VPN Remote Access Manual For Externals

a step-by-step manual for Windows & MAC OS X

Version: 2.9

Date: 17.12.2024

Contents

1. Windows Manual 3
1.1 Product Description 3
1.2 Software Download 3
1.3 Software Installation 5
1.4 Create Connection to the VIG Network 9
1.5 Connect and Authenticate with Certificate 14
1.6 Disconnect from VPN 18
2. MAC OS X Manual 19
2.1 Product Description 19
2.2 Software Download 19
2.3 Software Installation 20
2.4 Create Connection to the VIG network 25
2.5 Connect and Authenticate with Certificate 29
2.6 Disconnect from VPN 31

1. Windows Manual

1.1 Product Description

The software product is used to establish a secure connection to the network of the Vienna Insurance Group (VIG). The installation package contains legacy VPN functionality. Other features like Desktop-Firewall, Anti-Virus, Full Disk Encryption, IPS or SVC components are not included. Authentication is achieved by using a certificate (.p12 file) and a password (in the .txt file).
Note:
There is no IPv6 support and no support for clients using multiple VPN clients on the same device, notebook.

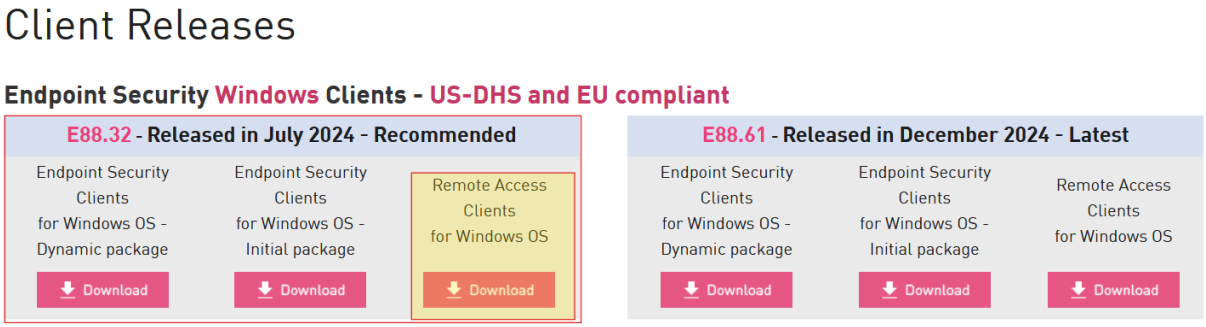
1.2 Software Download

To download the recommended VPN Client version, please visit the following URL:

https://support.checkpoint.com/results/sk/sk117536

Scroll down to the section "**Client Releases**"; here you will find the currently recommended Version of the VPN Client, which, at the time of writing this documentation, is Version E88.32.

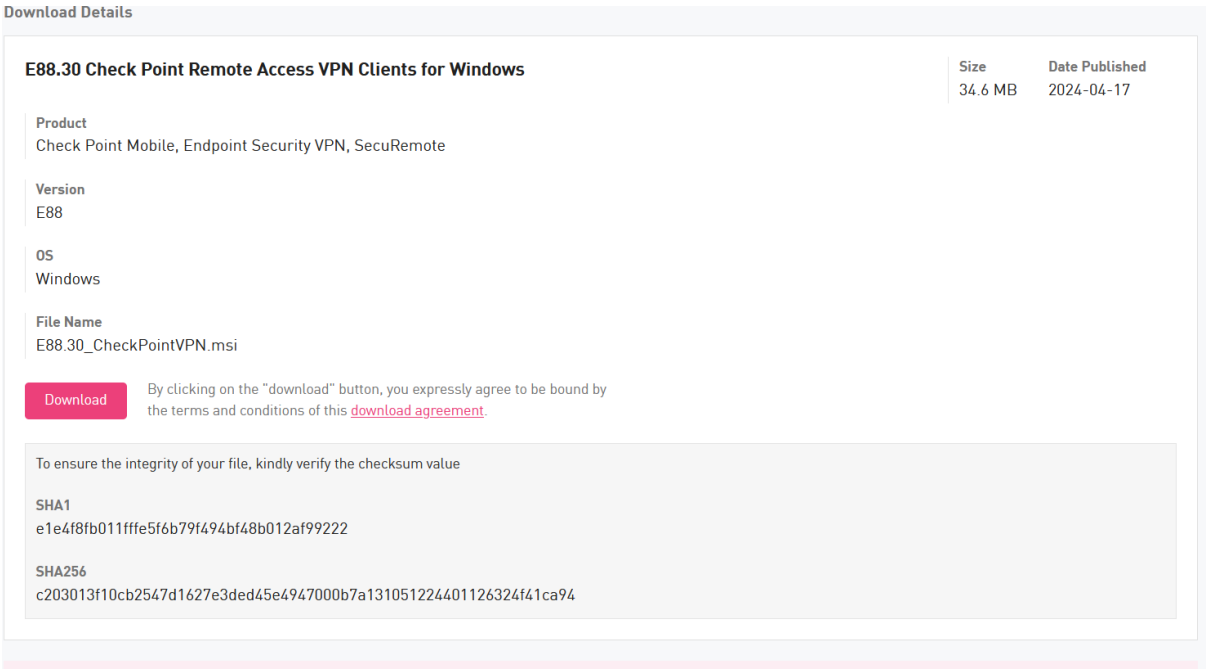
The next step is to download the VPN Client by clicking on "**Download**" in the "**Remote Access Clients for Windows OS**" section as seen in Screenshot 1.1 bellow. (Yellow highlighted section)



Screenshot 1.1: Download recommended VPN Client

Clicking on "**Download"** will open a new Browser Window as seen bellow in Screenshot 1.2

Click the "**Download**" button to download the VPN Client



Screenshot 1.2: VPN Client Download

1.3 Software Installation

To install the software a user account with administrative permissions is required. After executing the setup file (.msi file), the software installation process will start.

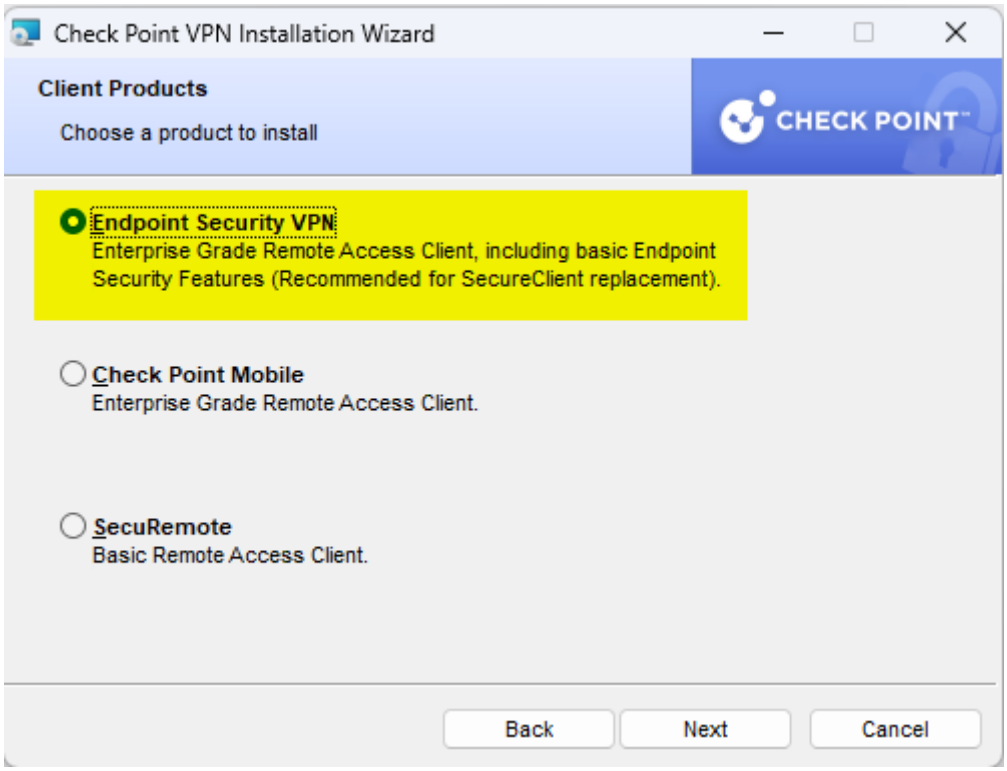
PLEASE NOTE: A reboot is required after successful installation!

Before starting the installation, you will be prompted to accept the terms in the license agreement (see screenshot 1.3) and provide an installation path for the application. It is highly recommended to install the VPN client at the predefined path.
The following screenshots (1.3-1.14) show the installation and configuration of the VPN client.

Please make sure that you have selected „Endpoint Security VPN“ as Client Product (see screenshot 1.4)!

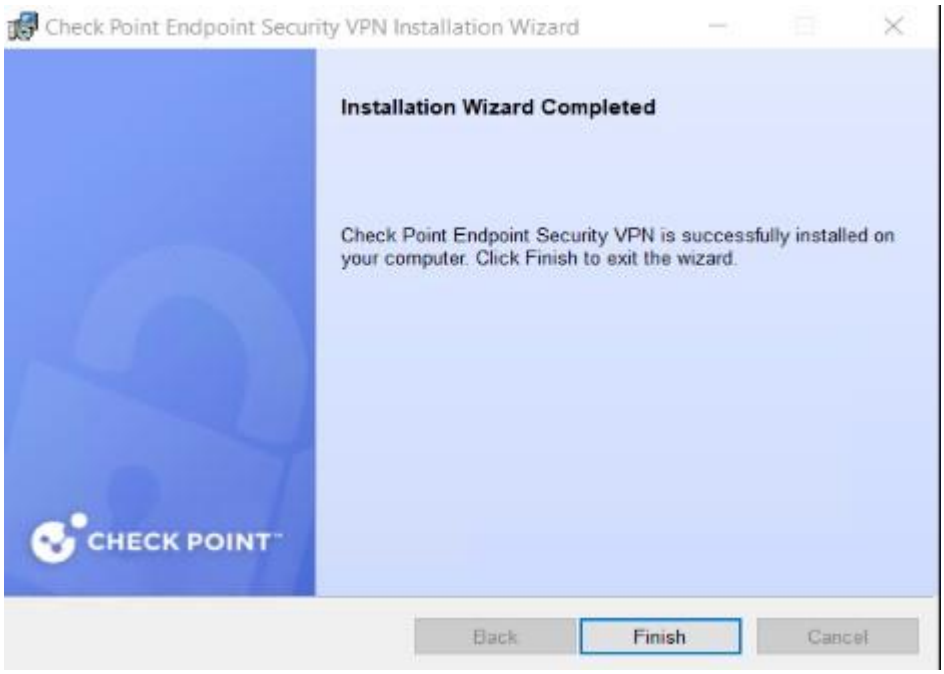
SecuRemote is not supported and won’t work!
Check Point Mobile is not permitted unless otherwise told!

