HARMONY

21 March 2025

HARMONY ENDPOINT WEB MANAGEMENT

R81.10

Administration Guide

Check Point Copyright Notice

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.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R81.10 Harmony Endpoint Web Management Administration Guide

For more about this release, see the R81.10 home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

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

Patent Notice

Check Point Harmony Endpoint Web Management is protected by the following patents in the United States and elsewhere.
This page is intended to serve as notice under 35 U.S.C. § 287(a):
US7,340,770, US7,540,013, US7,546,629, US7,627,896, US7,725,737,US7,788,726, US7,930,744, US8,074,277, US8,136,149, US8,136,155,US8,161,188, US8,200,818, US8,281,114, US8,370,934, US8,769,268,US8,843,993, US9,208,317, US9,298,921, US9,356,945, US9,536,090,US9,686,307, US9,888,032, US10,050,995, US10,193,906, US10,291,634,US10,382,493, US10,440,036, US10,462,160, US10,467,407, US10,511,616,US10,567,395, US10,728,266, US10,880,316, US10,972,488, US11,165,820,US11,606,375, US11,960,606

Revision History

Date	Description
20 November 2024	Updated the *"Supported Operating Systems for the Endpoint Client" on page 20* topic.
30 September 2024	Updated the *"Super-Node" on page 166* topic.
24 June 2024	Added *"Downloading Forensics Reports" on page 204*.
29 March 2023	Connection Awareness now supports macOS. See *"Connection Awareness" on page 166*.
30 January 2023	Added *"Check Point Full Disk Encryption Self-Help Portal" on page 111*.
17 January 2023	Added a new field *"Enable visual impaired support in pre-boot environment" on page 104* in *"Advanced Pre-boot Settings" on page 103*.
06 December 2022	Remote Command, Isolate Computer and Release Computer push operations are supported for macOS-based endpoints. See *" Performing Push Operations" on page 206*.
02 December 2022	Added the following *" Performing Push Operations" on page 206*: ■ Search and Fetch files ■ Registry Actions ■ File Actions ■ VPN Site ■ Collect Processes
01 December 2022	Added Initial Encryption information in *"Check Point Disk Encryption for Windows" on page 101*.
11 November 2022	Added information about High-Availability out-of-sync alert. See *"Monitoring Harmony Endpoint Deployment and Policy" on page 60*.
05 August 2022	Added information about the new Self-Unlock feature.
14 July 2022	Updated *"Uninstalling Third-Party Anti-Virus Software Products" on page 64*

Date	Description
13 July 2022	Added information about the new Easy Unlock feature. It allows you to **Accept** or **Reject** a **Network One-Time Logon** request or a **Network Password Change** request from a user who has forgotten the login credentials of the endpoint or the endpoint is locked due to invalid login attempts using incorrect credentials. **Note** - This feature is available only to customers in the Early Availability program.
20 June 2022	Added automatic deployment information for macOS and Linux. See *"Automatic Deployment of Endpoint Clients" on page 29*.
07 June 2022	Updated *"Configuring Clients for Non-Persistent Desktops" on page 234*
17 May 2022	Updated *"Viewing Computer Information" on page 73* about viewing click logs by IP address.
17 May 2022	Updated *"Adding Exclusions to Rules" on page 89*
31 March 2022	Added *"Supported Operating Systems for the Endpoint Client" on page 20*.
07 March 2022	Added *"Compliance" on page 143*.
04 March 2022	Added *"Uninstalling Third-Party Anti-Virus Software Products" on page 64*.
03 March 2022	Added *"Harmony Endpoint for Terminal Server / Remote Desktop Services" on page 252*.
03 March 2022	SUSE Linux enterprise server (SLES) and OpenSUSE are supported only with the Anti-Malware blade. Refer *"Harmony Endpoint for Linux Overview" on page 222*.
25 February 2022	Updated *"Configuring Clients for Non-Persistent Desktops" on page 234*
07 February 2022	Added *"Customized Browser Block Pages" on page 161* to the *"User Interface" on page 160* topic.
28 January 2022	Updated: ■ Web and Files Protection.
12 January 2022	Updated: ■ Configuring Threat Prevention Policy

Date	Description
9 January 2022	Updated: ■ VDI Configure Clients for Non Persistent Desktops
6 January 2022	Added: ■ IOC Management
3 January 2022	Updated: ■ VDI-Assigning-Policies-to-VDI-Pools ■ VDI-Basic-Golden-Image-Settings ■ VDI Configure Clients for Non Persistent Desktops ■ VDI-Configure-Clients-for-Persistent-Desktops ■ VDI-Limitations ■ VDI-Overview Removed: ■ VDI-Appendix
3 January 2022	Updated: FileVault Encryption for
2 January 2022	Updated: ■ Connected, Disconnected & Restricted ■ Policy Operation
29 December 2021	Updated: ■ Managing Users in Harmony Endpoint
26 December 2021	Added: ■ Managing Users in Harmony Endpoint
15 December 2021	Updated: ■ Authentication before the Loads (Pre boot)
13 December 2021	Added: ■ Super Node
12 December 2021	Added: ■ VDI Overview

Date	Description
11 December 2021	Updated: ■ *"Adding Exclusions to Rules" on page 89*
8 December 2021	Updated: ■ Deploying Harmony Endpoint for Linux
29 November 2021	Updated: ■ Performing-Push-Operations
14 November 2021	Added: ■ Connection Awareness Updated: ■ Configuring Client Settings ■ Connected, Disconnected and Restricted Rules
10 November 2021	Updated: ■ Connected, Disconnected, Restricted and Connection Awareness Rules
04 November 2021	Updated: ■ Active Directory Authentication
02 November 2021	Updated: ■ *"Configuring Endpoint Policy" on page 82*
31 October 2021	Updated: ■ *"User Interface" on page 160*
14 October 2021	Updated: ■ Deploying Endpoint Clients
13 October 2021	Updated: ■ Introduction
10 October 2021	Added: ■ *"Recent Tasks" on page 258*

Date	Description
01 October 2021	Updated: ■ *"Automatic Deployment of Endpoint Clients" on page 29* ■ *"Remotely Installing the Initial Client" on page 54*
26 September 2021	Added: ■ *"Configuring Client Settings" on page 160* Updated: ■ *"Adding Exclusions to Rules" on page 89*
13 September 2021	Updated: ■ *"Deploying Endpoint Clients" on page 27* ■ *"Firewall" on page 128* ■ *"BitLocker Encryption for Windows Clients" on page 108*
31 August 2021	Added: ■ *"Connected, Disconnected and Restricted Rules" on page 170* Updated: ■ *"Web & Files Protection" on page 84*
15 July 2021	Updated: ■ *"Developer Protection" on page 141*
28 June 2021	First release of this document

Table of Contents

Introduction to Endpoint Web Management

From R81, Check Point offers a new Web-based management interface for Endpoint components.

Currently the new web-based UI supports Harmony Endpoint and Full Disk Encryption.

In the future, all Endpoint components are planned to be supported by this Web UI.

The-user interface is already available for cloud management customers.

From R81, it is also available for on-premises customers.

Harmony Endpoint supports up to 400,000 endpoint clients.

Note - A Domestic Homeland Security (DHS) compliant Anti-Malware blade (or non-Kaspersky Anti-Malware blade) supports only periodic and contextualized scan (In the endpoint, right-click a file, and click **Scan with Check Point Anti-Malware**).

Logging into Endpoint Web Management Console

1. Install an Endpoint Security Management Server.

   See the *R81.10 Installation and Upgrade Guide* > Chapter *Installing an Endpoint Server* > Section *Installing an Endpoint Security Management Server*.

2. Connect with SmartConsole to the Endpoint Security Management Server.
3. Enable the required Software Blades:
   a. From the left navigation panel, click **Gateways & Servers**.
   b. Open the Endpoint Security Management Server object.
   c. On the **Management** tab, select these Software Blades:
      - Endpoint Policy Management
      - SmartEvent Server - Required for the **Security Overview** tab only.
   d. Click **OK**.
4. Install the database:
   a. Click **Menu** > **Install database**.
   b. Select the Endpoint Security Management Server.
   c. Click **Install**.
5. Start the Endpoint Web Interface:
   a. Connect to command line on the Endpoint Security Management Server.
   b. Log in to the Expert mode.
   c. Run:

      ```
      web_mgmt_start
      ```

6. Connect with a web browser to:

   ```
   https://<Main IP Address of Endpoint Security Management Server Object>/sba/index.html
   ```

   Log in with the same credentials you use to log in to SmartConsole.

Note - The default port is 443. If you have upgraded from R80.40 or older, then the default port is 4434. If you have changed default port, then use the updated port number.

```
https://<Main IP Address of Endpoint Security
Management Server Object>:<port
number>/sba/index.html
```

Supported Operating Systems for the Endpoint Client

Microsoft Windows

Microsoft Windows

Version	Editions	Supported starting from
11 LTSC (version 24H2)	Enterprise Pro	Endpoint Security Client E88.41 VPN Standalone Client E88.40
11 24H2	Enterprise Pro	Endpoint Security Client E88.41 VPN Standalone Client E88.40
11 23H2	Enterprise Pro	Endpoint Security Client E87.62 VPN Standalone Client E87.60
11 22H2	Enterprise Pro	Endpoint Security Client E86.70
11 21H2	Enterprise Pro	Endpoint Security Client E85.40
10 22H2	Enterprise Pro	EA support: Endpoint Security Client E86.80 GA support: Endpoint Security Client E87.00
10 LTSC (version 21H2)	Enterprise Pro	Endpoint Security Client E86.00
10 21H2	Enterprise Pro	Endpoint Security Client E86.00
10 21H1 (version 2103)	Enterprise Pro	Endpoint Security Client E85.00
10 20H2 (version 2009)	Enterprise Pro	Endpoint Security Client E85.00
10 20H1 (version 2004)	Enterprise Pro	Endpoint Security Client E85.00
10 19H2 (version 1909)	Enterprise Pro	Endpoint Security Client E85.00
10 19H1 (version 1903)	Enterprise Pro	Endpoint Security Client E85.00
10 LTSC (version 1809)	Enterprise Pro	Endpoint Security Client E85.00
10 (version 1809)	Enterprise Pro	Endpoint Security Client E85.00
10 (version 1803)	Enterprise Pro	Endpoint Security Client E85.00
10 (version 1709)	Enterprise Pro	Endpoint Security Client E85.00
10 LTSB (version 1607)	Enterprise Pro	Endpoint Security Client E85.00
8.1 Update 1	Enterprise Pro	Endpoint Security Client E85.00
7 SP1 Microsoft update KB3033929	Enterprise Professional	Endpoint Security Client E85.00

Notes:

- For existing Endpoint Security deployments, before upgrading your OS version, you must first upgrade the Endpoint Security Client to a version that supports the desired OS version based on the table above.
- For additional information on Windows 7 support, refer to sk164006.
- Windows Operating Systems are supported according to Check Point Client Support life cycles, also on Virtual Machines. However, there is no dedicated QA process for all possible variants of Windows. If you encounter a specific issue related to a different edition of a supported Windows OS version, Check Point will provide best-effort support through R&D assistance.

Microsoft Windows Server

Version	Editions	Supported starting from	Supported Features
2025 64-bit	All	E88.61	Anti-Bot and URL Filtering, Anti-Malware, Anti-Ransomware, Behavioral Guard and Forensics, Compliance and Posture, Firewall and Application Control, Media Encryption and Port Protection, Threat Emulation.
2022 64-bit	All	E85.40	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client), Media Encryption and Port Protection.
2019 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client), Media Encryption and Port Protection.
2016 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client).
2012 R2 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client)
2012 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client)
2008 R2 32/64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client)

Notes:

- To support Endpoint Compliance rules for Windows Server 2016 on versions older than R80.20, see sk122136.
- Windows Server CORE is not supported.
- If you install a client package with features that are not supported on the server, the installation succeeds but only the supported features are installed.
- The Anti-Exploit feature is supported starting from the 2016 64-bit version.

macOS

macOS Version	Supported starting from
macOS Sequoia (15)	EA support: Endpoint Security Client E88.70 GA support: Endpoint Security Client E89.00
macOS Sonoma (14)	EA support: Endpoint Security Client E87.60 GA support: Endpoint Security Client E87.70
macOS Ventura (13)	EA support: Endpoint Security Client E86.80 GA support: Endpoint Security Client E87.00
macOS Monterey (12)	EA support: Endpoint Security Client E85.30 GA support: Endpoint Security Client E86.20
macOS Big Sur (11)	Endpoint Security Client E84.30
macOS Catalina (10.15)	Endpoint Security Client E82.00

Notes:

- For existing Endpoint Security deployments, before upgrading your OS version, you must first upgrade the Endpoint Security Client to a version that supports the desired OS version based on the table above.
- Starting from E88.30, new features do not include support for macOS 10.15. Starting from E89.00, macOS 10.15 is not supported.

Linux

Distribution/OS Version	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
Ubuntu 24.04 (64-bit)	✓	–	–	–	–	–	–
Ubuntu 22.04 (64-bit) (Supported versions: 22.04 - 22.04.3)	✓	✓	✓	✓	–	–	–
Ubuntu 20.04 (64-bit) (Supported versions: 20.04 - 20.04.6)	✓	✓	✓	✓	–	–	–

Distribution/OS Version	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
Ubuntu 18.04* (64-bit) (Supported versions: 18.04 - 18.04.6)	✓	✓	✓	✓	–	–	–
Ubuntu 16.04 (64-bit)	✓	✓	✓	✓	–	–	–
Debian Linux 12 (64-bit) (Supported versions: 12.0 - 12.5)	✓	–	–	–	–	–	–
Debian Linux 11* (64-bit)	✓	✓	✓	✓	–	–	–
Debian Linux 10* (64-bit)	✓	✓	✓	✓	–	–	–
Debian Linux 9* (64-bit)	✓	✓	✓	✓	–	–	–
Red Hat Enterprise Linux (RHEL) 9[1] (64-bit) (Supported versions: 9.0 - 9.5)	✓	✓	✓	✓	✓	✓	✓
Red Hat Enterprise Linux (RHEL) 8 (64-bit) (Supported versions: 8.0 - 8.9)	✓	✓	–	–	–	–	–

Distribution/OS Version	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
Red Hat Enterprise Linux (RHEL) 8.10 (64-bit)	✓	–	–	–	–	–	–
Red Hat Enterprise Linux (RHEL) 7 (64-bit) (Supported versions: 7.8 and 7.9)	✓	✓	✓	✓	–	–	–
Alma Linux 9 (64-bit) (Supported versions: 9.0 - 9.3)	✓	✓	✓	✓	✓	–	–
Alma Linux 8 (64-bit) (Supported versions: 8.9 and 8.10)	✓	✓	✓	✓	✓	–	–
CentOS 8* (64-bit) (Supported versions : 8.0 - 8.5)	✓	✓	✓	✓	–	–	–
CentOS 7 (64-bit) (Supported versions: 7.8 - and 7.9)	✓	✓	✓	✓	–	–	–
Oracle Linux 8 (64-bit) (Supported versions: 8.0 - 8.10)	✓	✓	✓	✓	✓	✓	✓

Distribution/OS Version	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
Oracle Linux 7.9 (64-bit)	✓	✓	✓	✓	–	–	–
Amazon Linux 2 (64-bit)	✓	✓	✓	✓	–	–	–
SUSE Linux Enterprise Server (SLES) 15 (64-bit) (Supported versions: 15SP2 and 15SP3)	✓	✓	✓	✓	✓	✓	✓
SUSE Linux Enterprise Server (SLES) 12 (64-bit) (Supported versions: 12SP5)	✓	✓	✓	✓	–	–	–
OpenSUSE 15.4 and OpenSUSE 15.5	✓	✓	✓	✓	–	–	–
OpenSUSE 42.3	✓	✓	✓	✓	–	–	–
Fedora 39[1]	✓	✓	✓	✓	–	–	–
Fedora 38[1]	✓	✓	✓	✓	–	–	–
Fedora 37	✓	✓	✓	✓	–	–	–
Fedora 36	✓	✓	✓	✓	–	–	–
Fedora 35	✓	✓	✓	✓	–	–	–

Distribution/OS Version	1.20.7	1.18.16	1.18.12	1.15.10	1.15.7	1.13.3	1.13.2
Fedora 34	✓	✓	✓	✓	–	–	–

[1]Only Anti-Malware support.

Deploying Endpoint Clients

Notes:

- Check Point does not support both the Harmony Endpoint Security client and the Check Point Remote Access VPN client on the same endpoint. Uninstall the Check Point Remote Access VPN client before you deploy the Harmony Endpoint Security client.
- During the upgrade, you cannot remove the Full Disk Encryption component.

To deploy Harmony Endpoint clients to Windows devices:

1. Click **Overview** and then click **Download** on the top banner.

2. Click **Download** button under Windows or macOS, depending on the destination system.

To install the Initial Client:

1. Do any of these to download the Initial Client:

   a. From the left navigation panel, click **Service Management** and then in the Download Initial Client section, click on the **Download** button.

   b. From the left navigation panel, click **Overview**.and then click on the **Download** button on the top banner.

2. Deploy the Initial Client to all your Endpoint devices, using a third party deployment tool.

- **Automatic** - Use deployment rules to automatically download and install pre-configured packages on Endpoint devices (see *"Automatic Deployment of Endpoint Clients" on page 29*).
- **Manual** - Export component packages to the endpoint devices, using third party deployment software, a shared network path, email, or other method (see *"Manual Deployment of Endpoint Clients" on page 36*).

Notes:

- Admins are recommended not to pre-install Harmony Endpoint when using cloning utilities like Acronis. It is recommended to install Harmony Endpoint after the clone is created, or at least to block the initial registration before creating the clone.
- If you have initiated to deploy the Harmony Endpoint Security client on an endpoint that is not yet added to the domain, see the sk18127 to complete the deployment.

Notes:

- In Endpoint Web Management Console, an administrator can only view the MSI packages that were deployed in SmartEndpoint, but cannot upload or download them.
- In Endpoint Web Management Console, an administrator can upload or download only the Dynamic Package (*.EXE).

Installation Token

Token-limited installation protects against sending unauthorized copies of exported packages and installation of packages on computers which do not belong to the organization that created the packages.

Note - Installation token is not supported on macOS and Linux endpoints.

The administrator is responsible for enabling the token-limited installation feature and creating the token.

If token-limited installation is enabled, then you must enter the token during the registration of the Endpoint Security server with the Harmony Endpoint Management Server.

The token is limited in time. If the token is expired, the registration is rejected.

To enable token-limited registration:

1. Go **Settings** > **Authentication Settings** > **Installation Token**.
2. Click **Edit**.
3. In the **Value** field, enter a token.
4. In the **Valid until** field, click  to select the date for the token expiry.
5. Click **OK**.

To copy the token, click  .

Automatic Deployment of Endpoint Clients

Software deployment rules are supported for both Windows and macOS.

Use deployment rules to automatically download and install pre-configured packages on endpoint devices.

To deploy Endpoint Security clients with automatic deployment, install one of these deployment packages on the Endpoint clients.

Automatic Deployment of Endpoint Clients

Tiny Agent

The Tiny Agent functionality introduces a few major improvements to the current Initial Client package (which is a very thin client, without any blade, used for software deployment purposes).

The Initial Client is the Endpoint Agent that communicates with the Endpoint Security Management Server.

You can extract the Initial Client from the Tiny Agent.

The improvements include:

- The Tiny Agent has a very small executable (smaller than 1MB)
- It can be shared in various forms, enabling fast, easy and seamless first-time deployment.
- Once combined with the Dynamic Package, it installs only what is necessary for each machine.
- It is agnostic to the client version.
- It passes Smart Screen validation - no more download warnings
- It reduces network traffic for installing selected blades.

It is available for cloud deployments and for on-premises deployments running Endpoint Security Management Server R81 or higher.

To download the Tiny Agent:

1. Do one of these:
   - Click **Overview**, and then click **Download Endpoint** on the top banner.
   - Click **Policy** > **Deployment Policy** > **Software Deployment,** and then click **Download Endpoint** on the top banner.

   The **Download Harmony Endpoint** window appears.

2. Select a **Download version** and a **Virtual group**, and then click **Download** for an OS.
3. For Windows OS, the system downloads the **EndpointSetup.exe** file. Run the .exe file on the endpoint to install the Harmony Endpoint Security client.

   Note - To extract the `MSI` file, run:
   `EndpointSetup.exe /CreateMSI`

4. For macOS, the system downloads the **EPS_TINY.zip** file. Transfer the zip file to the endpoint.

   Caution - Do not change the **EPS_TINY.zip** file name.

   a. Unzip the file and open the **EPS_TINY** folder.

   b. To install the Harmony Endpoint Security client, do one of these:

      - Run the **EPNano.app** file.
      - In the terminal window, run:

        `./EPNano.app/Contents/MacOS/EPNano`

5. For Linux OS, the system downloads the **installScript.sh** file. Run the **installScript.sh** file on the endpoint to install the Harmony Endpoint Security client.

Note - You can deploy the Initial Client to all your endpoint devices, using a third-party deployment tool, manually or remotely (see *"Remote Installation of Initial Client" on page 48*).

Troubleshooting Issues with the Tiny Agent on Windows OS

The Tiny Agent shows simple error messages in cases of network issues (connectivity problems, proxy issue, and so on).

Error messages and Remediation

Console Error	Description	Remediation
`Endpoint Setup failed!`	Exception occurred (either allocation failed on any internal component, or another type of abnormal termination)	Download the file again and check its signature (it could be corrupted), and make sure you have enough free RAM.
`Failed to initialize Endpoint Setup!`	Either we cannot verify our own signature, or map the installer in the memory.	Make sure you have enough memory.
`Failed to parse internal data!`	Failed to parse the URL for downloading `eps.msi` from CDN	File downloaded from the Management Server is corrupted. Contact Check Point Support.
`Failed to download or verify Windows Installer package (EPS.msi)!`	Failed to verify downloaded `EPS.msi`	Make sure that your Security Gateway, or any network security component, does not corrupt the installer.
`Failed to find program files folder`	Failed to get program files from Microsoft.	Make sure your OS is updated.
`Failed to create our program files folder for config.dat`	Either there is some Check Point product installed, or the Administrator cannot create folders in the Program Files folder	Make sure that the Endpoint Security Client is not already installed.
`Failed to save config.dat`	Either there is some Check Point product installed, or the Administrator cannot create folders in program files folder	Make sure that the Endpoint Security Client is not already installed.
`Failed to install the product`	Cannot run Windows Installer to install `EPS.msi`	Make sure Windows Installer is enabled.

Console Error	Description	Remediation
`Failed to download Windows Installer package (EPS.msi)!`	Failed to download `eps.msi`	Make sure you have access to CDN: sc1.checkpoint.com
`Failed to authenticate EndpointSetup!`	Data corruption occurred, or data added to the file is corrupted	Make sure the file is not corrupted, and/or that you downloaded it from the correct location.
`Failed to parse configuration data`	Failed to find the server config information.	Make sure you downloaded the file from the portal.
`Setup failed another installation is currently in progress`	Another installation is stuck, or has not finished.	Reboot the machine, or fix/complete any pending installation.

Log File Location

The log file is located here:

```
C:\Windows\System32\LogFiles\WMI\EndpointSetup.etl
```

Silent Installation

Run:

```
PsExec.exe -accepteula -nobanner -s "C:\Users\<Administrator Username>\Desktop\EndpointSecurity.exe"
```

Endpoint Security Component Package

This package includes the specified components to be installed on the endpoint device.

You can distribute it automatically with deployment rules.

You can configure the policies for the components before or after you deploy the component package.

Deploy the Endpoint Security component package with deployment rules.

For more details on deployment methods of the Endpoint clients, see the *Harmony Endpoint Server Administration Guide* for your version.

Deployment Rules

Deployment rules let you manage Endpoint Security Component Package deployment and updates.

Deployment rules work on both Windows OS and macOS. Linux OS is **not** supported yet.

The Default Policy rule applies to all Endpoint devices for which no other rule in the Rule Base applies.

You can change the default policy as necessary.

You can define more rules to customize the deployment of components to groups of Endpoint devices with different criteria, such as:

- Specific Organizational Units (OUs) and Active Directory nodes.
- Specific computers.
- Specific Endpoint Security Virtual Groups, such as the predefined Virtual Groups ("All Laptops", "All Desktops", and others.). You can also configure your own Virtual Groups.

Deployment rules do **not** support user objects.

Mixed groups (that include both Windows OS and macOS objects) intersect only with the applicable members in each rule.

To create new deployment rules for automatic deployment

1. From the left navigation panel, click the **Policy** view.
2. Click **Deployment Policy** > **Software Deployment**.
3. From the top toolbar, click **Clone Above** or **Clone Below**.

   The **Clone Rule** window opens.
4. Configure the rule:
   - Enter the rule name
   - Select the groups to which the rule applies.

     Mixed groups (that include both Windows OS and macOS objects) intersect only with the applicable members in each rule.
   - Select the applicable parts of the organization.
   - Select the affected devices.
5. Click **OK** to create the new rule.
6. Click the new rule to select it.
7. In the right section **Capabilities & Exclusions**:
   a. Click **Windows**, **macOS** or **Linux**.
   b. Select the **Version**.

      For Linux, click **distros** to view the supported distributable and version. For example, CentOS or Ubuntu.

      Note - You can use the **Do not install** option to temporarily halt enforcing software deployment rules to the endpoints, for example, during maintenance or internal testing of Harmony Endpoint Security client.
   c. Select **Capabilities**.
      - For Linux, only the Anti-Malware blade is supported with the exported package.

        Note - If the Harmony EndpointAnti-Malware capability is installed, the third-party Anti-Malware status in the Harmony Endpoint Security Client is not displayed.
      - For general limitations on macOS, see sk110975.
8. Configure the deployment settings:

a. Select the applicable package version.

   Caution - The Endpoint Security client package version must match the client package version selected in the exported package. Otherwise, the system discards the capabilities selected in the **Software Deployment** rule.

b. Select the package capabilities.

9. Click **Save**.
10. Above the right section **Capabilities & Exclusions**, click **Install Policy**.

Manual Deployment of Endpoint Clients

You can export a package of Harmony Endpoint or Harmony Browse from the Endpoint Security Management Server to Endpoint devices using a third-party deployment software, a shared network path, email or other method.

When you download a package for manual deployment, the Initial Client is already included in the package for Harmony Endpoint and there is no need to install it separately.

Note - Initial Client is not supported for Harmony Browse.

Important - If you want to switch to a US-DHS and EU compliant Anti-Malware blade, make sure to switch to a complaint Endpoint Security Client before deploying the client. See *Anti-Malware Settings*.

Caution - Windows Server 2016 and higher requires that you turn off Microsoft Windows Defender before you install the Harmony Endpoint Security Client. Perform the instructions in the sk159373 before you install or contact *Check Point Support* to request assistance with the installation.

When you create the package for export, you select your set of components.

The package installation program automatically detects the computer type and installs the applicable components.

Using the Export Package

1. **Upload the package to the package repository**

    a. When you click the package repository icon, located in the toolbar of both the **Export package** and **Software Deployment** tabs, you are redirected to an internal **Package Repository** page.

    b. When you click the "**Upload Agent**" button, a "**Browse**" modal opens. It prompts you to select the relevant file/s (ZIP, EXE) and folder(s) to upload.

    Notes:
    - The administrator can abort an active package upload/download.
    - Packages that are in use cannot be deleted.

2. **Create the package for export**

a. Go to **Policy** >**Export Package**.

b. Do any of these:

   i. To export package for Harmony Endpoint, click **Endpoint Client**.

   ii. To export package for Harmony Browse, click **Browse Client** and continue with *"Export the package or file" on page 43*.

c. Click the plus sign to create a new export package.

   The **Create Export Package** window opens.

d. Enter the **Package Name** and select the applicable **Operating System**.

e. Select an **Operating System**.

   - **Windows**
   - **macOS**
   - **Linux**

f. Select the **Package version**.

g. Select **Capabilities**.

   - For Linux, only the Anti-Malware blade is supported with the exported package.

     Note - If the Harmony EndpointAnti-Malware capability is installed, the third-party Anti-Malware status in the Harmony Endpoint Security Client is not displayed.

   - For general limitations on macOS, see sk110975.

h. To add a new VPN site to the package, see *Adding a New VPN Site to an Exported Package*.

i. Optional: Select a **Virtual group** or create a new one.

   Users who install this package will automatically be part of this virtual group.

   You can use the virtual group to apply a security policy to the entire group instead of to each object in the group separately.

j. Optional: Select a **Software Signature.**

You can select a file signing method for MSI files that will be deployed using an external distribution system. By default, the client uses an internal signature to authenticate.

Select one of these file signing methods:

- None
- Internal Certificate Authority
- Custom - If you select Custom do these steps:
  i. Click **Browse** and get the certificate file (`*.p12`).
  ii. Enter certificate password.
  iii. Click **Validate**.

  The certificate is created on the Endpoint Security Management Server.
  iv. Send the `*.p12` file to client computers before you install the client package.

k. Select the settings for the **Dynamic Package**:

Note - Dynamic package is not supported for macOS and Linux.

i. Select the **Minimize package size (takes longer)** checkbox.

- **General**

  Disable the Endpoint Security Client user interface - for unattended machines, like ATMs.

  To learn about packages for ATMs, see sk133174. By default, the client user interface is included in the package.

- **Dependencies Settings**

  Select the dependencies to include in the package:

  - **.NET Framework 4.6.1 Installer** (60MB) - Recommended for Windows 7 computers without .NET installed.
  - **32-bit support** (40MB) - Selected by default. Recommended for 32-bit computers.
  - **Visual Studio Tools for Office Runtime 10.050903** (40 MB) - Recommended if the package includes Capsule Docs.

- **Smart preboot** (190MB) - Enables the **Easy Unlock** and **Self Unlock** features.

  Easy Unlock allows you to **Accept** or **Reject** a **Network One-Time Logon** request or a **Network Password Change** request from a user that has forgotten the login credentials of the endpoint or the endpoint is locked due to invalid login attempts using incorrect credentials. Such requests are indicated by the icon  in the **Asset Management > Computers** table. See *"Viewing Computer Information" on page 73*. It is supported:

  - Only with Endpoint Security client version 86.50 or higher.
  - Only on endpoints running Windows OS.
  - Only if the **Full Disk Encryption** is **Check Point encryption**.See *"Configuring Full Disk Encryption" on page 99*.

  Self-Unlock allows users to unlock their endpoint by scanning a QR code using their mobile device, without your (Administrator) intervention. It is supported:

  - Only with Endpoint Security client version 86.60 or higher.
  - Only on endpoints running Windows OS.

  Note - If the endpoint is connected remotely (not in the LAN), then ensure that your Endpoint Security Management Server is accessible over internet. Otherwise, you must set up a reverse proxy and specify the **Hide behind IP address** under **NAT** in the SmartConsole. For more information, see the SmartConsole Help.

  Additional settings for the **Self-Unlock** feature:

  i. Specify **Self-Unlock Settings** in **Computer Actions**. See *"Viewing Computer Information" on page 73*.

  ii. Enable **Self-Unlock** for Full Disk Encryption. See *"Advanced Pre-boot Settings" on page 103*.

  Note - **Smart pre-boot** is available only to customers in the Early Availability program.

- **Anti-Malware Settings**

  Select the signature to include in the package.

  This sets the level of Anti-Malware protection from the time that a client gets the package until it gets the latest Anti-Malware signatures from the signature provider:

  - **Full** - Recommended for installing on devices without high-speed connectivity to the Anti-Malware server.
  - **Minimum** - Selected by default. Recommended for a clean installation on devices that are connected to the Anti-Malware server.
  - **None** - Recommended for upgrades only.

ii. Optional: To download the package automatically after the system creates the package, select the **Download package when saved** checkbox.

l. Click **Finish**.

The system starts to create the package. It can take several minutes depending on the package size. When the package is ready, the system shows **Exported Package created** message.

Note - You can duplicate the package configuration for future use. Click the ⋮ icon.

3. **Export the package or file**

In the export package tile, click ⬇ to download the package or file.

Client	OS	Downloaded file
Endpoint	Windows	*EPS_<Year>_<Version>.exe*
	macOS	*EPS_TINY.zip*
	Linux	*installScript.sh*
Browse	Windows	*BrowserSetup.exe*
	macOS	*BrowserSetup.zip*
	ChromeOS	*BrowserSetup_chromeOS_Laptop.exe* or *BrowserSetup_chromeOS_Desktop.exe*

Note - Dynamic package is not supported for Harmony Browse.

4. Continue with *"Installing the Exported Package or Client" below*.

Installing the Exported Package or Client

You can also use a third-party deployment software, a shared network path, email, or some other method to distribute the package or file.

Endpoint Client

1. For Windows, distribute the downloaded package or file to users' endpoint or run the *EPS_<Year>_<Version>.exe /CreateMSI* on the users' endpoint.

   On Windows 8.1 and higher, right-click the *exe* file and click **Run as administrator** to install the client.

   The *EPS_<Year>_<Version>/CreateMSI* command is supported only with the Endpoint Security Client E85.20 or higher. It is supported for both 32-bit and 64-bit Windows.

   You can install the Endpoint Security client using the **EPS.msi** file through the Command Line Interface (CLI). To install:

   a. Transfer the **EPS.msi** file to the endpoints.

   b. In the endpoint's CLI, run:

      ```
      msiexec.exe /i <path to msi file>\EPS.msi
      ```

      For example, `msiexec.exe /i C:\users\admin\EPS.msi`

      Output

      ```
      USERINSTALLMODE=<blades' mask>

      Generating MSIs. It will take a few minutes.

      Please wait...

      ===> <location>\EPS.msi

      ===> <location>\32\EPS.msi
      ```

      The system creates the *msi* files for both 64-bit and 32-bit and opens Windows Explorer windows where the *msi* files are created.

   c. Make a note of the path where *msi* files are created.

   d. In the **Command Prompt** window, press any key to close.

   e. Transfer the *msi* file to the endpoints and run the *msi* file to install the Harmony Endpoint Security client.

   For more information, see sk179668.

2. For macOS, distribute the package or file to users' endpoint.
3. For Linux, run the *sh* script in the users' endpoint.

Browse Client

1. For Windows, distribute the downloaded package or file to users' endpoint or run the *EndpointSetup.exe /CreateMSI* on the users' endpoint.
2. For macOS, distribute the package or file to users' endpoint.
3. For ChromeOS, see sk173974.

You can only see the deployment status after the package is successfully installed.

Time Limit Installation

If you have enabled *"Installation Token" on page 28*, a prompt appears during the Endpoint Security client installation. The user must enter the **Server Authentication Token**.

If the server authentication fails, create a new server authentication token with the appropriate validity period and share it with your users.

Adding a New VPN Site to an Exported Package

When you use an exported package, you can configure each package to connect to a default VPN site which you create.

By default, no VPN site is configured for a new package.

To add a new VPN site to an exported package:

1. Create a package or edit an export package. See *"Manual Deployment of Endpoint Clients" on page 36*.
2. In the **Capabilities** screen of the **Create Export Package** wizard, select the **Remote Access VPN** checkbox.
3. In the **Virtual Groups and VPN Sites** screen, in the **VPN site** section:
    a. To add a VPN site manually, select **Manual**:
        i. Click **New** and enter these:
            - **Name** - Unique name for this VPN site.
            - **Site Address** - Site IP address.
            - **Authentication Method** - One of these:
                - **Username-password** - Endpoint users authenticate using their VPN user name and password.
                - **CAPI certificate** - Endpoint users authenticate using the applicable certificate.
                - **P12 certificate** - Endpoint users authenticate using the applicable certificate.
                - **SecurID KeyFob** - Endpoint users authenticate using a KeyFob hard token.
                - **SecurID PinPad** -Endpoint users authenticate using the an SDTID token file and PIN.
                - **Challenge-response** - Endpoint users authenticate using an administrator supplied response string in response to the challenge prompt.
        ii. Click **OK**.

b. To add a VPN site by importing a *.config* file, select **Import from file**:

   i. Click **Upload** and select the *.config* file you want to upload.

   Note - Only *.config* file with a maximum file size of 1000 KB is supported.

   ii. Click **Next** and continue with step **i** in **Create an export package**. See *"Manual Deployment of Endpoint Clients" on page 36*.

Remote Installation of Initial Client

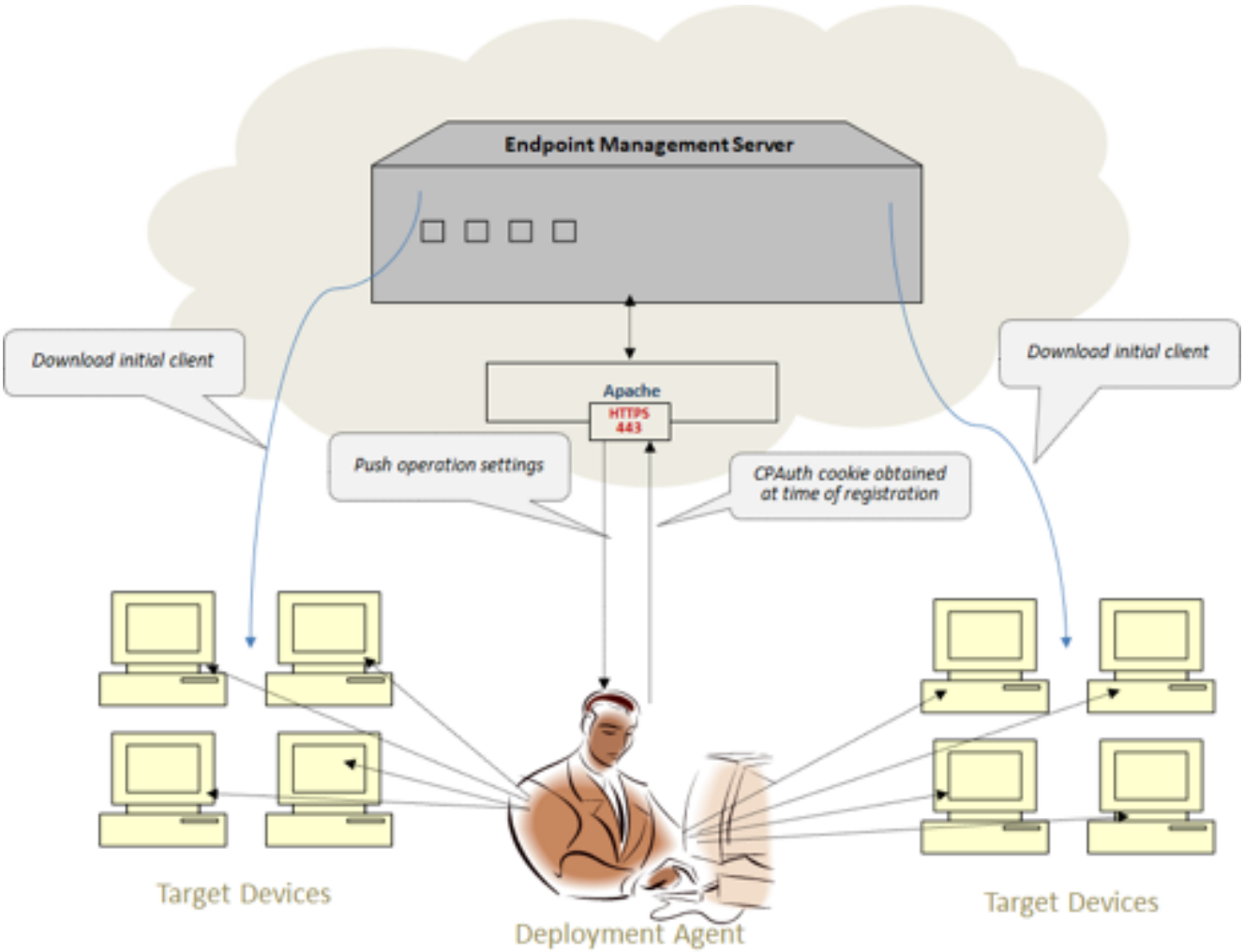
The Initial Client is the Endpoint Security agent that communicates with the Endpoint Security Management Server.

