabled, a fade-out pop-up appears above the IP Protect Client icon in the taskbar when a VPN tunnel is opened or closed.

This pop-up shows the tunnel status when it is being opened or closed and automatically fades out unless the mouse cursor is placed directly over it:

Tunnel is open	
Tunnel is closed	
Failed to open the tunnel: the window will briefly explain what happened.	

Then, open the **Configuration Wizard** by selecting the **Configuration** > **Configuration Wizard** menu item.



Use the wizard as described in section Configuration Wizard below.

5.4 Automating the opening of a VPN tunnel

IP Protect Client allows you to automate the opening of a VPN tunnel. It can be opened automatically in the following ways:

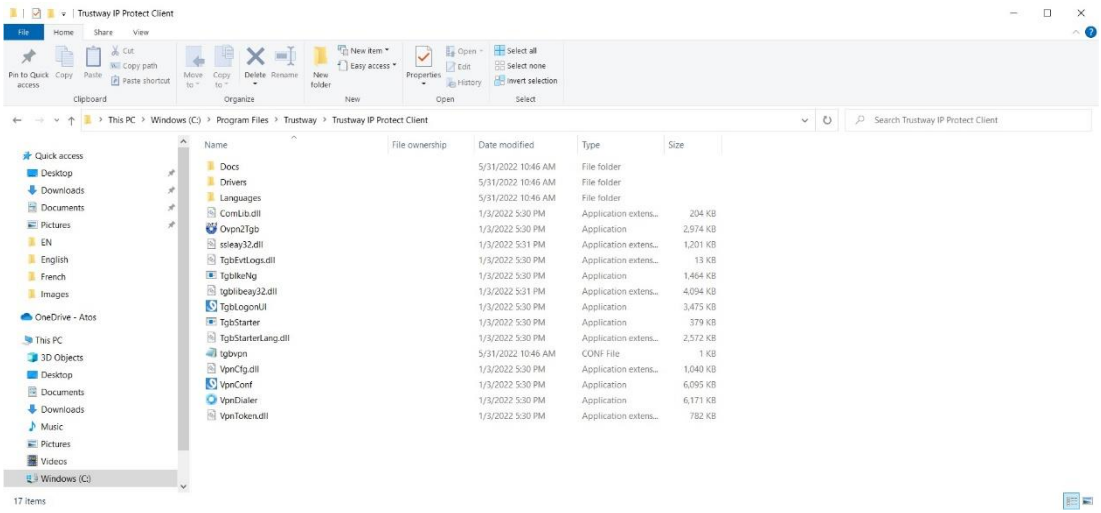
- When Windows is started, before or after logging on;
- When traffic to the remote network is detected (see section Automation) ;

- When inserting a USB drive containing the relevant VPN configuration (see section USB mode) ;
- When inserting the smart card or token containing the certificate used for this tunnel (see section Using a certificate stored on a smart card or token) ;
- When the **TrustedConnect Panel** is used, if IP Protect Client detects that the workstation is not located in the trusted network (see section Configuring the TrustedConnect Panel).

5.5 Opening a VPN tunnel from the TrustedConnect Panel

The **TrustedConnect Panel** is described in section TrustedConnect Panel. It is used to automate the opening of a VPN connection when the workstation is located outside the trusted network and keep the connection open even if the network interface changes.

Start the **TrustedConnect Panel** using the `VpnDialer.exe` executable file located in `C:\Program Files\Trustway\Trustway IP Protect Client` by default.



The **TrustedConnect Panel** is run using a different executable file than the one for the **Configuration Panel**. If the **TrustedConnect Panel** is not launched automatically when the session starts, it can be executed from IP Protect Client's installation folder: the executable file is named `VpnDialer.exe` (no desktop shortcut is created for this application during software installation).

The **TrustedConnect Panel** (run using the `VpnDialer.exe` executable file) cannot be run at the same time as the **Configuration Panel** or the **Connection Panel** (both run using the `VpnConf.exe` executable file, the desktop shortcut, or the Start menu).

When `VpnConf.exe` is running and you are running `VpnDialer.exe`, all tunnels opened in `VpnConf.exe` will be closed and `VpnDialer.exe` (TrustedConnect) will attempt to automatically launch the configured tunnel.

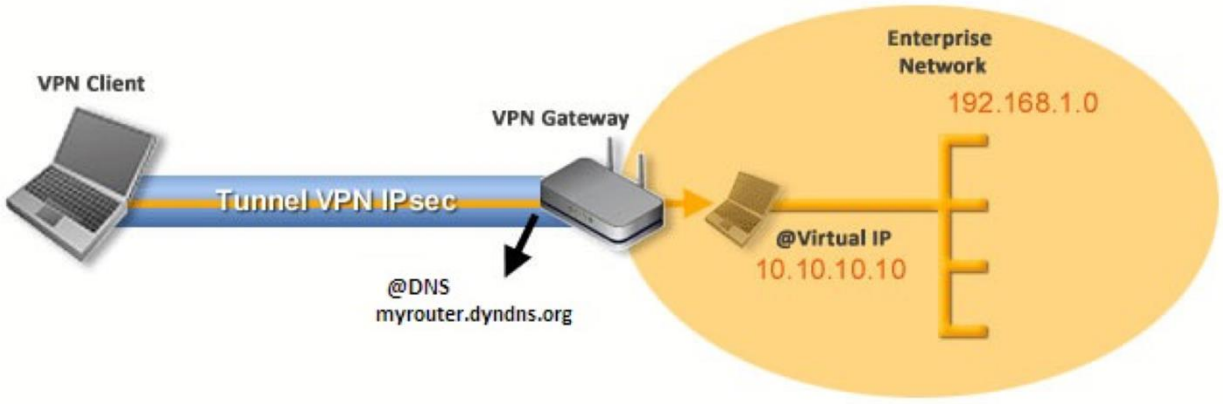
However, when `VpnDialer.exe` (TrustedConnect) is running, you cannot run `VpnConf.exe` immediately. You must first quit `VpnDialer.exe` before you can run `VpnConf.exe`.

Chapitre 6. Configuration Wizard

The **Configuration Wizard** is used to configure a VPN tunnel in three easy steps.

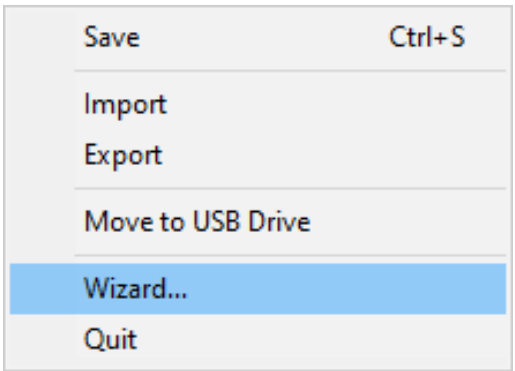
The way the **Configuration Wizard** works is illustrated in the example below:

- The tunnel is open between a workstation and a VPN gateway that has been assigned the DNS address "myrouter.dyndns.org".
- The company's local network is 192.168.1.0 (it may, for example, include machines that have been assigned the IP addresses 192.168.1.3, 192.168.1.4, etc.).
- Once the tunnel is open, the remote workstation will have the following IP address on the company's network: 10.10.10.10.



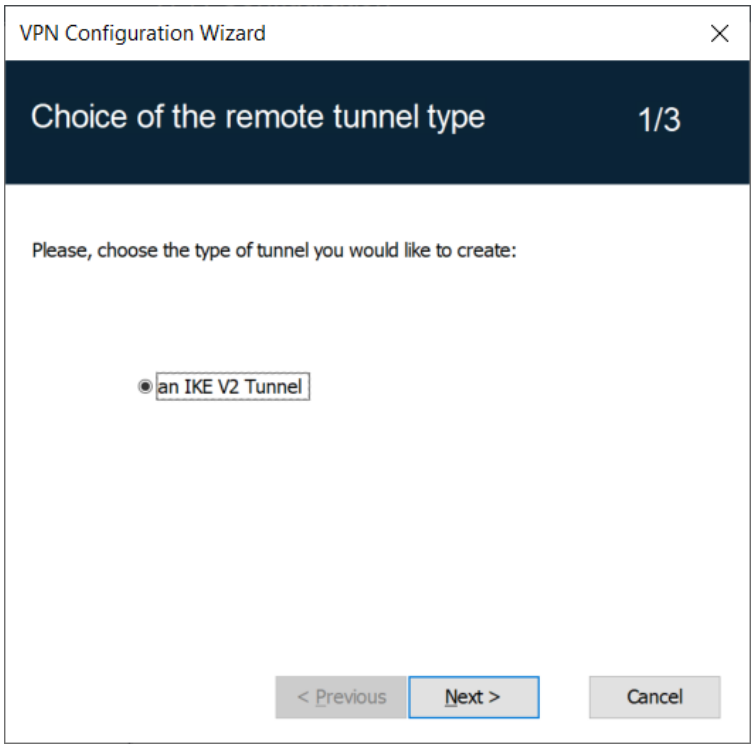
The VPN Gateway is an IP Protect in the figure above.

In the main interface, open the **VPN Configuration Wizard**: **Configuration** > **Wizard…**.



6.1 Step 1

Choose IKEv2 as the VPN protocol to use for the tunnel.



6.2 Step 2

Enter the following values:

- The IP or DNS address on the internet network side of the VPN gateway (e.g. myrouter.dyndns.org).
- A certificate that must be imported using the **Import Certificate…** button (see section Importing a certificate to the VPN configuration).

IP Protect only allows the opening of IKEv2 tunnels with certificate. Refer to section Security recommendations.

6.3 Step 3

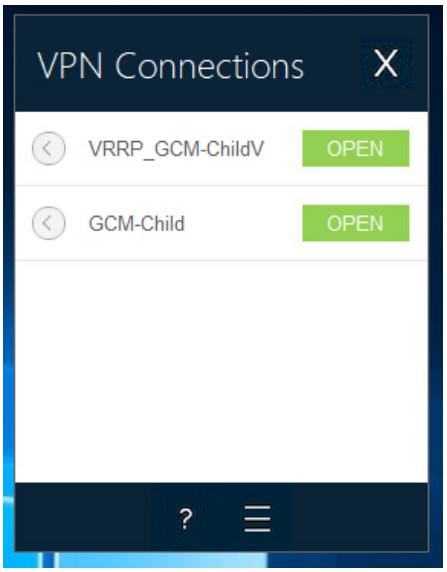
Review the Summary window to check whether the configuration is correct and then click **Finish**.

The tunnel that has just been configured now appears in the tunnel tree of the main interface.

Double-click the tunnel to open it or use the tabs of the main interface for further configuration.

Chapitre 7. Connection Panel

The **Connection Panel** allows you to easily open and close the configured VPN connections:



The **Connection Panel** can be customized. You can select the VPN connections to be shown. You can also rename or sort the VPN connections.

Refer to section Configuring the Connection Panel.

To open a VPN connection, simply click the relevant **OPEN** button.

The icon to the left of the connection name indicates the status of the connection:

Connection closed.

Click this icon to open the VPN configuration for this connection in the **Configuration Panel**.

Caution: Access to the Configuration Panel may be restricted (see section Restricting access to the Configuration Panel).

Connection being opened or closed

Connection open. When there is traffic on this connection, the color intensity of the disk at the center of the icon changes.

T
h

The connection experienced an incident while opening or closing. Clicking the warning icon will open a pop-up window giving detailed or additional information about the incident.

C
o
n

The **Connection Panel** has the following function:

Opens the **About…** window

Opens the **Configuration Panel**.

Caution: Access to the Configuration Panel may be restricted (see section Restricting access to the Configuration Panel).

Closes the **Connection Panel**

Wing keyboard shortcuts are available for the **Connection Panel**:

Esc (or Alt+F4)	Closes the **Connection Panel**.
Ctrl+Enter	Opens the **Configuration Panel** (if enabled).
Ctrl+O	Opens the selected VPN connection.
Ctrl+W	Closes the selected VPN connection.
Up/down arrows	Moves the cursor from one VPN connection to another.

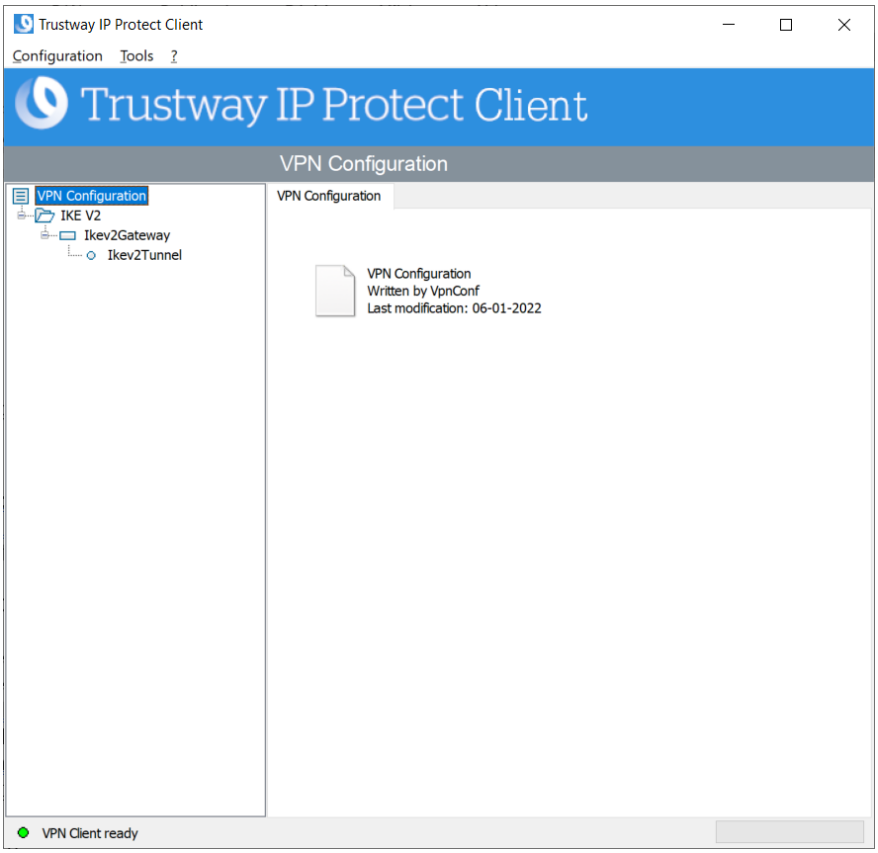
Chapitre 8. Configuration Panel

The **Configuration Panel** is the administrator's interface for IP Protect Client.

It is only accessible if IP Protect Client has been started as Windows administrator (see paragraph Starting IP Protect Client as administrator in section Starting the software above), or for any user if the option **Restrict access to the Configuration Panel to administrator** has been unchecked (not recommended).

It includes the following items :

- A set of menus for VPN configuration and software management;
- The VPN tunnel tree;
- VPN tunnel configuration tabs ;
- A status bar.



8.1 Menus

The following menus are available in the **Configuration Panel**:

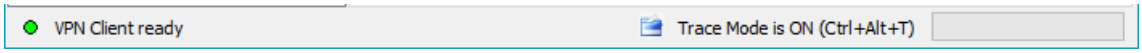
- Configuration
  - Save
  - Import: Import a VPN configuration
  - Export: Export a VPN configuration
  - Move to a USB drive: USB mode

- Configuration Wizard
- Quit: Close all open VPN tunnels and quit the software

- Tools
  - Connection Panel
  - Connections Configuration
  - Console: IKE connection traces window
  - Reset IKE: Restart the IKE service
  - Options: Protection, display, startup, language management, PKI management options
- ?
  - About…

8.2 Status bar

The status bar at the bottom of the main interface displays multiple items:



- The "LED" on the left edge is green when all the software's services are operational (IKE service).
- The text on the left shows the software status (**VPN Client ready**, **Saving configuration**, **Applying configuration**, etc.).
- When the trace mode is enabled, the text "Trace Mode is ON" is shown in the middle of the status bar.
- The  icon, which appears to the left of this text, is a clickable icon that opens the folder containing the log files generated by the trace mode.
- The progress bar on the right side of the status bar shows the progress when saving a configuration.

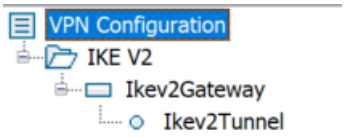
8.3 Shortcuts

CTRL+S	Save the VPN configuration
CTRL+ENTER	Switch to the **Connection Panel**
CTRL+D	Opens the **VPN Console** window
CTRL+ALT+R	Restart the IKE service
CTRL+ALT+T	Enable the trace mode (log generation)

8.4 Tunnel tree

8.4.1 Usage

The left side of the **Configuration Panel** is the tree structure of the VPN configuration. The tree can contain an infinite number of tunnels.



Under the root called "VPN Configuration", there are two levels that allow you to create IPsec IKEv2 tunnels, specified by an IKE Auth and a Child SA, knowing that each IKE Auth can contain more than one Child SA;

Clicking on an IKE Auth, Child SA, or TLS will open the corresponding VPN configuration tabs on the right-hand side of the **Configuration Panel**. See the following sections for further details:

Tunnel IPsec IKEv2

- IKEv2 (IKE Auth) : Authentification
- IKEv2 (Child SA) : IPsec

An icon is associated with each tunnel (Child SA, or TLS). This icon shows the status of the VPN tunnel :

	Tunnel is closed
	Tunnel is being opened
	Tunnel is open
	Incident when opening or closing the tunnel

Edit and change the name of any item in the tree by clicking twice in a row on it, without double-clicking.

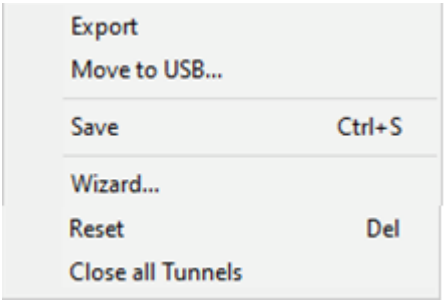
If there are any unsaved changes in the VPN configuration, the modified item is shown in bold. As soon as the tree is saved, all text formatting is removed.

Two items in the tree cannot have the same name. The software displays a message to the user if the name entered is already in use.

8.4.2 Contextual menus

8.4.2.1 VPN configuration

Right clicking the VPN configuration (root of the tree) displays the following contextual menu:



Export	Exports the entire VPN configuration.
Move to USB...	Moves the VPN configuration to a USB drive and initiates USB mode.
Save	Saves the VPN configuration.
Wizard	Opens the VPN Configuration Wizard.
Reset	Resets the VPN configuration after confirmation by the user.
Close all tunnels	Closes all open tunnels.

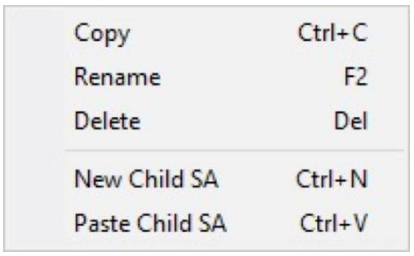
8.4.2.2 IKEv2

Right-clicking the **IKEv2** item will display the following contextual menu, which allows you to export, save, create, or paste an IKE Auth:

Export	Exports all IKEv2 tunnels.
Save	Saves all IKEv2 tunnels.
New IKE Auth	Creates a new IKE Auth. The parameters of this new IKE Auth will be filled in with default values.
Paste IKE Auth	Adds an IKE Auth/TLS that has been previously copied to the clipboard.

8.4.2.3 IKE Auth

Right-clicking an IKE Auth displays the following contextual menu:



Copy	Copies the selected IKE Auth to the clipboard.
Rename[4]	Renames the IKE Auth.
Delete[5]	Deletes the IKE Auth, including any associated Child SAs, after confirmation by the user.
New Child SA	Adds a new Child SA to the selected IKE Auth.
Paste Child SA	Adds the Child SA that has been copied to the clipboard to the IKE Auth.

