5 December 2017

ENDPOINT SECURITY
CLIENT
E80.71 FOR WINDOWS

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 E80.71
For more about this release, see the E80.71 home page http://supportcontent.checkpoint.com/solutions?id=sk119676.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=56989.
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 E80.71 for Windows User Guide.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 Dec 2017</td>
<td>Added <em>Ransomware Detection</em> on page 7 and <em>Anti-Ransomware Files</em> on page 34</td>
</tr>
<tr>
<td>29 Nov 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Contents

Important Information ................................................................................................... 3
Introduction to Endpoint Security .................................................................................. 6
Getting Started .......................................................................................................... 6
Making Sure that the Client is Installed .......................................................................... 6
Getting the Endpoint Security Installation ...................................................................... 7
Installing and Upgrading the Client ................................................................................ 7
Ransomware Detection .................................................................................................. 7

Using the Client ............................................................................................................. 8
Tour of the Endpoint Security Main Page .................................................................. 8
Compliance Blade ..................................................................................................... 9
Anti-Malware Blade .................................................................................................. 9
Media Encryption & Port Protection Blade .............................................................. 10
Remote Access VPN Blade ...................................................................................... 11
Firewall and Application Control Blades .................................................................. 11
Full Disk Encryption Blade ...................................................................................... 11
Capsule Docs Blade ................................................................................................ 12
URL Filtering Blade ................................................................................................. 12
Anti-Bot Blade ......................................................................................................... 12
Forensics and Anti-Ransomware Blade .................................................................. 13
Threat Emulation and Anti-Exploit Blade ................................................................ 14
Tools........................................................................................................................ 14
Advanced ....................................................................................................................... 15
Notification Area Icons and Options ........................................................................ 15

Responding to Alerts ................................................................................................... 16
New Application Alerts ............................................................................................. 16
New Network and VPN Alerts .................................................................................. 16
Compliance Alerts ................................................................................................... 17
Threat Emulation and Anti-Exploit Alerts ............................................................... 17
Anti-Ransomware Alerts ........................................................................................ 17
Media Encryption & Port Protection Alerts ............................................................. 17
Anti-Bot Alerts ........................................................................................................ 18
URL Filtering Alerts ................................................................................................ 18

Uninstalling the Client on Windows ............................................................................ 18
Anti-Malware .............................................................................................................. 19
Uninstalling other Anti-Virus Software ................................................................... 19
Your Anti-Malware Status ....................................................................................... 19
Updating Anti-Malware ........................................................................................ 20
Scanning.................................................................................................................. 20
Understanding Scan Results .................................................................................... 20
Viewing Quarantined Items ........................................................................................ 21

Media Encryption & Port Protection ............................................................................ 22
Components of Media Encryption & Port Protection ............................................... 22
Using Media Encryption & Port Protection .............................................................. 23
Encrypting Media...................................................................................................... 23
Encrypting CDs and DVDs ...................................................................................... 25
Accessing Encrypted Storage Device ...................................................................... 26
Introduction to Endpoint Security

In This Section:

Getting Started ................................................................................................................6

Check Point Endpoint Security™ is the first and only client with all essential components for total security on the endpoint.

Check Point Endpoint Security protects your computer without having to install 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 computer.

The exact instructions to install the Endpoint Security client depend on your administrator.

Here are some items that are referenced in the instructions below:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Endpoint Security icon in your taskbar notification area.</td>
</tr>
<tr>
<td>192.0.2.10</td>
<td>An example of an IP address that the administrator can ask you to connect to.</td>
</tr>
</tbody>
</table>

Making Sure that the Client is Installed

Your administrator can install the Endpoint Security client for you. If you do not know if you already have the Endpoint Security client installed, check your Endpoint Security status.

To see your Endpoint Security status:

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

2. Look at your status in the Endpoint Security Main Page.
   - If it shows that you are Connected, your client is properly installed and you do not have to do anything.
   - If you cannot connect successfully, contact your administrator.

Note - If you do not see the Endpoint Security client icon in your taskbar notification area, it could be hidden. Configure your taskbar to show the hidden Endpoint Security client icon. If you still do not see the Endpoint Security icon, it is likely that the Endpoint Security client failed to install correctly.
Getting the Endpoint Security Installation

If an Endpoint Security Installation window opens, follow the on-screen instructions to continue the installation ("Installing and Upgrading the Client" on page 7).

If an Endpoint Security Installation window does not open, do this procedure to get the installation. The exact steps depend on the choices made by your administrator.

Note - You must have administrator rights on your computer to install the client. For Windows versions higher than XP, you must also run the package using the Run as Administrator option. Consult with your system administrator.

To get the Endpoint Security client installation:

1. Double-click the installation package that your administrator sent you.
   The Endpoint Security icon appears in your taskbar notification area, if it was not there already.
2. If you are not connected, right-click the taskbar notification area icon, and select Connect.
3. If the window that opens shows Welcome, click Next.
   In the window shows Server address or Name, enter the IP address or computer name (usually it looks like this: name.domain.com:443)
4. If a window with a fingerprint opens, click Approve.
5. If you are asked to download and install the client package, click the button to do this.
6. Follow the on-screen instructions to complete the installation and restart your computer.

Installing and Upgrading the Client

⚠️ Important - Do NOT restart the computer during installation. Wait until the upgrade completes.

The client automatically gets updates from the server on a schedule. You can also update manually at any time. To do this, click Update Now from the Endpoint Security Main Page or the icon tray. During updates your computer might be slower than usual.

This update gets policies that changed after the last update. Policies that did not change are not downloaded.

To install or upgrade your Endpoint Security client:

1. When the Endpoint Security Installation window opens, click Install or Postpone.
   The Postpone option is not always available. If you click Postpone, installation is delayed until the Endpoint Security has resumed Installation window opens. You must click OK to continue.
   If you do not click Install, installation starts automatically at the specified time.
2. Wait for the Endpoint Security Client to install.
3. When the Endpoint Security Client installation is complete message window shows, click Restart to restart the computer immediately.
   If you do not click Restart, your computer will restart automatically after 90 seconds.

Ransomware Detection

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

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

สอง Point Protection Files 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 34).

Using the Client

Use the Endpoint Security Main Page and the taskbar notification area icon to see all the information related to Endpoint Security.

Tour of the Endpoint Security Main Page

The Endpoint Security Main Page provides one-stop access to the security features that keep your computer safe.

To launch the Endpoint Security Main Page, select Display Overview from the Endpoint Security system tray menu. You see the Software Blades that your administrator defined for you. (You might not see all of the Software Blades described here.)

- Click a Software Blade to see details and available options.
- The top section shows if everything is compliant and updated, or if you have alerts, status issues, or actions to do.
Compliance Blade

Compliance enables Endpoint Security client to protect your corporate network from Internet threats. Compliance enforces a security policy created by your administrator.

The status shows if you are compliant with the corporate security policy. Status can be:

- **Compliant** - Your computer has the required software and approved versions.
- **Warn** - Your computer is not compliant with the corporate security requirements. You can access your enterprise network, but you must do the actions shown to become compliant.
- **About to be restricted** - Your computer is not compliant with the corporate security requirements. Your access to the corporate network will be restricted if you do not do the actions shown to become compliant within the specified time.
- **Restricted** - Your computer is not compliant with the corporate security requirements. Your access to the corporate network is restricted. Do the actions shown to become compliant.

Click the **Compliance Blade** to see more about:

- **Policy Details** - A summary of the Compliance policy that is installed on your computer.
- **Current Status** - If your computer has Compliance policy violations. A **Message** tells you about each problem and gives recommended remedies.

To correct compliance violations:

- Select a compliance violation message and click **Fix it** to correct the selected violation.
- Click **Try Fix All** to try to correct all listed compliance violations.

If these actions do not resolve the violations, contact your help desk or system administrator.

