

HSC Checkpoint Remote Access Service User Guide

Version 4.6

Table of Contents

1. Overview	2
2. Connecting your HSC laptop to your Home Broadband.....	2
3. Connecting to the HSC/GP network.....	6
4. Connecting to the HSC/GP network using a WiFi Hotspot.....	9
5. Samsung with the MobilePASS app	12
6. GPs only – Connecting to the Practice PC and Secure Practice Email	13
7. Restrictions and Known Problems	15
7.1 Old version of Checkpoint VPN software installed	15
7.2 Web Browsing	15
7.3 Using the BT WiFi	17
7.4 Internal Systems are Unavailable	17
7.5 VPN Connectivity Lost Error.....	17
7.6 No Site Configured Error	17
7.7 Failed To Download Topology Error	20
7.8 Gateway Not Responding Error / Endpoint Security Is Disconnected	20
7.9 Access Denied – Wrong Username or Password	22
8. Improving Your Experience of the Service	23
8.1 Your Broadband Connection	23
8.2 Your Connection to your ISP router.....	24
8.3 Accessing your Email via the Outlook Client	24
8.4 Accessing your Email via Outlook Web Access (OWA)	25
8.5 Editing large documents.....	26
8.6 Using the Remote Desktop Connection.....	26
9. Reporting Problems	26

1. Overview

This guide details the procedures for connecting to the HSC and GP networks using the HSC Remote Access Gateway, from a corporate PC¹, using Checkpoint Endpoint Security VPN. This service is strictly for use with HSC corporate PCs/tablets. Further requirements are laid out in the separate document, **HSC Checkpoint Remote Access Service – Minimum Device Standards**.

This user guide is available under the following link as well as other guides <https://community.sharepoint.hscni.net/sites/FAQ/SitePages/Home.aspx> -> Wi-fi and Remote Access

2. Connecting your HSC laptop to your Home Broadband

This section has been provided as guidance. Due to the diversity of home broadband connections (wireless and wired) this document cannot cover all solutions. You should follow the same steps used to connect your personal PC to your home broadband. Each Internet Service Provider has posted detailed guides on the how to do this on the internet.

You should only need to do this once unless you make changes to your home broadband network.

- Ensure your home hub / router is switched on and the appropriate lights are displaying as recommended by your Internet Service Provider (ISP).
- Power on your laptop.
- From the taskbar system tray, right click on the **wireless** icon – see Figure 1.

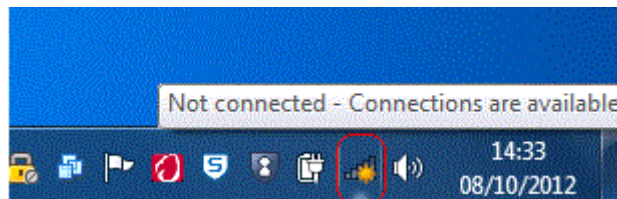


Figure 1

- For the **Windows 7** operating system the icons in Figure 1 may not be displayed automatically. To permanently display them:
 - Right click on the **Taskbar** at the bottom of your screen to display the Toolbar menu and select **Properties** - see Figure 2.

¹ Throughout this document the use of PC includes desktops and laptops.

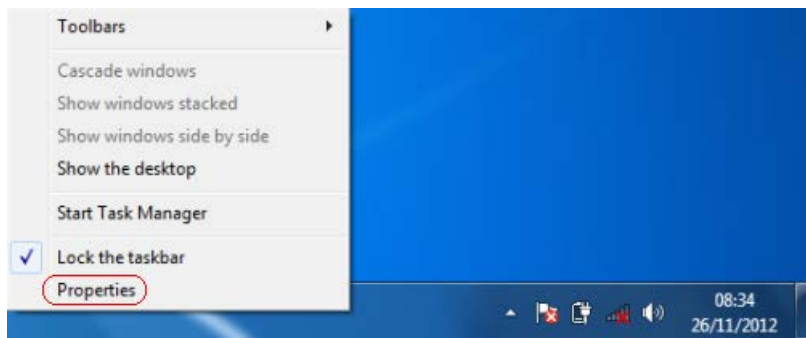


Figure 2

- In the **Taskbar and Start Menu Properties** window, click on the **Customize** button – see Figure 3

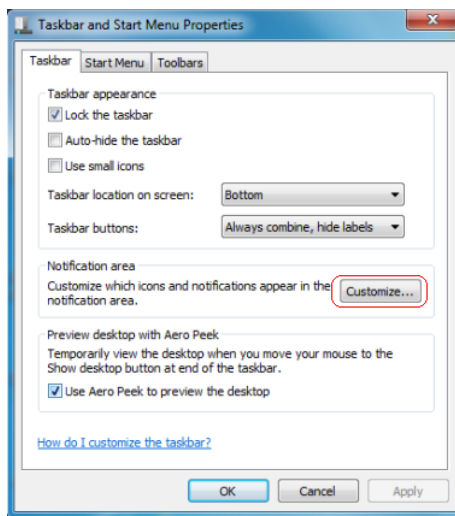


Figure 3

- In the **Notifications Area Icons** window, select **Always show all icons and notification on the the taskbar** and then click on the **OK** button – see Figure 4.

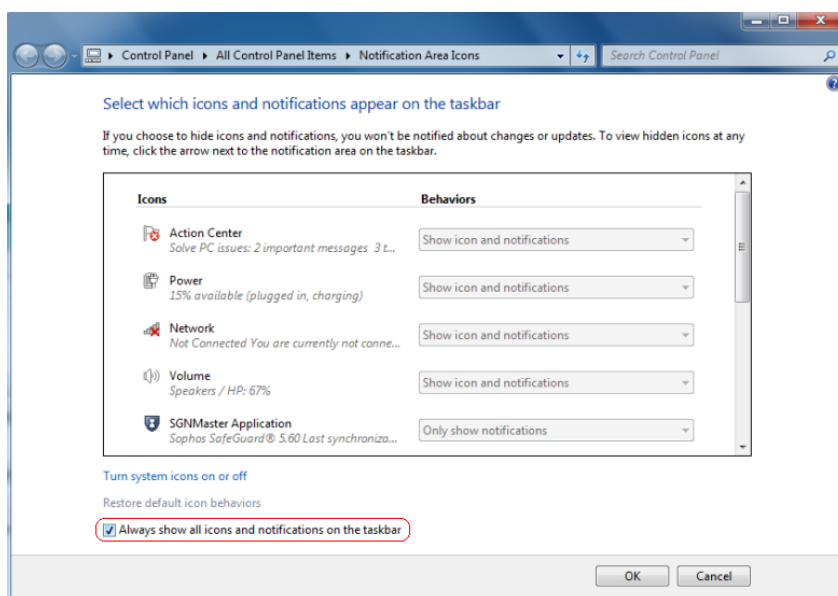


Figure 4

- Finally click on the **OK** button of the **Taskbar and Start Menu Properties** window.
- For the Windows 10 operating system, the icon in Figure 5 should always be displayed.



Figure 5

If not, you can follow the steps below to enable this icon:

- Right click on the **Taskbar** at the bottom of your screen to display the Toolbar menu and select **Taskbar Settings** - see Figure 6.

