30 December 2018

ENDPOINT SECURITY
CLIENT FOR MAC
E80.89
for Mac

User Guide
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 Endpoint Security Releases**
For more about this release, see the Endpoint Security home page

**Latest Version of this Document**
Download the latest version of this document
To learn more, visit the Check Point Support Center

**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 Help.

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 December 2018</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>6</td>
</tr>
<tr>
<td>- Ransomware Detection</td>
<td>6</td>
</tr>
<tr>
<td>- Using the Client</td>
<td>7</td>
</tr>
<tr>
<td>- Menu Bar Icons</td>
<td>7</td>
</tr>
<tr>
<td>- Checking if the Client is Installed</td>
<td>7</td>
</tr>
<tr>
<td>- Installing the Client</td>
<td>8</td>
</tr>
<tr>
<td>- Uninstalling the Client</td>
<td>8</td>
</tr>
<tr>
<td>Tour of the Main Client Window</td>
<td>9</td>
</tr>
<tr>
<td>- Basic Client Operations</td>
<td>10</td>
</tr>
<tr>
<td>Remote Access VPN</td>
<td>11</td>
</tr>
<tr>
<td>- VPN Options</td>
<td>11</td>
</tr>
<tr>
<td>- VPN Basics</td>
<td>11</td>
</tr>
<tr>
<td>- Creating a VPN Site</td>
<td>12</td>
</tr>
<tr>
<td>- Connecting to the VPN</td>
<td>13</td>
</tr>
<tr>
<td>- Disconnecting from a Site</td>
<td>14</td>
</tr>
<tr>
<td>- Opening the Site Wizard Again</td>
<td>14</td>
</tr>
<tr>
<td>- VPN Configuration Options</td>
<td>15</td>
</tr>
<tr>
<td>- Authentication</td>
<td>15</td>
</tr>
<tr>
<td>- Configuring Connection Options</td>
<td>20</td>
</tr>
<tr>
<td>- Collecting and Sending Log Files</td>
<td>22</td>
</tr>
<tr>
<td>Help Windows</td>
<td>23</td>
</tr>
<tr>
<td>- Connection Window</td>
<td>23</td>
</tr>
<tr>
<td>- Connecting with a User Name and Password</td>
<td>23</td>
</tr>
<tr>
<td>- Connecting with a Keychain Certificate</td>
<td>24</td>
</tr>
<tr>
<td>- Connecting with a p12 Certificate</td>
<td>24</td>
</tr>
<tr>
<td>- Connecting with a SecurID KeyFob</td>
<td>25</td>
</tr>
<tr>
<td>- Connecting with a SecurID PinPad</td>
<td>25</td>
</tr>
<tr>
<td>- Connecting with Challenge-Response</td>
<td>25</td>
</tr>
<tr>
<td>- Certificate Authentication</td>
<td>26</td>
</tr>
<tr>
<td>- Enrolling</td>
<td>26</td>
</tr>
<tr>
<td>- Renew Certificate</td>
<td>27</td>
</tr>
<tr>
<td>- VPN Options - Sites tab</td>
<td>27</td>
</tr>
<tr>
<td>- VPN Options - Advanced Tab</td>
<td>27</td>
</tr>
<tr>
<td>- Site Properties - Details</td>
<td>28</td>
</tr>
<tr>
<td>- Site Properties - Settings</td>
<td>28</td>
</tr>
<tr>
<td>- Proxy Settings</td>
<td>29</td>
</tr>
<tr>
<td>- Site Wizard</td>
<td>30</td>
</tr>
<tr>
<td>- Site Wizard SecurID Authentication</td>
<td>30</td>
</tr>
<tr>
<td>Firewall</td>
<td>31</td>
</tr>
<tr>
<td>- Disabling the Firewall</td>
<td>31</td>
</tr>
<tr>
<td>Compliance</td>
<td>32</td>
</tr>
<tr>
<td>Capsule Docs</td>
<td>33</td>
</tr>
<tr>
<td>Media Encryption</td>
<td>34</td>
</tr>
<tr>
<td>- Media Encryption Options</td>
<td>34</td>
</tr>
<tr>
<td>- Encrypting Media</td>
<td>34</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Native Encryption Management</td>
<td>36</td>
</tr>
<tr>
<td>Native Encryption Management Options</td>
<td>36</td>
</tr>
<tr>
<td>Threat Emulation</td>
<td>37</td>
</tr>
<tr>
<td>Anti-Ransomware</td>
<td>38</td>
</tr>
<tr>
<td>Options</td>
<td>38</td>
</tr>
<tr>
<td>Ransomware Detection</td>
<td>39</td>
</tr>
<tr>
<td>Anti-Ransomware Files</td>
<td>39</td>
</tr>
<tr>
<td>Anti-Ransomware Restoration</td>
<td>40</td>
</tr>
<tr>
<td>Advanced</td>
<td>41</td>
</tr>
<tr>
<td>Responding to Alerts</td>
<td>42</td>
</tr>
<tr>
<td>VPN Alerts</td>
<td>42</td>
</tr>
<tr>
<td>Compliance Alerts</td>
<td>42</td>
</tr>
<tr>
<td>Threat Emulation Alerts</td>
<td>43</td>
</tr>
<tr>
<td>Anti-Ransomware Alerts</td>
<td>43</td>
</tr>
<tr>
<td>Media Encryption Alerts</td>
<td>43</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>44</td>
</tr>
<tr>
<td>Technical Difficulties</td>
<td>44</td>
</tr>
<tr>
<td>Collecting Information for Technical Support</td>
<td>44</td>
</tr>
<tr>
<td>Index</td>
<td>45</td>
</tr>
</tbody>
</table>
Introduction to Endpoint Security

