

Endpoint Security Client for Mac

E80.50

User Guide

14 January 2014



© 2014 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (<http://www.checkpoint.com/copyright.html>) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation

The latest version of this document is at:

(http://supportcontent.checkpoint.com/documentation_download?ID=24675)

To learn more, visit the Check Point Support Center (<http://supportcenter.checkpoint.com>).

For more about this release, see the E80.50 home page

(<http://supportcontent.checkpoint.com/solutions?id=sk92971>).

Revision History

| Date | Description |
|-----------------|---|
| 13 January 2014 | Improved formatting and document layout |
| 29 August 2013 | First release of this document |

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 Endpoint Security Client for Mac E80.50 User Guide).

Contents

| | |
|---|-----------|
| Important Information | 3 |
| Introduction to Endpoint Security | 5 |
| Getting Started | 5 |
| Checking if the Client is Installed | 5 |
| Installing the Client | 5 |
| Uninstalling the Client | 6 |
| Using the Client | 6 |
| Tour of the Main Client Window | 6 |
| VPN Blade | 6 |
| Firewall Blade | 7 |
| Compliance Blade | 7 |
| Full Disk Encryption Blade | 7 |
| Advanced | 8 |
| Menu Bar Icons | 8 |
| Basic Client Operations | 9 |
| Responding to Alerts | 9 |
| VPN Alerts | 9 |
| Compliance Alerts | 9 |
| VPN | 11 |
| VPN Basics | 11 |
| Creating a VPN Site | 11 |
| Connecting to the VPN | 13 |
| Disconnecting from a Site | 13 |
| Opening the Site Wizard Again | 14 |
| VPN Configuration Options | 14 |
| Authentication | 14 |
| Configuring Connection Options | 18 |
| Collecting and Sending Log Files | 20 |
| Full Disk Encryption | 21 |
| Overview of the Login Screen | 21 |
| Using the Virtual Keyboard | 21 |
| Using Special Characters | 21 |
| Changing the Language | 22 |
| Authenticating to Full Disk Encryption | 22 |
| Authenticating for the First Time with a Fixed Password | 22 |
| If You Do Not Have Your Password | 22 |
| Troubleshooting | 24 |
| Technical Difficulties | 24 |
| Collecting Information for Technical Support | 24 |
| Index | 25 |

Chapter 1

Introduction to Endpoint Security

In This Chapter

| | |
|----------------------|---|
| Getting Started | 5 |
| Using the Client | 6 |
| Responding to Alerts | 9 |

Check Point Endpoint Security™ is the first and only single client that combines all essential components for total security on the endpoint. It includes these Software Blades:

- Firewall for desktop security
- Compliance
- Full Disk Encryption
- VPN for transparent remote access to corporate resources

Check Point Endpoint Security protects PCs and eliminates the need to deploy and manage multiple agents.

Getting Started

Endpoint Security is managed by an Endpoint Security Management Server that is controlled by an administrator. The administrator creates the Endpoint Security policy that your client uses to protect your Mac.

Checking if the Client is Installed



If you see the menu Endpoint Security icon on the menu bar, the client is installed.

Note: You should also see the Endpoint Security App in in Launchpad.

Installing the Client

Get the Endpoint Security client zip file from your administrator.

1. Double-click **Endpoint_Security_Installer.zip** to unzip the file.
Endpoint_Security_Installer.app shows next to the zip file.
2. Click **Endpoint_Security_Installer.app**.
The Check Point Endpoint Security Installer opens.
3. Click **Install**.
4. Enter a **Name** and **Password** to authorize the installation and click **OK**.
Wait while package installs.
5. A message shows that the package installed successfully or failed for a specified reason. Click **Close**.
If the installation was successful, the Endpoint Security icon shows in the menu bar.

Uninstalling the Client

1. Open a terminal window.
2. Run:

```
sudo "/Library/Application Support/Checkpoint/Endpoint Security/uninstall.sh"
```



Note - If the endpoint was encrypted, the uninstall script first prompts for a reboot so that HFS volumes can be decrypted. After decryption, the script continues to uninstall the client.

Using the Client

Use the main client window and the Menu Bar icon to see all of the information related to Endpoint Security.

The client automatically connects to a server for updates according to the schedule set by your administrator.

Tour of the Main Client Window

The main client window gives one-stop access to the security features that keep your Mac safe.

To launch the main client window, select **Display Overview** from the Endpoint Security icon on the menu bar. The Software Blades you see depends on settings defined by your administrator.



- Click on a Software Blade to see the details.
- The top section shows if your Mac is compliant, or if any component needs attention. All status issues or necessary actions are shown in this bar.
- The status of each component shows next to it.

VPN Blade

Endpoint Security VPN lets you connect securely to your enterprise network when working remotely. The display shows the state of the VPN (Connected, Disconnected, Connecting, or Disconnecting) and its default site.

