



Workspace Security

20 April 2026

CHECK POINT ENDPOINT SECURITY

Administration Guide



Check Point Copyright Notice

© 2020 - 2026 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.

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](#).



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](#).

Related Documents

Document Title	Description
Endpoint Security Client for Windows User Guide	Provides the end-user instructions on how to use the Endpoint Security Client installed on Windows endpoints.
Endpoint Security Client for macOS User Guide	Provides the end-user instructions on how to use the Endpoint Security Client installed on macOS endpoints.
Endpoint Security Client for Windows MDM Deployment Guide	Describes how to deploy the Endpoint Security Client on Windows endpoints using a device management system.

Document Title	Description
Endpoint Security Client for macOS MDM Deployment Guide	Describes how to deploy the Endpoint Security Client on macOS endpoints using a device management system.
Endpoint Security POC Guide	Describes the process of setting up the Proof of Concept (POC) evaluation for Endpoint Security.

Revision History

Date	Description
20 April 2026	Added: Microsoft Intune Wipe and Windows Reset with Full Disk Encryption. See "Appendix D - Microsoft Intune Wipe and Windows Reset with Full Disk Encryption" on page 779 .
16 April 2026	Added Endpoint Security for Linux Runtime Configurations. See "Endpoint Security for Linux Runtime Configurations" on page 680 .
29 March 2026	Released Endpoint Security for Linux version 1.28.12 and added support for these Linux distributions: ■ Alma 9.7 ■ Alma 10.1 ■ Debian 13.2 ■ Debian 13.3 ■ Mint 22.2 ■ Mint 22.3 ■ Oracle 10.1 ■ Oracle 9.7 ■ Red Hat 9.7 ■ Rocky 10.1 ■ Rocky 9.7 ■ SLES 15 SP7 ■ SLES 16.0 ■ Ubuntu 25.10 See "Endpoint Security for Linux Overview" on page 660.

Date	Description
26 March 2026	Released Endpoint Security for Linux version 1.28.11 and added support for these Linux distributions: ■ Alma 9.7 ■ Alma 10.1 ■ Debian 13.2 ■ Debian 13.3 ■ Mint 22.2 ■ Mint 22.3 ■ Oracle 10.1 ■ Oracle 9.7 ■ Red Hat 9.7 ■ Rocky 10.1 ■ Rocky 9.7 ■ SLES 15 SP7 ■ SLES 16.0 ■ Ubuntu 25.10 See "Endpoint Security for Linux Overview" on page 660.
26 March 2026	Updated product names and product grouping to align with the new Check Point strategic pillars and portal navigation. No functional changes were made. Harmony Endpoint is now referred to as Check Point Endpoint Security.
09 March 2026	Added "Configuring Threat Emulation (TE) Appliance for Endpoint Security" on page 715.
18 November 2025	Released Endpoint Security for Linux version 1.26.8 and added support for these Linux distributions: ■ Red Hat Enterprise Linux (RHEL) 10.1 ■ Oracle Linux 10 ■ OpenSUSE Leap 16.0 ■ Mint 22.1 ■ Debian Linux 13 See "Endpoint Security for Linux Overview" on page 660.
22 August 2025	Support for Memory Dump has been added on Endpoint Security for Windows client version E89.05 and later. See "Performing Push Operations (Old User Interface)" on page 580.
22 August 2025	Added Managing Quarantined Files. See "Managing Quarantined Files" on page 340

Date	Description
3 June 2025	Support for Linux Mint 22 has been introduced in Endpoint Security for Linux starting with version 1.22.16. See "Endpoint Security for Linux Overview" on page 660 .
26 May 2025	Updated the "General" on page 353 topic.
25 April 2025	Added: ■ Static Signatures in "Web & Files Protection" on page 259. ■ Static Signatures (YARA) Logs in "Endpoint Security Logs" on page 567.
16 April 2025	Added information about the Endpoint Security for Linux version 1.22.12. See "Supported Linux Versions " on page 662 .
11 April 2025	Added information about how to delete machines from a virtual group. See "Managing Virtual Groups" on page 539 .
21 March 2025	Added the Installation on Semi-Isolated Environments with Super Node Proxy section in "Endpoint Security for Linux Overview" on page 660 .
12 March 2025	Updated information about how to enable GenAI Protect. See "Enabling GenAI Protect" on page 524 .
19 February 2025	Updated "Data Loss Prevention" on page 483 to add Ask action and Application destination type.
31 January 2025	■ Updated: • "Optimizing the Endpoint Security Client for Servers and Profiles" on page 336 • "Behavioral Protection" on page 286 ■ Added the Data Storage and Retention section. See "Endpoint Security Logs" on page 567.
27 January 2025	Updated "Endpoint Security for Linux Overview" on page 660 .
15 January 2025	■ Updated information about how to access the Endpoint Security Remediation Manager for Administrators utility. See "Quarantine Management" on page 337. ■ Updated information about how to find the UUID of labels in the New Microsoft Purview portal. See "Managing Microsoft Sensitivity Labels for DLP" on page 505. ■ Added a video about how to deploy Endpoint Security client using Microsoft Intune. See Video Tutorials.

Date	Description
24 December 2024	Added information about <i>"Smart Pre-Boot" on page 371</i> and <i>"Passwordless Pre-boot Authentication" on page 382</i> .
25 November 2024	Updated <i>"Reconnect Tool" on page 65</i> topic.
19 November 2024	Updated <i>"Supported Operating Systems for the Endpoint Security Client" on page 69</i> topic.
30 October 2024	Added Gen AI Protect to <i>"Data Loss Prevention" on page 483</i> .
26 October 2024	Added Customizing the UserCheck messages .
17 October 2024	Added Control Browser Notifications to the Advanced Browser Settings in <i>"Web & Files Protection" on page 259</i> .
10 October 2024	■ Updated Super-Node topic. ■ Added Managing Microsoft Sensitivity Labels for DLP in <i>"Data Loss Prevention" on page 483</i>.
30 September 2024	Added macOS Sequoia (15) to the <i>"Supported Operating Systems for the Endpoint Security Client" on page 69</i> .
16 September 2024	Updated the Unified Dashboard . See <i>"Viewing Operational Overview, Security Overview and Reports" on page 149</i> .
03 September 2024	Added Incognito mode to Advanced Browser Settings .
22 August 2024	Added <i>"Infinity AI Copilot" on page 1</i> .
13 August 2024	■ Added Disable Network URL filtering pop-up notifications if they originate from a browser session to URL Filtering, and Vulnerable Driver Protection to Advanced Capabilities. See <i>"Web & Files Protection" on page 259</i>. ■ Added Upload CPInfo reports to AWS S3 to Agent Settings. See <i>"Performing Push Operations (Old User Interface)" on page 580</i>.
02 July 2024	■ Updated <i>"Getting Started Walkthrough Wizard" on page 54</i>. ■ Added <i>"Endpoint Security Client Device Restart Requirements" on page 346</i>

Date	Description
24 June 2024	Added "Downloading Forensics Reports" on page 656 .
19 June 2024	Added: ▪ "Data Loss Prevention" on page 483. ▪ Data Loss Prevention column in "Supported Browsers for the Browser Extension" on page 87.
6 May 2024	Updated "Configuring Alerts" on page 130 to add "Advanced Alerts" on page 133
2 May 2024	Added Client Language for Default Client User Interface. See "User Interface" on page 348
26 April 2024	Added video tutorial for automatic patch updates. See "Detecting Common Vulnerabilities and Exposures" on page 471 .
18 April 2024	Updated Disable Capabilities in "General" on page 353 . Added Advanced Capabilities . See "Web & Files Protection" on page 259 and "Configuring the Threat Prevention Policy" on page 248 .
16 April 2024	Added: ▪ Using Reconnect tool without uninstall password. See "Without Agent Uninstall Password (Recommended)" on page 66 ▪ Helpdesk Level 3. See "Specific Service Roles" on page 58 ▪ "Software Deployment Policy Template" on page 762 for MSSP.
19 March 2024	Added "Templates for Child Accounts" on page 756 (MSSP).
13 March 2024	Added: ▪ Enable patch updates (Automatic Patch Updates). See Detecting Common Vulnerabilities and Exposures. ▪ Admin Comment column. See "Viewing Computer Information" on page 173.
13 February 2024	Added "License Violation" on page 53 .
22 January 2024	Added: ▪ "Managing Microsoft Entra ID Scanners" on page 546. ▪ "Viewing Device Hardware Information" on page 182 ▪ Chained exclusions in "Smart Exclusions" on page 309

Click here to view the Revision History for 2023

Date	Description
18 December 2023	Added "Custom Settings" on page 271.
7 December 2023	Added: ▪ Video tutorial for Run Diagnostics. See "Performing Push Operations (Old User Interface)" on page 580. ▪ "Appendix B - Uninstalling the Endpoint Security Client (For macOS and Windows)" on page 771
20 November 2023	▪ Updated supported regions for "Threat Hunting" on page 647. ▪ Added video tutorial for "Viewing Endpoint Posture" on page 218.
17 November 2023	Added "Smart Exclusions" on page 309.
31 October 2023	Added video tutorials for: ▪ Automatic Deployment of Endpoint Clients"Using the Tiny Agent" on page 94. ▪ Creating a Custom Dashboard. See "Viewing Operational Overview, Security Overview and Reports" on page 149. ▪ Generating Reports. See "Viewing Operational Overview, Security Overview and Reports" on page 149.
26 October 2023	Updated Managing Licenses for AWS Marketplace .
10 October 2023	Added Helpdesk Level 1 and Helpdesk Level 2 Specific Service Roles.
18 October 2023	Application Scan now supports macOS. See "Application Control" on page 443.
10 October 2023	Added "Quarantine Management" on page 337.
3 October 2023	Added: ▪ "MSSP Essentials" on page 732. ▪ "MSSP Custom Dashboard" on page 737.
22 September 2023	Added "Certificate Management" on page 646.

Date	Description
11 September 2023	Added: ▪ "Patches By Status" on page 221. ▪ Posture Last Scan Status. See Table Filters and Column Description in "Viewing Computer Information" on page 173. ▪ New columns to "Vulnerability Assessment Table" on page 221.
7 September 2023	Added: ▪ Browser Status ▪ Anti-Bot Last Update See Table Filters and Column Description in "Viewing Computer Information" on page 173.
4 September 2023	Added "Smart App Control" on page 767 for Windows 11.
1 September 2023	Added "Global Exclusions" on page 754 for MSSP.
30 August 2023	Added "Reconnect Tool" on page 65 for macOS.
9 August 2023	Updated Policy Mode. See "Configuring the Threat Prevention Policy" on page 248.
1 August 2023	Added Disable Notification. See "Zero Phishing" on page 271.
28 July 2023	Added deploying the Endpoint Security Client "Using the Vanilla Client" on page 99.
24 July 2023	Added: ▪ Schedule Report. See "Viewing Operational Overview, Security Overview and Reports" on page 149. ▪ "Adding a New VPN Site to an Exported Package" on page 116.
20 July 2023	Added: ▪ Anti-Malware License Expiration Date column. See "Asset Management View" on page 173. ▪ Anti-Malware client's license is about to expire alert. See "Configuring Alerts" on page 130.

Date	Description
17 July 2023	Added Unified and Custom Dashboard. See "Viewing Operational Overview, Security Overview and Reports" on page 149 .
12 July 2023	Added Exporting Virtual Groups . See Managing Virtual Groups .
28 June 2023	Added Browser Status to the Table Filters and Column Description. See "Asset Management View" on page 173 .
20 June 2023	Added: ▪ Customs View. See "Viewing Computer Information" on page 173. ▪ "Override Default Files Actions" on page 270. ▪ "Supported Browsers for the Browser Extension" on page 87.
5 June 2023	Added "Reports for MSSP" on page 753 .
31 May 2023	Added Scan Targets and Scan Target Exclusions . See "Scan" on page 280 .
23 May 2023	Reconnect Tool is now supported for macOS with client version E87.50 or higher. See "Reconnect Tool" on page 65 .
11 May 2023	▪ Updated "Viewing Endpoint Posture" on page 218 and "Configuring Posture Assessment Settings" on page 472 for patch management.  Note - Patch Management feature is available only for customers in the Early Availability (EA) program. ▪ Added information on US-DHS and EU regulations compliant Anti-Malware blade. See "Anti-Malware Settings" on page 127. ▪ Added new fields: ◦ Low memory mode. See "Advanced Behavioral Guard & Anti-Ransomware Settings" on page 290. ◦ Scan On Idle. See "Scan" on page 280.
19 April 2023	Added information about moving a device or user from one virtual group to another. See Managing Virtual Groups .
18 April 2023	Updated the Policy Mode settings. See "Configuring the Threat Prevention Policy" on page 248 .
6 April 2023	Added "Capabilities of Offline Endpoint Security Client" on page 529 .
3 April 2023	Added new Reports . See "Viewing Operational Overview, Security Overview and Reports" on page 149 .

Date	Description
29 March 2023	▪ Connection Awareness now supports macOS. See "Connection Awareness" on page 354. ▪ Added "Working with the Computers Table" on page 182.
13 March 2023	▪ Added new columns: Threat Hunting Status and Threat Hunting Error Description. See "Viewing Computer Information" on page 173. ▪ Added support for folder actions to the File Actions push operation. See "Performing Push Operations (Old User Interface)" on page 580.
08 March 2023	Endpoint Security supports macOS Ventura 13 operating system for endpoints. See "Supported Operating Systems for the Endpoint Security Client" on page 69
27 February 2023	▪ Added new feature "Sending Security Reports" on page 579. ▪ Added file size for Upload and emulate files under. See "Emulation Environments" on page 269.
13 February 2023	▪ Added Custom Rules support for the Application Control policy. See "Configuring Application Permissions in the Application Control Policy" on page 449. ▪ Added "Show Last Diagnostics Report" on page 217
7 February 2023	▪ Added Policy Modes to "Configuring the Threat Prevention Policy" on page 248 ▪ Added Anti-Bot and Threat EmulationAnti-Exploit exclusions. See Adding Exclusions to Rules.
6 February 2023	▪ Added "Creating User Overrides (UserCheck)" on page 399. ▪ Added "Viewing Events" on page 410. ▪ You can allow all, essential or custom select the ports. See "Port Protection" on page 423
31 January 2023	▪ Added information about the new feature Scan local HTML files. See "Credential Protection" on page 271. ▪ Added information about the new event Accessing a local HTML file. See "Customized Browser Block Pages" on page 349. ▪ Added information about the new feature Browser Settings. See "Web & Files Protection" on page 259.
20 January 2023	Added a new Appendix. See "Appendix A - Deploying Endpoint Security Client using SCCM" on page 770 .

Date	Description
18 January 2023	Added information about how to manage widgets in the Security Dashboard for MSSP. See Security Dashboard. Added a Detect & Alert to Password Reuse Protection . See "Credential Protection" on page 271 .
11 January 2023	Added information about downloading reports. See "Viewing Operational Overview, Security Overview and Reports" on page 149 .
10 January 2023	Added information about Posture Management. See "Detecting Common Vulnerabilities and Exposures" on page 471 and Viewing Endpoint Posture. Note - This feature is available only to customers in the Early Availability program.

Click here to view the Revision History for 2022

Date	Description
29 December 2022	- Added "Authenticated Proxy" on page 353 , "Disable Capabilities" on page 361, and "Push Operations" on page 363. - Updated "Managing Licenses" on page 50.
06 December 2022	Remote Command, Isolate Computer and Release Computer push operations are supported for macOS-based endpoints. See "Performing Push Operations (Old User Interface)" on page 580 .
01 December 2022	Added Initial Encryption information in "Check Point Disk Encryption for Windows" on page 366 .
11 November 2022	Added a new information on optimizing the Endpoint Security clients for servers. See "Optimizing the Endpoint Security Client for Servers and Profiles" on page 336 .
23 November 2022	- Added a note about supported version for Run Diagnostics. See "Performing Push Operations (Old User Interface)" on page 580. - Updated Windows syntax for Anti-Ransomware and Behavioral GuardForensics exclusions. See Forensics -> Anti-Ransomware and Behavioral Guard Exclusions. - Added information about extensive data collection. See "Advanced Behavioral Guard & Anti-Ransomware Settings" on page 290.
22 November 2022	Added the Endpoint Security Client versions and policy mode supported for Block Volume Encryption tools (BitLocker and Similar Tools). See "Behavioral Protection" on page 286 .

Date	Description
11 November 2022	Added information about Operational Overview . See "Viewing Operational Overview, Security Overview and Reports" on page 149 .
09 November 2022	- Files Threat Emulation supports Detect, Prevent and Off modes. See "Files Protection" on page 275. This is supported with Endpoint Security client version E86.80 and higher. - Added how to install remotely using third-party tools. See "Remote Installation of Initial Client" on page 118. - Added information about Run Diagnostics. See "Performing Push Operations (Old User Interface)" on page 580. - Added a note to Randomize scan time in VDI. See "Configuring Clients for Persistent Desktops" on page 689.
4 November 2022	Added supported file types for Threat Emulation. See "Download (Web) Emulation & Extraction " on page 266 .
21 October 2022	Added information about Security view for MSSP. See Security Dashboard.
18 October 2022	- Added information about Token-Limited Installation. See "Manual Deployment of Endpoint Clients" on page 106 and "Installation Token" on page 93. - You can export operational and threat analysis reports to review and take appropriate counter measure. See Exporting Reports.
14 October 2022	Updated Asset Management view. See "Viewing Computer Information" on page 173 .
10 October 2022	Added support for the Endpoint Security client deployment on Linux. See "Automatic Deployment of Endpoint Clients" on page 94 and "Manual Deployment of Endpoint Clients" on page 106 .
03 October 2022	Added a limitation related to Shared Signature Server for non-persistent desktops. See "Limitations" on page 703 .
30 September 2022	Updated "Files Protection" on page 275 for the supported archive file formats by the Anti-Malware scan in the E1 and E2 blades.
13 September 2022	Added information about filters. See "Viewing Computer Information" on page 173 .

Date	Description
01 September 2022	Added information about Search and Fetch files, Registry Actions, File Actions, VPN Site, Collect Process push operations. See "Viewing Computer Information" on page 173 and "Performing Push Operations (Old User Interface)" on page 580 .
25 August 2022	- Added information that you can now share a download link with users to download the Tiny Agent. See "Automatic Deployment of Endpoint Clients" on page 94. - Added a new method to add exclusions from Security Overview. See Adding Exclusions from Security Overview.
28 July 2022	Added information about Delete, Recover, and Terminate computer actions. See "Viewing Computer Information" on page 173 .
27 July 2022	Updated "Viewing Computer Information" on page 173 for 2FA authentication to perform push operation.
26 July 2022	Added support for sending forensics data to third-party data analytics tool. See "Sending Forensics Data to Third-Party Analytics Tool" on page 656 .
22 July 2022	Added supported for migrating an on-premise Endpoint Security database to Endpoint Security on Check Point Portal. "Migrating an On-premises Security Management Server to Endpoint Security" on page 88 .
18 July 2022	Updated Adding Exclusions to Rules for the new method to add and edit an exclusion.
14 July 2022	Updated "Uninstalling Third-Party Anti-Virus Software Products" on page 147
13 July 2022	- Added information about the new "Web & Files Protection" on page 259. - Added three new options for "Web & Files Protection" on page 259. - 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 94 .

Date	Description
07 June 2022	Updated "Configuring Clients for Non-Persistent Desktops" on page 693
17 May 2022	Updated "Viewing Computer Information" on page 173 about viewing click logs by IP address.
17 May 2022	Updated Adding Exclusions to Rules
09 May 2022	Added information on Network URL Filtering in "Web & Files Protection" on page 259
4.May 2022	Added "Browser Settings" on page 166
31 March 2022	Added "Supported Operating Systems for the Endpoint Security Client" on page 69.
07 March 2022	Added "Compliance" on page 456.
04 March 2022	Added "Uninstalling Third-Party Anti-Virus Software Products" on page 147.
03 March 2022	Added "Endpoint Security for Terminal Server / Remote Desktop Services" on page 709.
03 March 2022	SUSE Linux enterprise server (SLES) and OpenSUSE are supported only with the Anti-Malware blade. Refer "Endpoint Security for Linux Overview" on page 660.
25 February 2022	Added Managing Browser Security.
25 February 2022	Updated "Configuring Clients for Non-Persistent Desktops" on page 693
07 February 2022	Added "Customized Browser Block Pages" on page 349 to the "User Interface" on page 348 topic.
28 January 2022	▪ Updated Managing Licenses. ▪ Updated Web and Files Protection.
21 January 2022	Updated Helpdesk User roles.
19 January 2022	Updated: Password Synchronization

Date	Description
18 January 2022	Updated: Adding Exclusions to Rules .
11 January 2022	Updated: Client User Interface Settings Configuring the Threat Prevention Policy
9 January 2022	Updated: VDI Configure Clients for Non Persistent Desktops
6 January 2022	Added: IOC Management Updated: Endpoint Security for Linux Overview Endpoint Security for Linux Commands
5 January 2022	Updated: Getting Started
4 January 2022	Removed: VDI-Appendix 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 Introduction
3 January 2022	Updated: FileVault Encryption for
2 January 2022	Updated: Policy Operation

Click here to view the Revision History for 2021

Date	Description
30 December 2021	Updated: Endpoint Security for Linux Overview Deploying Endpoint Security for Linux Endpoint Security for Linux CLI Commands
22 December 2021	Updated: Configuring the Treat Prevention Policy Connected, Disconnected and Restricted Rules
21 December 2021	Updated: Endpoint Security for Linux Overview

Date	Description
19 December 2021	Updated: Password Synchronization
15 December 2021	Updated: Authentication before the Loads (Pre boot)
13 December 2021	Added: Super Node
12 December 2021	Added: VDI Overview
11 December 2021	Updated: <i>Adding Exclusions to Rules</i>
9 December 2021	Added: Policy Operation
9 December 2021	Updated: Deploying Endpoint Security for Linux
2 December 2021	Updated: Introduction Updated: Performing Push Operations Updated: Deploying Endpoint Clients
29 November 2021	Updated: Performing Push Operations
14 November 2021	Updated: Configuring Client Settings Updated: Connected, Disconnected and Restricted Rules Added: Connection Awareness
10 November 2021	Updated: <i>"Connected, Disconnected and Restricted Rules" on page 478</i>
07 November 2021	Updated: Active Directory Authentication
04 November 2021	Updated: Client User Interface Settings
03 November 2021	Updated: Introduction Updated: Setting Deployment Agent

Date	Description
02 November 2021	Updated: "Configuring Endpoint Policy" on page 247
01 November 2021	The Computer Management view on the left navigation panel was renamed to Asset Management . Updated: "Configuring Endpoint Policy" on page 247
31 October 2021	Updated: "Configuring Endpoint Policy" on page 247
31 October 2021	Updated: "User Interface" on page 348
28 October 2021	Updated: Configuring the Data Protection Policy
21 October 2021	Updated: Giving Remote Help to FDE Users Authentication before OS Loads Pre boot
14 October 2021	Updated: Deploying Endpoint Clients
13 October 2021	Updated: Introduction
11 October 2021	Updated: "Configuring Media Encryption & Port Protection" on page 394 "Advanced Settings for Media Encryption" on page 415 Media Encryption Remote Help Media Encryption Access Rules
10 October 2021	Added: "Recent Tasks" on page 768
07 October 2021	Updated: "Known Limitations" on page 769 "Connected, Disconnected and Restricted Rules" on page 478
01 October 2021	Updated: ■ Adding Exclusions to Rules ■ "Automatic Deployment of Endpoint Clients" on page 94 ■ "Remotely Installing the Initial Client" on page 123

Date	Description
26 September 2021	Updated: ▪ "Configuring Client Settings " on page 347
13 September 2021	Updated: ▪ "BitLocker Encryption for Windows Clients" on page 375
02 September 2021	Added: ▪ "User Authentication to Endpoint Security Clients (OneCheck)" on page 378 ▪ "Configuring Client Settings " on page 347
31 August 2021	Added: ▪ "Connected, Disconnected and Restricted Rules" on page 478 Updated: ▪ "Web & Files Protection" on page 259
05 August 2021	Added: ▪ "Installation Token" on page 93 Updated: ▪ "Manual Deployment of Endpoint Clients" on page 106
14 July 2021	Updated: ▪ Managing Users in Check Point Endpoint Security ▪ "Developer Protection" on page 454
22 April 2021	Rebranded the product name across the Administration Guide - from SandBlast Agent to Harmony Endpoint.
06 April 2021	Updated: ▪ "Exporting Logs" on page 576
29 March 2021	Added: ▪ "Application Control" on page 443
22 March 2021	Updated: ▪ "Configuring Client Settings " on page 347 ▪ "Endpoint Security for Linux" on page 659

Date	Description
11 March 2021	Added: ▪ "Configuring Media Encryption & Port Protection" on page 394 Updated: ▪ "Viewing Computer Information" on page 173 ▪ "Exporting Logs" on page 576
25 February 2021	Updated: ▪ Registering to the Check Point Portal ▪ "Creating a New Endpoint Management Service" on page 50 ▪ "Managing Firewall Objects and Groups" on page 438 ▪ "Configuring Alerts" on page 130
23 February 2021	Rebranded the product name. Updated: ▪ "Configuring Client Settings " on page 347
22 February 2021	Added: ▪ "Endpoint Security for Linux" on page 659
08 February 2021	Updated: ▪ Managing Licenses ▪ "BitLocker Encryption for Windows Clients" on page 375 ▪ "Configuring Alerts" on page 130 ▪ "Performing Push Operations (Old User Interface)" on page 580
07 January 2021	Added ▪ "Firewall" on page 431

[Click here to view the Revision History for 2020](#)

Revision History	Description
11 November 2020	Added: ▪ "Remote Installation of Initial Client" on page 118 ▪ "Threat Hunting" on page 647 Updated: ▪ "Exporting Logs" on page 576

Revision History	Description
04 November 2020	First release of this document. The Endpoint Security service in the Check Point Portal was updated. This Endpoint Security Administration Guide replaces these: ▪ Endpoint Security Management Platform Administration Guide ▪ Endpoint Security Cloud Management Platform Administration Guide

Table of Contents

Introduction to Endpoint Security	45
API Support	46
Endpoint Security Management API	46
Getting Started	47
Creating an Account in the Check Point Portal	47
MSSP Account	47
Accessing the Endpoint Security Administrator Portal	48
Creating a New Endpoint Management Service	50
Managing Licenses	50
User Center	50
Amazon Web Services Marketplace	52
Activating the License	53
License Violation	53
Getting Started Walkthrough Wizard	54
Specific Service Roles	58
Reconnect Tool	65
Windows	65
macOS	66
Without Agent Uninstall Password (Recommended)	66
With Agent Uninstall Password	67
Supported Operating Systems for the Endpoint Security Client	69
Microsoft Windows	69
macOS	71
Linux	72
Supported Browsers for the Browser Extension	87
Migrating an On-premises Security Management Server to Endpoint Security	88
Use Case	88

Prerequisites	88
Known Limitationsc	89
Migrating to Endpoint Security	89
Deploying Endpoint Clients	91
Installation Token	93
Automatic Deployment of Endpoint Clients	94
Automatic Deployment of Endpoint Clients	94
Using the Tiny Agent	94
Troubleshooting Issues with the Tiny Agent on Windows OS	98
Using the Vanilla Client	99
Deployment Rules	103
Manual Deployment of Endpoint Clients	106
Using the Export Package	106
Using the Offline Installation	113
Installing the Exported Package or Client	115
Adding a New VPN Site to an Exported Package	116
Remote Installation of Initial Client	118
Using Third-Party Tools	118
Using Push Operation	118
Setting the Deployment Agent	119
Certificates and DNS	120
Privileges	122
Setting the Target Devices	122
Remotely Installing the Initial Client	123
Security Considerations	125
Progress of Installation and Error Handling	125
Ports and Permissions	127
Upgrades	127
Anti-Malware Settings	127
Heartbeat Interval	129

Configuring Alerts	130
Basic Alerts	130
Configuring Basic Alert Messages	130
Configuring an E-mail Server	132
Advanced Alerts	133
Configuring Advanced Alerts	133
Duplicating an Advanced Alert	142
Editing or Creating a Notification Profile	143
How to Verify that Endpoint Security can Access Check Point Servers	146
Uninstalling Third-Party Anti-Virus Software Products	147
Viewing Operational Overview, Security Overview and Reports	149
Unified Dashboard	149
Custom Dashboard	149
Creating a Custom Dashboard	150
Managing a Custom Dashboard	153
Operational Overview	154
Active Endpoints	154
Desktops	155
Laptops	155
Deployment Status	156
Pre-boot Status	156
Encryption Status	157
Anti-Malware Update	157
Operating System	158
Alerts	158
Security Overview	159
Reports	159
Generate Report	160
Scheduled Reports	162
Announcements	165

Browser Settings	166
Disabling Incognito Mode, BrowserGuest Mode, and InPrivate Mode	166
Overview	166
Chrome on Windows	166
Firefox on Windows	166
Microsoft Edge on Windows	167
Brave on Windows	167
Chrome on macOS	168
Firefox on macOS	168
Microsoft Edge on macOS	168
Enabling the Browser Extension on a Browser with Incognito or InPrivate Mode	169
Ending the Browser Process Running in the Background	169
Browser Extension Pinning	170
Managing Accounts in the Check Point Portal	171
Managing Browser Security	172
Overview	172
Limitations	172
Viewing Computer Information	173
Asset Management View	173
Select a View	173
Creating a Custom View	174
Status Icon	174
Filters	175
Working with the Computers Table	182
Viewing Device Hardware Information	182
Managing Computers	183
General Actions	183
Push Operations	186
Diagnostics	216
Full Disk Encryption	217

Remote Help and Recovery	218
Viewing Endpoint Posture	218
Vulnerabilities by Severity	219
Top 5 Risky Apps	220
Top Vulnerable Devices	220
Patches By Status	221
Vulnerability Assessment Table	221
Patch Status Messages	226
Device Details Widget	229
CVE Details Widget	229
Scanning Devices	230
Mitigating Vulnerable CVEs	230
Isolating a Device	230
Applying the Patch for CVEs	231
Verifying the Applied Patch	232
Managing Devices	232
Managing Storage and Peripheral Devices	233
Managing Storage Device Groups	240
Using Wild Card Characters	241
Viewing Events	242
Configuring Endpoint Policy	247
Configuring the Threat Prevention Policy	248
Unified Policy	248
Parts of the Policy Rule Base	249
Threat Prevention Policy Toolbar	249
Policy Mode	249
Updating a Predefined Policy Mode	257
Web & Files Protection	259
URL Filtering	259
Deny List	265

Download (Web) Emulation & Extraction	266
Unsupported Files	269
Additional Emulation Settings:	269
Emulation Environments	269
Override Default Files Actions	270
Custom Settings	271
Download Emulation and Extraction	271
Credential Protection	271
Zero Phishing	271
Password Reuse Protection	272
Safe Search	273
Search Reputation	273
Force Safe Search	274
Files Protection	275
Advanced Settings	278
Files Protection	279
General	279
Signature	280
Scan	280
Threat Emulation	282
Advanced Capabilities	283
Browser Settings	284
Pin Extension	284
Control Browser Notifications	284
Incognito Mode	284
Behavioral Protection	286
The Anti-Bot Component	286
Configuring Anti-Bot	287
Advanced Anti-Bot Settings:	287
The Behavioral Guard & Anti-Ransomware Component	288

Advanced Behavioral Guard & Anti-Ransomware Settings	290
Backup Settings	291
The Anti-Exploit Component	291
Analysis & Remediation	293
Automated Attack Analysis (Forensics)	293
Remediation & Response	293
Advanced Remediation & Response Settings	293
File Quarantine	293
File Remediation	294
Adding Exclusions to Rules	294
Legacy Exclusions	295
Adding Exclusions to a Specific Rule	295
Adding Global Exclusions	295
Adding Exclusions from Security Overview	295
Adding Exclusions from Logs	296
Adding a New Exclusion to an Exclusion Category	297
Editing an Exclusion	297
Smart Exclusions	309
Adding Exclusions to a Specific Rule	310
Adding Global Exclusions	322
Migrating Legacy Exclusions	333
Importing and Exporting Exclusions	334
Managing Exclusions	335
Optimizing the Endpoint Security Client for Servers and Profiles	336
Quarantine Management	337
Using the Quarantine Manager for Administrators	339
Managing Quarantined Files	340
Benefits	340
Viewing Quarantined Files and Applications	340
Acting on Quarantined Files and Applications	342

Fetching (download) a quarantined file	342
Restoring a quarantined file	344
Deleting a quarantined file	345
Endpoint Security Client Device Restart Requirements	346
Configuring Client Settings	347
User Interface	348
Default Client User Interface	348
Pre-Boot Images	348
Windows Background Image	349
Customized Client Image	349
Customized Browser Block Pages	349
Log Upload	351
Installation and Upgrade Settings	352
Agent Uninstall Password	352
Local Deployment Options	352
General	353
Authenticated Proxy	353
Sharing Data with Check Point	354
Connection Awareness	354
Super-Node	355
Disable Capabilities	361
Network Protection	362
Push Operations	363
Configuring the Data Protection Policy	363
Configuring Full Disk Encryption	363
Check Point Disk Encryption for Windows	366
Configuration Options	366
Authentication before the Operating System Loads (Pre-boot)	367
Temporary Pre-boot Bypass Settings	367
Advanced Pre-boot Settings	368

User Authorization before Encryption	369
User Assignment	370
Smart Pre-Boot	371
Easy Unlock	372
Self Unlock	373
BitLocker Encryption for Windows Clients	375
Taking Control of Unmanaged BitLocker Devices	375
FileVault Encryption for macOS	377
User Authentication to Endpoint Security Clients (OneCheck)	378
Pre-boot Authentication Methods	379
Before You Configure Smart Card	379
Password Complexity and Security	381
Passwordless Pre-boot Authentication	382
User Account Lockout Settings	383
Remote Help Permissions	384
Logon Settings	385
Bi-Directional Password Sync Settings	386
Installing and Deploying Full Disk Encryption	386
Client Requirements for Full Disk Encryption Deployment	387
Completing Full Disk Encryption Deployment on a Client	387
Stages of the Deployment Phase	388
Viewing Full Disk Encryption (FDE) Status of an Endpoint Device	388
Get-Status Command	388
To View the FDE Status:	388
Output Parameters	390
Configuring Media Encryption & Port Protection	394
Configuring the Read Action	395
Configuring the Write Action	397
Configuring Business-Related File Types	398
Creating User Overrides (UserCheck)	399

Configuring Authorization Settings	400
Managing Devices	401
Managing Storage and Peripheral Devices	401
Managing Storage Device Groups	408
Using Wild Card Characters	409
Viewing Events	410
Advanced Settings for Media Encryption	415
Authorization Scanning	415
UserCheck Messages	416
Enabling the UserCheck messages	416
Customizing the UserCheck messages	416
Advanced Encryption	417
Media Log	418
Site Configuration	419
Lockout Settings	420
Offline Access	421
Password Constraints	421
Media Encryption Remote Help	422
Port Protection	423
Device Category Descriptions for Windows	425
Media Encryption Access Rules	428
Configuring Access & Compliance Policy	430
Firewall	431
Configuring Security Zones	432
Configuring Firewall Rule Advanced Settings	434
Configuring Inbound/Outbound Rules	435
Inbound Traffic Rules	435
Outbound Traffic Rules	435
Parts of Rules	436
Editing a Rule	436

Deleting a Rule	437
Managing Firewall Objects and Groups	438
Supported Object Categories	438
Creating Objects	441
Used In	442
Application Control	443
Configuring Application Control in Windows	443
Configuring Application Control in macOS	443
Creating the List of Applications on the Reference Device	444
Appscan Command Syntax	445
Uploading the Appscan XML File to the Endpoint Security Management Server	448
Configuring Application Permissions in the Application Control Policy	449
Supported Actions	449
App Rules	449
Custom Rules	450
Disabling or Enabling Windows Subsystem for Linux (WSL)	453
Developer Protection	454
Exclusions to Developer Protection	454
Compliance	456
Planning for Compliance Rules	457
Configuring Compliance Policy Rules	458
Ensuring Alignment with the Deployed Profile	459
Remote Access Compliance Status	460
Compliance Action Rules	461
Compliance Check Objects	463
Compliance Remediation Objects	467
Service Packs for Compliance	470
Ensuring that Windows Server Updates Are Installed	471
Detecting Common Vulnerabilities and Exposures	471
Configuring Posture Assessment Settings	472

Anti-Virus for Compliance	474
Monitoring Compliance States	475
"About to be Restricted" State	475
IOC Management	476
Connected, Disconnected and Restricted Rules	478
Policy Operation	480
Data Loss Prevention	483
DLP Logs	485
Use Case	486
Known Limitations	486
Sample Data Type	486
Creating a Custom Data Type	488
Creating a Custom Data Type Group	494
Adding an Existing Data Type to a Group	497
Editing a Data Type or Group	498
Duplicating a Data Type or a Group	501
Deleting a Data Type or a Group	503
Managing Microsoft Sensitivity Labels for DLP	505
Step 1 - Copy the Microsoft Sensitivity label names and their UUIDs from Microsoft Purview	505
Step 2 - Creating Microsoft Sensitivity Labels in Endpoint Security	507
Step 3 - Assign Sensitivity Labels to DLP Rules	511
Creating a DLP Rule and Associating with an Event	511
Rule Configuration Logic	517
Scenarios	518
Specific Event	518
Result	518
Specific Event	519
Result	519
Specific Event	519

Result	519
Specific Event	519
Result	520
Specific Event	520
Result	520
Specific Event	520
Result	521
Specific Event	521
Result	521
Specific Event	521
Result	521
Specific Event	522
Result	522
Specific Event	522
Result	522
Specific Event	522
Result	523
Specific Event	523
Result	523
Context Objects	523
Enabling GenAI Protect	524
Prerequisites	524
Import or Export Policies	527
Overview	527
Limitations	527
Prerequisites	527
Exporting Policies	528
Importing Policies	528
Capabilities of Offline Endpoint Security Client	529
Performing Data Recovery	531

Check Point Full Disk Encryption Recovery	532
BitLocker Recovery	535
FileVault Recovery	536
Managing Virtual Groups	539
Managing Active Directory Scanners	544
Supported Directory	544
Prerequisites	544
Managing Microsoft Active Directory Scanner	545
Organization Distributed Scan	545
Full Active Directory Sync	545
Managing Microsoft Entra ID Scanners	546
Limitations	546
Configuring the Settings in the Microsoft Entra ID Portal	547
Importing Objects from Microsoft Entra ID	553
Giving Remote Help to Full Disk Encryption Users	559
Active Directory Authentication	560
Endpoint Security Active Directory Authentication	560
Configuring Active Directory Authentication	561
UPN Suffixes and Domain Names	564
Configuring Alternative Domain Names	564
Troubleshooting Authentication in Client Logs	566
Endpoint Security Logs	567
Data Storage and Retention	569
Static Signatures (YARA) Logs	569
Query Language Overview	570
Criteria Values	570
NOT Values	572
Wildcards	572
Field Keywords	573
Boolean Operators	575

Exporting Logs	576
Creating Security Certificates for TLS Mutual Authentication	576
Sending Security Reports	579
Performing Push Operations (Old User Interface)	580
Push Operations	611
Accessing Push Operations	611
Extending the Time Frame of Push Operations	611
Push Operations Dashboard Widgets	611
Push Operations Table	612
Available Actions from Push Operations	612
Creating a Push Operation	613
Affected Devices Table	645
Filtering the Push Operations	645
Certificate Management	646
Forensics Data	647
Threat Hunting	647
Supported Regions	648
Supported Versions	648
Enabling Threat Hunting	648
Using Threat Hunting	649
Saving a Query as a Bookmark	653
Use Case - Maze Ransomware Threat Hunting	655
Sending Forensics Data to Third-Party Analytics Tool	656
Downloading Forensics Reports	656
Two-Factor Authentication	658
Endpoint Security for Linux	659
Endpoint Security for Linux Overview	660
Prerequisites	660
Key Threat Prevention Technologies	660
Anti-Malware	660

Endpoint Detection and Response (EDR) / Threat Hunting	660
Behavioral Guard	661
Anti-Ransomware	661
Forensics	661
Minimum Hardware Requirements	661
Supported Linux Versions	662
Linux Kernel Support	676
Installation on Semi-Isolated Environments with Super Node Proxy	676
Prerequisite	676
Installation Procedure	676
Deploying Endpoint Security for Linux	678
Endpoint Security for Linux Runtime Configurations	680
Overview	680
Limitations	680
How Container Runtime Monitoring Works	680
Supported Container Runtimes	680
Prerequisites	680
Configuring Container Runtime Settings	681
Path Configuration Requirements	681
Runtime-Specific Configuration	681
Docker	681
containerd	682
CRI-O	682
Kubernetes-Specific Configuration	682
MicroK8s	683
K3s	683
Verification	683
Endpoint Security for Linux CLI Commands	684
Help & Information Commands	684
Quarantine Commands	685

Scans & Detections	685
Logs	685
Uninstall Endpoint Security for Linux	686
Endpoint Security for Linux Additional Information	687
Endpoint Security for Windows Virtual Desktop Infrastructure (VDI)	688
Configuring Clients for Persistent Desktops	689
Software Blades for Persistent Desktops	689
Creating a Basic Golden Image for Persistent Desktops	689
Client Machine Configuration for Persistent Desktops	690
Creating a Pool for Persistent Desktops	690
VMware Horizon Key Points	691
Citrix XenDesktop Key Points	692
Configuring Clients for Non-Persistent Desktops	693
General	693
Shared Signatures Server	694
Configuring the Signatures Server	695
Setup Validation	695
Client Machine Configuration for Non-Persistent Desktops	696
Creating a Basic Golden Image for Non-Persistent Desktops	696
Configuring the Client Machine	696
Post Setup Actions	697
Creating a Pool for Non-Persistent Desktops	697
VMware Horizon Key Points	697
Citrix Xen-Desktop Key Points	698
Pool Validation	699
Disabling the Anti-Malware Periodic Scan	699
Software Blades for Non-Persistent Desktops	699
Basic Golden Image Settings	700
Assigning Policies to VDI Pools	702
Limitations	703

Appendix	703
Disabling the Anti-Malware Periodic Scan	703
Advanced Settings Non-Persistent Desktops	705
Configuring the Shared Signatures Server	705
Configuring the Client Machine	707
Endpoint Security for Terminal Server / Remote Desktop Services	709
Software Blades for Terminal Servers	709
Licensing	709
Limitations	710
Deploying the Endpoint Security Client on a Terminal Server / Remote Desktop Service	711
Prerequisites	711
Procedure	711
Best Practice to Enable Software Blades	713
Configuring Threat Emulation (TE) Appliance for Endpoint Security	715
Prerequisites	715
Step 1 - Configure the TE Appliance on SmartConsole	715
Step 2 - Create a TE Appliance Object in the SmartConsole	719
Step 3 - Enable Threat Prevention API	724
Step 4 - Threat Emulation Configuration in Check Point Portal	726
Known Limitations	728
Managed Security Service Providers (MSSP)	729
Viewing Statistics for MSSP	729
Service Management	729
Accounts Info	729
Service Status	730
Hosting Sites	730
Account Details Table	731
MSSP Essentials	732
MSSP Total Endpoints	732

Account with Issues	733
Service Status	733
Contracts by Type	734
Contracts by Status	734
Active Endpoints Trend	734
Top 5 Attacked Accounts	735
Top 5 Ransomware Attacked Accounts	735
Top 5 Phishing Attacked Accounts	736
Top 5 Accounts with Exploit Attack Attempts	736
Alerts	737
MSSP Custom Dashboard	737
MSSP Dashboard	737
Account Dashboard	739
Managing a Custom Dashboard	743
Optional Widgets	744
Password Reuse Attacks	744
Phishing Attacks	744
Ransomware Attacks	744
Exploit Attacks	745
Malicious Site Attacks	745
Service Management	745
Accounts Info	746
Issues by Accounts	746
Service Status	747
Hosting Sites	748
Account Details Table	748
Contracts	749
Accounts Info	749
Accounts Contracts Distribution	750
Contracts by Accounts	750

Contract Details Table	750
Contract Status Report	751
Sending an Email to Account on Contract Status	752
Reports for MSSP	753
Global Exclusions	754
Adding Global Exclusions using Legacy Exclusion	754
Adding Global Exclusions using Smart Exclusion	755
Syncing Exclusions with Child Accounts	756
Templates for Child Accounts	756
Use Case	756
Benefits	757
Threat Prevention Policy Template	757
Creating a Threat Prevention Policy Template	757
Attaching the Threat Prevention Policy Template to a Child Account	758
Viewing the Accounts Attached to a Template	760
Software Deployment Policy Template	762
Creating a Software Deployment Policy Template	762
Attaching the Software Deployment Policy Template to a Child Account	763
Viewing the Accounts Attached to a Template	764
Smart App Control	767
Recent Tasks	768
Known Limitations	769
Appendix	770
Appendix A - Deploying Endpoint Security Client using SCCM	770
Prerequisites	770
Step 1: Create the Endpoint Security Windows Application in SCCM	770
Step 2: Deploy the Endpoint Security Windows Application in SCCM	771
Appendix B - Uninstalling the Endpoint Security Client (For macOS and Windows)	771
Appendix C - Deploying Endpoint Security Client Using Microsoft Intune	772
Use Case	772

Prerequisites	772
Preparing the Endpoint Security Client Windows Package for Deployment	772
Endpoint Security Configuration	773
Creating the Endpoint Security Windows App in Microsoft Intune	774
Appendix D - Microsoft Intune Wipe and Windows Reset with Full Disk Encryption	779
Overview	779
Notes and Limitations	779
Reset Behavior with Full Disk Encryption	779
Supported Reset and Wipe Configurations	779
Reset Without Full Disk Encryption	780
Reset with Full Disk Encryption Enabled	780
Autopilot Reset (Not Supported)	780
Intune Wipe with Enrollment Removal (Not Supported)	781
Trusted Platform Module (TPM) Considerations	781

Introduction to Endpoint Security

Check Point Endpoint Security is an endpoint protection solution that safeguards devices against a wide range of cyber threats. It integrates prevention, detection, and response capabilities to defend against malware, ransomware, phishing, and other targeted attacks. This solution combines local and cloud-based security technologies.

This guide helps administrators deploy, configure, and maintain Endpoint Security in the Check Point Portal, a cloud-based management console that centralizes security operations. It provides essential information and step-by-step instructions to support effective implementation and ongoing management.

Endpoint Security includes Endpoint Management as a Service (EPMaaS), a cloud-based service that manages policies and deployments for both Endpoint Security and Browser Security clients. For details about Browser Security, see the [Browser Security Administration Guide](#).

Key Features

- **Comprehensive threat prevention** - Uses Check Point's next-generation security technologies to protect endpoints from known and unknown threats, including zero-day attacks.
- **Cross-platform security** - Enforces consistent security policies across multiple operating systems.
- **Centralized management** - The cloud-based Check Point Portal console enables real-time monitoring, policy management, and response to security events, simplifying endpoint protection at scale.

Endpoint Security supports the management of these components:

- Threat Prevention
- Data Protection
- Media Encryption & Port Protection
- Firewall
- Application Control
- Developer Protection
- Compliance
- Software Deployment

Endpoint Security supports up to 400,000 endpoint clients.



Note - Google Chrome is the recommended browser for the Endpoint Security Administrator Portal.

API Support

Endpoint Security Management API

You can use Endpoint Security Management API to access and retrieve data from Endpoint Security External API.

To access Endpoint Security Management API:

1. Go to [Check Point API Reference](#).
2. Click **Workspace Security**.
3. In the **Endpoint Security Management API** widget, click **Open**.

Getting Started

To get started with Endpoint Security:

1. [Create an account in the Check Point Portal](#)
2. [Assign Specific Service Roles to Users](#)
3. [Access the Endpoint Security Administrator Portal](#)
4. [License the product](#)
5. [Create a New Endpoint Management Service](#)
6. [Getting Started Walkthrough Wizard](#)
7. [Deploy the Endpoint Security Client](#)
8. [Configure the Endpoint Security Policy](#)

Creating an Account in the Check Point Portal

Check Point Check Point Portal is a web-based interface that hosts the Check Point security SaaS services. With Check Point Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

To create an Check Point Portal account, refer to [Check Point Portal Administration Guide](#).

MSSP Account

Endpoint Security supports an interface for Managed Security Service Providers (MSSP) to:

- Create and manage (pause, stop, start and restart) the service of their child accounts
- View general statistics about their child accounts
- View operational statistics about their child accounts
- View contract details of their child accounts

To convert an existing account to MSSP account, refer to [Check Point Portal Administration Guide](#).

To create a new MSSP account and to add child accounts, refer to [Check Point Portal Administration Guide](#).

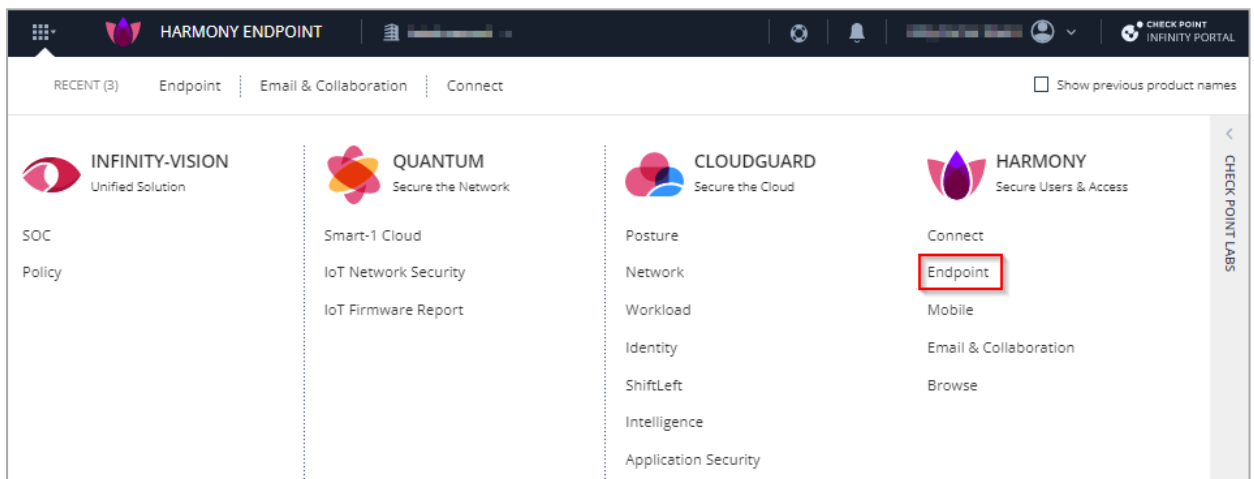
To manage your MSSP and its child accounts, see *"Managed Security Service Providers (MSSP)" on page 729*.

Accessing the Endpoint Security Administrator Portal

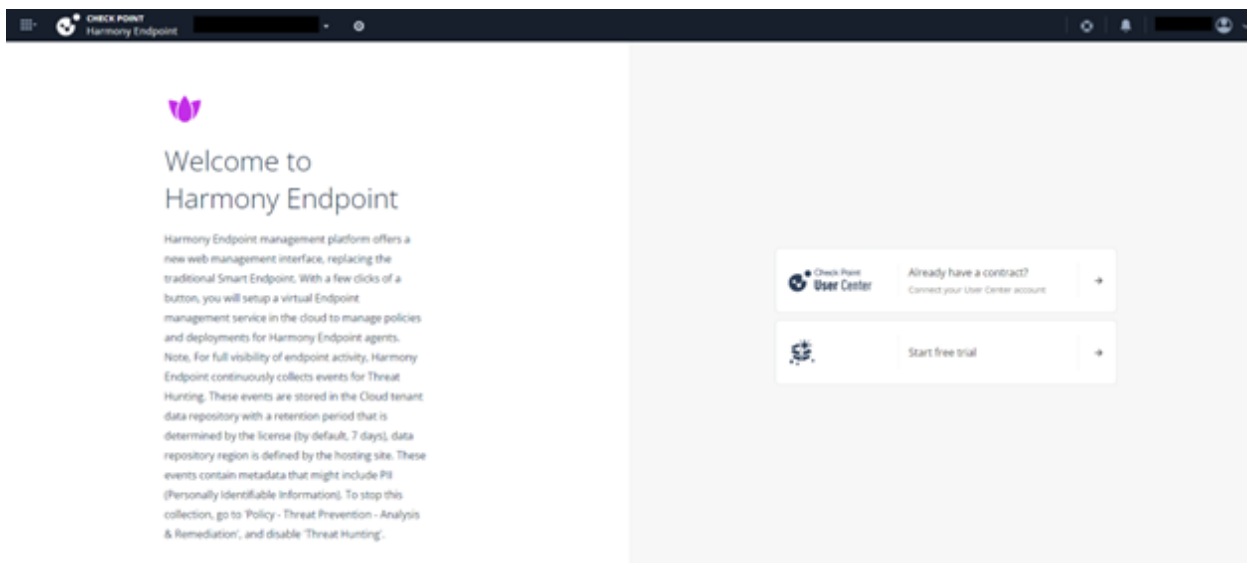
Note - The Endpoint Security Administrator portal (in the Check Point Portal) is supported only through the Google Chrome browser.

To access the Endpoint Security Administrator Portal:

1. Sign in to the Check Point Portal.
2. Click the **Menu** button () in the top left corner.
3. Under **Harmony**, click **Endpoint**.



4. If you are accessing the portal for the first time, do one of these:



- If you already have a Check Point contract, click **Already have a contract?** to attach the contract to the product. For more information, see **Associated Accounts** in the [Check Point Portal Administration Guide](#).
- If you want to trial the product, click **Start free trial**.

If you have already attached the contract with the product, the Endpoint Security [Getting Started](#) appears.

Creating a New Endpoint Management Service

After you registered to Endpoint Security, you must set your Endpoint Management Service to be able to manage your Endpoint clients. An administrator can create and deploy one virtual Endpoint Management service per account.

To create a New Endpoint Management Service:

1. From the left navigation panel, click the **Service Management** view.
2. Click **New Endpoint Management Service** and enter the information in these fields:

- **Connection Token** - Select your Endpoint Management Service name for this account. Use the Connection Token when you connect to SmartEndpoint Management Console.

The Connection Token:

- Must consist of 2-16 characters: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), or hyphens (-).
 - Must not start with a hyphen (-).
- **Hosting Site** - The cloud location where the Endpoint Management Service is deployed. This information is derived from your selection of data residency region when you created the account. See [Creating an Account in the Check Point Portal](#).

3. Click **Create**.

The deployment process starts.

You can monitor the deployment process in the portal. The portal sends an email on completion.

Managing Licenses

For information about the available licenses, see the [Endpoint Security product catalog](#).

User Center

When you create an account in the Check Point Portal and access the service, you get a free 30-day trial. After the 30-day trial period, you must purchase a software license to use the product. To purchase a license, you must create a [Check Point User Center](#) account.

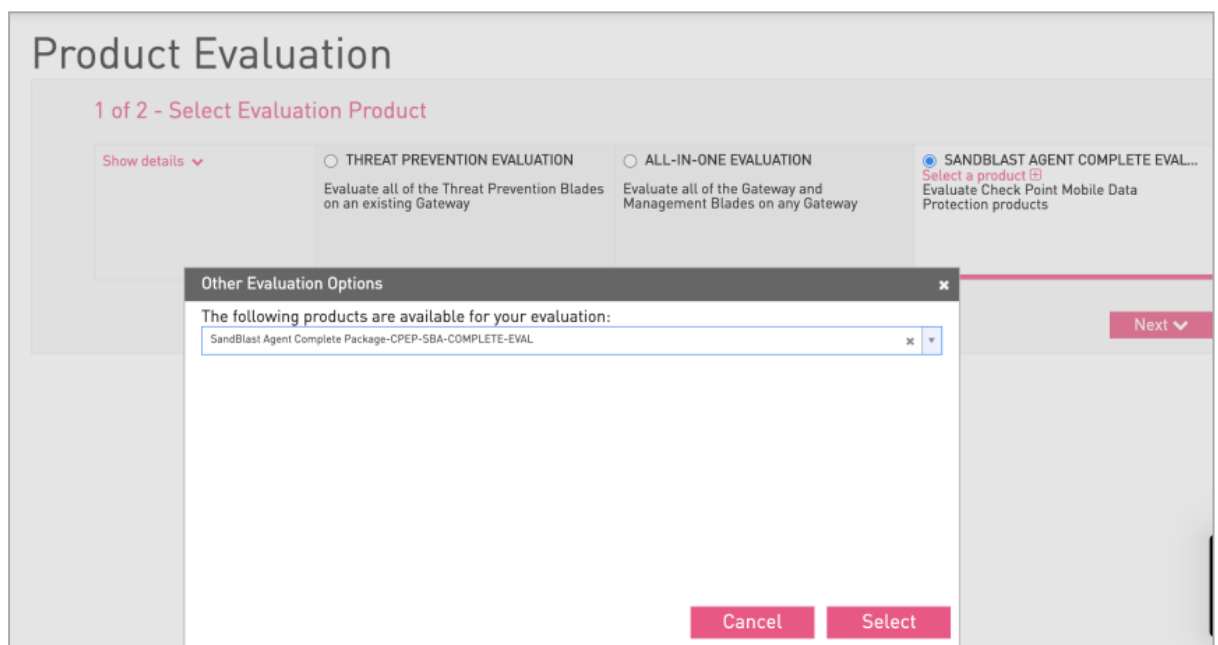
Once you create a User Center account, contact your Check Point sales representative to purchase a license.

To extend the trial period

1. Log in to the [Check Point User Center](#).
2. If you do not have a User Center account, go to **My Check Point > My accounts** and create a new User Center account.
3. Go to **My Check Point > Product Center**.
4. In the Product Center, go to the **Evaluations** tab.
5. Select **Other Evaluation Option** and click **Select a product**.

The **Other Evaluation Options** window opens.

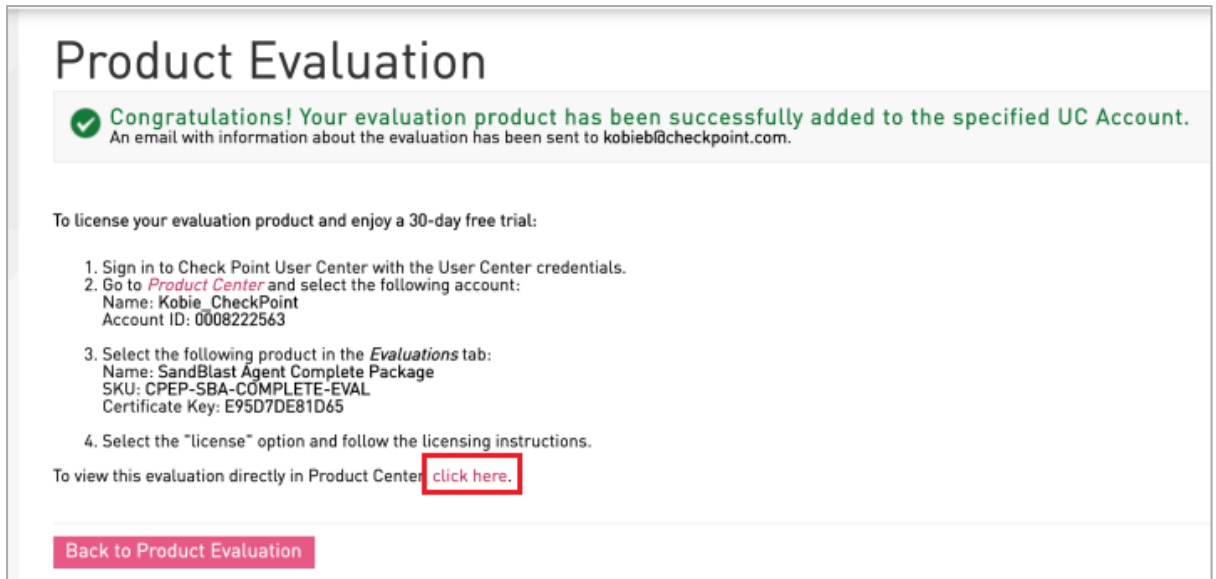
6. Select **CP-HAR-EP-COMPLETE-EVAL** or **CP-HAR-EP-ADVANCED-EVAL** from the drop-down list and click **Select**.



7. Click **Next**
8. In the **Provide Evaluation Info** section that opens, fill in these details:
 - a. **User Center Account**
 - b. **Email Address**
 - c. **Evaluation Product will be used by**
 - d. **Purpose of Evaluation**
9. Click **Get Evaluation**.

A confirmation notice is received that the product was successfully added to your User Center account.

Click the link in the confirmation notice to view the license in the Product Center.



Product Evaluation

✓ **Congratulations! Your evaluation product has been successfully added to the specified UC Account.**
An email with information about the evaluation has been sent to kobieb@checkpoint.com.

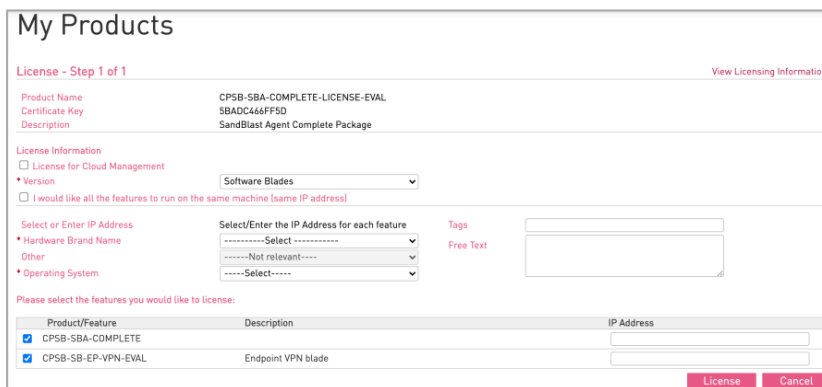
To license your evaluation product and enjoy a 30-day free trial:

1. Sign in to Check Point User Center with the User Center credentials.
2. Go to **Product Center** and select the following account:
Name: **Kobie_CheckPoint**
Account ID: 0008222563
3. Select the following product in the **Evaluations** tab:
Name: **SandBlast Agent Complete Package**
SKU: **CPEP-SBA-COMPLETE-EVAL**
Certificate Key: **E95D7DE81D65**
4. Select the "license" option and follow the licensing instructions.

To view this evaluation directly in Product Center: [click here.](#)

[Back to Product Evaluation](#)

10. In the Product Center, go to Selected Account and select the account to which the license was added.
11. Select the license and click the **License** button above the list of the licenses.
12. Under **License Information**, select the **License for Cloud Management** checkbox.



My Products

License - Step 1 of 1 [View Licensing Information](#)

Product Name: CPSB-SBA-COMPLETE-LICENSE-EVAL
Certificate Key: SBADC464FF5D
Description: SandBlast Agent Complete Package

License Information

☐ License for Cloud Management

• Version: Software Blades

☐ I would like all the features to run on the same machine (same IP address)

Select or Enter IP Address: Select/Enter the IP Address for each feature Tags

• Hardware Brand Name: -----Select----- Free Text

• Other: -----Not relevant-----

• Operating System: -----Select-----

Please select the features you would like to license:

Product/Feature	Description	IP Address
☒ CPSB-SBA-COMPLETE		
☒ CPSB-SB-EP-VPN-EVAL	Endpoint VPN blade	

[License](#) [Cancel](#)

13. If you have not subscribed to the VPN feature (Check Point Security Gateways are not used for client VPN), then click **License**.
14. If you have subscribed to the VPN feature that uses Check Point Security Gateways for client VPN, then in the **IP Address** field for **CPSB-SB-EP-VPN**, replace **164.100.1.8** with the IP address of the Gateway Security Management System and then click **License**.

Amazon Web Services Marketplace

Use the Amazon Web Services credit to purchase the Endpoint Security license from [Amazon Web Services Marketplace](#).

Activating the License

To activate a license

1. In Endpoint Security Administrator Portal, go to **Global Settings > Services and Contracts**.

At the upper-right of the screen, click **Link a User Center Account**.

The **Attach Accounts** window opens.

2. Enter your **User Center** credentials, select the **Account** and click **Next**.
3. Select the license to apply and click **Finish**.

Your license appears in the **Service and Contracts** page.

 **Note-** If you already have an associated account and wish to add another license, go to **Global Settings > Service and Contracts**. At the upper-right of the screen, click **Manage Accounts** and use the sync option to refresh the license.

4. To see your license information, go to the **Endpoint Settings > Licenses**.
5. To synchronize your license information, click **Sync** and then click **CONFIRM**.

License Violation

Endpoint Security notifies you about the license violations, such as expiry and exceeded permitted seats.

Depending on the level of violation, the system sends these notifications and takes these actions:

- Email
- Email and top banner
- Email, top banner and pop-up window
- Top banner, pop-up window and disables policy configuration¹
- Top banner, pop-up window, disables policy configuration¹ and disables new installations²

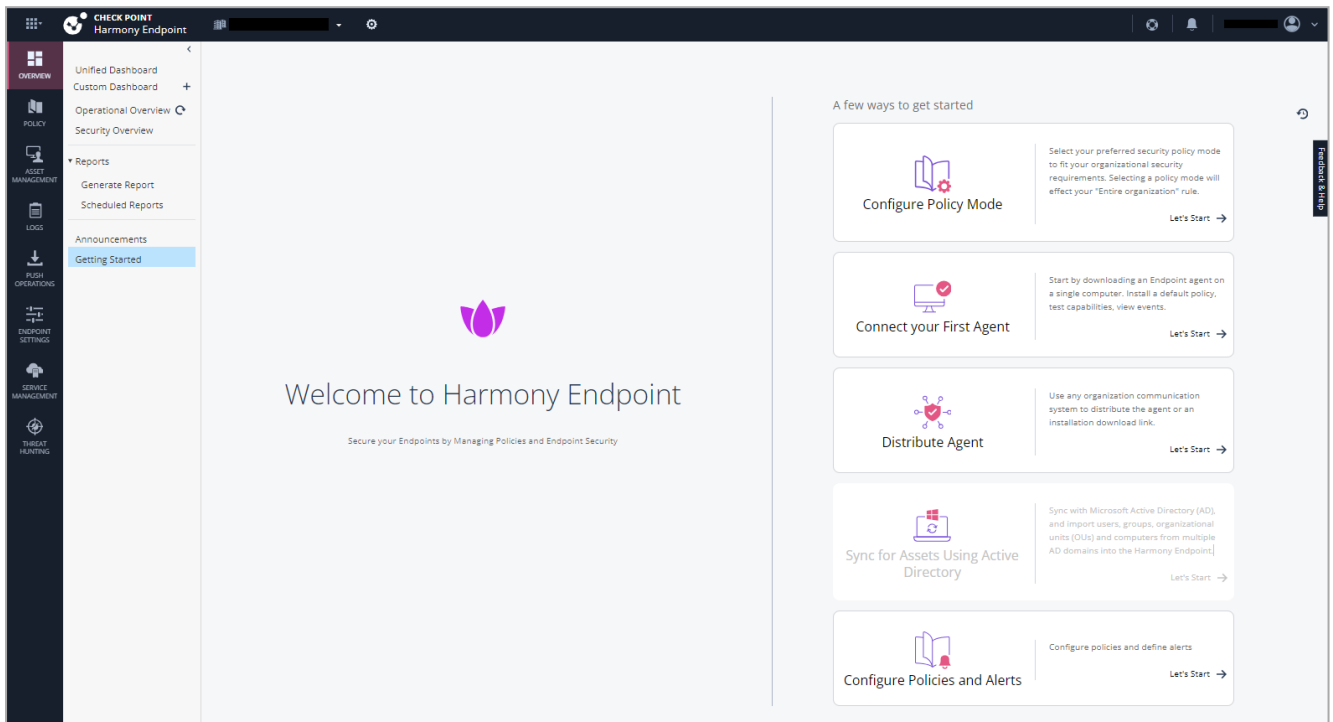
¹ All the configuration in the **Policy** menu is read-only except **Export Package** and **Export/Import Policies**. The **Save** button is disabled, however, previously saved changes can be installed.

² All the configuration in the **Policy** menu is read-only except **Export Package** and **Export/Import Policies**. The **Save** and **Install** buttons are disabled.

Getting Started Walkthrough Wizard

The Getting Started Walkthrough Wizard provides an overview of common operations for administrators on the Endpoint Security Administrator Portal, simplifying the on-boarding process.

After you successfully deploy a service, go to **Overview > Getting Started**.



The list of widgets in the getting started page of Endpoint Security Administrator Portal is as follows:

- **Configure Policy Mode**

To configure the Threat Prevention policy mode, click **Let's Start** in the **Configure Policy Mode** widget.

The **Configure policy mode** page appears.

To select the required policy mode and install the policy:

1. Select the best suitable policy mode and click the **Install** button provided for the respective policy mode. The predefined configurations available are:
 - **Detect** - This configuration provides basic protection and is recommended for the users on-boarding for the first time for a few days.

 **Note** - Detect mode can help optimize your work during the on-boarding process, but it is not recommended to remain in detect mode.

- **Tuning** - This configuration provides more protection than the detect only configuration.
- **Optimized** - This is a production recommended configuration which provides enhanced protection.

For more information, see [Policy Mode](#).

Note - The policy will be applied to the default rule (usually to Entire Organization).

2. Click **Continue** to proceed with the installation.

■ Connect your First Agent

To download and connect with the Endpoint agent, click **Let's Start** in the **Connect your First Agent** widget.

The **Connect your First Agent** page appears with the following widgets:

- **Download & Install Endpoint agent** - To download the Endpoint agent, click **Download** and select the suitable option. The available options are as follows:
 - **Online Install** - Download and install the Endpoint Security client using a tiny install agent on the endpoints. For more information, see [Automatic Deployment using the Tiny Agent](#).
 - **Offline Install** - Download the Endpoint Security client and export the same to the endpoints for offline installation. For more information, see [Manual Deployment using the Offline Installation](#).
 - **Copy installation link** - Download and install the Endpoint Security client using the installation link via third party installation agent. For more information, see [Automatic Deployment using the Vanilla client](#).

- **Change Uninstall Password** - The uninstall password will be required when an endpoint user is uninstalling the security client. To configure the uninstall password:

1. Click **Setup**.
2. Enter the password in the **Password** and **Confirm Password** field.
3. Click **Save**.

For more information, see [Agent Uninstall Password](#).

- **Monitoring** - To monitor the connected devices, click **Overview**. For more information, see [Viewing Operational and Security Overview](#).

■ Distribute Agent

To download and distribute the agent, click **Let's Start** in the **Distribute Agent** widget.

The **Distribute Agent** page appears with the following widgets:.

- **Distribute Agent Manually** - To download the Endpoint agent, click **Download** and select the suitable option. The available options are as follows:
 - **Online Install** - Download and install the Endpoint Security client using a tiny install agent on the endpoints. For more information, see [Automatic Deployment using the Tiny Agent](#).
 - **Offline Install** - Download the Endpoint Security client and export the same to the endpoints for offline installation. For more information, see [Manual Deployment using the Offline Installation](#).
 - **Copy installation link** - Download and install the Endpoint Security client using the installation link via third party installation agent. For more information, see [Automatic Deployment using the Vanilla client](#).
- **Distribute Agent via 3rd Party App** - To view the procedure to distribute the Endpoint agent using 3rd party applications for Windows, click **Setup**. For information about macOS application, see [Endpoint Security client for macOS MDM Deployment Guide](#).
- **Remote Installation** - To view the procedure for remote installation of the client, click **Overview**.

■ Sync for Assets Using Active Directory

To configure Active Directory scanners, click **Let's Start**.

The **Sync for Assets Using Active Directory** page appears with the following widgets:

- **Full Active Directory Scanner** - 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 and enable or disable Active Directory Default Scanner, click **Enable/Disable**. For more information, see [Full Active Directory Sync](#).

 **Note** - If your organization uses Microsoft Activity Directory (AD), you can import users, groups, organizational units and computers from multiple AD domains into the Endpoint Security Administrator Portal.

- **Organization Distributed Scan** - In this method, only devices with Endpoint Security installed report their paths. Other devices do not report any information. To enable or disable Organization Distributed Scan, click **Enable/Disable**. For more information, see [Organization Distributed Scan](#).

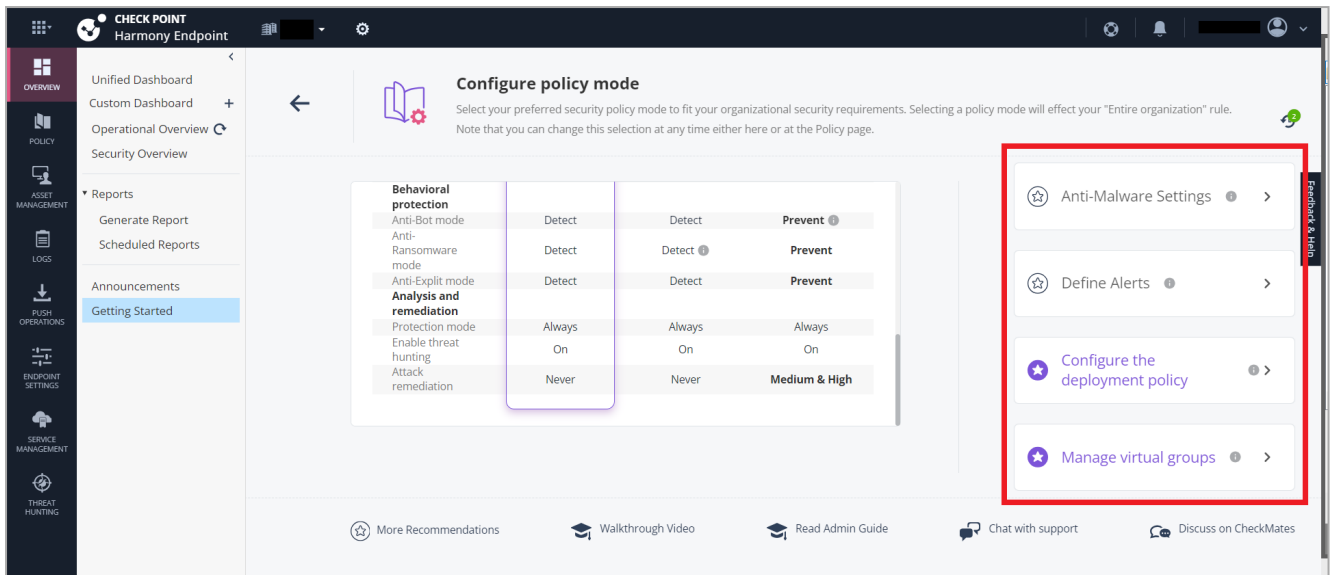
■ Configure Policies and Alerts

To configure Policies and Alerts, click **Let's Start** in the **Configure Policies and Alerts** widget.

The **Configure Policies and Alerts** page appears with the following widgets:

- **Manage virtual groups** - To configure the virtual groups, click **Manage**. For more information, see ["Managing Virtual Groups" on page 539](#).
-  **Note** - You can also configure the virtual groups outside the Active Directory.
- **Set Pre-Defined Policies** - To configure the security policies, click **Set Policy**. For more information, see ["Configuring the Threat Prevention Policy" on page 248](#).
- **Define Alerts** - To configure the notifications and alerts, click **Define**. For more information, see ["Configuring Alerts" on page 130](#).

Each section also contains a few general options, which are listed in the following table:



Element	Description
Define Alerts	To configure the alerts and notifications. For more information, see "Configuring Alerts" on page 130 .
Configure the security policy	To configure the Endpoint security policies. For more information, see "Configuring the Threat Prevention Policy" on page 248 .
Configure the deployment policy	To configure the software deployment. For more information, see "Automatic Deployment of Endpoint Clients" on page 94 .
Manage virtual groups	To configure the virtual groups. For more information, see Managing Virtual Groups .

Specific Service Roles

Endpoint Security supports specific service roles. The specific service roles are in addition to the global rules and do not override them. For more information, see [Check Point Portal Administration Guide](#).

To access **Specific Service Roles**, go to **Global Settings > Users > New > Add User** and expand **Specific Service 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.

Role	Description
Helpdesk Level 1	Has Read-only access to the service and Data Protection . Has Read & Write access to computer actions and Logs .
Helpdesk Level 2	Has the same access as Helpdesk Level 1 and, in addition, full access to Repair Client and Forensics and Remediation Push Operations .
Helpdesk Level 3	Has the same access as Helpdesk Level 2 and, in addition, full access to Manage Virtual Groups and Read-Only access to Software Deployment Policies .
Log Only User	Has full access to the Logs tab. Has no access to other features.
Power User	Has full Read & Write access to the Check Point Endpoint Security service, but cannot control the service.
Remote Help User	Helps Full Disk Encryption and Media Encryption users with access to encrypted media.