Anti-Malware Blade

Malware includes viruses, spyware, and other malicious software. Anti-Malware scans automatically detect malware on your computer and make them harmless before they can cause damage. The display shows the Anti-Malware policy and if any items are quarantined or deleted to protect your computer.

Click **Anti-Malware Blade** to see options:

- **Current Status** - A summary of the Anti-Malware status of your computer. See the history of when scans and updates occurred. If the status shows that the Anti-Malware signatures are out of date, click **Update Now**.
- **Infections** - Shows a list of infected files that were detected. In some cases, items detected during an Anti-Malware scan cannot be treated or removed automatically. These items are usually placed into quarantine so that they become harmless but preserved so that they can be treated in the future. It includes this information about each file:

  - **Infection Name** - Name of the malware
    - **Path** - The original location of the malware on your computer.
    - **Infection Status** - If the infection is treated or untreated.
    - **Detection Time** - When the file was detected.
    - **Treatment Time** - When the file was treated.
    - **Quarantined** - If the file was put in quarantine.
• You can select a file and choose one of these options:
  ▪ **Rescan** - Scan the file again (only if the file was not treated).
  ▪ **Delete** - Permanently delete the file (only if the file was in quarantine).
  ▪ **Restore** - Restore the file from quarantine. Do this only after you make sure that the file is safe.

• **Scan System Now** - Click to start an Anti-Malware scan immediately.
• **View Current Scans** - See the progress of scans that are running.

See Anti-Malware (on page 19) for more information.

---

**Media Encryption & Port Protection Blade**

The Media Encryption & Port Protection policy determines how you can use external devices that connect to your computer. Media Encryption & Port Protection can scan (for malware), encrypt, and decrypt external devices. The display shows the status of external devices connected to your computer.

Click **Media Encryption & Port Protection Blade** to see options:

• **Policy Details** - A summary of the Media Encryption & Port Protection 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 and the drive it is connected to.
  ▪ **Size** - The amount of storage space on the device.
  ▪ **Authorization Status** - The authorization status of the device based on an Anti-Malware scan.
    ▪ **Authorized** - Clean from malware.
    ▪ **Not Authorized** - Malware or suspicious files were found. You cannot open, encrypt, or decrypt a device that is not authorized.
    ▪ **Waiting for scan** - The device was not scanned.

• **Encryption Status** - If the device is encrypted or not. Only someone with permissions can view files on an encrypted device.

• **Scan Device** - Scans the device for malware or unauthorized files. If your Endpoint Security client does not have the Anti-Malware Blade installed, the scan can still look for unauthorized files.

• **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 applicable permissions, you can encrypt devices (see “Encrypting Media” on page 23) and access encrypted devices on a computer without Media Encryption & Port Protection (“Accessing Encrypted Storage Device” on page 26).

See Media Encryption & Port Protection (on page 22) for more information.
Remote Access VPN Blade

Endpoint Security VPN (Virtual Private Network) lets you connect securely to your enterprise network when you work from a remote site.

Click Remote Access VPN Blade to see options.

- **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 (or VPN gateway) that the client connects to.
  - **Gateway IP Address** - The IP address of the VPN site.
  - **Last time connected** - The time of your last connection. If you are connected, the time your connection began.

- **Connect to** - Click to select which VPN to connect to and to enter authentication information.
- **Connect** - Click to connect to the default VPN site.

See Remote Access VPN (on page 37) for more information.

Firewall and Application Control Blades

Firewall and Application Control are your front line of defense against Internet threats. The display shows the status of your firewall and the number of attempted connections and programs that the firewall has blocked.

Click Firewall and Application Control to see the options:

- **Policy Details** - A summary of the Firewall, Application Control and Access Zones policies that are installed on your computer.
- **Current Status** - Shows a summary of the firewall and Application Control activity.
  The List of blocked programs shows details of programs that were blocked.

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 as part of Endpoint Security, enter the correct credentials or Smart Card PIN to start your computer. Until you are authenticated, all information on the computer is encrypted.

Click Full Disk Encryption Blade to see options:

- **Policy Details** - Details of the Full Disk Encryption and OneCheck User Settings policies that are installed on your computer.
- **Encryption Status** - Shows the encryption status of components and drives on your computer. It also shows the size, encryption algorithm, and available space for each device.
- **Advanced** - Shows more details for the different parts of your Full Disk Encryption account.

See Full Disk Encryption (on page 30) for more information.
Capsule Docs Blade

The Capsule Docs Blade installs a Plugin lets you create and edit protected documents. Your administrator defines the permission that you have to view, edit, and share documents on different platforms.

Based on your permissions, you can change and edit who can read your documents.

See Capsule Docs (on page 44) for more information.

URL Filtering Blade

The Endpoint URL Filtering Software Blade controls access to web sites by category, user, or group to prevent access to sites with inappropriate content.

From the Endpoint Security Main Page, click the URL Filtering Blade. The status is shown to the right of the blade name. On means the blade is functioning normally. Below the blade name are the Policy Details and Current Status.

Your administrator can allow, limit, or block user access, group access, or access from specified computers to individual websites or categories of websites:

- **If the website you try to access is permitted:** The browser opens it automatically.
- **If you try to access a blocked site:** A message shows in the browser that the site you are attempting to reach is blocked. Sometimes pop-up messages can show outside of the browser, for example, if a different application tries to access a blocked site.
  
  If a site is blocked, you cannot open it through a different browser or application.

Read the information in the browser page or pop-up message about the blocked site and do the on-screen instructions.

Sometimes you can click OK to continue to a site. In this situation, the site is allowed for a period of time.

Anti-Bot Blade

The Endpoint Anti-Bot Software Blade detects and prevents bot activity both while you are in the organizational network or outside of it. A bot is malicious software that neutralizes Anti-Virus defenses, connects to a Command and Control center for instructions from cyber criminals, and carries out the instructions.

From the Endpoint Security Main Page, click the Anti-Bot Blade to see options:

- **Current Status** - A summary of the Anti-Bot status and policies of your computer. The status of the blade can be:
  - **On** - The blade is functioning normally.
  - **Off** - The blade is disabled in the policy.
  - **Initializing** - Anti-Bot is still starting.
  - **Not Running** - An error is preventing the Anti-Bot from working. Contact your administrator.
  - **Infected** - A bot was detected/prevented on your computer. The status changes from infected based on the policy configured by your administrator.
• **Infections** - Shows a list of bot activities that were detected. The Anti-Bot blade can be set to **Detect** or **Prevent** mode. The blade does not delete the bot.

This information shows for each file:

- **Protection Name** - Name of the bot.
- **URL** – The location to which the bot tries to connect.
- **Process Name** – The name of the process accessing the URL.
- **Process ID** – The PID of the process accessing the URL.
- **User Name** – The User Name of the process accessing the URL.
- **Parent Process Name** – The name of the process executing the process accessing the URL.
- **Parent Process ID** – The PID of the process executing the process accessing the URL.
- **Parent User Name** – The user name of the process executing the process accessing the URL.
- **First Infection Time** – When the file was detected.
- **Last Infection Time** – Most recent time the file was detected.
- **Action** – Was the bot detected or prevented.

When an infection is detected or prevented, this message shows:

"Your computer is trying to access a malicious server: [URL]. For more information and remediation, please contact your help desk."

The message that a bot has been prevented also shows in your network browser.

---

**Forensics and Anti-Ransomware Blade**

The Forensics and Anti-Ransomware Software Blade monitors file operations, processes, and network activity for suspicious behavior. It also analyzes attacks detected by other client blades or the Check Point gateway.

If a Ransomware attack occurs, the blade automatically backs up your files before they are encrypted. After the attack, you or your administrator can delete encrypted files created by the attack and restore the original files from the backup.

From the Endpoint Security Main Page, click the **Forensics and Anti-Ransomware Blade** to see details.