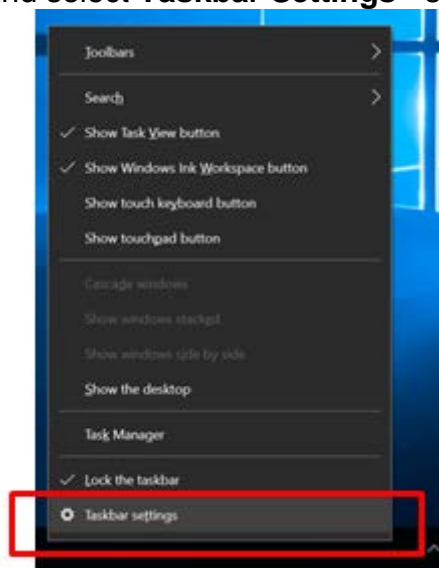


Figure 6

- In the **Taskbar settings** window, scroll down to the **Notification area** and click '**Select which icons appear on the taskbar**' – see Figure 7

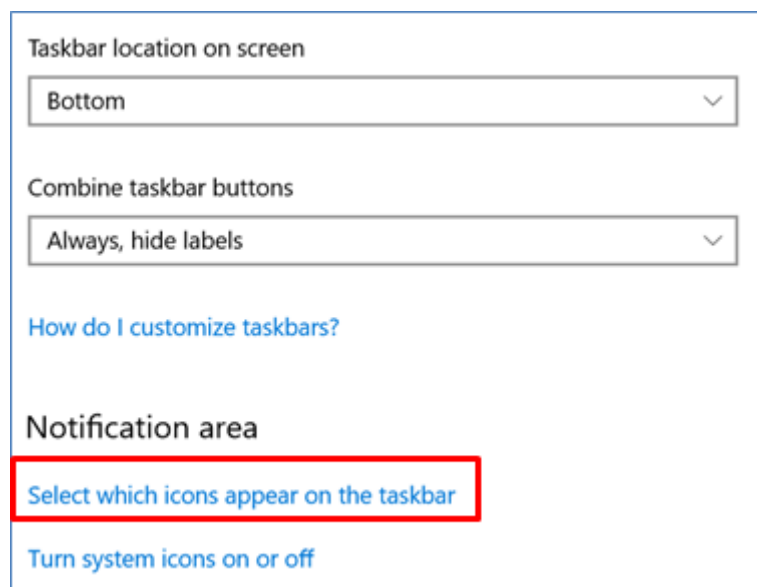


Figure 7

- In the '**Select which icons appear on the taskbar**' window, make sure Network is set to 'On' – see Figure 8

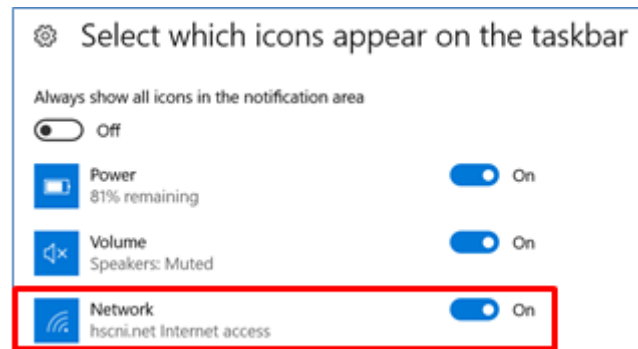


Figure 8

Note: Once you have displayed all available icons, right click on the wireless icon

The Wireless Network Connection window will be displayed. Samples of available wireless networks are shown in Figure 9.

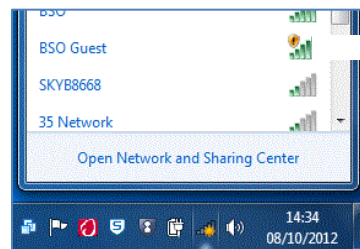


Figure 9

- **Double click** on **your home network** from the list displayed.

A connection will be made to your network.

- Assuming your home network is secured. You will then be prompted to enter your **Network Key (Wireless key)** provided by your ISP or configured manually by yourself – see Figure 10.



Figure 10

- Figure 11 shows an example of a wireless key found on a BT Home Hub router.



Figure 11

Once you have successfully connected to your home broadband, you should see **Connected**, see Figure 12.

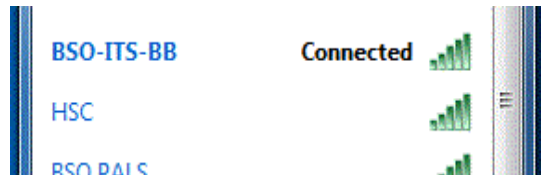


Figure 12

Even though you will be connected to your home wireless, you will have no access to the Internet or your HSC emails until you complete **Section 3 – Connecting to the HSC/GP network**.

3. Connecting to the HSC/GP network

After the Checkpoint Endpoint Security VPN software has been installed on your PC, a new icon (circled in red) in the system tray will appear, as shown in Figure 13.

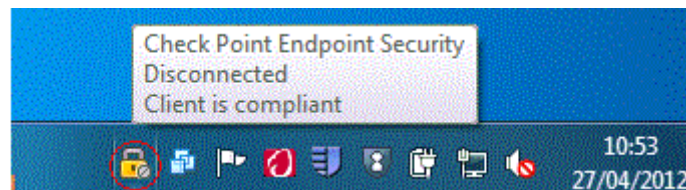


Figure 13

Right-click on this **Endpoint Security** icon and choose **Connect To**, as shown in Figure 14.

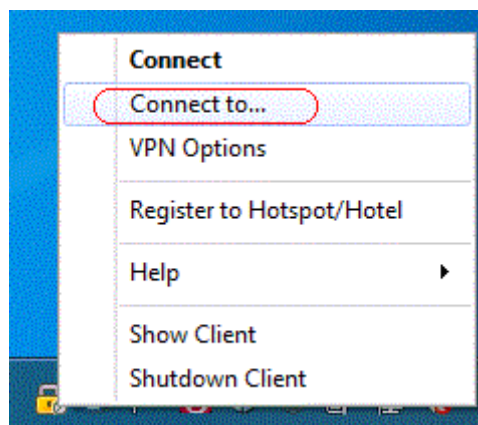


Figure 14

DO NOT use the **Connect** option as this will try to use previous log on details which have expired.

The **Show Client** link will open the Checkpoint Endpoint Security Client and allow you to see details about your session. You may be asked to access this by your ICT Support Team to help troubleshoot any connection issues you may have.

You should then see a dialogue box on the screen, which prompts you for authentication information, as shown in Figure 15. This information is for access through the HSC network gateway, not your Internet Service Provider (ISP).

Enter

- the **user name** you have been given,
- the **PIN** associated with your token and
- the six-digit number (**Tokencode**) displayed on the token, i.e. the number displayed on the screen of your Cryptocard key ring hardware token after you clicked the button on it.