Double-click to see more information and the **VPN Detail** pane opens. This pane includes:

- **Connection Status** - The status of the VPN connection:
 - **Duration** - How long it has been connected.
 - **Expiration** - When the authentication expires.
- **Connection Details** - Network details:
 - **Site Name** - The site the VPN will try to connect unless you change it.
 - **Gateway IP Address** - The IP address of the VPN site.
 - **Last time connected** - If you are disconnected, it shows the last time you were connected.
- **Encryption Settings** - How many packets and KB have been decrypted and encrypted during the connection.
- **Connect to** - Click to select which VPN to connect to and to enter authentication information.
- **Connect** - Click to connect to the default VPN site.
- **VPN Options** - Click to see more options for connection details, managing settings, and registering to a hotspot. See the VPN section for more information.

Firewall Blade

Firewall is your front line of defense against Internet threats. The display shows the status of your firewall.

Click **Firewall** and the **Firewall Detail** pane opens. This pane describes the Firewall policy and Access Zone policy installed on your Mac.

Compliance Blade

Compliance Enforcement lets the Endpoint Security client protect your enterprise network by enforcing a security policy created by your administrator.

There are four states of compliance:

- **Compliant** - Your Mac is compliant with the enterprise security policy.
- **Warn** - Your Mac is not compliant with the enterprise security requirements. Your ability to access your enterprise network does not change. To become compliant, do the actions shown.
- **About to be restricted** - Your Mac is not compliant with the enterprise security requirements. Your ability to access the enterprise network will be *restricted* if you do not do the actions shown to become compliant within the specified time.
- **Restricted** - Your Mac is not compliant with the enterprise security requirements. Your ability to access your corporate network is *restricted*. To become compliant, do the actions shown.

Click for more information and the **Compliance Detail** pane opens. It includes:

- **Policy Details** - A summary of the Compliance policy that is installed on your Mac.
- **Current Status** - A **Message** about each problem.

Full Disk Encryption Blade

Full Disk Encryption ensures that only authorized users can access desktops and laptops. If you have the Full Disk Encryption blade installed, you must enter a password to start your Mac. Until you are authenticated, all information on the Mac is encrypted. Click **Full Disk Encryption** and the **Full Disk Encryption Detail** pane opens. This pane shows:

- **Policy Details** - Details of the Full Disk Encryption and OneCheck User Settings policies that are installed on your Mac.
- **Current Status** - A summary of the Full Disk Encryption status of your Mac.
 - Encryption Status** - Shows the encryption status of devices connected to your Mac. It also shows the size and available space for each device.
- **Advanced** - Shows additional details for the different parts of your Full Disk Encryption account.

Advanced

The **Advanced** page has these sections:



- **Server**
Shows the Endpoint Server IP address, time and date of the last connection, and the connection status.
- **Policies**
Shows security policies enforced by the client.




| Name | Type | Version | Date | Mode |
|---|-----------------|---------|----------------|------------|
| Check Point Restricted | Firewall | 3 | 07/02/12 13:20 | Restricted |
| Check Point Restricted policy | Zone Definition | 1 | 06/28/12 19:05 | Restricted |
| Default Compliance settings for the entire organization | Compliance | 6 | 07/10/12 16:36 | Connected |

- **Logging**
Collects logs for technical support.

Menu Bar Icons

The icons displayed in the Menu Bar let you quickly monitor your security status and Internet activity and access your security settings in just a few clicks. Click any of the icons shown below to access a shortcut menu.

| Icon | Status |
|------|--|
| | VPN not installed. |
| | VPN connected. |
| | VPN connecting. |
| | VPN disconnected. |
| | <ul style="list-style-type: none"> • Full Disk Encryption encrypting or decrypting. • VPN is not installed or running. |
| | Full Disk Encryption encrypting or decrypting while VPN is connected. |

| Icon | Status |
|---|--|
|  | Full Disk Encryption encrypting or decrypting while VPN is disconnected. |
|  | Warning that requires you to take action, for example compliance issue. |
|  | <p>Icon with a flashing light. An error has occurred that requires you to take action:</p> <ul style="list-style-type: none"> • Compliance restriction • One or more blades is not running • One or more blades in a state of error <p>If you are not sure what to do, contact your system administrator.</p> |

Basic Client Operations

Basic operations can be done using commands available from the client's menu bar icon. The options available depend on the client status and configuration.

| Command | Function |
|------------------|---|
| Help | Shows the help file. |
| Connect | 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. |
| Display Overview | Opens the main client window. |
| Quit | Closes the GUI. |

Responding to Alerts

While you use the Endpoint Security client, you might see alerts. You must respond to some alerts while other alerts are just informative.

VPN Alerts

VPN Configuration alerts occur when the client detects a network connection or VPN connection. These alerts help you correctly configure your network and program permissions.

Compliance Alerts

The Compliance policy checks for:

- Running or up-to-date anti-virus software
- Allowed or disallowed processes
- Allowed or disallowed files
- Blades - Installed and running
- Authorized programs. Only authorized programs are allowed to run on your Mac.