The table below summarizes the permissions of each user type:

Tab on Left Panel	Section	Admin User	Helpdesk Level 1	Helpdesk Level 2	Helpdesk Level 3	Remote Help User	Log Only User	Power User	Read-Only
Overview	All	Read & Write	Read-Only	Read-Only	Read-Only	Read & Write	No Permission	Read & Write	Read-Only

Tab on Left Panel	Section	Admin User	Helpdesk Level 1	Helpdesk Level 2	Helpdesk Level 3	Remote Help User	Log Only User	Power User	Read-Only
Policy	All	Read & Write	Read-Only	Read-Only	Read-Only	No Permission	No Permission	Read & Write	Read-Only
	Software Deployment - Install Policy	Read & Write	Read & Write	Read & Write	Read-Only	No Permission	No Permission	Read & Write	Read-Only
	Software Deployment - Write Policy	Read & Write	Read & Write (Cannot edit groups, only select objects in rules)	Read & Write (Cannot edit groups, only select objects in rules)	Read-Only	No Permission	No Permission	Read & Write	Read-Only
	Threat Prevention - Exclusions	Read & Write	Read-Only	Read-Only	Read-Only	No Permission	No Permission	Read & Write	Read-Only

Tab on Left Panel	Section	Admin User	Helpdesk Level 1	Helpdesk Level 2	Helpdesk Level 3	Remote Help User	Log Only User	Power User	Read-Only
Asset Management	All	Read & Write	Read-Only	Read & Write	Read & Write	No Permission	No Permission	Read & Write	Read-Only

Tab on Left Panel	Section	Admin User	Helpdesk Level 1	Helpdesk Level 2	Helpdesk Level 3	Remote Help User	Log Only User	Power User	Read-Only
	Data Protection (Recover Media)	Read & Write	Read & Write	Read & Write	Read & Write	Read & Write	No Permission	Read & Write	Read-Only
	Data Protection (Full Disk Encryption Remote Help)	Read & Write	Read & Write	Read & Write	Read & Write	Read & Write	No Permission	Read & Write	Read-Only
	Push Operations (Remediation)	Read & Write	No Permission	Read & Write	Read & Write	No Permission	No Permission	Read & Write	Read-Only
	Push Operations (All, except Remediation)	Read & Write	Read & Write	Read & Write	Read & Write	No Permission	No Permission	Read & Write	Read-Only

Tab on Left Panel	Section	Admin User	Helpdesk Level 1	Helpdesk Level 2	Helpdesk Level 3	Remote Help User	Log Only User	Power User	Read-Only
	Computer Actions (Reset computer, Delete computer data, add Pre-boot users)	Read & Write	Read & Write	Read & Write	Read & Write	No Permission	No Permission	Read & Write	Read-Only
	Manage Virtual Groups	Read & Write	Read-Only	Read-Only	Read & Write	Read-Only	No Permission	Read & Write	Read-Only
Logs	All	Read & Write	Read & Write	Read & Write	Read & Write	No Permission	Read & Write	Read & Write	Read-Only
Push Operations	All	Read & Write	No Permission	Read & Write	Read & Write	No Permission	No Permission	Read & Write	Read-Only
	Remediation	Read & Write	No Permission	Read & Write	Read & Write	No Permission	No Permission	Read & Write	Read-Only
	All except Remediation	Read & Write	Read & Write	Read & Write	Read & Write	No Permission	No Permission	Read & Write	Read-Only

Tab on Left Panel	Section	Admin User	Helpdesk Level 1	Helpdesk Level 2	Helpdesk Level 3	Remote Help User	Log Only User	Power User	Read-Only
Endpoint Settings	All	Read & Write	No Permission	No Permission	No Permission	No Permission	No Permission	Read & Write	Read-Only
Service Management	All	Read & Write	No Permission	No Permission	No Permission	No Permission	No Permission	Read & Write	Read-Only
	Service Actions (Restart, pause or terminate the service)	Read & Write	No Permission	No Permission	No Permission	No Permission	No Permission	No Permission	Read-Only
Threat Hunting	All	Read & Write	No Permission	No Permission	No Permission	No Permission	No Permission	Read & Write	Read-Only
Posture Management	All	Read & Write	Read & Write	Read & Write	Read & Write	No Permission	No Permission	Read & Write	Read-Only

Reconnect Tool

You can use the Reconnect tool to reconnect all your Endpoint Security clients to a new Endpoint Management Server.

Windows



Notes:

- If you are using Smart App Control in Windows 11, see ["Smart App Control" on page 767](#) on how to use the Reconnect tool.
- For Endpoint Security Client version E87.20 and lower, the **Reconnect tool** removes pre-boot users and disables user acquisition while connecting endpoint clients to the new Endpoint Management Server. To prevent this issue, you must manually migrate the client database to the new Endpoint Management Server.
- For Endpoint Security Client version E87.30 and higher, the **Reconnect tool** automatically initiates user acquisition. However, the user must lock and unlock their computer to complete user acquisition.

To use the Reconnect tool:

1. Log in to the Endpoint Management Server to which you want to connect your Endpoint Security clients.
2. Go to **Service Management** and under **Reconnect Tool**, click **For Windows**.

The system downloads the *reconnect.utility.exe* file.

3. Run the *reconnect.utility.exe* file.

The system creates the **recovery_tool** folder.

4. Select **Start** and type **CMD**.
5. Right-click **Command Prompt** and select **Run as administrator**.

The **Command Prompt** window opens.

6. Change the directory to the **recovery_tool** folder.
7. Run:

```
maketool.bat .\config.dat <client_uninstall_password>
```

The system creates the **Reconnect.exe** file that contains the details of server that the endpoint requires to reconnect to the new Management Server.

**Notes:**

- `client_uninstall_password` is optional. If you do not specify the password, the user must enter the password when running the Recovery tool on their computer. If you use special (non-alphanumeric) characters in the password, such as `!,@,$`, enclose the password within quotation marks. For example, `"!1@3$5^7*9"`.
- If you do not want to show the confirmation message "The reconnect tool was run successfully", add `/silent` in the command. For example, `maketool.bat /silent \path_to\config.dat[client_uninstall_password]`.

8. Distribute the **Reconnect.exe** file to the computers.
9. Double-click the **Reconnect.exe** file and follow the on-screen instructions.

The Reconnect tool stops all the daemons, replaces the configuration file and then reloads the daemons, connecting the Endpoint Security clients with the new Endpoint Management Server.



Note - If the Endpoint Security clients with version E85.60 and higher cannot connect to the new Endpoint Management Server, your Endpoint Security client may still be connected to the old Endpoint Management Server. For more information, see [sk92329](#).

macOS



Note - This is supported only with the Endpoint Security Client version E87.50 and higher.

Without Agent Uninstall Password (Recommended)

To use the Reconnect tool without using the uninstall password on the endpoint:

1. Log in to the Endpoint Management Server to which you want to connect your Endpoint Security clients.
2. Go to **Service Management** and under **Reconnect Tool**, click **For macOS**.

The system downloads the *reconnect_tool_for_macOS.zip* file.

3. Unzip the file.

The system unzips to the **reconnect_tool_for_macOS** folder that contains the **EPReconnect** tool.

4. Connect to the command line and run:

```
<path to the EPReconnect tool>
./EPReconnectTool.app/Contents/MacOS/EPReconnect --password
<agent_uninstall_password> --make-tool -silent
```



Note - The parameter `-silent` creates a tool that runs without user dialogs.

The system recreates the *reconnect_tool_for_macOS.zip* file in a temporary directory.

5. Distribute the zip file to endpoints.
6. Unzip the file on the endpoint.

The system unzips to the **reconnect_tool_for_macOS** folder that contains the **EPReconnect** tool.

7. Using the **Finder** application, find and double-click **EPReconnectTool.app**.



Notes -

- **EPReconnectTool.app** does not require authentication, this allows the macOS standard users to reconnect the endpoints to the Endpoint Management server.
- Alternately, you can run the **EPReconnectTool.app** using either of the following options:
 - Command Line
 - MDM Script

The Reconnect tool runs and reconnects endpoints to the new Endpoint Management Server.

With Agent Uninstall Password

To use the Reconnect tool using the uninstall password on the computer:

1. Log in to the Endpoint Management Server to which you want to connect your Endpoint Security clients.
2. Go to **Service Management** and under **Reconnect Tool**, click **For macOS** to download the *reconnect_tool_for_macOS.zip* file.
3. Distribute the zip file to the endpoints.
4. On the endpoint, unzip the file.

The unzipped folder contains the **EPReconnect** tool.

5. Using the **Finder** application, find and double-click **EPReconnectTool.app**.
 - a. Enter the client uninstall password and click **OK**.
6. Alternatively, run the **EPReconnectTool.app** from the command line using the following command:

```
./EPReconnectTool.app/Contents/MacOS/EPReconnectTool --enter-  
password
```

- a. Enter the client uninstall password in the command line terminal and click **Enter**.

The Reconnect tool runs and reconnects endpoints to the new Endpoint Management Server.

Supported Operating Systems for the Endpoint Security Client

Microsoft Windows

Microsoft Windows

Version	Editions	Supported starting from
11 25H2	Enterprise Pro	Endpoint Security Client E89.05 VPN Standalone Client E89.00
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 LTSC (version 1607)	Enterprise Pro	Endpoint Security Client E85.00
8.1 Update 1	Enterprise Pro	Endpoint Security Client E85.00

Version	Editions	Supported starting from
7 SP1 Microsoft update KB3033929	Enterprise Professional	Endpoint Security Client E85.00

**Notes:**

- For existing 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.
- E89.10 is the last version supported on Windows 7 and Windows 8. For additional information on Microsoft Legacy Operating Systems support, refer to [sk183765](#).
- 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 operating system 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 & Port Protection, Threat Emulation.
2022 64-bit	All	E85.40	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Media Encryption & Port Protection.
2019 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Media Encryption & Port Protection.
2016 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation.
2012 R2 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation.
2012 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation.
2008 R2 32/64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation.



Notes:

- Windows Server CORE is not supported.
- E89.10 is the last version supported on Windows Server 2008 and Windows Server 2012. For additional information on Microsoft Legacy operating systems support, refer to [sk183765](#).
- 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 Windows 2016 64-bit version.

macOS

macOS Version	Supported starting from
macOS Tahoe (26.3)	Endpoint Security Client E89.21 (see note 2)
macOS Tahoe (26)	Endpoint Security Client E89.20
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 Version	Supported starting from
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:**

1. 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.
2. For computers running Endpoint Security with Threat Prevention Software Blades (Anti-Bot and URL Filtering, Anti-Ransomware and Forensics, and Threat Emulation), macOS **26.3** is supported starting from **E89.21**.
3. 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	1.28.12	1.28.11	1.26.8	1.24.02	1.22.18	1.22.16	1.22.12	1.20.7	1.18.6	1.18.2	1.15.0	1.13.7	1.13.3	1.13.2
Ubuntu 25.10	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Ubuntu 24.04 (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–

Distribution / OS Version	1.28.12	1.28.11	1.26.8	1.24.02	1.22.18	1.22.16	1.22.12	1.20.7	1.18.6	1.18.2	1.15.0	1.13.7	1.13.3	1.13.2
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	1.28.12	1.28.11	1.26.8	1.24.02	1.22.18	1.22.16	1.22.12	1.20.7	1.18.16	1.18.12	1.15.10	1.13.7	1.13.3	1.13.2
Ubuntu 18.04* (64-bit) (Supported versions: 18.04 - 18.04.6)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Ubuntu 16.04 (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Alma Linux 10.1	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Alma Linux 10	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Alma Linux 9.7	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Alma Linux 9.6	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Alma Linux 9.5	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
Alma Linux 9 (64-bit) (Supported versions: 9.0 - 9.3)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
Alma Linux 8 (64-bit) (Supported versions: 8.9 and 8.10)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
Amazon Linux 2023	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Amazon Linux 2 (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Cent OS 8* (64-bit) (Supported versions : 8.0 - 8.5)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Cent OS 7 (64-bit) (Supported versions: 7.8 - and 7.9)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Debian Linux 13.3	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.28.12	1.28.11	1.26.8	1.24.02	1.22.18	1.22.16	1.22.12	1.20.7	1.18.6	1.18.2	1.15.0	1.13.7	1.13.3	1.13.2
Debian Linux 13.2	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Debian Linux 13 (64-bit)	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
Debian Linux 12 (64-bit) (Supported versions: 12.0 - 12.5)	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–
Debian Linux 11* (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Debian Linux 10* (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Debian Linux 9* (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 39 ¹	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 38 ¹	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 37	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 36	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 35	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 34	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Mint 22.3	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Mint 22.2	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Mint 22.1	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
Mint 22	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–
Mint 21.3	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
OpenSUSE Leap 16.0	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
OpenSUSE Leap 15.6	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
OpenSUSE 15.4 and OpenSUSE 15.5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
OpenSUSE 42.3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
Oracle Linux 10.1	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Oracle Linux 10	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Oracle Linux 9.7	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Oracle Linux 9.6	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Oracle Linux 9.5	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Oracle Linux 9.4	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
Oracle Linux 8 (64-bit) (Supported versions: 8.0 - 8.10)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Oracle Linux 7.9 (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Distribution / OS Version	1.28.12	1.28.11	1.26.8	1.24.02	1.22.18	1.22.16	1.22.12	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) 10 (64-bit)	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Red Hat Enterprise Linux (RHEL) 9.7 (64-bit)	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Red Hat Enterprise Linux (RHEL) 9.6 (64-bit)	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
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	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	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)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Rocky 10.1	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Rocky 10	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Rocky 9.7	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Rocky 9.5	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
Rocky 8.10	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
SUSE Linux Enterprise Server (SLES) 16 (64-bit)	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
SUSE Linux Enterprise Server (SLES) 15 (64-bit) (Supported versions: 15SP7)	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
SUSE Linux Enterprise Server (SLES) 15 (64-bit) (Supported versions: 15S P2 and 15S P3)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SUSE Linux Enterprise Server (SLES) 12 (64-bit) (Supported versions: 12S P5)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

¹ Only Anti-Malware support.

Supported Browsers for the Browser Extension

The browser extension of Endpoint Security is supported for these browsers:

Operating System	Browser	URL Filtering	Threat Extraction & Threat Emulation	Zero Phishing	Password Reuse	Safe Search	Search Reputation	Malicious Script Protection	Data Loss Prevention
Windows	Chrome	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Edge Chromium	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Firefox	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	Brave ^{2,3}	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Internet Explorer	No	Yes	Yes	Yes	No	No	No	No
macOS ⁶	Chrome	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Firefox	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	Safari ¹	Yes	No	Yes	Yes	No	No	No	No
	Brave ^{3,4}	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Edge ⁴	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ChromeOS	Chrome ⁵	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes



Notes -

¹ Browser extension is supported in Safari version 14 and higher.

² Browser extension is supported in Brave version 1.43.89 and higher.

³ Brave for Windows is supported only with the Endpoint Security client version E86.70 and higher.

⁴ Brave and Edge for macOS is supported only with the Endpoint Security client version E87.40 and higher.

⁵ ChromeOS is supported only with the Browser Security client.

⁶ For macOS, DLP for browser extension is supported with the Endpoint Security client version E89.10 and later.

Migrating an On-premises Security Management Server to Endpoint Security

With Endpoint Security, you can migrate from an on-premises Security Management Server to a Endpoint Security cloud tenant in the Check Point Portal.

Use Case

You are using the on-premises Security Management Server to manage Endpoint Security clients installed on the endpoints. You wish to use the Endpoint Security cloud service on the Check Point Portal for management.

Prerequisites

Before migrating an on-premises Endpoint Security Management Server to Endpoint Security (EPMaaS), verify that the major versions of the EPMaaS service and the on-premises Security Management Server are identical. Migration is supported only when the major versions match.

To find the Endpoint Security (EPMaaS) service version:

1. Sign in to the [Check Point Portal](#).
2. Go to **Service Management**.
3. Note the **Endpoint Security service version**.

To find the Security Management Server version:

1. Connect to the Security Management Server using SSH.
2. Run the following command:

```
cpinfo -y all
```
3. In the output, locate the **Product Version** (for example, R82.10, R82 and so on).

Notes:

- Migration of Security Management Server from an environment with High Availability and Secondary server to Endpoint Security is not supported. For assistance, contact [Check Point Support](#).

- During the migration, the Endpoint Security Administrator Portal is temporarily locked and unavailable for use.

Known Limitations

See [sk179713](#).

Migrating to Endpoint Security

To migrate an on-premises Security Management Server to Endpoint Security:

1. Log in to [Check Point Portal](#) and access the Endpoint Security Administrator Portal.
2. Go to **Endpoint Settings > Migration Tool**.
3. Click **Download**.

The system downloads the migration script.

4. In the Endpoint Security Administrator Portal, copy the commands from the **Migration Tool** page **Export Data**.
5. Transfer the downloaded migration script to a directory on the Security Management Server.
6. On the Security Management Server, open the command line and run the commands you copied.

The system generates *encrypted_export.tgz* file.

7. Transfer the *encrypted_export.tgz* file to the local computer.
8. In the **Migration Tool** page **Import Data**, click **Browse** and select the *encrypted_export.tgz* file.
9. Click **Upload & Start**.

Note - Check Point Portal supports the upload of files up to 5 GB. If the export file size exceeds 5 GB, contact [Check Point Support](#).

You receive a confirmation mail when the import is complete.

10. Continue with the post-migration steps. For more information, see [sk179687](#).
11. Run the **Reconnect** tool on all the endpoints to reconnect to the Endpoint Security on the Check Point Portal. For more information, see ["Reconnect Tool" on page 65](#).



HARMONY

20 April 2026

CHECK POINT ENDPOINT SECURITY

Administration Guide



Deploying Endpoint Clients

Notes:

- Check Point does not support both the 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 Endpoint Security client.
- During the upgrade, you cannot remove the Full Disk Encryption component.

To deploy Endpoint Security 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 94](#)).
 - **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 106](#)).

**Notes:**

- Admins are recommended not to pre-install Endpoint Security when using cloning utilities like Acronis. It is recommended to install Endpoint Security after the clone is created, or at least to block the initial registration before creating the clone.
- If you have initiated to deploy the Endpoint Security client on an endpoint that is not yet added to the domain, see the [sk18127](#) to complete the deployment.
- For Mozilla Firefox users: If a user is accessing the browser for the first time after installing the Browser Security extension, a consent page appears that explains how the user's personal information is collected, used, and protected. The user must click **Confirm** to provide consent and activate the extension's protection features.

**Notes:**

- In Endpoint Management as a Service (EPMaaS), 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 Endpoint Security Web Management.

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

To enable token-limited registration:

1. Go to **Endpoint Settings > Authentication Settings > Installation Token**.
2. Select **Enable installation token** checkbox.
3. Click  to generate a token.

The token appears in the **Value** field.

4. To set an expiration date, select **Enable Expiration** and in the **Valid until** field, click  to select the date for the token expiry.
5. Click **Save**.

To copy the token, click .

Automatic Deployment of Endpoint Clients

Software deployment rules are supported for Windows, macOS and Linux.

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

To manage your Endpoint Security clients and install Endpoint Security Policy on them, you must first deploy the Initial Client to them.

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

-  **Notes-** 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 118](#)).
-  **Important** - If you want to switch to a US-DHS and EU compliant Anti-Malware security blade, make sure to switch to a complaint Endpoint Security Client before deploying the client. See ["Anti-Malware Settings" on page 127](#).
-  **Caution** - Windows Server 2016 and higher requires that you turn off Microsoft Windows Defender before you install the Endpoint Security client. Perform the instructions in the [sk159373](#) before you install or contact [Check Point Support](#) to request assistance with the installation.

Automatic Deployment of Endpoint Clients

Using the Tiny Agent

The Tiny Agent is supported with Windows, macOS, and Linux. It is an enhancement 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).
- Consolidates all the connection parameters in a single executable.
- 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.

i Notes The Tiny Agent is approximately 1.5 MB in size. However, the size of the resulting MSI file (Deployment package) depends on the capabilities selected for client installation and can range from 40 MB to 1.5 GB.

It is available for cloud deployments and for on-premises deployments running Endpoint Security Management ServerR81 or higher.



To deploy the Endpoint Security Client using the Tiny Agent:

1. Do any one of these:

Click	Steps																	
Policy > Deployment Policy > Software Deployment and then click Download Endpoint on the top banner.	a. Select a Download version and a Virtual group. b. Do one of these: ■ To download the file immediately, click Download for the relevant OS and transfer the file to the endpoints. <table><thead><tr><th>Client</th><th>OS</th><th>Downloaded file</th></tr></thead><tbody><tr><td rowspan="3">Endpoint</td><td>Windows</td><td><i>EPS_<Year>_<Version>.exe</i></td></tr><tr><td>macOS</td><td><i>EPS_TINY.zip</i></td></tr><tr><td>Linux</td><td><i>installScript.sh</i></td></tr><tr><td rowspan="3">Browse</td><td>Windows</td><td><i>BrowserSetup.exe</i></td></tr><tr><td>macOS</td><td><i>BrowserSetup.zip</i></td></tr><tr><td>ChromeOS</td><td><i>BrowserSetup_chromeOS_Laptop.exe</i> or <i>BrowserSetup_chromeOS_Desktop.exe</i></td></tr></tbody></table> ■ To download the file using a download link, click  and click Copy download link. When the download link is ready, the Send the Link by Email window appears. a. Click  to copy to the link. b. Share the download link with users (for example, by email) to download the file.	Client	OS	Downloaded file	Endpoint	Windows	<i>EPS_<Year>_<Version>.exe</i>	macOS	<i>EPS_TINY.zip</i>	Linux	<i>installScript.sh</i>	Browse	Windows	<i>BrowserSetup.exe</i>	macOS	<i>BrowserSetup.zip</i>	ChromeOS	<i>BrowserSetup_chromeOS_Laptop.exe</i> or <i>BrowserSetup_chromeOS_Desktop.exe</i>
Client	OS	Downloaded file																
Endpoint	Windows	<i>EPS_<Year>_<Version>.exe</i>																
	macOS	<i>EPS_TINY.zip</i>																
	Linux	<i>installScript.sh</i>																
Browse	Windows	<i>BrowserSetup.exe</i>																
	macOS	<i>BrowserSetup.zip</i>																
	ChromeOS	<i>BrowserSetup_chromeOS_Laptop.exe</i> or <i>BrowserSetup_chromeOS_Desktop.exe</i>																
Overview, and then click Download Endpoint on the top banner.																		
Overview > Getting Started > Let's Start Connect Your First Agent	a. In the Download & Install Endpoint agent widget, click Download. The Download & Install Endpoint Agent window appears. b. Click Online Install. c. From the Operating System list, select the OS. d. From the Version list, select the client version.																	

2. For Windows:

- Run the *exe* file to install the Endpoint Security client.
- If you want to use the *msi* file, then convert the *exe* file into a *msi* file:
 - a. Open the **Command Prompt** window by selecting **Run as administrator**.
 - b. Run:


```
cd [Path where you have downloaded the exe file]
```

For example, `cd C:\Users\User\Downloads`
 - c. Run:


```
EndpointSetup.exe /CreateMSI
```
 - d. Transfer the *msi* file to the endpoints and run the *msi* file to install the Endpoint Security client.

 **Note** - For silent installation, run `msiexec.exe /i [path to msi file]\EPS.msi /qn SILENTINSTALL=1`.

3. For macOS:

- a. Unzip the file and open the **EPS_TINY** folder.
- b. To install the Endpoint Security client, do one of these:
 - From Finder, double-click the directory **EPTiny.app**
 - In the terminal window, run:

```
./EPTiny.app/Contents/MacOS/EPTiny
```

4. For Linux:

- If you downloaded the **installScript.sh** file, run the file on the endpoint to install the Endpoint Security client.
- If you copy the download link, on the Linux machine, run:

- a. `curl [paste_download_link] -o install.sh`

- b. `chmod +x install.sh`

- c. `sudo ./install.sh install`

5. Continue with ["Deployment Rules" on page 103](#).

 **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 118](#)).

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 <code>eps.msi</code> 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 <code>EPS.msi</code>	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.

Using the Vanilla Client

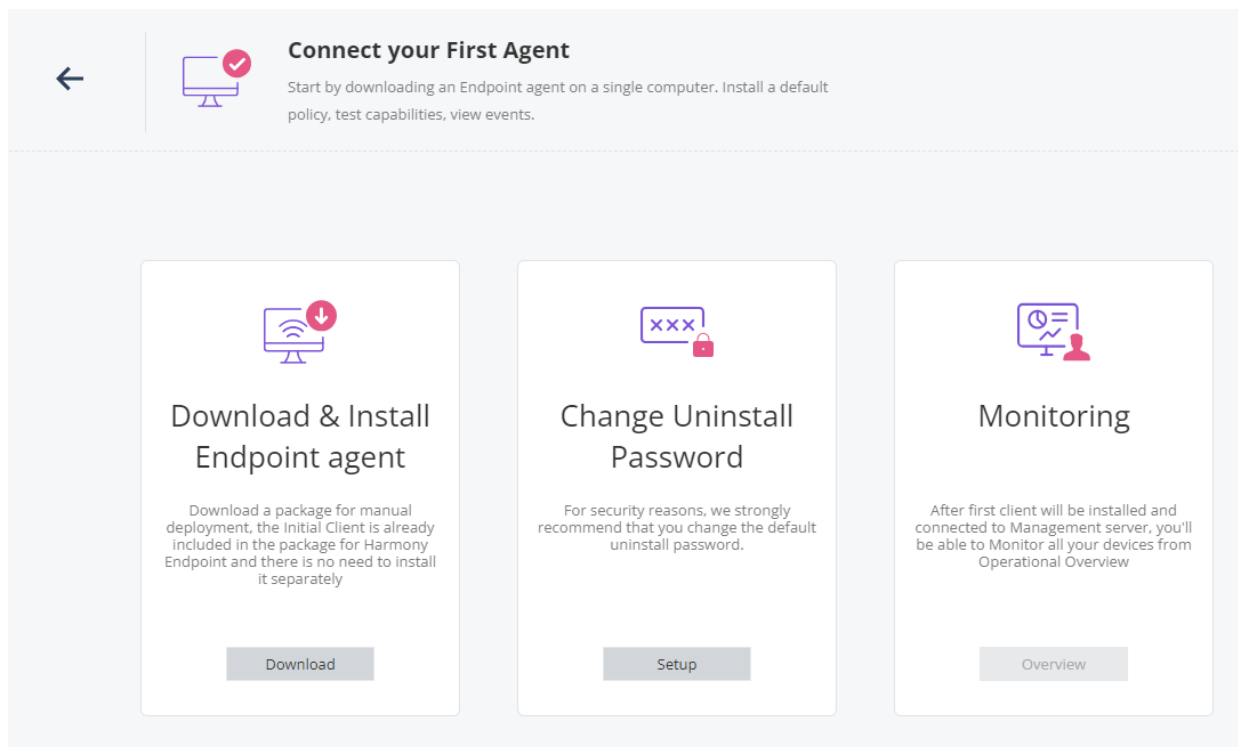


Note - The Vanilla client is supported only for Windows-based endpoints.

The Vanilla client is similar to the Tiny Agent but receives the connection parameters separately that prevents unauthorized clients to connect to the Endpoint Security Management Server.

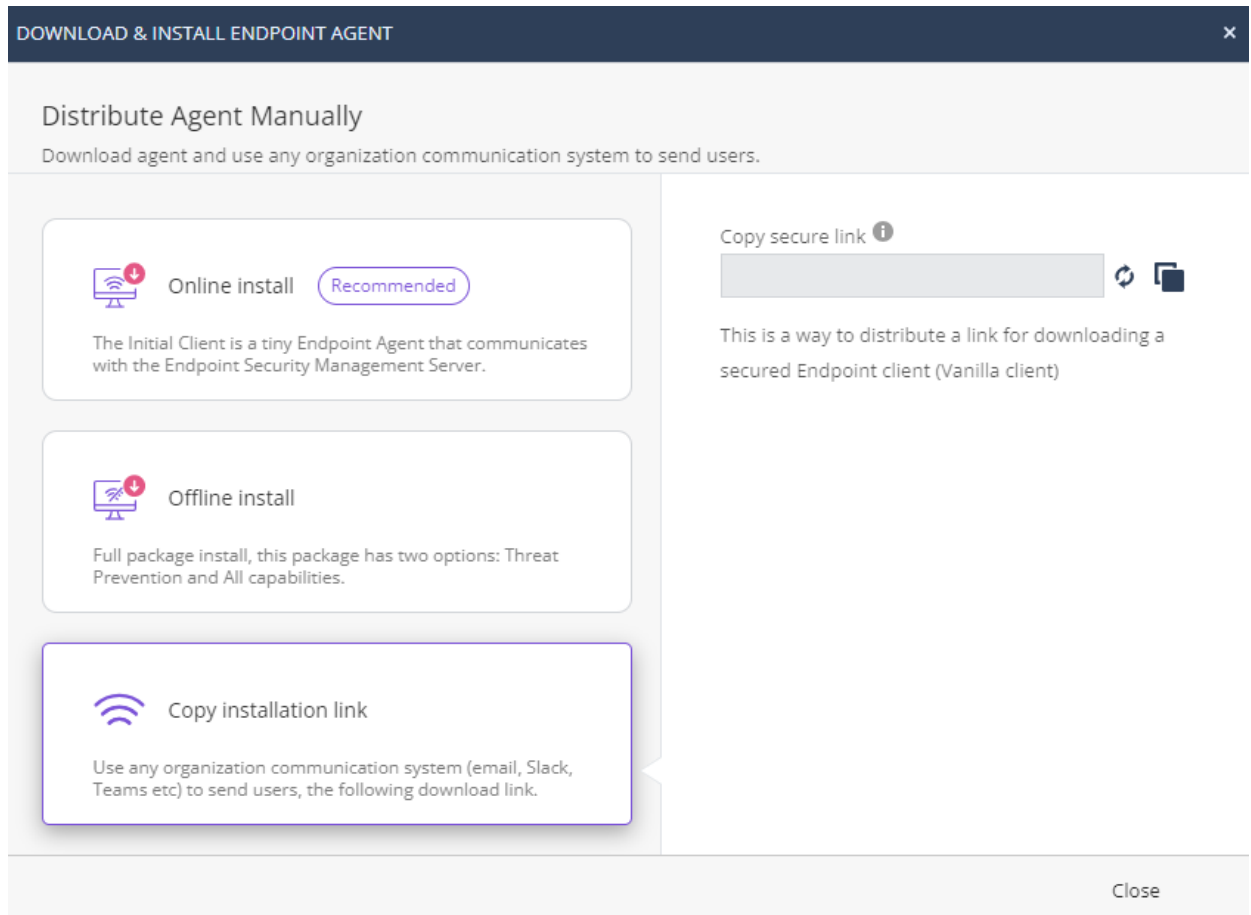
To deploy the Endpoint Security Client using the Vanilla Client:

1. Go to **Overview > Getting Started > Let's Start Connect Your First Agent**.



2. In the **Download & Install Endpoint agent** widget, click **Download**.

The **Download & Install Endpoint Agent** window appears.



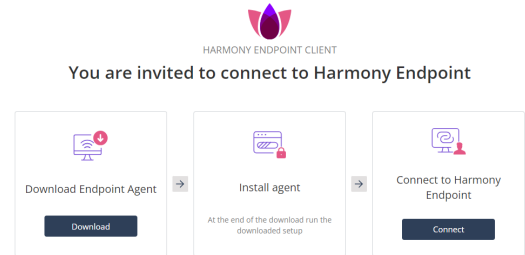
3. Click **Copy Installation link**.

4. Click  .

The download link appears in the field on the left.

5. Click  to copy the link.

6. Do one of these:

To	Do
Install the Vanilla client directly on the endpoint	a. On the endpoint where you want to install the client, open the link in a browser.  Note - Make sure that the user has Administrator role in the endpoint.  b. In the Download Endpoint Agent widget, click Download. The system downloads the <i>EndpointSetup.exe</i> file. c. Run the <i>EndpointSetup.exe</i> to register the client. The Ready to connect dialog box appears. d. Click OK. e. In the Connect to Endpoint Security widget, click Connect. The Endpoint Security dialog box appears that shows the client installation status.
Install the Vanilla client remotely on the endpoint	On the endpoint where you want to install the client, run this command as the Administrator: <pre>EndpointSetup.exe /url [link]</pre> The system downloads the Vanilla client, installs it and then connects to the Endpoint Security Management Server.

To	Do
Install the Vanilla client remotely on the endpoint using third-party distribution applications, for example, Microsoft Intune	- Run this command as the Administrator: <pre>EndpointSetup.exe /createmsi /url [link]</pre> The system downloads the <i>EPS.msi</i> file. - Distribute the <i>EPS.msi</i> file using third-party MDM application. For more information, see "Remote Installation of Initial Client" on page 118.

- When the installation is complete, the Endpoint Security Client is installed on the endpoint and connected to the Endpoint Security Management Server.
- Continue with ["Deployment Rules" below](#).

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 Endpoint Security client.

- c. Select **Capabilities**.

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

 **Note** - If the Endpoint Security Anti-Malware capability is installed, the third-party Anti-Malware status in the 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**.

See *"Installation and Upgrade Settings" on page 352* for local deployment options.

Manual Deployment of Endpoint Clients

You can export a package of Endpoint Security or Browser Security 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 Endpoint Security and there is no need to install it separately.



Note - Initial Client is not supported for Browser Security.



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" on page 127](#).



Caution - Windows Server 2016 and higher requires that you turn off Microsoft Windows Defender before you install the 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. Create the package for export

- a. Go to **Policy >Export Package**.
- b. Do any of these:
 - i. To export package for Endpoint Security, click **Endpoint Client**.
 - ii. To export package for Browser Security, click **Browse Client** and continue with ["Export the package or file" on page 112](#).
- 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**

- Select the **Package version**.

■ **macOS**

- Select the **Package version**.

■ **Linux**

- Select the **Package platform**.
- Select the **Package version**.

f. Select **Capabilities**.

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



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

- For general limitations on macOS, see [sk110975](#).

g. To add a new VPN site to the package, see *["Adding a New VPN Site to an Exported Package" on page 116](#)*.h. 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.

- i. 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** feature. It 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 173](#). 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**. For more information, see ["Configuring Full Disk Encryption" on page 363](#).

- **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](#). 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**.

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**.
- ii. Enable **Self-Unlock** for Full Disk Encryption. See [Advanced Pre-boot Settings](#).

■ 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.

- j. 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.

2. Export the package or file

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

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

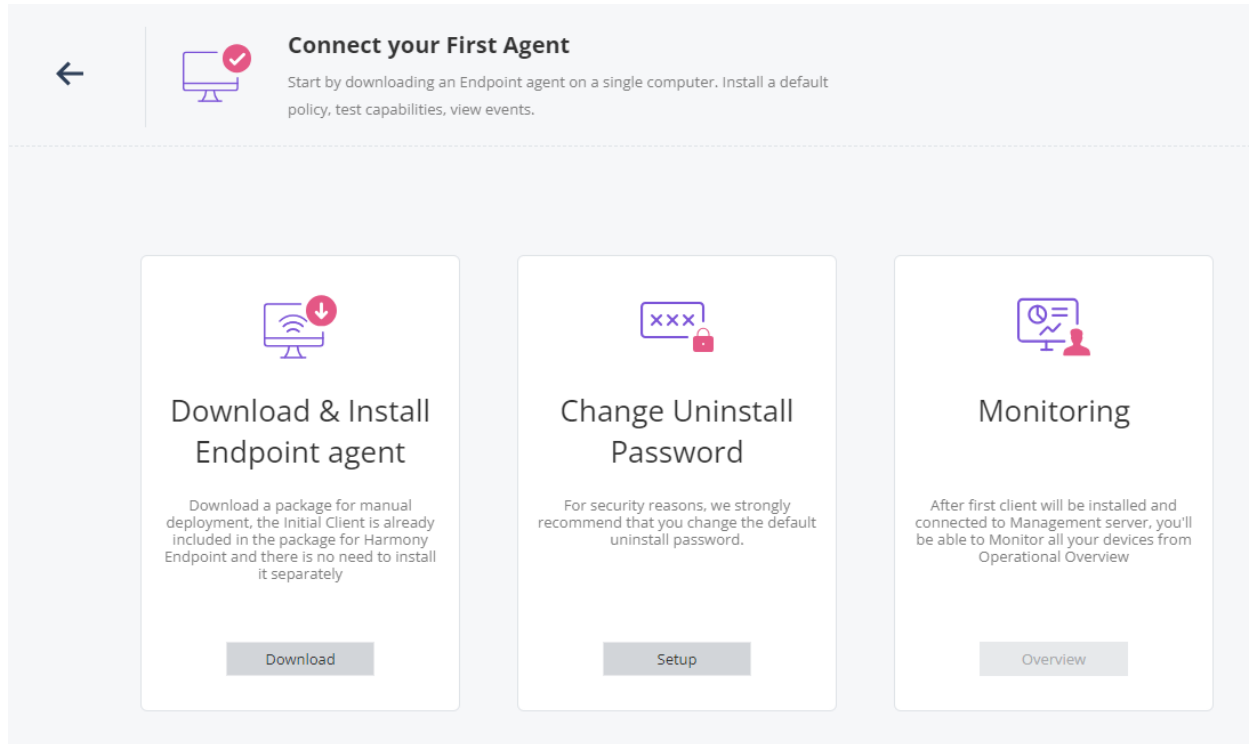
Note - Dynamic package is not supported for Browser Security.

3. Continue with *"Installing the Exported Package or Client" on page 115.*

Using the Offline Installation

 **Note** - This procedure applies only to Windows and macOS-based endpoints.

1. Go to **Overview > Getting Started > Let's Start Connect Your First Agent.**



2. In the **Download & Install Endpoint agent** widget, click **Download**.

The **Download & Install Endpoint Agent** window appears.

DOWNLOAD & INSTALL ENDPOINT AGENT

Distribute Agent Manually

Download agent and use any organization communication system to send users.

Online install Recommended

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

Offline install

Full package install, this package has two options: Threat Prevention and All capabilities.

Copy installation link

Use any organization communication system (email, Slack, Teams etc) to send users, the following download link.

Operating System

Windows

Version

Threat Prevention

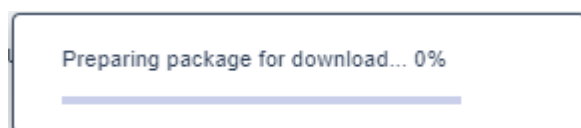
☒ Full package

DOWNLOAD

Close

- Click **Offline install**.
- From the **Operating System** list, select the OS.
- From the **Version** list, select the client version.
- Select **Threat Prevention** or **Full package**.
- Click **Download**.

The system prepares the package for download.



- Once the package is ready for download, click **Download**.



- Once the download is complete, continue with ["Installing the Exported Package or Client" on the next page.](#)

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 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 93*, 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 106*.
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 106](#).

Remote Installation of Initial Client

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

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.

You can install the Initial Client remotely using:

- Third-party tools
- Push Operation in the Endpoint Security Administrator Portal

 **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" on page 127](#).

Using Third-Party Tools

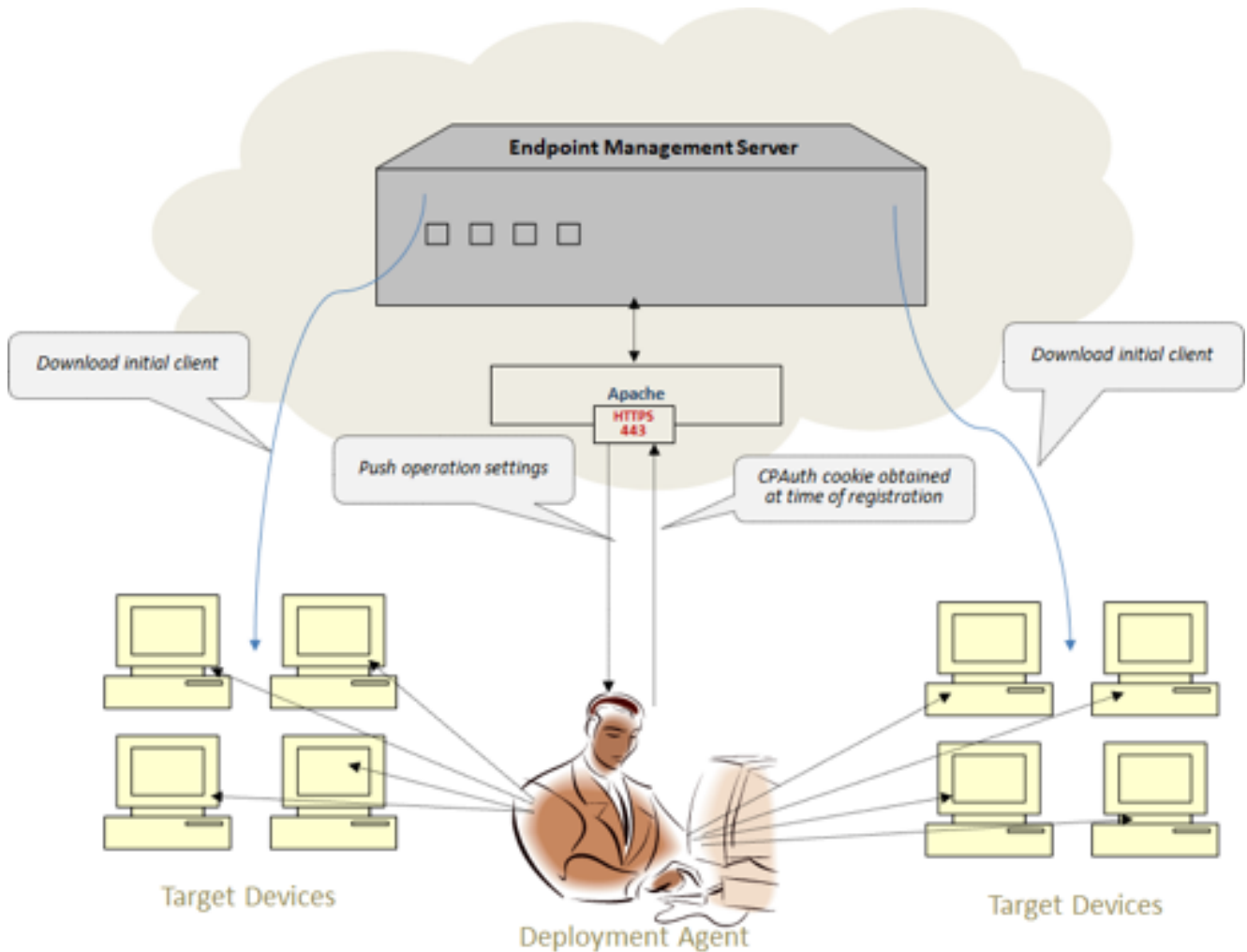
You can install the Endpoint Security Client on endpoints using third-party tools:

- To install the client on Windows-based endpoints:
 - Using Mobile Device Management (MDM), see [Endpoint Security for Windows MDM Deployment Guide](#).
 - Using System Center Configuration Manager (SCCM), see ["Appendix A - Deploying Endpoint Security Client using SCCM" on page 770](#).
- To install the client on macOS-based endpoints, see [Endpoint Security for macOS MDM Deployment Guide](#).

Using Push Operation

From Endpoint Security Client E84.40 and higher, using Push Operation, you can install the Initial Client remotely.

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



To install the Initial Client using Push Operation, see ["Remote Installation of Initial Client" on the previous page](#).

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.

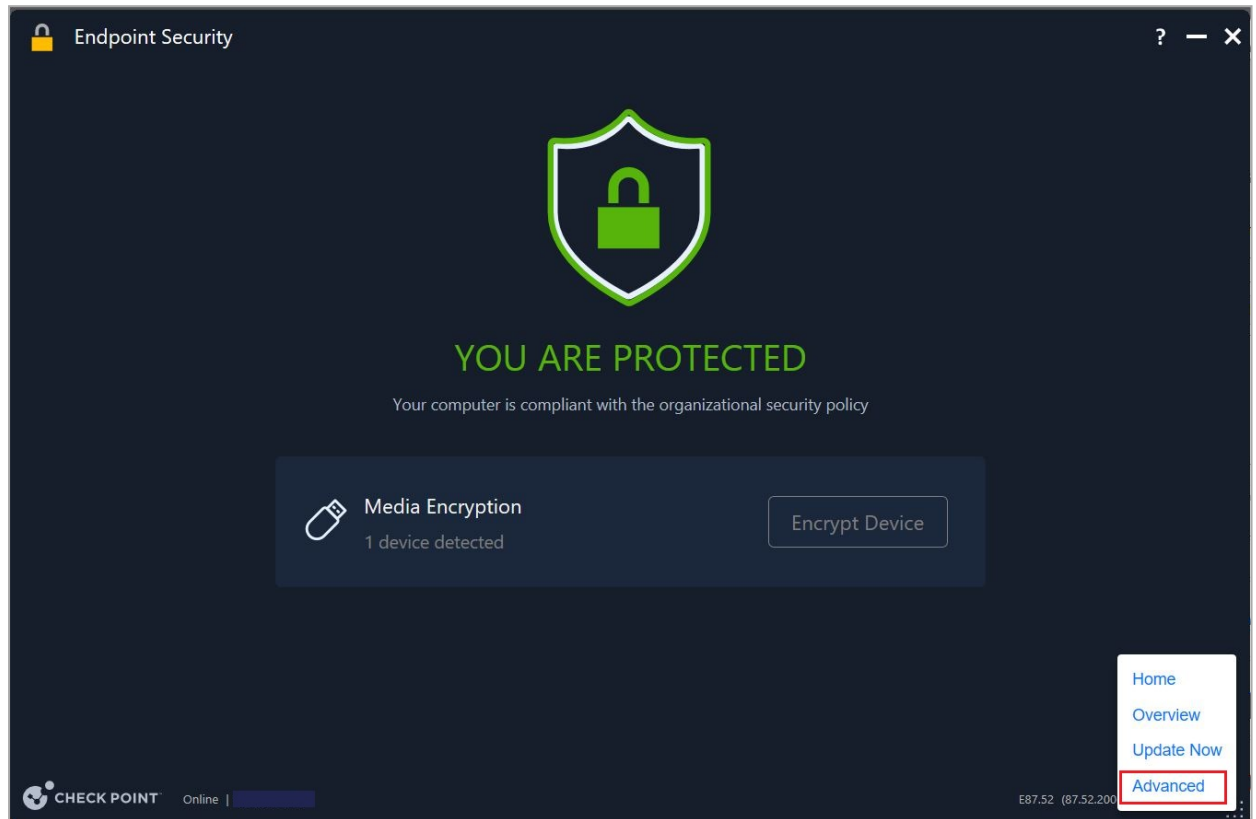
- ★ **Best Practice** - We recommend that the Deployment Agent has good hardware specs, network connectivity, availability and a "remote install" compatible Endpoint Security Client (E83.30 and higher).

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.

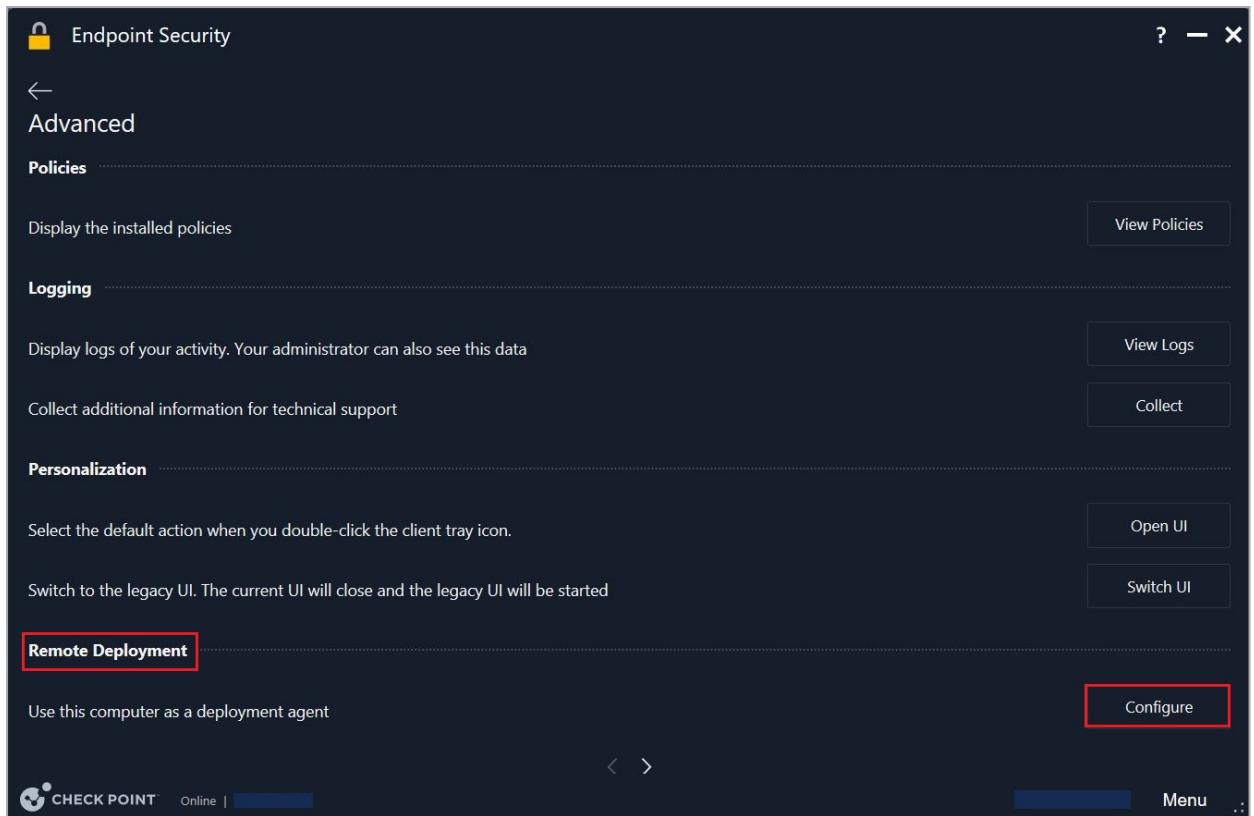
Certificates and DNS

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

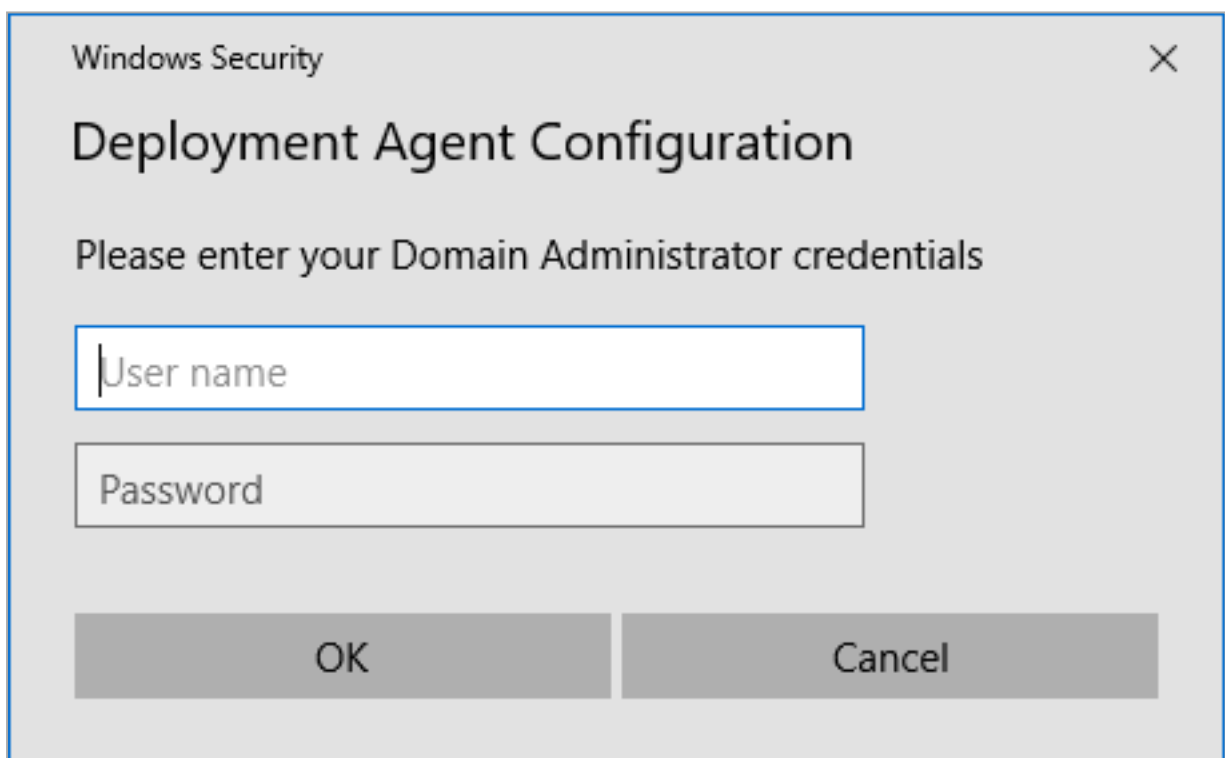
1. Open the Endpoint Security client screen, click **Menu** and select **Advanced**.



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 **Asset 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 "Asset 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

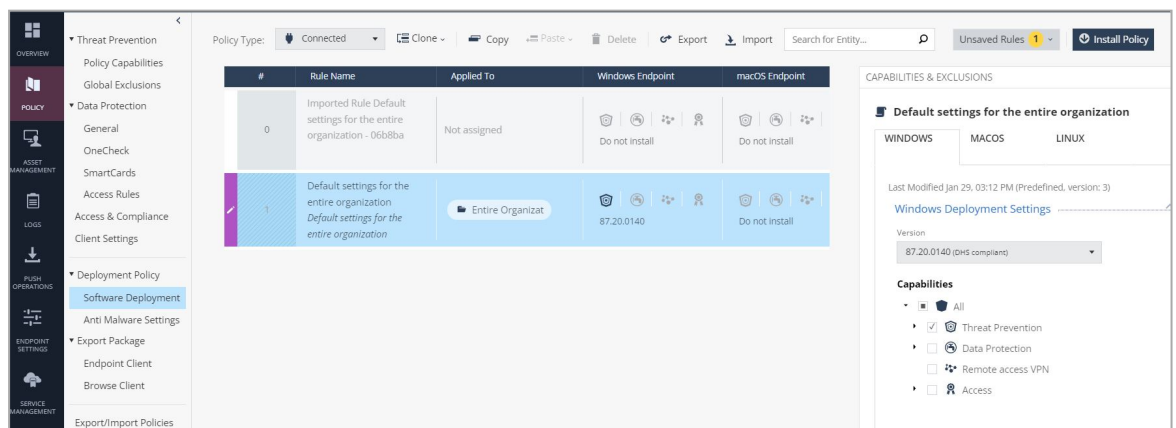
Upgrades are seamless to our users. A new type of Push Operation are rolled out and added to all Endpoint Security users.

Anti-Malware Settings

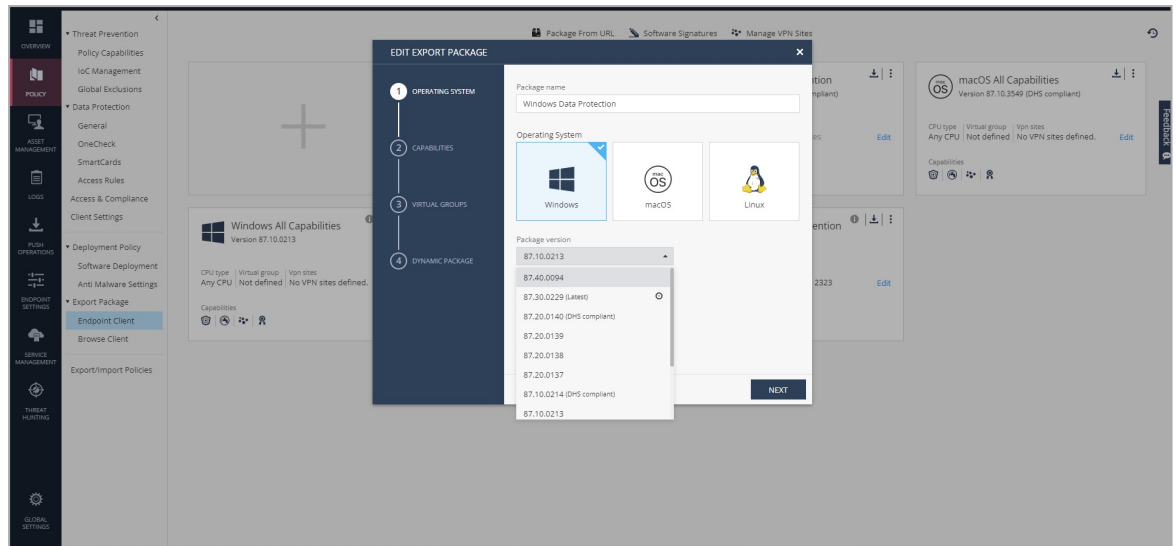
Endpoint Security allows you to switch to a United States Department of Homeland Security (DHS) and European (EU) regulations compliant Anti-Malware blade. After you successfully switch, you must redeploy the compliant Endpoint Security Client on the endpoints either through Deployment Rules or other methods.

To change to a US DHS and EU regulations compliant Anti-Malware blade:

1. Navigate to:
 - **Overview > Getting Started** and click > in the **Configure US-DHS and EU compliant method** icon.
 - **Policy > Deployment Policy > Anti-Malware Settings**.
2. Click **Switch To Compliant Version**.
A warning message appears.
3. Click **OK**.
Endpoint Security applies the changes instantly.
4. Redeploy the Endpoint Security Client on all endpoints. For more information, see:
 - ["Automatic Deployment of Endpoint Clients" on page 94](#)



■ *"Manual Deployment of Endpoint Clients" on page 106*



■ *"Remote Installation of Initial Client" on page 118*

After you redeploy the clients, the system automatically restarts the endpoints.



Note -

Please note that Check Point ceased support for DHS non-compliant Endpoint Security versions (E1) of Anti-Malware engine from September 29, 2024. For more information, see [sk182464](#).

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.

Configuring Alerts

You can configure alerts to receive a notification whenever an event occurs on an endpoint. Endpoint Security supports two types of alerts:

- ["Basic Alerts" below](#)
- ["Advanced Alerts" on page 133](#)

 **Note** - 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.

Basic Alerts

Basic alerts allows you to receive email notifications for these events:

- Compliance warning
- Failed deployment
- Encryption problem
- Anti-Malware issues
- Policy server out-of-sync
- Anti-Malware License Expiration Date

Configuring Basic Alert Messages

To define security alerts

1. Go to the **Endpoint Settings** view > **Alerts** > **Basic 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 be 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.

Advanced Alerts

Advanced alerts allows you to receive notifications for security and operational events. The notification is sent through preferred communication channels configured in Playblocks:

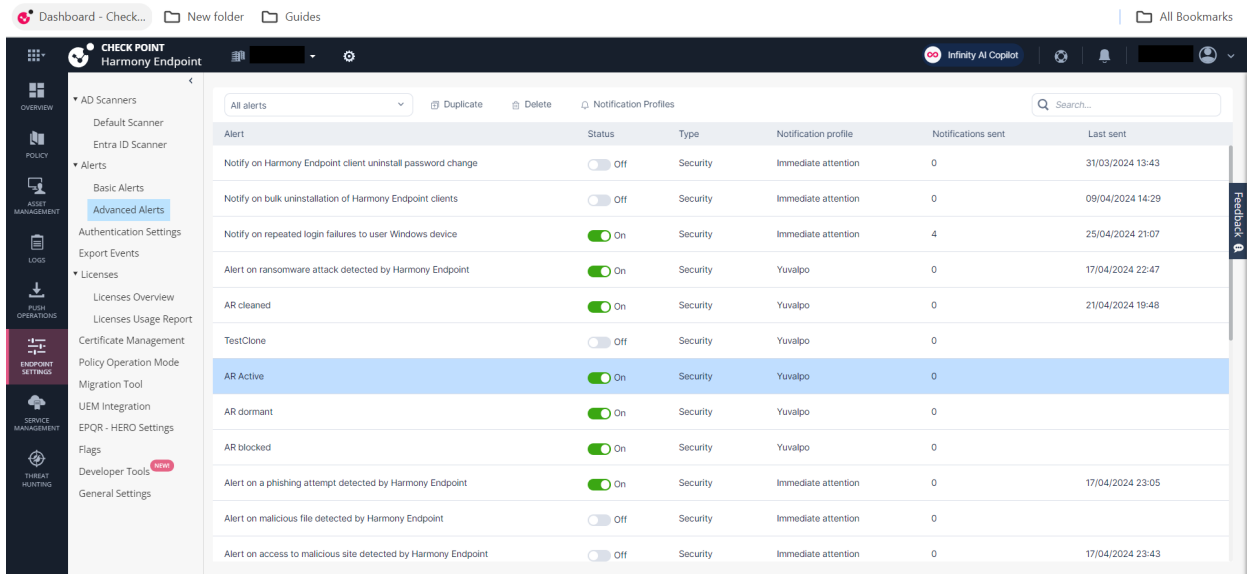
- SMS
- Email
- Slack
- Microsoft Teams

Notes -

- Make sure that you have configured [Connectors](#) and [Notifications](#) profiles in Playblocks. For more information, see [Playblocks Administration Guide](#).
- Advanced alerts are based on Playblocks capabilities and are limited to the regions it supports. To access these alerts, you must have an **Admin** role for the Infinity Playblocks application or inherit this role from the **Global** role. For more information, see [Check Point Portal Administration Guide](#).

Configuring Advanced Alerts

1. Go to **Endpoint Settings > Alerts > Advanced Alerts**.



Alert	Status	Type	Notification profile	Notifications sent	Last sent
Notify on Harmony Endpoint client uninstall password change	Off	Security	Immediate attention	0	31/03/2024 13:43
Notify on bulk uninstallation of Harmony Endpoint clients	Off	Security	Immediate attention	0	09/04/2024 14:29
Notify on repeated login failures to user Windows device	On	Security	Immediate attention	4	25/04/2024 21:07
Alert on ransomware attack detected by Harmony Endpoint	On	Security	Yuvalpo	0	17/04/2024 22:47
AR cleaned	On	Security	Yuvalpo	0	21/04/2024 19:48
TestClone	Off	Security	Yuvalpo	0	
AR Active	On	Security	Yuvalpo	0	
AR dormant	On	Security	Yuvalpo	0	
AR blocked	On	Security	Yuvalpo	0	
Alert on a phishing attempt detected by Harmony Endpoint	On	Security	Immediate attention	0	17/04/2024 23:05
Alert on malicious file detected by Harmony Endpoint	Off	Security	Immediate attention	0	
Alert on access to malicious site detected by Harmony Endpoint	Off	Security	Immediate attention	0	17/04/2024 23:43

2. Select an alert.
3. In the right pane:

The screenshot displays the Check Point Harmony Endpoint management console. The left sidebar contains navigation menus for Overview, Policy, Asset Management, Logs, RUGT Operations, Endpoint Settings, Service Management, and Threat Hunting. The main area shows a list of alerts under the 'Alerts' section. The alert 'Alert on access to malicious site detected by Harmony Endpoint' is selected, and its configuration is shown on the right.

Alert	Status	Type	Notification profile	Notifications sent
Alert on a phishing attempt detected by Harmony Endpoint	On	Security	Immediate attention	0
Alert on malicious file detected by Harmony Endpoint	Off	Security	Immediate attention	0
Alert on access to malicious site detected by Harmony Endpoint	Off	Security	Immediate attention	0
Alert on password reuse attempt detected by Harmony Endpoint	On	Security	Immediate attention	0
Alert on exploit attempt detected by Harmony Endpoint	Off	Security	Immediate attention	0
Alert on the outdated Harmony Endpoint Static Analysis capability	Off	Operational	Immediate attention	0
Alert on outdated Harmony Endpoint Offline Reputation capability	Off	Operational	Immediate attention	0
Alert on outdated Harmony Endpoint Behavioral Guard capability	Off	Operational	Immediate attention	0
Alert on disconnected Harmony Endpoint clients	Off	Operational	Immediate attention	0
Alert on Harmony Endpoint Compliance warnings	Off	Operational	Immediate attention	0
Alert on device restrictions by Harmony Endpoint	Off	Operational	Immediate attention	0
Alert on outdated Harmony Endpoint Anti-Malware	Off	Operational	Immediate attention	0
Alert if the device is not scanned by the Harmony Endpoint Anti-Malware capability	Off	Operational	Immediate attention	0

The configuration panel for the selected alert shows the following settings:

- Alert on access to malicious site detected by Harmony Endpoint**
- Status:** Off
- Profile name:** Immediate attention
- Edit notification in PlayBlocks:** [Link]
- Thresholds:**
 - Severity (Minimum): Low
 - Count events in time duration: 1 hours
 - Threshold (minimum number of events): 2
 - Threshold (minimum number of devices): 1
- Message:** [Empty field]
- Buttons:** Cancel, Save

- a. Turn on the **Off** toggle button.
- b. From the **Profile name** list, select a notification profile.

 **Note** - The system automatically displays the notification profiles created in Playblocks.

- c. In the **Thresholds** tab, configure the threshold parameters for the alert:

Alert Title	Alert Description	Threshold (Minimum number to trigger the action)
Security Alerts		
Alert on a phishing attempt detected by Endpoint Security	The automation notifies upon detection of phishing attack.	a. Severity (Minimum) - Select minimum severity level of the event to initiate the alert. b. Count events in time duration c. Threshold (minimum number of events) d. Threshold (minimum number of events)
Alert on exploit attempt detected by Endpoint Security	The automation notifies upon detection of exploit attack.	
Alert on access to malicious site detected by Endpoint Security	The automation notifies upon detection of access to malicious sites.	
Alert on password reuse attempt detected by Endpoint Security	The automation notifies upon reuse of the password.	

Alert Title	Alert Description	Threshold (Minimum number to trigger the action)
Alert on malicious file detected by Endpoint Security	The automation notifies upon detection of malicious files.	a. Attack status - Status of attack that must be considered for the alerts b. Severity (Minimum) - Select minimum severity level of the event to initiate the alert
Alert on ransomware attack detected by Endpoint Security	The automation notifies upon detection of ransomware attack.	c. Count events in time duration d. Threshold (minimum number of events) e. Threshold (minimum number of events)
Notify on bulk uninstallation of Endpoint Security clients	The automation notifies upon uninstallation of Endpoint Security clients on number of devices.	a. Number of uninstalled Endpoint Security clients b. In time duration
Notify on Endpoint Security client uninstall password change	The automation notifies upon change in Endpoint Security client uninstall password.	None

Alert Title	Alert Description	Threshold (Minimum number to trigger the action)
Notify on repeated login failures to user Windows device	The automation notifies upon detecting repeated login failures by the user on Windows devices.	a. Number of repeated failed login attempts b. Select Count failures for each user individually to count the failures for each user individually c. In time duration

Operational Alerts

Alert Title	Alert Description	Threshold (Minimum number to trigger the action)
Alert if Endpoint Security client capabilities stop running	The automation notifies if one or more capabilities on the Endpoint Security client stops running or the client is unable to report the capability status.	a. Number of devices found with this event b. Notify on alert activation c. Notify on alert resolution d. Remind every (Minutes) - Set interval for reminder notifications For example, If the threshold for number of devices with this event is set to 5, an automated alert will be sent once the event occurs in at least five endpoints.
Alert on Endpoint Security deployment failure	The automation notifies if the Endpoint Security Client deployment failed on the device.	
Alert if the device is not scanned by the Endpoint Security Anti-Malware capability	The automation alerts if the device was not scanned by Endpoint Security Anti-Malware since the specified duration.	
Notify on device restrictions by Endpoint Security	The automation notifies upon the device restrictions initiated by the Endpoint Security Compliance capability.	

Alert Title	Alert Description	Threshold (Minimum number to trigger the action)
Notify on Endpoint Security compliance warnings	The automation notifies upon the triggered compliance warnings.	
Alert on Endpoint Security compliance issues	The automation notifies upon the detected compliance issues in endpoints.	
Alert on Endpoint Security Anti-Malware license expiration	The automation notifies upon the Endpoint Security Anti-Malware license expiration. The parameters can be set to configure the frequency of the alert, time to alert before the license is about to expire and so on.	

- a. **Number of devices found with this event**
- b. **Near Expiry** - Time before expiration to initiate the alert
- c. **Notify on alert activation**
- d. **Notify on alert resolution**
- e. **Remind every (Minutes)** - Set interval for reminder notifications

Alert Title	Alert Description	Threshold (Minimum number to trigger the action)
Alert on disconnected Endpoint Security clients	The automation notifies if the Endpoint Security client is disconnected.	a. Number of devices found with this event b. Disconnected for - Minimum interval of disconnection to initiate the alert. c. Notify on alert activation d. Notify on alert resolution e. Remind every (Minutes) - Set interval for reminder notifications

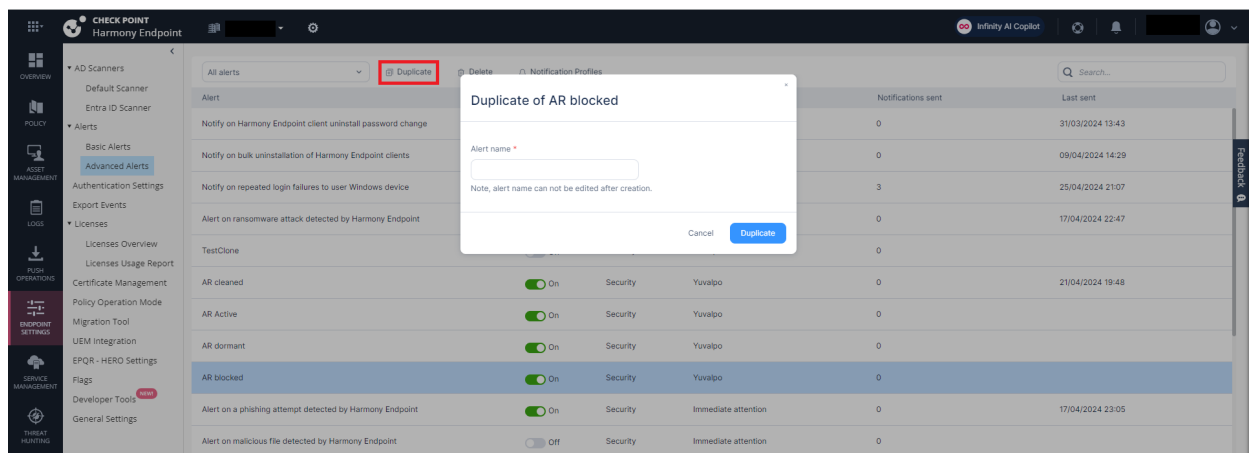
Alert Title	Alert Description	Threshold (Minimum number to trigger the action)
Alert on outdated Endpoint Security Anti-Malware	The automation notifies if the Endpoint Security Anti-Malware capability is outdated.	a. Number of devices found with this event b. Outdated - Minimum time a capability is outdated to initiate the alert c. Notify on alert activation d. Notify on alert resolution e. Remind every (Minutes) - Set interval for reminder notifications
Alert on outdated Endpoint Security Offline-Reputation capability	The automation notifies if the Endpoint Security Offline-Reputation capability is outdated.	
Alert on the outdated Endpoint Security Static Analysis capability	The automation notifies if the Endpoint Security Static Analysis capability is outdated.	
Alert on the outdated Endpoint Security Behavioral Guard capability	The automation notifies if the Endpoint Security Behavioral Guard capability is outdated.	

- d. On the **Messages** tab, you can view the **Subject** and **Message** of the alert.
- e. Click **Save**.

Duplicating an Advanced Alert

You can duplicate an alert and customize to use different thresholds and notification profiles.

1. Select the applicable alert from the list.
2. From the taskbar, click **Duplicate** button.



3. In the **Alert name** field, enter the alert name.
4. Click **Duplicate**.

Editing or Creating a Notification Profile

A notification profile is a configuration setting that defines who receives notifications, when they are sent, and how they are delivered, such as by email, SMS, Teams, or Slack, based on the event's importance.

Notification profiles are created in Playblocks and are automatically displayed in Endpoint Security. You can edit a notification either from Playblocks or Endpoint Security.

Note - To create and edit a notification profile in Playblocks, see [Notifications](#) section in the [Playblocks Administration Guide](#).

To edit a notification profile

1. From the taskbar, click **Notification profiles**.

The **Notification profiles** window appears.

Notification profiles

Profile name
Low attention (copy)

Profile is shared between portal applications and currently used by 0 alerts

Channels

Email

SMS

Slack

Microsoft Teams

☒ On

To *

bob1 x All Primary Administrators x x | v

fgdhdcdgs x

* Create new group

When *

Every 4 hours

Save as Cancel Save

2. From the **Profile name** list, select a profile.
3. Select a channel and turn on the toggle button.
4. Edit or specify these:
 - **To** - Recipients to receive the notification.
 - To create a new group, click **Create new group**.
 - a. In the **Group name** field, enter the group name.
 - b. Update the recipient information as follows:
 - **Emails** - For Email
 - **Phone numbers** - For SMS
 - **URL** - For Slack and Microsoft Teams
 - c. Click **Save**.
 - **When** - Time interval between notifications.
5. To create a new notification profile, click **Save As**.

- a. In the **Profile name** field, enter a profile name.
 - b. Click **Save**.
6. To save changes to the current profile, click **Save**.

How to Verify that Endpoint Security 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 -

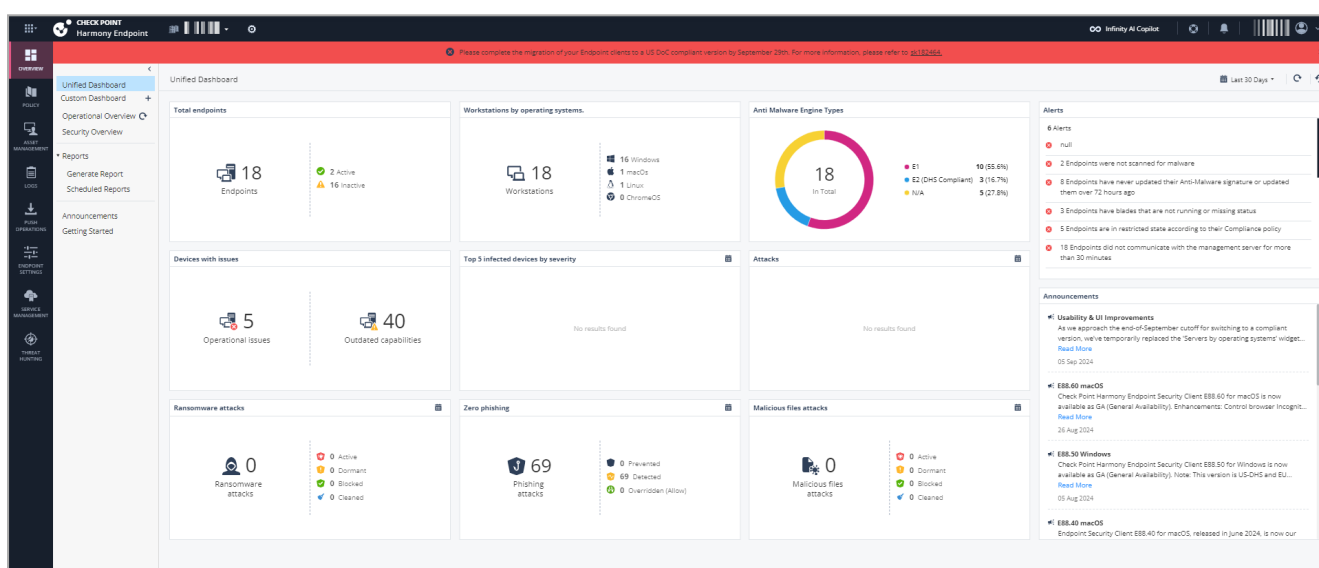
- Symantec.cloud is not supported by this command. To remove Symantec.cloud, navigate to *C:\Program Files\Symantec.cloud\PlatformAgent* and run *Uninstall.exe*.
- You cannot uninstall software products whose cached msi is not found on your computer.

Viewing Operational Overview, Security Overview and Reports

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

Unified Dashboard

The **Unified Dashboard** shows a consolidated view of the preselected widgets from the [Operational Overview](#) and [Security Overview](#), in addition to **Announcement** widget. The **Announcement** widget shows the latest news in the cyber security industry.



Custom Dashboard

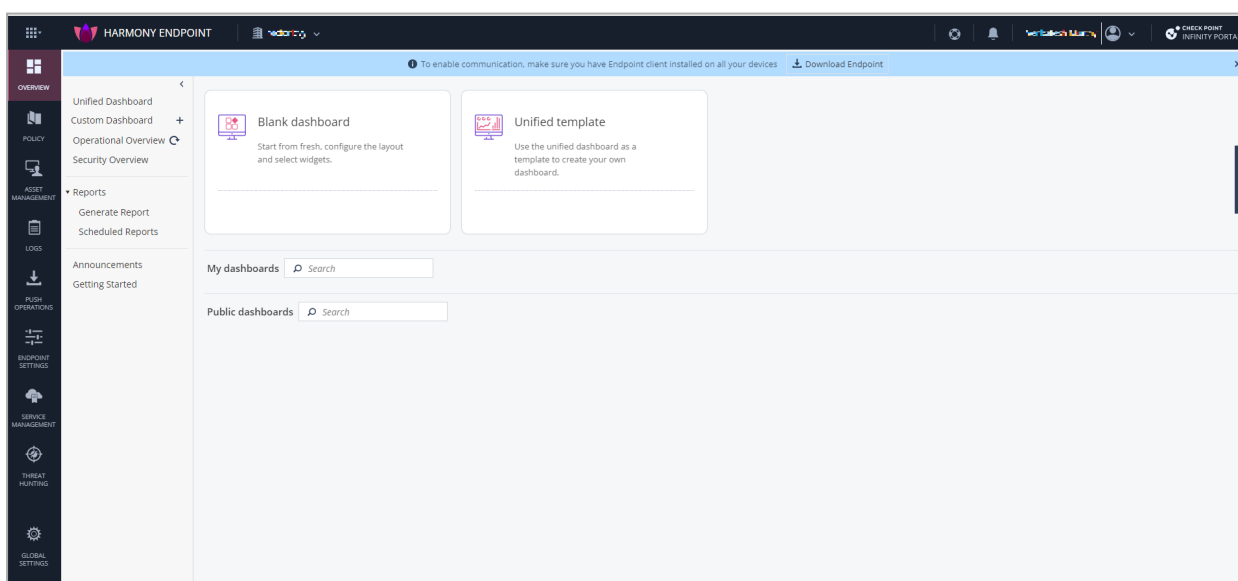
The **Custom Dashboard** allows you to create personalized dashboards with widgets of your preference and specify whether the dashboard should be private or public. **Private** dashboards are available only for you to view whereas, **Public** dashboards are available for all the users with access to the **Overview** page. However, only the owner of the dashboard can edit it.

