

ONE[®] Network

Installing Check Point SecuRemote Client for Windows

Document Identifier: 00041

Version: 5.0

Copyright Notice

This document is copyright of eHealth Ontario (eHO).

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHO. The information contained in this document is proprietary to eHO and may not be used or disclosed except as expressly authorized in writing by eHO.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Revision History:

Date	Version	Revision
Apr 2008	5.0	Update for Microsoft Vista support
Sep 2007	4.0	Removal of xWAVE email address
Dec 2005	3.0	Re-branded to ONE Network Release
Sep 2005	2.0	Updated Release
Dec 2004	1.0	Initial Release

Authorized Reader

This document is authorized to the following organizational roles:

Role(s)
<ul style="list-style-type: none">Physicians
<ul style="list-style-type: none">LAN installer
<ul style="list-style-type: none">Other Healthcare providers

Table of Contents

1.0	About this Document.....	5
1.1	Document Approach and Scope.....	5
1.2	Audience.....	5
1.3	Reference Material.....	5
2.0	Read Me First.....	6
3.0	General Overview of the ONE Network Design	7
4.0	Important Notes	9
4.1	Help Desk	9
4.2	Installation Check Point VPN-1 SecuRemote Client	9
	<i>4.2.1 Operating Systems.....</i>	<i>9</i>
	<i>4.2.2 The SOFA IP Address for your Site.....</i>	<i>9</i>
	<i>4.2.3 The SOFA IP Address of another Site within your ONE Network Group.....</i>	<i>9</i>
	<i>4.2.4 Connecting to Your Office.....</i>	<i>9</i>
	<i>4.2.5 Connecting to Another Office.....</i>	<i>9</i>
	<i>4.2.6 Moving to a New Office.....</i>	<i>10</i>
	<i>4.2.7 Obtaining a User ID and Password.....</i>	<i>10</i>
	<i>4.2.8 Forgotten User ID and/or Password.....</i>	<i>10</i>
	<i>4.2.9 Adding an Additional Account.....</i>	<i>10</i>
	<i>4.2.10 Deleting an Account from your Site.....</i>	<i>10</i>
	<i>4.2.11 Password Change.....</i>	<i>11</i>
5.0	Uninstall Check Point VPN-1 SecuRemote	12
5.1	Save and Close Documents.....	12
5.2	Open the Control Panel	12
5.3	Confirm Deletion.....	13
5.4	Reboot your System	14
6.0	CP Clean Utility	15
6.1	Save and Close Documents.....	15
6.2	Download the Clean Utility	15
6.3	Launch the Executable	16
6.4	Delete the Directories, Files and Registry Keys.....	17
6.5	Reboot your System	20

7.0	Install the New Check Point VPN-1 SecuRemote Client	21
7.1	Save and Close Documents.....	21
7.2	Gather Information.....	21
7.3	Download the Secure Client.....	21
7.4	Launch the Executable	22
7.5	Reboot your System	25
7.6	Connect to Check Point VPN-1 SecuRemote.....	26
7.7	Create a New Site	26
7.8	Enter the Username and Password.....	27
7.9	Communication Error	30
7.10	Successful Connection.....	30
8.0	Connection to your Site	31
8.1	Successful Connection.....	32
8.2	Communication Error	32
8.3	Disconnecting your Check Point SecuRemote VPN-1 Session	32
9.0	Clean your Desktop	34
	Appendix A – Glossary	35

Table of Tables

N/A

Table of Figures

N/A

1.0 About this Document

1.1 *Document Approach and Scope*

This document provides instructions on how to perform the following tasks:

- Remove **Check Point *SecuRemote*** software currently installed on your system.
- Install **Check Point SecuRemote Client** application for **Windows Vista**

Check Point SecuRemote Client will throughout this document be simply referred to as SecuRemote Client.

1.2 *Audience*

This document is intended for eHO Clients authorized to install the Check Point SecuRemote Client application on their office or home computer(s).

1.3 *Reference Material*

- *ONE Network Remote – What You Need To Know – Document ID: 00731*
- *Using Check Point SecuRemote Client for Windows – Document ID: 00041*

2.0 Read Me First

Check Point SecuRemote Client can be installed on any Windows Vista workstation, and because it is backward compatible, it can also be used on earlier versions of Microsoft Windows Operating Systems, e.g. 2000, NT or XP. This application will allow you to access to your office network from a remote location.

Triggers	<ul style="list-style-type: none"> ▪ Requirement to connect remotely to your office network or any office within your ONE Network group.
Inputs (Requirements)	<ul style="list-style-type: none"> ▪ The ONE Network account letter containing your: <ul style="list-style-type: none"> – Username and Password – Small Office Firewall Appliance (SOFA) ONE Network IP Address – Hub site’s SOFA ONE Network IP Address (optional)
Outputs (Deliverables)	<ul style="list-style-type: none"> ▪ A configured workstation enabling you to connect remotely to your office network or any office within your ONE Network group (depending on the access you have been authorized for).
Estimated Time to Completion	<ul style="list-style-type: none"> ▪ The installation process for SecuRemote Client software will take approximately 30 minutes.
Tools	<ul style="list-style-type: none"> ▪ Access to the Internet. ▪ Administrative rights to your system.
Competencies	<ul style="list-style-type: none"> ▪ Basic computer skills.

3.0 General Overview of the ONE Network Design

A ONE Network Group within the Ontario MD association consists of one **Hub site** with none, one, or more **Spoke sites** connected with IPsec VPN tunnels.

Sites

The **Hub Site** is typically the central location housing shared group applications such as the Clinical Management System (CMS) application which gathers administrative, billing and clinical information such as patient medication history, allergies and laboratory results.

The **Spoke Site** refers to another office within a ONE Network group that requires access to the **Hub site**.

Note: Each **Hub** and each **Spoke** resides on its own ONE Network circuit.

A **Hub** is distinguished from a **Spoke**, by the Managed Service Unit ID (MSUID). The **Hub** MSUID ends in **Hxxe**, the **Spoke** MSUID ends in **Sxxe**, e.g. **H01e** or **S02e**.

Contacts

Each site will have a **Primary Contact** (typically a physician) and a **Backup Contact**. Both are referred to throughout this document as the **Primary Contact**. They are responsible for maintaining the ONE Network accounts for the staff and vendors at their medical location and will have been listed on the *ONE Network Order Form*.

Accounts

To receive ONE Network remote access account(s) the Primary Contact must complete and sign a *ONE Network Remote Order Form* indicating the number of accounts required. The following three (3) ONE Network account configurations are available:

1. **Staff Accounts** are for medical location staff needing remote access to a Hub site and/or their own Spoke site. Note: If the staff's office is at the Hub site, their remote access is limited to the Hub site only.
 - If your site is a CMS Local Configuration 1 or 3, the staff account will provide access to your practice location.
 - If your site is a CMS Local Configuration 2 Hub Site, the staff account will provide access to your medical practice location ONLY
 - If your site is a CMS Local Configuration 2 Spoke Site, the staff account will provide access to your medical practice location AND the hub location
2. **Group Accounts** can only be requested by a CMS configuration 2 hub site.

- This account allows the user to gain access to the hub site and all the spokes associated with the ONE Network Group. This account is typically required for CMS vendors and/or any users who require access to all locations.

3. **Vendor Accounts** are provided to vendors only (referred to as a site account).

- If your site is a CMS Local Configuration 1 or 3, the vendor account will provide access to the practice location.
- If your site is a CMS Local Configuration 2 Hub Site, the vendor account will provide access to the medical practice location ONLY.
- If your site is a CMS Local Configuration 2 Spoke Site, the vendor account will provide access to the medical practice location ONLY.

There is no limit to the number of accounts that can be requested for a site or a ONE Network Group. However, there is a limit of 10 concurrent connections allowed and the maintenance of these accounts is the responsibility of the physician who orders them.

Account Changes

There are only three (3) types of ONE Network account changes that can be requested for an existing account: Add, Delete, and Password Reset.

1. An **Add** is used to allow a user access to additional spoke sites within a ONE Network Group. A *ONE Network Remote Change Form* must be completed and signed by the Primary Contact at the spoke site requesting access. In order to complete the Change Form, the Primary Contact at the new office will require the user's existing User ID and the MSUID (if available, otherwise, the address of the first location).
2. A **Delete** removes an existing account. Only the Primary Contact can remove a user from a site and this is completed by contacting your Help Desk. If the Primary Contact is the Hub Contact (physician) and the account being deleted is a hub and all spokes account he/she can approve the deletions of all sites.
3. A **Password Reset** simply changes the password. This too is facilitated by contacting your Help Desk.