The status of the blade is shown to the right of the blade name:

- **On** - Blade function is normal.
- **Off** - The blade is disabled by the policy.
- **Initializing** - The blade in startup mode.
- **Warning** - Low disk space.
- **Error** - Very low disk space (stops sensors recording).

The blade’s functionality is below the blade name:

- **Monitoring/Analyzed x cases**
- **Not monitoring** (the blade 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 the blade has examined, including ID, Source, Type, Description, and Date.

From the Analyzed cases list:

- Click the **Incident ID** to open a Forensics Analysis Report.
- 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.

**Threat Emulation and Anti-Exploit Blade**

Threat Emulation and Anti-Exploit 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 the **Threat Emulation and Anti-Exploit** blade to see options.

The status of the blade is shown to the right of the blade name:

- **On** - Blade function is normal.
- **Off** - The blade is disabled by the policy.
- **Initializing** - The blade in startup mode.
- **Warning** - Low disk space.
- **Error** – Very low disk space (stops sensors recording).

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

**Tools**

The **Tools** menu is on the left of the Endpoint Security Main Page.

<table>
<thead>
<tr>
<th>Tools</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan System Now</strong></td>
<td>Run the Anti-Malware scan.</td>
</tr>
<tr>
<td><strong>Update Now/Upgrade Now</strong></td>
<td>Update the Anti-Malware signatures and client policy (if there is a changed policy on the server for the client to update to). You can also start a postponed deployment.</td>
</tr>
<tr>
<td><strong>Connect</strong></td>
<td>Connect to the default VPN.</td>
</tr>
<tr>
<td><strong>Connect To</strong></td>
<td>Select a VPN to connect to.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td>See the security policy and configure advanced options.</td>
</tr>
</tbody>
</table>
Advanced

The **Advanced** page has these options:

- **View server information** - Shows the IP address of the server you are connected to and the state of the connection.

- **View policies** - Shows the policies that are installed as part of Endpoint Security, the version installed, the date the policy was installed by your administrator, and the mode it is in (Connected or Disconnected).

- **View Logs** - Shows a log of your Endpoint Security activity. Your administrator automatically sees this data also.

- **Collect information for technical support** - Selects which logs are sent to Technical Support to use for troubleshooting. You can specify how much information and the range of dates to include in the compiled logs.

- **Personalization** - Select the default action for the notification area icon.

Notification Area Icons and Options

The icons shown in the taskbar notification area let you quickly monitor your security status and Internet activity. You can also access your security settings in just a few clicks. Right-click any of these icons to access a shortcut menu:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="VPN connected" /></td>
<td>VPN is connected.</td>
</tr>
<tr>
<td><img src="image" alt="Scan" /></td>
<td>Security scan, encryption, or change in client settings is in progress.</td>
</tr>
<tr>
<td><img src="image" alt="Action necessary" /></td>
<td>Action is necessary (for example: the client is out of compliance with policy, there is an application error, or a reboot is needed).</td>
</tr>
</tbody>
</table>

When you right-click the Endpoint Security icon, you get several options. The options that are enabled for you depend on the permissions set by your administrator. Similar options are available in the Tools section of the Endpoint Security Main Page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Overview</td>
<td>Show the Endpoint Security Main Page.</td>
</tr>
<tr>
<td>Scan Now</td>
<td>Run the Anti-Malware scan.</td>
</tr>
<tr>
<td>Update Now</td>
<td>Update Anti-Malware signatures.</td>
</tr>
<tr>
<td>Connect</td>
<td>Connect to the VPN site.</td>
</tr>
<tr>
<td>Connect to</td>
<td>Select a VPN site to connect to.</td>
</tr>
<tr>
<td>Register to hotspot</td>
<td>Register for temporary access to a public wireless hotspot. Open a browser immediately and follow the hotspot instructions to register (usually click a button).</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.

New Application Alerts

The majority of the alerts you see will be New Application alerts. These alerts occur when a program on your computer requests access or server permission to the Internet or your local network. Use the New Application alert to give access permission to applications that need it, such as your browser and e-mail program.

Few applications or processes actually require server permission in order to function properly. Some processes, however, are used by Microsoft Windows to carry out legitimate functions. Some of the more common ones you may see in alerts are:

- lsass.exe
- spoolsv.exe
- svchost.exe
- services.exe
- winlogon.exe

If you do not recognize the applications or process that is asking for server permission, search the Microsoft Support Web site (http://support.microsoft.com/) for information on the process to determine what it is and what it is used for. Be aware that many legitimate Windows processes, including those listed above, have the potential to be used by hackers to disguise worms and viruses, or to provide backdoor access to your system for Trojan horses. If you were not performing a function (such as browsing files, logging onto a network, or downloading files) when the alert appeared, then the safest approach is to deny server permission. If you see many server applications alerts, you might want to run an Anti-Malware scan as an added precaution.

New Network and VPN Alerts

Other alerts you might see are the New Network alert and VPN Configuration alerts. These occur when the client detects a network connection or VPN connection. They help you configure your network and program permissions correctly so that you can work securely over your network.
Compliance Alerts

The Compliance blade makes sure that:

- All required Endpoint Security packages, with version updates, are installed on your computer.
- Required operating systems, with versions, service packs, and updates are installed on your computer.
- Only authorized programs are installed and running on your computer.

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

- One of these Compliance states:
  - **Warning** - Your computer is not compliant but you can continue to use network resources. Do the steps to make your computer compliant as quickly as possible.
  - **About to be restricted** - Your computer is not compliant. You must make your computer compliant immediately. If you do not do this, access to network resources from your computer will be restricted.
  - **Restricted** - Your computer is not compliant. Access to network resources from your computer is restricted until you make your computer compliant.
- Instructions for making your computer compliant with the policy.

Threat Emulation and Anti-Exploit Alerts

Threat Emulation and Anti-Exploit 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 blade 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 & Port Protection Alerts

If you have the Media Encryption & Port Protection blade as part of your Endpoint Security, you might see alerts related to device scanning or encryption. Follow the on-screen instructions.
Anti-Bot Alerts

Anti-Bot Alerts show when a restricted site is detected. Follow the on-screen instructions.

URL Filtering Alerts

URL Filtering Alerts show when a restricted site is detected. Follow the on-screen instructions.
If you only have an OK button, click on it to close the pop-up message.
If you have both OK and Cancel buttons:
- Click Cancel to close the pop-up message.
- Click OK to decide to allow browsing to the site. Browse to the site again to access it for a period of time.

Uninstalling the Client on Windows

Administrator privileges are required to uninstall the client.

To uninstall the Endpoint Security client on Windows computers:

1. Make sure that the original EPS.msi and PreUpgrade.exe files are present on the endpoint computer.
2. Go to Control Panel > Programs and Features > Uninstall or change a program.
4. If the client has Full Disk Encryption installed, run the Uninstall or change a program applet again after the disk completes the decryption.

After you uninstall the Endpoint Security client, you must reset the computer through SmartEndpoint on the Security Management Server. See Resetting a Computer.

Note - We recommend that you run a database backup on a daily basis.
Chapter 2

Anti-Malware

In This Section:

- Uninstalling other Anti-Virus Software ......................................................... 19
- Your Anti-Malware Status .............................................................................. 19
- Updating Anti-Malware .................................................................................. 20
- Scanning ......................................................................................................... 20

Anti-Malware protects your computer against viruses, spyware, and malicious software. Real-time and scheduled scans detect malicious software and make them harmless before they can damage your computer.

Uninstalling other Anti-Virus Software

Before you install Endpoint Security, uninstall any other Anti-Virus software from your computer, including suite products that include virus protection among their features. If you are using a program that cannot be uninstalled automatically, use Add/Remove Programs from the Windows Control Panel.

Your Anti-Malware Status

To view the status of your Anti-Malware Blade, from the Endpoint Security Main Page, click Anti-Malware Blade.