In This Section:

- Ransomware Detection ................................................................. 6
- Using the Client ............................................................................... 7
- Menu Bar Icons ............................................................................... 7
- Checking if the Client is Installed ................................................... 7
- Installing the Client ......................................................................... 8
- Uninstalling the Client .................................................................... 8

Check Point Endpoint Security™ combines all essential components for total security on the endpoint. It includes these blades:

- Remote Access VPN
- Firewall for desktop security
- Compliance
- Media Encryption
- Native Encryption Management
- Threat Emulation
- Anti-Ransomware
- Capsule Docs

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

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.

Ransomware Detection

SandBlast Agent creates honeypot files on client computers. It stops the attack immediately after it detects that the ransomware modified the files.

On Windows, the files are in folders that SandBlast Agent creates under C:\Users.

You can identify these folders by the lock icon that is associated with the name of the folder. For example

- Check Point Protection File Do Not Erase

If a file is deleted, it is automatically recreated after the next system boot.

To learn more, see Anti-Ransomware Files (on page 39).
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.

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>![VPN]</td>
<td>VPN not installed.</td>
</tr>
<tr>
<td>![VPN]</td>
<td>VPN connected.</td>
</tr>
<tr>
<td>![VPN]</td>
<td>VPN connecting.</td>
</tr>
<tr>
<td>![VPN]</td>
<td>VPN disconnected.</td>
</tr>
<tr>
<td>![Full Disk Encryption]</td>
<td>Full Disk Encryption encrypting or decrypting.</td>
</tr>
<tr>
<td>![VPN]</td>
<td>VPN is not installed or running.</td>
</tr>
<tr>
<td>![Full Disk Encryption]</td>
<td>Full Disk Encryption encrypting or decrypting while VPN is connected.</td>
</tr>
<tr>
<td>![Full Disk Encryption]</td>
<td>Full Disk Encryption encrypting or decrypting while VPN is disconnected.</td>
</tr>
<tr>
<td>![Warning]</td>
<td>Warning that requires you to take action, for example compliance issue.</td>
</tr>
<tr>
<td>![Warning]</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 features is not running</td>
</tr>
<tr>
<td></td>
<td>• One or more features is in an error state</td>
</tr>
</tbody>
</table>

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

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:
   