Compliance alerts show when your Mac does not match the Compliance policy. This can occur if there are changes to the Compliance rules or to your Mac configuration. If Endpoint Security determines that your Mac is not compliant, a compliance alert shows with this information:

- One of these Compliance states:
 - **Warning** - Your Mac is not compliant but you can continue to use network resources. Do the steps to make your Mac compliant as quickly as possible.
 - **About to be restricted** - Your Mac is not compliant. You must make it compliant immediately. If you do not do this, access to network resources will be restricted.
 - **Restricted** - Your Mac is not compliant. Access to network resources may be limited according the policy defined by your administrator for the restricted state.

Chapter 2

VPN

In This Chapter

[VPN Basics](#)

11

[VPN Configuration Options](#)

14

Endpoint Security lets you easily set up a secure VPN to connect to your corporate resources.

VPN Basics

Endpoint Security VPN lets you connect securely to your enterprise network from a remote location. The VPN connection can be made directly to the server or through an Internet Service Provider (ISP). You can connect to the organization using any network adapter (including wireless adapters).

The Endpoint Security VPN authenticates the parties and encrypts the data that passes between them. The VPN feature uses standard Internet protocols for strong encryption and authentication. Encryption ensures that only the authenticated parties can read the data passed, and is not altered during transit.

On the client, clicking the VPN Blade shows:

- Information about any current VPN connection (if any) and about the status of your remote connection to a VPN enabled security gateway.
- **VPN Options.** Clicking VPN options lets you
 - Launch the Site Wizard to create a site.
 - Open the **VPN Properties** of a defined site to enable:
 - **Always-Connect**, which allows the client to connect automatically to the active VPN site.
 - **VPN tunneling**, which encrypts all outbound traffic to the corporate gateway. Only traffic intended for corporate resources is inspected.
 - An **Authentication** method.
 - **Delete** a previously configured site

Creating a VPN Site

For remote VPN access to the corporate network, the client must have at least one site defined. The site is the VPN gateway. From your system administrator, get:

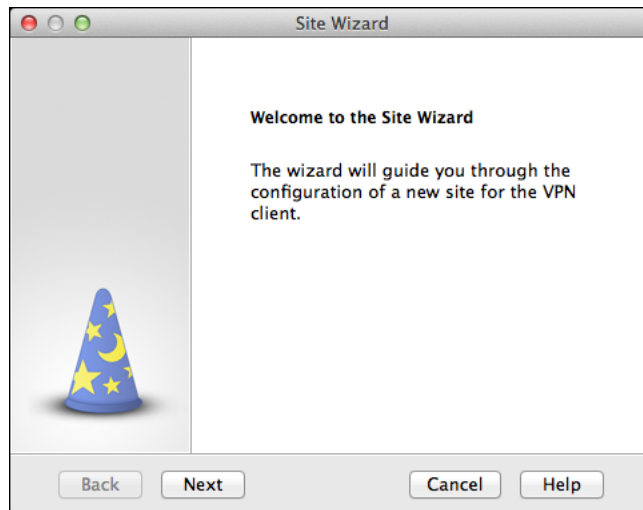
- The gateway fingerprint
- The gateway IP address or domain name
- Your authentication method
- Authentication materials (username and password, certificate file, RSA SecurID, or access to Help Desk for challenge/response authentication).

Your administrator may have already configured the corporate site for you. If not, this message shows when you first try to connect: *No site is configured. Would you like to configure a new site?* You cannot access the corporate VPN until you configure a site.

To configure site:

1. When asked if you want to configure a new site, click **Yes**.

The **Site Wizard** opens.



2. Click **Next**.
3. Enter the IP address, or the name of the corporate VPN gateway.



The wizard shows the progress while the Client resolves the site name or address to the actual gateway. This may take several minutes, depending on the speed of your network connection.

4. When prompted, confirm the fingerprint. (If you are not sure, consult your system administrator.) The fingerprint is stored internally and the security warning is not opened again, even if the client is upgraded.

The wizard shows the various methods of authentication available ("[Authentication](#)" on page 14).

5. Select the relevant method and click **Next**.
 - If **Certificate**, select **P12** or **Keychain** (make sure you know which to select), and click **Next**.
 - If **SecurID**, select the type (KeyFob or PinPad), and click **Next**.

If you are not sure of your authentication method, contact your system administrator.

6. Click **Finish**.
A message shows: Would you like to connect?
7. Click **Yes** to connect to the corporate VPN.



Note - You can create multiple VPN sites.

Connecting to the VPN

1. Click the **Menu Bar** icon
2. Select **Display Overview**.
The main client window opens.
3. From the main client window, click the **VPN Blade**.
4. Click:
 - **Connect**
To connect to active site.
 - **Connect to**
To select a site for the VPN connection, or to create a new site using the **Site Wizard**.

