

# Certificate Based VPN

HSE is moving to Certificate based VPN authentication. Users will authenticate using a Certificate saved on their device. This is a guide to help users to set up Certificate based VPN authentication on their device.

**PLEASE NOTE VPN REMOTE ACCESS REQUIRES A PRIVATE BROADBAND CONNECTION. IT WILL NOT WORK OVER A HSE NETWORK, HSE MIFI OR HSE MOBILE PHONE.**

1. **Section 1:** Preparation for VPN Remote Access for **all users**
2. **Section 2:** for **Existing National VPN** users with Checkpoint software installed on their device
3. **Section 3:** for New users to **National VPN** (Regional VPN no longer supported)

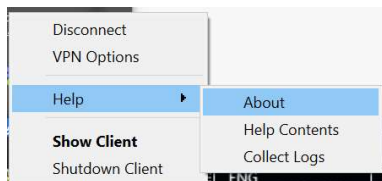
## Section 1: Preparation for VPN

### Checkpoint software verification and update

The recommended Checkpoint software version is **E85.00**

The earliest supported version is **E84.00**

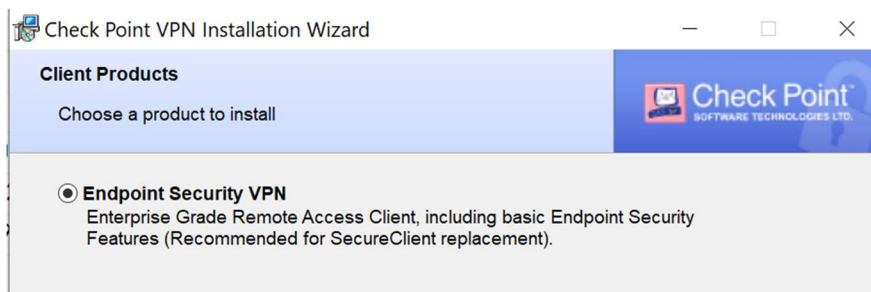
You can confirm your client version by right clicking the Checkpoint VPN tray icon and going **Help > About**



You may need to upgrade to the latest version which can be downloaded from the link below. Admin rights may be needed for installation – you may need to seek assistance from your local IT administrator or the National Service Desk – 0818-300-300 to install the upgrade.

[E85.00 Check Point Remote Access VPN Clients for Windows](#)

**Note:** Client must be installed as “Endpoint Security VPN”



## Section 2: Existing Users on National VPN

### First Time Enrolment and Cert Creation

The new method of authentication requires a cert to be saved on your device. During the enrolment process you create a password for the cert and save it to your device

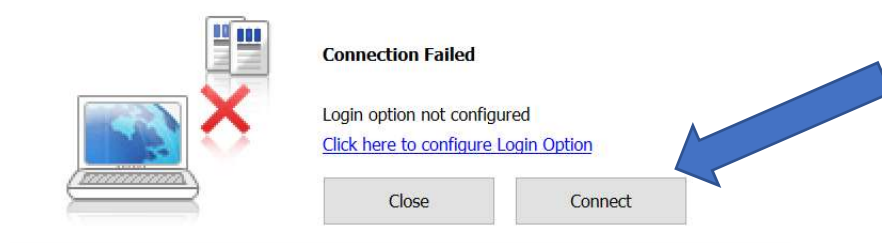
Before enrolling for their certificate users must be first issued a one-time **Registration Key** by text or email via the Service Desk.

To start the Enrolment process the user must attempt to login for the first time using their old legacy username and password. This will present the screen below in **Figure 2.0** which then allows you to follow instructions to register for their certificate.

**(Note: In some instances it may be necessary that user must re-create their VPN site please follow the instructions in Section 3 below for new users.**

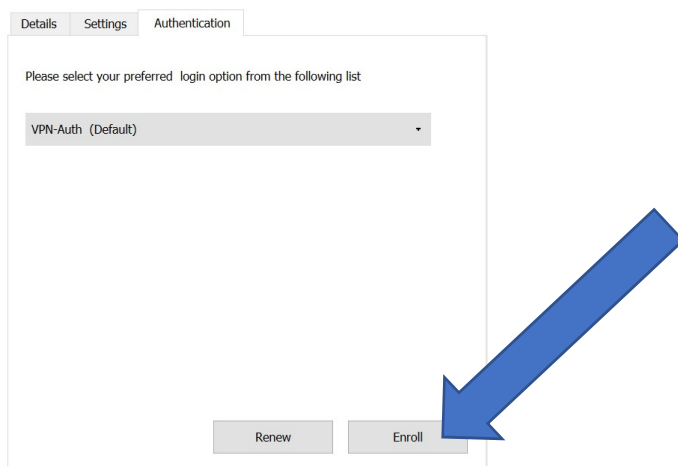
If logging in using their legacy Username / Password the user will be met with below:

**Figure 2.0 – Failed Login with Legacy Username/Password**



User must click the link above “Click here for configure Login Option” and they will then be presented with the options below.

**Figure 3 – Cert Enrolment**



Once presented with this screen choose “Enroll”.