   ```sh
   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.
Tour of the Main Client Window

In This Section:

Basic Client Operations................................................................................................ 10

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 features you see depends on settings defined by your administrator.

- Click on a feature 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.
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>
Remote Access VPN

In This Section:

- VPN Options .................................................................................................................. 11
- VPN Basics ..................................................................................................................... 11
- VPN Configuration Options .......................................................................................... 15
- Help Windows ............................................................................................................... 23

Endpoint Security lets you easily set up a secure VPN to connect to your corporate resources. The display shows the state of the VPN (Connected, Disconnected, Connecting, or Disconnecting) and its default site.

VPN Options

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.

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 VPN 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.

![Site Wizard](image)

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 (on page 15).

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 **VPN**.

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 15)
- Configuring Connection Options (on page 20)
- Collecting and Sending Log Files (on page 22)

**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 [on page 18].

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.
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 **VPN**.
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 > 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 > 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.
**Smart Card Removal**

If you are authenticating using a Smart Card, and the smart card or smart reader is removed from the USB port, the client detects that the certificate is no longer available and disconnects from the site. A **VPN tunnel has disconnected. Smart card was removed** message is displayed.

**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 > 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.
Help Windows

Connection Window

In the Connect window you authenticate to the VPN. Based on the settings that your administrator configures, you might have options to choose a Site and Gateway, or only a Site.

In the Connect Window:

1. In **Site**, select the site to connect to.
   
   If you were not instructed differently by your administrator, connect to the default site.

2. Enter authentication credentials:
   
   - If you have a **Certificate**, browse to the certificate file and enter 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**, enter the first key. When the challenge comes, enter the response.

3. Click **Connect**.

Getting Here -

Connecting with a User Name and Password

**What can I do here?**

In this window you can connect to a VPN site with user name and password authentication.
Tell me about the fields.
- **Site**: Select a VPN site from the list.
- **User name**: Enter your user name.
- **Password**: Enter your password.

**Getting Here** - Click the client icon in the menu bar > **Connect**

## Connecting with a Keychain Certificate

**What can I do here?**
In this window you can connect to a VPN site with a Keychain certificate.

Tell me about the fields.
- **Site**: Select a VPN site from the list.
- **Certificate**: Select a certificate from the list.
- To create a new site, select **New Site** from the list to open the **Site Wizard**.

**Getting Here** - Click the client icon in the menu bar > **Connect**

## Connecting with a p12 Certificate

**What can I do here?**
In this window you can enter your p12 certificate password or change your certificate.

Tell me about the fields.
- **Site**: Select a VPN site from the list.
- **Certificate File**: Click **Browse** to navigate to and select a different p12 certificate.
- **Password**: Enter the password of the selected p12 certificate.

**Getting Here** - Click the client icon in the menu bar > **Connect**
Connecting with a SecurID KeyFob

**What can I do here?**
You can connect to a VPN site with a SecurID KeyFob.

**What background information do I need?**
A KeyFob is a small hardware device with built-in authentication mechanisms that control access to network resources. The user first enters his personal PIN into the KeyFob. The KeyFob then displays a one-time password, a **token code**, which grants access to the network.

**Tell me about the fields.**
- **Site**: Select a VPN site from the list.
- **User name**: Enter your user name.
- **PIN**: Enter your SecurID KeyFob PIN.
- **Token Code**: Enter the token code shown on your KeyFob.

Getting Here - Click the client icon in the menu bar > Connect

Connecting with a SecurID PinPad

**What can I do here?**
You can connect to a VPN site with a SecurID PinPad.

**Tell me about the fields.**
- **Site**: Select a VPN site from the list.
- **User name**: Enter your user name.
- **Passcode**: Enter the passcode displayed on your PinPad.

Getting Here - Click the client icon in the menu bar > Connect

Connecting with Challenge-Response

**What can I do here?**
You can log on to a VPN site with challenge/response authentication.
Tell me about the fields.

- **Site**: Select a VPN site from the list.
- **User name**: Enter your user name.

Enter your response to the challenge question as presented.

---

**Getting Here** - Click the client icon in the menu bar > Connect

---

