GUIDE

STORMSHIELD IPSEC VPN CLIENT

INSTALLATION AND USER GUIDE

Version 1.1

Document last updated: July 27, 2026

Reference: sns-en-ipsec_vpn_client_installation_user_guide-v1

Table of contents

Change log ... 4

Introduction ... 5

Installing the VPN client ... 6

- Technical requirements ... 6
  - Operating system ... 6
  - Permissions and privileges ... 6
  - Hardware resources ... 6
  - Server-side VPN infrastructure ... 6
  - Certificates and PKI ... 6
  - Network ... 7
- Digital signature and version ... 7
- Client installation procedure ... 7
  - Manual installation ... 7
  - Managed installation ... 8

Updating the VPN client ... 9

- Manual update ... 9
- Managed update ... 9

Uninstalling the VPN client ... 10

- Manual uninstall ... 10
- Managed uninstall ... 10

Manual tunnel configuration ... 11

- Configuring a standard tunnel ... 11
  - Step 1 (General settings) ... 12
  - Step 2 (IKE settings) ... 13
  - Step 3 (ESP settings) ... 18
- Configuring a "Diffusion Restreinte" tunnel ... 21
  - Step 1 (General settings) ... 22
  - Step 2 (IKE settings) ... 23
  - Step 3 (ESP settings) ... 23
- Finalizing the creation of the tunnel ... 24
- Configuring multiple tunnels ... 25

Managed tunnel configuration ... 27

- Exporting and importing configurations ... 27
  - Exporting the configuration from a reference workstation ... 27
  - Importing the configuration to the fleet ... 27
- Finalizing the configuration ... 28
  - Manual configuration customization for PSK and certificate ... 28
  - Managed configuration customization for certificate ... 28

License ... 30

- Manual license configuration ... 30
- Managed license configuration ... 30
- How licensing works for Cybels VPN ... 30

Summary of the steps from installation to deployment ... 32

Step 1: Retrieve VPN client and license key 32
Step 2: Install the VPN client on a reference station 32
Step 3: Configure the VPN tunnel on the reference station and export the configuration 32
Step 4: Deploy VPN client and configuration to remote workstations 32
Step 5: Check for proper operation and manage the pool 32

Using the VPN client 33
Manual start 33
Automatic start 34

Event logs 35
Audit logs 35
Technical logs 36

"General settings" tab 37

“About" menu 38

Appendix 39

Change log

Date	Description
July 27, 2026	Added sections “Summary of steps from installation to deployment” and “Appendix” Modification of the sections “Installing the VPN client”, “Manual tunnel configuration”, “Managed tunnel configuration” and “License”
May 11, 2026	New document

Introduction

Welcome to the Stormshield IPsec VPN Client version 1.1 Installation and User Guide.

NOTE
Stormshield markets the Cybels VPN client, which is developed by partner vendor Ercom, under the name Stormshield IPsec VPN Client. The original document was written by Ercom, and published on the Stormshield technical documentation website with Ercom's consent.

This guide is intended for Cybels VPN client administrators who oversee the deployment, configuration and operation of the solution. The aim of this guide is to provide a comprehensive and operational overview of Cybels VPN, in order to guarantee secure, reliable remote access that meets the organization's requirements.

The VPN client allows authorized users to access the company's internal resources from remote environments, while guaranteeing the confidentiality of communications, user authentication, and data integrity. The client is to be integrated as part of the information system's global security policy, and must be managed in line with current best practices.

This document covers the range of aspects required to manage the solution, in particular:

- Technical requirements
- Steps in installation and configuration
- Profile management
- Authentication and encryption mechanisms
- Monitoring, maintenance and troubleshooting procedures

This guide acts as a reference to assist administrators throughout the life cycle of the VPN client, from its setup to its daily operations, in order to guarantee an efficient and controlled secure service.

Cybels VPN exists in 2 variants:

- **Cybels VPN Essential**: includes basic features
- **Cybels VPN Premium**: in addition to basic features, provides more advanced deployment and configuration features.

The Cybels VPN software program is supplied in the form of an MSI package, thereby ensuring a recognized standard that guarantees a reliable, reproducible and automatable installation, centralized life cycle management (installation, update, uninstall), as well as native integration with Windows-based deployment and administration tools.

Installing the VPN client

Technical requirements

Operating system

- Microsoft Windows 11 PC (version 22H2 or later versions)
- Professional or Enterprise edition recommended

Permissions and privileges

- Privileges required for software installations on the workstation (manual installation)

Hardware resources

- Available disk space: 500 MB
- Refer to Windows 11 requirements for other details https://www.microsoft.com/en-us/windows/windows-11-specifications?r=1

Server-side VPN infrastructure

Before operating the VPN client, the following items have to be available:

- A VPN server configured with one or several IKEv2 tunnels, depending on the desired network policy.
- Parameters required for setting up the VPN tunnel(s), provided by the administrator. These parameters include:
  - The address of the VPN server (IP address or FQDN)
  - If applicable, the cryptographic algorithm(s) to be used (encryption, integrity, key exchange)
  - If applicable, the network configuration if it has not been dynamically provided

Certificates and PKI

- CA and user certificate available on the PC
- User certificate:
  - X.509-compatible format in at least v3 (more details later)
  - Provisioned on the desired medium:
    - Windows Store
    - Smart card

> **NOTE**
> The smart card must be compatible with Windows **CNG (Cryptography Next Generation)** architecture (see Appendix for the list of cards tested).

- CA certificate:
  - Installed in stores of intermediaries
  - Minimum X.509 v3 compatible format

Network

- The UDP port dedicated to VPN traffic (4500 by default, or any other custom port) has to be explicitly authorized for incoming and outgoing traffic on the local firewall.
- No conflict with other installed VPN clients (prior uninstall recommended)
- For licensing needs:
  - Port 1947 open for input on the user workstation on the localhost interface
  - ercom.prod.sentinelcloud.com:443 open for output:

    - At the user workstation level if exchanges with the license server must pass outside VPN

    - At the IS/firewall level if exchanges with the license server must pass through the VPN

Digital signature and version

The Cybels VPN client installer is digitally signed with a certificate that is issued by **Ercom Engineering Reseaux Communications SAS**. This signature guarantees the software program's authenticity, and ensures that the installer has not been tampered with. The administrator or user may perform checks by looking up the properties of the MSI file (right-click), then by going to the "Digital signatures" tab.

Client installation procedure

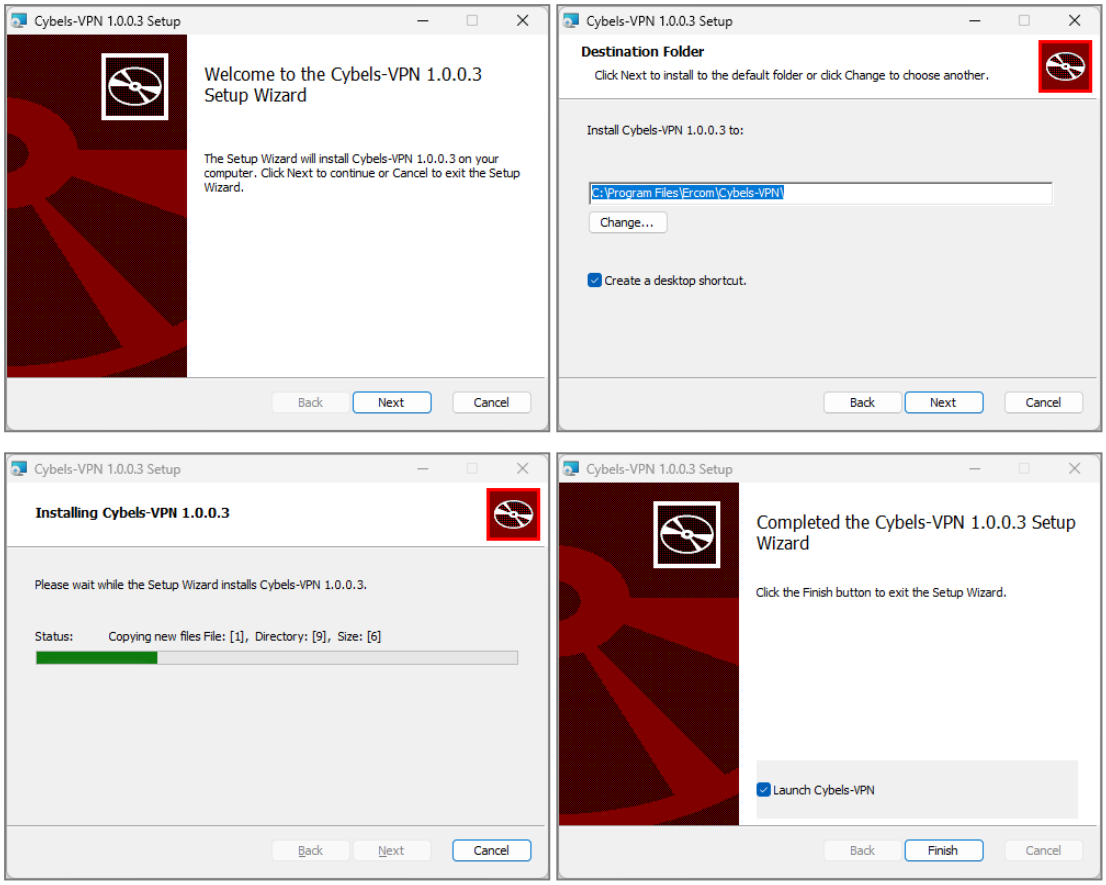
The Cybels VPN client can be installed in several ways:

- **Manual installation mode**: applies to both Cybels VPN Essential and Cybels VPN Premium, and is carried out through the VPN client graphical interface.
- **Managed installation mode**: allows the administrator to deploy the application, either automatically or in a distributed manner, over a pool of computers. Applies only to Cybels VPN Premium.

Manual installation

Through the Cybels VPN client installer (requires local administration privileges)

- After you have downloaded the MSI package, run the application
- Follow the step-by-step instructions in the installation wizard



By selecting "Launch Cybels VPN", the Cybels VPN client starts automatically once the update is complete.

Managed installation

The Cybels VPN client can be installed more comfortably in managed installation mode, which allows remote, batch and silent installations.

- If you are using a group policy (GPO)/EMM/MDM, ask your system administrator for advice on configuration.
- In command line (CLI) through a Windows command prompt.

