Important Information

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=11819

For additional technical information, visit the Check Point Support Center
(http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 January 2011</td>
<td>Initial version</td>
</tr>
</tbody>
</table>

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Check Point Mobile for Windows for Windows 32-bit/64-bit R75 HFA1 EA User Guide).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction to R75 Remote Access Clients</td>
<td>5</td>
</tr>
<tr>
<td>Client Platforms</td>
<td>5</td>
</tr>
<tr>
<td>The Installation Process</td>
<td>5</td>
</tr>
<tr>
<td><strong>Getting Started</strong></td>
<td>6</td>
</tr>
<tr>
<td>Defining a Site</td>
<td>6</td>
</tr>
<tr>
<td>Basic Operations</td>
<td>8</td>
</tr>
<tr>
<td>Connect Window</td>
<td>9</td>
</tr>
<tr>
<td>Client Icon</td>
<td>9</td>
</tr>
<tr>
<td>Compliance</td>
<td>10</td>
</tr>
<tr>
<td><strong>Setting up a Remote Access Client</strong></td>
<td>11</td>
</tr>
<tr>
<td>Configuring Proxy Settings</td>
<td>11</td>
</tr>
<tr>
<td>Configuring VPN</td>
<td>11</td>
</tr>
<tr>
<td>Changing the Site Authentication Scheme</td>
<td>12</td>
</tr>
<tr>
<td>Certificate Enrollment and Renewal</td>
<td>12</td>
</tr>
<tr>
<td>Importing a Certificate in the CAPI Store</td>
<td>14</td>
</tr>
<tr>
<td>Authenticating with Certificate File</td>
<td>14</td>
</tr>
<tr>
<td>SecurID</td>
<td>14</td>
</tr>
<tr>
<td>Challenge-Response</td>
<td>15</td>
</tr>
<tr>
<td><strong>Collecting Logs</strong></td>
<td>15</td>
</tr>
<tr>
<td>Secure Domain Logon</td>
<td>15</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction to R75 Remote Access Clients

R75 Remote Access Clients are lightweight remote access clients for seamless, secure IPSec VPN connectivity to remote resources. They authenticate the parties and encrypt the data that passes between them.

R75 Remote Access Clients are intended to replace the current Check Point remote access clients: SecureClient, Endpoint Connect, and SecuRemote client.

The clients offered in this release are:

- **Endpoint Security VPN** - Replaces SecureClient and Endpoint Connect.
- **Check Point Mobile for Windows** - New Remote Access Client.
- **SecuRemote** - Replaces SecuRemote.

In This Chapter

<table>
<thead>
<tr>
<th>Client Platforms</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Installation Process</td>
<td>5</td>
</tr>
</tbody>
</table>

Client Platforms

You can install R75 Remote Access Clients on several Windows platforms.

- Microsoft Windows XP 32 bit SP2, SP3
- Microsoft Windows Vista 32 bit and 64 bit SP1
- Microsoft Windows 7, all editions 32 bit and 64 bit

The Installation Process

⚠️ **Important** - To install a R75 Remote Access Client on any version of Windows, you need Administrator permissions. Consult with your system administrator.

To install a R75 Remote Access Client:

1. Log in to Windows with a user name that has Administrator permissions.
2. Get the installation package from your system administrator, and double-click the installation package.
3. Follow the installation wizard.

   📝 **Note** - On Windows Vista and Windows 7, there may be a prompt to allow access, depending on the UAC settings.

After installation, the Client icon appears in the system tray notification area.

4. Double-click the Client icon.
   
   If you are prompted to define a site, make a site with the IP address that your system administrator gave you.
Chapter 2

Getting Started

In This Chapter

Defining a Site 6
Basic Operations 8
Connect Window 9
Client Icon 9
Compliance 10

Defining a Site

You need at least one site to connect to a VPN. If your system administrator pre-configured the client package, you can connect to the VPN site immediately. If not, you must define the site.

Before you begin, make sure you know how you will authenticate to the VPN and that you have the credentials (password, certificate file, or whatever the system administrator says you need). Also, you may need the gateway fingerprint, to verify that the client is connecting to the correct gateway. You should get this from your system administrator.