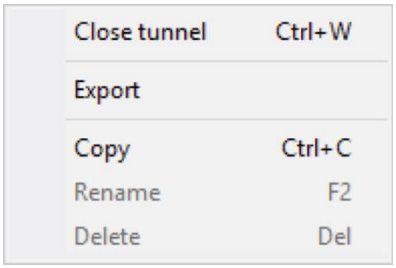
[4] This menu is disabled as long as one of the tunnels of the relevant IKE Auth is open.

[5] ibid

8.4.2.4 Child SA

Right-clicking a Child SA displays the following contextual menu:

Menu with tunnel closed



Menu with tunnel open

Open tunnel	Displayed if the VPN tunnel is closed. Opens the selected Child SA tunnel.
Close tunnel	Displayed if the VPN tunnel is open. Closes the selected Child SA tunnel.
Export[6]	Exports the selected Child SA.
Copy	Copies the selected Child SA.
Rename[7]	Renames the selected Child SA.
Delete[8]	Deletes the selected Child SA after confirmation by the user.

8.4.3 Shortcuts

The following shortcuts are available for tree management:

F2	Used to edit the name of the selected phase
Del	Deletes a selected phase, following confirmation by the user. If the actual VPN configuration is selected (root of the tree), the software asks whether a full reset of the configuration should be performed.
Ctrl+O	Opens the corresponding VPN tunnel if a Child SA is selected.

[6] This function allows users to export the entire tunnel, i.e. both the Child SA and its associated IKE Auth, and thus to create a fully operational, single-tunnel VPN configuration (which becomes immediately functional when imported).

[7] This menu is disabled while the tunnel is open.

[8] ibid

Ctrl+W	Closes the corresponding VPN tunnel if a Child SA is selected.
Ctrl+C	Copies the selected phase to the clipboard.
Ctrl+V	Pastes (adds) the phase that has previously been copied to the clipboard.
Ctrl+N	If the VPN configuration is selected, creates a new IKE Auth. If an IKE Auth is selected, creates a Child SA.
Ctrl+S	Saves the VPN configuration.

Chapitre 9. TrustedConnect Panel

9.1 Introduction

The **TrustedConnect Panel** allows you to permanently keep a secure connection to the trusted network thanks to the following features:

- **TND (Trusted Network Detection)** : Used to determine whether the workstation is within the trusted network based on the DNS suffixes and on beacon identification.
- **Always-On** : Ensures that the connection remains secure whenever the network interface changes, for example, between Ethernet, Wi-Fi and 4G/5G.

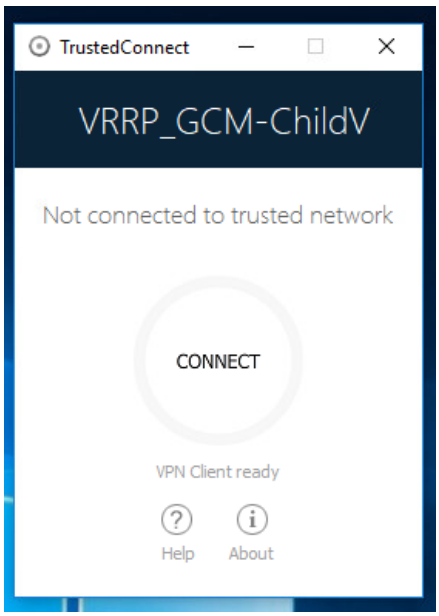
9.2 Interface

When it is used for the first time, the **TrustedConnect Panel** is displayed in the center of the screen.

For subsequent uses, the **TrustedConnect Panel** memorizes the place to which the user has moved it.

The interface of the **TrustedConnect Panel** includes the following items:

- A title that identifies the name of the connection being managed;
- An information message about the connection status ;
- A Connect button;
- A message that indicates the current status of the software and displays possible error codes ;
- A help button that gives access to a document with help for the user;
- An information button that displays essential information about the software;
- A set of icons whose color reflects the connection status.



You can minimize the **TrustedConnect Panel** at any time either to the taskbar, by clicking the **Minimize** button in the title bar, or to the notification area, by clicking on the **Close** button in the title bar.

Conversely, you can display the **TrustedConnect Panel** at any time by clicking the **TrustedConnect** icon in the taskbar or in the notification area.

You can quit the software by right clicking the **TrustedConnect** icon in the notification area and then selecting **Quit**.

9.3 Taskbar icon and color codes

The taskbar icon of the **TrustedConnect Panel** application is slightly different from that of IP Protect Client **Configuration Panel**/**Connection Panel**

The various icons in the **TrustedConnect Panel** have the following meaning :

This state means that the **TrustedConnect Panel** is not managing any connection on the workstation. Generally, this state is encountered when the user explicitly requests the VPN connection to be closed.

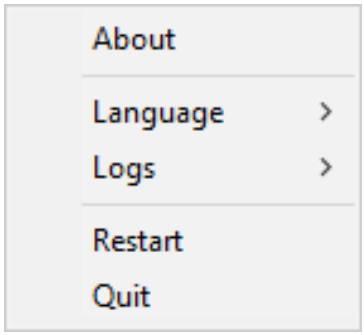
This state means that the workstation is directly connected to the corporate network, which is considered as a trusted network.

This state means that the workstation is connected to the corporate network through a VPN connection. The workstation thus is physically located on a network that is not considered as trusted .

This state means that the VPN connection could not be established.

9.4 Contextual menu

Right clicking the **TrustedConnect Panel** icon in the taskbar opens the contextual menu associated with the icon:



About…	Opens the **About…** window.
Language	Used to switch between French and English.
Logs	Used to start logging. Once logging is started, two additional options are shown to display the logs and stop logging.
Restart	Restarts the tunnel.
Quit	Closes the VPN tunnel and quits the software.

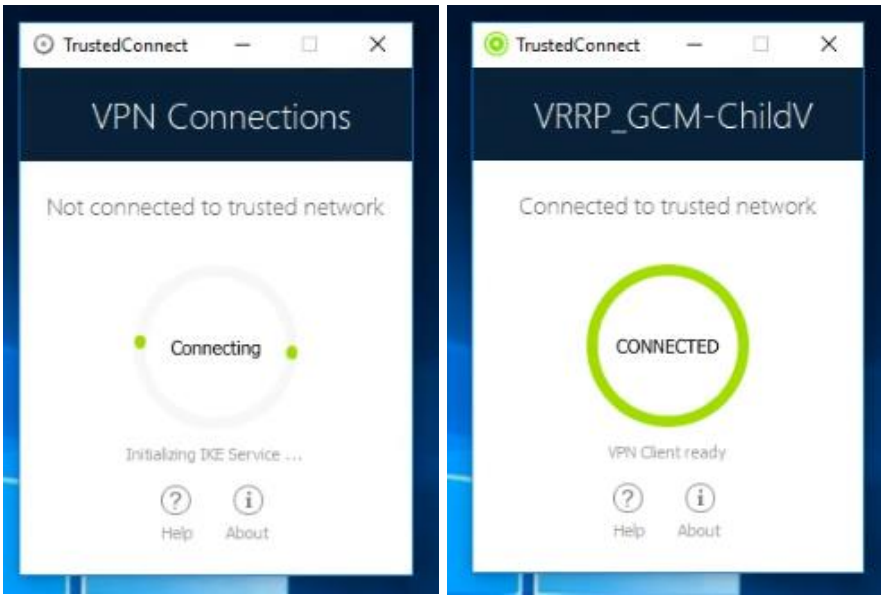
The contextual menu contains the following items:

9.5 Usage

There are two types of use depending on whether the workstation is already connected to the corporate network or not.

9.5.1 Workstation connected to corporate network

The **TrustedConnect Panel** switches to the **CONNECTED** status after having detected trusted networks:



The window of the **TrustedConnect Panel** then automatically minimizes either to the taskbar or to the notification area, depending on the behavior that the administrator has configured.

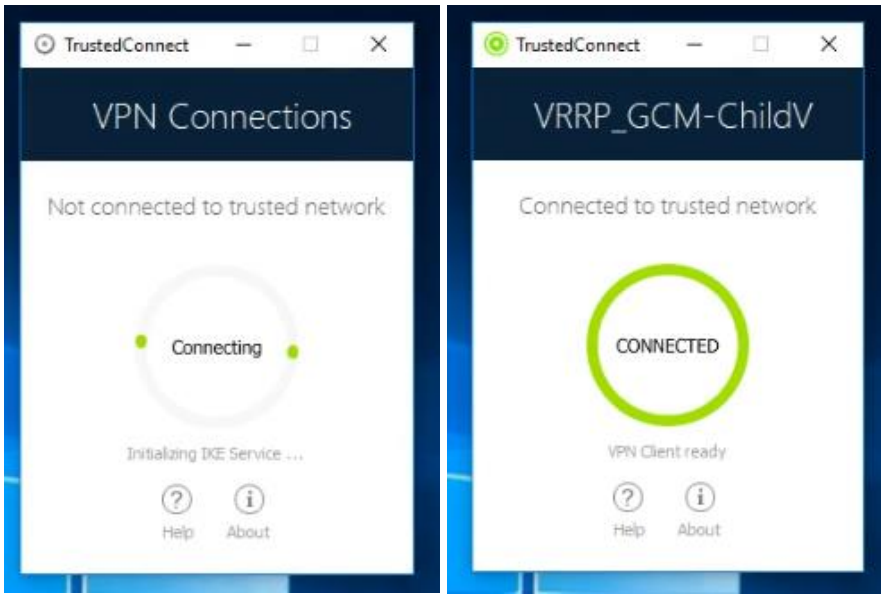
Refer to the “Deployment Guide”.

To display the window again, select the application in the taskbar. When connected to the corporate network, users cannot perform any action on the connection status.

9.5.2 Workstation not connected to corporate network

When switching to a network that is not considered as trusted, the **TrustedConnect Panel** will automatically open the VPN tunnel.

The button’s animation shows the progress of the connection being established until it is established.

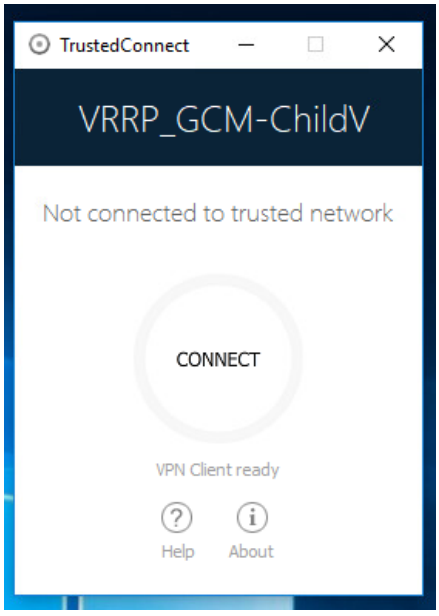


Once the connection is established, the window of the **TrustedConnect Panel** automatically minimizes either to the taskbar or to the notification area, depending on the behavior that the administrator has configured.

The connection may not be established for various reasons. The information message below the button provides a first level of information. The various possible cases of connection failure are detailed in the next section.

When the tunnel is mounted and the workstation is shown as being on the corporate network, you can click inside the connection status indicator ring to stop the tunnel.

The application then switches to the state **Not connected** and you can click the button to manually open the tunnel again:



9.6 Error cases

An orange Connect button, an error code, and a brief message describing the error are shown in the **TrustedConnect Panel** interface to identify the main error cases.

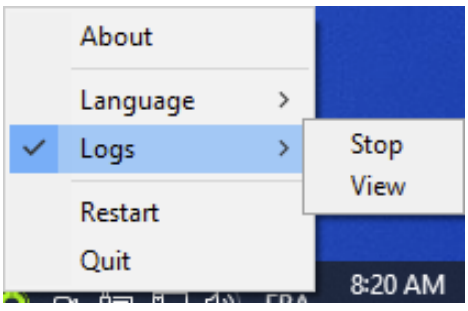
Contact the network administrator to resolve the issue. The error code shown may provide some indication or explanation as to the issue encountered. If the administrator requests the logs, refer to the procedure described in the next section.

The list of error codes is provided in the appendix of this document (see section TrustedConnect Panel diagnostics).

9.7 Generating logs

The **TrustedConnect Panel** allows you to create and view logs.

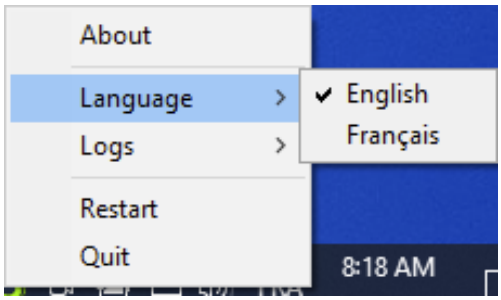
To initiate the creation of log files, right click the **TrustedConnect** icon in the notification area, select **Logs**. A check mark next to the menu item indicates that logging is enabled:



To view the logs, access the system menu and select the item **Access logs**. A window with the log folder is shown with a certain number of files. You can send these files to the administrator when you encounter any issues.

9.8 Selecting the language

The **TrustedConnect Panel** allows you to select the software's display language: French or English. To select the language, access the menu and select the **Languages** item. In the submenu, select **English** or **Français**:



9.9 Current limitations

The **TrustedConnect Panel** (run using the `VpnDialer.exe` executable file) cannot be run at the same time as the **Configuration Panel** or the **Connection Panel** (both run using the `VpnConf.exe` executable file, the desktop shortcut, or the Start menu).

When `VpnConf.exe` is running and you are running `VpnDialer.exe`, all tunnels opened in `VpnConf.exe` will be closed and `VpnDialer.exe` (TrustedConnect) will attempt to automatically launch the configured tunnel.

However, when `VpnDialer.exe` (TrustedConnect) is running, you cannot run `VpnConf.exe` immediately. You must first quit `VpnDialer.exe` before you can run `VpnConf.exe`.

The **TrustedConnect Panel** (`VpnDialer.exe`) is currently only available in French and English.

Chapitre 10. "About…" window

The **About…** window can be accessed as follows:

- Click the**?** menu in the **Configuration Panel** and choose **About…**,
- Use the system menu in the **Configuration Panel**,
- Click the [?] button in the **Connection Panel**,
- Click the [?] button in the **TrustedConnect Panel**.

The **About…** window displays the following information:

- The name and version number of the software;
- When the software is activated, the license number and email used for activation ;
- During the software trial period, the number of days remaining before the trial period expires;
- The version numbers of all software components[9]

[9] You can select and copy the contents of the entire list of version numbers (right-click on the list and choose **Select all**), for example to send the information for analysis purposes. When the **About…** window is open, if IP Protect Client has not been activated, the software tries to connect to the activation server to validate the license.

Chapitre 11. Importing and exporting the VPN configuration

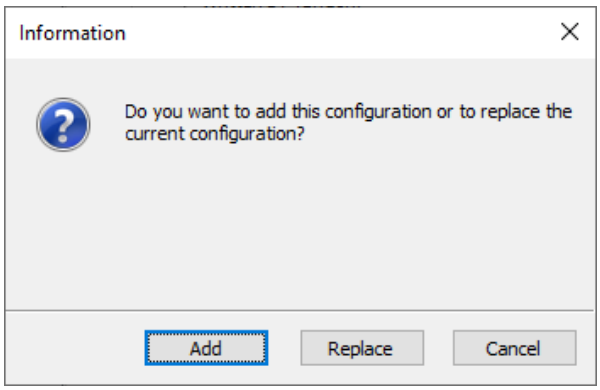
11.1 Importing a VPN configuration

IP Protect Client allows you to import a VPN configuration in various ways :

- From the **Configuration** menu in the **Configuration Panel** (main interface), choose **Import**;
- From the command line, use the /import option[10]

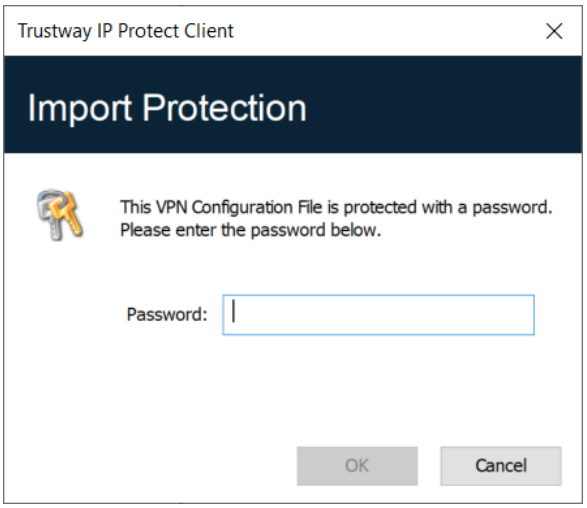
IP Protect Client monitor VPN configuration file integrity. In this case, a signature is generated during export and the integrity of the file is checked during import.

When importing a VPN configuration, users are prompted to specify whether they want to add the new VPN configuration to the current one or replace (overwrite) the current configuration with the new one:



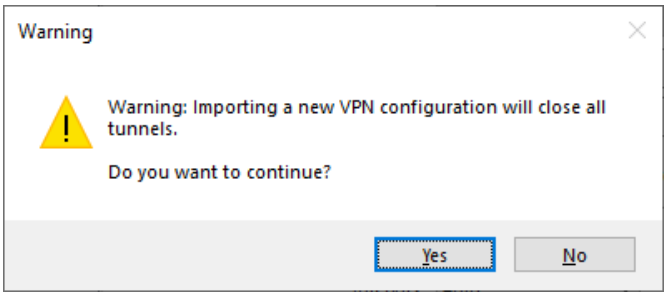
If the imported VPN configuration has been exported with a password protection (see section Exporting a VPN configuration below), users will have to provide the password.

[10] The use of command-line options within the software is covered in the "Deployment Guide". In particular, it details all the options available for importing a VPN configuration: `/import`, `/add`, `/replace` or `/importonce`.



If the VPN configuration is exported with an integritycheck (see section Exporting a VPN configuration below) and it has been corrupted, a warning will be displayed to the user and the software will not import the configuration.

If one or several tunnels are open when importing, the following information window will be displayed to let you know that the import will close all open tunnels:



Once this message has been confirmed and the import has been completed, you will need to reopen the tunnels.

If some of the VPN tunnels added have the same name as certain tunnels in the current configuration, they are automatically renamed during import (an increment will be added between brackets).

11.2 Exporting a VPN configuration

IP Protect Client allows you to export a VPN configuration in various ways:

- From the Configuration menu, choose Export: the complete VPN configuration is exported
- From the contextual menu at the root of the **VPN tree**, choose **Export**: the complete VPN configuration is exported.
- From the contextual menu associated with an **IKE Auth**, choose **Export**: the entire IKE Auth (including all Child SAs it contains) is exported.
- From the contextual menu associated with a **Child SA**, choose **Export**: the Child SA is exported along with the IKE Auth with which it is associated.
- Using the /export option in the command line.[11]

By default, the extension of exported VPN configuration files is `.tgb`.

Whether it is exported with or without encryption, the exported VPN configuration can benefit from integrity protection.
Protecting the integrity of a VPN configuration when it is exported is a feature that can be enabled using an MSI installer property. This function is covered in the “Deployment Guide”.

[11] The use of command-line options within the software is covered in the “Deployment Guide”. In particular, it details all the options available for exporting a VPN configuration: `/export` or `/exportonce`. Regardless of the method used, the export starts with the choice of protection for the exported VPN configuration: it can be exported with (encryption) or without (clear text) password protection. If a password has been set, users will be required to enter it when importing.

We recommend that you always export VPN configurations with a password protection (encrypted).

The password must contain at least 16 characters.

If an exported VPN configuration is integrity-protected, but is corrupted subsequently, a warning will be displayed to the user during the import and the software will not import the configuration (see section Importing a VPN configurationabove).

11.3 Merging VPN configurations

Several configurations can be merged by successively importing all VPN configurations and choosing **Add** each time (see section 11.1 Importing a VPN configuration above).

11.4 Splitting a VPN configuration

Using the various export options available (exporting an IKE Auth with all the corresponding Child SAs or exporting a single tunnel), a VPN configuration can be split into as many "sub-configurations" as desired (see section Exporting a VPN configuration above).

This method can be used to deploy the configurations for a pool of workstations: derive the VPN configurations for each individual workstation from a common VPN configuration prior to sending them to each user for import.