On this page you can:

- See the status of the Anti-Malware Blade. The status can be:
  - On - Anti-Malware has started and is up to date.
  - Off - Anti-Malware is not active.
  - Initializing - Anti-Malware is still starting.
  - Warning - Anti-Malware is not up to date. Update as soon as possible.
  - Alert - Anti-Malware is severely out of date. Update immediately.
  - Error - An error is preventing the Anti-Malware from working. Contact your administrator.
  - Infected - Untreated malware was detected on your computer.
  - Scanning - Anti-Malware scan is currently in progress.

- See the dates and times of your last scans and updates.
- Click Scan System Now to run a scan.
- See items that are quarantined. Quarantined items are deleted and put in a secure storage area. They can be restored from this area if necessary.
Updating Anti-Malware

Every Anti-Malware application contains a definition file, with information to identify and locate malware on the computer. As new malware applications are discovered, the client updates its database with the definition files necessary to detect these new threats.

The Endpoint Security client gets updates regularly. In the Client Status section of the Anti-Malware Detail pane, you can see when the last update occurred.

To run an update:
• In the Endpoint Security Main Page, under Tools, click Update Now.
• Right-click the Endpoint Security icon in the taskbar notification area and select Update Now.

If there is an error, you see a message:
• Anti-Malware was unable to update. No connection to the server - Make sure that you are connected to the network. If you continue to see this, contact your administrator.
• An unexpected error occurred - If you continue to see this, contact your administrator.
• Anti-Malware Updater is off.

Scanning

You can start a scan of your computer or a specific file, folder or directory in these ways:

To scan the full computer:
• In the Endpoint Security Main Page, click Tools > Scan system now.
• Right-click the notification area icon and select Scan system now.

To scan a file, folder, or drive:
Right-click a file, folder, or drive on your computer and choose Scan with Check Point Anti-Malware.

Based on the settings configured by your administrator, Anti-Malware scans the entire contents of your computer. It finds malware that might be dormant on all parts of your computer.

Because full-computer scans are very thorough, they require time and computer resources. Therefore, your computer’s performance might be slow while a full-computer scan is in progress. To avoid impact on your work, your administrator can schedule scans to run at a time when you are not likely to use your computer.

Note - If you click Pause in the Scan window while a scan runs, only the current scan stops. On-Access scanning is not disabled. Click Resume to continue the scan.

Understanding Scan Results

After the scan is completed, the details of malware detected show in the scan window. The details are:
• Threat - The name of the malware detected.
• Type - The type of threat.
- **Action** - What actions Endpoint Security took.
- **Result** - The result of the action.
- **Path** - Where the infection was found on the computer.

**Viewing Quarantined Items**

In some cases, items detected during an Anti-Malware scan cannot be treated or removed automatically. These items are usually placed into quarantine so that they become harmless but can be restored and treated in the future after an update to your malware files.

**To view and treat Anti-Malware in quarantine:**

1. **Open Anti-Malware Blade.**
   
The details of the quarantined files shows in the *Infections* list:
   - **Infection Name** - Name of the malware
   - **Path** - The original location of the malware on your computer.
   - **Infection Status** -
   - **Detection Time** - When the file was detected.
   - **Treatment Time** - When the file was treated.
   - **Quarantined** - If the file was put in quarantine.

2. **Select a file and click:**
   - **Rescan** - Scan the file again
   - **Delete** - Permanently delete the file.
   - **Restore** - Takes the file out of quarantine.

     **Note** - Only restore a file if you are sure that the file is not malware.
Media Encryption & Port Protection

In This Section:

Components of Media Encryption & Port Protection ..........................................................22
Using Media Encryption & Port Protection .................................................................23

The Media Encryption & Port Protection blade prevents leakage of sensitive data in these ways:

- The policy defines whether or not to allow access to devices connected to a physical port, such as USB storage devices.
- Based on your permissions, you can optionally encrypt external devices connected to your computer to prevent access without your permission.

The features of Media Encryption & Port Protection are described in the next sections.

Components of Media Encryption & Port Protection

The actions that you can do in Media Encryption & Port Protection depend on the policy set by your administrator. Therefore, all of the features described below might not be available for you.

- Port Protection rules control access to removable devices such as:
  - USB devices
  - CD/DVD Drives
  - PDAs
  - Smartphones
  - Flash memory
  - Floppy disk drives
  - Digital cameras
  - External hard disks (NTFS formatted)

The policy controls device access for all available ports including USB and Firewire. Policy rules define access rights for each type of removable storage device and the ports that they can connect to. Policy rules can also include requirements for malware scanning and data authorization. The policy can also prevent you from connecting unauthorized devices to your computer.

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

Your rules can apply different access permissions for business data (encrypted) and non-business data (non-encrypted). Rules can also define which file types are defined as business data and must be stored on encrypted storage.
Using Media Encryption & Port Protection

This section describes the process of encrypting, decrypting and managing removable storage devices. Media Encryption & Port Protection 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.

**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.

To work with Media Encryption & Port Protection, from the Endpoint Security Main Page, click **Media Encryption & Port Protection**.

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

**Encrypting Media**

Your organization’s policy defines access to business and non-business data. It is possible that your policy allows access only to business data, which is encrypted. Alternatively, your policy can allow access to business and non-business data, but the business data must be encrypted and password protected. In this case, Media Encryption creates two drives on the physical storage device. One encrypted drive for business data and a non-encrypted drive for non-business data.

If you have the required permissions you can:

- Define a password that gives users full access to the encrypted drive.
- 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.

  **Note** - If you define a drive that is smaller than the volume of data you want to encrypt, the encryption procedure fails.

  **Important** - 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.

To encrypt a new storage device:

1. Insert a removable storage device (CD, DVD, USB) into your computer.

   **Note** - You can also start the encryption procedure by dragging a business data file to a storage device in Windows Explorer that has not yet been encrypted. In the **Files Must be Encrypted** window, click **Encrypt**. Continue with step 3.

2. From **Media Encryption & Port Protection**, select a device and click **Create Encrypted Storage**.
The Removable Device Encryption window opens. The options shown are set by your administrator. You can also encrypt and decrypt devices.

3. In the Removable Device 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 (not available for CDs or DVDs).

4. Optional (if available): Click Advanced Settings to:
   - Set a password for read-only access to the device.
   - Set an owner for the device (not available for CDs or DVDs). Usually, the administrator sets a policy that only the owner of the device can access the files on the device. Select one of these options:
     - Media owner will be assigned on first use - The first user to insert the storage device into an endpoint computer automatically becomes the owner.
     - Assign media to a user: Assign ownership to the user running the encryption (that is, yourself) or click Browse to select a user from the active domain.

5. Click Encrypt.

6. If you are encrypting a CD or DVD, a window opens where you can add and remove the files that will be copied to the encrypted drive on the disk.
   a) Go up one step in the folder structure.
   b) Add files or add an entire folder copy to the disk.
   c) Select and delete any file or folder that you do not want to copy to the disk.
   d) Click Next. The files are copied to the disk.
   e) A message shows when the procedure completes.

7. 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.

8. When the Finish window opens, click Finish to complete the process.

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

Adding Business Data to an Encrypted Device

If you have the required permissions, you can:

- Add new business data files to and from the encrypted storage drive.
- Add non-business data to the unencrypted drive.

To add business data to an encrypted storage device:

1. Copy, move, or drag-and-drop files to the device.

2. If you try to copy business data to an unencrypted device or drive, a window opens asking you to encrypt the file. In the Check Point Endpoint Security window, click Encrypt and then click Yes to confirm.
The business data file is encrypted and copied to the encrypted storage device.

You can also encrypt a device to contain business data from the Media Encryption & Port Protection Details page of the Endpoint Security Main Page.

**Encrypting CDs and DVDs**

If allowed by your policy, you can encrypt CDs and DVDs with these limitations:

- Encryption can be done only on RW and blank R/RW disks.
- You cannot add or delete data from a CD or DVD once it is burned. You can only erase the disk completely.