To define a site:
1. Right-click the client icon and select VPN Options.
   The Options window opens.
2. On the Sites tab, click New.
The Site Wizard opens.

Welcome to the Site Wizard

The wizard will guide you through the configuration of a new site for the VPN client.

3. Click **Next**.

<table>
<thead>
<tr>
<th>Server address or Name:</th>
<th>example.domain.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name:</td>
<td>My Gateway</td>
</tr>
</tbody>
</table>

4. Enter the name or IP address of the Security Gateway and click **Next**.
   It may take a few minutes for the Client to identify the site name.

After resolving the site, a security warning may open:

The site's security certificate is not trusted!
While verifying the site's certificate, the following possible security risks were discovered:

Ask your system administrator for the fingerprint of the server. If the server fingerprint matches the fingerprint in the warning message, you can click **Trust and Continue**. Otherwise, consult with your system administrator.
The **Authentication Method** window opens.

<table>
<thead>
<tr>
<th><strong>Authentication Method</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the authentication method to be used.</td>
</tr>
</tbody>
</table>

- **Username and Password**
  - Click if your system administrator provided you with an account name and a password.

- **Certificate**
  - If you are using Hardware tokens or any other certificate type.

- **SecurID**
  - Click if you are using RSA SecurID.

- **Challenge Response**
  - Click if you are required to provide different responses to a challenge.

5. Select an authentication method according to your system administrator’s instructions.
6. Click **Next** and follow the instructions to enter your authentication materials.
7. Click **Finish**.
   - The client offers to connect you to the newly created site.
8. Click **Yes** to connect to the site, or **No** to save the site details and connect later.

**Basic Operations**

Right-click the Client icon in the system tray notification area to access basic operations.

(Not all options appear for every client status and configuration.)

If you are not connected to the VPN, to connect quickly to the last active site, double-click the Client icon. If you are connected to the VPN and you double-click on the Client icon, the Client Overview window opens.

To access other basic operations, right-click the Client icon and select an option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect</td>
<td>Opens the main connection window, with the last active site selected. If you authenticate with a certificate, the client immediately connects to the selected site.</td>
</tr>
<tr>
<td>Connect to</td>
<td>Opens the main connection window and lets you select which site to connect to.</td>
</tr>
<tr>
<td>VPN Options</td>
<td>Opens the <strong>Options</strong> window to set a proxy server, choose interface language, enable Secure Domain Logon, and collect logs.</td>
</tr>
<tr>
<td>Register to Hotspot</td>
<td>Lets you register to a hotspot. After you click this option, open a browser. It will open to the hotspot registration page.</td>
</tr>
<tr>
<td>Show Compliance Report</td>
<td>See if your computer is compliant with the Security Policy, and if not, why not and how to fix the issue.</td>
</tr>
<tr>
<td>Show Client</td>
<td>Open the Check Point Mobile for Windows overview.</td>
</tr>
<tr>
<td>Shutdown Client</td>
<td>Closes Check Point Mobile for Windows and the VPN connection.</td>
</tr>
</tbody>
</table>
You can also access most of these options from the Client Overview.

Connect Window

In the Connect window, you provide authentication to connect to the VPN
- If you have a Certificate, browse to the certificate file and provide the password.
- If you use SecurID, enter your PIN or passcode. If you get a key in response, copy it.
- If you use Username and Password, enter your username and password.
- If you use Challenge Response, provide the first key. When the challenge comes, provides the response.

Client Icon

The Client icon in the system tray notification area shows the status of R75 Remote Access Clients.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Disconnected" /></td>
<td>Disconnected</td>
</tr>
<tr>
<td><img src="image" alt="Connecting" /></td>
<td>Connecting</td>
</tr>
<tr>
<td><img src="image" alt="Connected" /></td>
<td>Connected</td>
</tr>
<tr>
<td><img src="image" alt="Encryption" /></td>
<td>Encryption (encrypted data is being sent or received on the VPN)</td>
</tr>
<tr>
<td><img src="image" alt="Error" /></td>
<td>Error. The error might be that a computer is not compliant based on compliance checks.</td>
</tr>
</tbody>
</table>

You can also hover your mouse on the icon to show the client status.
Compliance

Your administrator can configure checks for your computer or device to make sure it is compliant before you connect to the VPN site. Some examples of what these checks can include are:

- If your Operating System is supported.
- If you are logged in correctly.
- If you have an updated Anti-virus client.