> **NOTE**
> While the MSI's native capacities enable batch deployment in all variants (Essential and Premium), centralized configuration features (automatic and remote configuration of profiles and security policies) are exclusively available in Cybels VPN Premium.

Updating the VPN client

By updating the Cybels VPN client, you can upgrade to a newer version of the software while preserving the settings and VPN configuration.

Similarly to an installation, an update requires local administration privileges.

The previous version does not need to be uninstalled before launching the update.

Manual update

- After you have downloaded the package, run the application
- Follow the step-by-step instructions in the installation wizard

The Cybels VPN client starts automatically once the update is complete.

Managed update

- If you are using a group policy (GPO)/EMM/MDM, ask your system administrator for advice on configuration.
- In command line (local administrator privileges required)
  - After you have downloaded the MSI package, open the Windows command prompt.
  - Go to the folder containing the downloaded package
  - Run the following command to start the deployment:

```
msiexec /i "CybelsVPN_Setup.msi" /qn /norestart
```

Command details:

- /i: Installs or updates the product.
- /qn: "Quiet No UI" mode (completely silent installation as a background task).
- /norestart: Prevents the system from restarting automatically if a restart is required (optional).

The Cybels VPN client starts automatically once the update has been installed.

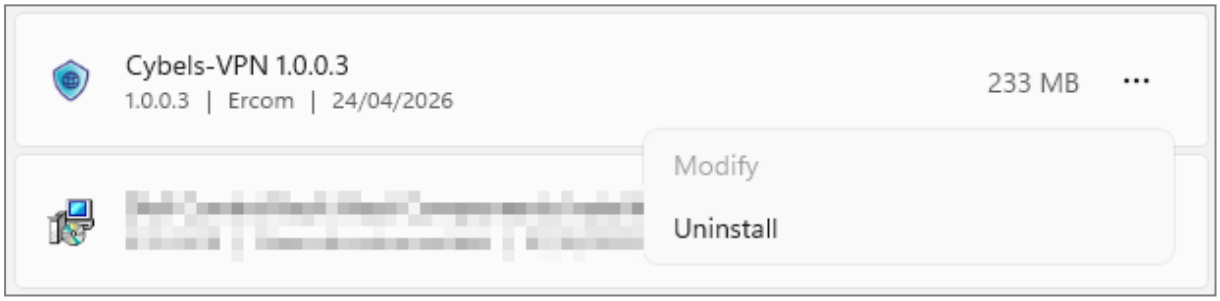
Uninstalling the VPN client

The application can be uninstalled from the PC regardless of which Essential or Premium variant was initially installed.
The administrator can uninstall the application in several ways:

Manual uninstall

Follow the steps below to uninstall the Cybels VPN client (local administrator privileges required):

1. Open the Windows **Control Panel**.
2. Select **Uninstall a program**.
3. Select Cybels VPN client from the list of programs.
4. Click on **Uninstall** and follow the instructions to uninstall the program.



Managed uninstall

- If you are using a **group policy** (GPO), EMM/MDM, ask your system administrator for advice on configuration.
- In command line (local administrator privileges required)

```
msiexec /x "CybelsVPN_Setup.msi" /qn
```

Once the uninstall has been launched, the installation folder will be deleted, the VPN service will no longer appear in the task manager, the Cybels VPN shortcut will be removed, and all entries relating to the application will be deleted.

By default, configuration files and the user's VPN profiles are retained even after an uninstall. This measure makes it possible to immediately restore the work environment if the application is reinstalled in the future.

Manual tunnel configuration

This section explains the required parameters for the manual configuration of options that are necessary for setting up a VPN tunnel, assuming that the installation was properly conducted, and the technical requirements were met.

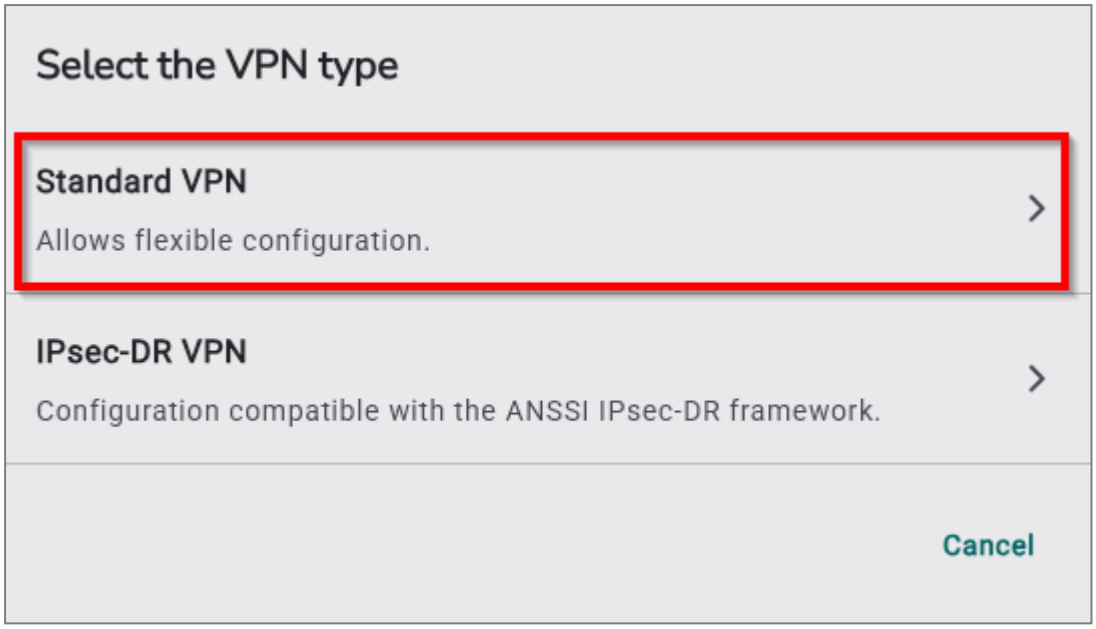
Configuring a standard tunnel

The chosen approach for standard tunnels involves displaying all IPsec tunnel parameters, including those that cannot be modified. By making all parameters visible, the administrator will be able to accurately confirm the validity of the application's behavior, and remove any ambiguity regarding the applied parameters.

To start configuring a VPN tunnel, open the application and click on "**Configure your first VPN**".

IMPORTANT
The user certificate and root CA have to be imported in advance into the relevant Windows storage locations. The Cybels VPN application will then search for these certificates respectively in the Personal folder (for user certificates), and in the Trusted root certification authorities folder (for the root CA) in the current user's Windows store.
Cybels VPN only reads certificates with their private keys.
For information, the gateway allows exporting a certificate with its private key in pem and p12 formats, however, Windows only manages certificates + keys in p12 format.

Select the desired VPN type, which is Standard VPN in this case.

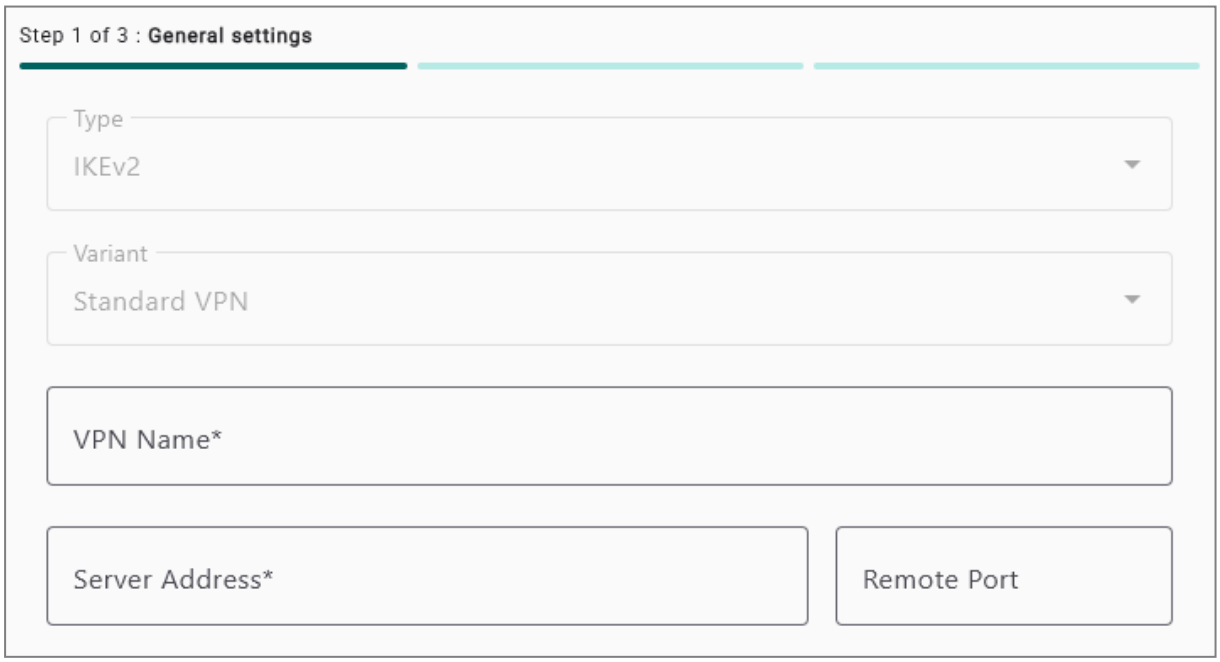


Step 1 (General settings)

Next, enter a name for the VPN tunnel that you wish to create, the server address and remote port in the fields "**VPN name**", "**Server address**" and "**Remote port**". If no ports have been configured, the default value 4500 will apply.

The address of the VPN server is the IP address or public DNS of the VPN gateway to which the client connects in order to set up the IPsec tunnel. This is the tunnel's entry point. Currently limited to the IPv4 protocol.

The negotiation and IPsec tunnel management protocol is an Internet Key Exchange version 2 (IKEv2) protocol, which offers a high level of security and performance, even for mobile users.