Chapitre 12. Configuring a VPN tunnel

12.1 IPsec IKEv2

IP Protect Client allows you to create and configure IPsec IKEv2 VPN tunnels.

The procedure used to create a new VPN tunnel is described in the previous sections: Configuration Wizard and from VPN configuration to Child SA.

IP Protect allows only to configure IKEv2 tunnels with a certificate.
Refer to section Security recommendations.

12.2 Editing and saving a VPN configuration

IP Protect Client allows you to modify the VPN tunnels and test these modifications "on-the-fly" without saving the VPN configuration.

All unsaved changes in the VPN configuration are clearly shown in the tree, as the name of modified items appears in bold.

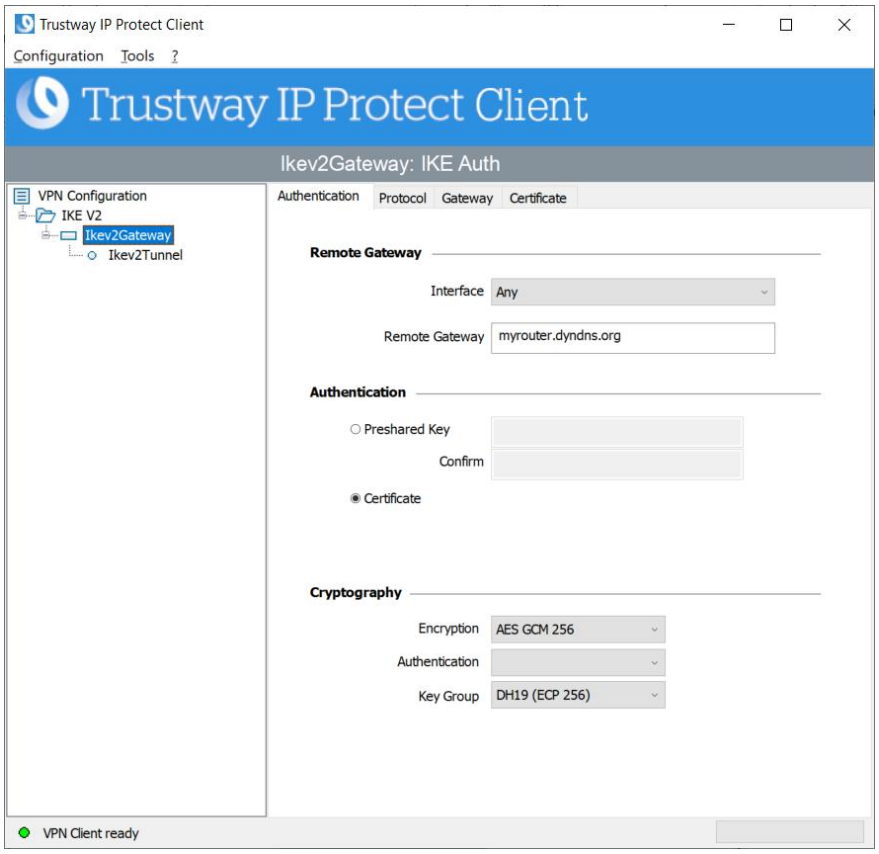
The VPN configuration can be saved at any time using either of the following:

- CTRL+S shortcut,
- **Configuration** > **Save** menu item.

A warning will be displayed if a VPN configuration has been changed and the user tries to quit the software without saving.

12.3 Configuring an IPsec IKEv2 tunnel

12.3.1 IKE Auth : IKE SA



IP Protect allows only to configure IKEv2 tunnels with a certificate.
Refer to section Security recommendations.

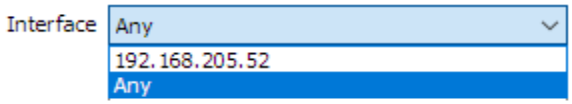
IP Protect only supports IPv4 addresses.

12.3.1.1 Adresses

Interface

Name of the network interface on which the VPN connection is open.

The software can decide automatically which interface to use by selecting **Any** .



We recommend choosing this option if the tunnel being configured is to be deployed on a different workstation.

Remote Gateway

IP (IPv4) or DNS address of the remote VPN gateway.

This field is mandatory.

12.3.1.2 Authentication

Preshared key Password or key shared by the remote gateway.

IP Protect does not allow authentification with Preshared key. Refer to section Security recommendations.

Certificate Use a certificate to authenticate the VPN connection.

Using the **Certificate** option strengthens the security in terms of VPN connection management (mutual authentication, verification of validity periods, revocation, etc.).
Refer to section Security recommendations.

Refer to the dedicated section Managing certificates

EAP

IP Protect does not allow authentification with EAP.
Refer to section Security recommendations.

Multiple AUTH Support

Not supported by IP Protect. Refer to section Security recommendations.

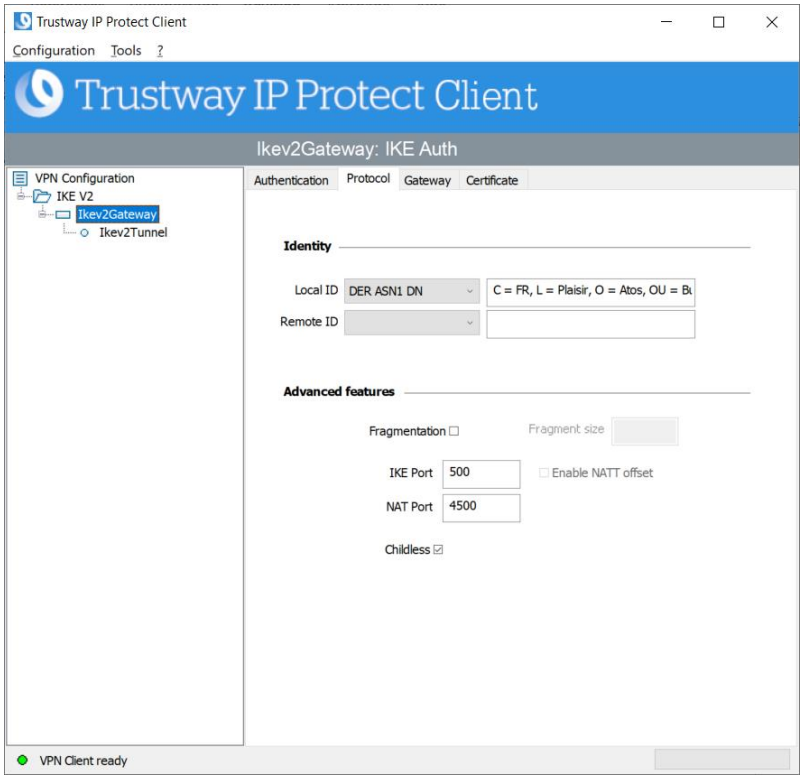
12.3.1.3 Cryptography

Encryption Encryption algorithm negotiated during the authentication phase:
AES GCM (256)

Authentification Authentication algorithm negotiated during the authentication phase:
SHA2 256.

Key group Length of Diffie-Hellman key :
DH19 (ECP 256).

12.3.2 IKE Auth : Protocol



12.3.2.1 Identity

Local ID

"Local ID" is the identifier that IP Protect Client sends to the remote VPN gateway during the authentication phase.

According to the type selected, this identifier can be any of the following:

- DER ASN1 DN: the X.509 subject of a certificate (type = DER ASN1 DN)
- X509 subject: this field is automatically filled in with the subject of an X.509 certificate when the tunnel is associated with a user certificate (see section Managing certificates)

This parameter is mandatory.

Remote ID

"Remote ID" is the identifier of the authentication phase that IP Protect Client expects to receive from the IP Protect gateway.

According to the type selected, this identifier can be any of the following:

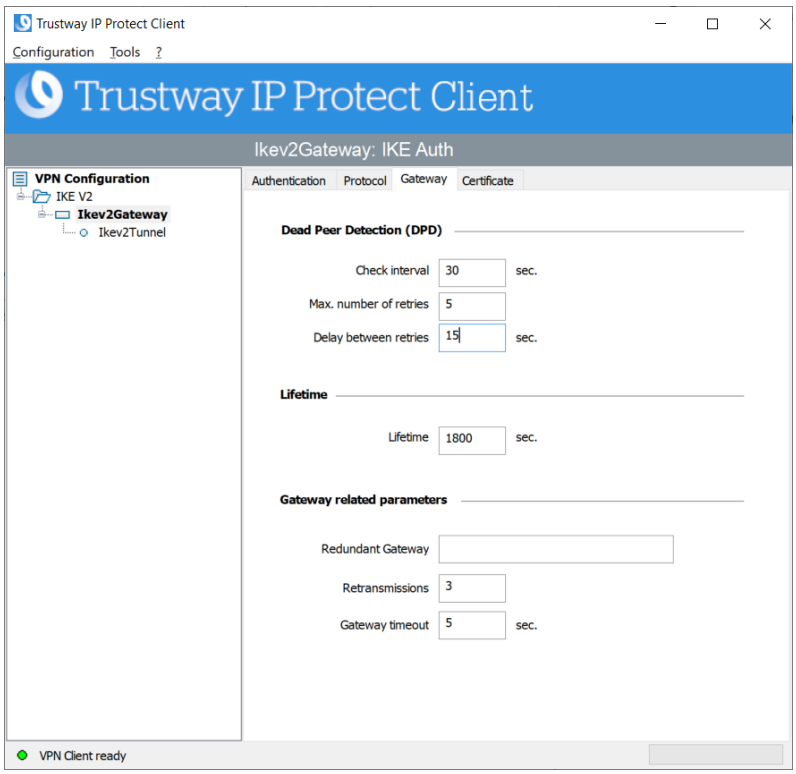
- DER ASN1 DN: the X.509 subject of a certificate (type = DER ASN1 DN). Be careful to respect the order of the fields in the IP Protect gateway certificate subject.

This parameter is mandatory.

12.3.2.2 Advanced functions

IKEv2 fragmentation	Enables IKEv2 packet fragmentation in accordance with RFC 7383. This option must not be checked.
IKE Port	The IKE port must be set to 4500.
NAT Port	The NAT port must be set to 4500.
Enable NATT offset	This option must be checked.
Childless	This option must be checked.

12.3.3 IKE Auth : Gateway



12.3.3.1 Dead Peer Detection (DPD)

Check interval

The Dead Peer Detection (DPD) function enables IP Protect Client to detect whether the IP Protect gateway has become unreachable or inactive.[12]

The check interval is the time period between two consecutive DPD check messages sent, expressed in seconds.

Max. number of retries

Number of consecutive unsuccessful attempts before concluding that the IP Protect gateway is unreachable.

Delay between retries

Time between two DPD messages when IP Protect gateway is not responding, expressed in seconds.

[12] The DPD function is enabled upon opening the tunnel (after the authentication phase). When linked to a redundant gateway, DPD allows IP Protect Client to automatically switch between gateways when one of them is unavailable.

12.3.3.2 Lifetime

Lifetime	Lifetime of the IKE Authentication phase. The lifetime is expressed in seconds. The default value is 14,400 seconds (4 h).

12.3.3.3 Gateway-related parameters

Passerelle redondante	The address of the redundant VPN gateway can be either an IP or a DNS address. Refer to section Redundant gateway.
Retransmissions	Number of IKE protocol message resends before failure.
Gateway timeout	Delay between two retransmissions

12.3.4 IKE Auth : Certificate

Refer to section Managing certificates.

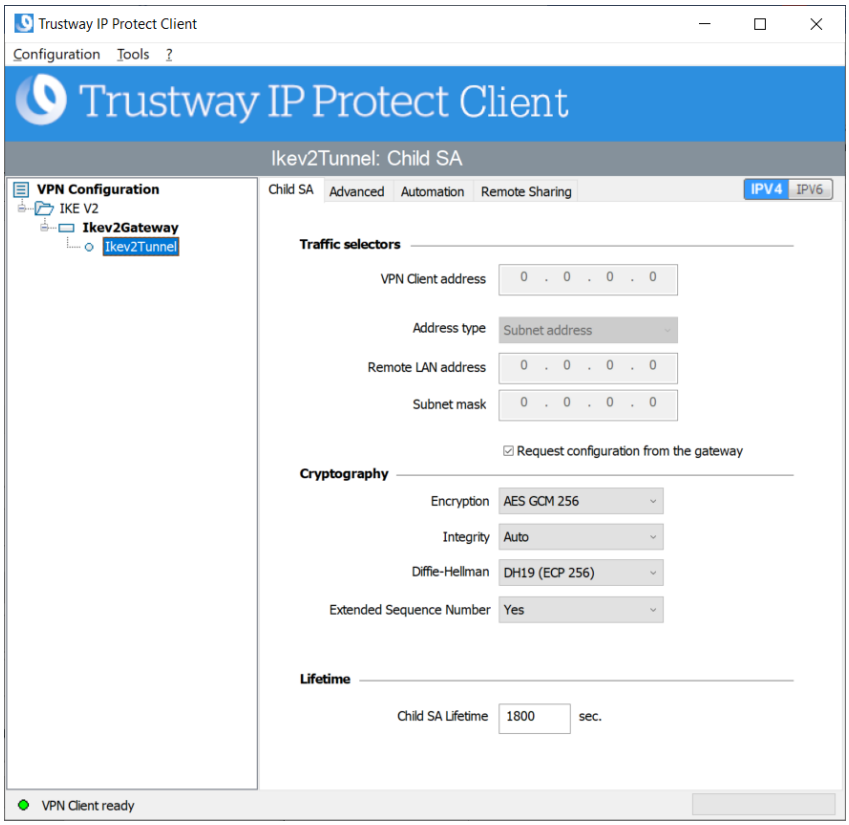
12.3.5 Child SA : Overview

The purpose of the "Child SA" (Security Association IPsec) of a VPN tunnel is to negotiate the security parameters that will be applied to the data going through the VPN tunnel.

To configure Child SA parameters, select the Child SA in the VPN tree on the **Configuration Panel**. The parameters can be configured in the right-hand tabs of the **Configuration Panel**.

If any changes are made to a tunnel, it will appear in bold in the VPN tree. You do not need to save a VPN configuration for it to be taken into account. The tunnel can be tested with the modified configuration immediately.

12.3.6 Child SA : Child SA



12.3.6.1 Traffic selectors

VPN Client address Greyed because the box « Request configuration from the gateway » must be checked.

Address type Greyed because the box « Request configuration from the gateway » must be checked.

Request configuration from the gateway This box must be checked.

12.3.6.2 Cryptography

Encryption Encryption algorithm negotiated during the IPsec phase :

Must be : AES GCM (256).

Integrity Authentication algorithm negotiated during the IPsec phase :

Must be : AES GCM (256).

Diffie-Hellman Length of Diffie-Hellman key :

Must be : DH19 (ECP 256).

Extended Sequence Number Allows you to use 64-bit extended sequence numbers (see RFC 4304) :

Must be : Yes.

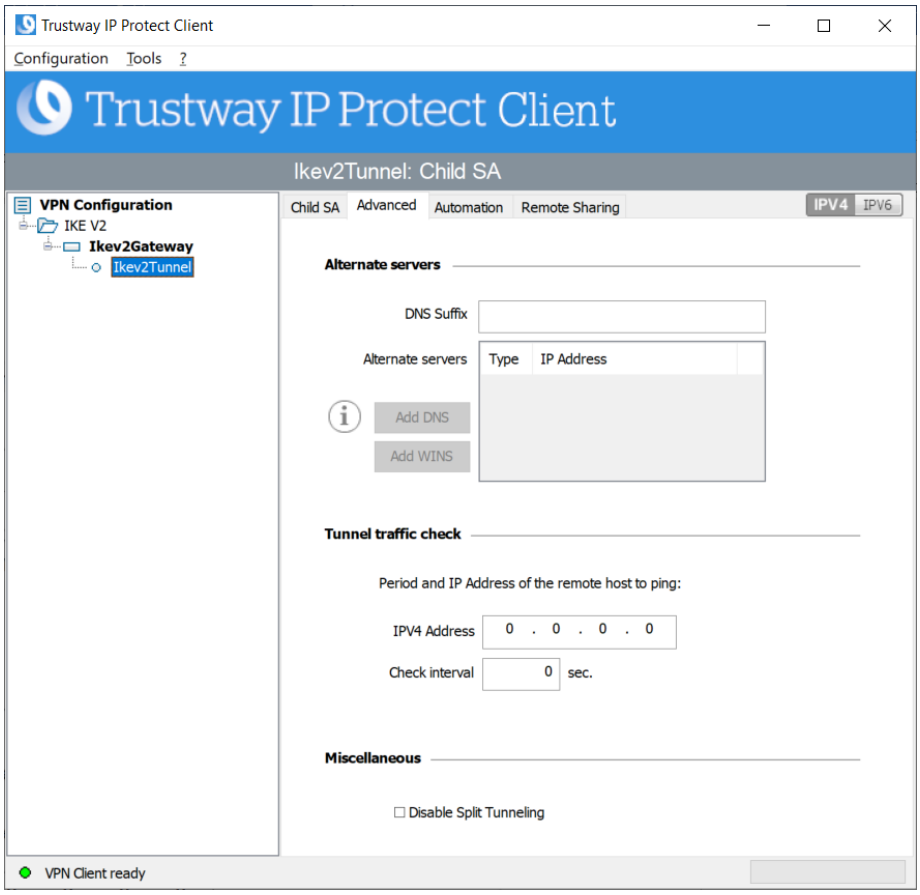
If the IP address of IP Protect Client workstation is included in the address range for a remote network (e.g. @workstation IP=192.168.10.2 and @remote network=192.168.10.x), then opening a tunnel will prevent the workstation from communicating on the local network. All communications will go through the VPN tunnel.

12.3.6.3 Lifetime

Child SA Lifetime Time interval, expressed in seconds, between two renegotiations.

The default value for the Child SA lifetime is 1,800 s (30 min).

12.3.7 Child SA : Advanced



12.3.7.1 Alternate servers

DNS Suffix

Domain suffix to be added to all machine names, e.g. `mozart.dev.atos`.

This is an optional parameter. When it is specified, IP Protect Client will try to translate the machine address without adding the DNS suffix. However, if translation fails, the DNS suffix will be added, and the Client will try to translate the address again.

Alternate servers

Table containing the IP addresses of the DNS (maximum 2) and WINS (maximum 2) servers available on the remote network.

When Mode CP is enabled (see the **Request configuration from the gateway** parameter in the **Child SA** tab), these fields will be grayed out (uneditable). They are automatically filled in as the tunnel is opened with the values sent by the VPN gateway during the Mode CP exchange.

12.3.7.2 Tunnel traffic check

Traffic check after opening

IP Protect Client can be configured so that connectivity to the remote network is checked on a regular basis. If connectivity has been lost, IP Protect Client will automatically close the tunnel and attempt to open it again.

The **IPV4** field is the address of a machine within the remote network, which should reply to pings sent by IP Protect Client. If a ping goes unanswered, the connection is considered lost.

The tunnel must be configured in IPv4 (button at the top right of the tab).

Check interval

The **Check interval** indicates the time interval in seconds between two pings sent by IP Protect Client to the machine with the IP address specified above.

12.3.7.3 Miscellaneous

Disable Split Tunneling	When this option is selected, only the traffic going through the tunnel is authorized.[13]

12.3.8 Child SA : Automation

?? Refer to section Automation

.

12.3.9 Child SA : Remote sharing

?? Refer to section Remote Desktop Sharing.

[13] The **Disable Split Tunneling** configuration option increases the "leakproofness" of the workstation, provided that the VPN tunnel is open. More specifically, this function eliminates the risk of incoming data flows that do not go through the VPN tunnel. When combined with the **All traffic through the VPN tunnel** configuration (see section **Erreur ! Source du renvoi introuvable. Erreur ! Source du renvoi introuvable.**), this option guarantees the complete leakproofness of the workstation, provided that the VPN tunnel is open. We recommend using this mode.

Chapitre 13. Redundant gateway

IP Protect Client can be used to manage a redundant IP Protect gateway.

When combined with Dead Peer Detection (DPD) settings, this function allows IP Protect Client to automatically switch to the redundant gateway as soon as the main gateway is detected as being down or unavailable.