Blank dashboard allows you to create a new dashboard with available widgets. **Unified template** allows you to customize the **Unified Dashboard**.

Creating a Custom Dashboard

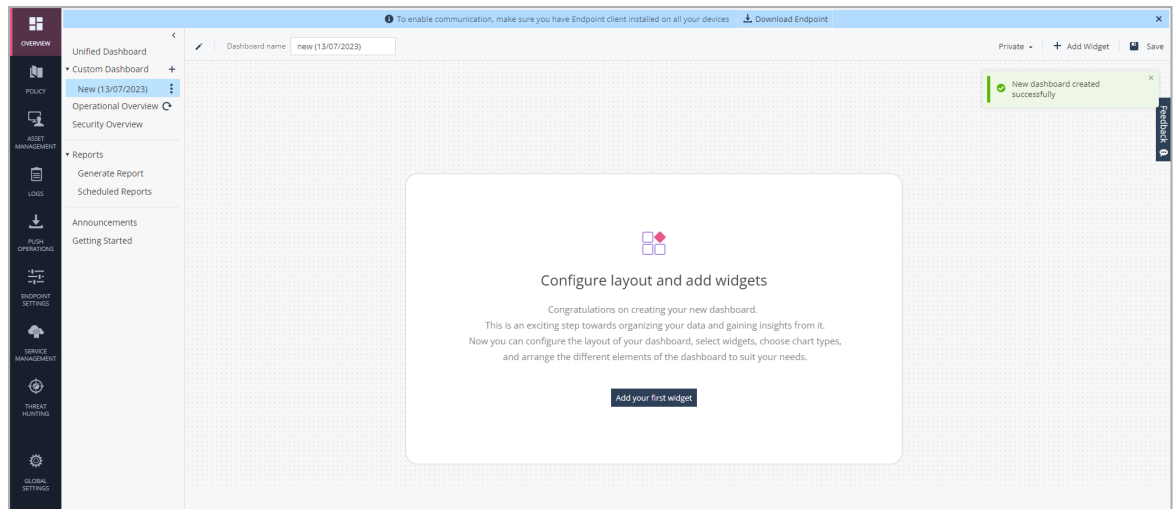


1. Go to **Overview** and click **+** next to **Custom Dashboard**.



2. To create a new custom dashboard from scratch:

- a. Hover over the **Blank dashboard** widget and click **Add**.



- b. In the **Dashboard name** field, enter a name.

- c. Click **Add Your First Widget**.

The **Add Widget** window appears.

3. To create a custom **Unified Dashboard**:

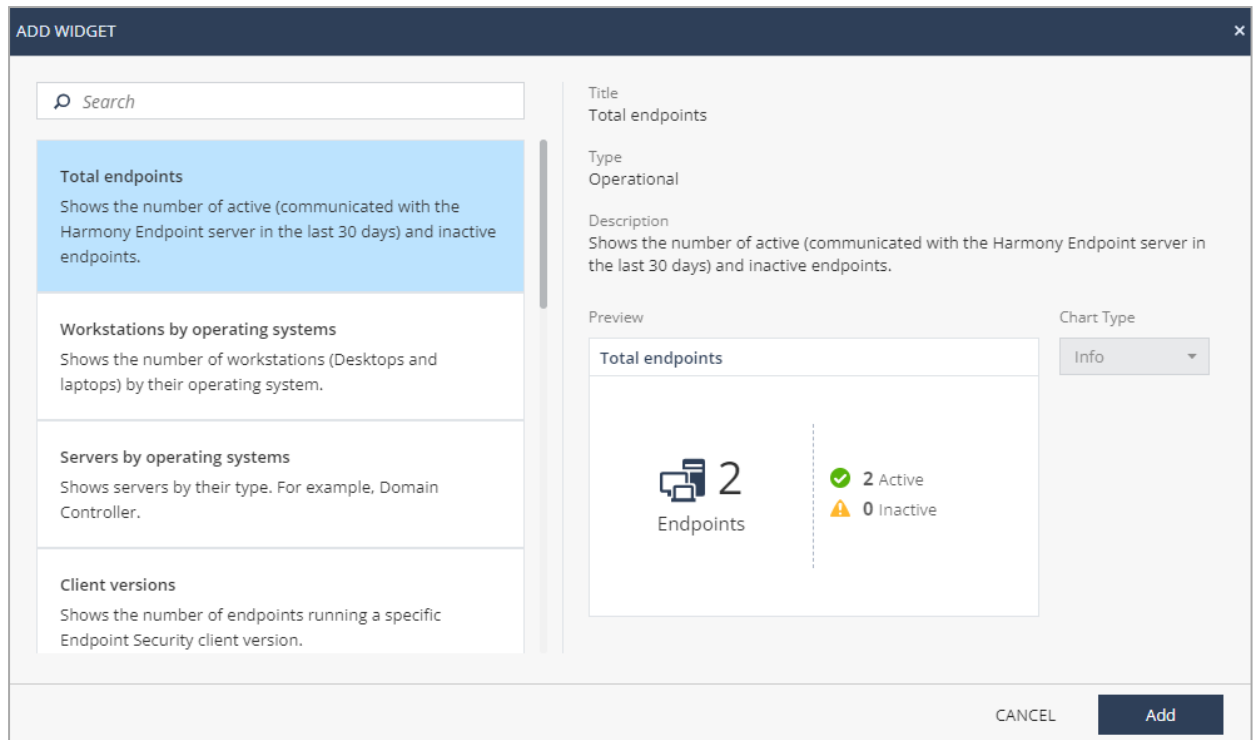
- a. Hover over the **Unified template** widget and click **Duplicate**.

- b. In the **Dashboard name** field, enter a name.

- c. Click **Add Widget**.

The **Add Widget** window appears.

4. From the left pane, select the widget and click **Add**.



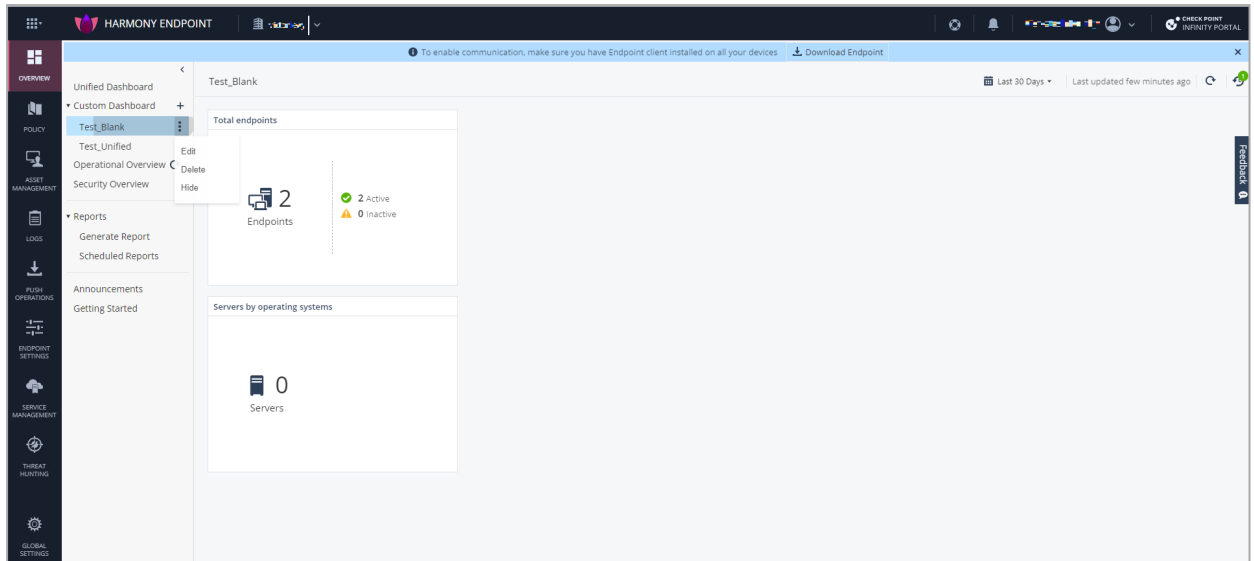
Note - The **Add** button is disabled if the widget is already added to the dashboard.

5. To add more widgets, click **Add Widget** and repeat step 4.
6. To delete a widget, on the widget, click and click **Delete**.
7. By default, all custom dashboards you create are set as **Private**. To make the custom dashboard available to all users with access to the **Overview page**, from the **Private** list on the upper-right corner, click **Public**. The system adds the dashboard under **Public dashboards** for other users.
8. Click **Save**.

The dashboard appears under **Custom Dashboard** on the left navigation pane, and it is also listed under **My dashboards** in the **Custom Dashboard** page.

Managing a Custom Dashboard

1. Click Overview.



2. To edit a dashboard:

- a. Expand **Custom Dashboard**.
- b. Click  for the dashboard you want to edit and click **Edit**.
- c. Make the necessary changes and click **Save**.

 **Note** - You cannot edit dashboards created by other users.

3. To delete a dashboard, expand **Custom Dashboard**, click for the dashboard you want to delete and click **Delete**.

 **Note** - You cannot delete dashboards created by other users.

4. To hide a dashboard, expand **Custom Dashboard**, click for the dashboard you want to hide and click **Hide**. The dashboard is removed from the list under **Custom Dashboard** on the left navigation pane.

5. To unhide a dashboard, click , hover over the dashboard you want to unhide and click **Add**. The dashboard is added to the list under **Custom Dashboard** on the left navigation pane.

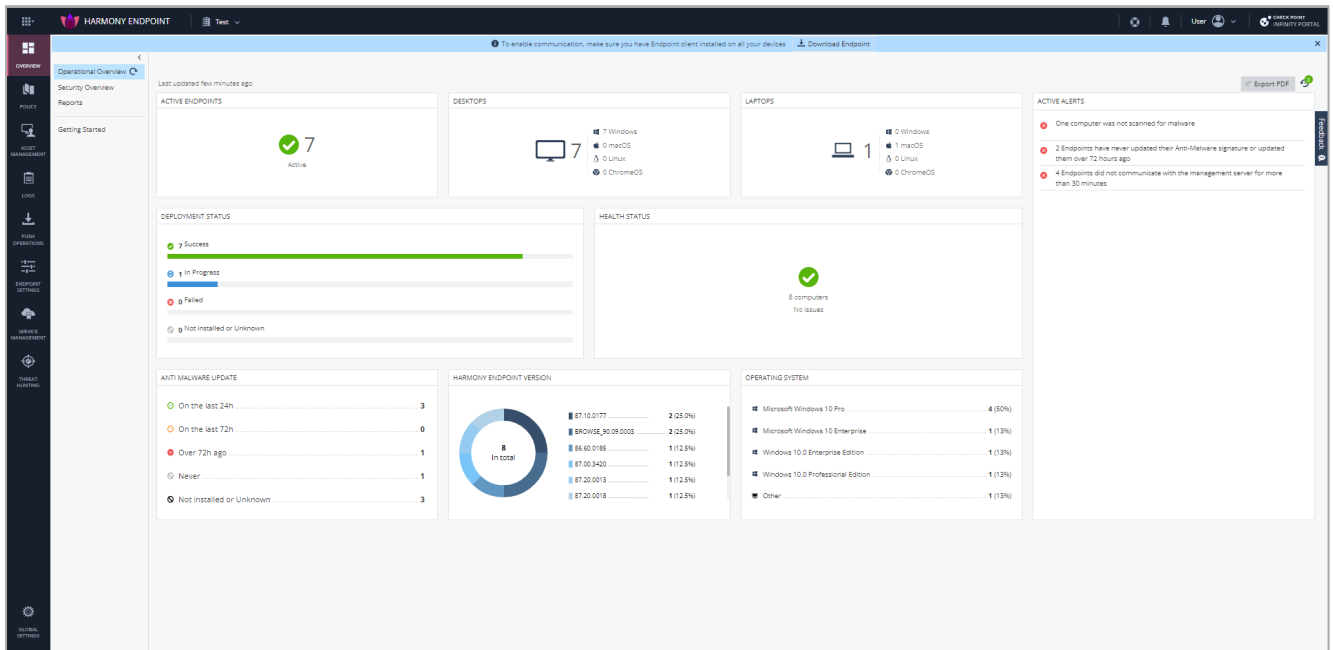
6. To duplicate a dashboard, click , hover over the dashboard and click **Duplicate**.

Operational Overview

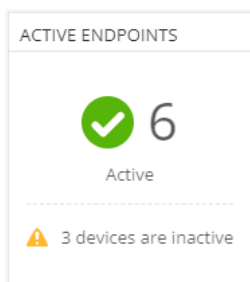
The **Operational Overview** page shows the deployment status of Endpoint clients in your organization, their health status, client versions and operating systems on the clients.

To view the **Operational Overview** page, click **Overview > Operational Overview**.

To export the **Operational Overview** data to a pdf, click **Export PDF**.



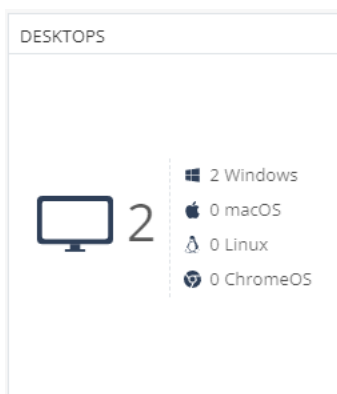
Active Endpoints



The **Active Endpoints** widget shows the number of active and inactive endpoints.

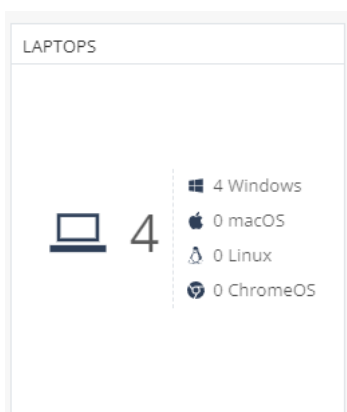
Click the numbers in the widget to view the endpoints in the ["Asset Management View" on page 173](#) tab.

Desktops



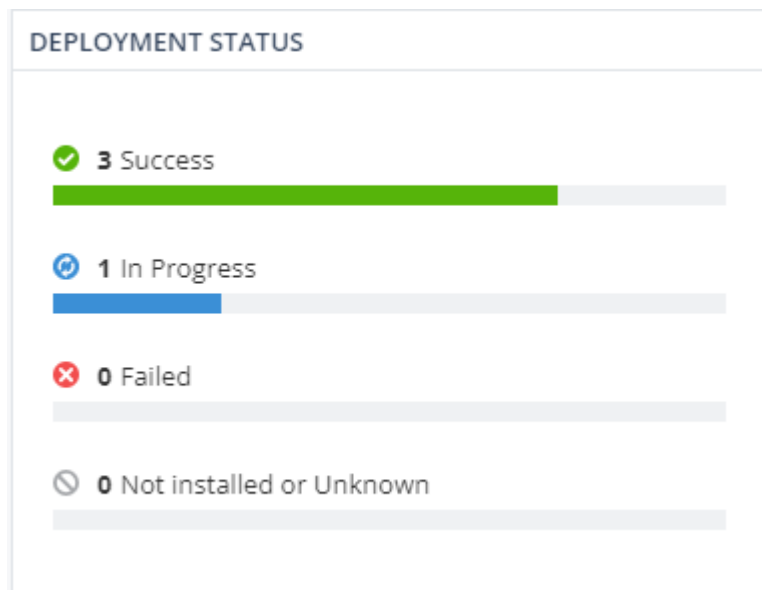
The **Desktops** widget shows the number of desktops by Operating System (Windows, macOS, Linux, and ChromeOS) that have the Endpoint Security client installed.

Laptops



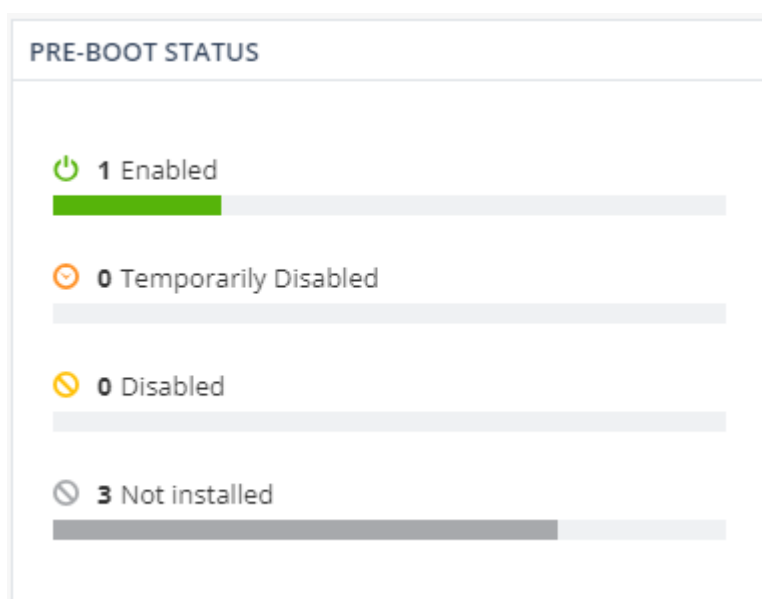
The **Laptops** widget shows the number of laptops by Operating System (Windows, macOS, Linux, and ChromeOS) that have the Endpoint Security client installed.

Deployment Status



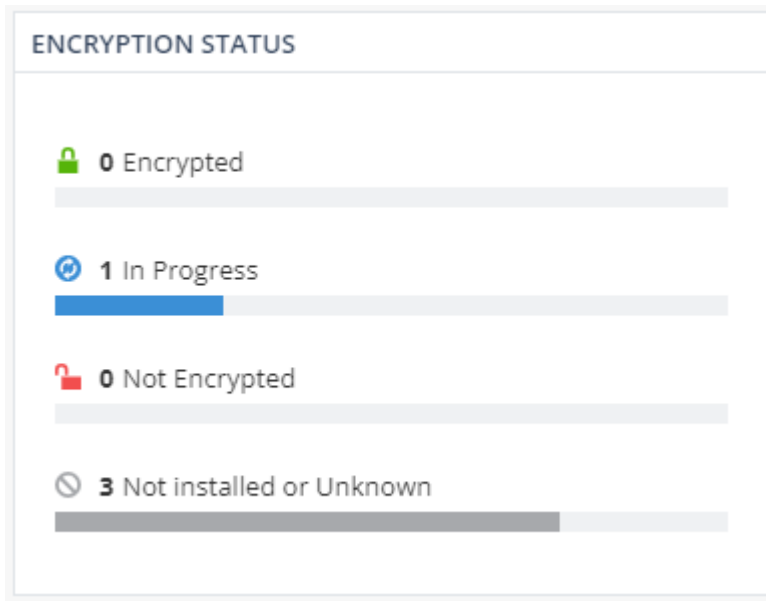
The **Deployment Status** widget shows the number of endpoints by deployment status.

Pre-boot Status



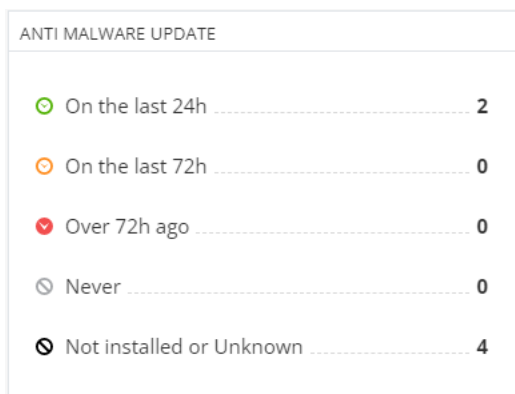
The **Pre-boot Status** widget shows the number of endpoints by pre-boot status.

Encryption Status



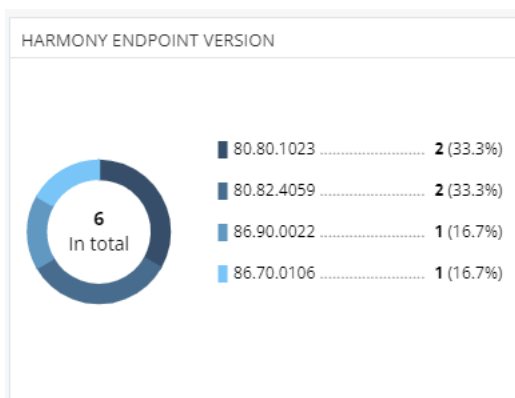
The **Encryption Status** widget shows the number of endpoints by encryption status.

Anti-Malware Update



The **Anti-Malware Update** widget shows the number of endpoints that had the Anti-Malware blade updated over different time periods.

Endpoint Security Version



The **Endpoint Security Version** widget shows the number of endpoints running a particular Endpoint Security client version.

Operating System

OPERATING SYSTEM	
 Microsoft Windows 10 Pro	2 (33%)
 Windows 7 Home Premium	1 (17%)
 Mac OSX	1 (17%)
 Windows Vista	1 (17%)
 Other	1 (17%)

The **Operating System** widget shows the number of endpoints running a particular Operating System.

Alerts

Alerts	
	One endpoint has never updated its Anti-Malware signature or updated them over 72 hours ago
	One endpoint has blades that are not running or missing status
	4 Endpoints did not communicate with the management server for more than 30 minutes

The **Alerts** widget shows the active alerts on all the endpoints in the account.

Security Overview

Shows the attack statistics of the Endpoint Security clients.

The information is presented in these widgets:

- **Hosts Under Attack**
- **Active/Dormant Attacks**
 - **Active Attacks** - Malicious process was executed and the system was infected. Termination and quarantine of the process or other elements of the attack is disabled in the policy.
 - **Dormant Attack** - No malicious process was executed but the system was infected. Quarantine of one of the detected files failed.
- **Cleaned/Blocked Attacks**
 - **Cleaned Attack** - Malicious process was executed and the system was infected. Termination and quarantine of all attack elements succeeded.
 - **Blocked Attack** - No malicious process was executed. Quarantine of all detected files succeeded.
- **Infected Hosts**
- **Attacks Timeline**



Note - The **Active**, **Dormant** and **Cleaned** attacks are based on **Forensics and Remediation** capability:

- If there is no remediation or the remediation capability is turned off, then attack status is either **Dormant** or **Blocked**.
- If remediation capability is turned on:
 - If the process is actively running and the remediation is **Terminate**, then the status is **Active**.
 - If the remediation failed, then status is **Dormant**.
 - If the remediation was successful, then the status is **Cleaned**.

Reports

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

- **Threat Analysis Report** - Shows the latest security events.
- **Threat Analysis Report Anonymized** - Shows the latest security events without specific user names.

- **High Risks Cyber Attack Report** - Shows the analysis of all the Endpoint Security events by statuses of the attack pillars.
- **Web Activity Checkup** - Shows the web activity in the organization.
- **Threat Emulation Report** - Shows a report about scanned and malicious files.
- **Threat Extraction Report** - Shows the insights on the downloaded files.
- **Software Deployment Report** - Shows the deployment status in the organization.
- **Policies Report** - Shows policies status.
- **Vulnerability Management** - Shows the detected vulnerabilities.
 - 📘 **Note** - Available only to customer subscribed to this feature and with server version R81.10.x and higher.
- **Posture Management** - Shows Vulnerability Management and patches information.
 - 📘 **Note** - Available only to customer subscribed to this feature and with server version R81.10.x and higher.
- **Operational Report** - Shows the operational status of the endpoints.
- **Compliance Report** - Shows the compliance status in the organization.
- **Check Point Cyber Security Report** - Shows the latest security trends as per Check Point.

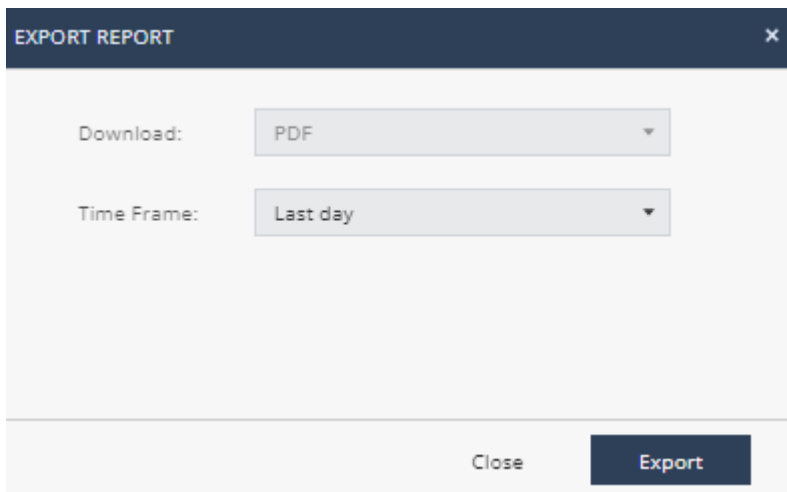
Generate Report



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.



EXPORT REPORT

Download: PDF

Time Frame: Last day

Close Export

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).
- Reports are generated in real-time for Vulnerability Management and Posture Management.

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.

SCHEDULE REPORT - 2023 THREAT ANALYSIS REPORT

Name:

2023 Threat Analysis Report

Frequency:

Daily

Time:

00

:

00

UTC Now: 04:06

Recipients:

Search...

- The Scheduled Report takes 24 hours to become effective after scheduling it.
- For performance reasons, it is recommended to schedule reports to run in off-peak hours.
- The default time zone for the schedule report is UTC. For example, to schedule the report at 1:00 A.M EST, specify the Time as 6:00 A.M (depending on Daylight Savings Time).

Close

Schedule

- From the **Generate Report** page, select the report, click  and select **Schedule Report**.

SCHEDULE REPORT - THREAT EMULATION REPORT

Name: Threat Emulation Report

Format: PDF

Time Frame: Last day

Frequency: Daily

Time: 00 : 00 UTC Now: 04:14

Recipients: Search...

- The Scheduled Report takes 24 hours to become effective after scheduling it.
- For performance reasons, it is recommended to schedule reports to run in off-peak hours.
- The default time zone for the schedule report is UTC. For example, to schedule the report at 1:00 A.M EST, specify the Time as 6:00 A.M (depending on Daylight Savings Time).

Close

Schedule

- From the **Name** list, select the report.
- From the **Time Frame** list, select the period for the report:
 - Last day**
 - Last 7 days**
 - Last 30 days**
- 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 Endpoint Security.

Browser Settings

Disabling Incognito Mode, BrowserGuest Mode, and InPrivate Mode

Overview

The browser extension is not installed automatically if the Incognito, Guest or InPrivate mode is enabled in your browser. We recommend that you disable these modes to secure your users.

Chrome on Windows

To disable Incognito mode and BrowserGuest mode:

1. Select **Start** and type **CMD**.
2. Right-click **Command Prompt** and select **Run as administrator**.

The Command Prompt window appears.

3.

To disable	Run
Incognito mode	<code>REG ADD HKLM\SOFTWARE\Policies\Google\Chrome /v IncognitoModeAvailability /t REG_DWORD /d 1</code>
BrowserGuest mode	<code>REG ADD HKLM\SOFTWARE\Policies\Google\Chrome /v BrowserGuestModeEnabled /t REG_DWORD /d 0</code>

Firefox on Windows

To disable InPrivate mode:

1. Select **Start** and type **CMD**.
2. Right-click **Command Prompt** and select **Run as administrator**.

The Command Prompt window appears

3.

To disable	Run
InPrivate mode	<code>REG ADD HKLM\SOFTWARE\Policies\Mozilla\Firefox /v DisablePrivateBrowsing /t REG_DWORD /d 1</code>

Microsoft Edge on Windows

To disable BrowserGuest mode and InPrivate mode:

1. Select **Start** and type **CMD**.
2. Right-click **Command Prompt** and select **Run as administrator**.

The Command Prompt window appears

3.

To disable	Run
BrowserGuest mode	REG ADD HKLM\SOFTWARE\Policies\Microsoft\Edge /v BrowserGuestModeEnabled /t REG_DWORD /d 0
InPrivate mode	REG ADD HKLM\SOFTWARE\Policies\Microsoft\Edge /v InPrivateModeAvailability /t REG_DWORD /d 1

Brave on Windows

To disable Incognito mode, Incognito mode with Tor and BrowserGuest mode:

1. Select **Start** and type **CMD**.
2. Right-click **Command Prompt** and select **Run as administrator**.

The Command Prompt window appears

3.

To disable	Run
Incognito mode	REG ADD HKLM\SOFTWARE\Policies\BraveSoftware\Brave /v IncognitoModeAvailability /t REG_DWORD /d 1
BrowserGuest mode	REG ADD HKLM\SOFTWARE\Policies\BraveSoftware\Brave /v BrowserGuestModeEnabled /t REG_DWORD /d 0
Incognito mode with Tor	REG ADD HKLM\SOFTWARE\Policies\BraveSoftware\Brave /v TorDisabled /t REG_DWORD /d 1

Chrome on macOS

To disable incognito mode and BrowserGuest mode:

1. In the Finder, click **Go > Utilities**.
2. Open the **Terminal** app.

The Terminal app window appears.

3.

To disable	Run
Incognito mode	<code>defaults write com.google.chrome IncognitoModeAvailability -integer 1z</code>
BrowserGuest mode	<code>defaults write com.google.Chrome BrowserGuestModeEnabled -bool false</code>

Firefox on macOS

To disable InPrivate mode:

1. In the Finder, click **Go > Utilities**.
2. Open the **Terminal** app.

The Terminal app window appears.

3.

To disable	Run
InPrivate mode	<code>defaults write /Library/Preferences/org.mozilla.firefox DisablePrivateBrowsing -bool TRUE</code>

Microsoft Edge on macOS

To disable BrowserGuest mode and InPrivate mode:

1. In the Finder, click **Go > Utilities**.
2. Open the **Terminal** app.

The Terminal app window appears.

3.	To disable	Run
	BrowserGuest mode	defaults write com.microsoft.edge BrowserGuestModeEnabled -integer 0
	InPrivate mode	defaults write com.microsoft.edge InPrivateModeAvailability -integer 1

Enabling the Browser Extension on a Browser with Incognito or InPrivate Mode

You can enable Browser Security extension on your browser in Incognito or InPrivate mode.

To enable the Browser Security extension on Chrome in the Incognito mode:

1. In your browser's address bar, type `chrome://extensions/` and locate the Browser Security extension.
2. Click **Details** and enable **Allow in Incognito**.

To enable the Browser Security extension on Edge in the InPrivate mode:

1. In your browser's address bar, type `Edge://extensions/` and locate Browser Security extension.
2. Click **Details** and select **Allow in Private** checkbox.

To enable the Browser Security extension on Firefox in the InPrivate mode:

1. In your browser's address bar, type `about:addons` and select **Extensions**.
2. Click the **Browser Security** Extension.
3. In **Run in Private Windows**, select **Allow**.

Ending the Browser Process Running in the Background

When you close Chrome and Edge browsers with the Browser Security extension installed, the browser process continues to run in the background. You can perform these procedures to end the browser process running in the background.

To end the Chrome browser process running in the background:

1. Select **Start** and type **CMD**.
2. Right-click **Command Prompt** and select **Run as administrator**.

The Command Prompt window appears.

3. Run:

```
REG ADD HKLM\SOFTWARE\Policies\Google\Chrome /v  
BackgroundModeEnabled /t REG_DWORD /d 0
```

4. Press **Enter**.

To end the Edge browser process running in the background:

1. Select **Start** and type **CMD**.

2. Right-click **Command Prompt** and select **Run as administrator**.

The Command Prompt window appears.

3. Run:

```
REG ADD HKLM\SOFTWARE\Policies\Microsoft\Edge /v  
BackgroundModeEnabled /t REG_DWORD /d 0
```

4. Press **Enter**.

Browser Extension Pinning

For more information, see **Browser Settings** in ["Web & Files Protection" on page 259](#).

Managing Accounts in the Check Point Portal

You can create additional accounts for the same user.

To create an additional account for an user

1. Go to the registration page:
<https://portal.checkpoint.com/register/endpoint>
2. For each new account, use a different account name (Company Name).

To switch between accounts

At the upper-middle of your screen, near the name **Endpoint Security**, click the current account and select the required account from the drop-down menu.

To add an administrators to an account

1. From the left navigation panel, click **Global Settings** (at the bottom of the panel).
2. In the top left section, click **Users**.

The list of currently defined users appears.

3. From the top toolbar, click  **New**.

The **Add User** window opens.

4. Configure the required details:

- **Name**
- **Email**
- **Phone**
- **User Groups**
- **Global Roles** - select **Admin** or **User Admin**

 **Note** - If the administrator you wish to add is not registered in Endpoint Security, they receive a registration invitation to establish login credentials for the portal.

5. Click **Add**.

Managing Browser Security

Overview

You can install and manage the Browser Security lightweight client through Endpoint Security. This is suitable when you want to provide only the Browser Security service to users and manage its policy through Endpoint Security. For more information on Browser Security, see [Browser Security Administration Guide](#).

After you install the Browser Security client:

- You can apply same **Client Setting** and **Threat Prevention** policies to both Browser Security and Endpoint Security clients.
-  in **Asset Management > Computers** indicates a Browser Security client. You can filter for clients using the **Agent Installed** filter.
- The **Overview** and **Logs** menu show the information for both Browser Security and Endpoint Security clients.

To manage Browser Security client through Endpoint Security:

1. Install the Browser Security client from Endpoint Security. For more information, see ["Manual Deployment of Endpoint Clients" on page 106](#)
2. Apply an existing **Threat Prevention** policy or [configure a new Threat Prevention policy](#) for the Browser Security client.
3. Apply an existing **Client Setting** policy or [configure a new Client Setting policy](#) for the Browser Security client.

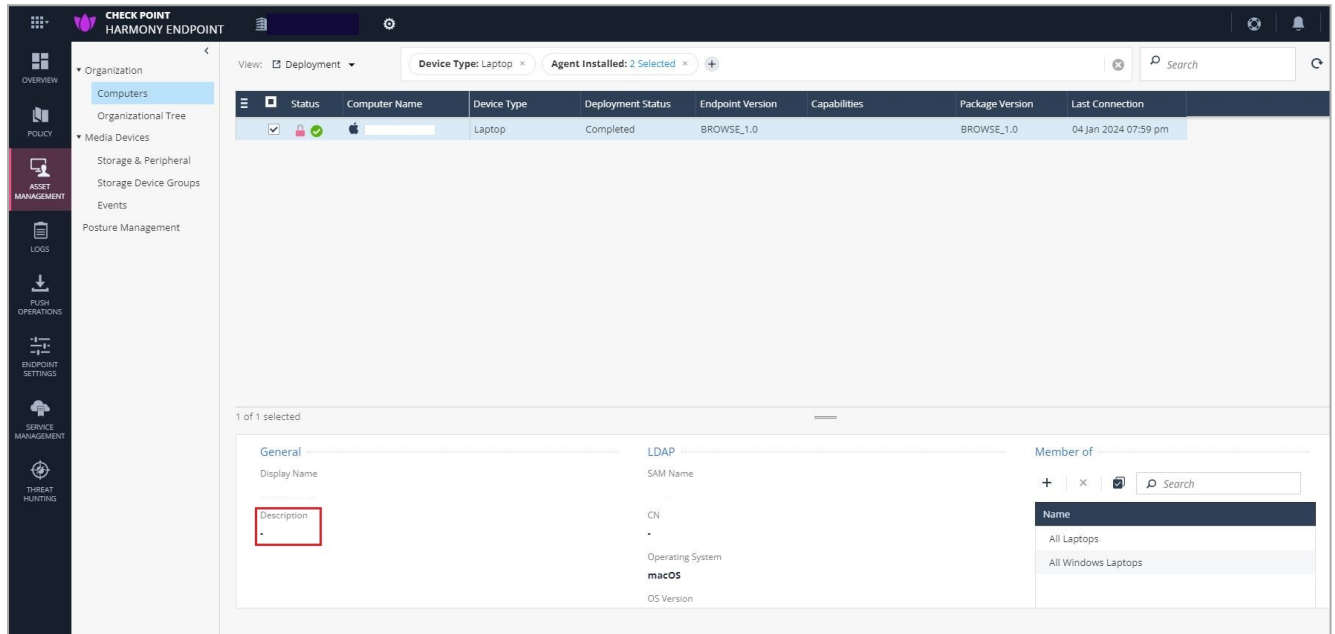
Limitations

Browser Security does not support **Push Operations** and **Threat Hunting**.

Viewing Computer Information

Asset Management View

The **Asset Management** view shows information on each computer, such as deployment status, active components on the computer, client 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.

Select a View

From the **View** drop-down on the top left, select a preconfigured view:

- Deployment
- Compliance
- Health
- Full Disk Encryption
- Anti-Malware
- Host Isolation
- Anti-Bot
- Policy Information
- Custom

Creating a Custom View

You can create a custom view with the filters and table column you specify.

To create a custom view:

1. Apply the filters and select the required columns for the table and click **Update**. For more information, see ["Table Filters and Column Description" on page 176](#).
2. From the **View** drop-down, click **Save View**.

The **Save New View** window appears.

3. In the **View name** field, enter a name for the view. For example, Active Laptops.
4. In the **Select what will be saved in this view** section, select the required checkbox:
 - **Filters**
 - **Table Columns**
5. Click **OK**.
6. To delete a **Custom View**:
 - a. From the **View** drop-down, go to **Custom Views**.
 - b. Hover over the custom view and click .

Status Icon

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

Status Icon	Description
	Indicates Endpoint Security client.
	Indicates Browser Security 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 top of the screen to filter the information in the table.

To add filters:

1. In the **Filters** pane, click **+**.
2. Select the required filter or search for the filter using the **Search** bar. For information on the filters, see ["Table Filters and Column Description" on the next page](#).
3. Click **Update**.

The system updates the table automatically for the added filters.

To modify the table:

1. Click  on the top left header of the table.
2. To select the columns for the table, search and select the columns.
3. To change the column position in the table, drag and drop the column to the required position.
4. Click **Update**.

Tip - The URL in the address bar of the web browser captures the filters you specify for the table. You can bookmark the URL to go to the **Asset Management > Computers** page and view the table with the specified filters.

Table Filters and Column Description

Filter / Column Name	Description
Status	Status of the connected computer. For more information, see "Status Icon" on page 174 .
Computer Name	Name of the connected computer.
Active	Active computers. Computers that have communicated with Endpoint Security in the last 30 days.
Deleted	Deleted computers.
Domain Name	Domain name of the connected computer.
Agent Installed	Endpoint Security client or Browse client installed on the computer.
Endpoint version	Version of the Endpoint Security client or browser extension installed on the computer.
Operating System	Version of the Operating System installed on the computer.
Device Type	Type of the computer (Desktop or Laptop).
Compliance Status	Compliance status of the computer.
Admin Comment	Comment for the device. For example, This computer is used by Bob and Jane.
Deployment Status	Deployment status of the computer.
Deploy Time	Time when the client was installed on the computer.
Inactive Capabilities	Capabilities that are not active on the computer. Reasons can be any of these: ■ Security blade is inactive ■ Security blade has stopped ■ Status of the security blade is missing
Deployment Error Code	Error code of the failed deployment.

Filter / Column Name	Description
Deployment Error Description	Error description of the failed deployment.
OS Build	Operating System build number of the computer.
Organizational Unit	Active directory tree of your organization.
FDE Status	Full Disk Encryption status of the computer.
FDE Version	Full Disk Encryption engine version.
Pre-boot Status	Full Disk EncryptionPre-boot screen status of the computer.
Pre-boot Status Updated On	Full Disk EncryptionPre-boot screen status last update time.
TPM Id	Trusted Platform Module (TPM) Manufacturer ID of the computer.
TPM Status	TPM status of the computer.
TPM Version	TPM specification version implemented in the computer.
Isolation Status	Isolation status of the computer.
Last Connection	Last connection date of the computer.
Endpoint CPU Tuning	Recommended CPU tuning usage based on the Run Diagnostics Push Operation performed either manually or automatically every 4 hours. ▪ Highly Recommended - Endpoint CPU usage is critically high and requires immediate action to address it. ▪ Recommended - Endpoint CPU usage is high and Check Point recommends that you take the necessary action to address it. ▪ Optional - Endpoint CPU usage is moderate and there is no immediate necessity to address it. ▪ Not needed - Endpoint CPU usage is optimal and does not require any action. Click the tuning recommendation level to view the diagnostics report.
Synced On	Sync date of the computer.

Filter / Column Name	Description
Last Logged In User	Last logged in user name on the computer.
Last Logged In FDE User	Last logged in user name on the Full Disk Encrypted computer.
Anti-Malware Status	Anti-Malware blade status of the computer.
Anti-Malware Updated on	Last update time of the Anti-Malware blade.
Virtual Groups	Pre-defined and custom virtual groups of the computer.
Remote Help Requests	Full Disk Encryption locked users that are pending for help (One-Time Logon or Password Change)
Anti-Malware Dat Version	Dat version of the Anti-Malware.
Dat Date	Dat date in a human readable format (Example: 09 Apr 2018 10:52 AM)
Total Infected	Number of files infected on the computer as detected by Anti-Malware.
Anti-Malware Infections	Anti-Malware name of infections found on the computer.
Package Name	Software Deployment package name (Example: Check Point Endpoint Total Security x64)
Package Version	Client version installed on the computer (Example: 86.25.5060)
Software Deployment Policy Name	Deployment policy name installed on the computer.
Software Deployment Policy Version	Deployment policy version installed on the computer.
Anti-Bot State	Anti-Bot blade status on the computer.
Protection Name	Anti-Bot protection name.

Filter / Column Name	Description
Scanned on	Anti-Malware last scan time.
Total Quarantined	Number of files quarantined by Anti-Malware.
Compliance Violations	Name of compliance violation on the computer.
Smart Card Status	Smart Card blade status on the computer.
Enforced & Installed Policy Name	Enforced and installed policy name.
Enforced & Installed Policy Version	Enforced and installed policy version.
Threat Emulation Status	Threat Emulation availability status.
Threat Emulation Reputation Status	Threat Emulation reputation status.
Static Analysis Update	Last time when the Threat Emulation Static Analysis was updated.
Offline Reputation Update	Last time when the Threat Emulation Offline Reputation was updated.
Behavioral Guard Update	Last update time of Behavioral Guard.
Installed Patch	Installed DA Windows patch version. For information on patch upgrade, see "Local Deployment Options" on page 352 .
Policy Profile	Profiles available for each blade in the policy.

Filter / Column Name	Description
Threat Hunting Status	Threat Hunting status on the Endpoint Security Client. The supported statuses are: ▪ Available - Threat Hunting is installed and running. ▪ Not Available - Threat Hunting is installed but not running due to an error. For the error description, see the Threat Hunting Error Description column. ▪ Not installed - Threat Hunting is supported by the client but not installed. ▪ N/A - Threat Hunting is not supported by the client. Upgrade to the client version 87.20 or higher.
Threat Hunting Error Description	Threat Hunting describes the reason why Threat Hunting is not running on the Endpoint Security Client. The supported values are: ▪ Available ▪ Not installed ▪ Authentication Failed ▪ Data Uploading Failed ▪ Fetching Settings Failed ▪ URL Creating Failed ▪ Connection Failed  Note - Threat Hunting error description is not supported by <i>"Filters" on page 175</i>.
Anti-Malware License Expiration Date	Shows the expiry date and time of the Anti-Malware license.

Filter / Column Name	Description
Browser Status	Shows the browser and the Browser Security extension status on the endpoint. The supported statuses are: ■ Not Installed - ○ The browser is not installed. ○ The browser is installed but not used since the last reboot. ○ The browser is used but the extension is disabled by the policy. For example,  indicates that the Chrome browser is not installed. ■ Running - The browser is active and the extension was detected. For example,  indicates that the Edge browser is active and the extension on it was detected. ■ Not Running - The browser is active but the browser extension is not detected. For example,  indicates that the Brave browser is active but the extension is not detected. Contact Check Point Support. ■ N/A - The installed Endpoint Security client version does not support Browser Status.  Note - This is supported only with these versions: ■ Endpoint Security Client for Windows version E86.10 and higher. ■ Endpoint Security Client for macOS version E88.30 and higher.
Anti-Bot Last Update	Shows the date and time when the signatures of the Anti-Bot blade were last updated. For example, 07 Jun 2023 04:53 PM. The other statuses are: ■ N/A - The Anti-Bot signatures are not updated. ■ Not Installed - The Anti-Bot blade is not installed.  Note - This is supported only with the Endpoint Security Client version E87.30 or higher .

Filter / Column Name	Description
Posture Last Scan Status	Shows the status of the latest scan. The statuses are: ■ Timed Out ■ Waiting For Client ■ Blade Not Installed ■ Starting Scan - Scan initiated. ■ Scan Started - Scan in progress. ■ Succeeded ■ Failed ■ Not Scanned ■ Aborted

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**.

Viewing Device Hardware Information

You can view the hardware information of each device in your organization, such as, CPU configurations, network connection, disk usage and RAM.

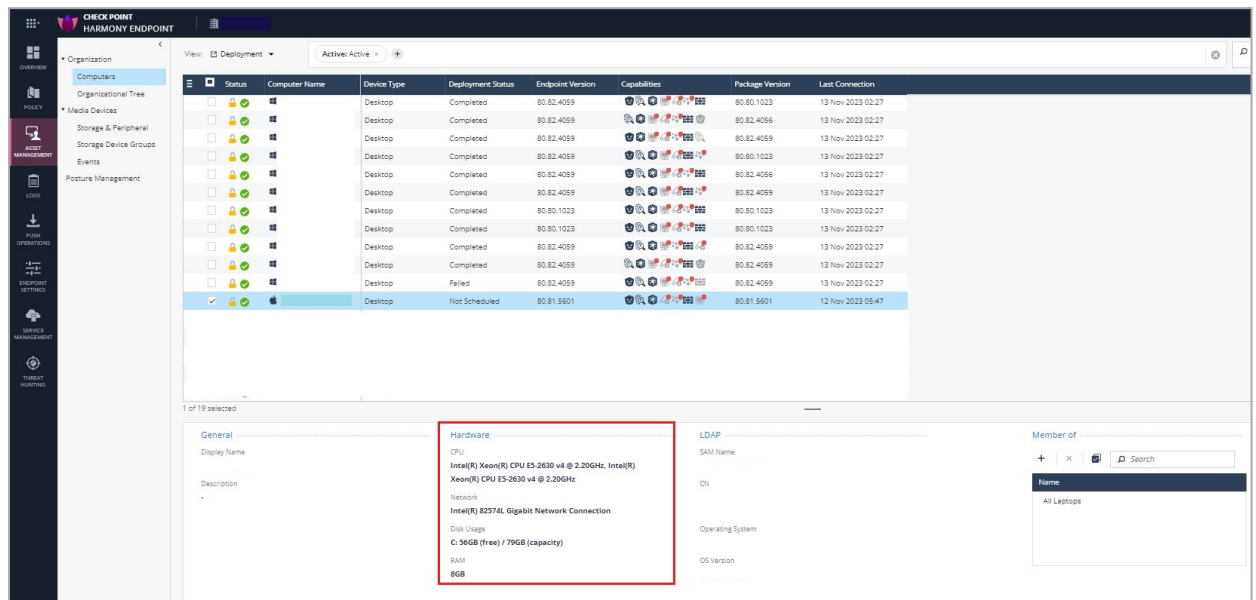
Note -

- For Windows clients, this feature is supported with Endpoint Security client version E88.00 and higher.
- For macOS clients, this feature is supported with Endpoint Security client version E88.40 and higher.

To view the device hardware information:

1. Navigate to **Asset Management**, expand **Organization** and select **Computers**.
2. Click the device.

The device information is displayed in the **Hardware** section.



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" on page 539](#).

Create and Add to Virtual Group

You can add computers to a new virtual group. See ["Managing Virtual Groups" on page 539](#).

Add to Virtual Group

You can add a computer to a virtual group. See ["Managing Virtual Groups" on page 539](#).

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 asset's 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 Endpoint Security 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

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

Push Operations

Perform Push Operation

1. Go to **Asset Management > Computers**.
2. Right-click on a computer, select a category and select a push operation.

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
Forensics and Remediation	Analyze by Indicator	Yes	Yes	No
	File Remediation	Yes	Yes	Yes
	Isolate Computer	Yes	Yes	No
	Release Computer	Yes	Yes	No

Category	Push Operations	Windows	macOS	Linux
Agent Settings	Deploy New Endpoints	Yes	No	No
	Collect Client Logs	Yes	Yes	No
	Collect Client Logs Offline	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
	Search and Fetch files	Yes	Yes	No
	Registry Actions	Yes	No	No
	File Actions	Yes	Yes	No
	VPN Site	Yes	Yes	No
	Collect Processes	Yes	No	No
	Run Diagnostics	Yes	Yes	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, <code>c:\temp\eicar.txt</code> 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: - Click + and select the organization. - Click Update Selection. - Select the device and click Next. - Add Comment, optional comment about the action. - To move the files to quarantine, select Move the following files to quarantine. - To restore the files from quarantine, select Restore the following files from quarantine. - Click +. - From the drop-down: - Select Full file path or Incident ID: - In the Element field, enter the incident ID from the Endpoint Security client or enter the incident UID for the corresponding incident from the Logs menu in the Endpoint Security Administrator Portal. To obtain the incident UID, open the log entry and expand the More section to view the incident UID. - Click OK - Select MD5 Hash: - Enter or upload the Element. - Click OK.	No

Push Operations	Description	2FA Required
	i. Click Finish .	
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

Push Operations	Description	2FA Required		
Deploy New Endpoints	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.	No		
	<table><tr><th>Field</th><th>Description</th></tr></table>		Field	Description
	Field		Description	
	Comment		Optional comment about the action.	
Select the deployment endpoint	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.			
Endpoint version	Select the Endpoint Security Client version to install on the target device.  Note - Only Endpoint Security client versions with a corresponding exported package (<i>"Manual Deployment of Endpoint Clients" on page 106</i>) are showed here. You can only push a client version if the package exists in the export packages.			

Push Operations	Description	2FA Required						
Collect Client Logs	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 <i>C:\ProgramData\CheckPoint\Endpoint Security\Temp</i>. • For Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory <i>C:\Windows\SysWOW64\config\systemprofile\CPInfo</i>. ■ For macOS, client logs are stored in the directory <i>/Users/Shared/cplogs</i>. <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></table>	Field	Description	Comment	Optional comment about the action.	Log set to collect	Select the scope of information for the logs.	No
Field	Description							
Comment	Optional comment about the action.							
Log set to collect	Select the scope of information for the logs.							

Push Operations	Description	2FA Required				
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Debug Info upload</td><td> Select the location to upload the logs: ▪ Upload CPInfo reports to AWS S3 - If the push operation is successful, the administrator will receive a download link in the Endpoint Security Administrator Portal to download the logs.  Notes - • This option is supported only with the Endpoint Security client for Windows version E88.30 and higher and for macOS version E88.50 and higher. • To enable this option, select a single user. • You can create and copy the link to download the logs using the copy to clipboard icon in the Operation output section of the Push Operation Endpoint Details. The copied link will be valid for 30 minutes. ▪ Upload CPInfo reports to Check Point servers ▪ Upload CPInfo reports to Corporate server - Update the relevant corporate server information. </td></tr></table>	Field	Description	Debug Info upload	Select the location to upload the logs: ▪ Upload CPInfo reports to AWS S3 - If the push operation is successful, the administrator will receive a download link in the Endpoint Security Administrator Portal to download the logs.  Notes - • This option is supported only with the Endpoint Security client for Windows version E88.30 and higher and for macOS version E88.50 and higher. • To enable this option, select a single user. • You can create and copy the link to download the logs using the copy to clipboard icon in the Operation output section of the Push Operation Endpoint Details. The copied link will be valid for 30 minutes. ▪ Upload CPInfo reports to Check Point servers ▪ Upload CPInfo reports to Corporate server - Update the relevant corporate server information.	
Field	Description					
Debug Info upload	Select the location to upload the logs: ▪ Upload CPInfo reports to AWS S3 - If the push operation is successful, the administrator will receive a download link in the Endpoint Security Administrator Portal to download the logs.  Notes - • This option is supported only with the Endpoint Security client for Windows version E88.30 and higher and for macOS version E88.50 and higher. • To enable this option, select a single user. • You can create and copy the link to download the logs using the copy to clipboard icon in the Operation output section of the Push Operation Endpoint Details. The copied link will be valid for 30 minutes. ▪ Upload CPInfo reports to Check Point servers ▪ Upload CPInfo reports to Corporate server - Update the relevant corporate server information.					

Push Operations	Description	2FA Required
Repair Client	Repairs the Endpoint Security client installation. This requires a computer restart.  Note - This push operation applies only to Endpoint Security clients that have been upgraded to a newer version at least once after the installation.	No
Shutdown Computer	Shuts down the computer or computers based on the configured settings.	No
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 Security 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 Endpoint Security Windows clients running version E85.30 and above	Yes

Push Operations	Description	2FA Required				
Search and Fetch files	Searches and uploads files to a server.	Yes				
	Supported fields are:					
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr></table>		Field	Description	Comment	Optional comment about the action.
	Field		Description			
	Comment		Optional comment about the action.			
	Search and Fetch files					
	Locate the following files in the specific folders		Searches for the files in the specified folders. a. In the File table, click +. b. Enter the file name. For example, <i>test.txt</i> or <i>test.zip</i> 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.			
Locate the following files by exact path	Searches for the files in the specified path. a. In the File table, click +. b. Enter the path where you want to search for the file and click OK. c. Repeat the steps for additional paths.					
Files upload						
Select the Upload files to	Select the checkbox to upload the files to a server.					

Push Operati ons	Description		2FA Requir ed
	Field	Description	
	Corporate Server Info	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 .	

Push Operations	Description	2FA Required						
Registry Actions	Add or remove a registry key.	No						
	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></table>		Field	Description	Comment	Optional comment about the action.	Action	Select an action. ■ Add Key to Registry ■ Remove Key From Registry  Caution - Removing a registry might impact the endpoint's operating system.
	Field		Description					
	Comment		Optional comment about the action.					
	Action		Select an action. ■ Add Key to Registry ■ Remove Key From Registry  Caution - Removing a registry might impact the endpoint's operating system.					
	Add Key to Registry							
	Key		Full path where you want to add the registry key. For example, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>					
	Subkey		Enter the key name to add in the registry. For example, ProductVersion .					
	Value Type		Select the registry type.					
Value	Enter the registry value.							
Is redirected	Indicates that virtualization is enabled and add the registry to 32-bit. By default, the registry is added for 64-bit.							
Remove Key From Registry								

Push Operations	Description	2FA Required								
	<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, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>  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.	Field	Description	Key	Full path of registry key that you want to delete. For example, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>  Caution - Removing a registry might impact the endpoint's operating system.	Subkey	Enter the key name to remove from the registry. For example, ProductVersion .	Is redirected	Indicates that virtualization is enabled and delete the registry in 32-bit. By default, the registry is deleted for 64-bit.	
Field	Description									
Key	Full path of registry key that you want to delete. For example, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>  Caution - Removing a registry might impact the endpoint's operating system.									
Subkey	Enter the key name to remove from the registry. For example, ProductVersion .									
Is redirected	Indicates that virtualization is enabled and delete the registry in 32-bit. By default, the registry is deleted for 64-bit.									

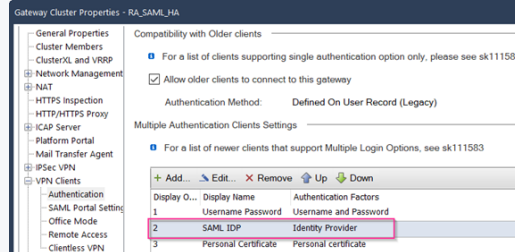
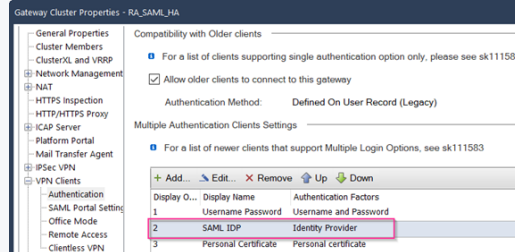
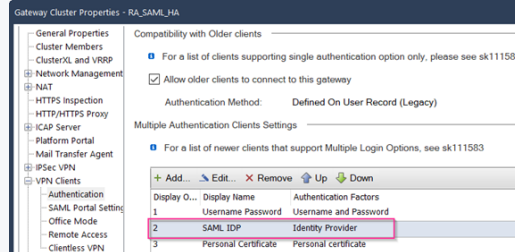
Push Operations	Description	2FA Required						
File Actions	Copy, move or delete the file or folder. Supported fields:	No						
	 Note - The folder actions are supported only with the Endpoint Security Client version 87.20 and higher.							
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</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 Endpoint Security's protected files.</td></tr></table>		Field	Description	Comment	Optional comment about the action.	Action	Select an action. ▪ Copy File ▪ Move File ▪ Delete File  Caution - Deleting a file might impact Endpoint Security's protected files.
	Field		Description					
	Comment		Optional comment about the action.					
Action	Select an action. ▪ Copy File ▪ Move File ▪ Delete File  Caution - Deleting a file might impact Endpoint Security's protected files.							
Copy File								
File path	Full path of the file or folder you want to copy, including the file or folder name. Example: ▪ For File - <i>C:\Users\<user_name>\Desktop\test.doc</i> ▪ For Folder - <i>C:\Users\Username\Desktop\</i>							

Push Operations	Description	2FA Required							
	<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 - <i>C:\Users\<user_name>\Documents</i> ■ For Folder - <i>C:\Users\Username2\</i>  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 - <i>C:\Users\<user_name>\Desktop\test.doc</i> ■ For Folder - <i>C:\Users\Username>\Desktop\</i> </td></tr></table>	Field	Description	Target file path	Full path where you want to paste the file or folder. Example: ■ For File - <i>C:\Users\<user_name>\Documents</i> ■ For Folder - <i>C:\Users\Username2\</i>  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.	Move File		File path	Full path of the file or folder you want to move, including the file or folder name. Example: ■ For File - <i>C:\Users\<user_name>\Desktop\test.doc</i> ■ For Folder - <i>C:\Users\Username>\Desktop\</i>
	Field	Description							
	Target file path	Full path where you want to paste the file or folder. Example: ■ For File - <i>C:\Users\<user_name>\Documents</i> ■ For Folder - <i>C:\Users\Username2\</i>  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.							
Move File									
File path	Full path of the file or folder you want to move, including the file or folder name. Example: ■ For File - <i>C:\Users\<user_name>\Desktop\test.doc</i> ■ For Folder - <i>C:\Users\Username>\Desktop\</i>								

Push Operations	Description	2FA Required				
	<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 - <i>C:\Users\<user_name>\Documents</i> ■ For Folder - <i>C:\Users\Username1\Documents\</i>  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></table>	Field	Description	Target file path	Path where you want to move the file or folder. Example: ■ For File - <i>C:\Users\<user_name>\Documents</i> ■ For Folder - <i>C:\Users\Username1\Documents\</i>  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.	
Field	Description					
Target file path	Path where you want to move the file or folder. Example: ■ For File - <i>C:\Users\<user_name>\Documents</i> ■ For Folder - <i>C:\Users\Username1\Documents\</i>  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.					
	Delete File <table><tr><td>File path</td><td> Full path of the file you want to delete, including the file name. For example, <i>C:\Users\<user_name>\Desktop\test.doc</i>  Caution - Deleting a file might impact Endpoint Security's protected files.  Note - Delete folder action is not supported. </td></tr></table>	File path	Full path of the file you want to delete, including the file name. For example, <i>C:\Users\<user_name>\Desktop\test.doc</i>  Caution - Deleting a file might impact Endpoint Security's protected files.  Note - Delete folder action is not supported.			
File path	Full path of the file you want to delete, including the file name. For example, <i>C:\Users\<user_name>\Desktop\test.doc</i>  Caution - Deleting a file might impact Endpoint Security's protected files.  Note - Delete folder action is not supported.					

Push Operations	Description	2FA Required				
VPN Site	Adds or removes a VPN site. Limitations: ■ This is not supported with Linux operating system. ■ You cannot create separate VPN sites for each user that access the endpoint. The same VPN site applies to all users. ■ SoftID and challenge-response authentication methods are not tested. ■ The system does not validate the entries (for example, Server Name or Fingerprint) that you specify. ■ Only one fingerprint operation is supported at a time. ■ You cannot add a new VPN site or remove a VPN site if a VPN site is already connected in the Endpoint Security client. Disconnect the VPN site before you add a new VPN site. ■ This operation is not supported if the firewall policy for the client is configured through the on-premise Security Gateway (Policy > Data Protection > Access & Compliance > Firewall > When using Remote Access, enforce Firewall Policy from is Remote Access Desktop Security Policy). To enable the operation on such a client: a. In the Security Gateway, change the parameter <i>allow_disable_firewall</i> to true in the <i>\$FWDIR/conf/trac_client_1.ttm</i> file. b. Install the policy on the Security Gateway. c. Reboot the Endpoint Security client. d. Perform the push operation. Note - If the operation fails with timeout, see sk179798 for troubleshooting instructions. Supported fields: <table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr></table>	Field	Description	Comment	Optional comment about the action.	No
Field	Description					
Comment	Optional comment about the action.					

Push Operations	Description		2FA Required
	Field	Description	
	Action	Select an action: ■ Add VPN Site ■ Remove VPN Site	
	Add VPN Site		
	Server Name	Enter the IP address or FQDN of the remote access gateway. Note - Ensure the endpoint can resolve the FQDN to the IP address of the gateway.	
	Use Custom Display Name	Select the checkbox if you want to change the display name of the server in the Endpoint Security client.	
	Display Name	Server name displayed in the Endpoint Security client. By default, it uses the Server Name . To change the display name ,select the Use Custom Display Name checkbox and enter a display name.	
	Use Custom Login Option	Select the checkbox if you want to use a custom login option.	

Push Operations	Description	2FA Required				
	<table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Login Option</td><td> Login option for the server. By default, Standard login option is selected. To use a custom login option, select Use Custom Login Option checkbox, and enter the login option. This must match the Display Name specified in the GW properties > VPN Clients > Authentication > Multiple Authentication Clients Settings in the SmartConsole. For example, SAML IDP.  For the Standard login option, make sure that the Authentication Method is Defined on User Record (Legacy). Otherwise, Standard: does not need authentication method error appears. </td></tr></tbody></table>	Field	Description	Login Option	Login option for the server. By default, Standard login option is selected. To use a custom login option, select Use Custom Login Option checkbox, and enter the login option. This must match the Display Name specified in the GW properties > VPN Clients > Authentication > Multiple Authentication Clients Settings in the SmartConsole. For example, SAML IDP.  For the Standard login option, make sure that the Authentication Method is Defined on User Record (Legacy). Otherwise, Standard: does not need authentication method error appears.	
Field	Description					
Login Option	Login option for the server. By default, Standard login option is selected. To use a custom login option, select Use Custom Login Option checkbox, and enter the login option. This must match the Display Name specified in the GW properties > VPN Clients > Authentication > Multiple Authentication Clients Settings in the SmartConsole. For example, SAML IDP.  For the Standard login option, make sure that the Authentication Method is Defined on User Record (Legacy). Otherwise, Standard: does not need authentication method error appears.					

Push Operations	Description	2FA Required						
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Authentication Method</td><td> Select an authentication method. The options displayed depend on the Login Option. Authentication methods for the Standard login option: ▪ username-password ▪ certificate (for a certificate stored in the CAPI store) ▪ p12-certificate ▪ securityIDKeyFob ▪ securityIDPinPad ▪ SoftID (not tested) ▪ challenge-response (not tested) Authentication methods for the custom login option: ▪ Select certificate from hardware or software token (CAPI) ▪ Use certificate from Public-Key Cryptographic Standard (PKCS #12) file ▪ Other Note - Select the relevant certificate authentication method if your custom login uses a certificate. Otherwise, select Other. </td></tr><tr><td>Fingerprint</td><td> Enter the fingerprint key. For information about how to collect fingerprint details, see "Collecting Fingerprint details for a VPN Site:" on page 606. </td></tr></table>	Field	Description	Authentication Method	Select an authentication method. The options displayed depend on the Login Option. Authentication methods for the Standard login option: ▪ username-password ▪ certificate (for a certificate stored in the CAPI store) ▪ p12-certificate ▪ securityIDKeyFob ▪ securityIDPinPad ▪ SoftID (not tested) ▪ challenge-response (not tested) Authentication methods for the custom login option: ▪ Select certificate from hardware or software token (CAPI) ▪ Use certificate from Public-Key Cryptographic Standard (PKCS #12) file ▪ Other Note - Select the relevant certificate authentication method if your custom login uses a certificate. Otherwise, select Other.	Fingerprint	Enter the fingerprint key. For information about how to collect fingerprint details, see "Collecting Fingerprint details for a VPN Site:" on page 606.	
Field	Description							
Authentication Method	Select an authentication method. The options displayed depend on the Login Option. Authentication methods for the Standard login option: ▪ username-password ▪ certificate (for a certificate stored in the CAPI store) ▪ p12-certificate ▪ securityIDKeyFob ▪ securityIDPinPad ▪ SoftID (not tested) ▪ challenge-response (not tested) Authentication methods for the custom login option: ▪ Select certificate from hardware or software token (CAPI) ▪ Use certificate from Public-Key Cryptographic Standard (PKCS #12) file ▪ Other Note - Select the relevant certificate authentication method if your custom login uses a certificate. Otherwise, select Other.							
Fingerprint	Enter the fingerprint key. For information about how to collect fingerprint details, see "Collecting Fingerprint details for a VPN Site:" on page 606.							

Push Operations	Description	2FA Required												
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Remote Access Gateway Name</td><td>Enter the remote access gateway name. For information about how to get the remote access gateway name, see "Collecting Remote Access Gateway Name" on page 609.</td></tr><tr><td colspan="2">Remove VPN Site</td></tr><tr><td>Display Name</td><td>Enter the display name for the server.</td></tr></table>	Field	Description	Remote Access Gateway Name	Enter the remote access gateway name. For information about how to get the remote access gateway name, see "Collecting Remote Access Gateway Name" on page 609 .	Remove VPN Site		Display Name	Enter the display name for the server.					
Field	Description													
Remote Access Gateway Name	Enter the remote access gateway name. For information about how to get the remote access gateway name, see "Collecting Remote Access Gateway Name" on page 609 .													
Remove VPN Site														
Display Name	Enter the display name for the server.													
Collect Processes	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>	Field	Description	Comment	Optional comment about the action.	Collect all processes	Collects information about all the processes running on the endpoint.	Collect process by name	Collects information about a specific process on the endpoint.	Process name	Enter the process name. Case-sensitive.	Additional output fields	Select the additional information you want to view in the collected information.	No
Field	Description													
Comment	Optional comment about the action.													
Collect all processes	Collects information about all the processes running on the endpoint.													
Collect process by name	Collects information about a specific process on the endpoint.													
Process name	Enter the process name. Case-sensitive.													
Additional output fields	Select the additional information you want to view in the collected information.													

Push Operations	Description	2FA Required
Run Diagnostics	Runs diagnostics on an endpoint to collect this information: ■ Total CPU and RAM usage in the last 12 hours. ■ CPU usage by processes initiated in the last 12 hours. For example, the CPU used by Anti-Malware to scan files. You can review the CPU usage data to identify processes (scans) that consume CPU more than the specified threshold and exclude such processes from future scans.  Note - This is supported with Endpoint Security client version E86.80 and higher.  Warning - Only exclude a process if you are sure that the file is not malicious and is not vulnerable to cyber-attacks. To view the latest diagnostics report, see "Show Last Diagnostics Report" on page 217.	
Enable / Disable Self Protection	This Push Operation allows the administrator to enable or disable the self protection capabilities on endpoints. Supported fields: ■ Enable - Enables the self protection capabilities. ■ Disable - Disables the self protection capabilities. ■ Timeout Command Expiration - Select the expiration time for the command.  Note - After the timeout, the command expires, and the self protection capabilities will be enabled automatically.	

Push Operations	Description	2FA Required						
Collect Memory Dump	Collects Memory Dump from an endpoint based on the configured settings. Memory dump is a snapshot of system memory at specific instance of the active process and the operating system.  Note - This push operation can be executed on one device at an instance. <table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr><tr><td>Type</td><td> Select the type of memory dump to be collected. ▪ Process - Captures memory dumps for one or more processes using process name or PID.  Notes: • The system generates multiple memory dumps if several processes share the same name. • Memory dumps are not supported for Protected Process Light (PPL) processes. ▪ Kernel - Collects a kernel memory dump without requiring a system reboot.  Note - Kernel memory dump is not supported on Windows 7 devices. ▪ Full - Initiates a BSOD to collect a full or active memory dump (requires prior configuration on the target device). For more information, see Dell documentation.  Note - It is optional to reboot the endpoint to collect the Full memory dump. </td></tr></table>	Field	Description	Comment	Optional comment about the action.	Type	Select the type of memory dump to be collected. ▪ Process - Captures memory dumps for one or more processes using process name or PID.  Notes: • The system generates multiple memory dumps if several processes share the same name. • Memory dumps are not supported for Protected Process Light (PPL) processes. ▪ Kernel - Collects a kernel memory dump without requiring a system reboot.  Note - Kernel memory dump is not supported on Windows 7 devices. ▪ Full - Initiates a BSOD to collect a full or active memory dump (requires prior configuration on the target device). For more information, see Dell documentation.  Note - It is optional to reboot the endpoint to collect the Full memory dump.	
Field	Description							
Comment	Optional comment about the action.							
Type	Select the type of memory dump to be collected. ▪ Process - Captures memory dumps for one or more processes using process name or PID.  Notes: • The system generates multiple memory dumps if several processes share the same name. • Memory dumps are not supported for Protected Process Light (PPL) processes. ▪ Kernel - Collects a kernel memory dump without requiring a system reboot.  Note - Kernel memory dump is not supported on Windows 7 devices. ▪ Full - Initiates a BSOD to collect a full or active memory dump (requires prior configuration on the target device). For more information, see Dell documentation.  Note - It is optional to reboot the endpoint to collect the Full memory dump.							

Push Operati ons	Description		2FA Requir ed
	Field	Description	
	Proces s name	Enter the process name of the process memory dump.	
	Proces s PID	Enter the process PID of the process memory dump.	

Push Operations	Description	2FA Required				
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Dump info upload</td><td> Select the location to upload the memory dump: ▪ Upload Memory Dump to AWS S3 - After the push operation is successful, the system shows a download option in the Operation output column of the Push Operation Endpoint Details section. ▪ Upload Memory Dump to Check Point servers - After the push operation is successful, the system uploads the memory dump to this location: • For Windows Endpoint Security Client versions E88.31 and higher, client logs are stored in the directory <i>C:\ProgramData\CheckPoint\EndpointSecurity\Temp.</i> • For Windows Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory <i>C:\Windows\SysWOW64\config\systemprofile\CPInfo.</i> • For macOS, client logs are stored in the directory <i>/Users/Shared/cplogs.</i> ▪ Upload Memory Dump to Corporate server - Enter your corporate server details. After the push operation is successful, the system uploads the memory dump to the configured location in the corporate server. </td></tr></table>	Field	Description	Dump info upload	Select the location to upload the memory dump: ▪ Upload Memory Dump to AWS S3 - After the push operation is successful, the system shows a download option in the Operation output column of the Push Operation Endpoint Details section. ▪ Upload Memory Dump to Check Point servers - After the push operation is successful, the system uploads the memory dump to this location: • For Windows Endpoint Security Client versions E88.31 and higher, client logs are stored in the directory <i>C:\ProgramData\CheckPoint\EndpointSecurity\Temp.</i> • For Windows Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory <i>C:\Windows\SysWOW64\config\systemprofile\CPInfo.</i> • For macOS, client logs are stored in the directory <i>/Users/Shared/cplogs.</i> ▪ Upload Memory Dump to Corporate server - Enter your corporate server details. After the push operation is successful, the system uploads the memory dump to the configured location in the corporate server.	
Field	Description					
Dump info upload	Select the location to upload the memory dump: ▪ Upload Memory Dump to AWS S3 - After the push operation is successful, the system shows a download option in the Operation output column of the Push Operation Endpoint Details section. ▪ Upload Memory Dump to Check Point servers - After the push operation is successful, the system uploads the memory dump to this location: • For Windows Endpoint Security Client versions E88.31 and higher, client logs are stored in the directory <i>C:\ProgramData\CheckPoint\EndpointSecurity\Temp.</i> • For Windows Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory <i>C:\Windows\SysWOW64\config\systemprofile\CPInfo.</i> • For macOS, client logs are stored in the directory <i>/Users/Shared/cplogs.</i> ▪ Upload Memory Dump to Corporate server - Enter your corporate server details. After the push operation is successful, the system uploads the memory dump to the configured location in the corporate server.					

Push Operations	Description	2FA Required
	 Notes: ■ Automated packaging and upload of memory dump - All memory dumps are automatically zipped, segmented if necessary, and uploaded to the designated destination (Check Point FTP, Amazon S3, or custom FTP servers). ■ On 32-bit Windows systems, the ZIP file name is not displayed when uploading full memory dumps to an FTP server. ■ The Memory Dump feature is supported only on Endpoint Security for Windows client version E89.05 and later.	

6. Under **User Notification:**

- To notify the user about the push operation, select the **Inform user with notification** checkbox.
- To allow the user to postpone 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. Specify the duration after which the system automatically terminates the unexecuted push operation (For example, if the Endpoint client is offline):

- **7 days**
- **Custom**
- **Never**

9. 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 [Check Point Portal Administration Guide](#).
 - To enable 2FA authentication for the current tenant, click **Global Settings**, and follow the instructions. For more information, see [Check Point Portal Administration Guide](#).
10. Click **Finish**.
 11. 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.

Report	Description
Run Diagnostics	To see the diagnostics report: 1. Go to Push Operations menu. 2. Select the row of the Run Diagnostics push operation you performed. 3. In the Endpoint List table, under Operation Output column, click View Report.  Note - This is supported with Endpoint Security client version E86.80 and higher. By default, the report shows the data for Total Usage. ■ To view the report per capability, in the left pane, under Process, click the capability. ■ In the CPU widget: • To change the CPU usage threshold, in the Threshold list, set a value (in percentage). The default value is 10 percent. • To set the selected threshold as default, click Set Default.  Note - After changing the threshold, Endpoint Security Administrator Portal re-evaluates to suggest processes that exceeded the new threshold. To add a suggested exclusion to the exclusion list: 1. In the Suggested Exclusions area, clear the checkboxes if you do not want to exclude the processes from future scans. By default, all the processes are selected for exclusion. 2. Click View Selected Exclusions. 3. To add the exclusions to all the rules, select Global Exclusions. a. Click Create & Review. b. Click Save. c. From the top, click Install Policy. 4. To add the exclusions to a specific rule, select Device Exclusions Per Rule. a. Click Create & Review for the rule.

Report	Description
	b. Click OK. c. Click Save. d. From the top, click Install policy.

Diagnostics

Run Diagnostics

Runs diagnostics on an endpoint to collect this information:

- Total CPU and RAM usage in the last 12 hours.
- CPU usage by processes initiated in the last 12 hours. For example, the CPU used by Anti-Malware to scan files.

You can review the CPU usage data to identify processes (scans) that consume CPU more than the specified threshold and exclude such processes from future scans.

 **Note** - This is supported with Endpoint Security client version E86.80 and higher.

 **Warning** - Only exclude a process if you are sure that the file is not malicious and is not vulnerable to cyber-attacks.

To view the latest diagnostics report, see ["Show Last Diagnostics Report" on the next page](#).

To see the diagnostics report:

1. Go to **Push Operations** menu.
2. Select the row of the **Run Diagnostics** push operation you performed.
3. In the **Endpoint List** table, under **Operation Output** column, click **View Report**.

 **Note** - This is supported with Endpoint Security client version E86.80 and higher.

By default, the report shows the data for **Total Usage**.

- To view the report per capability, in the left pane, under **Process**, click the capability.
- In the CPU widget:
 - To change the CPU usage threshold, in the **Threshold** list, set a value (in percentage). The default value is 10 percent.
 - To set the selected threshold as default, click **Set Default**.

 **Note** - After changing the threshold, Endpoint Security Administrator Portal re-evaluates to suggest processes that exceeded the new threshold.