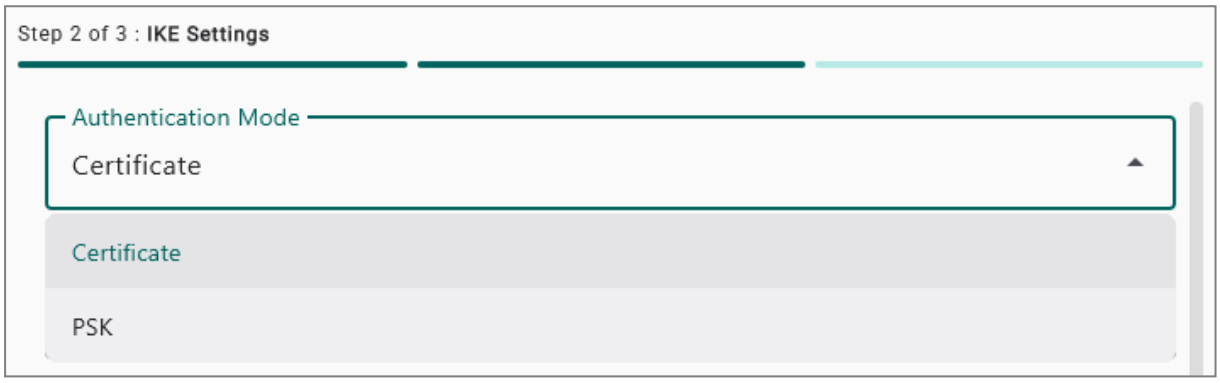


Once you have completed step 1, click on "**Next**".

Step 2 (IKE settings)

Step 2 defines the method that the workstation and gateway will use to authenticate and prove their identity.

NOTE
The selected configuration must be strictly aligned with the parameters that were configured on the VPN gateway.



These parameters include "**Authentication mode**": **certificate** or **PSK** (Pre-shared Key), based respectively on certificates or pre-shared keys.

In the VPN tunnel configuration, authentication modes determine how both tunnel endpoints prove their identity before setting up the secure connection.
"Certificate" and "PSK" modes are the two most common IKE authentication methods.

In "**Certificate**" mode, each tunnel endpoint (client and server) uses an X.509 digital certificate, which is signed by a certification authority (CA) to prove its identity. The certificate contains a public key, as the associated private key remains secret, and trust is established through the CA.

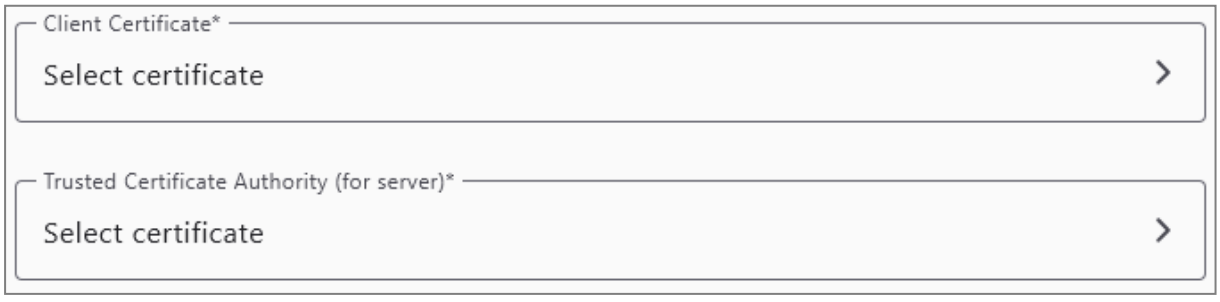
In "**PSK**" mode, both endpoints share a common secret (password), which is manually configured and identical on both sides. The client and server have to prove that they know the same key, and if the key matches, the tunnel will be set up.

"Certificate" authentication mode

Requirements: Before selecting this mode, ensure that:

- There is a valid user certificate on the workstation (Windows store or hardware medium).
- The server's CA (certification authority) certificate has been installed in the Windows certificate store.

If "certificate" authentication mode is selected: on the server side, the client certificate and trusted certification authority (CA) must then be selected from those automatically detected by the client and suggested in the form of a drop-down list, by clicking on the > symbol.



The **client certificate** is the X.509 digital certificate installed on the user's workstation, and is used as a strong authentication method for the VPN client when setting up the secure tunnel. When the Cybels VPN client uses certificate authentication, the client will present its certificate to the server during IKE negotiation.

This certificate was imported in advance into the hosting medium based on security requirements, client workstation capacities, and the certificate management policy.

There are several possible hosting options:

- The Windows user certificate store, with the private key protected by software modules
- A secure hardware medium (cryptographic USB key and smart cards)

Hardware storage modules are available only in the Cybels VPN Premium version.

NOTE
To simplify the selection of certificates, and to minimize the risk of errors, the application automatically filters certificates. As such, the following are not listed:

- Certificates that have expired, or which will only be valid in the future.
- Certificates that use an X.509 version lower than v3.
- Self-signed certificates (these cannot be used as user certificates).

The **trusted certification authority (for the server)** is the certification authority (CA) whose certificate the VPN client uses to verify the authenticity of the certificate presented by the VPN server. The client will only accept the connection if the server certificate is signed by this authority, and if it matches the expected identity.

NOTE
Likewise, only valid authorities are listed. The following are excluded:

- CA certificates that have expired, or which will only be valid in the future.
- CA certificates in an X.509 version lower than v3.
- Note: Unlike client certificates, self-signed CA certificates are accepted and listed.

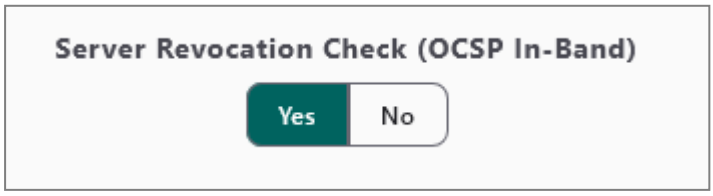
The CA would also have been imported in advance into the hosting medium based on security requirements, client workstation capacities, and the certificate management policy.

The following field, "**Server revocation check**", refers to the security mechanism that allows the Cybels VPN client to check whether the VPN server certificate presented during the connection has been revoked by the PKI that issued it.

This verification ensures that the VPN client does not trust a server with a certificate that the CA has explicitly declared to be untrustworthy.

The administrator will then choose to check the server certificate's validity by clicking on "**Yes**" or "**No**".

The revocation check is conducted directly in VPN traffic during IKE negotiation, by relying on in-band OCSP, as defined in RFC 4806.



The next section relates to local and remote IDs. The local ID is the identity that the client presents to the server, while the remote ID is the identity that the client expects to receive from the server.

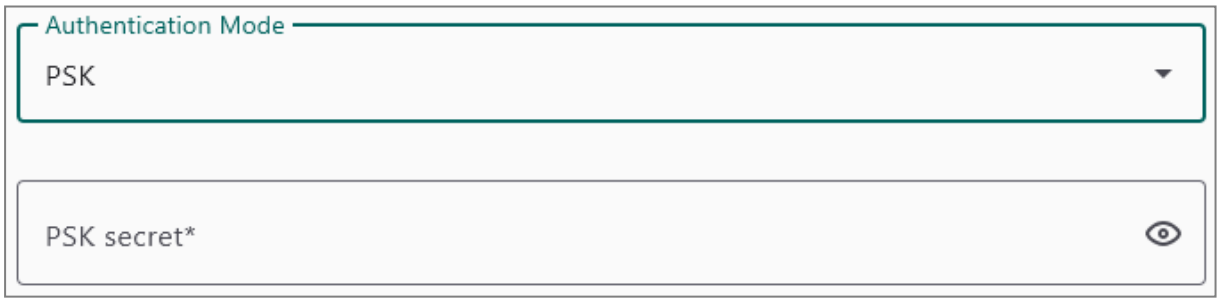
These identities are used during authentication and have to be consistent with the certificates or keys that have been configured.

The administrator can choose one of several modes from the drop-down menu:

- **FQDN** (Fully Qualified Domain Name): this is the full domain name that generally corresponds to the CN or DNS of the server certificate (e.g., vpn.entreprise.tld)
- **EMAIL**: this is the identity in email address format used as the logical ID that usually corresponds to the SubjectAltName in the client certificate
- **ASN.1 DN**: this is the identity based on the Distinguished Name of the X.509 certificate with ASN.1 encoding, which is an exact match to the certificate's Subject

"PSK" authentication mode

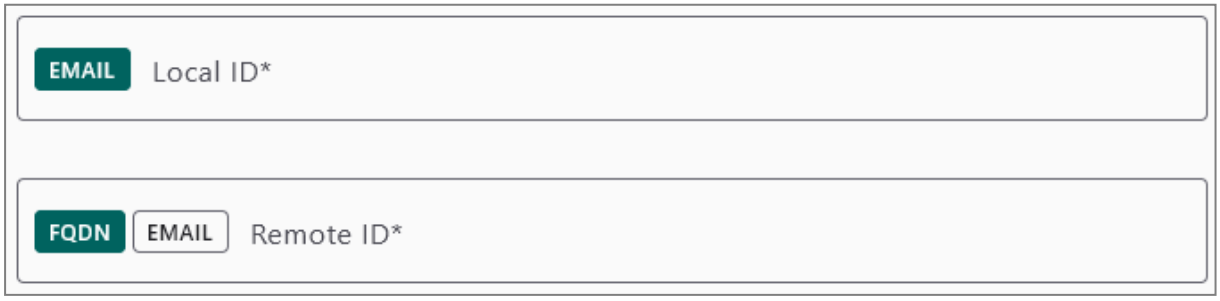
If "**PSK**" authentication mode is selected, the value of the pre-shared key will then need to be entered in the "**PSK secret**" field.



This key is used during IKE negotiation for authentication, and to prove that the client and server are who they claim to be.

The administrator can view the password by clicking on the **eye** icon. Clicking on the icon a second time will hide the password.