If a staff member moves within the ONE Network Group or to another Group the move will be treated as an **Add** and a **Delete**. Consequently, they will receive a new account for the new location.

4.0 Important Notes

4.1 *Help Desk*

If you experience a technical issue when installing or using your Check Point VPN-1 SecuRemote Client, please contact your Help Desk.

4.2 *Installation Check Point VPN-1 SecuRemote Client*

4.2.1 Operating Systems

The SecuRemote Client application is designed for workstations currently using Windows Vista Operating System. However, it is backward compatible and can be used on earlier versions of Microsoft Windows 2000, NT and XP Operating Systems.

4.2.2 The SOFA IP Address for your Site

The SOFA IP address for your location is included in the letter containing your ONE Network User ID and password.

If the SOFA IP address cannot be located, the Primary Contact should contact your Help Desk for support, who in turn will contact eHO. eHO will fax the SOFA IP address to your medical location. The turnaround time for this process is one business day.

4.2.3 The SOFA IP Address of another Site within your ONE Network Group

The SOFA WAN IP addresses for each site within the ONE Network group can be obtained from the Primary Contact for that medical location.

4.2.4 Connecting to Your Office

The SecuRemote Client download process can begin once the end user has received their letter containing:

- Username
- Password
- SOFA IP address

4.2.5 Connecting to Another Office

Once the end user has received his/her User ID for their main office, the Primary Contact at a second office within that ONE Network Group may complete and sign the **ONE**

Network Remote Change Form. To complete this form, the Primary Contact needs to know the individual's **User ID** and the **MSUID** for their current office. The completed form will initiate the user's ONE Network access to the second site.

The information required to connect to the second location arrives in a letter marked **Private and Confidential**, addressed to the Primary Contact of the new medical location. The turnaround time for this process is three (3) business days once eHO has received the completed form, plus any additional time taken by the courier.

Note: User IDs and passwords are unique to a ONE Network Group. If access is required to sites outside the ONE Network Group it is considered a new order.

4.2.6 Moving to a New Office

If a user moves to a new medical office outside their current ONE Network group, a new User ID and password are required to access the location. This is considered a new order.

4.2.7 Obtaining a User ID and Password

ONE Network Remote User IDs and passwords are sent to the Primary Contact in a letter marked **Private and Confidential** via a Courier. If the Primary Contact does not receive the account information within seven (7) business days of eHO receiving the order, the Primary Contact should call their Help Desk to initiate an investigation.

4.2.8 Forgotten User ID and/or Password

If you forget your User ID and/or password, please contact the Primary Contact at your medical facility.

4.2.9 Adding an Additional Account

To add additional account(s) the Primary Contact at the medical location completes and signs a **ONE Network Remote Order Form** and sends the completed form to:

Fax: 416-586-4397

Email: servicedesk@ehealthontario.on.ca

4.2.10 Deleting an Account from your Site

To delete an account the Primary Contact at the medical location must contact their Help Desk who in turn contacts eHO. The ONE Network account User ID and password are disabled within four (4) business hours of eHO being notified.

Note:

1. Only the Primary Contact can remove a user from a site. If the Primary Contact is the Hub Contact and the account being deleted is a **hub and all spokes** account he/she can approve the deletions of all sites.
2. A Primary Contact can request that the Back-up Contact be deleted and vice versa.

4.2.11 Password Change

If a password must be changed, the Primary Contact at the site should contact their Help Desk who in turn contacts eHO. A new password addressed to the Primary Contact arrives in a letter marked **Private and Confidential** within three business days of eHO receiving the request and any additional time taken by the Courier service.

5.0 Uninstall Check Point VPN–1 SecuRemote

The following steps in this section are to be completed **ONLY** if you currently have a version of Check Point VPN–1 SecuRemote Client on your system. If you have any concerns regarding the removal of your current version of SecuRemote, please contact your Help Desk.

1. If you do not have a version of **Check Point VPN–1 SecuRemote Client** on your computer, proceed to section **7.0 Install the Check Point VPN–1 SecuRemote Client**.

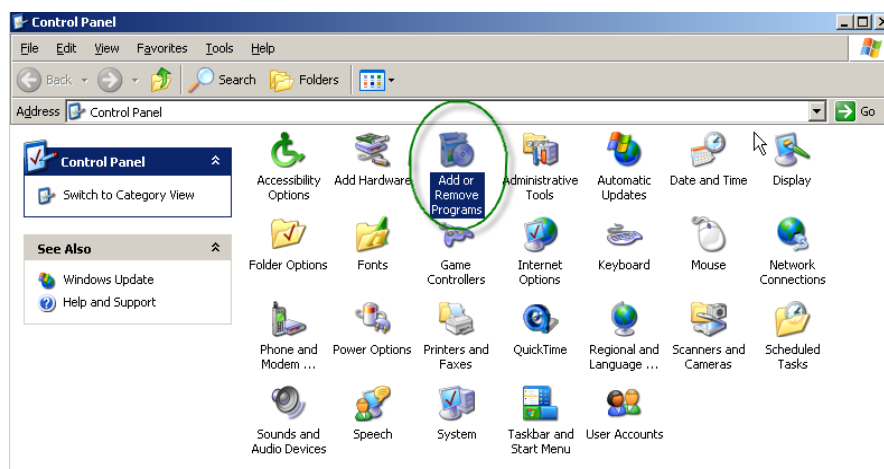
Note: Should you choose to run other VPN clients along with the Check Point VPN_1 SecuRemote, there could be implications such as restricted access to other clients or resources. eHO supports only a single instance of remote software, the version identified in this document.

5.1 Save and Close Documents

Before you start this procedure, please save and close all documents that are open on your desktop.

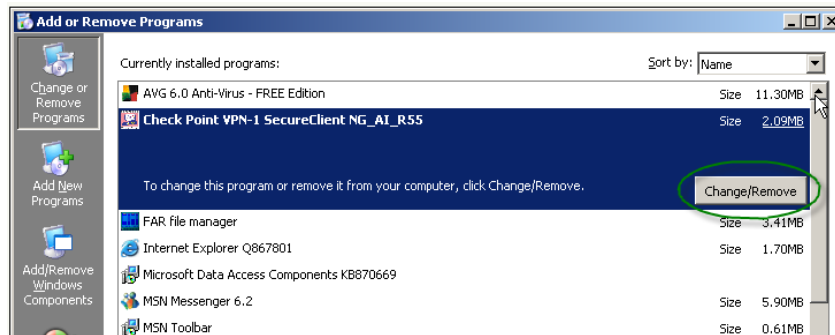
5.2 Open the Control Panel

1. From your Desktop, select Start, then Settings, then Control Panel.
2. In the **Control Panel**, select **Add or Remove Programs**.



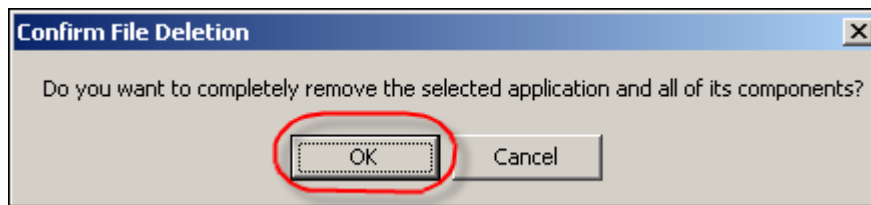
3. From the list, highlight the **Check Point VPN-1 SecureClient** application. Click **Change/Remove**.

Note: If the Check Point SecureClient software is not displayed in the list, proceed to section 7.0 *Install the New ONE Network Client*.