Screenshot 1.3: Check Point VPN installation wizard



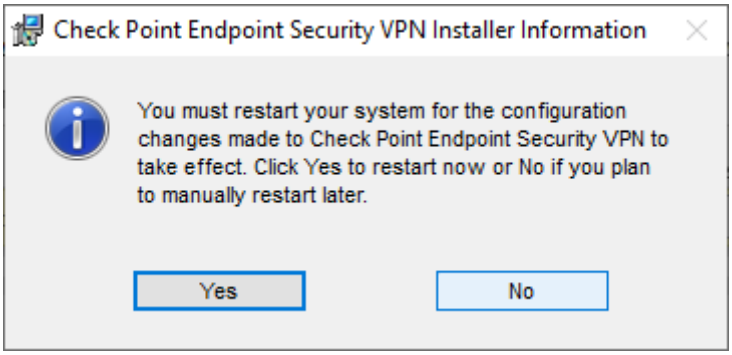
Screenshot 1.4: Select Endpoint Security VPN

Screenshot 1.5: License Agreement



Screenshot 1.6: Installation completed

Now that installation is complete, please ensure that you have saved all your recent work/data and restart your system.

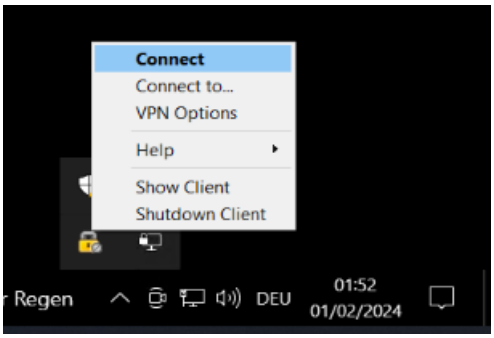


Screenshot 1.7: restart required

The next chapters will cover the configuration of the VPN Client itself.

1.4 Create Connection to the VIG Network

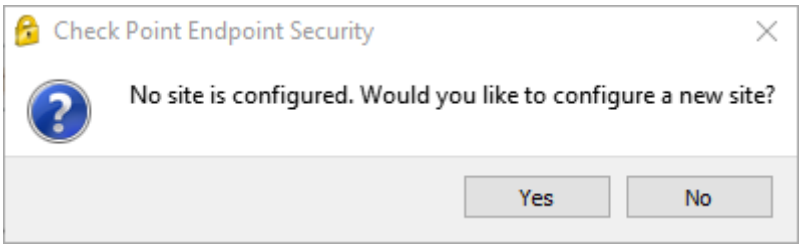
After the VPN client has been successfully installed, you can use the icon in the menu bar to access the client. Click "**VPN Options**" to create a new "**site**" (connection to the VIG network) or just right-click onto the yellow lock-symbol at the right corner of your Windows taskbar and click "**Connect**". Once you have created the site, the connection settings remain saved in the client's configuration.



Screenshot 1.8: run VPN client

PLEASE NOTE: If the Check Point VPN Client is not running (e.g. "autostart" is disabled for the client), please start it like you would usually start any other software.

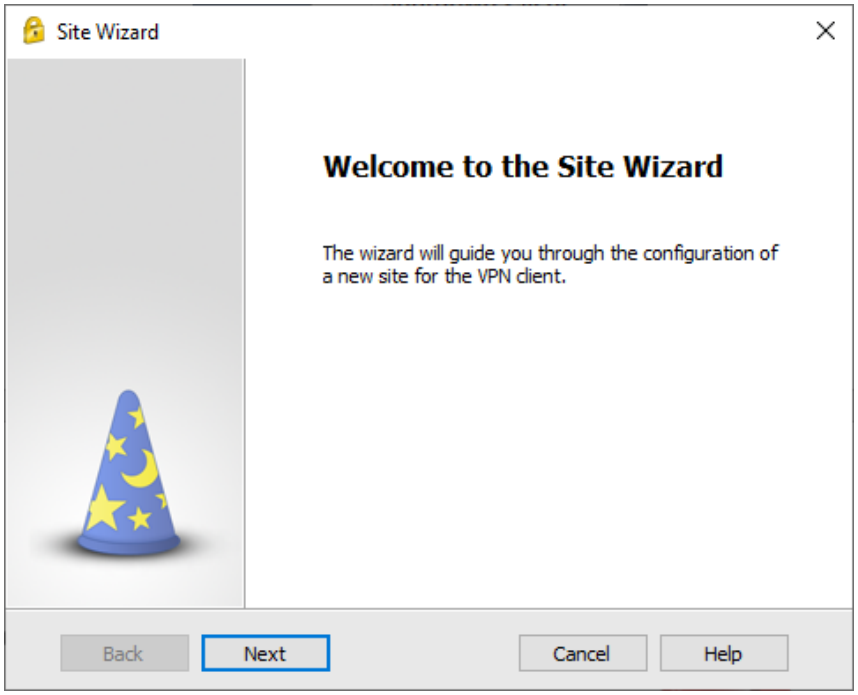
Depending on the version of your client, a pop-up states that no site is configured and asks if you want to configure a new one. Answer with "**Yes**":



Screenshot 1.9: "no site configured" pop-up

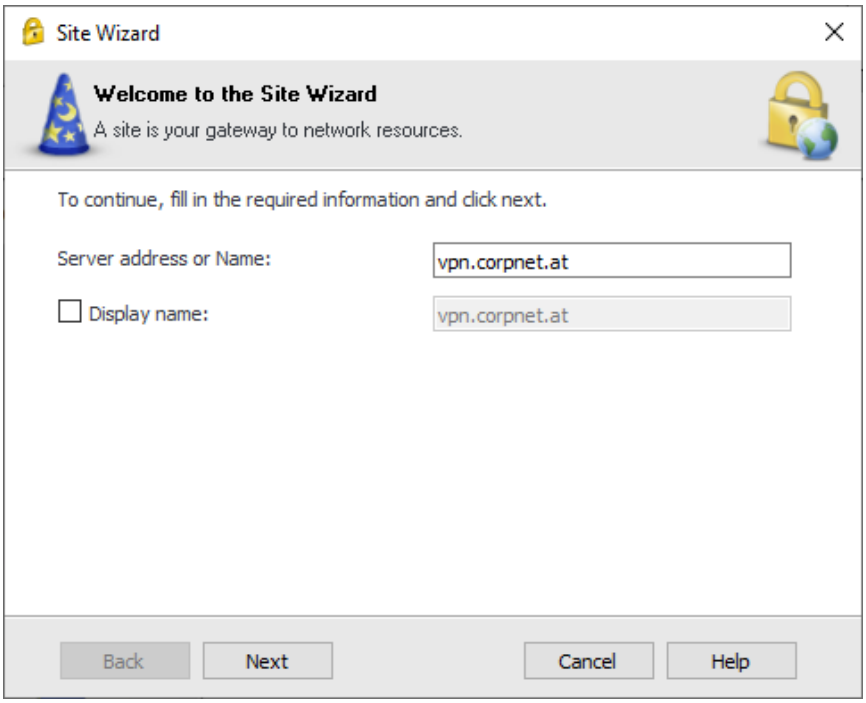
Create a new site by completing the wizard and the following settings:

1. Click "**Next**":



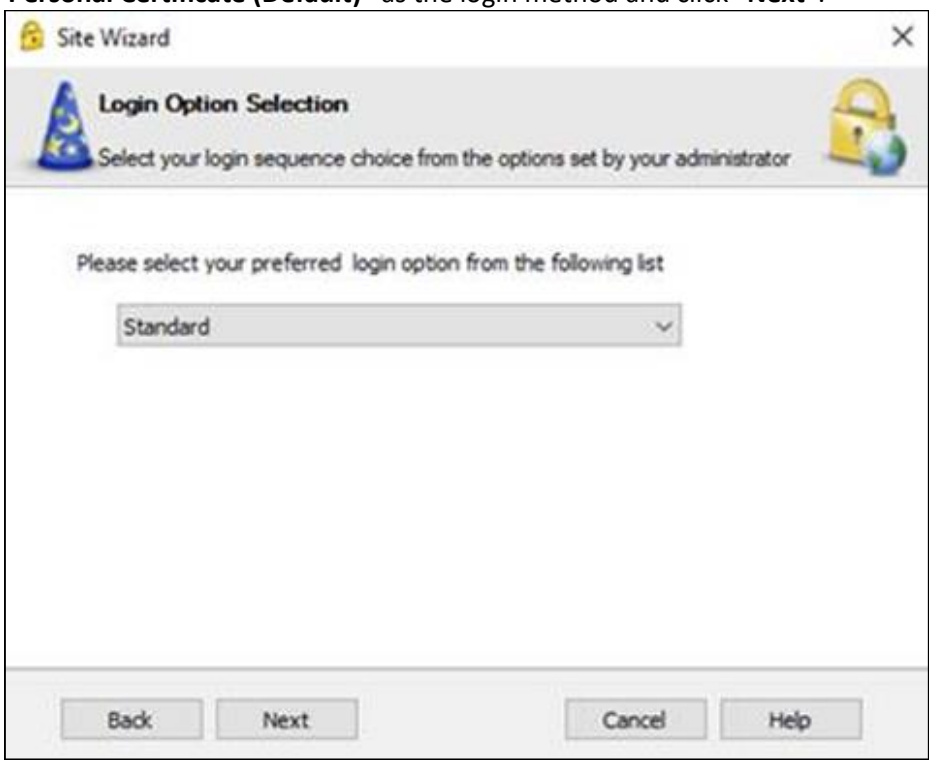
Screenshot 1.10: site creation wizard

2. Enter "**vpn.corpnet.at**" (DNS should resolve name to 185.202.151.126; as per 03.09.2020) and click "**Next**":



Screenshot 1.11: site name "vpn.corpnet.at"

3. Select "**Personal Certificate (Default)"** as the login method and click "**Next**":



Screenshot 1.12: login option "Standard"