The process of importing and exporting files to CD/DVDs is similar to that of other removable storage devices described in Encrypting Media (on page 23). Two differences between CD/DVDs and other removable storage devices are that you cannot encrypt only a part of a CD/DVD, and you cannot add or delete files once the disk has been burnt. If you want to remove information on a rewritable disk, you need to use the Erase feature to completely erase it.

**Burning Encrypted CDs and DVDs**

This table shows the supported methods available to burn encrypted CDs and DVDs in different Windows versions:

<table>
<thead>
<tr>
<th>Method</th>
<th>Windows XP</th>
<th>Windows Vista and Higher</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CD</td>
<td>DVD</td>
</tr>
<tr>
<td>Endpoint Security Main Page &gt; Media Encryption &amp; Port Protection</td>
<td>✓</td>
<td>✓ if KB932716 is installed</td>
</tr>
<tr>
<td>Windows CD/DVD built in burner from Windows Explorer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Nero Burning ROM (version 9 and higher)</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Burning Unencrypted CDs and DVDs**

Your ability to burn unencrypted CDs and DVDs is based on the policy set by your administrator.

**Encrypting Media in Windows 7 and Higher**

When you insert a new blank CD or DVD in Windows 7 or higher and attempt to write files to it for the first time, two options are available:

- Like a USB flash drive
- With a CD/DVD Player

To successfully encrypt data to the disk, select: **With a CD/DVD Player**. Media encryption only intercepts requests to burn that use this mode.
Accessing Encrypted Storage Device

As allowed by your policy, you can access business data on an encrypted storage device from a computer protected by Media Encryption & Port Protection. Access permissions can be full (read/write) or read only.

If allowed by your policy, you can also access business data from a computer that is not protected by Media Encryption & Port Protection. In this case you must enter a password to gain access. To do this, Media Encryption copies these files to the physical storage device:

- **autorun.inf** - Automatically runs the decryption program if auto run is enabled on the device.
- **Access to Business Data.exe** – The decryption program that lets you access business data on the endpoint client.

  **Note** - You must set a password during the encryption process to be able to access the information from computers that do not have Media Encryption & Port Protection installed.

To access data on an encrypted device from a computer without Media Encryption & Port Protection:

1. Insert the encrypted device into the computer.
2. If necessary, open the drive window in Windows Explorer window and double-click **Access to Business Data**.
3. Enter the applicable password.
   A Windows Explorer window shows the contents of the encrypted device. You can work with these files according to your permissions.
   - If you have Full access permissions, you can drag-and-drop or copy/paste business data to and from the encrypted device.
   - If you have read-only permissions, you can only read the file contents but cannot change the data, copy files, or delete files.

  **Note** - If you forget your password or do not have your Smartcard, you can use Remote Help for assistance.

Deleting Encrypted Files and Storage Devices

You can delete files from an encrypted storage device or delete the encrypted drive itself. Usually, the Media Encryption & Port Protection policy lets only the device owner or another authorized user remove files or delete an encrypted drive.

Make sure that you copy or back up files on the encrypted device before decrypting it. The decryption procedure automatically deletes all data on the encrypted storage device. If your policy does not let you decrypt files or a storage device, you must ask an administrator to do this for you.

To remove files from an encrypted storage device:

1. Connect the encrypted storage device to your computer.
2. If you do not have automatic access to the storage device, enter the password when prompted and click **OK**.
3. Select the files to delete.
4. Move the files to your local disk or delete them.
To delete an encrypted storage device:
1. Connect the encrypted storage device to your computer.
2. If you do not have automatic access to the storage device, enter the password when prompted and click OK.
3. From the Media Encryption & Port Protection Details page, click Remove Encryption.
   If there is data on the encrypted drive, a warning message shows saying that all data on the encrypted drive will be deleted. Click Yes to continue.
4. Click Finish to complete the process.
   The decryption procedure can take some time, depending on the size and type of device. When the decryption completes, all encrypted data is deleted and the encrypted drive is automatically deleted.

   **Important** - Do NOT remove the storage device during the decryption process. This will destroy your data and may damage the storage device.

### Scanning Devices

To start a Media Encryption & Port Protection scan:
In Media Encryption & Port Protection, select a device and click Scan Device. Files are scanned according to the Media Encryption & Port Protection policy.

**Note** - Clicking Pause in the Scan dialog while a scan is being performed will stop the current scan only. On Access scanning will not be disabled. Click Resume to resume the current scan.

### Changing the Encrypted Device Password

To change the removable storage device access password for an encrypted device:
1. Right-click a device in the Media Encryption & Port Protection Details window.
2. Select Advanced > Set Full Access Password or Set Read Only Password.
3. Enter the old password and click OK.
   You must have Full Access to change a Full Access password or a Read Only password.

   **Note** - The Full Access and Read Only passwords cannot be identical.
4. Enter and confirm the new password.

   **Note** - The password must meet the criteria defined by the administrator.
5. Click OK.

### Converting File Encryption Devices to Media Encryption

You can easily convert storage devices that were encrypted with Pointsec File Encryption R73 and earlier to Media Encryption E80.xx. When you insert a device encrypted with Pointsec File Encryption into an endpoint computer running this version, you are prompted to upgrade the device.
To convert a File Encryption device to Media Encryption:

1. Insert the device into a computer that has an Endpoint Security client with the Media Encryption & Port Protection blade active.
2. This message shows:
   **To access the device, you need to convert it to Media Encryption format.**
3. Click **OK**.
4. If necessary, enter the **File Encryption credentials of the device** in the window that opens. These must be the credentials originally to encrypt the storage device. They can be:
   - A corporate user name and password assigned by the administrator
   - A personal user name and password defined for this storage device
   *If the device was originally encrypted with a corporate password and Media Encryption & Port Protection can find the password on the computer, this window does not open.*
5. Enter and re-enter a new password for the device.
6. Click **Continue**.
7. Optionally, edit the Media Encryption settings.
8. Click **Encrypt**.
9. When the encryption is complete, click **Finish**.
Firewall & Application Control

In This Section:

Understanding Firewall Protection ................................................................. 29
Understanding Application Control ............................................................ 29

Firewall and Application Control is your front line of defense against Internet threats.

Understanding Firewall Protection

The firewall guards the "doors" to your computer—that is, the ports through which Internet traffic comes in and goes out. It examines all the network traffic and application traffic arriving at your computer, and asks these questions:

• Where did the traffic come from and what port is it addressed to?
• Do the firewall rules allow traffic through that port?
• Does the traffic violate any global rules?

The answers to these questions determine whether the traffic is allowed or blocked.

The Endpoint Security administrator sets the policies and rules that determine what traffic the firewall allows.

Understanding Application Control

The Application Control blade restricts network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block, or terminate applications and processes. Only applications that try to get network access can be blocked or terminated.

Based on the policy settings, an alert can show which application was blocked or terminated. You can also see which applications are blocked and terminated in the Current Status section of the Firewall and Application Control Blades tab of the Endpoint Security Main Page.
Full Disk Encryption

In This Section:

Overview of the Login Screen ................................................................. 30
Authenticating to Full Disk Encryption .................................................. 31

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 computer 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 your computer at all.

This is important protection for the information stored on your computer and corporate network. For example, if someone steals your computer and tries to access the information in it, the thief will not be able to get past this screen.

You can also use these options in the login screen:

- **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 Windows login and your Full Disk Encryption login. If you need to log in to Windows 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 you have set in Windows. All keyboard layouts that are loaded in Windows 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 computer. 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 computer restarts automatically. When it starts again, the Pre-boot screen is in the selected language.

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.

If You Do Not Have Your Password

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

There are two types of Full Disk Encryption Remote Help:

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

To use Remote Help to log in:

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

Ensuring That No One Tampered with Your Computer

If you did not personally start the machine yourself, you should always press **CTRL+ALT+DEL** to restart your computer before authenticating yourself. This ensures 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 Fixed Password

Usually you use your Windows credentials to log in to your Full Disk Encryption-protected computer as a new user. Sometimes an administrator will give you a user account name and a password.