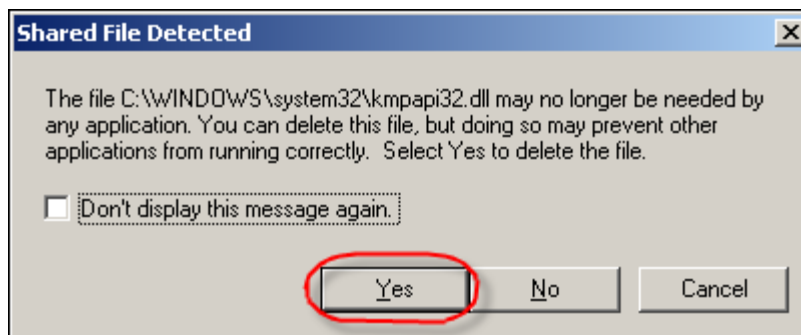


5.3 Confirm Deletion

1. In the **Confirm File Deletion** dialog box, click **OK** to confirm deletion.

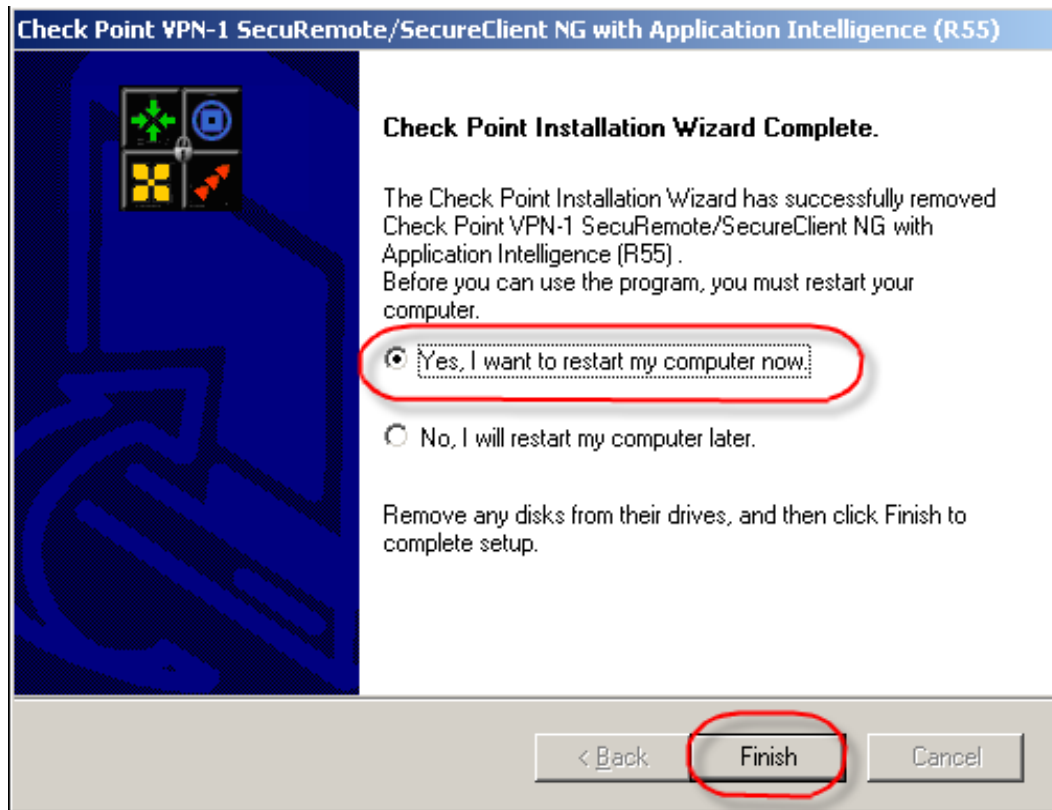


2. If the **Shared File Detected** dialog box appears, click **Yes** to delete shared files.



5.4 Reboot your System

1. A **Completion** dialog box appears. Check “Yes, I want to restart my computer now.” Click **Finish**.



2. After your system reboots, proceed to Section **6.0 CP Clean Utility**, below.

6.0 CP Clean Utility

The steps in this section are to be completed **ONLY** if you have completed section **5.0 *Uninstall Check Point VPN-1 Secure Remote.***

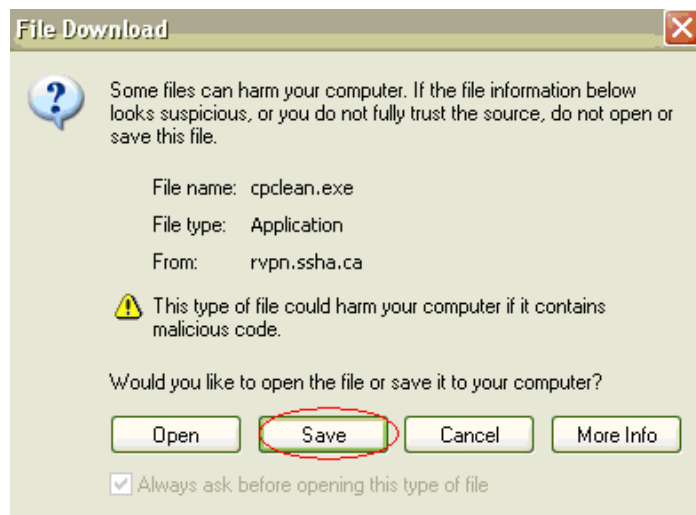
If you did not have a version of Check Point Secure Remote on your system, proceed to section **7.0 *Install the Check Point VPN-1 SecRemote Client.***

6.1 *Save and Close Documents*

Before beginning this section, save and close all documents open on your **Desktop**.

6.2 *Download the Clean Utility*

1. Hold down the CTRL + click to follow the link below to the Download Page:
<http://www.ehealthontario.on.ca/downloads>
2. Select the CP Clean Utility from the list of downloadable programs.
3. Click on Save and choose your desktop to save the file.



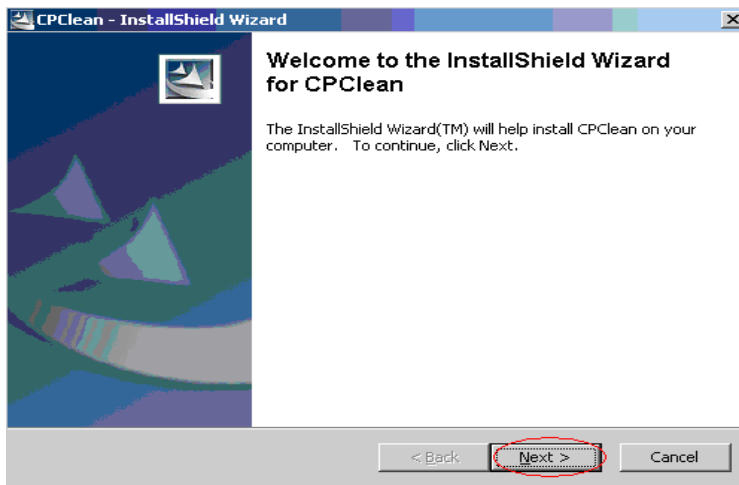
4. When the **File Download** dialog box states the download is complete, click **Close**.
5. Close the **Browser** window to return to your **Desktop**.

6.3 Launch the Executable

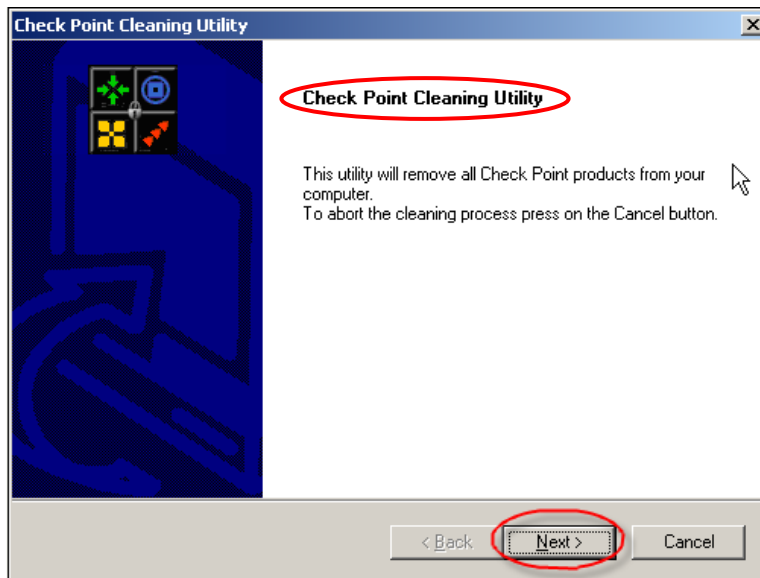
1. From your Desktop, double-click the **cpclean.exe** icon.