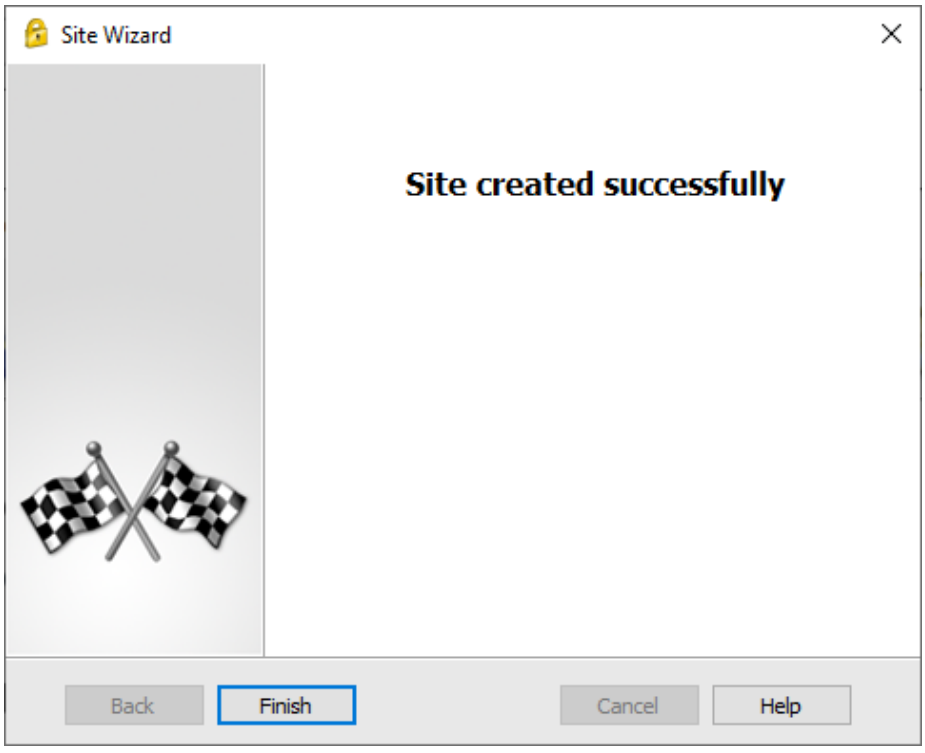
4. **Select** "**Certificate"** as the authentication method and click "**Next**":

Screenshot 1.13: authentication *option "Certificate"*

5. Select "**Use certificate from Public-Key Cryptographic Standard (PKCS #12) file**" as the authentication method and click "**Next**":

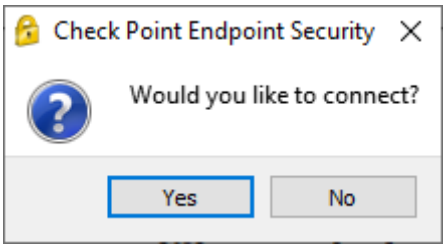
Screenshot 1.14: Certificate Authentication

6. Select "Certificate" as the authentication method and click "**Next**":



Screenshot 1.15: site created successfully

Once you have created a site configuration to vpn.corpnet.at, a pop up asks if you want to connect to the site. Click "**Yes**" and follow the instructions in section 1.5 ("Connect and Authenticate with Certificate") below.



Screenshot 1.16: "Connect" pop-up

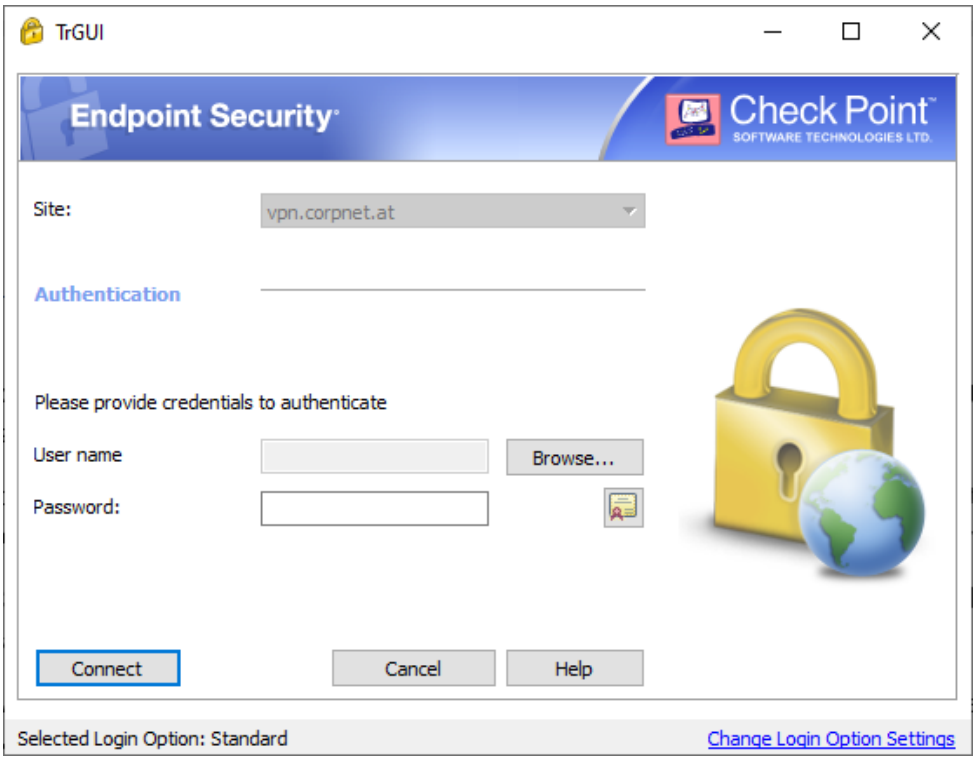
1.5 Connect and Authenticate with Certificate

The certificate and password you have been provided with are required for authentication and access to the Vienna Insurance Group (VIG) network.

You can run the Check Point VPN Client via your Start Menu or just right-click onto the yellow lock-symbol at the right corner of your Windows taskbar and click "**Connect**" (see screenshot 1.7).

PLEASE NOTE: If the Check Point VPN Client is not running (e.g. "autostart" is disabled for the client), please start it like you would usually start any other software.

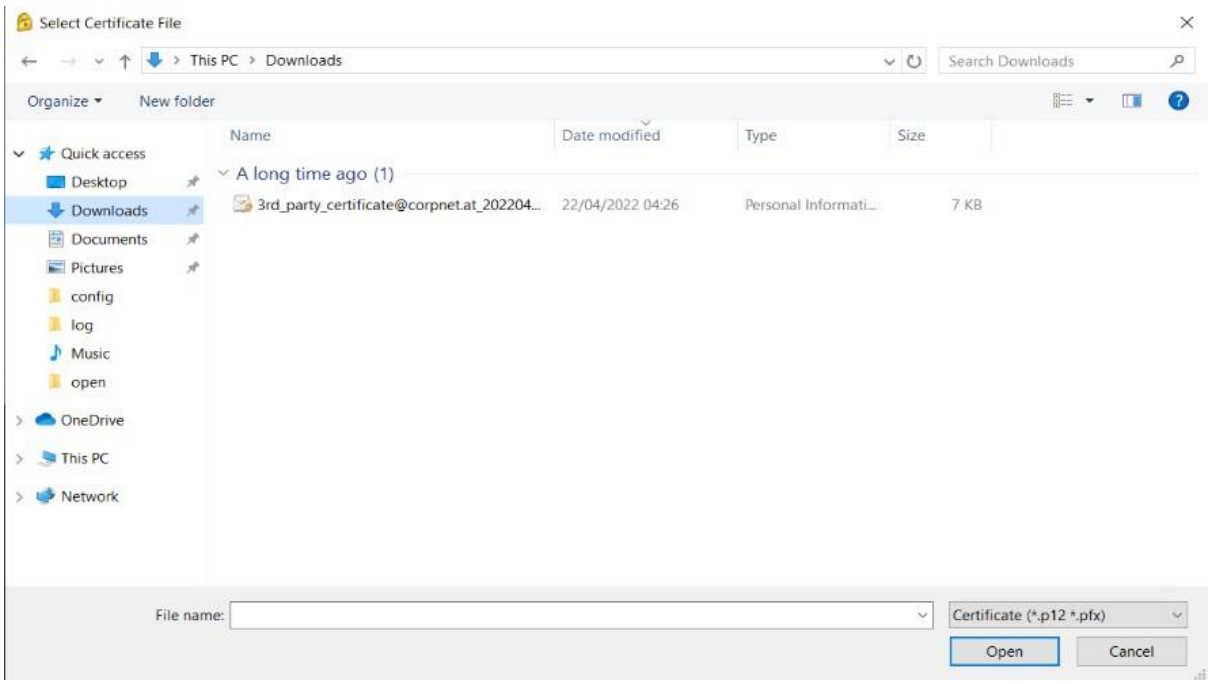
A new window pops up where you select the certificate and enter its password. The correct site "**vpn.corpnet.at**" should already be pre-configured.



Screenshot 1.15: empty VPN connection configuration

Click "**Browse…**", select the certificate file and click "**Open**":

PLEASE NOTE: Be sure to store your certificate on a local disk (e.g. "C:\...")

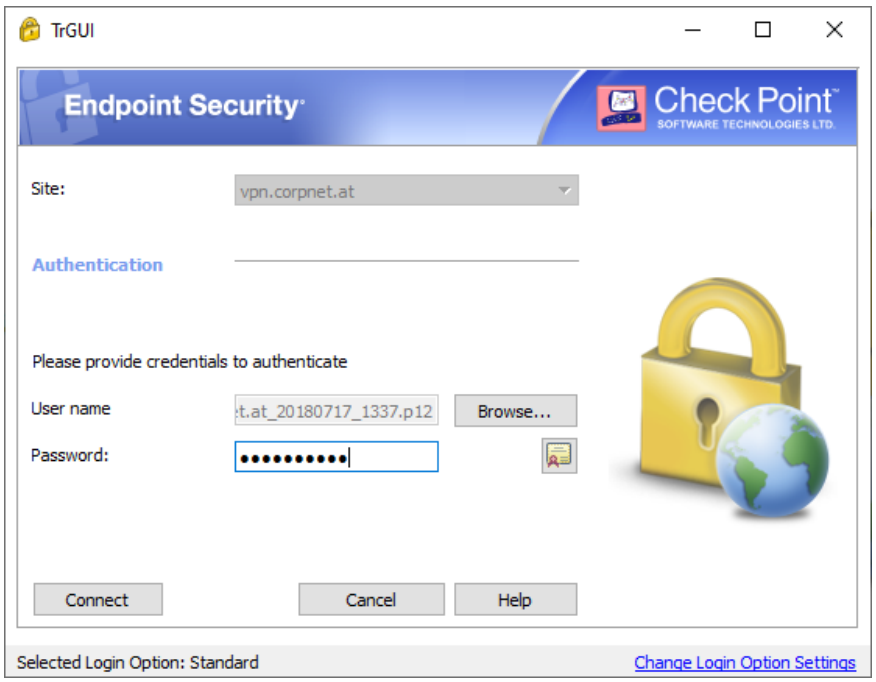


Screenshot 1.16: select VPN certificate

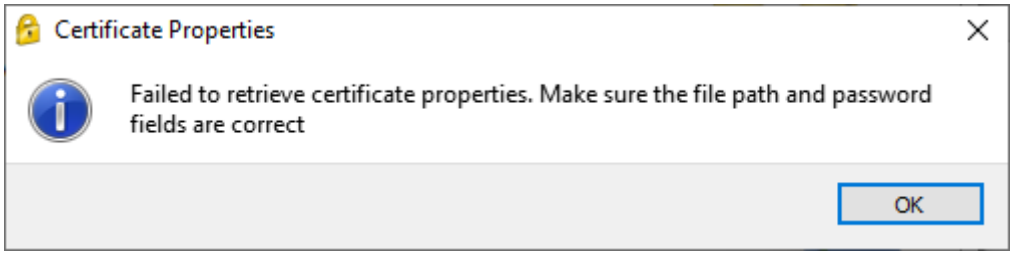
PLEASE NOTE: Once you have selected the certificate, it will be saved in the client. If you **move** the .p12 file (certificate) to a different folder must browse and **select** it **again**.