You install the Initial Client on Endpoint devices before you use automatic software deployment to deploy components.

The remote installation is the installation of an Initial Client on an Endpoint Security component package.

In Endpoint Security Client E84.40 and higher, you can now install the Initial Client remotely without third party tools such as Microsoft System Center Configuration Manager (SCCM) or Intune.

The Push Operation mechanism extends to devices that do not have the Initial Client installed yet.



Setting the Deployment Agent

The Deployment Agent is the cornerstone of the remote push feature. The agent is a domain-joined device that you select as an initiator for remote installation requests on target workstations in the same Active Directory domain.

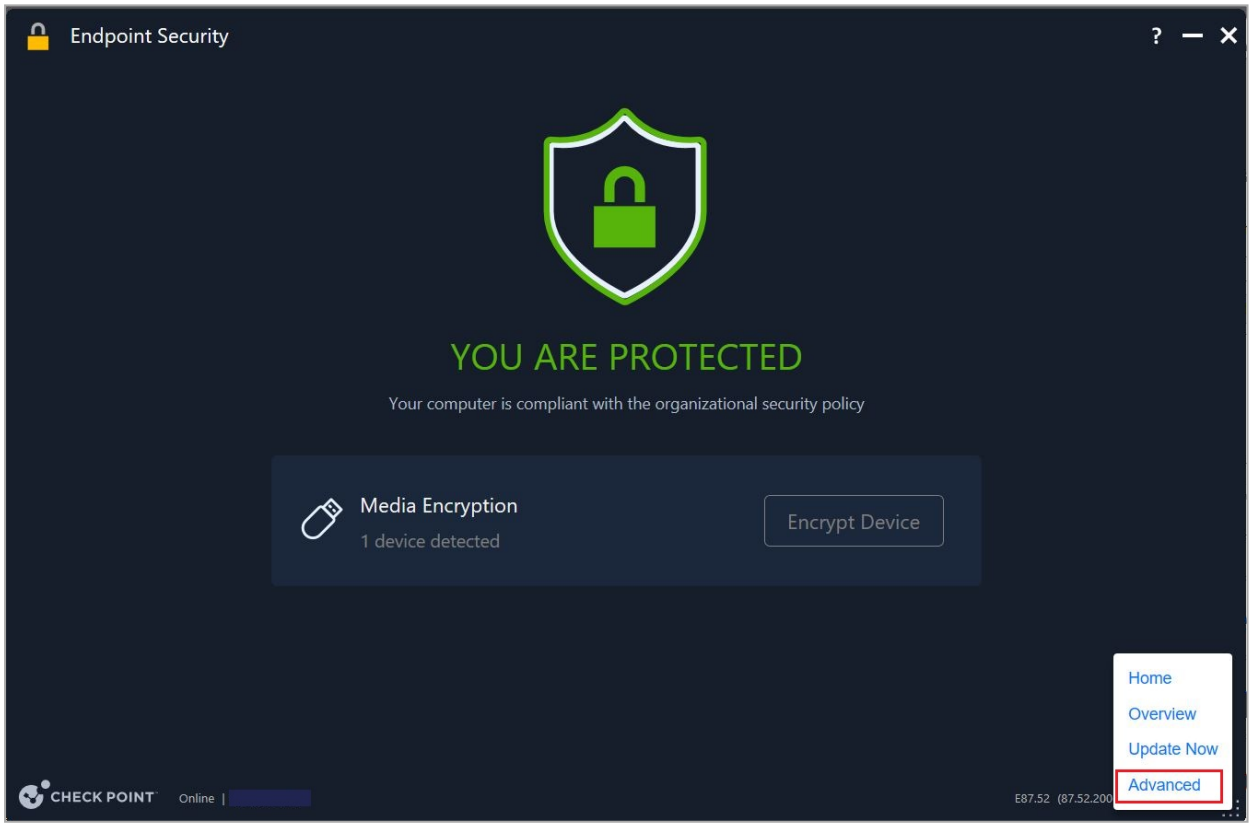
Best Practice - We recommend that the Deployment Agent has good hardware specs, network connectivity, availability and a "remote install" compatible Endpoint Security Client (E83.30 and higher).

You can configure multiple devices in each domain as Deployment Agents with no limitation on the total count. All devices qualify as an agent for an installation bundle.

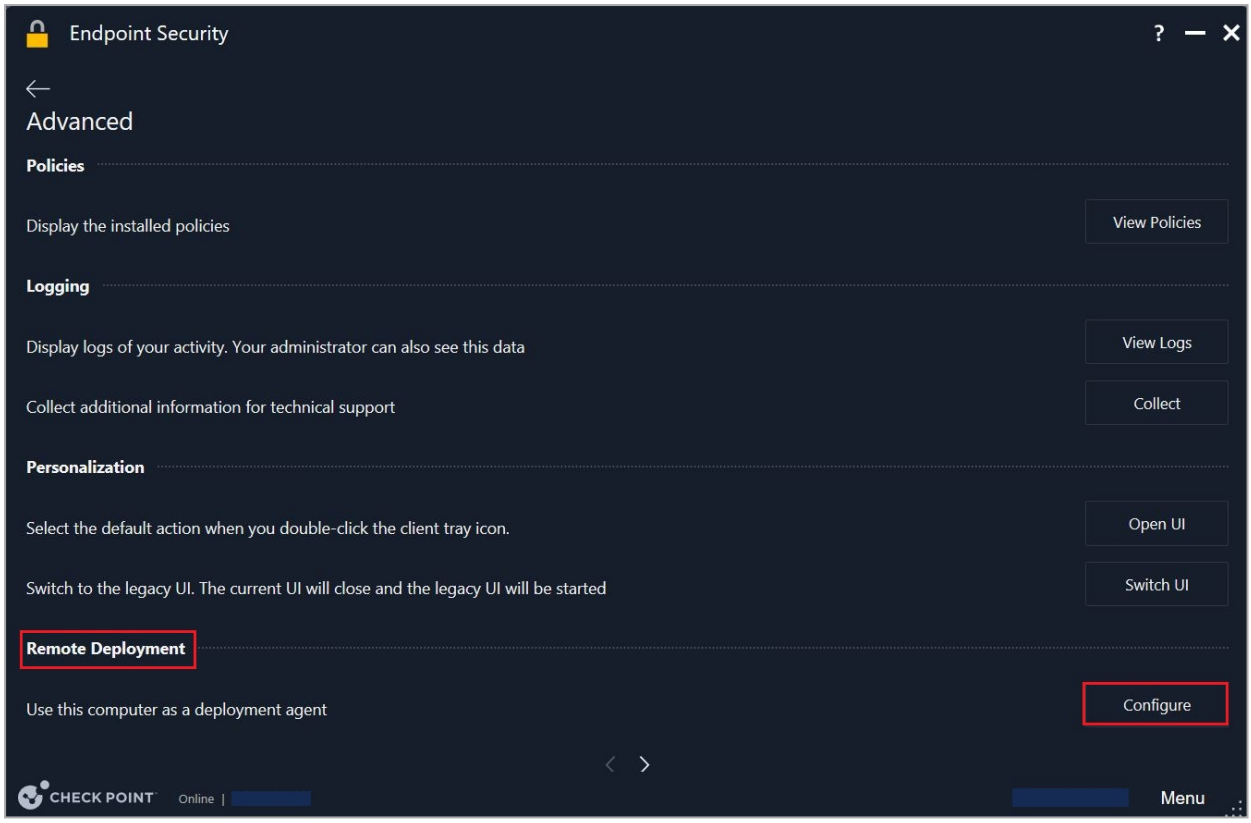
Certificates and DNS

To add Active Directory Credentials to the Deployment Agent on the Endpoint Security Client Screen:

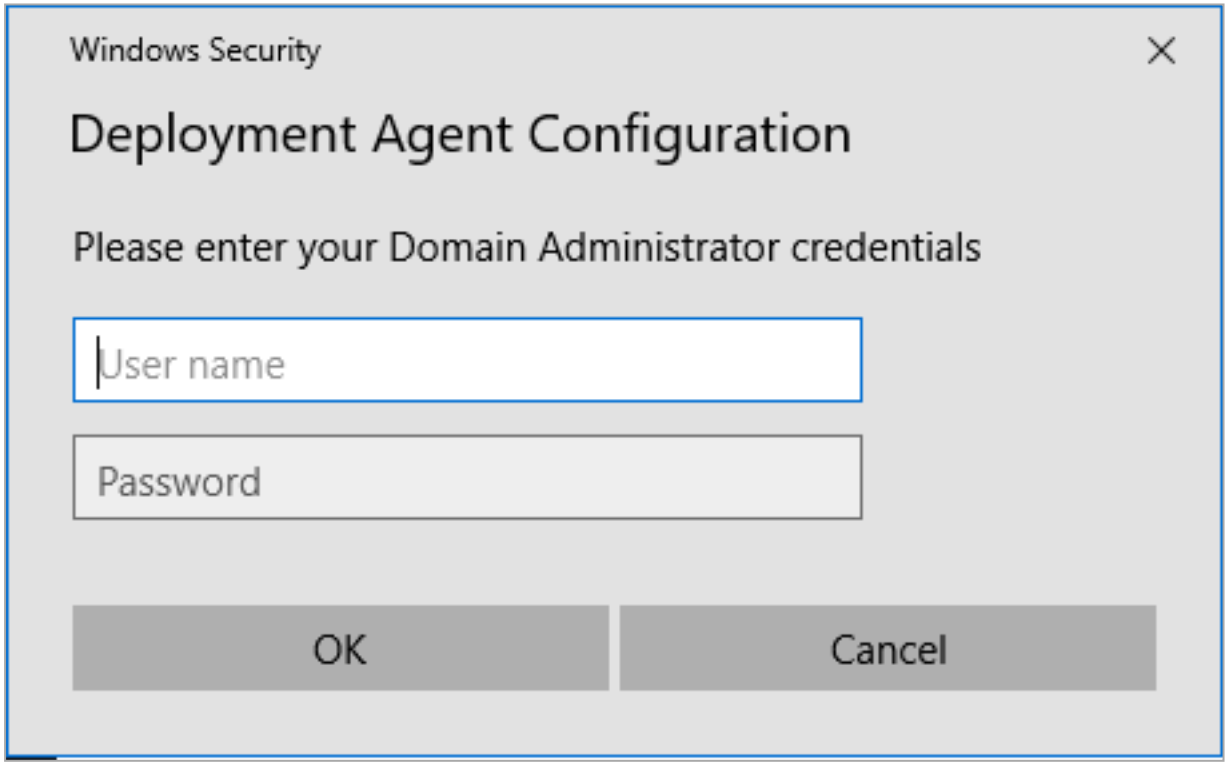
1. Open the Endpoint Security client screen, click **Menu** and select **Advanced**.



2. In the **Remote Deployment** section, click **Configure**.



3. Enter the **Domain Administrator** credentials with ad.com\administrator as the User Name.



Note -You must be in the Domain Administrators group in the Active Directory.

Privileges

User must have permission to connect from the Deployment agent computer to the target computer and create the scheduled task on the target computer.

For additional references, please see Microsoft's guide here: https://docs.microsoft.com/en-us/windows/win32/api/taskschd/nf-taskschd-itaskservice-connect

Setting the Target Devices

Windows Defender

- Windows 10 regards the remote execution of `msiexec.exe` through the Task Scheduler as malicious activity. Windows blocks this on the target computer.
- To disable Windows Defender's Anti-Malware with a PowerShell command on the target device: (For Windows server only)
  1. Open PowerShell as Administrator.
  2. Run:

     ```
     Uninstall-WindowsFeature -Name Windows-Defender
     ```

  3. Reboot the computer after the Windows Defender Anti-Malware uninstalls.
- If the remote installation procedure fails, the Windows Defender enables after a restart. Disable the Windows Defender's Real-Time Protection again.

Other AV Solutions

- We recommend that you disable the Windows Defender and disable or uninstall third-party anti-virus software on the target computer.
- An attempt to run remote software triggers a notification. The remote deployment procedure fails.

Enable Access to the Task Scheduler Through the Windows Firewall in a Domain Profile

- When the Windows Firewall blocks the remote connection to the target's Task Scheduler, run this PowerShell command on the target computer:

  ```
  Get-NetFirewallProfile -Name Domain | Get-NetFirewallRule | ?
  Name -like *RemoteTask-In-TCP-NoScope* | Enable-NetFirewallRule
  ```

- Configure these settings on the computer:
  1. Navigate to **Control Panel** > **Network and Internet** > **Network and sharing center** > **Advanced sharing settings**.
  2. In the **Network discovery** section, select **Turn on network discovery**.
  3. In the **File and printer sharing** section, select **Turn on file and printer sharing**.
- Allow user to access the `%windir%\Tasks` directory.
- Navigate to **Local Security Policy** > **Local Policies** > **User Rights assignment** and verify that the **Log on as a batch job** and **Log on a service** are configured.

- Navigate to **Windows Defender Firewall with Advanced Security** > **Windows Defender Firewall with Advanced Security - Local Group Policy Object** > **Inbound Rules** and verify that the:
  - **Remote Scheduled Tasks Management (RPC)** is enabled.
  - **Remote Event Log Management (RPC)** is enabled.
- Verify that the **Remote Registry** service is running.

Remotely Installing the Initial Client

You remotely install the Initial Client from the **Push Operations** view or from the **Computer Management** view.

To install the Initial Client remotely from the "Push Operations" view

1. From the left navigation panel, click **Push Operations**.
2. From the top toolbar, click **(+) Add**.

   The **Add Push Operation** window opens.
3. On the **Select push operation** page:
   a. From the menu, select **Agent Settings**.
   b. In the list of options, click **Deploy New Endpoints**.
   c. At the bottom, click **Next**.
4. On the **Select devices** page:
   a. Click **(+)**.
   b. Select devices that do not have Endpoint installed and are not in the process of deployment.

      Notes:
      - To select several non-adjacent entries, press and hold the **CTRL** key while you click the applicable entries.
      - To select several adjacent entries, press and hold the **SHIFT** key, click the applicable top entry, and then, click the applicable bottom entry.
      - To clear a selection, press and hold the **CTRL** key while click the applicable entry again.
      - You can select up to 5,000 entries.

   c. At the bottom, click **Update Selection**.
   d. In the table with the entries, select the checkboxes of applicable devices.
   e. At the bottom, click **Next**.
5. On the **Configure Operation** page:
   a. In the **Comment** field, enter the applicable text.
   b. In the **Select deployment agent** field, select one device for this push operation.
   c. In the **Endpoint version** menu, select the applicable version.Only devices with Windows 7 and higher are supported.

d. In the **Scheduling** section, configure one of the applicable settings:

- **Execute operation immediately**
- **Schedule operation for**, and click the calendar icon to configure the date and time

e. Click **Finish**.

To install the Initial Client remotely from the "Computer Management" view

1. From the left navigation panel, click **Asset Management**.
2. Select the checkboxes of applicable devices (up to 5,000).
3. From the top toolbar, click **Push Operation** > from the menu that appears click **Agent Settings** > **Deploy New Endpoints**.

   The **Push Operation Creation Dialog** window opens.
4. Enter the required values:
   a. In the **Comment** field, enter the applicable text.
   b. In the **Select deployment endpoint** field, select one device for this push operation.
   c. In the **Endpoint version** menu, select the applicable version.Only devices with Windows 7 and higher are supported.
   d. In the **Scheduling** section, configure one of the applicable settings:
      - **Execute operation immediately**
      - **Schedule operation for**, and click the calendar icon to configure the date and time
5. Click **Create**.

Windows Task Scheduler on endpoint devices

1. After a connection to the **Task Scheduler** service on Windows OS, the Deployment Agent registers a new task: "`CP_Deployment_{unique ID}`".
2. The Deployment Agent runs the task from the domain administrator's account on the target computer.
3. The Task Scheduler spawns the `msiexec.exe` to download the client installer and launch it in silent mode.
4. The installation proceeds with the MSI script instructions.

Security Considerations

- The Deployment Agent does not store the administrator password in clear text.
- The client UI collects the credentials and passes them to the device agent to store in separate values of a registry key under EP root.
- The password stores as an encryption and the principal name stores in plain text.
- Administrator accounts have access permissions of FULL CONTROL for the registry key.
- The SYSTEM account has READONLY access permissions for the registry key.
- The user and password never pass to the target devices. They establish the Task Scheduler connection.

Progress of Installation and Error Handling

The installation status shows at the bottom page of the **Push Operation** view.

Target devices that fail to install and download the Initial Client, set their status accordingly. In case of a connection failure, the Deployment Agent tries to connect to the target service three more times with increasing interval between attempts. The default is ten seconds. This mechanism increases the success rate in case of network-related issues.

The Deployment Agent Cannot Reach the Remote Task Scheduler

If the Deployment Agent cannot reach the remote task scheduler on the target device, the specific installation procedure fails. The target device's **Operation Status** changes to "Failed to access remote task scheduler".

The Target Device Fails to Download the Initial Client

If the target device cannot download the Initial Client, the target device's **Operation Status** changes to "Failed to download client".

Invalid Credentials

If the domain administrator credentials are invalid, the Deployment Agent stops connecting to remote targets, and the target device's **Operation Status** changes to "Access denied due to Invalid credentials".

Missing Credentials

If the domain administrator credentials are missing, the Deployment Agent stops connecting to remote targets, and the target device's **Operation Status** changes to "Deployment agent is not configured".

Failed to Install Initial Client on Target Device

If the target device fails to install the Initial Client, the target device's **Operation Status** changes to "Failed to install agent on target device".

Target Device Already Has an Agent installed

If the target device has an agent already installed, the Initial Client installation fails. The target device's **Operation Status** changes to "Agent already installed".

The Deployment Agent is Not Available to Deploy Targets

If the Deployment Agent cannot be reached while a push operation takes place, the push operation aborts, fails and sets the entire push-operation status to "The deploying Agent is not available to deploy targets".

Ports and Permissions

For installations that traverse a perimeter Firewall, enable this port: Port 135 for RPC over TCP traffic.

Upgrades

Upgrades are seamless to our users. A new type of Push Operation are rolled out and added to all Harmony Endpoint users.

Heartbeat Interval

Endpoint clients send "heartbeat" messages to the Endpoint Security Management Server to check the connectivity status and report updates. The time between heartbeat messages is known as the *heartbeat interval.* For more information, see Endpoint Security Server and Client Communication.

Note - The default heartbeat interval is 60 seconds. A shorter heartbeat interval can cause additional load on the management. A longer heartbeat interval may lead to less up-to-date logs and reports.

Monitoring Harmony Endpoint Deployment and Policy

Monitoring your Endpoint Security policy and deployment should be a very important part of your-day-to-day work.

The **Overview** view > **Operational Overview** page has the **Active Alerts** pane on the right. This page shows which endpoint computers are in violation of critical security rules.

These violation types can trigger alerts about various issues.

For example:

- Compliance warning
- Failed deployment
- Encryption problem
- Anti-Malware issues
- Policy server out-of-sync
- Anti-Malware License Expiration Date
- High-Availability server out-of-sync:
  - A data batch is in the error state.
  - The synchronization engine is offline.
  - The number of unsent data batches is more than 300. This occurs when the rate at which the synchronization server processes the sync data is lower than rate at which the sync data is generated.
  - A secondary server or a remote help server is not registered as the synchronization engine on the primary server.

Configuring Alert Messages

To define security alerts

1. Go to the **Endpoint Settings** view > **Alerts**, and select a security violation.
2. Select the applicable alert from the list.
3. In the right section **Alert Configuration**:
   a. Select **ON** in the top line:

      The computer is restricted or about to the restricted

b. Configure these settings:

- **Threshold Settings** - Select how the amount of endpoints that trigger alerts are measured, by percentage or number.
- **Notification Settings** - Select the notification type you receive when an alert is triggered:
  - **Notify on alert activation** - Sends a notification when an alert the number of Endpoint devices with violations exceeds the configured threshold.
  - **Notify on alert resolution** - Sends a notification when an alert the number of Endpoint devices with violations decreases below the configured threshold.
  - **Remind me every** - Sends a notification repeatedly according to a specified frequency, as long as the number of Endpoint devices with security violations exceeds the configured threshold.
  - **Recipients** - Enter the email addresses of the message recipients (separated by comma).
- **Email Template Settings** - You can configure a unique email template to be sent to you when an alert is triggered. The email Subject and Body contain dynamic tags. Dynamic tags are replaced by the server with the relevant information during email sending. Remove the tags you do not wish to include in the email.
  - **Attach report to mail notification** - If selected, a CSV report with all the device details related to a particular alert will be attached to email. If there are no affected devices, nothing is attached
  - **Subject** - Contains these dynamic tags: **type** (alert activation, alert resolution or alert reminder), **alert name**, and **tenant name**.
  - **Body** - Contains these dynamic tags: **type**(alert activation, alert resolution or alert reminder), **alert name**, **affected-count**, and **total-count**.
  - **Send Test Report** - If selected, a notification email according to the configured template is sent for a particular alert.

  To send emails for alerts, you must follow the steps in the *"Configuring an E-mail Server" on the next page* section below.

4. Click **Save**.

Note - Alerts are reevaluated every 10 minutes.
When the alerting criteria are updated, the alerting is reevaluated on the next iteration.
When alerting is (re)enabled, it forces the alerting mechanism to immediately (re)start and (re)evaluate.

Configuring an E-mail Server

You must configure your email server setting for Endpoint Security to send you alert email messages.

If you use Capsule Docs it is also important to configure this.

The settings include the network and authentication parameters necessary for access to the email server.

You can only configure one email server.

To configure the email server

1. In **Endpoint Settings** > **Alerts** > at the top, click **Email Service Settings**.

   The **Email Service Settings** window opens.

2. Enter these details:

   - **Host Name** - Email serve host name.
   - **From Address** - Email address from which you want to send the alerts.
   - **User Authentication is Required** - If email server authentication is necessary, select this option and enter the credentials in the **User Name** and the **Password** fields.
   - **Enable TLS Encryption** - Select this option if the email server requires a TLS connection.
   - **Port** - Enter the port number on the email server.
   - **Test Email** - Enter an email address to send the test to, and click **Send Test**:
     - If the verification succeeds, an email is sent to the email address entered and a success message shows in the **Email Service Settings** window.
     - If the verification fails, an error message shows in the **Email Service Settings** window.

       Correct the parameters errors or resolve network connectivity issues. Stand on the error message to see a description of the issue.

3. Click **OK** to save the email server settings and close the window.

How to Verify that Harmony Endpoint can Access Check Point Servers

See article in the following link:

https://support.checkpoint.com/results/sk/sk116590

Uninstalling Third-Party Anti-Virus Software Products

Note - We recommend that you test this procedure on a test environment before you implement it on a live environment.

The *EPS.msi* file contains the *Products.json* file that has a pre-configured list of Anti-Virus software products that are automatically deleted when you install the Endpoint Security client E84.70 or higher. By default, this list contains Symantec, McAfee, and Kaspersky.

You can also uninstall Symantec, McAfee, and Kaspersky manually.

To uninstall Symantec, McAfee or Kaspersky manually:

Open the command prompt window and run:

`msiexec /i EPS.msi REMOVEPRODUCTS="Product"`, where `Product` is Symantec, McAfee or Kaspersky.

For example, to uninstall Symantec, run:

```
msiexec /i EPS.msi REMOVEPRODUCTS="Symantec"
```

To uninstall Symantec, McAfee and Kaspersky together manually:

Open the command prompt window and run:

```
msiexec /i EPS.msi REMOVEPRODUCTS="Symantec, McAfee, Kaspersky"
```

To uninstall any other Anti-Virus software manually:

Open the command prompt window and run:

```
msiexec /i EPS.msi REMOVEPRODUCTS="{Product code or upgrade code of
Product1} {Product code or upgrade code of Product2}"
```

For example, to uninstall multiple Anti-Virus softwares, run:

```
msiexec /i EPS.msi REMOVEPRODUCTS="{8D92DEB1-A516-4B03-8731-
60974682B69C} {9BE518E6-ECC6-35A9-88E4-87755C07200F}"
```

Tip - To find the product code, do any of these:

- In the **Registry Editor**, navigate to the Uninstall folder under

  HKEY_LOCAL_MACHINE\SOFTWARE.

  For example, *HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall*.

- In **PowerShell**, run:

  Get-WmiObject win32_product -Filter "name like '%any part of the product name%"

- To find the upgrade code using the product code, run:

  gwmi -Query "SELECT Value FROM Win32_Property WHERE Property='UpgradeCode' AND ProductCode='{YourGuid}"

Note - With the Endpoint Security client 86.50 and higher, you can uninstall a product that is not listed in the default *Products.json* file by using an updated *Products.json* that contains the product. To get the updated *Products.json* file, contact Check Point Customer Support.

To uninstall a product using the updated *Products.json* file, open the command prompt window and run:

`msiexec /i EPS.msi REMOVEPRODUCTS="Product" RPCONFIG="c:\users\admin\downloads\Products.json"`, where `Product` is the Anti-Virus software that you want to uninstall.

Notes -

- Symantec.cloud is not supported by this command. To remove Symantec.cloud, navigate to *C:\Program Files\Symantec.cloud\PlatformAgent* and run *Uninstall.exe.*
- You cannot uninstall software products whose cached msi is not found on your computer.

Managing Licenses

For information about the available licenses, see the Harmony Endpoint product catalog.

This chapter includes license information for Endpoint Security Servers and Clients.

All Endpoint Security licenses are physically installed on the Endpoint Security Management Server on your premises.

Endpoint Security Product Licenses

You need to have a license for:

- Each Endpoint Security client. The license is per-seat.
- The Endpoint Security Management Server.

Demo and Temporary Licenses

These demo and trial Endpoint Security licenses are available:

License type	Explanation
Trial License	A 30 day trial license is automatically installed when you install Endpoint Security. This license lets you use all Endpoint Security components for a limited number of endpoint client seats.
Evaluation	An 30-day evaluation license is available for specified components for a specified number of seats. You must deploy a management evaluation license and an Endpoint Security client evaluation license.
Product	You must purchase a Product license for each Endpoint Security component running on a client. Licenses can be purchased as a Subscription, a contract that is renewed annually, or a one-time purchase.

License Enforcement

License activity conforms to these conditions:

- You can add Endpoint Security licenses as required using one of these methods:
  - SmartUpdate (see *"Getting and Applying Contracts" on the next page*).
  - The Gaia Portal (see the *R81.10 Gaia Administration Guide*).
  - The "`cplic`" CLI command (see the *R81.10 CLI Reference Guide*).
  - The "`cpconfig`" CLI command (see the *R81.10 CLI Reference Guide*)
- You can remove a client license by resetting the client or deleting the client using Endpoint Web Management Console. These licenses are returned to the license pool.
- Each client gets its Container and Endpoint Security component licenses from a pool of available licenses.
- If you have mixed licenses, for example Harmony Basic for Server and Harmony Advanced on Laptops, then each client gets a random license from the pool mixed licenses available.
- You can combine licenses to reach the total number of required clients.
- License validation occurs when the client sends a SYNC or heartbeat messages to the server.
- When there is no container license, components registration is blocked.

Getting Licenses

This procedure assumes that you have a user account for the Check Point User Center, and that the necessary licenses and contracts are purchased.

To get the license for your Endpoint Security Management Server:

1. Log in to *Check Point User Center*.
2. Click **My Products** > **My Products Center**.

   The page shows the purchased licenses.

   Endpoint Security licenses have these parts in the SKU:

- **"CPEP"** - Check Point Endpoint Security containers.
- **"CPSB"** - Check Point component. If the macro string includes the "`-SUBSCR`" suffix, you must get and apply a contract for this feature. See *"Getting and Applying Contracts" below*.

3. For each license:
   a. Click the license to open it.
   b. In the window that opens, click **License**.
4. Fill in the form that opens.
   - Make sure that **Version** is **R80 or higher**.
   - Make sure that the **IP Address** is the IP address of the Endpoint Security Management Server.
5. Click **License**.

   A window opens, showing the license data.
6. Save the license file.
7. Add your licenses using one of these methods:
   - SmartUpdate (see *"Getting and Applying Contracts" below*).
   - The Gaia Portal (see the *R81.10 Gaia Administration Guide*).
   - The "`cplic`" CLI command (see the *R81.10 CLI Reference Guide*).
   - The "`cpconfig`" CLI command (see the *R81.10 CLI Reference Guide*).

Getting and Applying Contracts

If the license includes "`-SUBSCR`", you must download the contract file and apply it to the server.

If the Endpoint Security Management Server has Internet access, it automatically renews contracts.

By default, the Endpoint Security Management Server looks for new contracts every two hours.

To change the default time interval:

1. Connect to the command line on the Endpoint Security Management Server.
2. Log in to the Expert mode.
3. Edit the `dl_prof_CNTRCTMNGR.xml` file:

   ```
   vi $CPDIR/conf/downloads/dl_prof_CNTRCTMNGR.xml
   ```

4. Change the "<`interval`>" value as necessary.
5. Save the changes in the file and exit the editor.
6. Restart Check Point services:

   ```
   cpstop ; cpstart
   ```

To apply a contract manually:

1. Log in to *Check Point User Center*.
2. Click **Products**.
3. Select **Get Contracts File** in the drop-down menu at the right of the row.
4. In the window that opens, save the contract file and click **Open**.
5. In SmartConsole, open **SmartUpdate**.

   (**Start** menu > **Check Point** > **SmartUpdate**)
6. Select **License & Contracts** > **Updated Contracts** > **From File**.
7. In the window that opens, browse to where you saved the contract file and click **Open**.

   The contract is applied to the Endpoint Security Management Server.

If the Endpoint Security Management Server does not have access to the Internet, prepare the contract file download from the User Center differently.

To download a contract to a different computer:

1. Log in to *Check Point User Center*.
2. Click **Products** > **Additional Services**.
3. Select the account of the contract.
4. Click **Email File** or **Download Now**.
5. When you have the contract file, move it to the Endpoint Security Management Server.

To configure a proxy for Internet access:

If the Endpoint Security Management Server requires a proxy to connect to the internet, configure the proxy details in SmartConsole.

1. In SmartConsole, open the Endpoint Security Management Server object.
2. Select **Network Management** > **Proxy**.
3. Select **Use custom proxy settings for this network object**.
4. Select **Use proxy server** and enter the URL and port.
5. Click **OK**.
6. Click the **Menu** > **Install Database** > select the Endpoint Security Management Server object > click **Install**.

License Status

You can see the status of container and component licenses in the Endpoint Web Management Console > **Endpoint Settings** view > **Licenses**.

This pane shows the total number of seats and seats in use.

If the number of seats exceeds the number of licenses, you must add the number of licenses shown as **Insufficient Seats**.

The lower section of the report shows the details of each license including:

- License Name and status
- Endpoint Security components
- Seats in Use
- Total seats
- Percentage of total licenses in use
- Expiration date
- IP address of license host

Managing Administrators for the Endpoint Web Management Console

To create an additional administrator account for an user

Configure the required administrators in SmartConsole.

See the *R81.10 Security Management Administration Guide*.

To switch between accounts

1. At the top right corner of the Endpoint Web Management Console, click the current administrator name and click **Sign Out**.
2. On the **My Account** page, enter the credentials for the required administrator and click **Sign In**.

Managing Users in Harmony Endpoint

On-premises servers have only two user roles: "Admin" & "Read-only".

These are the roles:

Role	Description
Admin	Full Read & Write access to all system aspects.
Read-Only User	Has access to all system aspects, but cannot make any changes.

Viewing Computer Information

The Asset Management View

The view shows information on each computer, such as deployment status, active components on the computer, version installed on the computer and more.

Note - The **General** > **Description** at bottom pane shows the text entered in the **Active Directory** for the asset. If no text is entered, it is blank.

From the top menu **Columns**, select a preconfigured view:

- **Deployment**
- **Compliance**
- **Health**
- **Full Disk Encryption**
- **Anti-Malware**
- **Host Isolation**
- Alternatively, click **Custom** and select the required columns.

Status Icon

The icon in the **Status** column shows the client or computer status.

Status Icon	Description
	Indicates .
	Indicates Harmony Browse client.
	Indicates that the client connection is active.
	Indicates that a new computer was discovered that has no client installed.
	Indicates that the computer was deleted from the Active Directory or from the Organizational Tree.

Status Icon	Description
	Indicates a pending **Network One-Time Logon** or **Network Password Change** request from a user. For more information, see the Easy Unlock feature. 1. Click the icon. The **Respond to Request** dialog box appears. 2. Click **Accept** or **Reject**. **Notes**: ■ You must refresh the table or the browser to view the icon. ■ This feature is available only to customers in the Early Availability program.

Filters

Use the **Filters** pane on the right side of the screen to filter the information in the table.

These are the main filters for this view:

- **Filter by computer property**
- **Filter by Virtual Group**
- **Filter by Organization Unit** (this information is pulled from your Active Directory)

Working with the Computers Table

1. Hover over the column and click  .
2. From the drop-down :
   - To freeze the column, click **Pin**.
   - To unfreeze the column, click **Unpin**.
   - Open the filter for the current column, click **Filter** and select the values.
   - To hide the column, click **Hide**.
   - To insert another column, click **Add Column**.
3. To adjust the column position in the table, drag and drop the column to the required position.
4. To copy the value of a cell to the clipboard, hover over a cell and click **Copy**.
5. To copy the values of a row to the clipboard, hover over a row and click **Copy row**.

Managing Computers

Select the checkbox to the left of the applicable computers and right-click to perform these actions:

General Actions

View Computer Logs

You can view logs of computers based on it's IP address.

To view computer logs by it's IP address:

1. Go to **Asset Management** > **Computers**.
2. Select the applicable computer or user from the list.
3. From the top toolbar, click .
4. Select **General Actions** > **View Computer Logs**.

   The system opens the Logs menu and shows the computer logs.

Create Virtual Group

You can create a virtual group. See *Managing-Virtual-Groups.htm.*

Create and Add to Virtual Group

You can add computers to a new virtual group. See *Managing-Virtual-Groups.htm.*

Add to Virtual Group

You can add a computer to a virtual group (see *"Managing Virtual Groups" on page 196*).

Reset Computer Data

When the Endpoint client is installed on a computer, information about the computer is sent to and stored on the Endpoint Security Management Server.

Resetting a computer means deleting all information about it from the server.

Resetting a computer does not remove the object from the Active Directory tree or change its position in the tree.

Important - You can only reset a computer if the Endpoint client is not installed. If you reset a computer that has Endpoint installed, important data is deleted and the computer can have problems communicating with the Endpoint Security Management Server.

Computer reset:

- Removes all licenses from the computer.
- Deletes Full Disk Encryption Recovery data.
- Deletes the settings of users that can log on to it.
- Removes the computer from Endpoint Security Monitoring.
- Deletes the Pre-boot settings.
- Marks the computer as unregistered.

After you reset a computer, you must reformat it before it can connect again to the Endpoint Security service.

You may decide to reset a computer if:

- The Endpoint client was uninstalled or the computer is re-imaged.
- It is necessary to reset the computer's configuration before a new Endpoint client is installed. For example, if the computer is transferred to a different person.

Delete

Removes the asset from the Local or Active Directory and adds it to **Deleted Entities** in the **Organizational Tree**. This operation discards the assets license information. You can use this operation when you remove an asset from your domain.

Note - If the Endpoint Security client is still installed on the asset, the client continues to receive the updates from the Endpoint Security Management Server.

To add the asset back to the Active Directory, see **Recover**.

Recover

Adds the deleted asset back to the Local or Active Directory from **Deleted Entities** in the **Organizational Tree**. The asset's status is not **Active** until its Endpoint Security client connects and synchronizes with the Endpoint Security Management Server. You can use this operation when you add an asset back to the domain.

Note - You can recover only a deleted asset.

Terminate

Warning - Removes the asset from the Harmony Endpoint management permanently. You cannot recover a terminated asset. We recommend to terminate an asset only if it is discarded or disposed or the Endpoint Security client is uninstalled.

Directory Scanner

Harmony Endpoint can scan and import users, groups, Organizational units (OUs) and computers from multiple supported directory domains. See Managing Active Directory Scanners.

The Overview View

The **Overview** page shows a graphical summary of important information about the clients in your organization.

Operational Overview

The information in the **Operational Overview** appears in widgets described below. Each widget is clickable, and takes you to the relevant view based on the **Computer Management** view.

The information is presented in these widgets:

Widget	Description
All Endpoints	Shows the number of protected endpoints and the number of endpoints which report issues. This widget is based on the **Health** view.
Desktops	Shows a division of the desktops by operating systems: Windows, macOS, and Linux. This widget is based on the **Health** view. This widget only includes protected entities.
Laptops	Shows a division of the laptops by operating systems: Windows, macOS, and Linux. This widget is based on the **Health** view. This widget only includes protected entities.
Deployment Status	Shows the deployment status of the devices according to these values: ■ **Success** - Devices with these Deployment Statuses: "**Completed**" in their status. ■ **In progress** - Devices with these Deployment Statuses: "**Deploying**", "**Uninstalling**", "**Retrying**", or "**Downloading**" in their status. ■ **Failed** - Devices with these Deployment Statuses: "**Not Installed**", "**Not Scheduled**" or "**Unknown**".
Health Status	Shows which computers have installed components that are not running.