NOTE: If you are using a software token, e.g. installed on your smartphone, you **leave the PIN field blank** as you have already used it to get the Tokencode. **If you have a Samsung MobilePass Token, see section 5 of this guide.**

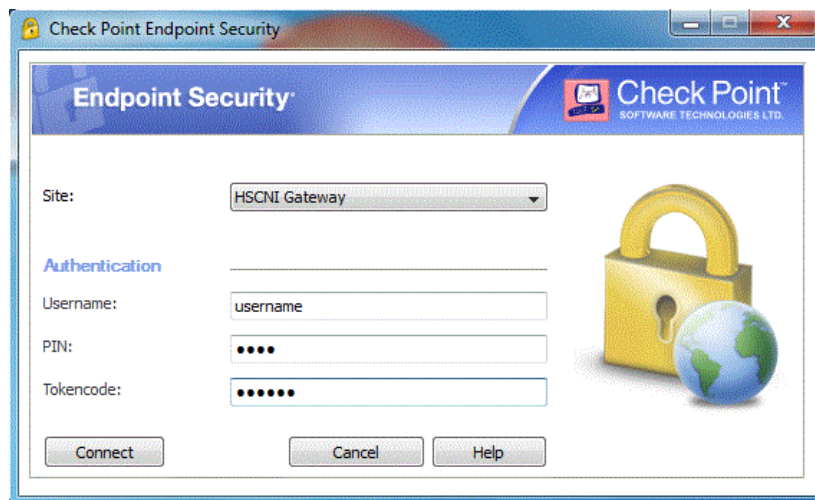


Figure 15

NOTE: If you have a **Cryptocard key ring hardware token** and this is the **first time you are using it** then you will be prompted to **change your PIN** as shown in Figure 16 below. Enter a new PIN that is **private** to you only in the **Response** field:

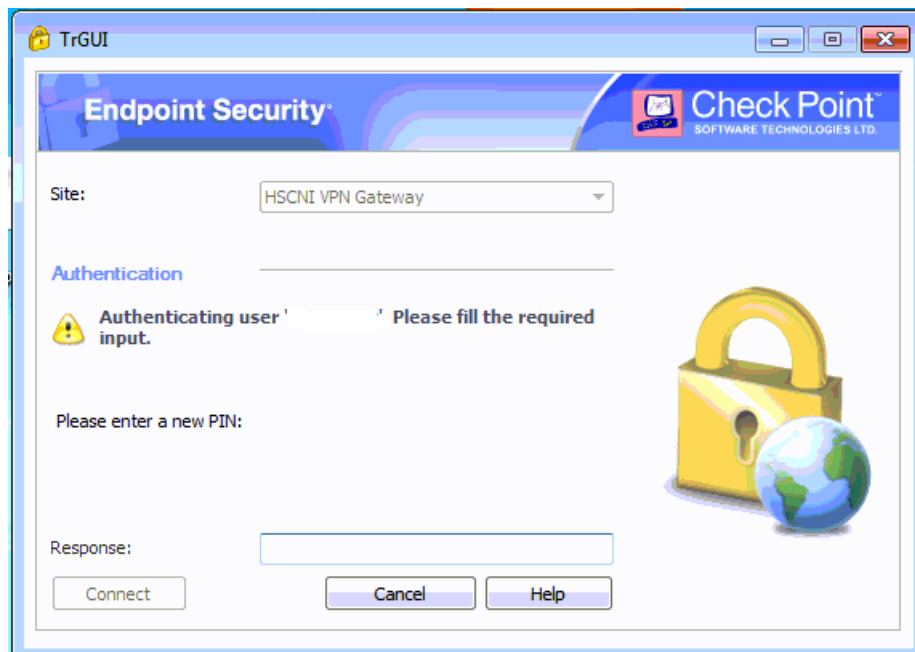


Figure 16

Next click the **Connect** button.

If all is well, you should see a message saying that your connection succeeded in the bottom-right corner of your screen, see Figure 17 below

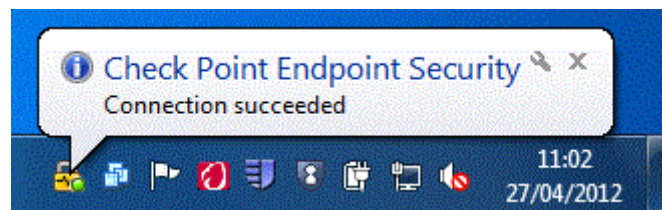


Figure 17

Figure 18 below shows a detailed version of the message, obtained by clicking the **Details** button.

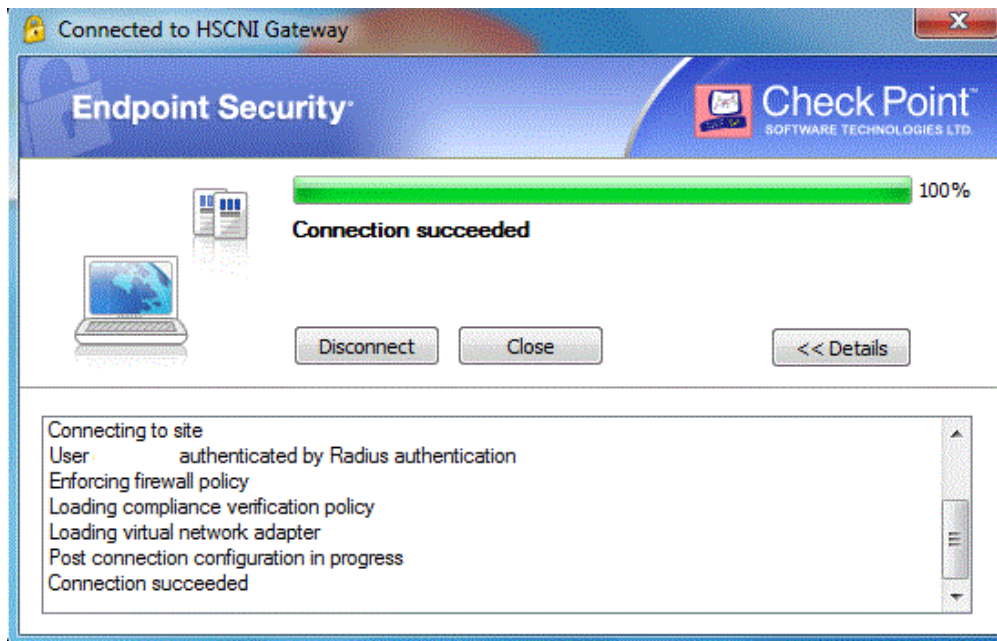


Figure 18

You now have an encrypted connection (“tunnel”) across the Internet to the HSC network and can connect to whatever systems and applications have been assigned to your HSC user account. Notice in Figure 19 how the icon in the system tray has now changed.

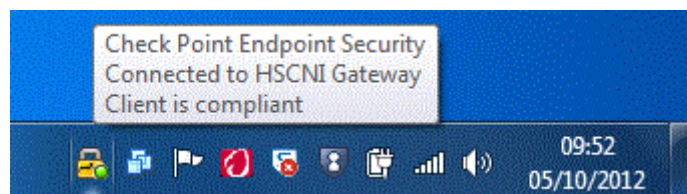


Figure 19

This lets you see at a glance whether the tunnel is in place in order to access systems on the HSC network.

When finished, you should disconnect from the gateway, by simply right-clicking on the **Checkpoint Endpoint Security** icon and choosing **Disconnect**.