Next, enter the information regarding the **Local ID** and **Remote ID** based on the **FQDN** or **Email address.**

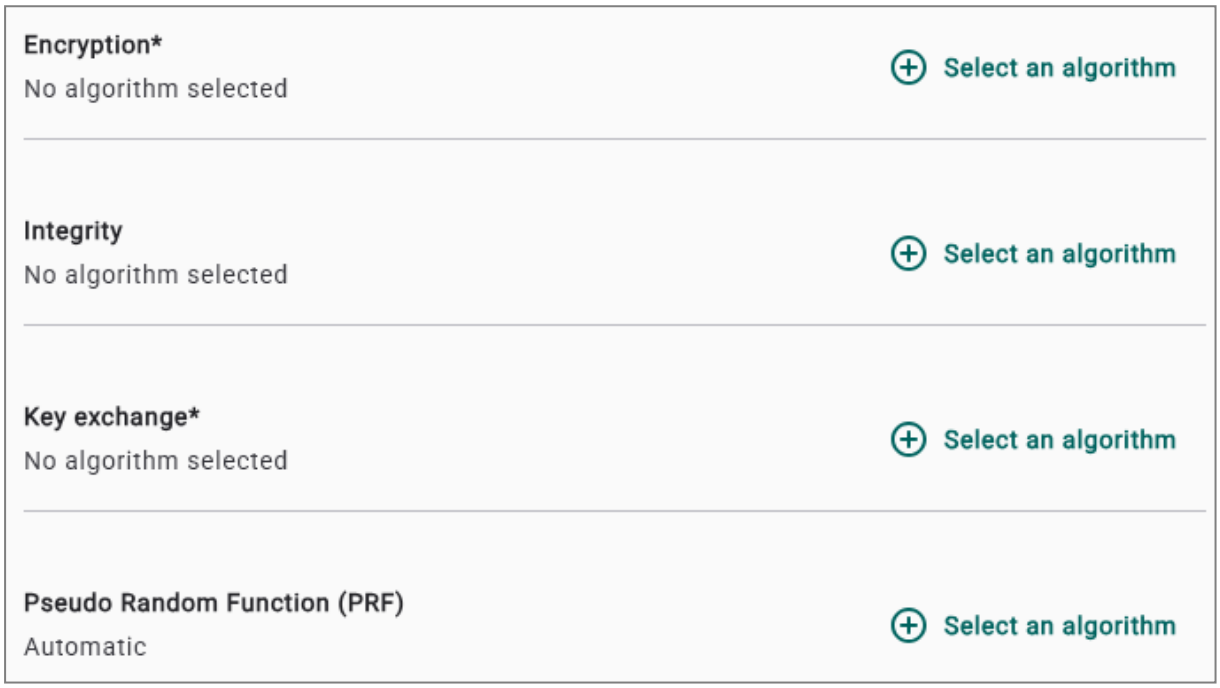


The Local ID and Remote ID are used to formally identify each VPN endpoint during IKE negotiation to inform each device (PC and VPN server) that it is about to set up the tunnel, and to ensure that the right peer is involved.

The administrator can choose the desired ID format by selecting "FQDN" or "EMAIL".

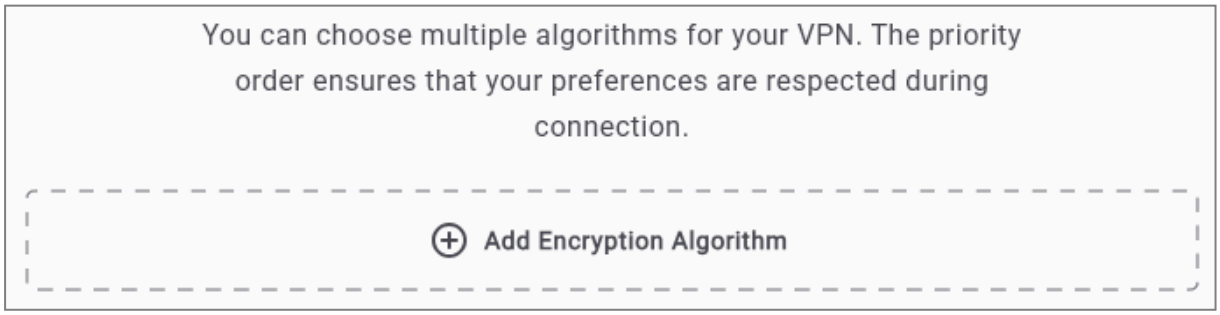
Cryptography for IKE (certificate or PSK mode)

In the following section, the administrator configures the desired cryptographic aspects for the VPN tunnel. Encryption, integrity, key exchange and pseudo-random function algorithms have to be selected from several suggestions.



To do so, the administrator starts by clicking on "Select an algorithm" in each section, according to the order in which they appear in the interface (encryption, integrity, key exchange and PRF).

For example, by starting with the "**Encryption**" section, the following window will appear, making it possible to add one or several encryption algorithms by clicking on "**Add Encryption Algorithm**".



The following encryption algorithms are available:

- AES CBC 128, AES CBC 192, AES CBC 256, AES CTR 128, AES CTR 192, AES CTR 256, AES GCM-16 128, AES GCM-16 192, and AES GCM-16 256

The following integrity algorithms are available:

- SHA 256, SHA 384, and SHA 512

The following key exchange algorithms are available:

- Group 14 (2048-bit MODP), Group 15 (3012-bit MODP), Group 16 (4096-bit MODP), Group 17 (6144-bit MODP), Group 18 (8192-bit MODP), Group 19 (256-bit ECP), Group 20 (384-bit ECP), Group 21 (521-bit ECP), Group 28 (256-bit ECP), Group 29 (384-bit ECP), and Group 30 (512-bit ECP)

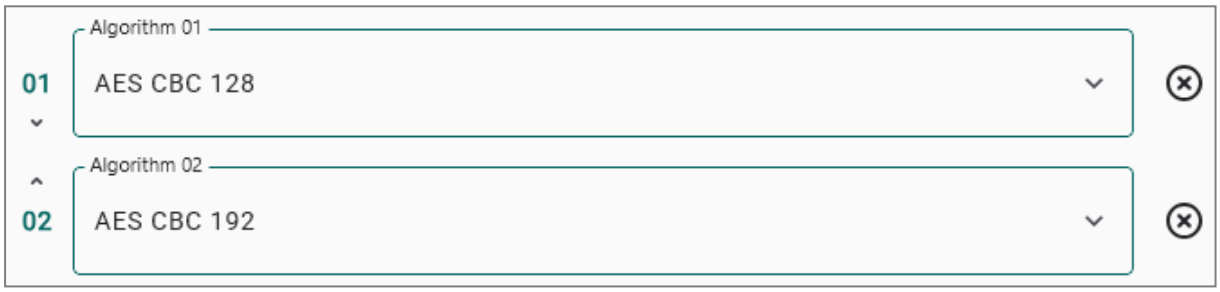
The following pseudo-random function algorithms are available:

- SHA 256, SHA 384, and SHA 512

The following signature algorithms are available:

- RSA PKCS#1 v1.5 SHA-2 256, RSA PKCS#1 v1.5 SHA-2 384, RSA PKCS#1 v1.5 SHA-2 512, ECDSA SHA-2 256, ECDSA SHA-2 384 DER, ECDSA SHA-2 512 DER, and ECDSA 256 RAW

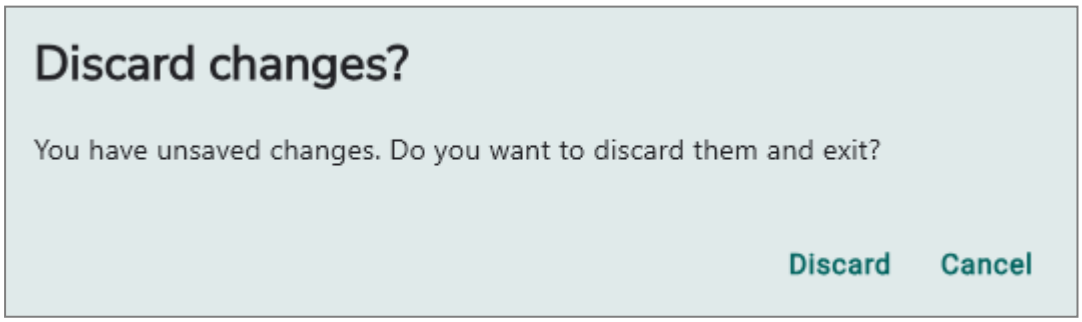
Several algorithms can be chosen from the list above, and an order of priority can also be set by using the arrows found next to the numbers. In the example below, AES CBC 128 will have priority over AES CTR 192 as it has been placed in the first position.



Once you have chosen your encryption algorithms in this first section, click on "Validate" to save your selection.

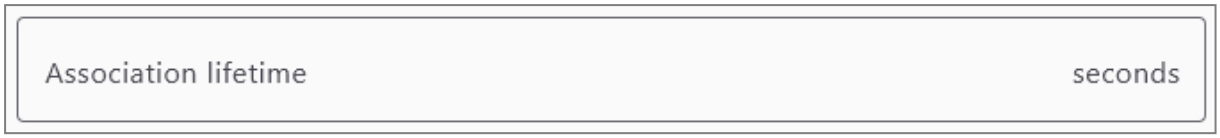
Follow the same process to select "Integrity", "Key exchange" and "Pseudo-random function (PRF)" algorithms. PRF has an automatic selection option (by default), which means that all algorithms will be supported to facilitate interoperability.

You can backtrack at any time, or decide not to save the current selection, by clicking on "Discard". A pop-up will warn the administrator in this case.



The following field relates to the association lifetime, which corresponds to the validity period of the IKE before its mandatory renewal (IKE reauth).

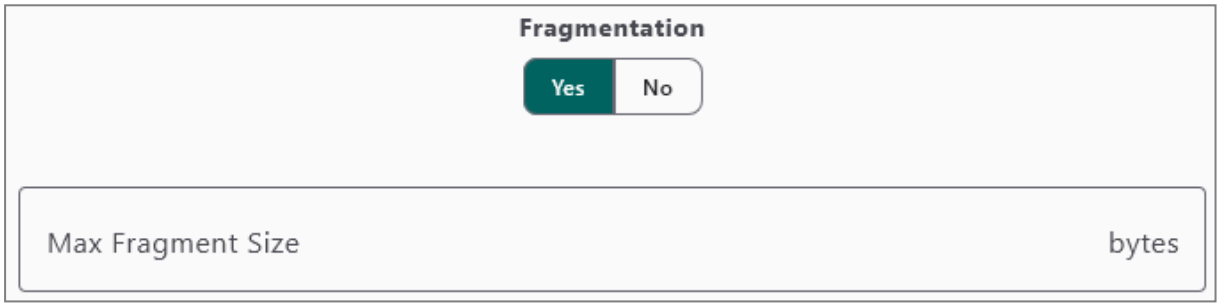
When this period expires (expressed in seconds), the client will launch a **full reauthentication** of both endpoints (peers). This process will generate new encryption keys to guarantee that the tunnel remains secure.



If no value has been entered, the default lifetime will be applied. It is 14,440 seconds.

NOTE
The renewal process may briefly disrupt the connection (generally for 2 to 3 seconds) while the new session is being validated.

The next step is the configuration of fragmentation, which makes it possible to segment large messages so that they can pass through certain restrictive networks more easily.



The administrator can choose whether to enable fragmentation by selecting "Yes" or "No".

- Disabled (No): the client does not offer fragmentation.
- Enabled (Yes): the client offers fragmentation at the gateway.
- Max fragment size: sets the upper fragmentation limit in bytes (default value: 1280 bytes).