Now type in the password which can be found in the provided .txt file (under "pw: ").

You can verify the correct password by clicking the symbol which will display details of your certificate after entering the password. If a wrong password was used, you will receive an error message (see screenshot 1.19).

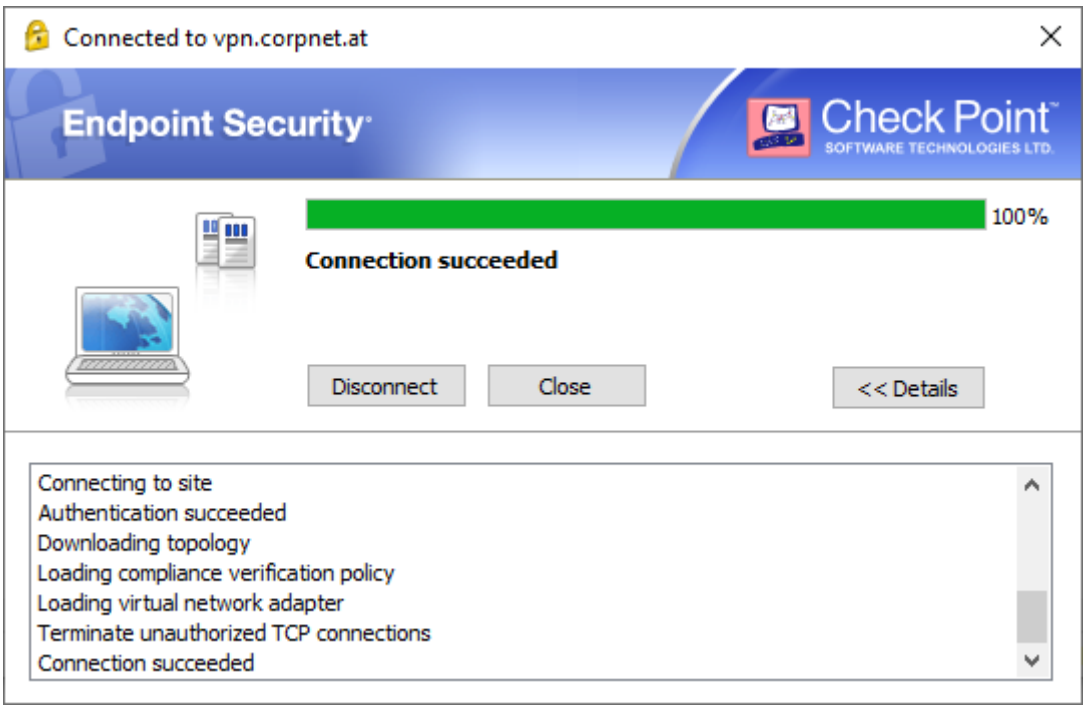


Screenshot 1.17: VPN Client ready



Screenshot 1.18: wrong password used for certificate

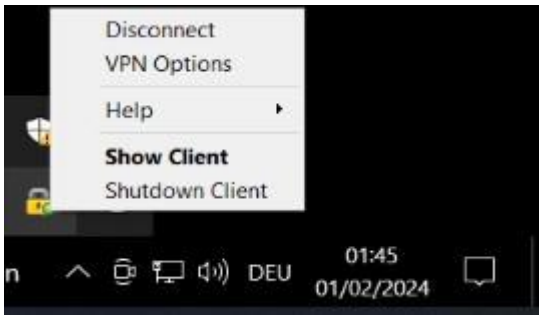
If you have used the correct password, click "**Connect**" and the VPN connection will be established:



Screenshot 1.19: VPN connection established

1.6 Disconnect from VPN

You can always disconnect by clicking the "**Disconnect**" Button or right-click on the yellow lock symbol in the right corner of your Windows taskbar and choose "**Disconnect**"



Screenshot 1.20: disconnect from VPN

2. MAC OS X Manual

2.1 Product Description

The software product is used to establish a secure connection to the network of the Vienna Insurance Group (VIG). The installation package contains legacy VPN functionality. Other features like Desktop-Firewall, Anti-Virus, Full Disk Encryption, IPS or SVC components are not included. Authentication is achieved by using a certificate (.p12 file) and a password (in the .txt file).

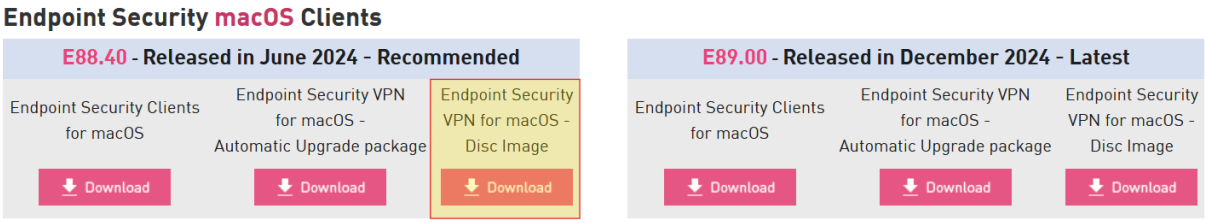
2.2 Software Download

To download the recommended VPN Client version, please visit the following URL:

https://support.checkpoint.com/results/sk/sk117536

Scroll down to the section "**Client Releases**"; here you will find the currently recommended Version of the VPN Client, which, at the time of writing this documentation, is Version E88.40.

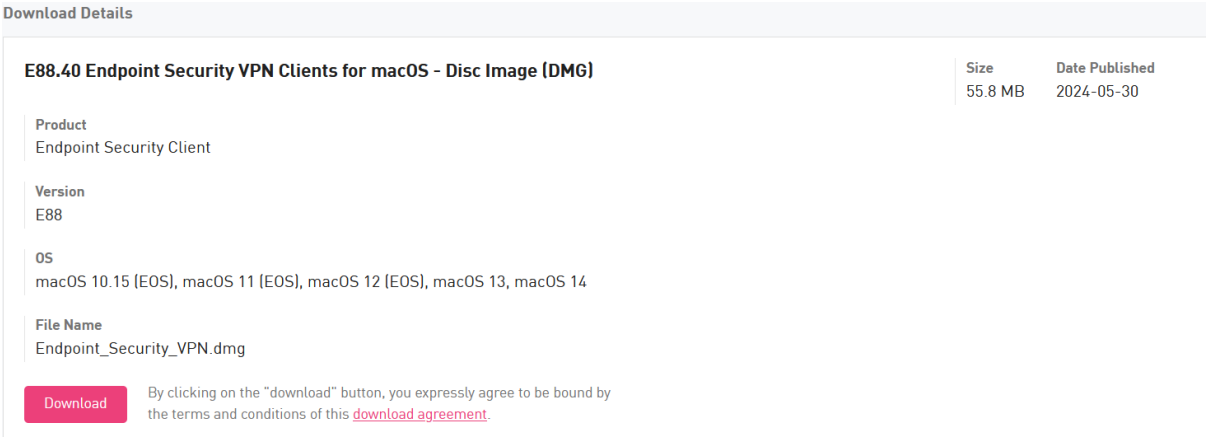
The next step is to download the VPN Client by clicking on "**Download**" in the "**Endpoint Security VPN for macOS – Disc Image**" section as seen in Screenshot 2.1 bellow. (Yellow highlighted section)



Screenshot 2.1: Download recommended VPN Client

Clicking on "**Download"** will open a new Browser Window as seen bellow in Screenshot 2.2

Click the "**Download**" button to download the VPN Client



Screenshot 2.2: VPN Client Download

2.3 Software Installation

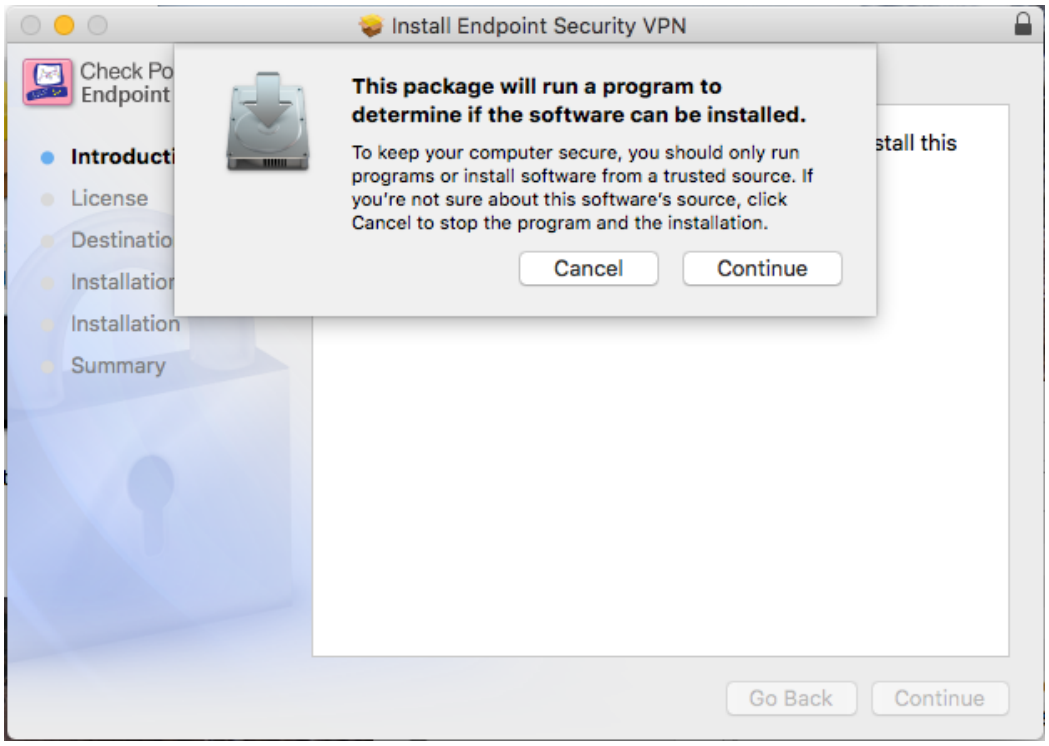
To install the software a user account with administrative permissions (root) is required.