4. Connecting to the HSC/GP network using a WiFi Hotspot

The Checkpoint Endpoint Security client has the ability to connect to Wifi Hotspots such as would be present in hotels, cafés etc. Connecting to a hotspot involves a few extra steps as detailed below.

Wifi networks like these will allow you to connect your HSC laptop to them. They generally will require further authentication steps such as entering a username and/or password on a webpage.

Ensure you have this additional information before you attempt to connect.

Connect to the hotspot network as you would a normal wifi network; section 2 provides further guidance on this.

Right-click on the **Endpoint Security** icon and choose **Register Hotspot/Hotel** - See figure 14. (Alternatively, skip to **Automated Process to Register on a Hotspot/Hotel** section below)

You will then be informed that you have 60 seconds to complete the registration (Figure 20).

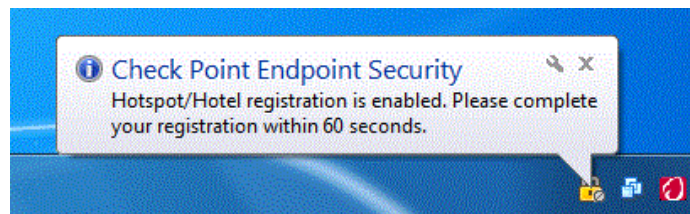


Figure 20

Open a new browser window and you should then be redirected to the hotspot's log in page. Figure 21 shows the authentication page for the BSO Guest wireless service. The hotspot you are attempting to connect to will look **similar** to this if they have enabled security on it.

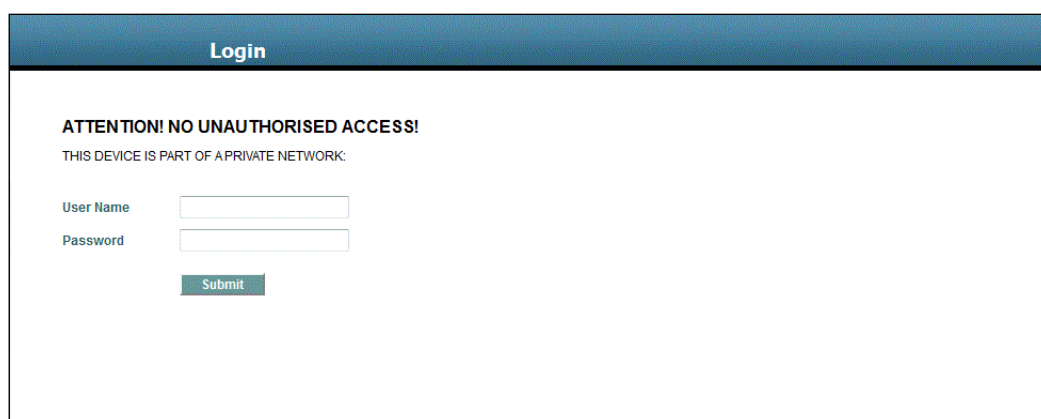
A web browser window showing a login page. The page has a dark blue header with the word "Login" in white. Below the header, the text "ATTENTION! NO UNAUTHORISED ACCESS!" is displayed in bold, followed by "THIS DEVICE IS PART OF A PRIVATE NETWORK:". There are two input fields: "User Name" and "Password". Below the "Password" field is a green "Submit" button.

Figure 21

Enter the credentials you have for the wifi network and you should then be successfully authenticated with the hotspot network.

If a login page does not display, try clicking on **Register Hotspot/Hotel** again and enter www.hscni.net in to the browser address bar. This should automatically re-direct to the local login page.

If you have successfully entered the details, the webpage will close with a message that the network path is open and it is starting a VPN connection (Figure 22).

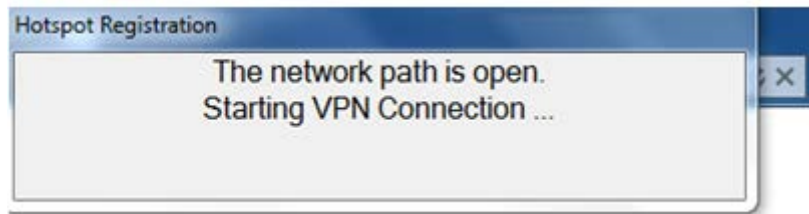


Figure 22

The Check Point Endpoint Security will then open, allowing you to connect through the HSCNI Gateway, (Figure 23).

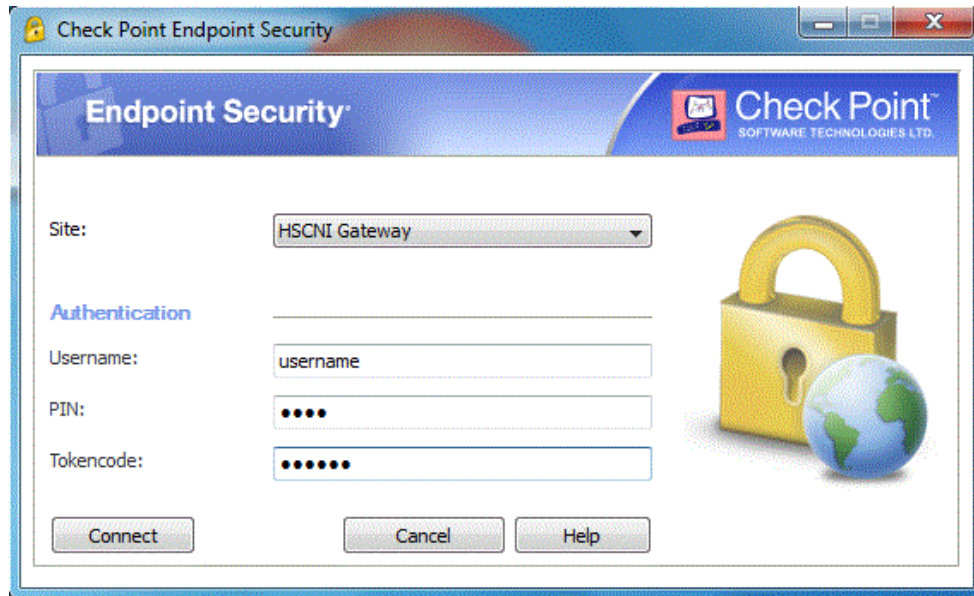


Figure 23

Enter your details and click on the **Connect** button.

Automated Process to Register on a Hotspot/Hotel

If on version E80.90 or higher (see Section 7.1 to find instructions on how to find the version installed), you can use the **Connect via Wifi Hotspot** shortcut (see Figure 24) on your desktop. This shortcut automates some of the steps:

- Connect to the wifi hotspot network as normal.
- Double-click the **Connect via WiFi Hotspot** icon which opens Internet Explorer to display the local sign-in page / terms and conditions.

Once you have signed in / accepted the terms and conditions, the webpage will automatically close and the same message as in Figure 22 will display. The Check Point Endpoint Security will then open allowing you to connect through the HSCNI Gateway, (Figure 23).

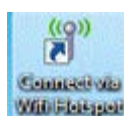


Figure 24

If using the automated method, you may see a warning appear that your 60 seconds have expired. This can be ignored as long as the message displayed in Figure 22 has been shown. Otherwise you will need to try again / use the manual process.