To authenticate for the first time with your fixed password:

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

Authenticating with a Smart Card or USB Token

Smart Cards and USB tokens contain certificates protected by PIN codes. To be authenticated by Full Disk Encryption, you must connect the card or token to the computer and enter a valid card or token PIN.

Your administrator will supply you with your Smart Card or USB token and the information that you need to use it.
Make sure that your Smart Card or USB token is connected to your computer before you start to authenticate.

To authenticate with a Smart Card or USB token:

1. Connect your smart card/USB token to your Full Disk Encryption-protected computer.
2. Start your computer or press Ctrl+Alt+Delete.
   The User Account Identification window opens.
3. When the PIN field shows, enter your PIN.
4. Click OK.
   Full Disk Encryption lets Windows start.
Forensics and Anti-Ransomware

In This Section:

- Anti-Ransomware Files ................................................................. 34
- SandBlast Agent Forensics Analysis Report ..................................... 34
- Anti-Ransomware Restoration ....................................................... 35

The Forensics and Anti-Ransomware Software Blade monitors file operations, processes, and network activity for suspicious behavior.

In the Endpoint Security Main Page, you can see a list of incidents that Forensics has analyzed 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.

Anti-Ransomware Files

SandBlast Agent 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 SandBlast Agent 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

\CheckPoint\Protection\Files\Do Not Erase

The file names include these strings, or similar:

CP
CheckPoint
Check Point
Check-Point
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.

SandBlast Agent Forensics Analysis Report

The SandBlast Agent Forensics Analysis Report provides full information on attacks and suspicious behavior with an easy interface. The report includes:

- **EntryPoint** - How did the suspicious file enter your system?
• **Business Impact** - Which files were affected and what was done to them?
• **Remediation** - Which files were treated and what is their status?
• **Suspicious Activity** - What unusual behavior occurred that is a result of the attack?
• **Incident Details** - A complete visual picture of the paths of the attack in your system.

Use the Forensics Analysis Report to prevent future attacks and to make sure that all affected files and processes work correctly.

**Opening a Forensics Analysis Report**

To open a Forensics Analysis Report for an incident:

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 **Forensics and Anti-Ransomware** blade.
3. In the **Analyzed cases** table, click an Incident ID.
   The **Forensics Analysis Report** opens in your browser.

**Anti-Ransomware Restoration**

In the SandBlast Agent Forensics Analysis Report (on page 34), you can see details of which files restored and deleted during the restoration.

- 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 the **Forensics and Anti-Ransomware** blade.
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**.
Remote Access VPN

*In This Section:*

- **VPN Basics:** ................................................................. 37
- **Changing the Site Authentication Scheme:** .................. 38
- **Collecting Logs:** ............................................................. 43

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 when working remotely. You can then access private files over the Internet knowing that unauthorized persons cannot view or alter them. The VPN connection can be made directly to the server or through an Internet Service Provider (ISP). Remote users can connect to the organization using any network adapter (including wireless adapters) or modem dialup.

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 between them. In addition, the integrity of the data is maintained, which means the data cannot be altered during transit.

The **VPN Detail** page displays information about any current VPN connection (if any) and about the status of your remote connection to a VPN enabled Security Gateway. From the VPN page, you can click **Manage Settings > New** to launch the Site Wizard to create a VPN site, connect to or disconnect from a VPN site, or open the VPN Settings window to configure profiles and sites, configure any special connection options, or manage certificates.

**Creating a VPN Site**

You can configure multiple VPN sites. If you are in a hotspot environment, connect to the hotspot before you connect to the VPN site.

**To configure a VPN site:**

1. If you do not have a VPN site configured, open the Site Wizard: right-click the notification area icon and select **Connect**.
2. When the wizard opens, click **Next**.
3. Enter a server address or name.
   - The wizard can detect a site that your administrator configured. You can leave this site or change it.
4. **Optional:** Select the **Display name** option and enter a name, if you want to see a name of the site that is meaningful for you. For example, you can call the site “Corporate Headquarters”.
5. Click **Next** and wait while the new site is created.
   - If you see the message about the **site’s certificate**, contact your system administrator.
6. Click **Finish** to complete the Wizard.
Connecting to the VPN

To connect to a VPN site you can:

- From the Endpoint Security Main Page, click **Remote Access VPN Blade > Connect to** or **Connect**.
- From the taskbar notification area icon, right-click and select **Connect**.

Configuring Proxy Settings

If you are at a remote site which has a proxy server, the client must be configured to go through the proxy server. Usually the client can find proxy settings automatically. If not, you can configure it.

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

**To configure proxy settings:**

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

Changing the Site Authentication Scheme

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

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

1. Right-click the Client icon and select **Display Overview**.
2. Click **Remote Access VPN Blade**.
3. Click the **Manage Settings** link.
   The **Options** window opens.
4. On the **Sites** tab, select the site and click **Properties**.
   The **Properties** window for the site opens.
   On the **Settings** tab, select an option from the **Authentication Scheme** drop-down menu.
   - Username and password
Certificate Enrollment and Renewal

A. To enroll a certificate:
1. Right-click the Client icon and select Display Overview.
2. Click Remote Access VPN Blade.
3. Click the Manage Settings link.
   The Options window opens.
4. On the Sites tab, select the site from which you will enroll a certificate and click Properties.
   The site Properties window opens.
5. Select the Settings tab.
6. Choose the setting type you want, CAPI or P12, and click Enroll.
   The CAPI or P12 window opens.
7. For CAPI, choose the provider to which you will enroll the certificate.
8. For P12, choose a new password for the certificate and confirm it.
9. Enter the Registration Key that your administrator sent you.
10. Click Enroll.
    The certificate is enrolled and ready for use.

B. To renew a certificate:
1. Right-click the Client icon and select Display Overview.
2. Click Remote Access VPN Blade.
3. Click the Manage Settings link.
   The Options window opens.
4. On the Sites tab, select the site from which you will renew a certificate and click Properties.
   The site Properties window opens.
   The authentication method you chose is set and the certificate will be renewed accordingly.
5. Select the Settings tab.
6. Click the Renew button.
   The CAPI or P12 window opens.
7. For CAPI, choose the certificate you want to renew from the drop-down list. For P12, choose a P12 file and enter its password.
8. Click Renew.
    The certificate is renewed and ready for use.
Importing a Certificate into the CAPI Store

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

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

If the system administrator instructed you to save the certificate on the computer, import it to the CAPI store. If not, the administrator will give you the certificate file on a USB or other removable media. Make sure you get the password.

To import a certificate file to the CAPI store:

1. Double-click the certificate file.
   
   **Windows Certificate Import Wizard** opens the Welcome screen.

2. Click Next.

3. Make sure the correct certificate file is selected in the **File to Import** screen.

4. Click Next.

5. In the **Password** screen, enter the password for the private key.

6. Select options as necessary:
   - **Enable strong private key protection** - will prompt for the private key access permission, every time you try to access the certificate.
   - **Mark this key as exportable** - lets you export the certificate into a .pfx file and set a new password.
   - **Include all extended properties** - Recommended.

7. Click Next.

8. Select certification store location:
   - **Automatically select the certificate store based on the type of certificate** - default.
   - **Place all certificates in the following store** - browse to the location where you want to store the certificate.

9. Click Next.

10. Review the summary screen and click **Finish**.

11. Click **OK**.

Authenticating with PKCS#12 Certificate File

For security reasons, your system administrator might require you to authenticate directly with the PKCS#12 certificate and not from the certificate stored in the CAPI. For example, if you use several desktop workstations and laptops, you might not want to leave your certificate on different computers. If the PKCS#12 certificate is in the CAPI store and someone steals your laptop, they can use the client to connect to the site. For increased security, your administrator might instruct you to save the PKCS#12 certificate to a USB stick or other storage device.