First, run the downloaded "**.dmg**" and select "**Endpoint_Security_VPN.pkg**".

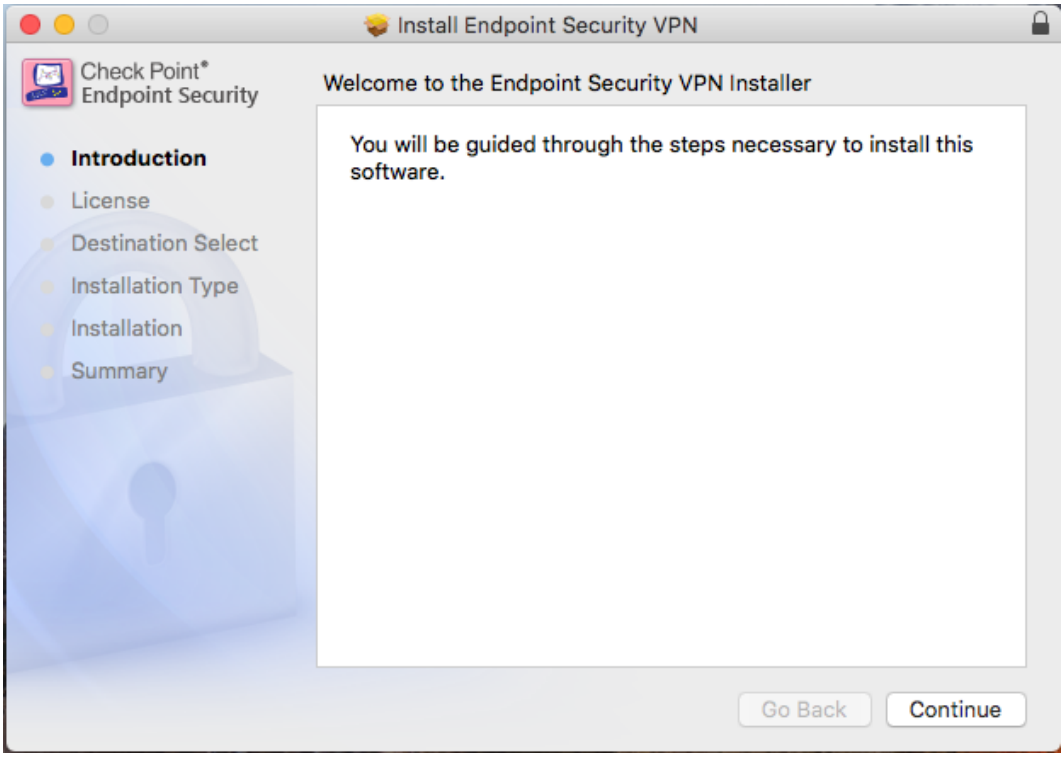
Screenshot 2.3: VPN Client package

The following screenshots show all steps for installing the VPN client.

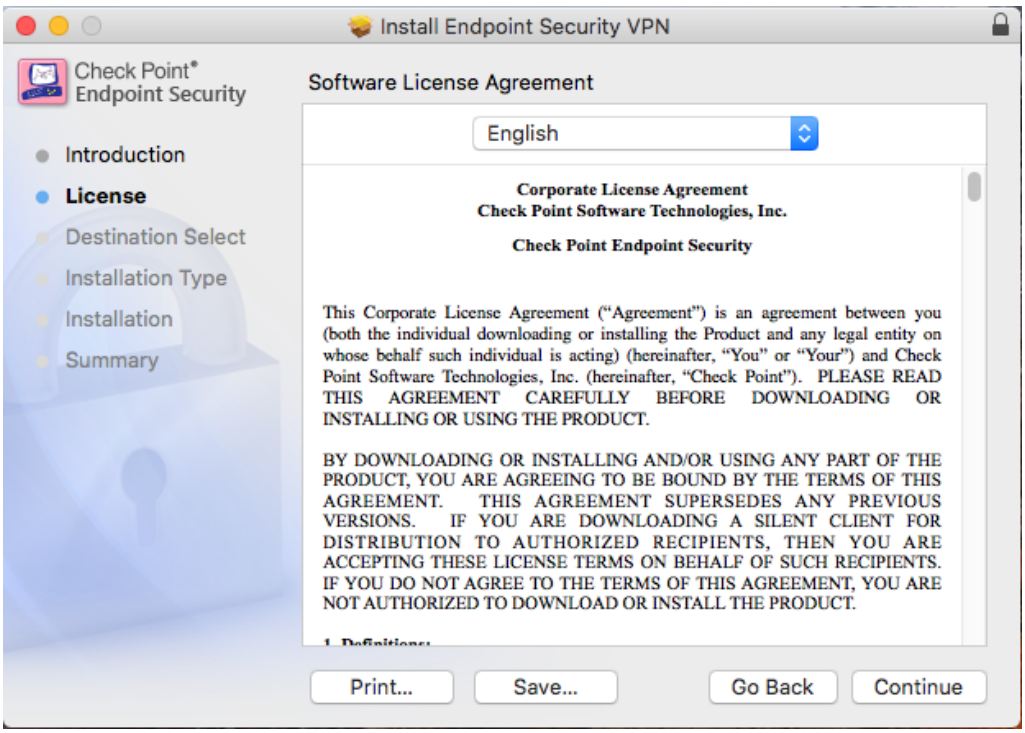
A pre-install verifier checks if the software can be installed on your system. Please click "**Continue**":



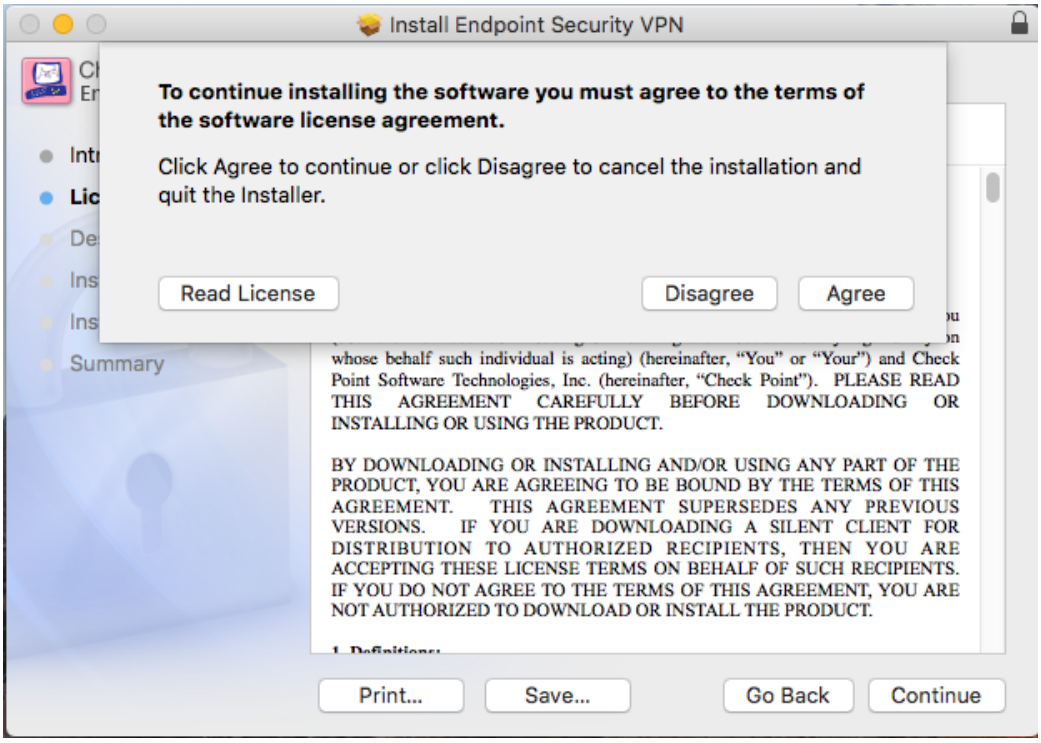
Screenshot 2.4: Installation Wizard: pre-install verifier