Widget	Description
Anti-Malware Update	Shows the time when updates were installed on the endpoint clients: ■ **On the last 24h** ■ **On the last 72h** ■ **Over 72h ago** ■ **Never** ■ **Not installed or Unknown** This widget is based on the **Anti-Malware update ON** data in the **Deployment Status**.
Harmony Endpoint Version	Shows the client versions installed on the endpoint clients. This widget is based on the **Deployment** view.
Operating System	Shows the type of operating system installed on the endpoint clients: ■ Windows ■ macOS ■ Linux ■ Other

In addition, in the top right section **Active Alerts** you can see alerts for the thresholds you created in the **Endpoint Settings** view > **Alerts** (see *"Monitoring Harmony Endpoint Deployment and Policy" on page 60*).

Reports

On the **Reports** page, you can download the reports in the pdf format:

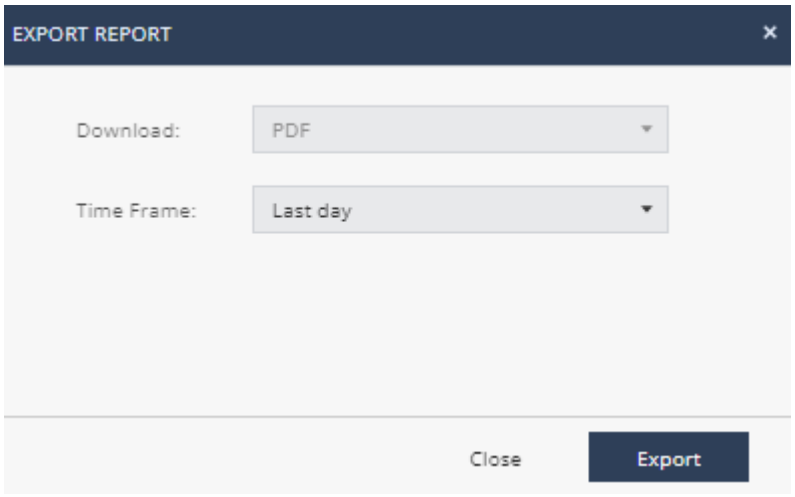
- **Threat Extraction Report** - Shows the insights on the downloaded files.
- **Check Point Cyber Security Report** - Shows the latest security trends as per Check Point.

Generate Report

To generate a report:

1. Go to **Overview** > **Reports** > **Generate Report**.
2. Select a report, click ⚙ and select **Export Report**.

   The **Export Report** window appears.



3. In the **Time Frame** list, select **Last day**, **Last 7 days**, or **Last 30 days**.
4. Click **Export**.

Scheduled Reports

Scheduled Reports allows you to automatically generate reports at the specified date and time, and email it to the specified recipients.

Notes:

- The report becomes effective 24 hours after you schedule it. For example, if you schedule for a new report today for 02:00 PM, then it is enforced from the next day at 02:00 PM.
- This feature is not supported for **Check Point Cyber Security Reports**.
- For performance reasons, it is recommended to schedule reports to run in off-peak hours. For example, during non-business hours.
- The default time zone for the schedule report is Coordinated Universal Time (UTC). For example, to schedule the report at 1:00 AM EST, specify the time as 6:00 AM (depending on Daylight Savings Time).

To schedule a report:

1. Navigate to **Overview**> **Reports** and do one of these:
   - From the **Scheduled Reports** page, click **Add** and from the **Name** list, select the report.
   - From the **Generate Report** page, select the report, click  and select **Schedule Report**.
2. From the **Name** list, select the report.
3. From the **Time Frame** list, select the period for the report:
   - **Last day**
   - **Last 7 days**
   - **Last 30 days**
4. From the **Frequency** list, select the frequency to generate the report:
   - To generate the report everyday, select the day of the week.
   - To generate the report weekly, select the day of the week.
   - To generate the report every month, select the date.
5. In the **Time** field, specify the time for the system to generate the report and send it to the recipients. By default, the time is in UTC. For example, if you want to generate the report at 01.00 AM Eastern Standard Time (EST), you must specify the time as 06.00 AM UTC.
6. In the **Recipients** field, enter the recipients for the report.
7. Click **Schedule**.

   The schedule is added to the table. The report becomes effective 24 hours after you schedule it.
8. To edit a scheduled report, select the report in the table and click **Edit**.
9. To delete a scheduled report, select the report in the table and click **Delete**.

Announcements

The **Announcements** page shows the latest news and enhancements in .

Configuring Endpoint Policy

The security policy in the Endpoint Web Management Console contains these components:

- **Threat Prevention** - which includes Web & Files Protection, Behavioral Protection and Analysis & Remediation. The Threat Prevention policy is unified for all the Threat Prevention components. This is different than the Policy Rule Base in SmartEndpoint, where each Harmony component has its own set of rules.
- **Data Protection** - which includes Full Disk Encryption.

In addition, the Endpoint policy contains the Global Policy Settings (see *Configuring Global Policy Settings*) and the Deployment Policy (see *"Deploying Endpoint Clients" on page 27*).

You can add more rules to each Rule Base and edit rules as necessary. Changes are enforced after the policy is installed.

When you plan the security policy, think about the security of your network and convenience for your users. A policy should permit users to work as freely as possible, but also reduce the threat of attack from malicious third parties.

The security policy has these on-screen options:

- **User-Based Policy** - Policy is arranged by blades, each blade has its own set of rules (same as the SmartEndpoint view)
- **Computer-Based Policy** - Policy is arranged by the protected scope. Each rule contains the protected scope and the blades which are activated for that protected scope.

To switch between the views, go to **Endpoint Settings** > **Policy Operation Mode**.

Configuring the Threat Prevention Policy

The Threat Prevention policy includes these components:

- **Web & Files Protection** - Includes download protection, credential protection and Files protection.
- **Behavioral Protection** - Includes Anti-Bot, Anti-Ransomware and Anti-Exploit.
- **Analysis & Remediation** - Includes forensics and file Remediation.

The Threat Prevention policy unifies all the Threat Prevention components. This is different from the Policy Rule Base in SmartEndpoint, where each Threat Prevention component has its own set of rules. The unified policy lets the administrator control all Threat Prevention components in one Policy. Each rule in the Policy defines the scope which the rule applies to and the Threat Prevention components which are activated.

The Threat Prevention policy contains a pre-defined Default Policy rule, which applies to the entire organization.

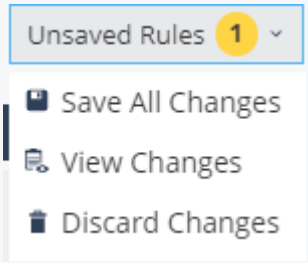
Each new rule you create, has pre-defined settings, which you can then edit in the right section of the screen.

The Policy Rule Base consists of these parts:

Column	Description
Rule Number	The sequence of the rules is important because the first rule that matches traffic according to the protected scope is applied.
Rule Name	Give the rule a descriptive name.
Applied to	The protected scope, to which the rule applies.
▪ **Web & Files Protection** ▪ **Behavioral Protection** ▪ **Analysis & Remediation**	The policy components.

The **Policy** toolbar includes these options:

To do this	Click this
Create a new rule	

To do this	Click this
Save, view, or discard changes	
Duplicate a rule	
Install Policy	
Search for entity	
Delete a rule	

Web & Files Protection

This category includes URL Filtering, Download (web) Emulation & Extraction, Credential Protection and Files Protection.

URL Filtering

URL Filtering rules define which sites can be accessed from within your organization. You select these sites in the **Categories** and **Blacklisting** sections, and define the mode in which the rule operates.

When you select a category of sites, the URL Filtering rule applies to all sites in the selected category.

In Blacklisting, you enter the names of specific domains, IP addresses or sites.

Notes:

- You can add the domain names manually or upload a CSV file with the domain names you want to include in the blacklist.
- You can use `*` and `?` as wildcards for blacklisting.
  - `*` is supported with any string. For example: `A*` can be `ADomain` or `AB` or `AAAA`.
  - `?` is supported with another character. For example, `A?` can be `AA` or `AB` or `Ab`.
- You can export your blacklist.

There are 3 configuration modes for the URL Filtering protection:

- **Prevent** - Currently supported only in Hold mode. The request to enter a site is suspended until a verdict regarding the site is received.
  - **Unclassified URLs** - URLs that the service has no verdict about. Unclassified URLs are allowed by default. To change this configuration to **Block**, contact *Check Point Support*.
  - **Ask** - This option is selected by default. This lets you access a site determined as malicious, if you think that the verdict is wrong.
- **Detect** - Allows an access if a site is determined as malicious, but logs the traffic.
- **Off**

Note:
SmartEndpoint does not support the new capability. It is only supported for web users.

You can define specific URLs or domains as blacklisted. These URLs/domains will be blocked automatically, while other traffic will be inspected by the URL Filtering rules. You can add the URLs/domain names manually or upload a CSV file with the URLs/domain names you want to include in the blacklist.

To add a URL to the blacklist:

1. Go to **Advanced Settings** > **URL Filtering** > **Blacklist** > **Edit**.
2. In the **URLs** pane, for each required URL, enter the URL and click the **+** sign
3. click **OK**.

Notes:
You can use `*` and `?` as wildcards for blacklisting.

- `*` is supported with any string. For example: `A*` can be `ADomain` or `AB` or `AAAA`.
- `?` is supported with another character. For example, `A?` can be `AA` or `AB` or `Ab`.

To search for a URL:

1. Go to **Advanced Settings** > **URL Filtering** > **Blacklist** > **Edit**.
2. In the search box, enter the required URL.

   The search results appear in the URLs pane.

   You can edit or delete the URL.

To import URLs from an external source:

1. Go to **Advanced Settings** > **URL Filtering** > **Blacklist** > **Edit**.
2. Next to the search box, click the  sign (import domains list from a 'csv' file).
3. Find the required file and click **Open**.
4. Click **OK**.

To export a list of URLs to from the Endpoint Security Management Server to an external source:

1. Go to **Advanced Settings** > **URL Filtering** > **Blacklist** > **Edit**.
2. Next to the search box, click the  sign (export domains list to a 'csv' file).
3. Click **OK**.

Download (Web) Emulation & Extraction

Harmony Endpoint browser protects against malicious files that you download to your device. The Harmony Endpoint Browser extension is supported on Google Chrome. Threat Emulation detects zero-day and unknown attacks. Files on the Endpoint device are sent to a sandbox for emulation to detect evasive zero-day attacks. Threat Extraction proactively protects users from malicious content. It quickly delivers safe files while the original files are inspected for potential threats.

There are three configuration options for this protection:

- **Detect** - Emulate original file without suspending access to the file and log the incident.
- **Off** - Allow file

Credential Protection

This protection includes two components:

- **Zero Phishing** - Phishing prevention checks different characteristics of a website to make sure that a site does not pretend to be a different site and use personal information maliciously.
  There are three configuration options for this protection: **Prevent**, **Detect** and **Off**.
- **Password reuse protection** alerts users not to use their corporate password in non-corporate domains.
  There are three configuration options for this protection: **Detect & Alert**, **Detect** and **Off**.

Files Protection

This protection includes two components:

- **Anti-Malware** - Protection of your network from all kinds of malware threats, ranging from worms and Trojans to adware and keystroke loggers. Use Anti-Malware to manage the detection and treatment of malware on your endpoint computers.

  There are three configuration options for this protection:

  - **Prevent** - Prevents your files from malware threats.
  - **Detect** - Provides detection of the threats, so they appear in the logs, although the virus or malware are still executable. Administrators must use this mode with caution.
  - **Off** - No protection from malware.

  Note - Starting from E83.20 Endpoint Security client, Check Point has certified the E2 client version (the Anti-Malware engine is based on Sophos as opposed to Kaspersky) for Cloud deployments.

- **Files Threat Emulation** - Emulation on files on the system.

Behavioral Protection

The Anti-Bot component

- Uses the ThreatCloud repository to receive updates and queries the repository for classification of unidentified IP, URL, and DNS resources
- Prevents damage by blocking bot communication to C&C sites and makes sure that no sensitive information is stolen or sent out of the organization.

There are 3 configuration options for the Anti-Bot protection: **Prevent**, **Detect**, and **Off**.

The Anti-Ransomware Component

The Anti-Ransomware constantly monitors files and network activity for suspicious behavior. It creates honeypot files on client computers.

It stops the attack immediately after it detects that the ransomware modified the files.

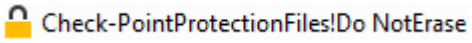
The Anti-Ransomware creates the honeypot files in these folders:

- `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)
- C:\Program Files (x86)
- C:\ProgramData
- C:\Users\<User>\AppData\Roaming
- C:\Users\<User>\AppData\Local
- C:\Users\<User>\Downloads

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

For example:



The file names include these strings, or similar:

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

Before ransomware attack can encrypt files, Anti-Ransomware backs up your files to a safe location.

The Anti-Exploit Component

Harmony Endpoint 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.

Analysis & Remediation

Forensics - Harmony Endpoint Forensics analyzes attacks detected by other detection features like Anti-Ransomware or Behavioral Guard, the Check Point Gateway and some third party security products. On detection of a malicious event or file, Forensics is informed and a Forensics analysis is automatically initiated. After the analysis is completed, the entire attack sequence is then presented as a Forensics Analysis Report. If Endpoint Security servers do not have internet connectivity, Forensics information is stored and sent for evaluation immediately when a server connects to the internet.

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

Remediation & Response - The Harmony Endpoint Files Remediation component applies Remediation to malicious files. When Harmony Endpoint components detect malicious files, they can quarantine those files automatically based on policy and remediate them if necessary.

Adding Exclusions to Rules

1. Go to the applicable policy rule, for which you want to create the exclusion.
2. In the **Capabilities & Exclusions** pane, click **Exclusions Center**.

   The **Exclusions Center** window opens.
3. Add the required type of exclusion.
4. Click **OK**.
5. In the bottom right corner of the policy configuration pane, click **Save**.
6. From the top, click **Install Policy**.

Notes -

- You can also add exclusions from the **Logs** menu:
  - In the **Logs** menu, right-click a log to add and configure an exclusion to your endpoint device. This redirects you to the appropriate rule, section, and capability.
  - Apply the exclusions through:
    - Effective option: Pertains to a specific device or a user rule.
    - All options: Pertains to a specific rule.
- This is supported with Harmony Endpoint client version 86.20 or higher.
- For Harmony Endpoint client version 86.20 or lower, or for blades/capabilities which are not supported, the system redirects you to the relevant rule in the exclusions center to create exclusions.

Below is the list of supported exclusions.

Web and Files Protection Exclusions

Anti-Bot Exclusions

By default, the Anti-Bot component inspects all entities except:

- **Process** - Name of an executable
- **URL** - Website URL
- **Domain** - Full Domain name

- **Protection Name** - Predefined malware signature
- **IP range** - Internal or external IP address

Process Exclusions

Harmony Endpoint scans files when you create, open, or close them.

When you exclude a trusted process from inspection, it's file or network operation is not scanned. Exclude a process only if you are sure, it is not Malware.

Best Practice - We recommend excluding a process if:

- It's behaviour is abnormal.
- It's performance is slow after you installed the Anti-Malware blade.
- A false-positive is detected.

Windows

You can exclude only .EXE files.

Syntax:

Fully qualified paths or an environment variable for the trusted executable.

Examples:

- `C:\Program Files\MyTrustedDirectory\MyTrustedProgram.exe`
- `%programdata%\MytrustedProgram.exe`

macOS

Syntax:

Fully qualified path for the trusted executable file.

Example:

```
/Applications/FileZilla.app/Contents/MacOS/filezilla
```

Files and Folders Exclusion

Files and Folder Exclusions are applied to all types of scans except contextual scan. The reason for configuring exclusions is to reduce the CPU usage of Anti-Malware.

Note - Files and folders must be excluded only if they are located in a Trusted zone or are considered a low-risk target for viruses.

Windows

Syntax:

Directory paths must end with a backlash.

Examples:

- Directory:
  - `C:\Program Files\MyTrustedDirectory\`
  - `%programdata%\MyTrustedDirectory\`
- Specific file:
  - `C:\ProgramFiles\MyTrustedDirectory\excludeMe.txt`
  - `%programdata%\MyTrustedDirectory\excludeMe.txt`
- File type:
  - `*.exe`
  - `\\ServerName\Share\folder\file.txt or \\ip_addres\Share\folder\file.txt` depending on a way file is attached.
  - `C:\Program Files\MyTrustedDirectory**.exe`(recursive exclusion - applies for all `.exe` in `C:\Program Files\MyTrustedDirectory\` and all subfolders)
- For Harmony Endpoint client version E80.80 or higher, you can exclude MD5 hash from the scheduled malware scan. For example:
  - `md5:0123456789012345`
    - Exclude by hash in any folder
  - `md5:0123456789012345:app.exe`
    - Exclude by hash and exact file name
  - `md5:0123456789012345:c:\folder\app.exe`
    - Exclude by hash and full path
  - `md5:0123456789012345:%ENV%\app.exe`
    - Exclude by hash and environment variable
- For Harmony Endpoint client version E86.10 or higher, you can exclude URL from the scheduled malware scan. For example:
  - `url:*.example.com`
  - `url:http://*.example.com`
  - `url:http://example.com/*`
  - `url:www.example.com/abc/123`

- `url:*192.168.*`
- `url:http://192.168.*`

Notes for URL exclusions-

- The * character replaces any sequence that contains zero or more characters.
- The www. character sequence at the beginning of an exclusion mask is interpreted as a *. sequence.
- If an exclusion mask does not start with the * character, the content of the exclusion mask is equivalent to the same content with the *. prefix.
- If an exclusion mask ends with a character other than / or *, the content of the exclusion mask is equivalent to the same content with the /* postfix.
- If an exclusion mask ends with the / character, the content of the exclusion mask is equivalent to the same content with the /*. postfix.
- The character sequence /* at the end of an exclusion mask is interpreted as /* or an empty string.
- URLs are verified against an exclusion mask, taking into account the protocol (http or https).

Note - For Windows, files and folder names are not case-sensitive.

macOS

Syntax:

Directory path, a specific file, or a file type. Environment variables are not supported.

Example:

Trusted directory

- `/Users/Shared/MyTrustedDirectory/`

Specific file

- `/Users/*/Documents/excludeMe.txt`

File type

- `*.txt`

Note - For macOS, files and folder names are case-sensitive.

Anti-Malware \ Exclude Infection by Name Exclusion

You can exclude some riskware files and infections from the scheduled malware scan on your computer.

Best Practice:

- Exclude when the specific software is allowed.
- As a temporary exclusion when there is a false positive detection.

Syntax

Infection name and protection name in your log.

Example:

- EICAR-Test-File

Notes -

- The infection name is case-sensitive.
- If you get a file protection detection, share the file with Check Point to resolve the file protection.

Threat Emulation, Threat Extraction, and Zero-Phishing Exclusions

You can exclude specific folders, domains or SHA1 hashes from the Threat Emulation, Threat Extraction and Zero-Phishing protection.

Domain exclusions

- Relevant only for Harmony Endpoint extension for Browsers.
- To exclude an IP, in the **Element** field, enter IP address followed by subnet mask in the format <X.X.X.X>/ <subnet mask >. For example, to exclude a computer with IP address 192.168.100.30, enter 192.168.100.30/24.
- Domain exclusions must be added without http/s, *, or any other special characters.

  Domain exclusions can be added with or without www.
- Sub-domain exclusions are supported.

  Exclusion of a domain will exclude all its subdomains as well.

For example:

If you enter the domain	It excludes these domains	It does not exclude these domains
www.domain.com	■ https://www.domain.com ■ http://www.domain.com	■ https://domain.com ■ http://domain.com ■ https://sub.domain.com ■ http://sub.domain.com
domain.com	■ https://www.domain.com ■ http://www.domain.com ■ https://domain.com ■ http://domain.com ■ https://sub.domain.com ■ http://sub.domain.com	-
sub.domain.com	■ https://sub.domain.com ■ http://sub.domain.com	https://sub2.domain.com

SHA1 exclusions -

- Relevant only for Threat Emulation blade (File system monitoring).

  For Harmony Endpoint version E86.40, SHA1 exclusion is supported on Harmony Endpoint extension for browsers as well (not including Internet Explorer). SHA1 can be used to exclude downloaded files from File Protection.

- It is not supported with Internet Explorer.
- File Reputation exclusions are set by SHA1.

Folder exclusions -

- Relevant only for Threat Emulation blade (File system monitoring).
- Folder path cannot contain environment variables.
- When you exclude a folder, enter the folder as a windows path. For example:

  ```
  C:\Program Files\MyTrustedDirectory\
  ```

- If the path of created file begins with exclusion, it will be excluded.
- Folder exclusions support wildcards. These wildcards are supported:

  ? - Each question mark masks one character.

  ***** - Each star masks zero or more characters.

- It is not advised to add * in the middle of path exclusions, as it may hurt the performance.

- Exclude network files by path `\\ServerName\Share\folder\`.This excludes all files located under `\ServerName\Share\folder\\`.

Behavioral Protections

Threat Emulation -> Anti-Exploit Exclusions

You can exclude these elements from the Anti-Exploit protection:

- **Protection Name** - Predefined malware signature
- **Process** - To exclude an executable

Currently there are five different Anti-Exploit protections available. Following is a list of the protections per-name.

Syntax for exclusions:

Protection	Protection Rule Name
Import-Export Address Table Parsing	Gen.Exploiter.IET
Return Oriented Programming	Gen.Exploiter.ROP
VB Script God Mode	Gen.Exploiter.VBS
Stack Pivoting	Gen.Exploiter.SP
RDP Vulnerability (CVE-2019-0708)	Gen.Exploiter.CVE_2019_0708
RCE Vulnerability (CVE-2019-1181)	Gen.Exploiter.CVE_2019_1181/2

Excluding a protection means that files will not be monitored by Anti-Exploit.

- Process and protection
  - `C:\Program Files\MyTrustedDirectory\excludeMe.exe`
  - Gen.Exploiter.ROP
- Protection
  - Gen.Exploiter.ROP

Anti-Ransomware and Behavioral Guard Exclusions

You can exclude these elements from the Anti-Ransomware and Behavioral Guard protection:

- **Folder** - To exclude a folder or non-executable files

- **Process** - To exclude an executable by element, MD5, and signer.
- **Certificate** - To exclude processes based on the company that signs the certificate.
- **Protection** - To exclude signature by it's name.

Notes:

- Excluded process will be monitored but not triggered.
- Excluded protection will not be triggered.

Syntax:

- Folder **can** contain environment variables
- Folder **cannot** contain wildcards (*)
- By default, sub-folders are included.

Excluding a Certificate / Process means that files modified / created by a certain process will not be backed up, or monitored by Anti-Ransomware and Behavioral Guard.

Windows

Syntax:

- You must specify name or full path
- Full path **can** contain environment variables
- Path or file name **cannot** contain wildcards

Examples:

- Full path
  - `C:\Program Files\MyTrustedDirectory\`
- Process
  - `C:\Program Files\MyTrustedDirectory\ExcludeMe.exe`
- Certificate
  - Microsoft
- md5: 0123456789012345
- Protection: win.blocker

macOS

Syntax:

- You **must** specify full path or wildcard
- Path or file name **can** contain wildcards
- Paths are case sensitive

Examples:

- Full path or Xcode exclusion:
  `:/Applications/Xcode.app/Contents?MacOS/Xcode`
- To cover all Xcode-related executables (not only GUI app):
  `/Applications/Xcode.app/*`

Excluding a Certificate / Process means that files modified / created by a certain process will not be backed up, or monitored by Anti-Ransomware and Behavioral Guard.

Analysis & Response Exclusions

Monitoring Exclusions

You can exclude these elements from monitoring:

- **Process** - To exclude an executable by element, MD5 and signer.
- **Certificate** - To exclude processes based on the company that signs the certificate.

Syntax:

- Process can be excluded by name only, or by full path.

  For example `C:\Program Files\MyTrustedDirectory\excludeMe.exe`
- Full path can contain environment variables.
- Full path CANNOT contain wildcards
- Certificate
  - Microsoft
- md5:0123456789012345
  - Exclude a process by hash.
- Excluding a Certificate / Process means thBAat files modified / created by a certain process will not be backed up, or monitored by Anti-Ransomware and Behavioral Guard.

Remediation

Excluding a file / folder / certificate from quarantine means that even if it is detected by one of the following blades: Threat Emulation / Anti-Ransomware / Anti-Bot, the file will not be quarantined:

- Full path can contain wildcards (*).
- Full path CANNOT contain environment variables.

Quarantine Exclusions

You can exclude a file or process from quarantine. You can define the exclusion by these criteria: certificate, file, folder, MD5 hash, SHA1 hash, and file extension. When an element is excluded from quarantine, even if there is a detection of malware, the file is not quarantined.

Configuring the Data Protection Policy

Configuring Full Disk Encryption

Full Disk Encryption gives you the highest level of data security for Endpoint Security client computers.

It combines boot protection and strong disk encryption to ensure that only authorized users can access data stored in desktop and laptop PCs.

Check Point's Full Disk Encryption has two main components:

- *"Check Point Disk Encryption for Windows" on page 101* - Ensures that all volumes of the hard drive and hidden volumes are automatically fully encrypted. This includes system files, temporary files, and even deleted files. There is no user downtime because encryption occurs in the background without noticeable performance loss. The encrypted disk is inaccessible to all unauthorized people.
- *"Authentication before the Operating System Loads (Pre-boot)" on page 102* - Requires users to authenticate to their computers before the computer boots. This prevents unauthorized access to the operating system using authentication bypass tools at the operating system level or alternative boot media to bypass boot protection.

Full Disk Encryption also supports *"BitLocker Encryption for Windows Clients" on page 108* and *"FileVault Encryption for macOS" on page 110*

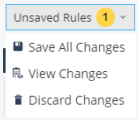
The Full Disk Encryption policy contains a pre-defined Default Policy rule, which applies to the entire organization.

Each new rule you create, has pre-defined settings, which you can then edit in the right section of the screen.

The Policy Rule Base consists of these parts:

Column	Description
Rule Number	The sequence of the rules is important because the first rule that matches traffic according to the protected scope is applied.
Rule Name	Give the rule a descriptive name.
Applied to	The protected scope to which the rule applies.
Full Disk Encryption	The configurations that apply to data encryption.

The **Policy** toolbar includes these options:

To do this	Click this
Create a new rule	
Save, view, or discard changes	
Duplicate a rule	
Install Policy	
Search for entity	
Delete a rule	

To disable Full Disk Encryption:

1. Go to the **Policy** view.
2. Click **Data Protection** > **General**.
3. In the **Capabilities and Exclusions** pane, click **Full Disk Encryption**.
4. In **Enable Pre-boot**, select **OFF**.
    - Smart
    - Legacy
    - Off
5. Click **Save & Install**.

Check Point Disk Encryption for Windows

Ensures that all volumes of the hard drive and hidden volumes are automatically fully encrypted. This includes system files, temporary files, and even deleted files. There is no user downtime because encryption occurs in the background without noticeable performance loss. The encrypted disk is inaccessible to all unauthorized people.

Configuration Options

- **Algorithms used**

  Go to **Advanced Settings** > **Encryption > Choose Algorithm**

  Full Disk Encryption can use these encryption algorithms

  - AES-CBC 256 bit (Default)
  - XTS-AES 128 bit
  - XTS-AES 256 bit

- **Volumes encrypted**

  By default, all drives that are detected after the installation and all visible disk volumes are encrypted. Intel Rapid Recover Technology (IRRT) are not encrypted.

  Go to **Advanced Settings** > **Encryption** > **Allow Self-Encrypting Drives (SED) hardware functionality** - Lets Full Disk Encryption probe and use SED disks that comply with the OPAL standard. If a compatible system and disk are detected, Full Disk Encryption uses the hardware encryption on the disk instead of the traditional software encryption.

  When using SED drives, leave **Encrypt hidden disk volumes** checked (which is the default setting)

  - AES encryption is always used with SED drives
  - Manage SED drives in the same way as software-encrypted drives

- **Initial Encryption**

  - **Encrypt entire drive** - Recommended for computers that are in production and already have user data, such as documents and emails.
  - **Encrypt used disk space only** - Encrypts only the data. Recommended for fresh Windows installations.

Authentication before the Operating System Loads (Pre-boot)

Protection requires users to authenticate to their computers before the operating system loads. This prevents unauthorized access to the operating system using authentication bypass tools at the operating system level or alternative boot media to bypass boot protection.

To enable Pre-boot:

Go to the **Policy** view > **Data Protection** > **General** > **Capabilities and Exclusions** > **Full Disk Encryption** > click **Enable Pre-boot**.

Best Practice - We recommend to enable Pre-boot. When Pre-boot is disabled, the user can bypass the Pre-boot authentication at the cost of reducing the security to a level below encryption strength. Users authenticate to their computers only at the operating system level. If Pre-boot is disabled, consider using SSO or enable bypass pre-boot when connected to LAN.

Temporary Pre-boot Bypass Settings

Temporary Pre-boot Bypass lets the administrator disable Pre-boot protection temporarily, for example, for maintenance. It was previously called Wake on LAN (WOL). You enable and disable Temporary Pre-boot Bypass for a computer, group, or OU from the computer or group object. The Pre-boot settings in the Full Disk Encryption policy determine how Temporary Pre-boot Bypass behaves when you enable it for a computer.

Temporary Pre-boot Bypass reduces security. Therefore use it only when necessary and for the amount of time that is necessary. The settings in the Full Disk Encryption policy set when the Temporary Pre-boot Bypass turns off automatically and Pre-boot protection is enabled again.

You can configure the number of minutes the Pre-boot login is displayed before automatic OS logon.

There are different types of policy configuration for Temporary Pre-boot Bypass:

- **Allow OS login after temporary bypass**.
- **Allow bypass script**

  If you run scripts to do unattended maintenance or installations (for example, SCCM) you might want the script to reboot the system and let the script continue after reboot. This requires the script to turn off Pre-boot when the computer is rebooted . Enable this feature in the Temporary Pre-boot Bypass Settings windows. The Temporary Pre-boot Bypass script can only run during the timeframe configured in Temporary Pre-boot Bypass Settings.

Running a temporary bypass script:

In a script you execute the `FdeControl.exe` utility to enable or disable Pre-boot at the next restart:

- To disable Temporary Pre-boot Bypass, run:

  ```
  FDEControl.exe set-wol-off
  ```

- To enable Temporary Pre-boot Bypass, run:

  ```
  FDEControl.exe set-wol-on
  ```

The above commands fail with code 13 (UNAUTHORIZED) if executed outside the timeframe specified in the policy.

You can select the Temporary Pre-boot Bypass duration:

- **On demand**, **Once**, or **Weekly**,
- **Disable after X automatic logins** - Bypass turns off after the configured number of logins to a computer.
- **Disable after X days or hours** - Bypass turns off after the configured days or hours passed.

Note - If you select both **Disable after X automatic logins** and **Disable after X days or hours**, bypass turns off when any of these options occurs.

Best Practice - Select a small number so that you do not lower the security by disabling the Pre-boot for a long time.

Advanced Pre-boot Settings

Action	Description
Display last logged on user in Pre-boot	The username of the last logged on user shows in the Pre-boot logon window. That user only needs to enter a password or Smart Card pin to log in
Reboot after [x] failed logon attempts were made	■ If active, specify the maximum number of failed logons allowed before a reboot takes place. ■ This setting does not apply to smart cards. Smart Cards have their own thresholds for failed logons.
Verification text for a successful logon will be displayed for	Select to notify the user that the logon was successful, halting the boot-up process of the computer for the number of seconds that you specify in the Seconds field.

Action	Description
Enable USB devices in Pre-boot environment	Select to use a device that connects to a USB port. If you use a USB Smart Card you must have this enabled. If you do not use USB Smart Cards, you might need this enabled to use a mouse and keyboard during Pre-boot.
Enable visual impaired support in pre-boot environment	Select to enable sound-based assistance to visually challenged users to complete pre-boot login. 1. When the pre-boot screen is ready, a sound is played. User must type the user name and press the **Tab** key. 2. When it is ready, a sound is played. User must type the password and press the **Enter** key. If the login is not successful, a sound is played, and cursor is placed in the **Username** field, and repeat steps 1 and 2.
Enable TPM two-factor authentication (password & dynamic tokens)	Select to use the TPM security chip available on many PCs during pre-boot in conjunction with password authentication or Dynamic Token authentication. The TPM measures Pre-boot components and combines this with the configured authentication method to decrypt the disks. If Pre-boot components are not tampered with, the TPM lets the system boot. See sk102009 for more details.
Firmware update friendly TPM measurements	Disables TPM measurements on Firmware/BIOS level components. This makes updates of these components easier but reduces the security gained by the TPM measurements because not all components used in the boot sequence are measured. If this setting is enabled on UEFI computers, the Secure Boot setting is included in the measurement instead of the firmware.
Enable remote help without pre-boot user	Select to enable remote help without the need of assigning any Pre-boot user to the computer. When giving remote help, select the Pre-Boot Bypass Remote Help type that performs a One-Time logon. The setting is only available if Pre-boot is configured to be disabled.
Remote Help	**Enable remote help on pre-boot** - Users can use Remote Help to get access to their Full Disk Encryption protected computers if they are locked out. **Select security level** - Here you configure the number of characters in the Remote Help response that users must enter. **Enable Self-Unlock** - Users can unlock their endpoint by scanning a QR code using their mobile device, without the Administrator's intervention.

User Authorization before Encryption

Full Disk Encryption policy settings enable user acquisition by default. If user acquisition is disabled, the administrator must assign at least one Pre-boot user account to each client computer before encryption can start. You can require one or more users to be acquired before encryption can start. You can also configure clients to continue user acquisition after Pre-boot is already enabled. This might be useful if a client computer is used by many users, also called roaming profiles.

Usually a computer has one user and only one user must be acquired. If the computer has multiple users, it is best if they all log on to the computer for Full Disk Encryption to collect their information and acquire them.

User acquisition settings

- **Enable automatic user acquisition**
- **Amount of users to acquire before Pre-boot is enabled** - Select the number of users to acquire before the Harmony Endpoint enforces Pre-boot on acquired users.
- **Enable Pre-boot if at least one user has been acquired after X days** - Select the number of days to wait before Pre-boot is enforced on acquired users. This setting limits the number of days when user acquisition is active for the client. If the limit expires and one user is acquired, Pre-boot is enforced and encryption can start. If no users are acquired, user acquisition continues. Pre-boot is enforced on acquired users after one of the criteria are met.

To configure the advanced settings for user acquisition, go to **Advanced Settings** > **User Acquisition**:

- **Continue to acquire users after Pre-boot has been enforced** - Pre-boot is active for users who were acquired and user acquisition continues for those who were not acquired.
- **User acquisition will stop after having acquired additional X users** - User acquisition continues until the selected number of additional users are acquired.

Note - If you need to terminate the acquisition process, for example, if the client fails to acquire users although an unlimited time period is set, define a new automatic acquisition policy.

User Assignment

You can view, create, lock and unlock authorized Pre-boot users.

To add a user to the list of users authorized to access a device:

1. In the Endpoint Web Management Console, go to **Computer Management** > **Full Disk Encryption** > **User Assignment**.

The **Authorize Pre-Boot Users** window opens. You can see the authorized users for each device you search.

2. Click the  icon.

   The **Create New Pre-boot User** window opens.

3. Enter these details:

   - **Logon Name**
   - **Password**
   - **Account Details**
     - **Lock user for Pre-boot**
     - **Require change password after first logon** - Applies only to password authentication. Select this option to force users to change their password after the first pre-boot logon.
   - **Expiration Settings** - Select an expiration date for the user authorization.

To lock or unlock a user -

1. In the Endpoint Web Management Console, go to **Computer Management** > **Full Disk Encryption** > **User Assignment**.

   The **Authorize Pre-Boot Users** window opens.

2. In the search box, search for the applicable device.

   The list of authorized users to access the device appears.

3. Click on the user on the list to select it and click on the lock icon above the list to lock or unlock the user.

Single Sign-On with OneCheck Logon

OneCheck Logon is a Single Sign-On solution that let users log at one time to authenticate to all these :

- Full Disk Encryption
- DLP
- Windows
- VPN

When OneCheck Logon is enabled, a different logon window opens that looks almost the same as the regular Windows authentication window. The logon credentials are securely stored internally. These actions define if you enable OneCheck Logon:

To configure OneCheck Logon properties, go to **Advanced Settings** > **Windows Authentication**:

- **Enable lock screen authentication (OneCheck)** - Users log on one time to authenticate to the operating system, Full Disk Encryption, and other Endpoint Security components. To configure the password properties for the single sign-on, go to **Policy** > **Global Policy Settings** > **Full Disk Encryption**.
- **Enable Check Point Endpoint Security screen saver** - The screen saver is active only after a Full Disk Encryption policy has been installed on the client. After selecting the Check PointEndpoint Security screen saver option, enter the text that appears when the screen saver is active, and the number of minutes the client remains idle before the screen saver activates.
- **Only allow authorized Pre-boot users to log into the operating system** - If selected, only users that have permission to authenticate to the Pre-boot on that computer can log on to the operating system.
- **Use Pre-boot account credentials in OS lock screen** - If selected, users authenticate in the regular Operating System login screen but with the credentials configured for Pre-boot.

  Best Practice - Best practice is to only use this feature when there is no Active Directory available. For customers that use Active Directory, we recommend a combination of User Acquisition, OneCheck Logon, and Password Synchronization that will let users use the same credentials for Pre-boot and Windows login.

BitLocker Encryption for Windows Clients

BitLocker encrypts the hard drives on a Windows computer, and is an integral part of Windows.

Check Point BitLocker uses the Endpoint Security Management Server, Client Agent and the Harmony Endpoint UI to manage BitLocker.

BitLocker Management is implemented as a Windows service component called Check Point BitLocker Management.

It runs on the client together with the Client Agent (the Device Agent).

Check Point BitLocker Management uses APIs provided by Microsoft Windows to control and manage BitLocker.

Configuration options:

Setting	Description
Initial Encryption	■ **Encrypt entire drive** - Recommended for computers that are in production and already have user data, such as documents and emails. ■ **Encrypt used disk space only** - Encrypts only the data. Recommended for fresh Windows installations.
Drives to encrypt	■ **All drives** - Encrypt all drives and volumes. ■ **OS drive only** - Encrypt only the OS drive (usually, C:\). This is the default.
Encryption algorithm	■ **Windows Default** - This is recommended. On Windows 10 or later, unencrypted disks are encrypted with XTS-AES-128. On encrypted disks, the encryption algorithm is not changed. ■ **XTS-AES-128** ■ **XTS-AES-256**

Note - To take control of a BitLocker-encrypted device, the target device must have a Trusted Platform Module (TPM) module installed.