Alternatively:

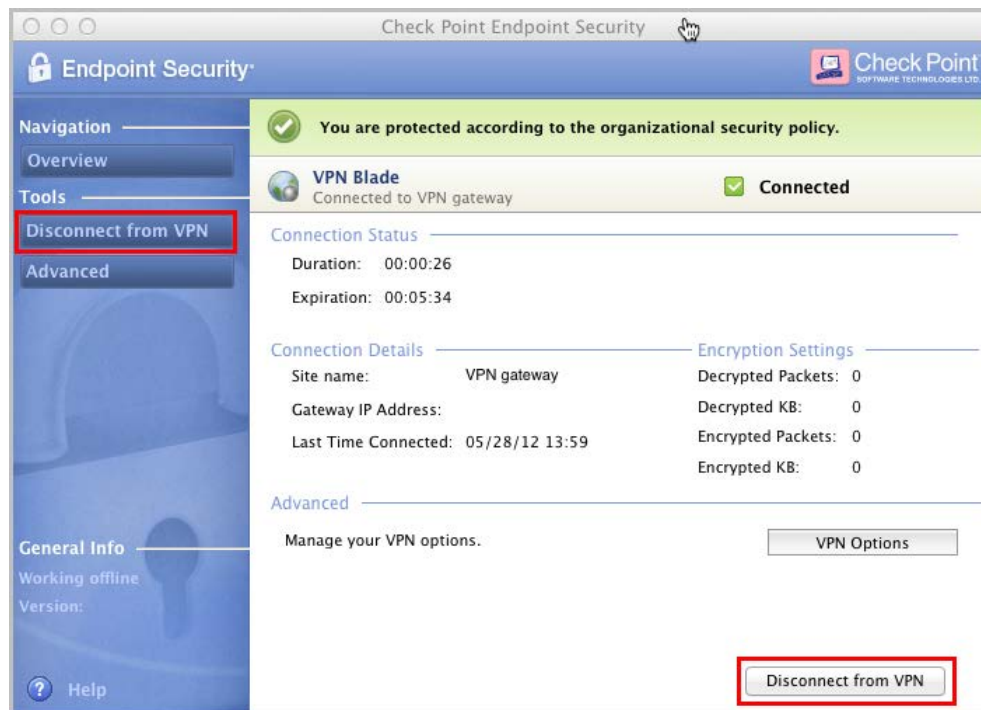
1. Click the **Menu Bar** icon.
2. Select **Connect**.

Disconnecting from a Site

To disconnect from a site:

1. Click the client icon on the **Menu bar**.
2. Click **Disconnect from VPN**.
3. Click **Yes** to disconnect.

You can also disconnect using the **Disconnect from VPN** buttons.



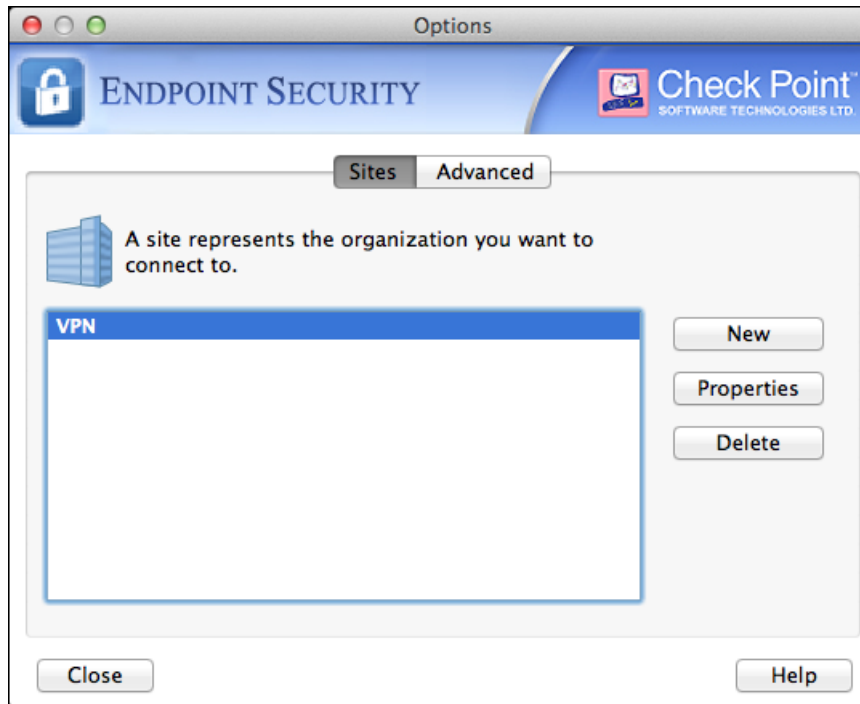
Opening the Site Wizard Again

The Site wizard opens automatically the first time the VPN client is opened. You can also manually open the site wizard .