If the DPD is lost and a redundant gateway has been configured, the tunnel will automatically try to open again. You can configure a redundant gateway that is identical to the main one, in order to benefit from the automatic reopening mode without actually having to use two gateways.

The algorithm for taking into account the redundant gateway is as follows:

- IP Protect Client contacts the initial gateway to open the VPN tunnel.
- If the tunnel cannot be opened after N attempts, IP Protect Client contacts the redundant gateway.

The same algorithm applies to the redundant gateway:

- If the redundant gateway is unavailable, IP Protect Client will try to open the VPN tunnel with the initial gateway.

IP Protect Client will not try to contact the redundant gateway if the initial gateway can be reached, but issues are experienced when opening the tunnel.

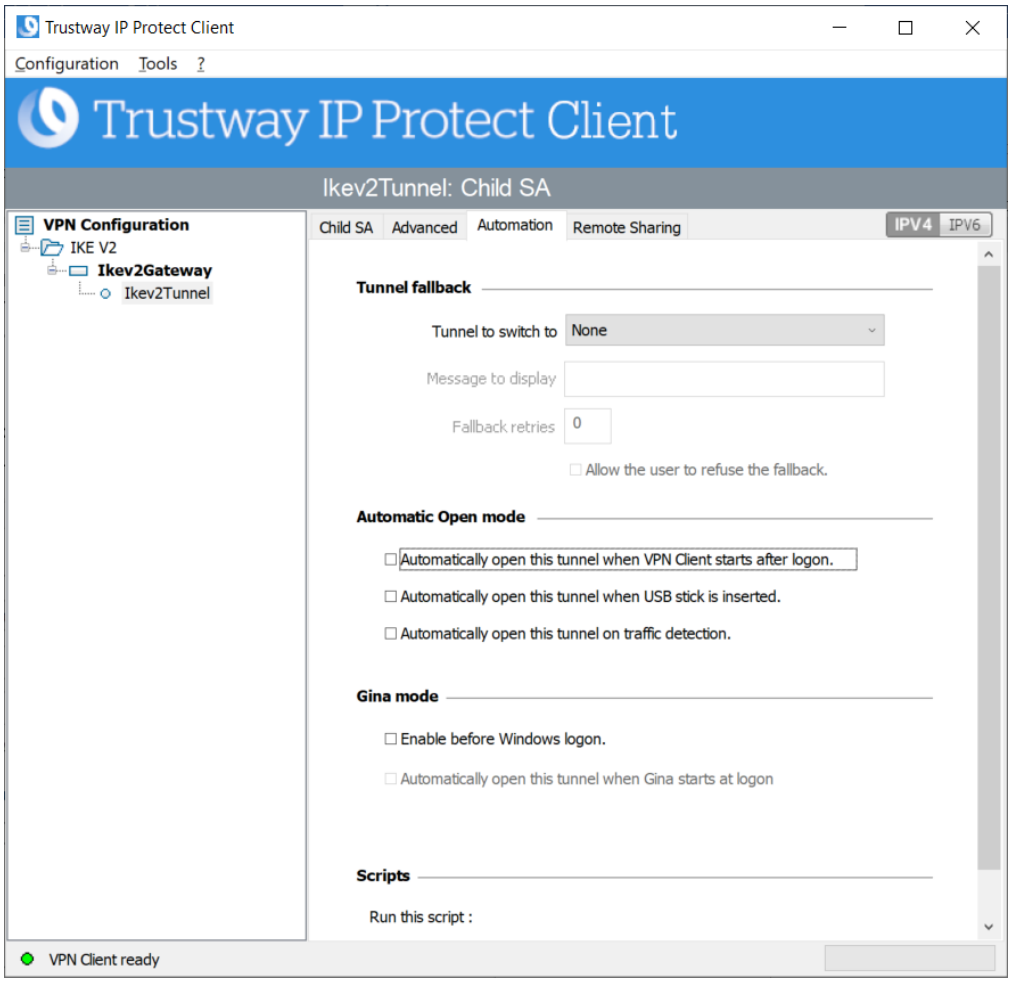
IP Protect Client will not try to contact the redundant gateway if the initial gateway cannot be reached due to a DNS resolution issue.

The IP Protect gateway offers a redundancy solution based on the VRRP protocol for communications between encryptors. Redundant gateways in a VRRP group use the same address which is the IPsec address of the VRRP group. It is therefore necessary to indicate the IPsec address of the VRRP group as the gateway address and this same IPsec address as the redundant gateway address.
When DNS is used, the same DNS address that represents the IPsec address of the VRRP group must also be used.

Chapitre 14. Automation

IP Protect Client can perform automated actions for each VPN tunnel, such as switching to a fallback tunnel, opening the tunnel automatically if certain criteria are met, running batches or scripts at various stages while opening or closing a tunnel, etc.

These automated actions are configured for each tunnel type on the **Automation** tab of the corresponding tunnel.



14.1 Tunnel fallback

☞ Refer to section Tunnel fallback .

14.2 Automatic Open mode

Automatically open this tunnel when VPN Client starts after logon	The tunnel will automatically open when IP Protect Client is started
Automatically open this tunnel when USB stick is	If the tunnel is part of a configuration on a USB drive (see section USB mode), it will automatically be opened when

inserted	the USB drive is inserted. If the tunnel is configured with a certificate stored on a smart card or token, it will automatically be opened when the smart card or token is inserted.
Automatically open this tunnel on traffic detection	The tunnel will automatically open when traffic is detected that is heading towards an IP address on the remote network.

14.3 GINA mode

Enable before Windows logon	This option specifies that the VPN connection can be opened before the Windows logon: it appears in the GINA connections window (refer to section GINA mode below).
Automatically open this tunnel when GINA starts at logon	When this option is enabled, the tunnel will automatically open before the Windows logon. This option is enabled if the option **Enable before Windows logon** is selected.

14.4 Scripts

Before tunnel opens	The specified command line is executed before the tunnel opens.
When tunnel is opened	The specified command line is executed as soon as the tunnel is open.
Before tunnel closes	The specified command line is executed before the tunnel closes.
After tunnel is closed	The specified command line is executed as soon as the tunnel is closed.

The command lines can be as follows:

- Calling a "batch" file, e.g. `C:\vpn\batch\script.bat`
- Running a program, e.g. `C:\Windows\notepad.exe`
- Opening a web page, e.g. `https://my.site`
- etc.

There are many possible applications, such as the following:

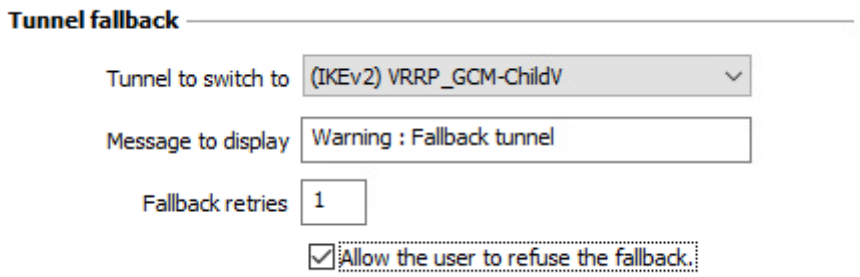
- Creating a semaphore file when the tunnel is open, so that a third-party application can detect the instant when the tunnel is open
- Opening one of the company's intranet servers automatically once the tunnel is open
- Cleaning or checking a configuration before opening the tunnel
- Checking the workstation (antivirus is up-to-date, correct versions of applications, etc.) before opening the tunnel
- Automatic cleaning (file deletion) of a workspace on the workstation before closing the tunnel
- Application for counting openings, closings, and durations of VPN tunnels
- Changing the network configuration, once the tunnel has been opened, then restoring the initial network configuration once the tunnel has been closed
- etc.

Scripts cannot be configured for a tunnel configured in GINA mode.
Data entry fields are disabled.

Chapitre 15. Tunnel fallback

IP Protect Client is equipped with a fallback tunnel function, which automatically attempts to open a second tunnel if the first one cannot be opened.

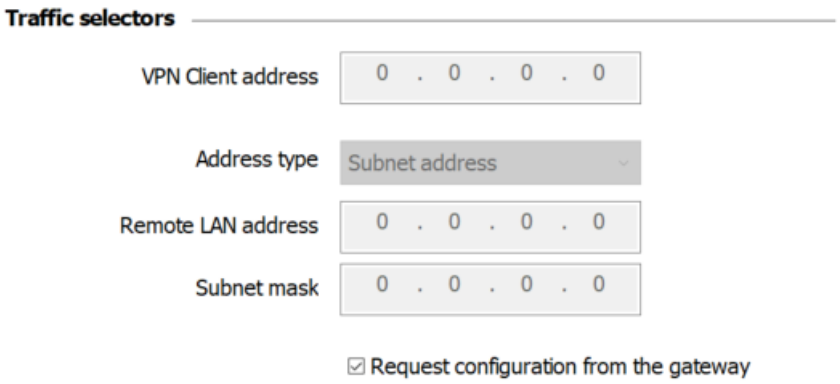
This function can be configured on the **Automation** tab of each tunnel IKEv2.



Tunnel to switch to	This field displays the list of tunnels to which the software can automatically switch if the current tunnel is unavailable.
Message to display	As this function can automatically switch from one tunnel to another, with the second being, for example, less secure than the first, this option is used to display a warning message to the user. This message will be displayed every time the connection switches to the fallback tunnel.
Max. number of retries	The number of fallback attempts is set to avoid infinite switching loops (tunnel 1 falling back to tunnel 2 falling back in turn to tunnel 1).
Allow the user to refuse the fallback	Used to configure the fallback function so that the user gets to decide whether to fall back from one tunnel to another.

Chapitre 16. IPv4 et IPv6

IP Protect Client only supports IPv4 addressing.



Chapitre 17. Managing certificates

17.1 Introduction

IP Protect Client includes a selection of interfacing functions with all types of certificates, issued by any PKI, and on any type of storage device, such as smart card, token, certificate store, and configuration file.

More specifically, IP Protect Client implements the following features:

- Automatic selection of the medium to use from among several
- PKCS#11 and CNG access to tokens and smart cards
- Selection of certificates to use according to multiple criteria: subject, key usage, etc.
- Management of certificates on user's side (IP Protect Client's side), such as VPN gateway certificates, including validity date, certificate chain, root certificate, intermediate certificate, and CRL management
- Certification authority management (Certificate Authority: CA)
- Option to pre-configure all PKI parameters for automatic integration during installation

IP Protect Client provides additional security features for PKI management, such as automatically opening or closing a tunnel upon insertion or removal of a smart card or token, or even the ability to configure the PKI interface in the software setup file in order to automate deployment.

The certificates to be used are configured and specified in three steps as follows:

1. The **Certificate** tab of the relevant tunnel.
5. The **PKI Options** tab of the **Tools** > **Options** window in the **Configuration Panel**.
6. A configuration file for smart card readers and tokens: `vpnconf.ini`—refer to the "Deployment Guide".

Only available certificates that have not expired are displayed.

17.2 User certificate

IP Protect Client sends the user certificate to IP Protect gateway so that it can authenticate the user.

It must comply with the following constraints (ANSSI security recommendations):

- The Key Usage extension must be present, marked as critical, and only contain the value digitalSignature.
- The Extended Key Usage extension must be present, marked as critical, and only contain the value id-kp-clientAuth.

If these constraints are not observed, IP Protect Client will display a warning in the console but will not prevent communication with the gateway. However, the gateway should refuse the authentication of IP Protect Client.

17.3 Selecting a certificate (Certificate tab)

IP Protect Client can assign a user certificate to a VPN tunnel.

There can only be one certificate per tunnel, but each tunnel can have its own certificate.

IP Protect Client allows you to choose a stored certificate:

- In the VPN configuration file (see below Importing a certificate to the VPN configuration)
- In the Windows Certificate Store (see below Windows Certificate Store)
- On a smart card or token (see below Using a certificate stored on a smart card or token)

The **Certificate** tab for the relevant tunnel lists all accessible storage media that contain certificates.

- The smart card or token is compatible with CNG or PKCS#11
- The smart card or token middleware is correctly installed on the computer
- Where appropriate, the smart card is correctly inserted into the corresponding reader

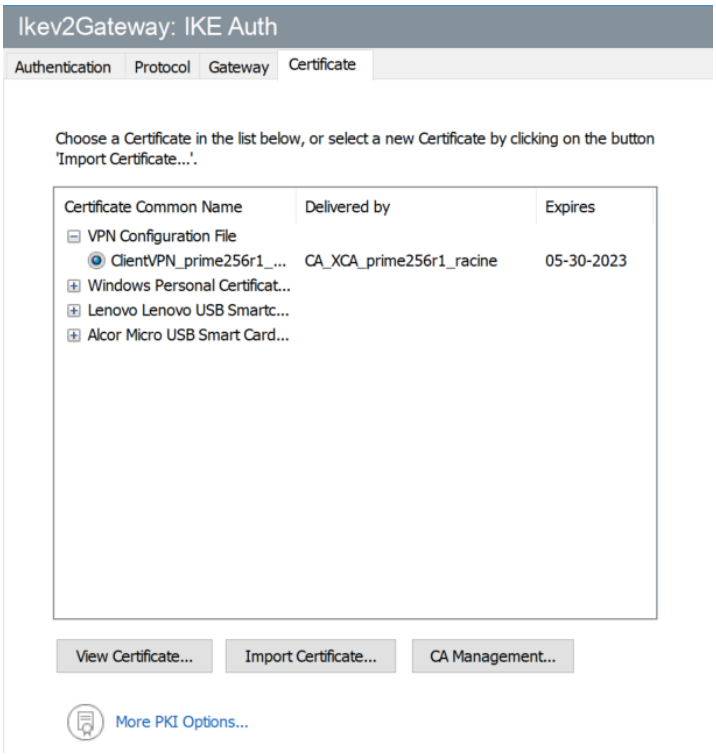
If a medium does not contain any certificates, it simply will not appear in the list (e.g. if the VPN configuration file does not contain any certificates, it will not appear in the list).

Clicking the desired medium displays the list of certificates it contains.

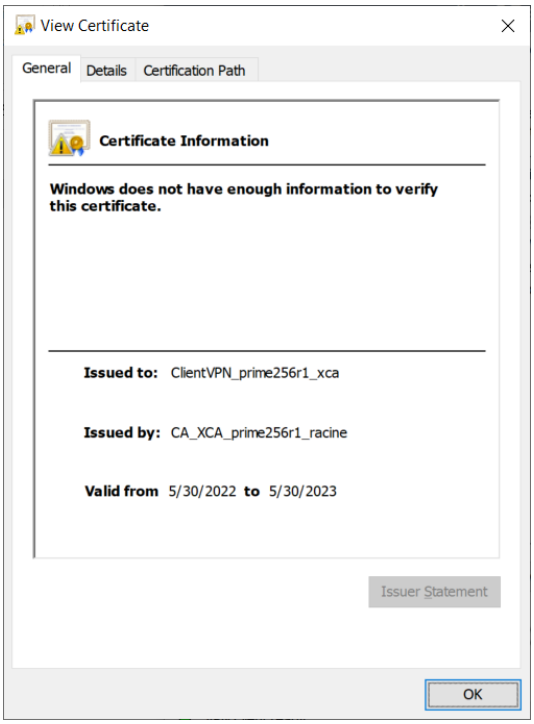
Click the desired certificate to assign it to the VPN tunnel.

Only available certificates that have not expired are displayed.

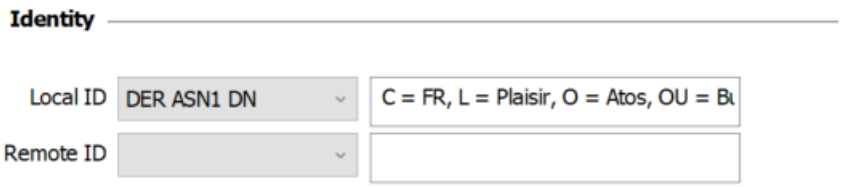
For smart cards readers, the reader is displayed with a warning icon in front, if the smart card is not inserted.



Once a certificate has been selected, the **View Certificate** button will show detailed information about the certificate.



Once a certificate has been selected, the tunnel's Local ID type will automatically switch to **X509 subject** or "DER ASN1 DN" and the certificate's subject will be used as the default value of this **Local ID**.



17.4 Importing a certificate to the VPN configuration

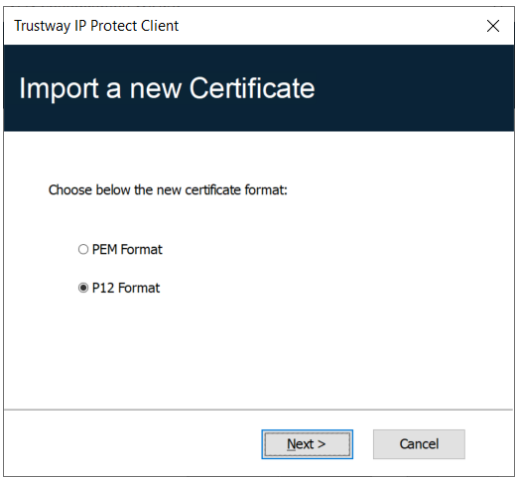
IP Protect Client can import certificates in PEM/PFX or PKCS#12 format to the VPN configuration. This solution is less secure than using the Windows Certificate Store, a smart card, or a token, but it makes it easier to transport certificates.

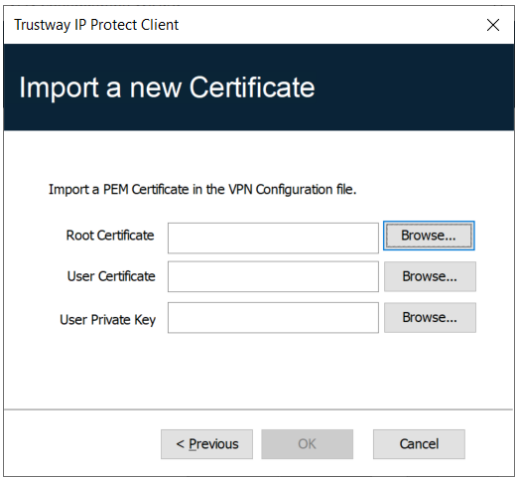
This solution has the advantage of combining the certificate (user-specific) and the VPN configuration (generic) in a single file, which can easily be sent to the user's workstation and imported into IP Protect Client.

Nevertheless, the disadvantage of transporting certificates in a VPN configuration is that each configuration then becomes user-specific. We therefore do not recommend this solution for a substantial deployment.

17.4.1 Importing a PEM certificate

1. On the **Certificate** tab of an IKE Auth, click **Import Certificate…**.
2. Choose **PEM Format**.
3. Click **Browse** to select the **Root Certificate** and the **User Certificate** as well as the **User Private key** to import.
4. Confirm.





The certificate is shown and is selected in the certificate list displayed on the **Certificate** tab.

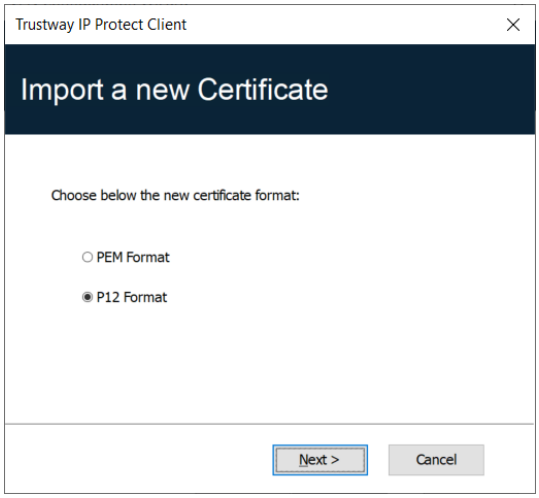
Save the VPN configuration. The certificate will be saved in the VPN configuration.