Best Practices:

- When you change the encryption engine of a client from Check Point Full Disk Encryption to BitLocker Management, or from BitLocker Management to Check Point Full Disk Encryption, the disk on the client is decrypted and then encrypted.
  This causes the disk to be in an unencrypted state for some time during the process.
  We recommend that you do not change the entire organization to BitLocker in one operation.
  Make the change for one group of users at a time.
- Configure the BitLocker policy **before** you install the Endpoint Security package on the client computers.
  This makes sure that encryption happens just one time, with BitLocker - instead of the cycle of Check Point FDE encryption > FDE decryption > BitLocker encryption.

FileVault Encryption for macOS

FileVault encrypts the hard drive on a Mac computer, and is an integral part of macOS. The Harmony Endpoint automatically starts to manage the disk encrypted with FileVault without disabling the encryption.

Global Policy Settings for Full Disk Encryption

- **Password Complexity** - Here you configure the password properties for OneCheck Logon.
- **Pre-boot Authentication Settings** - If the Pre-boot is required on a computer as part of Full Disk Encryption, users must authenticate to their computers in the Pre-boot, before the computer boots. Users can authenticate to the Pre-boot with these methods:
  - **Password** - Username and password. This is the default method.
  - **SmartCard (requires certificates)** - A physical card that you associate with a certificate. Users must have a physical card, an associated certificate, and Smart Card drivers installed.
  - **Either SmartCard or Password**
- **Pre-boot Images** - For each of these graphics, you can select to upload a new image or **Revert to Default** image:

Item	Description	Size of Image
Pre-boot Background Image	Image on Pre-boot screen behind the smaller logon window	800 x 600 pixels
Pre-boot Screen Saver	Image that shows when the system is idle	260 x 128 pixels
Pre-boot Banner Image	The banner image on the smaller logon window	447 x 98 pixels
OneCheck Background Image	Image in the background of the Windows logon window if OneCheck Logon is enabled	256 KB or smaller
Client Notification (UserCheck) Icon	Icon in the top-right of a Client Notification (UserCheck)	135 x 46 pixels

Check Point Full Disk Encryption Self-Help Portal

The Self-Help Portal lets users reset their own passwords for Full Disk Encryption. To use the Self-Help Portal, the user must register to the portal first. After registration users can use the Self-Help Portal for password recovery.

The Self-Help Portal only works with Active Directory users. Make sure that the Endpoint Security Active Directory Scanner is configured and that the Active Directory is scanned.

The portal is available for desktop and mobile devices.

For supported browsers and devices, see the *R81.10 Release Notes*.

Activating the Self-Help Portal

You must enable the Self-Help Portal on the Endpoint Security Management Server to activate it.

Note - In **Gaia Portal > Hosts and DNS** page, make sure to configure:

- The DNS Sever
- Domain Name
- DNS suffix

To enable the Self-Help Portal:

On the Endpoint Security Management Server, run these commands:

```
cd $UEPMDIR/engine/scripts
selfhelp_cmd enable
```

Note that this restarts the Endpoint Security Management Server.

After activation, the Self-Help Portal is available at:

```
http://<IP Address of Endpoint Security Management Server>/eps_shp
```

To disable the Self-Help Portal, run:

```
selfhelp_cmd disable
```

To query the status the Self-Help Portal, run:

```
selfhelp_cmd status
```

Configuring the Self-Help Portal

The Self-Help Portal only works with Active Directory users. Before you can use the Portal, make sure that the Endpoint Security Active Directory Scanner is configured and that the Active Directory is scanned.

Users must be authorized for Pre-boot on one or more computers before they register in the Portal.

To configure Self-Help Portal settings in SmartEndpoint:

1. In the **Policy** Tab, in a **OneCheck User Settings** rule, right-click the **Allow password Self Help** action and select **Edit**.
2. Select **Allow password self-help** to let users recover their password by answering questions. Clear the option to not let users recover their password by answering questions.
3. Make selections to configure the options for **Enrollment** to the Portal and **Password Assistance**.
4. Click **Questions Bank** to select which questions are asked for user enrollment to the Self-Help Portal.
5. Click **OK**.
6. Click **OK**.
7. Save.
8. Click **Install Policy** and select the **Self-Help Settings** Policy.

Users can register to the Self-Help Portal and use it to recover passwords.

The portal address is:

`http://<IP Address of Endpoint Security Management Server>/eps_shp`

User Settings for the Self-Help Portal

You can force users to re-register to the Self-Help Portal or block users from recovering password in the portal.

To change a user's settings for the Self-Help Portal:

1. In SmartEndpoint, in the **Users and Computers** tab, right-click on a user and select **User Authentication (OneCheck)**.
2. Select **Reset Self-Help Enrollment** to force the user to re-register to the portal.

Select **Lock Password Self-Help** to prevent users from recovering passwords in the portal.

3. A confirmation message shows. Click **Yes**.

Monitoring the Self-Help Portal Policy

To see the status of user enrollment and recovery for the Self-Help Portal:

In SmartEndpoint, in the **Reporting** tab, select **User Authentication Policy** > **Self Help Status**.

Configuring Media Encryption & Port Protection

Media Encryption & Port Protection protects data stored in the organization by encrypting removable media devices and allowing tight control over computer ports (USB, Bluetooth, and so on). Removable devices are for example: USB storage devices, SD cards, CD/DVD media and external disk drives.

On the client-side, Media Encryption & Port Protection protects sensitive information by encrypting data and requiring authorization for access to storage devices and other input/output devices.

Media Encryption lets users create encrypted storage on removable storage devices that contain business-related data. Encrypted media is displayed as 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. Rules can apply different access permissions for business data and non-business data.

Port Protection controls, according to the policy, device access to all available ports including USB and Firewire (a method of transferring information between digital devices, especially audio and video equipment). Policy rules define access rights for each type of removable storage device and the ports that they can connect to. The policy also prevents users from connecting unauthorized devices to computers.

Media Encryption & Port Protection functionalities are available in both Windows and macOS clients (for macOS starting at client version E85.30).

Best Practice - We recommend to 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.

For instructions on how to encrypt, see sk166110.

Configuring the Read Action

The Read action defines the default settings for read access to files on storage devices. For each action, you can define different settings for specified device types. The default predefined actions are:

- **Allow encrypted data** - Users can read encrypted data from storage devices (typically business-related data).
- **Allow unencrypted data** - Users can read unencrypted data from storage devices (typically non business-related data).

You can configure these actions for specific devices.

To configure the Read action:

1. In the **Media Encryption** tab, go to **Exclusions Center**.
2. Click **New** to create a new exclusion or configure an existing exclusion on the list.

3. Configure the options as necessary for: **Read Encrypted**, **Read Unencrypted**:
    - **Read Encrypted**
        - **Accept** - Allow reading only encrypted data from the storage device. Users cannot read unencrypted data from the storage device.
        - **According to Policy** - According to the default Media Encryption & Port Protection rule.
        - **Block** - Block all reading from the storage device.
    - **Read Unencrypted**
        - **Accept** - Allow reading of unencrypted files from the storage device.
        - **According to Policy** - According to the default Media Encryption & Port Protection rule
        - **Block** - Block reading of unencrypted files from the storage device.

To import exclusions:

You can import an exported exclusion file in the JSON format.

1. In the **Media Encryption** tab, click **View Exclusions**.
2. Click **Import** and select the JSON file.

To export exclusions:

1. In the **Media Encryption** tab, click **View Exclusions**.
2. Select the exclusion from the list.
3. Click **Export**.

Configuring the Write Action

The Write action lets users:

- Create new files
- Copy or move files to devices
- Delete files from devices
- Change file contents on devices
- Change file names on devices

The default predefined write actions are:

- **Data Type - Encrypt business-related data on storage devices** - All Files that are defined as business-related data must be written to the encrypted storage. Non-business related data can be saved to the device without encryption. See *"Configuring Business-Related File Types" on the next page*.
- **Allow writing data on storage devices:**
  - **Allow encryption** - Users can write only encrypted files to storage devices.
  - **Enable deletion of file on read-only media** - Allow users to delete files on devices with read-only permissions.

You can configure these settings for specific devices.

To configure the Write action:

1. In the **Media Encryption** tab, go to **Exclusions Center**.
2. Click **New** to create a new exclusion or configure an existing exclusion on the list.
3. Per each device, configure the options as necessary for: **Data Type** and **Write Encrypted**:
   - **Data Type** - Select one of these options:
     - **Allow any data** - Users can write all file types to storage devices.
     - **Encrypt business-related data** - Users must encrypt all business-related files written to storage devices. Other files can be written without encryption. See *"Configuring Business-Related File Types" on the next page*.
     - **Encrypt all data** - Users must encrypt all files written to storage devices.
     - **Block any data** - Users cannot write any files to storage devices.
   - **Write Encrypted** - Select one of these options:
     - **Accept** - Users must encrypt files written to storage devices.
     - **According to Policy** - According to the default Media Encryption & Port Protection rule.
     - **Block** - Block all writing to storage devices.

Notes:

- If no read policy is allows, the write policy is disabled automatically.
- If **Block any Data** is selected, **Allow encryption** and **Configure File Types** are disabled.

To import exclusions:

You can import an exported exclusion file in the JSON format.

1. In the **Media Encryption** tab, click **View Exclusions**.
2. Click **Import** and select the JSON file.

To export exclusions:

1. In the **Media Encryption** tab, click **View Exclusions**.
2. Select the exclusion from the list.
3. Click **Export**.

Configuring Business-Related File Types

The organization's policy defines access to business and non-business related data. Business-related files are confidential data file types that are usually encrypted in the business-related drive section of storage devices. These files are defined as business-related file types by default:

- **Multimedia** - QuickTime, MP3, and more.
- **Executable** - Exe, shared library and more.
- **Image** - JPEG, GIF, TIF and more.

These files are defined as non-business related file types by default:

- **Spreadsheet** - Spreadsheet files, such as Microsoft Excel.
- **Presentation** - Presentation files, such as Microsoft Power Point.
- **Email** - Email files and databases, such as Microsoft Outlook and MSG files.
- **Word** - Word processor files, such as Microsoft Word.
- **Database** - Database files, such as Microsoft Access or SQL files.
- **Markup** - Markup language source files, such as HTML or XML.
- **Drawing** - Drawing or illustration software files, such as AutoCAD or Visio.
- **Graphic** - Graphic software files such as Photoshop or Adobe Illustrator.
- **Viewer** - Platform independent readable files, such as PDF or Postscript.
- **Archive** - Compressed archive files, such as ZIP or SIT.

To see the list of business-related file types and non-business related file types:

In the Endpoint Web Management Console, go to the **Policy** view > **Data Protection** > **Capabilities and Exclusions** pane > **Media Encryption** > **Write Policy** > **Configure File Types** > **View Mode**. Select **Non-Business-Related** or **Business-Related** to see the relevant file types.

To configure business and non-business related file types:

1. In the Endpoint Web Management Console, go to the **Policy** view > **Data Protection** > **Capabilities and Exclusions** pane > **Media Encryption** > **Write Policy** > **Configure File Types**.
2. You can:
   - Add or delete files from the business-related or non-business related file list. In **View Mode**, select **Business-related** or **Non-business related**. Add or delete the required files. A file type which is not in the business-related file list, is automatically included in the non business-related file type list.
   - Create new file types in the business-related or non-business related file type list. Click the **Create new file type** button. The **File type add/edit** window opens. Configure **Name**, **File Extension** and **File Signatures** and click **OK**.

Managing Devices

You can configure custom settings for specified devices or device types. These device settings are typically used as exceptions to settings defined in Media Encryption & Port Protection rules.

There are two types of devices:

- **Storage Device** -Removable media device on which users can save data files. Examples include: USB storage devices, SD cards, CD/DVD media and external disk drives.
- **Peripheral Device** - Devices on which users cannot save data and that cannot be encrypted.

Click the icon to filter your view.

New devices are added manually or are automatically discovered by the Endpoint Server.

To view your devices, in the **Data Protection** view, go to **Manage Devices**. You can select to see **Manually added devices** or **Discovered devices**. In the **Device Type** column, you can see if the device is a storage device or a peripheral device.

To manually add a new device:

1. In the **Data Protection** view, go to **Manage Devices**.
2. Click the **Add Manually** icon , and select **Storage Device** or **Peripheral Device**.
3. Edit device details:

- **Device Name** - Enter a unique device display name, which cannot contain spaces or special characters (except for the underscore and hyphen characters).
- **Connection type** - Select the connection type Internal, External or Unknown (required).
- **Category** - Select a device category from the list.
- **Serial Number** - Enter the device serial number. You can use wild card characters in the serial number to apply this device definition to more than one physical device. See *"Using Wild Card Characters" on the next page*.
- **Extra Information** - Configure whether the device shows as fixed disk device (Hard Drive with Master Boot Record), a removable device (Media without Master Boot Record) or None.
- **Icon** - Select an icon to show in the GUI.
- **Device ID Filter** - Enter a filter string that identifies the device category (class). Devices are included in the category when the first characters in a Device ID match the filter string. For example, if the filter string is My_USB_Stick, these devices are members of the device category:
  - `My_USB_Stick_40GB`
  - `My_USB_Stick_80GB`
- **Supported Capabilities**
  - **Log device events** - Select this option to create a log entry when this device connects to an endpoint computer (Event ID 11 or 20 only).
  - **Allow encryption** - Select this option if the device can be encrypted (storage devices only).

4. **Assign Groups** (relevant for storage devices only) - you can assign the device to an **existing group**, **create a new group** or **do not add to group**.
5. Click **Finish**.

To add an exclusion to a device:

1. In the **Data Protection** view, go to **Manage Devices**.

   The **Manage storage and peripheral devices** window opens.
2. Right-click the applicable device and select **Create Exclusion**.

   The **Device Override Settings** window opens.

3. Configure the required **Read Policy** and **Write Policy**. For more information on the configuration options, see *"Configuring the Read Action" on page 114* and *"Configuring the Write Action" on page 115*
4. Click **Finish**.

Note - If a device has an exclusion already in place, the new exclusion overrides an existing exclusion.

Managing Groups

You can create groups for storage devices. Using device groups facilitates policy management because you can create exclusion rules for an entire group of devices instead of per one device each time. To create a new device group, in the **Policy** view, go to **Data Protection** > **Manage Devices** > **Storage Device Groups**. You can create new groups or edit existing groups.

Note - You cannot delete groups that are in use.

Using Wild Card Characters

You can use wild card characters in the Serial Number field to apply a definition to more than one physical device. This is possible when the device serial numbers start with the same characters.

For example: If there are three physical devices with the serial numbers 1234ABC, 1234BCD, and 1234EFG, enter 1234* as the serial number. The device definition applies to all three physical devices. If you later attach a new physical device with the serial number 1234XYZ, this device definition automatically applies the new device.

The valid wild card characters are:

The '*' character represents a string that contains one or more characters.

The '?' character represents one character.

Examples:

Serial Number with Wildcard	Matches	Does Not Match
1234*	1234AB, 1234BCD, 12345	1233
1234???	1234ABC, 1234XYZ, 1234567	1234AB, 1234x, 12345678

Because definitions that use wildcard characters apply to more endpoints than those without wildcards, rules are enforced in this order of precedence:

1. Rules with serial numbers containing * are enforced first.
2. Rules with serial numbers containing ? are enforced next.
3. Rules that contain no wildcard characters are enforced last.

For example, rules that contain serial numbers as shown here are enforced in this order:

1. 12345*
2. 123456*
3. 123????
4. 123456?
5. 1234567

Advanced Settings for Media Encryption

Authorization Settings

You can configure a Media Encryption & Port Protection rule to require scans for malware and unauthorized file types when a storage device is attached. You also can require a user or an administrator to authorize the device. This protection makes sure that all storage devices are malware-free and approved for use on endpoints.

On E80.64 and higher clients, CDs and DVDs (optical media) can also be scanned.

After a media device is authorized:

- If you make changes to the contents of the device in a trusted environment with Media Encryption & Port Protection, the device is not scanned again each time it is inserted.
- If you make changes to the contents of the device in an environment without Media Encryption & Port Protection installed, the device is scanned each time it is inserted into a computer with Media Encryption & Port Protection.

You can select one of these predefined options for a Media Encryption & Port Protection rule:

Require storage devices to be scanned and authorized -

- **Scan storage devices and authorize them for access** - Select to scan the device when inserted. Clear to skip the scan.

- **Enable self-authorization** - If this option is selected, users can scan the storage device manually or automatically. If this setting is cleared, users can only insert an authorized device.
    - **Manual media authorization** - The user or administrator must manually authorize the device.

      Allow user to delete unauthorized files - The user can delete unauthorized files detected by the scan. This lets the user or administrator authorize the device after the unauthorized files are deleted.
    - **Automatic media authorization** -The device is authorized automatically.

      Allow user to delete unauthorized files - The user can delete unauthorized files detected by the scan. This lets the user or administrator authorize the device after the unauthorized files are deleted.

- **Exclude optical media from scan** - Exclude CDs and DVDs from the scan.

In **Advanced Settings** > **Authorization Scanning**, you can configure authorized and non-authorized file types.

Unauthorized - Configure the file types that are blocked. All other file types will be allowed.

Authorized - Configure file types that are allowed. All other file types will be blocked.

UserCheck Messages

UserCheck for Media Encryption & Port Protection tells users about policy violations and shows them how to prevent unintentional data leakage. When a user tries to do an action that is not allowed by the policy, a message shows that explains the policy.

For example, you can optionally let users write to a storage device even though the policy does not allow them to do so. In this case, users are prompted to give justification for the policy exception. This justification is sent to the security administrator, who can monitor the activity.

Advanced Encryption

- **Allow user to choose owner during encryption** - Lets users manually define the device owner before encryption. This lets users create storage devices for other users. By default, the device owner is the user who is logged into the endpoint computer. The device owner must be an Active Directory user.
- **Allow user to change the size of encrypted media** - Lets users change the percentage of a storage device that is encrypted, not to be lower than Minimum percentage of media capacity used for encrypted storage or Default percentage of media capacity used for encrypted storage. .
- **Allow users to remove encryption from media** - Lets users decrypt storage devices.

- **When encrypting, unencrypted data will be -** Select one of these actions for unencrypted data on a storage device upon encryption:
  - **Copied to encrypted section** - Unencrypted data is encrypted and moved to the encrypted storage device. We recommend that you back up unencrypted data before encryption to prevent data loss if encryption fails. For example, if there is insufficient space on the device.
  - **Deleted** - Unencrypted data is deleted.
  - **Untouched** - Unencrypted data is not encrypted or moved.
- **Secure format media before encryption** - Run a secure format before encrypting the storage device. Select the number of format passes to do before the encryption starts.
- **Change device name and icon after encryption** - When selected, after the device is encrypted, the name of the non-encrypted drive changes to Non Business Data and the icon changes to an open lock. When cleared, the name of the non-encrypted drive and the icon do not change after the device is encrypted.
- **When encrypting media, file system should be:**
  - **As already formatted** -According to the original format.
  - **ExFAT**
  - **FAT32**
  - **NTFS**

  Allow user to change the file system of the encrypted storage - After storage was encrypted in a specific format, the user can change this format to another format.

Site Configuration

Site Actions control when to allow or prevent access to encrypted devices that were encrypted by different Endpoint Security Management Servers. Each Endpoint Security Management Server (known as a Site) has a Universally Unique Identifier (UUID). When you encrypt a storage device on an Endpoint Security client, the Endpoint Security Management Server UUID is written to the device. The Site action can prevent access to devices encrypted on a different Endpoint Security Management Server or from another organization. The Site action is enabled by default.

When a user attaches a storage device, Media Encryption & Port Protection makes sure that the device matches the UUID the Endpoint Security Management Server UUID or another trusted Endpoint Security Management Server. If the UUIDs match, the user can enter a password to access the device. If the UUID does not match, access to the device is blocked.

Allow access to storage devices encrypted at any site - Endpoint Security clients can access encrypted devices that were encrypted at any site.

Allow access to storage devices encrypted at current site only - Media Encryption Site (UUID) verification is enabled. Endpoint Security clients can only access encrypted devices that were encrypted by the same Endpoint Security Management Server.

Media Lockout (Lockout Settings)

You can configure Media Encryption & Port Protection to lock a device after a specified number of unsuccessful login attempts:

- **Temporarily** - If a device is locked temporarily, users can try to authenticate again after a specified time. You can configure the number of failed login attempts before a temporary lockout and the duration of lockout.
- **Permanently** - If a device is locked permanently, it stays locked until an administrator unlocks it. You can configure the number of failed login attempts before a permanent lockout

Offline Access

Password protect media for access in offline mode - Lets users assign a password to access a storage device from a computer that is not connected to an Endpoint Security Management Server. Users can also access the storage device with this password from a non-protected computer.

Allow user to recover their password using remote help - Lets user recover passwords using remote help.

Copy utility to media to enable media access in non-protected environments - Copies the Explorer utility to the storage device. This utility lets users access the device from computers that are not connected to an Endpoint Security Management Server.

Media Encryption Remote Help

Media Encryption & Port Protection lets administrators recover removable media passwords remotely, using a challenge/response procedure. Always make sure that the person requesting Remote Help is an authorized user of the storage device before you give assistance.

To recover a Media Encryption & Port Protection password with Remote Help assistance from Harmony Endpoint:

1. In the **Computer Management** view, go to **Data Protection Actions** > **Media Encryption Remote Help**.

   The **Media Encryption Remote Help** window opens.

2. Fill in these details:

a. Select the user

b. In the **Challenge** field, enter the challenge code that the user gives you. Users get the Challenge from the Endpoint client.

c. Click **Generate Response**.

Media Encryption & Port Protection authenticates the challenge code and generates a **Response** code..

d. Give the **Response** code to the user.

e. Make sure that the user can access the storage device successfully.

Port Protection

Port Protection protects the physical port when using peripheral devices.

Peripheral devices are for example, keyboards, screens, blue tooth, Printers, Smart Card, network adapters, mice and so on.

To create a new Port Protection rule:

1. In the **Data Protection** policy, go to the right pane - **Capabilities & Exclusions** > **Port Protection** > **Edit Policy**.

   The **Port Protection Settings** window opens.

2. Click **New**.

   The **New Port Protection Rule** window opens.

3. Select a device from the drop-down menu or click **New** to create a new device (see Managing Devices for details on how to create a new device).

4. Select the **Access Type** from the drop-down menu:

   Accept - Allow connecting the peripheral device.

   Block - Do not allow connecting the peripheral device.

5. In the **Log Type** field, select the log settings:

   - **Log** - Create log entries when a peripheral device is connected to an endpoint computer (Action IDs 11 and 20).
   - **None** - Do not create log entries.

6. Click **Create**.

Global Policy Settings for Media Encryption

You can select a global action that defines automatic access to encrypted devices. This has an effect on all Media Encryption & Port Protection rules, unless overridden by a different rule or action.

Make sure that the Read Policy allows access to the specified users or devices.

In the **Policy** view > **Global Policy Settings** > **Media Encryption Access Rules**, you can select one of these settings or create your own custom rules for automatic access to encrypted devices:

- **Encrypted storage devices are fully accessible by all users** - All users can read and change all encrypted content.
- **All users in the organization can read encrypted storage devices, only owners can modify** - All users can read encrypted files on storage devices. Only the media owner can change encrypted content.
- **Only owners can access encrypted storage devices** - Only media owners can read and/or change encrypted content.
- **Access to encrypted storage devices requires password authentication** - Users must enter a password to access the device. Automatic access in not allowed.
- **Custom** - Create a customized automatic access rule to encrypted devices. There are two predefined action rules in this window. You cannot delete these rules or change the media owner or media user. But, you can change the access permissions. The two predefined actions are defaults that apply when no other custom action rules override them. The Any/Media Owner action rule is first by default and the Any/Any action rule is last by default. We recommend that you do not change the position of these rules.

  To create a new customized automatic access rule to encrypted devices:

  1. Click **Add** and **Edit** to create a new rule.

     The **Edit Media Access Rule** window opens.

2. Configure these settings:
    - In the **Encrypted Media Owner** field, select one of these options:
        - **Rule applies to any encrypted media owner** - This action applies to any user.
        - **Choose a user/group/ou from your organization** - Select the applicable user, group or OU to which this action applies.
    - In the **Encrypted Media User** field, select one of these options:
        - **Rule applies to any encrypted media user** - This action applies to any user.
        - **Select the media owner as the encrypted media user** - The media owner is also defined as the user.
        - **Choose a user/group/ou from your organization** - Select the applicable user, group or OU to which this action applies.
3. Click **OK**.
4. Click the field in the **Access Allowed** column, and select one of these parameters:
    - **Full Access**
    - **No Automatic Access**
    - **Read-Only**

Configuring Access & Compliance Policy

Firewall

The Firewall guards the "doors" to your devices, 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 device, 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.

When you plan a Firewall Policy, think about the security of your network and convenience for your users.

A policy must let users work as freely as possible, but also reduce the threat of attack from malicious third parties.

Firewall rules accept or drop network traffic to and from Endpoint computers, based on connection information, such as IP addresses, Domains, ports and protocols.

Configuring Inbound/Outbound Rules

The Endpoint client checks the firewall rules based on their sequence in the Rule Base. Rules are enforced from top to bottom.

The last rule is usually a Cleanup Rule that drops all traffic that is not matched by any of the previous rules.

Important - When you create Firewall rules for Endpoint clients, create explicit rules that allow all endpoints to connect to all the domain controllers on the network.

Note - The Endpoint client do not support DNS over HTTPS.

Inbound Traffic Rules

Inbound traffic rules define which network traffic can reach Endpoint computers (known as localhost).

The Destination column in the Inbound Rule Base describes the Endpoint devices to which the rules apply (you cannot change these objects).

These four inbound rules are configured by default:

No.	Name	Source	Service	Action	Track	Comment
1	Allow Trusted Zone	Trusted_ Zone	Any	Allow	None	
2	Allow IP obtaining	Internet_ Zone	bootp dhcp-relay dhcp-req-local dhcp-rep-local	Allow	None	
3	Allow PPTP	Internet_ Zone	gre pptp-tcp L2TP	Allow	None	
4	Cleanup rule	Any	Any	Block	Log	

Outbound Traffic Rules

Outbound traffic rules define which outgoing network traffic is allowed from Endpoint computers.

The **Source** column in the outbound Rule Base describes the Endpoint devices to which the rules apply.

This outbound rule is configured by default:

No.	Name	Destination	Service	Action	Track	Comment
1	Allow any outbound	Any	Any	Allow	None	

Parts of Rules

As opposed to SmartEndpoint GUI, Harmony Endpoint has a unified Rule Base, which enables the user to view the entire Rule Base at a glance - both inbound and outbound. Both are sections of the same Rule Base.

These are the parts of the Firewall inbound/outbound rules:

Column	Description
#	Rule priority number.
Rule name	Name of the Firewall rule.
Source	Source location of the network traffic. For an outbound rule, the source is always set to the local computer/user/group.
Destination	Destination location of the network traffic. For an inbound rule, the destination is always set to the local computer/user/group.
Service	Network protocol or service used by the traffic.
Action	The action that is done on the traffic that matches the rule - **Allow** or **Block**.
Track	The tracking and logging action that is done when traffic matches the rule: ■ **Log** - Records the rule enforcement in the Endpoint Security Client Log Viewer. ■ **Alert** - Shows a message on the endpoint computer and records the rule enforcement in the Endpoint Security Client Log Viewer. ■ **None** - Logs and Alert messages are not created.

Editing a Rule

1. From the left navigation panel, click **Policy** > **Access**.
2. Click the rule to select it.

   When you edit a rule, a purple indication is added next to it (on the left of the rule).
3. In the right pane, in the section **Capabilities & Exclusions**, click the **Firewall** tab.
4. Click the **Edit Inbound/Outbound Rulebase** button.
5. Make the required changes.

   To add a new rule, do one of these:

- From the top toolbar, the applicable option (**New Above** or **New Below**)
- Right-click the current rule and select the applicable option (**New Above** or **New Below**)

6. Click **OK** in the bottom right corner.
7. Click **Save** in the bottom right corner.

   You can click **Cancel** to revert the changes.
8. Above the rule base, click **Install Policy**.

Deleting a Rule

1. Click the rule to select it.
2. From the top toolbar, click the garbage can icon ("**Delete rule**").

   If you are inside the **Edit Inbound/Outbound Rulebase** view, then a red indication is added next to it (on the left of the rule).
3. If you are inside the **Edit Inbound/Outbound Rulebase** view, then click **OK** in the bottom right corner.
4. If your are in the Firewall policy view, click **Delete** to confirm.
5. Click **Save** in the bottom right corner.
6. Above the rule base, click **Install Policy**.

Configuring Security Zones

Security Zones let you create a strong Firewall policy that controls the traffic between parts of the network.

A Security Zone object represents a part of the network (for example, the internal network or the external network).

There are two types of Security Zones:

- **Trusted Zone** - The Trusted Zone contains network objects that are trusted. Configure the Trusted Zone to include only those network objects with which your programs must interact. You can add and remove network objects from a Trusted Zone. A device can only have one Trusted Zone. This means that if the Firewall policy has more than one rule, and more than one Trusted Zone applies to a device, only the last Trusted Zone is enforced.

  These two network elements are defined as Trusted Zones by default:

- **All_Internet** - This object represents all legal IP addresses.
- **LocalMachine_Loopback** - Endpoint device's loopback address: 127.0.0.1. The Endpoint device must always have access to its own loopback address. Endpoint users must not run software that changes or hides the local loopback address. For example, personal proxies that enable anonymous internet surfing.

- **Internet Zone** - All objects that are not in the Trusted Zone are automatically in the Internet Zone.

Objects in the Trusted Zone:

These object types can be defined as Trusted Zones:

- Hosts
- Networks
- Network Groups
- Domains
- Address Ranges

To configure a Trusted Zone:

1. In the **Access** policy view, go to the right pane - **Firewall Rule Settings**, and click **Manage Trusted Zone**.
2. Click the **+** icon to see the list of objects you can define as a Trusted Zone.

   Note - To add objects to the list , go to the **Access** view > **Manage** > **Manage Firewall Objects**, and click **Create**.

3. Select the required object.
4. Click **OK**.

Configuring Firewall Rule Advanced Settings

To configure the advanced settings for a Firewall rule:

1. From the left navigation panel, click **Policy** > **Access**.
2. Click the rule to select it.
3. In the right pane, in the section **Capabilities & Exclusions**, click the **Firewall** tab.
4. In the **Advanced Settings** section, select the applicable options:

- **Allow wireless connections when connected to the LAN** - This protects your network from threats that can come from wireless networks.

  If you select this checkbox, users can connect to wireless networks while they are connected to the LAN.

  If you clear this checkbox, users cannot connect to wireless networks while they are connected to the LAN.

- **Allow hotspot registration** - Controls whether users can connect to your network from hotspots in public places, such as hotels or airports.

  If you select this checkbox, the Firewall is bypassed to let users connect to your network from a hotspot.

  If you clear this checkbox, users are not able to connect to your network from a hotspot.

- **Block IPv6 network traffic** - Controls whether to block IPv6 traffic to endpoint devices. Clear this checkbox to allow IPv6 traffic to endpoint devices.

- From the **When using Remote Access, enforce Firewall policy from** menu, select the applicable option:

  - **Above Endpoint Firewall policy** (this is the default)
  - **Remote Access Desktop Security Policy**

    If your environment had Endpoint Security VPN and then moved to the complete Endpoint Security solution, select this option to continue using the Desktop Policy configured in the legacy SmartDashboard.

    To learn how to configure a Desktop Policy, see the *Remote Access Clients for Windows Administration Guide*.

5. Click **Save** in the bottom right corner.

Note - For more information about Firewall, see sk164253.

Application Control

The Application Control component of Endpoint Security restricts network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes. The administrator can also configure that an application is terminated when it tries to access the network, or as soon as the application starts.

This is the workflow for configuring Application Control:

1. Set up a Windows device with the typical applications used on protected Endpoint computers in your organization. This is your reference device. If you have several different standard images, set up a reference device for each. See *"Creating the List of Applications on the Reference Device" below*.
2. Generate the list of applications on the computer by running the Appscan tool. This generates an XML file that contains the details of all the applications on the computer. See *"Creating the List of Applications on the Reference Device" below*.
3. Upload the Appscan XML file to the Endpoint Security Management Server. See *"Uploading the Appscan XML File to the Endpoint Security Management Server" on page 138*.
4. Configure the action for each application in the Application Control policy. You can configure which applications are allowed, blocked, or terminated. See *"Configuring Application Permissions in the Application Control Policy" on page 139*.
5. Install policy.

Creating the List of Applications on the Reference Device

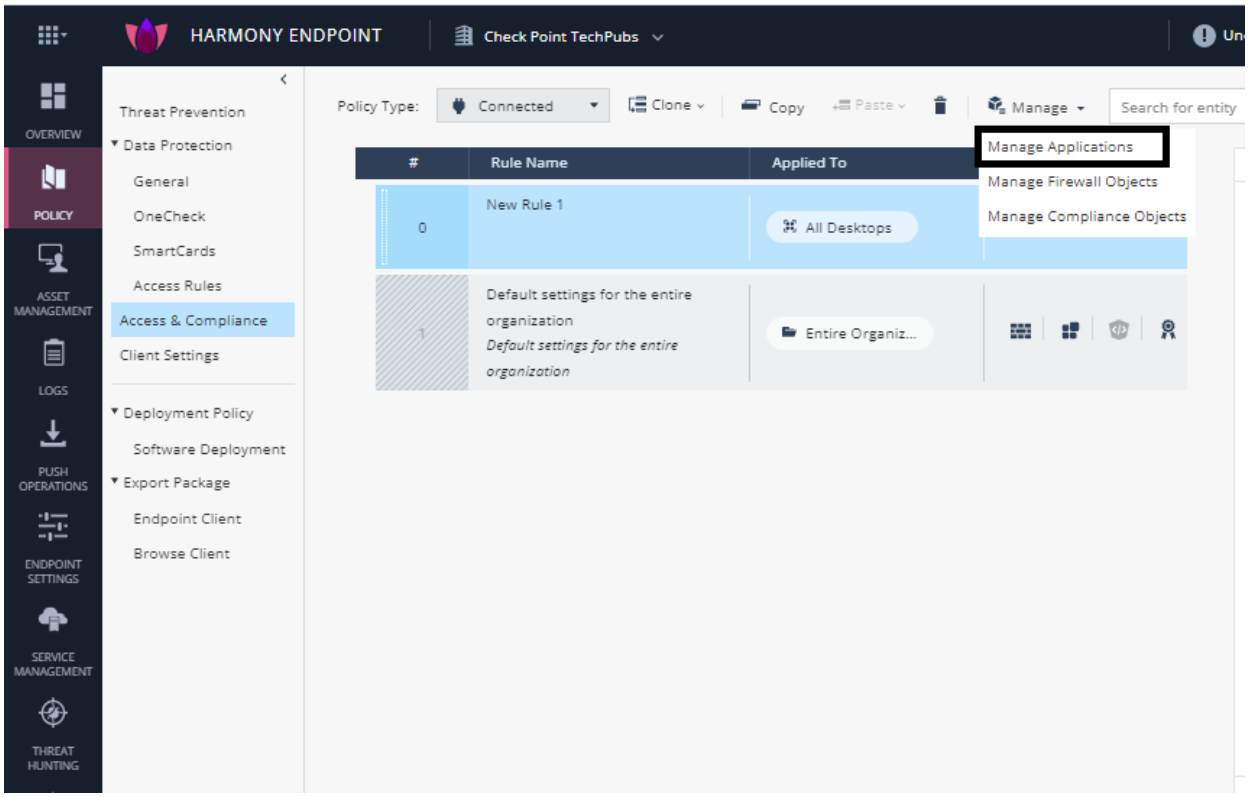
You need to generate a list of the applications on your reference device. This is a Windows device with a tightly-controlled disk image that contains the typical applications used on protected Endpoint devices in your organization. If you have several different standard images, set up a reference device for each.

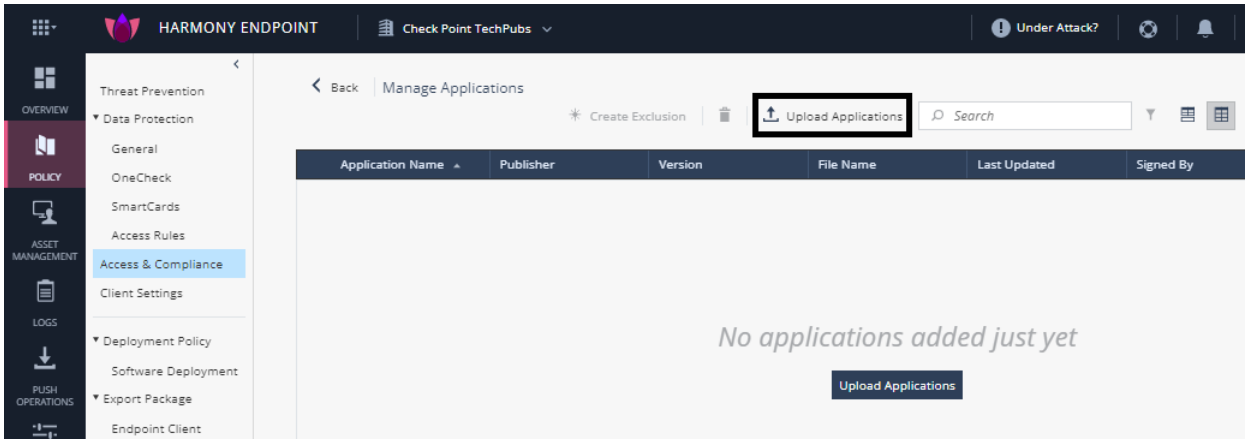
Important - The reference device must be free of malware.