To add a suggested exclusion to the exclusion list:

1. In the **Suggested Exclusions** area, clear the checkboxes if you do not want to exclude the processes from future scans. By default, all the processes are selected for exclusion.
2. Click **View Selected Exclusions**.
3. To add the exclusions to all the rules, select **Global Exclusions**.
 - a. Click **Create & Review**.
 - b. Click **Save**.
 - c. From the top, click **Install Policy**.
4. To add the exclusions to a specific rule, select **Device Exclusions Per Rule**.
 - a. Click **Create & Review** for the rule.
 - b. Click **OK**.
 - c. Click **Save**.
 - d. From the top, click **Install policy**.

Show Last Diagnostics Report

Shows the latest diagnostics report. By default, Endpoint Security runs the diagnostics every four hours.

 **Note** - This is supported with the Endpoint Security client version E86.80 and higher.

For more information about the diagnostics report, see Run Diagnostics in ["Performing Push Operations \(Old User Interface\)" on page 580](#).

Full Disk Encryption

Preboot User Assignment

You can view, create, lock and unlock authorized Pre-boot users. See [Authentication-before-OS-Loads-Pre-boot.htm](#).

Remote Help and Recovery

Recovery

If the operating system does not start on a client computer due to system failure, you can recover your data from the computer:

- ["Check Point Full Disk Encryption Recovery" on page 532](#)
- ["BitLocker Recovery" on page 535](#)
- ["FileVault Recovery" on page 536](#)

Media Encryption

You can recover removable media passwords remotely, using a challenge/response procedure. See ["Media Encryption Remote Help" on page 422](#).

Full Disk Encryption

You can give access to users who are locked out of their Full Disk Encryption protected computers. See ["Giving Remote Help to Full Disk Encryption Users" on page 559](#).

Viewing Endpoint Posture

[After the scan is complete](#), Endpoint Security shows the detected Common Vulnerability and Exposures (CVE) and its Common Vulnerability Scoring System (CVSS).

For the supported applications for scan and patch management, see [sk181034](#).

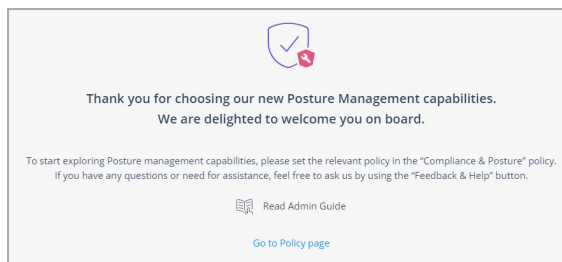


Note -

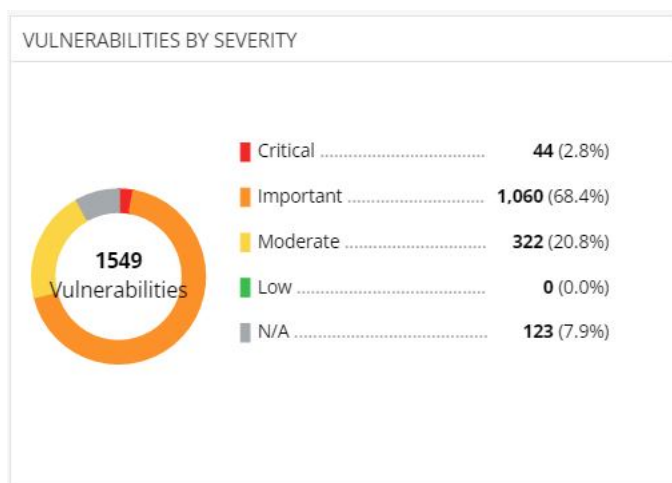
- End-users can also initiate the scan and view the vulnerable CVEs from the Endpoint Security client (Compliance and Posture).
- Endpoint Security can apply the patch only to applications installed in the *C:\Program Files* directory.
- Endpoint Security can download and apply a patch only if its size is less than 2 GB.

To view the posture for endpoints, click **Asset Management > Posture Management**.

If you see the following screen, make sure to configure the posture assessment settings. See ["Configuring Posture Assessment Settings" on page 472](#).

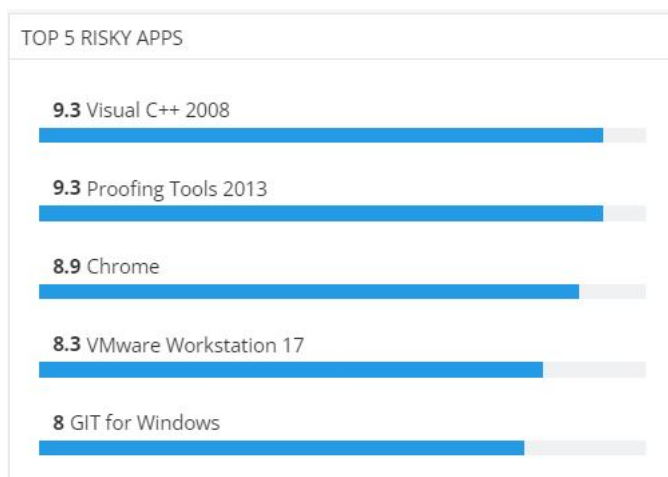


Vulnerabilities by Severity



The **Vulnerabilities by Severity** widget shows the total number of vulnerable CVEs by severity.

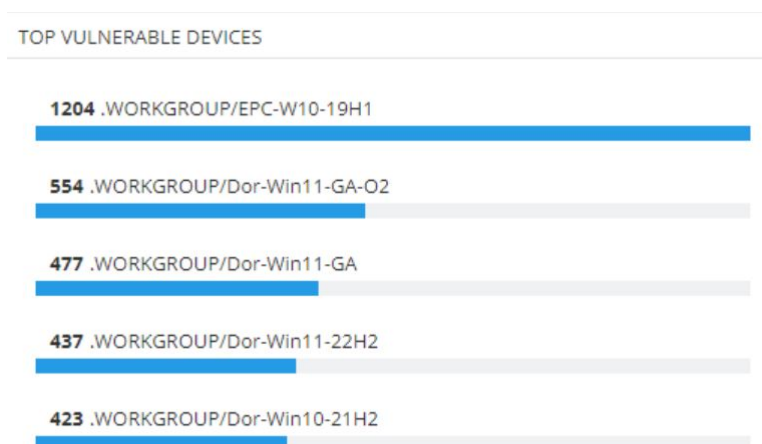
Top 5 Risky Apps



The **Top 5 Risky Apps** widget shows the top five applications with vulnerable CVEs and their average CVSS score.

For example, if Visual C++ 2008 has different CVEs, then the average CVSS score is 9.3.

Top Vulnerable Devices



The **Top Vulnerable Devices** widget shows the top five vulnerable endpoints (most vulnerable CVEs detected).

The number to the left of the machine name indicates the total number of CVEs detected in the machine.

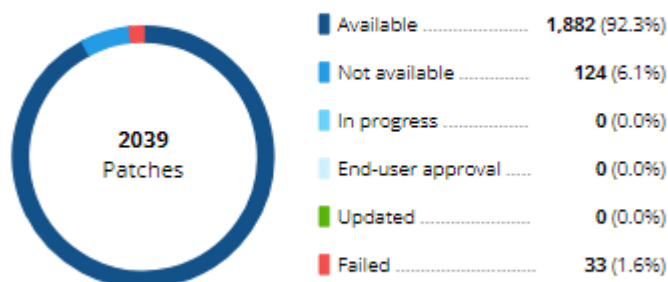
To view vulnerable CVEs in the machine, click the machine name. It shows the details in the ["Vulnerability Assessment Table" on the next page](#).

There are two three types of **View** available for risk assessment:

- Vulnerabilities view - Shows all the vulnerable CVEs and their CVSS score detected in the endpoints. See ["Vulnerability Assessment Table" on the next page](#)
- Devices view - Shows devices that have at least one CVE detected.

Patches By Status

PATCHES BY STATUS



The **Patches By Status** widget shows the total number of patches by the status.

Click the status to filter the *"Vulnerability Assessment Table" below* by the status.

Vulnerability Assessment Table

The Vulnerability Assessment table shows the details about the detected CVE and its CVSS score.

Item	Description
 Export	Exports the table information. Supported exports are: ■ CSV Files ■ Vulnerability Report ■ Posture Report For more information on vulnerability and posture reports, see Reports in the <i>"Viewing Operational Overview, Security Overview and Reports" on page 149</i> .
Refresh	Refresh the table information.
Search	Enter the required search options.
 Toggle Filters	Opens the Filters widget. You must specify the filter criteria.
Scan All	Scans all devices for CVEs. See <i>"Scanning Devices" on page 230</i> .

Item	Description
Scan Now	Scans selected devices for CVEs. See "Scanning Devices" on page 230 .
Patch	Updates patches to the specified CVEs. See "Applying the Patch for CVEs" on page 231 .
Push Operations	Perform any of these Push Operations: - Isolate Device - See "Isolating a Device" on page 230. - Release Device - See "Verifying the Applied Patch" on page 232. - Reboot Device - See "Verifying the Applied Patch" on page 232.
Add Filter	Allows you to filter the columns by a specific value.
Vulnerabilities View	
 Group by CVE	Lists CVEs by group.
 Group by Application	Lists CVEs by application.
 Expand All	Expands CVEs listed by application.
 Collapse all	Collapses CVEs listed by application.
CVSS Score	CVSS score of the detected CVE.
CVE Number	Click the CVE number to view "CVE Details Widget" on page 229 and all impacted devices: - Device Name - OS - OS Version - Last Scanned - Comment - Add a comment. For example, do not patch this application.
App Name	Application name.
App Version	Application version number.

Item	Description
Last Detected	Date and time the CVE was last detected.
First Detected	Date and time the CVE was first detected.
Affected Devices	Number of machines with vulnerable CVEs.
Comments	Add a comment. For example, do not patch this device.

Device View

Item	Description
Device Name	Click the device name to view the "Device Details Widget" on page 229 and all CVEs in the device: ■ CVSS Score ■ CVE Number ■ App Name ■ App Version ■ Last Detected ■ First Detected ■ Patch Name ■ Patch Size ■ Patch Status ○ Available - Patch is available for the CVE. ○ Cancelled - Deployment is cancelled before patch installation is completed. ○ Not Available ○ Update not available - Patch updates are not available. You must manually search, download and apply the patch. ○ In progress ○ Downloaded ○ Executing ○ Checking ○ Pending ○ Update available - Patch updates are available for the CVEs. ○ Downloading - System is downloading the patch. ○ Pending execution - Waiting for other patches in the bulk to be installed. ○ Pending scan - Patch installed successfully. Waiting for the scan. ○ Pending reboot - Patch installed successfully. Waiting for device reboot. ○ End user approval ○ Failed ○ Timeout - Connection to the Endpoint Security Client timed out. ○ Download failed ○ Replaced ○ Not installed

Item	Description
	◦ Updated ◦ Interrupted - The patch installation by Endpoint Security is interrupted by other services, such as Windows update, that is either installing or installed the patch. ▪ Comment
OS	Operating System name.
OS Version	Operating System version.
Last Scan Status	Shows the status of the latest scan. The supported statuses are: ▪ Timed Out ▪ Waiting For Client ▪ Blade Not Installed ▪ Starting Scan ▪ Scan Started ▪ Succeeded ▪ Failed ▪ Not Scanned ▪ Aborted
Last Scanned	Date and time the machine was last scanned.
Number of Vulnerabilities	Number of vulnerabilities detected in the machine.
Number of Apps At Risk	Number of applications in the machine with vulnerable CVEs.
Comments	Add a comment. For example, do not patch this device.
Application view	
App Name	Application name. Click the application name to view all the CVEs affecting the corresponding application. It takes you to the Vulnerabilities view and shows the relevant information. For more details, see Vulnerability view.
App Version	Application version number.
Patch Name	Full name of the patch.
Patch Size	Size of the patch file.

Item	Description
First Detected	Date and time the CVE was first detected.
Last Detected	Date and time the CVE was last detected.
Affected Devices	Number of devices that have the application affected by the corresponding CVE. Click the number to view all the impacted devices for the corresponding patch. It takes you to the Devices view and shows the relevant information. For more details, see Devices view.
Patch Status	Status of the patch of the CVE. For more information, see <i>"Patch Status Messages" below</i>.

Patch Status Messages

Category	Status	Description
Patch Status States	Downloading	Patch is currently being downloaded.
	Downloaded	Patch has been successfully downloaded and verified.
	Executing	Patch installation is in progress.
	Pending	Patch is awaiting verification
	Updated	Patch has been successfully installed and verified.
	Replaced	Patch has been superseded by another patch and will not be installed. Install the latest patch to fix this CVE.
	Failed	Patch installation failed.
	Download Failed	Patch download failed.

Detailed Status States

Initial States	Update Available	Patch is available for download; URL exists and download method is automatic.
	Update Not Available	Patch URL is missing or download method is not automatic

Category	Status	Description
Download States	Downloading	Patch download is in progress.
	Download Failed	Download failed due to a specific reason.
	Ready	Download completed successfully.
User Interaction States	Pending UC	Waiting for user response or user postponed the action.
	Pending Execution	The user-approved or forced installation time has passed, but another patch in the deployment set is still being installed.
Installation States	Executing	Patch is currently being installed.
	Pending Scan	Installation finished; awaiting the scan to verify that patch is no longer needed.
	Pending Reboot	Installation finished but system reboot is required.
Final States	Updated	Patch successfully installed and verified; no longer appears in scans.
	Failed	Installation failed.
	Not Installed	Installation completed but patch still appears in verification scan.
	Replaced	Patch was replaced by another patch.
	Cancelled	The operation was canceled before completion because the administrator initiated a different deployment using the Patch Now feature.
	Interrupted	Patch disappeared from scan results (likely installed by another process).

Category	Status	Description
Download Failure Reasons	HTTP errors	Network connectivity issues, server unavailable, or authentication failures.
	Signature validation failed	Downloaded file failed digital signature verification.
	Patch file does not exist	File missing after download attempt.
	Failed to create packager (Err=X)	System component initialization failure.
	Failed to initialize packager (Err=X)	Packager configuration failure.
	Cannot get patch download info	Unable to retrieve patch metadata from vendor.
	Failed to get installable patches (Err=X)	System error retrieving available patches.
Installation Failure Reasons	Patch installation failed (Error=X)	Where X is the exit code from the patch installer. Exit code 0: Success Exit code 3010: Success but reboot required Other codes: Various installer-specific errors
	Failed To create Process	Unable to start the patch installation process.
	Deployment process finished with status X	Process completed with non-zero exit code.

Device Details Widget

DEVICE DETAILS		
OS	OS Version	Last Scanned
	10.0-19044-SP0.0-SMP	03 Apr 2023 11:33 pm
Number of Vulnerabilities	Total Apps Scanned	Number of Apps at Risk
410	31	12
Comment		

To view the **Device Details** widget, in the *"Vulnerability Assessment Table" on page 221*, under the **Device Name** column, click a device name.

The Device Details widget shows:

- Operating System name.
- Operating System version.
- Date and time the device was last scanned.
- Number of vulnerabilities detected in the device.
- Number of applications at risk.
- Comment

CVE Details Widget

CVE DETAILS				
CVSS Score	10	Last Detected	First Detected	Comment
App Name	Windows 10	03 Apr 2023 08:48 pm	03 Apr 2023 08:48 pm	
App Version	6.4	Patch Name	Patch Size	
		windows10.0-kb4592449-x64-1903-1909.msu	407 MB	

To view the **CVE Details** widget, in the *"Vulnerability Assessment Table" on page 221*, under the **Vulnerabilities** view, click a CVE number.

- CVSS score of the device.
- The application with the CVE.
- The version of the application with the CVE.
- Date and time the CVE was last detected.

- Date and time the CVE was first detected.
- Patch name available for update.
- Size of the patch available for update.
- Comment

Scanning Devices

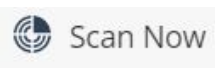
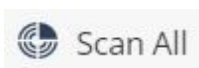
You can scan devices for vulnerable CVEs or to verify if the patch has been applied or not.

 **Note** - To start the scan for the first time:

- a. Go to **Asset Management > Computers**.
- b. Select the devices for which you want to scan.
- c. Right-click and select **Vulnerabilities > Scan Now**.

You can start subsequent manual scans by clicking **Scan Now** in **Asset Management > Posture Management** or by using the **Run Diagnostics** push operation.

To scan the devices:

1. Go to **Asset Management > Posture Management**.
2. To scan specific devices:
 - a. From the **View** list, select **Devices**.
 - b. Select the devices and click .
3. To scan all the devices affected by the CVE:
 - a. From the **View** list, select **Vulnerabilities**.
 - b. Select the CVE and click .

Mitigating Vulnerable CVEs

You can mitigate vulnerable CVEs by either isolating or applying the patch.

Isolating a Device

You can isolate a device from the network until you patch its vulnerable CVEs.

To isolate devices:

1. Go to **Asset Management > Posture Management**.
2. To isolate specific devices:

- a. From the **View** list, select **Devices**.
 - b. Select the devices and click **Push Operation > Isolate Device**.
3. To isolate all the devices affected by the CVE:
 - a. From the **View** list, select **Vulnerabilities**.
 - b. Click the vulnerability.
 - c. Select the devices and click **Push Operation > Isolate Device**.

Endpoint Security initiates the **Isolate Device** push operation. For more information, see ["Push Operations" on page 222](#).

Applying the Patch for CVEs

Notes:

- Make sure that the **Enable patch updates & reboot enforcement** checkbox is selected for the policy. Otherwise, the patch is not applied to the endpoint. For more information, see ["Configuring Posture Assessment Settings" on page 472](#).
- A single patch can fix multiple CVEs.

To apply a patch for CVE:

1. Go to **Asset Management > Posture Management**.
2. To apply patches for specific vulnerabilities:
 - a. From the **View** list, select **Vulnerabilities**.
 - b. Select the CVEs and click  **Patch** .
The **Patch Details** window appears.
 - c. Click **Update Patch**.
3. To apply the patches for specific device:
 - a. From the **View** list, select **Devices**.
 - b. Select and click the specific **Device Name**.
The **Device Details** window appears.
 - c. Select the CVEs and click  **Patch** .
The **Patch Details** window appears.
 - d. Click **Update Patch**.

Verifying the Applied Patch

 **Note** - Make sure that the vendor sites are accessible for the endpoints to download the patches directly.

1. Scan the device to verify that all CVEs are patched.
2. If all the CVEs are patched and if the device is isolated (To verify, go to **Asset Management > Organization > Computers**, from the **View list**, select **Host Isolation**, and then view the **Isolation Status** column) from the network, then add the device back to network. To add:
 - a. Go to **Asset Management > Posture Management**.
 - b. From the **View list**, select **Devices**.
 - c. Select the devices and click **Push Operations > Release Device**.
3. If required, reboot the device. To reboot:
 - a. Go to **Asset Management > Posture Management**.
 - b. From the **View list**, select **Devices**.
 - c. Select the devices and click **Push Operations > Reboot Device**.

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.

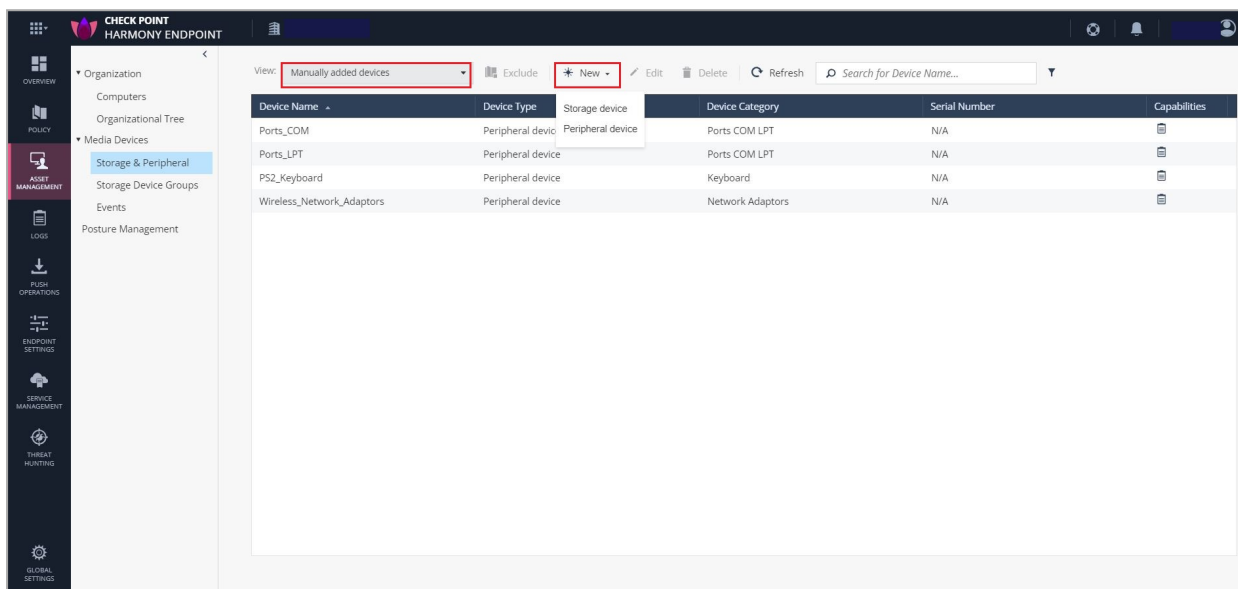
New devices are added manually or are automatically discovered by the Endpoint Server.

You can view **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.

Managing Storage and Peripheral Devices

To manually add a new device:

1. Click **Asset Management > Media Devices > Storage & Peripheral**.
2. From the **View** list, select **Manually added devices**.
3. Click  .



4. Select :

■ Storage Device

The **New Storage Device** window appears.

The screenshot shows the 'NEW STORAGE DEVICE' window. On the left is a dark blue sidebar with a tab labeled '1 EDIT DEVICE'. The main area is light gray and contains the following sections:

- Device Information**:
 - Name: Text box containing 'Test'.
 - Connection Type: Dropdown menu showing 'Internal'.
 - Category: Dropdown menu showing 'DVD CD-ROM Drives'.
 - Serial Number: Text box containing '1234'.
 - Extra Information: Dropdown menu showing 'None'.
- Device ID Filter**:
 - Device ID begins with: Text box.
- Supported Capabilities**:
 - ☒ Log device events
 - ☒ Allow encryption

A 'FINISH' button is located at the bottom right of the window.

■ Peripheral Device

The **New Peripheral Device** window appears.

NEW PERIPHERAL DEVICE

1 EDIT DEVICE

Device Information

Name: test

Applies to: Windows

Connection Type: Unknown

Category: Camera device

Serial Number: 1234

Extra Information: Hard drive with Master Boot Record

Device ID Filter

Device ID begins with: www

Supported Capabilities

☒ Log device events

FINISH

5. Enter these:

- **Name** - Enter a unique device display name, which cannot contain spaces or special characters (except for the underscore and hyphen characters).
- **Applies to** - This setting is valid for peripheral devices only.
- **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 page 241](#).
- **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.

- **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).

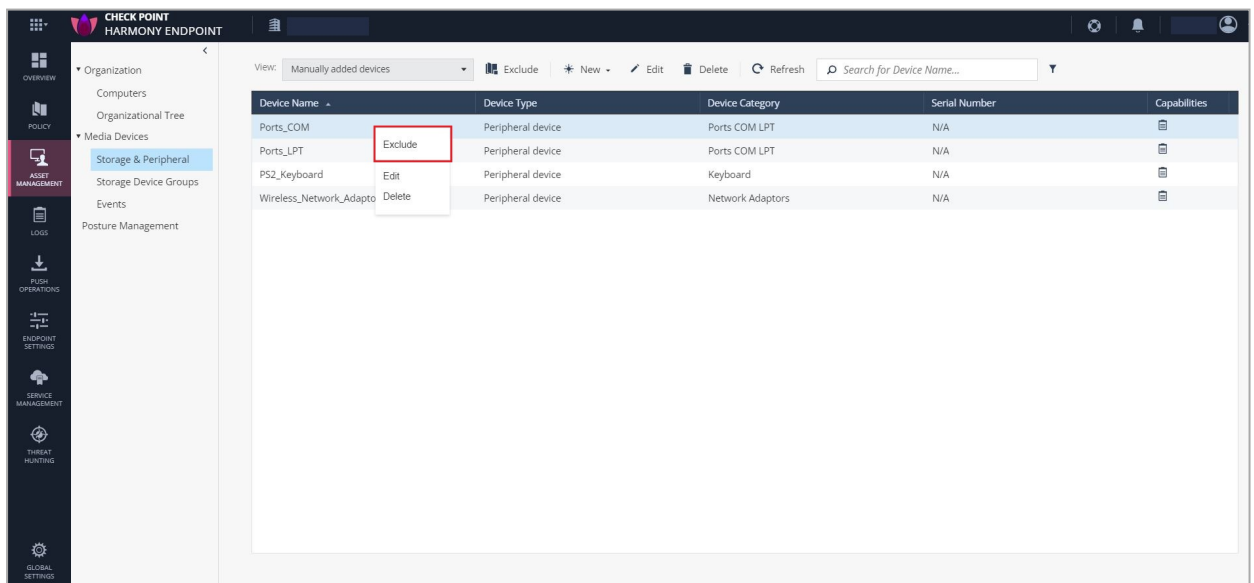
6. Assign Groups (relevant for storage devices only):

- To assign the device to an existing group, from the **existing group** list, select a group.
- To assign the device to a new group, in the **create a new group** field, enter the new group name.
- If you do not want to add the device to any group, select **do not add to group**.

7. Click **Finish**.

To add an exclusion to a device:

- Click **Asset Management > Media Devices > Storage & Peripheral**.
- Right-click the applicable device and select **Exclude**.



The **Device Override Settings** window appears.

3. Configure the required **Read Policy** and **Write Policy** (relevant to storage devices only). For more information on the configuration options, see ["Configuring the Read Action" on page 395](#) and ["Configuring the Write Action" on page 397](#)
4. **Define Behavior** (relevant for peripheral devices only):
 - a. From the **Rule(s)** list, select a rule.
 - b. From the **Access type** list, select **Accept** or **Block**.
 - c. From the **Log type** list, select a log.
 - d. Add details in the **Description** field.
5. Click **Finish**.

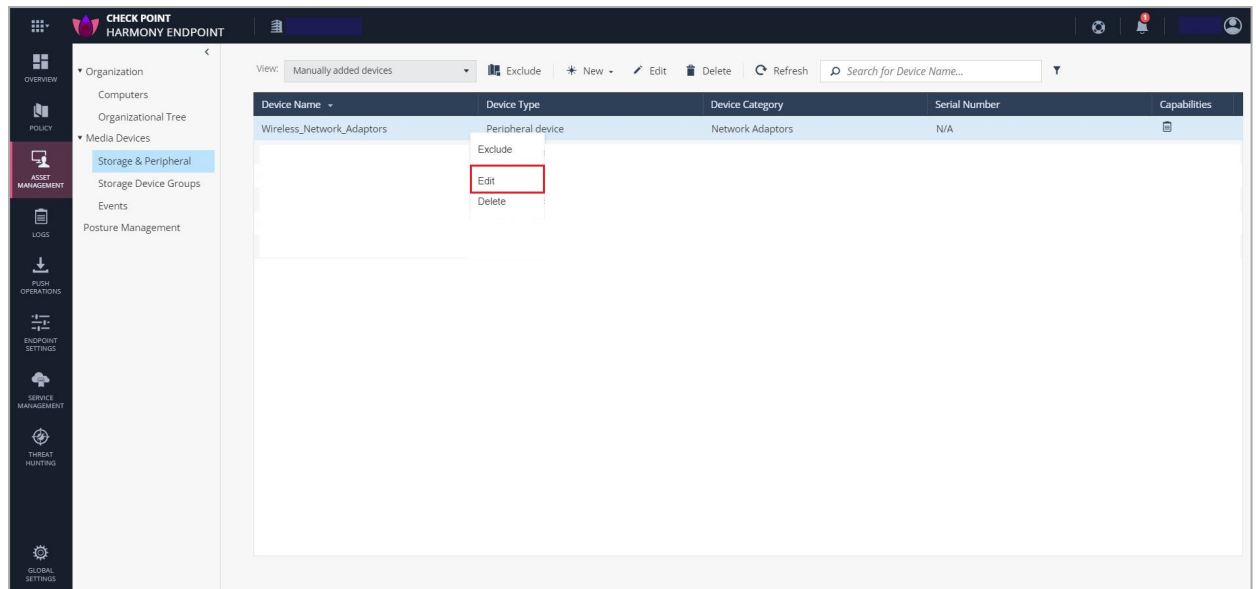


Note - If a device has an exclusion already in place, the new exclusion overrides an existing exclusion.

The **Discovered devices** view lists the details of the devices automatically discovered by the Endpoint server.

To edit a device:

1. Click **Asset Management > Media Devices > Storage & Peripheral**.
2. Right-click the applicable device and select **Edit**.



The **Edit Peripheral Device** window opens.

The 'EDIT PERIPHERAL DEVICE' window is shown with a dark sidebar on the left containing a '1 EDIT DEVICE' button. The main form area is divided into sections:

- Device Information:** Includes a 'Name' field (containing 'Ports_COM'), an 'Applies to' dropdown (set to 'Windows'), a 'Connection Type' dropdown (set to 'Unknown'), a 'Category' dropdown (set to 'Ports COM LPT'), a 'Serial Number' field with an information icon, and an 'Extra Information' dropdown (set to 'None').
- Device ID Filter:** Includes a 'Device ID begins with' field (containing 'COM').
- Supported Capabilities:** Includes a checkbox for 'Log device events' which is checked.

 A 'FINISH' button is located at the bottom right of the form.

3. Enter these:

- **Name** - Enter a unique device display name, which cannot contain spaces or special characters (except for the underscore and hyphen characters).
- **Applies to** - This setting is valid for peripheral devices only.

- **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 page 241](#).
- **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.
- **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):

- a. To assign the device to an existing group, from the **existing group** list, select a group.
- b. To assign the device to a new group, in the **create a new group** field, enter the new group name.
- c. If you do not want to add the device to any group, select **do not add to group**.

5. Configure the required **Read Policy** and **Write Policy** (relevant to storage devices only). For more information on the configuration options, see ["Configuring the Read Action" on page 395](#) and ["Configuring the Write Action" on page 397](#).

6. **Define Behavior** (relevant for peripheral devices only):

- a. From the **Rule(s)** list, select a rule.
- b. From the **Access type** list, select **Accept** or **Block**.
- c. From the **Log type** list, select a log.
- d. Add details in the **Description** field.

7. Click **Finish**.

Managing Storage Device 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.

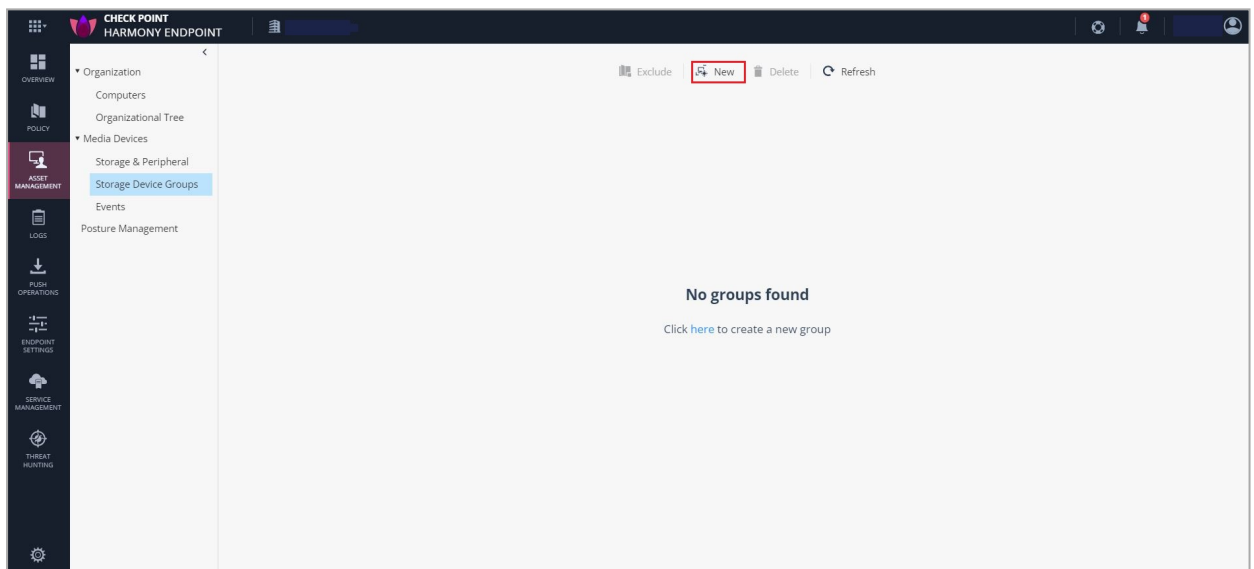
To create a new device group, or click **Asset Management > Media Devices > Storage Device Groups**. You can create new groups or edit existing groups.



Note - You cannot delete groups that are in use.

To create a Storage Device Group:

1. Click **Asset Management > Media Devices > Storage Device Groups**.
2. Click **New**.



The **Create Storage Device Group** window appears.

3. In the **Group Name** field, enter a name.
4. (Optional) In the **Comments** field, enter your comments.
For example, USB storage device.
5. To add devices to the group, click **+**.
6. Select the devices and click **OK**.
7. To delete the device, select the device and click **X**.

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

Viewing Events

Endpoint Security allows you to monitor activities related to storage and peripheral devices as events and if required, change the device details and status. For example, if a device that should be allowed was blocked and vice versa.

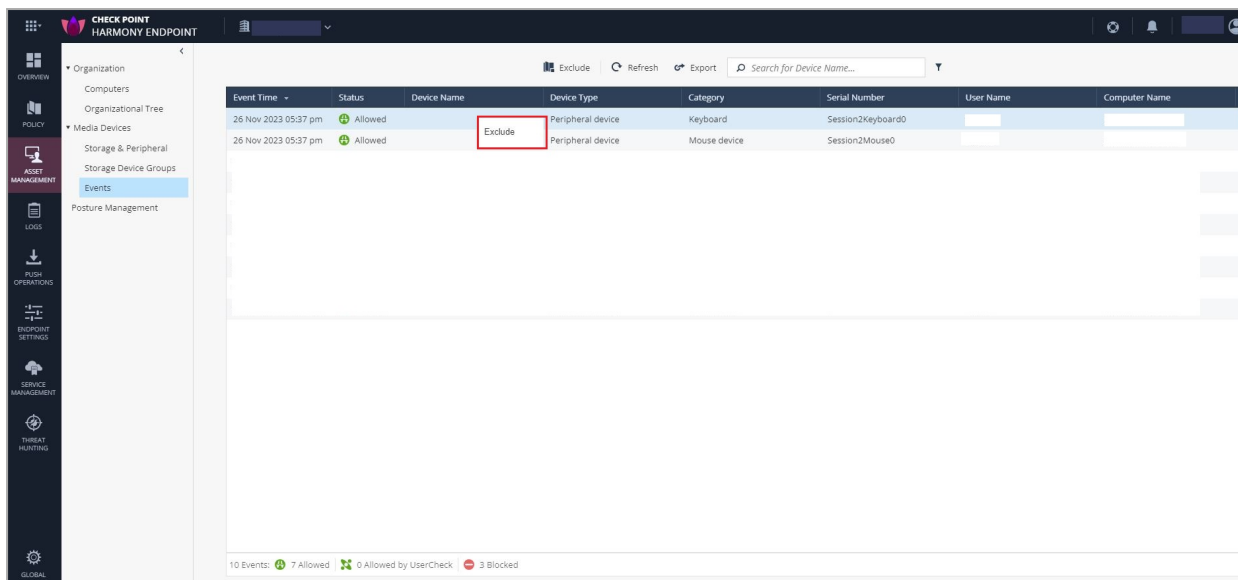
Event Time	Status	Device Name	Device Type	Category	Serial Number	User Name	Computer Name
26 Nov 2023 05:37 pm	Allowed		Peripheral device	Keyboard	Session2Keyboard0		
26 Nov 2023 05:37 pm	Allowed		Peripheral device	Mouse device	Session2Mouse0		

10 Events: 7 Allowed 0 Allowed by UserCheck 3 Blocked

Column	Description
Event Time	Date and time when the device was connected to the endpoint.
Status	Whether the device was blocked or allowed.
Device Name	Name of the device.
Device Type	Type of device.
Category	Category of the device.
Serial Number	Serial number of the device.
User Name	Name of the user.
Computer Name	Name of the computer.

To modify the device details and status:

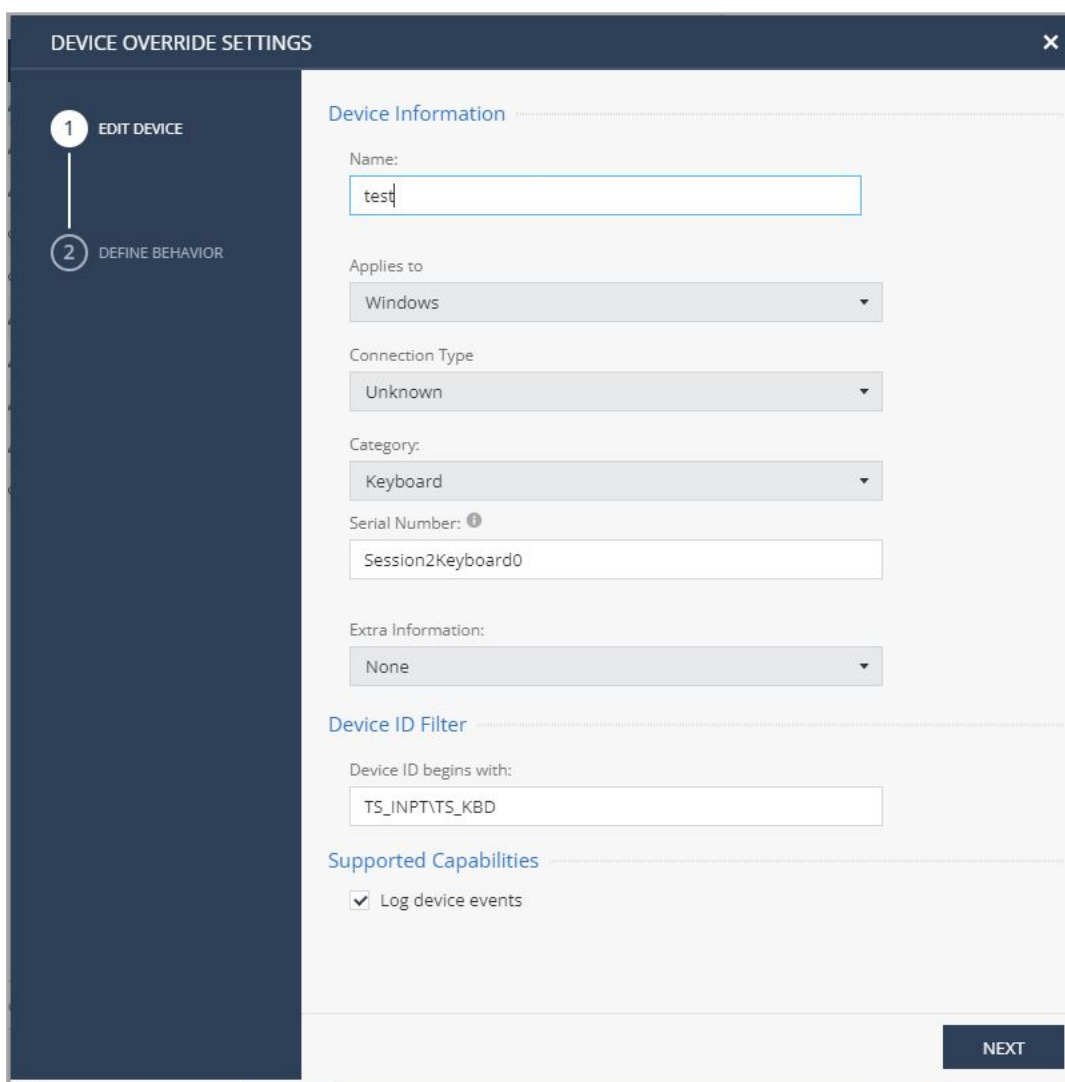
1. Click **Asset Management > Media Devices > Events**.
2. Right-click the event and select **Exclude**.



Event Time	Status	Device Name	Device Type	Category	Serial Number	User Name	Computer Name
26 Nov 2023 05:37 pm	Allowed	Exclude	Peripheral device	Keyboard	Session2Keyboard0		
26 Nov 2023 05:37 pm	Allowed		Peripheral device	Mouse device	Session2Mouse0		

10 Events: 7 Allowed 0 Allowed by UserCheck 3 Blocked

The **Device Override Settings** window opens.



1 EDIT DEVICE
2 DEFINE BEHAVIOR

Device Information

Name:

Applies to:

Connection Type:

Category:

Serial Number:

Extra Information:

Device ID Filter

Device ID begins with:

Supported Capabilities

☒ Log device events

NEXT

3. Enter these:

- **Name** - Enter a unique device display name, which cannot contain spaces or special characters (except for the underscore and hyphen characters).
- **Applies to** - This setting is valid for peripheral devices only.
- **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 page 241](#).
- **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.
- **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):

- a. To assign the device to an existing group, from the **existing group** list, select a group.
- b. To assign the device to a new group, in the **create a new group** field, enter the new group name.
- c. If you do not want to add the device to any group, select **do not add to group**.

5. Configure the required **Read Policy** and **Write Policy** (relevant to storage devices only). For more information on the configuration options, see ["Configuring the Read Action" on page 395](#) and ["Configuring the Write Action" on page 397](#).

6. **Define Behavior** (relevant for peripheral devices only):

- a. From the **Rule(s)** list, select a rule.
 - b. From the **Access type** list, select **Accept** or **Block**.
 - c. From the **Log type** list, select a log.
 - d. Add details in the **Description** field.
7. Click **Finish**.

The screenshot shows a web interface titled "DEVICE OVERRIDE SETTINGS" with a close button (X) in the top right corner. On the left is a dark blue sidebar with two steps: "1 EDIT DEVICE" (marked with a checkmark) and "2 DEFINE BEHAVIOR" (marked with a circle containing the number 2). The main area is titled "Behavior for device test" and contains the following fields:

- Rule(s)**: A search bar containing the text "Default Full Disk Encryption settings for the entire organization" with a close button (X) and a search button (Q).
- Access type**: A dropdown menu showing "Allow" with a green plus icon.
- Log type**: A dropdown menu showing "Log" with a document icon.
- Description**: A large text area for additional details.

At the bottom right of the main area are two buttons: "BACK" and "FINISH".

Configuring Endpoint Policy

The Endpoint Security policy 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 component has its own set of rules.
- **Data Protection** - which includes Full Disk Encryption and Media Encryption & Port Protection.
- **Access Policy** - Includes Firewall, Application Control, Developer Protection, Deployment Policy and Client Settings.

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.

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

Configuring the Threat Prevention Policy

 **Note** - For Managed Security Service Providers (MSSP), Endpoint Security allows you to create Threat Prevention policy templates and attach them to the child accounts. For more information, see ["Templates for Child Accounts" on page 756](#).

Unified Policy

Endpoint Security introduces the unified policy for the Endpoint components.

The unified policy lets you control all security components in a single policy. The policy is composed of a set of rules. Each rule in the policy defines the scope which the rule applies to and the activated components. This is different from the policy Rule Base in SmartEndpoint, where each component has its own set of rules.

A Default Policy rule which applies to the entire organization is predefined in your **Policy** tab. **Policy > Threat Prevention > Policy Capabilities**.

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

The Threat Prevention policy contains these capabilities which you can edit:

- ["Web & Files Protection" on page 259](#)
- ["Behavioral Protection" on page 286](#)
- ["Analysis & Remediation" on page 293](#)

The Threat Prevention policy contains device rules and user rules.

- You can use user objects only in the user policy, and you can use device objects only in the device policy.
- There is no default rule for the user policy.
- User rules override device rules.
- You can use the same group in user and device rules at the same time.
- If a group contains both users and devices, the rule is implemented according to the policy in which the rule is included.

To enable user policy, go to the **Endpoint Settings** view > **Policy Operation Mode**, and select **Mixed mode**.

Parts of the Policy Rule Base

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.
Mode	The policy mode applicable to the rule.
Web & Files Protection	The configurations that apply to Download Protection, Credential Protection and Files Protection.
Behavioral Protection	The configurations apply to Anti-Bot, Anti-Ransomware and Anti-Exploit protections.
Analysis & Response	The configurations that apply to attack analysis and Remediation.
Client Version	Version number of the Initial Client that you downloaded.

Threat Prevention Policy Toolbar

To do this	Click this
Clone, copy, paste, and delete rules	
Search	
Save, view, and discard changes Note - The View Changes functionality shows the policy type that was changed and the date of the change.	

Policy Mode

Policy mode allows you to:

- Quickly configure a Threat Prevention policy by selecting a predefined policy mode (**Detect only**, **Tuning** and **Optimized**). Check Point automatically sets the appropriate operation mode (**Detect**, **Prevent**, **Off**) and **Advanced Settings** options for each capability.
- Manually set the operation mode (**Detect**, **Prevent**, **Off**) and **Advanced Settings** options for each capability (**Custom**).

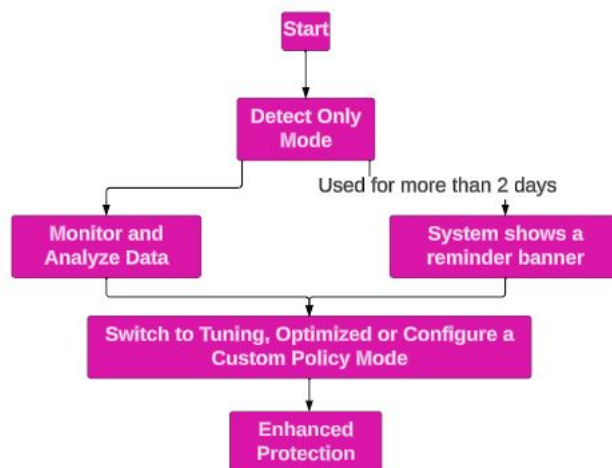


Notes:

- The **Detect only** mode provides the basic protection. We recommend that you use the **Detect only** policy mode for the first few days to gather, monitor and analyze the data. Based on the analysis, you must switch to **Tuning**, **Optimized** or configure a **Custom** policy mode for enhanced protection. If you use the **Detect only** policy mode for the **Default settings for the entire organization** rule (default) for more than two days, the system shows a banner as a reminder to configure a stricter policy mode.

❗ The policy mode of Threat Prevention rule for Entire Organization is set to "Detect only". It is recommended to harden the policy configuration. [Show Policy](#) [Remind me later](#) or [Dismiss](#)

If you click **Dismiss**, the system stops the notification only for you while it continues to appear for other users.



- If you modify a predefined policy mode, it automatically changes to **Custom**.

To select a mode for a policy:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the policy in the table.
3. In the **Capabilities and Exclusion** pane, from the **Policy Mode** list:

■ Select a predefined mode:

- **Detect only**
- **Tuning**
- **Optimized**

The table shows the appropriate operation mode set for each capability for a policy mode.

Web & File Protection

Capability	Policy Mode		
	Tuning	Detect only	Optimized
URL Filtering	Detect	Detect	Prevent
Download Protection	Detect	Detect	Prevent
Zero Phishing	Prevent	Detect	Prevent
Password Reuse	Detect	Detect	Prevent
Search Reputation	Off	Off	On
Force Safe Search	Off	Off	On
Anti-Malware Mode	Prevent	Detect	Prevent
Files Threat Emulation Mode	Detect	Detect	Prevent
Advanced Capabilities			
Advanced Settings			

Capability	Policy Mode		
	Tuning	Detect only	Optimized
URL Filtering	Allow user to dismiss the URL Filtering alert and access the website is disabled. Under Categories, Service is selected. Under Malicious Script Protection: ◦ Block websites where Malicious Scripts are found embedded in the HTML is selected. ◦ Allow user to dismiss the Malicious Scripts alert and access the website is disabled.		Allow user to dismiss the URL Filtering alert and access the website is selected. Under Categories, Service is selected. Under Malicious Script Protection: ◦ Block websites where Malicious Scripts are found embedded in the HTML is selected. ◦ Allow user to dismiss the Malicious Scripts alert and access the website is selected.

Capability	Policy Mode		
	Tuning	Detect only	Optimized
Download Protection	Under Supported files, Emulate original file without suspending access is selected. Under Unsupported files, Allow Download is selected. Under Emulation Environments: ◦ Upload and emulate files under 50 MB is selected. ◦ Use Check Point recommended emulation environments is selected.		Under Supported files: ◦ Get extracted copy before emulation completes is selected. ◦ Extract potential malicious elements is selected. Under Unsupported files, Allow Download is selected. Under Emulation Environments: ◦ Upload and emulate files under 50 MB is selected. ◦ Use Check Point recommended emulation environments is selected.
Credential Protection	Under Zero Protection, Allow user to dismiss the phishing alert and access the website is disabled. Under Password Reuse, Allow users to dismiss the password reuse alert and access the website is disabled.		Under Zero Protection, Allow user to dismiss the phishing alert and access the website is selected. Under Password Reuse, Allow users to dismiss the password reuse alert and access the website is selected.

Capability	Policy Mode		
	Tuning	Detect only	Optimized
Files Protection - General	Under Malware Treatment, Quarantine file if cure failed is selected. Under Riskware Treatment, Treat as malware is selected. Under Threat Cloud Knowledge Sharing, Allow sending infection info and statistics to Check Point servers for analysis is selected. Under Scan on Access: ◦ Enable reputation service for files, web resources and processes is selected. ◦ Connection timeout 600 ms.		
Files Protection - Signature	Under Frequency: ◦ Update signatures every 10 hours. ◦ Signature update will fail after every 60 seconds without server response.	Under Frequency: ◦ Update signatures every 11 hours. ◦ Signature update will fail after every 60 seconds without server response.	Under Frequency: ◦ Update signatures every 2 hours. ◦ Signature update will fail after every 60 seconds without server response.
	Under Signature Sources: ◦ First Priority: External CheckPoint Signature Server. ◦ Second Priority: N/A ◦ Third Priority: N/A		

Capability	Policy Mode		
	Tuning	Detect only	Optimized
Files Protection - Scan	Run initial scan after Anti-Malware blades installation is selected. Allow user to cancel scan is selected. Prohibit cancel scan if more than 30 Days passed since last successful scan is selected. Under Scan targets: ◦ Critical areas is selected. ◦ Local drives is selected. ◦ Mail messages is selected. Under Scan Target Exclusions: ◦ Skip archives and non executables is selected. ◦ Do not scan files larger than 20 MB is selected.		Run initial scan after Anti-Malware blades installation is selected. Under Scan targets: ◦ Critical areas is selected. ◦ Local drives is selected. ◦ Mail messages is selected. Under Scan Target Exclusions: ◦ Skip archives and non executables is selected. ◦ Do not scan files larger than 20 MB is selected.
Advanced Capabilities			

Behavioral Protection

Capability	Policy Mode		
	Tuning	Detect only	Optimized
Anti Bot	Detect	Detect	Prevent
Behavioral Guard & Anti Ransomware	Detect	Detect	Prevent
Anti Exploit	Detect	Detect	Prevent
Advanced Settings			

Capability	Policy Mode		
	Tuning	Detect only	Optimized
Anti Bot	Under Background Protection Mode, Background - connections are allowed until threat check is complete is selected. Hours to suppress logs for same bot protection is set to 1. Days to remove bot reporting after is set to 3. Under Confidence Level: ◦ High Confidence is set to Detect. ◦ Medium Confidence is set to Detect. ◦ Low Confidence is set to Detect.		
Behavioral Guard & Anti Ransomware	Anti-Ransomware Maximum backup size on disk is disabled. Backup Time Interval is disabled. Under Disk Usage, Maximum Forensics Database size on disk is disabled.	Anti-Ransomware Maximum backup size on disk is set to 1025 MB. Backup Time Interval is set to 60 Minutes. Under Disk Usage, Maximum Forensics Database size on disk is set to 1 GB.	

Analysis & Remediation

Capability	Policy Mode		
	Tuning	Detect only	Optimized
Protection Mode	Always	Always	Always
Enable Threat Hunting	On	Off	On
Remediation & Response	Never	Never	Medium & High
Advanced Settings			

Capability	Policy Mode		
	Tuning	Detect only	Optimized
File Quarantine	Under File Quarantine : ◦ File Quarantine is set to Never. ◦ Allow users to delete items from quarantine is disabled. ◦ Allow users to restore items from quarantine is disabled. ◦ Copy quarantine files to central location is disabled. ◦ Choose location is disabled. ◦ Quarantine folder name is disabled.		Under File Quarantine : ◦ File Quarantine is set to Medium & High. ◦ Choose location is disabled. ◦ Enter the location of the Quarantine folder name.
File Remediation	Under File Remediation : ◦ Malicious Files is set to Quarantine. ◦ Suspicious Files is set to Quarantine. ◦ Unknown Files is set to Quarantine. ◦ Trusted Files is set to Ignore.		Under File Remediation : ◦ Malicious Files is set to Quarantine. ◦ Suspicious Files is set to Quarantine. ◦ Unknown Files is set to Quarantine. ◦ Trusted Files is set to Terminate.

- Select **Custom** and set the operation mode manually. For more information, see ["Web & Files Protection" on page 259](#).

4. Click **Save**.

5. Click **Save & Install**.

Updating a Predefined Policy Mode

Based on internal analysis and research, Check Point may suitably modify the operation mode or **Advanced Settings** of a predefined policy mode. If a predefined mode is updated, a notification appears.

Policy Mode ⓘ

Detect only ▼



Settings do not match "Detect only" policy mode

[Align](#)[Keep](#)

- Click **Align** to accept the updates. The system automatically updates to the new settings for the predefined mode.
- Click **Keep** to retain the current settings. The policy mode changes to **Custom**.

Web & Files Protection

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

URL Filtering

URL Filtering rules define which sites you can access in your organization. The URL Filtering policy is composed of the selected sites and the mode of operation applied to them.



Note: URL Filtering is not supported with SmartEndpoint.

To create the URL Filtering policy:

1. Go to **Policy > Threat Prevention > Policy Capabilities**. In the **Capabilities & Exclusions** pane, select **Web & Files Protection**.
2. In the **Web & Files Protection** tab, scroll-down to **URL Filtering**.
3. Select the **URL Filtering Mode** of operation:
 - **Prevent** - Currently supported only in Hold mode. The request to enter a site is suspended until a verdict regarding the site is received.
 - **Detect** - Allows access if a site is determined as malicious, but logs the traffic.
 - **Off** - URL Filtering is disabled.
4. Select the categories to which the URL Filtering policy applies:

- a. Go to **Web & Files Protection > Advanced Settings > URL Filtering > Categories**.

b. Select the required categories:

■ **Bandwidth Consumption**

- Media Streams
- File Storage and Sharing
- P2P File Sharing
- Media Sharing

■ General Use

- Computers / Internet
- Education
- Entertainment
- Financial Services
- Government / Military
- Greeting Cards
- Health
- Political / Legal
- Job Search / Careers
- News / Media
- Newsgroups / Forums
- Uncategorized
- Real Estate
- Recreation
- Religion
- Restaurants / Dining / Food
- Sex Education
- Shopping
- Alcohol & Tobacco
- Art / Culture
- Blogs / Personal Pages
- Business / Economy
- Software Downloads
- Sports
- Translation
- Travel
- Vehicles
- Fashion

- Non-profits & NGOs
- General
- Nature / Conservation
- URL Filtering
- Lifestyle
- Lingerie and Swimsuit / Suggestive
- Very Low Risk
- Low Risk
- Email
- Web Advertisements
- Search Engines / Portals
- **Legal Liability / Regulatory Compliance**
 - Gambling
 - Hacking
 - Hate / Racism
 - Illegal / Questionable
 - Illegal Drugs
 - Nudity
 - Pornography
 - Tasteless
 - Violence
 - Weapons
 - Sex
 - Child Abuse
 - Marijuana

- **Productivity**

- Personals / Dating
- Instant Messaging
- Games
- Social Networking
- Instant Chat

- **Service**

- Phishing
- Spyware / Malicious Sites
- Botnets
- Spam
- Inactive Sites
- Suspicious Content
- Medium risk
- High risk
- Critical risk
- Anonymizer

 **Note** - For each category, click **Edit** to see the sub-categories you can select. You can either select the whole category or some sub-categories as per the requirement.

- c. Click **OK**.
5. (Optional) You can select specific URLs to which access is denied. See ["Deny List" on the next page](#).
 6. Configure **Network URL Filtering**:
 - a. To verify and filter all the URLs accessed by an application or a process, select **Enable Network URL Filtering**. If this option is not selected, the URL filtering is applied only to the URLs accessed through a browser.

- b. To disable Endpoint Security client notifications for network URL filtering, select **Disable Network URL filtering pop-up notifications if they originate from a browser session**.

 **Note** - This option is applicable only when the Endpoint Security Browser extension is installed in the client device.

The selected mode of operation now applies to the selected categories.

The user can access any site which was not selected in one of the categories or which was not in the Deny List.

You can **Allow user to dismiss the URL Filtering alert and access the website** - This option is selected by default. This lets you access a site determined as malicious, if you think that the verdict is wrong. To do this, go to **Advanced Settings > URL Filtering**.

Deny List

You can add specific URLs or domains to the Deny List which blocks the users from accessing them. 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 deny list.

To add a URL to the Deny List:

1. Go to **Advanced Settings > URL Filtering > Deny List > 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 the deny list.

- * 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 > Deny List > 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 > Deny List > 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 > Deny List > Edit**.
2. Next to the search box, click the  sign (export domains list to a CSV file).
3. Click **OK**.

Download (Web) Emulation & Extraction

Endpoint Security browser protects against malicious files that you download to your device. For the browsers supported with the Endpoint Security Browser extension, see [Browser Security Administration Guide](#).

Threat Emulation detects zero-day and unknown attacks. Files on the endpoint computer are sent to a sandbox for emulation to detect evasive zero-day attacks. The following files types are supported:

Threat Emulation Supported File Types

7z	Ink	slk
aspx ³	msi ¹	swf
app ¹	msg ¹	tar
arj	O ¹	tbz2
bat	one ²	tbz
bz2	pif	tb2
CAB	pdf	tgz
csv	pkg ¹	udf
com	ppt	uue
cpl	pptx	wim
dll	pps	wsf ²
doc	pptm	xar ²
docx	potx	xlt
dot	potm	xls
dotx	ppam	xlsx
dotm	ppsx	xlm
docm	ppsm	xltx
dmg ¹	ps1	xlsm
dylib ¹	qcow2 ¹	xltm
exe	rar	xlsb
gz	rtf	xla
hwp	sh ¹	xlam
iso	scr	xll

Threat Emulation Supported File Types

img ¹	sldx	xlw
iqy	sldm	xz
jar		zip



Notes:

- ¹ These file types are supported only with Endpoint Security Client version E87.40 and higher.
- ² These file types are supported only with Endpoint Security Client version E87.60 and higher.
- ³ These file types are supported only with Endpoint Security Client version E88.10 and higher.

Threat Extraction proactively protects users from malicious content. It quickly delivers safe files while the original files are inspected for potential threats.

To see the list of file types which are supported by Threat Emulation and Threat Extraction:

1. Go to **Policy > Threat Prevention > Policy Capabilities**. In the **Capabilities & Exclusions** pane, select **Web & Files Protection**.
2. In the **Web & Files Protection** tab, go to **Advanced Settings > Threat Emulation > Override Default File Actions > Edit**.

These are the configuration options for supported file types:

- **Prevent** - Send files for emulation and extraction. For further configuration for supported files, go to **Advanced Settings > Supported Files**:
 - **Get extracted copy before emulation completes** - You can select one of these two options. The system appends *.cleaned* to the file name. For example, *xxx.cleaned*.
 - **Extract potential malicious elements** - The file is sent in its original file type but without malicious elements. Select which malicious parts to extract. For example, macros, Java scripts and so on.
 - **Convert to PDF** - Converts the file to PDF, and keeps text and formatting.
 - ★ **Best Practice** - If you use PDFs in right-to-left languages or Asian fonts, preferably select **Extract files from potential malicious parts** to make sure that these files are processed correctly.

- **Suspend download until emulation completes** - The user waits for Threat Emulation to complete. If the file is benign, the gateway sends the original file to the user. If the file is malicious, the gateway presents a Block page and the user does not get access to the file. This option gives you more security, but may cause time delays in downloading files. The system downloads the file with the original file name.
 - **Emulate original file without suspending access** - The gateway sends the original file to the user (even if it turns out eventually that the file is malicious).
 - **Allow** - All supported files are allowed without emulation. This setting overrides the Prevent setting selected in the main page.
- **Detect** - Emulates original file without suspending access to the file and logs the incident. The file is blocked if it is malicious or blocked by file extension (**Advanced Settings > Download Protection**). If not, the file is downloaded before the emulation is complete.
 - **Off** - Allow file. No emulation or extraction is done. The download of all supported files is allowed.

Unsupported Files

File types which are not supported by Threat Emulation and Threat Extraction. Unsupported files types can be allowed or blocked. To configure, go to **Advanced Settings > Download Protection > Unsupported Files**. The settings selected here override the settings selected in the main page.

Additional Emulation Settings:

Emulation Environments

To define the maximum size of files that are sent for emulation, go to **Advanced Settings > Download Protection > Emulation Environments** and specify the file size for **Upload and emulate files under**.



Notes -

- Only the Endpoint Security Client version E86.40 and higher support a maximum file size up to 100 MB. Client versions lower than E86.40 support a maximum file size up to 15 MB.
- Increasing the file size increases the client processing and network traffic required to process large files.

To select the operating system images on which the emulation is run, go to **Advanced Settings > Download Protection > Emulation Environments**, and select one of these options:

- **Use Check Point recommended emulation environments**
- **Use the following emulation environments** - Select other images for emulation, that are closest to the operating systems for the computers in your organization. This is supported only if configured from the SmartConsole.

Override Default Files Actions

Endpoint Security allows you to override the default file action for the supported and unsupported files.

To override the default file actions, navigate to **Advanced Settings > Download Protection > Override default file actions (download)**.

To override the file action for supported files:

1. In the **Supported Files** section, click **Edit**.
2. Select the **File action** and **Extraction Mode**.
3. Click **OK**.

To override the file action for unsupported files:

1. In the **Unsupported Files** section, click **Edit**.
 - a. To add a file type, click  and enter the **File type**.
 - b. To edit a file type, select the file type and click .
 - c. To delete a file type, select the file type and click .
2. Select the **Download action** for the file:
 - **Default** - The action specified in *"Unsupported Files" on the previous page*.
 - **Allow**
 - **Block**
3. (Optional) In the **Comments** field, enter a comment.
4. Click **OK**.

Custom Settings

Download Emulation and Extraction

- **Block downloads when emulation fails due to size limit or connectivity problem** - Select the checkbox to block download of a file if the Threat Emulation of the file fails due to technical reasons, such as file size limit, no internet connectivity and invalid licenses.
- **Block downloads when emulation fails due to file encryption** - Select the checkbox to block download of a file if the Threat Emulation of the file fails to extract the file due to the file encryption.

Credential Protection

To configure the credential protection policy:

1. Go to **Policy > Threat Prevention > Policy Capabilities**. In the **Capabilities & Exclusions** pane, select **Web & Files Protection**.
2. In the **Web & Files Protection** tab, scroll-down to **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** - If the site is determined to be a phishing site, users cannot access the site. A log is created for each malicious site.
- **Detect** - When a user uses a malicious site, a log is created.
- **Off** - Phishing prevention is disabled.

For further configuration of the Zero Phishing protection, go to **Advanced Settings > Credential Protection**:

- **Allow user to dismiss the phishing alert and access the website** - Users can select to use a site that was found to be malicious.
- **Send log on each scanned site** - Send logs for each site that users visit, whether malicious or not.
- **Allow user to abort phishing scans** - Users can stop the phishing scan before it is completed.

- **Scan local HTML files** - By default, the Endpoint Security extension in Chromium-based browsers (Chrome, Microsoft Edge, and Brave) cannot access the local HTML files opened by the browser to scan them for phishing attacks. This setting prompts users to grant permission to Chromium-based browsers to access and scan local HTML files on your PC.

 Notes:

- You can customize the prompt page. For more information, see ["Customized Browser Block Pages" on page 349](#).
- This feature is not supported with Safari and Internet Explorer browser extensions.
- This feature is supported with the Endpoint Security Client version E86.50 and higher.

To grant permission to access and scan the local HTML files:

1. When a user opens a local HTML file, the **Browser Security request access to file URLs** prompt appears. Click **Click to copy**.
 2. Paste the copied path in the address bar of the Chrome browser and press **Enter**.
 3. Scroll down and turn on **Allow access to file URLs**.
 4. If the HTML file has an input field, Browser Security scans the file and blocks it, if identified as phishing.
- **Disable notifications** - Allows you to disable the browser zero-phishing scan notification that appears when users try to enter in an input field.

-  **Note** - Only the notification is disabled but the browser zero-phishing scan is performed in the background indicated by the yellow highlight around the input field.

Password Reuse Protection

Alerts users not to use their corporate password in non-corporate domains.

To set the Password Reuse mode:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the rule.
3. In the **Capabilities & Exclusions** pane, select **Web & Files Protection**.
4. In the **Web & Files Protection** tab, scroll-down to **Credential Protection**.
5. In the **Credential Protection** section, under **Password Reuse**, select a mode:

- **Prevent mode** - Blocks the user from entering the corporate password and opens the blocking page in a new tab. If you enable **Allow users to dismiss the password reuse alert and access the website**, then it allows the user to dismiss the blocking page and continue to enter the corporate password.
- **Detect & Alert** - Blocks the user from entering the corporate password and opens the blocking page in a new tab and allows the user to dismiss the blocking page and continue to enter the corporate password.

 Notes:

- This option is available only in older releases of Endpoint Security. In the newer releases, it is deprecated by **Prevent mode**.
 - If you enable this option, then Endpoint Security automatically disables **Allow users to dismiss the password reuse alert and access the website**.
- **Detect mode** - The system does not block the user from entering the corporate password. If a user enters the corporate password, it is captured in the logs.
 - **Off** - Turns off password reuse protection.

6. For **Advanced Settings**, see ["Credential Protection" on page 271](#).

For further configuration options for password reuse protection, click **Edit > Protected Domains**:

Add domains for which Password Reuse Protection is enforced. Endpoint Security keeps a cryptographic secure hash of the passwords used in these domains and compares them to passwords entered outside of the protected domains.

Safe Search

Search Reputation

Search Reputation is a feature added to search engines that classifies search results based on URL's reputation.

 Notes:

- It is supported only with Google, Bing, and Yahoo search engines.
- To enable this feature, ensure that you set **URL Filtering Mode** to either **Prevent** or **Detect**.

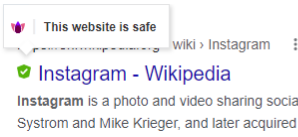
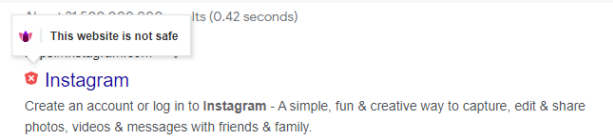
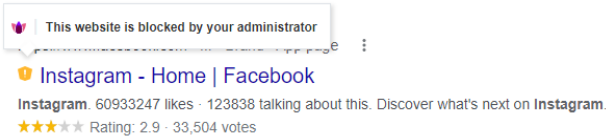
To set the Search Reputation mode:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the rule.
3. In the **Capabilities & Exclusions** pane, select **Web & Files Protection**.

4. In the **Web & Files Protection** tab, scroll-down to **Search Reputation** section and select a mode:

- **On** - Turns on the feature.
- **Off** - Turns off the feature.

When you enable this feature, the icon across the URL in the search results indicate the classification:

Icon	Classification
	The website is safe. Example: 
	The website is not safe. Example: 
	The website is blocked by the Administrator. Example: 

Note - If the Search Reputation cannot classify a URL, then it does not display an icon across the URL. If you want such URLs to be classified and blocked, then enable the **Uncategorized** checkbox in **URL Filtering > Categories > General Use**. The Search Reputation classifies **Uncategorized** URLs as **The website is blocked by the Administrator**.

Force Safe Search

Force Safe Search is a feature in search engines that acts as an automated filter for potentially offensive and inappropriate content.

To set the Force Search Reputation mode:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the rule.

3. In the **Web & Files Protection** tab, under **Force Safe Search**, select a mode:
 - **On** - Hides explicit content from the search results.
 - **Off** - User sees the most relevant results for their search, which may include explicit content like images consisting of violence.

Main features:

- When 'Force Safe Search' is on, Browser Security turns on Safe Search on the supported search engines.
- It is supported with Google, Bing, and Yahoo search engines.
- Force Safe Search is off by default.
- Force Safe Search is supported with Google Chrome, and Microsoft Edge browsers.

Files Protection

Protects the files on the file system. To configure the Files Protection policy:

1. Go to **Policy > Threat Prevention > Policy Capabilities**. In the **Capabilities & Exclusions** pane, select **Web & Files Protection**.
2. In the **Web & Files Protection** tab, scroll-down to **Files Protection**.

This protection has two components:

- **Anti-Malware Mode** - 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** - Protects your files from malware threats.
- **Detect** - Detects the threats, so they appear in the logs, although the virus or malware are still executable. Use this mode with caution.
- **Off** - No protection from malware.

**Notes -**

- Starting from the Endpoint Security Client E83.20, Check Point certified the E2 client version (the Anti-Malware engine is DHS compliant) for Cloud deployments.
- The E1 Anti-Malware blade can scan these archive file formats:
 - ZIP
 - Z
 - LZIP
 - 7Z
 - RAR
 - ISO
 - CAB
 - JAR
 - BZIP2
 - GZIP
 - DMG
 - XAR
 - TAR
 - ACE
- The E2 DHS Anti-Malware blade can scan these archive file formats:
 - ZIP
 - Z
 - 7Z
 - RAR
 - ISO
 - CAB
 - JAR
 - BZIP2
 - GZIP
 - DMG
 - XAR
 - TAR
 - ACE

■ **Files Threat Emulation Mode** - Emulation of files on the system.

There are three configuration options for this protection:

- **Prevent** - Detects a malicious file, logs the event and deletes the file.
- **Detect** - Detects a malicious file and logs the event.
- **Off** - Files Threat Emulation mode is off. Does not run the Threat Emulation on the file.

This is supported with Endpoint Security client version E86.80 and higher.

- **Advanced Capabilities** - You can set an action for each of these capabilities separately:

 **Note** - This is supported only with the Endpoint Security client version E88.30 and higher.

Advanced Capability	Description
ThreatCloud Reputation	Verifies the reputation of files based on their hash in Check Point Cloud-Based Database. This feature is supported from E88.50 and later.
Offline Reputation	Verifies file reputation by hash using local data. When connected to the network, the data gets updated with ThreatCloud's common hashes for offline verification.
Vulnerable Driver Protection	Provides protection against potentially malicious drivers by blocking the vulnerable drivers introduced to the device. This also includes drivers that are downloaded, extracted, or copied to the device.  Note - This feature is supported in Endpoint Security Client version E88.50 and higher.
Static Signatures	Inspects files using YARA (Yet Another Recursive Acronym) signatures to protect against malware.  Notes: • For Static Signatures (YARA) to work, the Anti-Malware security blade must be in Prevent/Detect mode. • Supports E89.00 Endpoint Security Client for Windows and 1.22.x for Linux. • Endpoint Security records YARA logs within the Anti-Malware logs. For more information, see Static Signature (YARA) Logs. • Supported actions are: ◦ Prevent - Detects a malicious file, logs the event and quarantines the file. ◦ Detect - Detects a malicious file and logs the event. ◦ Off - No protection from malicious file.
Office Files	Performs static analysis ¹ on Microsoft Office files.
Executables Files	Performs static analysis ¹ on executable files.
DDL Files	Performs static analysis ¹ on DLL files.

¹Analyzes files without executing them against data models to identify potentially malicious files.

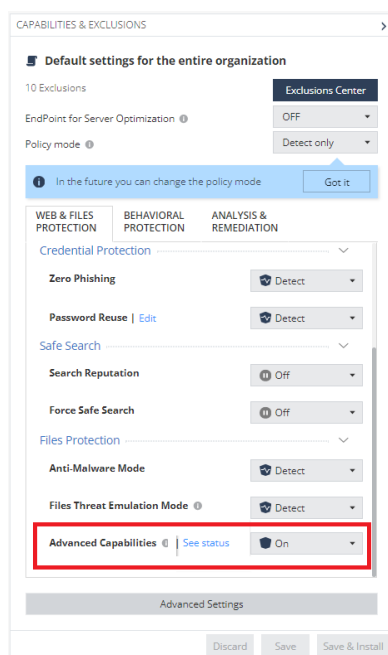
The supported actions are:

- **Prevent** - Detects a malicious file, logs the event and quarantines the file.
- **Detect** - Detects a malicious file and logs the event.
- **Off** - No protection from malicious file.

For more information, see ["Advanced Capabilities" on page 283](#).

To enable Advanced Capabilities:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select a rule.
3. In the **Web & Files Protection** tab, in the **Advanced Capabilities** list, select **On**.



 **Note** - To view the set action for each capability, click **See status**.

Advanced Settings

To configure the advanced settings of the threat prevention policy:

1. Go to **Policy > Threat Prevention > Policy Capabilities**. In the **Capabilities & Exclusions** pane, select **Web & Files Protection**.
2. In the **Web & Files Protection** tab, click **Advanced Settings**.
3. Use the following sections to modify the respective settings.

Files Protection

To configure the advanced settings for files protection, go to **Advanced Settings > Files Protections**.

General

- **Malware Treatment** - The malware treatment options let you select what happens to malware that is detected on a client computer:
 - **Quarantine file if cure failed** - If Endpoint Security cannot repair the file, it is deleted and put in a secure location from where it can be restored if necessary.
 - **Delete file if cure failed** - If Endpoint Security cannot repair the file, it is deleted.
- **Riskware Treatment** - Riskware is a legal software that might be dangerous.
 - **Treat as malware** - Use the option selected for Malware.
 - **Skip file** - Do not treat riskware files.
 - **Detect unusual activity** - Use behavior detection methods to protect computers from new threats whose information were not added to the databases yet. It does not monitor trusted processes.
 - **Enable reputation service for files, web resources & processes** - Use cloud technologies to improve precision of scanning and monitoring functions. If you enable or disable this setting, it takes affect after the client computer restarts.

Connection timeout - Change the maximum time to get a response from Reputation Services (in milliseconds). Default is 600.

 **Note** - If you decrease this value, it can improve the performance of the Anti-Malware component but reduces security, as clients might not get a reputation status that shows an item to be zero-day malware.

 - **Enable web protection** - Prevents access to suspicious sites and execution of malicious scripts Scans files, and packed executables transferred over HTTP, and alerts users if malicious content is found.
- **Threat Cloud Knowledge Sharing** - To share infected information, statistics and infected file samples with Check Point for analysis, select any of these:
 - **Allow sending infection info and statistics to Check Point servers for analysis**
 - **Allow sending infected file samples to Check Point servers for analysis**

 **Note** - This is supported only with a DHS compliant Endpoint Security client.
- **Mail Protection** - Enable or disable scans of email messages when they are passed as files across the file system.

Signature

■ Frequency

Anti-Malware gets malware signature updates at regular intervals to make sure that it can scan for the newest threats. These actions define the frequency of the signature updates and the source:

- **Update signatures every [x] hours** - Signature updates occur every [x] hours from the Endpoint Policy Server and the External Check Point Signature Server.
- **Signature update will fail after [x] seconds without server response** - The connection timeout, after which the update source is considered unavailable.

■ Signature Sources

- **External Check point Signature Server** - Get updates from a dedicated, external Check Point server through the internet.
- **Other External Source** - Get updates from an external source through the internet. Enter the URL.

- **Shared signature source** - Get updates from a shared location on an Endpoint Security client that acts as a Shared Signature Server. This solution is curated for Virtual Desktop Infrastructure (VDI) environments, but can be leveraged for other scenarios as well. This makes it possible to protect non-persistent virtual desktops in Virtual Desktop Infrastructure (VDI) environments. Each non-persistent virtual desktop runs an Endpoint Security, and gets Anti-Malware and Threat Prevention signatures from a shared folder on the Shared Signature Server that is a persistent virtual machine.

- **Second Priority** - Set a fallback update source to use if the selected update source fails. Select a different option than the first signature source.
- **Third Priority** - Set a fallback update source to use if the other sources fail.

 **Note** - If only update from local Endpoint Servers is selected, clients that are disconnected from an Endpoint Security server cannot get updates.

- **Shared Signature Server** - To set the server as a Shared Signature Server, select the **Set as shared signature server** checkbox and enter the local path of the folder. For example, *C:\Signatures*. For more information, see ["Shared Signatures Server" on page 694](#).

Scan

Anti-Malware scans computers for malware at regular intervals to make sure that suspicious files are treated, quarantined, or deleted.