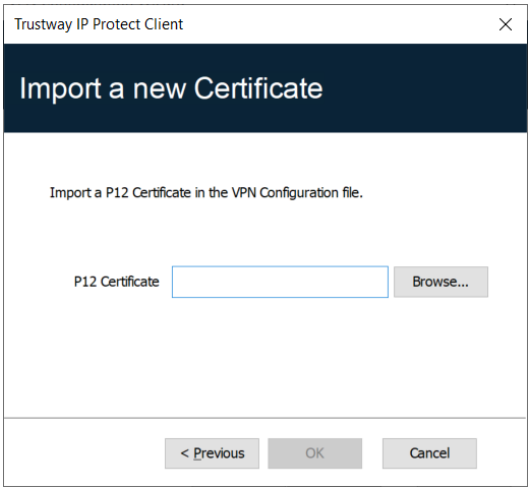
As soon as a certificate is imported into a VPN configuration, it is strongly recommended when exporting the configuration file, to protect it with a password (see section Exporting a VPN configuration), to prevent the certificate is clearly visible

17.4.2 Importing a PKCS#12 certificate

1. On the **Certificate** tab of a Child SA, click **Import Certificate…**.
2. Choose **P12 Format**.
3. Click **Browse** to select the PKCS12 certificate to import.
4. If it is password-protected, enter the password and confirm.

The file containing the private key may not be encrypted.





The certificate is shown and is selected in the certificate list displayed on the **Certificate** tab.

Save the VPN configuration. The certificate will be saved in the VPN configuration.

All CAs in the file that are in PKCS#12 format will also be imported to the VPN configuration.

17.5 Using a certificate stored on a smart card or token

When a VPN tunnel is configured to use a certificate stored on a smart card or token, users will be prompted for the PIN code required to access this smart card or token every time a tunnel is opened.

If the smart card is not inserted or the token cannot be accessed, the tunnel will not open.

If the certificate found does not meet the configured criteria (see section PKI options: specifying the certificate and its storage device above), the tunnel will not open.

If an incorrect PIN code is entered, IP Protect Client will show a warning, informing users that they only have three (in most cases) consecutive attempts to unlock the smart card or token.

IP Protect Client implements a mechanism to automatically detect smart card insertion.

Tunnels that are associated with a certificate stored on a smart card will therefore be established automatically when the smart card is inserted. Likewise, removing the smart card will close all the corresponding tunnels.

To implement this function, check **Automatically open this tunnel when a USB stick is inserted** (see section Automation).

17.6 Using a certificate stored in the Windows Certificate Store

For the IP Protect Client to identify a certificate available in the Windows Certificate Store, the certificate must meet the following criteria:

- The certificate must be certified by a certification authority (which excludes self-signed certificates,
- By default, the certificate must be located in the "Personal" Certificate Store (it represents the personal identity of the user who wants to open a VPN tunnel to the corporate network) To use the Windows Machine Certificate Store, the MACHINESTORE property must be set to 1 when installing the software.

Refer to the "Deployment Guide" for the corresponding instructions.

Microsoft provides a standard management tool (`certmgr.msc`) to manage the certificates in the Windows Certificate Store. To run this tool, go to the Windows **Start** menu and then enter `certmgr.msc` in the **Search for programs or files** field.

17.7 PKI options: specifying the certificate and its storage device

IP Protect Client provides several ways in which to specify the certificate to use, as well as to select the smart card reader or token that contains the certificate.

This feature is available under the **More PKI options** link at the bottom of the **Certificate** tab and on the **PKI options** tab of the **Options** configuration window.

17.8 VPN gateway certificate

We recommend forcing the IP Protect Client to check the certificate chain of the certificate received from the IP Protect gateway (default behavior).

See section Certificate Check.

To do this, you need to import the root certificate and all certificates in the certificate chain (root certification authority and intermediate certification authorities) to the configuration file.

If the option is checked, IP Protect Client will also use the Certificate Revocation List (CRL) of the various certification authorities.

If these CRLs are not in the certificate store, or if these CRLs cannot be downloaded when the VPN tunnel is opened, IP Protect Client will not be able to validate the gateway certificate.

Checking each item in the chain implies the following:

- Checking gateway certificate expiration date
- Checking certificate validity start date
- Checking signatures of all certificates in the certificate chain (including root certificate, intermediate certificates, and server certificate)
- Checking whether the CRLs of all certificate issuers within the chain of trust.

17.8.1 Constraints on the Key Usage extension

The gateway certificate must comply with the following constraints on the Key Usage extension. It must:

- Be present
- Be marked as critical, and
- Only contain the values digitalSignature and/or keyEncipherment

In the event that the IP Protect gateway does not comply with the constraints on the Key Usage extension mentioned above, you can configure IP Protect Client so that it validates the certificate despite this, by adding the dynamic parameter `allow_server_extra_keyusage` set to the value `true`.

In this configuration, the certificate will also be validated if the Key Usage extension contains one of the following combinations of values:

- digitalSignature + keyEncipherment + keyAgreement
- digitalSignature + keyAgreement
- nonRepudiation
- nonRepudiation + keyEncipherment
- nonRepudiation + keyEncipherment + keyAgreement
- nonRepudiation + keyAgreement
- keyEncipherment + keyAgreement

Moreover, in this configuration the Key Usage extension can be marked as non-critical.

17.8.2 Constraints on the Extended Key Usage extension

The gateway certificate must comply with the following constraints on the Extended Key Usage extension. It must:

- Be present
- Be marked as non-critical, and
- Only contain the value id-kp-serverAuth

In the event that the IP Protect gateway does not comply with the constraints on the Extended Key Usage extension mentioned above, you can configure IP Protect Client so that it validates the certificate despite this, by adding the dynamic parameter `allow_server_and_client_auth` set to the value `true`.

In this configuration, the certificate will also be validated if the Extended Key Usage extension contains the following combination of values:

- id-kp-ServerAuth + id-kp-ClientAuth

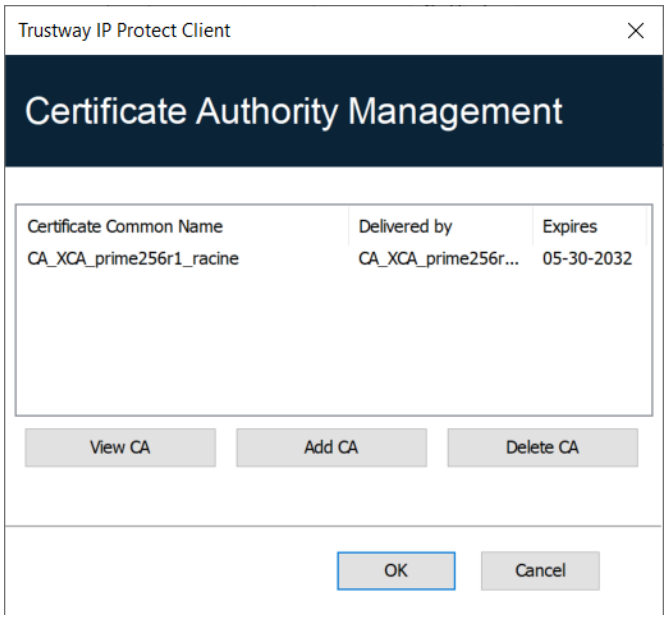
17.9 Managing certification authorities

If IP Protect Client is configured to check the client and gateway certificates, you may need to import Certification Authorities (CAs) in addition to the certificates used.

This is particularly the case any time the software is unable to find the gateway certificate's CA locally, i.e. in the following situations:

1. The gateway certificate's CA is different from the client's, and this gateway CA is not available/accessible on the workstation.
2. The gateway certificate's CA is the same as the client's, but the client's CA is stored on a smart card or token. In this case, the software cannot access it.

For security reasons, the Windows Certificate Store may not be used to access CAs.



1. In the **Certificate Authority Management** window, click **Add CA**.
2. Choose the desired CA certificate type (PEM or DER).
3. Click **Browse** and then select the CA to import.

17.10 Certificate authentication methods

IP Protect Client supports the following certificate authentication methods:

- Method 9 : ECDSA with SHA-256 on the P-256 curve [RFC4754]

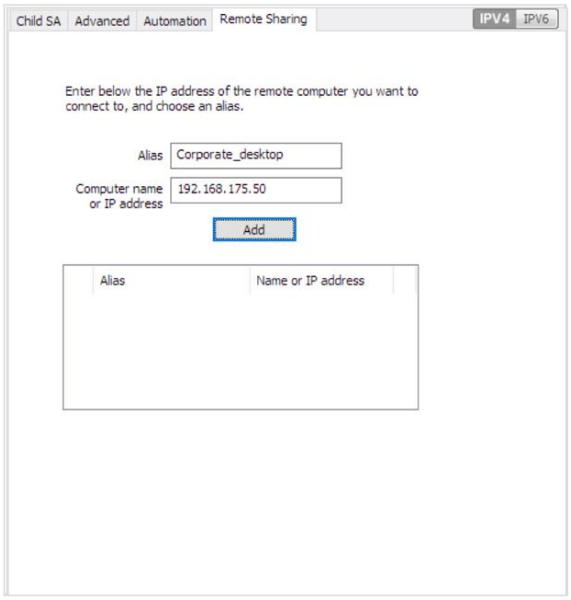
Chapitre 18. Remote Desktop Sharing

Opening a "Remote desktop" session on a Windows computer over the internet usually requires that you establish a secure connection and enter the connection parameters (address of the remote computer, etc.).

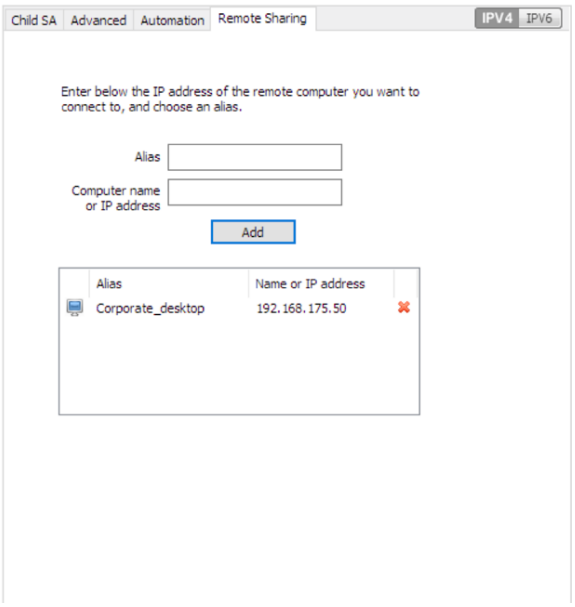
IP Protect Client allows you to simplify and automatically secure the opening of a Remote Desktop session: The VPN connection to the remote workstation is established and the Remote Desktop Protocol (RDP) session automatically opens on this remote workstation with a single click.

To set up Remote Desktop Sharing, proceed as follows:

1. Select the VPN tunnel in which the "Remote desktop" session will be opened.
2. Select the **Remote Sharing** tab.
3. Enter an alias for the connection (the name will be used to identify the connection in the various software menus), then enter the IP address or the Windows name of the remote workstation.



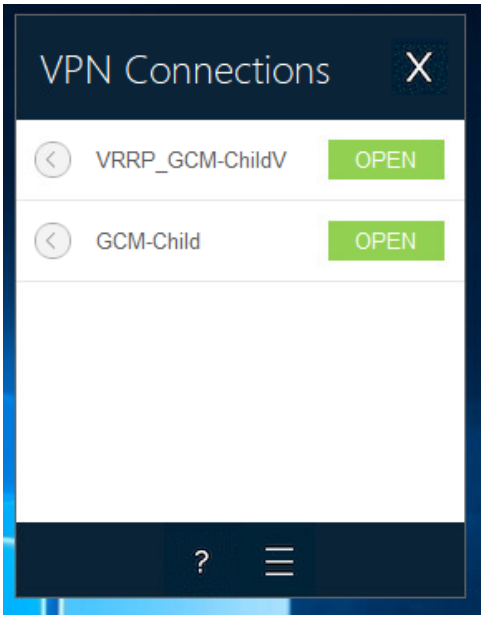
4. Click **Add**. The Remote Desktop Sharing (RDP) session will be added to the list of sessions



To open this RDP connection with a single click, we recommend displaying it specifically in the **Connection Panel** using the function described in detail in the section entitled Configuring the Connection Panel in the next chapter.

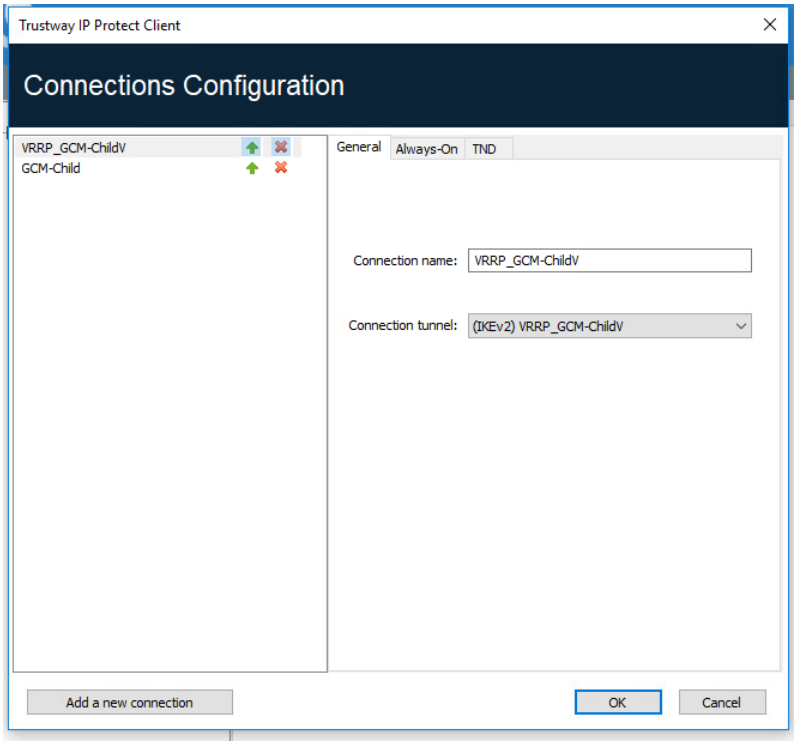
Chapitre 19. Configuring the Connection Panel

The **Connection Panel** of the IP Protect Client is entirely configurable.



VPN connections can be VPN tunnels or **Remote desktop** connections, i.e. a VPN tunnel for which the **Remote desktop** function has been specified.

A window that can be accessed from the **Tools** > **Connections Configuration** menu allows you to manage VPN connections in the **Connection Panel**, i.e. creating, naming, and sorting them.



The configuration window in the **Connection Panel** is used for the following actions:

- Choosing the VPN connections that are shown in the **Connection Panel**
- Creating and sorting VPN connections
- Renaming VPN connections
- Configuring **Always-On** in the **TrustedConnect Panel**
- Configuring **TND** (Trusted Network Detection) in the **TrustedConnect Panel**

The left side of the window shows the list of connections as they appear in the **Connection Panel**.

The right side contains the following three tabs:

- **General**
- **Always-On**
- **TND**

The **General** tab shows the parameters of each connection: its name, the associated VPN tunnel and possibly the Remote Desktop Sharing (RDP) connection, if it has been configured.

To create a new VPN connection, click **Add a new connection**, choose a name and select the corresponding VPN tunnel. If a Remote Desktop Sharing connection is configured, an option used to select it automatically appears below the selected tunnel. Once they have been confirmed, changes made in the **Connection Panel** configuration window instantly appear in the **Connection Panel**.

The **Always-On** and **TND** tabs are described in section Configuring the Connection Panel below.

The **Connection Panel**'s configuration is stored in the VPN configuration file. Therefore, it can be exported into `.tgb` files, which are useful for deploying an identical **Connection Panel** across all workstations.

Chapitre 20. Configuring the TrustedConnect Panel

The **TrustedConnect Panel** is described in section TrustedConnect Panel. It allows you to automatically open a VPN connection when you're outside the trusted network and keep the connection open even if the network interface changes.

For it to be taken into account, this VPN connection must meet the following conditions:

1. The VPN connection must be the first VPN connection defined in the **Connection Panel**. To configure this first connection, refer to section Configuring the Connection Panel below.

The following functions of the **TrustedConnect Panel** can be configured:

- Exclude network interfaces from Always-On
- Trusted Network Detection (TND)
- Manage token or smart card removal
- Manage scripts linked to the VPN tunnel
- Minimize the HMI
- Purge log files

20.1 Always-On

20.1.1 Operating principle

The **Always-On** feature, which is always enabled with the **TrustedConnect Panel**, ensures that the connection remains secure whenever the network interface changes.

The following network interfaces are supported:

- Virtual adapter (e.g. vmware)
- Wi-Fi
- Ethernet
- USB modem (i.e. smartphone)
- Bluetooth modem (i.e. smartphone)

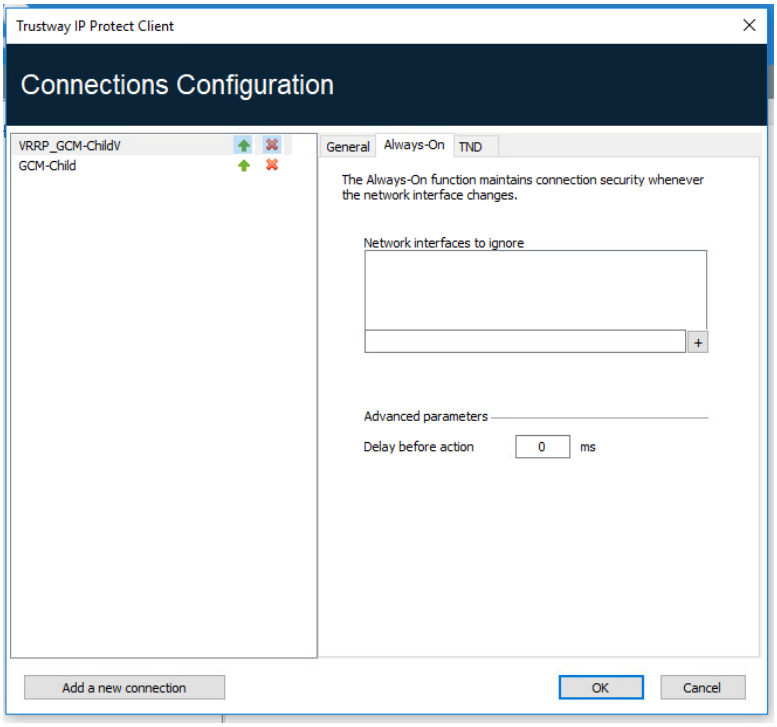
The following network events trigger automatic tunnel reconnection (and, where appropriate, detection of the trusted network), unless they have been explicitly excluded (see section Configuring Always-On):

- Connection to a network (API addresses ignored)
- Disconnection from a network
- An adapter changes IP address or DHCP switches to static or vice versa
- ipconfig /release
- ipconfig /renew
- Switch to airplane mode

20.1.2 Configuring Always-On

The **Always-On** feature is enabled as soon as the **TrustedConnect Panel** is used for open a VPN tunnel. You can configure it to exclude certain network interfaces from automatic reconnection to the VPN tunnel.

The **Always-On** tab in the **Connections Configuration** window allows you to configure the settings for the **Always-On** feature.



Network interfaces to ignore

Network interfaces can be excluded from Always-On monitoring. An interface is excluded using the **description** property (visible with ipconfig /all).

The value of this parameter must contain part or all of the **description** field of the network interface to be excluded. If the value only contains part of the description, then any interface whose **description** field contains the value defined will be excluded from monitoring.

The values of this parameter are not case sensitive (all character strings are converted to lowercase before comparison).

You can specify several network interfaces to exclude by specifying the parts of their respective descriptions separated by a comma.

Example: To exclude any interface whose **description** field contains the character strings `Hyper-V` et `vmnet`, enter `Hyper-V,vmnet`.

Delay before action

The time required to take into account a new network interface varies from one system to the next. If it is too long, it may interfere with the TND mechanism, which may lead IP Protect Client to attempt establishing a VPN connection even though the workstation is connected to the trusted network.

To avoid this issue, this parameter is used to delay the triggering of the TND mechanism (see next section).