Screenshot 2.5: Installation Wizard: Introduction

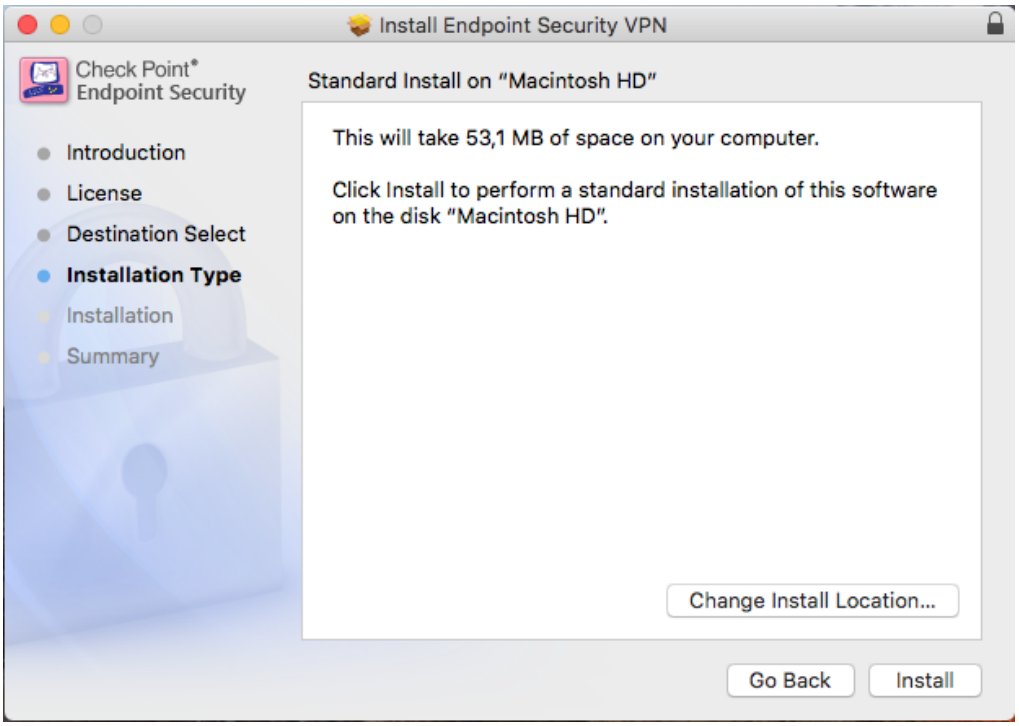


Screenshot 2.6: License Agreement #1



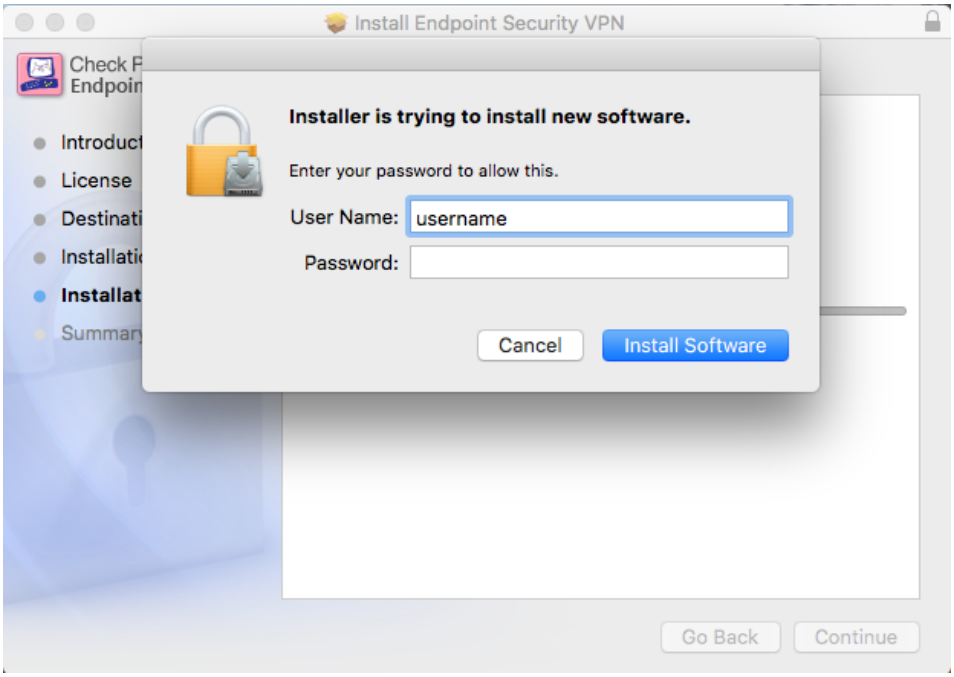
Software 2.7: License Agreement #2

It is highly recommended to install the VPN client at the predefined path.

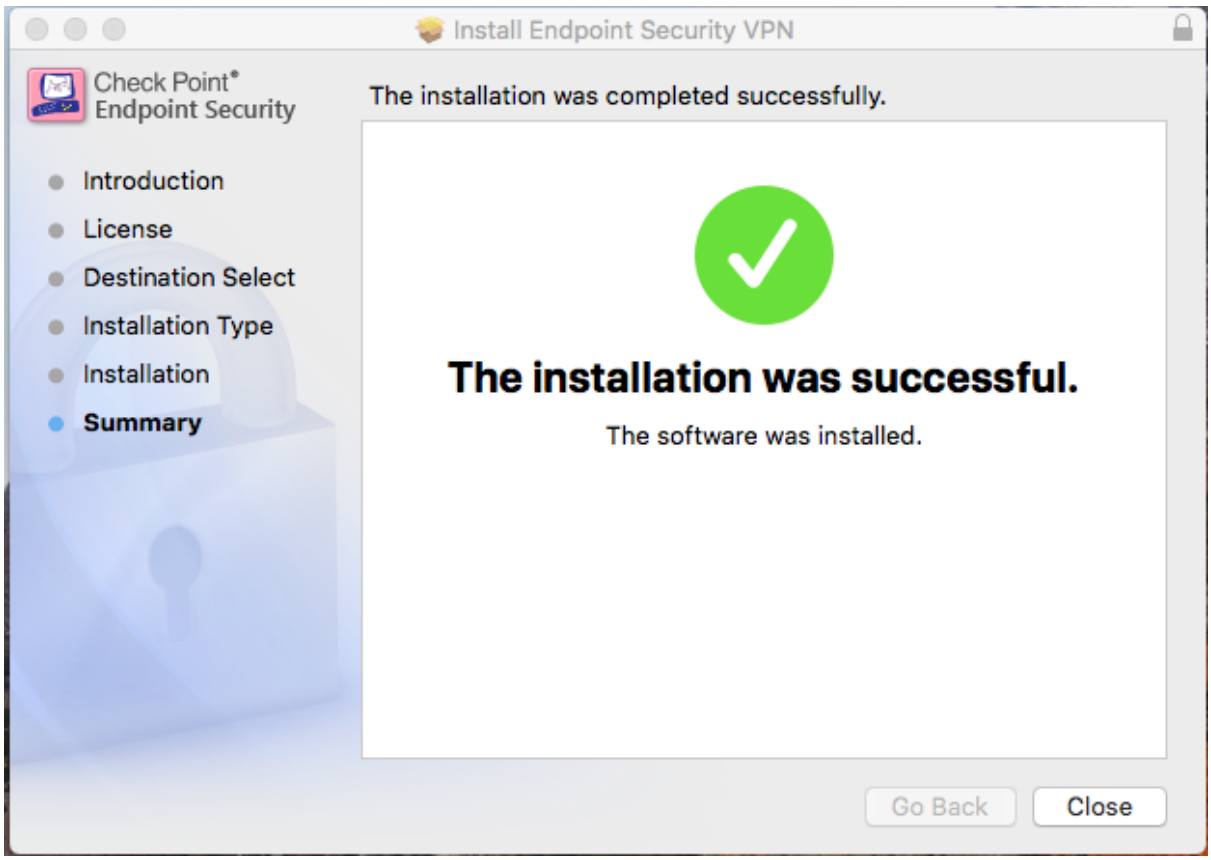


Screenshot 2.8: Installation Path

Provide user credentials of an account with root privileges and click "Install Software".



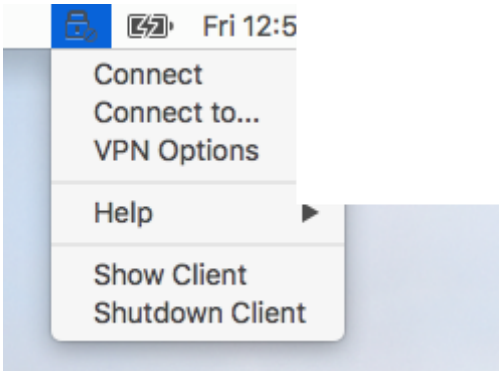
Screenshot 2.9: account with root privileges



Screenshot 2.10: Installation successful

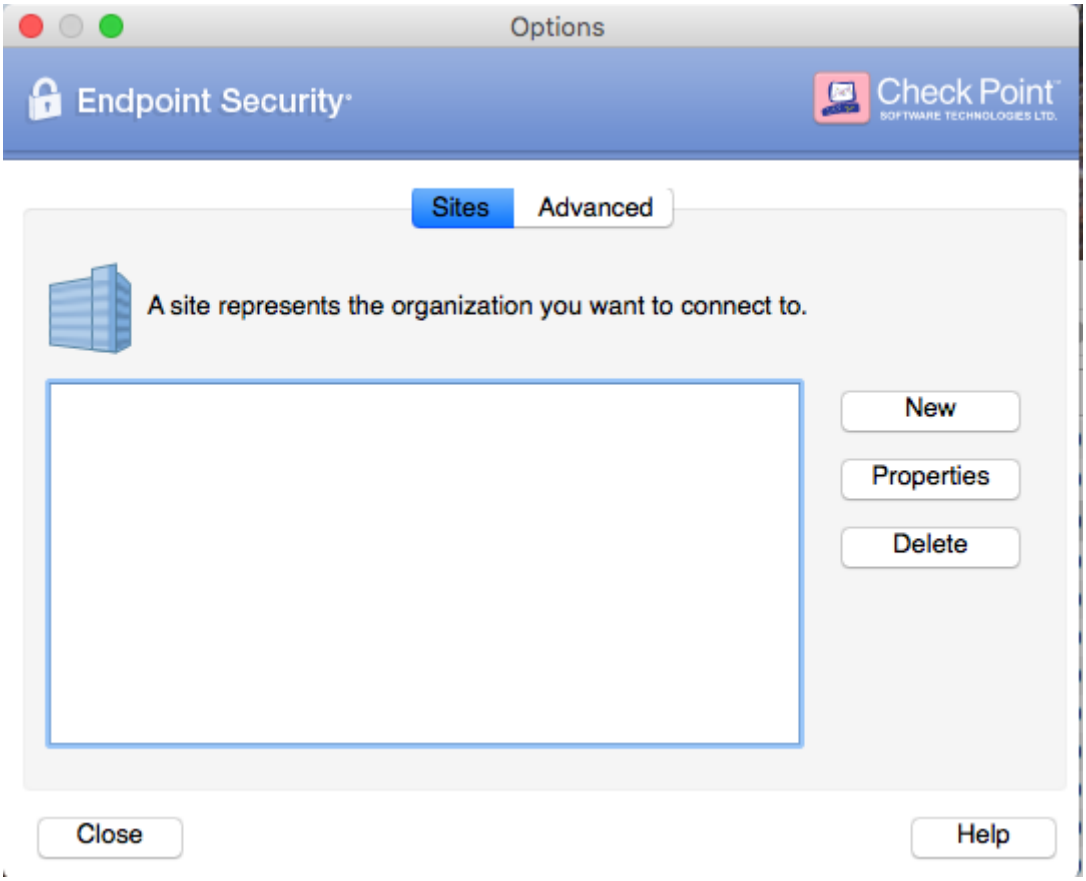
2.4 Create Connection to the VIG network

After the VPN client has been successfully installed, you can use the icon in the menu bar to access the client. Click "**VPN Options**" to create a new "site" (connection to the VIG network). Once you have created the site, the connection settings remain saved in the client's configuration.