To create a new site for the client:

1. Click the client icon and select **VPN Options**.

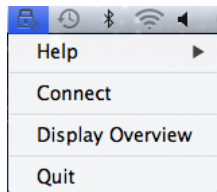
The Options window opens.



2. On the **Sites** tab, click **New**.

The Site Wizard opens.

Alternatively, click on the **Menu Bar** client icon, and select **Connect** from the menu.



If no sites are configured, the site wizard opens.

VPN Configuration Options

This section covers:

- Authentication (on page [14](#))
- Configuring Connection Options (on page [18](#))
- Collecting and Sending Log Files (on page [20](#))

Authentication

This section covers authentication and credential management for the VPN client.

User Name and Password

User name and password is the simplest form of authentication. Together with your system administrator, decide on an appropriate user name and password.

Strong passwords:

- **Are lengthy**
A 15-character password composed of random letters and numbers is much more secure than an 8-character password composed of characters taken from the entire keyboard. Each character that you add to the password increases the protection that the password provides.
- **Combine letters, numbers, and symbols**
A mixture of upper and lower case letters, numbers, and symbols (including punctuation marks not on the upper row of the keyboard).
- **Avoid sequences or repeated characters**
For example 12345, or aaaaa.
- **Avoid look-alike substitutions of numbers or characters**
For example replacing the letter "i" with the number "1", or zero with the letter "o".
- **Avoid your login name**
- **Avoid dictionary words in any language**

These authentication credentials are stored either in the security server database, on an LDAP or RADIUS server.

Understanding Certificates

A certificate is the digital equivalent of an ID card issued by a trusted third party known as a Certification Authority (CA). While there are well known external CAs such as *VeriSign* and *Entrust*, the VPN client typically uses the digital certificates issued by the site's security gateway, which has its own Internal Certificate Authority (ICA).

The digital certificate used by the VPN client contains:

- Your name
- A serial number
- Expiration dates
- A copy of the certificate holder's public key (used for encrypting messages and digital signatures)
- The digital signature of the certificate-issuing authority, in this instance the ICA, so that the security gateway can verify that the certificate is real and (if real) still valid.
- A certificate is a file in the P12 format with the **.p12** extension.

Storing a Certificate in the Keychain

If you are using certificates for authentication, your system administrator will supply (out of band) a file with a P12 extension. This is a PKCS#12 file, a format commonly used to store private encryption keys. The PKCS#12 file is password protected, and can be stored in the keychain. Keychain is the password management system on the Mac OS.

To enter a certificate issued by a public Certificate Authority (CA) into the keychain:

1. Double-click the file with the p12 extension.
2. When prompted, enter the private key password set by your system administrator.
3. Click **OK**.

The certificate is entered into the keychain.

If your administrator supplies a certificate issued by the Internal Certificate Authority (ICA), use the certificate enrollment process ("[Certificate Enrollment and Renewal](#)" on page 17).

The client will automatically enter the certificate into the keychain. If you are not sure which kind of certificate you are using for authentication, contact your system administrator.

Saving the Certificate to a Folder of your Choice

If you do not wish to save your certificate to the keychain, for example you use several desktop workstations and laptops and for security reasons do not wish to leave your certificate on different endpoints, then save the **PKCS#12** certificate to an external device, such as a USB disk. Then:

1. Configure the client to use certificates for authentication.
2. From the drop-down **Certificate - p12** box, select **From File**.
3. In the **From File** area, browse to the certificate file.
4. Enter the certificate's password.
5. Click **Connect**.



Note - If you have the **Always-Connect** option configured, then each time the client loses communication with the site, you will be prompted to enter the certificate's password.

Another advantage of not having the **PKCS#12** certificate in the keychain is that, if someone steals your laptop, they will not be able to use the client to connect to the site without knowing the password—even if they have the **PKCS#12**. For this reason, your system administrator may switch from using the certificate stored in the keychain and to require you to authenticate using the **PKCS#12** certificate directly. If this happens, a message displays when you try to connect to the active site. Browse to the folder where the certificate is stored.

SecurID

The RSA SecurID authentication mechanism consists of either hardware (FOB, USB token) or software (softID) that generates an authentication code at fixed intervals (usually one minute) using a built-in clock and an encoded random key.

The most typical form of SecurID Token is the hand-held device. The device is usually a key FOB or slim card. The token can have a PIN pad, onto which a user enters a Personal Identification Number (**PIN**) to generate a **passcode**. When the token has *no* PIN pad, a **tokencode** is displayed. A **tokencode** is the changing number displayed on the key FOB.

The VPN client uses both the PIN and tokencode or just the passcode to authenticate to the security gateway.



Note - The client's site connection wizard supports hardware tokens only.

Challenge Response

Challenge-response is an authentication protocol in which one party presents a question (the challenge) and another party provides an answer (the response). For authentication to take place, a valid answer must be provided to the question. Security systems that rely on smart cards are based on challenge-response.