It is expressed in milliseconds. If the default value needs to be changed, we recommend specifying a value greater than or equal to 3000 ms.

By default, the value is equal to 0 and the TND mechanism is started immediately, which is suitable in most cases.

20.2 Trusted Network Detection (TND)

20.2.1 Operating principle

This feature consists in detecting whether the workstation is connected to the corporate network (trusted network) or not.

When IP Protect Client detects that workstation is not on the corporate network, the predefined tunnel is opened automatically. This feature is referred to as Trusted Network Detection (TND) in this document.

The **TrustedConnect Panel** uses the following two methods to detect whether the workstation is on a trusted network or not:

7. It checks whether the DNS suffixes of the network interfaces available on the workstation are part of the list of trusted DNS suffixes (list configured in the software, see below).

8. Automatically accesses a trusted web server in HTTPS mode and checks that its certificate is valid.

The two methods are used in combination to detect whether the workstation is on a trusted network: IP Protect Client starts by testing whether a trusted DNS suffix is available; if none are found, IP Protect Client does not continue the test and concludes that the workstation is not connected to the trusted network; if it does find one, it continues the test sequence by verifying the access to the trusted server and the validity of its certificate.

At the first accessible trusted server found whose certificate is valid, IP Protect Client concludes that the workstation is connected to the trusted network.

In all of the following other cases, IP Protect Client concludes that the workstation is not connected to the trusted network and automatically attempts to open the configured VPN connection:

- No DNS suffix has been found in the list of trusted DNS suffixes
- The list of trusted DNS suffixes is empty
- The list of trusted server URLs is empty
- No trusted server is accessible or none has a valid certificate

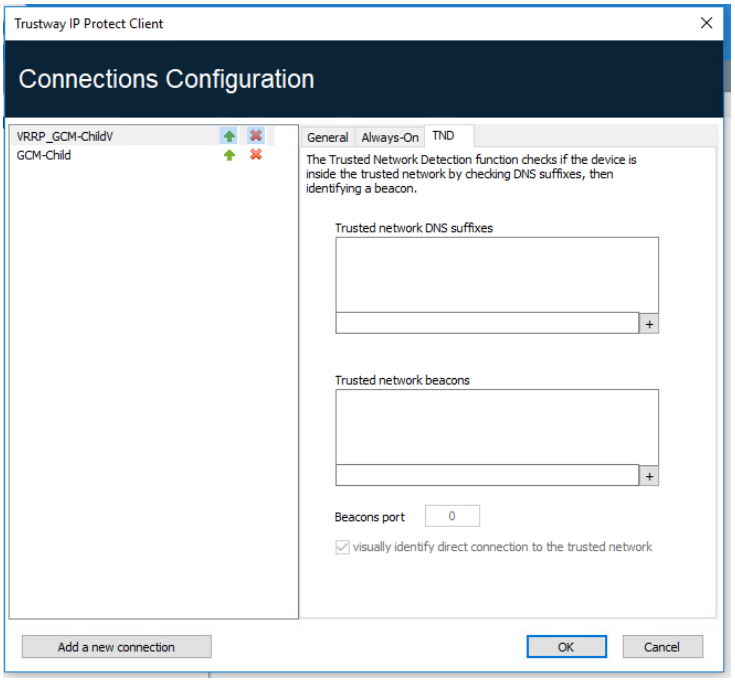
Therefore, to enable the Trusted Network Detection (TND) feature, the following parameters must be configured:

- A list of DNS suffixes
- A list of trusted server URLs.

On some workstations, a few seconds are required before the interface is ready to transmit when a network interface appears. To mitigate this time delay, there is a **Delay before action** option on the **Always-On** tab (see previous section).

20.2.2 Configuring TND

The **TND** tab in the **Connections Configuration** window allows you to configure the settings for the **Trusted Network Detection** feature.



Trusted network DNS suffixes	This parameter defines the list of trusted DNS suffixes. This list can be empty or contain several DNS suffixes. The suffixes must be separated by a comma in the list, without any blank spaces.
Trusted network beacons	This parameter defines the list of trusted server URLs to use. The list of URLs can be empty: IP Protect Client will then fall back to the list of DNS suffixes to determine whether the workstation is connected to the trusted network or not. This list can contain several trusted server URLs. IP Protect Client will then successively test all the URLs and all the certificates associated with each server until it finds one that is accessible and valid. The URLs must be separated by a comma in the list, without any blank spaces. There is no need to add the `https://` prefix to an URL.
Beacons port	This parameter defines the port to be used to reach trusted servers. Only one port that will be used for all URLs can be configured. If this parameter is not configured, IP Protect Client will use the port 443 by default.
Visually identify direct connection to the trusted network	This option adds a visual cue to the **TrustedConnect Panel** to indicate that IP Protect Client is connected to the trusted network. If the box is checked, the taskbar icon and the color of the circle in the panel is blue when the machine is connected to the trusted network and green when a tunnel is open. If the box is unchecked, the taskbar icon and the color of the circle in the panel remains green in both cases. No distinction is made between the trusted network and an open tunnel.

20.3 Scripts

The **TrustedConnect Panel** can run scripts when a tunnel is opened or closed. To configure this feature, refer to section Automation.

20.4 Minimizing the panel

By default, the **TrustedConnect Panel** is automatically minimized to the notification area (systray) after two seconds, when the workstation has been detected as being connected to the trusted network (either physically or through the VPN tunnel).

You can set the time delay before the IP Protect Client's HMI is minimized, as well as the type of minimization. The **TrustedConnect Panel** can be minimized to the taskbar or to the notification area (systray, by default).

The time delay and minimization type only apply to automatic minimization of the **TrustedConnect Panel** when a connection to the trusted network is detected.

Refer to the “Deployment Guide” for the corresponding instructions.

20.5 Purging logs

You can configure the number of days during which log files are kept. The default value is 10 days.

This configuration must be made in the properties of the IP Protect Client installer.

Refer to the “Deployment Guide” for the corresponding instructions.

20.6 Behavior when smart card or token is removed

You can configure the behavior of the **TrustedConnect Panel** when the smart card or token is removed from the reader while a VPN tunnel is open.

This configuration must be made in the properties of the IP Protect Client installer.

Refer to the “Deployment Guide” for the corresponding instructions.

Chapitre 21. USB mode

21.1 Overview

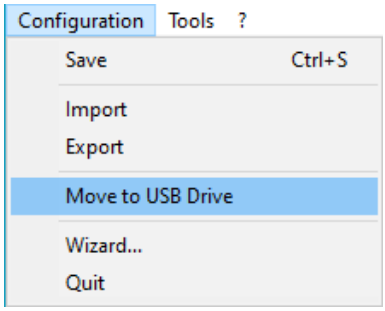
IP Protect Client features a unique VPN connection management mode known as the USB mode.

In this mode, the VPN configuration is securely stored on a removable storage device (USB drive). No VPN security elements are stored on the workstation from which the VPN connection is opened. The VPN connection is established automatically as soon as the USB drive is inserted and closed when the USB drive is removed.

Hereinafter, the USB drive containing the VPN configuration will be referred to as "VPN USB drive".

21.2 Configuring the USB mode

The USB mode is configured using the **Configuration Wizard** available from the **Configuration** > **Move to USB drive** menu of the **Configuration Panel**.



21.2.1 Step 1: Choosing a USB drive

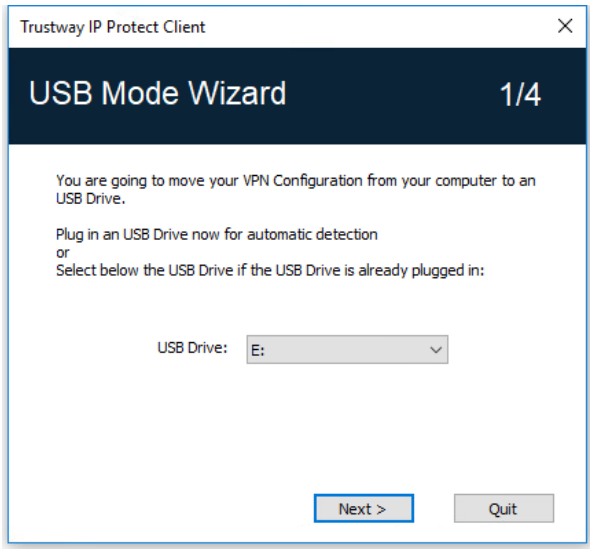
Screen 1 allows you to choose the removable storage device (USB drive) to use to protect the VPN configuration.

If a drive is already inserted, it is automatically displayed in the list of available USB drives.

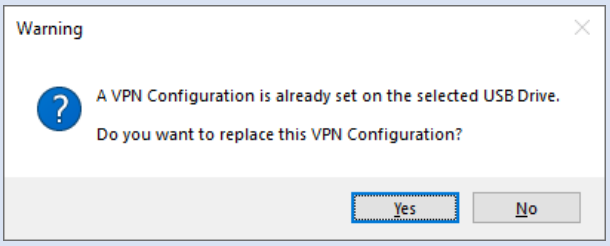
Otherwise, simply insert the selected USB drive at this stage. It will be detected automatically as soon as it is inserted.

No USB drive inserted

USB drive already inserted



The USB mode only allows you to protect a single VPN configuration on a USB drive. If there already is a VPN configuration on the inserted USB drive, the following warning will be displayed:



If an empty USB drive is inserted and it is the only drive inserted into the workstation, the wizard will automatically proceed to step 2.

21.2.2 Step 2: Protecting the VPN configuration in USB mode

The following two protections are available:

1. Pairing with the user's workstation:

The option **With this computer only** is no longer available in the current version of the software (the option is grayed out).

The USB VPN configuration can be uniquely paired to the workstation from which it originates.

The VPN USB drive cannot be paired with a specific workstation, but it can be used on any workstation on which IP Protect Client is installed.

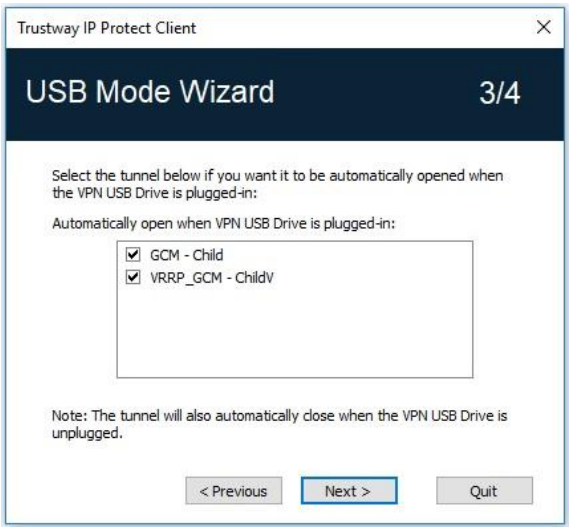
2. Password protection:

   The USB VPN configuration can be password-protected.

   In this case, the password will be required every time the VPN USB drive is inserted.

21.2.3 Step 3: Automatically opening the tunnel

L'assistant permet de configurer les connexions VPN qui seront automatiquement ouvertes à chaque insertion de la clé USB VPN.



21.2.4 Step 4: Summary

The summary gives you the opportunity to check whether the VPN USB drive has been properly configured.

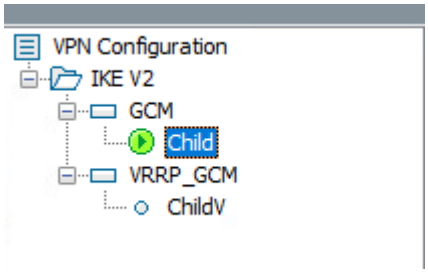
Once this final step is confirmed, the workstation's VPN configuration is transferred onto the USB drive.

It remains enabled for as long as the USB drive is inserted. When the VPN USB drive is removed, IP Protect Client will revert to an empty VPN configuration.

21.3 Using the USB mode

After starting IP Protect Client, regardless of whether a VPN configuration is loaded, insert the VPN USB drive. The following information window is automatically displayed:

Once the prompt has been confirmed, the USB VPN configuration is loaded automatically and, where appropriate, the corresponding tunnel(s) is (are) opened automatically. A "USB mode" icon is shown in the top-right corner of the tree on the **Configuration Panel** when the USB mode is enabled:



The VPN connections running in USB mode automatically close when the VPN USB drive is removed. The VPN configuration contained in the USB drive is removed from the workstation. (If a VPN configuration had already been set on the workstation before the USB drive was inserted, it will be restored in the software.)

IP Protect Client can only take into account a single VPN USB drive at a time. As long as a VPN USB drive is inserted, any additional VPN USB drives that are inserted will not be taken into account.

The import function is disabled in USB mode.

The VPN configuration can be edited in USB mode. Any changes made to the VPN configuration are saved to the VPN USB drive.

IP Protect Client does not provide any function to directly change the password or the pairing with a workstation.
In order to change these parameters, follow the steps below:

1. Insert the VPN USB drive.
2. Export the VPN configuration.
3. Remove the VPN USB drive.
4. Import the VPN configuration exported in step 2.
5. Reload the USB mode wizard with this configuration and the desired new parameters.

Chapitre 22. GINA mode

22.1 Overview

The GINA mode allows you to open VPN connections before the Windows logon.

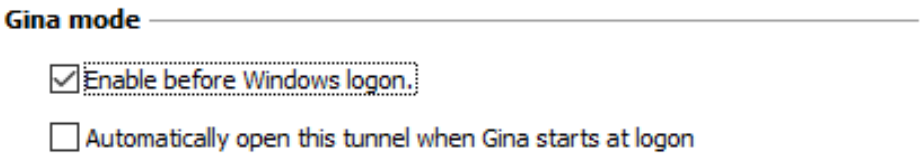
This function can, for example, create a secure connection to an access rights management server so that the user workstation access rights can be obtained before opening a user session.

When a tunnel is configured "in GINA mode", the following two situations are possible:

1. If IP Protect Client is configured to start up in **TrustedConnect** mode (refer to section General), then the **TrustedConnect Panel** will be displayed on the Windows logon screen and IP Protect Client tries to automatically connect to the trusted network.
2. Otherwise, a window allowing you to open a tunnel that is similar to the **Connection Panel** will be displayed on the Windows logon screen. It allows you to open a VPN tunnel manually or automatically.

22.2 Configuring the GINA mode

Configuring the GINA mode for a VPN connection is done on the **Automation** tab of the relevant tunnel.



Refer to section Automation.

22.3 Using the GINA mode

When the VPN tunnel is configured in GINA mode, the window used to open GINA tunnels is displayed on the Windows logon screen. The tunnel will open automatically if it is configured accordingly.

Security considerations

A tunnel configured in GINA mode can be opened before Windows logon, i.e. by any user of the workstation. We therefore strongly recommend that you set up a strong authentication method that is certificate-based and, if possible, stored on a removable device.

For the **Automatically open this tunnel on traffic detection** option to be operational after Windows logon, the **Enable before Windows logon** option must not be checked.

Limitation: Scripts and USB mode are not available for VPN tunnels configure in GINA mode.

A VPN tunnel configured with a certificate stored in the Windows Certificate Store will not work in GINA mode. The reason for this is that the GINA mode is run before a Windows user is identified (prior to opening any session). Therefore, the software cannot identify the user store to use in the Windows Certificate Store.

Chapitre 23. Options

23.1 Display

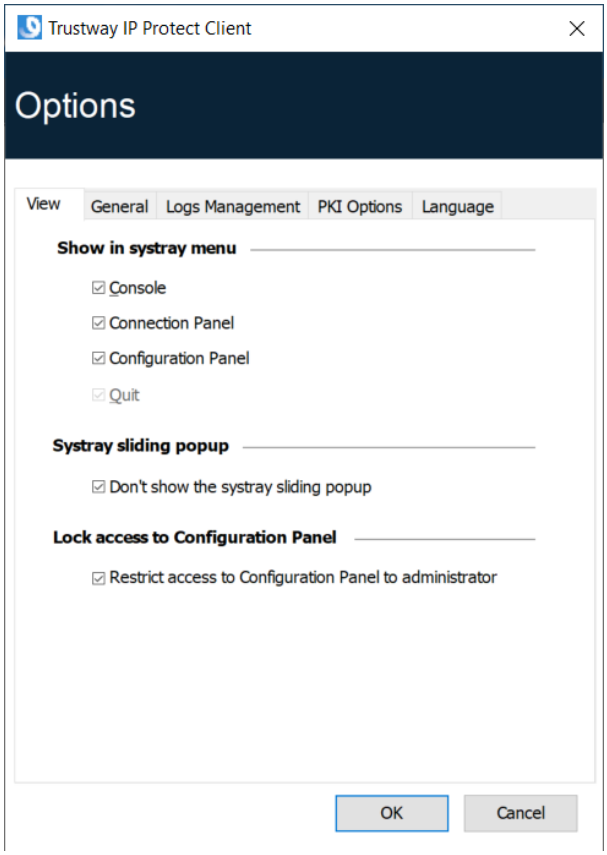
Using the options listed on the **View** tab in the **Options** window, you can hide nearly all of the software's interfaces:

- Options in the taskbar menu
- Fade-out pop-up in the taskbar
- Access to the **Configuration Panel**

23.1.1 Showing options in systray menu

You can choose to hide the **Console**, **Configuration Panel** and **Connection Panel** options in the taskbar (systray) menu. The menu can thus be reduced to the single item **Quit**.

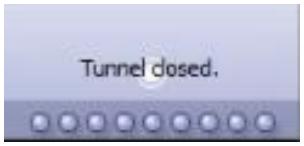
The taskbar menu's **Quit** item cannot be removed using the software. However, it can be deleted using the installation options (see "Deployment Guide").



23.1.2 Showing the systray fade-out pop-up

When the **Don't show the systray sliding popup** option is disabled, a fade-out pop-up appears above the IP Protect Client icon in the taskbar when a VPN tunnel is opened or closed.

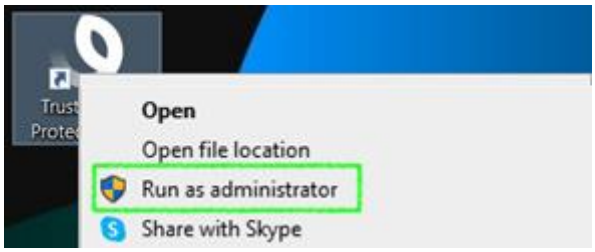
This pop-up shows the tunnel status when it is being opened or closed and automatically fades out unless the mouse cursor is placed directly over it:

Tunnel is open	
Tunnel is closed	
Failed to open the tunnel: the window will briefly explain what happened.	

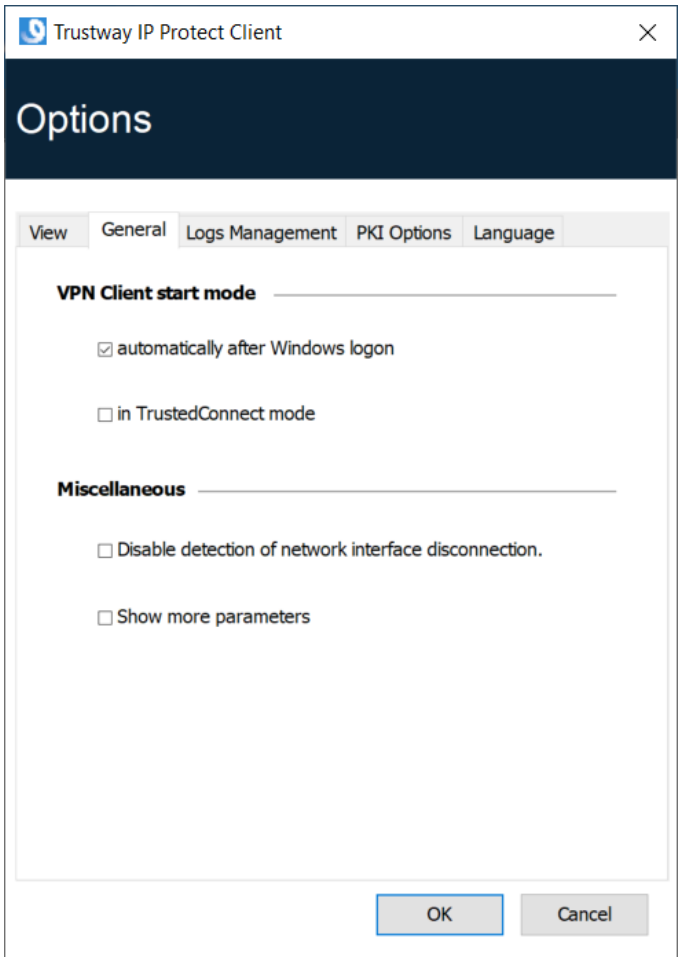
23.1.3 Restricting access to the Configuration Panel

In IP Protect Client, the interface of the **Configuration Panel** is restricted to administrators, by default. To give users access to the **Configuration Panel**, uncheck the **Restrict access to Configuration Panel to administrators** option.

