# Preface

- Who Should Use This Guide ................................................................. 7
- Feature and Product Names ................................................................. 8
- Summary of Contents .......................................................................... 8
- Product Documentation ........................................................................ 9
- More Information ................................................................................ 10
- Documentation Feedback ..................................................................... 10

## Chapter 1

### Introduction

- Endpoint Security Features ................................................................. 12
- Endpoint Security Deployment Utility .............................................. 13
  - Upgrading Currently Installed Features ......................................... 13
- Installation Options ............................................................................ 13
  - Evaluation on Local Computers ...................................................... 13
  - “Silent” Licensed Working Installation Packages ............................ 14
- Endpoint Security Client Licensing .................................................. 14

## Chapter 2

### Pre-Installation Steps

- Obtaining an Evaluation License ...................................................... 16
- Creating an FDE Installation Profile .................................................. 16
- Creating an Installation Package ....................................................... 17
  - Importing the Default Installation Package .................................. 18
  - Creating and Exporting an Installation Package ......................... 21
  - Suppressing the Reboot Prompt ...................................................... 22
  - Converting the Installation Package to an MSI File ..................... 24
- Running the Deployment Utility ......................................................... 25

## Chapter 3

### Local Computer Deployment

- Evaluation Profiles & Policies ........................................................... 28
- Installation Procedure ....................................................................... 30

## Chapter 4

### Using Installation Packages

- Creating Installation Packages ......................................................... 37
- Deploying an Installation Package ..................................................... 41
  - Pre-Installation Steps ................................................................. 41
  - Running the Installation Package .................................................. 41

## Chapter 5

### Completing the Installation

- Initializing Full Disk Encryption ....................................................... 44
- Defining Endpoint Security Networks .............................................. 46
- Uninstalling Endpoint Security Client ............................................. 47
Chapter 6

**Troubleshooting**

Overview ......................................................................................................... 49
Using CPInfo Scripts...................................................................................... 50
In This Chapter

<table>
<thead>
<tr>
<th>Who Should Use This Guide</th>
<th>page 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature and Product Names</td>
<td>page 8</td>
</tr>
<tr>
<td>Summary of Contents</td>
<td>page 8</td>
</tr>
<tr>
<td>Product Documentation</td>
<td>page 9</td>
</tr>
<tr>
<td>More Information</td>
<td>page 10</td>
</tr>
<tr>
<td>Documentation Feedback</td>
<td>page 10</td>
</tr>
</tbody>
</table>

**Who Should Use This Guide**

This guide is intended for administrators responsible for deploying endpoint security protections within an enterprise, including policy management and user support.

This guide assumes that the reader has an in-depth understanding of the following subjects:

- Network administration
- Operating systems used in network environments (Linux, Unix, Windows, etc.)
- Communication protocols (IP, TCP, UDP etc.)
- Check Point FireWall and VPN-1 concepts and procedures
Feature and Product Names

Previous versions of several Check Point products contained many of the features now contained in Endpoint Security Client. The following cross reference table is presented for the convenience of users currently using these products or who are already familiar with them.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Previous Product Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Disk Encryption</td>
<td>Pointsec PC</td>
</tr>
<tr>
<td>Media Encryption</td>
<td>Pointsec Protector Client</td>
</tr>
<tr>
<td>Port Protection</td>
<td>Pointsec Protector Client</td>
</tr>
<tr>
<td>Firewall</td>
<td>Integrity Client</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>Integrity Client</td>
</tr>
<tr>
<td>VPN Client</td>
<td>SecureClient, SecuRemote</td>
</tr>
</tbody>
</table>

Summary of Contents

This table provides a quick reference to the contents of this guide.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Installation Steps</td>
<td>Describes the steps required before installing Endpoint Security Client or creating installation packages.</td>
</tr>
<tr>
<td>Local Computer Deployment</td>
<td>Presents procedures for installing evaluation versions of Endpoint Security Client on local computers.</td>
</tr>
<tr>
<td>Using Installation Packages</td>
<td>Presents procedures for creating “silent” installation packages that are used to automatically install Endpoint Security Client on client computers.</td>
</tr>
<tr>
<td>Completing the Installation</td>
<td>Describes procedures for completing the installation process and logging on for the first time.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Describes troubleshooting procedures using CPInfo scripts.</td>
</tr>
</tbody>
</table>
# Product Documentation

