



TELECOMMUTING RESOURCE | TROUBLESHOOTING CONNECTION ISSUES

Table of Contents


1. Verify Internet Connectivity	2
2. Troubleshooting Home Network Issues	2
3. Verify the Check Point VPN Client is Working	3
4. Validate the Check Point VPN Client Configuration	3
4.1 Checking the VPN client version.....	3
5. RSA Token Troubleshooting	4
5.1 RSA Expiration	5
5.2 Verify RSA PIN.....	6
6. Credential Prompts or issues loading INL Websites	6
6.1 Verify Logon Account	6
6.2 Smart Card and Credentials Prompts on INL websites.....	6

1. Verify Internet Connectivity

An adequate high-speed internet connection is needed to use VPN.

Note: If you are at an INL facility and are connected to the INL network, VPN will not function correctly. You will need to be connected to a third party (external) network such as a Home network or a hot spot to verify your VPN connection.

Once you attempt to connect to an external network, verify your connection by looking at your network icon.

For Windows 10, wireless should look like  and wired should look like .

If you see that you have network connection, try going to an external site, such as [Google.com](https://www.google.com) or [inl.gov](https://www.inl.gov).

2. Troubleshooting Home Network Issues

Troubleshooting home network issues should be done through your ISP (internet service provider). One suggestion is rebooting your home router which often fixes connection issues.


Here are some contact phone numbers for common ISPs in eastern Idaho. If your provider is not listed, you will need to look up your provider contact information:

- Sparklight (formerly Cable One): 208-523-4567
- CenturyLink: 1-877-598-8568
- Rise Broadband: 1-866-988-7163
- SafeLink: 1-888-692-5776
- SpeedConnect: 1-866-297-2900

Troubleshooting Hotel and Convention Center Internet Service

1. In some instances, you may need to contact the front desk in a hotel for a password to access the internet.
2. The same may apply in convention centers. Contact your host to make sure you can get clear internet access before trying to use VPN.
3. Some third-party networks may have VPN access blocked by their firewall.
4. If possible, connect using a secondary means such as a hot spot service from your mobile phone. Nearby businesses such as coffee shops also usually offer a free Wi-Fi service.
5. If the hotel you are staying at has a user agreement page, please attempt to go to an external site such as [Google.com](https://www.google.com). If your browser is attempting to authenticate to an internal site such as the INL homepage, you may not be able to accept the agreement terms.

3. Verify the Check Point VPN Client is Working

Verify on the bottom right corner (for Windows) or top right corner (Mac) there is a padlock icon showing. 

Sometimes the client may be having issues and you may need to reboot the computer, which will also reboot the VPN client. Once back up and you have verified that you are connected to the network, try again to connect with the VPN client.

Note: Verify you have no other VPN clients installed. Some VPN clients have been known to conflict with each other. One known conflict is with Check Point VPN Client and Cisco VPN Client. If you do have two VPN clients, try uninstalling the secondary VPN client and see if you are then able to connect.

4. Validate the Check Point VPN Client Configuration

In most cases if your device was originally configured by a Field Services technician, your Check Point VPN client is probably configured properly.


To verify what hostname or IP address you are using to connect, right-click on your VPN padlock icon and go to VPN Options. Select the site you have created and click on Properties. You should see the hostname or IP address. Unless there is some type of exception, this is the hostname/IP address that should be used.