To authenticate with a PKCS#12 certificate file:


2. Connect to the site.
   
   The Connect window opens.
3. In the **Certificate File** area, browse to the certificates stored on the floppy or USB disk.
4. In the **Password** field, enter the certificate password.
5. Click **Connect**.

   **Note** - If you selected the **Always-Connect** option, whenever communication between the site and client is closed, the user will be prompted to enter the certificate password.

### 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), with a built-in clock and encoded random key.

The most common 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 does not have a PIN pad, a **tokencode** is displayed. A **tokencode** is the changing number displayed on the key FOB.

The site wizard supports both methods, as well as softID. The client uses both the PIN and tokencode, or just the passcode, to authenticate to the gateway.

### Challenge-Response

Challenge-response is an authentication protocol in which one party provides the first string (the challenge), and the other party verifies it with the next string (the response). For authentication to take place, the response is validated.

### Secure Authentication API (SAA)

Secure Authentication API (SAA) lets you use third-party authentication technologies with your client. To work, it requires a DLL file that is installed on your client.

If your administrator instructs you to select Secure Authentication API (SAA) as the authentication method when you create a site, you need this information:

- The type of SAA authentication that you must select - one of these:
  - **Username and Password** - Users enter a username and password.
  - **Challenge Response** - Users enter a response to a challenge.
- You might need a DLL file. If your administrator already configured this, then you do not need it.

   **Note** - Only users with administrator permissions can replace the DLL.
If you select SAA as the authentication in the site wizard, a new page opens where you select the type of SAA authentication and a DLL file, if required.

**Secure Authentication API (SAA)**
Select the type of third party authentication that you use.

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

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

**Use a Secure Authentication API File:**

![Select a SAA DLL file](Browse...)

Select the Secure Authentication API DLL file supplied by your administrator. If you do not have this, contact your administrator.

---

**Replacing the SAA DLL File**

Your administrator might instruct you to replace the DLL file on your client.

![Note](Only users with administrator permissions can replace the DLL.)

To replace the local DLL file:

1. Right-click the Client icon and select **Display Overview**.
2. Click **Remote Access VPN Blade**.
3. Click the **Manage Settings** link.
   The **Options** window opens.
4. In the **Advanced** tab, next to **Use a Secure Authentication API File**, browse to select the new DLL file.
   This file is used for SAA authentication.
Connecting to a Site with SAA

Usually, when you connect to a site, a login window opens and you enter your authentication information directly in that window. If SAA is the authentication method for the site, there are no fields for authentication information in the login window. You must click the **Connect** button in the window and a new window opens for authentication information.

### Collecting Logs

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

**To collect logs:**

1. Right-click the Client icon and select **Display Overview**.
2. Click **Remote Access VPN Blade**.
3. Click the **Manage Settings** link.
   - The **Options** window opens.
4. Open the **Advanced** tab.
5. Select **Enable Logging**.
6. Reproduce the problem.
7. Click **Collect Logs**.

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

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

---

Remote Access VPN

Connecting to a Site with SAA

Usually, when you connect to a site, a login window opens and you enter your authentication information directly in that window. If SAA is the authentication method for the site, there are no fields for authentication information in the login window. You must click the **Connect** button in the window and a new window opens for authentication information.

### Collecting Logs

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

**To collect logs:**

1. Right-click the Client icon and select **Display Overview**.
2. Click **Remote Access VPN Blade**.
3. Click the **Manage Settings** link.
   - The **Options** window opens.
4. Open the **Advanced** tab.
5. Select **Enable Logging**.
6. Reproduce the problem.
7. Click **Collect Logs**.

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

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

In This Section:

Using the Plugin .......................................................................................................... 44
Using the Client Console .............................................................................................. 47

Capsule Docs installs a Plugin that lets you create and edit protected documents using the Capsule Docs supported Windows applications.

Using the Plugin

After it is installed, the Capsule Docs plugin is enabled for all supported applications.

Microsoft Office and Adobe Acrobat and Reader

For supported Microsoft Office and Adobe Reader and Professional versions, the Capsule Docs menu shows in the document. These are:

• Microsoft Office 2016 32/64-bit
• Microsoft Office 2013 32/64-bit
• Microsoft Office 2010 32/64-bit
• Microsoft Office 2007 32-bit
• Microsoft Office 2003 32-bit (English version)
• Adobe Reader 8 - 11 and DC
• Adobe Acrobat Pro 8 and 9

If you use Capsule Docs with MS Office 2010 32-bit or lower: Changes that you make in the Capsule Docs menu are automatically applied when you click outside of the Capsule Docs menu.

If you use Capsule Docs with MS Office 2010 64-bit, MS Office 2013, or MS Office 2016: You must click **Apply** and **Save** the document for changes to apply to the document.

If you do an action in a protected document and you are not connected to a Capsule Docs server, a login page opens.

A pink lock icon in the Capsule Docs menu shows that the document is encrypted and only users with access can open it.

Documents without the pink lock icon have Capsule Docs protection but are not encrypted. Everyone can access them.

Creating a Protected Document

When you create a new document in a supported application, the protection settings of your default Capsule Docs community are applied to the document.
To protect a document or change protection settings:

- **From within the document** - Use the Capsule Docs menu.
  
  In some MS Office versions, the menu shows in the upper-right corner of documents. In others it shows in the Home tab.

- **From File Explorer** - Right-click the document and select **Protect with Capsule Docs > Change protection** or **Protect**

Based on the permissions that your administrator gives you, you can:

- Change Classification
- Change Community
- Remove protection
- Add or remove users and groups
- Set a document expiration date (only document Authors can do this)
- Create Favorites lists of users and groups.
  
  **Note** - The Favorites lists can be used across the supported applications, to share the documents with different sets of users.

To see the Capsule Docs settings for a file:

- Use the Capsule Docs menu.
- Open the file **Properties >Capsule Docs** tab.

**Changing Classification**

Each community has a set of classifications. The community administrator defines permissions for each classification. You can change the Classification of the document, if the applicable permission is set.

To change the classification:

1. In the Capsule Docs menu, click the arrow next to the current classification name.
   The drop-down list of classifications shows. You can hover over the names of the classifications to see the associated permissions.
2. Select a classification.

**Changing Community**

You can change the community association of the document to any community in which you are a member.

To change the community:

1. In the Capsule Docs menu, click the Settings icon.
   The drop-down list shows all the communities of which you are a member or the administrator.
2. Select a community.
**Removing Protection**

To remove protection:
Do one of these:
- In the Capsule Docs menu, click the Settings icon and select **Remove Protection**.
- Apply **Personal** classification to the document - All classification markings are removed.
- Right-click the document from File Explorer and select **Protect with Capsule Docs > Remove protection**.

**Adding or Removing Users**

To share a document with others, you can add them to the list of authorized users. You can add as many users or groups as your security permissions allow. The added groups can be internal or external. The added users can be categorized as one of these:
- **Internal** - User from one of the internal domains, as defined by the administrator
- **External** - User from a domain other than the internal domains
- **New** - User that was invited to view a document but did not register yet
- **Unknown** - User for which the state cannot be verified (can happen when an error in communication, or on a server, occurs)

To add a user or a group:
1. In the **Add group or people** field of the Capsule Docs menu, enter the name of the group or the email address of a user.
   - **Note** - You can also select a user from the list of users imported from your Outlook address book.
2. Click the plus sign, or press Enter.

**Changing Expiration Settings**

A document author can configure expiration settings for a document. The expiration settings do not apply to the document authors.

This is supported when an R77.30.02 or higher server manages E80.64 or higher clients.

To set expiration settings:
1. In the Capsule Docs menu, go to the **Expiration** tab.
2. Turn expiration **On** and set the expiration date.

To remove expiration settings:
In the **Expiration** tab, turn **Off** expiration.
Creating a Favorites List
You can create Favorites lists to save sets of users with the associated classification settings.