Your computer must be compliant with all checks to access the VPN.

If your computer is not compliant, the Client icon looks like this:

If your computer is found to be non-compliant based on one check, you cannot access the VPN. In the Client Overview window, it shows that you are not compliant and a message opens. If your computer does not comply based on multiple factors you can see multiple messages.

Follow the instructions in the message to make your computer is compliant. If you have questions, contact your administrator.

You can see a compliance report that shows if your computer is compliant with the Security Policy, and if not, how to fix the issue. To get a compliance report, right-click the Client icon in the system tray and select Show Compliance Report.

The compliance check always works in the background, when you are connected to the VPN or not. At any time it can report that your computer has failed a check and is not compliant.
Chapter 3

Setting up a Remote Access Client

In This Chapter

- Configuring Proxy Settings .................................................. 11
- Configuring VPN ......................................................... 11
- Changing the Site Authentication Scheme ...................... 12

Configuring Proxy Settings
If you are at a remote site which has a proxy server, the client must be configured to pass through the proxy server. Usually the client can detect proxy settings automatically. If not, you can configure it.

Before you begin, get the IP address of the proxy server from the local system administrator. Find out if the proxy needs a user name and password.

To configure proxy settings:
1. Right-click the Client icon and select **VPN Options**.
   The **Options** window opens.
2. Open the **Advanced** tab.
3. Click **Proxy Settings**.
   The **Proxy Settings** window opens.
4. Select an option.
   - **No Proxy** - Make a direct connection to the VPN.
   - **Detect proxy from Internet Explorer settings** - Take the proxy settings from Internet Explorer > Tools > Internet options > Connections > LAN Settings.
   - **Manually define proxy** - Enter the IP address port number of the proxy. If required, enter a valid user name and password for the proxy.
5. Click **OK**.

Configuring VPN
You may have the option to go through the VPN for all your Internet traffic. This is more secure.

To configure VPN Tunneling:
1. Right-click the Client icon and select **VPN Options**.
   The **Options** window opens.
2. On the **Sites** tab, select the site to which you want to connect, and click **Properties**.
   The **Properties** window for the site opens.
3. Open the **Settings** tab.

![Image of Properties window]

4. In **VPN tunneling**, click **Encrypt all traffic and route to gateway**.

   **Note** - In SecuRemote, this option is disabled. If this option is disabled in Endpoint Security VPN or Check Point Mobile for Windows, consult your system administrator.

5. Click **OK**.

### Changing the Site Authentication Scheme

If you have the option from your system administrator, you can change the way that you authenticate to the VPN.

**To change the client authentication scheme for a specific site:**

1. Right-click the Client icon and select **VPN Options**.
   The **Options** window opens
2. On the **Site** tab, select the relevant site and click **Properties**.
   The **Properties** window for the site opens.
   On the **Settings** tab, select the appropriate **Authentication Scheme** drop-down menu option.
   - Username and password
   - Certificate - CAPI
   - Certificate - P12
   - SecurID - KeyFob
   - SecurID - PinPad
   - SecurID – Software Token
   - Challenge Response

### Certificate Enrollment and Renewal

You can import a certificate to the CAPI store or save it to a folder of your choice.

Before you enroll a certificate, make sure you have the registration key from the system administrator. Ask the system administrator whether you should use CAPI (if so, ask for the provider name) or P12.
To enroll a certificate:
1. Right-click the Client icon in the system tray, and select **VPN Options**.
2. On the **Sites** tab, select the site from which you want to enroll a certificate and click **Properties**.
   The site **Properties** window opens.
3. Select the **Settings** tab.