2. In the **Welcome** dialog box, click **Next**.

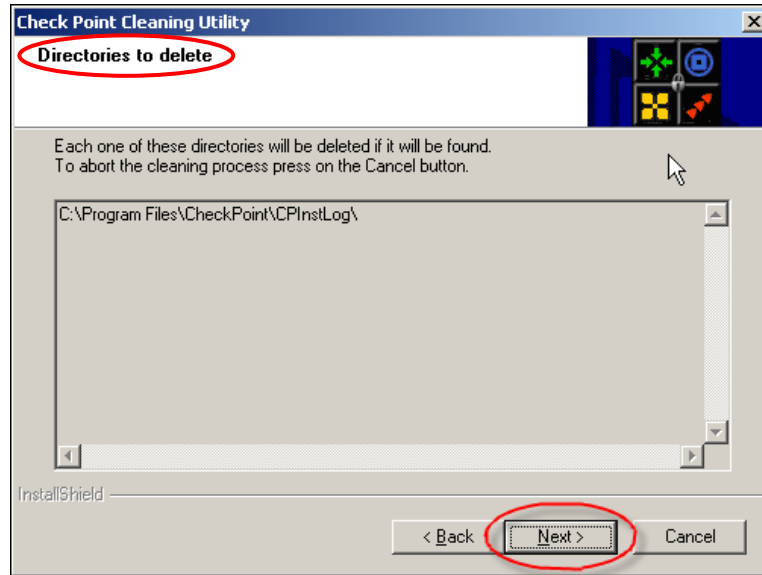


3. In the Check Point Cleaning Utility dialog box, click Next.

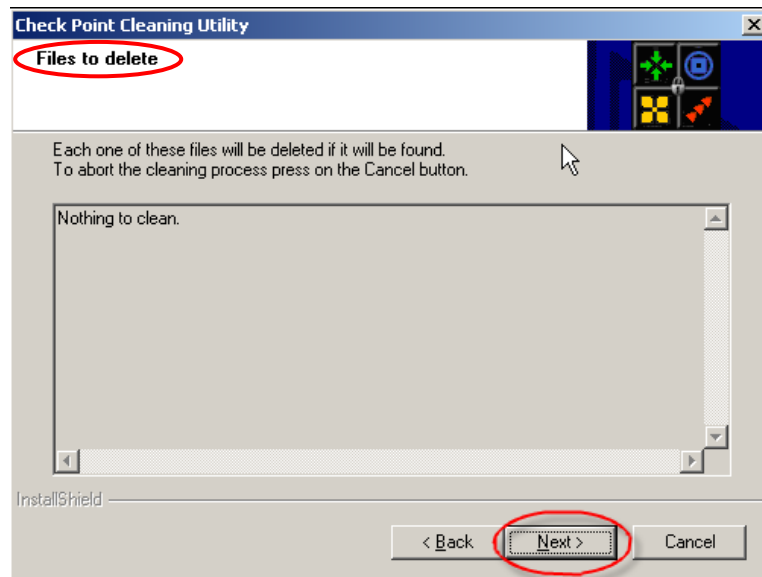


6.4 Delete the Directories, Files and Registry Keys

1. In the **Directories to Delete** dialog box, click **Next**.

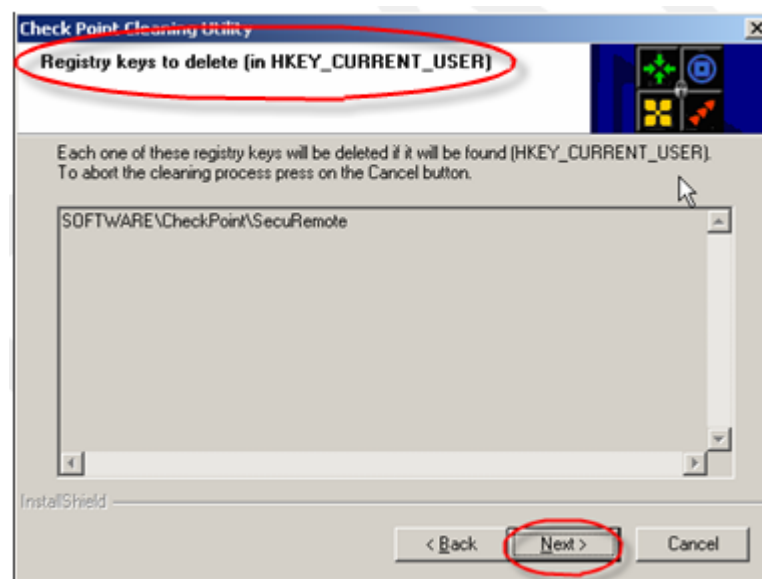
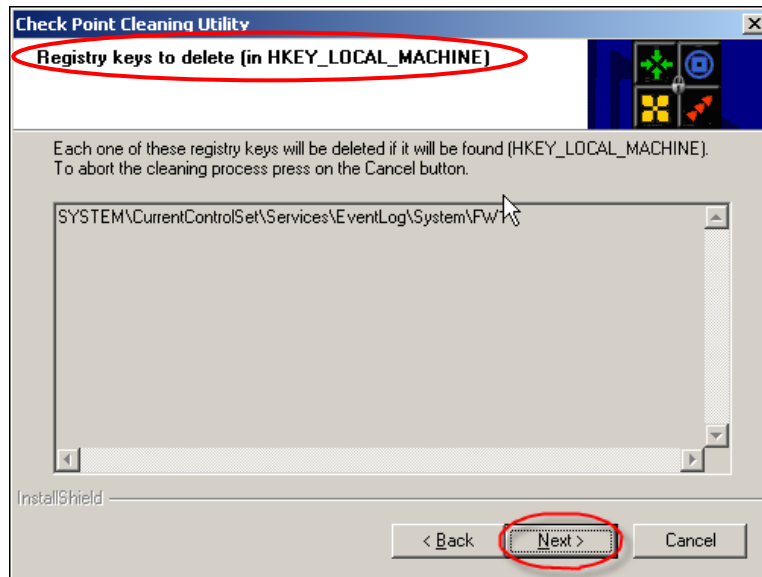


2. In the **Files to Delete** dialog box, click **Next**.

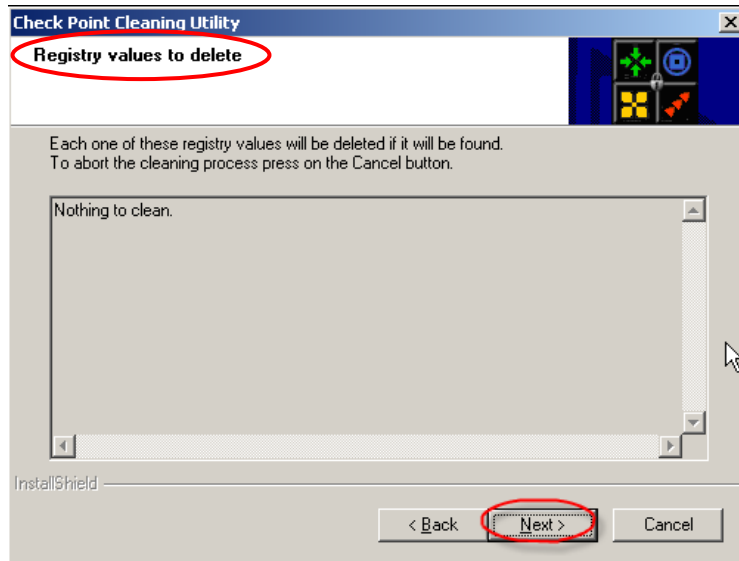


3. In the **Registry Keys to Delete** dialog box, click **Next**.

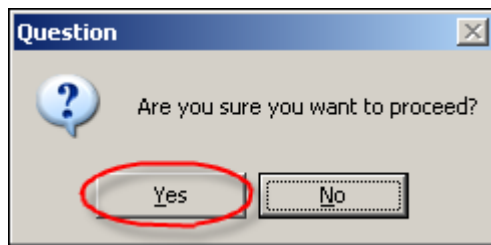
Note: As there could be more than one key to be deleted, you might be presented with more than one dialog box.