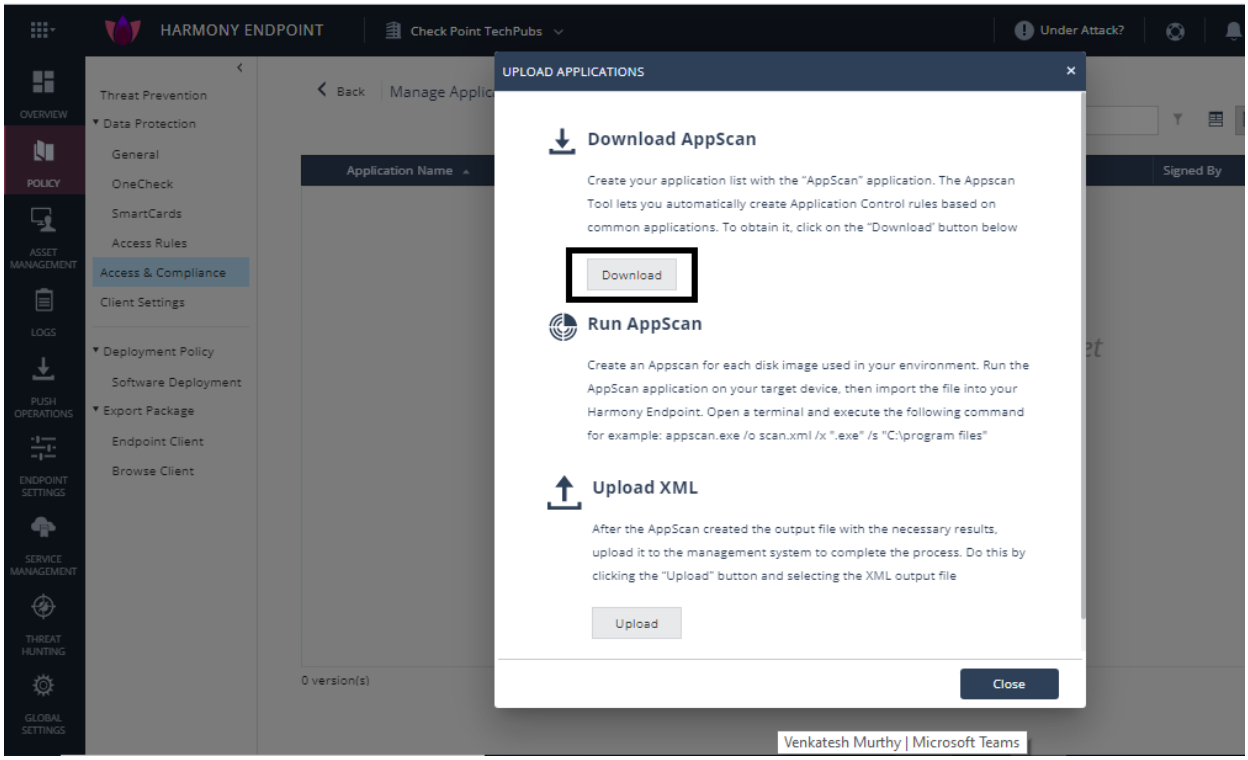
To generate the list of applications, run the `Appscan` command on the reference device. This generates an XML file that contains the details of all the applications and operating system files on the device. In the XML file, each application, and each application version, is uniquely identified by a checksum. A checksum is a unique identifier for programs that cannot be forged. This prevents malicious programs from masquerading as other, innocuous programs.

To collect a list of applications on the reference device:

1. Go to **Policy** > **Access & Compliance** > **Manage** > **Manage Applications** > **Upload Applications** > **Download Appscan**, and click **Download**.







2. Run the Appscan application on your target device with the applicable parameters. See *"Appscan Command Syntax" below*.

   This creates an Appscan XML file for each disk image used in your environment. When the scan is complete, an output file is created in the specified directory. The default file name is `scanfile.xml`

Appscan Command Syntax

Description

Scans the host device and creates an XML file that contains a list of executable programs and their checksums.

Syntax

```
Appscan [/o <filename> /s <target directory> /x <extension strung
/e /a /p /verbose /warnings /?
```

Parameters

Parameter	Description
`/o`	Sends output to the specified file name. If no file name is specified, `Appscan` uses the default file name (`scanfile.xml`) in the current folder.

Parameter	Description
`file name`	Output file name and path.
`/s <target directory>`	Specifies the directory, including all subdirectories, to scan. ■ You must enclose the directory/path string in double quotes. ■ If no directory is specified, the scan runs in the current directory only.
`/x <extension string>`	Specifies the file extension(s) to include in the scan. ■ The extension string can include many extensions, each separated by a semi-colon. ■ You must put a period before each file extension. ■ You must enclose full extension string in double quotes. ■ You must specify a target directory using the /s switch. ■ If you do not use the `/x` parameter only `.exe` executable files are included in the scan
`/e`	Include all executable files in the specified directory regardless of the extension. Do not use `/e` together with `/x`.
`/a`	Includes additional file properties for each executable.
`/p`	Shows progress messages during the scan.
`/verbose`	Shows progress and error messages during the scan.
`/warnings`	Shows warning messages during the scan.

`/?`
or
`/help`
	Shows the command syntax and help text.

Examples

- `appscan /o scan1.xml`

  This scan, by default, includes .exe files in the current directory and is saved as `scan1.xml`.

- `appscan /o scan2.xml /x ".exe;.dll" /s "C:\"`

  This scan includes all .exe and .dll files on drive C and is saved as `scan2.xml`.

- `appscan /o scan3.xml /x ".dll" /s c:\program files`

This scan includes all .dll files in `c:\program files` and all its subdirectories. It is saved as `scan3.xml`.

- `appscan /s "C:\program files" /e`

  This scan includes all executable files in `c:\program files` and all its subdirectories. It is saved as the default file name `scanfile.xml`.

Uploading the Appscan XML File to the Endpoint Security Management Server

After you generate the Appscan XML file, upload it to the Endpoint Security Management Server.

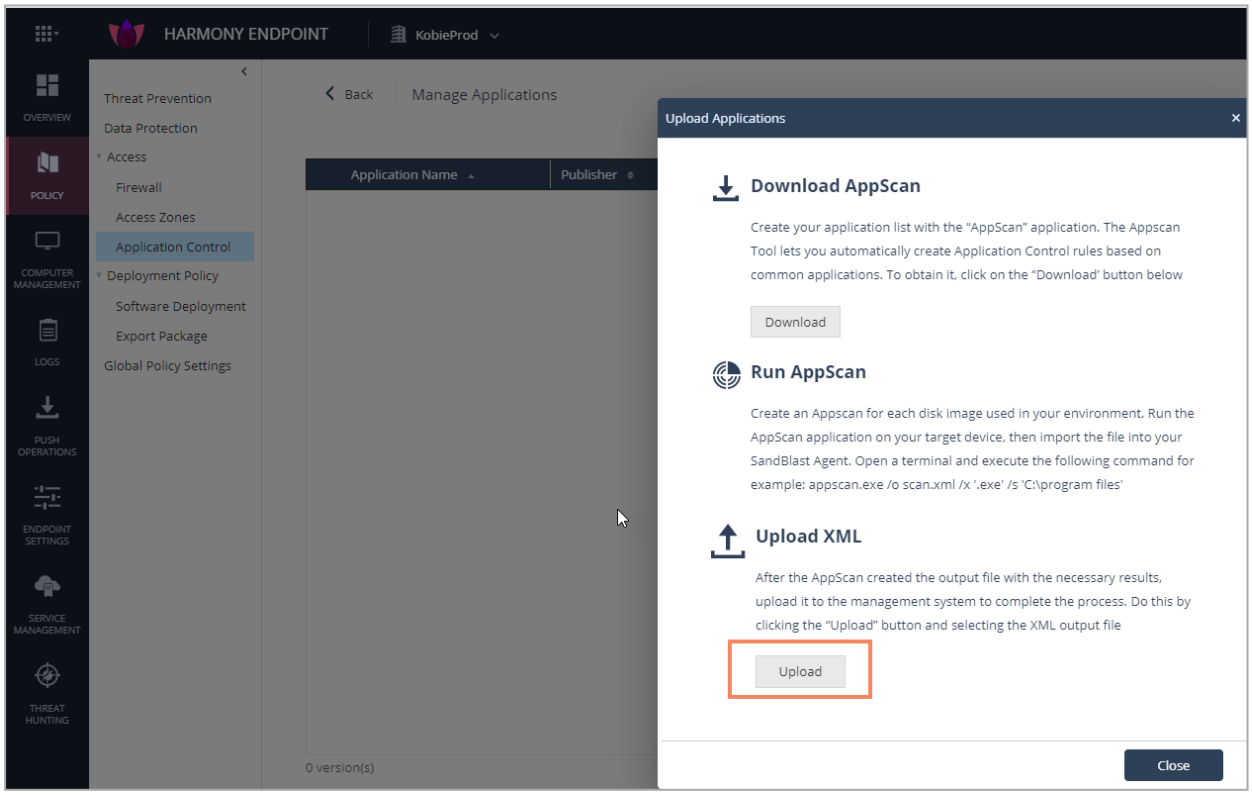
Note - Before you upload the Appscan XML file, remove all special characters, such as trademarks or copyright symbols, from the Appscan XML .

To upload the Appscan XML file:

1. In the **Policy** view, go to **Access** > **Application Control**> **Manage** > **Manage applications** > **Upload Applications**.

   The **Upload Applications** window opens.

2. In the **Upload XML** section, click **Upload**.



3. Search for the Appscan XML file and click **Open**.

Configuring Application Permissions in the Application Control Policy

Applications that were uploaded with the Appscan XML file are allowed by default. You cannot change the default action for the uploaded applications.

After the applications are uploaded, you can review the actions for each application In the Application Control policy.

For applications and application versions that you are know are secure, change the permission setting to **Allow** .

If you know the applications or application versions are not secure, change the permission setting to **Block**.

You can also configure that blocked applications will be *terminated* when they are started, or when they try to establish a network connection.

To review the policy settings for applications and application versions:

1. In the **Policy** view, go to **Access** > **Application Control** > **Application Management** > **Edit Application Control Policy**.
2. The **Action** column shows the permission for each application. Left-click the **Action** column to select the permission.

Permission	Explanation
Allow	The application is allowed.
Block	The application is blocked.
Terminate	The application is terminated when it tries to access the network or immediately when it runs.

3. The **Version** column shows the details for each version of the application, including a unique hash value that identifies the signer of the application version. You can block or allow specific versions of the same program. Each version has a unique **Version** number, **Hash**, and **Created On** date.

To configure termination settings:

1. In the **Policy** view, go to **Access** > **Application Control** > **Application Management**.
2. Select one of these options:
   - **Terminate on execution** - Selected by default. Makes sure that all terminated applications terminate immediately when they run.

- **Terminate on connection** - Terminate an application when the application tries to access the network

Application Control in Backward Compatibility Mode

Default Action for Unidentified Applications

Changing the default action for unidentified applications is only supported in backward compatibility mode.

To enable backward compatibility mode:

1. Go to **Endpoint Settings** > **Policy Operation Mode**.
2. Go to the required policy and select **Mixed mode**.

To change the default action for uploaded applications:

1. In the **Policy** view, go to **Access** > **Application Control** > **Application Management** > **Default action**.
2. Select the required default action.

Configuring the Application Control Policy

In addition to Allow, Block and Terminate, there are two more actions that you can configure in backward compatibility mode:

Unidentified (Allow) - The application is allowed because the default setting for applications that are imported from the Appscan XML is
Allow, and the administrator did not change this action.

Unidentified (Block) - The application is blocked because the default setting for applications that are imported from the Appscan XML is **Block**, and the administrator did not change this action.

Disabling or Enabling Windows Subsystem for Linux (WSL)

Windows Subsystem for Linux (WSL) is the scripting language in Windows 10 and higher. It makes it possible to run Linux binary executables under Windows. WSL has the potential for compromising security.

To enable or disable Windows Subsystem for Linux (WSL) on Endpoint Security client computers:

1. In the **Policy** view, go to **Access** > **Application Control** > **Windows Sub-systms for Linux (WSL) Traffic**
2. Select **Allow Windows Sub-systms for Linux (WSL) Traffic** or leave this option cleared.

Developer Protection

Developer Protection prevents developers leaking sensitive information such as RSA keys, passwords, and access tokens through the Git version control system. It also detects and warn the developer when using packages with known vulnerabilities.

Developer Protection intercepts `git commit` commands issued by the developer, and scans all modified files in a Git repository. It prevents the uploading of private information in plain text and vulnerable dependencies from Endpoint Security client computers to public locations.

Developer protection is supported on Endpoint Security Client release E84.60 and higher.

To configure Developer protection:

1. Access the Harmony Endpoint Administrator Portal.
2. Click **Policy** > **Access & Compliance**.
3. Select the policy and in the **Capabilities & Exclusions** pane, click **Developer Protection**.
4. Select the **Developer Protection** mode:

Mode	Description
Off	Developer Protection is disabled. By default, this option is selected.
Detect	■ Information leakage is detected and a log message is generated, but the Commit is allowed. ■ The administrator can examine the audit log *Detect* messages of the Application Control component. ■ The developer sees a notification on the client computer.
Prevent	■ Information leakage is detected, a log message is generated, and the Commit is blocked. ■ The administrator can examine the audit log *Prevent* messages of the Application Control component. ■ The developer sees a warning notification on the client computer. The developer can decide to override the notification and allow the traffic (with or without giving a justification). The notification message suggests how to fix the problem. For example, by adding a file to `.gitignore`, or updating the version in `package.json`

5. Click **Save**.
6. Install the policy.

Exclusions to Developer Protection

You can define exclusion to developer protection based on the SHA256 hash of the files.

To define an exclusion to **Developer Protection**:

1. Access the Harmony Endpoint Administrator Portal.
2. Click **Policy** > **Access & Compliance**.
3. Select the policy and in the **Capabilities & Exclusions** pane, click **Developer Protection**.
4. Click **Edit Exclusions**.
5. Click **Add**.

   The **New Exclusion** window appears.
6. In the **Exclusion** drop-down, select **Developer Protection**.
7. In the **Method** drop-down, select **SHA256 Hash**.
8. In the **Value** field, enter the SHA256 hash of the file.
9. (Optional) in the Comment field, enter a description.
10. (Optional) To copy the exclusion to all existing **Developer Protection** rules, select **Copy to all rules**.
11. Click **OK**.
12. Click **Save & Install** to install the policy.

Compliance

The Compliance component of Endpoint Security makes sure that endpoint computers comply with security rules that you define for your organization. Computers that do not comply show as non-compliant and you can apply restrictive policies to them.

The Compliance component makes sure that:

- All assigned components are installed and running on the endpoint computer.
- Anti-Malware is running and that the engine and signature databases are up to date.
- Required operating system service packs and Windows Server updates are installed on the endpoint computer through Windows Servers Update Services.

  Note - This is not supported through **Windows Settings** > **Update & Security** on your endpoint computer.
- Only authorized programs are installed and running on the endpoint computer.
- Required registry keys and values are present.

  Note - For macOS limitations, see sk110975.

If an object (for example an OU or user) in the organizational tree violates its assigned policy, its compliance state changes, and this affects the behavior of the endpoint computer:

- The compliant state is changed to non-compliant.
- The event is logged, and you can monitor the status of the computer and its users.
- Users receive warnings or messages that explain the problem and give a solution.
- Policy rules for **restricted** computers apply. See *"Connected, Disconnected and Restricted Rules" on page 170*.

Planning for Compliance Rules

Before you define and assign compliance rules, do these planning steps:

1. Identify the applications, files, registry keys, and process names that are required or not permitted on endpoint computers.
2. Collect all information and Remediation files necessary for user compliance. Use this information when you create Remediation objects to use in compliance rules.

   Compliance rules can prevent users from accessing required network resources when they are not compliant. Think about how to make it easy for users to become compliant.
3. Make sure that the Firewall rules gives access to Remediation resources. For example, sites from which service packs or Anti-virus updates can be downloaded.

   Note - In Windows 7, make sure the **Interactive Service Detection** service is running. This is necessary for Remediation files (running with system credentials) that must interact with the user.
4. Define rule alerts and login policies to enforce the rules after deployment.

Configuring Compliance Policy Rules

Ensuring Alignment with the Deployed Profile

This action makes sure that all installed components are running and defines what happens if they are not running. The action options are:

Action	Description
Inform if assigned Software Blades are not running	Send a warning message if one or more Endpoint Security components are not running.
Restrict if assigned Software Blade are not running	Restrict network access if one or more Endpoint Security components are not running.
Monitor if assigned Software Blades are not running	Create log entries if one or more Endpoint Security components are not running. No messages are sent.
Do not check if assigned Software Blades are not running	No check is made whether Endpoint Security components are running.

Remote Access Compliance Status

Remote Access Compliance Status selects the procedure used to enforce the **upon verification failure** from **Policy** > **Access & Compliance > Remote Access Compliance Status**.

The options available are:

- **Endpoint Security Compliance** - Uses the Endpoint Security policy to control access to organizational resources.
- **VPN SCV Compliance** - Uses SCV (Security Configuration verification) settings from the Security Gateway to control access to organization resources. SCV checks, which are defined in the **Local.scv** policy, always run on the client. This option is described in the "*Secure Configuration Verification (SCV)*" section of the *Remote Access VPN Client for Windows Administration Guide*.

  Note - Endpoint Security clients on macOS always get their compliance status from Endpoint SecurityCompliance, even if **VPN Client verification process will use VPN SCV Compliance** is selected.

Compliance Action Rules

Many of the Compliance Policy actions contain **Action Rules** that include these components:

- **Check Objects (Checks)** - Check objects define the actual file, process, value, or condition that the Compliance component looks for.
- One of these **Action** options - What happens when a computer violates the rule:

Action	Definition
Observe	Log endpoint activity without further action. Users do not know that they are non-compliant. Non-compliant endpoints show in the **Observe** state in the **Reporting** tab.
Warn	Alerts the user about non-compliance and automatically does the specified Remediation steps. Send a log entry to the administrator.
Restrict	Alerts the user about non-compliance and automatically does the specified Remediation steps. Send a log entry to the administrator. Changes applicable policies to the restricted state after a pre-defined number of heartbeats (default =5). Before this happens, the user is in the *about to be restricted* state. On the monitoring tab, the user is shown as *pre-restricted*.

- One or more **Remediation** objects - A Remediation object runs a specified application or script to make the endpoint computer compliant. It can also send alert messages to users.

The Compliance component runs the rules. If it finds violations, it runs the steps for Remediation and does the Action in the rule.

Some Action Rules are included by default. You can add more rules for your environment.

Basic Workflow for defining additional compliance rules:

1. Click **Policy** > **Access & Compliance** > **Compliance** > **Compliance Rulebase**.
2. Click **New Above** or **New Below** to create new **Action Rules** as necessary:
   a. In the **Name** field, enter the Action rule name.
   b. Click **Check** to add Check objects to add to the Action *"Compliance Check Objects" on page 149*.
   c. Select an **Action** from the list.

d. Click the **Remediation** tab to add Remediation objects to the *"Compliance Remediation Objects" on page 153*. If the selected **Action** is **Observe**, the rule does not require a Remediation object.

e. Optional: In the **Comment** field, enter a comment for the action rule.

Do these steps again to create additional Action rules as necessary.

Compliance Check Objects

Each Compliance Action Rule contains a **Check** object that defines the actual file, process, value or condition that the Compliance component looks for.

To create a new or change an existing Check object:

1. In the **Checks** column or in the manage objects in your toolbar, click the relevant Check object.

   Note: To edit the existing check object, click the existing check object.

2. Click **New** to create a new Check object.
3. For **System/Application/File Checks**, fill in these fields.

Option	Description
Name	Unique name for this Check Object.
Comment	Optional: Free text description.
Operating System	Select the operating system that this Check object is enforced on.
Registry value name	Enter the registry key. Enabled only if the **Modify and check registry** checkbox is selected. To detect Log4j vulnerability, in the **Registry value name** field enter: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint Security\Compliance\Log4jScan` and in the **Registry value** field, enter 1. Applies only to Windows.
Registry value	Enter the registry value to match. Enabled only if the **Modify and check registry** checkbox is selected. Applies only to Windows.

Option	Description
Modify registry key and value	Select an action: ◦ Add ◦ Replace ◦ Update ◦ Remove Enabled only if the **Modify and check registry** checkbox is selected. Applies only to Windows.
Reg type	Select a registry type: ◦ REG_SZ ◦ REG_DWORD Enabled only if the **Modify and check registry** checkbox is selected. Applies only to Windows.
Check registry key and value	Select one of these options to enable the registry check or clear to disable it: **Registry key and value exist** - Find the registry key and value. If the registry key exists, the endpoint computer is compliant for the required file. **Registry key and value do not exist** - Make sure the registry key and value do not exist. If the key does not exist, the endpoint computer is compliant for an application that is prohibited.
Check File	Select one of these options to check if an application is running or if a file exists: **File is running at all times** - For example, make sure that client is always running. **File exists** - For example, make sure that the user browsing history is always kept. **File is not running** - For example, make sure that DivX is not used. **File does not exist** - For example, make sure that a faulty DLL file is removed.
File name	Enter the name of the file or executable to look for. To see if this file is running or not, you must enter the full name of the executable, including the extension (either .exe or .bat).

Option	Description
File path	Enter the path without the file name. Select the **Use environment variables of logged in user** option to include paths defined in the system and user variables. Do not add the "\" character at the end of the path.macOS uses "/" and file PATH is case sensitive. For more information on macOS limitations, see sk110975.
Check files Properties	Additional options to check for an existing or non-existing file.
Match the file version	Make sure that a specific version or range of versions of the file or application complies with the file check.
Match MD5 checksum	Find the file by the MD5 Checksum. Click **Calculate** to compare the checksum on the endpoint with the checksum on the server.
File is not older than	Select this option and enter the maximum age, in days, of the target file. If the age is greater than the maximum age, the computer is considered to be compliant. This parameter can help detect recently installed, malicious files that are disguised as legitimate files.
Check Domain	Enable Check domain in order to specify the domain. Select a domain: ◦ Any Domain ◦ Specific Domain Applies only to macOS.
Domain Name	Enter the domain name if the specific domain is selected. Applies only to macOS.

4. **System Check** can be grouped
   - **Require at least one check to succeed** – At least one of the Checks must match in order for Check to succeed.
   - **Require all checks to succeed** - All Checks must match in order for Check to succeed.

For **Group Check** window, fill in these fields.

Option	Description
Name	Unique name for this Check Object.
Comment	Optional: Free text description.

Option	Description
	Select the action ◦ Require at east one check to succeed ◦ Require all checks to succeed
	Name of the check object. Click + to add check objects to the table

Compliance Remediation Objects

Each Compliance Action Rule contains one or more **Remediation** objects. A Remediation object runs a specified application or script to make the endpoint computer compliant. It can also send alert messages to users.

After a **Remediation object** is created, you can use the same object in many Action rules.

To create a new or change an existing Remediation object:

1. Click **Manage Object** of Compliance Rulebase, click * and select **Remediation**.
2. In the **Remediation Properties** window, fill in these fields:

Option	Description
Name	Unique name for the Remediation.
Comment	Optional: Free text description.
Operations	
Run Custom File	Run the specified program or script when an endpoint computer is not compliant.
Download Path	■ Enter the temporary directory on the local computer to download the program or script to. This path must be a full path that includes the actual file and extension (*.bat or *.exe). ■ This parameter is required. ■ The endpoint client first tries to access the file from the specified path. If the client fails, it downloads the file from the URL to the temporary directory and runs it from there. ■ To run multiple files, use one of the popular compression programs such as *WinRAR* to produce a self-extracting executable that contains a number of .exe or .bat files.

Option	Description

URL	■ Enter the URL of an HTTP or file share server where the file is located.
	Example:
	• Using file share:
	`file://\\<IP ADDRESS>/...../<file name>`
	• Using local file:
	`file://C:\path\to\file.exe`
	■ Enter the full path that includes the actual file with one of the supported extensions (*.bat or *.exe).
	■ This field can be left empty.
	■ Make sure the file share is not protected by a username or password.

Parameters	If the executable specified in the URL runs an installation process, make sure that the executable holds a parameter that specifies the directory where the program should be installed. If the executable does not hold such a parameter, enter one here.
MD5 Checksum	Click **Calculate** to generate a MD5 Checksum, a compact digital fingerprint for the installed application or the Remediation files.
Run as System	Apply system rights for running the executable file. Not all processes can run with user rights. System rights may be required to repair registry problems and uninstall certain programs.
Run as User	Apply user rights and local environment variables for running the executable file.
Messages	
Automatically execute operation without user notification	Run the executable file without displaying a message on the endpoint computer.
Execute operation only after user notification	Run the executable file only after a user message opens and the user approves the Remediation action. This occurs when **Warn** or **Restrict** is the selected action on a compliance check.

Option	Description
Use same message for both Non-Compliant and Restricted messages	Select that the same text be used for both messages. A Non-Compliant message tells the user that the computer is not complaint and shows details of how to become compliant. A Restricted message tells the user that the computer is not compliant, shows details of how to achieve compliance, and restricts computer use until compliance is achieved.
Message Box	Displays selected non-compliant and restricted messages. The message box is available only by selecting the Execute only after user notification setting. Click **Add**, **Remove**, or **Edit** to add a message, and remove or revise a selected message. **Note**: User cannot prevent the Remediation application or file from running.

Service Packs for Compliance

The **Service Packs Compliance** check makes sure that computers have the most recent operating system service packs and updates installed. The default settings show in the **Latest Service Packs Installed** Action Rules.

For more information, see *"Compliance Action Rules" on page 147*.

Anti-Virus for Compliance

The Anti-Virus check makes sure that computers have an anti-malware program installed and updated. The default settings show in the **Anti-Virus Compliance** Action Rules.

For more information, see *"Compliance Action Rules" on page 147*.

Ensuring that Windows Server Updates Are Installed

Windows Server Update Services (WSUS) allows administrators to deploy the latest Microsoft product updates.The WSUS compliance check ensures that Windows update are installed on the Endpoint Security client computer. You can restrict network access of the client computer if Windows updates have not been installed within a specified number of days. Alternatively, you can warn the user by means of a pop-up message without restricting access, or log the non-compliance event without restricting or informing the user

To configure the WSUS compliance check:

Under **Windows Server Update Services** action, select a preset action. The action is applied if Windows updates have not been installed on the Endpoint Security client computer for a specified number of days (default is 90 days):

Preset Action	Meaning
Restrict if Windows Server Updates are not installed	Restrict the network access of the user.
Observe Windows Server Update Services	Create a log, and show a warning message to the user.
Monitor Windows Server Update Services	Create a log. The user is not notified.
Do not check Windows Server Update Services	No compliance check. This is the default.

1. **Optional**: The compliance check makes sure that the Windows updates have been installed within a specified number of days (default is 90 days).

   To change the number of days,

   a. Click **Compliance** and under **Windows Server Update Services** , select the **Enable Windows software update services check** checkbox.

   b. Change the number of days in **Windows updates must be installed within**.

Monitoring Compliance States

Monitor the compliance state of computers in your environment from:

1. Click **Asset Management** > **Computers**.
2. Select the **Compliance** view in the Columns profile selector in your toolbar.

These compliance states are used in the Security Overview and Compliance reports:

- **Compliant** - The computer meets all compliance requirements.
- **About to be restricted** - The computer is not compliant and will be restricted if steps are not done to make it compliant. See *"About to be Restricted" State" below*.
- **Restricted** - The computer is not compliant and has restricted access to network resources.
- **N/A** – Compliance policy is not applicable for the computer.
- **Warn** - The computer is not compliant but the user can continue to access network resources. Do the steps necessary to make the computer compliant.
- **Not Running** – Compliance policy is not running on the computer.
- **Unknown** – Compliance status is unknown.
- **Not Installed** – Compliance policy is not installed on the computer.

The endpoint computer Compliance state is updated at each heartbeat. The heartbeat interval also controls the time that an endpoint client is in the **About to be restricted** state before it is restricted.

It is possible to create restricted policies that will automatically be enforced once the endpoint client enters a restricted state

"About to be Restricted" State

The **About to be restricted** state sends users **one last warning** and gives an opportunity to immediately correct compliance issues before an endpoint computer is restricted.

The formula for converting the specified time period to minutes is:
`<number of heartbeats > * <heartbeat interval (in seconds)> * 60.`

Configuring Client Settings

Client Settings define:

- General user interface settings
- If users can postpone installations and for how long.
- The client uninstall password
- When log files are uploaded to the server
- Specified Network Protection settings

To configure these settings go to the **Policy** view > **Client Settings.**

User Interface

Default Client User Interface

You can select the default Harmony Endpoint Security Client interface settings or edit them to customize the Endpoint Security client interface on user computers.

You can change these settings:

- **Display client icon** - When selected, the client icon shows in the windows notification area when the Endpoint Security client is installed.
- **New client User Interface** - Select an interface for the client.
  - **Default** - Applies the default interface specified in the client. Default is the new UI.
  - **On** - Applies the new interface.
  - **Off** - Applies the legacy interface.
- **Client language** - Select the default language for client. **OS Locale** indicates the default OS language.

  Note - If the default language is not supported by the client, then system uses the English language for the client.
- **Notification level** - You can decide which type of messages can be shown to the user, and which must not be visible. The administrator can select one of three options:
  - **Critical only** - Do not show any messages unless critical (e.g. system boot warning) or user interface messages (yes/no questions).
  - **When-affecting user experience (recommended)** - Only show messages related to operation flows affecting user activity, or requiring user interaction (e.g. "Malware was detected and removed").

- **All** - Show all messages.

Note: This change applies to the Endpoint Security Client only. Events are still being logged on the server, and the administrator can still see everything on the management interface.

Pre-Boot Images

For each of these graphics, you can select to upload a new image or **Revert to Default** image:

Item	Description	Size of Image
Pre-boot Background Image	Image on Pre-boot screen behind the smaller logon window	800 x 600 pixels
Pre-boot Background Image high resolution	Pre-boot background image high resolution	3840×2160
Pre-boot Screen Saver	Image that shows when the system is idle	260 x 128 pixels
Pre-boot Banner Image	The banner image on the smaller logon window	447 x 98 pixels
Windows Background Image	Image in the background of the Windows logon window if OneCheck Logon is enabled	256 KB or smaller

Windows Background Image

Description	Size of Image
Image in the background of the Windows logon window if OneCheck Logon is enabled	256 KB or smaller

Customized Client Image

Description	Size of Image
Icon in the top-right of a Client Notification (UserCheck)	134 x 46 pixels

Customized Browser Block Pages

Browser extension uses block pages to warn the end users about security incidents and prompts for additional permissions. There are four events which trigger a blocking page:

1. Accessing a site that is blocked by URL Filtering policy – The block page blocks access to the site and warns the end user that attempted to enter the site that it is blocked by the policy.
2. Providing credentials in a phishing site – The block page warns the end user that it is a phishing site and the user is therefore blocked from providing credentials there.
3. Using corporate password in a non-corporate domain - End users are warned that use of corporate password in a non-corporate domain is prohibited, and that his/her corporate password was just exposed.
4. Accessing a local HTML file without the permission by the browser extension.

The blocking pages above are customizable. The following can be changed per each of them:

1. Company logo (replacing the Check Point logo).
2. Blocking page title.
3. Blocking page description.

The user may preview the change before saving the policy by pressing the preview button.

Note - The preview only works in the Chrome or Edge browsers, when the browser extension is installed.

Log Upload

The components upload logs to the Endpoint Policy Server.

These log upload options are available:

Option	Description
Enable Log Upload	Select to enable log upload (this is the default). Clear to disable log upload.
Log upload interval	Frequency in minutes between logged event uploads. The clients upload logs only if the number of logs is more than the **Minimum number of events before attempting an upload**. The default is 3 minutes.
Minimum number of events before attempting an upload	Upload logged events to the server only after the specified number of events occur. The default is 1.
Maximum number of events to upload	Maximum number of logged events to upload to the server. The default is 100.

Option	Description
Maximum age of event before upload	**Optional**: Upload only logged events that are older than the specified number of days. The default is 5 days.
Discard event if older than	**Optional**: Do not upload logged events if they are older than the specified number of days. The default is 90 days.

Installation and Upgrade Settings

The default installation and upgrade setting is that users can postpone the Endpoint Security Client installation or upgrade.

You can change these settings:

- **Default reminder interval** - Set the time, in minutes, after which users are reminded to install the client.
- **Force Installation and automatically restart after** - Set the time, in hours, after which the installation starts automatically.
- **Maximum delay in download of packages** - Set the maximum time, in hours, by which to postpone the download.

Agent Uninstall Password

You can allow a user to uninstall the Endpoint Security client on their remote Windows computer.

Agent Uninstall Password is the password you use to uninstall the client. The password protects the client from unauthorized removal. The password can only contain English letters in lower or upper case, and these special characters: 0-9 ~ = + - _ ( ) ' $ @ , .

The default uninstall password is "secret".

Best Practice - For security reasons, we strongly recommend that you change the default uninstall password.

Local Deployment Options

When you use Automatic Deployment, you can configure clients to use local storage to upgrade Endpoint Security clients. This lets administrators use Automatic Deployment, without the need for each Endpoint Security client to download a package from the Endpoint Security Management Server

This is only supported on Windows clients.

Note - If local deployment is enabled for a client, the administrator can still choose whether clients try to download packages from the Endpoint Security Management Server if packages are not found in local storage. This option is called: Enable Deployment from server when no MSI was found in local paths.

To enable Deployment with a locally stored package:

1. Upload each package to the Package Repository of the Endpoint Security Management Server.
2. Put the same packages in local storage location on client computers, for example: `C:\TEMP\EPS\32bit\EPS.msi`
3. Go to the **Policy** view > **Client Settings** > **Installation** > **Deployment from Local Paths and URLs**
4. Select **Allow to install software deployment packages from local folders and URLs**.
5. Optional: Select **Enable Deployment from Server when no MSI was found in local paths**. When selected, if no MSI file is in the local paths or URLs, the client checks the Endpoint Security Management Server for packages.
6. Click **Deployment Paths** and add the package or patch location.
7. Click **OK**.
8. Go to **Deployment Policy** > **Software Deployment**, and create or edit a deployment rule which includes the package version.
9. Click **Save**
10. Install Policy to deploy the rule to the clients.

Note - If the version of the Endpoint Security client in the Deployment rule and in the local file path is not the same, the client is not deployed. If the version on the server and in the local file path are not the same, an error shows.

Sharing Data with Check Point

Clients can share information about detected infections and bots with Check Point.

The information goes to ThreatCloud, a Check Point database of security intelligence that is dynamically updated using a worldwide network of threat sensors.

ThreatCloud helps to keep Check Point protection up-to-date with real-time information.

Note - Check Point does not share any private information with third parties.

To configure data ThreatCloud sharing:

1. Go to the **Policy** view > **Client Settings** > the **General** tab > **Sharing Data with Check Point**.
2. **Enable anonymized telemetry** - Select to enable sharing information with Check Point.

   Select or clear any of these options:

   - **Anonymized forensics reports** - Forensics reports include a lot of private identifiable information. This option lets customers anonymize this information.
   - **Files related to detection** - Select to allow Check Point learn more about the attacks through metadata.
   - **Memory dumps related to detections** - Select to allow sharing memory dumps from the RAM with Check Point.
3. Click **Save**.

Users Disabling Network Protection

You can let users disable network protection on their computers.

Note - Check Point does not share any private information with third parties.

Network Protection includes these components:

- Firewall
- Application Control

To configure the Network Protection Alerts :

1. Go to the **Policy**view > **Client Settings** > **General** > **Network Protection**.
2. In the **Network Protection** section, select or clear these options for each Firewall and Application Control:
   - **Allow Log** - To generate logs for events.
   - **Allow Alert** - To generate alerts for events. You must also select this to use **Alert** in the **Track** column of Firewall rules.

Connection Awareness

Connection Awareness - Connection awareness controls how an endpoint enforces its Connected or Disconnected policy. By default, the client checks connectivity to the Endpoint Management Server to determine its connectivity state. Alternatively, the administrator can configure the client's connection status by checking its connectivity to a different network component, for example, a web server or a router, through ICMP packets or HTTP/HTTPS/IPv4 requests. If the client can connect to the network component, then its connection status is Connected. Otherwise, its connection status is Disconnected.

To configure the connection awareness setting:

1. Go to the **Policy** > **Client Settings** > **General** > **Connection Awareness**.

   The Connection Awareness feature allows the administrator to choose between two options:

   a. Connected to management - The client's status is Connected if it is connected to the Endpoint Security Management Servers. This is the default mode.

   b. Connected to a list of specified targets - The client's status is Connected if it is connected to the specified target (network component) regardless of its connection to the Endpoint Security Management Servers.

      If you do not specify a disconnected policy for these addresses, the user is automatically considered connected.

2. Click **Save**.

Notes:

- The client triggers HTTP GET requests to the server for connected or disconnected status in intervals of 30 seconds.
- Connection Awareness is supported with Endpoint Security Client version E85.30 and higher for windows and E87.30 and higher for macOS.
- Some capabilities, such as Full Disk Encryption (FDE) remain active even if the client's status is disconnected. However, it cannot perform operations that require connection to the server, such as acquire users from the server or send recovery data to the server.

Super-Node

What is a Super Node?

A Super Node is a Windows device running a specially configured Endpoint Security Client that also consists of server-like and proxy-like capabilities, and which listens on port 4434 and port 3128 to proxy by default. Super Node is a light-weight proxy (based on NGNIX) that allows admins to reduce their bandwidth consumption and enable offline updates, where only the Super Node needs connectivity to the update servers.

Super Node Workflow

When a device is assigned as a super node and has the supported blades installed, it downloads signatures from the sources defined in the policy and stores a local copy. This local copy serves as the signature source for other Endpoint Security Clients.

When an Endpoint Security Client initiates an update, it follows this process:

1. The Endpoint Security client checks for the latest signatures from a randomly selected super node listed in the **Client Settings** > **General** policy.
2. If the update fails with the chosen super node, the Endpoint Security client attempts the update with another super node in the list.
3. If the update fails with all the super nodes listed in the General Client Settings policy, the Endpoint Security client will update directly from the sources specified in the policy.

Primary Advantages:

- Reduces site bandwidth usage.
- Reduces server workload.
- Reduces customer expense on server equipment, as there is no need for a local appliance.
- Improved scale.

Notes -

- Super Node is available in both Domain and Work group environments.
- If the Endpoint Security client configured as a super node is of a lower version than its connection clients, the super node will return a 404 error response when a connection client tries to download the policy signatures. In this case the connection client downloads the signatures from the fallback location.

Supported Features

Endpoint Security Client Version	Features Supported
E85.30 and higher	▪ Downloading the software upgrades for Windows installer (MSI) packages from the super nodes. ▪ Super node tries to cache the requested files in the local folder. **Note** - The files are cached based on the available free space in the super node device and the cache size configured.

Endpoint Security Client Version	Features Supported
E85.40 and higher	▪ Downloading the software upgrades for Dynamic (EXE) packages from super nodes. ▪ Downloading Behavioral-Guard & Static Analysis signature updates from super nodes.
E86.10 and higher	Downloading client policies and policy changes from super nodes.
E87.00 and higher	Harmony Endpoint Security Client for macOS can be configured to create a local mirror of the Anti-Malware signatures which can be used as a signature source for other Endpoint Security clients for macOS.
E88.70 and higher	Super node proxies are supported for offline environment.