NOTE
Fragmentation on the client side is only a suggestion. For messages to be effectively fragmented, the feature must be simultaneously enabled and supported on the VPN server.

The last menu enables the selection of "Childless mode". In this mode, only the VPN control connection is set up, without creating the data tunnel. No encrypted network traffic is exchanged.

This mode operates as follows:

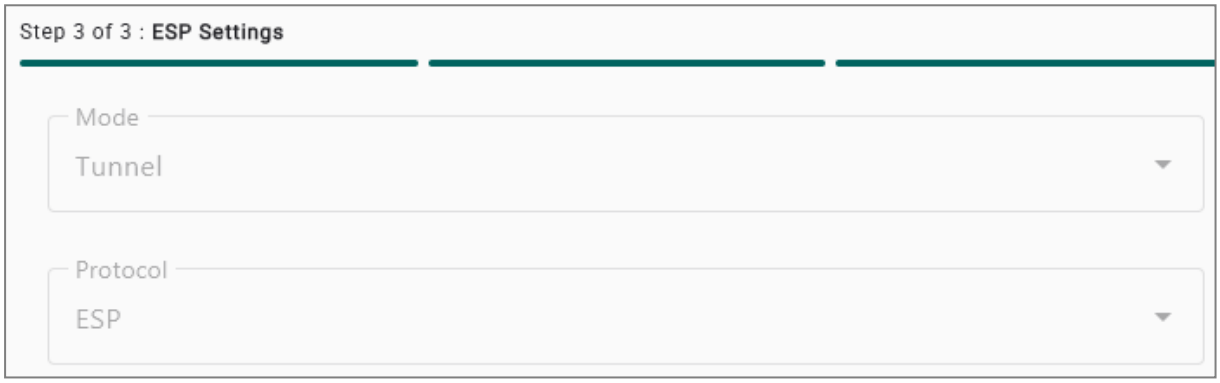
- If enabled (Yes): The application sets up only the initial control channel. The data tunnel (Child SA) will only be created when actual network traffic is detected. In this way, gateway resources will not be unnecessarily consumed when there is no data traffic.
- If disabled (No): The data tunnel will be systematically and immediately created after a successful IKE authentication, even when there is no traffic.

Step 3 (ESP settings)

Step 3 consists of configuring the data traffic protection policy.

- "Tunnel" mode (imposed): Unlike transport mode, tunnel mode encapsulates the entire original IP packet (data + header). This is the only mode that makes it possible to hide the internal architecture of the client network from the public network.
- "ESP" protocol (imposed): The application relies exclusively on the Encapsulating Security Payload. This is the benchmark protocol that simultaneously guarantees confidentiality (encryption), integrity and the authentication of communications.

NOTE
Both of these fields are displayed in the interface to allow the administrator to confirm the tunnel's compliance, but they are locked to prevent a lower level of security from being configured.

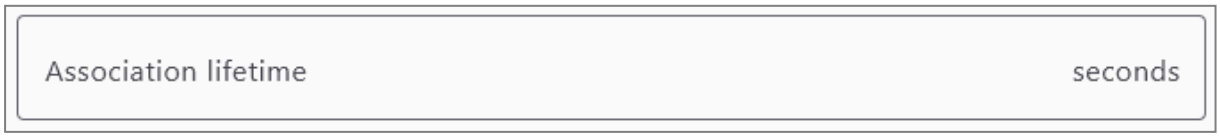


Algorithm selection

Next, the administrator will select the encryption, integrity and key exchange algorithms in the same way as in step 2, by clicking on "**Select an algorithm**" for each of the parameters below.

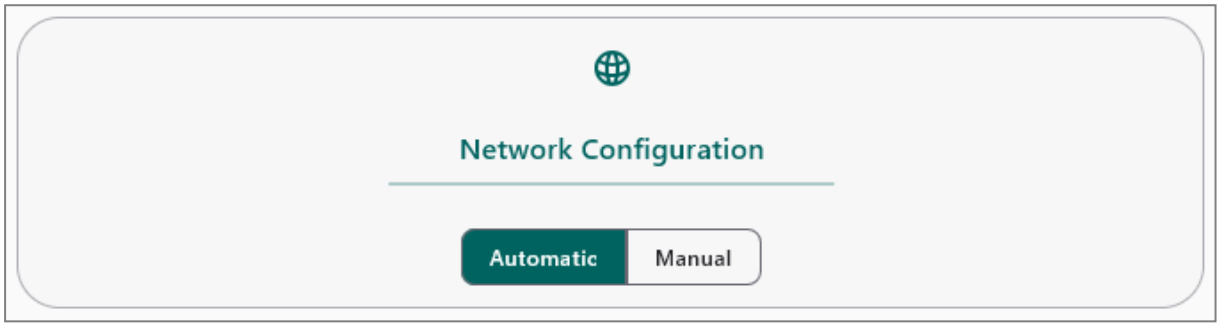
Association lifetime and network configuration

If necessary, set the "**Association lifetime**" that corresponds to the period for which the ESP keys and the association's security settings will remain valid (rekey). The lifetime is expressed in seconds. If no value has been entered, the default lifetime will be applied. It is 900 seconds.



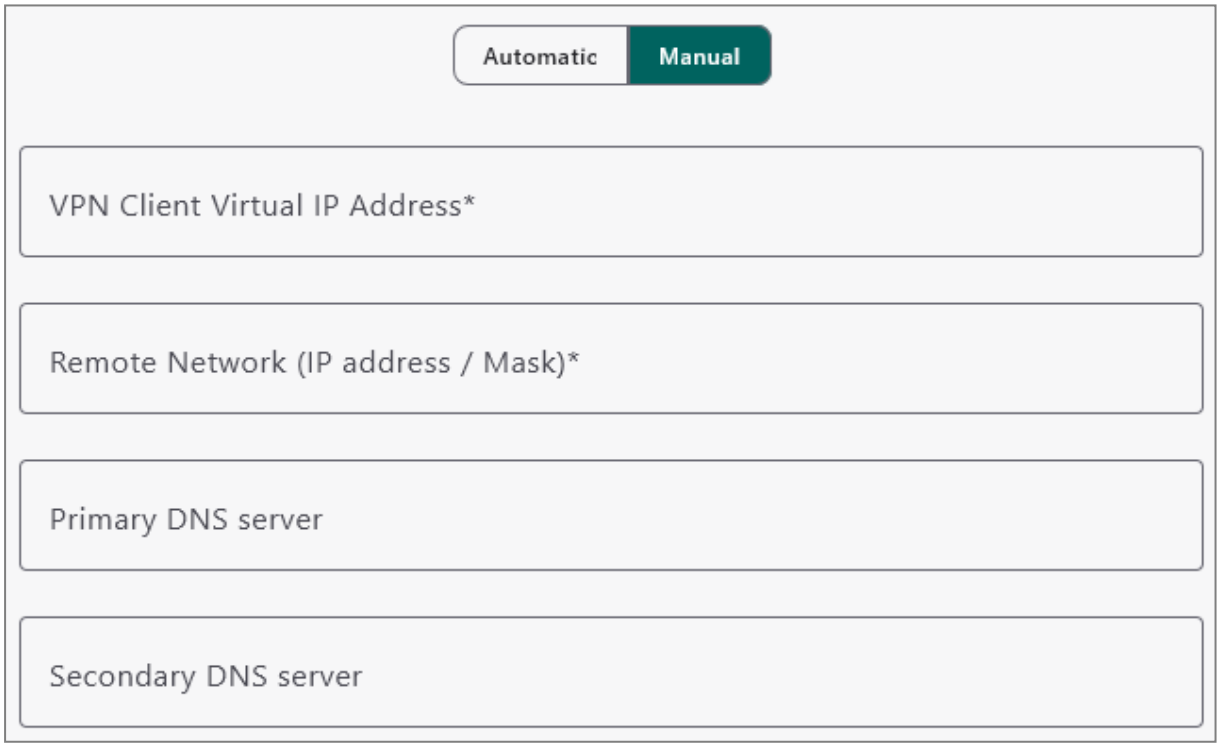
NOTE
The rekey process has been designed to be transparent, and generally does not disrupt traffic, unlike IKE reauthentication, which may cause a brief disruption.

The administrator then sets the network configuration mode, "**Automatic**" or "**Manual**". This configuration involves setting the characteristics of the network traffic to be protected, meaning the traffic that has to pass through the IPsec tunnel.



In automatic mode (also known as "Configuration Payloads" in IKEv2), network parameters are automatically provided by the remote IPsec server.

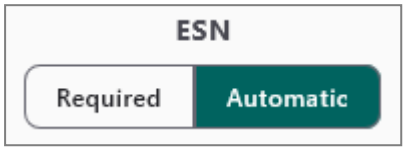
In manual mode, the administrator configures all the following fields: "**IP address**", "**Remote network**", "**Primary DNS server**", and "**Secondary DNS server**".



- The IP address is used to route traffic, and can also be used as the client's unique identifier on the network.
- The remote network is the network found on the other side of the VPN tunnel, which the client has to access. The expected format is expressed in CIDR address notation *IP/mask*.
- The primary DNS server is the priority domain name resolution server, and has to be accessible from the network or VPN.
- The secondary DNS server will take over when an error occurs or when there is an issue with the configuration of the primary server.

Extended Sequence Number (ESN)

In the last step, the administrator will choose whether to enable the ESN. This parameter makes it possible to use longer sequence numbers (64 bits instead of 32 bits) for IPsec packets. This parameter is negotiated by default.



Without ESN ("**No**" selected), the counter is set to **32 bits** and can quickly overflow onto very fast links or very active tunnels.

With ESN ("**Yes**" selected), the counter switches to **64 bits**, which practically removes the risk of overflow, and the tunnel is more robust over the long term.

To complete step 3, click on "**Create tunnel**".

The implemented signature algorithms are RSA PKCS#1 v1.5 SHA-2 256, RSA PKCS#1 v1.5 SHA-2 384, RSA PKCS#1 v1.5 SHA-2 512, ECDSA SHA-2 256, ECDSA SHA-2 384 DER, ECDSA SHA-2 512 DER, and ECDSA 256 RAW.

NOTE
Algorithms cannot be selected for signatures. The contents of the certificate will determine the signature algorithm used.

Configuring a "*Diffusion Restreinte*" tunnel

The Cybels VPN client (Premium version) makes it possible to automatically configure VPN tunnels that comply with the IPsec *Diffusion Restreinte* (DR) guidelines set out by the ANSSI.