5. Samsung with the MobilePASS app

On your Samsung, navigate to the apps screen and locate the **SafeNet MobilePASS** app as shown in Figure 25.

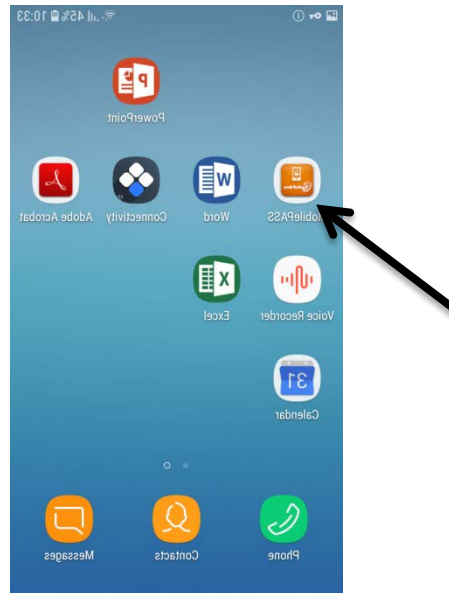


Figure 25

Open the app by tapping on the icon and you will be asked to enter your PIN as shown in Figure 26.



Figure 26

Enter your PIN and then tap the **Continue** button and a passcode will be displayed as in Figure 27.

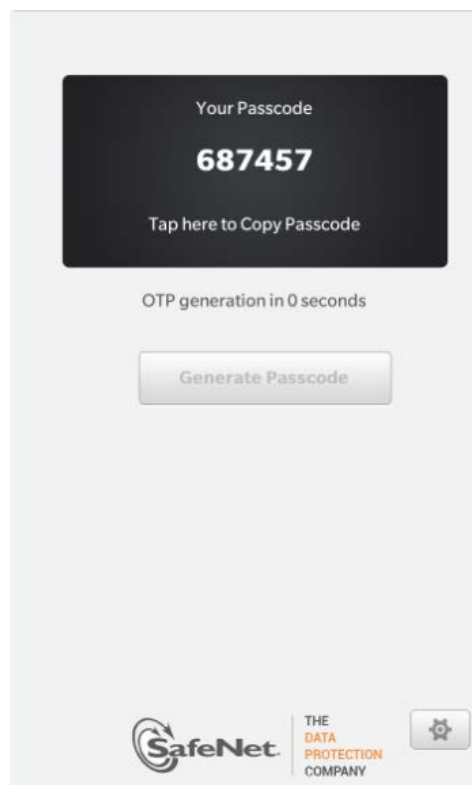


Figure 27

Back on your PC, in the dialogue box shown in Figure 15

- Enter the **user name** (it may already be there from previous use).
- Leave the **PIN** blank and
- Enter the six-digit number (**Tokencode**) displayed on the MobilePASS App (Figure 27).

NOTE: As the PIN has been used to generate the next Tokencode, it is not required during the Checkpoint Endpointy Secuirty client log in.

Now click the **Connect** button as shown in Figure 15.

6. GPs only – Connecting to the Practice PC and Secure Practice Email

The laptop used for remote access will have been configured with desktop shortcuts to access SecurePracticeMail and remote desktop sessions to PCs in the practice – see Figure 28.

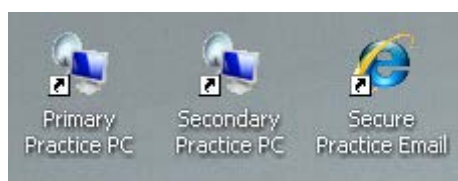


Figure 28

Double clicking on the **Secure Practice Email** icon will open the GP Web Portal and follows the same logon process as if you were in the practice.

Double clicking the **Primary Practice PC** icon will open the normal Windows logon screen to your practice PC. After entering your practice Windows username and password your practice PC desktop will be displayed (usually in full screen mode). You now have the same access you would if at the practice.

When you have taken control of the practice PC no-one else is able to connect to it and the screen is locked out preventing anyone at the practice seeing what you are doing.

Closing the remote access window will automatically lock the windows session on the PC. Therefore it is preferable to log off before closing the remote access window as this is more secure and allows someone to access it.

If configured, the **Secondary Practice PC** icon provides the same access to a second PC as the Primary one does.

7. Restrictions and Known Problems

7.1 Old version of Checkpoint VPN software installed

If your PC is using an older version of the Checkpoint VPN software (previously known as Checkpoint SecureClient) you may get a connection and then it disconnects within a few minutes. You will need to request the software be updated by your ICT Support if you get these disconnets.

To check the version **right-click** on this **Endpoint Security** icon and choose **Help -> About**, as shown in Figure 29, which will display a window listing the version.

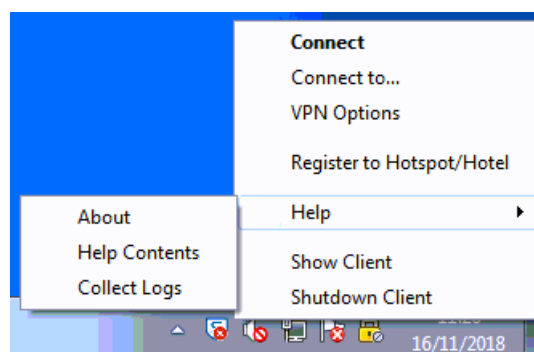


Figure 29

Also with older versions of Checkpoint VPN software you may not have access to wifi hot spots. Should you need this type of access please log a service request to have it upgraded.

The following Checkpoint VPN software versions support wifi hotspots:

- E80.42
- E80.51
- E80.60
- E80.62
- E80.70
- E80.83
- E80.90

Windows 10 is supported from E80.62 onwards.

- E80.62 supports Windows 10 builds 10240 and 10586.
- E80.70 supports Windows 10 versions 1511, 1607 and 1703.
- E80.83 supports Windows 10 versions 1607 (LTSC), 1703, 1709 and 1803.
- E80.90 supports Windows 10 version 1809.

Should you require connection from wifi hotspots and/or are using an older version please log a request with your ICT Service Desk to have it upgraded.

7.2 Web Browsing

The Checkpoint Endpoint Security software has an in-built firewall mechanism to control access between your PC and other computers. This means, for example, that it will not allow your PC to access most WWW sites, unless you first establish a connection to the HSCNI Gateway, as shown in the procedures above. There are three notable exceptions to this rule:

- the HSC SSL Remote Access Service
- the HSC Bomgar Remote Support Website – support.hscni.net
- BT WiFi (formerly OpenZone) sign-in

These services are available without first having to connect the HSCNI Gateway.

The reason that most web browsing is forced through the remote access gateway is this allows the necessary web traffic filtering to be applied which helps protect your PC from malicious web sites. Malicious web sites have now become the primary means by which the security of corporate PCs is compromised.

The exception to this is the 60 seconds you have to register to a wifi hotspot.

7.3 Using the BT WiFi

If your PC has wireless networking enabled, you should be able to use the BT WiFi wireless networking service. In this case you must first sign-on to BT WiFi and then connect to the HSCNI Gateway. Further information is available from <http://www.btwifi.com/>.

