Getting Started with Remote Access to the CMS Network

Table of Contents

Getting Started with Remote Access to the CMS Network

Introduction

This document will assist you with remotely accessing the Centers for Medicare & Medicaid Services (CMS) network infrastructure via wired or wireless connectivity through a Virtual Private Network (VPN).

- The CMS Network and all resources – including Internet, Mainframe, Microsoft (MS) Outlook, and any network drives – will be available when you have successfully logged into the CMS Network via the VPN.
- If you have been issued a Personal Identity Verification (PIV) card, use this card to access the network remotely. An RSA Token can also be used as a remote login option.

Prerequisites

To access the CMS Network remotely, you must have the following items:

- CMS-furnished laptop.
- A PIV Card or RSA Token "fob" (if it was issued to you).
- High-speed Internet access from a remote location.

Remote Access via a Wired Connection (Network Cable Connector)

Remote access can be accomplished by establishing connectivity via a wired connection from a remote network to the Dell E6400/E6410/E6420 laptop. You will need to have a network cable, with one end plugged into a network router and the other end connected to the back of your laptop.

1. Boot up your machine.
2. Wait for the machine to completely boot up.
3. Plug the network cable into your machine.
4. Log in using your CMS user ID and password. (Ignore the VPN Client window that displays in the lower left corner of the screen.).
5. Proceed to the "Connecting to the VPN" section (see page 13).
6. Select one of the VPN connectivity steps for using either your **PIV** card or an **RSA Token.**

Getting Started with Remote Access to the CMS Network

Remote Access via a Wireless Connection

Remote access via a wireless connection is managed by the **SpectraGuard S.A.F.E.** software installed on your laptop. The S.A.F.E. **icon** is found in the lower right corner of your system tray and looks like a shield.

To gain a wireless connection to the network you will need to turn on wireless for the Dell laptop, activate the **S.A.F.E.** Wireless card, then activate the wireless adapter on the computer. Follow the steps below.

Note: You will need to know the name of the wireless network – also referred to as the service set identifier (SSID) – and the encryption password for the wireless network to which you are connecting for this procedure. The SSID and encryption password are provided by the Internet Service Provider (ISP) that supplies the wireless service.

1. Select the wireless switch located on the right side of the laptop and move it towards you so that the slot does ***not*** show red. 
2. Boot up your machine.
3. Wait for the machine to completely boot up.
4. Log in using your CMS user ID and password. (Ignore the VPN client window that displays in the lower left corner of the screen.)
5. Configure your WiFi by double-clicking the **WiFi adapter** icon.  **(**Configuring WiFi is required for each new wireless remote access site.)
6. After a list of available WiFi networks displays, select **your named network** in the list.
7. Click the **Connect** button. The Connect window displays.
8. If prompted, enter the Wireless Security Password for your network, then click **OK**. If you entered the password correctly, your Wireless Adapter turns green. 

Note: There is a 10-minute window for you to establish a VPN connection. Once 10 minutes has elapsed, the Wireless Adapter will automatically disable. If the adapter disables, right-click the S.A.F.E icon, then select "enable wireless" and follow Steps 5–8 again.

Getting Started with Remote Access to the CMS Network

Connecting to SpectraGuard SAFE

The SpectraGuard SAFE client resides in the taskbar and displays as a white box with a shield in the middle.

The shield will be one of three colors – green, yellow, or red, representing the following levels of risk of intrusion:

- Green – low risk of intrusion.
- Yellow – medium risk of intrusion.
- Red – high risk of intrusion.

The SAFE client is location sensitive and operates in either "Work" or "Away" mode.

NOTE: It is not a requirement to open the SAFE console when connecting to VPN. This description is simply an explanation of what is happening in the background.