- **Perform Periodic Scan** - Select one of these options to define the frequency of the scans:

- **Every Month**- Select the day of the month on which the scan takes place and the **Scan start hour**.
- **Every Week** - Select the day of the week on which the scan takes place and the **Scan start hour**.
- **Every Day** - Select the scan start hour.
- **Scan on Idle** - Specify the idle time duration for the endpoint. The Endpoint Security client initiates the initial or periodic Anti-Malware scan only when the endpoint remains idle for the specified duration. If the device is not idle, the scan is postponed for 24 hours. After this 24-hour period, the Endpoint Security client initiates the initial or periodic Anti-Malware scan, irrespective of whether the device is idle or in use.

 **Note** - Scan on Idle is only supported by Endpoint Security Client E87.60 and higher.

Optional :

- **Randomize scan time** - Mandatory for Virtual Desktop Infrastructure (VDI). Select this option to make sure that not all computers do a scan for malware at the same time. This makes sure that network performance is not affected by many simultaneous scans. In **Start scan** and **End scan**, specify the time range during which the scan can start and end.
 - **Run initial scan after the Anti-Malware blades installation.**
 - **Allow user to cancel scan.**
 - **Prohibit cancel scan if more than X Days passed since last successful scan.**
- **Scan Targets** - Select the target for the Anti-Malware scan:
- **Critical areas**
 - **Optical drives**
 - **Local drives**
 - **Mail messages**
 - **Removable drives**
 - **Unrecognized devices**
 - **Network devices**

 **Notes:**

- **Mail messages** is not supported with the **DHS compliant Anti-Malware blade** in macOS.
- **Critical areas** is supported with the **DHS compliant Anti-Malware blade** from **E88.00 and higher**.

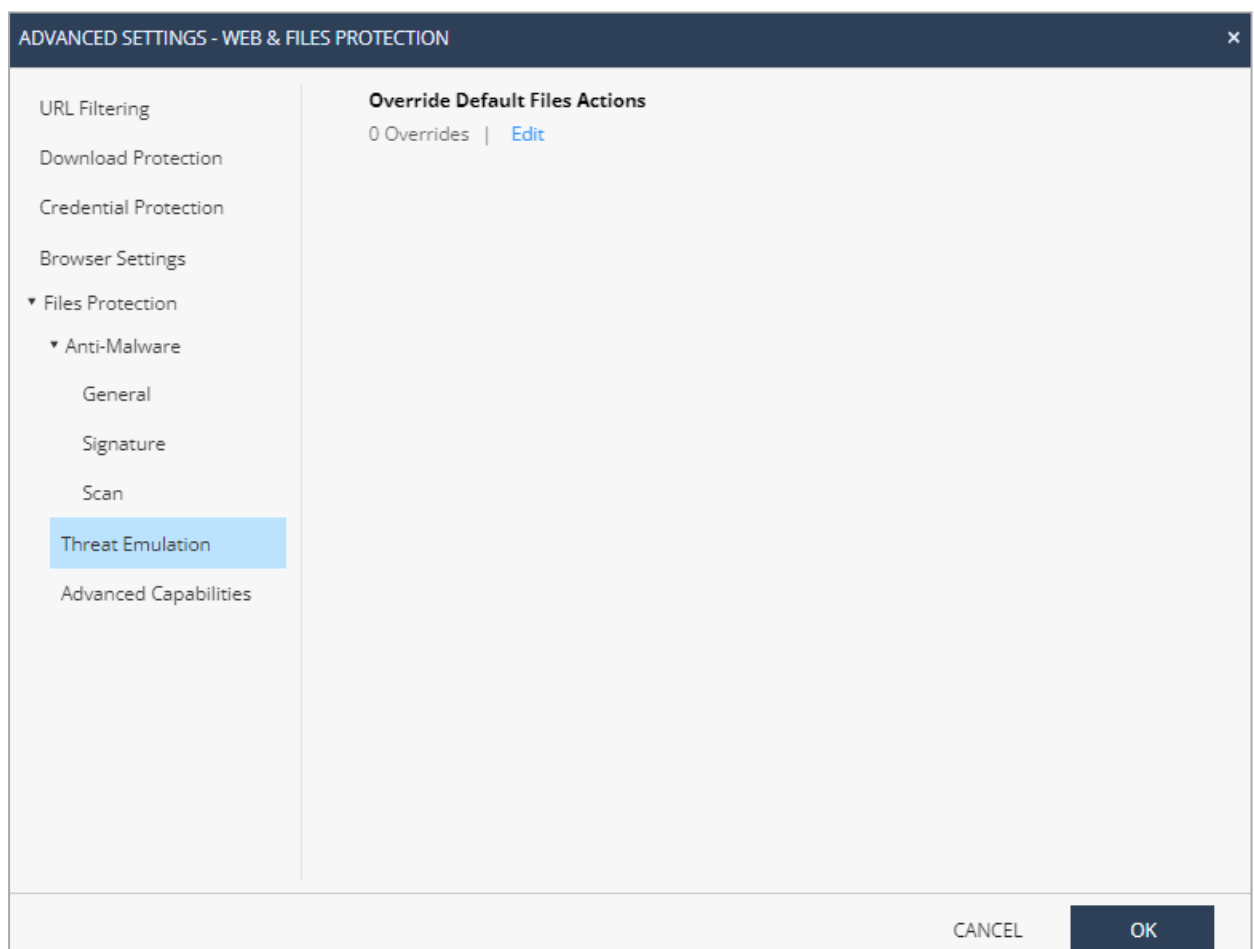
- **Scan Target Exclusions** - Select the checkboxes to skip scanning of certain files.
 - **Skip archives and non executables** - Skips scanning of archive file formats (for example, .zip, 7zip, tar.gz, rar, and so on) and non-executable files (files without the execute permission).
 -  **Note** - **Skip archives and non executables** are not supported with the DHS compliant Anti-Malware blade.
 - **Do not scan files larger than** - Specify the file size limit. If the file size is larger than the specified limit, then the system skips scanning the file. The default file size limit is 20 MB.
 -  **Note** - The maximum supported file size for the Anti-Malware scan depends on the endpoint's system specifications, such as CPU, RAM and so on.

Threat Emulation

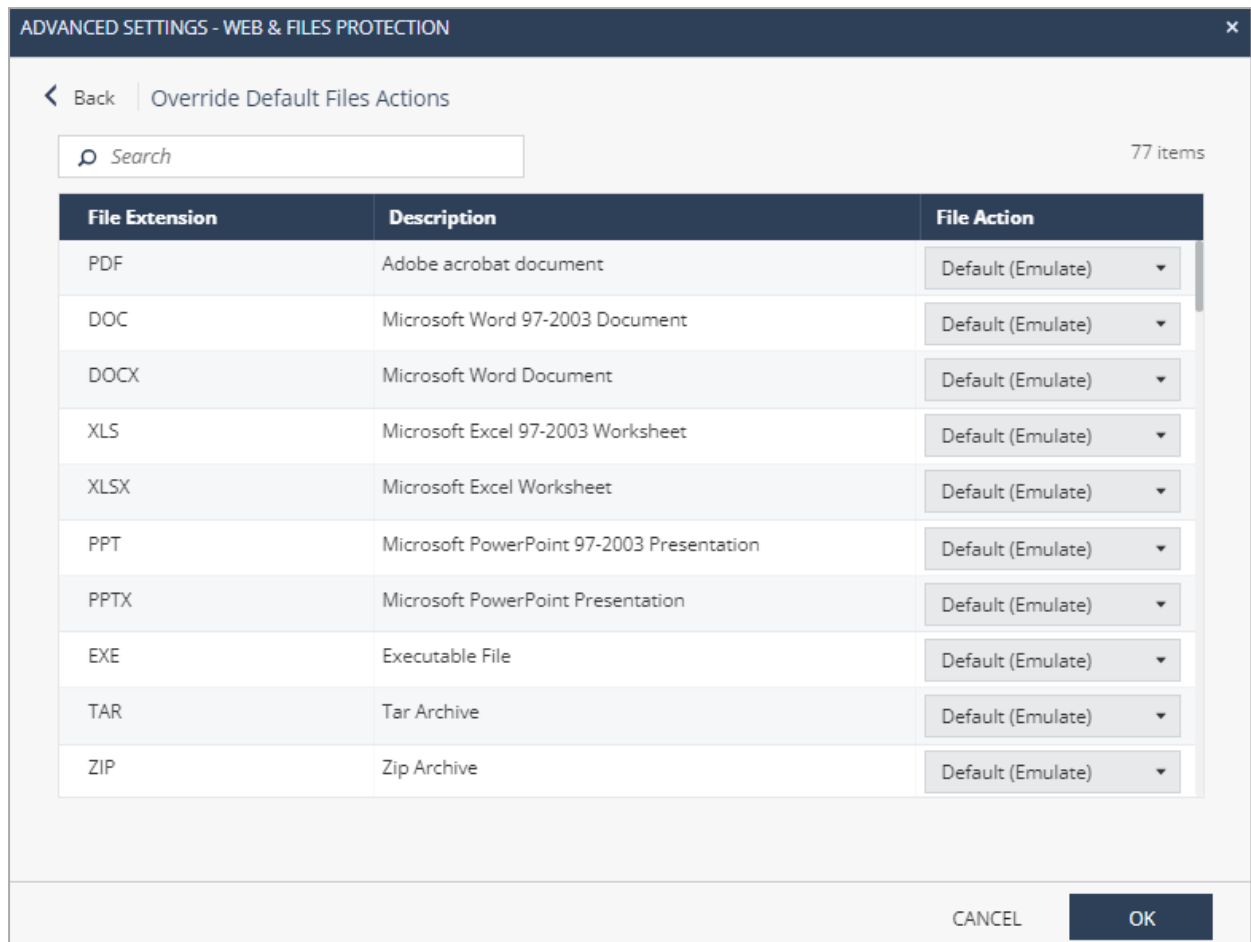
You can define the default file action for threat emulation.

To override the default file actions:

1. In the **Override Default Files Actions** section, click **Edit**.



2. From the **File action** list, select an action.



3. Click **OK**.

Advanced Capabilities

In the **Advanced Capabilities** window, select an action for these capabilities:

- **ThreatCloud Reputation**
- **Offline Reputation**
- **Vulnerable Driver Protection**

 **Note** - This feature is supported in Endpoint Security Client versions E88.50 and higher.

- **Static Analysis:**

- **Static Signatures**

 **Note** - This feature is supported in Endpoint Security Client version E89.00 and higher.

- **Office Files**

- Executables Files
- DDL Files

Browser Settings

Pin Extension

This feature enables the administrator to configure to allow users to pin or unpin the browser extension to the toolbar.

Notes -

- You can allow users to unpin the extension only on Chromium browsers, such as Chrome, Edge and Brave. You cannot unpin an extension in Firefox.
- Starting from the Endpoint Security client version E87.10, the extension is pinned to the browser by default for the users.

To allow users to unpin the browser extension, clear **Always pin the browser extension to the tool bar** under **Pin Extension**.

Control Browser Notifications

This feature allows administrators to control the following browser notifications:

- **Disable Zero-Phishing notifications** - Select the checkbox to disable the zero-phishing scan notification that appears when users try to enter in an input field.

 **Note** - Only the notification is disabled but the browser zero-phishing scan is performed in the background indicated by the yellow highlight around the input field.

- **Disable Download Emulation & Extraction notifications** - Select the checkbox to disable the download emulation and extraction notifications whenever a file is downloaded.

Incognito Mode

This feature allows administrators to control the availability of incognito mode for users. The default option is **Off**.

 **Note** - This feature is supported only for Endpoint Security client versions E88.60 and higher.

- **Off** - The feature does not control the availability of incognito mode.



Note - Users can access incognito mode depending on the organization policies.

- **Enable** - Forces incognito mode to be available for users, overriding any existing settings that might restrict its availability.
- **Disable** - Prevents users from accessing incognito mode by disabling it completely.

Behavioral Protection

Behavioral protection includes Anti-Bot, Behavioral Guard and Anti-Ransomware protections.

The Anti-Bot Component

There are two emerging trends in today's threat landscape:

- A profit-driven cybercrime industry that uses different tools to meet its goals. This industry includes cyber-criminals, malware operators, tool providers, coders, and affiliate programs. Their "products" can be easily ordered online from numerous sites (for example, do-it-yourself malware kits, spam sending, data theft, and denial of service attacks) and organizations are finding it difficult to fight off these attacks.
- Ideological and state driven attacks that target people or organizations to promote a political cause or carry out a cyber-warfare campaign.

Both trends are driven by bot attacks.

A bot is malicious software that can invade your computer. There are many infection methods. These include opening attachments that exploit a vulnerability and accessing a website that results in a malicious download.

When a bot infects a computer, it:

- Takes control over the computer and neutralizes its Anti-Virus defenses. Bots are difficult to detect because they hide within your computer and change the way they appear to the Anti-Virus software.
- Connects to a Command and Control (C&C) center for instructions from cyber criminals. The cyber criminals, or bot herders, can remotely control it and instruct it to execute illegal activities without your knowledge. These activities include:
 - Data theft (personal, financial, intellectual property, organizational)
 - Sending SPAM
 - Attacking resources (Denial of Service Attacks)
 - Bandwidth consumption that affects productivity

In many cases, a single bot can create multiple threats. Bots are often used as tools in attacks known as Advanced Persistent Threats (APTs) where cyber criminals pinpoint individuals or organizations for attack. A botnet is a collection of compromised computers.

The Check Point Anti-Bot component detects and prevents these bot threats

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.

The Endpoint Anti-Bot component uses these procedures to identify bot infected computers:

- Identify the C&C addresses used by criminals to control bots
- These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

Configuring Anti-Bot

There are three configuration options for the Anti-Bot protection:

- **Prevent** - Blocks bots.
- **Detect** - Logs information about bots, but does not block them.
- **Off** - Ignores bots (does not prevent or detect them)

Advanced Anti-Bot Settings:

- **Background Protection Mode:**
 - **Background** - This is the default mode. Connections are allowed while the bots are checked in the background.
 - **Hold** - Connections are blocked until the bot check is complete.
- **Hours to suppress logs for same bot protection** - To minimize the size of the Anti-Bot logs, actions for the same bot are only logged one time per hour. The default value is 1 hour. To change the default log interval , select a number of hours.
- **Days to remove bot reporting after** - If a bot does not connect to its command and control server after the selected number of days, the client stops reporting that it is infected. The default value is 3 days.
- **Confidence Level** - The confidence level is how sure Endpoint Security is that an activity is malicious. High confidence means that it is almost certain that the activity is malicious. Medium confidence means that it is very likely that the activity is malicious. You can manually change the settings for each confidence level. Select the action for High confidence, medium confidence and low confidence bots:

- **Prevent** - Blocks bots
- **Detect** - Logs information about bots, but does not block them.
- **Off** - Ignores bots (does not prevent or detect them).
- **DNS Inspection Mode** - DNS Inspection Mode is a security feature that monitors and inspects all websites your device attempts to access, ensuring protection against malicious or harmful sites. This feature is turned on by default, even before any Security Policies are applied to the device. Once you manually configure DNS Inspection Mode (turning it on or off), your settings will override the default settings from the management server. This ensures your device is protected immediately, allowing you to customize the settings later.

The Behavioral Guard & Anti-Ransomware Component

Behavioral Guard constantly monitors files and network activity for suspicious behavior.

 **Note** - Behavioral Guard also parses the email (through an add-in to Microsoft Outlook) to include the details in the forensics report in the event of a malicious attack through an email.

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

For E88.50 and later

Starting from version E88.50 and later, the Anti-Ransomware creates the honeypot files in these folders:

- Drive root (C:\ , D:\ , Etc)
- 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

For versions prior to E88.50

For versions prior to E88.50, 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

For E88.41 and later

Starting with version E88.41 and later, folders with restricted access are identified by a lock icon next to the folder name.

For example:

 eZH@IFF#tvcG31IX\$QytjrV

For versions prior to E88.41

For versions prior to E88.41, folders with restricted access are identified by a lock icon next to the folder name.

For example:

 Check-PointProtectionFiles!Do NotErase

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. After the attack is stopped, it deletes files involved in the attack and restores the original files from the backup location.

- **Prevent** - The attack is remediated. Logs, alerts and a forensic report are created.
- **Detect** - Logs, alerts and a forensic report are created.
- **Off** - Nothing is done on the detection, a log is not created

Advanced Behavioral Guard & Anti-Ransomware Settings

- **Enable network share protection** - Enables the protection of shared folders on the network. All shared folders are protected, regardless of the protocol. Remote devices are not protected.
- **Block Volume Encryption tools (BitLocker and Similar Tools)**: As many ransomwares use volume encryption software, such as BitLocker to encrypt drives.

 **Note** - This feature is supported with the Endpoint Security Client version E86.30 with the default client mode as **Detect**. With the Endpoint Security Client version E86.50 and higher, the default client mode is **Prevent**.

You can block such programs from:

- Encrypting unencrypted drives
- Modifying the encryption of encrypted drives (such as changing password)

If you want to encrypt your drive with BitLocker or a similar software:

- Encrypt the drive before you install the Endpoint Security Client, or
- Disable this protection, encrypt and resume this protection

- **Allow extensive data collection**: Allow Endpoint Security to collect extended information from endpoints.

 **Note** - This may increase the resources used.

■ **Low memory mode:**

This setting reduces memory usage by loading a carefully selected subset of threat signatures, optimized for protection effectiveness and minimal memory footprint. While this can help improve performance on devices with limited memory, it may slightly reduce detection coverage in some scenarios.

Check Point recommends to enable this mode only on systems with low memory capacity, where resource constraints justify the trade-off.

 **Note** - The **Low memory mode** setting is supported starting with Endpoint Security Client version E87.30 and above.

Backup Settings

When Anti-Ransomware is enabled, it constantly monitors files and processes for unusual activity. Before a ransomware attack can encrypt files, Anti-Ransomware backs up your files to a safe location. After the attack is stopped, it deletes files involved in the attack and restores the original files from the backup location.

- **Restore to selected location** - By default, files are restored to their original location. To restore files to a different location, select this option and enter the location to which you want to restore the files in the Choose location field. Each time files are automatically restored, they will be put in the selected location.
- **Anti-Ransomware maximum backup size on disk** - Set the maximum amount of storage for Anti-Ransomware backups. The default value is 1 GB.
- **Backup time interval** - Within this time interval, each file is only backed up one time, even if it is changed multiple times. The default value is 60 minutes.
- **Backup Settings - Change default types to be backed up** - Click this to see a list of file types that are included in the Anti-Ransomware backup files. You can add or remove file types from the list and change the Maximum Size of files that are backed up.

 Notes:

- By default, the maximum file size for back up is 25 MB. To change the maximum file size, edit the **Maximum Size (MB)**.
 - For information on the Endpoint Security folder, see [sk147454](#).
- **Disk Usage** - By default, Forensics uses up to 1 GB of disk space on the client computer for data.

The Anti-Exploit Component

Endpoint Security Anti-Exploit detects zero-day and unknown attacks, and provides protection to vulnerable processes from exploitation. Files on your computer are sent to a testing area for emulation to detect malicious files and content.

There are three configuration options for the Anti-Exploit protection:

- **Prevent** - Prevents the attack and suspends the application under attack.
- **Detect** - Detects and logs the attack information. Does not prevent the attack.
- **Off** - The Anti-Exploit protection is disabled.

Analysis & Remediation

Automated Attack Analysis (Forensics)

Endpoint Security Forensics analyzes attacks detected by other detection features like Anti-Ransomware or Behavioral Guard, 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 presented as a Forensics Analysis Report. If Endpoint Security Management 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.

Protection mode - Define in which confidence level the incident is analyzed: **Always**, **High**, **Medium & High**, or **Never**. The confidence level is how sure Endpoint Security is that a file is malicious. High confidence means that it is almost certain that a file is malicious. Medium confidence means that it is very likely that a file is malicious. The default value is **Always**.

Enable Threat Hunting - Threat Hunting is enabled by default. To learn more about Threat Hunting, see ["Threat Hunting" on page 647](#).

Remediation & Response

The Endpoint Security File Remediation component applies Remediation to malicious files. When Endpoint Security components detect malicious files, they can quarantine those files automatically based on policy, and remediate them if necessary.

You can manually define the confidence level in which Remediation is performed: **Always**, **High**, **Medium & High**, or **Never**. The confidence level is how sure Endpoint Security is that a file is malicious. High confidence means that it is almost certain that a file is malicious. Medium confidence means that it is very likely that a file is malicious. The default value is **Medium & High**.

Advanced Remediation & Response Settings

File Quarantine

Define the settings for files that are quarantined. By default, items are kept in quarantine for 90 days and users can delete items from quarantine.

- **File quarantine** - Select the confidence level in which Remediation is performed: **Always**, **High**, **Medium & High**, **Never**. The default value is **Medium & High**.
- **Allow users to delete items from quarantine** - When selected, users can permanently delete items from the quarantine file on their computers.

- **Allow users to restore items from quarantine** - When selected, users can restore items from the quarantine file on their computers.
- **Copy quarantine files to central location** - Enter a central location to which the quarantined files from the client computers are copied.

File Remediation

Define what happens to the components of an attack that is detected by Forensics. When files are quarantined, they are deleted and put in a secure location from which they can be restored, if necessary.

You can manually edit the treatment for each category of file: **Malicious**, **Suspicious**, or **Unknown**. For each category, you can select:

- **Quarantine** - Files are deleted and put in a secure location from which they can be restored, if necessary.
- **Delete** - Files are permanently deleted.
- **Backup** -- Delete the file and create an accessible duplicate.
- **None** -- No action is taken.

Trusted files are those defined as trusted by the Check Point Reputation Service. The Remediation options for Trusted Files are:

- **Terminate** - stop the suspicious process.
- **Ignore** - Do not terminate processes. Activity is monitored.

Adding Exclusions to Rules



You can use either [Legacy Exclusions](#) and [Smart Exclusions](#) to add your exclusions. However, we recommend that you use [Smart Exclusions](#) for the easy of managing exclusions.

Note - [Smart Exclusions](#) is supported only with Endpoint Security Client version E87.40 and higher.

Legacy Exclusions

You can exclude specific objects (exclusions) from inspection by Endpoint Security. You can add exclusions to a rule or create global exclusions that apply to all rules.

Adding Exclusions to a Specific Rule

To add exclusions to a specific rule:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the rule for which you want to create the exclusion
3. In the **Capabilities & Exclusions** pane, click **Exclusions Center**.
4. Expand an exclusion category. For example, **Anti-Bot -> URL Filtering Exclusions**.

Note - Global Exclusions is read-only. To add **Global Exclusions**, see ["Adding Global Exclusions" below](#).

5. Expand **Rule Exclusions**.
6. Select the exclusions you want to add to the rule.
7. Click **OK**.
8. In the bottom right corner of the policy configuration pane, click **Save**.
9. From the top, click **Install Policy**.

Adding Global Exclusions

To add global exclusions that apply to all the rules:

1. Go to **Policy > Threat Prevention > Global Exclusions**.
2. Expand an exclusion category. For example, **Anti-Bot -> URL Filtering Exclusions**.
3. Select the exclusions you want to add to the rule.
4. Click **Save**.
5. From the top, click **Install Policy**.

Adding Exclusions from Security Overview

To add exclusions from Security Overview:

1. Go to **Overview > Security Overview**.
2. Right-click the security event and select **Drill Down**.

3. Right-click the event and select one of these options:

- **Create Exclusion for Effective Rule**

The **Edit Exclusions Center** window appears and automatically adds the exclusion.

- **Create Exclusion for All Rules**

- If **Global Exclusions** is not enabled, the **Edit Exclusions Center** window opens and automatically adds the exclusion to all the rules under **Policy Capabilities**.
- If **Global Exclusions** is enabled, the **Edit Exclusions Center** window opens and automatically adds the exclusion to **Global Exclusions**. For more information, see ["Adding Global Exclusions" on the previous page](#).

4. Click **OK**.

5. Click **Save** for all the modified policies.

6. Click **Install Policy**.

Notes:

- You cannot add exclusions for Forensic events triggered by Anti-Bot.
- You cannot add exclusions for Forensic events triggered by Anti-Malware engine that has no reference event.
- This procedure is not supported for macOS endpoints.

Adding Exclusions from Logs

To add exclusions from the Logs menu:

1. Go to **Logs** menu.
2. Right-click a log to add and configure an exclusion to your endpoint device. This redirects you to the appropriate rule, section, and capability.
3. Select one of these options to apply the exclusions:
 - **Effective option:** For a specific device or a user rule.
 - **All options:** For a specific rule.

Notes:

- This option is available only for Endpoint Security client version E86.20 and later.
- For Endpoint Security client version 86.20 or earlier, or for unsupported blades/capabilities, you are redirected to the relevant rule in the exclusions center to create exclusions.

Adding a New Exclusion to an Exclusion Category

To add an exclusion to an exclusions category:

1. Do one of these:

- Go to **Policy > Threat Prevention > Policy Capabilities**.
- Go to **Policy > Threat Prevention > Global Exclusions**.

The **Edit Exclusions Center** window appears.

2. Click .

The **New Exclusion** window appears.

3. Specify these details:

- a. **Exclusion**
- b. **Method**
- c. **Value**
- d. (Optional) **Comment**
- e. To add the exclusion to all the rules, select the **Add to all rules** checkbox. This step does not apply to **Global Exclusions**.

Note - If the current rule contains this exception, then the system adds a duplicate exclusion.

4. Click **OK**.

5. In the bottom right corner of the policy configuration pane, click **Save**.

6. From the top, click **Install Policy**.

Editing an Exclusion

To edit an exclusion:

1. Do one of these:

- Go to **Policy > Threat Prevention > Policy Capabilities**.
- Go to **Policy > Threat Prevention > Global Exclusions**.

The **Edit Exclusions Center** window opens.

2. Expand an exclusion category. For example, **Anti-Bot -> URL Filtering Exclusions**.
3. If you are editing a local exclusion, expand **Local Exclusions**. This step does not apply to **Global Exclusions**.
4. Select the exclusion you want to edit.
5. Click  .

The **Edit Exclusion** window appears.

6. Specify these details:
 - a. **Exclusion**
 - b. **Method**
 - c. **Value**
 - d. (Optional) **Comment**
 - e. To apply the changes to all the rules that contain this exclusion, select the **Update all rules** checkbox. This step does not apply to **Global Exclusions**.
 - f. To add the exclusion to all the rules that does not contain this exclusion, select the **Add to all rules** checkbox. This step does not apply to **Global Exclusions**.
7. Click **OK**.
8. In the bottom right corner of the policy configuration pane, click **Save**.
9. From the top, click **Install Policy**.

Below is the list of supported 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

Anti Bot -> URL Filtering Exclusions

You can exclude specific domains from a rule. Click **+** to add the required domain you want to exclude from the rule.

Syntax

- * indicates a string or a character. For example, A* can be ADomain or AB or AAAA.
- ? indicates a character. For example, A? can be AA or AB or Ab.

For example:

If you enter	It excludes these	It does not exclude these
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
*.domain.com	Sub-domain of domain.com such as: ▪ https://sub1.domain.com ▪ http://sub2.domain.com	

Anti-Malware -> Process Exclusions (on-access only)

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

When you exclude a trusted process from inspection, its 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:

- Its behaviour is abnormal.
- Its 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

Anti-Malware -> Files and Folders Exclusion (system, scheduled and on-demand)

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_address\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 Endpoint Security 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 Endpoint Security 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

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

i 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 Endpoint Security 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, https or any other special characters except asterisk (*).

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	It excludes these	It does not exclude these
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

If you enter	It excludes these	It does not exclude these
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
*.domain.com	Sub-domain of domain.com such as: ■ https://sub1.domain.com ■ http://sub2.domain.com	

SHA1 exclusions -

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

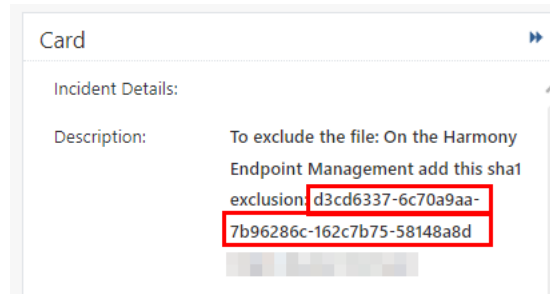
For Endpoint Security version E86.40, SHA1 exclusion is supported on Endpoint Security extension for browsers as well (not including Internet Explorer). SHA1 can be used to exclude downloaded files from [File Protection](#) and local HTML files from *"Zero Phishing" on page 271*.

- It is not supported with Internet Explorer.
- File Reputation exclusions are set by SHA1.
- Macro exclusion - To exclude the office files which includes a macro, set exclusions for the SHA1 hash of the macro.

For example, if an exclusion is set to SHA1 hash of the macro, all the files which includes this macro are excluded.

Notes -

- This is supported with Endpoint Security Client version E88.00 or higher.
- To view the hash of a macro, see the **Description** in the **Forensic Details** section in the **Card** of the event. For more information see, [Adding Exclusions from Logs](#).



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.
- For Endpoint Security Client version E87.10 or higher, if the value of exclusion start with `FileEx:\\` then the value will be treated as path to the file.

To exclude specific type of files in a folder, use the following format:

`FileEx:\\<Path_to_directory>\*.<file_extension>.`

For example, `FileEx:\\D:\mydir\*.xls` will exclude all XLS files in D:\mydir folder.

- 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\\.`

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

Forensics -> Anti-Ransomware and Behavioral Guard

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 the process name or full path to the process
- Exclusion can contain environment variables
- Wildcards are supported.

Note - This is supported with Endpoint Security client version E86.70 and higher.

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.

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

Example	Supported/Unsupported	Description
<code>C:\Program Files\MyTrustedDirectory*</code>	Not supported	Excludes all the processes under MyTrustedDirectory
<code>C:\Program Files\MyTrustedDirectory\excludeMe.exe</code>	Supported	Excludes the <code>excludeMe.exe</code> under MyTrustedDirectory

Example	Supported/Unsupported	Description
<i>excludeMe.exe</i>	Supported	Process can be excluded by name only. Note - Supported but recommended to be used together with Certificate and/or MD5.
<i>%ProgramFiles%\MyTrustedDirectory\excludeMe.exe</i>	Supported	Full path can contain environment variables. Note - Supports only for System Environment Variables (not user Environment Variables).
<i>C:*process.exe</i>	Not supported	Full path cannot contain wildcards.

Forensics -> 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.

Smart Exclusions

Smart Exclusions allows you to add exclusions to one or more capabilities and types easily, whereas the Legacy Exclusions allows you to add exclusion only for one capability at a time.

With Smart Exclusions, you can:

- Set exclusions to all capabilities and operating systems at once.
- Use standard syntax across all exclusion types.
- Use wider range of wildcard characters for nuanced and customized exclusion patterns.
- Easily enable or disable exclusions with a simple toggle button without the need to delete exclusions temporarily.

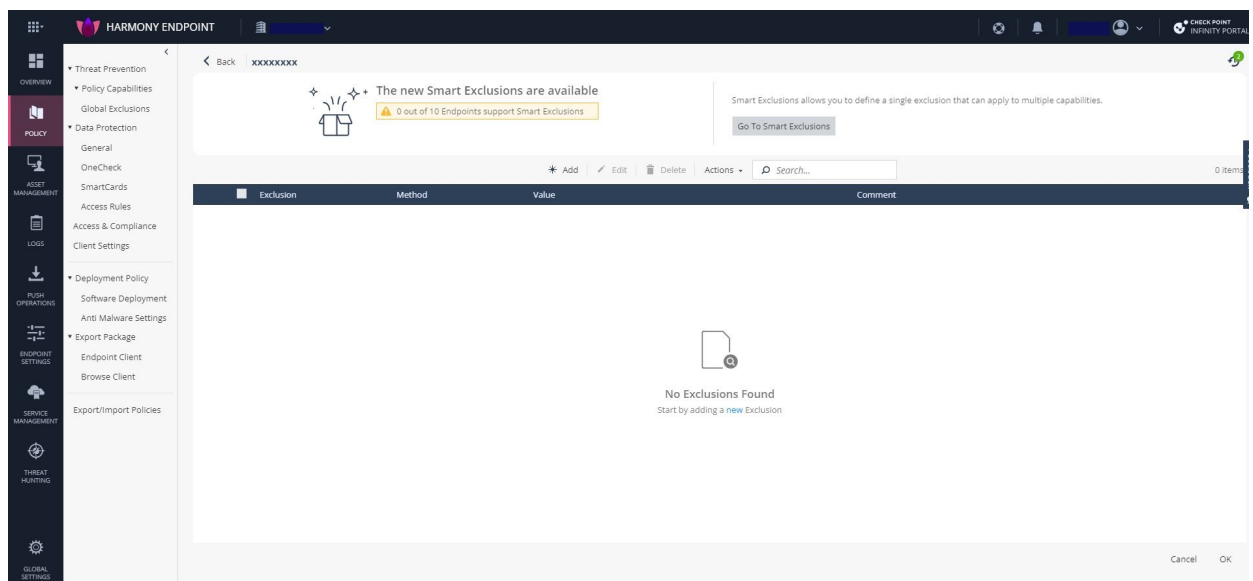
Note - Smart Exclusions is supported only with Endpoint Security Client version E87.52 and higher for Windows and E87.50 and higher for macOS.

Adding Exclusions to a Specific Rule

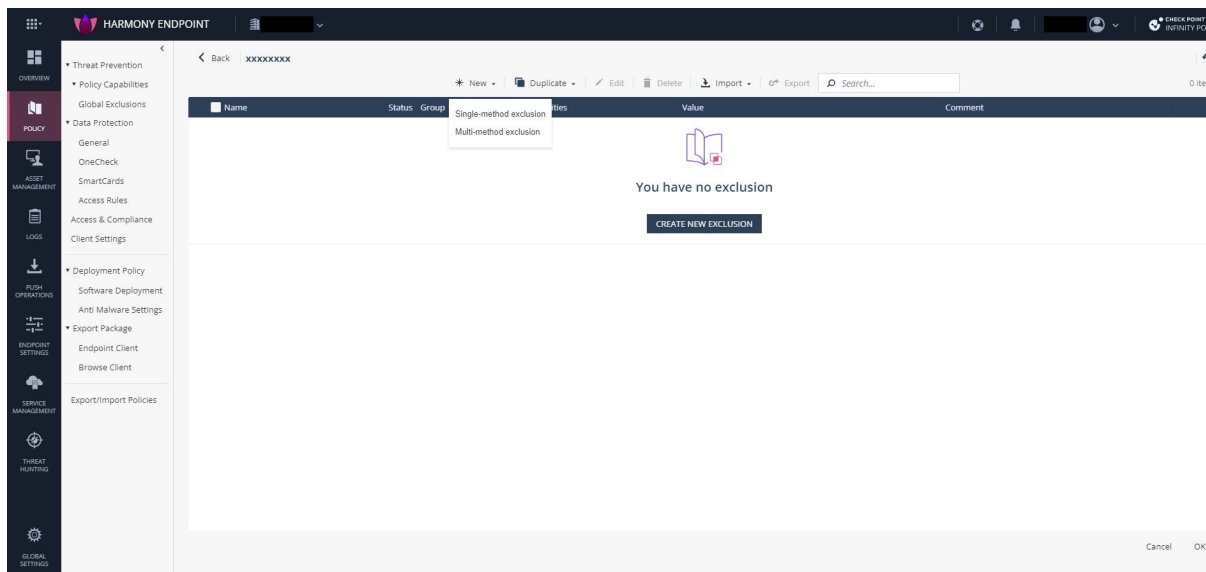


To add a new exclusion to a specific rule:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the rule for which you want to create the exclusion.
3. In the **Capabilities & Exclusions** pane, click **Exclusions Center**.
4. Click **Go to Smart Exclusions**.

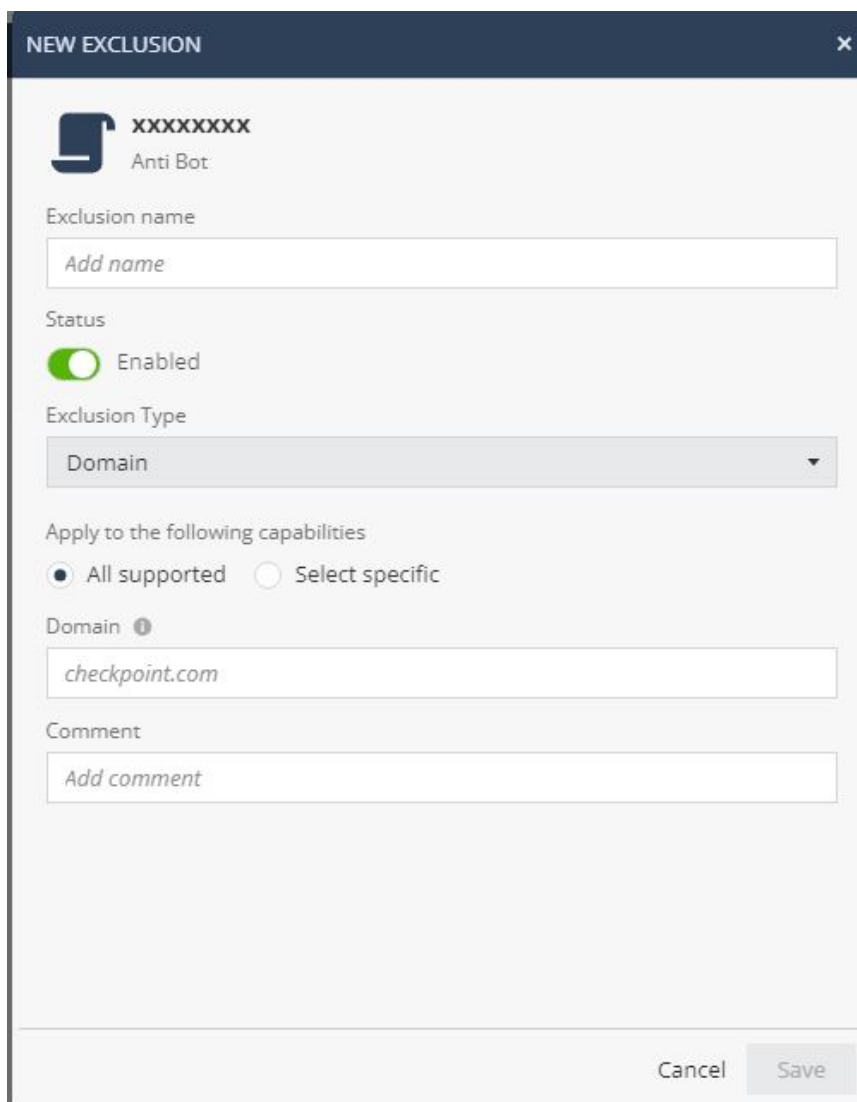


5. Click  or click **Create New Exclusion**.
6. To add an exclusion for only one exclusion type:



- a. Click **Single-method exclusion**.

A wizard appears.



The screenshot shows a 'NEW EXCLUSION' dialog box with a dark blue header and a close button (X) in the top right corner. The main content area is light gray and contains the following fields and controls:

- Logo and Name:** A logo with the text 'XXXXXXXX' and 'Anti Bot' below it.
- Exclusion name:** A text input field with the placeholder text 'Add name'.
- Status:** A green toggle switch labeled 'Enabled'.
- Exclusion Type:** A dropdown menu currently showing 'Domain'.
- Apply to the following capabilities:** Two radio buttons: 'All supported' (selected) and 'Select specific'.
- Domain:** A text input field with the placeholder text 'checkpoint.com'.
- Comment:** A text input field with the placeholder text 'Add comment'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

- b. In the **Exclusion name** field, enter a name for exclusion.
- c. To enable the exclusion, toggle **Status** to **Enabled**.
- d. From the **Exclusion Type** list, select the exclusion type.

- e. From the **Operating system** list, select the operating system to which you want to apply the exclusion. For example, endpoints running Windows operating system only. It is not available if you select **All supported** in the **Apply to the following capabilities** section.



Caution - If you make exclusions in the **Forensics Monitoring** capability, the activities of the excluded processes are omitted from forensic analysis. As a result, you cannot query for these activities in **Threat Hunting** and they are excluded from Horizon XDR/XPR analysis, detections, and the creation of security incidents related to sophisticated attacks.

f. In the **Apply to the following capabilities** section:

- To apply the exclusion to all capabilities, select **All supported**.
- To apply the capabilities to specific capabilities, select **Select specific** and from the **Capabilities** list, select the capabilities.

 Notes:

- Capabilities not relevant to the selected group are not available.
- For supported syntax and capabilities for exclusion types, see [sk181679](#).

If the Exclusion Type is	Then
Process path	a. In the Process path field, enter the path of the process. For example, C:\windows\system\cmd.exe. b. To specify additional criteria, expand Process path options, and select: ■ Case sensitive ■ Trusted process ■ Argument and if required, select Regex, and in the Argument value field, enter the value.
Process hash	a. From the Process hash type list, select the hash type: ■ MD5 ■ SHA1 ■ SHA2 ■ cdhash (for macOS only) b. In the Process hash value, enter the value.
Process signer	In the Process signer value field, enter the process signer value. For example, Check Point Ltd.
File path	a. In the File path field, enter the path of the file. For example, C:\windows\system\. b. To specify additional criteria, expand File path options, and select Case sensitive.

If the Exclusion Type is	Then
File hash	a. From the File hash type list, select the hash type: ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) b. In the File hash value, enter the value.
File signer	In the File signer value field, enter the process signer value. For example, Check Point Ltd.
IP Range	In the IP Range fields, enter the IP address range. For example, to enter IPv4 range, enter 192.168.1.30-192.168.1.198. For example, to enter IPv6 range, enter 2001::1-2001::254.
Url	In the URL field, enter the URL.
Domain	In the Domain field, enter the domain. For example, checkpoint.com.
Infection	In the Infection/Protection field, enter the infection (for example, not-a-virus:Adware.Win32.BroAssist.a) or a protection (for example, Gen.Exploiter.ROP).

g. (Optional) In the **Comment** field, enter comments.

h. Click **Save**.

7. To add exclusions for multiple types of exclusions:

- a. Click **Multi-method exclusion**.

A wizard appears.

NEW EXCLUSION

1 EXCLUSION PROPERTIES

2 METHOD SELECTION

XXXXXXXXXX
Anti Bot

Exclusion name
Add name

Status
☒ Enabled

Exclusion group
Web Asset

Operating system
All

Apply to the following capabilities
☒ All supported ☐ Select specific

Comment
Add comment

NEXT

- b. In the **Exclusion name** field, enter a name for exclusion.
- c. To enable the exclusion, toggle **Status** to **Enabled**.
- d. From the **Exclusion Group** list, select the exclusion type.
- e. From the **Operating system** list, select the operating system to which you want to apply the exclusion. For example, endpoints running Windows operating system only. It is not available if you select **All supported** in the **Apply to the following capabilities** section.

Caution - If you make exclusions in the **Forensics Monitoring** capability, the activities of the excluded processes are omitted from forensic analysis. As a result, you cannot query for these activities in **Threat Hunting** and they are excluded from Horizon XDR/XPR analysis, detections, and the creation of security incidents related to sophisticated attacks.

f. In the **Apply to the following capabilities** section:

- To apply the exclusion to all capabilities, select **All supported**.
- To apply the capabilities to specific capabilities, select **Select specific** and from the **Capabilities** list, select the capabilities. *"To enable Chained Exclusions, in the Chained Exclusion are available for section, turn on the Inherit exclusion to child processes button. It automatically excludes all the child processes of the excluded process." on the next page*

 Notes:

- Capabilities not relevant to the selected group are not available.
- Anti-Exploit capability supports only **Process path** and **Infection/Protection** exclusions.

- g. To enable **Chained Exclusions**, in the **Chained Exclusion are available for** section, turn on the **Inherit exclusion to child processes** button. It automatically excludes all the child processes of the excluded process.

Notes:

- Chained exclusion is supported only with the **Exclusion group** of the type **System** and to these specific exclusions:
 - Process path
 - Process original name
 - Process hash
 - Process signer
- For Endpoint Security Client version E88.40 and lower, it is mandatory to provide either `Process path` or the `Process signer` parameter. All the other parameters are optional.
- With the Endpoint Security Client version E88 and higher, it supports only the **Forensics Monitoring** capability.
- With the Endpoint Security Client version E88.20 and higher, it additionally supports **Threat Emulation**, **Anti-Bot**, **Anti-Malware** (DHS compliant), **SSLi** and **URL Filtering** capabilities.

- h. (Optional) In the **Comment** field, enter comments.

- i. Click **Next**.



Note - For supported syntax and capabilities for exclusion types, see [sk181679](#).

If the Exclusion Group is	Exclusion Type	Then
System	Process path	- In the Process path field, enter the path of the process. For example, C:\windows\system\cmd.exe. - To specify additional criteria, expand Process path options, and select: ▪ Case sensitive ▪ Trusted process ▪ Argument and if required, select Regex, and in the Argument value field, enter the value.
	Process original name ¹	Enter the process original name. For example, Cmd.exe. Supported only for Windows-based endpoints.  Notes - ▪ To find the original name of the process: - Right-click on the executable file. - Go to Properties > Details > Original filename. ▪ Process original name is case-sensitive.
	Process hash	- From the Process hash type list, select the hash type: ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) - In the Process hash value, enter the value.
	Process signer ¹	In the Process signer value field, enter the process signer value. For example, Check Point Ltd.

If the Exclusion Group is	Exclusion Type	Then
	File path	a. In the File path field, enter the path of the file. For example, C:\windows\system\. b. To specify additional criteria, expand File path options, and select Case sensitive.
	File hash	a. From the File hash type list, select the hash type: ■ MD5 ■ SHA1 ■ SHA2 ■ cdhash (for macOS only) b. In the File hash value, enter the value.
	File signer	In the File signer value field, enter the process signer value. For example, Check Point Ltd.
Web Asset	IP Range	In the IP Range fields, enter the IP address range. For example, to enter IPv4 range, enter 192.168.1.30-192.168.1.198. For example, to enter IPv6 range, enter 2001::1-2001::254.
	Url	In the URL field, enter the URL.
	Domain	In the Domain field, enter the domain. For example, checkpoint.com.
Infection/Detection	Infection	In the Infection/Protection field, enter the infection (for example, not-a-virus:Adware.Win32.BroAssist.a) or a protection (for example, Gen.Exploiter.ROP).

¹ It is mandatory to provide either `Process original name` or the `Process signer` parameter. All the other parameters are optional.

j. Click **Finish**.

8. Click **OK**.

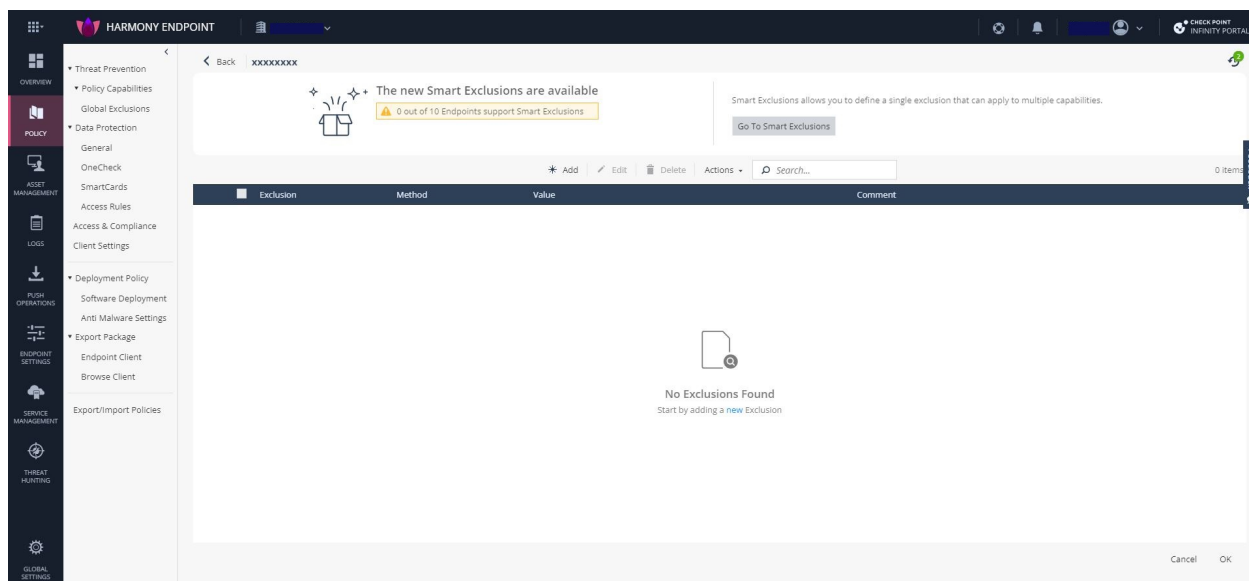
9. Click **Save & Install**.

 **Note** - You can change **Single-method exclusion** to **Multi-method exclusion**. See [Managing Exclusions](#).

Adding Global Exclusions

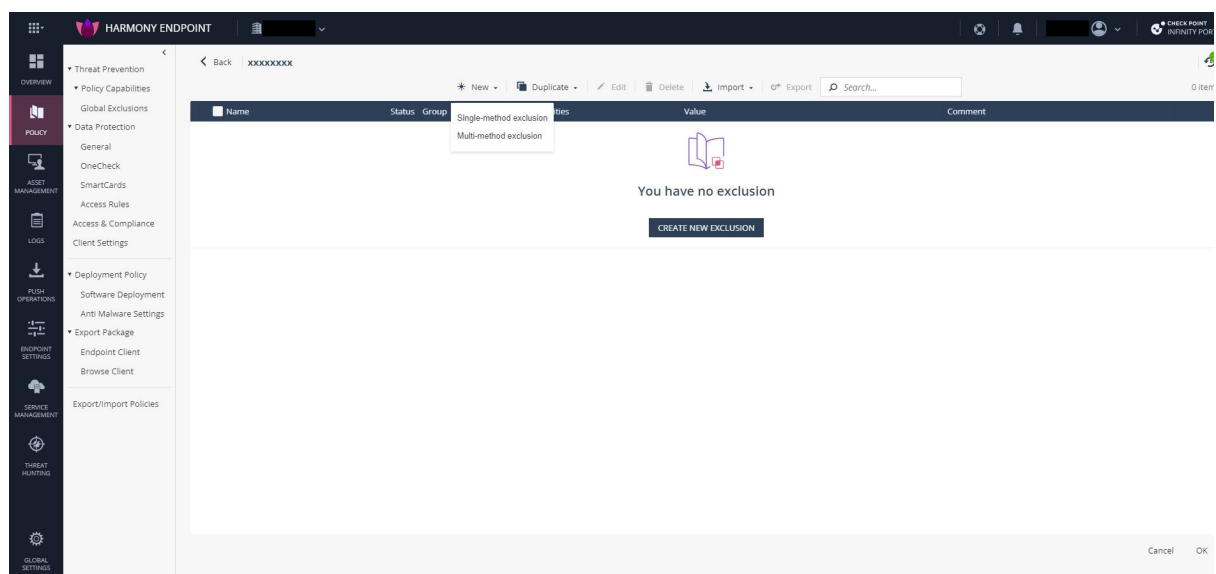
To add global exclusions that apply to all the rules:

1. Go to **Policy > Threat Prevention > Global Exclusions**.
2. Click **Go to Smart Exclusions**.



3. Click  or click **Create New Exclusion**.

4. To add an exclusion for only one exclusion type:



- a. Click **Single-method exclusion**.

A wizard appears.

The screenshot shows a 'NEW EXCLUSION' dialog box with a dark blue header bar containing a close button (X). The main area is light gray and contains the following fields and controls:

- Logo and Name:** A logo with the text 'XXXXXXXXX' and 'Anti Bot' below it.
- Exclusion name:** A text input field with the placeholder text 'Add name'.
- Status:** A green toggle switch labeled 'Enabled'.
- Exclusion Type:** A dropdown menu currently showing 'Domain'.
- Apply to the following capabilities:** Two radio buttons: 'All supported' (selected) and 'Select specific'.
- Domain:** A text input field with the placeholder text 'checkpoint.com'.
- Comment:** A text input field with the placeholder text 'Add comment'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

- b. In the **Exclusion name** field, enter a name for exclusion.
- c. To enable the exclusion, toggle **Status** to **Enabled**.
- d. From the **Exclusion Type** list, select the exclusion type.

- e. From the **Operating system** list, select the operating system to which you want to apply the exclusion. For example, endpoints running Windows operating system only. It is not available if you select **All supported** in the **Apply to the following capabilities** section.



Caution - If you make exclusions in the **Forensics Monitoring** capability, the activities of the excluded processes are omitted from forensic analysis. As a result, you cannot query for these activities in **Threat Hunting** and they are excluded from Horizon XDR/XPR analysis, detections, and the creation of security incidents related to sophisticated attacks.

f. In the **Apply to the following capabilities** section:

- To apply the exclusion to all capabilities, select **All supported**.
- To apply the capabilities to specific capabilities, select **Select specific** and from the **Capabilities** list, select the capabilities.

 Notes:

- Capabilities not relevant to the selected group are not available.
- For supported syntax and capabilities for exclusion types, see [sk181679](#).

If the Exclusion Type is	Then
Process path	a. In the Process path field, enter the path of the process. For example, C:\windows\system\cmd.exe. b. To specify additional criteria, expand Process path options, and select: ■ Case sensitive ■ Trusted process ■ Argument and if required, select Regex, and in the Argument value field, enter the value.
Process hash	a. From the Process hash type list, select the hash type: ■ MD5 ■ SHA1 ■ SHA2 ■ cdhash (for macOS only) b. In the Process hash value, enter the value.
Process signer	In the Process signer value field, enter the process signer value. For example, Check Point Ltd.
File path	a. In the File path field, enter the path of the file. For example, C:\windows\system\. b. To specify additional criteria, expand File path options, and select Case sensitive.

If the Exclusion Type is	Then
File hash	a. From the File hash type list, select the hash type: ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) b. In the File hash value, enter the value.
File signer	In the File signer value field, enter the process signer value. For example, Check Point Ltd.
IP Range	In the IP Range fields, enter the IP address range. For example, to enter IPv4 range, enter 192.168.1.30-192.168.1.198. For example, to enter IPv6 range, enter 2001::1-2001::254.
Url	In the URL field, enter the URL.
Domain	In the Domain field, enter the domain. For example, checkpoint.com.
Infection	In the Infection/Protection field, enter the infection (for example, not-a-virus:Adware.Win32.BroAssist.a) or a protection (for example, Gen.Exploiter.ROP).

g. (Optional) In the **Comment** field, enter comments.

h. Click **Save**.

5. To add exclusions for multiple types of exclusions:

- a. Click **Multi-method exclusion**.

A wizard appears.

NEW EXCLUSION

1 EXCLUSION PROPERTIES

2 METHOD SELECTION

XXXXXXXXXX
Anti Bot

Exclusion name
Add name

Status
☒ Enabled

Exclusion group
Web Asset

Operating system
All

Apply to the following capabilities
☒ All supported ☐ Select specific

Comment
Add comment

NEXT

- b. In the **Exclusion name** field, enter a name for exclusion.
- c. To enable the exclusion, toggle **Status** to **Enabled**.
- d. From the **Exclusion Group** list, select the exclusion type.
- e. From the **Operating system** list, select the operating system to which you want to apply the exclusion. For example, endpoints running Windows operating system only. It is not available if you select **All supported** in the **Apply to the following capabilities** section.

Caution - If you make exclusions in the **Forensics Monitoring** capability, the activities of the excluded processes are omitted from forensic analysis. As a result, you cannot query for these activities in **Threat Hunting** and they are excluded from Horizon XDR/XPR analysis, detections, and the creation of security incidents related to sophisticated attacks.

f. In the **Apply to the following capabilities** section:

- To apply the exclusion to all capabilities, select **All supported**.
- To apply the capabilities to specific capabilities, select **Select specific** and from the **Capabilities** list, select the capabilities. *"To enable Chained Exclusions, in the Chained Exclusion are available for section, turn on the Inherit exclusion to child processes button. It automatically excludes all the child processes of the excluded process." on page 318*

 Notes:

- Capabilities not relevant to the selected group are not available.
- Anti-Exploit capability supports only **Process path** and **Infection/Protection** exclusions.

- g. To enable **Chained Exclusions**, in the **Chained Exclusion are available for** section, turn on the **Inherit exclusion to child processes** button. It automatically excludes all the child processes of the excluded process.

Notes:

- Chained exclusion is supported only with the **Exclusion group** of the type **System** and to these specific exclusions:
 - Process path
 - Process original name
 - Process hash
 - Process signer
- For Endpoint Security Client version E88.40 and lower, it is mandatory to provide either `Process path` or the `Process signer` parameter. All the other parameters are optional.
- With the Endpoint Security Client version E88 and higher, it supports only the **Forensics Monitoring** capability.
- With the Endpoint Security Client version E88.20 and higher, it additionally supports **Threat Emulation**, **Anti-Bot**, **Anti-Malware** (DHS compliant), **SSLI** and **URL Filtering** capabilities.

- h. (Optional) In the **Comment** field, enter comments.

- i. Click **Next**.



Note - For supported syntax and capabilities for exclusion types, see [sk181679](#).

If the Exclusion Group is	Exclusion Type	Then
System	Process path	- In the Process path field, enter the path of the process. For example, C:\windows\system\cmd.exe. - To specify additional criteria, expand Process path options, and select: ▪ Case sensitive ▪ Trusted process ▪ Argument and if required, select Regex, and in the Argument value field, enter the value.
	Process original name ¹	Enter the process original name. For example, Cmd.exe. Supported only for Windows-based endpoints.  Notes - ▪ To find the original name of the process: - Right-click on the executable file. - Go to Properties > Details > Original filename. ▪ Process original name is case-sensitive.
	Process hash	- From the Process hash type list, select the hash type: ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) - In the Process hash value, enter the value.
	Process signer ¹	In the Process signer value field, enter the process signer value. For example, Check Point Ltd.

If the Exclusion Group is	Exclusion Type	Then
	File path	a. In the File path field, enter the path of the file. For example, C:\windows\system\. b. To specify additional criteria, expand File path options, and select Case sensitive.
	File hash	a. From the File hash type list, select the hash type: ■ MD5 ■ SHA1 ■ SHA2 ■ cdhash (for macOS only) b. In the File hash value, enter the value.
	File signer	In the File signer value field, enter the process signer value. For example, Check Point Ltd.
Web Asset	IP Range	In the IP Range fields, enter the IP address range. For example, to enter IPv4 range, enter 192.168.1.30-192.168.1.198. For example, to enter IPv6 range, enter 2001::1-2001::254.
	Url	In the URL field, enter the URL.
	Domain	In the Domain field, enter the domain. For example, checkpoint.com.
Infection/Detection	Infection	In the Infection/Protection field, enter the infection (for example, not-a-virus:Adware.Win32.BroAssist.a) or a protection (for example, Gen.Exploiter.ROP).

¹ It is mandatory to provide either `Process original name` or the `Process signer` parameter. All the other parameters are optional.

j. Click **Finish**.

6. Click **Save**.

The exclusions are automatically enforced on the client without installing the policy.

 **Note** - You can change **Single-method exclusion** to **Multi-method exclusion**. See [Managing Exclusions](#).

Migrating Legacy Exclusions

 **Best Practice** - Check Point recommends to follow these steps before migrating to **Smart Exclusions**:

1. Go to **Policy > Threat Prevention > Policy Capabilities**
2. Pick a rule to test the migration and clone the rule.
3. Place the newly created rule at the top.
4. Under **Applied To**, select a test group.
5. Click **Exclusion Center** for the newly created rule and export the legacy exclusions for backup purposes.
6. For the newly created rule, migrate to Smart Exclusions. See *["To migrate legacy exclusions to smart exclusions:" below](#)*.
7. Click **Save and Install**.
8. Go to **Logs** and filter the logs for the computer in the test group. Verify that there are no false positives and all the detections are excluded correctly. If there are issues, contact [Check Point Support](#).
9. Perform the steps 1 through 8 for each rule at a time.
10. Repeat the process for **Global Exclusions**.

To migrate legacy exclusions to smart exclusions:

1. To migrate legacy exclusions for a rule:
 - a. Go to **Policy > Threat Prevention > Policy Capabilities**.
 - b. Select the rule.
 - c. In the **Capabilities & Exclusions** pane, click **Exclusions Center**.
2. To migrate legacy global exclusions, go to **Policy > Threat Prevention > Global Exclusions**.
3. Click **Go to Smart Exclusions**.
4. To migrate all legacy exclusions:
 - a. Click **Migrate from Legacy Exclusions** (available only if there are no exclusions) or click  and click **All exclusions from legacy**.

The **Import All Legacy Exclusions** window appears.

- b. (Recommended) To remove all the legacy exclusions after you migrate to smart exclusions, select **Remove all the imported exclusions from legacy**.
 - c. Click **Import**.
5. To migrate specific exclusions:
 - a. Click  and **Select exclusions from legacy**.
The **Transfer from Legacy - Select Exclusions** window appears.
 - b. Select the exclusions.
 - c. Click **OK**.
The exclusions are added to smart exclusions.
6. For specific rule, click **OK** and **Save & Install**.
7. For global exclusions, click **Save**.

The exclusions are automatically enforced on the client without installing the policy.

Importing and Exporting Exclusions

To import or export exclusions:

1. To import or export exclusions for a rule:
 - a. Go to **Policy > Threat Prevention > Policy Capabilities**.
 - b. Select the rule.
 - c. In the **Capabilities & Exclusions** pane, click **Exclusions Center**.
2. To import or export global exclusions, go to **Policy > Threat Prevention > Global Exclusions**.
3. Click **Go To Smart Exclusions**.
4. To import exclusions:
 - a. Click  and click **Import Files**.
 - b. Browse and select the import file in the JSON format.
 - c. For specific rule, click **OK** and **Save & Install**.
 - d. For global exclusions, click **Save**.

The exclusions are automatically enforced on the client without installing the policy.

5. To export exclusions, click .

The file is exported in the JSON format.

Managing Exclusions

To manage exclusions:

1. To manage smart exclusions for a rule:
 - a. Go to **Policy > Threat Prevention > Policy Capabilities**.
 - b. Select the rule.
 - c. In the **Capabilities & Exclusions** pane, click **Exclusions Center**.
2. To manage global smart exclusions, go to **Policy > Threat Prevention > Global Exclusions**.
3. Click **Go To Smart Exclusions**.
4. To edit an exclusion:

- Select the exclusion and click .
- Right-click the row and click **Edit**.

To a change **Single-method exclusion** to **Multi-method exclusion**, click **Edit in multi-value wizard** at the bottom of the wizard.

Refer to ["Adding Exclusions to a Specific Rule" on page 310](#) to edit the exclusion.

5. To delete exclusions:
 - Select the exclusions and click .
 - Click the row and at the end of the row, click .
 - Select the exclusions, right-click and click **Delete**.

6. To duplicate exclusions:

- Select the exclusion and click .
- Click the row and at the end of the row, click .
- Select the exclusion, right-click and click **Duplicate**.

7. To enable or disable the exclusion, toggle the button in the **Status** column.
8. To edit **Name**, **Capabilities** and **Comment**:

- a. Click the row.
 - b. At the end of the row, click .
 - c. Edit the details.
 - d. Click .
9. For a specific rule, click **OK** and **Save & Install**.
 10. For global exclusions, click **Save**.

The exclusions are automatically enforced on the client without installing the policy.

Optimizing the Endpoint Security Client for Servers and Profiles

Servers such as exchange servers, database servers, domain controllers, and additional profiles like Exclude ConnectWise and Not a Virus need specific settings in the Endpoint Security client for proper data security and processing (allowing and blocking).

To automatically apply these specific optimization settings to the Endpoint Security client when installed on a server, follow these steps:

1. Select the **EndPoint for Server Optimization** option for the policy rule.
2. Specify the servers for which you want to select this option.

This action assigns the Windows server roles to the server and profile roles to the additional profiles, containing pre-defined exclusions (based on Microsoft and Check Point's recommendations) and server-specific processes applied by the policy.

Supported servers:

- Domain Controller
- Exchange Server
- SharePoint 2007
- SharePoint 2010
- SharePoint 2013
- SharePoint 2016
- SQL Server
- Terminal Server
- DHCP Server
- DNS Server
- File Server

- Hyper-V
- Web Server (IIS)
- Print Server

Additional Profiles:

- Exclude ConnectWise
- Not a Virus
- Not a Virus TE
- Not a Virus AM



Notes :

- This is supported only with:
 - Endpoint Security Client version E86.60 and higher.
 - Management Server R81.20 JHF 53 and higher.
- Oracle servers are not supported.

To automatically optimize the Endpoint Security client for a server:



Note - Proxy is not supported.

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select a policy rule.
3. In the **Capabilities & Exclusions** pane > **EndPoint for Server Optimization**, select **On**.
4. Click **Choose the relevant roles to optimize the EndPoint for your servers**, and select the servers.
5. Click **OK**.
6. Click **Save**.
7. Click **Install Policy**.

Quarantine Management

When Endpoint Security components (Forensics and Anti-Ransomware, Anti-Bot, Threat Extraction and Threat Emulation) detect malicious files, it quarantines the files automatically based on the configured policy. All components use the same Remediation service, that:

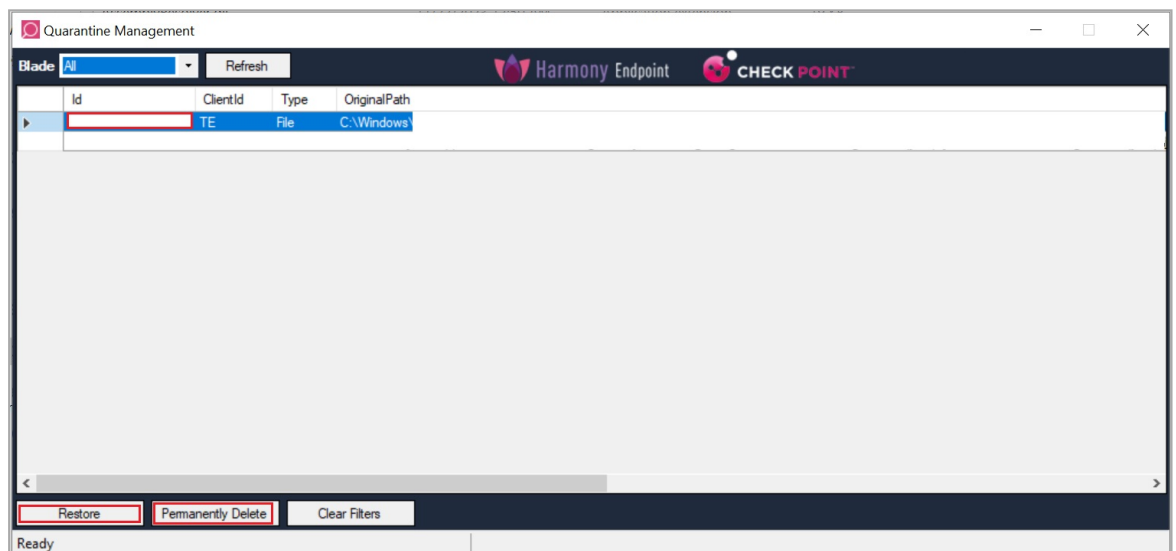
- Receives the request to quarantine a file.
- Terminates the file's process, if running.
- Encrypts the file and stores it compressed along with metadata in a protected folder.

Two utilities let administrators and end-users manage quarantined files.

■ Endpoint Security Quarantine Manager

The **Endpoint Security Quarantine Manager** utility is called **RemediationManagerUI.exe** and it is located in `C:\Program Files (x86)\CheckPoint\Endpoint Security\Remediation` on client computers. It lets end-users to view the files in quarantine.

- To delete the quarantined files, select the file and click **Permanently Delete**.
- To restore the quarantined files, select the file and click **Restore**.



■ Endpoint Security Quarantine Manager for Administrators

The administrator utility is called **AdminRemediationManagerUI.exe** and it contains the capabilities of the end-user utility plus these additional features:

- **Quarantine** - Send files to quarantine.
- **Delete** - Use the Endpoint Security Remediation service to delete a file.
- **Import** - Import a quarantined file from a different computer or location.

The **Endpoint Security Remediation Manager for Administrators** utility is dependent on your Endpoint Security client version. To download the utility that matches your Endpoint Security client:

1. Go to the [Endpoint Security Homepage SK](#).
2. In the **Client Releases** section, choose the Endpoint Security client version that matches your installed Endpoint Security client version.
3. Click the SK mentioned in the **Release Home page** column.
4. In the SK that opens, in the **Utilities/Services Downloads** section, click the EXE file for **Endpoint Security Remediation Manager for Administrators** to download it.

Using the Quarantine Manager for Administrators

When you open the Endpoint Security Quarantine Manager or the Endpoint Security Quarantine Manager for Administrators, each quarantined item is shown as a file. The name of the file is the incident ID. To find a file, search for the incident ID found in the Endpoint Security logs.

By default, quarantined files stored on the client are in

C:\ProgramData\CheckPoint\Endpoint Security\Remediation\quarantine on the client computer.

Best practice is to configure **Copy quarantine files to a central location** in the *"File Quarantine" on page 293* settings. Then you can use the Quarantine Manager for Administrators to import all files related to an incident from one location that you can access.

From the Quarantine Manager for Administrators you can:

- Restore files in a protected location to test them.
- Collect all malicious files related to an attack for research.

To permanently delete an item:

1. Open the Endpoint Security Quarantine Manager for Administrators.
2. Select one or more items.
3. Click **Delete**.

To send a file to quarantine from outside of the utility:

1. Open the Endpoint Security Quarantine Manager for Administrators.
2. Click **Quarantine**.
3. In the window that opens, browse to select the file to move to quarantine.

To import a suspicious file to the utility:

1. Open the Endpoint Security Quarantine Manager for Administrators.
2. Click **Import**.
3. In the window that opens, browse to select the quarantined file to import.

The file, with its metadata, is imported to the quarantine database from where the utility is run.

Managing Quarantined Files

Quarantine Management helps protect the network by isolating potentially harmful files and applications (malware, ransomware, suspicious files, and so on), preventing threats from spreading across the environment. It offers a centralized view, enabling security teams to manage quarantined items efficiently. Administrators can respond quickly to incidents, inspect suspicious content, and resolve issues by restoring safe files or removing malicious ones.

To view the **Quarantine Management** page, from the left navigation panel, click **Asset Management > Quarantine Management**.



Note - Quarantine Management feature is supported only on the Endpoint Security client for Windows version E89.05 and later.

Benefits

- **Centralized control:** View and manage quarantined items across all endpoints from a unified location.
- **Safe investigation:** Download and analyze quarantined files in a secure, password-protected format for further examination by SOC analysts.
- **Efficient threat response:** Restore or delete files in bulk across impacted devices, swiftly addressing actual threats and false positives.

Viewing Quarantined Files and Applications

The **Quarantine Management** page shows all quarantined files and applications in two switchable views:

- **View by Files:** Each row represents an individual file. Shows file details including name, path, hash, responsible blade, status, and the number of devices where this file was quarantined.

View quarantined files by Files Devices Restore Delete Fetch file Refresh Search... Filter 471 items									
☐ File name	File hash	File path	Active blade	Status on device	Devices with files	Quarantined date	Last device updated	Last action	
☐ demo4.txt	A87FF679A2F3E71D9181...	C:\temp\demo4.txt	Forensics	Quarantined	GrigoryK-180	14/08/2025, 1:30:36	14/08/2025, 1:30:36	Restore Failed	
☐ demo3.txt	ECCBC87E4B5CE2FE28...	C:\temp\demo3.txt	Forensics	Restored	GrigoryK-180	14/08/2025, 1:30:35	14/08/2025, 1:33:20	N/A	
☐ olivierf100.txt	E7E5FA40569514EC442...	C:\Users\KiprushkinTest\...	File Protectio	Quarantined	DESKTOP-32NNG	17/07/2025, 15:41:36	17/07/2025, 15:41:36	N/A	

- **View by Devices:** Each row represents an individual endpoint. It shows device details, including name, operating system, version, and the total count of quarantined files on that device.

View quarantined files by Files Devices Restore Delete Fetch file Refresh Search... Filter 5 items									
File name	File hash	File path	Active blade	Status on device	Devices with files	Quarantined date	Last device updated	Last action	
☐ E89-05-quarantine	238 files								
☐ 0ac066f740d81ae472730892ADA616F8...		C:\Users\javivgo\...	File Protection	Quarantined	E89-05-quarantine	18/06/2025, 14:1...	18/06/2025, 14:15:30	N/A	
☐ 27ad2f83965ddd499698BD642E6418...		C:\Users\javivgo\...	File Protection	Quarantined	E89-05-quarantine	17/06/2025, 16:0...	17/06/2025, 16:00:58	N/A	
☐ 71b2bec10c5409d8ce3A8836AECF72F...		C:\Users\javivgo\...	File Protection	Quarantined	E89-05-quarantine	17/06/2025, 16:0...	17/06/2025, 16:00:55	N/A	

To change the view, click **Files** or **Devices** next to **View quarantined files**.

Column	Description
File name	Name of the quarantined file.
File hash	Hash of the quarantined file.
File path	Location of the quarantined file on the device.
Active blade	Security blade that quarantined the file. For example, Anti-Malware, Forensics, or File Protection.
Status on device	Status of the quarantined file. ■ Quarantined ■ Deleted ■ Restored ■ Failure / Error
Devices with files	Name of other devices that have the same quarantined file.
Quarantined date	Date on which the file was quarantined.

Column	Description
Last action	Recent action taken on the quarantined file.
Last device updated	The date on which the device was recently updated. (Appears only on Devices view)

Acting on Quarantined Files and Applications

Administrators can take these actions on the quarantined files and applications:

- [Fetch \(download\) a quarantined file](#)
- [Restore a quarantined file](#)
- [Delete a quarantined file](#)

Fetching (download) a quarantined file

The **Quarantine Management** page allows you to download quarantined files for further analysis or inspection and ensure secure handling.



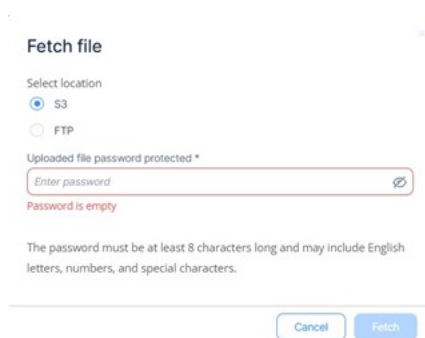
Note - You can fetch only one file at a time.

To fetch a quarantined file:

1. Choose the quarantined file to download.
2. Select where you want to upload the file:

■ To upload the file to AWS S3:

a. Select **S3**.



Fetch file

Select location

☒ S3

☐ FTP

Uploaded file password protected *

Enter password

Password is empty

The password must be at least 8 characters long and may include English letters, numbers, and special characters.

Cancel Fetch

b. In the **Uploaded file password protected** field, enter a password.

You need this password to open the file in AWS S3.

c. Click **Fetch**.

 Notes -

- To upload a file to S3, the file size must not exceed 25 MB.
- The file is retained only for 30 days in S3.
- You can archive up to 100 MB of files.

- To upload the file to your corporate FTP server:
 - a. Select **FTP**.
 - b. Enter your FTP server details.

Fetch file

Select location

☐ S3

☒ FTP

Protocol

Server address *

Path on server

Server fingerprint

FTP server username *

FTP server password *

Password to protect uploaded file *

Password is empty

The password must be at least 8 characters long and may include English letters, numbers, and special characters.

Cancel Fetch

- c. In the **Password to protect uploaded file** field, enter the password.
You need this password to open the file in the FTP server.
- d. Click **Fetch**.

Restoring a quarantined file

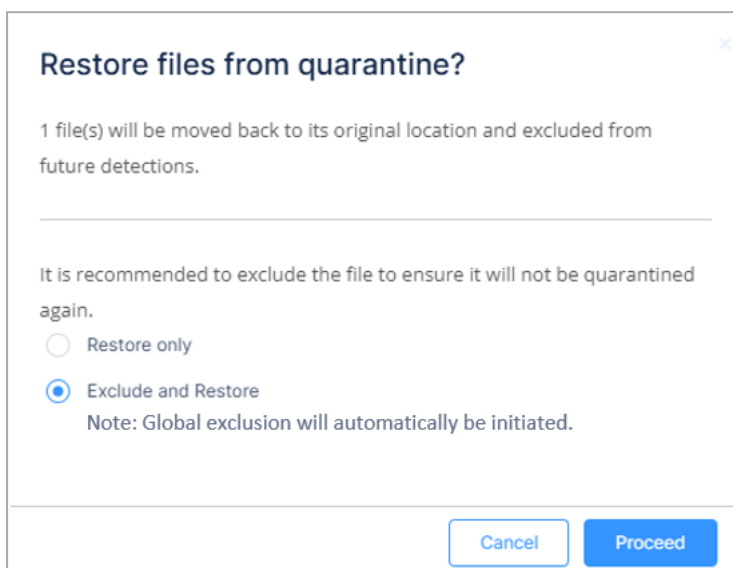
Restoring a quarantined file allows an administrator to recover a file that was incorrectly identified as malicious.

Notes -

- Restore a quarantined file if it was wrongly flagged (a false positive), and only after confirming that the file is safe.
- To prevent the restored file from being quarantined again, you need to create a global exclusion.

