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.

Check Point E80.64
For more about this release, see the home page http://supportcontent.checkpoint.com/solutions?id=sk112793.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=51804.
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

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 E80.64 User Guide.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 November 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# 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 Endpoint Security</td>
<td>5</td>
</tr>
<tr>
<td>Getting Started</td>
<td>5</td>
</tr>
<tr>
<td>Checking if the Client is Installed</td>
<td>5</td>
</tr>
<tr>
<td>Installing the Client</td>
<td>5</td>
</tr>
<tr>
<td>Uninstalling the Client</td>
<td>6</td>
</tr>
<tr>
<td>Using the Client</td>
<td>6</td>
</tr>
<tr>
<td>Tour of the Main Client Window</td>
<td>6</td>
</tr>
<tr>
<td>VPN Blade</td>
<td>7</td>
</tr>
<tr>
<td>Firewall Blade</td>
<td>7</td>
</tr>
<tr>
<td>Compliance Blade</td>
<td>7</td>
</tr>
<tr>
<td>Capsule Docs Blade</td>
<td>8</td>
</tr>
<tr>
<td>Media Encryption Blade</td>
<td>8</td>
</tr>
<tr>
<td>Full Disk Encryption Blade</td>
<td>9</td>
</tr>
<tr>
<td>Advanced</td>
<td>9</td>
</tr>
<tr>
<td>Menu Bar Icons</td>
<td>10</td>
</tr>
<tr>
<td>Basic Client Operations</td>
<td>11</td>
</tr>
<tr>
<td>Responding to Alerts</td>
<td>11</td>
</tr>
<tr>
<td>VPN</td>
<td>13</td>
</tr>
<tr>
<td>VPN Basics</td>
<td>13</td>
</tr>
<tr>
<td>Creating a VPN Site</td>
<td>13</td>
</tr>
<tr>
<td>Connecting to the VPN</td>
<td>15</td>
</tr>
<tr>
<td>Disconnecting from a Site</td>
<td>15</td>
</tr>
<tr>
<td>Opening the Site Wizard Again</td>
<td>16</td>
</tr>
<tr>
<td>VPN Configuration Options</td>
<td>17</td>
</tr>
<tr>
<td>Authentication</td>
<td>17</td>
</tr>
<tr>
<td>Configuring Connection Options</td>
<td>21</td>
</tr>
<tr>
<td>Collecting and Sending Log Files</td>
<td>23</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>24</td>
</tr>
<tr>
<td>Overview of the Login Screen</td>
<td>24</td>
</tr>
<tr>
<td>Using the Virtual Keyboard</td>
<td>24</td>
</tr>
<tr>
<td>Using Special Characters</td>
<td>24</td>
</tr>
<tr>
<td>Changing the Language</td>
<td>25</td>
</tr>
<tr>
<td>Authenticating to Full Disk Encryption</td>
<td>25</td>
</tr>
<tr>
<td>Making Sure that No One Tampered with your Computer</td>
<td>26</td>
</tr>
<tr>
<td>Authenticating for the First Time with a Fixed Password</td>
<td>26</td>
</tr>
<tr>
<td>If You Do Not Have Your Password</td>
<td>26</td>
</tr>
<tr>
<td>Media Encryption</td>
<td>27</td>
</tr>
<tr>
<td>Encrypting Media</td>
<td>27</td>
</tr>
<tr>
<td>Media Encryption Offline Access Utility</td>
<td>28</td>
</tr>
<tr>
<td>Uninstalling the Media Encryption Offline Utility</td>
<td>28</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>29</td>
</tr>
<tr>
<td>Technical Difficulties</td>
<td>29</td>
</tr>
<tr>
<td>Collecting Information for Technical Support</td>
<td>29</td>
</tr>
</tbody>
</table>
Introduction to Endpoint Security

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
- Remote Access VPN
- Media Encryption
- Secure Mobile Document Viewer

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

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

Installing the Client

Get the Endpoint Security client zip file from your administrator.

1. Double-click the ZIP file to expand it.
2. Click the APP file that shows next to the zip file.
   The Check Point Endpoint Security Installer opens.
3. Click Install.
4. Enter a Name and Password to authorize the installation.
5. Click OK.
   Wait while package installs.
6. 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, to decrypt HFS volumes. 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.

If your client is not **Compliant**, open the **Compliance Detail** pane from the main client window to see actions required to become compliant again.

The **Compliance Detail** pane includes:

• **Policy Details** - A summary of the Compliance policy that is installed on your Mac.

• **Current Status** - A **Message** about each problem.

---

**Capsule Docs Blade**

The Capsule Docs blade, Alpha, is available from E80.60.

Capsule Docs lets you view and unprotect documents, according to the permissions granted by the document author.

Double-click a protected document to open it. If you have the required permissions, the document opens in the Capsule Docs Viewer application.