Changing Authentication Schemes

1. Click the client icon on the **Menu bar** and select **Display Overview**.
2. Select **VPN blade**.
3. In the **VPN** window, click **VPN Settings**.
The **Options** window opens
4. On the **Site** tab, select the relevant site and click **Properties**.
The **Properties** window for that site opens.

On the **Settings** tab, use the drop-down **Authentication Method** box to either:

- a) Username and password
- b) Certificate - keychain
- c) Certificate - P12
- d) SecurID - Keyfob
- e) SecurID - PinPad
- f) Challenge Response

Certificate Enrollment and Renewal

Enrollment refers to the process of applying for and receiving a certificate from a recognized Certificate Authority (CA), in this case Check Point's Internal CA. In the enrollment process, your system administrator creates a certificate and sends you the certificate's registration key. The client sends this key to gateway, and in return receives the certificate. The certificate is saved as a p12 file or stored in the keychain.

You can enroll either when creating a site or after a site is created.

Enrolling During Site Creation

1. Open the **VPN** panel > open **VPN Options**.
2. On the **Sites** tab, click **New**.
The Site wizard opens.
Follow the wizard until you reach the Certificate Authentication window
3. Select **Check this if you don't have a certificate yet (only works with ICA certificates)**.
4. Click **Next**.
When the **Site Created Successfully Message** appears, click **Finish**.
5. When asked if you would like to create a certificate now, click **Yes**.
6. In the Certificate Authentication window, select keychain or PKCS#12.
7. Enter the required authentication details, such as the registration key, and click **Enroll**.
 - If you have a PKCS#12 certificate, the **SAVE AS** window opens. Save the certificate to an appropriate directory.
 - (i) You are asked if you want to connect. Click **Yes**.
 - (ii) When the main connection window opens, browse to the location of your PKCS#12 certificate.
 - If you selected keychain, the certificate is automatically entered into the keychain store.
The certificate will be a protected item. Each time the client uses the certificate, you will be required to manually grant permission.
8. The **Enrollment** window opens.
9. When prompted, add the certificate to the root store.
10. After the Enrollment succeeded message, the connection window opens with the certificate selected.
11. Click **Connect**.

Enrolling After Site Creation

1. In the VPN window, click **VPN Settings**.
2. Select the site and click **Properties**.
3. On the Settings tab, click **Enroll**.
The Connection window opens.
4. Enter a password
5. Confirm the password
6. Enter the Registration key
7. Click **Enroll**
 - If you have a PKCS#12 certificate, the **SAVE AS** window opens. Save the certificate to an appropriate directory.

- (i) You are asked if you want to connect. Click **Yes**.
 - (ii) When the main connection window opens, browse to the location of your PKCS#12 certificate.
 - If you selected keychain, the certificate is automatically entered into the keychain store.
- The certificate will be a protected item. Each time the client uses the certificate, you will be required to manually grant permission.
8. The **Enrollment** window opens.
9. When prompted, add the certificate to the root store.
10. After the Enrollment succeeded message, the connection window opens with the certificate selected.
11. Click **Connect**.

Automatic Certificate Renewal

When using certificates for authentication, each time you connect to the site, the client checks to see how close the certificate is to its expiration date. If necessary, and simultaneously with the connect process, the certificate is renewed. A message balloon appears in the system tray: **Certificate renewal in progress**.

Certificate Renewal

A certificate can be renewed at any time.

To renew a certificate:

1. In the VPN window, click **VPN Settings**.
2. Select the site and click **Properties**.
3. On the **Settings** tab, click **Renew**.
The **Authentication** window opens.
4. Using the drop-down box, select your certificate.
5. When prompted, grant access to the protected item (your certificate).
After the **Renewal Succeeded** message shows, the **Connection** window opens.

Configuring Connection Options

This section describes connection and log in options.

Password Caching for Single Sign-On

If your site administrator has enabled password caching, the VPN client stores the password you entered during the last successful connect and authenticate operation. For example if you authenticate through a username/password (or enter the password to a p12 certificate) this password word is cached.

- This password is held only in memory and deleted once you explicitly disconnect from a site.
- If, for example, location awareness is enabled, then as the client automatically reconnects to the site, the password is supplied transparently from cache.
- If you see the password field already populated when you attempt to connect to a site, this means that the cached credentials will be used. If necessary, you can override them and enter new credentials.

Staying Connected all the Time

1. Click the client icon on **Menu bar**, select Display **Overview**.
2. Click the **VPN Blade**.
3. Click **VPN Options**.
4. Select a site, click **Properties**.
5. On the **Settings** tab, select **Enable Always-Connect**.
6. Click **OK**.
7. Click **Close**.

Connecting through a Hotspot

For wireless connections, the VPN client can automatically detect the presence of a hotspot. (This behavior has to be configured by your administrator). When connecting for the first time through the hotspot server:

1. The connection logically fails because no registration details have been presented.
The client shows a link.
2. Click the link to open the hotspot registration form in a browser window.
3. Enter the relevant authentication and payment credentials.
4. Try again to connect to the site.