**Certificate Authentication**

**What can I do here?**

In this window you can configure how the Client gets certificates for authentication.

**What background information is necessary?**

The Client can access the p12 certificate directly, or retrieve it from the Keychain store.

Tell me about the Fields...

- **Select certificate from hardware or software token (Keychain)**
  The Client retrieves a certificate from the Keychain store.

- **Use certificate from Public-Key Cryptographic Standard (PKCS#12) file**
  Browse to a certificate stored in a folder or removable media.

- **If you don’t have a certificate yet**
  Enroll with the Certificate Authority to receive a certificate. Make sure you have the Registration Key and password from the system administrator.

---

**Enrolling**

**What can I do here?**

In this window you can get a certificate from the Certificate Authority.

**What background information do I need to know?**

Enroll to apply for and receive a certificate from Check Point’s Internal Certificate Authority. You must get the registration key from the system administrator to complete authentication.

Tell me about the fields...

- **Site**: Select a VPN site from the list.
- **Provider**: Select the Cryptographic Service Provider (CSP) for Keychain certificate storage.
- **Registration Key**: Enter the certificate registration key supplied by your system administrator.
Renew Certificate

What can I do here?
Connect to a VPN gateway to renew your certificate.

What background information do I need to know?
You must have the password (for P12 certificates) from your system administrator and the registration key.

Tell me about the fields...
- Method - Select Certificate - Keychain or Certificate - P12
  If you do not know which to select, ask your system administrator.

VPN Options - Sites tab

What can I do here?
In this window, you can define and manage connections to VPN sites.

What background information do I need to know?
Each site represents a unique VPN connection, as defined by the system administrator.
You can define multiple sites. You must authenticate to each site to connect to its VPN.

VPN Options - Advanced Tab

What can I do here?
Use this tab to:
- Download VPN activity log files to your client computer
• Configure proxy server settings for your client

**What background information do I need to know?**

**Proxy** - In some locations, a proxy server sits between clients and the Internet. If you know the IP address of the proxy server, you can configure Endpoint Security VPN to go through the proxy server to the VPN.

**Tell me about the fields.**

• **Collect logs**  
  Select **Enable logging** to create activity logs for VPN.  
  Click **Collect Logs** to download the logs as one file. Your system administrator will tell you how to send the file for troubleshooting.

• **Change the current proxy settings**  
  Click to configure the local proxy.

• **Choose the interface language**  
  Select a language to change the fields and window names.

---

**Getting Here** - Click the client icon in the menu bar > **VPN Options** > **Advanced** tab

**Site Properties - Details**

**What can I do here?**

In this window you can see the details of the selected VPN connection.

This window shows:

• Name of the site

• IP address

• Date and time of last connection

• Last office mode IP address (if applicable)

---

**Getting Here** - Click the client icon in the menu bar > **VPN Options** > **Sites** tab > Select site > **Properties** > **Details** tab

**Site Properties - Settings**

**What can I do here?**

Use this window to configure connection settings for the selected site. The connection behavior and authentication method are based on these settings. You might not have all the options available.
Tell me about the fields...

- **Enable Always-Connect** - Automatically connect again if the connection stops.

- **VPN Tunneling**
  - **Encrypt all traffic and route to gateway** - Encrypt all traffic. This can cause browsing on public sites to be slower or restricted, but it is more secure.

- **Authentication scheme** - Select an authentication method for traffic routed to the gateway from the list. Make sure that you have the credentials needed if you change this field. Consult with your system administrator.

- **Import** - Import a certificate to the Keychain store. This is easier to manage, but anyone can access the VPN if they access your computer.

- **Enroll** - Receive a new certificate. Make sure you have the registration key and password.

- **Renew** - Renew existing certificates. Make sure you have the registration key and password.

---

**Getting Here** - Click the client icon in the menu bar > VPN Options > Sites tab > Select site > Properties > Settings tab

---

**Proxy Settings**

**What can I do here?**
Use this window to configure client proxy settings.

**What background information do I need to know?**
In most cases, the proxy server in a remote location is detected automatically.

Tell me about the fields

- **No proxy** - default

- **Detect proxy from System Preferences settings**
  - When this option is selected, the Client uses proxy settings as defined in your System Preferences.
  - To see the settings there, select: System Preferences > Network > Advanced > Proxies.

- **Manually define proxy**
  - If the proxy settings cannot be automatically detected, enter the IP address and port number of the proxy as supplied by your system administrator.

- **Proxy Authentication**
  - Get a valid user name and password from your system administrator. This user name and password lets you authenticate to the proxy server.

---

**Getting Here** - Click the client icon in the menu bar > VPN Options > Advanced tab > Proxy Settings
Site Wizard

What can I do here?
Use this wizard to define a VPN site and to select an authentication method.