These are the different types of permissions you can have for a document:

• You cannot open or view the document.

• You can view the document, but you cannot save, edit, or share the document. If you try to do an action for which you have no permission, a message opens.

• You can view and unprotect the document. You can edit and share an unprotected document.

**To unprotect a document:**

1. Find the **Capsule Docs** menu.

   When you open a protected document, if you have permission to unprotect it, a Capsule Docs menu shows in the menu bar.

2. From the **Capsule Docs** menu, click **Unprotect Document**.

   The document saves as unprotected and opens in its native application.

**Capsule Docs Preferences:**

The Capsule Docs **Preferences** window shows the servers that your Capsule Docs client worked with. Each server has a descriptive icon to show what kind of server it is: **Cloud**, **On-Premises**, or **External**. You can log out from Cloud or External servers, but not from an On-Premises server.

---

**Media Encryption Blade**

Click **Media Encryption** and the **Media Encryption Detail** pane opens. This shows the policy installed and a list of removable devices that are inserted in your computer. If you click a device from the list you can create encrypted storage on the device or remove encryption from the device.

The Media Encryption policy determines how you can use external devices that connect to your computer. Media Encryption can encrypt, and decrypt external devices. The display shows the status of external devices connected to your computer.
Click Media Encryption and the Media Encryption Detail pane opens with this information:

- **Policy Details** - A summary of the Media Encryption policy that is installed on your computer.
- **Detected Removable Devices** - Shows the status of devices attached to your computer. It includes these details:
  - **Device** - The type of device.
  - **Size** - The amount of storage space on the device.
  - **Encryption Status** - If the device is encrypted or not. Only someone with permissions can view files on an encrypted device.
- **Create Encrypted Storage** - Click this to create an encrypted storage device.
- **Remove Encryption** - Click this to remove encryption from a device.

If you have the necessary permissions, you can encrypt devices and access encrypted devices on a computer without Media Encryption.

**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.

![Endpoint Security Client](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Version</th>
<th>Date</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Restricted</td>
<td>Firewall</td>
<td>3</td>
<td>07/02/12 13:20</td>
<td>Restricted</td>
</tr>
<tr>
<td>Check Point Restricted policy</td>
<td>Zone Definition</td>
<td>1</td>
<td>06/28/12 19:05</td>
<td>Restricted</td>
</tr>
<tr>
<td>Default Compliance settings for the entire organization</td>
<td>Compliance</td>
<td>6</td>
<td>07/10/12 16:36</td>
<td>Connected</td>
</tr>
</tbody>
</table>

- **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 an icon to access a shortcut menu.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="VPN icon" /></td>
<td>VPN not installed.</td>
</tr>
<tr>
<td><img src="image" alt="VPN connected icon" /></td>
<td>VPN connected.</td>
</tr>
<tr>
<td><img src="image" alt="VPN connecting icon" /></td>
<td>VPN connecting.</td>
</tr>
<tr>
<td><img src="image" alt="VPN disconnected icon" /></td>
<td>VPN disconnected.</td>
</tr>
<tr>
<td><img src="image" alt="Full Disk Encryption icon" /></td>
<td>Full Disk Encryption or Media Encryption are encrypting or decrypting.</td>
</tr>
<tr>
<td><img src="image" alt="Fully connected icon" /></td>
<td>VPN is not installed or not running.</td>
</tr>
<tr>
<td><img src="image" alt="Full Disk Encryption connected icon" /></td>
<td>Full Disk Encryption or Media Encryption are encrypting or decrypting while VPN is connected.</td>
</tr>
<tr>
<td><img src="image" alt="Full Disk Encryption disconnected icon" /></td>
<td>Full Disk Encryption or Media Encryption are encrypting or decrypting while VPN is disconnected.</td>
</tr>
<tr>
<td><img src="image" alt="Warning icon" /></td>
<td>Warning that requires you to take action, for example, a Compliance issue.</td>
</tr>
<tr>
<td><img src="image" alt="Warning with flashing light icon" /></td>
<td>Icon with a flashing light. An error has occurred that requires you to take action:</td>
</tr>
<tr>
<td></td>
<td>• Compliance restriction</td>
</tr>
<tr>
<td></td>
<td>• One or more blades is not running</td>
</tr>
<tr>
<td></td>
<td>• One or more blades in a state of error</td>
</tr>
</tbody>
</table>

If you are not sure what to do, contact your system administrator.
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>Opens the Help page in the browser.</td>
</tr>
<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>Display Overview</td>
<td>Opens the main client window.</td>
</tr>
<tr>
<td>Quit</td>
<td>Closes the GUI.</td>
</tr>
</tbody>
</table>

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 to the policy defined by your administrator for the restricted state.
**Media Encryption Alerts**

If you have the Media Encryption blade as part of your Endpoint Security, you might see alerts related to encryption. Follow the on-screen instructions.
VPN

In This Section:

VPN Basics .................................................................................................................... 13
VPN Configuration Options .......................................................................................... 17

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 a 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 17).