4. In the **Registry Values to Delete** dialog box, click **Next** to delete registry values.

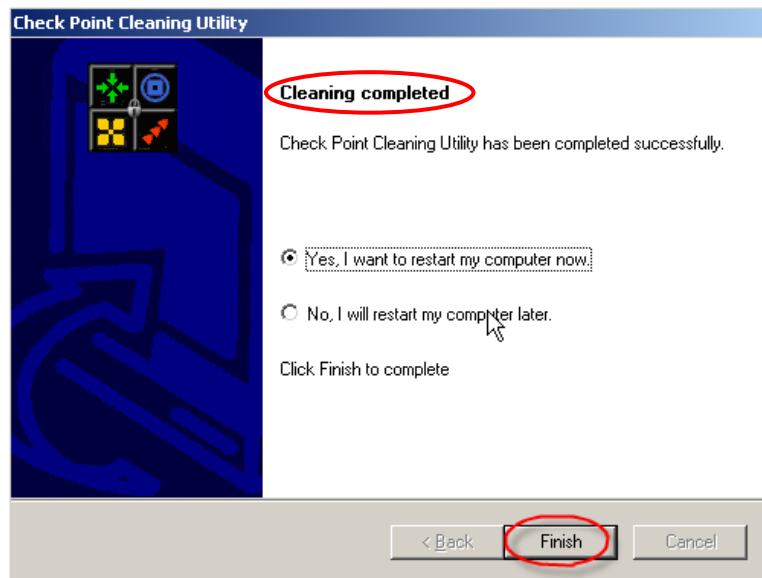


5. Click **Yes** to confirm the deletions.



6.5 Reboot your System

1. A **Cleaning Completed** dialog box appears. Check “**Yes, I want to restart my computer now**”. Click **Finish**.



2. After your system reboots, proceed to section 7.0 *Install the Check Point VPN-1 SecuRemote Client*, below.

7.0 Install the New Check Point VPN-1 SecuRemote Client

7.1 *Save and Close Documents*

Before beginning this section, save and close all documents open on your **Desktop**.

7.2 *Gather Information*

Gather the **ONE Network account letter** containing the following information:

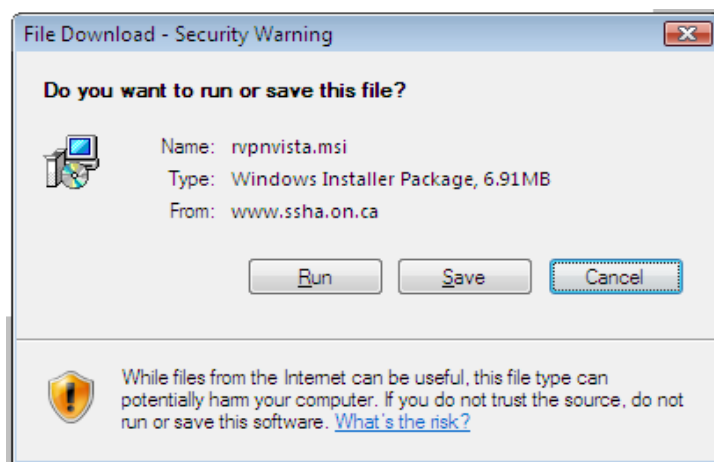
- Username and Password
- SOFA ONE Network IP address for your office
- SOFA IP addresses of any other sites within your ONE Network group that connection is required (optional).

7.3 *Download the Secure Client*

1. Hold down the CTRL + click to follow the link below to the Download Page:

<http://www.ehealthontario.on.ca/downloads>

2. Select the software client to suite your operating system.
3. In the **File Download** dialog box, click **Save**.



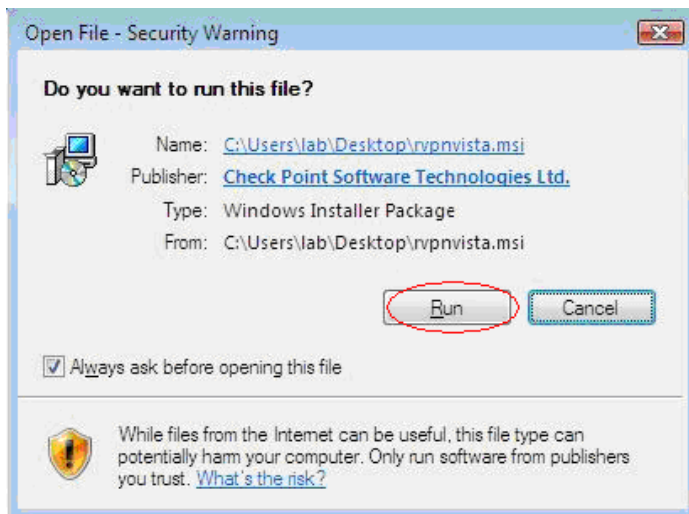
4. Save the file to your **Desktop**, using the filename provided.
5. When the **File Download** dialog box states the download is complete, click **Close**.
6. Close the Browser window to return to your **Desktop**.

7.4 Launch the Executable

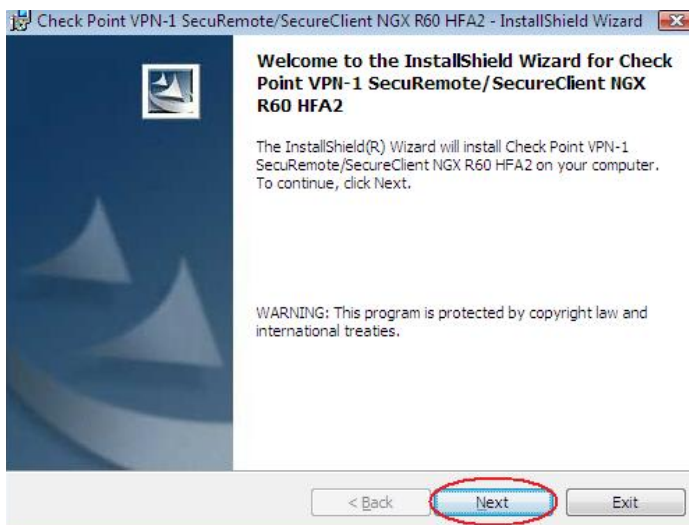
1. On your **Desktop**, double-click the **rvpnvista** icon.



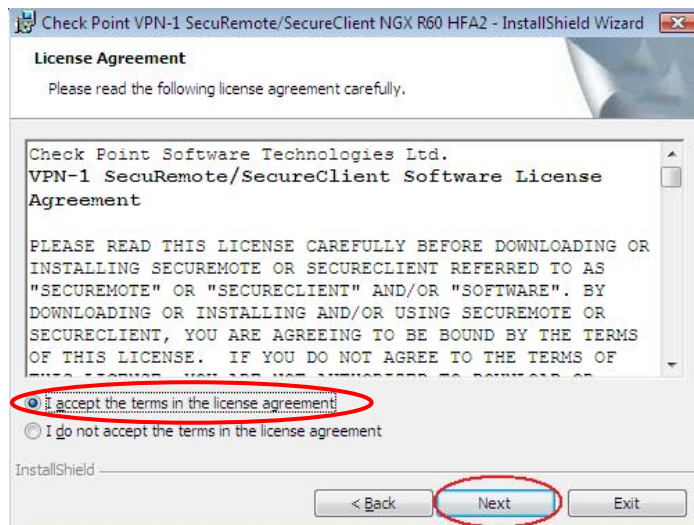
2. Click **Run**.



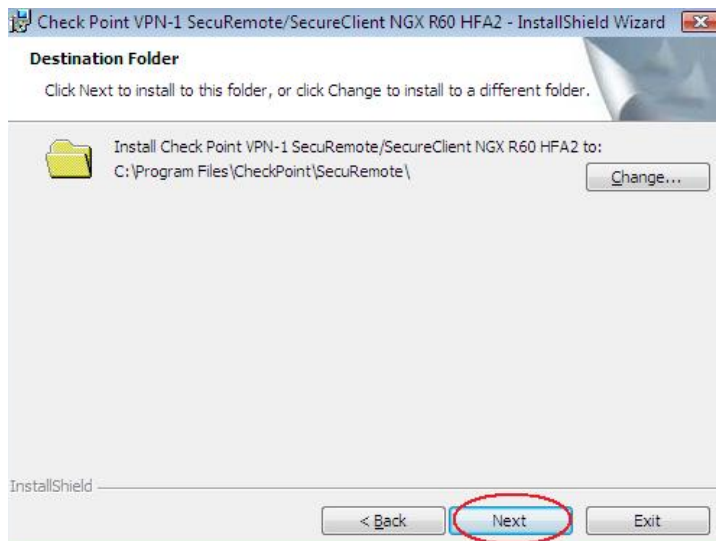
3. Click **Next** on the Welcome Screen



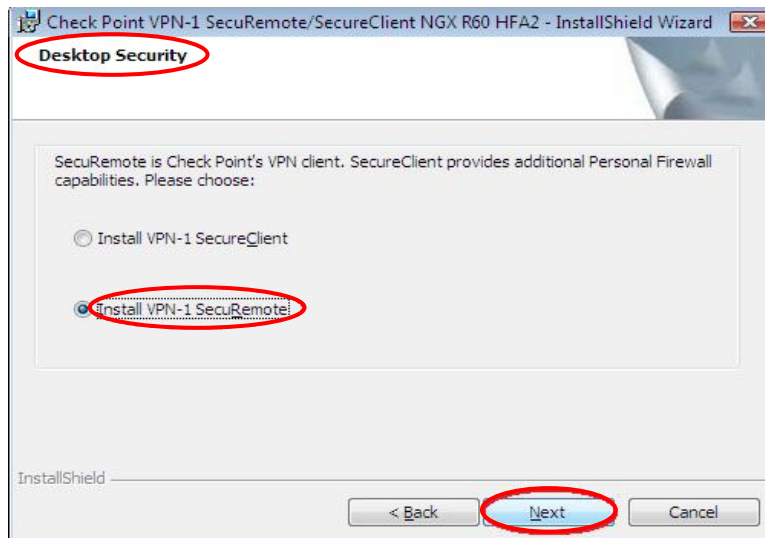
4. In the **License Agreement** dialog box, check the box “I accept the terms in the license agreement”. Then click **Next**