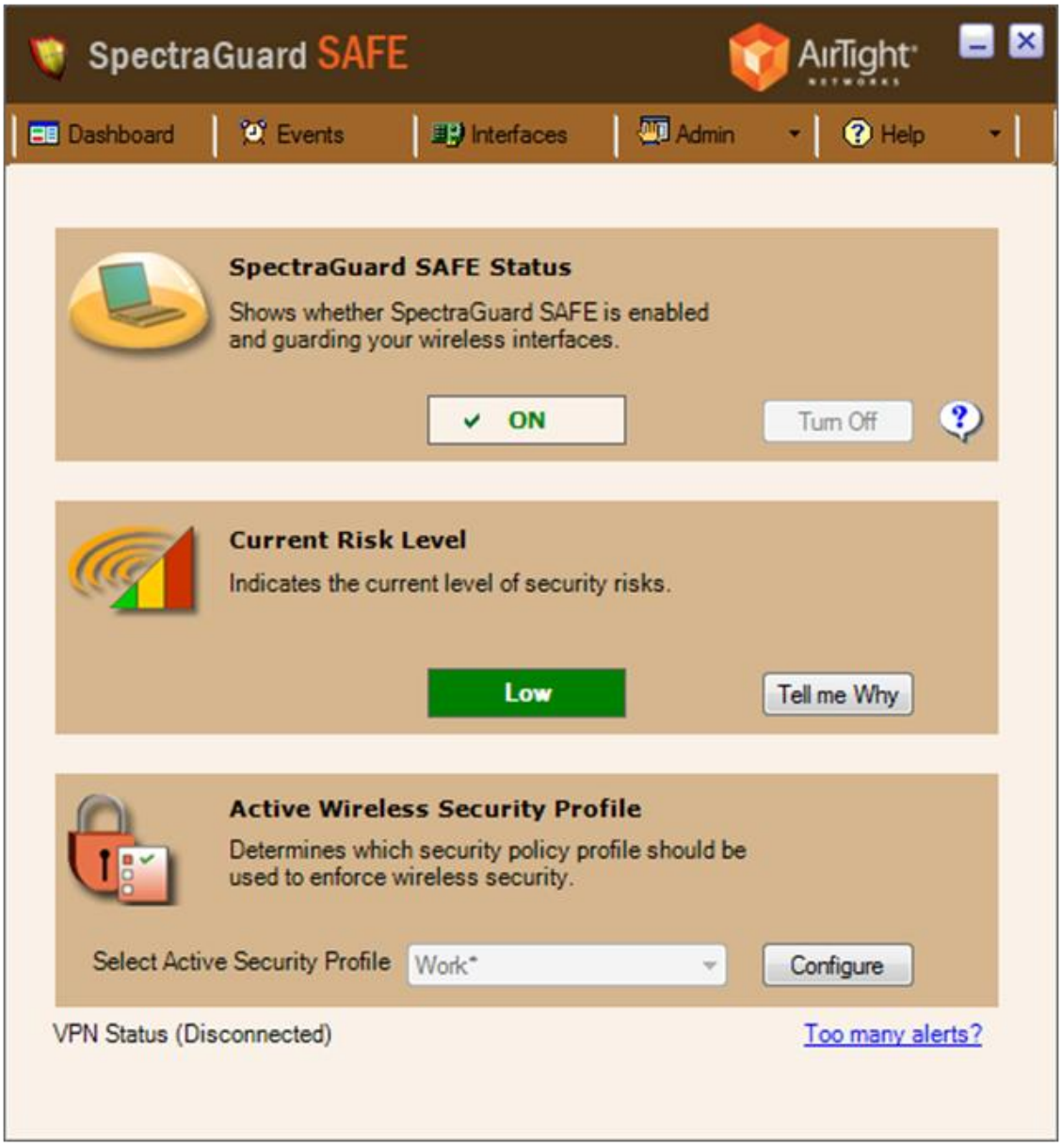
Figure 1 – SpectraGuard Icon in Task Bar

Getting Started with Remote Access to the CMS Network

Connecting to SpectraGuard SAFE in the Office

When connected at work using a docking station, the risk level is considered "Low," which also is indicated by a green shield icon in the taskbar. As depicted below, the Active security profile is automatically set to "Work."