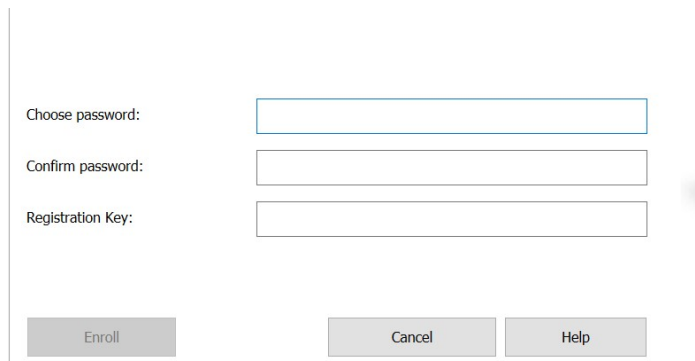
The password screen below will appear. This password must meet minimum HSE defined password requirements and users must remember this password as it cannot be reset remotely. Do not reuse any passwords used previously or on other systems. Special characters that can be used in passwords are

! " # \$ % & ' ( ) \* + - . / : < = > ? @ { }

## Certificate Based VPN

Other special characters such as £ or € are not supported and cannot be used in passwords.

You enter your new chosen password twice and then populate the **Registration Key** in the bottom box provided by the Service Desk.



Choose password:

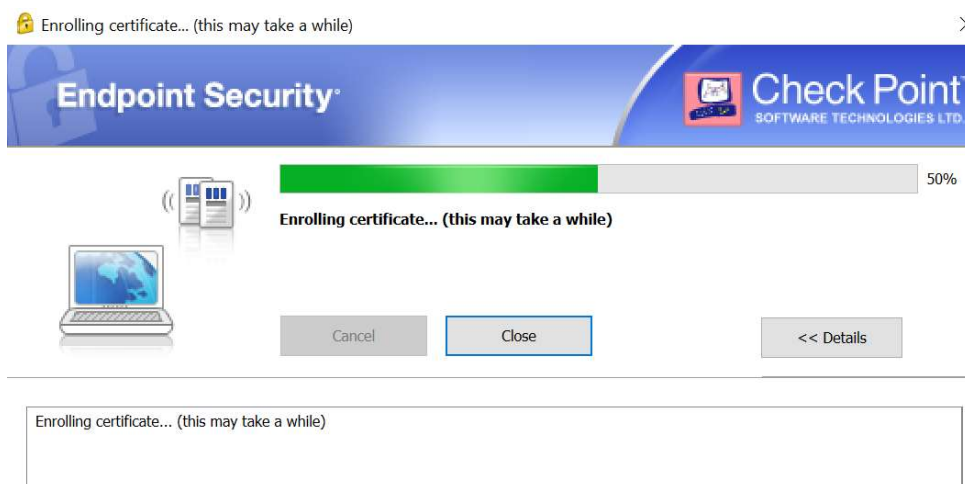
Confirm password:

Registration Key:

Enroll Cancel Help

Once all fields have been filled out you will be able to choose “Enroll” and the Enrolment process will start as per the below:

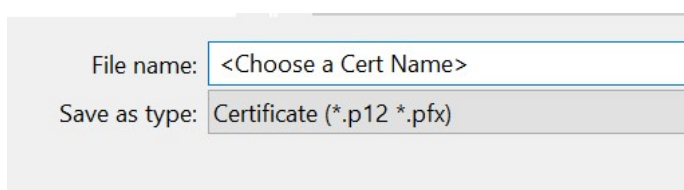
**Note:** If this process returns a failure then it can be attempted again by entering in the password again along with Registration Key.



You then choose a location on your device to save the cert to. Save this to a folder and not to your desktop or C: drive. This cert is unique to you and must never be shared with anyone.



The cert should be given a name that is related to its purpose e.g. name it based on your VPN username. Do not delete the cert as it is required for connecting over the VPN.

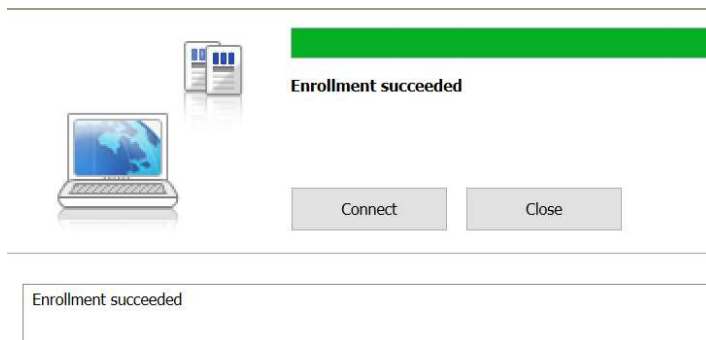


File name: <Choose a Cert Name>

Save as type: Certificate (\*.p12 \*.pfx)