The Endpoint Security Client documentation set include following materials:

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Disk Encryption Administration Guide</strong></td>
<td>Provides an overview and detailed instructions for configuring and maintaining Full Disk Encryption and for using the Master Installation. This document is intended for administrators.</td>
</tr>
<tr>
<td><strong>Full Disk Encryption Installation Guide</strong></td>
<td>Presents procedures for performing Full Disk Encryption master installation.</td>
</tr>
<tr>
<td><strong>License Server Administration Guide</strong></td>
<td>Provides and overview and detailed instruction for using the Check Point License Server and Reporting Tool utilities.</td>
</tr>
<tr>
<td><strong>Endpoint Security Client Release Notes</strong></td>
<td>Provides an overview of new and improved features as well all known limitations of the current version.</td>
</tr>
</tbody>
</table>
More Information

- For additional technical information about Check Point products, consult the Check Point knowledge base at http://support.checkpoint.com/.
- See the latest version of this document in the User Center at http://www.checkpoint.com/support/technical/documents/

Documentation Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

cp_techpub_feedback@checkpoint.com
Chapter 1

Introduction

In This Chapter

- Endpoint Security Features page 12
- Endpoint Security Deployment Utility page 13
- Installation Options page 13
- Endpoint Security Client Licensing page 14

This document presents the procedures for installing Check Point Endpoint Security Client on a local machine and for creating a self-extracting installation package for deploying Endpoint Security Client on remote client computers. Endpoint Security Client combines firewall, network access control, program control, anti-malware, data security, and remote access, enabling administrators to deploy endpoint security with a single deployment utility.
Endpoint Security Features

The Endpoint Security Client suite consists of the following features:

Table 1  Endpoint Security Client features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Disk Encryption</td>
<td>Provides centrally managed, full disk encryption that protects data, operating systems and temporary files without relying on user interaction. Encryption is transparent to the user, who never needs to bother about what to encrypt or when.</td>
</tr>
<tr>
<td>Port Protection</td>
<td>Controls access to devices through all PC ports, such as IrDA, Com, USB, Firewire and LPT ports. This feature prevents users from connecting unauthorized devices to client machine ports, including hardware such as a modem and provides On/Off/read only protection.</td>
</tr>
<tr>
<td>Media Encryption</td>
<td>Encrypts and protects information stored on removable media, such as USB disks, external disk drives, CDs, DVDs, floppy disks, etc. Access is limited to authorized personnel with the appropriate password.</td>
</tr>
<tr>
<td>Endpoint Security</td>
<td>A collection of endpoint security protections including the following:</td>
</tr>
<tr>
<td>Firewall</td>
<td>Protects endpoint systems by restricting both inbound and outbound traffic, ensuring that they are in a secure state before allowing access to the network and automatically enforcing policies that specify which programs are allowed to run on client machines.</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>Detects and removes viruses, spyware, and other malware based on a combination of signatures, behavior blockers, and heuristic analysis, featuring the highest detection rates and hourly signature updates through the SmartDefense™ update service. Based on the award-winning ZoneAlarm® Internet Security Suite.</td>
</tr>
<tr>
<td>VPN</td>
<td>Enables secure remote access to end users by encrypting and authenticating data transmitted during remote access sessions between endpoints and corporate network.</td>
</tr>
</tbody>
</table>

This document assumes that the reader is familiar with functionality of these features as well as the procedures for configuring and managing them. For more detailed information, refer to the appropriate document as described in “Product Documentation” on page 9.
Endpoint Security Deployment Utility

Endpoint Security Client includes a Deployment Utility, which allows administrators to deploy customized installations to endpoint machines quickly and easily. Administrators typically use “silent” installation packages to deploy licensed working versions on endpoint computers.

Administrators create these silent installation packages using the Deployment Utility. Administrators can also use the Deployment Utility to install licensed, working deployments or evaluation deployments on local computers.

Note - The Deployment Utility does not verify or perform any validation on installation packages. Please ensure that any installation packages used to install Endpoint Security Client are obtained from a trusted source.

Upgrading Currently Installed Features

The Deployment Utility and silent installation packages automatically upgrade currently installed features to the latest version. However, you must remove any Windows Group Policy Object (GPO) deployments prior to using the Deployment Utility.