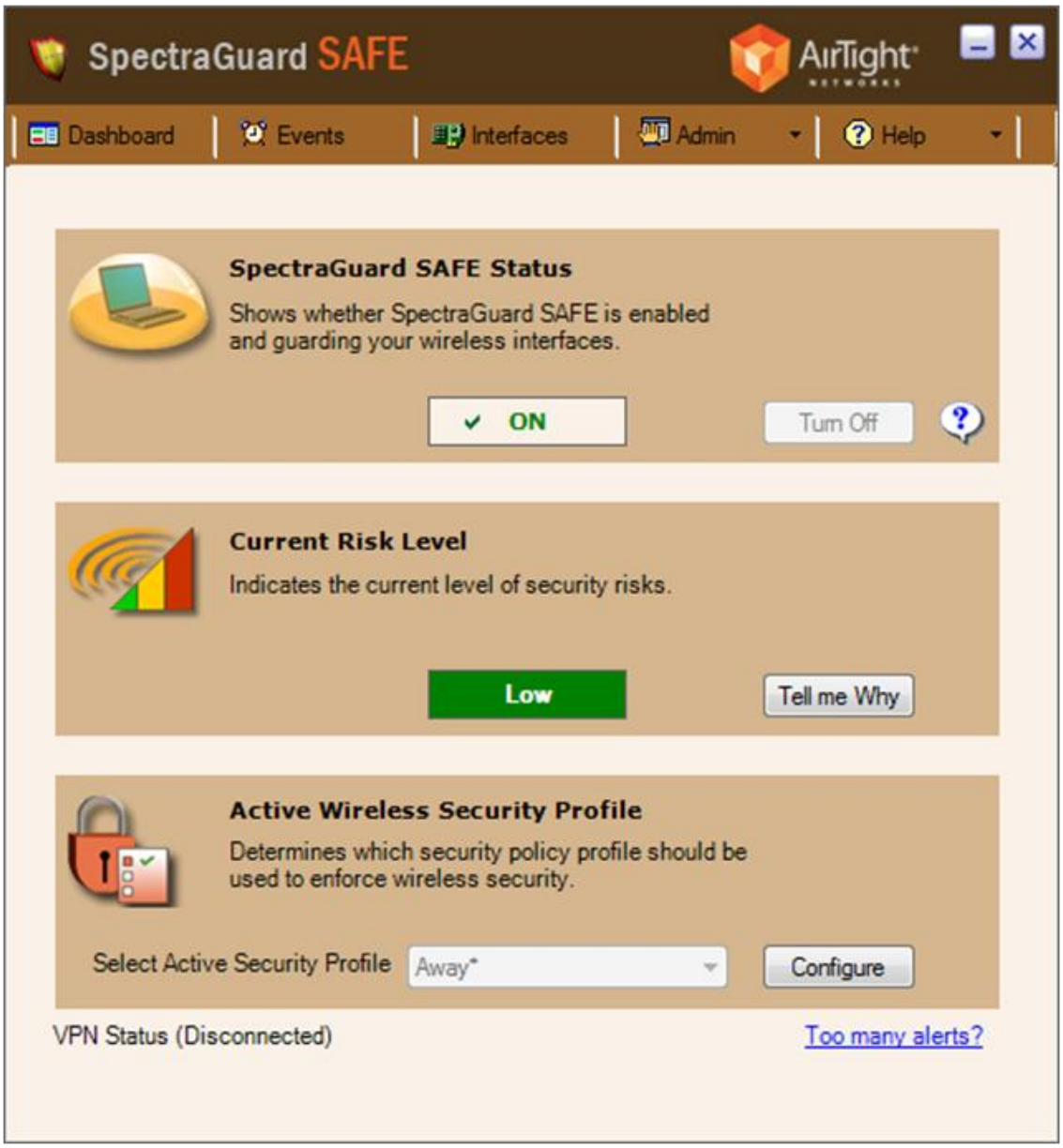
Figure 2 – SpectraGuard Console ("Work" Status)



Getting Started with Remote Access to the CMS Network

Once you are disconnected from the work network, your profile is automatically switched to "Away." In this profile, the risk still is considered low as long as you have not made a connection to any non-CMS networks.