Limitations

- By default, the cache max size is 4 GB and will automatically purge files after 7 days of inactivity. Files stored for a longer time without access are removed from cache.
- Super Node requires approximately 350 MB of additional space to operate properly.

To configure a Super Node:

For Management Servers supporting **Manage Super Nodes** capability:

1. Go to **Policy** > **Client Settings**.
2. From the toolbar, click **Manage Super Nodes**.

   The **Manage Super Nodes** page is displayed.
3. Click **+** and select the devices you want to define as Super Nodes and then click **Add**.

   Note - You can also use the search bar to search for a device or devices that you want to define as Super Nodes.

   Widgets are created for each entities selected as super nodes.
4. After selecting the devices, click **Save**.

   Note - Configuring a device as a Super Node does not require policy installation.

5. Go to **Client Settings** and select the required rule. In the **Capabilities & Exclusions** pane, click **General** and scroll-down to **Super Nodes** section.
6. Click **+** and add Super Nodes with all its specific devices to the relevant **Client Settings** rule.
7. Click **Save** and install the rule.

Note - Super Node settings are rule dependent. It means that Super Nodes defined in the **General** tab will be applied only to devices which are related to a specific rule.

Connected, Disconnected and Restricted Rules

Endpoint Security can enforce policy rules on computers and users based on their connection and compliance state.

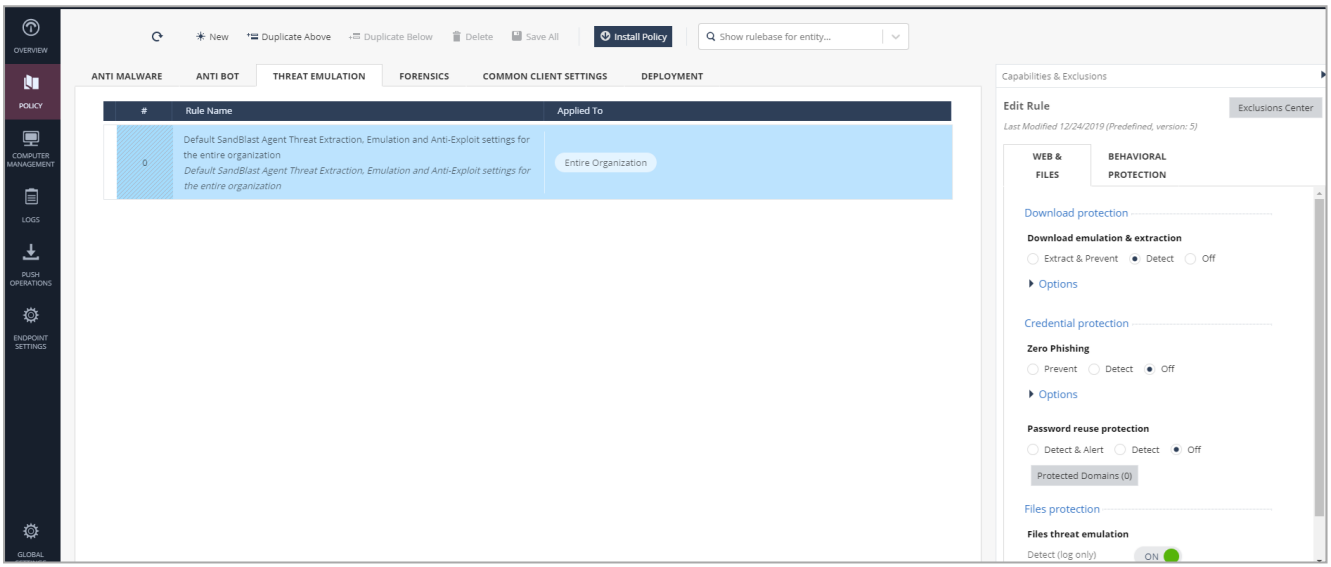
When you create a policy rule, you select the connection and compliance states for which the rule is enforced. You can define rules with these states:

- **Connected** state rule is enforced when a compliant endpoint computer has a connection to the Harmony Endpoint Security Management Server. This is the default rule for a component policy. It applies if there is no rule for the Disconnected or Restricted states of the component. All components have a Connected Rule.
- **Disconnected** state rule is enforced when an endpoint computer is not connected to the Harmony Endpoint Security Management Server. For example, you can enforce a more restrictive policy if users are working from home and are not protected by organizational resources. You can define a *Disconnected policy* for only some of the Endpoint Security components.
- **Restricted** state rule is enforced when an endpoint computer is not in compliance with the enterprise security requirements. In this state, you usually choose to prevent users from accessing some, if not all, network resources. You can define a *Restricted policy* for only some of the Endpoint Security components.

Component	Connected	Disconnected	Restricted
Full Disk Encryption	X		
Media Encryption & Port Protection	X	X	X
OneCheck	X		
Anti-Malware	X	X	
Anti-Ransomware, Behavioral Guard and Forensics	X		
Threat Exclusion, Emulation and Anti-Exploit	X	X	
Compliance	X	X	
URL Filtering & Anti-Bot	X	X	
Firewall	X	X	X
Access Zones	X	X	X
Application Control	X	X	X
Client Settings	X		

Backward Compatibility

You can manage Endpoint components through the Endpoint Web Management Console and SmartEndpoint concurrently. The Endpoint Web Management Console does not support all of the SmartEndpoint functionalities. Therefore, when you manage Endpoint components both through the Endpoint Web Management Console and SmartEndpoint, conflicts can arise. When you do an action in SmartEndpoint that is not supported by the Endpoint Web Management Console, the policy display view in the Endpoint Web Management Console changes to the policy display view in SmartEndpoint (backward compatible mode):



The display view changes back from the backward compatible mode to the regular Endpoint Web mode only when the policy enables it.

Policy Operation

The new policy operation mode allows greater flexibility to the user by proving him with a choice of capability rule applicability. While under the old policy calculation the rule type of each capability determined whether the capability can work on user or computer, under the new policy the user has the ability to define for himself which method he wants the capability to work in (except in cases where it only makes sense for the capability to apply to users or computers, but not both).

In this new operation mode, most capabilities are "mixed", which means they can function per users or computers, according to the user's choice. In each capability, the rules are ordered both by their assigned environment, from the specific down to the general, as well as by user/computer applicability: the first rule applies to the users, and if no match is found, the following rules apply to computers/devices as well.

To view the Policy Operations Mode page, click **Endpoint Settings** > **Policy Operations Mode**.

Old Policy Calculation Mode

Component	Rule Type
Full Disk Encryption	Computer only
Media Encryption & Port Protection	Computer (default) / User
Onecheck	User only
Anti-Malware	Computer (default) / User
Anti-Ransomware, Behavioral Guard & Forensics	Computer only
Anti-Bot & URL Filtering	Computer (default) / User
Threat Emulation, Threat Extraction & Anti-Exploit	Computer (default) / User
Compliance	Computer (default) / User
Firewall	Computer (default) / User
Access Zones	Computer (default) / User
Application Control	Computer (default) / User
Client Settings	Computer (default) / User

.

New Policy Calculation Mode

Family Type	Blade	Mixed Mode			Computer Mode	
		Mixed (User/Computer)	Computer Only	User Only	Computer	User
Threat Prevention	Anti-Malware	X	N/A	N/A	X	N/A
	Anti-Bot & URL Filtering	X	N/A	N/A	X	N/A
	Anti-Exploit	X	N/A	N/A	X	N/A
	Threat Emulation & Extraction	X	N/A	N/A	X	N/A
	Anti-Ransomware	N/A	X	N/A	X	N/A
	Behavioral Guard	N/A	X	N/A	X	N/A
	Forensics	N/A	X	N/A	X	N/A
Data Protection	Media Encryption & Port Protection	X	N/A	N/A	X	N/A
	Port Protection	X	N/A	N/A	X	N/A
	Full Disk Encryption	N/A	X	N/A	X	N/A
	OneCheck	N/A	N/A	X	N/A	X
Access & Compliance	Firewall	X	N/A	N/A	X	N/A
	Application Control & Developer protection	X	N/A	N/A	X	N/A
	Compliance	X	N/A	N/A	X	N/A

IOC Management

IoC stands for Indicators of Compromise. These indicators arrive from various sources, such as Internet, personal research and so on. Such indicators are not identified by default and you can block them manually.

For example, if a user receives an indication that a particular URL is malicious, the user can contact their System Administrator to block access to this URL. The System Administrator tags this URL as an Indication of Compromise IoC and the policy is enforced on all the endpoints through the Harmony Endpoint client or the browser extension.

Notes:

- This is supported with the Endpoint Security Client version E86.20 and higher.
- The browser extension that can enforce the IoC policy is supported with the Endpoint Security Client version E86.50 and higher for Windows and E86.80 and higher for macOS.
- Files with digital signature by trusted signer is not blocked using IoC.

To configure an IoC:

1. In Infinity Portal, go to **Policy** > **Threat Prevention**.
2. In the toolbar, select **Manage IoC**. No need to install policy.
3. In the table that appears, manually add new Indicators of Compromise by type:

IoC Type	Example
Domain	`checkpoint.com`
IP Address	`192.168.1.1`
URL	`checkpoint.com/test.htm`
MD5 Hash	`2eb040283b008eee17aa2988ece13152`
SHA1 Hash	`510ce67048d3e7ec864471831925f12e79b4d70f`

4. Hover over the icon next to **Type** to view the capabilities required for each type:
   - URL, Domain and IP require Anti-Bot and URL Filtering capabilities.
   - SHA1 and MD5 Hashes require Threat Extraction and Threat Emulation capabilities.
5. The user can also upload his own manually-created CSV list of indicators.

6. To verify, on the endpoint, access the IoC (for example, a URL). The system blocks the access to the IoC.

Performing Data Recovery

If the operating system does not start on a client device due to system failure, you can recover your data from the device.

Check Point Full Disk Encryption Recovery

If the operating system does not start on a client computer due to system failure, Check Point Full Disk Encryption offers these recovery options:

Full Recovery with Recovery Media

Client computers send recovery files to the Endpoint Security Management Server so that you can create recovery media if necessary. After the recovery, the files are restored as decrypted, as they were before the Full Disk Encryption installation, and the operating system can run without the Pre-boot.

Full recovery with recovery media decrypts the failed disk and recovers the data. This takes more time than the time taken when you use the Full Disk Encryption Drive Slaving Utility. It lets you access data quickly.

Recovery Media:

- Is a snapshot of a subset of the Full Disk Encryption database on the client.
- Contains only the data required to do the recovery.
- Updates if more volumes are encrypted or decrypted.
- Removes only encryption from the disk and boot protection.
- Does not remove Windows components.
- Restores the original boot procedure.

Users must authenticate to the recovery media with a username and password. These are the options for the credentials to use:

- Using SmartEndpoint - Users that are assigned to the computer and have the **Allow use of recovery media** permission can authenticate with their regular username and password. In SmartEndpoint, go to the **OneCheck User Settings** rule > **Advanced** > **Default** logon settings.
- When you create the recovery media, you can create a temporary user who can authenticate to it. A user who has the credentials can authenticate to that recovery media. Users do not require **Allow use of recovery media** permission to use the recovery media. SmartCard users must use this option for recovery.

To perform full recovery with recovery media:

1. In the Endpoint Web Management Platform, go to the **Computer Management** view > **Full Disk Encryption Actions** > **Recovery**> **Full Disk Encryption Recovery**.

   The **Full Disk Encryption Recovery** window opens.

2. Search for the computer which you want to decrypt.

   The **OS Name** and **OS version** of the computer are displayed.

3. **User List** - This list shows the users who have permission to use recovery media for the computer. There must be at least two users on the list to perform recovery.

   - If there are two users or more on the list, continue to the next step.
   - If there are less than two users on the list:

     a. Click the **+** sign to create a temporary users or temporary users who can use the recovery media.

     b. In the window that opens add a username and a password that the users will use to access the file.

4. Download the recovery file.

5. Create the recovery media:

Step	Instructions
1.	On the Endpoint Security client, go to folder: `C:\Program Files(x86)\CheckPoint\Endpoint Security\Full Disk Encryption\`
2	Double-click `UseRec.exe` to start the external recovery media tool.
3	Follow instructions in the tool to create the recovery media.

Note - During the decryption process, the client cannot run other programs

Full Disk Encryption Drive Slaving Utility

Use this to access specified files and folders on the failed, encrypted disk that is connected from a different "host" system.

The Drive Slaving Utility is hardware independent.

Full Disk Encryption Drive Slaving Utility replaces older versions of Full Disk Encryption drive slaving functionality, and supports all E80.x versions. You can use the Full Disk Encryption Drive Slaving Utility instead of disk recovery.

Note:

- On an E80.x client computer with 2 hard disk drives, the Full Disk Encryption database can be on a second drive. In this case, you must have a recovery file to unlock the drive without the database.
- Remote Help is available only for hard disk authentication. It is not available for recovery file authentication.

To use the Drive Slaving Utility

1. On a computer with Check Point Full Disk Encryption installed, run this command to start the Full Disk Encryption Drive Slaving Utility:

   ```
   <x:>\Program files(x86)\CheckPoint\Endpoint Security\Full Disk Encryption\fde_drive_slaving.exe
   ```

   Note - To unlock a protected USB connected hard disk drive, you must first start the Drive Slaving Utility, and then connect the disk drive.

   The **Full Disk Encryption - Drive Slaving** window opens.

2. Select a Full Disk Encryption protected disk to unlock.

   Unlock volume(s) authentication window opens.

3. Enter User account name and Password.

4. Click **OK**.

After successful authentication, use Windows Explorer to access the disk drive. If you fail to access the locked disk drive, use the Full Disk Encryption recovery file, then run the Drive Slaving Utility again.

Note - To prevent data corruption, shut down the system or use a safe removal utility before you disconnect the USB connected drive.

BitLocker Recovery

BitLocker recovery is the process by which you can restore access to a BitLocker-protected drive in the event that you cannot unlock the drive normally. You can use the Recovery Key ID for a computer to find the Recovery Key for an encrypted client computer. With the Recovery Key, the user can unlock encrypted drives and perform recoveries.

Important - Treat the Recovery Key like a password. Only share it using trusted and confirmed channels.

To get the recovery key for a client computer

1. Go to **Computer Management** > **Full Disk Encryption Actions** > **Recovery** > **BitLocker Recovery**

   The **BitLocker Management Recovery** window opens.

2. Enter the **Computer's Recovery Key ID** of the client. The Recovery Key ID is a string of numbers and letters that looks like this:

   C9F38106-9E7C-46AE-8E88-E53948F11776

   After you type a few characters, the Recovery Key ID fills automatically.

3. Click **Get Recovery Key**.

   The recovery key appears. It is a string of numbers that looks like this:

   409673-073722-568381-219307-302434-260909-651475-146696

4. On the client computer, type the recovery key.

FileVault Recovery

You can help users recover FileVault-encrypted data if they cannot log in to their Mac.

You can help users recover their data or reset their password using a personal recovery key that is unique to the client computer. You can reset the password remotely.

Password Reset using a Personal Key

If a user forgets the login password, the administrator can send a personal recovery key to the remote user, to allow them to log in. The key is a string of letters and numbers separated by dashes.

1. **The user locates the serial number of the locked device**.

Step	Instructions
1	Find the serial number of the locked device. It is usually printed on the back of the device.
2	Give the serial number to the support representative.

2. **The Administrator gives a recovery key to the user.**

Step	Instructions
1	Get the serial number of the locked device from the user.
2	In the Endpoint Web Management platform, go to **Computer Management** > **Full Disk Encryption Actions** > **Recovery** > **FileVault Recovery Media.** The FileVault Recovery Media window opens.
3	In the **Computer's Serial Number** field. type the serial number.
4	Click **Get Recovery Key**.
5	Give the recovery key to the user.

3. User resets their password.

Step	Instructions
1	Get the Recovery Key from the support representative.

Step	Instructions
2	Restart the Mac.
3	In the FileVault pre-boot screen, click the ? button A message shows: **If you forgot your password you can reset it using your Recovery Key**.
4	Type the Recovery Key, and click ->\ A progress bar shows.
5	For Local Users: a. In the **Reset Password** window, the user enters a new password, and optionally, a password hint. b. Click **Reset Password.**

How to update the Personal Recovery Key (PRK) for Native Encryption Management FileVault, see sk138352.

A personal key is unique to the client Mac computer or device. The key is a string of letters and numbers separated by dashes. To recover a user's FileVault-encrypted Mac using the personal key, the administrator reads the key to the user, and uses the key to decrypt and unlock the computer.

To decrypt and recover the user's FileVault-encrypted Mac:

For a volume formatted as APFS on macOS Mojave 10.14 and higher

1. Show the disk volumes on the Mac. Run this command:

   ```
   diskutil apfs list
   ```

   The volume to recover is the OS Volume. It has a name similar to disk2s1.

2. Run this command:

   ```
   diskutil apfs unlockVolume <Diskname> -passphrase <personal recovery key>
   ```

   The volume is now unlocked.

3. Get the list of apfs cryptousers. Run:

   ```
   diskutil apfs listcryptousers <Diskname>
   ```

   For example:

   ```
   diskutil apfs listcryptousers disk2s1
   ```

For a local user, select the UUID of the user that has `Type: Local Open Directory User`

4. Decrypt the volume. Run:

   ```
   diskutil apfs decryptVolume <diskname> -user <user UUID>
   ```

5. Enter the password of the local user
6. To monitor the progress of the decryption, run:

   ```
   diskutil apfs list
   ```

For a volume formatted as CoreStorage on macOS 10.12 or higher

1. Run this command:

   ```
   diskutil cs unlockVolume <lvUUID> -passphrase <personal recovery key>
   ```

2. The user interface shows a prompt to allow access. Enter the keychain password.

   The volume is now unlocked.

3. Start the decryption. Run:

   ```
   diskutil cs decryptVolume <lvUUID>
   ```

4. When prompted, enter the password for the local user.
5. To monitor progress of the decryption, run:

   ```
   diskutil cs list
   ```

The user can now reboot the Mac normally. They do not see the FileVault pre-boot screen.

Giving Remote Help to Full Disk Encryption Users

Use this challenge/response procedure to give access to users who are locked out of their Full Disk Encryption protected computers.

1. Go to the **Computer Management** view > **Full Disk Encryption** > **Remote Help**.

   The **Full Disk Encryption Remote Help** window opens.

2. Search for the locked computer.
3. Select the applicable user from the list.
4. Select the type of assistance the end-user needs:
   - **One-Time Logon** - Gives access as an assumed identity for one session without resetting the password.
   - **Remote Password change** - Resets the user's password. This option is for users who have forgotten their fixed passwords.
   - **Pre-Boot Bypass Remote Help** - Provides One-Time Logon assistance for computers that are configured to disable pre-boot, and uses the option to give remote help without pre-boot user.
5. Tell the user to enter the **Response one** text string in theRemote Help window on the locked computer.

   The endpoint computer shows a challenge code.

6. In the **Challenge (from user)** field, enter the challenge code that the user gives you.
7. Click **Generate Response**.

   Remote Help authenticates the challenge code and generates a response code.

8. Tell the user to enter the **Response Two (to user)** text string in the Remote Help window on the locked computer.
9. Make sure that the user changes the password or has one-time access to the computer before ending the Remote Help session.

Managing Active Directory Scanners

If your organization uses Microsoft Active Directory (AD), you can import users, groups, Organizational units (OUs) and computers from multiple AD domains into the Endpoint Security Management Server. After the objects are imported, you can assign policies.

When you first log in to the Endpoint Web Management Console, the AD tree is empty. To populate the tree with computers from the Active Directory, you must configure the Directory Scanner.

The Directory Scanner scans the defined Active Directory and fills the AD table in the **Computer Management** view, copying the existing Active Directory structure to the server database.

Harmony Endpoint Management Platform supports the use of multiple AD scanners per Active Directory domain, and multiple domains per service.

Required Permissions to Active Directory:

For the scan to succeed, the user account related to each Directory Scanner instance requires full read permissions to:

- The Active Directory root.
- All child containers and objects.
- The deleted objects container.

An object deleted from the Active Directory is not immediately erased, but moved to the Deleted Objects container.

Comparing objects in the AD with those in the Deleted objects container gives a clear picture of network resources (computers, servers, users, groups) that have changed since the last scan.

The Active Directory Scanner does not scan Groups of type "Distribution".

Required Configuration for Domains:

On the Active Directory server, set the Groups Scope to Domain Local only.

The Endpoint Web Management Console supports two methods of Active Directory scanning:

- Organization distributed scan
- Full Active Directory sync

Organization Distributed Scan

Organization Distributed Scan is enabled by default. You can see its configured settings in the **Endpoint Settings** view > **AD Scanners**.

Each Endpoint client sends its path to the Security Management Server.

By default, each Endpoint client sends its path every 120 minutes. In this method, only devices with Harmony Endpoint installed report their paths, other devices with do not report their information.

Full Active Directory Sync

In the Full Active Directory Sync, one Endpoint client is defined as the Active Directory scanner, it collects the information and sends it to the Security Management Server.

To configure the AD scanner:

1. In the **Computer Management** view, click **Create Directory Scanner**.

   The **Scanner** window opens.

2. Fill in this information:

   a. **Computer name** - Select a computer as your AD scanner.

   b. **AD Login Details** - Enter the user name and password information to access the Active Directory.

   c. **Domain controller** - Enter the name of the Domain controller and the port for the scan.

   d. **Use SSL communication (recommended)** - Select this checkbox if you want the connection between the AD scanner to the Domain Controller to be over SSL.

   e. **LDAP path** - The address of the scanned directory server.

   f. **Sync AD every** - Select the interval at which the scanning will be performed

When you create a new AD scanner, the Organization Directory Scan is automatically disabled.

To see information on your activated AD scanners, go to the **Endpoint Settings** view.

Note - You can also reach scanner configuration form through the **Endpoint Settings** view > **Setup full Active Directory sync**.

Active Directory Authentication

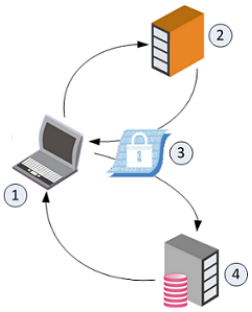
Endpoint Security Active Directory Authentication

When an Endpoint Security client connects to the Endpoint Security Management Server, an authentication process identifies the endpoint client and the user currently working on that computer.

The Endpoint Security system can function in these authentication modes:

- **Unauthenticated** mode - Client computers and the users on those computers are not authenticated when they connect to the Endpoint Security Management Server. They are trusted "by name". This operation mode is recommended for evaluation purposes only.
- **Strong Authentication** mode - Client computers and the users on those computers are authenticated with the Endpoint Security Management Server when they connect to the Endpoint Security Management Server. The authentication is done by the Active Directory server using the industry-standard Kerberos protocol. This option is only available for endpoints that are part of Active Directory.

The authentication process:



1. The Endpoint Security client **(1)** requests an authentication ticket from the Active Directory server **(2)**.
2. The Active Directory server sends the ticket **(3)** to the client **(1)**.
3. The client sends the ticket to the Endpoint Security Management Server **(4)**.
4. The Endpoint Security Management Server returns an acknowledgment of authentication to the Endpoint Security client **(1)**.

Important - If you use Active Directory Authentication, then Full Disk Encryption and Media Encryption & Port Protection are only supported on endpoint computers that are part of Active Directory.
Note - Full Disk Encryption and Media Encryption & Port Protection are not supported on endpoint computers in your environment that are not part of the Active Directory.

Configuring Active Directory Authentication

Make sure you configure Strong Authentication for your production environment. Do not set up Strong Authentication before you are ready to move to production. When you are ready to move to production, follow this process.

Workflow for Configuring Strong Authentication:

Step 1 of 3: Configuring the Active Directory Server for Authentication

Endpoint Security Strong Authentication uses the Kerberos network authentication protocol.

To enable the Active Directory server to validate the identity of clients that authenticate themselves through Kerberos, run the `ktpass.exe` command on the Active Directory Server. By running the `ktpass` command, you create a user that is mapped to the `ktpass` service. This creates a *Principal Name* for the AD server. The Principal Name must have this format: `ServiceName/realm@REALM`

Important - After you create the user that is mapped to the `ktpass` service, do not make changes to the user. For example, do not change the password. If you do change the user, the key version increases and you must update the **Version Key** in the **New Authentication Principal** window in the Endpoint Web Management Console.

To prepare the Active Directory Server for authentication:

1. Go to **Start** menu > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
2. Create a domain user and clear the option **User must change password at next logon**.
3. Open an elevated Windows Command Prompt.
4. In Windows Command Prompt, go to this folder:

   ```
   cd %WinDir%\System32\
   ```

5. Map a service to a user with this command:

   ```
   ktpass princ <Service Name>/<realm name>@<REALM NAME>
   mapuser <Username>@<REALM NAME> pass <Password> out <Name of
   Output File>
   ```

   Example:

```
ktpass princ tst/nac1.com@NAC1.COM mapuser auth-
user@NAC1.COM pass 123456 out outfile.keytab
```

Parameters:

Syntax	Example Value	Explanation
<Service Name>	tst	Name of the service.
<realm name> *<REALM NAME>*	nac1.com NAC1.COM	Domain name of the Active Directory server. The first instance is in lower case. The second instance in upper case.
<Username>	auth-user	The Active Directory domain user.
<Password>	123456	Password for user.
<Name of Output File>	outfile.keytab	Name of the encrypted keytab file.

6. Save the console output to a text file.

   See the version number (vno) and encryption type (etype).

   Sample output:

```
Targeting domain controller: nac1-dc.nac1.com
Successfully mapped tst/nac1.com to auth-user.
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to outfile.log:
Keytab version: 0x502
keysize 74 tst/nac1.com@NAC1.COM ptype 0 (KRB5_NT_UNKNOWN) vno 7 etype 0x17 (RC4-HMAC) keylength 16
(0x32ed87bdb5fdc5e9cba88547376818d4)
```

Important - We recommend that you do not use DES-based encryption for the Active Directory Domain Controller server, as it is not secure. If you choose to use DES encryption and your environment has Windows 7 clients, see sk64300

Notes:

- Make sure that the clock times on the Endpoint Security servers and the Kerberos server are less than 5 minutes apart. If the difference in the clock times is more than 5 minutes, a runtime exception shows and Active Directory authentication fails. On Gaia, use NTP or a similar service.
- To use Capsule Docs with Single Sign-On, disable the **User Access Control** (UAC) on Windows Active Directory Servers.

Step 2 of 3: Configuring Authentication Settings

Configure the settings in the Endpoint Web Management Console for client to server authentication.

Important - Use the **Unauthenticated** mode only for evaluation purposes. Never use this mode for production environments. Configure the authentication settings before moving to production.

How the Authentication Settings are Used in Deployment Packages

When you configure client package profiles, you select an authentication account. The SSO Configuration details are included in the client deployment package, which allows the server to authenticate the client.

To configure authentication settings:

1. In the Endpoint Web Management Console, click **Manage** > **Endpoints Authentication Settings**.

   The **Authentication Settings Properties** window opens.

2. Click **Add**.

   The **New Authentication Principal** window opens.

3. Enter the details from the output of `ktpass.exe`, that you configured in *"Step 1 of 3: Configuring the Active Directory Server for Authentication" on page 188*:

Field	Description
Domain name	Active Directory domain name. For example: `nac1.com`
Principle Name	Authentication service name in the format: `ServiceName/realm@REALM` This value must match the name that was configured in Active Directory > **New Object**. For example: `tst/nac1.com@NAC1.COM`
Version Key	Enter the version number according to the Active Directory output in the `vno` field. For example: `7`
Encryption method	Select the encryption method according to the Active Directory output in the `etype` field. For example: `RC4-HMAC`

Field	Description
Password	Enter (and confirm) the password of the Active Directory Domain Admin user you created for Endpoint Security use. For example: `123456`

4. Click **OK**.
5. When you are ready to work in Strong Authentication mode, select **Work in authenticated mode** in the **Authentication Settings Properties** window.
6. Click **OK**.

Important - After you turn on Strong Authentication, wait one minute before you initiate any client operations.
It takes time for the clients and the Endpoint Security Management Server to synchronize. During this time, the environment remains unauthenticated, and some operations fail. The exact amount of time depends on the Active Directory scanner (see *"Managing Active Directory Scanners" on page 185*).

Step 3 of 3: Save Changes

After you finished configuring strong authentication for Active Directory, save your changes.

1. In the Endpoint Web Management Console, go to the **Policy** tab.
2. In the Policy Toolbar, click **Save All Changes**.

UPN Suffixes and Domain Names

The User Principal Name (UPN) is the username in "email format" for use in Windows Active Directory (AD). The user's personal username is separated from a domain name by the "`@`" sign.

UPN suffixes are part of AD logon names. For example, if the logon name is `administrator@ad.example.com`, the part of the name to the right of the ampersand is known as the UPN suffix. In this case `ad.example.com`

When you configure a new user account in AD, you are given the option to select a UPN suffix, which by default will be the DNS name for your AD domain. It can be useful to have a selection of UPN suffixes available. If your AD domain name is `ad.example.com`, it might be more convenient to assign users a UPN suffix of `example.com`. To make additional UPN suffixes available, you need to add them to AD.

Configuring Alternative Domain Names

When you configure Strong Authentication for Active Directory communication between the Endpoint Security client and the Endpoint Security Management Server, you can configure multiple UPN suffixes for the Active Directory domain name.

To Configure Additional UPN Suffixes for Active Directory Authentication

1. In the Endpoint Web Management Console, open **Manage** > **Endpoints Authentication Settings**.

   The **Authentication Settings** window opens.

2. Click **Add**.

   The **New Authentication Principal** window opens.

3. In the **Domain name** field, enter the alternative Active Directory domain name. For example, if the previously configured domain name is `nac1.com` add an alternative domain name such as `ad.nac1.com`

4. Configure the other fields with the same values as the previously configured authentication settings:

   - **Principle Name**
   - **Version Key**
   - **Encryption Method**
   - **Password**

5. Click **OK**.

6. Go to the **Policy** tab and click **Save All Changes**.

Troubleshooting Authentication in Server Logs

To troubleshoot problems related to Active Directory Authentication, use the authentication log on the Endpoint Security Management Server or Endpoint Policy Server in `$UEPMDIR/logs/Authentication.log`.

To see full debugging information in the authentication log file on the Endpoint Security server:

1. Connect to the command line on the Endpoint Security server.

2. Log in to the Expert mode.

3. Set the debug environment variable:

```
export TDERROR_ALL_KERBEROS_SERVER=5
```

4. Restart the Endpoint Security server:

```
uepm_stop ; uepm_start
```

Results in the authentication log

- If the **Authentication.log** file on the Endpoint Security server shows:

  ```
  ERROR: Config file contains no principals.
  ```

  The database was cleaned or the process to include authentication in the client package was faulty.

  To fix:

  1. Repeat the process to configure Active Directory authentication.
  2. Make a new client package.
  3. Restart the Endpoint Security server.

- If the **Authentication.log** file on the Endpoint Security server shows:

  ```
  Permission denied in replay cache code
  ```

  Restart the Endpoint Security server.

- If the **Authentication.log** file on the Endpoint Security server shows:

  ```
  Clock skew too great
  ```

  - Make sure that the Endpoint Security server and all clients are synchronized with the Active Directory server.
  - Make sure that in the Windows Date and Time Properties window, the **Automatically adjust clock for daylight saving changes** option has the same value (selected or cleared) for all computers in the system, including the Active Directory server.

- The following workaround is not recommended, for security reasons, but is offered if you cannot fix the clock skew error with synchronization changes.

  To ensure that authentication occurs even if the clocks of the client, the Endpoint Security server and the Active Directory server are out of synch, define an acceptable skew.

  By default, the authentication clock skew is 3600 seconds. You can change the Endpoint Security settings.

  In the `$UEPMDIR/engine/conf/global.properties` file , add this line:

  ```
  authentication.clockSkew.secs=<Allowed Number of Seconds for Clock Skew>
  ```

- If the **Authentication.log** file on the Endpoint Security server shows:

  ```
  Key version number for principal in key table is incorrect
  ```

  Update the **Key version number** in the **Active Directory SSO Configuration** window.

  You might have changed the user that is mapped to the `ktpass` service.

To turn off full debugging information on the Endpoint Security server:

1. Connect to the command line on the Endpoint Security server.
2. Log in to the Expert mode.
3. Unset the debug environment variable:

   ```
   unset TDERROR_ALL_KERBEROS_SERVER
   ```

4. Make sure that the output is empty:

   ```
   echo $TDERROR_ALL_KERBEROS_SERVER
   ```

5. Restart the Endpoint Security server:

   ```
   uepm_stop ; uepm_start
   ```

Troubleshooting Authentication in Client Logs

The authentication log file for each Endpoint Security client is located on the client computer:

`%DADIR%\logs\Authentication.log`

A normal log looks like this:

```
[KERBEROS_CLIENT(KerberosLogger_Events)] : Credentials acquired
for John@ACME-DOM.COM
[KERBEROS_MESSAGE(KerberosLogger_Events)] : Message is Empty.
[KERBEROS_CLIENT(KerberosLogger_Events)] : Security context is not
yet established.continue needed.
```

- If the **Authentication.log** file on the client shows:

  ```
  No authority could be contacted for authentication.
  ```

  The Endpoint Agent cannot find a Domain Controller to supply credentials.

  To fix this:

  1. Make sure that the client is in the domain and has connectivity to your Domain Controller.
  2. To authenticate with user credentials, log off and then log in again.

     To authenticate with device credentials, restart the computer.

- If the **Authentication.log** file on the client shows:

  ```
  The specified target is unknown or unreachable.
  ```

  Check the service name. Make sure that there are no typing errors and that the format is correct.

  If there was an error, correct it on the Check Point Endpoint Security Management Server.

Managing Virtual Groups

Virtual Groups manage groups of devices.

You can use Virtual Groups with Active Directory for added flexibility or as an alternative to Active Directory.

Objects can be members of more than one virtual group.

The benefits of using Virtual Groups include:

- Using the Active Directory without using it for Endpoint Security.

  For example: Different administrators manage the Active Directory and Endpoint Security.

- Your Endpoint Security requirements are more complex than the Active Directory groups. For example, you want different groups for laptop and desktop computers.
- Using a non-Active Directory LDAP tool.
- Working without LDAP.

Some virtual groups are pre-defined with computers assigned to them automatically.

These groups are: Andi, Desktops, External Users, Laptops, MacLaptops, MacDesktops, , My Organization, Servers, WinDesktops, WinLaptops.

To create, edit or delete a virtual group, click **Manage Groups** in the **Computer Management** view.

Notes:

- A device can belong to multiple virtual groups.
- Selecting a certain device shows the Active Directory information collected about them.
- You cannot edit Active Directory groups, but you can view their content.
- You can create a group and then assign the devices to the group, or select devices first and then create a group from them.

To add a device to a virtual group:

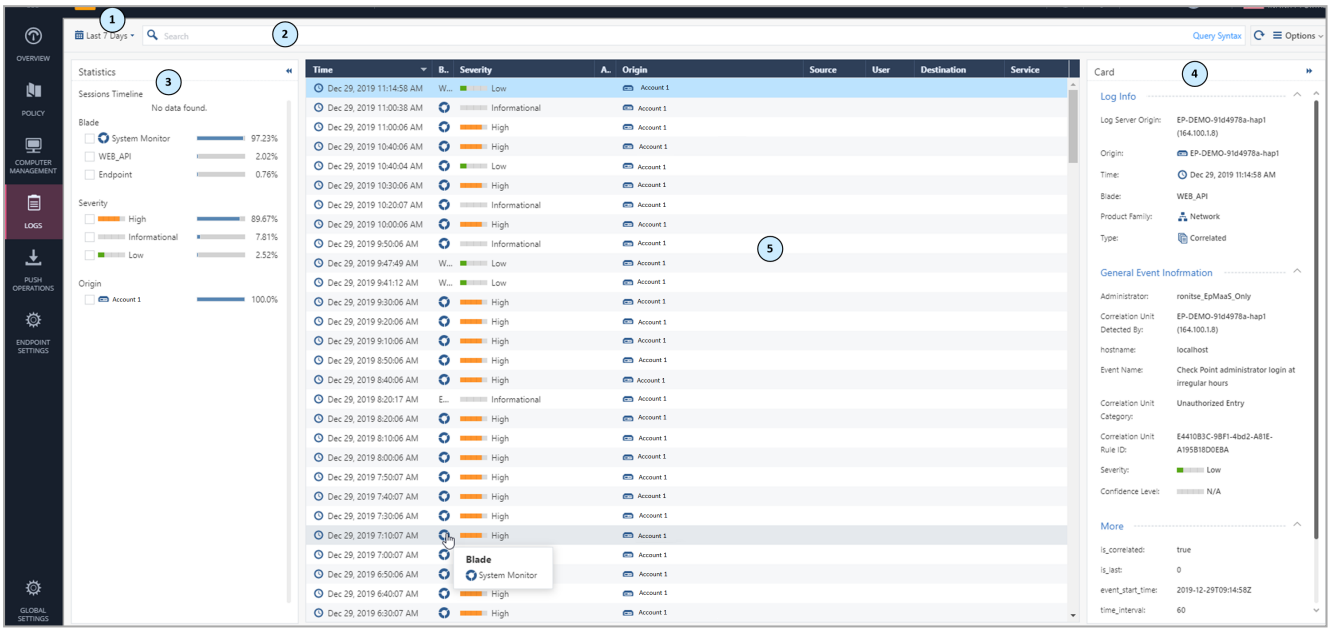
1. Select the applicable device from the list.
2. In the menu bar of the **Computer Management** view, click **Add to Virtual Group**
3. Select the applicable Virtual Group and click **OK**.

To delete a device from a virtual group:

1. Select the applicable device from the list.
2. In the menu bar of the **Computer Management** view, click  to edit virtual groups.
3. Select the applicable virtual groups and click **Delete selected members**.

Viewing Logs

The Logs view shows information about the security events that occurred in your Endpoint clients.



Item	Description
1	**Time period** - Search with predefined custom time periods or define another time period for the search.
2	**Query search bar** - Enter your queries in this field.
3	**Statistics pane** - Shows statistics of the events by Blades, severity of the event and origin.
4	**Card** - Log and additional information
5	**Results pane** - shows log entries for the most recent query

Exporting Logs

Check Point Log Exporter is an easy and secure method to export Check Point logs over syslog. Log Exporter is a multi-threaded daemon service which runs on a log server. Each log that is written on the log server is read by the Log Exporter daemon. It is then transformed into the applicable format and mapping and sent to the end target.