To create a Favorites list:
1. In the Capsule Docs menu, go to the Favorites tab.
2. Enter a name for the new list.
   The new Favorites list includes the users and groups currently listed in the plugin, with their classification settings.

You can also remove unused Favorites lists.

To remove a Favorites list:
In the Favorites tab, click the remove icon next to the list name.

Changing Your Password
To change your password, click the Settings icon from the Capsule Docs menu and select Change Password.

This option is only for users who are not logged in with their Active Directory credentials or with Single Sign-On.

Changing the Author
The author of a document can have different permissions than other document users. If you are an author, you can make additional users or groups authors also.

- A document created with Capsule Docs must have one or more authors. A document created automatically with a tool, such as DLP, might not have an author.
- User Groups can be authors.
- The person who originally protected a document can be the author but does not have to be the author.
- Only an author can set an expiration date on a document. Authors can also view a document that is expired.

Viewing a Protected Document
You must have the Capsule Docs plugin installed to open the protected documents in their native applications. Otherwise, you can view them in the Capsule Docs Viewer.

Using the Client Console
To change the behavior and settings of your Capsule Docs plugin, make configuration changes through the Client Console.

To open the Client Console:
From the Windows Start menu, go to All Programs > Check Point > Capsule Docs > Check Point Capsule Docs.

The Capsule Docs - Client Console window opens.
From the Client Console you can:

- Change logged in user
- View classifications of Capsule Docs communities, in which you are a member
- Enable or disable the Capsule Docs plugin
- Collect diagnostics for troubleshooting

After you make changes, click **Close** to exit the **Capsule Docs Client Console**.

**Logging in as a Different User**

When you install the plugin, your sign-up credentials are used for your default user configuration. You can switch users, if necessary.

**To switch users:**

1. In the **Classification Service** tab of the Client Console, click **Switch User**. The Authentication Credentials window opens.
2. Enter the email and password of a different user.
3. Click **OK**.

**Viewing Classifications from Other Communities**

**To view classifications from a community other than the current default one:**

1. In the **Classification Service** tab of the Client Console, select a Community from the **Show Classifications From** drop-down list.
   The classifications of the selected community are shown in the table view below.
2. Select which classifications you want to see:
   - **All** - includes classifications that are configured in the Community, but are not available to you
   - **Selectable in menu** - includes only classifications that are available to you
   To view permissions set for a specific classification, select that classification from the table. The permissions show in the **Your Rights** section below.

**Updating Capsule Docs Settings**

Settings for the Capsule Docs communities are configured by the administrator.

When you run an update, all the classifications, security settings, users, and groups are updated.

**To run an update:**

1. In the **Classification Service** tab of the Client Console, click **Update Now**. The update progress window opens.
2. Click **Close**, when the update is complete.
Enabling and Disabling the Plugin

When you install the Capsule Docs plugin, it is enabled by default and lets you create and view protected documents. You can disable the plugin for troubleshooting purposes. Before you disable the plugin, close all supported applications.

To temporarily disable the Capsule Docs plugin:
In the Client State tab of the Client Console, click Standby. The client will get enabled after the computer is rebooted.

To completely disable the Capsule Docs plugin:
In the Client State tab of the Client Console, click Disable. The client must be manually enabled.

To enable the Capsule Docs plugin:
In the Client State tab of the Client Console, click Enable.

Note - If you disabled the client with the Disable button, you must restart the computer after you enable it again.

Collecting Diagnostics

You can collect diagnostics data for troubleshooting purposes.

To collect diagnostics data:
In the Diagnostics tab of the Client Console, do one of these procedures:

| To collect only essential system logs: | 1. Click Save Diagnostics.  
  Collect Diagnostic Output window opens.  
  2. Choose a location where you want to save the logs.  
  3. Click Save.  
  Output files are collected and saved in a .cab archive.  
  4. Click OK. |
|---|---|
| To collect a complete set of system logs: | 1. Click Start.  
  The data starts collecting in a set of logs.  
  2. Click Stop.  
  Collect Diagnostic Output window opens.  
  3. Choose a location where you want to save the logs.  
  4. Click Save.  
  Output files are collected and saved in a .cab archive.  
  5. Click OK. |
To collect a detailed log for a specific process:

1. Click **Dump Process**.
2. Select a process in the window that opens.
3. Click **OK**.
   
   The process memory dump is generated.
4. Click **OK**.
   
   **Collect Diagnostic Output** window opens.
5. Choose a location where you want to save the log.
6. Click **Save**.
   
   Output files are collected and saved in a .cab archive.
7. Click **OK**.
Troubleshooting

In This Section:

Technical Difficulties .................................................................................................... 51
Using Logs .................................................................................................................... 51
Collecting Information for Technical Support............................................................. 52

Technical Difficulties

The policies and setting of your Endpoint Security are set by your Endpoint Security administrator. The administrator can solve many issues by making slight changes to your settings. Therefore, if you have technical difficulties, contact your administrator.

Using Logs

Endpoint Security activity is recorded in logs. Your administrator might use information from the logs for various reasons that include:

- To identify the cause of technical problems.
- To monitor Anti-Malware or VPN traffic more closely.
- To see if there is proper communication between your client and other machines that it needs to communicate with.
- To make sure that all features function as they should

To see the logs go to Endpoint Security Main Page > Advanced > View Logs.

What Can I do with Logs

The table below lists actions that you can do in the Log page.

<table>
<thead>
<tr>
<th>What You Want to Do</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>See details of a log entry</td>
<td>Double-click the log entry</td>
</tr>
<tr>
<td>Export logs to a file</td>
<td>Select File &gt; Export to file</td>
</tr>
<tr>
<td>See logs of a specific type</td>
<td>Select View &gt; Event Filter</td>
</tr>
<tr>
<td>See logs from a specific date</td>
<td>Select View &gt; Event Filter</td>
</tr>
<tr>
<td>Sort logs According to a specific column</td>
<td>Click the column heading</td>
</tr>
<tr>
<td>Update the displayed logs one time</td>
<td>Select File &gt; Refresh or click the Refresh icon</td>
</tr>
<tr>
<td>Update the displayed logs every 5 seconds</td>
<td>Select File &gt; Auto Refresh or click the Auto Refresh icon</td>
</tr>
<tr>
<td>Copy log entries to the clipboard</td>
<td>Select the entries and click Control +C</td>
</tr>
</tbody>
</table>
Using the Event Filter

The Event Filter lets you filter the logs to see the information that is relevant to you.

You can filter by:

- **Event types** - Select or clear the checkboxes that relate to the different Endpoint Security features. Only logs of events from the selected features are included in the results.
- **Time period** - Select a **Start** date and time and **End** date and time. Clear either the **Start** or **End** options if you want to keep them blank.
- **Number of events** - Select the maximum number of events that will show in results.
  - **Show Newest or Oldest first** - Select which logs should be at the top of the list.

To use the Event Filter:
1. Open the Event Filter pane:
   - Click the **View Event Filter** window icon.
   - Select **View > Event Filter**.
2. Click the black arrows to open and close the sections of the Events Filter pane.
3. Make selections to filter the log results.
4. Click **Filter**.
   - The results of the filter show in the Log Viewer.

Exporting Logs

You might need to export the logs to a file to send to your administrator.

To export the logs:
1. From the Log Viewer window:
   - Click the Export icon.
   - Select **Edit > Export to File**.
   - The **Save As** window opens.
2. In the **Save As** window, select the location where you want the file to be saved, enter a **File name**, and click **Save**.
   - The logs are saved in a text file.

You can email this file to your administrator.

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 Endpoint Security Main Page select **Advanced** and click **Collect**.
   - A command line window opens.
2. Press **Enter** to run the tool.
3. Wait while the tool runs.
4. When it finishes, it says that a cab file was created and opens the window where the cab file is located.

5. You can email this file to an address that you are given.