   ![VPN Client Settings](image)

   - **Always-Connect**
     Enable Always-Connect to allow the client to connect automatically to your active site when possible.
     - Enable Always-Connect

   - **VPN tunneling**
     When connected, all outbound traffic is encrypted and sent to the gateway but only traffic directed at site resources is passed.
     - Encrypt all traffic and route to gateway

   - **Authentication**
     Choose an **Authentication Method** (Certificate - CAPI or Certificate - P12), and click **Enroll**.
     - **CAPI**: In the window that opens, select the provider.
     - **P12**: In the window that opens, enter a new password for the certificate and confirm it.

4. Enter the Registration Key that your administrator sent you.
5. Click **Enroll**.

Your system administrator may tell you to renew your certificate, or you see a message that the certificate expired.

To renew a certificate:
1. In the **Settings** tab > **Method**, select either **Certificate - CAPI** or **Certificate - P12**.
2. Click **Renew**.
   In the window that opens, select your certificate type:
   - **CAPI**: select the certificate from the list.
   - **P12**: browse to the P12 file and enter the password.
3. Click Renew.

Importing a Certificate in the CAPI Store

Before you can use the certificate to authenticate your computer, you must get:

- The certificate file.
- The password for the file.
- The name of the site (each certificate is valid for one site).

If the system administrator said to save the certificate on the computer, import it to the CAPI store. (Otherwise, the administrator will give you the certificate file on a USB or other removable media. Make sure you get the password.)

To import a certificate file to the CAPI store:
1. Right-click the client tray icon, and select VPN Options.
2. On the Sites tab, select the gateway and click Properties.
3. Open the Settings tab.
4. Make sure that Certificate - CAPI is selected in the Method list.
5. Click Import.
7. Enter the certificate password and click Import.

Authenticating with Certificate File

If Certificate – P12 is used, browse to the P12 file to authenticate.

To authenticate with a P12 file:
2. Connect to the site.
   The connection dialog opens.
3. In the Certificate File area, browse to the P12 file.
4. Enter the certificate password.
5. Click Connect.

Note - If Always-Connect is on, the Client asks for the certificate password if a secure connection is lost. You do not have to browse to the certificate file again.

SecurID

RSA SecurID authentication uses hardware (Key Fob or PINPad) or software (softID) that generates an authentication code at fixed intervals (usually one minute), with a built-in clock and an encoded random key. The Client uses both the PIN and tokencode, or just the passcode, to authenticate to the Security Gateway.

- The most common form of SecurID token is the hand-held device, usually a Key Fob or PINPad.
  - With PINPad, you enter a personal identification number (PIN), to generate a passcode that you can use for the client.
  - When the token does not have a PINPad, a tokencode is displayed. A tokencode is the changing number displayed on the Key Fob. If Key Fob is the authentication method, you enter the PIN and the tokencode separately.
- SoftID operates the same way as a passcode device, but consists only of software that sits on the desktop. You can use it as a simple Key Fob and copy the token code. Or, you can set the authentication method to SecurID Software Token, and the client will take the token code automatically.
Challenge-Response

Challenge-response is an authentication protocol in which one party provides the first string (the challenge), and the other party verifies it with the next string (the response). For authentication to take place, the response is validated. Security systems that rely on smart cards are based on challenge-response.

Collecting Logs

If your system administrator or help desk asks for logs to troubleshoot issues, you can collect the logs from your client.

To collect logs:
1. Right-click the Client icon and select VPN Options.
2. Open the Advanced tab.
3. Click Enable Logging.
4. Click Collect Logs.

Note - The logs are saved to %TEMP%\trac\trlogs_timestamp.cab. It opens after the logs are collected.

This folder is sometimes hidden. If you need to locate this folder, in Control panel > Folder Options > View, select Show hidden files and folders.

Secure Domain Logon

If the system administrator says that you should use SDL, you can configure your client.

To enable SDL on a client:
1. Right-click the Client icon and select VPN Options.
2. In Options > Advanced, select Enable Secure Domain Logon (SDL).
3. Click OK.
4. Restart the computer and log in.