7.4 Internal Systems are Unavailable

Occasionally you will find that you are unable to access some systems that you would be able to access when in your office. This normally occurs where the system in question is not within your own organisation. Please report such problems to your ICT Service Desk, who will then be able to resolve them in conjunction with BSO ITS.

7.5 VPN Connectivity Lost Error

This issue can usually be resolved by restarting the laptop or restarting your Broadband router

However, when this issue occurs on a Surface Pro it needs to be done in a particular way. Most users will restart the Surface Pro by holding down the power button and then swiping down to restart when prompted. However this method does not resolve the issue.

Instead, you will need to go to your desktop. Right click the **Start button/Windows orb** at the bottom left corner of the taskbar. Hover over **shut down** until a list with more options appears and then click on **Restart** from that list.

Once the device has been restarted, Checkpoint will function as normal and connection should be restored. If this is not the case, then an install of a later version of Checkpoint VPN software may be required. Please contact your ICT Service Desk and request that a call be logged with this issue described.

7.6 No Site Configured Error

When attempting to connect remotely, if you encounter the error message **No site configured. Would you like to configure this now?** Select **Yes** and it will take you through the **Site Wizard**.

Alternatively, you can also access this by right-clicking the Checkpoint icon (Gold padlock) located at the bottom right of your taskbar, bringing up a list of options. Within that list, click on **VPN Options** (Figure 30), and then click on **New** which will bring up the **Site Wizard**.

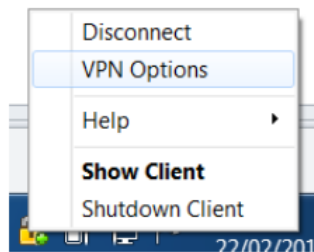


Figure 30

Click on the **Next** button and then enter **194.168.231.129** in the **Server Address or Name** field (Figure 31). Then tick the box for **Display name:** and replace whatever text is in there with either **HSC2** or **HSC Gateway 2** (the name must be different to the existing configuration).

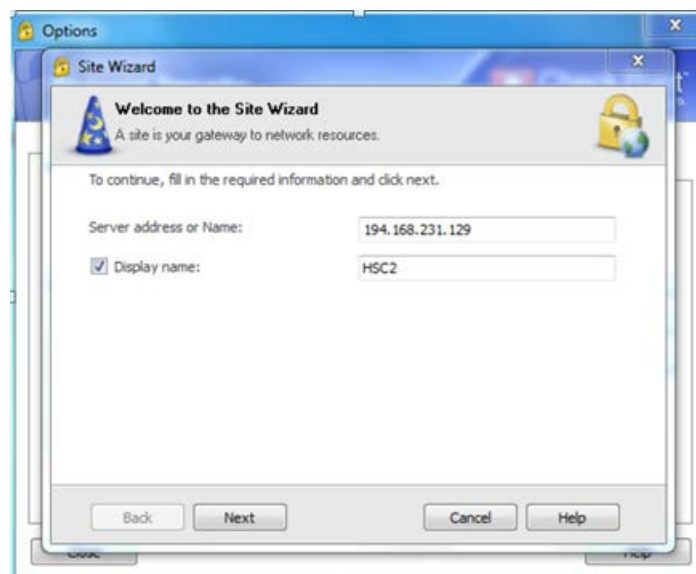


Figure 31

Click the **Next** button and it will say **Please wait while creating the new site** (Figure 32). At this point, you may have a Security message pop up. Select **Trust and continue**.

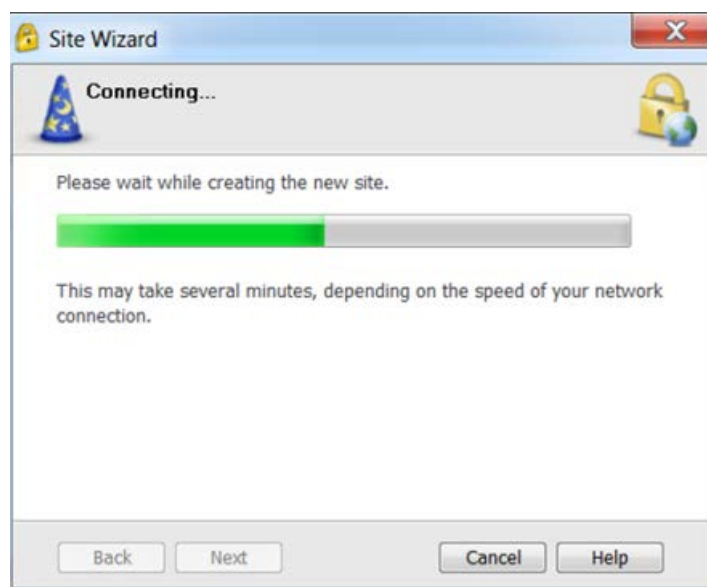


Figure 32

You will then be prompted to select an **Authentication Method** (Figure 33). Select **SecurID** and then click the **Next** button.



Figure 33

In the next screen, the option **Use keyFOB hard token** should already be selected. Leave this default setting, even if you have a MobilePASS or software token on and click the **Next** button.

Finally click the **Finish** button and then the **Yes** button when asked if you would like to connect.

NOTE: Please be aware that you will need to type in your remote access username.

Once connected successfully, you will then need to delete the old site. This can be done by right clicking the Checkpoint icon and selecting **VPN options** (Figure 34).

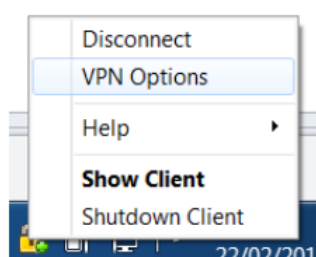


Figure 34

Highlight the site which is **NOT** called **HSC2** or **HSC Gateway 2** (whichever name you used during site creation) and click the **Delete** button. (Figure 35)

Finally you can click the **Close** button and continue as normal.




Figure 35

7.7 Failed To Download Topology Error

This error can be fixed by restarting your laptop/tablet. However, it is a known issue in the software version that this may not always work first time. If after 2 or 3 restarts the issue still persists, the device may need a more updated version of Checkpoint VPN software installed. Please contact your ICT Service Desk and request that a call be logged with this issue described.

7.8 Gateway Not Responding Error / Endpoint Security Is Disconnected

Ensure the HSC device is connected to the WiFi and ensure that it states there is **Internet Access** (You can check this by hovering over the WiFi icon ). If you are unable to see any wireless networks, please ensure that the wireless on the laptop is switched on.

Depending on the device, this is generally indicated by a lit up wireless icon on the laptop itself. If the wireless is switched off, again depending on the laptop it can be turned on by

- A **slider switch** on the side (Dell Latitude Users Figure 36),
- A **button** above the F1-12 keys (HP Laptop users Figure 37 (**Note:** It may not exactly be in that position. It could be to the right of where it is displayed in the example image)) or
- By holding the **FN** key and pressing an **F1-12 key** (Again, this is different depending on the laptop model e.g. F3 on one laptop, F8 on another.) See Figure 38 for an example of the wireless icon on an **F Key**.