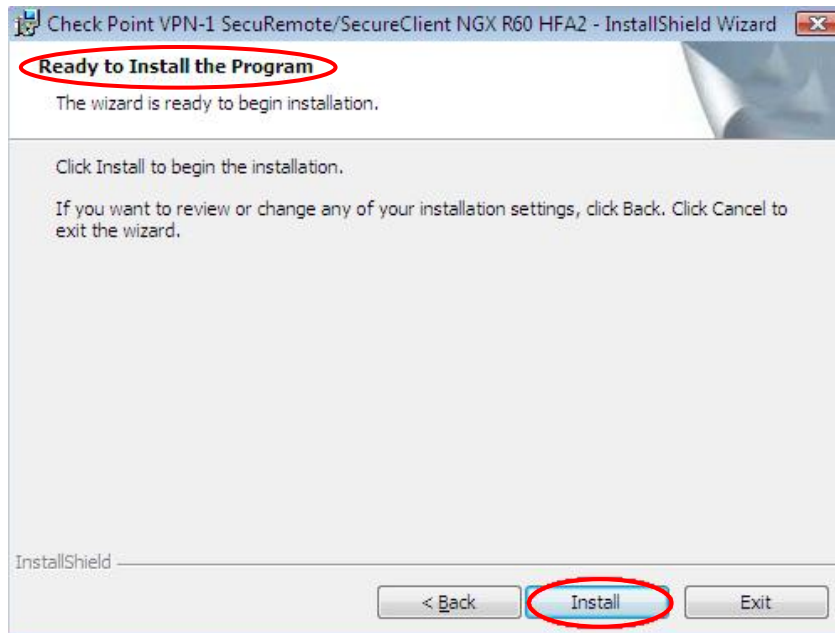
5. In the **Destination Location** dialog box, the **Destination Folder** is automatically supplied. Click **Next** to accept the default.



6. In the **Desktop Security** dialog box, ensure **Install VPN-1 SecuRemote** is selected. Click **Next**.

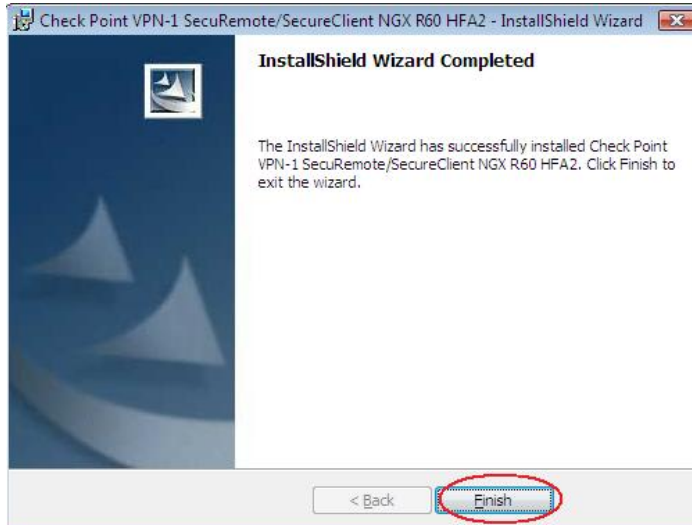


7. In the **Ready to Install the Program** box, click **Install**.

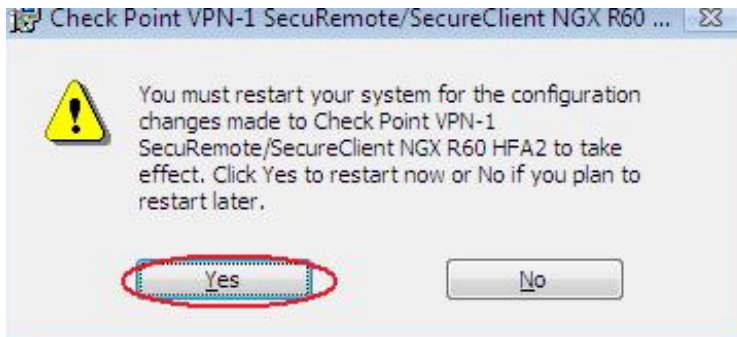


7.5 Reboot your System

8. Click **Finish**.



9. Click **"Yes"**, to restart your computer now.

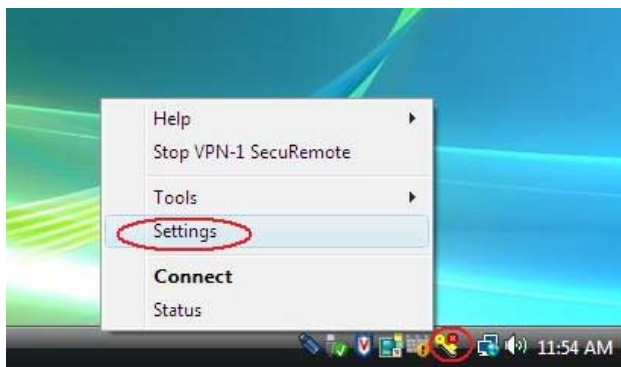


7.6 Connect to Check Point VPN-1 SecuRemote

1. After your system reboots, ensure you are connected to the **Internet**.
2. On the **Desktop** task bar, in the bottom right corner of your screen, locate the **SecuRemote** icon.

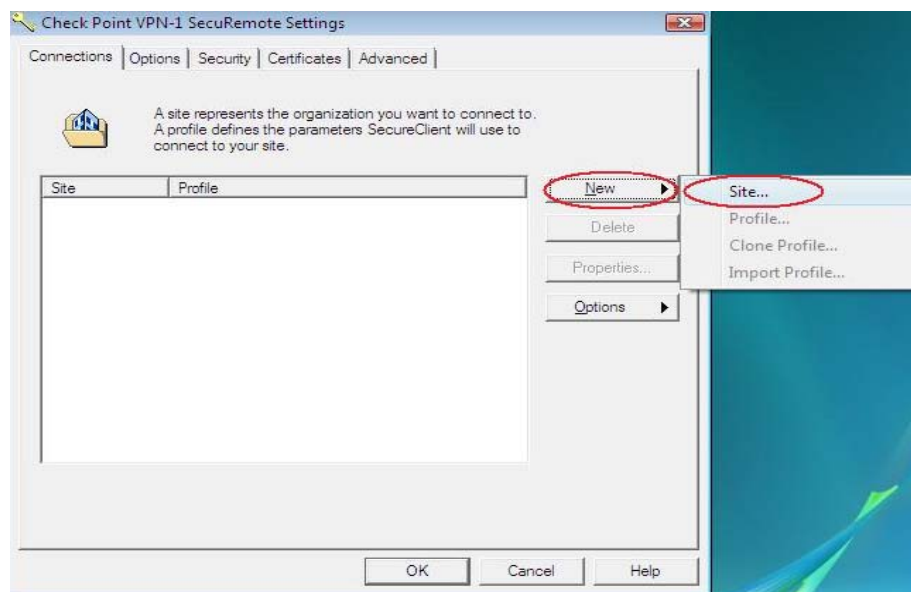


3. Click the **SecuRemote** icon and select **Settings**.



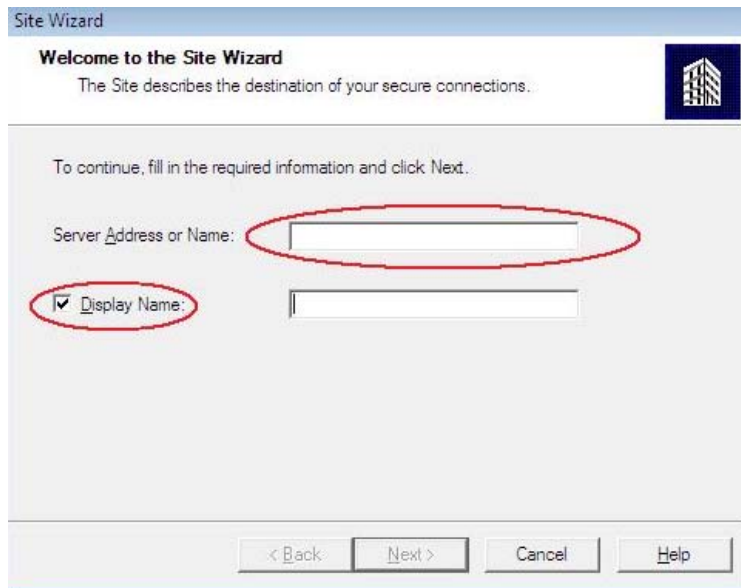
7.7 Create a New Site

1. In the **SecuRemote Connection** dialog box, click **New**. Then click **Site**.



2. In the **Server Address or Name** field, enter the **SOFA IP** address for your office. Check the **Display Name** box. In the **Display Name** field, type the word **Office**. Or if your office is the Hub site for your ONE Network group, type the word **Hub**.