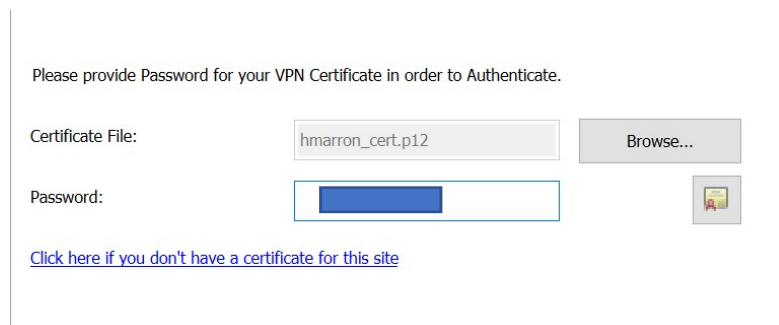
## Certificate Based VPN

Once all above is completed then the user should receive an “Enrollment succeeded” as per below.

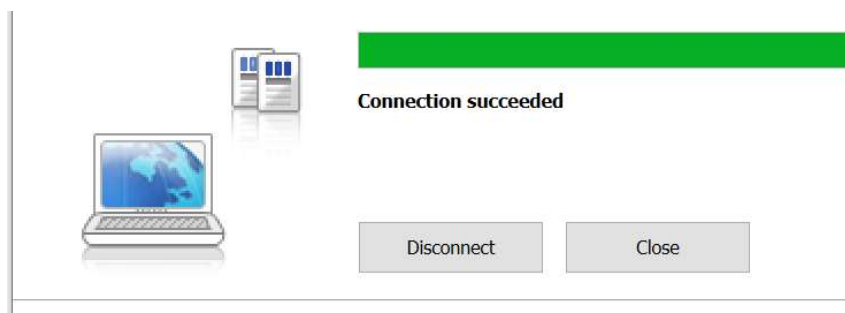


### Connection

You can now choose to “Connect” and enter the new password you have set



Below is the “Connection succeeded” message that should be received. You are now connected to the HSE network.



## Section 3 for new users to create a new VPN Site

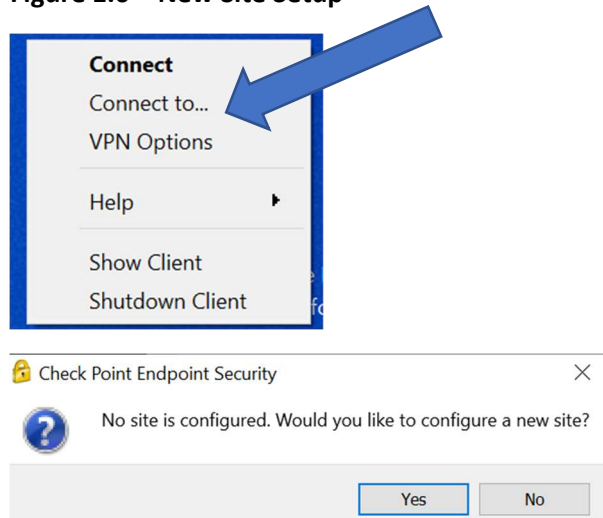
**This section is for new users of VPN or for users that need to recreate their VPN site**

Users creating their setup for first time or users who must re-create their configuration should follow these instructions. **(Note: In some instances it may be necessary that existing users must re-create their VPN site and these same instructions apply there)**

## Creating first time Configuration

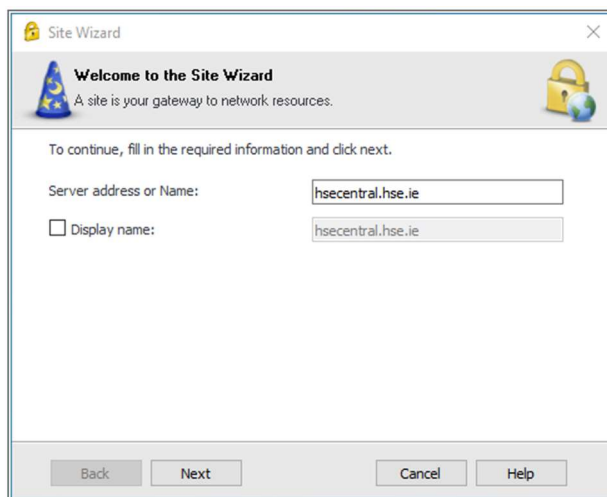
First time users or users that need to re-create their configuration must create a new Site for **hsecentral.hse.ie** as per below **Figure 1.0** > “**Connect To**” when they first open the client via the Windows tray icon:

**Figure 1.0 – New Site Setup**



Connect above to **hsecentral.hse.ie** (The adding of the “site” above is summarised in below **Figure 1.1**) **Note:** In some instances if user is re-creating their site then they can’t create a second site named hsecentral.hse.ie and it may need a differing Display name or the first one can be removed.

**Figure 1.1**



On the next screen, if presented, you can choose “**Trust and Continue**”

The site has been created and you now need to **Enrol and Create** your cert and password.

Please continue setup by following the instructions on Page 2 under the heading

**Enrolment and Cert Creation** beginning at **Figure 3 – Cert Enrolment** and continuing until process is completed.