Installation Options

The Deployment Utility enables you to perform the following types of product installations:

Evaluation on Local Computers

You can install an Endpoint Security Client evaluation on a local computer. The evaluation period is limited to 30 days, after which you must purchase the appropriate license. Users evaluating Full Disk Encryption need to download and install an evaluation license prior to installation.

The evaluation uses a predefined user name and password, which replaces existing user names and passwords. It is important to note that the evaluation version simulates protection, but does not physically secure the local computer. You cannot protect an endpoint client using the evaluation version.
“Silent” Licensed Working Installation Packages

The Deployment Utility allows administrators to create “silent” installation packages that automatically install licensed versions of Endpoint Security Client on endpoint computers without user intervention.

Administrators can use one of the following methods to install licensed working deployments on endpoint computers:

• Remote installation using Microsoft System Management Server (SMS)
• Remote installation by means of a login script
• Deliver the installation package to the end user by email, FTP or other means. The user runs the package, which installs Endpoint Security Client without user intervention.

Endpoint Security Client Licensing

For all working deployments, you must obtain the appropriate license(s) for the Endpoint Security Client features and install this license on the appropriate feature server or the Check Point License server. Evaluation deployments that include Full Disk Encryption require a special evaluation license, which is available from any Check Point partner or reseller.
Chapter 2

Pre-Installation Steps

- Obtaining an Evaluation License  page 16
- Creating an FDE Installation Profile  page 16
- Creating an Installation Package  page 17

This chapter presents several procedures that must be completed prior to using the Deployment Utility to install Endpoint Security Client.
Obtaining an Evaluation License

Endpoint Security evaluations require an evaluation license. Evaluation licenses can be obtained from the Check Point User Center at http://usercenter.checkpoint.com.

Creating an FDE Installation Profile

Administrators create Full Disk Encryption installation profiles, consisting of configuration sets and profiles, prior to using the Deployment Utility to install a licensed working deployment. When using the Deployment Utility to install Full Disk Encryption, you must define a path to the installation profile file (.isp). Evaluation versions use predefined profiles and no further configuration steps are required.

The procedures for defining configuration sets and profiles is beyond the scope of this document. Please refer to the Full Disk Encryption Administration Guide for detailed information and procedures.
Creating an Installation Package

In This Section

- Importing the Default Installation Package  page 18
- Creating and Exporting an Installation Package  page 21
- Suppressing the Reboot Prompt  page 22
- Converting the Installation Package to an MSI File  page 24

Administrator must create appropriate Endpoint Security installation packages (.msi) for licensed working deployments on end user computers before using the Deployment Utility. Evaluation versions use the default installation packages and do not require any further configuration steps.

The process for creating an installation package consists of the following steps:

1. Importing the default Endpoint Security installation package from the installation CD, or from a shared network folder, into Endpoint Security Dashboard
2. Creating and exporting your deployment package to a shared network folder
3. Converting the installation executable file into an .msi file

The following sections describe these procedures. These descriptions assume that the administrator is familiar with Endpoint Security management. For further details, please refer to the Endpoint Security Administration Guide.

Note - When installing or upgrading a licensed working deployment, make certain that you use the installation packages (.msi) from the installation CD.
Importing the Default Installation Package

To import the default installation package:

1. Using your Internet browser, navigate to and log in to Endpoint Security Dashboard. The **Main** window opens.
2. In the **Main** window, click **Client Configuration**. The **Client Configuration** window opens.

![Client Configuration window](image)

3. Click **Manage Installer Versions**. The **Client Package Installer Versions** window opens.

![Client Package Installer Versions window](image)
4. Click New. The Import Client Installer window opens.

![Import Client Installer Window](image)

a. Enter the version number in the designated field. The version number consists of a maximum of nine numeric digits separated by at least one decimal point (for example: 7.0.843.000).

b. Select a language from the list.

c. Enter the fully qualified path to the default installation file (.msi) on the distribution media, or a shared network folder, in the designated field.

d. Click Export to continue. The Client Package Installer Versions window appears, showing the newly imported package.

5. Click Back to return to the Client Configuration window.
Creating and Exporting an Installation Package

1. In the **Client Configuration** window, click **New Package** and select a package type from the list. The **New Client** window opens.

![New Client Configuration Window](image)

   a. Enter a name for the package in the designated field. Make sure that the file name contains only alphanumeric characters and contains no spaces.

   b. Select the client version from the **Client Version** drop-down list.

   c. Click **Save** to return to the **Client Configuration** window. The new package appears in the **Package** list.