Left Side View

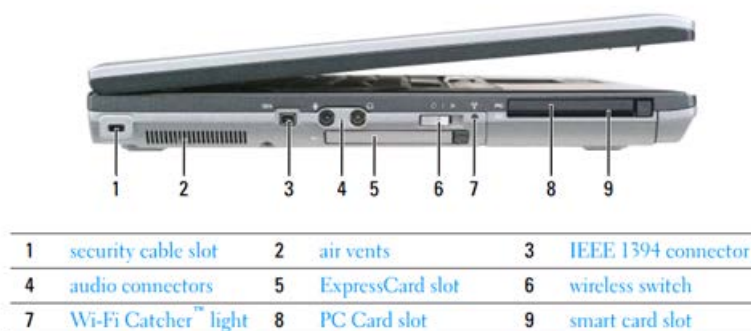


Figure 36

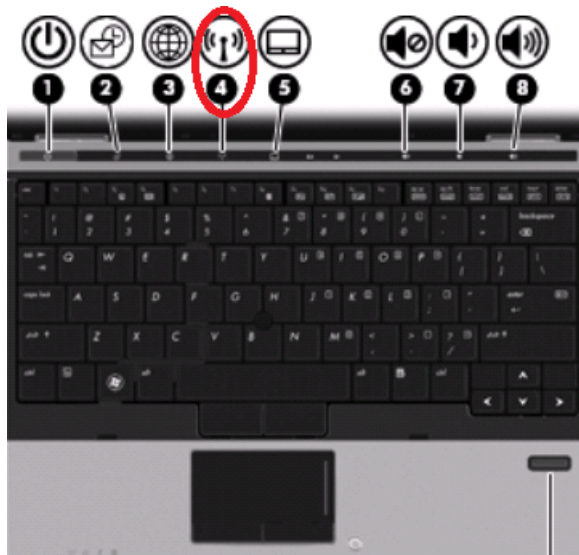


Figure 37

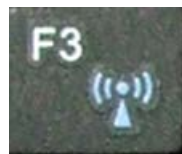


Figure 38

If it is connected but there is **No Internet Access**, take a look at any other device (e.g *personal computer*) you have connected to the WiFi and check to see if they have access to the internet. You can check this simply by opening a webpage such as Google. If the webpage does not open up then it most likely means the problem is with your broadband configuration and you will need to speak to your Internet Service Provider.

NOTE: Simply rebooting your broadband router can often successfully restart wireless and internet connections in your home.

If the webpage does open up on another device, you will need to reconnect to your WiFi on the HSC Device. This can be done by left-clicking on the WiFi icon to bring up the list of available networks and then right-clicking the network you are currently connected to and selecting **Forget This Network**. This will disconnect you from the WiFi and upon reconnecting it will prompt you to input the WiFi password. Once you have done this, connection should be restored and it should say **Internet Access** when you hover over the WiFi icon.

If reconnecting to the WiFi does not resolve the issue either, then you may be running an out of date version of CheckPoint, in which case an installation of the latest version of Checkpoint VPN software may be necessary. Please contact your ICT Service Desk and request that a call be logged with this issue described.

7.9 Access Denied – Wrong Username or Password

Ensure your username is correct. It should be the first letter of first name, followed by the first four letters of your surname and ending in triple digits e.g. jblog001.

NOTE: If your surname is three letters long, add an extra zero e.g. jblo0001.

Assuming the username is correct; ensure you are entering your token code (6-digit code) correctly. This code is generated either by your cryptocard key ring or a software token stored on an app you have installed onto your mobile device.

NOTE: A new token code must be generated every time you attempt to log in regardless if the attempt was successful or not. This can be done by holding the button down on a cryptocard key ring until it turns off, or by re-opening the app your software token is stored on.

If you are still experiencing issues, it may be due to the PIN field of the Check Point login. Make sure this is left blank if you are using a software token as you will have already entered the PIN into the app.

For cryptocard key ring users, you will need to enter your 4-digit PIN into the PIN field of the Checkpoint login.

See Figure 39 for an example of the Check Point login screen.

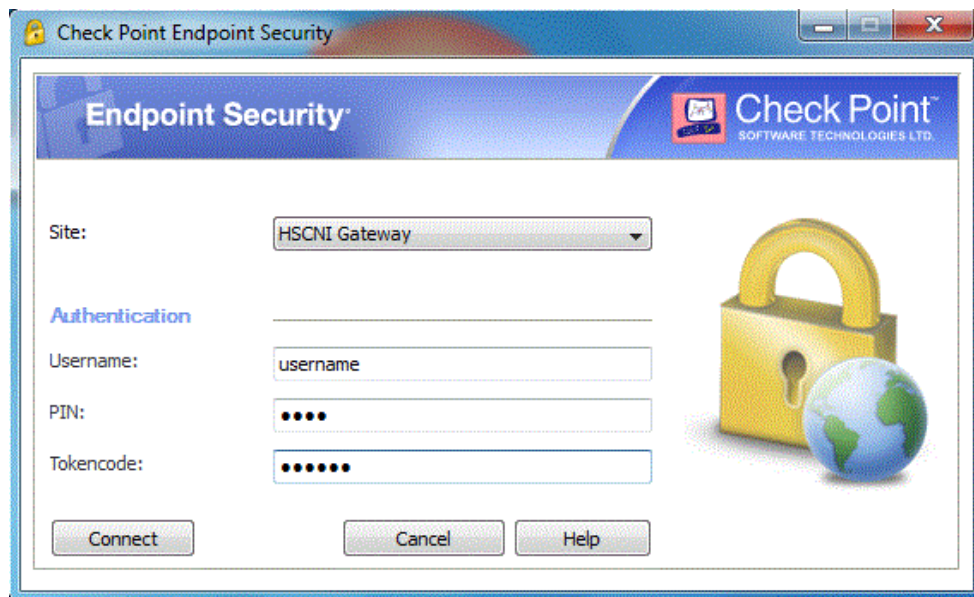


Figure 39

8. Improving Your Experience of the Service

When using the remote access service you may encounter poor performance. This can be caused by a number of factors. Below are some things that you can do to mitigate them.

8.1 Your Broadband Connection

Depending on the contract you have with the Internet Service Provider (ISP) this will ultimately determine the best performance you can get. Your contract may state download speeds of up to 8Mbps or higher. However these levels are not often achievable. This may be down to the distance from your home to your nearest telephone exchange and/or the number of other customers contending for the bandwidth in your area. If you have a number of PCs in your home connected at the same time they will all be vying for the bandwidth and if someone is downloading or streaming video this will greatly reduce what bandwidth is available to you.

To check the speed of your internet connection you can use a broadband speed checker. You need to run this test from your own PC, not the HSC provided laptop. If run from the HSC laptop, the checker will test the speed of the HSC web access.

There are a number of these available. One that is easy to use and understand is available at <https://www.broadbandspeedchecker.co.uk>

It displays the results in speedometers for download and upload speeds. An example is shown in Figure 40.