To restore or exclude a quarantined file:

1. Choose the file to restore using the multi-select checkboxes.
2. Click **Restore**.



3. Select one of these options:

- To restore a file from quarantine, select **Restore only**.

 Notes:

- The system restores the file to the same location from where it was quarantined.
- If Endpoint Security detects the same file as malicious in any other endpoint, it quarantines the file again.

- To restore a file and also exclude it from quarantine in the future, select **Exclude and Restore**.

The system adds an exclusion to the [Global Exclusions](#) which affects all endpoints on the network, ensuring that the file is not flagged as malicious again.

4. Click **Proceed** to complete the restoration.

The system sends a push operation to the relevant device.

Deleting a quarantined file

Deleting a quarantined file permanently removes it from the system, ensuring it cannot be restored or executed again. This action is typically used for files identified as confirmed threats, such as malware or spyware.

To delete a quarantined file:

1. Go to the **Quarantine Management** page.
2. Using multi-select checkboxes, select the file you want to delete permanently.
3. Click **Delete**.

In the confirmation pop-up that appears, click **OK**.



Note - Once a file is deleted, it cannot be restored.

Endpoint Security Client Device Restart Requirements

When an administrator make changes to these actions for the Endpoint Security client, the endpoint devices must be restarted to enforce the changes on the endpoint:

- When adding or removing the following capabilities:
 - Full Disk Encryption
 - Media Encryption & Port Protection.
- When removing the Anti-Malware capability during an upgrade or policy change.
- When switching the Anti-Malware engine from E1 to E2 (DHS compliant) client version.
- After successfully installing the Endpoint Security client on endpoints with KMDF (Kernel-Mode Driver Framework) versions 1.10 or lower.

Configuring Client Settings

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

Configure the following Client Settings from the respective tabs:

- ["User Interface" on page 348](#) - Customize the Endpoint Security client user interface
- ["Log Upload" on page 351](#) - Configure Log upload settings
- ["Installation and Upgrade Settings" on page 352](#) - Configure settings for Endpoint Security client installation or upgrade
- ["General" on page 353](#) - Configure general settings for proxy authentication, data sharing, connection awareness, super-node, disabling capabilities, network protection, and push operations.

User Interface

Default Client User Interface

You can select the default 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

Item	Description	Size of Image
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.
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 number of hours an end user can postpone the Endpoint Security Client installation or upgrade.

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.

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.
- When specifying the path to the EPS installer, you must enter the complete path to the EPS.msi file. For example, C:\Installers\EPS\EPS.msi

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 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.

General

Authenticated Proxy

If you have a proxy server to authenticate access to a resource:

1. Go to **Policy** > **Client Settings** > **General** > **Authenticated Proxy**.
2. Enter:
 - **Proxy** - Proxy server address in the format address:host. For example, 192.168.79.157:3128
 - **Username** - User name for the proxy server.
 - **Password** - Password for the proxy server.
3. Click **Save**.

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 share the data with Check Point ThreatCloud:

1. Go to **Policy > Client Settings > General > 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**.

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 one of the 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.

 **Note:** Connection Awareness determines policy assignment based on a device's connection to defined network targets, not its online/offline status.

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 with server-like and proxy capabilities. It functions as a light-weight proxy (based on NGINX) that helps reduce bandwidth consumption and supports offline updates, so that only the Super Node requires direct connectivity to the update servers.

By default, a Super Node listens on TCP port 4434 and TCP port 3128 (proxy mode) for client connections. Endpoint clients also use TCP port 4436 (HTTPS) for Super Node proximity calculations.

 **Note** - Ensure ports 4434 and 4436 are allowed between endpoints and the Super Node under the same firewall rules. If port 4436 is blocked, the Super Node cannot perform proximity calculations.

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.



Note - Super-Node is available in both Domain and Workgroup environments.

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.
- Super Node is supported for macOS through a Windows Super Node (preferred), or via a macOS machine for Anti-Malware only.
- Super Node is now supported on Endpoint Security Clients for Linux, starting from version 1.22.12.

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.
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	Endpoint Security Client for macOS and 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

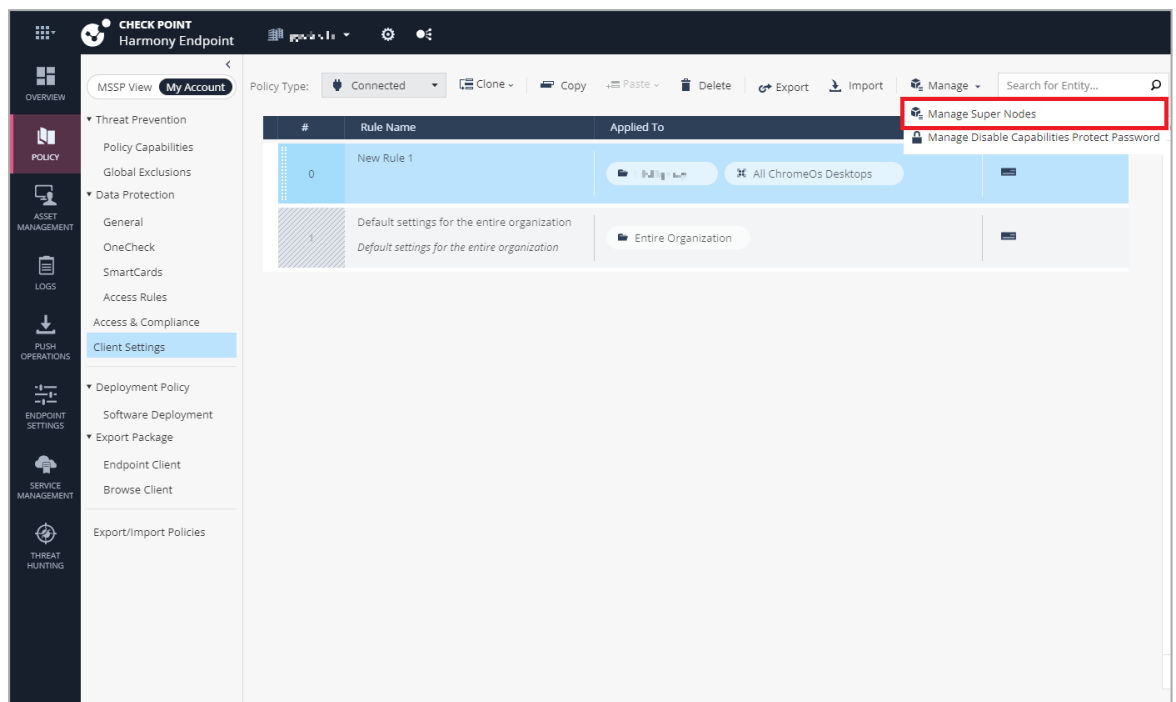
- By default, the cache max size is 4 GB and will automatically purge files after 7 days of inactivity. Files stored for a longer time without access are removed from cache.
- Super Node requires approximately 350 MB of additional space to operate properly.

To configure a Super Node through the toolbar:

For Management Servers supporting **Manage Super Nodes** capability:

1. Go to **Policy > Client Settings**.
2. Configure the Super Node:

- a. From the toolbar, click **Manage Super Nodes**. The **Manage Super Nodes** page will be displayed.



- b. Click the **+** icon.
- c. Select the required devices and click **Add**.

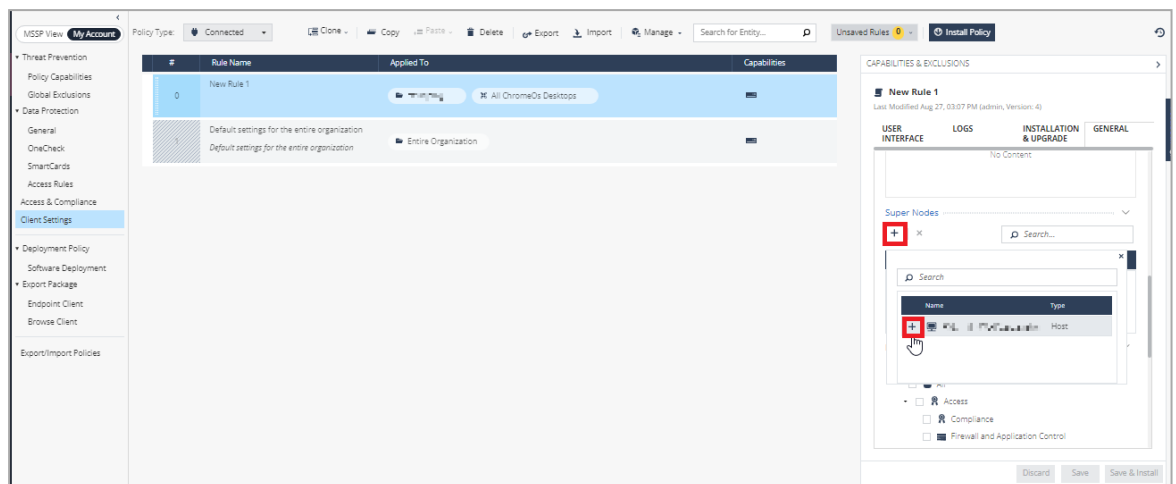
You can use the search bar to find the required device(s).

The system creates a widget for each device selected as a super node.

- d. Click **Save**.

3. Apply the super node to the required policy.

- a. Select the relevant policy (**Policy > Client Settings**).
- b. In the **Capabilities & Exclusions** pane, go to the **General** tab.



- c. Scroll down to the **Super Nodes** section and click the **+** icon.
- d. Select the devices you want to assign as super nodes and click **Add**.
- e. Click **Save & Install**.

Note - The system applies the selected super nodes only to the devices (users) selected in the policy.

4. To edit the maximum number of concurrent connections a super node can handle simultaneously:

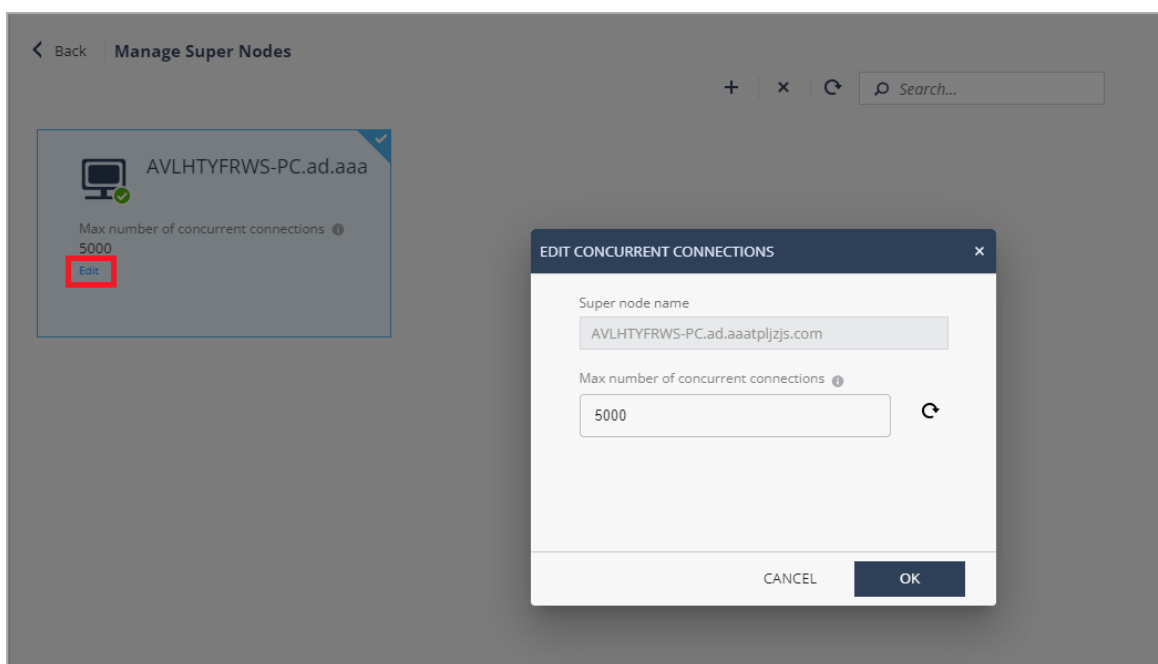
Notes -

- This feature is supported only on Endpoint Security Client versions E88.70 and higher.
- The default value of maximum number of simultaneous connections is 5000.

- a. In the super node widget, click **Edit**.

The **Edit Concurrent Connections** window is displayed.

- b. In the **Max number of concurrent connections** field, enter the maximum number of concurrent connections the super node can handle.



- c. Click **OK**.

5. After selecting the devices and configuring concurrent connections, click **Save**.

Note - Configuring a device as a Super Node does not require policy installation.

To configure a super node proxy for offline environment:

Super node proxy configuration is available for Endpoint Security client version 88.70 and higher.

Notes -

- **(Recommended)** Do not configure more than five proxies in the **Client Settings**.
 - Super node itself requires internet access.
1. After installing Endpoint Security, configure a device with the internet access to be a super node.
 2. Configure the **Client Settings** policy for the groups related to machines without access to internet.
 3. Create an **Export package**.
 4. Install the package with the super node policy on the device without access to the internet.

Limitations of the Super node proxy:

- Super node proxy do not support:
 - VPN
 - Browser Security extension
 - FDE Remote Help
 - Uploading CPIInfo
 - Tiny Agent
 - IPv6
- Super node does not support environments that require an explicit proxy.
- Super node does not support an authenticated proxy configured in the **Client Settings** policy.

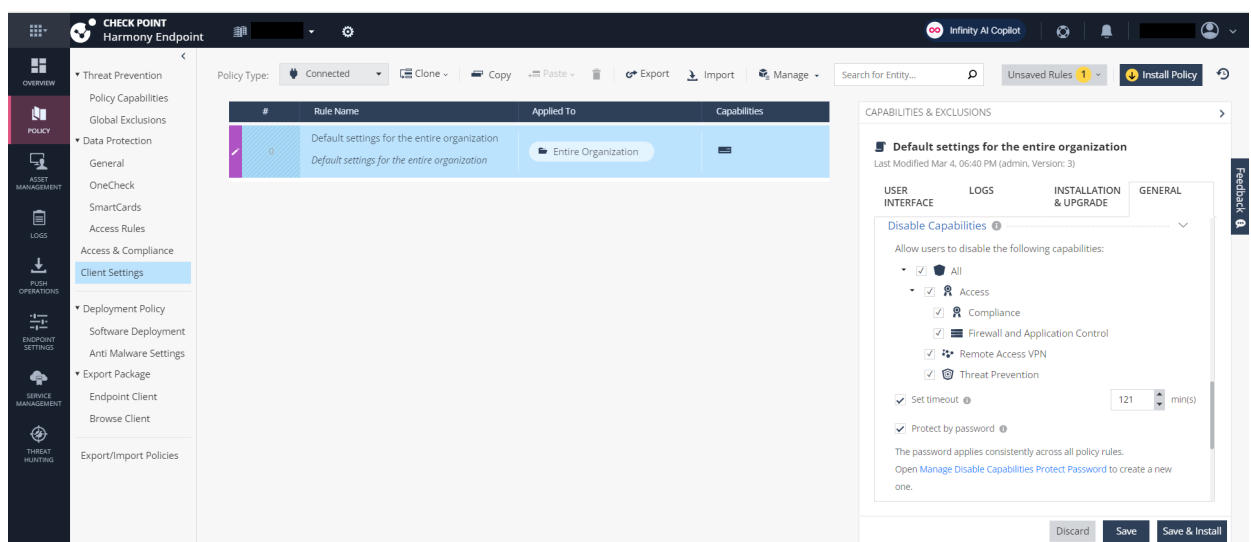
Disable Capabilities

Disable Capabilities allows users to turn on or turn off capabilities, such as Threat Prevention, Compliance, and so on in the Endpoint Security client.

Note - If the Endpoint Security Client device is restarted, the option to enable or disable the capabilities will only be available after five minutes.

To allow users to disable capabilities:

1. Go to **Policy > Client Settings > General > Disable Capabilities**.



2. Select the capabilities that can be disabled by the user on the client.
3. To enable the disabled capabilities automatically after a set interval of time:

Note - This is supported only on Windows with Endpoint Security client version E88.30 and higher.

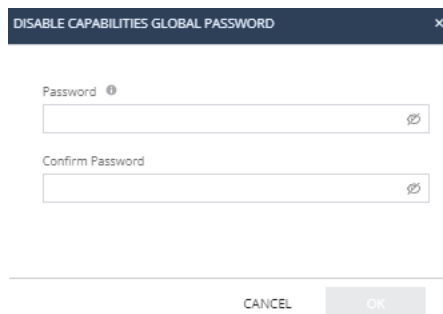
- a. Select the **Set timeout** checkbox.
 - b. In the timeout field, enter the time in minutes.
4. To allow users to disable the capabilities only after entering a password, select the **Protect by password** checkbox.

Note - This is supported only on Windows with Endpoint Security client version E88.30 and higher.

- a. Click **Manage Disable Capabilities Protect Password**.

Note - Optionally, from the taskbar, click **Manage** and select the **Manage Disable Capabilities Protect Password** from the list.

- b. In the **Password** field, enter a password and re-enter the password in the **Confirm Password** field.



Note - Make sure the password is at least eight characters long, without spaces, and includes:

- An uppercase letter
- A lower case letter
- A number.

- c. Click **OK**.

5. Click **Save & Install**.

Network Protection

You can let users disable network protection on their computers.

Network Protection includes these components:

- Firewall
- Application Control

To configure network protection alerts:

1. Go to the **Policy > Client Settings > General > Network Protection**.
2. You may select **Allow users to disable network protection on their computers** - To disable network protection.
3. 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.
4. Click **Save**.

Push Operations

Push Operations are operations that the server pushes directly to client computers with no policy installation required. You can set the minimum time interval between status updates of Push Operations.

For more information, see ["Performing Push Operations \(Old User Interface\)" on page 580](#).

To set the minimum time interval between status updates of Push Operations:

1. Go to the **Policy > Client Settings > General > Push Operation**.
2. Set the **Minimum interval between status updates of Push Operations**.
3. Click **Save**.

Configuring the Data Protection Policy

Configuring the Data Protection Policy includes:

- ["Configuring Full Disk Encryption" below](#)
- ["Configuring Media Encryption & Port Protection" on page 394](#)

Configuring Full Disk Encryption

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



Note - When you add or remove Full Disk Encryption for the Endpoint Security client, the client must restart to enforce them on the endpoint.

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 366](#) - 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 367](#) - 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 375](#) and ["FileVault Encryption for macOS" on page 377](#)

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

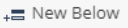
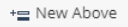
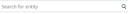
Each new rule you create, has pre-defined settings, which you can then edit in the right section of the screen.

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	 NEW
Save, view, or discard changes	Unsaved Rules 1  Save All Changes  View Changes  Discard Changes

To do this	Click this
Duplicate a rule	 
Install Policy	
Search for entity	
Delete a rule	

For Crypto-Shredding a computer, see [sk179911](#).

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. IRRT are not encrypted.

Go to **Advanced Settings > Encryption > Allow Self-Encrypting Drives (SED) hardware functionality**.

Full Disk Encryption probes and uses 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)

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.

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.
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.

Action	Description
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	Users can use Remote Help to get access to their Full Disk Encryption protected computers if they are locked out. Here you configure the number of characters in the Remote Help response that users must enter.

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 Endpoint Security 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. Go to **Asset Management > Organization > Computers**.
2. Click  and select **Full Disk Encryption > Preboot User Assignment**.

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

3. Click the  icon.

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

4. 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. Go to **Asset Management > Organization > Computers**.
2. Click  and select **Full Disk Encryption > Preboot User Assignment**.

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

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

The list of authorized users to access the device appears.

4. 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.

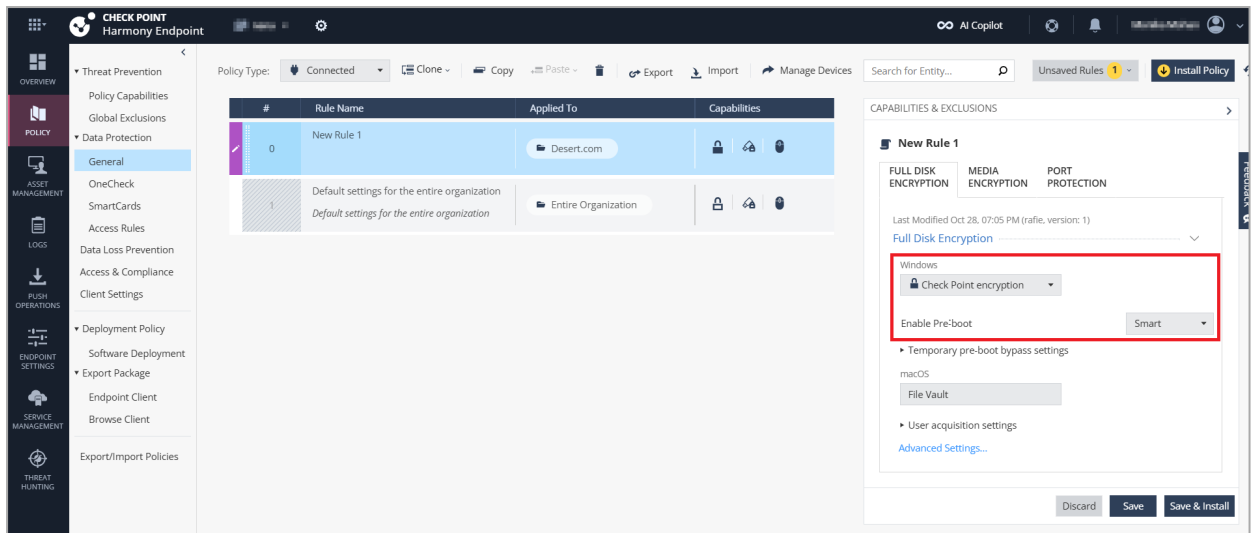
Smart Pre-Boot

With Smart Pre-boot, you can allow end-users to unlock their devices that have been locked due to forgotten passwords or multiple failed log in attempts.

- [Easy Unlock](#) - End user requests an unlock and the administrator must approve the request in the Endpoint Security Administrator Portal.
- [Self Unlock](#) - End user can unlock the device using a QR code, without requiring the administrator's approval.

To enable Smart Pre-boot:

1. Access the Endpoint Security Administrator Portal and click **Policy**.
2. Go to **Data Protection > General**.
3. Select a rule.
4. Click the **Full Disk Encryption** tab.
5. From the **Windows** list, select **Check Point encryption**.



6. From the **Enable Pre-boot** list, select **Smart**.

7. Click **Save & Install**.

Now, that the Smart Pre-boot is enabled, [Easy Unlock](#) is enabled automatically. If required, you can configure the Endpoint Security Administrator Portal to allow end-users to use [Self Unlock](#) and [Passwordless Pre-boot authentication](#).

Easy Unlock

Easy Unlock allows administrators to **Accept** or **Reject** a **One-Time Logon** request or a **Password Change** request from a user.

Easy Unlock is enabled automatically when [Smart Pre-boot](#) is enabled.

This feature is supported:

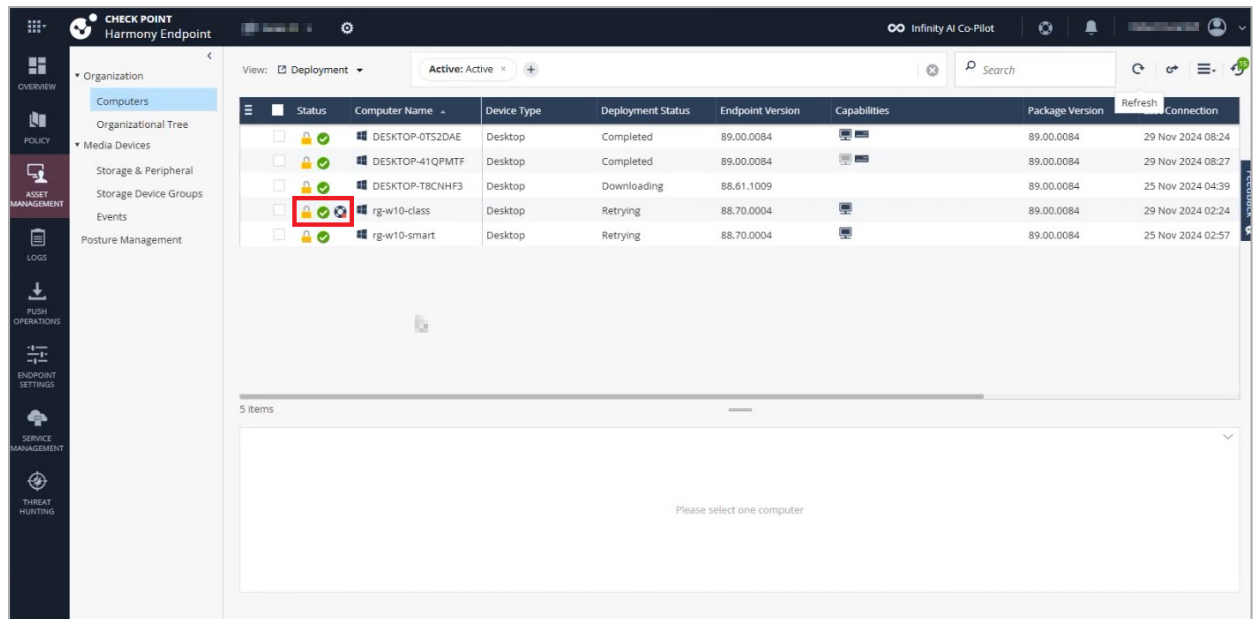
- Only with Endpoint Security client for Windows version 86.50 and later.
- Only if the **Check Point encryption** is used for **Full Disk Encryption**.

When a end-user requests for unlock, the  icon appears for the device in **Computers** page under **Asset Management**.

To respond to the request:

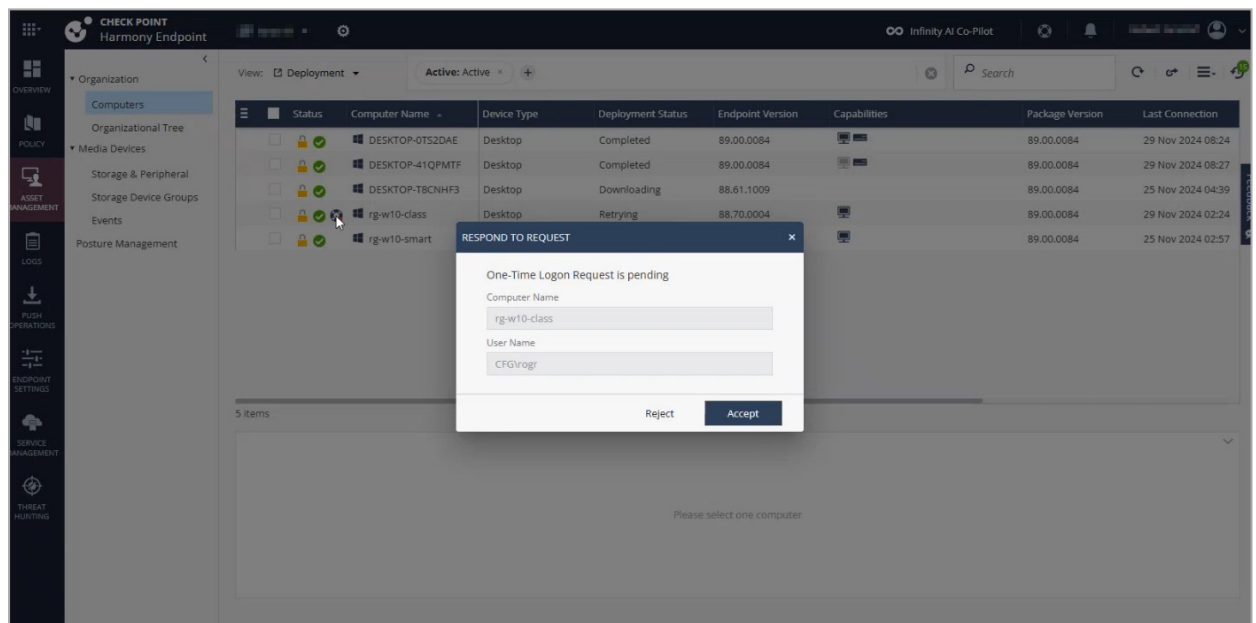
1. Go to **Asset Management > Organization**.
2. Click **Computers**.

You can view the  icon in the **Status** column.



3. Click the  icon.

The **Respond to Request** dialog box appears.



4. Click **Accept** or **Reject**.

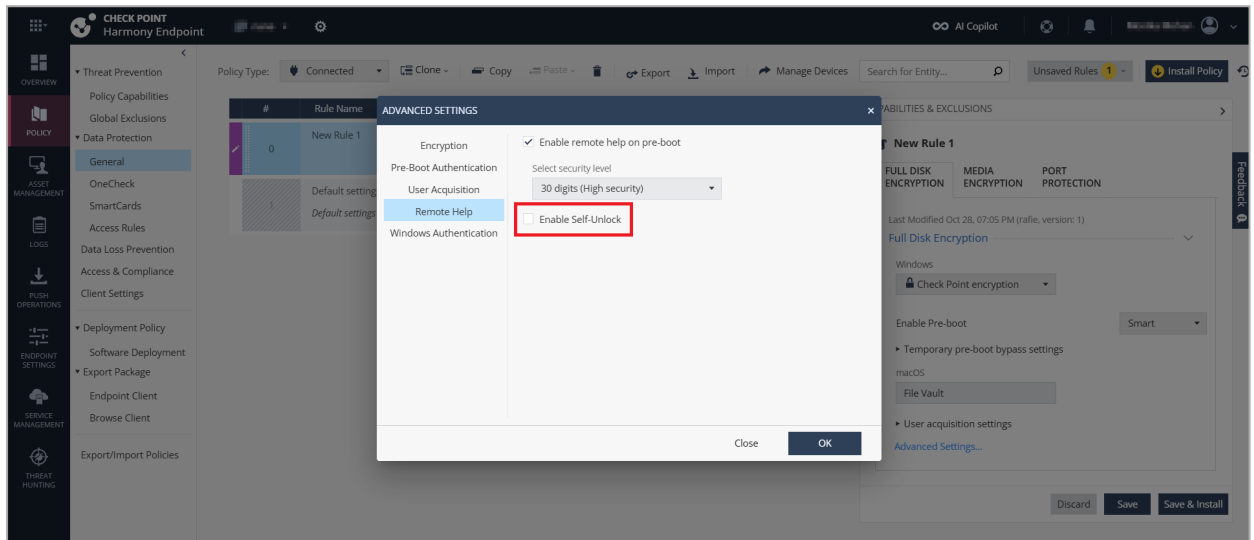
Self Unlock

Self Unlock allows users to unlock their computers by scanning a QR code using their mobile device, without administrator intervention.

It is supported only with Endpoint Security client for Windows version 86.60 and later.

To enable Self-Unlock for Full Disk Encryption:

1. Go to the **Policy > Data Protection > General** .
2. Select a rule.
3. Click the **Full Disk Encryption** tab.
4. Click **Advanced Settings**.
5. Click **Remote Help**.



6. Select the **Enable Self-Unlock** checkbox.
7. Click **OK**.
8. Click **Save & Install**.

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 Endpoint Security 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.

Taking Control of Unmanaged BitLocker Devices

You can do a takeover of BitLocker-encrypted devices that are not managed by Endpoint Security, and make them centrally managed. You can do this using BitLocker Management or Check Point Full Disk Encryption.

To take control of unmanaged BitLocker devices using BitLocker Management:

Define and install a Full Disk Encryption policy with BitLocker Management. Follow these guidelines:

- Define a Full Disk Encryption rule that applies to the entire organization or only to the entities that need BitLocker Management.
- In **BitLocker Encryption Settings**, select **Windows Default** as the **Encryption Algorithm**. This is important because it leaves the existing BitLocker encryption in place. Selecting another algorithm explicitly may result in a re-encryption, if the existing algorithm does not match the algorithm in the policy. It is a good idea to avoid re-encryption because it can take a long time. The time it takes depends on the disk size, disk speed and PC hardware.

To take control of unmanaged BitLocker devices using Check Point Full Disk Encryption:

1. Follow the procedure for ["To take control of unmanaged BitLocker devices using BitLocker Management:" on the previous page](#).
2. After the devices are under Check Point BitLocker Management, define a rule with Check Point Full Disk Encryption that applies to the Entire Organization or only to the entities that need Check Point Full Disk Encryption. See ["Check Point Disk Encryption for Windows" on page 366](#)



Best Practice - When you change the encryption policy for clients 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 encryption policy for entire organization in one operation. Make the change for one group of users at a time.

FileVault Encryption for macOS

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

User Authentication to Endpoint Security Clients (OneCheck)

OneCheck User Settings define how users authenticate to Endpoint Security client computers.

OneCheck User Settings include:

- How users authenticate to Endpoint Security.
- If users can access Windows after they are authenticated to Endpoint Security or if they must also log on to Windows.
- What happens when a user enters invalid authentication details.
- A limit for how many times a user can access a computer.
- If Remote Help is permitted. This lets users get help from an administrator, for example if their computers become locked after too many failed authentication attempts.

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 the **Policy** view > **Data Protection** > **General** > **Full Disk Encryption** > **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** > **Data Protection** > **OneCheck** > **Password Constraints**.
- **Enable Check Point Endpoint Security screen saver** - The screen saver is active only after a Full Disk Encryption policy was installed on the client. After selecting the Check Point Endpoint 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.

Pre-boot Authentication Methods

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.
The password can be the same as the Windows password or created by the user or administrator.
- **Smart Card** - A physical card that you associate with a certificate. Users must have a physical card, an associated certificate, and Smart Card drivers installed.
- **Passwordless authentication** - Allows users to securely access their device without entering a password. For more information, see ["Passwordless Pre-boot Authentication" on page 382](#).

To configure the authentication method for Password or Smart Card:

1. Go to the **Policy view > Data Protection > SmartCards > Pre-boot Authentication**.
2. Select one of these options:
 - a. **Password** - Users can only authenticate with a username and password.
 - b. **Smart Card (requires certificate)** - Users can only authenticate with a Smart Card. **Change authentication method only after user successfully authenticates with a Smart Card** - If you select this option, users can authenticate with a password until all of the requirements for Smart Card authentication are set up correctly. After users successfully authenticate one time with a Smart Card, they must use their Smart Card to authenticate. If you configure a user for Smart Card only and do not select this, that user is not able to authenticate to Full Disk Encryption with a password
 - c. **Either SmartCard or Password** - Users can authenticate with a user name and password or a SmartCard.

Before You Configure Smart Card

- Users must have the physical Smart Card in their possession.
- Users' computers must have a Smart Card reader driver and token driver installed for their specific Smart Card. Install these drivers as part of the ["To configure the Smart Card options:" on the next page](#).
- Each user must have a certificate that is active for the Smart Card. The Directory Scanner can scan user certificates from the Active Directory. Configure this as part of the ["To configure the Smart Card options:" on the next page](#)

- In the Full Disk Encryption Policy rule > **Advanced Settings** > **Pre-boot Authentication**, make sure that **Enable USB devices in pre-boot environment** is selected

To configure the Smart Card options:

1. In the **Format used in your organization** area, select the Smart Card protocol that your organization uses:
 - **Not Common Access Card (Not CAC)** - all other formats
 - **Common Access Card (CAC)** - the CAC format
2. In the **Smart Card driver deployment** area, select the drivers for your Smart Card and Reader. All selected drivers will be installed on endpoint computers when they receive policy updates.

If you do not see a driver required for your Smart Card, you can:

- Enter a text string in the **Search** field.
 - Click **Import** to import a driver from your computer. If necessary, you can download drivers to import from the [Check Point Support Center](#).
3. In the Directory Scanner area, select **Scan user certificates from Active Directory** if you want the Directory Scanner to scan user certificates.
 4. If you selected to scan user certificates, select which certificates the Directory Scanner will scan:
 - **Scan all user certificates**
 - **Scan only user certificates containing the Smart Card Logon OID** - The OIDs are: 1.3.6.1.4.1.311.20.2.2.

Password Complexity and Security

To configure the password for OneCheck Logon, go to **Policy > Data Protection > OneCheck > Password Constraints**. These actions define the requirements for the OneCheck password:

Action	Description
Use Windows complexity requirements	The standard Windows password requirements are enforced: The password must: ■ Have at least six characters ■ Have characters from at least 3 of these categories: uppercase, lowercase, numeric characters, symbols.
Use custom requirements	If you select this, select the requirements for which type of characters the password must contain or not contain: ■ Consecutive identical characters, for example, aa or 33 ■ Require special characters. These can be: ! " # \$ % & ' () * + , - . / : < = > ? @ { ■ Require digits, for example 8 or 4. ■ Require lower case characters, for example g or t. ■ Require upper case characters, for example F or G. ■ Password must not contain user name or full name.
Minimum length of password	Enter the minimum number of characters for a valid password.
Password can be changed only after	Enter the minimum number of days that a password must be valid before the user can change it.
Password expires after	Enter the maximum number of days that a password can be valid before the user must change it.
Number of passwords before a previously used password may be used again	Enter the minimum number of password changes needed before a previously used password can be used again.

Passwordless Pre-boot Authentication

Passwordless Pre-boot authentication allows users to securely access their device without entering a password.

 **Note** - This option is available only for Endpoint Security Client for Windows version E87.60 and later.

To enable passwordless Pre-boot authentication:

1. Go to the **Policy > Data Protection > General** .
2. Select a rule.
3. Click the **Full Disk Encryption** tab.
4. Click **Advanced Settings**.
5. Click **Pre-boot Authentication**.
6. Select **Enable passwordless Pre-boot authentication** checkbox.
7. Click **OK**.

User Account Lockout Settings

You can configure Full Disk Encryption to lock user accounts after a specified number of unsuccessful Pre-boot login attempts:

- **Temporarily** - If an account is locked temporarily, users can try to log on again after a specified time.
- **Permanently** - If the account is locked permanently, it stays locked until an administrator unlocks it.

To configure an Account Lock Action:

1. Go to the **Policy** view > **Data Protection** > **OneCheck** > **User Account Lockout Settings**.
2. Configure the settings as necessary:

Option	Description
Number of failed logins before a user account is temporarily locked	Maximum number of failed logon attempts before an account is temporarily locked out.
Number of failed logins before a user account is permanently locked	Maximum number of failed logon attempts allowed before an account is permanently locked. The account is locked until an administrator unlocks it.
Duration for a temporary user lockout	Duration of a temporary lockout period, in minutes.

Remote Help Permissions

Remote Help lets users access their Full Disk Encryption protected computers if they are locked out. The user calls the designated Endpoint Security administrator and does the Remote Help procedure.

There are two types of Full Disk Encryption Remote Help:

- **One Time Login** - One Time Login allows access as an assumed identity for one session, without resetting the password.
If users lose their Smart Cards, they must use this option.
- **Remote password change** - This option is for users who use fixed passwords and forgot them.

For devices protected by Media Encryption & Port Protection policies, only remote password change is available.

To let users work with Remote Help:

1. Go to the **Policy** view > **Data Protection** > **OneCheck** > **Remote Help**
2. Select the allowed type(s) of Remote Help:

Option	Description
Allow account to receive remote password change help	Let users get help from an administrator to reset the account password (for example, if the user forgets the password).
Allow account to receive One-Time Logon help	Let the user get help from an administrator to log on, one time. One-time logon is for users who have lost their Smart Card. It is also useful if the user made too many failed attempts but does not want to change the password.

Logon Settings

OneCheck Logon Settings define additional settings for how users can access computers.

To configure Logon Settings, go to the **Policy** view > **Data Protection** > **OneCheck** > **Logon**:

Option	Description
Allow logon to system hibernated by another user	Lets a different user than the logged on user authenticate in Pre-boot to a system in hibernate mode.
Allow use of recovery media	Let user authenticate to use recovery media to recover and decrypt data from an encrypted system. Note: In E80.20 and higher, if this is not selected, users can still access recovery media that is created with a temporary user and password.
Allow user to change his credentials from the endpoint client	Let users change the password on an endpoint client during the Pre-boot.
Allow Single Sign-On use	Let users use Single Sign On to log on to Pre-boot and Windows when OneCheck Logon is disabled. Single Sign on applies only to Pre-boot and Windows and not to different components, such as VPN or Media Encryption. Users are always allowed to use Single Sign On when OneCheck Logon is running.

Bi-Directional Password Sync Settings

OneCheck Bi-Directional Password Sync Settings define additional settings password synchronization.

Options	Description
Allow OS password reset upon Pre-boot password reset	Reset the OS password after a successful Pre-boot password reset.

Installing and Deploying Full Disk Encryption

After a package that includes Full Disk Encryption is successfully installed on a client, many requirements must be met before the Full Disk Encryption policy can be enforced. Before these requirements are met, the Pre-boot does not open. The period of time between the installation and when the policy can be enforced is called the Full Disk Encryption Deployment Phase.

To move from Deployment phase to Full Disk Encryption policy enforcement, these requirements must be met:

- There must be communication between the client and the server.
- The client must receive Full Disk Encryption and user policies from the server.
- Users must be acquired according to the configured policy.
- At least one user account must be configured.
- The client must send a recovery file to the server.
- The required System Area must be created and boot records must be updated according to the configuration (this includes the activation of Pre-boot).
- The device must have the Client requirements or Full Disk Encryption.

If there is communication between the client and server and the client meets the Client requirements, all of the requirements are completed automatically. However, if these requirements are not met, Full Disk Encryption cannot protect the computer and the Pre-boot cannot open.

Client Requirements for Full Disk Encryption Deployment

Note -

- Not all the Full Disk Encryption (FDE) requirements are shown here. For the complete FDE requirements, see the [Release Notes for your Endpoint Security client version](#).
- The FDE System Area (SA) partition requires 512 MB of disk space. During the installation of the operating system, it is recommended to leave 512 MB of free, unpartitioned disk space to allow FDE to create the System Area without modifying existing partitions.
- If sufficient unpartitioned space is not available, the FDE service automatically shrinks existing partitions to allocate the required space.
- If FDE is unable to allocate the full 512 MB, it attempts to create a 32 MB System Area, and the Smart Preboot feature is disabled.
- FDE also requires at least 15 MB of free space on the UEFI System Partition (ESP). To avoid space-related issues, it is recommended to configure the ESP with a minimum size of 512 MB during operating system installation.
- During the initial background encryption process, FDE temporarily suspends Windows hibernation.

Clients must **not** have:

- RAID.
- Partitions that are part of stripe or volume sets.
- Hybrid Drive or other similar Drive Cache Technologies. See [sk107381](#).
- A compressed root directory. Subdirectories of the root directory can be compressed.

Other Requirements:

- All disks that are encrypted by FDE must have the same format (MBR or GPT)
- GPT-formatted disks are supported only on UEFI devices.
- Update the BIOS on the client computer to the latest version.
- If using the BIOS\UEFI option Fastboot, follow the precautions in [sk140215](#).
- If using a third-party credential provider to log in to Windows, configure FDE to use (wrap) the third-party provider. See [sk118817](#).

Completing Full Disk Encryption Deployment on a Client

For Check Point Full Disk Encryption, users are prompted to reboot their computers twice while Full Disk Encryption deploys. One time to make sure the Pre-boot is running before Full Disk Encryption encrypts the hard drive, and one time to validate the authentication credentials.

For BitLocker Encryption, users are prompted to reboot their computers once during the installation.

Stages of the Deployment Phase

You will see the status of the Deployment phase in:

- The Client Endpoint Security Main Page - In the Full Disk Encryption status.
- In the **Asset Management > Organization > Computers**. From the **View** dropdown, select **Full Disk Encryption**. The **FDE status** column shows the status of the FDE deployment.
- The debug logs

These are the statuses as shown in the Client Endpoint Security Main Page:

- **Waiting for Policy** - Waiting for policy to be downloaded from server.
- **User Acquisition** - Users are acquired when they log on to Windows on the computer that has Full Disk Encryption installed. The number of users that must be acquired depends on the settings configured. Full Disk Encryption can become active after all users are acquired. User accounts must have passwords and fulfill password rules to be acquired.
- **Verifying Setup** - The client verifies that all of the settings are fulfilled properly and checks that users acquired are correct and fulfill password policies.
- **Deliver Recovery File** - The client sends a recovery file to the server. It includes users on the computer that have permission to use the recovery media.
- **Waiting for Restart** - The user must reboot the client. After it is rebooted, users will see the Pre-boot. Users get a message to log in with their Windows credentials. Then Full Disk Encryption starts to encrypt the volumes according to the policy.
- **Encryption in Progress** - Full Disk Encryption is encrypting the volumes.

Viewing Full Disk Encryption (FDE) Status of an Endpoint Device

Using `fdecontrol.exe`, the administrators can view the FDE status of an endpoint.

Get-Status Command

To View the FDE Status:

1. Using any command-line interface (CLI) on the endpoint, navigate to the directory where the `fdecontrol.exe` file is located.
2. Run the following command:


```
fdecontrol.exe get-status
```

Example Output:

```
clientStatus=70
clientStatusDetails=100
currentProgress=997812095
encryptionState=3
errorMessage=
freeSpace=358 GB
lastRecoveryDelivery=2023-12-06 11:43:40+01:00
lastRecoveryUpdate=2023-12-06 11:43:39+01:00
loggedInOneCheckUser=Pete
loggedInUser=Pete
maxProgress=997812095
mountPoint=C:\
opalDisks=
targetProtection=3
totalSpace=476 GB
tpmDeviceStatus=4
tpmManufacturerId=
tpmSpecVersion=0.0
version=86.8.82.12
volumeCount=1
wilEnabled=false
wolEnabled=false
```



Note - You can also view the FDE status and parameter values from the Registry Editor.

Output Parameters

- `clientStatus` Shows the encryption state of the endpoint (Integer).

Value	State
During pre-deployment and initial deployment	
0	INIT
5	WAIT_CONFIGURATION
10	ACQUIRE_USERS
20	VERIFY_SETUP
30	SETUP_PROTECTION
40	WAIT_REBOOT
45	DELIVER_RECOVERY
During background encryption or decryption	
50	ENCRYPTING
60	DECRYPTING
On completing the encryption	
70	ENCRYPTED
Miscellaneous	
80	UNENCRYPTED
90	REENCRYPTING
103	DISABLED

- `clientStatusDetails` - Shows the progress of the encryption status in percentage (Integer).
- `currentProgress` - List of number of sectors that have been encrypted for each volume (Comma-separated list).
- `encryptionState` - List of encryption state of each volume. (Comma-separated list.)

Value	State
0	DECRYPTED
1	ENCRYPTING
2	DECRYPTING
3	ENCRYPTED
4	REENCRYPTING
255	DEFAULT

- `errorMessage` - Shows error messages. If there are multiple error messages, they are separated by a comma.
- `freeSpace` - List of free space available for each volume. (Comma-separated list.)
- `lastRecoveryDelivery` - Shows the date and time when the previous recovery data was delivered to the server.
- `lastRecoveryUpdate` - Shows the date and time when the recovery data was last updated in the client.
- `loggedInOneCheckUser` - Username of the current logged in windows user.
- `loggedInUser` - Username of the logged in pre-boot user.
- `maxProgress` - List of number of sectors to encrypt per volume (Comma-separated list).
- `mountPoint` - List of names of the volumes that will be or are encrypted (Comma-separated list).
- `opalDisks` - List of device number of the opal encrypted disks.
- `targetProtection` - List of values of the target algorithms (Comma-separated list).

Value	Target Algorithm
0	None
1	BLOWFISH
2	CAST
3	AES

Value	Target Algorithm
4	3DES
5	XTSAES512
6	XTSAES256

- `totalSpace` - List of total space available for each volume.
- `tpmDeviceStatus` - Shows bit field status of the endpoint's TPM chip (Integer).

Value	Status	Bit Size
0	NO_MEASUREMENTS	1
1	FAILED_REPORT	2
2	POLICY_NOT_ENABLED	4
3	POLICY_ENABLED	8
4	POLICY_APPLIED	16
5	TEMP_PREVENTED	32
6	PREVENTED	64
7	HW_PRESENT	128
8	HW_ENABLED	256
9	HW_ACTIVE	512
10	HW_OWNED	1024

- `tpmManufacturerId` - TPM manufacturer ID.
- `tpmSpecVersion` - TPM chip specification version. If the information is not available, it will be shown as 0.0.
- `version` - Epsinstaller version.
- `volumeCount` - Number of volumes that FDE will manage.
- `wilEnabled` - Status indicating whether the windows integrated logon is enabled or not (True/False).

- `wolEnabled` - Status indicating whether the WOL (Wake-On-LAN) is enabled or not (True/False).

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).



Note - When you add or remove Media Encryption & Port Protection for the Endpoint Security client, the client must restart to enforce them on the endpoint.



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](#).

The Media Encryption & Port Protection can be configured in the Check Point Portal.

To configure Media Encryption:

1. Navigate to **Policy > Data Protection > General**.
2. In the **Capabilities and Exclusion** pane, click **Media Encryption**.

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, click **View Exclusions**.
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.

- a. In the **Media Encryption** tab, click **View Exclusions**.
- b. Click **Import** and select the JSON file.

To export exclusions:

- a. In the **Media Encryption** tab, click **View Exclusions**.
- b. Select the exclusion from the list.
- c. 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, click **View Exclusions**.
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 Endpoint Security, 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 Endpoint Security, 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**.

Creating User Overrides (UserCheck)

You can allow users to override the Media Encryption policy.

To allow users to override the Media Encryption policy:

1. In the **Media Encryption** tab , click **Write Policy > User Overrides**.
2. Select the **Allow user to override company policy** checkbox.
3. From the **User can gain the following permission** list, select:
 - **Encrypt business-related data**
 - **Encrypt all data**
 - **Ask user**

Configuring 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 Windows 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.

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.

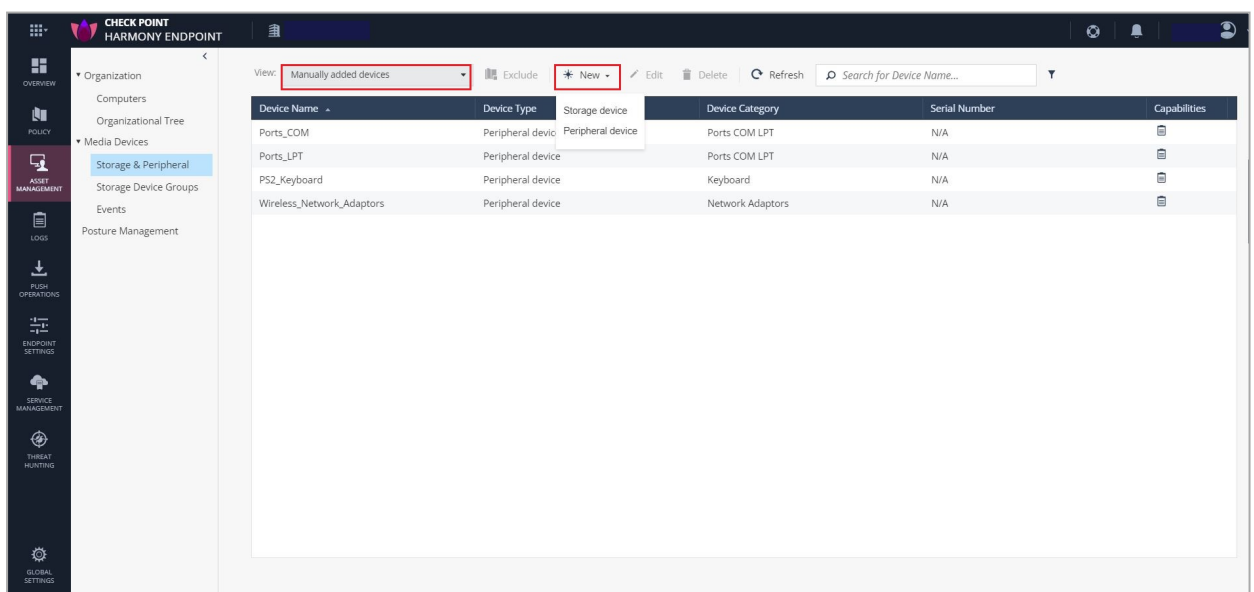
New devices are added manually or are automatically discovered by the Endpoint Server.

You can view **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.

Managing Storage and Peripheral Devices

To manually add a new device:

1. Click **Asset Management > Media Devices > Storage & Peripheral**.
2. From the **View** list, select **Manually added devices**.
3. Click .



4. Select :

■ Storage Device

The **New Storage Device** window appears.

The screenshot shows the 'NEW STORAGE DEVICE' window with a dark blue header and a sidebar. The sidebar contains a '1 EDIT DEVICE' button. The main content area is divided into sections: 'Device Information', 'Device ID Filter', and 'Supported Capabilities'. The 'Device Information' section includes fields for Name (Test), Connection Type (Internal), Category (DVD CD-ROM Drives), Serial Number (1234), and Extra Information (None). The 'Device ID Filter' section has a field for Device ID begins with. The 'Supported Capabilities' section has two checked checkboxes: 'Log device events' and 'Allow encryption'. A 'FINISH' button is located at the bottom right.

NEW STORAGE DEVICE

1 EDIT DEVICE

Device Information

Name:

Connection Type:

Category:

Serial Number:

Extra Information:

Device ID Filter

Device ID begins with:

Supported Capabilities

☒ Log device events

☒ Allow encryption

FINISH

■ Peripheral Device

The **New Peripheral Device** window appears.

The screenshot shows the 'NEW PERIPHERAL DEVICE' window. On the left is a dark blue sidebar with a button labeled '1 EDIT DEVICE'. The main content area is light gray and divided into sections. The 'Device Information' section includes: 'Name' (text box with 'test'), 'Applies to' (dropdown menu with 'Windows'), 'Connection Type' (dropdown menu with 'Unknown'), 'Category' (dropdown menu with 'Camera device'), 'Serial Number' (text box with '1234'), and 'Extra Information' (dropdown menu with 'Hard drive with Master Boot Record'). Below this is the 'Device ID Filter' section with 'Device ID begins with' (text box with 'www'). The 'Supported Capabilities' section has a checkbox labeled 'Log device events' which is checked. At the bottom right is a dark blue button labeled 'FINISH'.

5. Enter these:

- **Name** - Enter a unique device display name, which cannot contain spaces or special characters (except for the underscore and hyphen characters).
- **Applies to** - This setting is valid for peripheral devices only.
- **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 page 409](#).
- **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.

- **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).

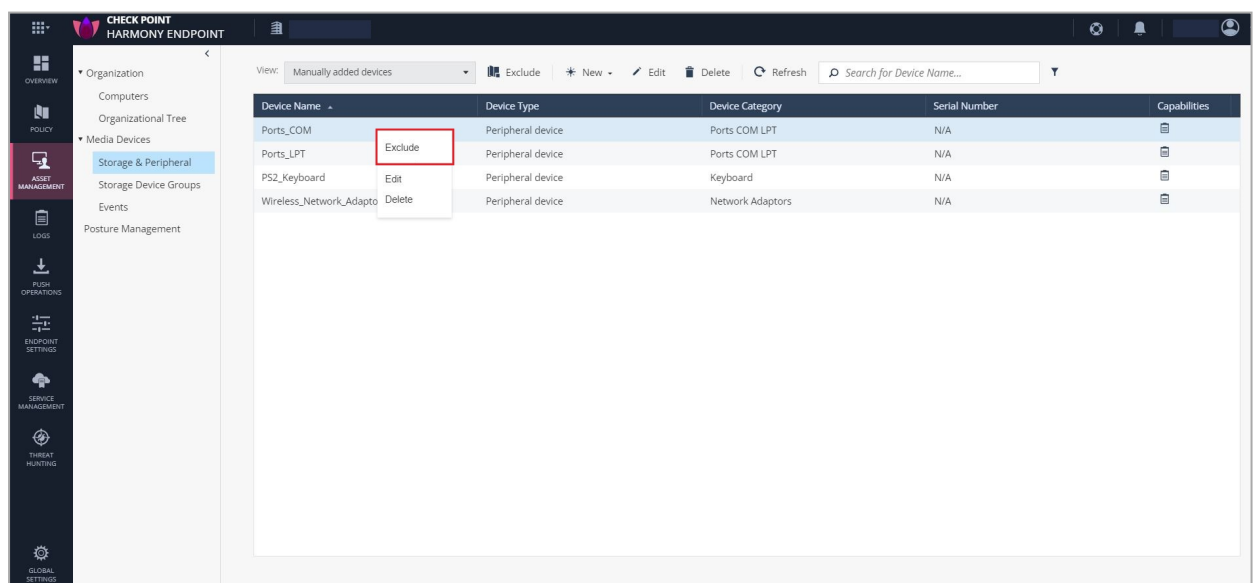
6. Assign Groups (relevant for storage devices only):

- To assign the device to an existing group, from the **existing group** list, select a group.
- To assign the device to a new group, in the **create a new group** field, enter the new group name.
- If you do not want to add the device to any group, select **do not add to group**.

7. Click **Finish**.

To add an exclusion to a device:

- Click **Asset Management > Media Devices > Storage & Peripheral**.
- Right-click the applicable device and select **Exclude**.



The **Device Override Settings** window appears.

3. Configure the required **Read Policy** and **Write Policy** (relevant to storage devices only). For more information on the configuration options, see ["Configuring the Read Action" on page 395](#) and ["Configuring the Write Action" on page 397](#)
4. **Define Behavior** (relevant for peripheral devices only):
 - a. From the **Rule(s)** list, select a rule.
 - b. From the **Access type** list, select **Accept** or **Block**.
 - c. From the **Log type** list, select a log.
 - d. Add details in the **Description** field.
5. Click **Finish**.

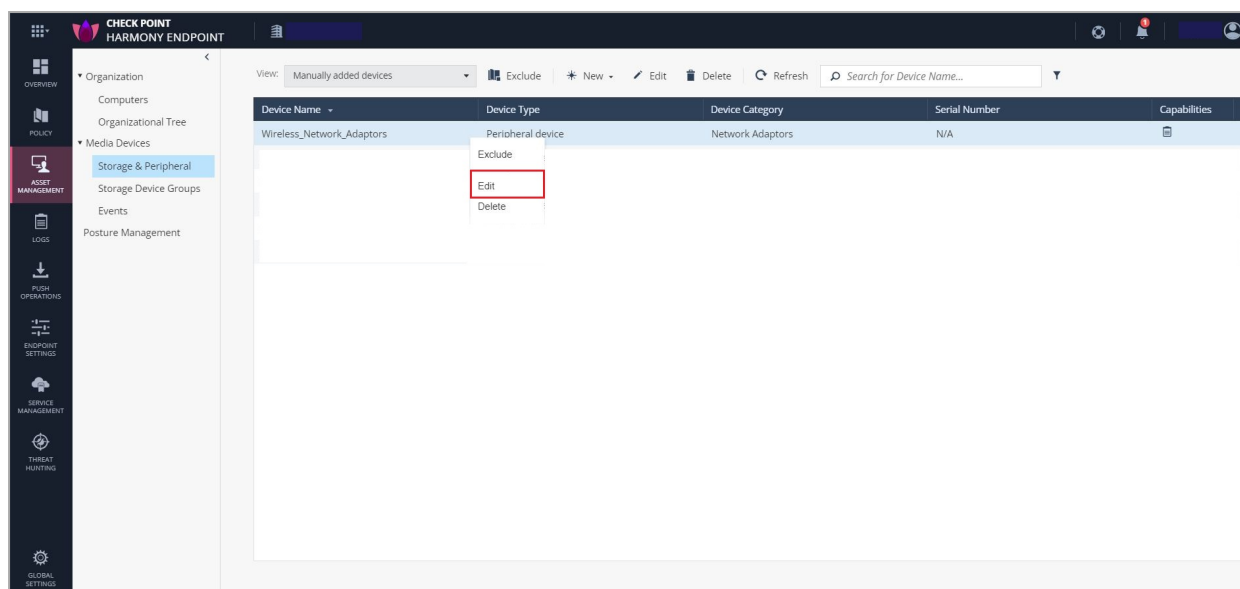


Note - If a device has an exclusion already in place, the new exclusion overrides an existing exclusion.

The **Discovered devices** view lists the details of the devices automatically discovered by the Endpoint server.

To edit a device:

1. Click **Asset Management > Media Devices > Storage & Peripheral**.
2. Right-click the applicable device and select **Edit**.



The **Edit Peripheral Device** window opens.

The 'EDIT PERIPHERAL DEVICE' window is shown with a dark sidebar on the left containing a '1 EDIT DEVICE' button. The main area is divided into sections:

- Device Information:** Includes fields for Name (set to 'Ports_COM'), Applies to (set to 'Windows'), Connection Type (set to 'Unknown'), Category (set to 'Ports COM LPT'), Serial Number (empty), and Extra Information (set to 'None').
- Device ID Filter:** Includes a field for Device ID begins with (set to 'COM').
- Supported Capabilities:** Includes a checked checkbox for 'Log device events'.

 A 'FINISH' button is located at the bottom right of the window.

3. Enter these:

- **Name** - Enter a unique device display name, which cannot contain spaces or special characters (except for the underscore and hyphen characters).
- **Applies to** - This setting is valid for peripheral devices only.

- **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 page 409](#).
- **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.
- **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):

- a. To assign the device to an existing group, from the **existing group** list, select a group.
- b. To assign the device to a new group, in the **create a new group** field, enter the new group name.
- c. If you do not want to add the device to any group, select **do not add to group**.

5. Configure the required **Read Policy** and **Write Policy** (relevant to storage devices only). For more information on the configuration options, see ["Configuring the Read Action" on page 395](#) and ["Configuring the Write Action" on page 397](#).

6. **Define Behavior** (relevant for peripheral devices only):

- a. From the **Rule(s)** list, select a rule.
- b. From the **Access type** list, select **Accept** or **Block**.
- c. From the **Log type** list, select a log.
- d. Add details in the **Description** field.

7. Click **Finish**.

Managing Storage Device 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.

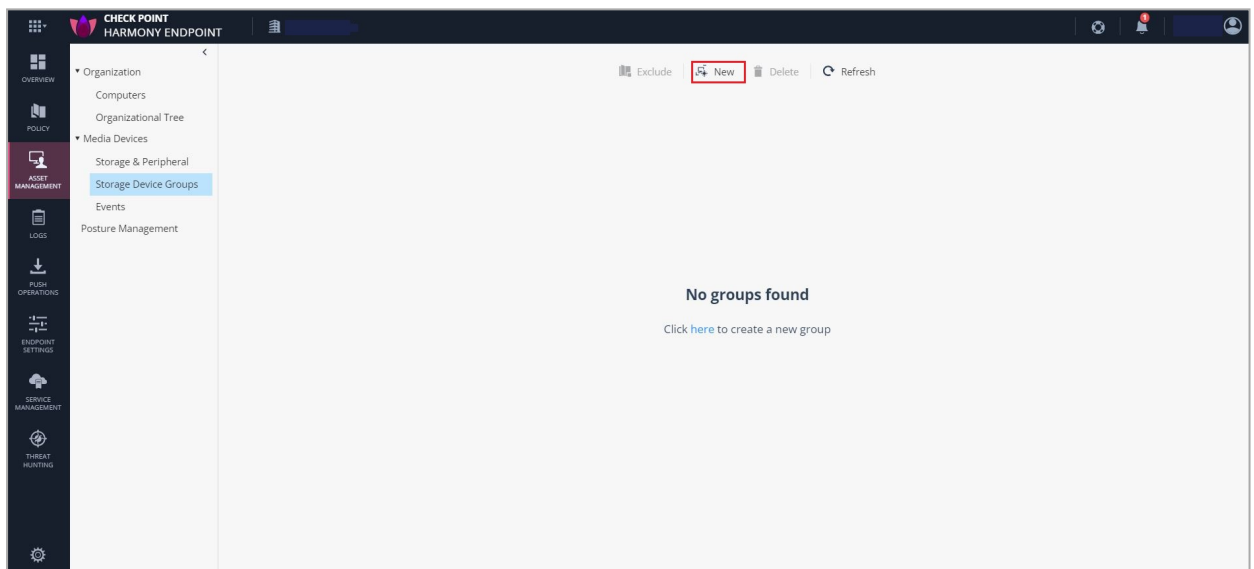
To create a new device group, or click **Asset Management > Media Devices > Storage Device Groups**. You can create new groups or edit existing groups.



Note - You cannot delete groups that are in use.

To create a Storage Device Group:

1. Click **Asset Management > Media Devices > Storage Device Groups**.
2. Click **New**.



The **Create Storage Device Group** window appears.

3. In the **Group Name** field, enter a name.
4. (Optional) In the **Comments** field, enter your comments.
For example, USB storage device.
5. To add devices to the group, click **+**.
6. Select the devices and click **OK**.
7. To delete the device, select the device and click **X**.

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

Viewing Events

Endpoint Security allows you to monitor activities related to storage and peripheral devices as events and if required, change the device details and status. For example, if a device that should be allowed was blocked and vice versa.

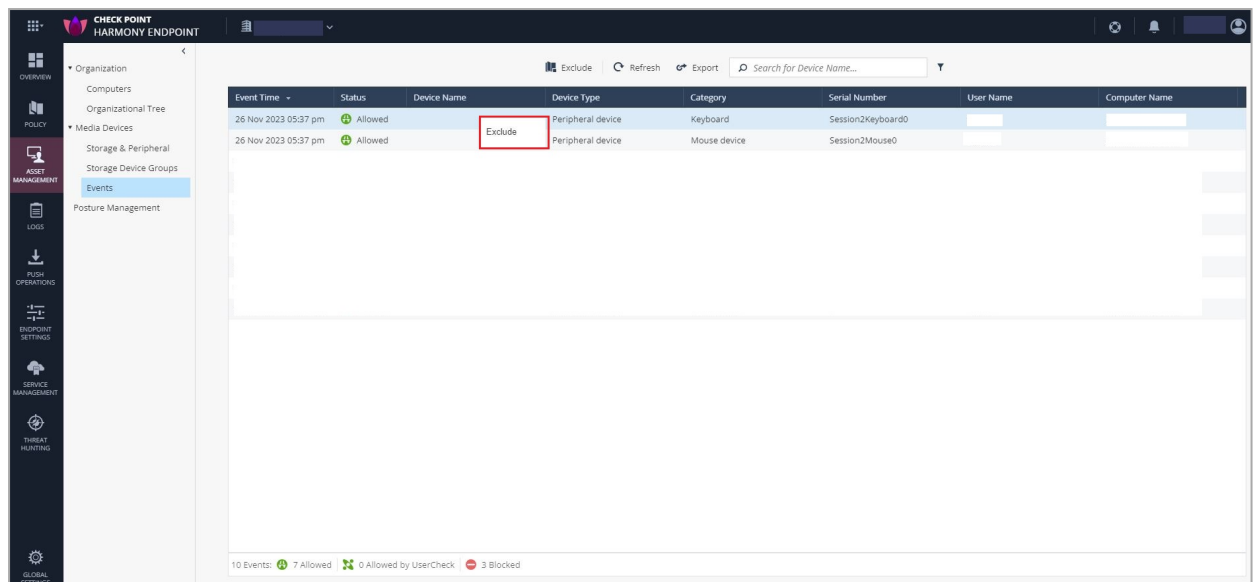
Event Time	Status	Device Name	Device Type	Category	Serial Number	User Name	Computer Name
26 Nov 2023 05:37 pm	Allowed		Peripheral device	Keyboard	Session2Keyboard0		
26 Nov 2023 05:37 pm	Allowed		Peripheral device	Mouse device	Session2Mouse0		

10 Events: 7 Allowed 0 Allowed by UserCheck 3 Blocked

Column	Description
Event Time	Date and time when the device was connected to the endpoint.
Status	Whether the device was blocked or allowed.
Device Name	Name of the device.
Device Type	Type of device.
Category	Category of the device.
Serial Number	Serial number of the device.
User Name	Name of the user.
Computer Name	Name of the computer.

To modify the device details and status:

1. Click **Asset Management > Media Devices > Events**.
2. Right-click the event and select **Exclude**.



The **Device Override Settings** window opens.

The screenshot shows the 'DEVICE OVERRIDE SETTINGS' window. On the left is a sidebar with two steps: '1 EDIT DEVICE' (active) and '2 DEFINE BEHAVIOR'. The main area contains the following fields:

- Device Information**
 - Name:
 - Applies to:
 - Connection Type:
 - Category:
 - Serial Number:
 - Extra Information:
- Device ID Filter**
 - Device ID begins with:
- Supported Capabilities**
 - ☒ Log device events

A 'NEXT' button is located at the bottom right.

3. Enter these:

- **Name** - Enter a unique device display name, which cannot contain spaces or special characters (except for the underscore and hyphen characters).
- **Applies to** - This setting is valid for peripheral devices only.
- **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 page 409](#).
- **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.
- **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):

- a. To assign the device to an existing group, from the **existing group** list, select a group.
- b. To assign the device to a new group, in the **create a new group** field, enter the new group name.
- c. If you do not want to add the device to any group, select **do not add to group**.

5. Configure the required **Read Policy** and **Write Policy** (relevant to storage devices only). For more information on the configuration options, see ["Configuring the Read Action" on page 395](#) and ["Configuring the Write Action" on page 397](#).

6. **Define Behavior** (relevant for peripheral devices only):

- a. From the **Rule(s)** list, select a rule.
 - b. From the **Access type** list, select **Accept** or **Block**.
 - c. From the **Log type** list, select a log.
 - d. Add details in the **Description** field.
7. Click **Finish**.

The screenshot shows a 'DEVICE OVERRIDE SETTINGS' dialog box with a dark blue header and a light gray body. On the left, a dark blue sidebar contains two steps: '1 EDIT DEVICE' (marked with a checkmark) and '2 DEFINE BEHAVIOR' (marked with a '2'). The main area is titled 'Behavior for device test'. It contains a 'Rule(s)' field with a search bar containing 'Default Full Disk Encryption settings for the entire organization'. Below this are two dropdown menus: 'Access type' set to 'Allow' (with a green plus icon) and 'Log type' set to 'Log' (with a document icon). A 'Description' text area is below the dropdowns. At the bottom right, there are 'BACK' and 'FINISH' buttons.

DEVICE OVERRIDE SETTINGS

Behavior for device test

Rule(s)

Default Full Disk Encryption settings for the entire organization x x Q

Access type

Allow

Log type

Log

Description

BACK FINISH

Advanced Settings for Media Encryption

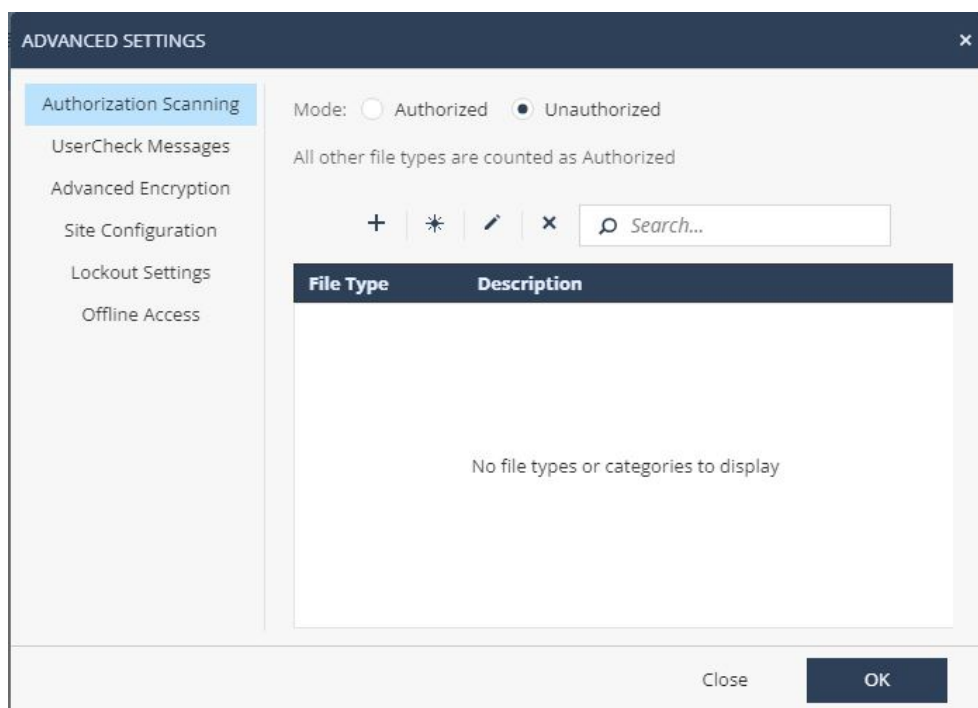
Authorization Scanning

In **Advanced Settings > Authorization Scanning**, you can specify authorized and unauthorized file types for scanning. The authorized and unauthorized scan configures the file types that you can allow and block.

To specify the file types:

1. Select the scan mode:

- **Authorized**
- **Unauthorized**



2. To add a file type:

- a. Click **+**.

The **Add a File Type or Category** window appears.

- b. From the drop down, select a file type or category.
- c. Click **OK**.

3. To create a new file type:

- a. Click *****.

The **File type Add / Edit** window appears.

b. Enter the **Name**, **Comments** and **File Extension**.

c. To add a File Signature:

i. Click  .

The **Add new file signature** window appears.

ii. Select the **Offset**.

iii. In the **Signature** field, enter the file signature.

iv. Click **OK**.

v. To delete a **File Signature**, select the file signature and click  .

d. Click **OK**.

4. To edit a file, select the file and click  .

5. To delete a file, select the file and click  .

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.

Enabling the UserCheck messages

Select the checkbox to enable the UserCheck message:

- Suggest to encrypt device when encryption is not mandatory
- Suggest to encrypt device in order to get write access when inserting
- Suggest to encrypt device in order to get write access when writing
- Notify user that device has been blocked
- Notify user that device has read only access
- Notify when encrypting business related data

Customizing the UserCheck messages

You can customize UserCheck messages including the title, notification message, replacement text for the OK and Cancel buttons and also present them in multiple languages.

To customize the UserCheck messages:

1. Click **Edit** for the particular UserCheck message you need to customize.
 2. Customize the message:
 - **Message languages** - Select multiple languages to add messages in different languages.
 - **Edit language** - Select the language to modify the message for the selected language.
 - **Title** - Edit the title of the notification.
 - **Main text** - Edit the text of the notification.
 - **Body text** - Edit the text of the notification.
 - **OK button** - Modify the UI text for the OK button.
 - **Cancel button** - Modify the UI text for the Cancel button.
 - **More button** - Modify the UI text for the More options button.
-  **Note** - UserCheck messages asking justification for copying the files additionally include:
- **Check box** - Modify the UI text for the check box.
 - **Notes** - Edit the text of notes.
 - **Justification** - Edit the text of the justification.
 - **Warning** - Edit the warning text.
3. Click **OK**.

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.

Media Log

The **Media Log** setting defines when Media Encryption & Port Protection creates log entries when a storage device is attached to an endpoint computer. You can select one of these predefined log actions:

Action	Description
Do not log security events	Disable all log entries.
Log only critical events	Create log entries only for events that are classified as critical.
Log critical and security events	Create log entries only for events that are classified as critical or security events.
Log all events	Create log entries for all events.

You cannot define custom log actions.

This table shows the applicable Media Encryption & Port Protection events and their severity classification.

Event ID	Description	Classification
3	Policy update completed successfully	Low
7	Device authorization successful	Low
8	Device authorization failed	Critical
11	Device access is blocked when attached to the endpoint computer	Critical
15	Encrypted storage created successfully	Low
16	Encrypted storage device removed	Critical
20	Device is attached to an endpoint computer and access is allowed	Security
21	A user follows the Ask User procedure to override a rule	Critical
22	A users does not follow the Ask User procedure to override a rule	Critical
23	A storage device file operation is blocked	Critical
24	A storage device file operation is allowed	Security

You can define different log settings for ["Managing Devices" on page 401](#).

Log entries are initially stored on client computers and then uploaded to the server at predefined intervals.

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.

Lockout Settings

You can configure Media Encryption & Port Protection in the **Lockout Settings** to lock a device after a specified number of unsuccessful log in attempts.

To configure lockout settings:

1. Select **Lock storage device after failed authentication attempts**.
2. To lock the storage device temporarily:
 - a. Select **Temporarily lock device**.
 - b. In the **Temporarily lock device after authentication failed** field, enter the failed log in attempts after which the system should lock the device.



Notes:

- If a device is locked temporarily, users can try to authenticate again after the specified time.
- A temporary lock only occurs when its value is less than the permanent lock.

3. To lock the storage device permanently:
 - a. Select **Permanently lock device**.
 - b. In the **Permanently lock device after authentication failed** field, enter the failed log in attempts after which the system should permanently lock the device. This should be greater than the value specified in **Temporarily lock device after authentication failed** field.



Note - If the device is locked permanently, users can request to unlock through Remote Help. For more information, see ["Media Encryption Remote Help" on page 422](#).

4. In the **Duration for temporary storage device lock** field, enter the duration after the failed log in attempts the system should unlock the device.

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.

Password Constraints

You can specify the password requirements for users to follow to log in to the device.

To configure the password constraints, select one of these:

- **Use Windows Complexity Requirements**
- **Use Custom Requirements**
 - Consecutive identical characters are not allowed
 - Require special characters
 - Require digits
 - Require lower case characters
 - Require upper case characters
 - Password must not contain user name or full name
 - In the **Minimum length of password** field, enter the number of characters required in the password. The minimum supported length is four characters.

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.



Note - Remote Help does not support drives that are encrypted by non-domain users.