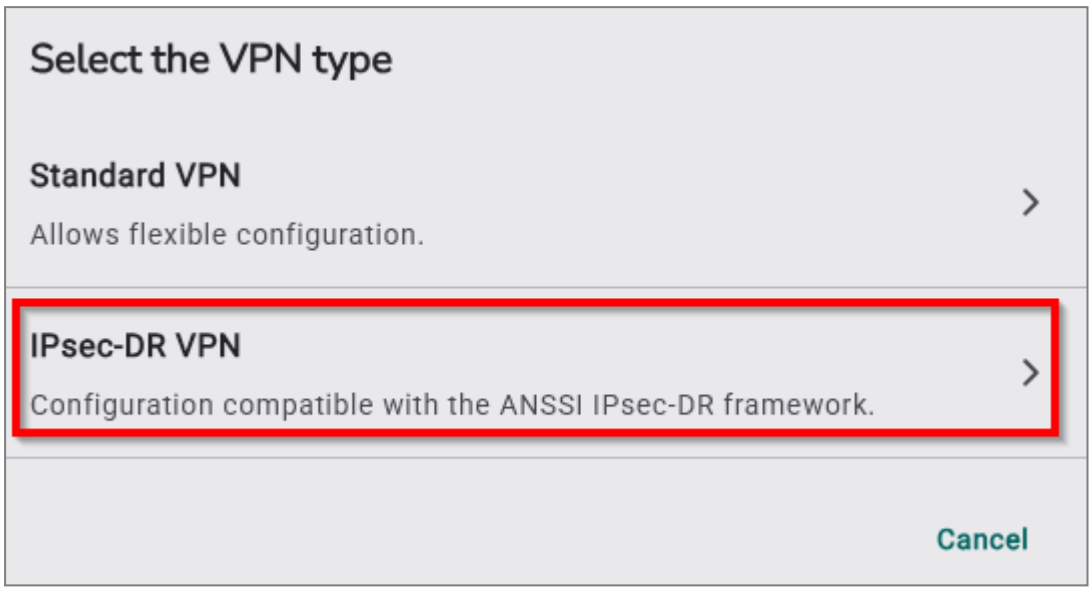
The IPsec DR profile aims to guarantee a high and consistent level of security for IPsec VPNs used in:

- Government agencies,
- Vital operators,
- Systems that handle sensitive data, but which are not classified as national defense secrets.

In this mode, the administrator does not need to manually select all parameters imposed by the IPsec DR profile (cryptographic suites, childless mode, etc.). These settings are applied natively by the application during initialization, thereby guaranteeing a configuration that complies with ANSSI guidelines, while drastically reducing the risk of human error.

IMPORTANT
In order for the connection to be successful, the VPN gateway (firewall or hub) must also be configured in an IPsec DR-compliant mode. All devices in the architecture have to meet these ANSSI requirements.

To initiate the configuration of an IPsec DR VPN tunnel, click on "**Add a VPN**", then select "**IPsec-DR VPN**".



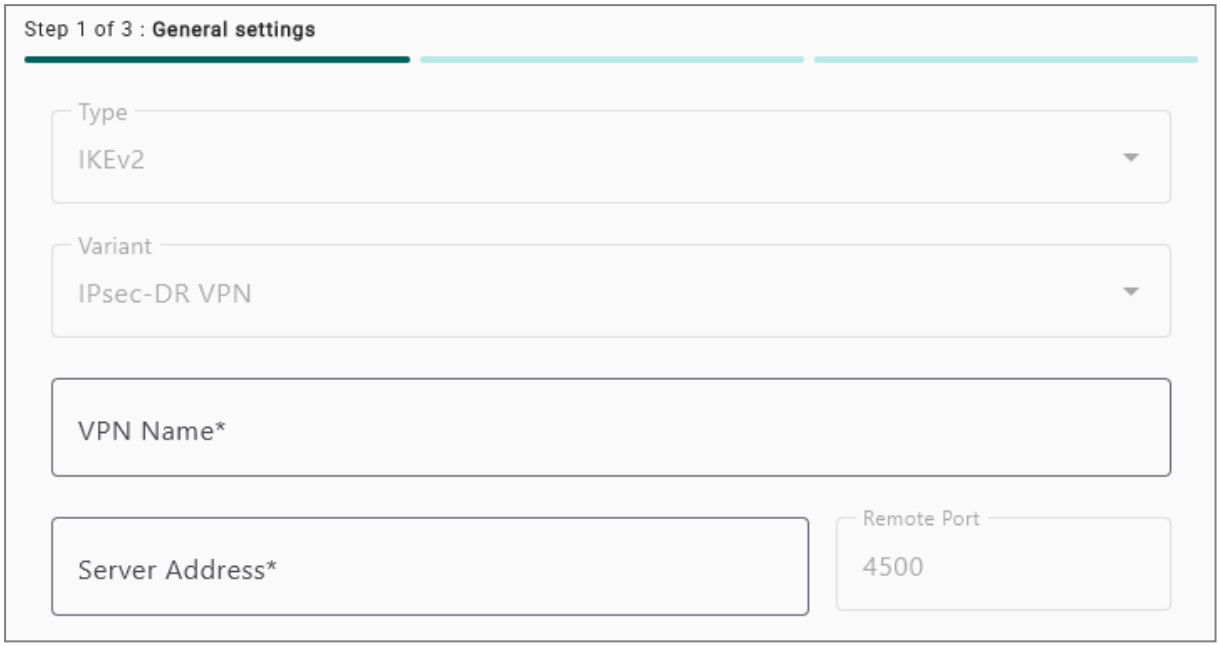
Step 1 (General settings)

Next, enter a name for the VPN tunnel that you wish to create, as well as the server address in the "**VPN name**" and "**Server address**" (IP address or FQDN of the VPN gateway) fields.

NOTE
Currently, only the IPv4 protocol is supported.

The default port is **4500 (NAT-T)** when this mode is selected.

NOTE
In line with the imposed security profile, this port cannot be modified, in order to guarantee the use of the NAT traversal standard, as required by the guidelines.



Cryptographic settings

Cryptographic suites are pre-configured according to IPsec DR mode requirements. For the purpose of clarity, these parameters are hidden in the interface.

Do note that the application offers the following combinations during negotiation:

	Encryption	Integrity	Key exchange	PRF
Suite 1	AES GCM-16 256	None*	Group 19 (256-bit ECP)	SHA 256
Suite 2	AES GCM-16 256	None*	Group 28 (256-bit Brainpool ECP)	SHA 256
Suite 3	AES CTR 256	SHA 2256	Group 19 (256-bit ECP)	SHA 256
Suite 4	AES CTR 256	SHA 2256	Group 28 (256-bit Brainpool ECP)	SHA 256

(*) Integrity is natively guaranteed through the GCM encryption mode.

Step 2 (IKE settings)

By default, the authentication mode is "**Certificate**" in the IPsec DR variant. PSK (pre-shared key) mode is disabled and cannot be selected for IPsec DR tunnels.

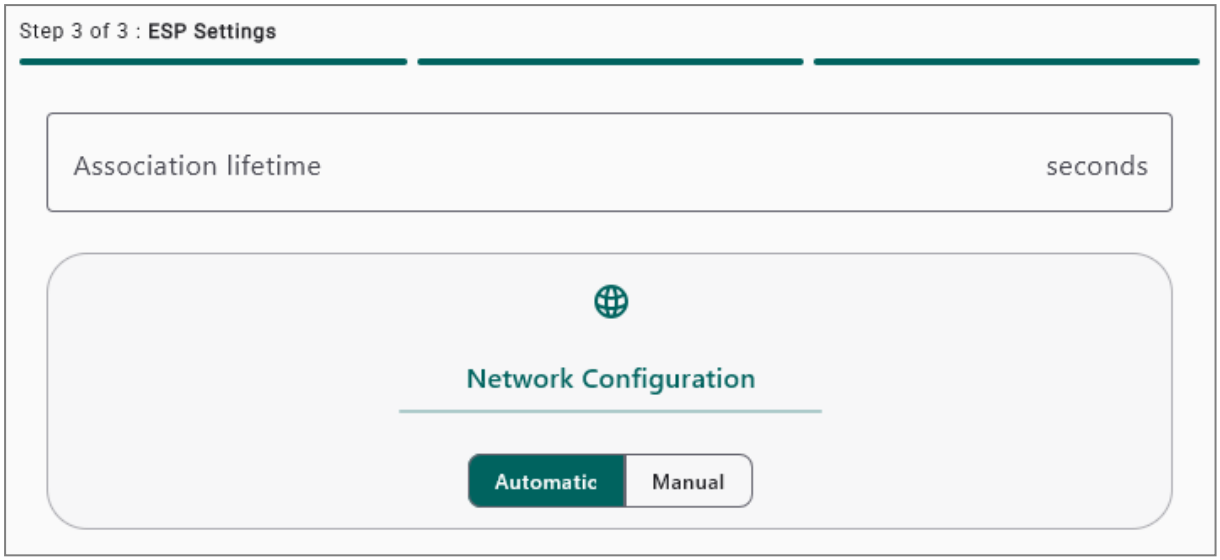
To configure this step, refer to chapter "Certificate" authentication mode.

Childless mode is enabled by default and imposed, in line with the IPsec DR guidelines.

Step 3 (ESP settings)

Step 3 consists of entering the ESP (Encapsulating Security Payload) parameters that will be used to protect data passing through the VPN.

The administrator will then select the association lifetime and network configuration mode, "Automatic" or "Manual".



Refer to chapter Association lifetime and network configuration.

The ESN is forced to 64 bits in the case of a DR type tunnel.

Cryptographic settings

Cryptographic suites are pre-configured according to IPsec DR mode requirements. For the purpose of clarity, these parameters are hidden in the interface.

Do note that the application offers the following combinations during negotiation:

	Encryption	Integrity	Key exchange
Suite 1	AES GCM-16 256	None*	Group 19 (256-bit ECP)
Suite 2	AES GCM-16 256	None*	Group 28 (256-bit Brainpool ECP)
Suite 3	AES CTR 256	SHA 2256	Group 19 (256-bit ECP)
Suite 4	AES CTR 256	SHA 2256	Group 28 (256-bit Brainpool ECP)

(*) Integrity is natively guaranteed through the GCM encryption mode.