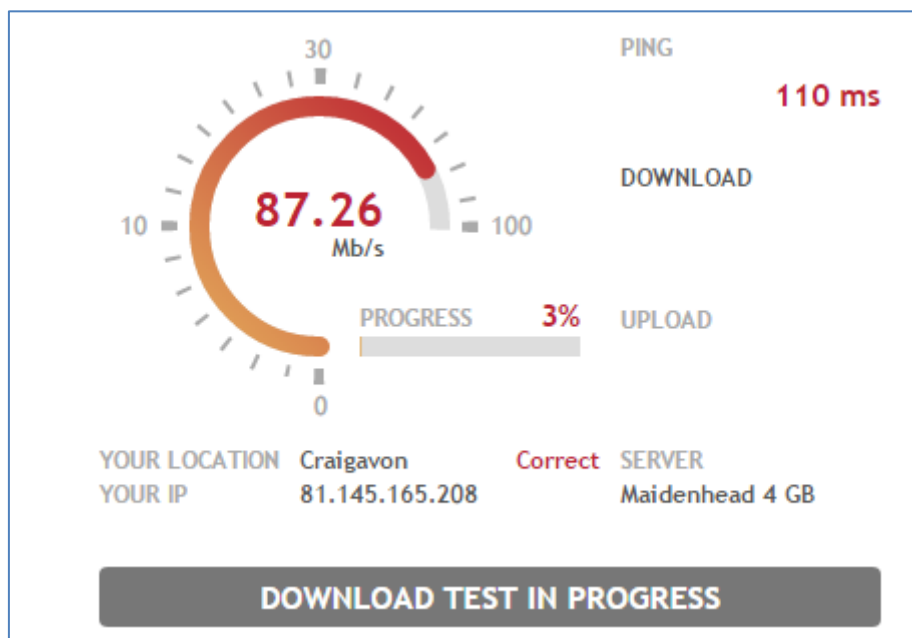


Figure 40

As a general rule of thumb, if your download speeds are below 2Mb you may encounter performance issues if you use the Outlook client for mail and edit files from their network share. Alternative ways of working are described below.

8.2 Your Connection to your ISP router

In general a wired connection will provide better performance than a wireless one. You can test this by connecting your laptop directly to one of the network points on your router with an ethernet cable.

To remove the need to run network cables around your home you may want to consider the use of Homeplugs. These provide wired connections between a pair or more if required of devices through your home's electrical wiring system. The advantage is they can provide faster and more stable connections than wireless. Further information is available from <https://en.wikipedia.org/wiki/HomePlug>

8.3 Accessing your Email via the Outlook Client

The use of the full client version of Outlook can cause performance problems when working remotely, such as not responding or being extremely slow to respond.

If you have enabled the Cache Exchange Mode i.e. a full copy of your mailbox is stored on your laptop to enable you to work on it offline, this may cause delays when you first make a connection as it synchronises.

Exchange will immediately synchronise your laptop copy with the one held on the relevant HSC exchange server. This may take some time if you have received a large number of emails since you last connected the laptop to the network or large attachments are involved.

To turn Cached Exchange Mode off, do the following.

Outlook 2010

Open Outlook. Go to **File > Account Settings** and then **Account Settings** (Figure 41)



Figure 41

Once in **Account Settings** select **Change**

Ensure that **Use Cached Exchange Mode** is unchecked – see Figure 42.

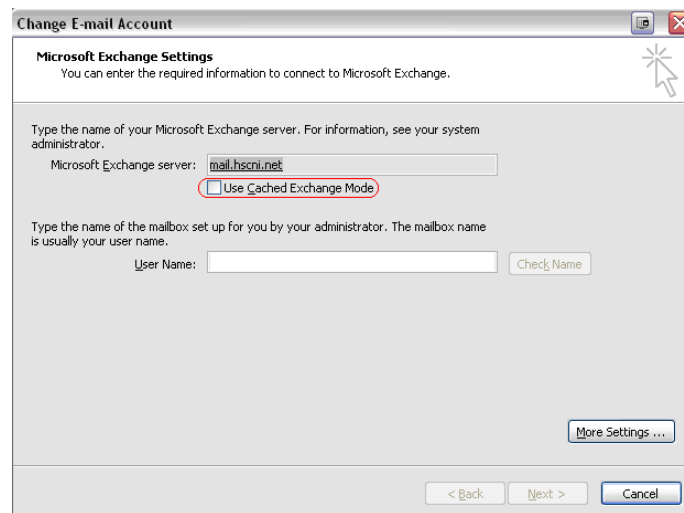


Figure 42

Exit and restart Outlook.

8.4 Accessing your Email via Outlook Web Access (OWA)

This provides access to your email account via a web browser, i.e Internet Explorer. Over a slower connection this provides a quicker response than using the Outlook client.

To access this open Internet Explorer and enter your OWA url. Your ICT Support Team can provide this.

For @hscni.net users the link is <https://mail.hscni.net/owa>

You can save this in your favourites for future use.

The following window will be displayed (Figure 43)

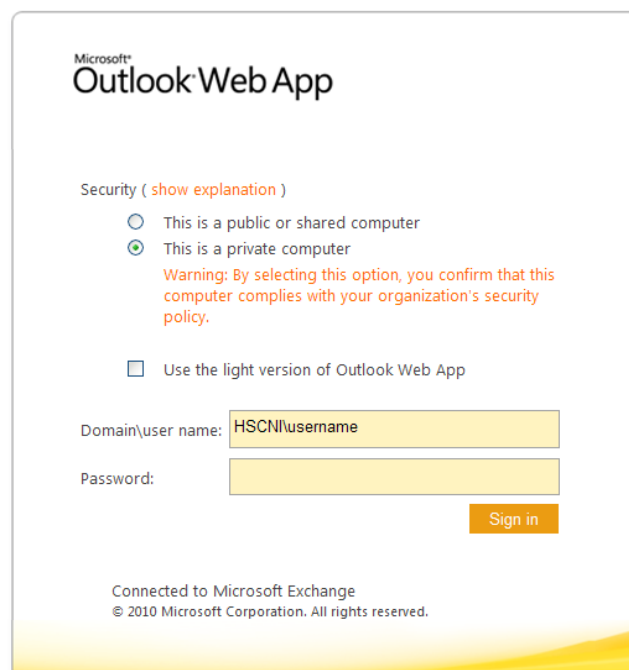


Figure 43

The format for logging in is as follows:

Username: Domain Name\Your network userid id e.g.HSCNI\blog001

Password: Your network password

Then click on the **Sign In** button.

You will be able to use this as you would the full Outlook client.

8.5 Editing large documents

If you need to edit or review large documents, especially if they contain images, it is best to transfer them to your laptop. This would most commonly apply to Word documents, PDF files and spreadsheets.

Once you have finished the editing you should transfer the edited version back its original location.

If you have only reviewed the document and are finished with it, it can be deleted from your laptop.

8.6 Using the Remote Desktop Connection

If you have a desktop PC as well as a laptop then you can use the Remote Desktop Connection application on your laptop to connect to your desktop. You should log a Service Request to have this enabled.

9. Reporting Problems

If you are experiencing issues or have any queries about the HSC Checkpoint Remote Access Service you should contact your **ICT Service Desk**.

Please provide details of any errors messages that are displayed and how far you get in the connection process before the error appears. This greatly helps the ICT teams when investigating the problem.