For more information, see sk122323.

To export logs from the Endpoint Web Management Console:

1. Go to **Endpoint Settings** > **Export Events**.
2. Click **Add**.

   The **New Logging Service** window opens.
3. Fill in the export details:
   - **Name** - Enter a name for the exported information.
   - **IP Address** - Enter the IP Address of the target to which the logs are exported.
   - **Protocol** - Select the protocol over which to export the logs: TCP or UDP.
   - **Format** - Select the export format.
   - **Port** - Select the port over which to export the logs. Only these ports are supported for outgoing communication: 514, 6514, 443.
   - **TLS/SSL** - Select this checkbox if you want log information to be TLS/SSL encrypted. The only allowed authentication method through TLS is mutual authentication. For mutual authentication, log exporter needs these certificates:
     - A `*.pem` Certificate Authority certificate (should contain only the certificate of the CA that signed the client/server certificates, not the parent CA).
     - A `*.p12` format client certificate (log exporter side).

     For instructions on how to create the certificates, see *"Creating Security Certificates for TLS Mutual Authentication" below*.
4. Click **Add**.

Creating Security Certificates for TLS Mutual Authentication

This section explains how to create self-signed security certificates for mutual authentication.

Notes:

- Make sure to run the `openssl` commands on a 3rd party CA server (not on the log exporter device). The log exporter device must have a connectivity to the CA server.
- The commands are not supported on a Check Point Security Management Server or a Multi-Domain Server.

Procedure

1. **Create a CA certificate**

Step	Instructions
1	Generate the self-signed root CA key: `openssl genrsa -out ca.key 2048`
2	Generate the root CA certificate file in the PEM format: `openssl req -x509 -new -nodes -key ca.key -days 2048 -out ca.pem` Enter the information regarding the certificate. This information is known as a Distinguished Name (DN). An important field in the DN is the Common Name(CN), which should be the exact Fully Qualified Domain Name (FQDN) of the host, with which you intend to use the certificate. Apart from the Common Name, all other fields are optional and you can skip it. If you purchase an SSL certificate from a certificate authority, it is often required that these additional fields, such as "Organization", accurately reflect your organization's details. **Best Practice** - We recommend to use the device IP address as the Common Name.

2. **Create a client certificate**

Step	Instructions
1	Generate a client key: `openssl genrsa -out cp_client.key 2048`
2	Generate a client certificate sign request: `openssl req -new -key cp_client.key -out cp_client.csr`
3	Sign the certificate using the CA certificate files: `openssl x509 -req -in cp_client.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out cp_client.crt -days 2048 -sha256`

Step	Instructions
4	Convert the certificate to the P12 format: `openssl pkcs12 -inkey cp_client.key -in cp_client.crt -export -out cp_client.p12` **Note** - The challenge phrase used in this conversion is required in the `log_exporter` TLS configuration.

3. **Update the security parameters on the Check Point exporting server**

Step	Instructions
1	On a Multi-Domain Server or Multi-Domain Log Server, go to the context of the applicable Domain Management Server or Domain Log Server: `mdsenv <Name or IP Address of Domain Management Server or Domain Log Server`
2	Go to the deployment directory: `cd $EXPORTERDIR/targets/<Deployment Name>/`
3	Create a directory for the certificate files: `mkdir -v certs`
4	Copy the `ca.pem` and `cp_client.p12` certificate files to the `$EXPORTERDIR/targets/<Deployment Name>/certs/` directory. **Note** - The `ca.key` must **not** be published.

5	Assign the read permissions to the `ca.pem` and `cp_client.p12` certificate files:
	`chmod -v +r ca.pem`
	`chmod -v +r cp_client.p12`

6	Update the secured target: `cp_log_export set name <Name> domain-server <Domain-Server> encrypted true ca-cert <Full Path to CA Certificate *.pem File> client-cert <Full Path to *.p12 Certificate File> client-secret <Challenge Phrase for the *.p12 File>`

4. **Create a server (target) certificate**

Step	Instructions
1	Generate a server key: `openssl genrsa -out server.key 2048`
2	Generate a server certificate sign request: `openssl req -new -key server.key -out server.csr`
3	Sign the certificate using the CA certificate files: `openssl x509 -req -in server.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out server.crt -days 2048 -sha256`

Note - Some SIEM applications require the server certification to be in a specific format. For more information, refer to sk122323 > section "*SIEM Specific Instructions*".

Downloading Forensics Reports

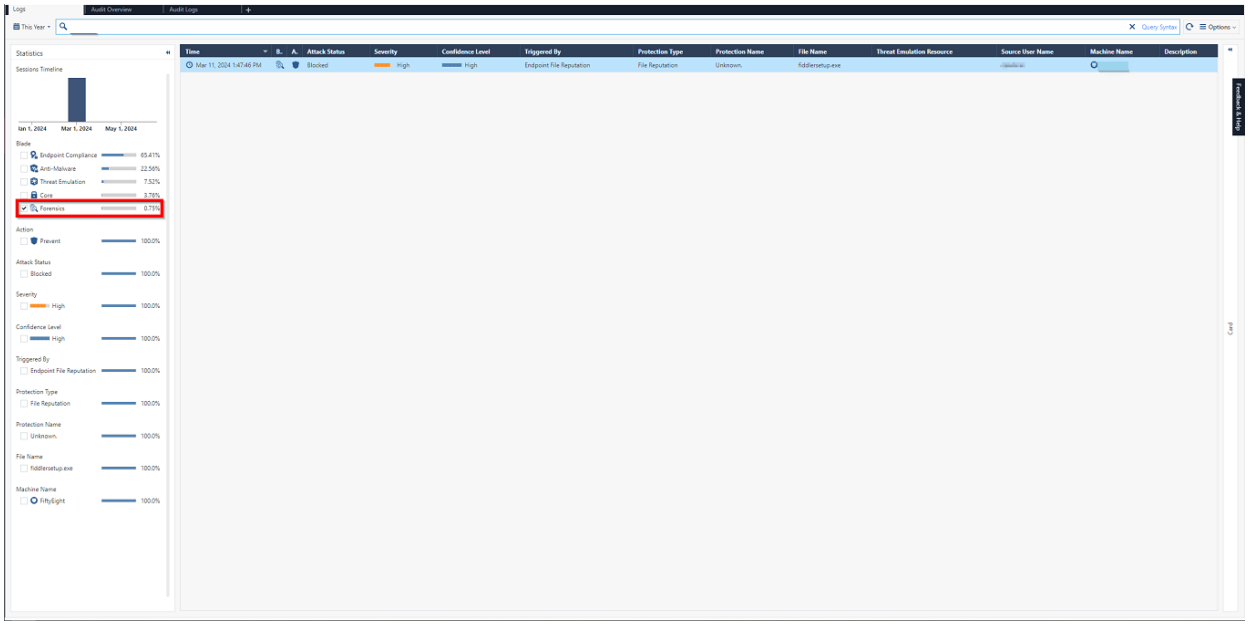
The Forensic Report shows a comprehensive analysis of the entire sequence of an attack, as analyzed by the Forensics software blade in Harmony Endpoint.

It provides information about attacks and suspicious behavior. The report includes:

- **Entry Point** - 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.

To download the forensics report of an event:

1. Go to **Logs** and from the **New Tab Catalog**, select **Logs**.
2. Expand the **Statistics** pane and in the **Blade** section, select **Forensics**. For more information, see *"Viewing Logs" on page 198*.

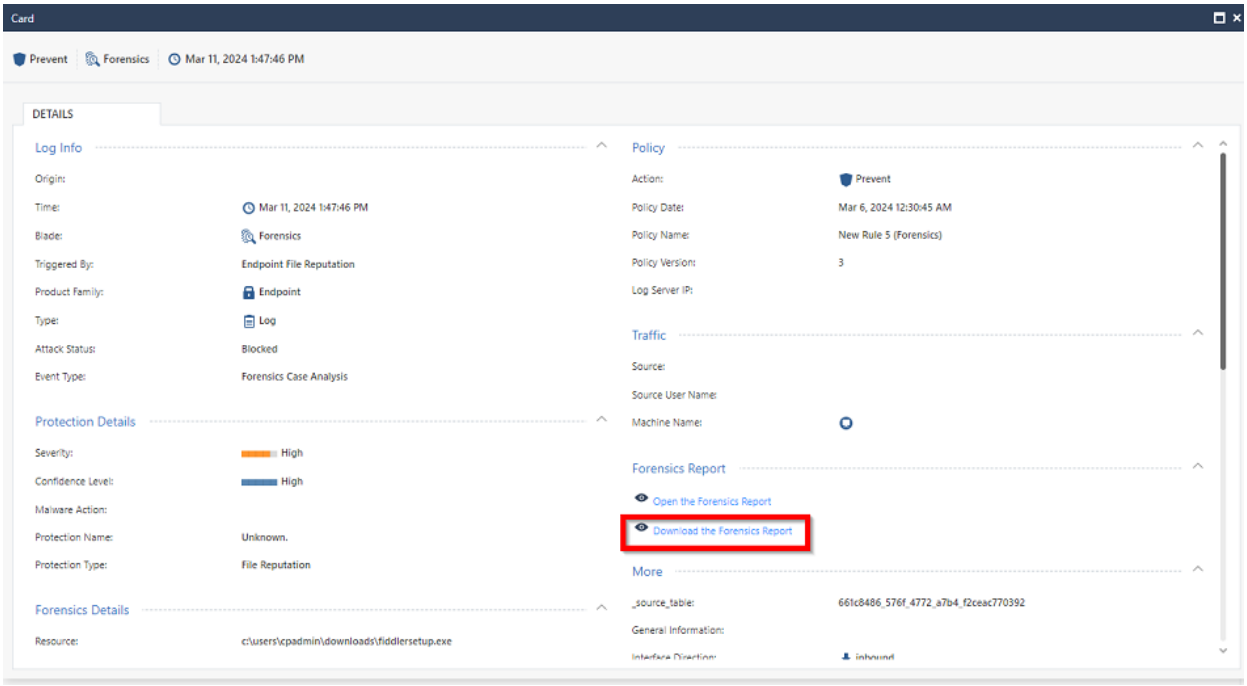


Note - To search the Forensics event using the machine name, enter the machine name in the search field and click **Enter**.

3. From the list, double-click the event for which you want to download the report.

   The **Card** window with the log details appears.

4. Scroll-down to **Forensics Report** section and click **Download the Forensics Report**.



Note - To view the Forensics Report without downloading, click **Open the Forensics Report**.

The report file is downloaded to the computer in the JSON format.

Performing Push Operations

Push operations are operations that the server pushes directly to client computers with no policy installation required.

Note - If there is no response from the Endpoint Security client, the Push Operation will time out after 24 hours. You must reinitiate the Push Operation.

To add a Push Operation:

1. Go to the **Push Operation** view and click **Add**.
2. Select the push operation and click **Next**.

Category	Push Operations	Windows	macOS	Linux
Anti-Malware	Scan for Malware	Yes	Yes	Yes
	Update Malware Signature Database	Yes	Yes	Yes
	Restore Files from Quarantine	Yes	Yes	Yes

Category	Push Operations	Windows	macOS	Linux
Forensics and Remediation	Analyze by Indicator	Yes	Yes	No
	File Remediation	Yes	Yes	Yes
	Isolate Computer	Yes	Yes	No
	Release Computer	Yes	Yes	No
Agent Settings	Deploy New Endpoints	Yes	No	No
	Collect Client Logs	Yes	Yes	No
	Repair Client	Yes	No	No
	Shutdown Computer	Yes	Yes	No
	Restart Computer	Yes	Yes	No
	Uninstall Client	Yes	Yes	No
	Application Scan	Yes	Yes	No
	Kill Process	Yes	Yes	No
	Remote Command	Yes	Yes	Yes
	Registry Actions	Yes	No	No
	File Actions	Yes	Yes	No
	Collect Processes	Yes	No	No

3. Select the devices on which you want to perform the push operation.

Note - You can perform **Run Diagnostics** on only one device at a time.

4. Click **Next**.
5. Configure the operation settings.

Anti-Malware

Push Operations	Description	2FA Required
Scan for Malware	Runs an Anti-Malware scan on the computer or computers, based on the configured settings.	No
Update Malware Signature Database	Updates malware signatures on the computer or computers, based on the configured settings.	No
Restore Files from Quarantine	Restores files from quarantine on the computer or computers, based on the configured settings. **To restore files from quarantine:** a. In the **Full Path** field, enter the path to file before it was quarantined including the file name. For example, `c:\temp\eicar.txt` b. Click **OK**.	No

Forensics and Remediation

Push Operations	Description	2FA Required
Analyze by Indicator	Manually triggers collection of forensics data for an endpoint device that accesses or executes the indicator. The indicator can be a URL, an IP, a path, a file name or an MD5.	No

Push Operations	Description	2FA Required
File Remediation	Quarantines malicious files and remediates them as necessary. **To move or restore files from quarantine:** a. Click + and select the organization. b. Click **Update Selection**. c. Select the device and click **Next**. d. Add **Comment**, optional comment about the action. e. To move the files to quarantine, select **Move the following files to quarantine**. f. To restore the files from quarantine, select **Restore the following files to quarantine**. g. Click +. h. From the drop-down: i. Select **Full file path or Incident ID**: I. In the **Element** field, enter the incident ID from the Harmony Endpoint Security client or enter the incident UID for the corresponding incident from the Logs menu in the Harmony Endpoint portal. To obtain the incident UID, open the log entry and expand the **More** section to view the incident UID. II. Click **OK** ii. Select **MD5 Hash**: I. Enter or upload the **Element**. II. Click **OK**. i. Click **Finish**.	No

Push Operations	Description	2FA Required
Isolate Computer	Makes it possible to isolate a specific device that is under malware attack and poses a risk of propagation. This action can be applied on one or more devices. The Firewall component must be installed on the client in order to perform isolation. Only DHCP, DNS and traffic to the management server are allowed.	No
Release Computer	Removes device from isolation. This action can be applied on one or more devices.	No

Agent Settings

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>Deploy New Endpoints</td><td>Installs the Initial Client on the target devices remotely using any device as the medium to run the push operation. This is suitable if do not have third party tools such as Microsoft System Center Configuration Manager (SCCM) or Intune to install the client.
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Comment</td><td>Optional comment about the action.</td></tr>
<tr><td>Select the deployment endpoint</td><td>Select the target endpoint or device where you want to install the Initial Client from the organizational tree.
⚠ Caution - The target device must not be the same as the source device.</td></tr>
<tr><td>Endpoint version</td><td>Select the Harmony Endpoint Security Client version to install on the target device.</td></tr>
</table></td><td>No</td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>Collect Client Logs</td><td>Collects CPInfo logs from an endpoint based on the configured settings.
For Windows:
For Endpoint Security Client versions E88.31 and higher, client logs are stored in the directory C:\ProgramData\CheckPoint\Endpoint Security\Temp.
For Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory C:\Windows\SysWOW64\config\systemprofile\CPInfo.
For macOS, client logs are stored in the directory /Users/Shared/cplogs.
<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr><tr><td>Log set to collect</td><td>Select the scope of information for the logs.</td></tr><tr><td>Debug Info upload</td><td>Select the location to upload the logs:
Upload CPInfo reports to Check Point servers
Upload CPInfo reports to Corporate server - Update the relevant corporate server information.</td></tr></table></td><td>No</td></tr>
<tr><td>Repair Client</td><td>Repairs the Endpoint Security client installation. This requires a computer restart.
Note - This push operation applies only to Harmony Endpoint Security clients that have been upgraded to a newer version at least once after the installation.</td><td>No</td></tr>
<tr><td>Shutdown Computer</td><td>Shuts down the computer or computers based on the configured settings.</td><td>No</td></tr>
</table>

Push Operations	Description	2FA Required
Restart Computer	Restarts the computer or computers based on the configured settings.	No
Uninstall Client	Uninstalls the Endpoint Security client remotely on the selected devices. This feature is supported for E84.30 client and above.	Yes
Application Scan	Collects all available applications in a certain folder on a set of devices and then adds them to the application repository of the "Application Control" blade on that specific tenant.	No
Kill Process	Remotely kills/ terminate the processes.	No
Remote Command	■ Allows administrators to run both signed (introduced by CP) and unsigned (ones the customer creates) scripts on the Endpoint Client devices. ■ Especially useful in a non-AD environment. ■ Supplies tools/fixes to customers without the need to create new EP client/server versions. ■ Saves passwords securely when provided. The Remote Command feature is supported only in Windows clients running version E85.30 and above	Yes

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>Search and Fetch files</td><td>Searches and uploads files to a server.

Supported fields are:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Comment</td><td>Optional comment about the action.</td></tr>
<tr><td colspan="2">Search and Fetch files</td></tr>
<tr><td>Locate the following files in the specific folders</td><td>Searches for the files in the specified folders.
a. In the File table, click + .
b. Enter the file name. For example, test.txt or test.zip and click OK.
c. Repeat the steps 1 and 2 for additional files.
d. In the Folder Path table, click +
e. Enter the path and click OK.
f. Repeat the steps 4 and 5 for additional paths.</td></tr>
<tr><td>Locate the following files by exact path</td><td>Searches for the files in the specified path.
a. In the File table, click + .
b. Enter the path where you ant to search for the file and click OK.
c. Repeat the steps for additional paths.</td></tr>
<tr><td colspan="2">Files upload</td></tr>
<tr><td>Select the Upload files to</td><td>Select the checkbox to upload the files to a server.</td></tr>
</table></td><td>Yes</td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Corporate Server Info</td><td>a. Specify these:
i. Protocol
ii. Server address
iii. Path on server
iv. Server fingerprint
b. If the server requires login to access it, select the Use specific credentials to upload checkbox, and enter Login and Password.</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>Registry Actions</td><td>Add or remove a registry key.

Supported fields:<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr><tr><td>Action</td><td>Select an action.
Add Key to Registry
Remove Key From Registry
Caution - Removing a registry might impact the endpoint's operating system.</td></tr><tr><td colspan="2">Add Key to Registry</td></tr><tr><td>Key</td><td>Full path where you want to add the registry key.
For example, Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</td></tr><tr><td>Subkey</td><td>Enter the key name to add in the registry. For example, ProductVersion.</td></tr><tr><td>Value Type</td><td>Select the registry type.</td></tr><tr><td>Value</td><td>Enter the registry value.</td></tr><tr><td>Is redirected</td><td>Indicates that virtualization is enabled and add the registry to 32-bit. By default, the registry is added for 64-bit.</td></tr><tr><td colspan="2">Remove Key From Registry</td></tr></table></td><td>No</td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Key</td><td>Full path of registry key that you want to delete.
For example, Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis
Caution - Removing a registry might impact the endpoint's operating system.</td></tr>
<tr><td>Subkey</td><td>Enter the key name to remove from the registry. For example, ProductVersion.</td></tr>
<tr><td>Is redirected</td><td>Indicates that virtualization is enabled and delete the registry in 32-bit. By default, the registry is deleted for 64-bit.</td></tr>
</table>
To change the working hours to allow the Anti-Malware signature updates on a DHS compliant Endpoint Security client, see sk180559.
</td><td></td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>File Actions</td><td>Copy, move or delete the file or folder.
Supported fields:
  Note - The folder actions are supported only with the Endpoint Security Client version 87.20 and higher.
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Comment</td><td>Optional comment about the action.</td></tr>
<tr><td>Action</td><td>Select an action.
■ Copy File
■ Move File
■ Delete File
  Caution - Deleting a file might impact Harmony Endpoint's protected files.</td></tr>
<tr><td colspan="2">Copy File</td></tr>
<tr><td>File path</td><td>Full path of the file or folder you want to copy, including the file or folder name.
Example:
■ For File - C:\Users\<user_name>\Desktop\test.doc
■ For Folder - C:\Users\Username\Desktop\</td></tr>
</table></td><td>No</td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Target file path</td><td>Full path where you want to paste the file or folder.
Example:
■ For File - C:\Users\<user_name>\Documents
■ For Folder - C:\Users\Username2\
Notes:
■ The file or folder name you specify is used to rename the copied file.
■ If you provide the folder path only, the file is copied with the original file name.
■ If the file or folder already exists, the file is not overwritten and the operation fails.
■ If the file path or target folder does not exist, it is created during the operation.</td></tr>
<tr><td colspan="2">Move File</td></tr>
<tr><td>File path</td><td>Full path of the file or folder you want to move, including the file or folder name.
Example:
■ For File - C:\Users\<user_name>\Desktop\test.doc
■ For Folder - C:\Users\Username>\Desktop\</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Target file path</td><td>Path where you want to move the file or folder.
Example:
■ For File - C:\Users\<user_name>\Documents
■ For Folder - C:\Users\Username1\Documents\
Notes:
■ If you provide the full file path, the is moved with the specified name.
■ If you provide the folder path only, the file is moved with the original file name.
■ If the file or folder already exists, the file or folder is not overwritten and the operation fails.
■ If the file path or target folder does not exist, it is created during the operation.</td></tr>
<tr><td colspan="2">Delete File</td></tr>
<tr><td>File path</td><td>Full path of the file you want to delete, including the file name.
For example, C:\Users\<user_name>\Desktop\test.doc
Caution - Deleting a file might impact Harmony Endpoint's protected files.
Note - Delete folder action is not supported.</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr><th>Push Operations</th><th>Description</th><th>2FA Required</th></tr>
<tr><td>Collect Processes</td><td>Collects information about the process running on the endpoint.

Supported fields:<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr><tr><td>Collect all processes</td><td>Collects information about all the processes running on the endpoint.</td></tr><tr><td>Collect process by name</td><td>Collects information about a specific process on the endpoint.</td></tr><tr><td>Process name</td><td>Enter the process name. Case-sensitive.</td></tr><tr><td>Additional output fields</td><td>Select the additional information you want to view in the collected information.</td></tr></table></td><td>No</td></tr>
</table>

6. Under **User Notification**:
   - To notify the user about the push operation, select the **Inform user with notification** checkbox.
   - To allow the user to post pone the push operation, select the **Allow user to postpone operation** checkbox.
7. Under **Scheduling**:
   - To execute the push operation immediately, click **Execute operation immediately**.
   - To schedule the push operation, click **Schedule operation for** and click to select the date.
8. For Push Operations that support 2FA authentication, you are prompted to enter the verification code.

   If you have not enabled 2FA authentication, a prompt appears to enable 2FA authentication:

- To enable 2FA authentication for your profile, click **Profile Setting**, and follow the instructions. For more information, see *Infinity Portal Administration Guide*.
- To enable 2FA authentication for the current tenant, click **Global Settings**, and follow the instructions. For more information, see *Infinity Portal Administration Guide*.

9. Click **Finish**.
10. View the results of the operations on each endpoint in the **Endpoint List** section (in the **Push Operations** menu) at the bottom part of the screen.

Harmony Endpoint for Linux

This chapter describes the installation and use of Harmony Endpoint on Linux operating systems in a web management environment.

Harmony Endpoint for Linux Overview

Check Point Harmony Endpoint for Linux protects Linux Endpoint devices from malware, and provides Threat Hunting / Endpoint Detection and Response capabilities. The solution is centrally managed and can be used as a Management-as-a-Service or deployed on a local on-premises server.

Note - Starting in R81, the on-premises Endpoint Security Server supports Harmony Endpoint for Linux. To enable Harmony Endpoint for Linux, you must enable the Linux installation package flag as described in sk177250.

Prerequisites

- Available Internet access for the protected device.
- For RHEL/CentOS, it is necessary to have access to EPEL (Extra Packages for Enterprise Linux) repository.
- If the device has no internet access, you must enable access to certain URLs. For more information, see sk116590.

Minimum Hardware Requirements

- x86 processor, 64-bit (32-bit is not supported)
- 2 GHz Dual-core CPU
- 4 GB RAM
- 10 GB free disk space

Deploying Harmony Endpoint for Linux

This section explains how to install Harmony Endpoint on Linux operating systems in a web management environment.

If the server environment includes a proxy server for Internet access, it is necessary to configure a proxy server as described in this section. Otherwise, skip to *"Downloading the Installation Script" on the next page*

Configuring a Proxy Server on the Endpoint Security Management Server

1. Connect to the command line on the Endpoint Security Management Server.
2. Log in to the Expert mode..
3. Stop the Check Point services:

   ```
   cpstop
   ```

4. Edit the `/$UEPMDIR/engine/conf/local.properties` file:

   ```
   vi /$UEPMDIR/engine/conf/local.properties
   ```

5. Add these properties:

   Important - Delete the **#** character from the beginning of each row that you edit.

   - The proxy server's IP address:

     ```
     http.proxy.host=<IP Address>
     ```

   - The proxy server's listening port:

     ```
     http.proxy.port=<Port>
     ```

   - The proxy server username:

     If basic authentication is enabled on the proxy server, enter the user name. If no authentication is required, leave it empty.

     ```
     http.proxy.user=<Username>
     ```

- The proxy server password:

  If basic authentication is enabled on the proxy server, then enter the password. If no authentication is required, leave it empty.

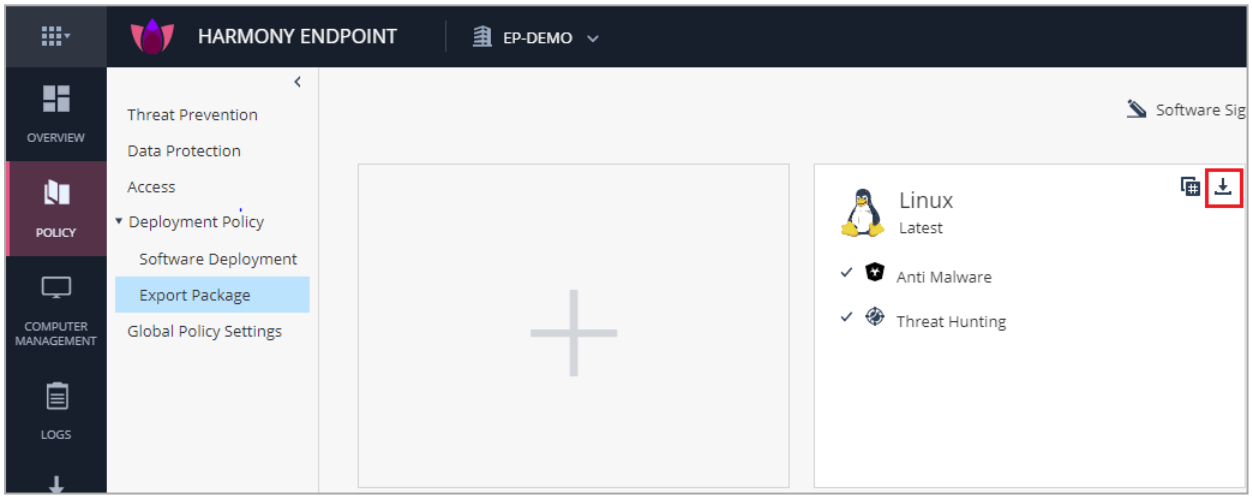
  ```
  http.proxy.password=<Password>
  ```

6. Save the changes in the file and exit the editor.
7. Start the Check Point services:

   ```
   cpstart
   ```

Downloading the Installation Script

1. Download the installation script from the **Policy > Deployment Policy** section to the target device.



2. Follow the applicable options:

   - To allow execution permission to the file, run:

     ```
     chmod +x ./<Name of Install Script>
     ```

   - To deploy both Anti-Malware and Threat Hunting, run:

     ```
     sudo ./<Name of Install Script> install
     ```

   - To deploy Anti-Malware only, run:

     ```
     sudo ./<Name of Install Script> install --product am
     ```

- To deploy Threat Hunting only, run:

```
sudo ./<Name of Install Script> install --product edr
```

- To enable Threat Hunting, make sure that Threat Hunting is enabled in the applicable policy rule.

Notes:

- If Kerberos authentication is enabled, then HTTP 401 is in the `/var/log/checkpoint/cpla/cpla.log` file.
- It is necessary to put the keytab file used for authentication set up in: `/var/lib/checkpoint/cpmgmt/auth.keytab` file (the file is generated by the *ktpass* utility).

Harmony Endpoint for Linux CLI Commands

Help & Information Commands

To show a list of all the help commands with their descriptions, run:

```
cpla --help
```

To show the help for available Anti-Malware commands, run:

```
cpla am --help
```

To show information about the product and the security modules installed (Anti-Malware, EDR) run:

```
cpla info
```

To show the information about the installed Anti-Malware module, run:

```
cpla am info
```

To show the help for available commands for the installed EDR module, run:

```
cpla edr --help
```

To show information about the installed EDR, run:

```
cpla edr info
```

Quarantine Commands

To see a list of all current quarantined files, run:

```
cpla am quarantine list
```

To add a file to quarantine, run:

```
sudo cpla am quarantine add <path_to_file>
```

To remove a file from quarantine, and restores the file to its original place, run:

```
sudo cpla am quarantine restore <path_to_file>
```

To show the help for available Anti-Malware quarantine commands, run:

```
cpla am quarantine --help
```

Scans & Detections

To trigger a scan of files in the provided path by the Anti-Malware module, run:

```
cpla am scan <path_to_scan>
```

To show the detections of Anti-Malware for the latest <number_of_days>, run:

```
cpla am detections <number_of_days>
```

Note - You can use this command without a parameter (as in *cpla am* detections). In this case, it sets the default value is 7.

Logs

To collect the logs of the product:

```
cpla collect-logs
```

Note - When you use this command, it prepares a Zip file which you can send to the support manually.

Uninstall Harmony Endpoint for Linux

To uninstall Harmony Endpoint from Linux, run:

```
sudo ./ <install script name> uninstall
```

To uninstall EDR only, run:

```
sudo ./ <install script name> uninstall --product edr
```

Harmony Endpoint for Linux Additional Information

- After the first installation, wait two to three minutes for the Anti-Malware service to complete the signature package. When complete, the **service** button shows as **running mode**. This procedure take up to 15 minutes, depending on your network connectivity.
- For information about Threat Hunting, go to the Threat Hunting tab. Threat Hunting lets you threat hunt files, processes, and domains accessed by the protected Virtual Machines.

Best Practice - We recommend that you remove any other 3rd party Anti-Malware solution before you install Harmony Endpointfor Linux.

Harmony Endpoint for Windows Virtual Desktop Infrastructure (VDI)

Virtual Desktop Infrastructure (VDI) is the technology to create and manage virtual desktops. VDI is available as a feature in Check Point's Endpoint Security Client releases.

- VMware Horizon is supported in E81.00 (and higher) for Persistent Mode and as a feature on E83.10 (and higher) for Non-Persistent Mode.
- Citrix XenDesktop is supported in E84.20 (and higher).

A virtual machine monitor (the hypervisor) controls the virtual machine that creates the virtual desktops. All the activity on the deployed virtual desktops occurs on the centralized server.

The "Golden Image" is the base ("Master") desktop image and the model for clone images. Desktop Pools define the server resources for the virtual desktops and solutions to hold the latest Anti-Malware signatures on all the virtual desktops.

Virtual desktop software applications support two modes.

- Persistent Mode:
  - Each user has a single specific desktop for their solitary use.
  - Each user's desktop retains data on the desktop itself between logins and reboots.
  - The user's machine is not "refreshed" for other users.
- Non-Persistent Mode:
  - Each user has a desktop from a pool of resources. The desktop contains the user's profile.
  - Each user's desktop reverts to its initial state when the user logs out.
  - The user's machine is fresh in each instance.

Important - Non-Persistent virtual desktops access Anti-Malware signatures in a shared folder in the Shared Signatures Solution.

The tested versions are:

- VMware Horizon 7 version 7.6 and 7.10 (E81.00 for Persistent Mode, E83.10 for Non-Persistent Mode)
- VMware Horizon 7 version 7.13 (E86.60 for both Persistent Mode and Non-Persistent Mode)

- VMware Horizon 8 version 8.3 (E86.60 for both Persistent Mode and Non-Persistent Mode)
- Citrix Virtual Apps and Desktops 7 1912

The software environments between and after these versions should work. Earlier versions may work. Contact *Check Point Support* for assistance with earlier versions.

Important - AD Scanner feature must be enabled in VDI environments.

Minimal Requirements for Virtual Machines:

For information on minimal requirements for virtual machines, see Client Requirements.

Configuring Clients for Persistent Desktops

Software Blades for Persistent Desktops

Persistent virtual desktops have the same Endpoint Security client capabilities as non-virtual desktops.

Creating a Basic Golden Image for Persistent Desktops

See *"Basic Golden Image Settings" on page 241* for the procedure to create a basic golden image.

Client Machine Configuration for Persistent Desktops

Configurations for client machines are part of the creation of the Golden Image.

We recommend that you disable Periodic Scan to avoid "Scan Storms".

"Anti-Malware Scan Storms" can occur when anti-virus scans run at the same time on multiple virtual machines on the same physical server. A degradation of system performance is possible that can affect disk I/O and CPU usage.

Setting up the Client Machine for Persistent Desktops

1. Disable the Anti-Malware Periodic Scan.

   See *"Appendix" on page 245*.

2. If you did **not** disable the Anti-Malware Periodic Scan, then enable the Anti-Malware Randomized Scan.

   Procedure

   a. From the left navigation panel, click **Policy**.

   b. In the left pane, click **Threat Prevention**.

   c. In the policy, click the applicable rule.

   d. In the right pane, click the **Web & Files Protection** tab.

   e. Scroll down and click the **Advanced Settings** button.

   f. From the left tree, click **Files Protection** > **Scan**.

   g. Select **Randomize scan time**.

   Note - On the VDI environment, you can configure Harmony Endpoint to randomize the **Periodic Scan** according to the scanning period. For example, if the **Scan Periodic** is set as **Every Week**, Harmony Endpoint further randomizes the scan within the week.

   h. Configure the applicable schedule.

   i. Click **OK**.

   j. At the bottom, click **Save**.

   k. At the top, click **Install Policy**.

Creating a Pool for Persistent Desktops

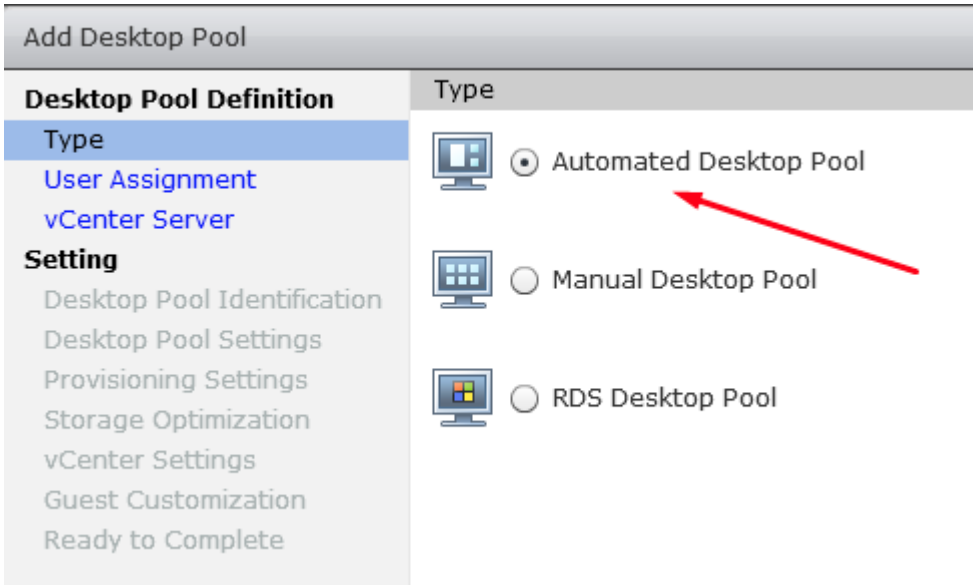
Best Practice - We recommend to use a different naming pattern for each machine in each pool.

VMware Horizon Key Points

This procedure is mandatory to create supported Horizon pools for **Persistent Virtual Desktops**.

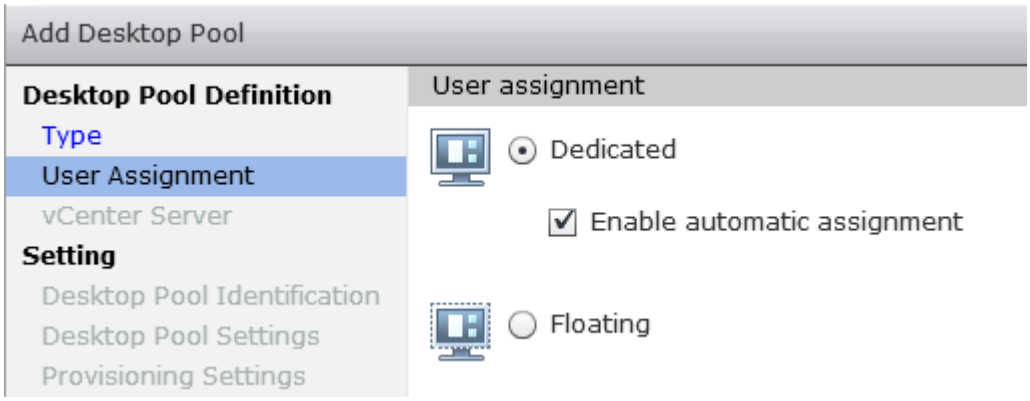
Procedure

1. In **VMware Horizon**, select **Automated Desktop Pool** in the **Type** panel of **Add Desktop Pool**.



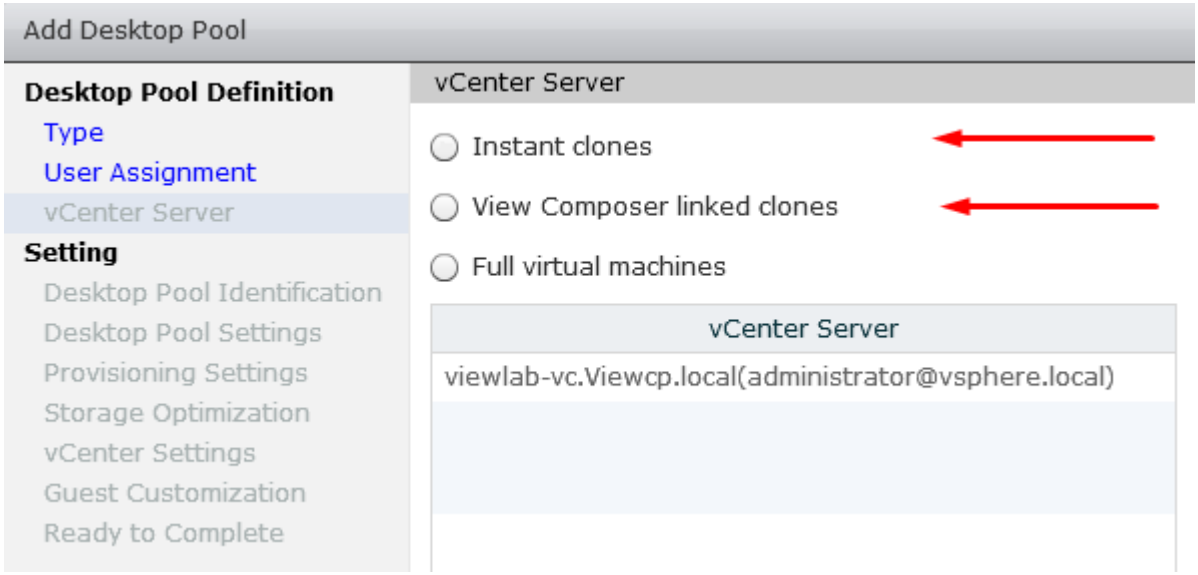
2. In the **User Assignment** panel, select **Dedicated**.