2. Click the **Export** option under the newly created package. A **Save** window opens.

   a. In this window, enter or browse to the shared network folder in which you wish to save the installation executable file.

   b. Close the window.

The executable installation file now appears in the designated shared network folder. You can now exit the Endpoint Security Dashboard.
Suppressing the Reboot Prompt

You can optionally configure the Endpoint Security installation package to suppress the reboot prompt after installation.

To suppress the reboot prompt:

1. From the Main window, select Client Configuration.

2. In the Client Configuration Window, select the desired client package and then click Edit under the package name. The Edit Client window opens.
3. In the **Edit Client** window, click the **Advanced Settings** tab.

4. Enter the text string `REBOOT=R` in the **Custom Parameters** field.

5. Click **Save** to return to the **Client Configuration** window.

6. Click the **Export** option under the newly created package. A **Save** window opens.
   a. In this window, enter or browse to the shared network folder in which you wish to save the installation executable file.
   b. Close the window.
Converting the Installation Package to an MSI File

Endpoint Security, by default, creates installation packages as executable (.exe) files. Although you can use the executable package files with the deployment utility, we recommend that you convert them to .msi files first.

To do so, perform the following steps:

1. From a Windows command line, navigate to the shared network folder containing the newly created installation executable file.
2. Make this folder the current folder.
3. Enter the executable file name followed by `-msi` and then press Enter.
   (for example: `MyInstaller -msi`)

The operating system creates the .msi file in the same folder. You then use this file when configuring Endpoint Security using the Deployment Utility.
Running the Deployment Utility

To install Endpoint Security Client on a local computer or to create an automatic installation package:

1. Insert CD 1 or into a drive. If the Deployment Utility runs automatically, the **Welcome** window opens. If the Deployment Utility does not run automatically, run **Setup.exe** in the CD root directory.

2. The **Welcome** window opens.
Chapter 3

Local Computer Deployment

In This Chapter

Evaluation Profiles & Policies  page 28
Installation Procedure  page 30

This chapter describes the procedures for installing Endpoint Security Client on a local computer, either as an evaluation or as a fully licensed working deployment.
Checkpoint Endpoint Security Client comes with predefined evaluation profiles and security policies for all components. This section describes these profiles and policies for each of the components.

**Port Protection**

**Low Security Profile:**
- Removable devices are permitted and users may freely encrypt and decrypt them.
- Scanning and authorization are not required.
- Users can disable and enable the Removable Media Manager, the Device Manager and the Program Security Guard.
- Selected actions are recorded in the log and generate alerts.

**Medium Security Profile**
- Removable devices are permitted, but must be scanned and authorized. Users may delete infected files to enable authorization.
- Users can disable and enable the Removable Media Manager, the Device Manager and the Program Security Guard.
- All events are recorded in the log.

**High Security Profile:**
- Removable devices are blocked.
- Users cannot encrypt removable devices.
- Users cannot disable the Removable Media Manager, the Device Manager or the Program Security Guard.
- All events are recorded in the log.
**Network Security**

**Low Evaluation Profile:**
This evaluation policy is set to a "low" level that allows nearly all end user activity. This policy is designed for observing endpoint behavior and testing client deployment.

- Newly-detected network locations are assigned to the **Internet Zone**, which is set to the **Low** security level allowing unrestricted traffic and maximum functionality.
- The security level for the **Trusted** zone is also set to **Low**.
- Unknown programs can access the network as either clients or servers.
- Connectivity alerts let administrators confirm connections to the server.
- Anti-Virus and Anti-Malware protection is enabled
- SmartDefense is enabled
- Entries are recorded in the logs for all traffic.

**High Evaluation Profile:**
This evaluation policy demonstrates high security and will block legitimate as well as suspicious traffic.

- Newly-detected network locations are assigned to the **Internet Zone**, which is set to the **High** security level blocking most traffic.
- Flex users can add locations to their personal **Trusted Zones**.
- Program Control blocks unknown programs from accessing the network. This policy produces a high number of alerts for evaluation purposes.
- Anti-Virus and Anti-Malware protection is enabled
- SmartDefense is enabled
- Entries are recorded in the logs for all traffic.
This section presents the steps for installing an evaluation of Endpoint Security Client on a local computer. You can install a full evaluation of all features or a custom evaluation where you select specific features to evaluate and choose an evaluation profile for each feature.