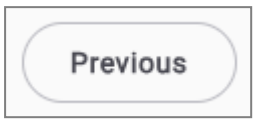
The implemented signature algorithm is: ECDSA 256 RAW

To complete step 3, click on "**Create tunnel**".

Finalizing the creation of the tunnel

The VPN client will show a recap of all the parameters that were set in steps 1, 2 and 3, allowing the administrator to make changes if necessary, by clicking on "**Back to configuration**", or by confirming the configuration and clicking on "**Save configuration**".

By clicking on "Back to configuration", the administrator will be redirected to step 3, and can browse through the various steps by using the "Previous" button.



By clicking on "Save configuration", the tunnel will be created. A toast notification will indicate that the tunnel was successfully created.

All parameters will then be grouped together in the "**General**", "**IKE**" and "**Child SA**" tabs for consultation.

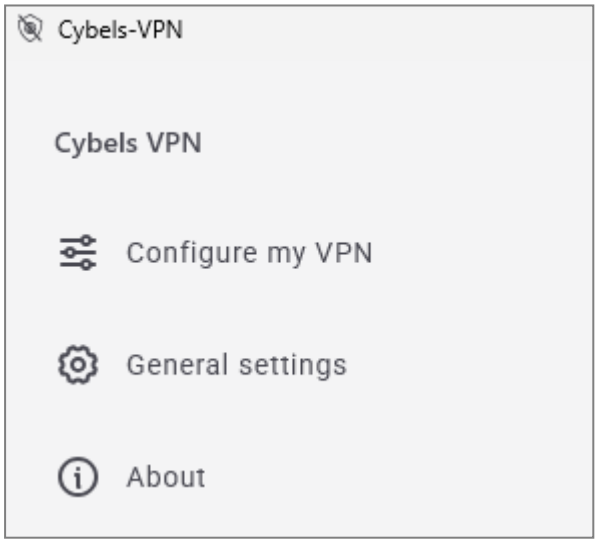
Additional actions

The administrator has 2 additional buttons on the recap page to **Edit** or **Delete** the created tunnel.

Configuring multiple tunnels

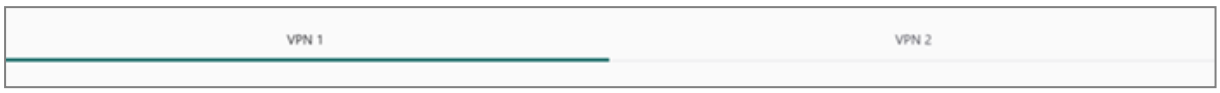
Multiple VPN tunnels can be configured. To do so, simply repeat the same steps described for the creation of a tunnel.

All configured tunnels can be found in the application's "**Configure my VPN**" side menu.



Click on this menu to view and obtain information, and to edit and delete tunnels.
In the example below, 2 tunnels have been configured: test and Cybels VPN Client.

All configured VPNs are shown on the application's welcome page.
In the example below, 2 VPNs are available:



As soon as a green dot appears next to the VPN, this means that this VPN's tunnel is active.

The following chapter describes how to activate a VPN tunnel.

NOTE
Although multiple VPN tunnels can be configured, only one tunnel can be active at a time.

Managed tunnel configuration

This section explains the required parameters for the managed configuration of options that are necessary for setting up a VPN tunnel, assuming that the installation was properly conducted, and the technical requirements were met.

IMPORTANT
The user certificate and root CA have to be imported in advance into the relevant Windows storage locations. The Cybels VPN application will then search for these certificates respectively in the Personal folder (for user certificates), and in the Trusted root certification authorities folder (for the root CA) in the current user's Windows store.

Managed configuration means that the administrator:

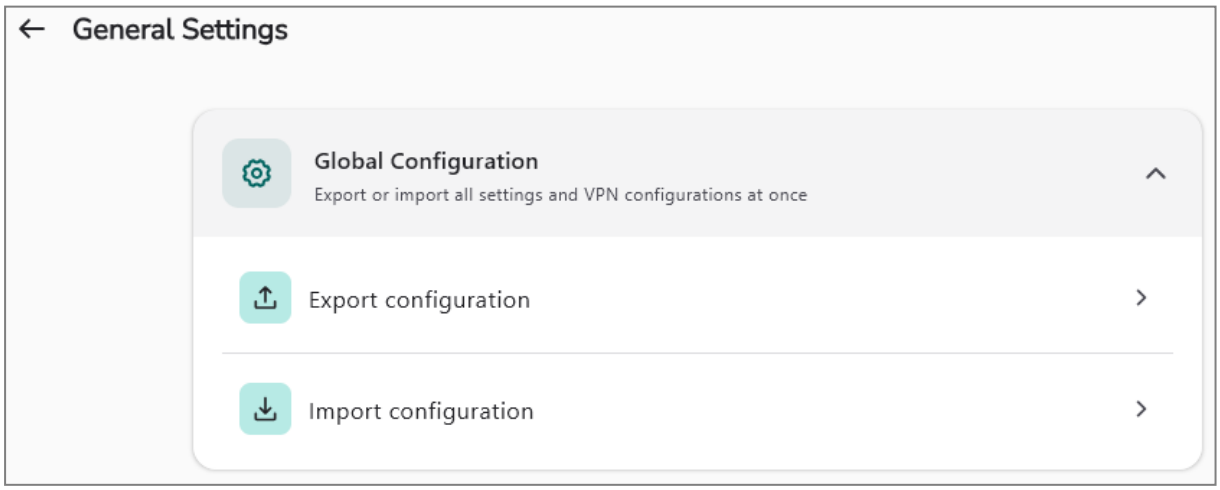
1. Sets and runs the steps in the manual configuration (see Manual tunnel configuration) on a workstation, and finalizes the creation of the configuration.
2. Exports this configuration (see Exporting and importing configurations)
3. Manually deploys this configuration on several user workstations through the Cybels VPN application (importing configurations) or with administration tools such as an EMM/GPO.

This configuration feature is useful for creating configuration backups before making changes or conducting tests, and also for building a configuration "template" that can be replicated on several workstations, which saves time, compared to individual manual configurations on several workstations.

Exporting and importing configurations

Exporting the configuration from a reference workstation

In the VPN client interface, the administrator opens the Cybels VPN application's general settings and selects "**Export configuration**". The application generates a json file according to the configuration created manually and anonymized (no exported user information in the json file)



Importing the configuration to the fleet

Individually:

This configuration can be imported by clicking on "**Import a configuration**" on one or several workstations.

Bulk (*Available in the Cybels Premium version*):

- Simply place this configuration file in the following folder **C:\ProgramData\Ercom\Cybels-VPN**
- The name of the file has to follow the format **vpn_config.json**

Finalizing the configuration

As mentioned previously, user settings are not exported to the json configuration file. They must be filled in after importing the generic configuration.

There are two ways to do this.

Manual configuration customization for PSK and certificate

For PSK and certificate, from the VPN client interface: from the Configure my VPNs menu, click on the icon associated with the tunnel whose configuration you want to complete.

And enter the missing information to finalize the configuration of the tunnel in PSK mode or select the desired user certificate if the tunnel was configured in certificate mode.

> **NOTE**
> If ModeConfig is activated (see Association lifetime and network configuration, the application does not request the virtual IP address of the VPN client

Managed configuration customization for certificate

Available in Cybels Premium version

BEFORE importing the configuration to the fleet of PCs to be configured (see Importing the configuration to the fleet), the administrator can simplify the selection of the user certificate **from the configuration file** by filtering on one or more criteria.

To do this, open the imported configuration file in a text editor. This file contains empty values in the "certificateFilters" tag which must be completed based on the configuration/certificate of the reference station.

Filtering can be performed on one or more of the following criteria:

- Organization (O) of the user certificate
- Organizational unit (OU) of the user certificate
- Country (C) of the user certificate
- User certificate State/Region (ST)
- Location/City (L) of user certificate
- Distinguishing name of the issuer of the user certificate. To avoid any format incompatibility, the issuer's DN must be copied (using the copy button on the Cybels VPN interface) from a user certificate from the reference station.

Then, these fields are filled in via the configuration file in the different "value" tags corresponding to the above criteria.

```
"certificateFilters": [
        {
                "criteria": [
                        {
                                "field": "O",
                                "value": ""
                        },
                        {
                                "field": "OU",
                                "value": ""
                        },
                        {
                                "field": "C",
                                "value": ""
                        },
                        {
                                "field": "ST",
                                "value": ""
                        },
                        {
                        "field": "L",
                        "value": ""
                        }
                ],
                "issuer": ""
        }
]
```

The json configuration file can then be deployed on the fleet of PCs to be configured, and when the application is started, it searches for a user certificate as follows:

- Case 1: If no certificate is found: no certificate is selected in the tunnel configuration (the tunnel configuration is therefore incomplete).
- Case 2: If only one certificate is found: this certificate is automatically selected in the tunnel configuration. The administrator does not have the possibility to select it himself (and cannot change it).
- Case 3: If several certificates match the criteria: the administrator must select one of these certificates.

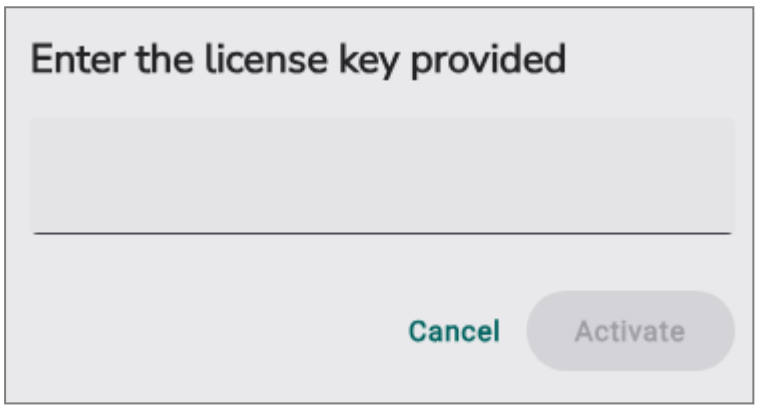
NOTE
The more criteria are entered, the more precise the certificate selection will be

License

To activate Cybels VPN, the administrator has to enter a valid license key, regardless of whether a Cybels VPN Essential or Cybels VPN Premium client is being configured.

Manual license configuration

In the Cybels VPN client interface, open the "General settings" menu and go to the License field to enter the key provided by your distributor.



Then click the “Activate” button to finalize the license configuration for the Cybels VPN client.