Figure 3 – SpectraGuard Console ("Away" Status)

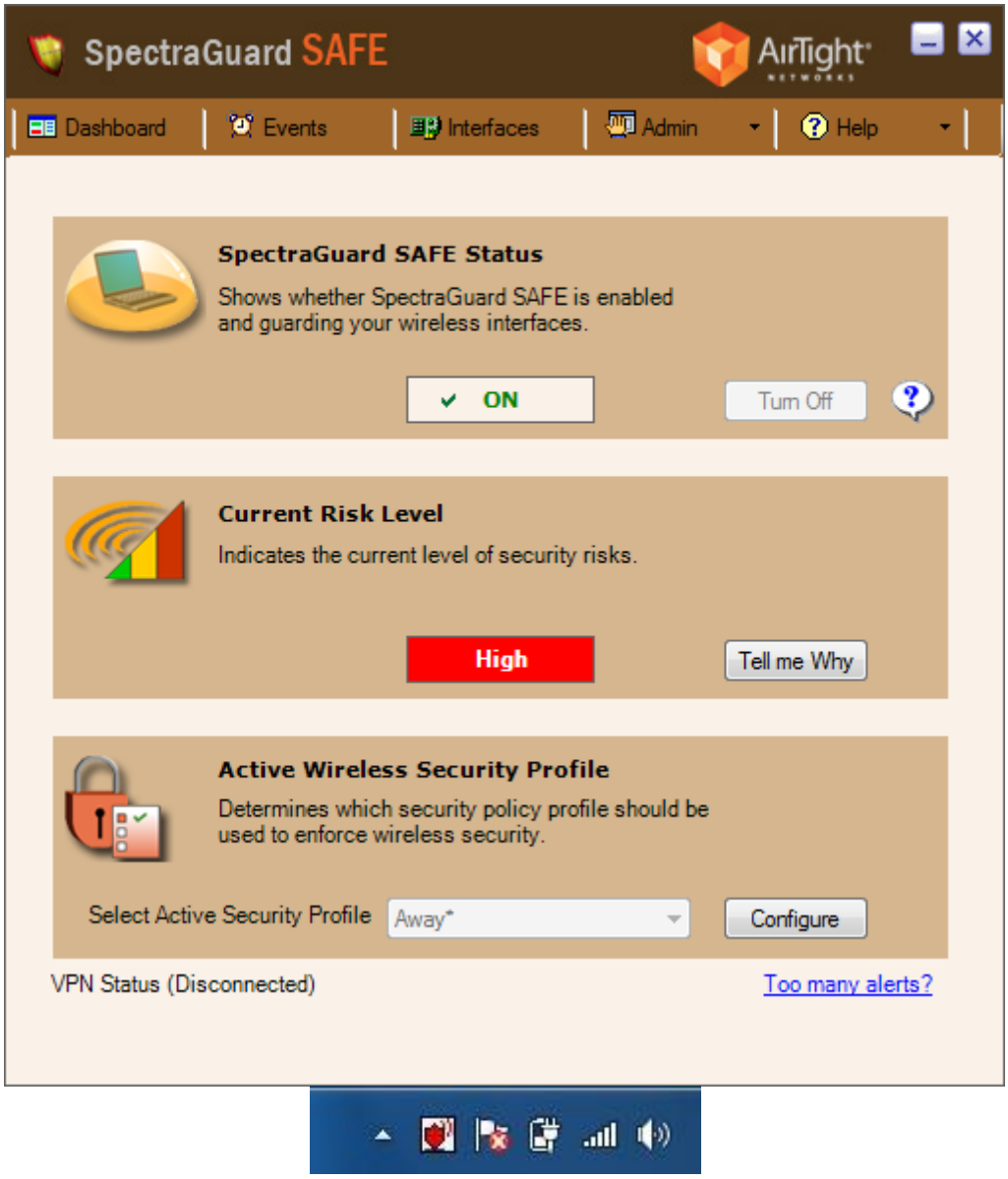


Getting Started with Remote Access to the CMS Network

Connecting to SpectraGuard SAFE via VPN

Once a connection is made to any non-CMS network, the risk level will be raised to "High," which also is reflected in the taskbar as a red shield.