To start IP Protect Client in administrator mode, right-click the **Trustway IP Protect client** icon and then select the **Run as administrator** menu item..



23.2 General



VPN Client startup mode

If the option **automatically after Windows logon** is checked, IP Protect Client will start automatically when the user session is opened.

If the option is not checked, the user must start IP Protect Client manually, either by double-clicking on the desktop icon or by selecting the software in the Windows **Start** menu.

Refer to section Starting the software.

If the **in TrustedConnect mode** option is also checked, IP Protect Client will start up showing the **TrustedConnect Panel**. Otherwise, IP Protect Client will start up showing the **Connection Panel**.

Disabling detection of network interface disconnection

The standard behavior of IP Protect Client is to close the VPN tunnel at its end as soon as a communication issue is encountered on the remote VPN gateway.

For unreliable physical networks prone to frequent micro-disconnections, this function can have drawbacks (which can go as far as not being able to open a VPN tunnel).

When the **Disable detection of network interface disconnection** box is checked, IP Protect Client will not close tunnels as soon as a disconnection is observed. This guarantees a very stable VPN tunnel, even on unreliable physical networks, typically wireless networks such as Wi-Fi, 4G, 5G or satellite.

Show connection popup

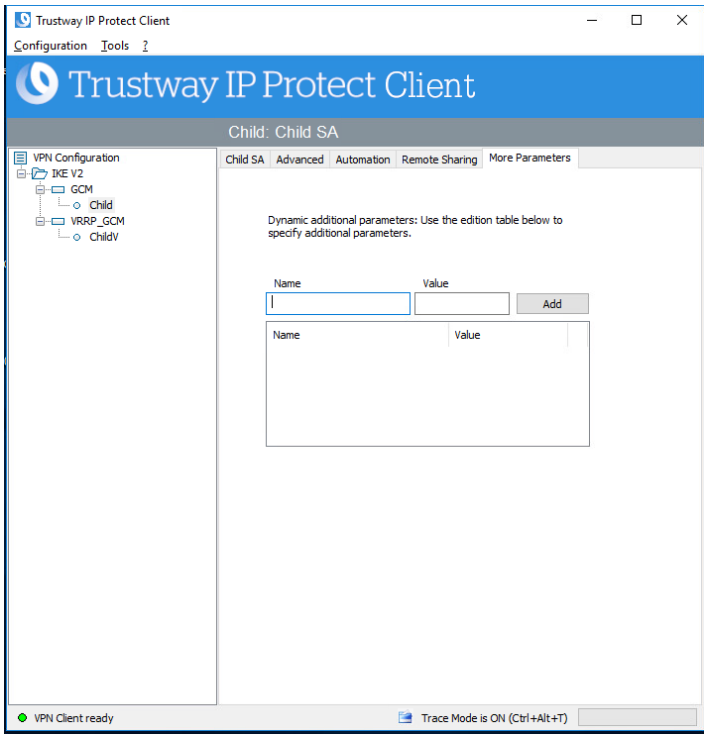
A connection window will be displayed automatically every time a VPN connection is established.

This feature can be disabled by unchecking the **Show connection popup** box.

Displaying more parameters

If required, IP Protect Client allows you to configure additional parameters, which are not documented in this document.

To enable the **More parameters** tab in the VPN tunnel configuration window as shown below, check the **Show more parameters** option.



23.3 Managing logs

Refer to section Administrator logs.

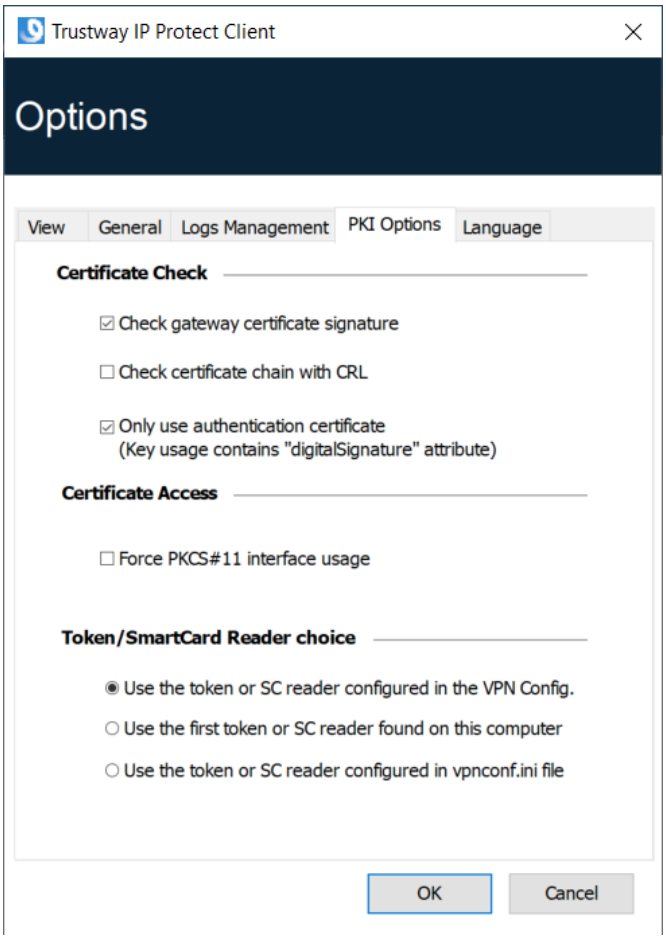
23.4 PKI options

The **PKI Options** tab is used to fine-tune smart card and token management and to further specify certificate access.

PKI options include the following:

- Configuring rules for gateway certificate verification (validity, CRL, key usage)
- Specifying the certificate that IP Protect Client must use to open a VPN tunnel
- Defining the smart card reader or token to use on the user workstation

When deploying the software, all these options can be preconfigured when the IP Protect Client is installed. This mechanism is described in the document entitled “Deployment Guide”.



23.4.1 Certificate Check

Check gateway certificate signature

When this option is selected, the VPN gateway certificate is checked (including its validity date), as well as all certificates in the certificate chain down to the root certificate.

> Security advisory: When this option is selected, the subject of the gateway certificate must be entered in the Remote ID of the tunnel concerned to prevent vulnerability 2018_7293 from being exploited.

Check certificate chain with CRL

When this option is selected, the Certificate Revocation List (CRL) of the IP Protect gateway certificate is checked, as well as the CRL of all certificates in the certificate chain down to the root certificate.

The root and intermediate certificates must be imported into the configuration or available in the Windows Certificate Store. Likewise, the CRLs must also be accessible, either in the Windows Certificate Store or available for download.

Only use authentication certificate

When this option is checked, IP Protect Client will only take into account **Authentication** certificates (i.e. certificates whose `key usage` extension contains the `digitalSignature` attribute).

This function allows you to automatically select a certificate when several are stored on the same smart card or token.

The checkbox is grayed out when the `KEYUSAGE` property is set to 2 or 3 during installation (refer to the “Deployment Guide”.

23.4.2 Certificate Access

Force PKCS#11 interface usage	IP Protect Client knows how to handle the PKCS#11 and CNG APIs in order to access the certificate for smart cards or tokens. When this option is checked, IP Protect Client will only consider the PKCS#11 API to access the certificate for smart cards and tokens.
Use the first certificate found	When this option is checked, IP Protect Client will use the first certificate found on the specified smart card reader or token.

23.4.3 Token/Smart Card Reader choice

Use the token/SC reader configured in the VPN Config.	IP Protect Client uses the reader or token specified in the VPN configuration file to search for a certificate.
Use the first token or SC reader found on this computer	IP Protect Client uses the first smart card or token found on the workstation to search for a certificate.
Use the token or SC reader configured in vpnconf.ini file	IP Protect Client uses the vpnconf.ini configuration file to identify the smart card readers or tokens to use to search for a certificate. Refer to the “Deployment Guide”. Since the use of the `vpnconf.ini` file only applies to the PKCS#11 interface, this option requires that the **Force PKCS#11 interface usage** option be selected.

23.5 Managing languages

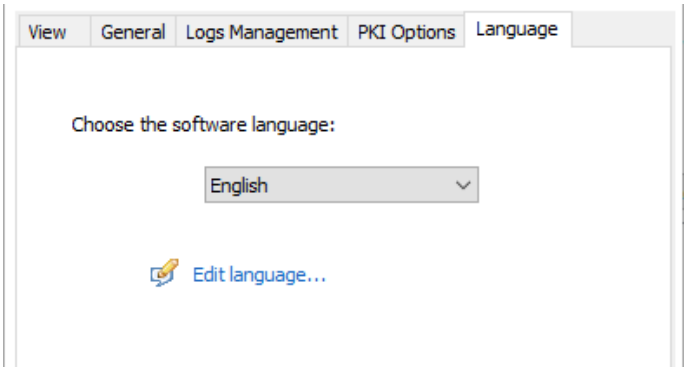
23.5.1 Choosing a language

IP Protect Client can run in several languages.

You can change languages while running the software.

To choose another language, open the **Tools** > **Options** menu, then select the **Language** tab.

Choose the desired language in the drop-down menu:



The list of languages available in the standard version of the software is provided in an appendix in 28.4 IP Protect Client technical data.

Chapitre 24. Administrator logs, console, and traces

IP Protect Client comes equipped with three types of logs:

1. Administrator logs are specifically designed for software activity and usage reports.
2. The **Console** provides detailed information on the tunnels as well as the related opening and closing steps. It essentially consists of the IKE messages and provides high-level information about the establishment of the VPN tunnel. It is intended for administrators to identify possible VPN connection issues.
3. The Trace mode makes every component of the software write an activity log about its inner workings. This mode is intended for support to diagnose software issues

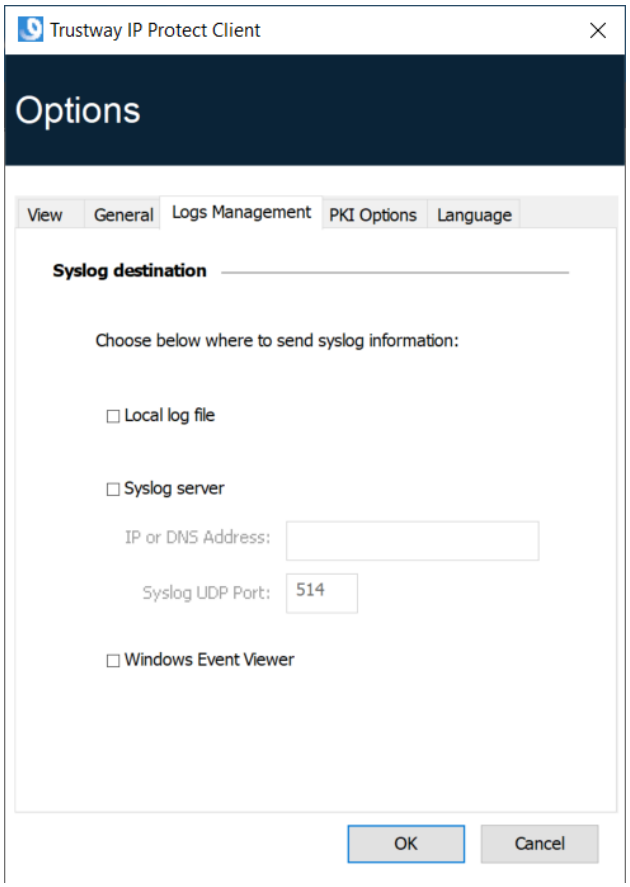
24.1 Administrator logs

IP Protect Client can collect administrator logs: tunnel opening, expired certificate, connection duration, wrong login/password, changes to the VPN configuration, import or export of this configuration, etc. Administrator logs provide a first level of analysis for any issues that may be encountered.

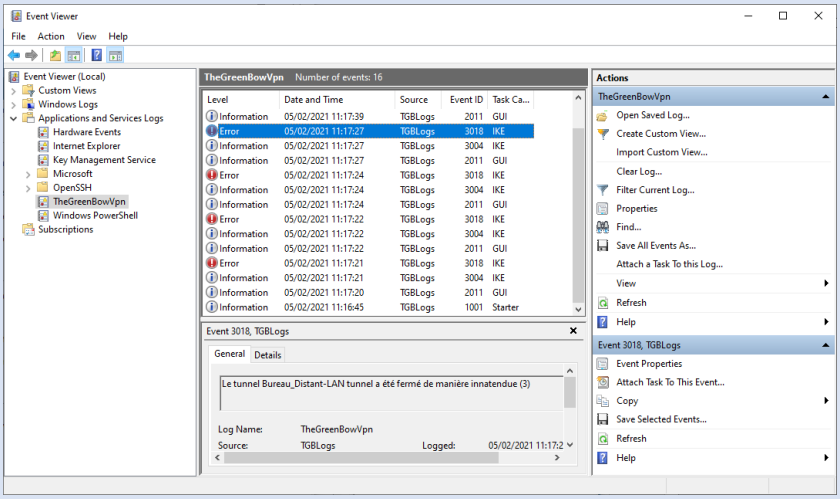
The following actions can be performed on collected logs either exclusively or simultaneously:

- Store in a local file
- Record in the Windows Event Log
- Send to a Syslog server

Administrator logs are configured in the **Tools** > **Options…** window on the **Logs management** tab.



The path for Windows Enterprise VPN Client logs in the Windows Event Viewer is the following:



Administrator logs are listed in section 28.2Administrator logs in the appendixes.

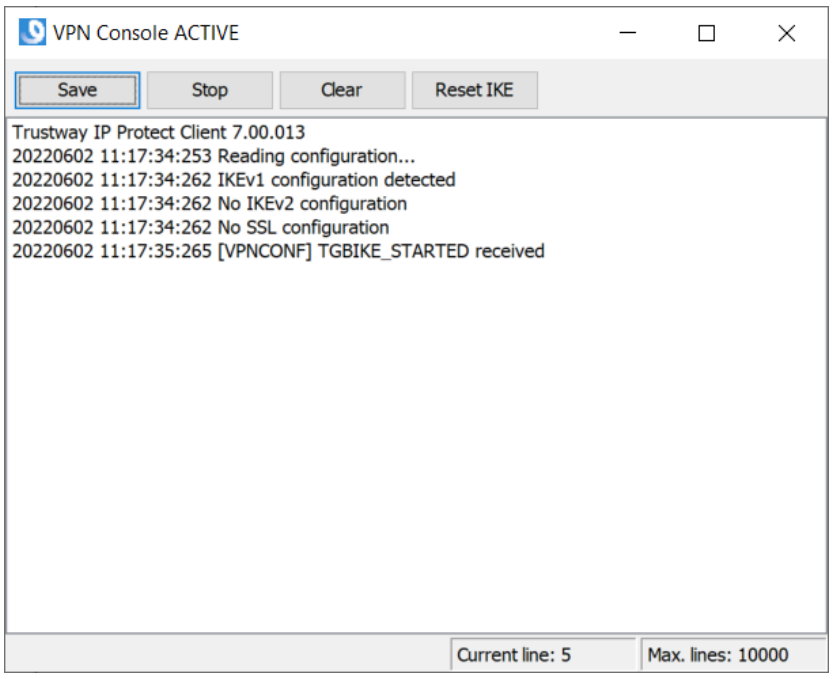
When administrator logs are stored in a local file, the path to these logs is the **System** sub-directory in the logging directory: `C:\ProgramData\Trustway\Trustway IP Protect Client\LogFiles\System`.

Read access to this directory is available in all modes, but write access is only available in Administrator mode.

24.2 Console

Access the Console using either of the following methods:

- **Tools** > **Console** menu in the **Configuration Panel** (main interface)
- CTRL+D shortcut when the **Configuration Panel** is open
- From the software's taskbar menu, choose **Console**



The **Console** has the following functions:

- Save**: Saves all the traces displayed in the window into a file**
- Start / Stop**: Starts/stops a console log**
- Clear**: Clears the contents of the window**
- Reset IKE**: Restarts the IKE service**

24.3 Trace mode

Trace mode is enabled using the following shortcut: Ctrl+Alt+T.

You do not need to restart the software when you enable the trace mode.

When the trace mode is enabled, every component of IP Protect Client generates activity logs. The logs produced are stored in a folder that you can access by clicking the blue **folder** icon located in the status bar of the **Configuration Panel** (main interface).

Logs can only be enabled on the **Configuration Panel** and access to the **Configuration Panel** can be restricted to administrators.

Even though logs do not contain any sensitive information, we recommend that, if enabled by the administrator, said administrator ensures that they are disabled and, if possible, deleted when quitting the software.

Trace logs are kept for 10 days. The software automatically deletes any older files.

When stored in a local file, administrator logs are not deleted.

Chapitre 25. Security recommendations

25.1 Assumptions

To maintain a proper security level, the operating conditions and usages listed below must be observed.

25.1.1 Profile and responsibilities of administrators

The system and network administrator as well as the security administrator, respectively tasked with installing the software and defining the VPN security policies, are nonhostile. They are trained to carry out the tasks for which they are responsible and follow administrative manuals and procedures.

The security administrator regularly ensures that the product's configuration is in line with the one that he or she has set up and performs the necessary updates when necessary.

The product's logging function is enabled and properly configured. Administrators are responsible for regularly reviewing the logs..

25.1.2 Profile and responsibilities of users

Users of the software are nonhostile and have been properly trained on how to use it. More specifically, users execute the tasks for which they are responsible to ensure proper operation of the product and do not reveal the information used for their authentication with the IP Protect gateway.

25.1.3 Compliance with management rules for cryptographic elements

Key pairs and certificates used to open the VPN tunnel are generated by a trustworthy certification authority that guarantees compliance with management rules for these cryptographic elements and, more specifically, with the specifications laid out by your local cybersecurity agency, e.g. [RGS_B1] and [RGS_B2] in France (only available in French).

25.2 User workstation

The machine on which IP Protect Client is installed and run must be clean and properly administered. More specifically:

- Antivirus software must be installed, and its signature database must be updated on a regular basis.
- It must be protected by a firewall that controls (partitions or filters) the workstation's inbound and outbound communications that do not go through IP Protect Client.
- Its operating system is up to date with the various security patches.

- Its configuration is such that it is protected against local attacks (memory forensics, patch, or binary corruption).

Configuration recommendations to strengthen the workstation are available on the ANSSI website (in French), such as the following (the list is non-exhaustive):

- Computer health guide (Guide d'hygiène informatique, document only available in French)
- Configuration guide (Guide de configuration, document only available in French)
- Password (Mot de passe, document only available in French)

25.3 IP Protect Client administration

IP Protect Client is designed to be installed and configured with "administrator" privileges and then to be used with "user" privileges only.

We recommend that you protect access to the VPN configuration with a password and restrict the software's visibility to end users (default behavior of IP Protect Client) as detailed in section Restricting access to the Configuration Panel.

We recommend that you enable the hash integrity check for the VPN configuration file using the MSI `SIGNFILE` property set to 1 when installing the software (see MSI `SIGNFILE` property in the "Deployment Guide"). When the property is not specified during installation, its default value is 0 (disabled).

The software must therefore be run as administrator to be able to access the **Configuration Panel**.

We recommend keeping the **Start VPN Client after Windows Logon** mode enabled, which is the default mode upon installation.

Lastly, please note that IP Protect Client will apply the same VPN configuration to all users of a multiple-user workstation. We therefore recommend running the software on a dedicated workstation (for instance by keeping an administrator account and a user account, as mentioned above).