Managed license configuration

After you have exported the configuration, open the file with a text editor, then enter the key provided by your distributor in the “key” field.

```
"generalSettings": {
       “license”: {
       "key": ""
       }
}
```

After you have saved your changes, import the new configuration, and then deploy it on the desired workstation(s) with the administration tool of your choice, an EMM or GPO.

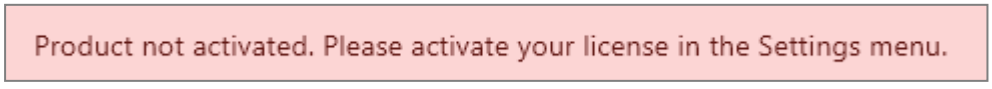
How licensing works for Cybels VPN

When purchasing the Cybels VPN software, the administrator receives a license key corresponding to the chosen variant (Essential or Premium).

This key must be entered and activated at the earliest during configuration (see above), and at the latest before the end of the automatic token release period (after 90 days).

For 90 days from the installation of the VPN client on the workstation and if no valid license key is entered, the VPN tunnel automatically disconnects every 15 minutes.

In addition, a persistent message is displayed to indicate that the configuration is incomplete.



After this 90-day period, if no license key has been entered or if the license key entered is invalid, the license cannot be activated. A new 90-day token is then automatically renewed by the Cybels VPN application.

Summary of the steps from installation to deployment

Step 1: Retrieve VPN client and license key

1. Download the .msi package
2. Retrieve license key

Step 2: Install the VPN client on a reference station

1. Install the .msi package on a reference station

Step 3: Configure the VPN tunnel on the reference station and export the configuration

1. Enter the license key (VPN client **Configuration** menu)
2. Configure the VPN tunnel
3. Export configuration in JSON format
4. If necessary, edit the .json file to add filters to make it easier to select the certificate
5. Upload the .msi package and the .json file to the EMM/GPO console

Step 4: Deploy VPN client and configuration to remote workstations

1. Set up the deployment of the .msi package and the .json file on the EMM/GPO console
2. *- Silent installation and configuration on remote workstations -*
3. Complete VPN client configuration (manual PSK entry or manual choice of certificate)

Step 5: Check for proper operation and manage the pool

- On the user side: connection tests, getting started, etc.
- Administrator side: pool management, gateway console view, log reporting and diagnostics, etc.

Using the VPN client

Manual start

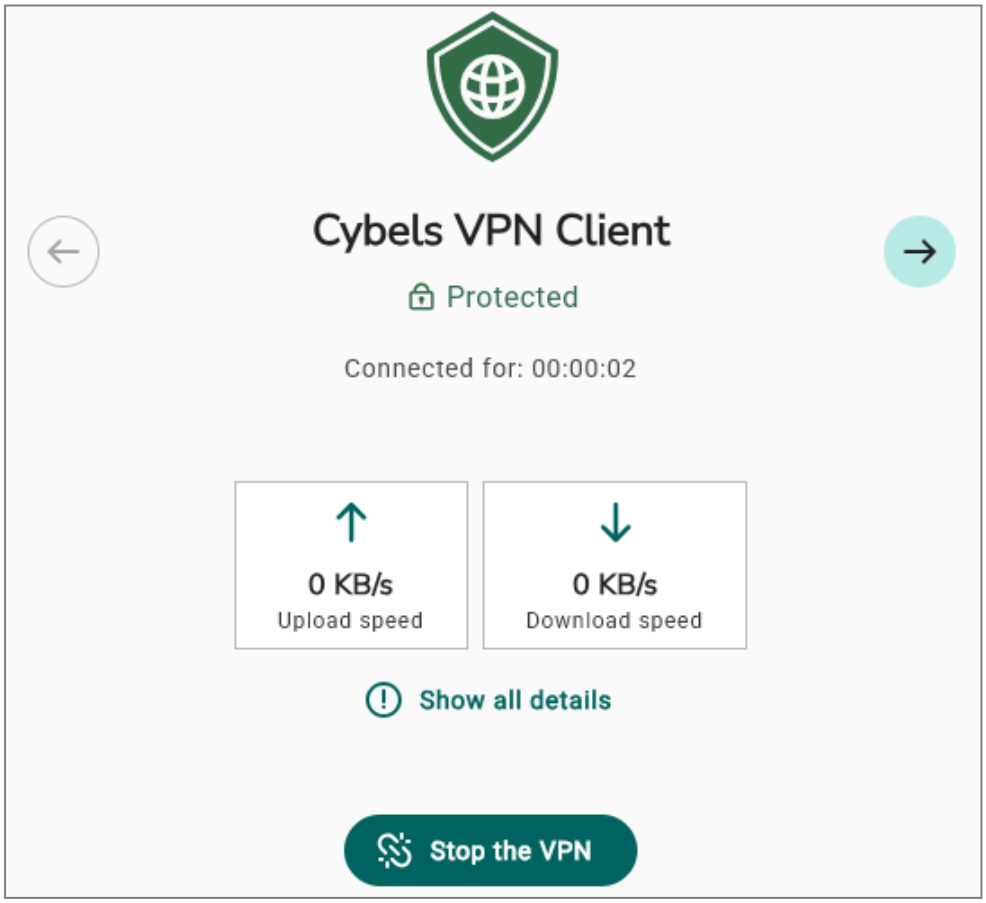
Manually starting Cybels VPN consists of voluntarily initiating a secure connection between the user's workstation and the remote network over an encrypted tunnel.

The connection remains active until it is manually disconnected, or when the network connection is lost or expires.

Click on "**Start the VPN**" to start the VPN session. Ensure that the workstation has an Internet connection.

The application indicates that the VPN has indeed been started, by showing several indicators such as:

- The "**Protected**" status with a green padlock in front of it
- The application logo in green
- How long the tunnel has been up, in the "**Connected for: ...**" field
- The name of the tunnel, "**Cybels VPN Client**" in the example below
- The upload and download speeds expressed in KB/s
- Additional details in "**Show all details**", to view all the parameters that were negotiated when the tunnel was being set up, based on the administrator's configuration.



Click on "**Stop the VPN**" to shut down the tunnel.

The connection remains up until it is voluntarily disconnected, there is an extended loss of network signal, or the session expires.

Automatic start

In a future version of Cybels VPN Premium

Event logs

The Cybels VPN client has a built-in logging mechanism that can record events relating to the operation of the application, including the local context in which it is run.

The log files generated by the mechanism contain various details, such as when the application starts and shuts down, configuration settings, when the tunnel is opened and closed, as well as error messages, warnings and information messages.

These logs are collected and can be read locally on the user's workstation through the Windows Event Manager (also known as Event Viewer), which can be accessed from the **Start/Event viewer** menu, or by running the command eventvwr.msc.

In the Cybels VPN Premium version, logs can also be consulted in managed mode through an EMM/GPO with a remote AD server.

Three log families are available: audit logs, technical logs and functional logs.

Audit logs

The following is the list of the various audit logs:

Audit type	ID	Severity	What this audit indicates	Parameters	Example	Remarks
App.Start	101	Info	The application was started	The software version (softwareVersion), and whether managed mode is enabled (Managed)	App.Start softwareVersion: 0.5.99.16 Managed: no	
App.Stop	102	Info	The application was shut down		App.Stop	This audit may not be saved if the application shuts down unexpectedly
Tunnel.Start	201	Info	A tunnel was initiated	Tunnel name (tunnelName)	Tunnel.Start tunnelName: Official_Ercom	This audit indicates that a tunnel was initiated, but does not indicate whether the connection was successful or failed
Tunnel.Stop	202	Info	A tunnel was shut down	Tunnel name (tunnelName)	Tunnel.Stop tunnelName: Official_Ercom	
Config.CreateTunnel	301	Info	A tunnel was created	Tunnel name (tunnelName), tunnel mode (DR or not)	Config.CreateTunnel tunnelName: valid_standard_cert isDr: no	

Audit type	ID	Severity	What this audit indicates	Parameters	Example	Remarks
Config.ModifyTunnel	302	Info	A tunnel was modified	Tunnel name (tunnelName)	Config.ModifyTunnel tunnelName: valid_standard_cert	
Config.DeleteTunnel	303	Info	A tunnel was deleted	Tunnel name (tunnelName)	Config.DeleteTunnel tunnelName: valid_standard_cert	
Config.TunnelChange	304	Info	New configuration for a tunnel	Tunnel name (tunnelName), parameters in question in key-value format	Config.TunnelChange tunnelName: valid_standard_cert fieldName: IkeKeyExchange fieldValue: Group 14	See note below
Config.ExportConfig	305	Info	A configuration was exported		Config.ExportConfig	
Config.ImportConfig	306	Info	A configuration was imported		Config.ImportConfig	

NOTES

- Config.TunnelChange appears when a tunnel is either added or modified
- When a tunnel is added, the parameters of the new tunnel are shown => one event for each parameter
- When a tunnel is modified, only the parameters that were changed are shown (the new value) => one event for each modified parameter
- Some parameters cannot be shown: PSK (for security reasons), certificates (for technical reasons)

Technical logs

In a future version

"General settings" tab

This menu groups the global options that apply to all VPN connections and configured tunnels.

These options notably include global configuration parameters for exporting and importing configurations, parameters relating to the PKI and configuration, and the status of the license to be activated (or already activated) on the user's workstation. The license makes it possible to find out which type of product, Essential or Premium, was configured on the workstation, and its validity period.

"About" menu

This menu shows information relating to the software version (SDK, multi-platform client and build), and third-party licenses used.

Standard version information

The main screen shows information on the identity of the product:

- Client version: application's major version (e.g., 0.4.0)
- Copyright: legal notice and intellectual property (Ercom)
- Third-party licenses: by clicking on the dedicated link, you will be able to see the list of open-source components that are built into the solution's components, thereby guaranteeing software transparency.

Detailed information (Expert/Debug)

By clicking on "More version information", a side panel will open to show advanced technical data:

- SDK: software development kit used:
- StrongSwan: version of the IPsec cryptography engine that powers tunnels
- Build number: unique identifier of the software compilation (e.g., 20260130)
- Version of the VPN client activation license server

NOTE
The detailed information provided is intended for use in advanced troubleshooting. In general, this information is not needed on a daily basis, but has to be sent to technical support teams upon request when an incident ticket is opened. This information will make it possible to accurately analyze the client's behavior based on its compilation environment.

Appendix

References of smart cards tested with the Cybels VPN client:

Card/driver	ID Prime MD 830-FIPS Rev B/GlobalSign SAC Win X64 v10.9-R2

STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2026. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.