   Check **Enable automatic assignment**.

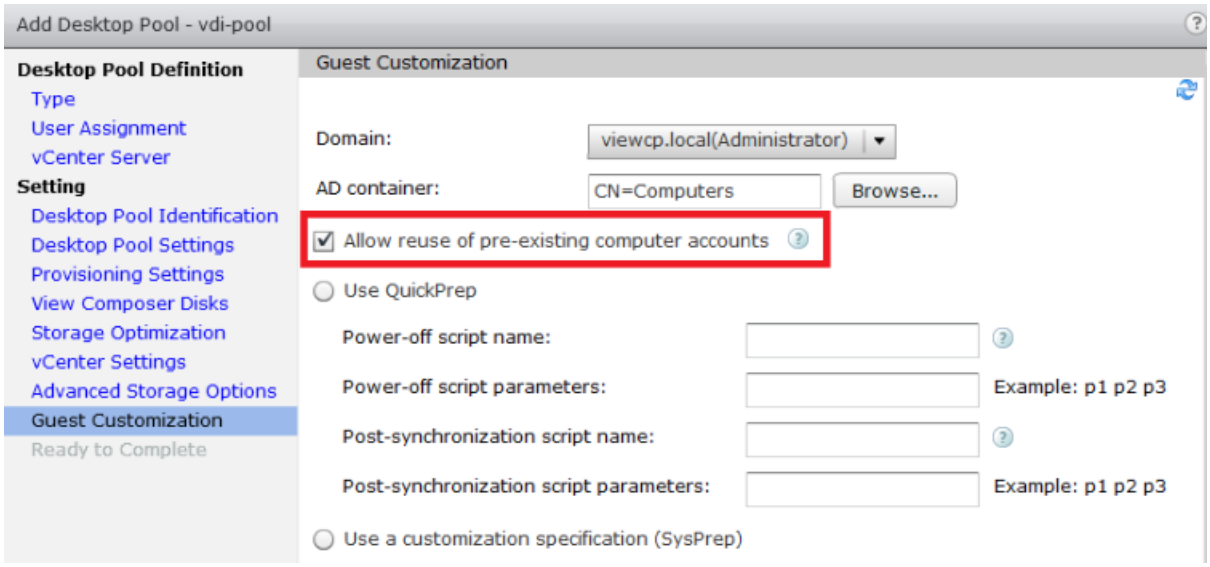


3. In the **vCenter Server** panel, select **Instant Clones** or **View Composer Linked Clone**.

   Full Clones are not currently supported.



4. In **Guest Customization** panel, select **Allow reuse of pre-existing computer account**.



Citrix XenDesktop Key Points

- When you select the **Operating System** type, use **Single-Session OS**.
- When you select **User Experience**, use a **dedicated** desktop experience.

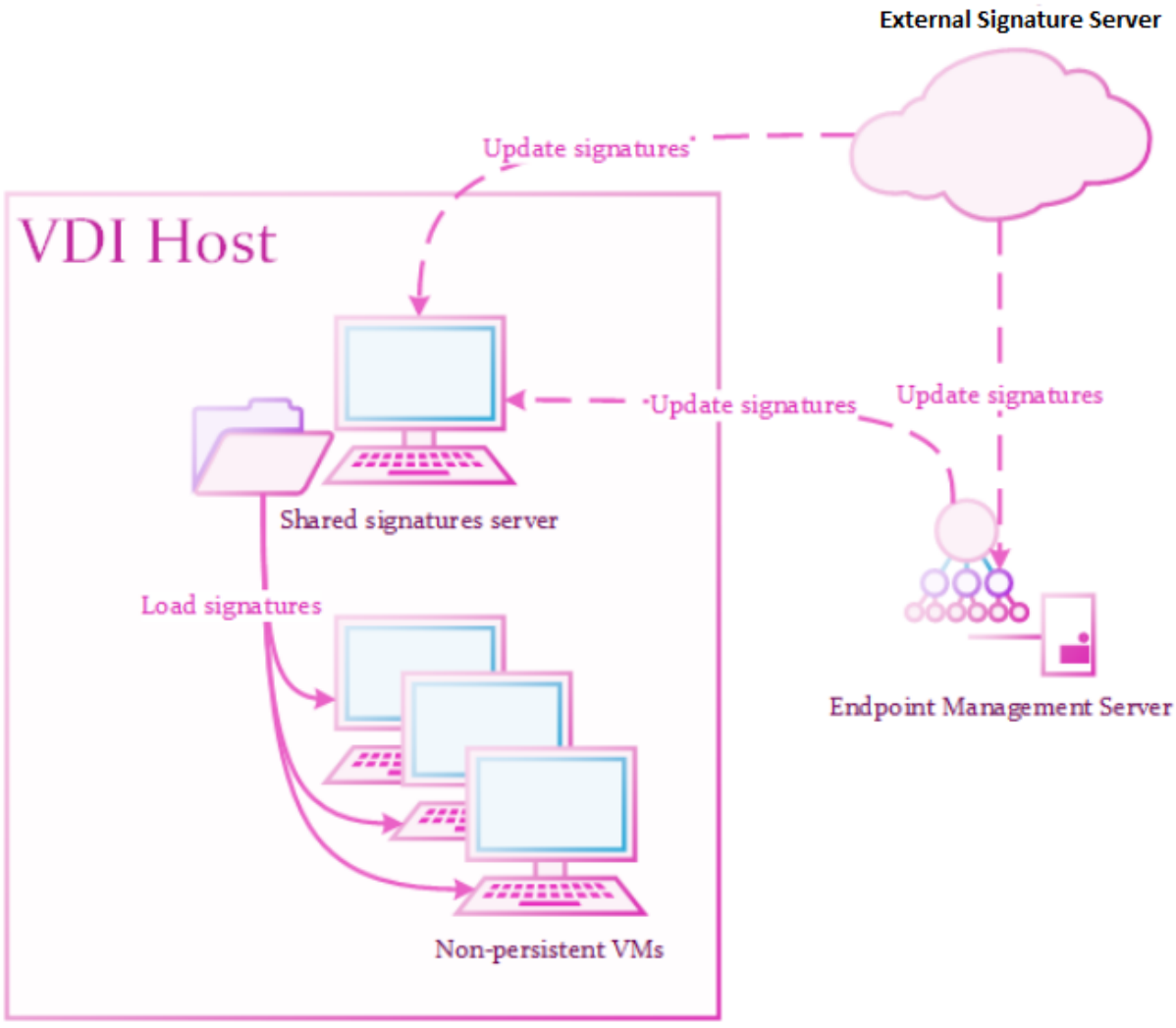
Configuring Clients for Non-Persistent Desktops

General

The Solution:

- One or more Signature Servers responsible to store the latest Anti-Malware signatures in a shared location.
- Many specially configured clients that load signatures from the shared folder.
- If the shared signatures server is not available, the client uses signatures from the golden image.

Note - All endpoints connected to the Shared Signature Server must be on the same domain.



Recommended Steps:

1. Configure a signature server machine.
2. Configure a client machine (golden image).
3. Create a test pool.
4. Deploy the production pool.

Shared Signatures Server

A Shared Signatures Server:

- Installs as a regular Endpoint Security Client and becomes a "signature server" later.
- Responsible for holding the latest Anti-Malware signatures.

  The signatures store in a read-only shared folder and update according to policy.
- Must run on a persistent virtual machine, preferably on the same storage as the clients.
- Must connect to the Endpoint Policy Server or the Internet to update signatures.

Configuring the Signatures Server

For the Endpoint Security Clients version E84.20 (and higher), you can configure the Signature Server with a policy.

Procedure

1. Create a new **Virtual Group**.
2. Assign a *Golden Image* machine to the new group.
3. From the left navigation panel, click **Policy**.
4. In the left pane, click **Threat Prevention**.
5. In the policy, clone the applicable **Threat Prevention** rule.
6. Assign the new **Threat Prevention** rule to the new **Virtual Group**.
7. In the right pane, click the **Web & Files Protection** tab.
8. Scroll down and click the **Advanced Settings** button.
9. From the left tree, click **Files Protection** > **Signature**.
10. In the **Shared Signature Server** section, select the “Set as shared signature server” and enter the local path of the folder.

    Example: `C:\Signatures`

    Note - If the folder does not exist, the endpoint creates it automatically.

11. Configure the applicable frequency in the **Frequency** section.
12. Click **OK**.
13. At the bottom, click **Save**.
14. At the top, click **Install Policy**.

Setup Validation

Wait 20 minutes to make sure:

- Anti-Malware Signatures version is current.
- Shared Signatures folder exists with Anti-Malware signatures.

  Important - If the folder is empty, the setup is not valid.

Client Machine Configuration for Non-Persistent Desktops

Creating a Basic Golden Image for Non-Persistent Desktops

See *"Basic Golden Image Settings" on page 241* for the procedure to create a basic golden image.

Configuring the Client Machine

For the Endpoint Security Clients version E84.20 (and higher), you can configure up the client machines (the golden image) by policy.

1. Disable the Anti-Malware Periodic Scan.

   See *"Appendix" on page 245*.

2. Configure signature source for the VDI client.

   Procedure

   a. Create a new **Virtual Group**.

   b. Assign a *Golden Image* machine to the new group.

   c. From the left navigation panel, click **Policy**.

   d. In the left pane, click **Threat Prevention**.

   e. In the policy, clone the applicable **Threat Prevention** rule.

   f. Assign the new **Threat Prevention** rule to the new **Virtual Group**.

   g. In the right pane, click the **Web & Files Protection** tab.

   h. Scroll down and click the **Advanced Settings** button.

   i. From the left tree, click **Files Protection** > **Signature**.

   j. In the **Shared Signature Server** section, enter the UNC of the shared folder.

   Example: `\\192.168.18.5\Signatures`

   k. Configure the applicable frequency.

   l. Click **OK**.

   m. At the bottom, click **Save**.

   n. At the top, click **Install Policy**.

Important:

- When you apply VDI settings through Policy to Golden Image, you must apply VDI settings through Policy to cloned Virtual Machines.

Post Setup Actions

- Make sure the Shared Signatures folder is accessible from the golden image and the folder has signatures.
- Make sure the Anti-Malware signatures are current.
- Scan for malwares with the latest signatures.

Creating a Pool for Non-Persistent Desktops

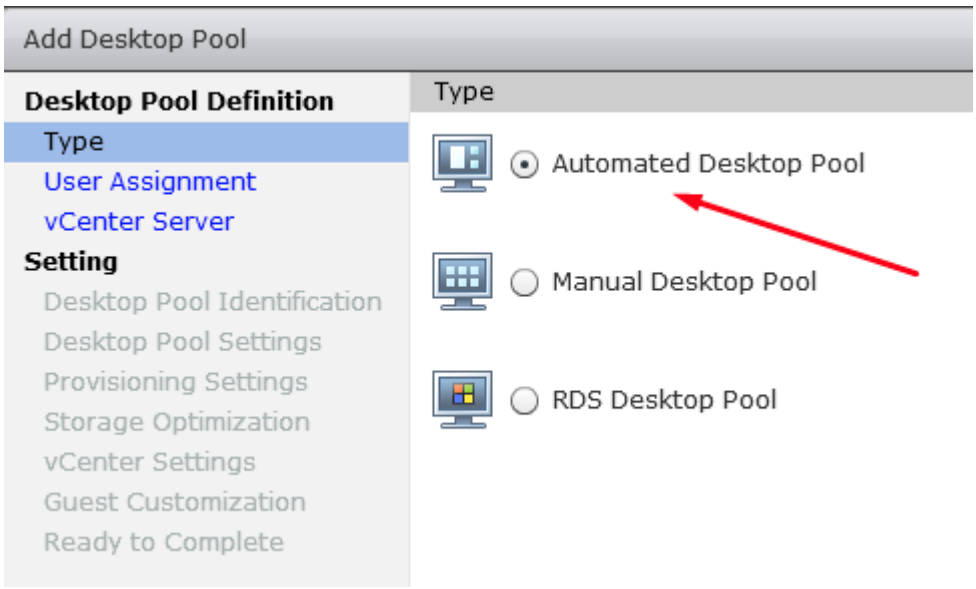
Note - Check Point recommends that each created pool will use a different machine naming pattern. This will prevent situations where Management Server has duplicate machine entries from different pools.

VMware Horizon Key Points

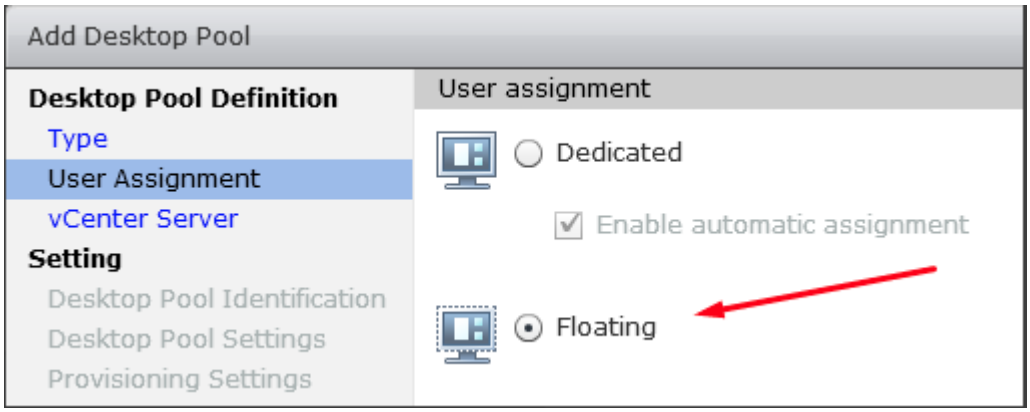
This procedure is mandatory to create supported Horizon pools for **Non-Persistent Virtual Desktops**.

Procedure

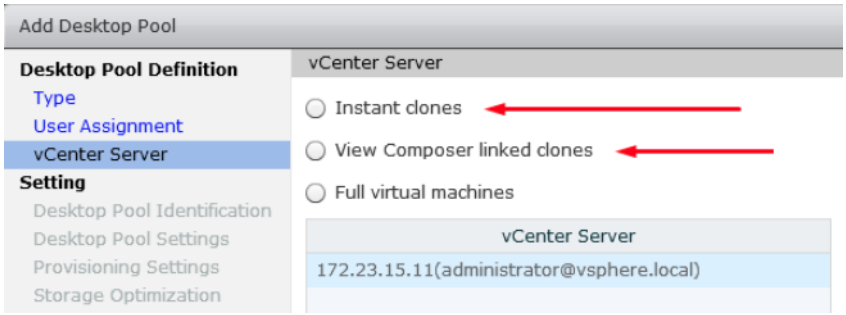
1. In **VMware Horizon**, choose **Automated Desktop Pool** in the **Type** panel of **Add Desktop Pool**.



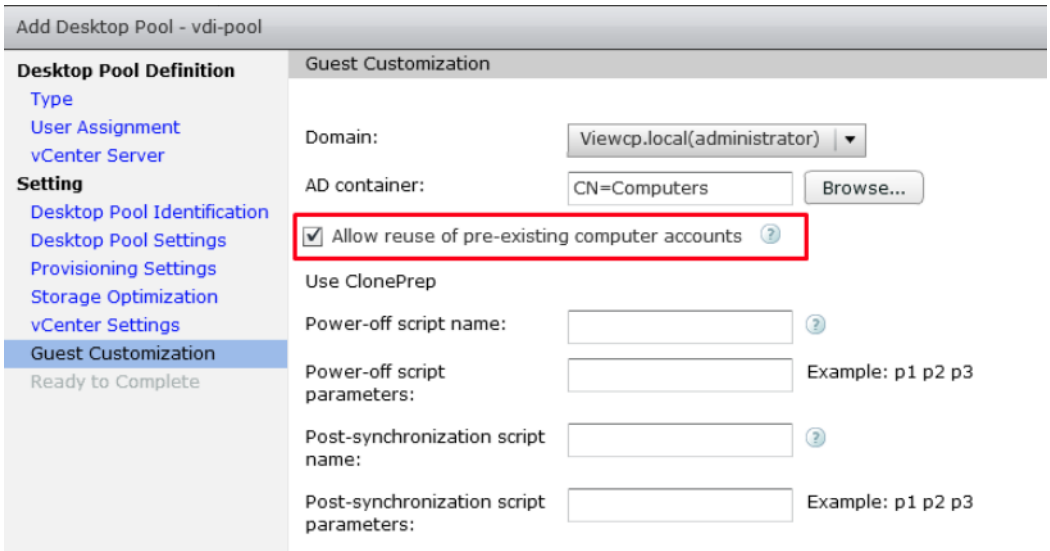
2. In the **User Assignment** panel, choose **Floating**.



3. In the **vCenter Server** panel, choose **Instant Clones** or **Linked Clones**.



4. In the **Guest Customization** panel, select **Allow reuse of pre-existing computer account**.



Citrix Xen-Desktop Key Points

- When you select the Operating System type, use Single-Session OS.
- When you select the User Experience type, use a non-dedicated desktop experience.

Pool Validation

Access a few cloned machines and make sure that:

- Machines connect to the Endpoint Security Management Server.
- Applicable Software Blades run.
- Anti-Malware Signatures are current.
- Machines appear on the Server User Interface.

Disabling the Anti-Malware Periodic Scan

"Anti-Malware Scan Storms" can occur when several anti-virus scans run simultaneously on multiple virtual machines on the same physical server. In such situation, a degradation of system performance is possible, which can affect disk I/O and CPU usage. It is then recommended that you disable the Anti-Malware periodic scan:

1. Go to the Policy Page.
2. In the right pane, click the **Web & Files Protection** tab.
3. Scroll down and click the **Advanced Settings** button.
4. From the left tree, select **Files Protection > Scan**.
5. In the **Perform Periodic Scan Every** field, select **Never**.

Software Blades for Non-Persistent Desktops

The Endpoint Security client capabilities for non-persistent virtual desktops are:

- **Anti-Malware**
  - Fully supported when configured with the **Shared Signatures Server**.
- **Compliance**, **Firewall and Application Control**, **Remote Access VPN**, and **URL Filtering**
  - Fully supported.
- **Forensics**
  - Partially supported.
    - The Forensics database contains data for the current session.
    - Forensics Reports generate as usual.

- **Threat Emulation and Anti-Exploit**
  - Partially supported.
    - Signatures are not in cache.
    - Signatures download for each new instance.
- **Anti-Bot**
  - Partially supported.
    - Signatures are not in cache.
    - Signatures download for each new instance.
    - Cached data (such as the URLs checked against **Threat-Cloud** and **Detection List**) are lost on logoff.
- **Ransomware "Honeypots"**
  - Partially supported.
    - Part of the Golden Image.
- **Behavioral Guard**
  - Partially supported.
    - Signatures are not in cache.
    - Signatures download for each new instance.
- **Full Disk Encryption** and **Capsule Docs**
  - Not supported for non-persistent desktops.
- **Media Encryption & Port Protection**
  - Fully supported with VMware Horizon running the Harmony Endpoint client version E86.40 and higher.
  - Fully supported with Citrix Provisioning Services (PVS) running the Harmony Endpoint client version E86.50 and higher.

Basic Golden Image Settings

A "Golden Image" is the base ("Master") desktop image. It is the model for clone images.

To create the Golden Image:

1. Install the Windows OS.
2. Configure the network settings:
    a. Configure the network settings to match your environment settings (DNS, Proxy).
    b. To verify that the configuration is correct, add it to your domain.
    c. Make sure you can ping Domain FQDN.
    d. Make sure you can ping Connection Server FQDN.
3. Install the required software and tools.
4. Install the latest Windows updates.
5. Optimize the Guest machine in one of these ways:
    a. Optimize the master image according to the Microsoft VDI Recommendation.
    b. Use the Vendor's specific optimization tool:
        - VMware - VMware OS Optimization Tool.
        - Citrix - Citrix Optimizer.

    Important - Make sure that you do not disable the Windows Security Center service.
6. Install the Virtual Delivery Agent (VDA).
    - VMware Horizon:
        - Version 7.10 supports up to 19H1.
        - Make sure that during installation you choose the correct settings (Linked clones or Instant Clones).
    - Citrix:
        - Make sure that during installation you choose the correct settings (MCS / PVS).

    Notes for Citrix PVS:
    - Before the first Endpoint installation, boot the machine from the network using the relevant vDisk in Read / Write mode.
    - When upgrading Endpoint in maintenance mode, make sure that you upgrade the vDisk through the golden image and not one of the clones.
    - The transfer of a clone back to the golden image is not supported.

7. Configure Trust with the Domain Controller:
   - Make sure that the *golden image* has a Trust Relationship with the Domain Controller.
   - You can use this PowerShell command:

     ```
     Test-ComputerSecureChannel
     ```
8. Install an Endpoint Security Client:
   a. Create an exported Endpoint client package.
   b. Install the Endpoint client package as administrator.
   c. Get the latest Anti-Malware signatures.

      Best Practice - Update manually with **Update Now** from the Endpoint tray icon at least once a day.
   d. Scan for malware.

      Best Practice - Scan manually with **Scan System Now** from the Endpoint tray icon for every signature update.
9. Shut down the Virtual Machine.
10. Save the snapshot.

Assigning Policies to VDI Pools

To assign specific behaviors to blades, you must configure policies.

Some policies assign by default to users, not machines.

Two options are available for assigning a policy to VDI machines:

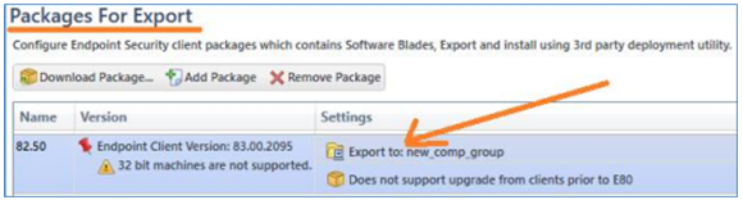
- **Assignment prior to pool creation**

  Assignment to a pre-defined computer group occurs during the Export Package phase.

  All clones from this Exported Package enter the computer group upon registration to the Endpoint Security Management Server.

  1. Create a new **Computer Group**.
     - In Endpoint Web Management Console:
     - In SmartEndpoint:

2. Export the applicable packages.
    - In Endpoint Web Management Console:
        a. From the left navigation panel, click **Policy**.
        b. In the **Deployment Policy** section, click **Export Package**.
    - In SmartEndpoint:
        a. Click the **Deployment** tab.
        b. Go to **Packages For Export**.
        c. Click **Export to:**



3. Assign the new **Computer Group** to a relevant policy.
    - In Endpoint Web Management Console:
    - In SmartEndpoint:
4. Install the exported package on the Golden Image.

- **Assignment after pool creation**

  Provision all VDI machines. Once the machines exist, assign them to a policy.

  1. Create a new **Virtual Group** and add all the relevant machines.
  2. Create a policy and assign it to the **Virtual Group**.

Limitations

- VDI Clients must be part of a domain. Workgroup configurations are not supported.
- FDE capability is not supported. Do not enable FDE in packages for Non-Persistent VDI machines.
- "Anti-Malware Scanning Storms" may occur when the Anti-Virus scan runs at the same time on multiple Virtual Machines on the same physical server. A serious degradation of the system performance is possible that can affect disk I/O and CPU utilization.
- The "**Repair**" push operation does not work for VDI machines.

- The Shared Signature Server does not share signatures with non-persistent desktops if you clear and select the **Set as shared signature server** checkbox in the **Policy** > **Web & Files Protection** > **Advanced Settings** > **Files Protection** > **Signature** window. To resolve this issue, uninstall and redeploy the Endpoint Security client on the Shared Signature Server.

Appendix

Disabling the Anti-Malware Periodic Scan

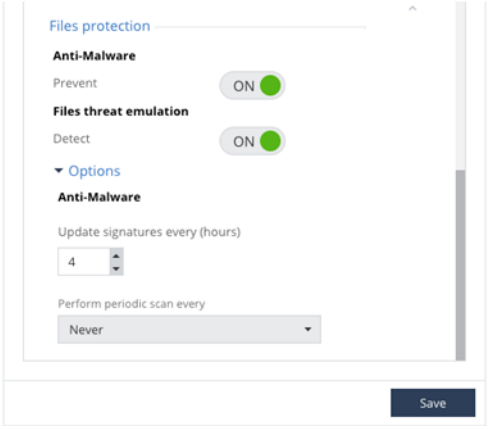
"Anti-Malware Scan Storms" can occur when anti-virus scans run at the same time on multiple virtual machines on the same physical server.

A degradation of system performance is possible that can affect disk I/O and CPU usage.

We recommend that you disable the Anti-Malware periodic scan in one of these ways:

In Endpoint Web Management

1. Go to the **Policy Page**.
2. In the right pane, click **Web & Files Protection**.
3. In the **Perform periodic scan every** field, select **Never**.



4. Click **Save**.
5. Install policy.

Configure the Windows Registry settings on the client machine

1. In Windows Registry, configure the value `0x0b` for the `AVSchedOf` key:
   - On 64-bit operating system:

     ```
     HKEY_LOCAL_
     MACHINE\SOFTWARE\Wow6432Node\CheckPoint\EndPoint
     Security\Anti-Malware\AVSchedOf=(DWORD)0x0b
     ```

   - On 32-bit operating system:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\EndPoint
     Security\Anti-Malware\AVSchedOf=(DWORD)0x0b
     ```

2. Restart the machine to restore Self-Protection.

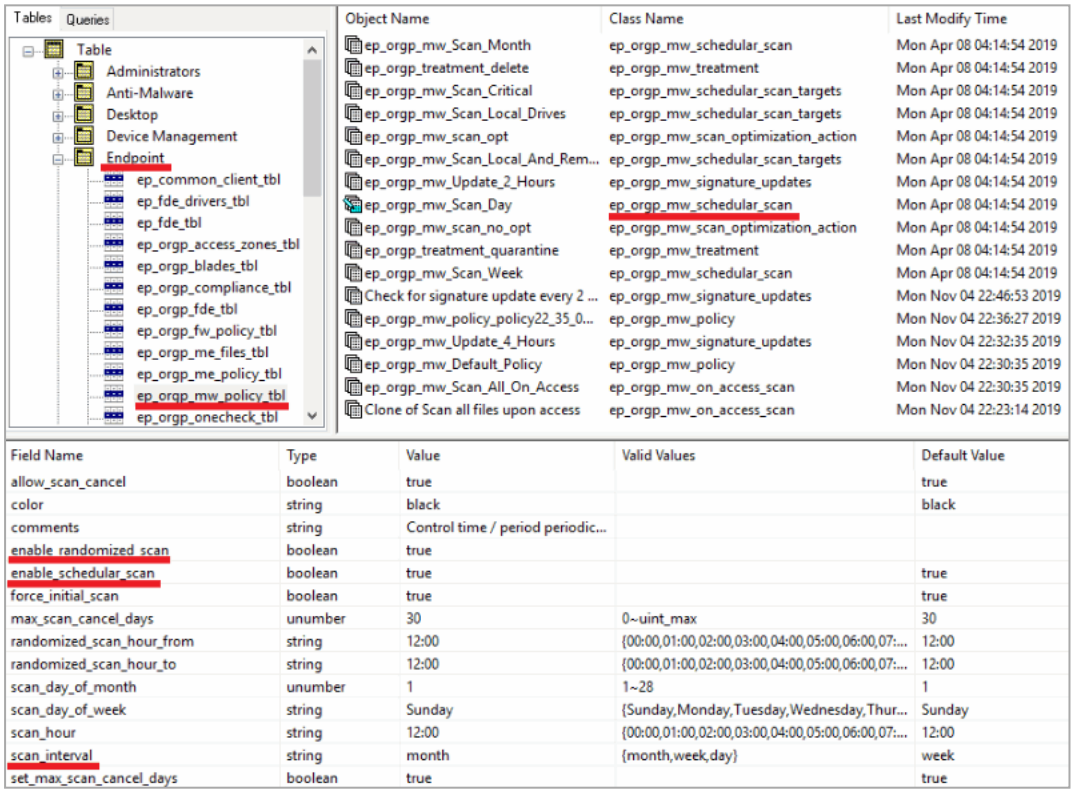
   Use the Compliance Software Blade to change the registry. See sk132932.

Advanced Settings for Persistent Desktops

This section shows how to configure clients manually for the Persistent VDI solution.

Use this approach if the "Policy Approach" is not available.

1. Disable the Anti-Malware Periodic Scan. See the instructions above.
2. If you cannot disable the Anti-Malware Periodic Scan, then enable the Anti-Malware Randomized Scan:
   a. Connect with the Database Tool (GuiDBEdit Tool) (sk13009) to the Endpoint Security Management Server.
   b. Configure the value `true` for the attribute `enable_randomized_scan`.
   c. Configure the value `true` for the attribute `enable_schedular_scan`.
   d. Configure the applicable value for the attribute `scan_interval`.



3. In SmartEndpoint, install policy.

Advanced Settings Non-Persistent Desktops

This section shows how to configure clients manually for the Non-Persistent VDI solution in the Signature Server and Signature Server Consumers roles.

Use this approach if the "Policy Approach" is not available.

Configuring the Shared Signatures Server

You can configure the Signature Server manually or with a script.

Manual Configuration

Create a Shared Folder

1. Create a folder to store the shared signatures.
2. Share the folder and grant read access to members of the Domain Computers' group.

Note - On Workgroup machines, the "SYSTEM" account does not have network login rights. This configuration is not supported.

Configure the Windows Registry Keys

1. Configure the value `0x01` for the key `VdiSignatureServer` (to configure the machine as "Shared Signatures Server"):
   - On 64-bit operating system:

     ```
     HKEY_LOCAL_
     MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint
     Security\Anti-Malware\VdiSignatureServer=(DWORD)0x01
     ```

   - On 32-bit operating system:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Endpoint
     Security\Anti-Malware\VdiSignatureServer=(DWORD)0x01
     ```

2. Configure the path to the shared signatures folder in the key `AVSharedBases`:
   - On 64-bit operating system:

     ```
     HKEY_LOCAL_
     MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint
     Security\Anti-Malware\AVSharedBases=
     (SZ)"DISK:\\Path\\To\\Shared\\Folder"
     ```

- On 32-bit operating system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Endpoint
Security\Anti-Malware\AVSharedBases=
(SZ)"DISK:\\Path\\To\\Shared\\Folder"
```

Notes:

- If you do not configure the path, then the default shared folder is:

```
C:\ProgramData\CheckPoint\Endpoint
Security\Anti-Malware\bases\shared
```

- The default shared folder exists after the first successful update.

3. Reboot the machine to restart the Anti-Malware blade.

Configuration with the Script

1. Download the Shared Signatures Server Configuration script file.
2. Execute the script on the Signature Server and follow the instructions.
3. Make sure the script finishes successfully.
4. Make sure you reboot the machine to restart the Anti-Malware blade.

Configuring the Client Machine

You can configure the Client Machine (the Golden Image) manually or with a script.

Manual Configuration

1. Disable the Anti-Malware Periodic Scan. See the instructions above.
2. In Windows Registry, configure the value `0x01` for the key `AVBasesScheme` (to enable the "Shared Signatures" scheme):
   - On 64-bit operating system:

     ```
     HKEY_LOCAL_
     MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint
     Security\Anti-Malware\AVBasesScheme=(DWORD)0x01
     ```

   - On 32-bit operating system:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Endpoint
     Security\Anti-Malware\AVBasesScheme=(DWORD)0x01
     ```

3. In Windows Registry, configure the path to the shared signatures folder in the key `AVSharedBases`:
   - On 64-bit operating system:

     ```
     HKEY_LOCAL_
     MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint
     Security\Anti-Malware\AVSharedBases=
     (SZ)"\\Server\FolderWithSharedSignatures"
     ```

   - On 32-bit operating system:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Endpoint
     Security\Anti-Malware\AVSharedBases=
     (SZ)"\\Server\FolderWithSharedSignatures"
     ```

   Notes:
   - If you do not configure the path, then the default shared folder is:

     ```
     C:\ProgramData\CheckPoint\EndpointSecurity\Anti-
     Malware\bases\shared
     ```

   - The default shared folder exists after the first successful update.
4. Reboot the machine or restart the Anti-Malware process.

Configuration with the Script

1. Download the Golden Image Configuration script file.
2. Execute the script on the Golden Image and follow the instructions.
3. Make sure the machine is rebooted.

Harmony Endpoint for Terminal Server / Remote Desktop Services

Terminal Server / Remote Desktop Service is a physical server that allows multiple users to log on and access desktops remotely (For example, from a PC).

Check Point Harmony Endpoint supports these servers through the Endpoint Security client E86.20 or higher:

- Microsoft Terminal Services
- Microsoft Remote Desktop Services
- Citrix Xen App (Formerly known as Virtual app)
- VMware Horizon App

Software Blades for Terminal Servers

- Anti-Malware
- Firewall and Application Control
- URL Filtering
- Anti-Bot
- Anti-Ransomware
- Behavioral Guard
- Forensics
- Threat Emulation and Extraction
- Anti-Exploit

Licensing

Licensing is per user. Each user is counted as a seat (using existing SKUs).

Limitations

- User-based policy is not supported. By default, computers will receive the **entire organization** policy unless you create a computer-based rule.
- By default, the Endpoint Security client icon is turned off in the notification area (system tray) for all the users logged on to the server. This is to prevent client notifications triggered by a specific user action sent to all users. User checks (For example, Malware detections, upgrade process and push operations) are not displayed. To turn on the Endpoint Security client icon in the notification area for a specific user, see step 3 in the procedure below.
- The **Logs** menu does not show user details. The Terminal Server shows all logged on users as *ntlocal*.
- Compliance Remediation **Run as User** is not supported. For more information, see *"Compliance" on page 143*.
- For the Anti-Malware capability:
  - Terminal Server exclusions does not support *User Environment Variables*.
  - Scanning and quarantine are supported only for a directory that can be accessed by the *System Account*.
  - Reporting - When infections are found, the Network Drive appears as "unknown" when a network drive cannot be accessed by *System Account*.
- Configure proxy settings for the Windows Server machine in the *System Account*.
- The **Full Disk Encryption** blade is not supported.
- The **Media Encryption** blade is not be supported.
- Windows Subsystem for Linux (WSL) is not be supported.
- Internet Explorer extension is not supported.

Deploying the Harmony Endpoint Client on a Terminal Server / Remote Desktop Service

Prerequisites

- Disable Windows Defender manually on the Terminal Server. For more information, see sk159373.
- Make sure you have the uninstall password for the Endpoint Security client. For more information, see *"Installation and Upgrade Settings" on page 163*.

Procedure

1. Install the Endpoint Security client package version E86.20 or higher to the Terminal Server. For more information, see *"Deploying Endpoint Clients" on page 27*.
2. Enable the Terminal Server mode on the Endpoint Security client through one of these methods:
   - Use the export package or Tiny Agent/ Initial Client:
     a. Open the Command Prompt window in **Administrator** mode and run:

        `msiexec /i eps.msi TS=1` OR `EndpointSetup.exe TS=1`.

     b. Once Client is installed, open the **Registry Editor** and navigate to

        `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint Security]` and make sure that the value of the **TSM** key is **dword:00000001**.

   - Manually change the registry:
     a. Navigate to *C:\Windows\Temp\<GUID>* and run *passdialog.exe* file.

     b. When prompted, enter the uninstall password.

     c. Open Registry Editor and navigate to

        `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint Security`. Add a new **TSM** key with the value **dword:00000001**.

     d. Reboot the server.

3. **Optional** - By default, the Endpoint Security client is turned off in the notification area (system tray) for all the users logged on to the server. This is to prevent sending notifications for a specific user action. To turn on the Endpoint Security client icon in the notification area for a specific user:
   a. Remove Self-Protection: Run the *passdialog.exe* file.
   b. When prompted, enter the uninstall password.
   c. Navigate to *C:\Program Files (x86)\CheckPoint\Endpoint Security\UIFramework\Bin\WUI* and run the *cptrayUI.exe* file.

Best Practice to Enable Software Blades

We recommend you to enable the Software Blade and the operating modes in the order shown in the table below.

- Add exclusions before you enable a Software Blade.
- Enable the Software Blade on a test group before you enable it on the organization level.

Order	Software Blade	Operating Mode	Applicable Group Level
1.1	Anti-Malware [1,2,3]	Prevent	Test
1.2		Prevent	Organization
2.1	Forensics	Prevent	Test
2.2		Off	Organization
3.1	Anti-Ransomware and Behavioral Guard[1]	Detect	Test
3.2		Detect	Organization
3.3		Prevent	Test
3.4		Prevent	Organization
4.1	Threat Emulation [1]	Prevent	Test
4.2		Prevent	Organization
5.1	Anti-Exploit [1]	Detect	Test
5.2		Detect	Organization
5.3		Prevent	Test
5.4		Prevent	Organization
6.1	Anti-Bot [1] and URL Filtering [1]	Detect	Test
6.2		Detect	Organization
6.3		Prevent	Test
6.4		Prevent	Organization

Order	Software Blade	Operating Mode	Applicable Group Level
7.1	Analysis and Remediation [1]	High	Test
7.2		High	Organization
7.3		Always	Test
7.4		Always	Organization

[1] Add exclusions before enabling the blade.

- For Citrix Anti-Malware, click here.
- For Microsoft Terminal Server Anti-Virus, click here.
- For FSLogix Anti-Virus, click here.

[2] Schedule the scan during non-active period.

[3] To add exclusions, see sk122706.

Recent Tasks

The running and the queued tasks appear in the Recent Tasks window at the top right of your screen.

Known Limitations

These are the current known limitations for Harmony Endpoint Web Management:

- In order to use WSL2 on Windows 10 and 11 with Harmony Endpoint installed you must alter your firewall configuration. These changes apply only when you use the firewall blade. For additional information please see sk177207.