To Install an Endpoint Security Client evaluation:

1. From the Welcome window, select Evaluate.
2. Select Yes to accept the end user license agreement.

3. The **Evaluation Options** window opens. To include **Data Security** features in your evaluation, enable one or more of the feature options.

   a. If you enable the **Firewall** feature, select one of the evaluation profile options. The default is **High**. See “**Network Security**” on page 29 for a description of the various profiles.
4. To include **Data Security** features in your evaluation, enable one or both of the feature options.

   a. If you enable the **Port Protection** feature, select one of the evaluation profile options. The default is **High**. See “**Port Protection**” on page 28 for a description of the various profiles.

5. Select an interface language from the list. The default is English.
6. In the User Credentials window, enter the evaluation user name, passwords and password confirmation in the designated fields.

   a. If you are installing a Full Disk Encryption evaluation, enter the path to the location where the recovery information is to be stored. The recovery information allows you to recover your data in the event that you cannot log onto or access your encrypted disk.
7. In the **Evaluation License** window, add the license file that you received from your reseller or the Check Point User Center. An evaluation license is required to evaluate Endpoint Security Client.

You have two options for adding an evaluation license:

a. Click **Fetch From File** to import a license file. In the **Open** window, enter a path or navigate to the evaluation license file.

**Warning** - Make certain that the evaluation license is valid for this installation. An invalid or expired evaluation license may cause the installation to fail without warning.
b. Click **Add** to manually add the license information or to paste the license information from the clipboard.

8. In the **Important Notice** window, read the notice carefully and then click **Yes**. Click **Install** to proceed with the installation.
9. If you installed Media Encryption, copy the CPMEview.exe file from the Media Encryption folder on the distribution CD to your local computer. This utility allows you to view Media Encryption logs.

Chapter 4

Using Installation Packages

In This Chapter

Creating Installation Packages  page 37
Deploying an Installation Package  page 41

This chapter presents procedures for creating “silent” installation packages using the Deployment Utility and for installing Endpoint Security Client on local computers using these packages.

Creating Installation Packages

This section describes the procedure for creating a “silent” installation package for licensed working deployments. Administrators and end users use silent installation packages to install Endpoint Security Client on endpoint computers without user intervention.
To create a new installation package:

1. In the *Distribution Method* window, select **Create a licensed working distribution package**.

2. Select **Yes** to accept the EULA.
3. In the Configuration window, select the features you wish to install.

![Check Point Endpoint Security - R71 Configuration](image)

a. If you enabled **Firewall / Anti-Malware / VPN**, enter or navigate to the path containing the desired Endpoint Security profile.

b. If you enabled **FDE**, enter or navigate to the path containing the desired Full Disk Encryption installation profile.

c. If you enabled **Media Encryption / Port Protection**, enter the Media Encryption Server IP address or network name together with the port.

![Warning](image) **Warning** - You must configure the client firewall to allow UDP traffic over the port designated above.

4. In the **Confirmation** window, verify the features and installation type. If you wish to add or delete features, or to change the configuration, click **Back** to go to the appropriate window and then change the configuration settings.

a. Enable the **Ask the user to verify the installation file** option to create a checksum that ensures the validity of the installation package.

b. Enter the destination path for the installation package file in the designated field.

5. Click **Next** to create the installation package. This process may take several minutes, depending on your configuration.
6. When the **Finished** window appears, click **Finish**. The package location appears in this window.

![Image of the Finished window with package location and checksum]

**Note** - The checksum appears in this window if you selected the **Ask the user to verify the installation file** option. You should provide this checksum to endpoint users, together with the installation package, so that they can verify the validity of the package.

- To view the installation log, click **Open**.
- To install this package on your local computer, enable the Install **Locally** option.
Deploying an Installation Package

This section describes the end-user procedure for installing a licensed working version of Endpoint Security Client on a remote machine using a “silent” installation package.

Pre-Installation Steps

Perform the following steps before installing Endpoint Security Client on your computer:

1. Obtain the silent installation package executable file from your system administrator and copy it to a temporary directory.
2. Obtain the verification check sum from your system administrator (if required).
3. Obtain special login credentials, if your installation package includes Full Disk Encryption.
4. Terminate any running applications and close any open windows on your computer.