inlaccess.inl.gov

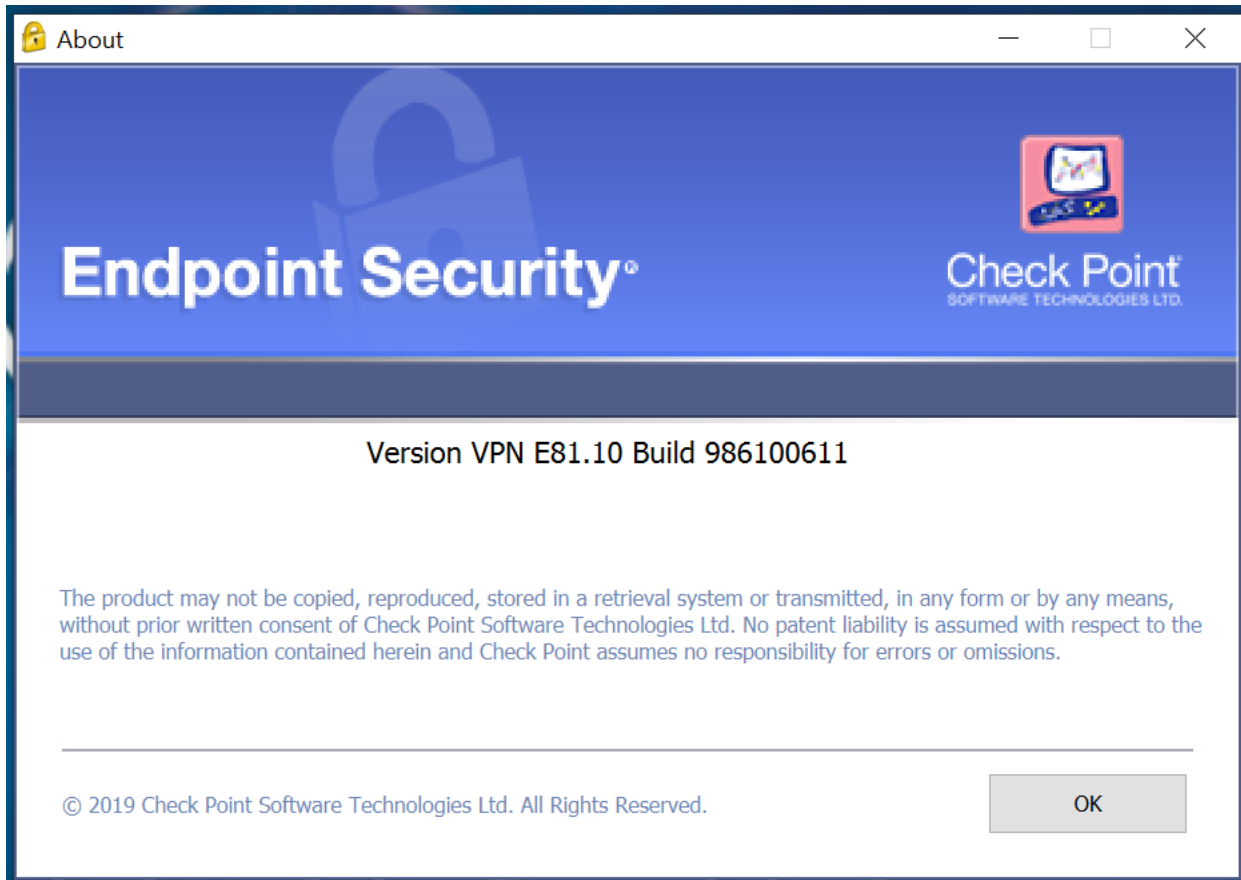
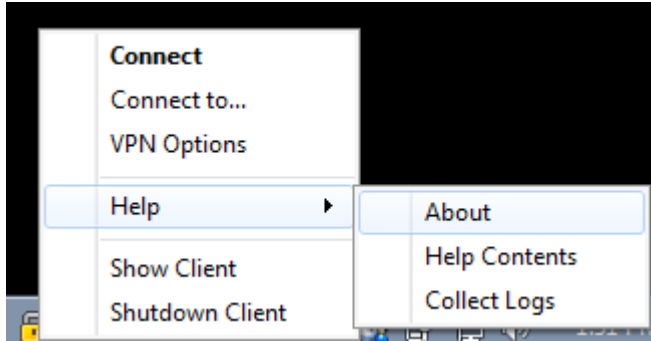
For step-by-step instructions on configuring Check Point VPN, we refer you to the guides “How To Configure Check Point VPN client (Windows)” or “How to Install and Configure Check Point VPN (Mac)” that can be found at inl.gov/gethelp.

4.1 Checking the VPN client version.

Note: The VPN client is to be installed *only* on INL-owned (government-furnished equipment) computers for BEA employees. Subcontractors can use VPN on third-party (non-GFE) computers if approved by the subcontract. (See LWP-1302, section 4.2 for details).

Right-click (Windows) or normal click (Mac) on the VPN icon in the system tray , select **Help > About** such as the screenshot shows below. A new window will appear showing the version. The approved versions are:

- E81.10 for Windows 10
- E80.71 for Mac OS X



Check Point installation can be found on the file share <\\Deploy1\install\vpn>, but if you are not in a position to install the client, you may need to call the OpsCenter at 208-526-1000 for further instructions.

5. RSA Token Troubleshooting

An RSA token provides the authentication code used in conjunction with the VPN client. This token can be a hard token (physical) or a soft token that is installed on either an Android or iOS device. This section goes through common steps that will help ensure your RSA token is functioning properly.

5.1 RSA Expiration

Hard Token: Expiration dates can be located on the back of your RSA token. If your token has expired, it will not work with the VPN and you will need to order a new one. You can email VMOPS@inl.gov



Soft Token: To locate the expiration date of your soft token, please see the applicable section below based on the type of device you use.

iPhone

- Open the RSA app.
- Enter your PIN.
- In the bottom right corner, select the information icon.

Android

- Open the RSA app.
- At the top right of the screen, select the information icon.

If the software token has expired, reinstall the application and email the binding id/device to VMOPS@inl.gov

5.2 Verify RSA PIN

If this is the first time you have used VPN, chances are that you have not yet set the PIN for your RSA token. For help with creating a PIN, please call the OpsCenter at 208-526-1000.

If you are not a first-time VPN user, your token may need to be resynchronized with the server. The OpsCenter (208-526-1000) can assist with resyncing your token. You will need to speak to an OpsCenter technician over the phone and have your RSA token available to complete this process.

If you have forgotten the PIN, an OpsCenter technician can clear the old PIN and then you will enter the six-digit code from the token in order to create a new PIN.

6. Credential Prompts or issues loading INL Websites

6.1 Verify Logon Account

Make sure you are not logged in with a local account if using a Windows device. Only a network account (logging in with badge) will allow you to log in without prompts. A local account will prompt for your network credentials every time since the logon credentials are used by single sign on for authentication.

6.2 Smart Card and Credentials Prompts on INL websites

Another cause for credential prompts while going to INL websites through VPN is that your card needs to be put back into the reader so it can pass your credentials through. Credentials need to be passed through the card before accessing file shares or home shares. Once the connection is established to the share or website, the card can be taken out.