Figure 4 – SpectraGuard Console (High Risk)

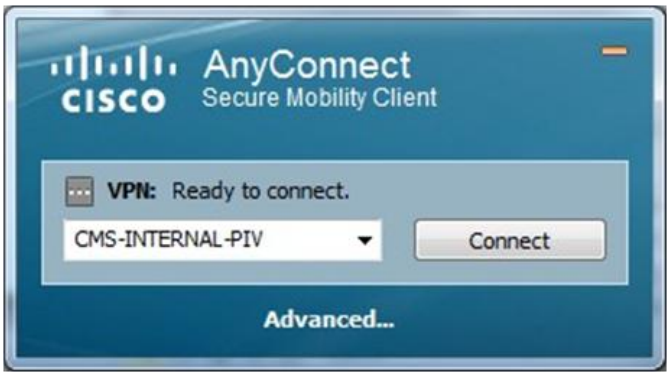


1. Upon connection to any non-CMS network, follow the prompt to establish a Virtual Private Network (VPN) connection within 10 minutes.

Figure 5 – VPN Connection 10-Minute Warning

2. Within this 10-minute window, open the Cisco AnyConnect VPN client, then establish a connection.

Figure 6 – AnyConnect Connection Prompt



3. If you do not complete the VPN login process before the 10-minute counter expires, your network interface will be disabled. If this happens, you will need to re-enable it:
    a. Right-click the **SAFE shield** in the taskbar. A popup menu displays.
    b. Select **Enable Wi-fi** or **Enable Interface** (depending on whether you are attempting a wireless or wired connection), as shown in Figure 7 on page 9.