Running the Installation Package

To deploy Endpoint Security Client using an installation package:

1. Locate and run the silent installation package executable. This installation is really silent - no user interaction is required until the computer reboots.

   **Warning** - Please be patient. The silent installation process may take some time to complete, and no messages or other user feedback appears on the window. Do not run any programs and do not perform any other actions on the computer until the computer reboots and the silent installation process finishes.

2. If the administrator requires checksum validation, the Installation Verification window opens.

   ![Installation Verification Window]

   If the checksum appearing in this window matches the checksum provided by the administrator, click **Yes**. If the checksums do not match, click **No** and contact the administrator. This situation could result from using an incorrect, forged or corrupt installation package.
3. You will be prompted to reboot your computer.
   – Click **Yes** to reboot immediately
   – Click **No** to reboot manually later.

   The installation process may take several minutes to complete depending on your system and configuration.
Chapter 5

Completing the Installation

Initializing Full Disk Encryption  page 44
Defining Endpoint Security Networks  page 46

This section describes procedures that need to be performed once the installation has finished and the endpoint computer reboots.
Initializing Full Disk Encryption

If you installed Full Disk Encryption, complete the following steps to initialize the system and perform initial disk encryption:

1. When the computer reboots, a pre-boot login window opens.

   ![Login Window](image)

   If you installed the evaluation version, an information window opens. Click OK to continue to the login window.

   a. Log in using the evaluation credentials that you defined in the Deployment Utility. Your normal login credentials will not be accepted. The disk encryption process begins. Disk encryption may take a long time to complete. Do not turn off your computer while encryption is in process.

   b. The following window appears once the encryption is complete. Click Continue.

   ![Login Successful](image)
2. The normal Windows login window appears. Log in using your administrator credentials. If you installed the evaluation version, click **OK** to log in without a password.

![Log On to Windows](image)
Defining Endpoint Security Networks

If Endpoint Security Client displays a **New Network** window, similar to the below example, enter a name for the network and select a security zone from the list.

![New Network Window](image)

If you have multiple interfaces on your computer, this window will appear once for each interface.
Uninstalling Endpoint Security Client

There is no uninstall utility for the Endpoint Security Client. You must uninstall each feature individually.

To uninstall features, use the Add or Remove Programs option in the Windows Control Panel. Select a feature and follow the instructions on the screen. Repeat this step for each feature. You may be required to reboot your computer several times during this process.

The uninstallation process is the same for both evaluation versions and licensed working deployments, with the following exception:
Troubleshooting

Overview

CPInfo is collection of command line scripts that collects information from Endpoint Security Client computers. This information assists technical support engineers to analyze and resolve problems.

When executed on a target client, these scripts collect the required information automatically without user intervention. In some instances this operation may take significant time to complete. While the script is gathering information, the cursor continues to blink and activity messages occasionally appear.

Using CPInfo Scripts

This chapter describes troubleshooting procedures using CPInfo scripts.
Using CPInfo Scripts

Use CPInfo if you encounter issues while installing or working with Endpoint Security Client.

**To run a CPInfo script:**

1. Execute one of the commands shown in the following table:

<table>
<thead>
<tr>
<th>Component</th>
<th>Location of CPinfo Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Components</td>
<td>C:\Program Files\Common Files\Check Point\CPInfo\CPInfoRunAll.cmd</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>C:\Program Files\Common Files\Check Point\CPInfo\FDECPInfo.cmd</td>
</tr>
<tr>
<td>Media Encryption</td>
<td>C:\Program Files\Common Files\Check Point\CPInfo\PDPCPINFO.CMD</td>
</tr>
<tr>
<td>Firewall, Anti Malware and VPN Client</td>
<td>C:\Program Files\Common Files\Check Point\CPInfo\SACPInfo.cmd</td>
</tr>
</tbody>
</table>

2. Each script produces several files compressed into a .cab archive file stored in the same directory as the CPInfo executable. If you ran the CPInfoRunAll script, all of the .cab archives are stored in a single .zip archive file.
   
   - The archive files are stored at the following location or in its subdirectories: C:\Documents and Settings\Administrator\CheckPoint\CPInfo\Output
   
   - The archive files are named according to the date and time of creation in the following format:CPInfo_<date>_<time>.cab.

   Example: CPInfo_PC-HECA-HPNC64_2007-06-08_13.17.18.cab

3. Send these files to your technical support engineer.