Screenshot 2.11: Check Point VPN client in menu bar

A new window pops up and you can create a new "site". Click "**New**":



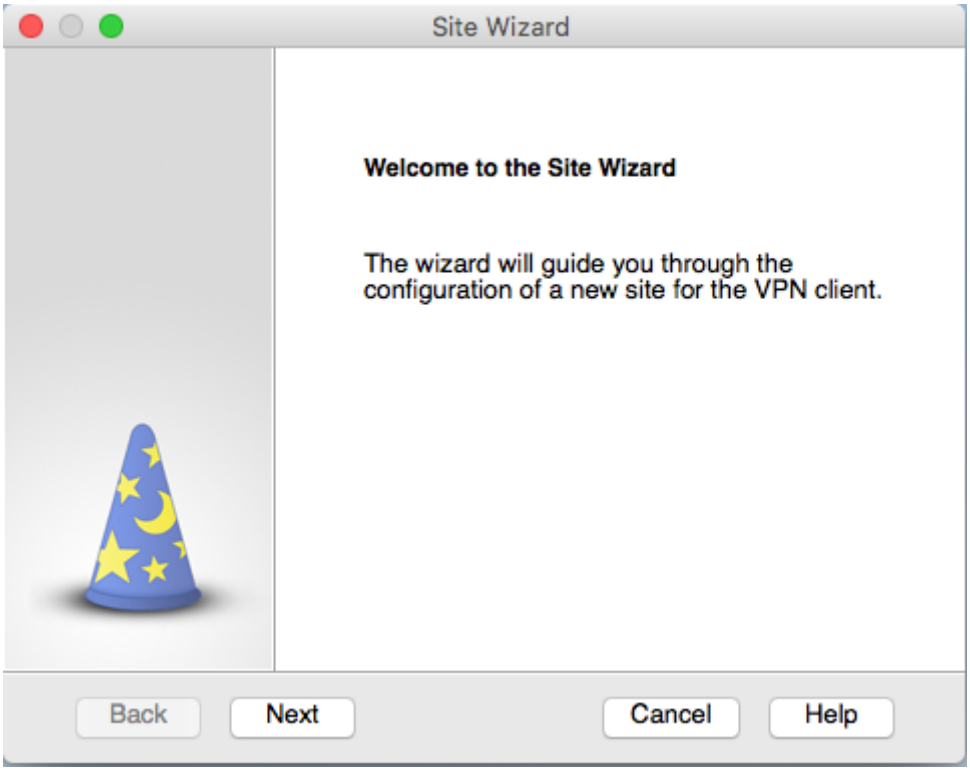
Screenshot 2.12: empty VPN client configuration

Depending on the version of your client, maybe another pop-up states that no site is configured and asks if you want to configure a new one. Answer with "**Yes**":

Screenshot 2.13: "no site configured" pop-up

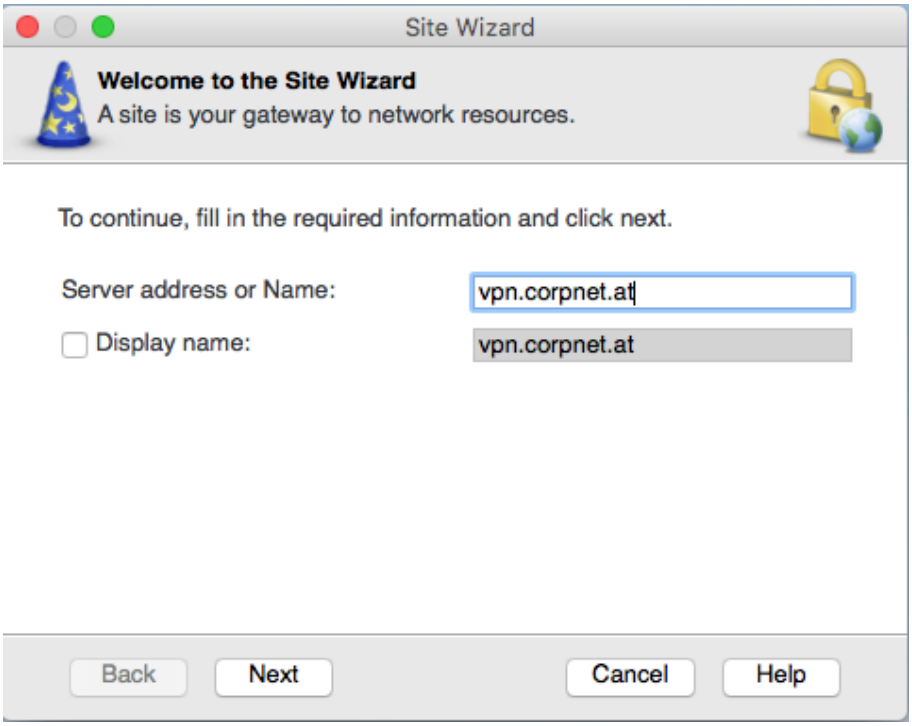
Create a new site by completing the wizard and the following settings:

1. Click "**Next**"



Screenshot 2.14: site creation wizard

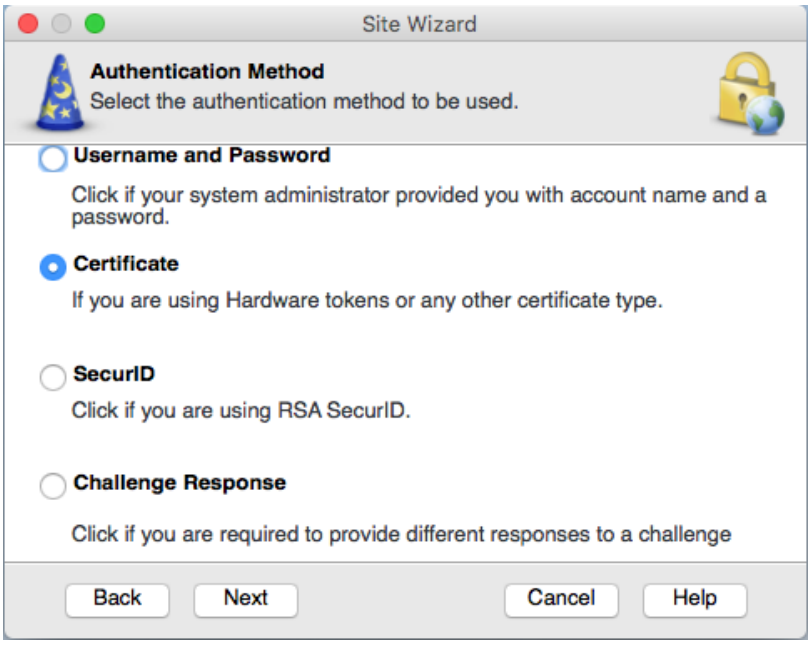
2. Enter "**vpn.corpnet.at**" (DNS should resolve name to 185.202.151.126; as per 03.09.2020) and click "**Next**":



Screenshot 2.15: site name: vpn.corpnet.at

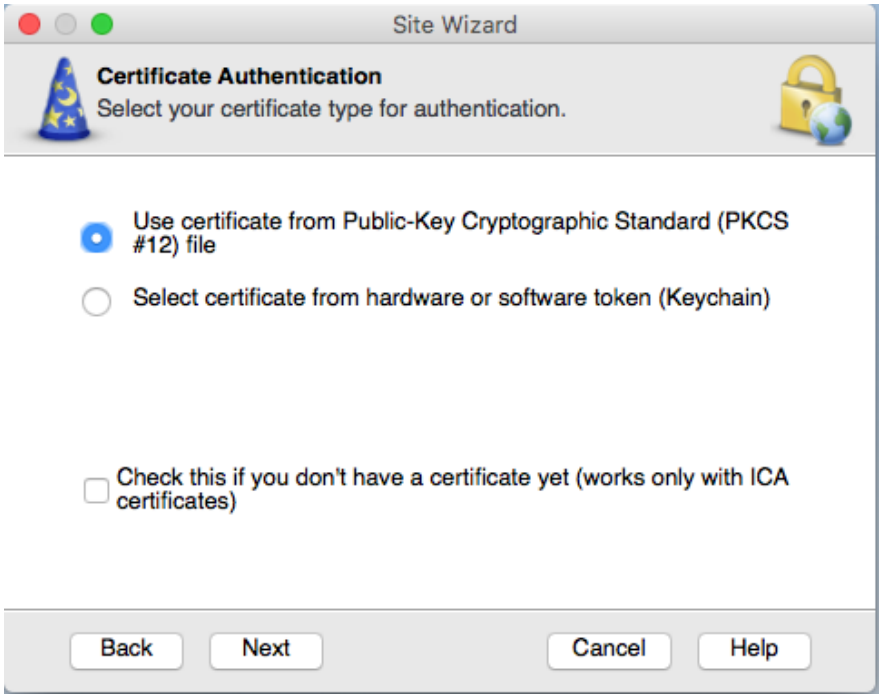
3. Select "**Standard (Default)**" as Login Option if the installation wizard asks for it (depends on version) as it can be seen in screenshot 1.11 under the Windows 10 Section.