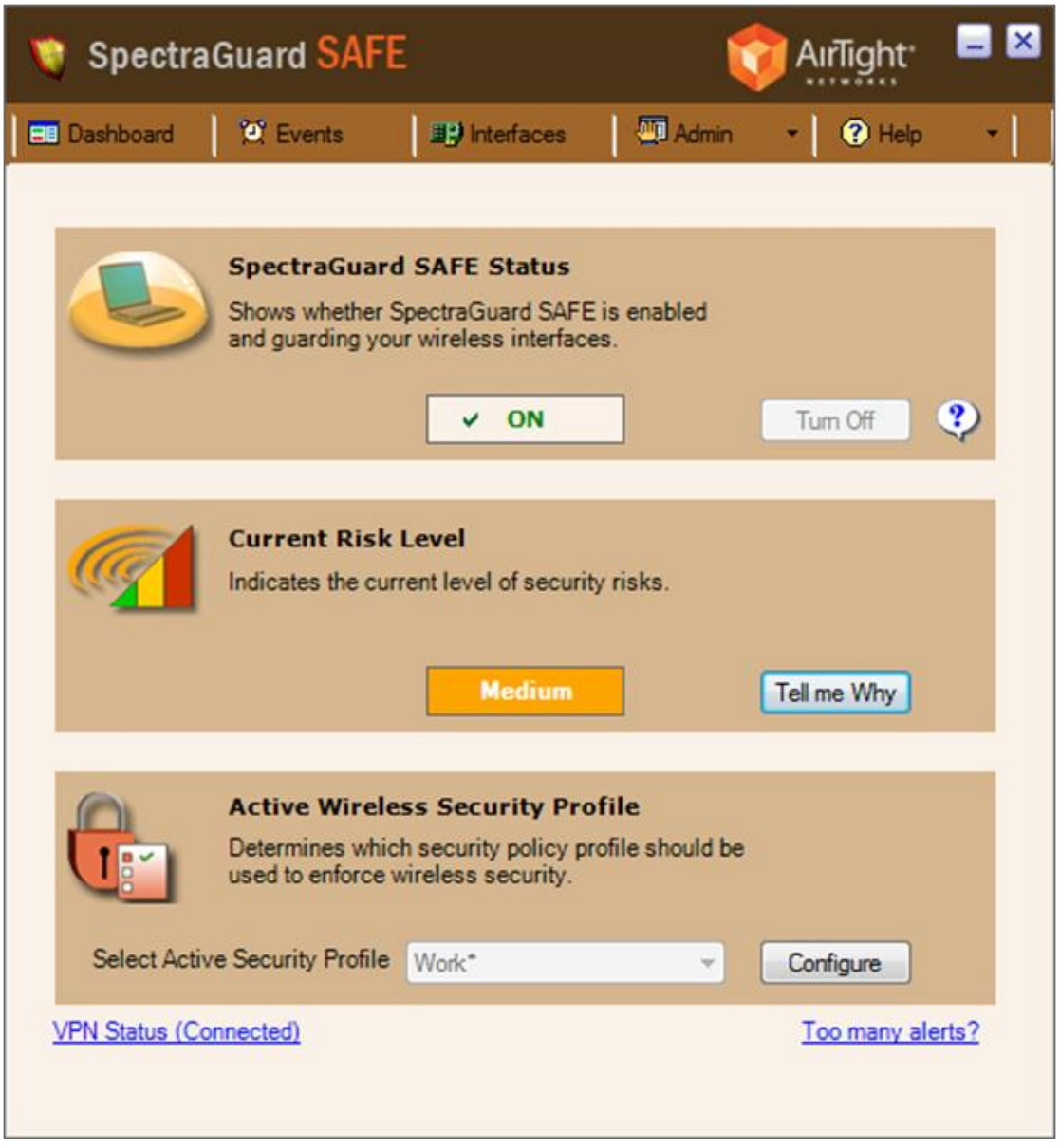
Figure 7 – Re-enable Connection menu

4. If you meet the security requirements for VPN, a "Full Network Access" confirmation page displays.

Figure 8 – VPN Connection confirmation page

The shield in your taskbar now is yellow, your risk level is set to "Medium," and you have full network access.

Figure 9 – SpectraGuard Console – VPN Access



Getting Started with Remote Access to the CMS Network

SpectraGuard SAFE Policies

Policies from SpectraGuard SAFE that are enforced on the CMS network are listed below.

- Block Wi-Fi completely? **No**
- Block connection to non-allowed APs? **Yes**
- Allow connection to non-allowed APs if firewall/anti-virus is running? **Yes**
- Allow connection to non-allowed APs if VPN tunnel is active? **Yes**
- Block communication below minimum Wi-Fi security? **No**
- Block ad hoc networks? **Yes**
- Block simultaneous connections? **Yes**
- Block bridging between network interfaces? **Yes**
- Block Ethernet connections? **Yes**
- Allow Ethernet connection if firewall/anti-virus is running? **Yes**
- Allow Ethernet connection if VPN tunnel is active? **Yes**
- Block Wireless 2.5G/3G (EV-DO, GPRS, CDMA, HSDPA, 3G modems)? **No**
- Block Bluetooth? **Yes**
- Block Infrared? **Yes**
- Block Firewire (1394)? **Yes**
- Block dial-up (phone) modems? Yes
- Allow dial-up (phone) modems if VPN tunnel is active? **No**
- Block WiMAX (WiBro, 802.16)? **No**
- Allow WiMAX (WiBro, 802.16) if firewall/anti-virus is running? **No**
- Allow WiMAX (WiBro, 802.16) if VPN tunnel is active? **No**
- Block external mass storage device? **No**
- Minimum security settings – **802.11i**
- Wait time for VPN tunnel to become active before applying Security Policies – **10 minutes**

Getting Started with Remote Access to the CMS Network

About Wireless Hotspots

Wireless hotspots often require that you accept a "terms and conditions" agreement before allowing connectivity to the Internet. Many providers will automatically redirect you to this agreement page as soon as you open Internet Explorer. If you are not automatically redirected, an error page displays; this error is normal, as your default homepage can be accessed only after the VPN tunnel has been created. You will need to manually type in the address of the agreement page if you are not redirected automatically. (This address will need to be provided by the hotspot provider.) After you have agreed to the provider's terms and conditions, you should be granted Internet access.