Proxy Settings

From time to time you may need to change your proxy server settings.

To change the proxy settings for the VPN client:

1. Click the **Menu Bar** icon, and select **Display Overview**.
2. Select **VPN Blade > VPN Options**.
3. On the **Advanced** tab, select **Proxy Settings**.
The **Proxy Settings** window opens.
4. Click the **Advanced** tab and select **Proxy Settings**.
The **Proxy Settings** window opens.
5. Configure your **Proxy Definition**:
 - **No proxy** - No proxy is defined.
 - **Detect proxy from System Preferences settings** - This is the default setting. The client takes proxy settings from system preferences.
 - **Manually define proxy** - Configure the proxy settings manually. Ask your administrator for the IP address and port number of the proxy.
6. Enter your Proxy Authentication details. Ask your system administrator for the correct user name and password.

VPN Tunneling

VPN tunneling makes sure all traffic between the client and the site is encrypted.

To configure VPN Tunneling:

1. Click the **Menu Bar** icon, and select **Display Overview**.
2. Select **VPN Blade > VPN Options**.
3. Select the site and click **Properties**.
4. On the **Settings** tab, in the **VPN tunneling** area, select **Encrypt all traffic and route to gateway**.
 - If you select **Encrypt all traffic and route to gateway**, all outbound traffic on the client is encrypted and sent to the security gateway but only traffic directed at site resources passes through the gateway. All other traffic is dropped.
 - If you do *not* select **Encrypt all traffic and route to gateway**, only traffic directed at site resources is encrypted and sent to the gateway. All other outbound client traffic passes in the clear.

Tunnel Idleness

If you see a **VPN tunnel has disconnected. Tunnel inactivity timeout reached** message, this means that no traffic has passed between you and the site during a period set in minutes by your system administrator.

Your organization may have specific security requirements, such that an open VPN tunnel should be transporting work-related traffic to the site at all times. An idle or inactive tunnel should be shut down.

A mail program such as OUTLOOK performing a send-receive operation every five minutes would be considered work-related, and the tunnel kept open.

Collecting and Sending Log Files

To troubleshoot unforeseen issues with Endpoint Security, your system administrator may ask you to send log files. Before you can collect and send log files, logging must be enabled.

To enable Logging:

1. Click the **Menu Bar** icon, and select **Display Overview**.
2. Select **VPN Blade > VPN Options**.
3. On the **Advanced** tab, select **Enable Logging**.

To collect and send log files:

1. Click the **Menu Bar** icon, and select **Display Overview**.
2. Clicked **Advanced**.
3. In the **Logging** section, click **Collect**.

Log files are gathered into a single compressed file. The location of the compressed file is shown in an open window. Send the contents of the compressed file to your site administrator.

Chapter 3

Full Disk Encryption

In This Chapter

| | |
|--|----|
| Overview of the Login Screen | 21 |
| Authenticating to Full Disk Encryption | 22 |

Full Disk Encryption combines boot protection with Pre-boot authentication, and strong encryption to ensure that only authorized users are granted access to information stored in desktop and laptop PCs.

Overview of the Login Screen

If your administrator enables Full Disk Encryption, when you log in to your Mac you will get a Pre-boot login screen where you enter your authentication credentials. If you do not enter the correct credentials, you cannot access the Mac.

You also have these options:

- **Remote Help** - Click this if you do not know your password. You and the help desk or administrator will exchange information to recover your password.
- **SSO Options**- Select the SSO Active option to use the same credentials for your OSX login and your Full Disk Encryption login. If you need to log in to OSX with different credentials than the Full Disk Encryption credentials, make sure the SSO Active option is cleared.
- **Keyboard Layout** - To change the keyboard layout to a different language, click on the shaded area that says your keyboard layout, for example, **en-US** or **sv-SE**. You can also press Alt +Shift at this point to switch the keyboard layout to another language.
All keyboard layouts that are loaded in the operating system are supported in the Pre-boot environment.
- **Options** - Click this to:
 - **Virtual Keyboard** - Open an on-screen keyboard to use in the authentication process.
 - **Language** - Change the language of the Pre-boot screen.
 - **Help** - Opens **Help** for more information.
 - **Character Map** - Open a set of Latin characters on-screen that you can use in the authentication process.

Using the Virtual Keyboard

From the Pre-boot page, select **Options > Virtual Keyboard** to open a Virtual Keyboard. You can use the virtual keyboard throughout the authentication.

To close the virtual keyboard, click it again from the **Options** menu.

Using Special Characters

Your user credentials might contain characters that are not easily available on your keyboard. From the Pre-boot screen, you can select **Options > Character Map** to enter characters into the login screen.

To insert a character into a field in the Pre-boot login screen:

1. In the Pre-boot login screen, select **Options > Character Map**.
A set of Latin characters shows on the screen.
2. Click in a field in the login window, for example **User account name**.