What background information do I need to know?
The authentication confirms your identity for connection to a VPN site.

Tell me about the fields...

• **Server address or Name**
  Enter the IP address or DNS name of the VPN gateway.

• **Display name**
  Enter a site name to show in Client windows. (Optional)

• **User Name and Password**
  Enter the user name and password assigned by your system administrator.

• **Certificate**
  Select this option if you use p12 certificates (Keychain or p12 files) or hardware tokens.

• **SecurID**
  Select this option if you use one of the SecurID authentication methods. SecurID authentication mechanisms consist of a KeyFob or PinPad that generates an authentication code at fixed intervals.

If the Site Wizard fails to connect to the site, click Back and make sure that:

• You entered the correct IP address or DNS name for the site.
• You are using the correct authentication method for your site.

Getting Here - Click the client icon in the menu bar > VPN Options > Sites > New

Site Wizard SecurID Authentication

What can I do here?
In this window, select your SecurID device.

Select one of these options:

• KeyFOB hardware token
• PinPad hardware token

Getting Here - In the Site Wizard, select the SecurID authentication method.
Firewall

In This Section:
Disabling the Firewall ..................................................................................................31

The firewall protects the ports through which Internet traffic flows. The Endpoint Security administrator sets the policies and rules that determine what traffic the firewall allows.

The display shows the status of your firewall.

Click Firewall. The Detail pane opens. This pane shows Policy Details - a summary of the Firewall policies installed on your Mac.

Disabling the Firewall

Your administrator can give you the option to disable the firewall on your computer. If you do have this option, when you right-click the Endpoint Security VPN icon in the system tray, one of the choices is Disable Security Policy.

If you select this, the firewall is disabled. Depending on the compliance settings, you might not be able to connect to the VPN if your firewall is disabled.

If the firewall is disabled, the option Enable Security Policy shows in the right-click menu of the Client icon. Select this to enable the firewall.
Compliance

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

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

In This Section:
- Media Encryption Options ................................................................. 34
- Encrypting Media ............................................................................... 34

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. This shows removable storage devices that are attached to 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.

Media Encryption Options

Click Media Encryption and the Media Encryption Details 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.

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.

  **Note** - 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.
Native Encryption Management

In This Section:

Native Encryption Management Options..........................................................36

Native Encryption Management uses Pre-boot authentication provided by FileVault, the native OS encryption from Apple. It ensures that only authorized users can access desktops and laptops. If you have Native Encryption Management installed, you must enter a password to start your Mac. Until you are authenticated, all information on the Mac is encrypted.

Native Encryption Management Options

Click Native Encryption Management and the Native Encryption Management Detail pane opens. This pane shows:

- **Policy Details** - Details of the Native Encryption Management and OneCheck User Settings policies that are installed on your Mac.

- **Current Status** - A summary of the Native Encryption Management 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 Native Encryption Management account.
Threat Emulation

Threat Emulation detects zero-day and unknown attacks. Files on your computer are sent to a testing area for emulation to detect malicious files and content.

From the Endpoint Security Main Page, click **Threat Emulation** to see options.

The status is shown to the right of the name:

- **On** - Working normally.
- **Off** - Disabled by the policy.
- **Initializing** - In startup mode.
- **Warning** - Low disk space.
- **Error** – Very low disk space (stops sensors recording).

The **Infections** table shows incidents that Threat Emulation detected. Click an incident ID to open a report.
Anti-Ransomware

In This Section:

Options ........................................................................................................................................... 38
Ransomware Detection .................................................................................................................. 39
Anti-Ransomware Files .................................................................................................................. 39
Anti-Ransomware Restoration ....................................................................................................... 40

Anti-Ransomware monitors file operations, processes, and network activity for suspicious
behavior.

It also analyzes attacks detected by other client features or the Check Point gateway.

In the Endpoint Security Main Page, you can see a list of incidents and click the incident to get
more information.

If a Ransomware attack occurs, you can restore your original files and delete encrypted files
created by the attack. Your administrator might do this automatically.

Best practice is to speak with your technical support before you do the Anti-Ransomware