Checking your Network Connectivity

Network connectivity means that you have access to the Internet and can browse to **https://owa.hhs.gov**. If you cannot reach this site, you do not have connectivity, and the VPN connection will fail.

Once you have verified that you have Internet connectivity, proceed to the "Connecting to the VPN" section (see page 13). Select one of the VPN connectivity steps for using either your **PIV** card or an **RSA Token.**

Getting Started with Remote Access to the CMS Network

Connecting to the VPN

Once you have established network connectivity either through a wired or wireless connection, you are ready to access the CMS Network via the VPN. Remember that CMS network resources are not available until a VPN connection has been established. Connecting to the VPN is achieved by clicking the **Cisco AnyConnect** icon and using either your PIV card or RSA Token.

Using a PIV Card to Connect to the VPN

1. Insert and leave your PIV card in the card reader (located at the front left side of the CMS issued laptop).

2. Click the **Cisco AnyConnect Secure Mobility Client** icon located on the desktop.
3. From the Network drop-down field on the AnyConnect screen, select **CMS-Internal-PIV**.

4. Click **Connect**. The ActivClient Login window displays.
5. Type in your PIN (established when your PIV card was issued, which is composed of 6–8 digits), then click **OK**. The system displays a number of screens indicating progress while connecting to the network.
6. The Cisco NAC agent scans the system for patch updates before it connects you to the CMS network. If updates are required, you must install the updates, then reboot your system before continuing.
7. Once established, a notification window displays to confirm that you are successfully connected via the VPN.
8. Click the **VPN Drive Mappings** icon located on your desktop to map your network drives.

9. If you lose VPN or network connectivity, insert your PIV card again, then repeat steps 2–8.

Getting Started with Remote Access to the CMS Network

Using the RSA Token (fob) to Connect to the VPN

When you get your new laptop, you will be given an RSA SecureID Token.

Note: You will need to set up your 8-character PIN only the first time when you connect using the RSA Token.

First-time Login to the VPN with the RSA Token

1. Connect to the Network using either a wireless or wired connection. (See the "Remote Access via a Wired Connection" or "Remote Access via a Wireless Connection" instructions in the previous section.)
2. Once you have Internet connectivity, click the **Cisco AnyConnect Secure Mobility Client** icon located on the desktop. 

3. From the drop-down field that displays, select **CMS-Internal-Token**.

4. Click the **Connect** button.
5. Enter your alphanumeric CMS user ID and the 6-digit number displayed on your RSA Token, then click the **OK** button. (For more information, refer to "Your RSA Token" on page 17.)
6. In the Answer field, type a new 8-character alphanumeric PIN (which will contain exactly 8 characters, consisting of upper case letter, lower case letter, and numbers), then click the **Continue** button.
7. Again in the Answer field, re-type the PIN established in Step 6 above, then click the **Continue** button.
8. Wait for the 6-digit number displayed on the RSA Token to change, then enter the combination (no spaces) of the PIN followed by the 6-digit RSA Token number.
9. Click the **Continue** button.
10. The Cisco NAC agent scans the system for patch updates before it connects you to the CMS network. If updates are required, you must install the updates by following the prompt instructions, then reboot your system before continuing.

11. Once the "You are Successfully Logged in" message window displays, you are ready to work on the CMS network.
12. Click the **VPN Drive Mappings** icon located on your desktop to map your network drives.

Note: If a message window displays for the third consecutive time that requests your PIN once you have entered it incorrectly, your PIN account may be locked and would need to be reset. Please contact the CMS IT Service Desk for assistance at 410-786-2580 or 1-800-562-1963.