Note: The **Display Name** must not contain any spaces.

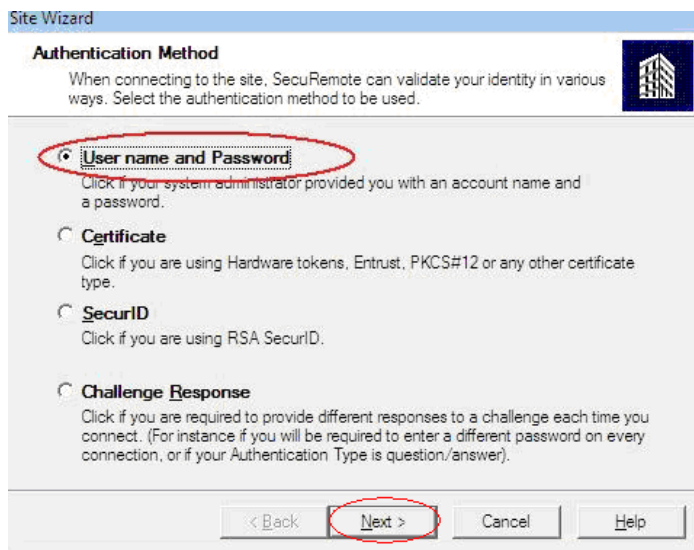


The screenshot shows the 'Site Wizard' dialog box with the title 'Welcome to the Site Wizard'. Below the title, it says 'The Site describes the destination of your secure connections.' There is a small icon of a building. Below that, it says 'To continue, fill in the required information and click Next.' There are two input fields: 'Server Address or Name:' and 'Display Name:'. The 'Display Name' checkbox is checked. The 'Server Address or Name' field and the 'Display Name' checkbox are circled in red. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

3. Click **Next** after entering the SOFA IP and the Display Name.

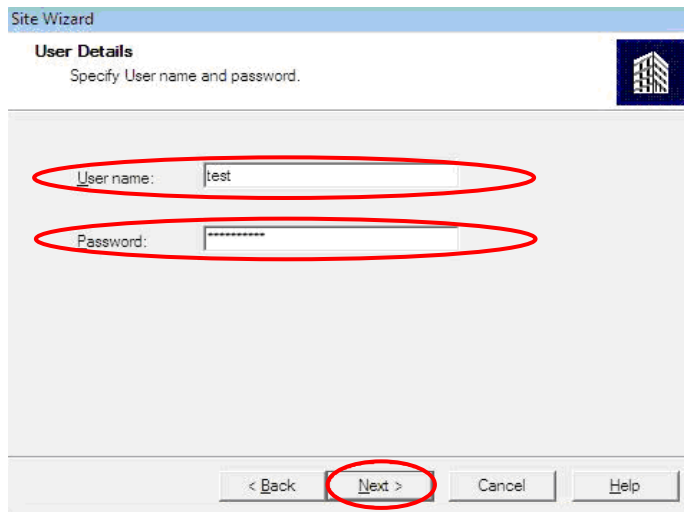
7.8 Enter the Username and Password

1. Check the box “**Username and Password**”, and then click **Next**



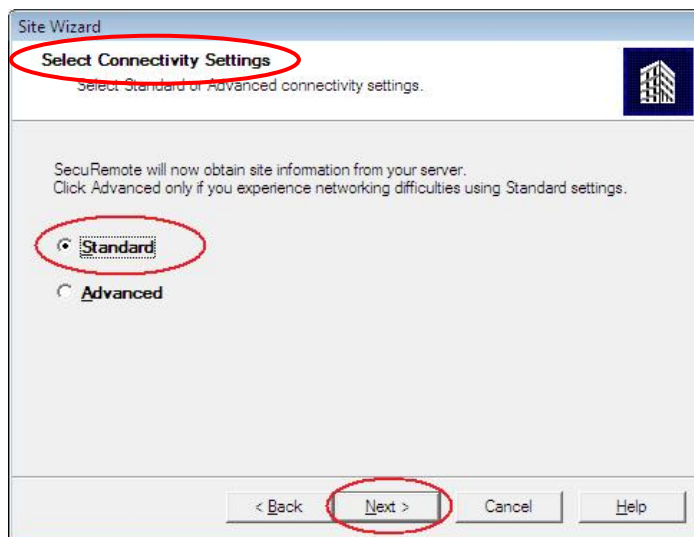
The screenshot shows the 'Site Wizard' dialog box with the title 'Authentication Method'. Below the title, it says 'When connecting to the site, SecuRemote can validate your identity in various ways. Select the authentication method to be used.' There is a small icon of a building. Below that, there are four radio button options: 'User name and Password', 'Certificate', 'SecurID', and 'Challenge Response'. The 'User name and Password' option is selected and circled in red. Below the options, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is also circled in red.

2. The **Authentication** dialog box automatically appears.
3. In the **User Name** field, enter the **Username**.
4. In the **Password** field, enter the **Password**.
5. Click **Next**.



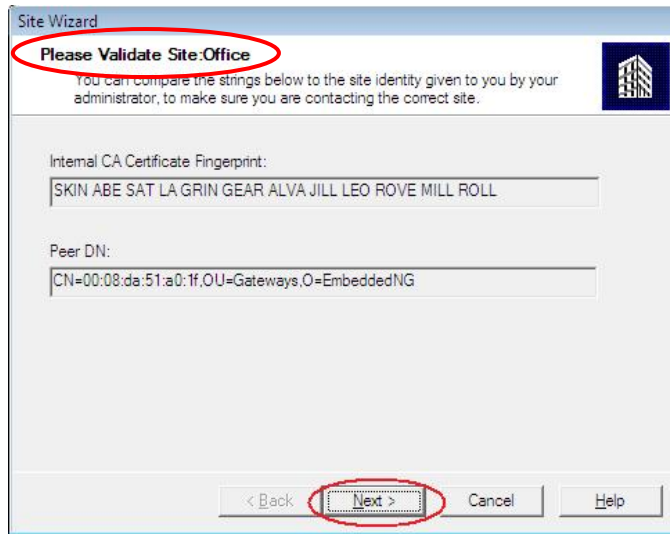
The screenshot shows the 'Site Wizard' dialog box with the 'User Details' tab selected. The title bar reads 'Site Wizard' and the subtitle is 'User Details'. Below the subtitle, it says 'Specify User name and password.' There are two text input fields: 'User name:' containing 'test' and 'Password:' containing a masked password. Both fields are circled in red. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is circled in red.

In the Select Connectivity Settings box, check **“Standard”**, and then click **Next**.