Restoration procedure.

Options

From the Endpoint Security Main Page, click Anti-Ransomware to see details.

The status shows to the right of the name:

- **On** - Working normally.
- **Off** - Disabled by the policy.
- **Initializing** - In startup mode.
- **Warning** - Low disk space.
- **Error** - Very low disk space (stops sensors recording).

You can see the functionality below the name:

- **Monitoring/Analyzed x cases**
- **Not monitoring** (the feature is Off)
- **Insufficient disk space** (in warning/error state)
- **Analyzing**

More information available:

- **Policy Details** - The enforced policy.
- **Current Status** – Data about the monitoring process.
  - **Disk Space Usage** - The amount of data that is saved on the computer.
  - **Monitor Duration** - The period of time included in the saved data.
- **Analyzed cases** – A list of the incidents that Anti-Ransomware has examined, including ID,
  Source, Type, Description, and Date.
From the Analyzed cases list:

- Click the Incident ID to open the report from ThreatCloud in PDF format.
- Right-click an incident to delete it.
- Click Restore Files to restore files after a Ransomware attack. This might not be necessary if your administrator restored the files automatically.

Ransomware Detection

SandBlast Agent creates honeypot files on client computers. It stops the attack immediately after it detects that the ransomware modified the files.

On Windows, the files are in folders that SandBlast Agent creates under C:\Users.

You can identify these folders by the lock icon that is associated with the name of the folder. For example

![Check-PointProtectionFilesDo NetErase](image)

If a file is deleted, it is automatically recreated after the next system boot.

To learn more, see Anti-Ransomware Files [on page 39].

Anti-Ransomware Files

Anti-Ransomware creates honeypot files on client computers. It stops the attack immediately after it detects that the ransomware modified the files.

The files are in these folders that Anti-Ransomware creates:

- C:\Users\Public\Music
- C:\Users\<User>\Music (MyMusic)
- C:\Users\Public\Documents
- C:\Users\<User>\Documents (MyDocuments)
- C:\Users\Public\Videos
- C:\Users\<User>\Videos (MyVideos)
- C:\Users\Public\Pictures
- C:\Users\<User>\Pictures (MyPictures)

You can identify these folders by the lock icon that is associated with the name of the folder. For example

![Check-PointProtectionFilesDo NetErase](image)

The file names include these strings, or similar:

- CP
- CheckPoint
- Check Point
- Check-Pont
- Sandblast Agent
- Sandblast Zero-Day
- Endpoint

You can open and look at the files. They are real documents, images, videos, and music.

If a file is deleted, it is automatically recreated after the next system boot.
Anti-Ransomware Restoration

In the report from ThreatCloud, you can see details of the files that were restored when running the Anti-Ransomware Restoration Wizard:

- See which files will be restored in the **Business Impact** section.
- See which files will be deleted in the **Remediation** section.

To run Anti-Ransomware restoration from a client computer:

1. Right-click the Endpoint Security icon in the taskbar notification area and select **Display Overview**.
   
   The **Endpoint Security Main Page** opens.

2. Click **Anti-Ransomware**.

3. In the **Analyzed cases** table, click **Restore Files** in the row of the relevant incident.
   
   The **Anti-Ransomware Restoration** windows open.

4. Click **Restore** to start the restoration process.
   
   If you see a note that the files were already restored, click **Cancel**. It is not necessary to restore the files again.

5. In the **Restore Step 1 of 2** window:
   a) Select the location to place the restored files:
      
      - **Restore files to the original location** (default)
      - **Restore to selected location** - If you select this, you are prompted to select the location.

   b) **Delete files created by the attack, including encrypted files** - This is selected by default. Clear it if you do not want to delete the files.

   c) Click **Next**.

6. In the **Restore Step 2 of 2** window, click **Restore** to start the process.
   
   The Endpoint Security Restoration window opens and shows the files that were restored and where they are located.

7. Click **Close**.
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.

- **Logging**
  Collects logs for technical support.
Responding to Alerts

In This Section:

- VPN Alerts
- Compliance Alerts
- Threat Emulation Alerts
- Anti-Ransomware Alerts
- Media Encryption 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
- Features - 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.
Threat Emulation Alerts

Threat Emulation and Forensics always analyze files on your computer.

If you see a message that a threat was detected or quarantined, you do NOT need to do anything. Your Endpoint Security client works automatically to protect you from threats and your administrator will see the related logs.

To see more information about the incident, you can:

1. Right-click the Endpoint Security icon in the taskbar notification area and select Display Overview.
   The Endpoint Security Main Page opens.
2. Click the feature that showed the alert.
3. Click an Incident ID in the table to open a report.

Anti-Ransomware Alerts

Anti-Ransomware Alerts show that a potential ransomware attack occurred.

Contact your technical support for more information.

Media Encryption Alerts

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

In This Section:

- Technical Difficulties ............................................................................................................. 44
- Collecting Information for Technical Support ......................................................................... 44

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.