25.4 VPN configuration

25.4.1 Sensitive information in the VPN configuration

We recommend that you do not store any sensitive data in the VPN configuration file.

In this regard, we recommend that you do not use the following features of the software:

- Do not use the EAP (password/login) mode alone, but only in combination with a certificate.
- If EAP is used, do not store the EAP login name/password in the VPN configuration (function described in section Authentication).

- Do not import any certificates to the VPN configuration (function described in section Importing a certificate to the VPN configuration) and preferably use certificates stored on removable devices (tokens) or in the Windows Certificate Store.
- Do not use the "Preshared key" mode (function described in section IKE Auth : IKE SA") and preferably use the "Certificate" mode with certificates stored on removable media (tokens) or in the Windows Certificate Store.
- Do not export the VPN configuration without encrypting it, i.e. not password-protected (function described in section Exporting a VPN configuration).

25.4.2 User authentication

The user authentication functions available in IP Protect Client are described below, from the weakest to the strongest.

It should be noted that preshared key authentication, despite being easy to implement, enables any user of the workstation to establish a VPN tunnel without cross-checking their authentication.

Type of user authentication	Strength
Certificate stored in the VPN configuration	
Certificate in the Windows Certificate Store	
Certificate on a smart card or token	Strong

25.4.3 VPN gateway authentication

We recommend that you implement a check on the VPN gateway certificate as described in section 23.4 PKI options.

We recommend that you do not configure IP Protect Client to validate certificates that do not comply with the constraints on the Extended Key Usage and Key Usage extensions (do not use the dynamic parameter `allow_server_and_client_auth`).

25.4.4 "All through the tunnel" and "split tunneling" modes

We recommend that you configure the VPN tunnel using the "All traffic through the tunnel" mode and enable the "Disable Split Tunneling" mode.

Refer to section Miscellaneous.

25.4.5 GINA mode

We recommended that you choose a strong authentication method for all tunnels configured in GINA mode.

25.4.6 ANSSI recommendations

The recommendations described above can be complemented by French National Cybersecurity Agency's (ANSSI) IPsec configuration document: Recommendations for securing IPsec networks.

Chapitre 26. Certification environment

The security recommendations specified in section Security recommendations apply within the scope of the IP Protect Client certification. Moreover, the following requirements must be met:

1. Administrators must make sure that functions not included in the scope of the evaluation are deactivated in the configuration and that users cannot access the configuration.
2. The user's workstation is dedicated to a single user, no multiple user accounts.
3. The product's logging function is enabled and configured in such a way that logs are sent to local files or to a syslog server. Administrators are responsible for the configuration and its security. If local logs are used, Windows will prevent them from being modified (administrator rights are required for writing).

Chapitre 27. Support

In the event of a problem with one of our products, or for any question relating to them, the means of accessing Trustway support are specified below.
There are now two distinct ways:

1. « SOL » (Support On Line), for the demands others than opening support tickets:

• Download different versions of Trustway's applications

• Access to technical information (Manual and BLL)

• Access from this website: http://support.bull.com/ols

• Login & Password is obtained on first connection by providing a serial number (and zip code) of a Trustway hardware under support contract

• If the hardware is no longer under contract, the login is deleted. The registration procedure must then be repeated once the contract has been renewed

• Follow the website http://support.bull.com/ols/online/calls/new-subscription for help with the first connection.

2. « A-Smile » (Previously known as « Bull Tickets ») to report and track issues and problems:

• Access via " https://tickets.bull.com/otrs/customer.pl

• Login : your e-mail address in minuscules

• Password : obtained during the first connection via the contact form or through your support contacts (srv.support-trustway@atos.net). The password can be retrieved later by clicking on "forgotten password".

• For more details on the use of « A-Smile », refer to the instructions for use

mode-operat-client-fr-V5.4.4.pdf

• Specify when opening the ticket that it is a Trustway product.

You can also open a ticket via the CAU (Centre d'Appel Unique) by calling the following number:
08 20 08 20 00.
Do not hesitate to contact us using the support email address srv.support-trustway@atos.net.
To open a ticket, we recommend that you use the A-Smile application.

Trustway Products Support Team
BULL S.A.S., An Atos Compagny
Rue Jean Jaurès - BP 68
78340 Les Clayes Sous-Bois - FRANCE
Visit Trustway Products

Chapitre 28. Appendixes

28.1 Shortcuts

28.1.1 Connection Panel

Esc	Closes the window.
Ctrl+Enter	Opens the **Configuration Panel** (main interface).
Arrow keys	The Up and Down arrow keys are used to select a VPN connection.
Ctrl+O	Opens the selected VPN connection.
Ctrl+W	Closes the selected VPN connection.

28.1.2 Configuration Panel tree

F2	Used to edit the name of the selected.
Del	Deletes a selected phase, following confirmation by the user. If the actual configuration is selected (root of the tree), the software asks whether a full reset of the configuration should be performed.
Ctrl+O	Opens the corresponding VPN tunnel if a Child SA is selected.
Ctrl+W	Closes the corresponding VPN tunnel if a Child SA is selected.
Ctrl+C	Copies the selected phase to the clipboard.
Ctrl+V	Pastes (adds) the phase that has previously been copied to the clipboard.
Ctrl+N	If the VPN configuration is selected, creates a new IKE Auth. If an IKE Auth is selected, creates a Child SA.
Ctrl+S	Saves the VPN configuration.

28.1.3 Configuration Panel

Ctrl+Enter	Switches to the **Connection Panel**.
Ctrl+D	Opens the **Console** window with VPN traces.
Ctrl+Alt+R	Restarts the IKE service.
Ctrl+Alt+T	Enables trace mode (log generation).
Ctrl+S	Saves the VPN configuration.

28.2 Administrator logs

ID Log define	ID Log value	Severity	Log string
LOGID_STARTERINIT	1001	Notice	Starter service is started.
LOGID_VPNCONFSTARTING	2001	Notice	GUI is starting.
LOGID_VPNCONFSTOPPED	2002	Notice	GUI has closed.
LOGID_TGBIKESTARTED	3001	Notice	IKE has started (status %d).
LOGID_TGBIKESTOPPED	3002	Notice	IKE has stopped.
LOGID_TUNNELOPEN	3004	Info	Tunnel %s is asked to open.
LOGID_VPNCONFCRASHED	2003	Notice	GUI crashed (state %d).
LOGID_TGBIKECRASHED	3003	Notice	IKE crashed (state %d).
LOGID_STARTERSTOP	1002	Notice	Starter service is stopped.
LOGID_RESETIKE	2007	Warning	IKE is asked to reset.
LOGID_VPNCONFSTARTED	2008	Notice	GUI has started from user %s.
LOGID_VPNCONFSTOPPING	2009	Notice	GUI is stopping from user %s.
LOGID_VPNCONFLOADERROR	2010	Error	Configuration couldn’t load (reason: %s).
LOGID_VPNCONFOPENTUNNEL	2011	Info	GUI opens tunnel (source: %s).
LOGID_VPNCONFCLOSETUNNEL	2012	Info	GUI closes tunnel (source: %s).
LOGID_VPNCONFSAVE	2013	Notice	New configuration is saved.
LOGID_VPNCONFIMPORT	2014	Info	%s has been imported.
LOGID_VPNCONFIMPORTERR	2015	Error	%s could not be imported (status %d).
LOGID_VPNCONFEXPORT	2016	Info	%s has been exported.
LOGID_TOKENINSERT	2017	Info	Token %s has been inserted.
LOGID_TOKENEXTRACT	2018	Info	Token %s has been extracted.
LOGID_USBINSERT	2019	Info	USB Key has been inserted.
LOGID_USBEXTRACT	2020	Info	USB Key has been extracted.
LOGID_INSTALLATION	2021	Info	VPN running for the 1st time.

ID Log define	ID Log value	Severity	Log string
LOGID_UPDATE	2022	Info	VPN software has been updated to version %s.
LOGID_VERSION	2023	Info	VPN Version is %s.
LOGID_GINASTARTED	4001	Notice	GINA has started.
LOGID_GINASTOPPING	4002	Notice	GINA is stopping.
LOGID_GINAOPENTUNNEL	4003	Info	GINA opens tunnel (source: %s).
LOGID_GINACLOSETUNNEL	4004	Info	GINA closes tunnel (source: %s).
LOGID_TUNNELAUTH_OK	3005	Info	Tunnel authentication Ok (%s).
LOGID_TUNNELTRAFIC_OK	3006	Info	Tunnel %s Ok
LOGID_TUNNELAUTH_NOK	3007	Error	Tunnel authentication failed (reason %d).
LOGID_TUNNELTRAFIC_NOK	3008	Error	Tunnel %s failed (reason %d).
LOGID_AUTHREKEYING	3009	Info	Tunnel %s initiated rekey (source %d).
LOGID_AUTHREKEYED	3010	Info	Tunnel %s rekeyed.
LOGID_TUNNELREKEYING	3011	Info	Tunnel %s initiated rekey (source %d).
LOGID_TUNNELREKEYED	3012	Info	Tunnel %s rekeyed.
LOGID_PINCODE	3013	Notice/Error	Pin code is entered (status %d).
LOGID_DRIVERNOK	3014	Critical	Driver could not be loaded (status %d).
LOGID_IKEEXT_STOP	1003	Warning	IKEEXT service is stopped.
LOGID_IKEEXT_RESTART	1004	Notice	IKEEXT service is restarted.
LOGID_IKEEXT_ERROR	1005	Critical	IKEEXT could not be stopped (status %d).
SYSTEMLOGID_VIRTIFOK	3015	Info	Virtual interface created successfully (instance %d).
SYSTEMLOGID_VIRTIFNOK	3016	Error	Virtual interface could not be created (error %d).
LOGID_TUNNELCLOSED	3017	Notice	%s tunnel successfully closed (%d min).
LOGID_TUNNELCLOSED_ERR	3018	Error	%s tunnel closed unexpectedly (%d).
LOGID_CERTERROR	3019	Error	Error %d when handling certificate %s.

28.3 TrustedConnect Panel diagnostics

The **TrustedConnect Panel** informs the user of any issues that may have occurred while establishing the VPN connection by displaying an error code.

These error codes, their diagnosis and possible solutions are detailed below. This list allows administrators to find possible answers to any issues that users may encounter and report.

Code	Diagnostics	Solution
0	**VPN configuration issue** VPN connection not found in configuration	• Make sure that the `tgbvpn.conf` file is available in the IP Protect Client installation directory.
1	**Issue with a certificate** The VPN configuration uses a certificate whose private key cannot be found.	• Check the IP Protect Client's configuration and any possible associated authentication devices (smart card reader, token, or Windows Certificate Store). • Reimport the VPN configuration and then reimport the certificate concerned. • Create a ticket and send it to Trustway support making sure to attach all log files.
3	**Configuration issue** The message **No proposal chosen** has been received during an IKE exchange: the cryptographic algorithm suite configured for the IKE_SA_INIT sequence does not match the one configured on the gateway.	• Verify that the cryptographic algorithm suite for THE IKE_SA_INIT sequence of the VPN connection matches that of the gateway (refer to IKE Auth in the **Configuration Panel**).
4	**Configuration issue** The message "No proposal chosen" has been received during an IKE exchange: the cryptographic algorithm suite of the ESP protocol does not match the one configured on the gateway.	• Verify that the cryptographic algorithm suite of the ESP protocol (refer to Child SA in the **Configuration Panel**) matches that of the gateway.
5	**Cannot access gateway** The gateway address ("Remote Router Address") specified in the VPN configuration is not reachable. If it is an IP address, it cannot be found or cannot be reached. If it is a DNS address it may be inaccessible, indefinite, or cannot be resolved.	• Check the address of the gateway/remote workstation. For example, try "pinging" this address.

Code	Diagnostics	Solution
6	**Configuration issue** The message **Remote ID other than expected** has been received. This means that the value of the **Remote ID** does not match the value expected by the remote VPN gateway.	• Make sure that the **Local ID** parameter on IP Protect Client's **Protocol** tab matches the Remote ID of the remote gateway (or workstation). **Caution**: The Remote ID on the router is the Local ID on IP Protect Client and vice versa.
7	**Gateway certificate** Checking the certificate chain of the certificate received from the VPN gateway is enabled. The gateway certificate chain could not be validated.	• Check the gateway certificate expiration date. • Check the validity start date of the gateway certificate. • Check the signatures of all certificates in the certificate chain (including root certificate, intermediate certificates, and gateway certificate). • Check whether the CRLs of all certificate issuers in the certificate chain are up to date. • Make sure that none of the certificates concerned have been revoked in the corresponding CRL lists. • Make sure that the root certificate and all certificates in the certificate chain (root certification authority and intermediate certification authorities) are available in the Windows Certificate Store on the workstation. • Make sure that the CRLs of the various certification authorities are available in the Windows Certificate Store, or that these CRLs can be downloaded when the VPN connection is opened.
9	**No response from gateway** IP Protect Client has abandoned the connection, most often after several connection attempts.	• Check whether the gateway is still accessible from the workstation.
10	**Authentication issue** The gateway has declined the user's authentication credentials.	• Check the user certificate. • Check that the Local ID on the **Protocol** tab of the **Configuration Panel** matches the value and type defined on the gateway. **Caution**: The Local ID on IP Protect Client is the Remote ID on the router and vice versa. • Check the logs on the remote gateway to get more information about this issue.
13	**Configuration issue** An error occurred while establishing the VPN connection. Establishing the VPN connection has been abandoned.	• Retrieve the user log files. They must be analyzed. • Create a ticket and send it to Trustway support making sure to attach all log files.
14	**Network configuration** An error occurred while creating the	• Retrieve the user log files. They must be analyzed. • Create a ticket and send it to Trustway support making

Code	Diagnostics	Solution
	virtual interface used for the VPN connection.	sure to attach all log files.
15	**Network configuration** The virtual IP address assigned during the VPN connection already exists on one of the workstation's interfaces.	• Change the virtual IP address (**VPN Client address** parameter) specified in IP Protect Client's configuration. • Change the IP address provided by the gateway to IP Protect Client.
16	**Network configuration** An error occurred while creating the virtual interface used for the VPN connection.	• Retrieve the user log files. They must be analyzed. • Create a ticket and send it to Trustway support making sure to attach all log files.
24	**Configuration issue** The gateway did not accept the cryptographic algorithm suite provided by IP Protect Client.	• Make sure that IP Protect Client's cryptographic algorithm suites match those of the gateway. • Check the Local ID and Remote ID. **Caution**: The Local ID on the router is the Remote ID on IP Protect Client and vice versa.
25	**Configuration issue** The gateway did not accept the remote network configured in IP Protect Client or the virtual IP address provided by IP Protect Client.	• Make sure that the virtual IP address (**VPN Client address** parameter) specified in IP Protect Client's configuration is acceptable at the gateway end. • Make sure that the remote network (**Remote network address** parameter) specified in IP Protect Client's configuration is acceptable on the gateway end.
26	**Configuration issue** IP Protect Client provides its own traffic selectors, while the gateway is configured to provide them.	• Check the **Request configuration from the gateway** parameter on the **Child SA** tab.
27	**Gateway error** The gateway reported an error not supported by IP Protect Client.	• Analyze the logs on the gateway end. • Retrieve the user log files. They must be analyzed. • Create a ticket and send it to Trustway support making sure to attach all log files.
28	**Login/password error** The gateway has rejected the EAP authentication while establishing the VPN connection.	• Check the EAP authentication parameters in IP Protect Client's configuration. • Make sure that the user knows his or her credentials, should he or she need them while establishing the connection.
30	**Smart card or token error** Cannot access the certificate stored the on the smart card or token.	• Check that the smart card reader or token is correctly configured on the workstation, and that IP Protect Client can access it.
31	**Captive portal authentication timeout expired** No session has been opened on the	• Click the Connect button in order to authenticate on the captive portal.

Code	Diagnostics	Solution
	captive portal. The workstation therefore has no internet connectivity.	
100	**Cannot load the VPN configuration** No VPN connection has been found in the configuration file.	• Make sure that at least one tunnel is configured in the **Connection Panel**. Go to **Tools** > **Connections Configuration**, then add a tunnel and save the configuration.
101	**GINA configuration error** A tunnel is active before logon, but has not been configured to be used by the **TrustedConnect Panel**.	• Make sure that the tunnel which is active before logon is also configured in the **Connection Panel**. Go to **Tools** > **Connections Configuration**, then add a tunnel and save the configuration.
102	**IKE initialization error** An error occurred while initializing the IKE daemon.	• Retrieve the user log files. • Create a ticket and send it Trustway support making sure to attach all log files.
103	**DNS error** A DNS name could not be resolved in the set of rules for the filtering mode.	• Make sure that the workstation can access the internet. • Make sure that the filtering mode does not itself block access to DNS queries. • Replace DNS names with IP addresses.
200	**Software activation** The software is not activated and the trial period has expired.	• Retrieve the user log files. • Check software activation.

28.4 IP Protect Client technical data

Windows version	Windows 10 64-bit
Languages	Arabic, Chinese (simplified), Czech, Danish, Dutch, English, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai, Turkish

28.4.1 General

28.4.2 Operating mode

Invisible mode	Automatically open tunnel when traffic is detected Control access to VPN configurations Hide part or all the interfaces
USB mode	No more VPN configurations stored on the workstation Open tunnel when a USB drive configured for VPN is inserted Automatically close tunnel when a USB drive configured for VPN is removed
Gina	Open a tunnel before Windows logon using: GINA/Credential providers on Windows 10
Scripts	Run configurable scripts when opening or closing a VPN tunnel
Remote Desktop Sharing	Open a remote computer with a single click via RDP and VPN tunnel
TrustedConnect Panel	Automatically open tunnel with Always-On and trusted network detection (TND)

28.4.3 Connection/Tunnel

Connection mode	Peer-to-gateway
Networks	IPv4
Protocols	IPsec/IKEv2
Tunneling modes	Main mode
Mode Config/Mode CP	Automatically retrieve network parameters from VPN gateway

28.4.4 Cryptography

Encryption, Key group, Hash (IKEv2)

Symmetric : AES GCM 256bits

Diffie-Hellman : DH19 (ECP 256)

Hash: SHA-256

User authentication

Administrator : Protect access to the VPN configurations

User :

- X.509 certificates

Certificate authentication

- Method 9: ECDSA “secp256r1” with SHA-256 on the P-256 curve [RFC4754]

PKI

- Support for certificates in X.509 format
- Importing PKCS#12, PEM/PFX certificates
- Multiple media: Windows Certificate Store, smart card, token, configuration file
- Support for Certificate Revocation List (CRL)
- Automatically detect a smart card reader or token according to criteria
- PKCS#11 and CNG access to tokens and smart cards
- Complete check of the “user” and “gateway” certificate chain

28.4.5 Divers

NAT/NAT-Traversal	NAT-Traversal Draft 1 (enhanced), Draft 2, Draft 3 and RFC 3947, IP address emulation, includes support for: NAT_OA, NAT keepalive, NAT-T aggressive mode, NAT-T in forced, automatic or disabled mode
DPD	RFC3706. Detection of inactive IKE endpoints.
Redundant gateway	Redundant gateway management, automatically selected when DPD is triggered (inactive gateway)

28.4.6 Administration

Deployment	Silent installation using Microsoft Installer (MSI)
VPN configuration management	Import and export options for VPN configurations Secure import/export using passwords, encryption, and integrity control
Automation	Ability to open, close, and monitor a tunnel using command lines (batch and scripts) Ability to start and quit the software using batches
Logs and traces	IKE/IPsec log console and trace mode can be enabled Administrator logs: local file, Windows Event Log, syslog server
Updates	Check for available updates from within the software
License and activation	Licenses available on a subscription basis, manual/automatic/silent activation

28.5 Third-party licenses

28.5.1 OpenSSL

OpenSSL is licensed under the Apache License 2.0 license, reproduced here.

```
                                 Apache License
                           Version 2.0, January 2004
                        https://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
```

the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their

Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions

of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

28.5.2 LZ4

Lz4 is licensed under the Simplified BSD License, reproduced here.