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 17)
- Configuring Connection Options (on page 21)
- Collecting and Sending Log Files (on page 23)

**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 19).

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, select an option from the **Authentication Method** list:
   - Username and password
   - Certificate - keychain
   - Certificate - P12
   - SecurID - Keyfob
   - SecurID - PinPad
   - 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 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.
Full Disk Encryption

In This Section:
- Overview of the Login Screen ...................................................................... 24
- Authenticating to Full Disk Encryption .......................................................... 25

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.
Making Sure that No One Tampered with your Computer

If you did not personally start the Mac yourself, you should always restart before authenticating. This makes sure that your computer has not been tampered with, and that your user account name and password cannot be hijacked.

Authenticating for the First Time with a Fixed Password

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.
3. Select either Password Change or One-Time Logon.
4. Call your administrator or helpdesk to guide you through the process.
Media Encryption

In This Section:

Encrypting Media .......................................................................................................... 27

This section describes the process of encrypting, decrypting and managing removable storage devices. Media Encryption secures a removable storage device by encrypting some or all of the storage device. It then puts the specified files (typically business data) on the encrypted device.

To work with Media Encryption, from the Endpoint Security Main Page, click Media Encryption.

The Media Encryption Details window opens, showing removable storage devices that are attached to your computer.

Encrypting Media

Media Encryption lets you create encrypted storage on removable storage devices that contains business related data. After you create the encrypted storage, you will see two drives in the Finder window. One drive is encrypted for business data. The other drive is not encrypted and can be used for non-business data.

If you have the required permissions you can:

- Define a password that gives users full access to the encrypted drive through an offline tool. This tool works on Mac or Windows computers that do not have an Endpoint Security client installed, or that have Endpoint Security installed but are not connected to the Endpoint Security Management Server.

- Define the percentage of the physical device to be encrypted. For example, if you encrypt 50% of a device, the encrypted [business data] drive will occupy 50% of the physical device. The remainder is assigned to non-encrypted [non-business data] drive. When you import and encrypt files, they are always put on the business data drive.

⚠️ Important -

- Media Encryption has no way of detecting hardware faults on external drives. For this reason, the encrypted drive might be created on a damaged section of the external drive, resulting in unexpected data loss.

  We strongly recommend that you back up all files and data stored on an external device (such as HDD, USB or other flash-based device), before encrypting the device. See sk44844 http://supportcontent.checkpoint.com/solutions?id=sk44844.

- We recommend that you do not encrypt non-computer external devices such as: digital cameras, Smartphones, MP3 players, and the like. Do not encrypt removable media that can be inserted in or connected to such devices.

نسخ - If you define a drive that is smaller than the volume of data you want to encrypt, the encryption procedure fails.
To encrypt a new storage device:

1. Insert a removable storage device into your computer.
2. From Media Encryption, select a device and click Create Encrypted Storage. The Removable Disk Encryption window opens. The options shown are set by your administrator. You can also encrypt and decrypt devices.
3. In the Removable Disk Encryption window, configure the available options. If you do not see an option, that option is not allowed by your policy.
   - Set a password to allow full access to the device while online (connected to your network) and offline.
   - Select a percentage of the storage device to encrypt.
4. Click Encrypt.
5. A window shows the encryption progress. Based on the type of storage device and the quantity of data, this process may take a long time.
   Important - Do NOT remove the storage device during the encryption process. This will destroy your data and may damage the storage device.
6. When the Finish window opens, click Finish to complete the process.

The encrypted storage device status now appears as Encrypted in the Media Encryption window. Non-business data is not changed, deleted or encrypted. It remains on the non-encrypted device.

Media Encryption Offline Access Utility

The Media Encryption Offline Access Utility for Mac lets you:

- Read information on devices encrypted with Media Encryption for Windows or Mac.
- Write to removable media devices (this depends on the type of removable media device and on the security policy used when encrypting the device). Information that you add to the device becomes encrypted.

Note: The utility does not encrypt previously unencrypted removable devices with the Media Encryption for Mac component.

Download the utility from the release homepage [http://supportcontent.checkpoint.com/solutions?id=sk112793].

The Media Encryption Offline Access Utility for Mac and the Media Encryption blade cannot both be installed on a device at the same time.

Uninstalling the Media Encryption Offline Utility

To uninstall:

1. Open a Terminal window
2. Run

   sudo /Library/Application\Support/Checkpoint/MediaEncryption/uninstall.sh
Troubleshooting

In This Section:

Technical Difficulties .......................................................................................................................... 29
Collecting Information for Technical Support .................................................................................. 29

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.