3. Click a character from the **Character Map**.

It shows in the selected field.

To change the set of characters that shows:

1. Click the arrow in the top right corner of the **Character Map**.
2. Select a set of characters from the list.

Changing the Language

You can set the Pre-boot to recognize a language other than the default language of your Mac. After you change the language, it is used as the default the next time you authenticate with Full Disk Encryption.

To set the language for the Pre-boot screen:

1. From the Pre-boot screen, select **Options > Language**.
The Language window opens.
2. Select a language and click **OK**.
The Mac restarts automatically.

Authenticating to Full Disk Encryption

This section describes how to authenticate to a computer protected by Full Disk Encryption.

Being authenticated means being verified by Full Disk Encryption as someone who is authorized to use a specified computer. Authentication can happen in one of these ways, depending on the setting configured by your administrator:

- **Pre-boot** - When you turn on or restart a Full Disk Encryption-protected computer, the Pre-boot login screen opens.
Enter a valid user name and password or insert your Smart Card and enter the PIN. Full Disk Encryption verifies that you are authorized to access the computer and lets operating system start.
- **Through a LAN connection** - You authenticate automatically if your computer is connected to a LAN. This is supported on Mac and Windows UEFI systems.
- **Operating System Login** - You bypass Full Disk Encryption authentication and log in to your operating system.



Note - Depending on the settings configured by your administrator, you might not be able to start your operating system in Safe Mode.

Authenticating for the First Time with a Fixed Password

1. Start your Full Disk Encryption-protected computer.
The User Account Identification window opens.
2. Enter your **User account name** and **Password**. The password is obscured with asterisks (*) when entered.
3. Click **OK**.
4. Click **Continue** to close the window.
Full Disk Encryption lets the operating system start.

If You Do Not Have Your Password

If you forget your password or do not have your Smart Card, use **Remote Help** for assistance.

There are two types of Full Disk Encryption Remote Help:

- **One Time Login** - Allows access as an assumed identity for one session, without resetting the password.
- **Remote password change** - Use this option if you use a fixed password and forgot it.

To use Remote Help to log in:

1. Enter your **User account name** and click in the next field.
2. Click **Remote Help**.
The Remote Help Logon window opens.
3. Select either **Password Change** or **One-Time Logon**.
4. Call your administrator or helpdesk to guide you through the process.

Chapter 4

Troubleshooting

In This Chapter

[Technical Difficulties](#)

24

[Collecting Information for Technical Support](#)

24

Technical Difficulties

The policies and settings of your client are determined by your Endpoint Security administrator. The administrator can solve many issues by making changes to your policy and settings.

Collecting Information for Technical Support

Your administrator might tell you **Collect information for technical support**. This tool collects information from your system that technical support can use to resolve issues.

To use the **Collect information for technical support** tool:

1. From the main client window, select **Advanced** and click **Collect information from technical support**.
 - The tool runs.
 - A window opens showing the location of a compressed zip file.
2. Email the zip file to your Technical Support contact.

Index

A

Advanced • 8
Authenticating for the First Time with a Fixed Password • 21
Authenticating to Full Disk Encryption • 21
Authentication • 14
Automatic Certificate Renewal • 17

B

Basic Client Operations • 9

C

Certificate Enrollment and Renewal • 16
Certificate Renewal • 17
Challenge Response • 16
Changing Authentication Schemes • 16
Changing the Language • 21
Checking if the Client is Installed • 5
Collecting and Sending Log Files • 19
Collecting Information for Technical Support • 23
Compliance Alerts • 9
Compliance Blade • 7
Configuring Connection Options • 18
Connecting through a Hotspot • 18
Connecting to the VPN • 12
Creating a VPN Site • 11

D

Disconnecting from a Site • 13

E

Enrolling After Site Creation • 17
Enrolling During Site Creation • 17

F

Firewall Blade • 7
Full Disk Encryption • 20
Full Disk Encryption Blade • 7

G

Getting Started • 5

I

If You Do Not Have Your Password • 21
Important Information • 3
Installing the Client • 5
Introduction to Endpoint Security • 5

M

Menu Bar Icons • 8

O

Opening the Site Wizard Again • 13
Overview of the Login Screen • 20

P

Password Caching for Single Sign-On • 18
Proxy Settings • 18

R

Responding to Alerts • 9

S

Saving the Certificate to a Folder of your Choice • 15
SecurID • 16
Staying Connected all the Time • 18
Storing a Certificate in the Keychain • 15

T

Technical Difficulties • 23
Tour of the Main Client Window • 6
Troubleshooting • 23
Tunnel Idleness • 19

U

Understanding Certificates • 15
Uninstalling the Client • 5
User Name and Password • 14
Using Special Characters • 20
Using the Client • 6
Using the Virtual Keyboard • 20

V

VPN • 11
VPN Alerts • 9
VPN Basics • 11
VPN Blade • 6
VPN Configuration Options • 14
VPN Tunneling • 19