Subsequent Login to the VPN with the RSA Token

1. Connect to the Network using either a wireless or wired connection. (See the "Remote Access via a Wired Connection" or "Remote Access via a Wireless Connection" instructions in the previous section.)
2. Once you have Internet connectivity, click the **Cisco AnyConnect Secure Mobility Client** icon located on the desktop.

3. From the drop-down field that displays, select **CMS-Internal-Token**.

4. Click the **Connect** button.
5. In the Username field, enter your CMS user ID.
6. In the Passcode field, enter the combination (no spaces) of your PIN and the 6-digit number on the RSA token.
7. Click **OK**.
8. The Cisco NAC agent scans the system for patch updates before it connects you to the CMS network. If updates are required, you must install the updates by following the prompt instructions, then reboot your system before continuing.
9. Once you the "You are Successfully Logged in" message window displays, you are ready to work on the CMS network.
10. Click the **VPN Drive Mappings** icon on your desktop to map your network drives.

Getting Started with Remote Access to the CMS Network

Using the RSA USB Token to Connect to the VPN

Note: You will need to set up your PIN only the first time when you connect using the RSA Token.

1. Remove the cap from the end of the RSA Token (fob).
2. Insert the RSA Token into one of the USB slots on the laptop.
3. Click the **Cisco AnyConnect Secure Mobility Client** icon located on the desktop.

4. From the drop-down field that displays, select **CMS –Internal-Token**.

5. Click the **Connect** button.
6. Enter your alphanumeric CMS user ID and RSA Token PIN, then click the **OK** button. (For more information, refer to "Your RSA Token" on page 17.).
7. Wait for the Cisco NAC Agent window to display, which indicates if you are connected successfully to the Network to begin using CMS resources.
8. The Cisco NAC agent scans the system for patch updates and connects before it connects you to the CMS network. If updates are required, you must install the updates, then reboot your system before continuing.
9. Click the **VPN Drive Mappings** icon on your desktop to map your network drives.

Additional Information Concerning your Wireless Connection

When connecting via wireless, remember:

- ***You must make a VPN connection within 5 minutes of starting your computer***, or the wireless card will be disabled. (One reminder message displays before the card is disabled.)
- If the card is disabled, you may re-enable it by right-clicking the **S.A.F.E.** icon to display a popup menu, then click the **Enable** option, and click **Intel WiFi 5100 AGN (for the E6400) or the Intel Centrino Advanced N 6200 AGN (for the E6410)** RU ,QWHO &HQWULQR $GYDQFHG 1 **$*1 IRU WKH (.**

- ***You cannot establish simultaneous wired and wireless connections.*** If you plug into a wired connection (e.g., by connecting your laptop to the Ethernet connection at home or at work), the wireless card will be disabled.

Terminating your Remote Access Connection

1. In the System Tray on your desktop, right-click the **Cisco AnyConnect** icon  . A popup menu displays.
2. Click the **Disconnect** menu option. The VPN connection is terminated if you turn off your machine.
3. If you get disconnected while working, click the **VPN Client** icon again, then connect using your PIV Card or RSA Token.

Your RSA Token

Note: The RSA Token number resets every 60 seconds, and it will change when the countdown timer reaches zero bars. If the countdown is close to finishing, wait until the RSA Token number resets before you begin entering password information.

1. Choose a PIN with eight (8) characters. This PIN will always be a part of your VPN password. In the Response field, enter your PIN, then click **OK**.
2. In the Response field, re-enter your PIN, then click **OK**.
3. Wait until the RSA Token number resets at least once.
4. A g a i n i n the Response field, enter your PIN followed by the RSA Token number, then click **OK** to log in.

NAC Agent

The NAC Agent ensures that your laptop computer is protected and up-to-date when you log into the VPN. If the NAC Agent detects no problems, click **OK** to begin working.

To update your laptop:

You will be notified about all of the components that need to be updated.

1. In the Cisco NAC Agent window, click the **Continue** button.
2. Click **Update** to update your system. (Some updates may require you to restart your computer.)