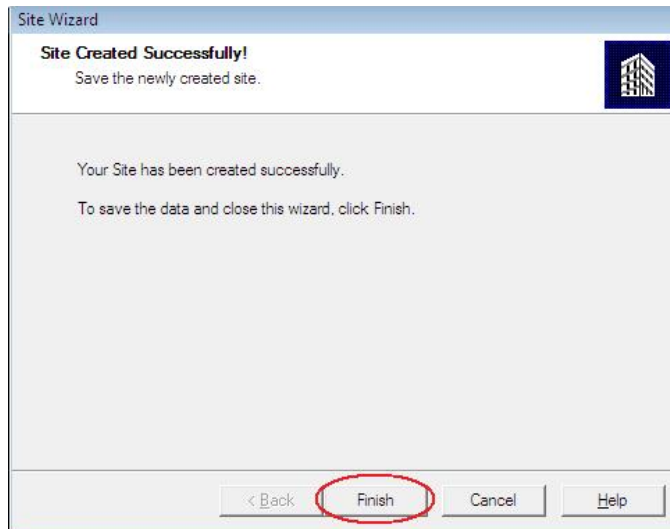
The screenshot shows the 'Site Wizard' dialog box with the 'Select Connectivity Settings' tab selected. The title bar reads 'Site Wizard' and the subtitle is 'Select Connectivity Settings'. Below the subtitle, it says 'Select Standard or Advanced connectivity settings.' There is a paragraph of text: 'SecuRemote will now obtain site information from your server. Click Advanced only if you experience networking difficulties using Standard settings.' There are two radio button options: 'Standard' (which is selected and circled in red) and 'Advanced'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is circled in red.

When the **Please Validate Site Office** box appears, please click **Next**.



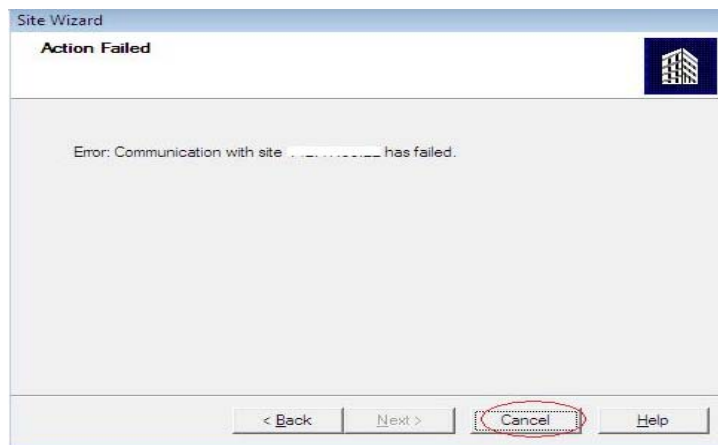
Note: If the connection isn't immediate, the message *"Getting data from the site"* is displayed.

6. Click **Finish**.



7.9 Communication Error

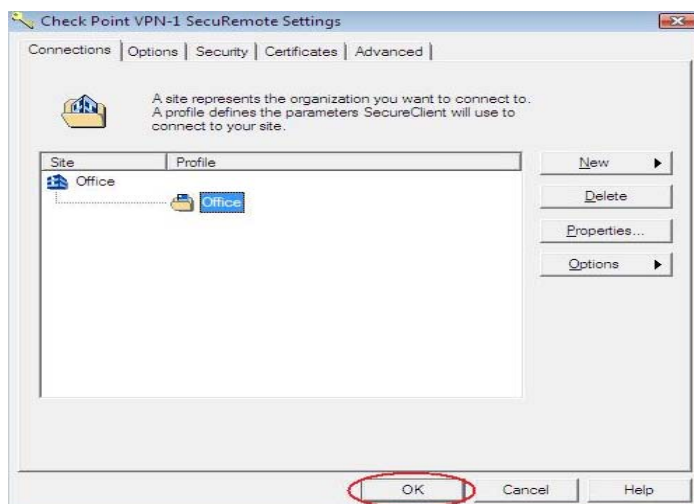
1. If the **Connection** fails, you receive a **Communication Error**.
2. Click **Cancel** and return to Section **7.7 Create a New Site**, and repeat the instructions.



3. If the Connection fails again, please open a ticket with your Help Desk.

7.10 Successful Connection

1. The **VPN-1 SecuRemote** dialog box appears on your screen showing the **Connection** to your office. Click **OK** on this screen.



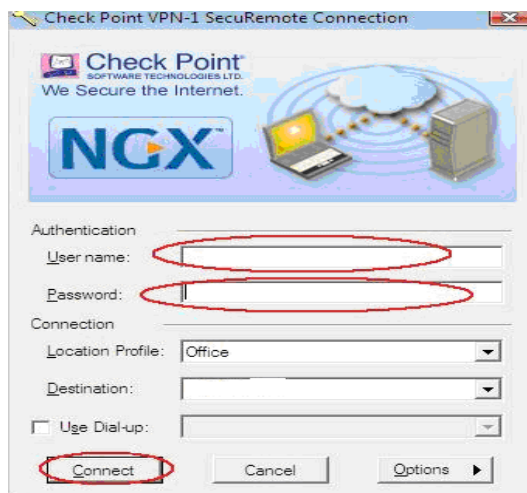
2. If you require a connection to another site within your ONE Network group, follow instructions from section 7.7 to add another site.

8.0 Connection to your Site

1. After creating the site, you will need to authenticate to your office.
2. Click on the **SecuRemote** icon in your taskbar and then click **Connect**

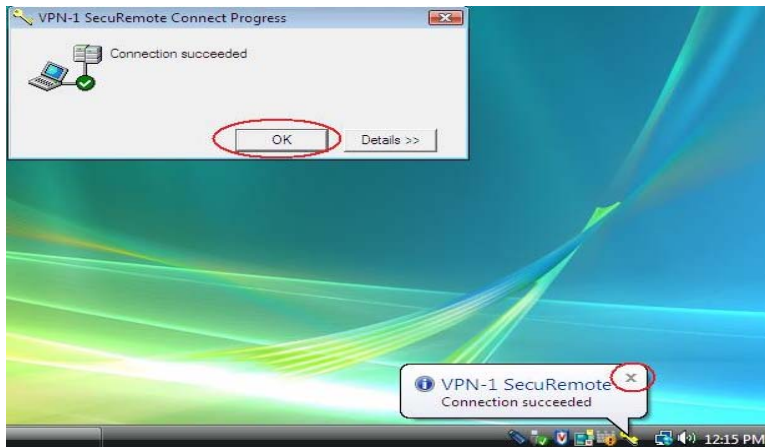


3. The **Authentication** dialog box automatically appears.
4. In the **User name** field, enter the **Username**.
5. In the **Password** field, enter the **Password**.
6. Please check that your **Location Profile**, shows **Office**
7. Please check that your **Destination** box shows your **SOFA IP address**.
8. Click **Connect**.



8.1 Successful Connection

If you have entered the correct information, you will get a Connection Succeeded notification. Click **OK** in the Connection Succeeded box.



8.2 Communication Error

1. If the **Connection** fails, you will receive a **Communication Error**.
2. Click **OK** and return to Section **8.0 Connecting to your site** and repeat the instructions.
3. If the connection fails again, please open a ticket with your Help Desk.

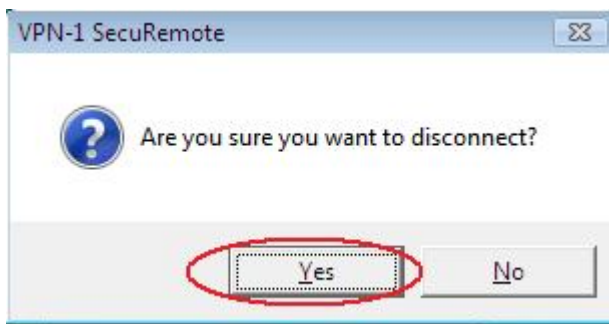


8.3 Disconnecting your Check Point SecuRemote VPN-1 Session

1. To terminate the SecuRemote VPN-1 connection, click on the **SecuRemote** Icon on the task bar as shown, click **Disconnect**.



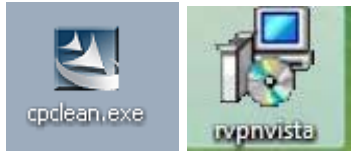
2. Click **Yes** to disconnect.



3. The **VPN-1 SecuRemote** dialog box disappears and all connections (Hub and/or Spoke) are closed.

9.0 Clean your Desktop

From your **Desktop**, delete the following icons, as they are no longer required.



Appendix A – Glossary

Term	Definition
CMS	Clinical Management System.
ONE Network Group	A ONE Network Group within the OntarioMD association consists of one hub site with none, one, or more spoke sites connected with IPSec VPN tunnels.
Hub	<ul style="list-style-type: none"> ▪ A common connection point for devices in a network. ▪ Typically the central location housing shared group applications such as the Clinical Management System (CMS).
ONE Network	Remote Virtual Private Network.
Site Vendor	A vendor who requires remote access to your medical office location, such as a LAN installer.
Spoke	A spoke site refers to an office within a ONE Network group that requires access to the hub site.
eHO	eHealth Ontario.
URL	Uniform Resource Locator.