4. Select "**Certificate**" as the authentication method and click "**Next**":



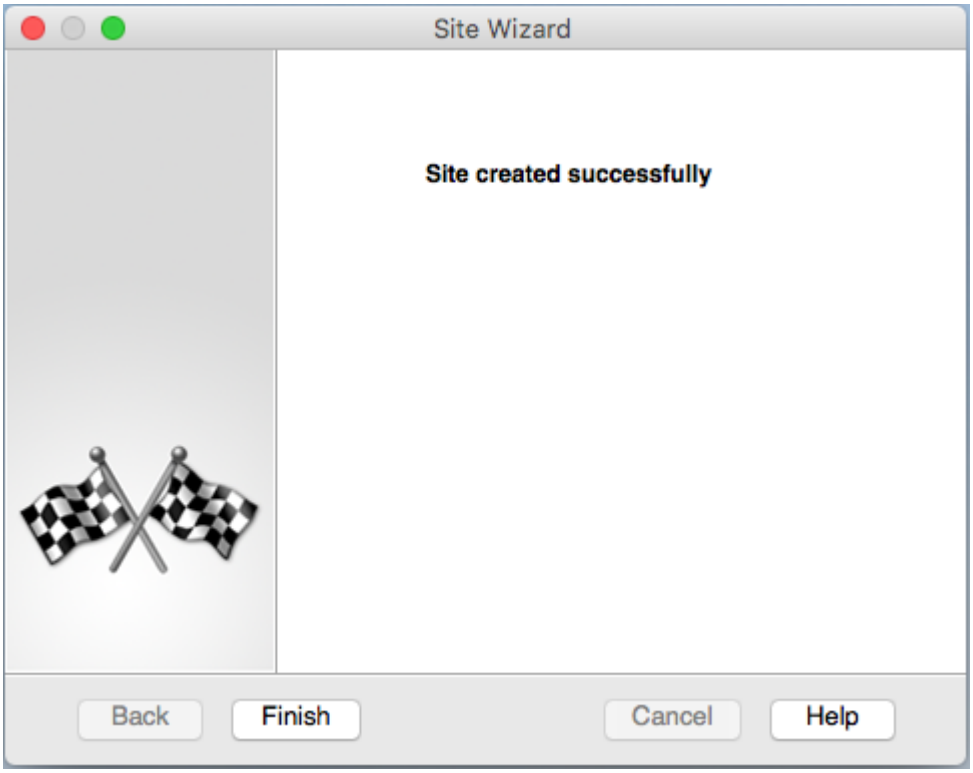
Screenshot 2.16: authentication mode: "Certificate"

5. Select "**Use certificate from Public-Key Cryptographic Standard (PKCS #12) file**" and click "**Next**":



Screenshot 2.17: use PKCS #12 certificates

6. Click "**Finish**":

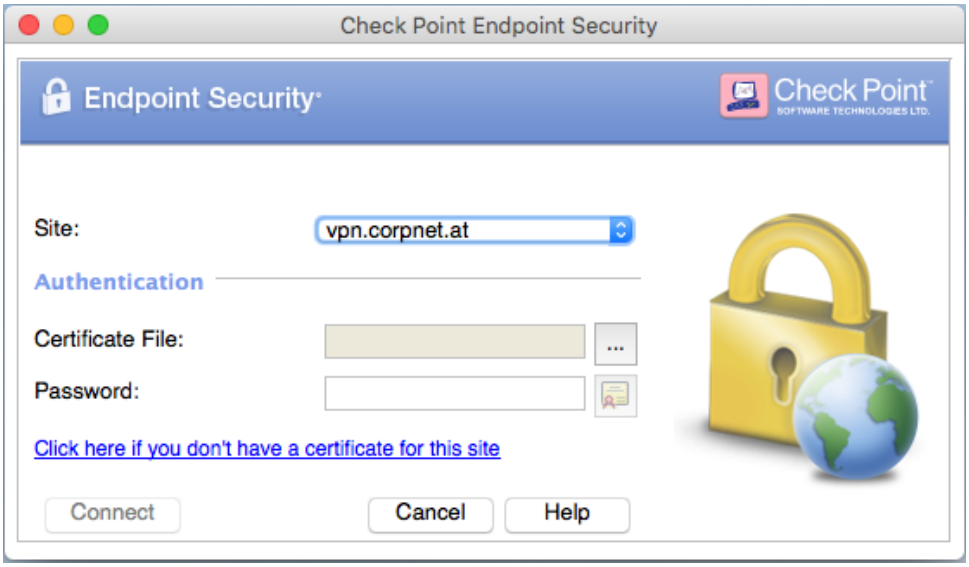


Screenshot 2.18: site created successfully

2.5 Connect and Authenticate with Certificate

The certificate and password you have been provided with are required for authentication and access to the Vienna Insurance Group (VIG) network.

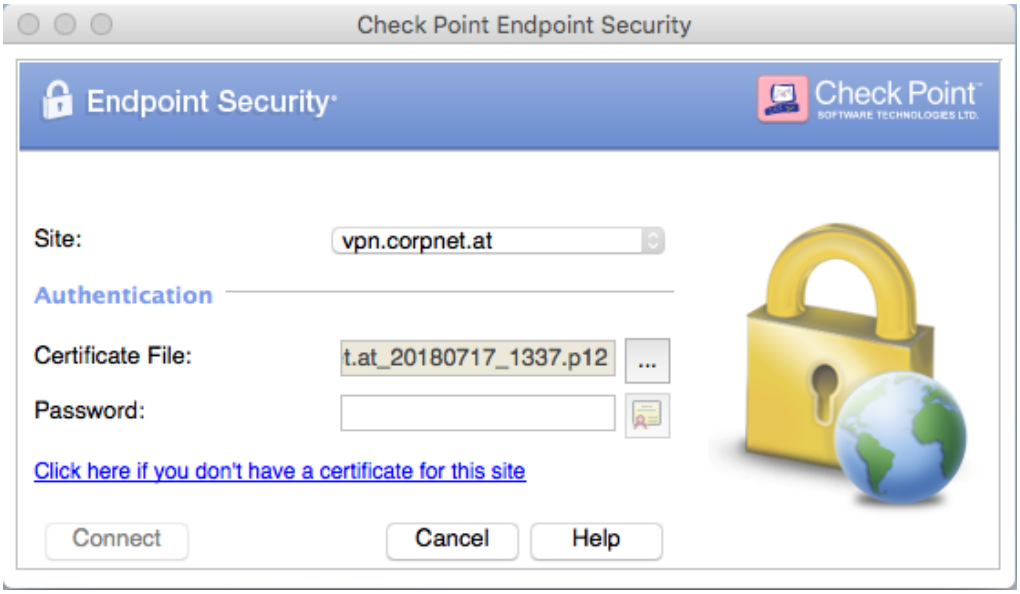
Access the Check Point VPN client (lock symbol in menu bar, see screenshot 2.9) and click “Connect” or “Connect to…”. A new window pops up and you have to select the certificate and enter its password. If “**Site**” is empty, select “**vpn.corpnet.at**”.



Screenshot 2.19: choose site

Click “**…**” and browse to your usercertificate file (.p12 file) you have been provided with and click “Open”.

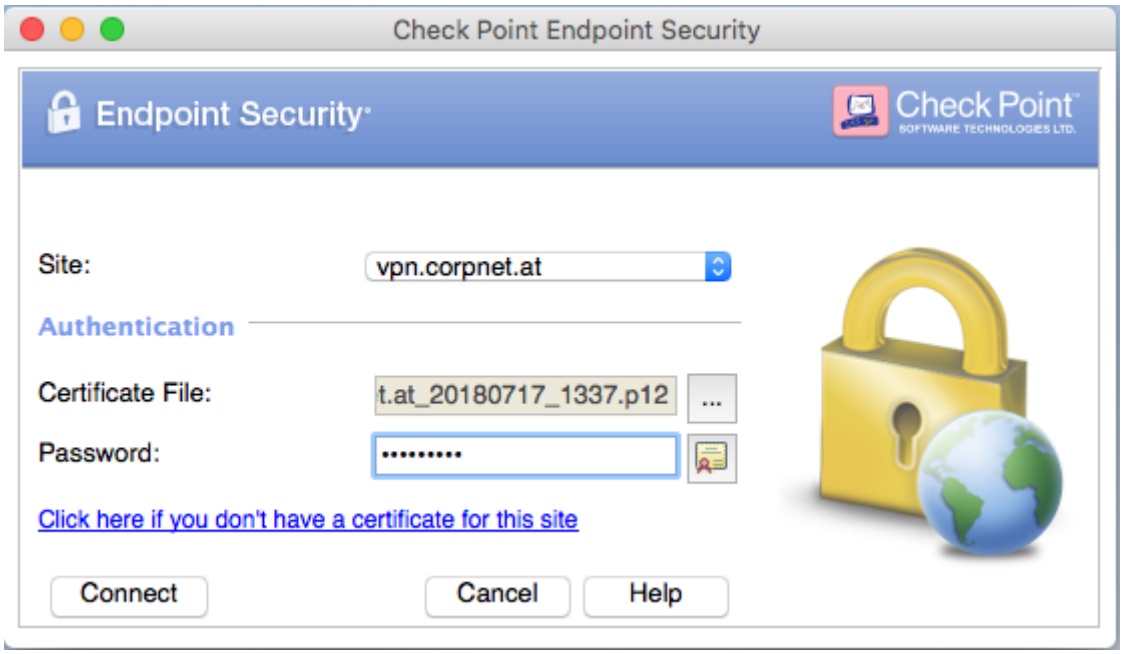
PLEASE NOTE: Be sure to store your certificate on a local disk!



Screenshot 2.20: select certificate

PLEASE NOTE: Once you have selected the certificate, it will be saved in the client. If you **move** the .p12 file (certificate) to a different folder you have to **select** it **again**.

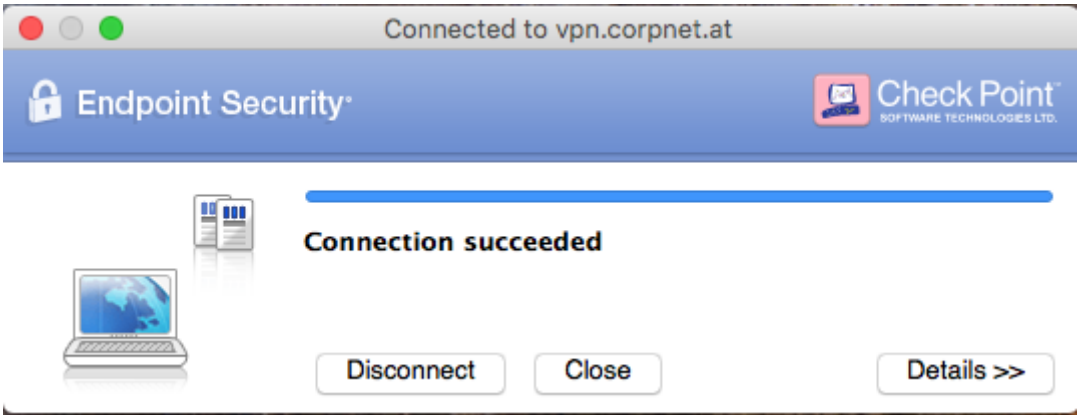
Now type in the password which can be found in the provided .txt file (under "pw: ").



Screenshot 2.21: enter password

You can verify the correct password by clicking the  symbol which will display details of your certificate. If a wrong password was used, you will receive an error message.

Click "**Connect**". After successfully establishing the connection you can access resources on the VIG network:



Screenshot 2.22: VPN connection established

2.6 Disconnect from VPN

You can always disconnect by clicking the “Disconnect” Button in the VPN client’s window or using the lock-symbol in your menu bar.