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

1. Go to **Asset Management > Organization > Computers**.
2. Click  and select **Remote Help & Recovery > Media Encryption**.

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

3. Do these:
 - 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**.
2. From the **Port Protection Policy** list:

- To allow all the devices, select **Allow all**.
- To allow only essential devices, select **Allow essential**.

- The essential ports for Windows are:

- Smart Card Readers
- Keyboard
- Network Adaptors
- Modems
- Mouse

- The essential ports for macOS are:



Note - The device names of macOS ports are prefixed with "MAC_".

- USB Network
- USB Video
- USB HID
- USB Health
- USB Audio
- USB Wireless controller
- USB SmartCard (Supported only with the Endpoint Security Client version E86.20 and higher.)
- Bluetooth Audio
- Bluetooth Computer
- Bluetooth Health
- Bluetooth HID
- Bluetooth Imaging
- Bluetooth Phone
- Bluetooth Toy
- Bluetooth Wearable
- Printers

- To customize device settings, click **Custom** and then click **Edit**.

3. Click **New**.

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

4. Select a device from the list or click **New** to create a new device (see [Managing Devices](#) for details on how to create a new device).
5. Select the **Access Type** from the list:
 - **Accept** - Allow connecting the peripheral device.
 - **Block** - Do not allow connecting the peripheral device.
6. 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.
7. Click **Create**.

To import exclusions:

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

1. In the **Port Protection** tab, select the **Port Protection Policy**.
2. Click **Edit**.
3. Click **Import** and select the JSON file.

To export exclusions:

1. In the **Port Protection** tab, select the **Port Protection Policy**.
2. Click **Edit**.
3. Select the device that you want to export from the list.
4. Click **Export**.

Device Category Descriptions for Windows

The following table describes each device category available in the Port Protection policy.

Category	Type of Devices
Printers_USB	Printers
Windows_CE_Devices_USB	Legacy Windows CE Device

Category	Type of Devices
Bluetooth 2	Legacy Bluetooth device
Bluetooth Radio	Bluetooth devices
PCMCIA_Memory	Memory devices such as flash memory cards.
Bluetooth	Legacy Bluetooth device
USB_Controllers	USB host controllers and USB hubs
Keyboard	Keyboards
Floppy_disks	Floppy disk
Network_Adaptors	Network adapters
Infrared Devices	Infrared devices
Tape Drives	Tape drives including all tape miniclass drivers.
Camera device	Web cameras
Palm_OS_Devices_USB	Legacy Palm devices
Modems	Modem devices
Still_image_devices	Scanner devices
Mouse device	Mouse
Bluetooth Devices	Legacy Bluetooth
Smart_Card_Readers	Smart Card readers
Firewire IEEE_1394	1394 host controllers connected on a PCI bus, but not 1394 peripherals.
Ports COM_LPT	Serial and parallel port devices.

Category	Type of Devices
IEEE_1284.4_printers	Dot4 printer device
Bluetooth_USB	Legacy Bluetooth
SAMSUNG_Android_Debug_Bridge	Devices on Android debug Bridge

Media Encryption Access Rules

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 > **Data Protection** > **Access Rules** > **Preset** > click the list menu. 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 is 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. 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.
2. 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" on page 431*
 - *"Configuring Security Zones" on page 432*
 - *"Configuring Firewall Rule Advanced Settings" on page 434*
- *"Application Control" on page 443*
 - *"Creating the List of Applications on the Reference Device" on page 444*
 - *"Uploading the Appscan XML File to the Endpoint Security Management Server" on page 448*
 - *"Configuring Application Permissions in the Application Control Policy" on page 449*
 - *"Disabling or Enabling Windows Subsystem for Linux (WSL)" on page 453*
- *"Developer Protection" on page 454*
- *"Compliance" on page 456*
 - *"Planning for Compliance Rules" on page 457*
 - *"Configuring Compliance Policy Rules" on page 458*
 - *"Monitoring Compliance States" on page 475*

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 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 & Compliance**.
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](#).

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, Endpoint Security 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 & Compliance**.
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**.

Managing Firewall Objects and Groups

Objects defined in Endpoint Security and stored in the object database, represent physical and virtual network components (such as Endpoint devices and servers), and logical components (such as IP address ranges). You can create new objects to be used in the policy.

Supported Object Categories

Endpoint Security supports the object categories described below.

Hosts

A host can have multiple interfaces, but no routing takes place. It is an Endpoint device that receives traffic for itself through its interfaces. (In comparison, a Security Gateway routes traffic between its multiple interfaces). For example, if you have two unconnected networks that share a common Endpoint Security Management Server and a Log Server, configure the common server as a host object.

A host has no routing mechanism, it is not capable of IP forwarding, and cannot be used to implement Anti-Spoofing.

The Endpoint Security Management Server object is a host.

Enter these properties data to define a host

- **Name** - A name for the host. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited
- **IPv4** and/or **IPv6** addresses of the host you want to use.
- **Description** (Optional) - A description of the host object.

Networks

A network is a group of IP addresses defined by a network address and a net mask. The net mask indicates the size of the network.

A Broadcast IP address is an IP address which is destined for all hosts on the specified network. If this address is included, the Broadcast IP address is considered as part of the network.

Enter these properties to define a network:

- **Name** - A name for the network. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
- **Network Address (IPv4)** and **Netmask (IPv4)** of the network object you want to use.
or
Network Address (IPv6) and **Prefix (IPv6)** of the network object you want to use.
- **Description** (optional)- A description of the network object.

Network Groups

A network group is a collection of hosts, networks, or other groups. The use of groups facilitates and simplifies network management. When you have the same set of objects which you want to use in different places in the Rule Base, you can create a group to include such set of objects and reuse it. Modifications are applied to the group instead of to each member of the group.

Groups are also used where Endpoint Security lets you select only one object, but you need to work with more than one.

Enter these properties to define a network group object:

- **Name** - A name for the network object. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited
- Click the + icon to add the required objects to your group.
- **Description (Optional)** - A description of the group.

Domains and Domain Groups

A Domain object lets you define a host or a DNS domain by its name only. It is not necessary to have the IP address of the site. You can use the Domain object in the source and destination columns of the Firewall Policy.

Enter these properties to define a Domain:

- **Name** - A name for the Domain. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
- **Host name** - Use the Fully Qualified Domain Name (FQDN).

Sub-sites must be added separately, if you want to apply the rule to them as well. Wildcard symbols like * are not allowed. Non-Qualified Domain Names are not supported.

 **Note** - The DNS resolution is executed only once the policy is applied, or following a reboot.

- **Description (Optional)** - A description of the Domain or Domain group object.

Enter these properties to define a Domain group:

- **Name** - A name for the Domain. The name must start with a letter and can include capital and small letters, numbers and '_'. All other characters are prohibited.
- Click the + icon to add the required Domains to the Domain group.
- **Description** - A description of the Domain group

Address Ranges

An address range is a range of IP addresses on the network, defined by the lowest and the highest IP addresses. Use an Address Range object when you cannot define a range of IP addresses by a network IP and a net mask. The Address Range objects are also necessary for the implementation of NAT and VPN.

Enter these properties to define an address range object:

- **Name**
- **From IP address (IPv4) - To IP address (IPv4)** - First and last IPv4 addresses of the range.

or

From IP address (IPv6) - To IP address (IPv6) - First and last IPv6 addresses of the range.
- **Description (Optional)** - A description of the address range.

Security Zones

See ["Configuring Security Zones" on page 432](#).

Services and Service Groups

Data transmission services, such as UDP and TCP.

The Endpoint identifies (matches) a service according to IP protocol, TCP and UDP port number, and protocol signature.

Creating Objects

Create objects for areas that programs must have access to, or areas that programs must be prevented from accessing.

Configure objects for each policy or define objects before you create a policy. After you configure an object, you can use again it in other policies.

To create an object:

1. In the **Access** view, go to **Manage > Manage Firewall Objects > Manage Objects and Groups**

(or, in the in the **Access** view > go to **Edit Inbound/Outbound Rule Base**).

The **Manage Objects and Groups** window opens.

2. Click this icon: 
3. Configure the relevant properties and click **OK**.

When you create a new network object, the name must start with a letter and can include capital and small letters, numbers and "_ / -". All other characters are prohibited.

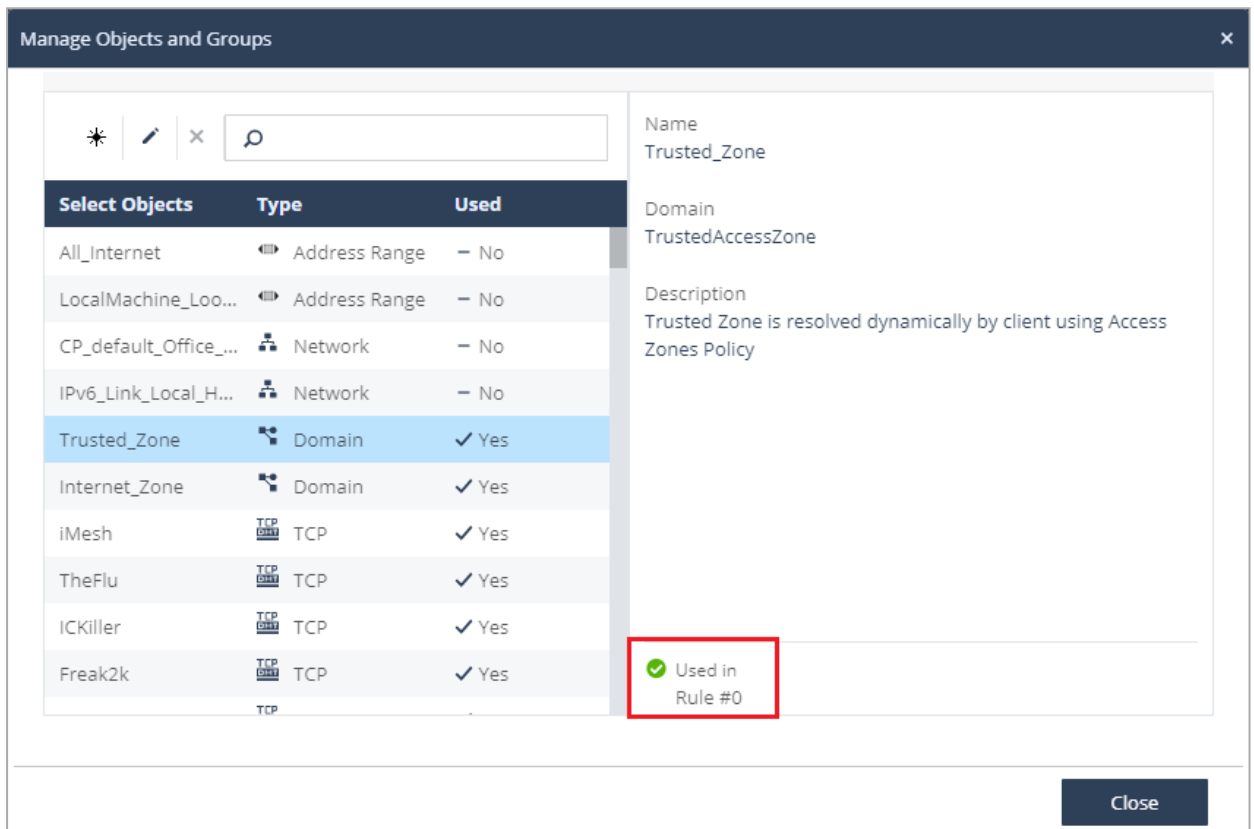
Used In

You can check in which rule each object is used.

To check in which rule an object is used:

1. In the **Access** view, go to **Manage > Manage Firewall Objects > Manage Objects and Groups**.
2. Select the object and look at the right corner of the window to see the rules in which the object is used.

For example:



The screenshot shows the 'Manage Objects and Groups' window. On the left, a table lists various objects. The 'Trusted_Zone' object is selected, and its details are displayed on the right. A red box highlights the 'Used in Rule #0' status.

Select Objects	Type	Used
All_Internet	Address Range	No
LocalMachine_Loo...	Address Range	No
CP_default_Office_...	Network	No
IPv6_Link_Local_H...	Network	No
Trusted_Zone	Domain	Yes
Internet_Zone	Domain	Yes
iMesh	TCP	Yes
TheFlu	TCP	Yes
ICKiller	TCP	Yes
Freak2k	TCP	Yes

Details for **Trusted_Zone**:

- Name: Trusted_Zone
- Domain: TrustedAccessZone
- Description: Trusted Zone is resolved dynamically by client using Access Zones Policy
- Used in Rule #0

Close

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:

Configuring Application Control in Windows

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.
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.
3. [Upload the Appscan XML file](#) to the Endpoint Security Management Server using Endpoint Security.
4. [Configure the action for each application in the Application Control policy](#). You can configure which applications are allowed, blocked, or terminated.
5. Install policy.

Configuring Application Control in macOS

1. Run the **Application Scan Push Operation**. See *"Performing Push Operations (Old User Interface)" on page 580*.
2. [Configure the action for each application in the Application Control policy](#). You can configure which applications are allowed, blocked, or terminated.
3. 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.

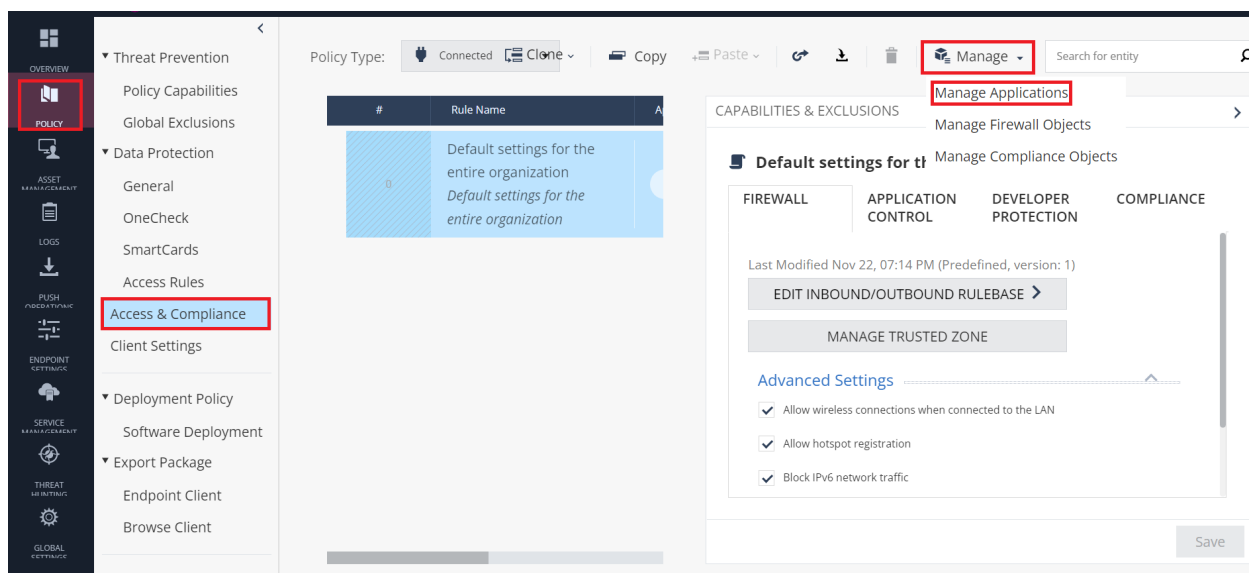


Important - The reference device must be free of malware.

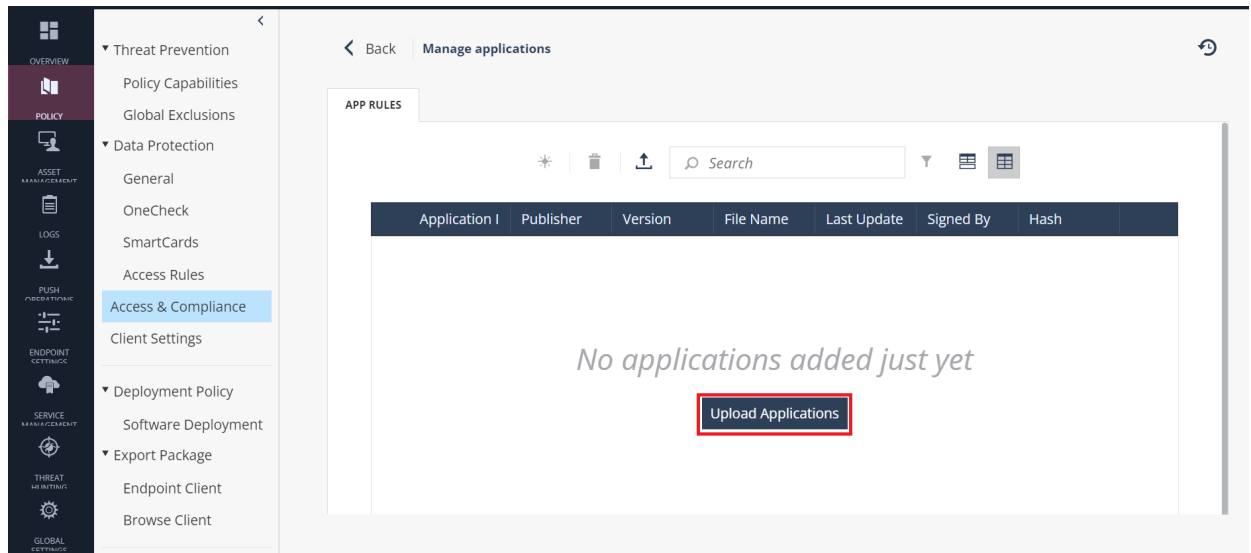
To generate the list of applications, run the `Appscan` command on the reference device. This generates an XML file that contains the details of all the applications and operating system files on the device. In the XML file, each application, and each application version, is uniquely identified by a 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**.

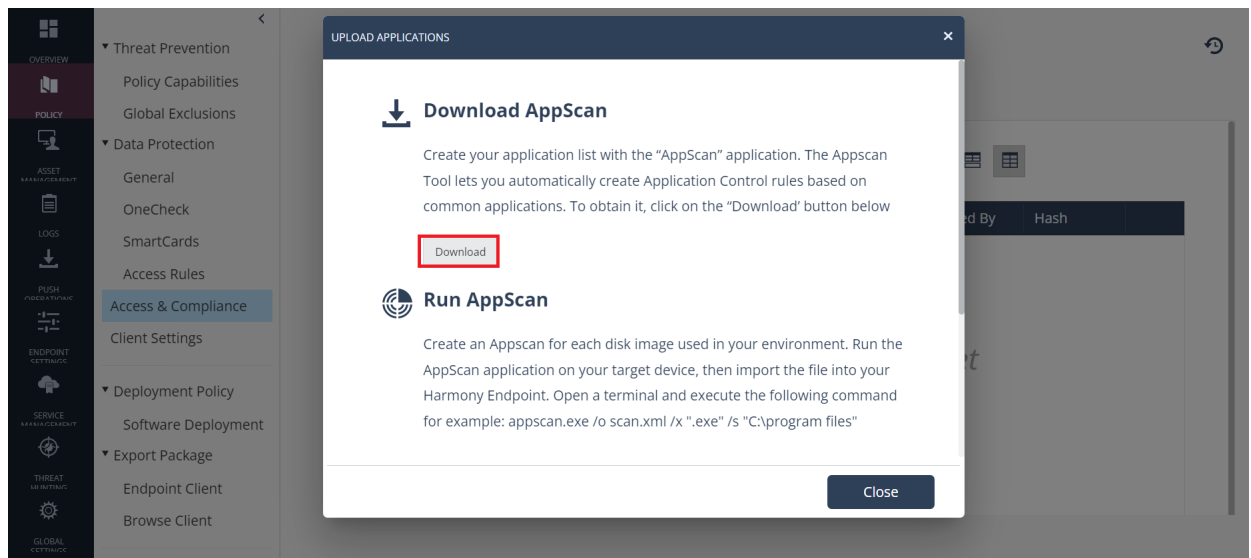


2. Under **Manage Applications**, click **Upload Applications**.



The Upload Applications window appears.

- Under Download Appscan, click Download.



- 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

```
C:\>Appscan [/o <filename> /s <target directory> /x <extension
string> /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.
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

- `C:\>appscan /o scan1.xml`

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

- `C:\>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.

- `C:\>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.

- `C:\>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.



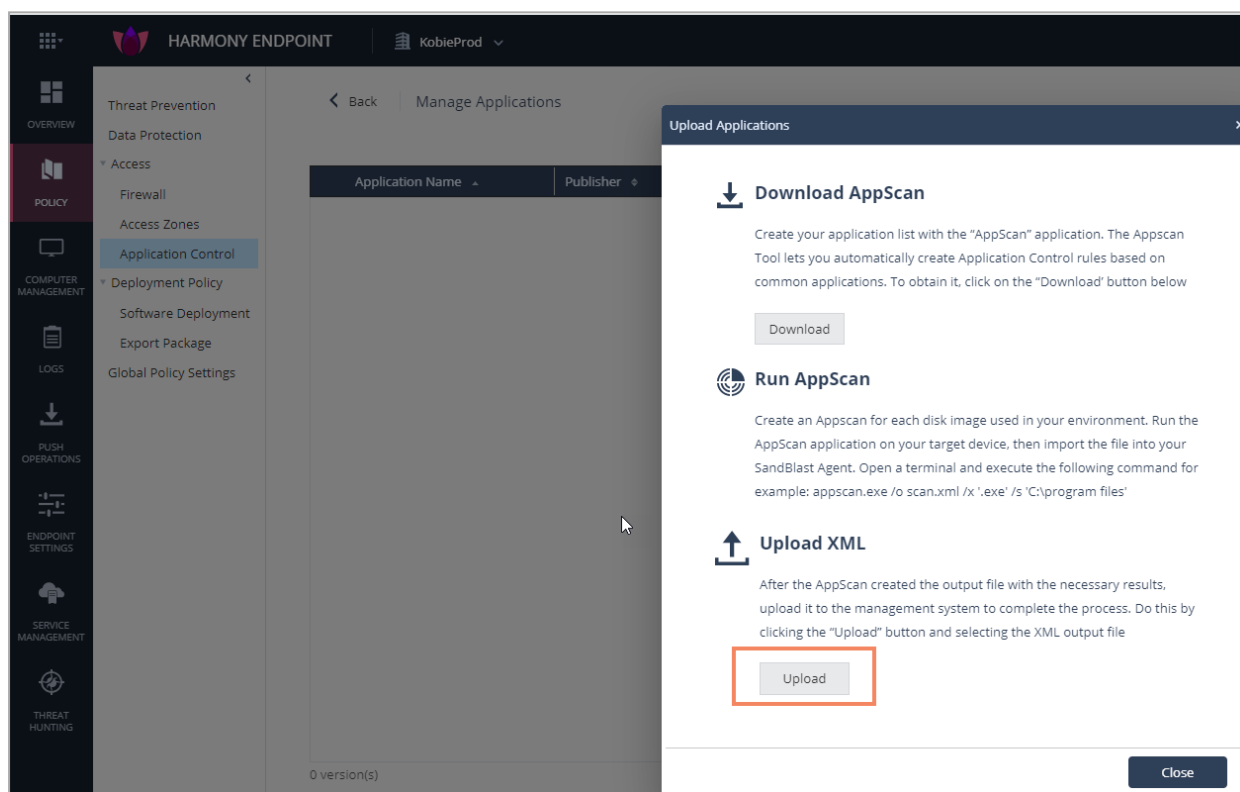
Note - Before you upload the Appscan XML file, remove all special characters, such as trademarks or copyright symbols, from the Appscan XML

To upload the Appscan XML file:

1. In the **Policy** view, go to **Access and Compliance > 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.

Depending on whether the application is secure or not, you can set the **Action** (network access) to **Allow**, **Block** or **Terminate**:

- For each application in the Application Control policy.
- For specific applications that match the wildcard character supported string in its name, publisher, version and so on.

Supported Actions

The supported actions for the applications are:

Action	Description
Allow	Allows network access to the application.
Block	Blocks network access to the application.
Terminate	Terminates the application if it tries to access the network or immediately when it runs.

To configure terminate settings:

1. In the **Policy** view, go to **Access and Compliance > 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

App Rules

To review the policy for each application and its versions:

1. In the **Policy** view, go to **Access and Compliance > Application Control > Application Management > Edit Application Control Policy**.
2. Click **App Rules**.

The **Action** column shows the permission for each application. Left-click the **Action** column to select the action.

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.

Custom Rules

 **Note** - The Custom Rules feature is supported only on the Windows client.

To review the policy for specific applications:

1. In the **Policy** view, go to **Access and Compliance > Application Control > Application Management > Edit Application Control Policy**.
2. Click **Custom Rules**.
3. Click **New**.
4. Enter a **Rule Name**.
5. Enter at least one of these details:

Notes:

- Use the wildcard character (*) to match a specific string.
 - Enter ***abc*** to apply the [rule](#) for all applications that contain the string **abc** in its details. For example, ***abc*** matches **abc**, **xyzabc**, **abcxyz**, **xyzabcxyz**.
 - Enter ***abc** to apply the [rule](#) for all applications ending with the string **abc** in its details. For example, ***abc** matches **abc**, **xyzabc**.
 - Enter **abc*** to apply the [rule](#) for all applications starting with the string **abc** in its details. For example, **abc*** matches **abc**, **abcxyz**.
- Enter **abc** to apply the [rule](#) for all applications that contain only the string **abc** in its details. For example, **abc** matches **abc**.
- A rule is considered **True** only when all **non-empty fields** evaluate to **True**, applying a **logical AND** across those fields.
- **Application Name**

For example, the application name of Chrome is **Google Chrome**.

To find the application name of Chrome, on a Windows PC, navigate to *C:\Program Files\Google\Chrome\Application*, right-click **chrome** and click **Properties**. Click the **Details** tab and see **Product name**.

■ Publisher

For example, the publisher of Chrome is **Google LLC**.

To find the publisher of Chrome, on a Windows PC, navigate to *C:\Program Files\Google\Chrome\Application* and see the name listed under the **Company** column for **chrome**.

■ Version

For example, the version of Chrome is **107.0.5304.107**.

To find the version of Chrome, on a Windows PC, navigate to *C:\Program Files\Google\Chrome\Application*, right-click **chrome** and click **Properties**. Click the **Details** tab and see **File version**.

■ File Name

For example, the file name of Chrome is **chrome.exe**.

To find the file name of Chrome, on a Windows PC, navigate to *C:\Program Files\Google\Chrome\Application*.



Note - Do not enter the path or directory to the file.

■ Issued By

For example, the issuer of Chrome is **DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1**.

To find the certificate issuer for Chrome, on a Windows PC:

- a. Navigate to *C:\Program Files\Google\Chrome\Application*.
- b. Right-click **chrome** and click **Properties**.
- c. Click the **Digital Signatures** tab.
- d. In the **General** tab, click **View Certificate** and see **Issued by**.



Note:

- If the file has several signatures, the Endpoint Security client checks all the signatures and applies the rule only if anyone of the signatures match the specified signature.
- Only certificates with [printable ASCII characters](#) are supported.

■ Issued To

For example, the issued to for Chrome is **Google LLC**.

To find the certificate issued to for Chrome, on a Windows PC:

- a. Navigate to *C:\Program Files\Google\Chrome\Application*.
- b. Right-click **chrome** and click **Properties**.
- c. Click the **Digital Signatures** tab.
- d. Click **Details**.
- e. In the **General** tab, click **View Certificate** and see **Issued to**.



Notes:

- If the file has several signatures, the Endpoint Security client checks all the signatures and applies the rule only if at least one of the signatures match the specified signature.
- Only certificates with [printable ASCII characters](#) are supported.

■ Command Line

For example, the command line of Chrome is *C:\Program Files\Google\ChromeApplication\chrome.exe*.

To find the command line for Chrome, on a Windows PC, open **Task Manager**. Click the **Details** tab and see the **Command line** column for the **chrome.exe**. If the **Command line** column is not visible in the table, right-click the header row, click **Select columns** and select **Command line** checkbox.

6. To review the policy for an application with specific Hash:

- In the **Hash** field, enter the MD5 hash key of the application.
- Click **Calculate** and select the binary file of the application. The system automatically retrieves the hash and enters it in the **Hash** field.

7. Click **OK**.

8. Left-click the **Action** column to select the 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 and Compliance > Application Control > Windows Sub-systems for Linux (WSL) Traffic**
2. Select **Allow Windows Sub-systems 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 the Git repository. It prevents to upload the private information in plain text and vulnerable dependencies from Endpoint Security client computers to public locations.

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

To configure Developer Protection:

1. Access the Endpoint Security 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 <i>Detect</i> 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 <i>Prevent</i> 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 <code>.gitignore</code>, or updating the version in <code>package.json</code>

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 Endpoint Security 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 478](#)*.

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:

 **Note** - Multiple checks can be added to a single rule. A rule is considered successful if at least one of its checks succeeds.

- **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 <i>about to be restricted</i> state. On the monitoring tab, the user is shown as <i>pre-restricted</i> .

- 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 463*.
- c. Select an **Action** from the list.
- d. Click the **Remediation** tab to add Remediation objects to the *"Compliance Remediation Objects" on page 467*. 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: <code>HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint Security\Compliance\Log4jScan</code> 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 least 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 <i>WinRAR</i> 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: <code>file://\<IP ADDRESS>/...../<file name></code> - Using local file: <code>file://C:\path\to\file.exe</code> - 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 461](#).

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 updates 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**.

Detecting Common Vulnerabilities and Exposures

With Endpoint Security, you can perform custom scans on endpoints for Common Vulnerabilities and Exposures (CVE) in applications.



Notes:

- Supported only for Windows and macOS-based endpoints.
- Supported with the Endpoint Security client version E87.30 and higher.

Configuring Posture Assessment Settings

Endpoint Security periodically scans endpoints against the list of applications specified on the signature server and detects vulnerable CVEs in applications.



To configure the Posture Assessment Settings:

1. Go to **Policy > Access & Compliance**.
2. In the Capabilities & Exclusions pane on the right, click the **Compliance & Posture** tab.
3. Scroll-down to **Posture Assessment Settings**.
4. Select the **Enable Vulnerability assessment** checkbox.
5. Select the scan type:

- To manually start the scan, click **Manual**.



Note - To start the scan for the first time:

- a. Go to **Asset Management > Computers**.
- b. Select the devices for which you want to scan.
- c. Right-click and select **Vulnerabilities > Scan Now**.

You can start subsequent manual scans by clicking **Scan Now** in **Asset Management > Posture Management** or by using the **Run Diagnostics** push operation.

- To automatically start the scan, click **Automated** and specify the **Interval** (**Weekly** or **Monthly**), **at** (time) and **every** (frequency in days).
6. Under **Update server type**, select the signature server:
 - **External Check Point Signature Server**
 - **Other External Source**
 - Under **Path**, enter the URL of the external source.
 7. To enforce the patch updates and reboot the endpoint immediately, select the **Enable patch updates & reboot enforcement** checkbox. To apply patch manually, see ["Applying the Patch for CVEs" on page 231](#).

- To allow users to postpone patch updates, specify **Max user delay in patch update** and **Force patch update after** in hours or days.

8. To enforce the patch updates, select the **Enable patch updates** checkbox:



Note - To apply patch manually, see ["Applying the Patch for CVEs" on page 231](#).

- To allow users to postpone patch updates, select the **Enable patch updates & reboot enforcement** checkbox and specify **Max user delay in patch update** and **Force patch update after** in hours or days.
- To enable automatic patch updates, click **Advanced Settings** and select the **Enable automated patch management** checkbox:



Note - This is supported only with Endpoint Security Client version E88.20 and higher.

- To specify the interval for patch updates, from the **Set automated patch on** list, select **Interval**, **Weekly** or **Monthly** and specify the interval.
- In the **Applications** section, specify the application to which you want to apply the patch and select:
 - **All applications**
 - **Select specific applications**. Search and select one or more applications.
- In the **Severities** section, specify the severities to which you want to apply the patch and select:
 - **All Severities**
 - **Select specific severity**. Search and select one or more severities.
- To exclude an application from applying the patch, in the **Exclude applications** section, search and select one or more applications.

9. Click **Save**.

10. At the top, click **Install Policy**.

After you enable Posture Assessment settings and install the policy, you can view the detected CVE and its CVSS score in the Viewing Endpoint Posture .

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 461](#).

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.`

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 Endpoint Security 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 Check Point 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.

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 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 cannot connect with its management server either the on-premises Endpoint Security Management Server or the Endpoint Security (EPMaaS). In this state, the client is temporarily disconnected from management and continues to enforce the last locally cached policy.

Disconnection can happen for several reasons, including:

- Loss of internet connectivity
- Network restrictions such as firewalls, proxy rules, or VPN configurations
- Captive portals or authentication gateways
- Scenarios where the device is connected to internal resources but cannot reach the management service

Use the Disconnected state rule to define how endpoints behave when they are unable to access their management service.

- **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		

Policy Operation

The new policy operation mode allows greater flexibility to the user by providing 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 Model

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

Data Loss Prevention

Data Loss Prevention (DLP) detects and prevents unauthorized transmission of confidential information, such as social security numbers, credit card numbers, bank account numbers and so on.

Browser-Based DLP capabilities allow you to enforce DLP by associating data types with a DLP rule.

In the Data Loss Prevention tab, you can set rules based on specific events, data types and actions.

These actions are available within the DLP rules:

- **Detect** - Performs the DLP scan but does not block the data.
- **Prevent** - Performs the DLP scan and prevents data transfer if it finds a match to a data type.
- **Allow** - Acts as exclusions, allowing data transfer in certain events.
- **Block** - Blocks the data without the DLP scan.
- **Ask** - Asks the user to provide justification before allowing data transfer based on the DLP scan results.
- **Redact** - Performs a DLP scan and removes sensitive data based on a pre-defined set of Data Types. This action is available only for the **Text-control** category.
 - **Force redact** - Automatically replaces sensitive data with asterisk.

The Data Loss Prevention policy allows the administrators to enable the **Gen AI Protect** feature on the endpoints. Gen AI Protect monitors the use of various generative AI applications by the endpoints. It detects and prevents the sharing of potential confidential information in the prompts to any Gen AI tools by the Endpoint Security Clients. For more information, see ["Enabling GenAI Protect" on page 524](#).

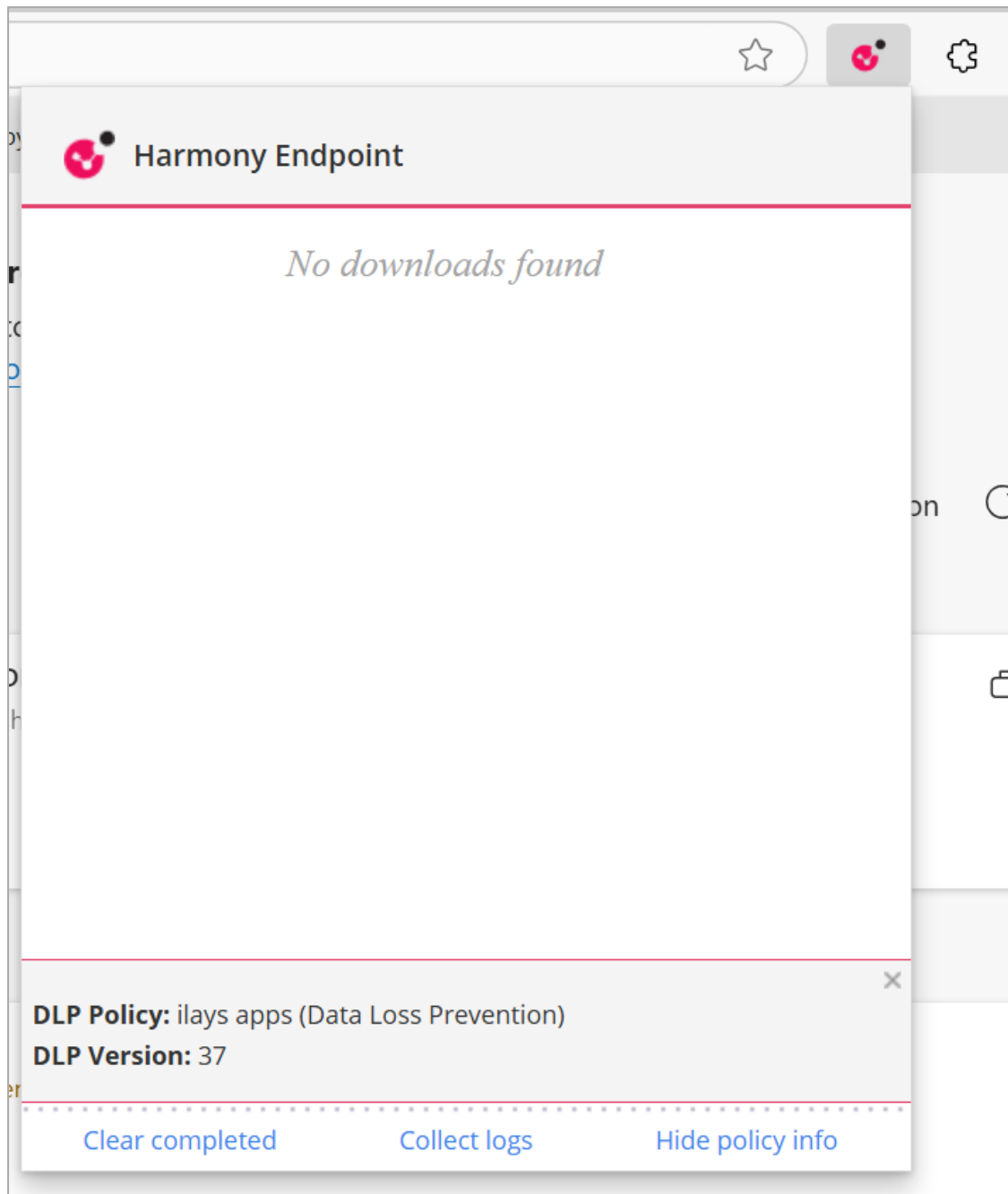


Notes:

- You can find the policy version number in the bottom left corner of the page.

The screenshot displays the Check Point Data Loss Prevention (DLP) policy configuration interface. The left sidebar contains a navigation menu with options like Threat Prevention, Policy Capabilities, Global Exclusions, Data Protection, General, OneCheck, SmartCards, Access Rules, Data Loss Prevention (highlighted), Access & Compliance, Client Settings, Deployment Policy, Software Deployment, Anti-Malware Settings, Export Package, Endpoint Client, and Browse Client. The main area shows a table of policies. The bottom left corner of the page, within the 'Data Loss Prevention' section, displays the policy name and version number 'E88.70', which is highlighted with a red box.

- You can find both policy name and policy version number in the browser extension which is supported only for Windows client E88.70 and higher.



DLP Logs

- [Logs](#) are sent for **Block**, **Prevent**, **Detect**, **Ask**, and **Redact** actions.
- **File upload** and **File download** events generate log for each handled file, regardless of whether the event is blocked, prevented, detected, or allowed.
- **Text control**, **Copy** and **Paste** events send logs for blocked, prevented, or detected incidents.



Use Case

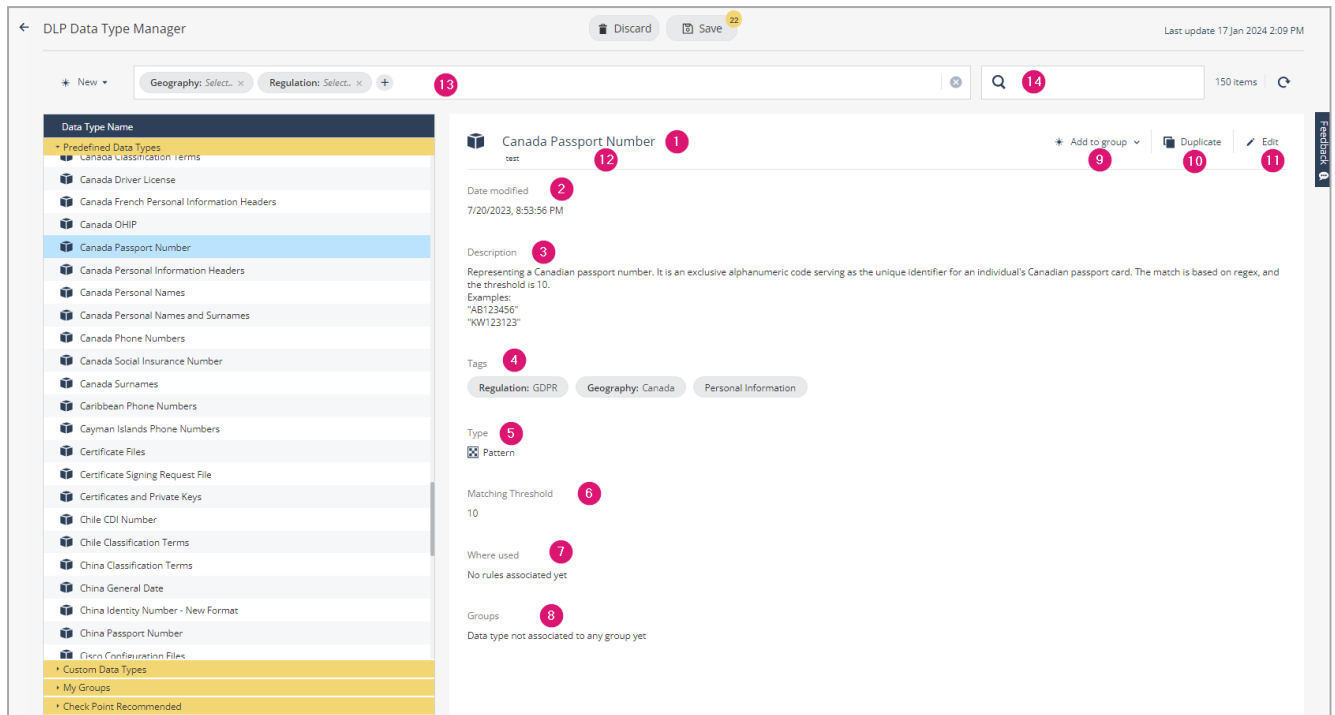
You are a financial organization aiming to prevent the upload or download of files containing confidential and sensitive data, such as bank account numbers, tax and revenue details, by unauthorized users.

Known Limitations

- This feature is supported only in the EU, US, India, Australia, and UAE regions.
- Supported on the following versions of Endpoint Security Clients:
 - Windows: E88.50 and later
 - macOS: E89.10 and later
- DLP is not applied if the file size is greater than 10 MB.
- DLP is not applied when you drag and drop a folder to upload files, and in such cases, the upload of the folder gets blocked.
- If the downloaded file is scanned by DLP, it is not sent to Threat Emulation.
- The **Application** destination type is applicable only to **Text Control** and **Paste** events and is supported only on Windows client version E88.70 or later.
- DLP policies do not apply to User-Based Virtual Groups. However, they do apply to machines and Machine-Based Virtual Groups.

Sample Data Type

For supported data and file types, see [sk181662](#).



Legends	Description
1	Name of the data type.
2	Date and time (in MM/DD/YY, HH:MM:SS XM format) when the data type was last modified.
3	Brief description of the data type.
4	Custom tags (category) for the data type. Helps in searching for data types.
5	Matching criteria: ■ Pattern ■ Keyword ■ Dictionary ■ Weighted Words ■ Template ■ File attribute ■ Compound (Combination of data types with a logical separator) ■ Group (Data type group)
6	The minimum number of times the matching criteria must be present in the file to trigger the DLP action specified in the policy capability rule. For example, if the matching criteria is Keyword , the value is credit and the Matching Threshold is 5 , then the system takes the action specified by the policy capability rule if the file contains the term credit five times or more.

Legends	Description
7	Policy capability rules where the data type is used.
8	Groups associated with the data type.
9	Add the data type to a group.
10	Duplicate the data type.
11	Edit the data type.
12	Comment.
13	Filter data type by category.
14	Search for a data type.

Creating a Custom Data Type

To create a custom data type:

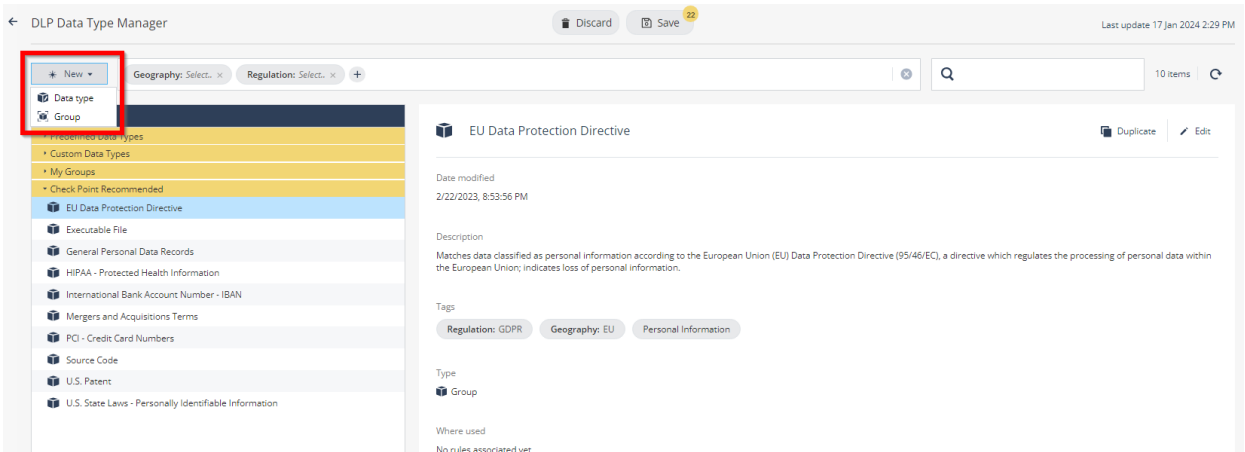
1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.

The screenshot displays the Check Point Harmony Endpoint DLP Data Type Manager interface. The top navigation bar includes a red box around the 'DLP Data Type Manager' button. The main area shows a table of data types with columns: #, Rule Name, Applied To, Inbound events, and Outbound events. Below this, there is a section for 'Outbound events' with a table showing event details, destinations, data types, and actions.

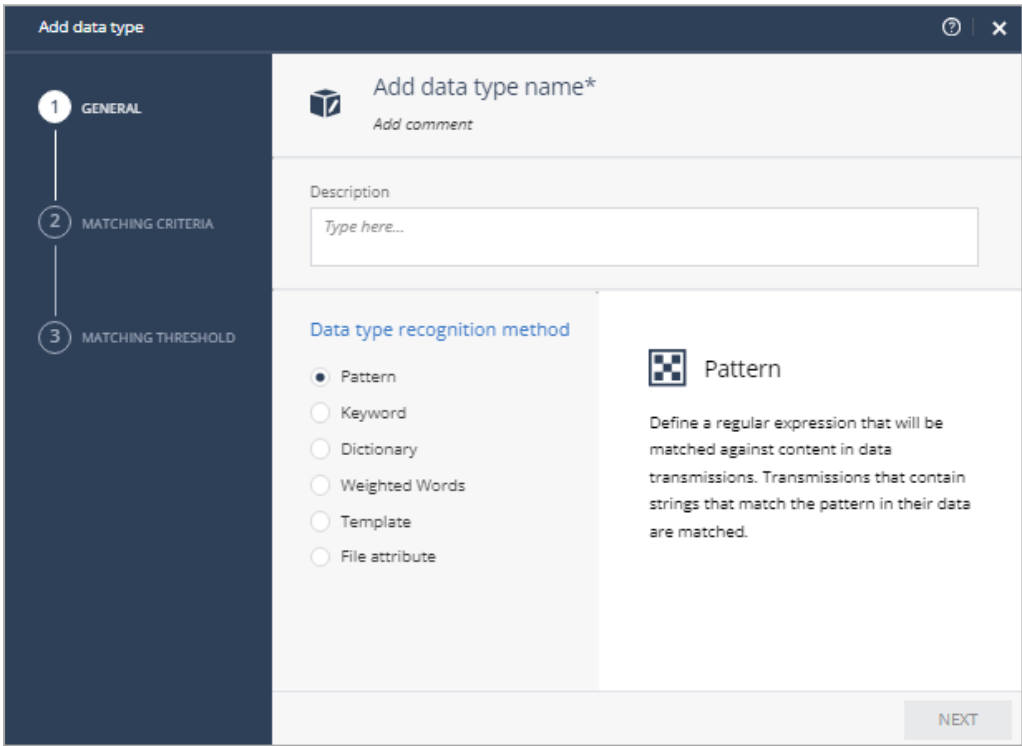
#	Rule Name	Applied To	Inbound events	Outbound events
0	Testing_001	All ChromeOs Desktops	File download	Paste, File upload, Text control
1	EXPO Policy	DESKTOP-169	File download	Paste, File upload, Text control
2	148	DESKTOP-MJAEIRL	File download	Text control, File upload, Paste
3	Threat Rule	CHECKPOINT-TEST	File download	Paste, File upload, Text control
4	New Rule 2	All ChromeOs Laptops	File download	Text control, File upload, Paste

Status	Event	Destinations	Data types	Action
☒	Paste	Artificial Intelligence (AI)	PCI - Card Security Code, IP Address	Prevent
☒	File upload	web.whatsapp.com	IP Address	Prevent
☒	File upload	mail.google.com	N/A	Block
☒	File upload	chat.openai.com, bing.com	IP Address	Prevent
☒	File upload	https://cloud.ai/login	PCI - Card Security Code	Prevent
☒	File upload	Artificial Intelligence (AI)	PCI - Card Security Code	Detect
☒	Text control	Artificial Intelligence (AI)	PCI - Card Security Code, IP Address	Prevent

2. Click **New** and select **Data type**.

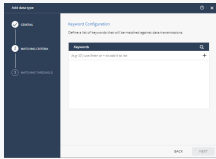
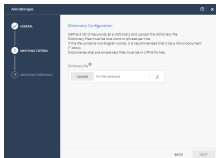


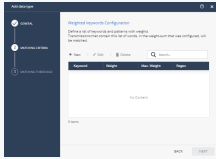
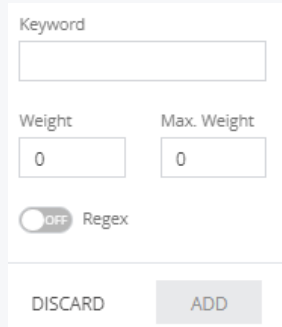
The Add data type wizard appears.

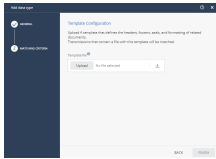
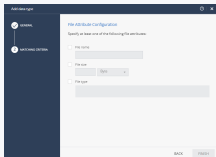


- 3. Enter the data type name, object comment (optional) and description.
- 4. From the **Data type recognition method** list, select a recognition method:

Recognition method	Description	Action
Pattern 	Applies the action specified in the policy capability rule if the file contents match the threshold for the pattern. For example, 5523-2342.	In the Patterns section, enter the pattern and click +.

Recognition method	Description	Action
Keyword 	Applies the action specified in the policy capability rule if the file contents match the threshold for the keyword. For example, <i>Confidential</i>, <i>Secret</i>.	In the Keywords section, enter the keywords and click +.
Dictionary 	Applies the action specified in the policy capability rule if the file contents match the threshold for the terms in the dictionary. For example, <i>Spain</i>, <i>China</i>, <i>United Kingdom</i>. Each keyword must be specified in a single line in the UTF-8 format. Note - The recommended file formats are Microsoft Word and <i>.txt</i>.	Upload the dictionary file.

Recognition method	Description	Action
Weighted Words 	Applies the action specified in the policy capability rule if the file contains keywords and the cumulative weight matches or exceeds the threshold. Use this method to specify multiple keywords. For example, consider two keywords: ▪ credit with Weight=1 and Max. Weight=3 ▪ transaction with Weight=2 and Max. Weight=30 and Matching Threshold=15. If the file contains six occurrences of credit, each contributing a Weight of 1. That is, $1 \times 6 = 6$. As the Max. Weight=3, the final weight is 3. If the file contains eight occurrences of transaction, each contributing a Weight of 2. That is, $2 \times 8 = 16$. As the Max. Weight=30, the final weight is 16. As the sum of final weights of credit and transaction, that is, $16 + 3 = 19$ is greater than the Matching Threshold, the system applies the specified action in the policy capability rule. If the sum of the final weights of the keywords is less than the Matching Threshold, then the file is uploaded or downloaded.	a. Click New.  b. Enter these: ▪ Keyword ▪ Weight - Weight for each occurrence of the keyword. ▪ Max. Weight - Maximum allowed for weight for the keyword. c. If the keyword is a regular expression, turn on the Regex toggle button. d. Click Add. e. Repeat steps <i>a</i> through <i>d</i> to add the next keyword.

Recognition method	Description	Action
Template 	Applies the action specified in the policy capability rule if the file contents match the threshold for the terms in the template. For example, a template with a set header, footer and logo. If the template contains images, the DLP is triggered only if the file contains the images in the same format as in the specified template.	Upload the template file.
File attribute 	Applies the action specified in the policy capability rule if the file: ■ Matches the specified file name. ■ Size is equal to or greater than the specified file size. ■ Type matches the specified file type.	Select any of these and enter a value: ■ File name. For example, <i>Account Numbers</i>, <i>Employee Details</i>. ■ File size. File size in Byte, KB, MB or GB. ■ File type. • Click  and select the file type(s) from the list.

5. Click **Next**.

 **Note** - This step does not apply to **Template** and **File attribute** recognition methods.

6. Select the matching threshold.

The minimum number of times the matching criteria must be present in the file to trigger the DLP. For example, if the matching criteria is **Keyword**, the value is **credit** and the **Matching Threshold** is **5**, then the system takes the action specified by the policy capability rule if the file contain the term **credit** five times or more.

 **Note** - This step does not apply to **Template** and **File attribute** recognition methods.

7. Click **Finish**.

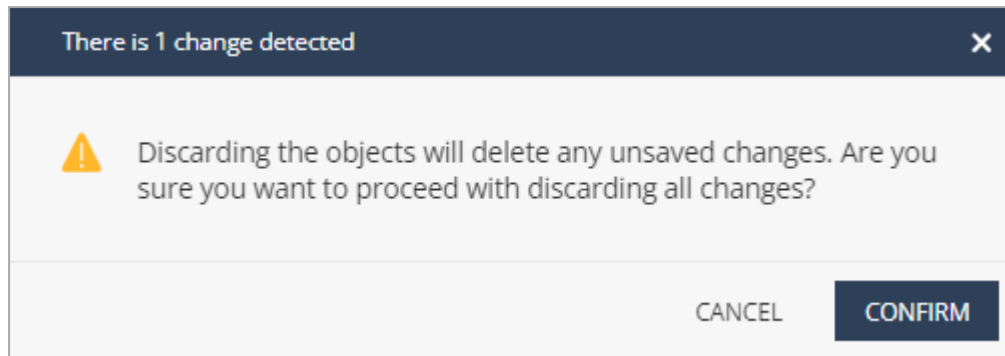
The new custom data type is listed under **Custom Data Types**.

8. To permanently save all the changes to the database, click **Save** at the top.

The **change detected** window appears.

9. Click **Confirm**.
10. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.

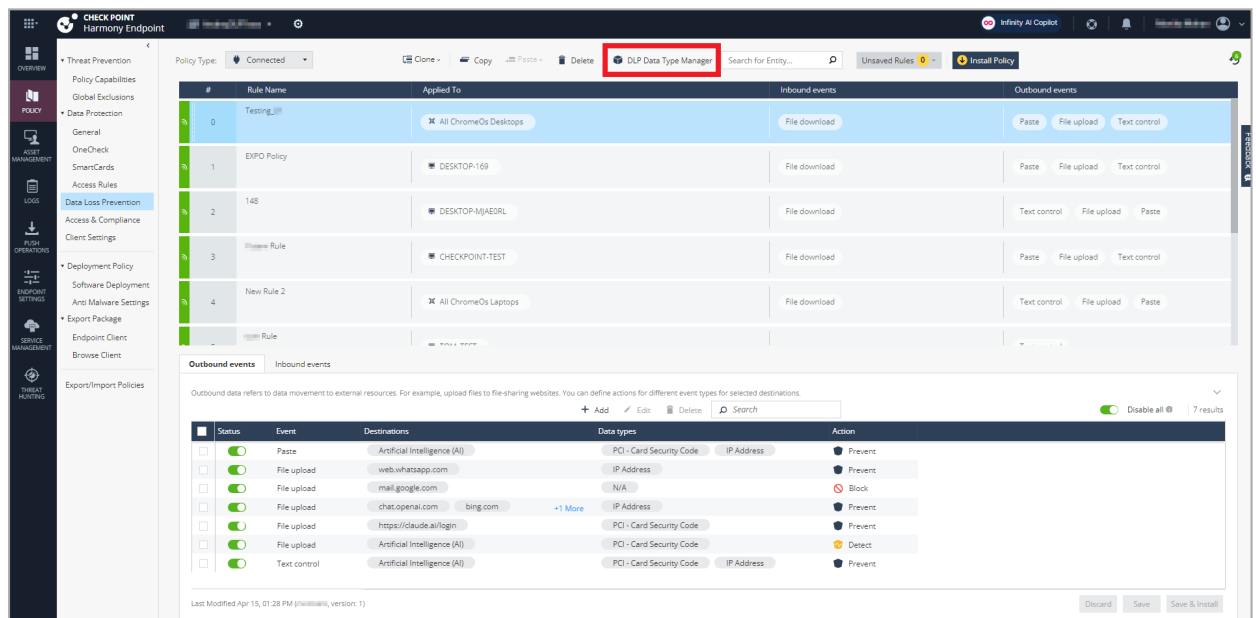


11. Click **Confirm**.

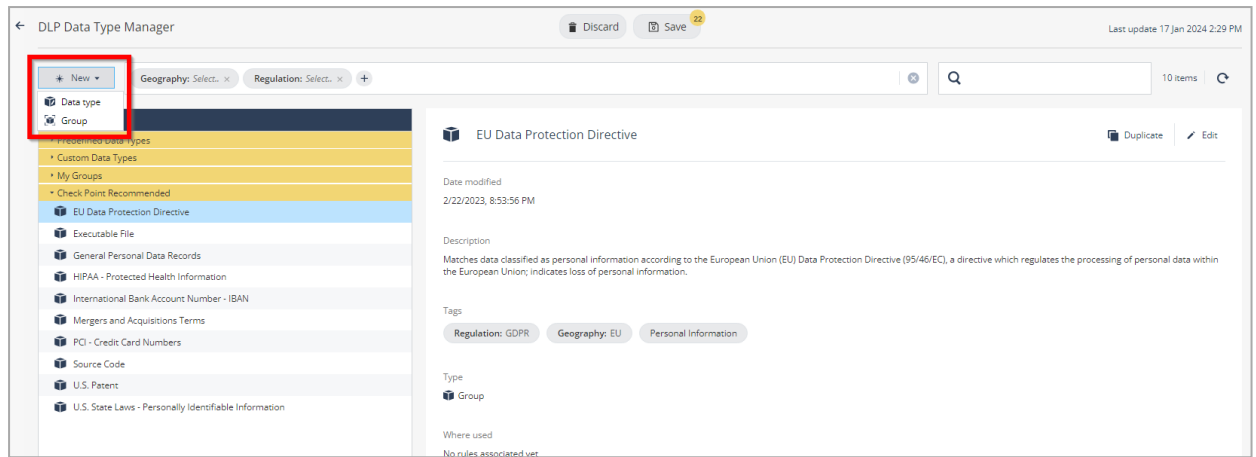
Creating a Custom Data Type Group

To create a custom data type group:

1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.



2. Click **New** and select **Group**.



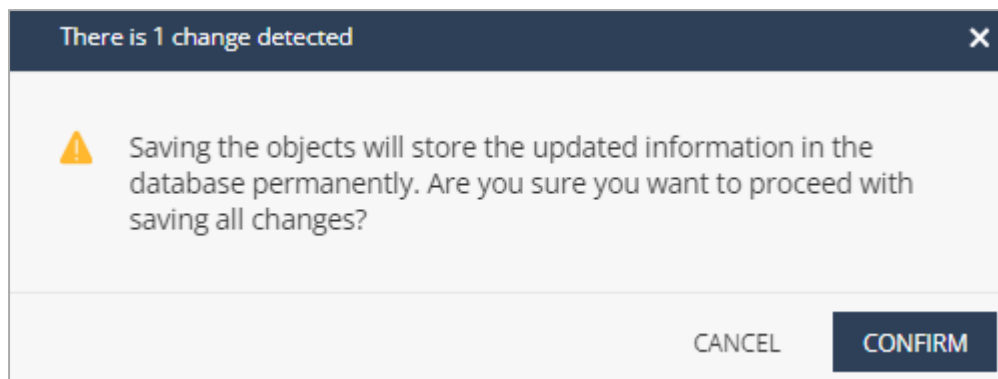
The **New Data type Group** window appears.

3. Enter a group name, object comment (optional) and description.
4. To add predefined data types to the group, click **+** in the **Predefined Data types** field and select the data type.
5. To add [custom data types](#) to the group, click **+** in the **Custom Data types** field and select the data type.
6. Click **Save**.

The new data type group is listed under **My Groups**.

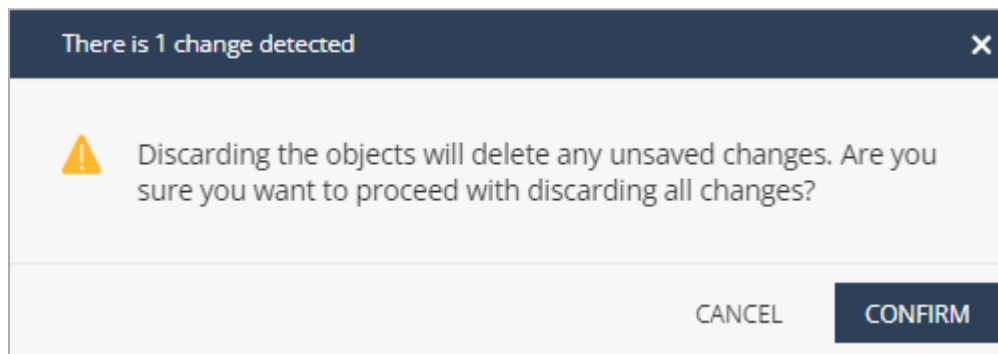
7. To permanently save all the changes to the database, click **Save** at the top.

The **change detected** window appears.



8. Click **Confirm**.
9. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.

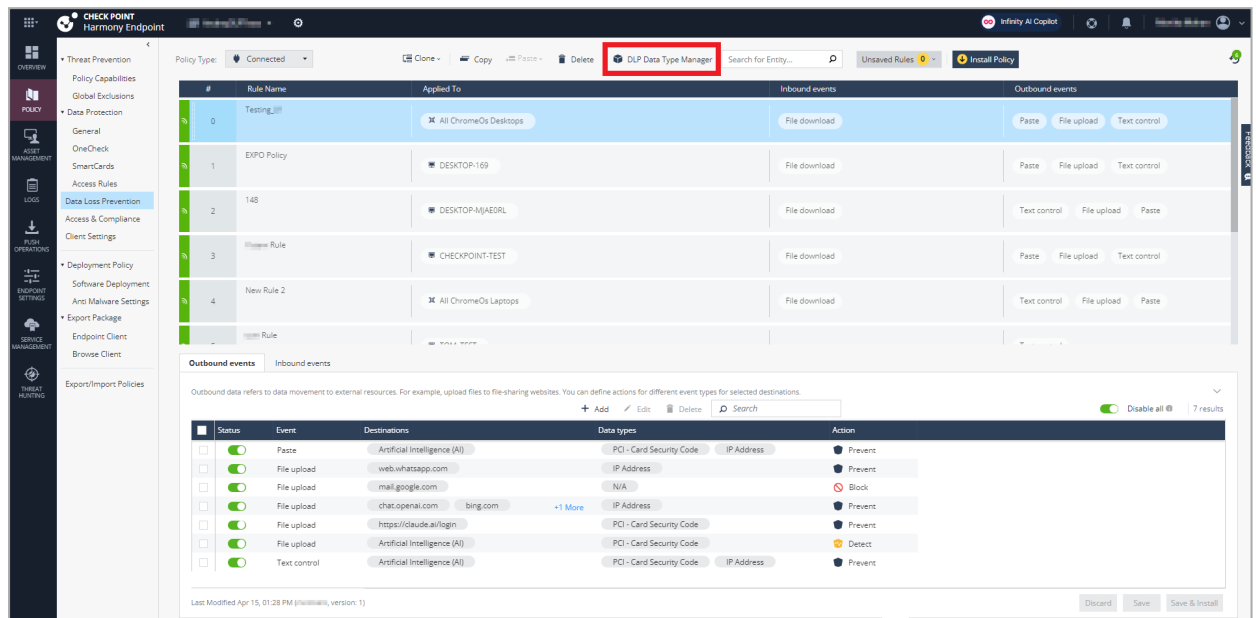


10. Click **Confirm**.

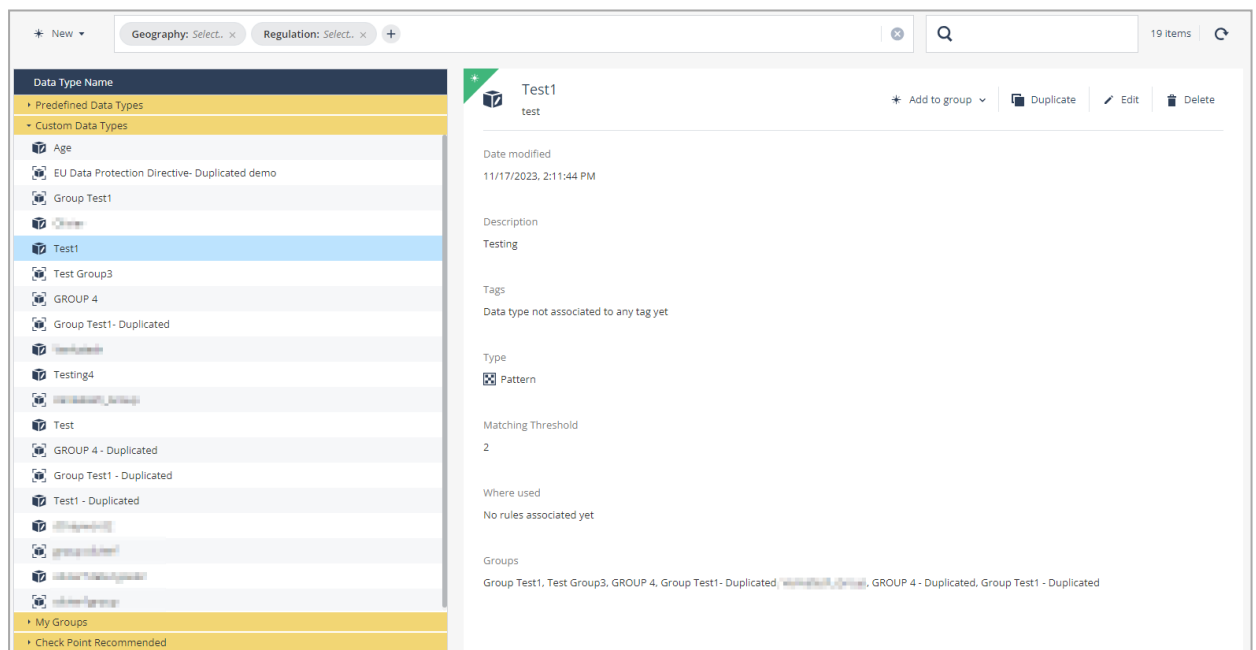
Adding an Existing Data Type to a Group

To add an existing data type to a group:

1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.



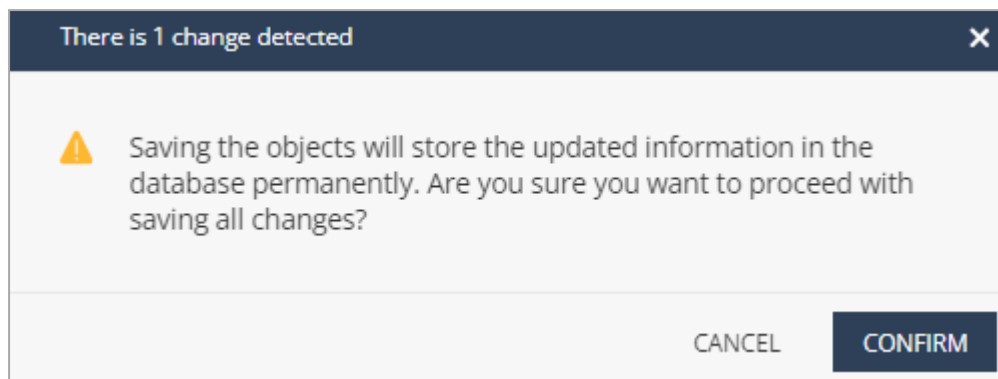
2. In the **Data Type Name** list, expand **Custom Data Types** or **Predefined Data Types** and select the data type.



3. Click **Add to group**.
4. Select the group(s) from the list.
5. Click **Add**.

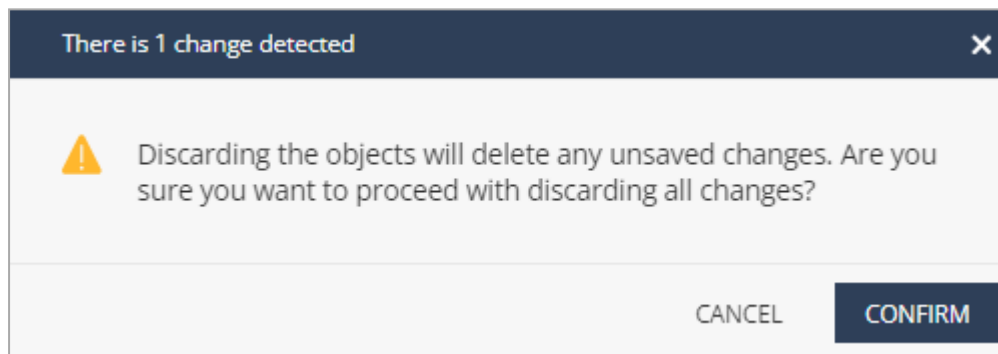
6. To permanently save all the changes to the database, click **Save** at the top.

The **change detected** window appears.



7. Click **Confirm**.
8. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.



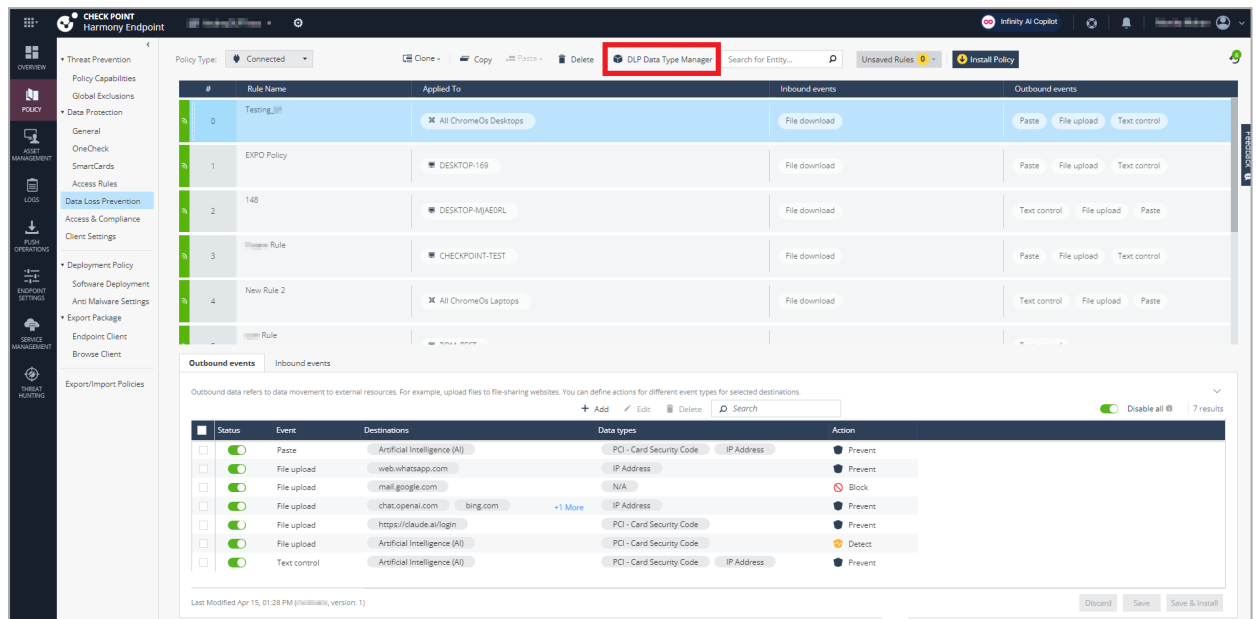
9. Click **Confirm**.

Editing a Data Type or Group

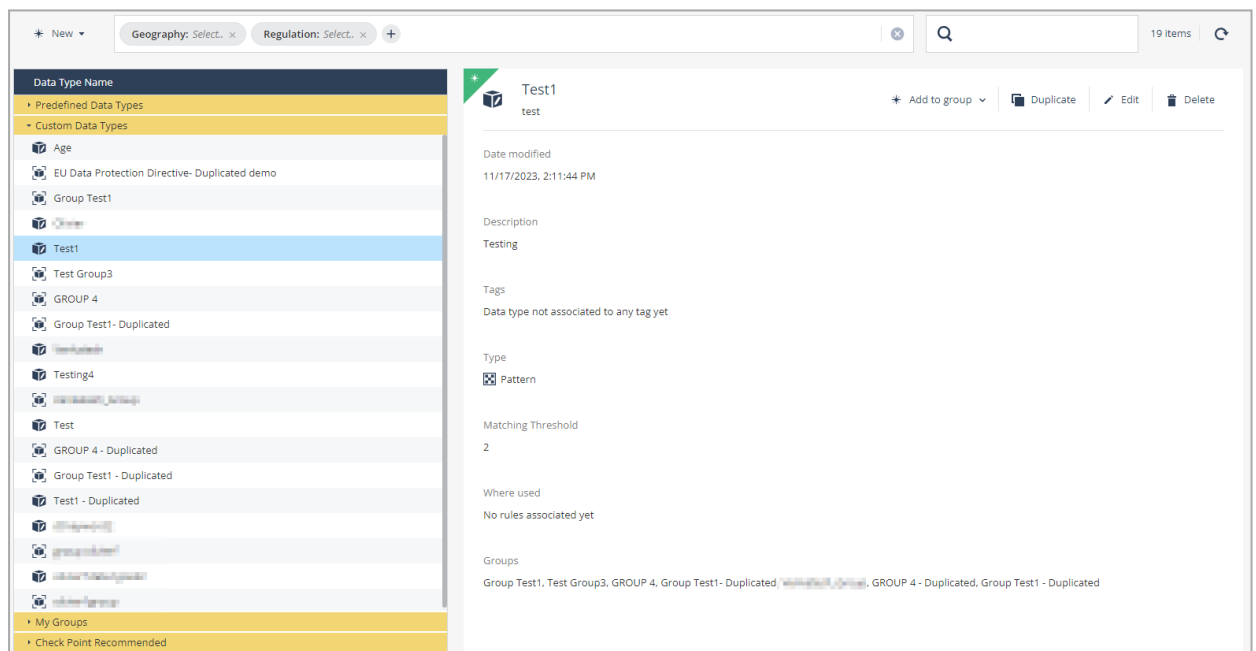
-  **Note** - If you edit a data type, the changes are reflected in all the groups that contain this data type.

To edit a data type or group:

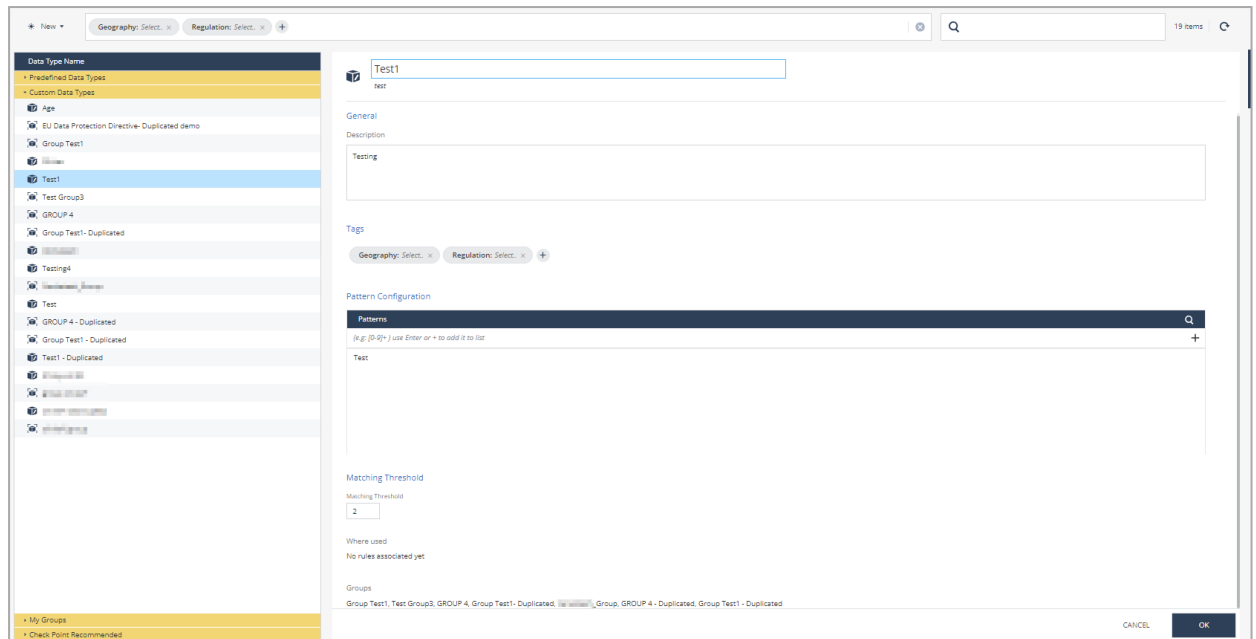
1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.



2. In the **Data Type Name** list, expand the DLP group and select the data type or the group.



3. Click **Edit**.

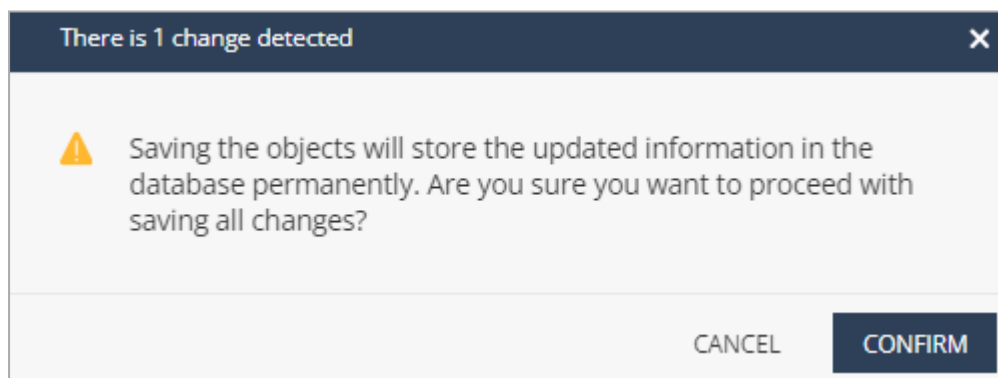


4. Make the required changes.

Note - In the **Check Point Recommended** and **Predefined Data Types DLP** groups, you can edit only **Matching level** and **Add object comment**.

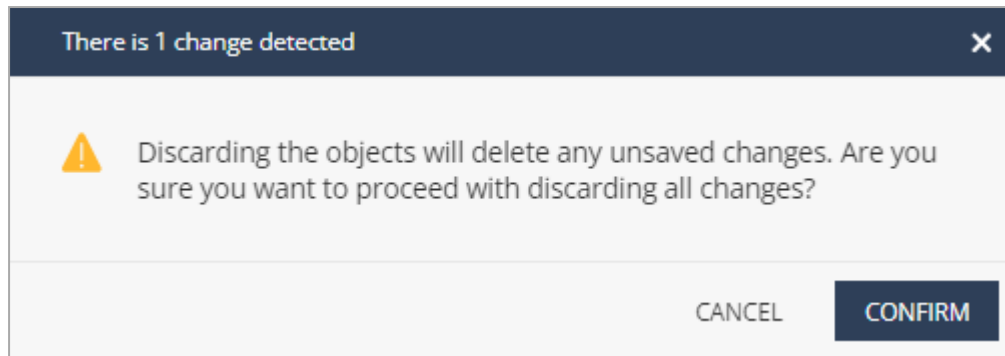
- Click **OK**.
- To permanently save all the changes to the database, click **Save** at the top.

The **change detected** window appears.



- Click **Confirm**.
- To discard all the changes, click **Discard** at the top.

The **change detected** window appears.

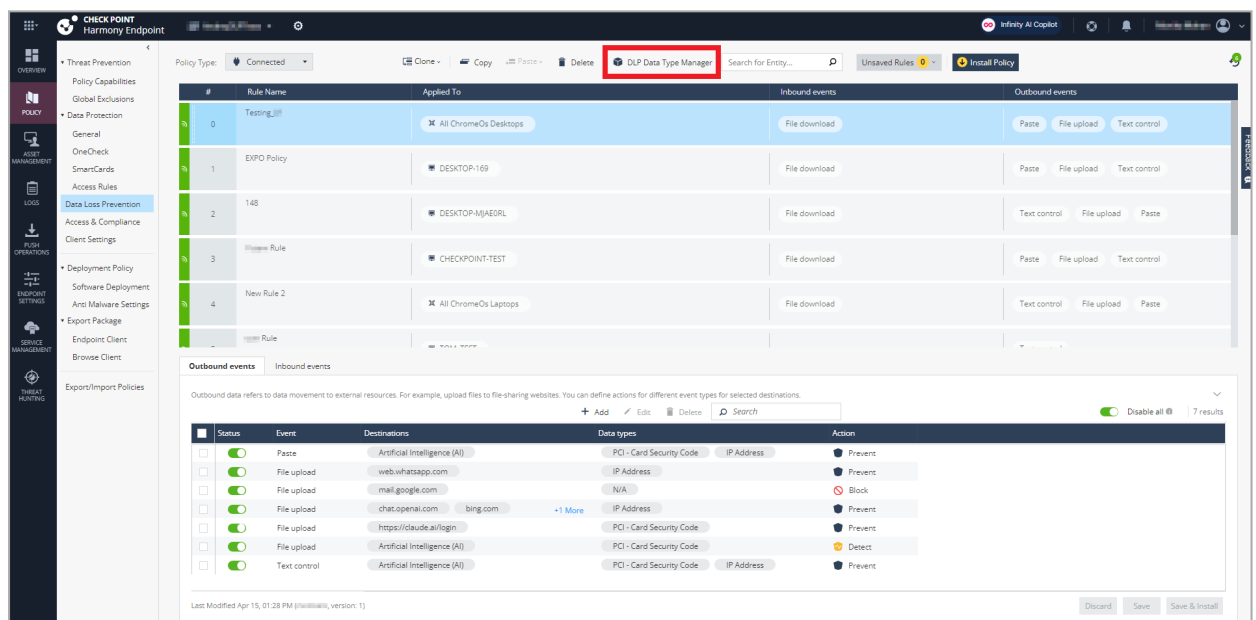


9. Click **Confirm**.

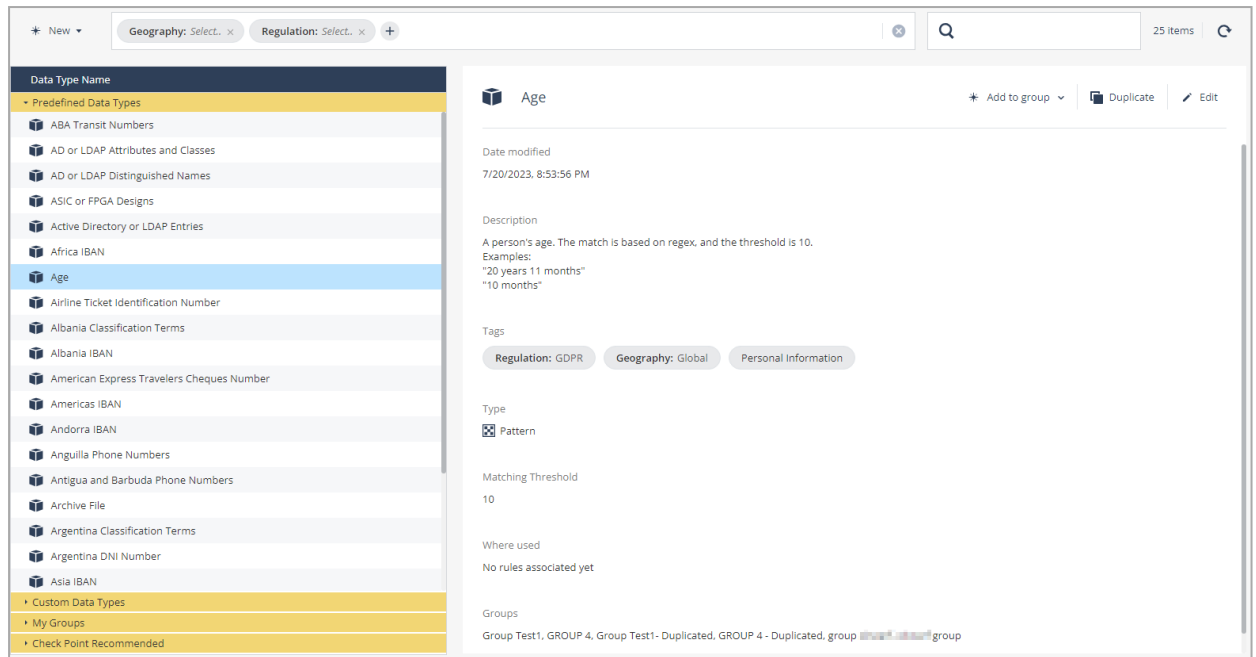
Duplicating a Data Type or a Group

To duplicate a data type or group:

1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.

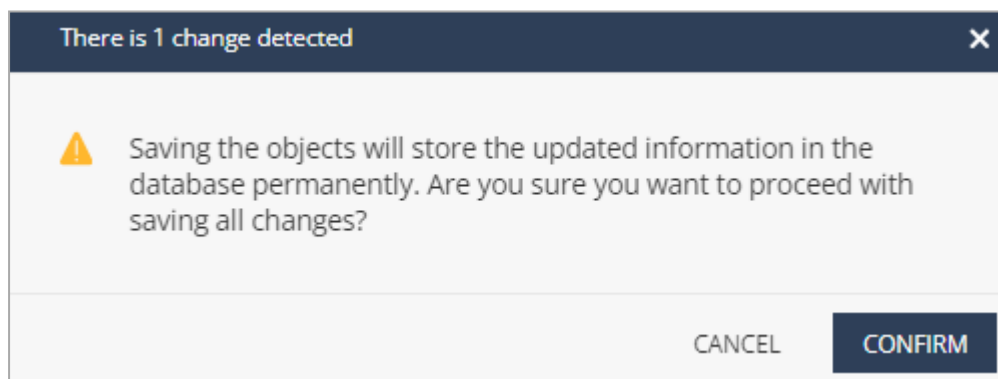


2. In the **Data Type Name** list, expand the DLP group and select the data type or the group within.



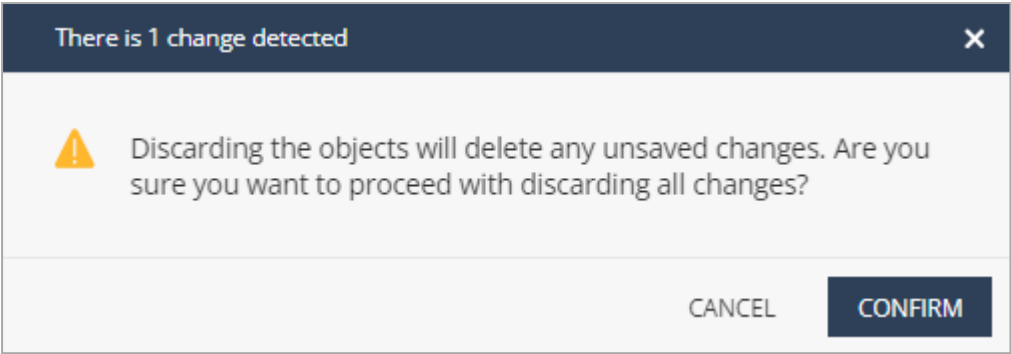
3. Click **Duplicate**.
4. Make the required changes.
5. Click **OK**.
6. To permanently save all the changes to the database, click **Save** at the top.

The **change detected** window appears.



7. Click **Confirm**.
8. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.



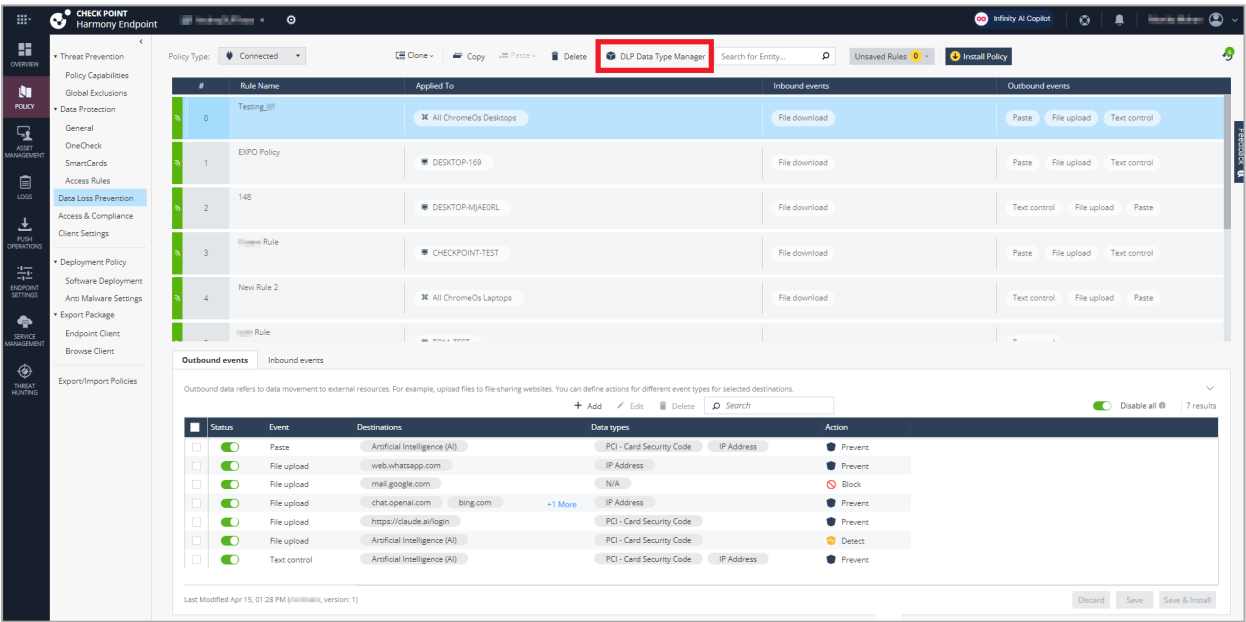
9. Click **Confirm**.

Deleting a Data Type or a Group

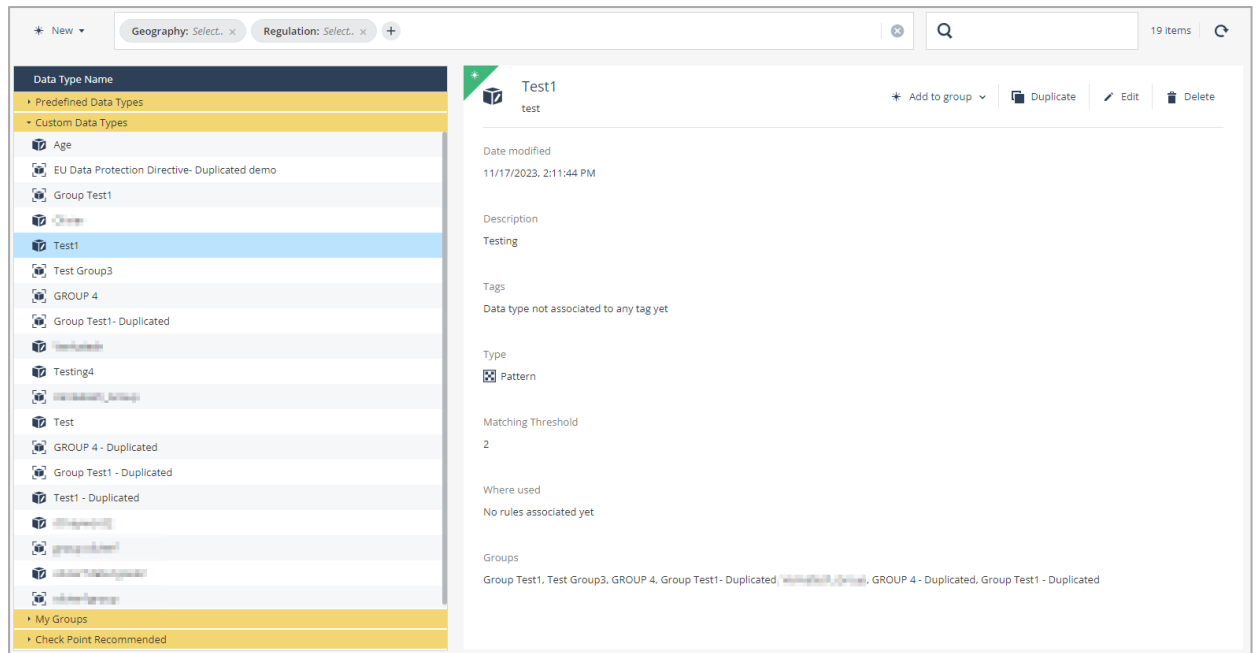
Note - Before you delete a data type, make sure to remove the data type from the group(s) and policy capability rules.

To delete a data type or group:

1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.

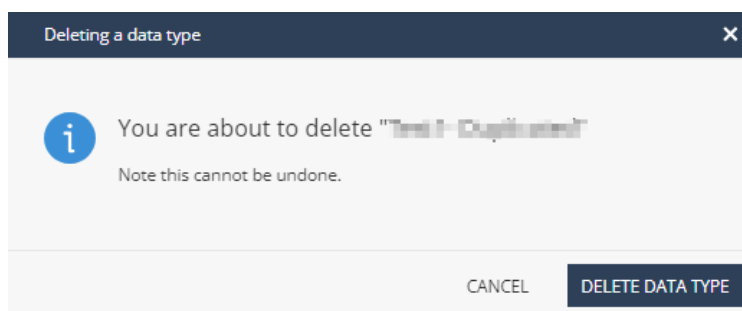


2. In the **Data Type Name** list, expand the DLP group and select the data type or the group within.



3. Click **Delete**.

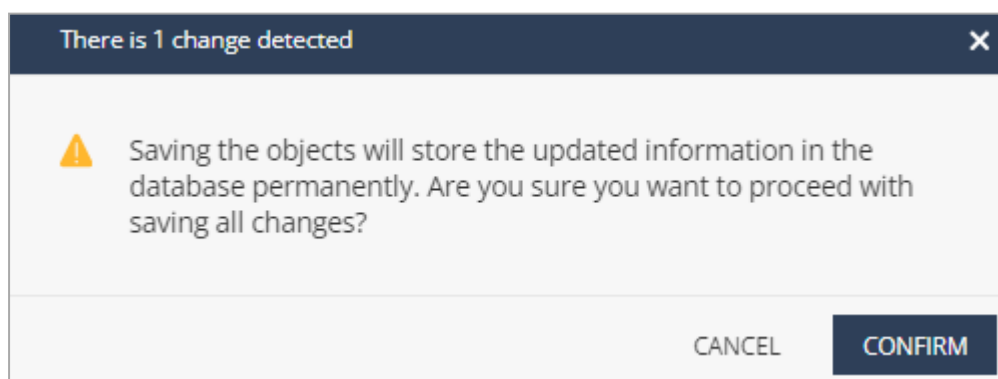
The **Deleting a data type** window appears.



4. Click **Delete Data Type**.

5. To permanently save all the changes to the database, click **Save** at the top.

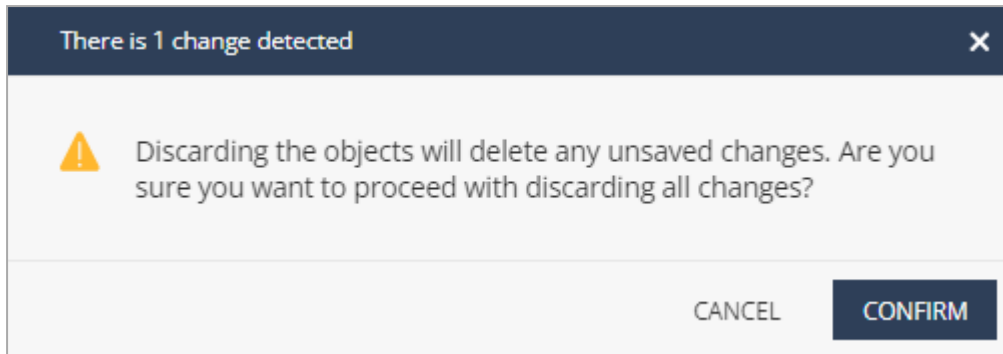
The **change detected** window appears.



6. Click **Confirm**.

7. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.



8. Click **Confirm**.

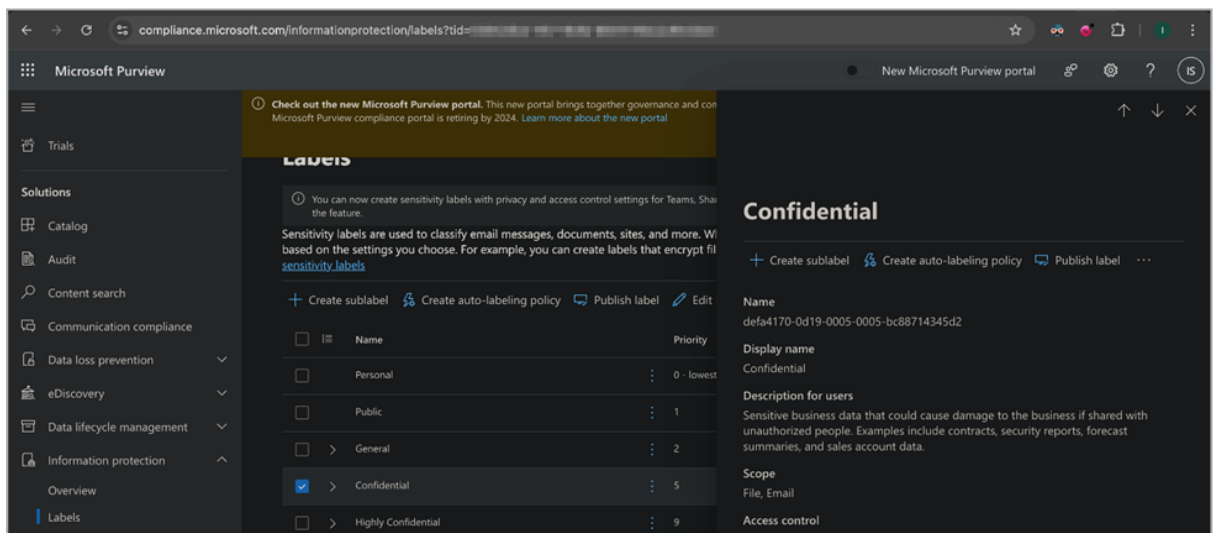
Managing Microsoft Sensitivity Labels for DLP

Endpoint Security allows you to integrate Sensitivity labels from Microsoft Purview Information Protection into your DLP system, providing an additional layer of data protection based on predefined sensitivity classifications.

Step 1 - Copy the Microsoft Sensitivity label names and their UUIDs from Microsoft Purview

Finding the UUID of labels in the Old Microsoft Purview portal

1. Log in to Microsoft Purview Portal: <https://purview.microsoft.com/>
2. Go to **Solutions > Information protection > Labels**.



3. Click the label name for which you want to find the UUID.
4. Copy the UUID in the **Label ID** or **GUID** section.

Finding the UUID of labels in the New Microsoft Purview portal

1. Install the Exchange Online Management Module

The Microsoft Purview Security & Compliance PowerShell uses the Exchange Online Management Module for connection.

- a. Open PowerShell as an administrator.
- b. Run the following command:

```
Install-Module -Name ExchangeOnlineManagement -Force
```

- c. If the system prompts to install NuGet or trust the repository, enter Y and press Enter.

2. Connect to the Microsoft Purview Security & Compliance Center.

- a. Run the following command to create a session:

```
Connect-IPPSession
```

- b. In the Microsoft login page that appears, authenticate with the Microsoft 365 administrator credentials.



Note - The administrator must have **Compliance Administrator** or **Information Protection Administrator** roles.

- c. If your Microsoft Purview portal has Multi-Factor Authentication (MFA), complete the MFA process.

Once authenticated, the session connects to the Microsoft Purview Security & Compliance Center.

Now, you can run Microsoft Purview Security & Compliance PowerShell commands, such as managing labels, policies, or settings.

3. To view the UUID of the labels, run the following commands:

```
Get-Label | Select-Object DisplayName, Name, Guid
```

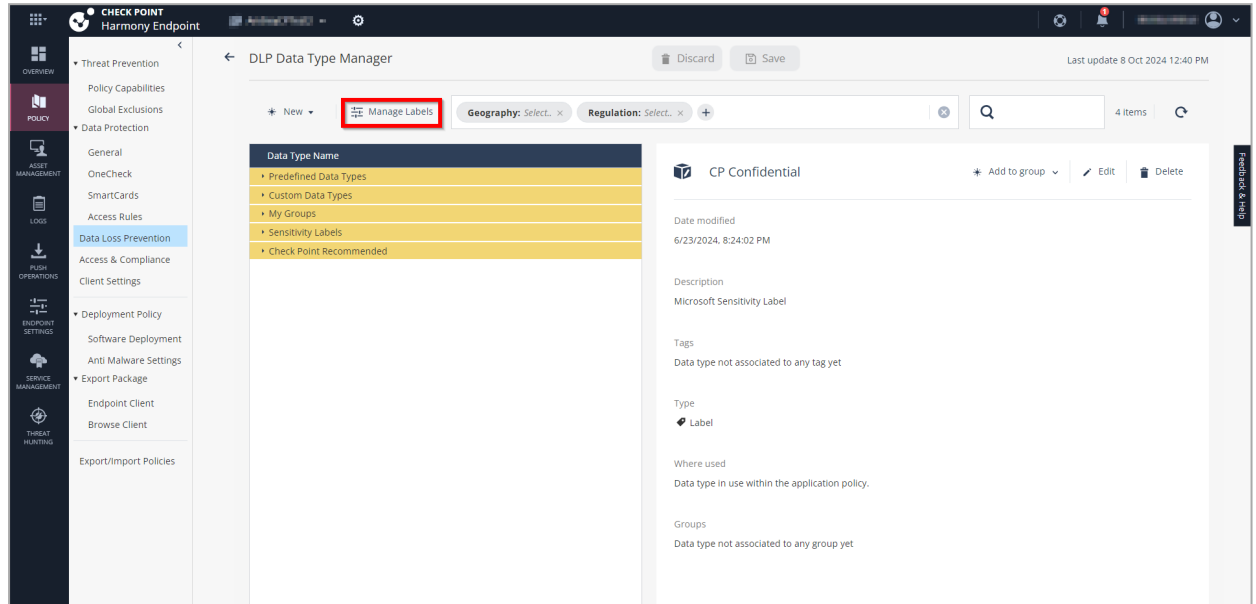
DisplayName	Name	Guid
Personal	def4170-8d19-0005-0000-bc88714345d2	def4170-8d19-0005-0000-bc88714345d2
Public	def4170-8d19-0005-0001-bc88714345d2	def4170-8d19-0005-0001-bc88714345d2
General	def4170-8d19-0005-0002-bc88714345d2	def4170-8d19-0005-0002-bc88714345d2
General (unrestricted)	def4170-8d19-0005-0003-bc88714345d2	def4170-8d19-0005-0003-bc88714345d2
All Employees (unrestricted)	def4170-8d19-0005-0004-bc88714345d2	def4170-8d19-0005-0004-bc88714345d2
General (unrestricted)	def4170-8d19-0005-0005-bc88714345d2	def4170-8d19-0005-0005-bc88714345d2
All Employees (unrestricted)	def4170-8d19-0005-0006-bc88714345d2	def4170-8d19-0005-0006-bc88714345d2
All Employees	def4170-8d19-0005-0007-bc88714345d2	def4170-8d19-0005-0007-bc88714345d2
Trusted People	def4170-8d19-0005-0008-bc88714345d2	def4170-8d19-0005-0008-bc88714345d2
Highly Confidential	def4170-8d19-0005-0009-bc88714345d2	def4170-8d19-0005-0009-bc88714345d2

4. Copy the UUID of the labels.
5. To disconnect the session, run the following command:

```
Disconnect-ExchangeOnline
```

Step 2 - Creating Microsoft Sensitivity Labels in Endpoint Security

1. Log in to Check Point Portal and access the Endpoint Security Administrator Portal:
2. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.
3. Click **Manage Labels**.



The **Manage Sensitivity Labels Dashboard** window appears.

Manage Sensitivity Labels Dashboard

Labels configuration

Define a list of Microsoft Sensitivity label names and their corresponding UUIDs. The labels will be represented as data types in the system.

New

Edit

Delete

Search...

Name	UUID
Highly Confidential	804b1907-8000-4000-9000-400000000000
High	804b1907-8000-4000-9000-400000000000
Medium	804b1907-8000-4000-9000-400000000000
Low	804b1907-8000-4000-9000-400000000000

4 items

OK

4. Click **New**.

Manage Sensitivity Labels Dashboard

Labels configuration

Define a list of Microsoft Sensitivity label names and their corresponding UUIDs. The labels will be represented as data types in the system.

* New | Edit | Delete | Search...

Name

UUID

CANCEL ADD

4 items

OK

5. In the **Name** field, enter a name for the label. For example, MIP_EXAMPLE.
6. In the **UUID** field, enter the label UUID. For more information, see ["Step 1 - Copy the Microsoft Sensitivity label names and their UUIDs from Microsoft Purview" on page 505](#).
7. Click **Add**.
8. Click **OK**.

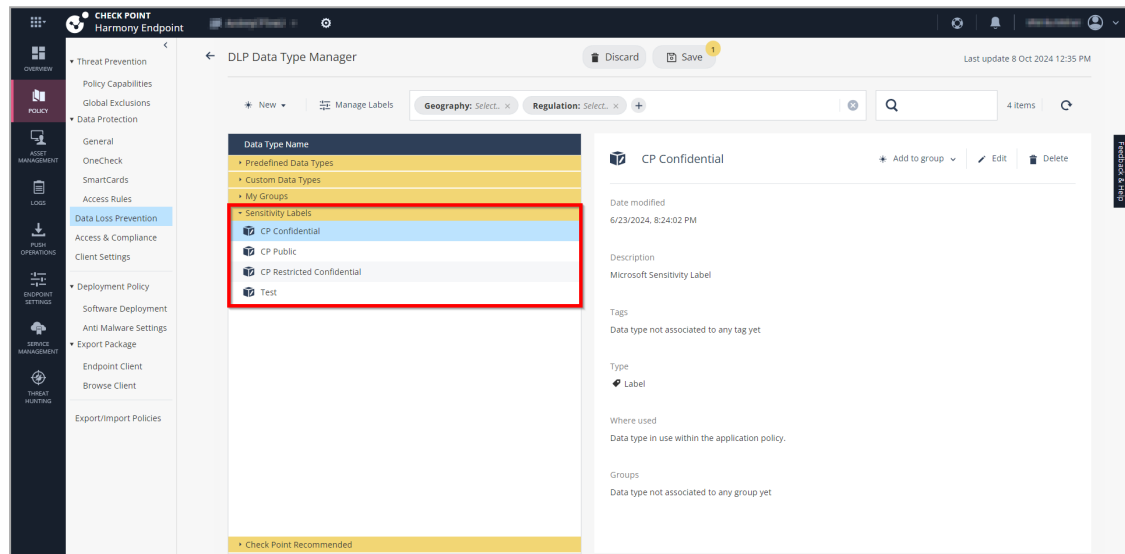


Note - The newly created label is now listed in **Sensitivity Labels** under **Data Type Name** section.

It also shows the label details:

- Date modified
- Description
- Tags - Shows tags assigned, if any, for further categorization
- Where used - Shows the DLP rule name that uses this label to enforce protection.
- Groups - Shows if the label is part of any group.

You can use Tags and Groups to better organize and manage the sensitivity labels.



9. To edit a label, select the label you want to edit, click **Edit**, update the field and then click **Apply**.

Name

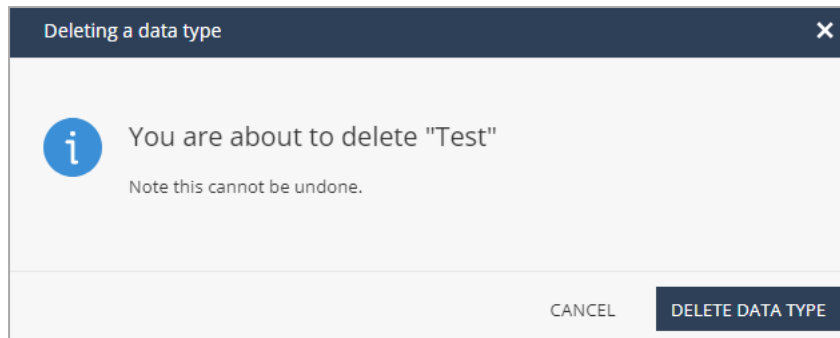
Test

UUID

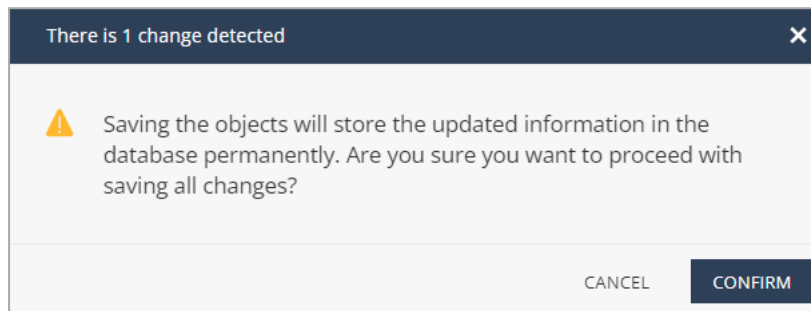
655f5e5e-5e5e-5e5e-5e5e-5e5e5e5e5e5e

CANCEL APPLY

10. To delete a label, select the label you want to delete, click **Delete** and then click **Delete Data Type**.



11. Click **Save**.



12. Click **Confirm**.

Step 3 - Assign Sensitivity Labels to DLP Rules

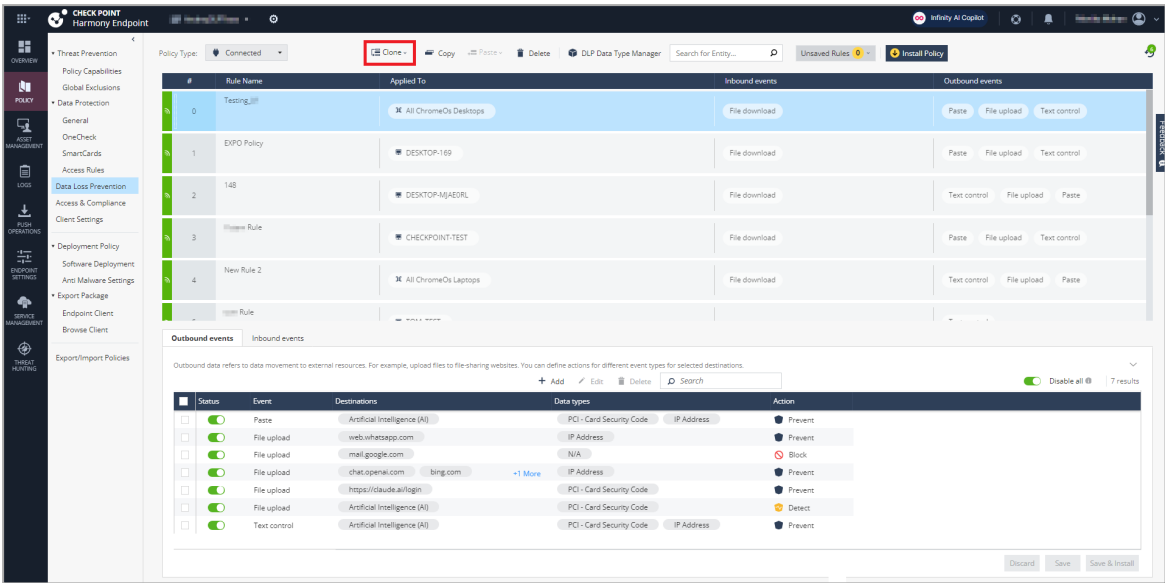
After creating Sensitivity labels in Endpoint Security, you must assign them to the DLP rules to enforce data protection based on these sensitivity labels.

To assign sensitivity labels to a DLP rules, see ["Creating a DLP Rule and Associating with an Event" below](#).

Creating a DLP Rule and Associating with an Event

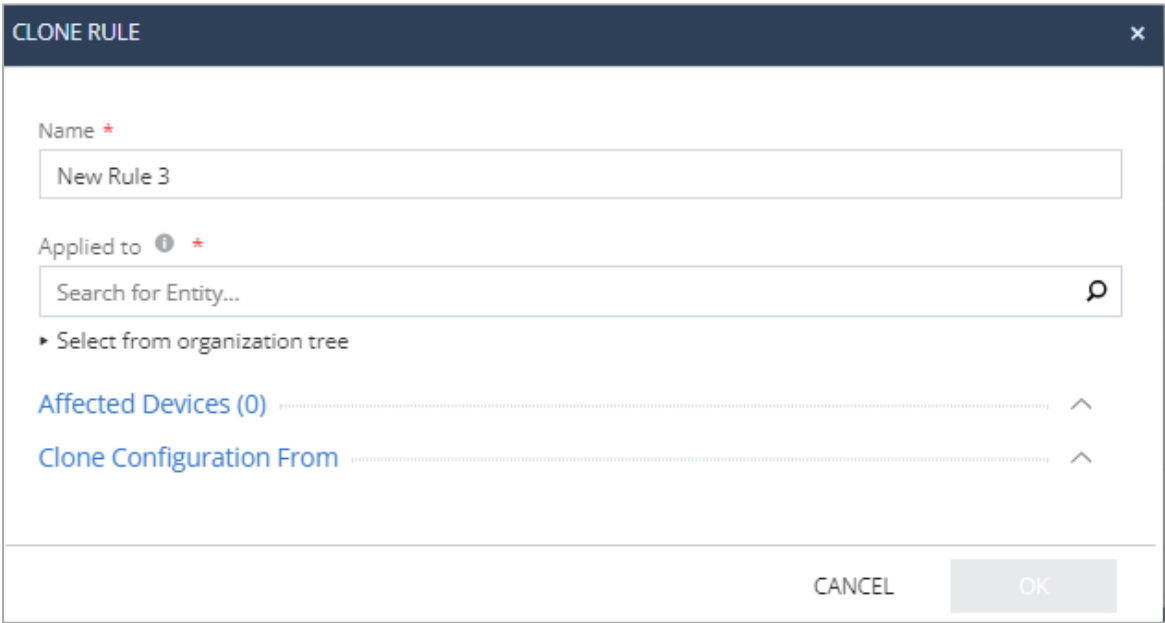
1. Go to **Policy > Data Loss Prevention**.
2. Add a rule:

- a. Select a rule.
- b. Click **Clone** and click **Clone Above** or **Clone Below**.



Note - If you have selected the default rule, select **Clone Above**.

The **Clone Rule** window appears.



- c. In the **Name** field, enter a rule name.
 - d. From the **Applied to** list, select a device(s) to which you want to apply the rule.
 - e. Click **OK**.
3. To enable the Gen AI protection, see ["Enabling GenAI Protect" on page 524](#).
4. Click one of these tabs:

- **Outbound events** - Outbound data refers to transferring content to external resources.

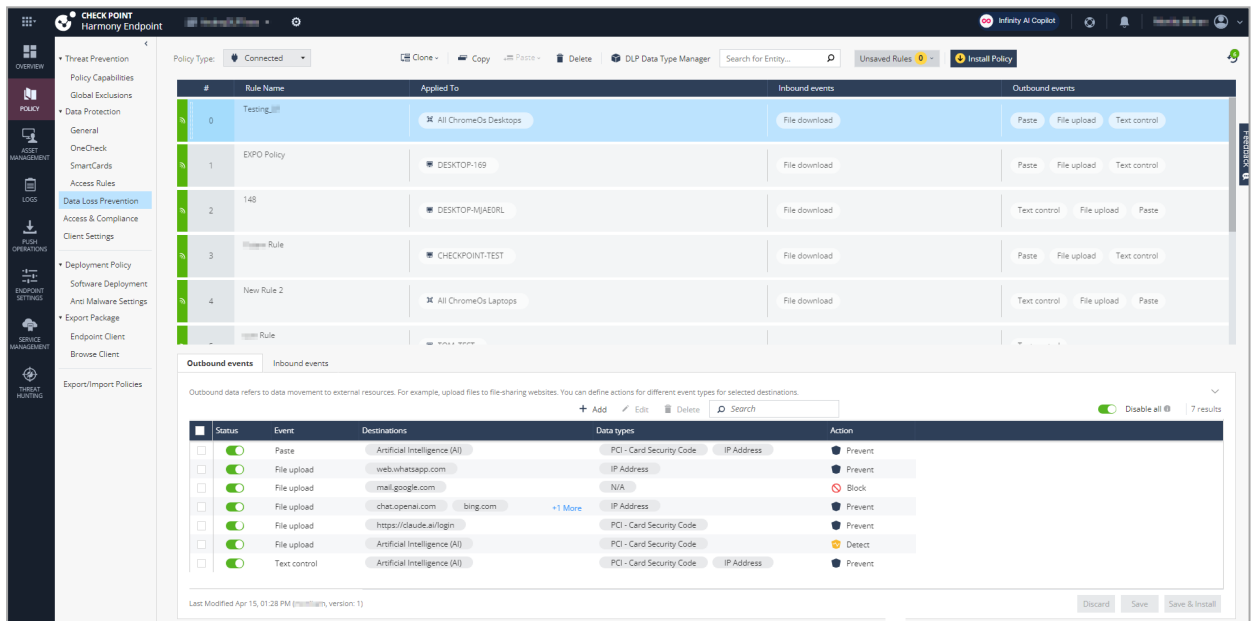
Examples:

- Uploading file to a file sharing website.
- Entering text in a text box of an external resource, such as ChatGPT.
- Pasting text in a text box of an external resource, such as ChatGPT.

 **Note** - Enforcement of DLP for **Paste** and **Text Control** events is only supported for Generative AI sites.

- **Inbound events** - Inbound data refers to downloading data and sharing content within internal corporate resources.

Example - Downloading file from a file sharing website.



#	Rule Name	Applied To	Inbound events	Outbound events
0	Testing...all	All ChromeOs Desktops	File download	Paste, File upload, Text control
1	EXPO Policy	DESKTOP-169	File download	Paste, File upload, Text control
2	148	DESKTOP-MJAEURL	File download	Text control, File upload, Paste
3	Rule	CHECKPOINT-TEST	File download	Paste, File upload, Text control
4	New Rule 2	All ChromeOs Laptops	File download	Text control, File upload, Paste

Status	Event	Destinations	Data types	Action
☒	Paste	Artificial Intelligence (AI)	PCI - Card Security Code, IP Address	Prevent
☒	File upload	web.whatsapp.com	IP Address	Prevent
☒	File upload	mail.google.com	N/A	Block
☒	File upload	chat.openai.com, bing.com	IP Address	Prevent
☒	File upload	https://cloud.ai/login	PCI - Card Security Code	Prevent
☒	File upload	Artificial Intelligence (AI)	PCI - Card Security Code	Detect
☒	Text control	Artificial Intelligence (AI)	PCI - Card Security Code, IP Address	Prevent

5. Click **Add**.

The **Data Protection - New Event** window appears.

data protection - New event

Status *
☒ On

Event type *
 File upload

Destination type *
 Category

Categories & sub categories *
 Security

Action *
 Prevent

Data types *
 + | × Search 1 Results

Data types
 Age- Duplicated

Cancel Save

6. By default, the event is enabled. To disable, turn off the **Status** toggle button.
7. From the **Event type** list, select one of these:

Event Type	Applies to	Description
File upload	Outbound events	To apply the DLP rule when you upload a file to an external resource.
Text control	Outbound events	To apply the DLP rule when you type text in an external resource text box. For example, in ChatGPT.
Paste	Outbound events	To apply the DLP rule when you paste content into an external resource. For example, ChatGPT.
File download	Inbound events	To apply the DLP rule when you download a file from an internal resource.

Event Type	Applies to	Description
Copy	Inbound events	To apply the DLP rule when you copy content from an internal resource.

 **Note** - Enforcement of DLP for **Paste** and **Text Control** events is only supported for Generative AI sites.

8. From the **Destination type** list, select one of these type to which you want to apply the rule:

Destination type	Applies to	Description
All	File upload	N/A
Url	■ File upload ■ File download ■ Copy	In the URL field, enter the web addresses to which you want to apply the rule.
Application	■ Text control ■ Paste	In the Applications field, select the application (s) to which you want to apply the rule.
Domain	■ File upload ■ File download ■ Copy	In the Domain field, enter the domain to which you want to apply the rule.
Category	■ File upload ■ Text control ■ Paste	From the Categories & sub categories list, select one or more categories.

-  **Notes:**
- In **Inbound events**, you can only choose a **URL** or **Domain**.
 - In **Inbound events**, if a source is added for DLP scanning, files downloaded from that source are not scanned by [Threat Emulation](#).

9. From the **Action** list, select one of these:

- **Detect** - Performs the DLP scan but does not block the data.
- **Prevent** - Performs the DLP scan and prevents data transfer if it finds a match to a data type.
- **Allow** - Acts as exclusions, allowing data transfer in certain events.
- **Block** - Blocks the data without the DLP scan.

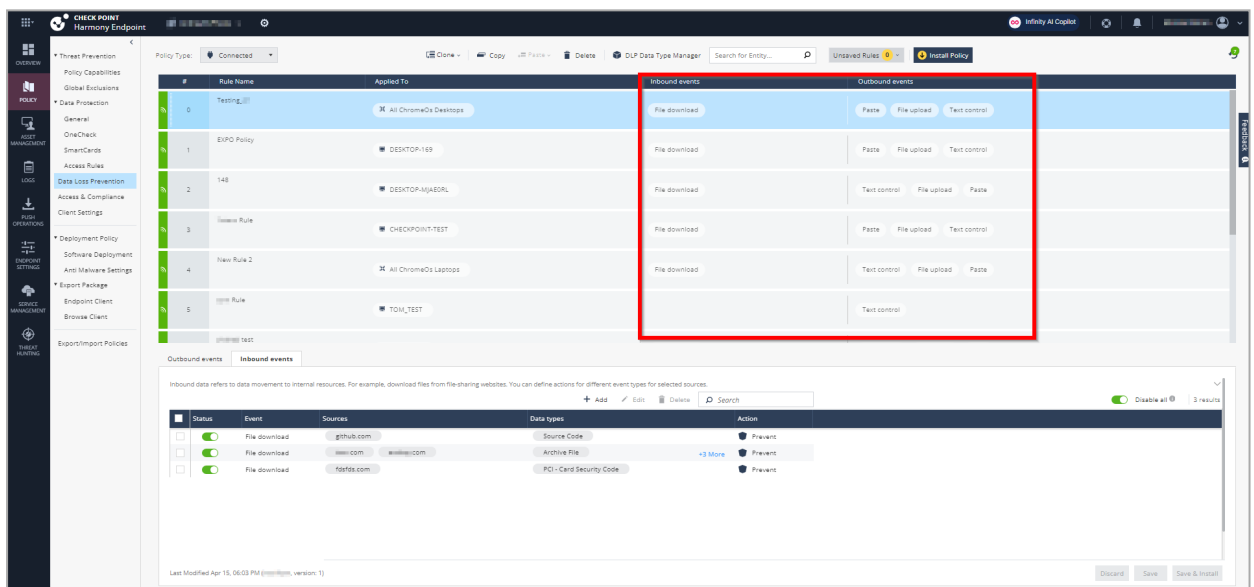
- **Ask** - Asks the user to provide justification before allowing data transfer based on the DLP scan results.
- **Redact** - Performs a DLP scan and removes sensitive data based on a pre-defined set of Data Types. This action is only available for the **Text-control** category.
- **Force redact** - Automatically replaces sensitive data with asterisk.

10. To associate data types with an event, in the **Data types** section, click **+** and select the data type or a group.

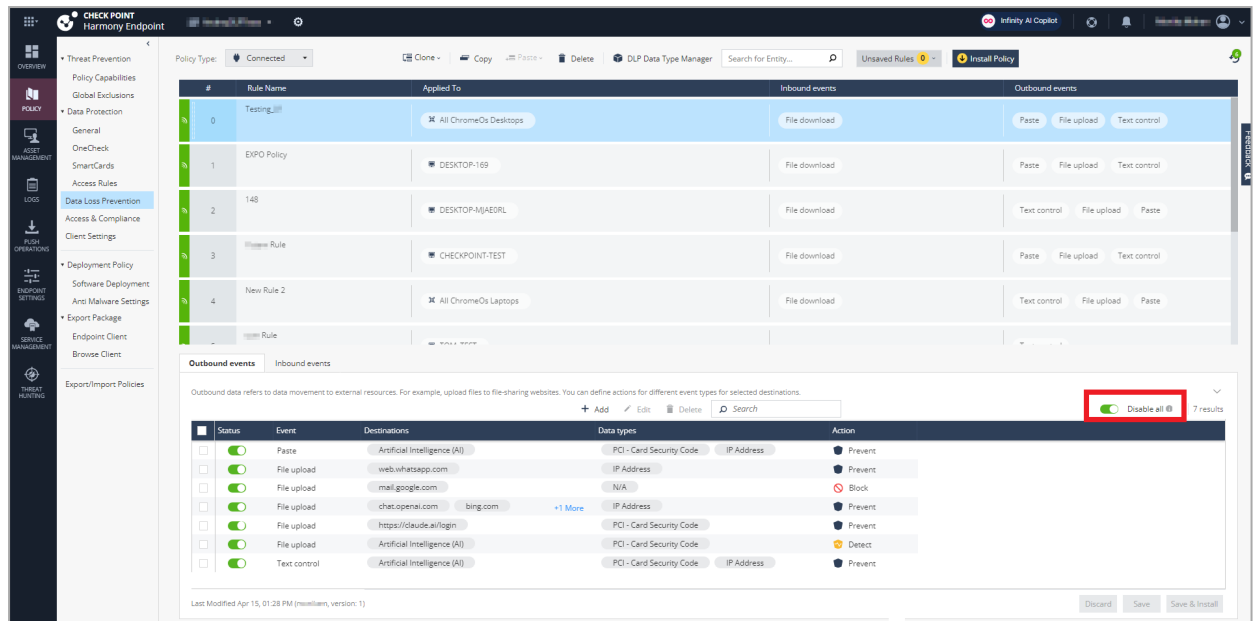
 **Note** - This step is applicable only if the **Action** is **Ask**, **Detect** or **Prevent**.

11. Click **Save**.

The events are displayed in the **Outbound events** and **Inbound events** columns in the DLP rule.

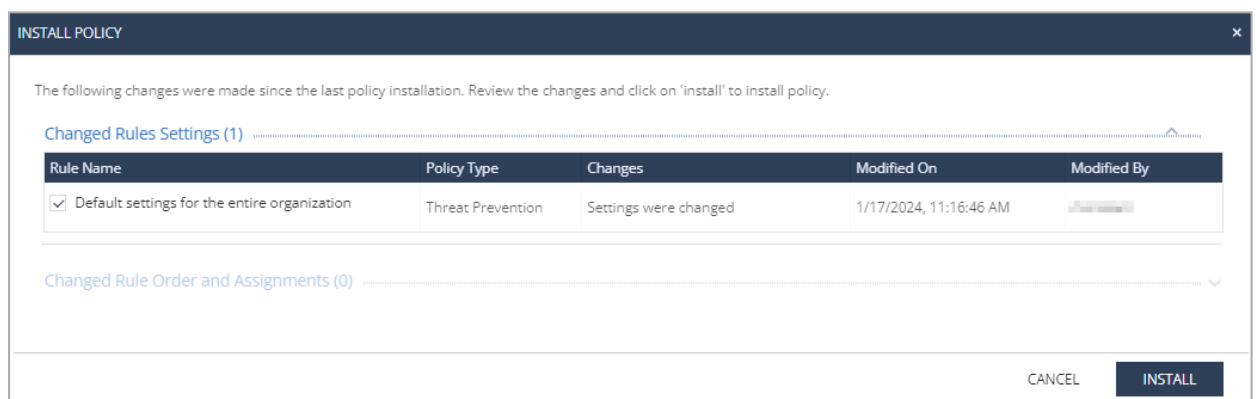


12. To delete an event, select the event that you want to delete and click **Delete**.
13. To edit an event, select the event that you want to edit, click **Edit**, make the required changes and click **OK**.
14. To disable all events, turn off the **Disable all** toggle button.



15. Click **Save & Install**.

The **Install Policy** window appears.

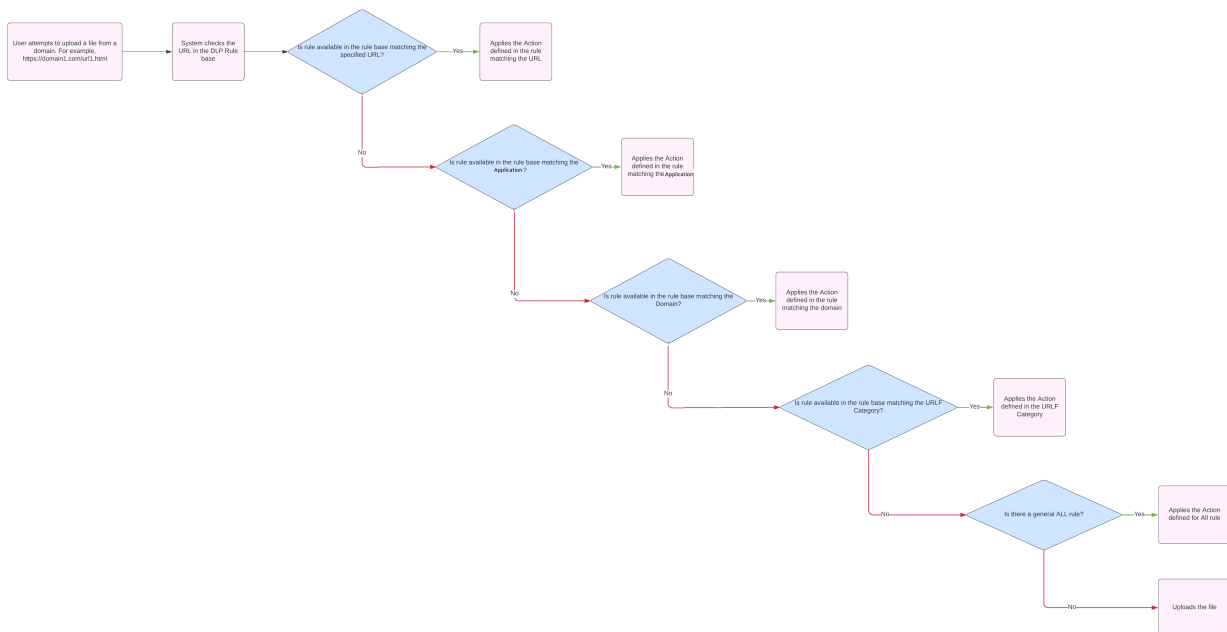


16. Click **Install**.

Rule Configuration Logic

The rule configuration logic offers a systematic method for applying policy rules to events. The system prioritizes the most specific events and progresses through these levels of specificity:

1. **URL**
2. **Application**
3. **Domain**
4. **Category**
5. **All**



Note - The **Paste** and **Text control** events have access only to the **Application** and **Category** levels.

Scenarios

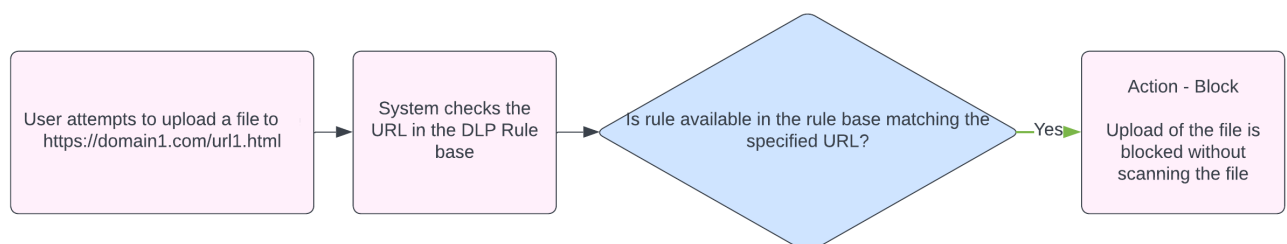
Status	Event	Destinations	Data types	Action
☐	☒ File upload	All	ABA Transit Numbers	Detect
☐	☒ File upload	https://domain1.com/url1.html	N/A	Block
☐	☒ File upload	https://domain1.com/url2.html	N/A	Allow
☐	☒ File upload	domain1.com	PCI - Card Security Code	Prevent
☐	☒ File upload	Computers / Internet	N/A	Allow
☐	☒ File upload	Education	N/A	Block
☐	☒ Paste	ChatGPT	IP Address	Prevent
☐	☒ Paste	Artificial Intelligence (AI)	N/A	Block
☐	☒ Paste	Grammarly	Secret API Key	Ask

Scenario 1: User attempts to upload a file to `https://domain1.com/url1.html`

Specific Event

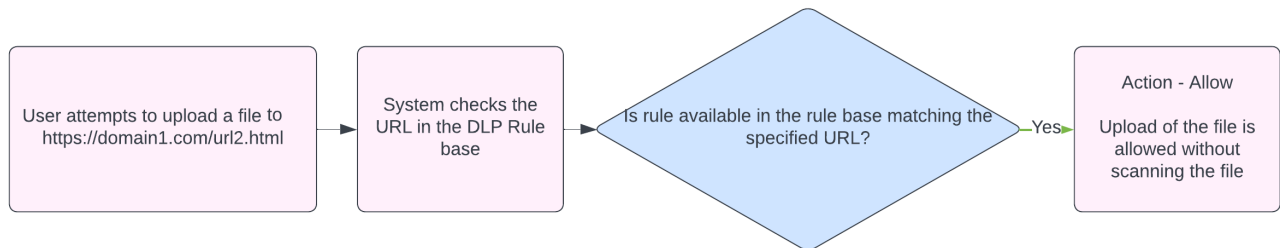
Most specific event is the **URL** `https://domain1.com/url1.html`.

Result

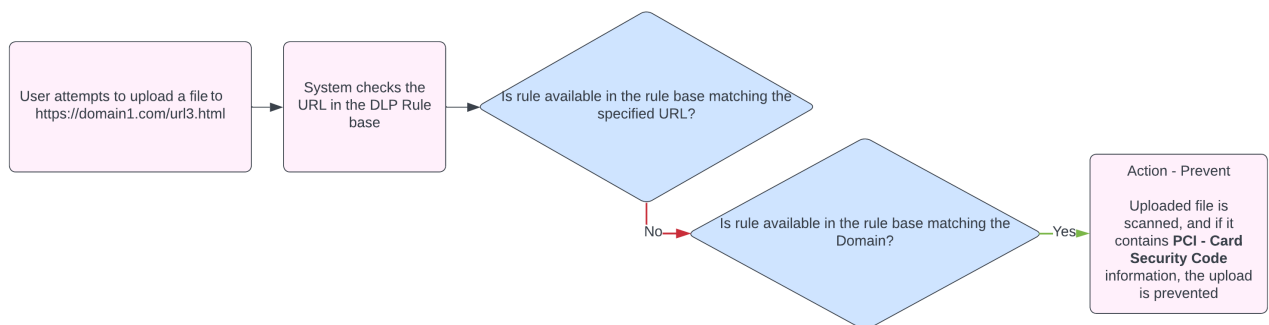


Scenario 2: User attempts to upload a file to `https://domain1.com/url2.html`**Specific Event**

Most specific event is the **URL** `https://domain1.com/url2.html`.

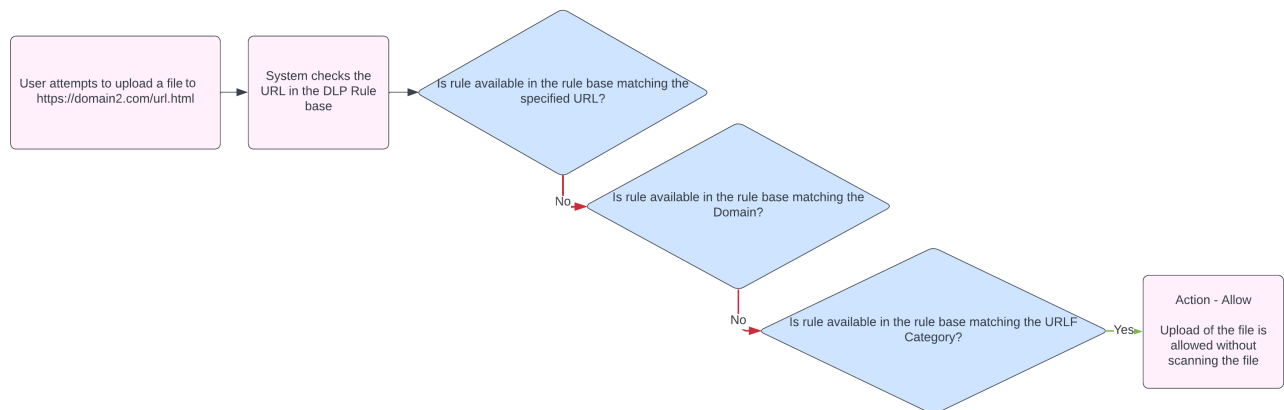
Result**Scenario 3: User attempts to upload a file to `https://domain1.com/url3.html`****Specific Event**

Most specific event is the **Domain** `domain1.com`.

Result**Scenario 4: User attempts to upload a file to `https://domain2.com/url1.html`****Specific Event**

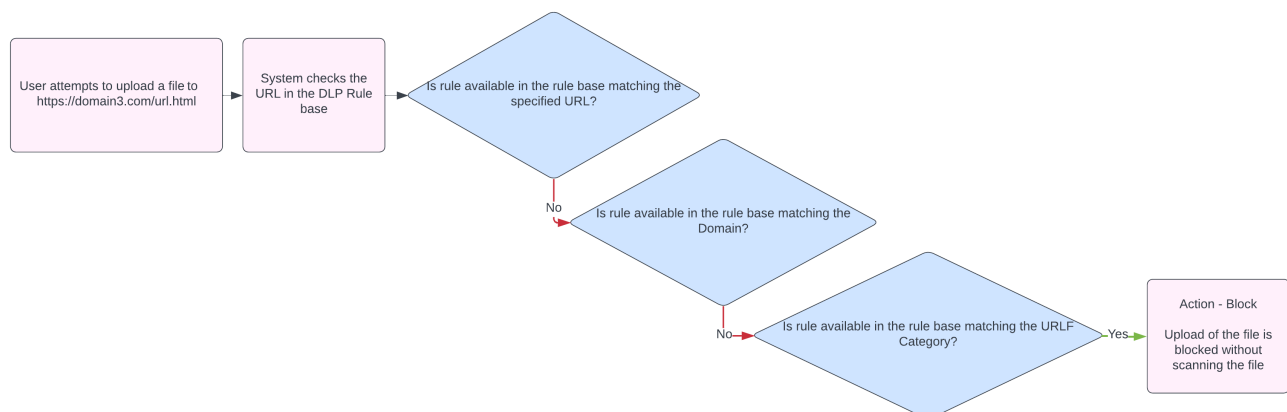
The Category of `domain2.com` is *Computers / Internet*.

Since there are no specific events for the URL or Domain, the **Category** event is selected.

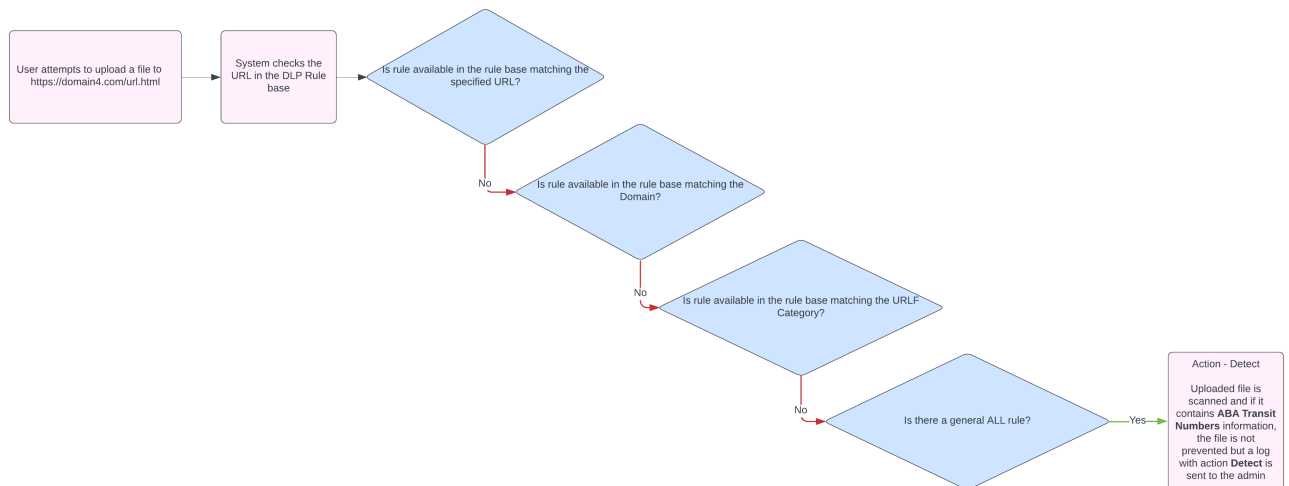
Result**Scenario 5: User attempts to upload a file to `https://domain3.com/url.html`****Specific Event**

The Category of `domain3.com` is *Education*.

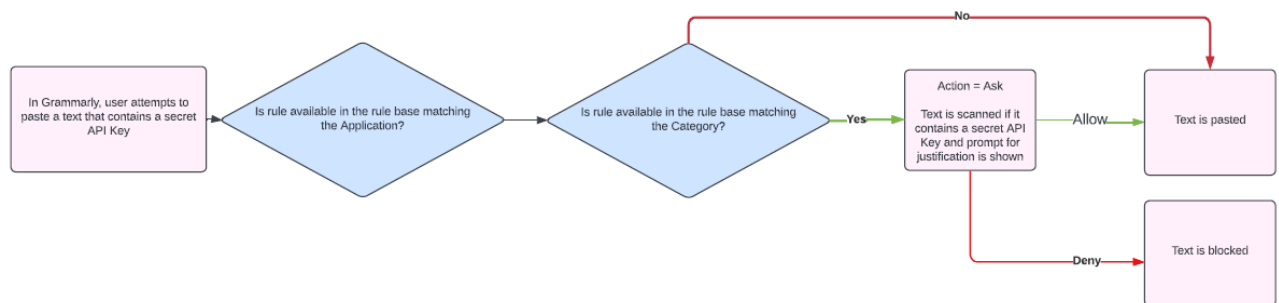
Since there are no specific events for the URL or Domain, the **Category** event is selected.

Result**Scenario 6: User attempts to upload a file to `https://domain4.com/url.html`****Specific Event**

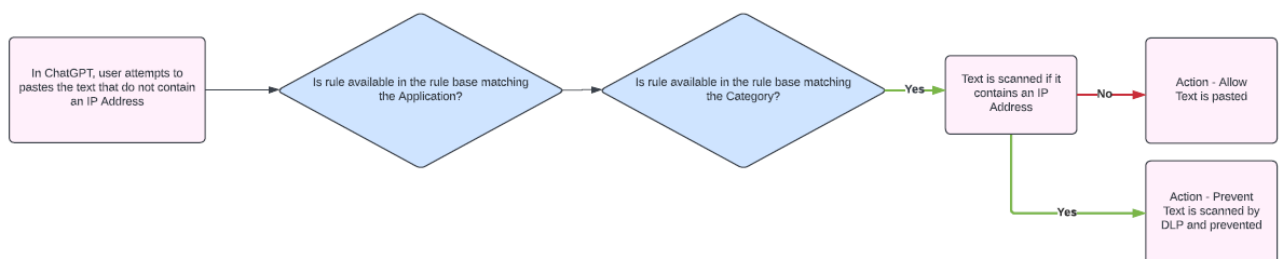
Since there are no specific events for the URL, Domain, or Category, the event with the destination **All** is selected.

Result**Scenario 7: In Grammarly, user attempts to paste a secret API Key****Specific Event**

Most specific event is the **Application Grammarly**.

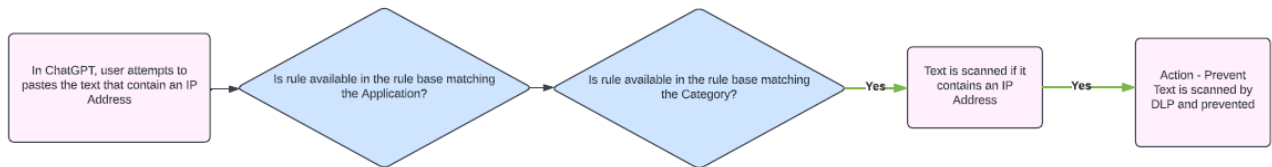
Result**Scenario 8: In ChatGPT, user attempts to paste the text that do not contain an IP address****Specific Event**

Most specific event is the **Application ChatGPT**.

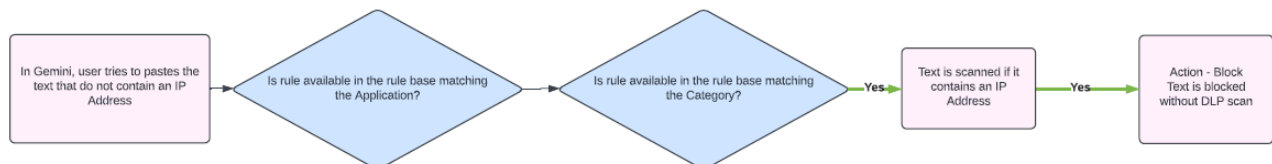
Result

Scenario 9: In ChatGPT, user attempts to paste the text that contain an IP address**Specific Event**

Most specific event is the **Application** *ChatGPT*.

Result**Scenario 10: In Gemini, user attempts to paste the text that do not contain an IP address****Specific Event**

Most specific event is the **Category** *Artificial Intelligence (AI)*.

Result

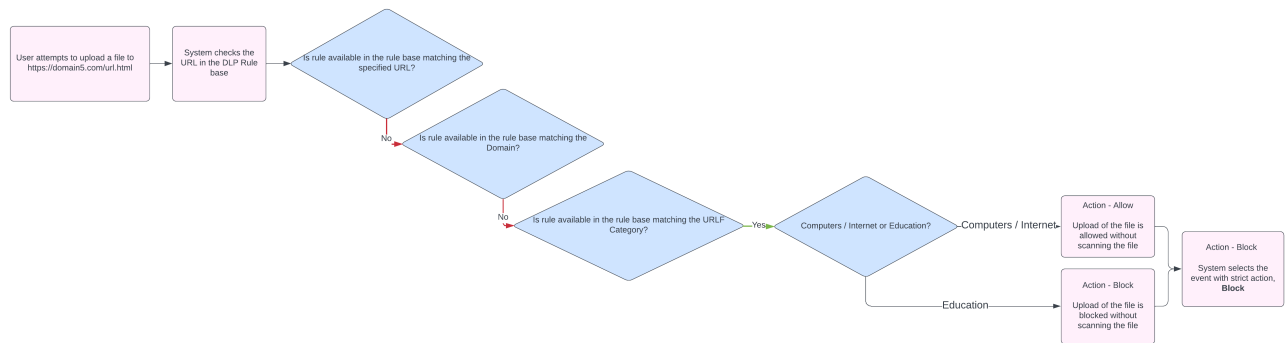
When multiple events are relevant for the same incident, the events with the strict action is selected.

Status	Event	Destinations	Data types	Action
☐	File upload	domain1.com	PCI - Card Security Code	Prevent
☐	File upload	Computers / Internet	N/A	Allow
☐	File upload	Education	N/A	Block
☐	File upload	domain1.com	IP Address	Detect

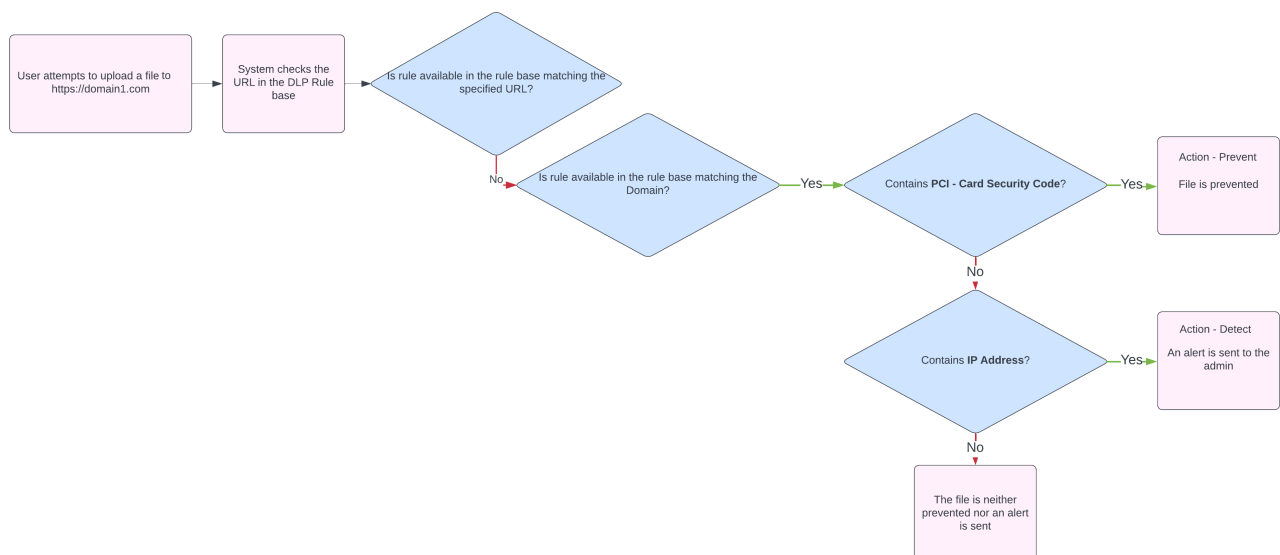
Scenario 11: User attempts to upload a file to `https://domain5.com/url.html`**Specific Event**

The Category of `domain5.com` are *Computers / Internet* and *Education*.

Since there are no events for the URL or Domain, only two events for the **Category** are relevant, and the system selects the event with stricter action.

Result**Scenario 12: User attempts to upload a file to `https://domain1.com`****Specific Event**

Since there are no events for the URL, only two events for the **Domain** *domain1.com* are relevant.

Result

Context Objects

Context objects are AI-based data classification models designed to improve the detection of sensitive information through contextual analysis. These are used exclusively to detect prompts in GenAI applications.

Note - Context Objects are available only for **Artificial Intelligence (AI)** category and can only be used in **Text Control** and **Paste** events.

For the list of available Context Objects, see [sk181662](#).

Enabling GenAI Protect

The Data Loss Prevention policy allows the administrators to enable the **Gen AI Protect** feature on the endpoints. It monitors the use of various generative AI applications in the endpoints. It detects and prevents the sharing of potential confidential information in the prompts to any generative AI applications by the Endpoint Security Clients.

 **Note** - GenAI Protect feature is supported only for the Check Point Portal tenants residing in the EU, India, US, and Australia, and Canada regions.

Prerequisites

- Ensure that the administrator account used to configure GenAI Protect has the required permissions before you enable the feature.
- Create a DLP policy.

 **Note** - The GenAI Protect SaaS dashboard becomes visible only after the first DLP policy is created.

To assign the required permissions:

1. Log in to the Check Point Portal.
2. Go to **Settings > Users**.
3. Select the administrator profile that will be used to configure GenAI Protect, and click **Edit**.
4. In the **Edit User** tab, scroll to the **Global Role** section.
5. In the **Service** drop-down list, select **SaaS**.
6. In the **Specific service role(s)** drop-down list, select **Admin - View All Sensitive Prompts**.
7. Click **Save**.

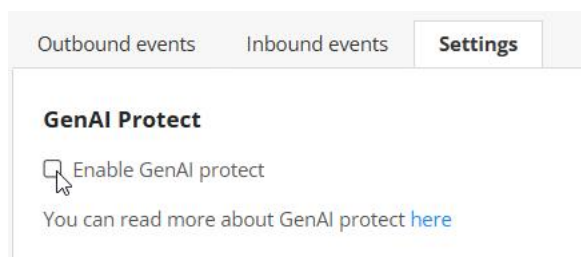
Notes -

- The GenAI Protect SaaS service is visible only to administrators with the **Admin - View All Sensitive Prompts** permission.
- When accessing the GenAI Protect SaaS page for the first time, both the **Add Contract** and **Start Trial** options are displayed. Select **Start Trial**, even if the organization already has a valid license. This step only initializes the service.

To enable GenAI Protect and view the Dashboard:

1. Access the Endpoint Security Administrator Portal.
2. From the left navigation panel, click **Policy > Data Loss Prevention**.

3. Create a Data Loss Prevention policy with **Outbound events** for **Text Control** or **Paste** actions with these options:
 - a. In the **Categories & Subcategories** list, select **Artificial Intelligence (AI)**.
 - b. In the **Action** list, select the action required.
 - Prevent
 - Detect
 - Ask
 - c. In **Data types**, select the data types required for the policy.
 - d. Click **Save**.
4. Go to **Settings** tab and select the **Enable GenAI protect** checkbox.



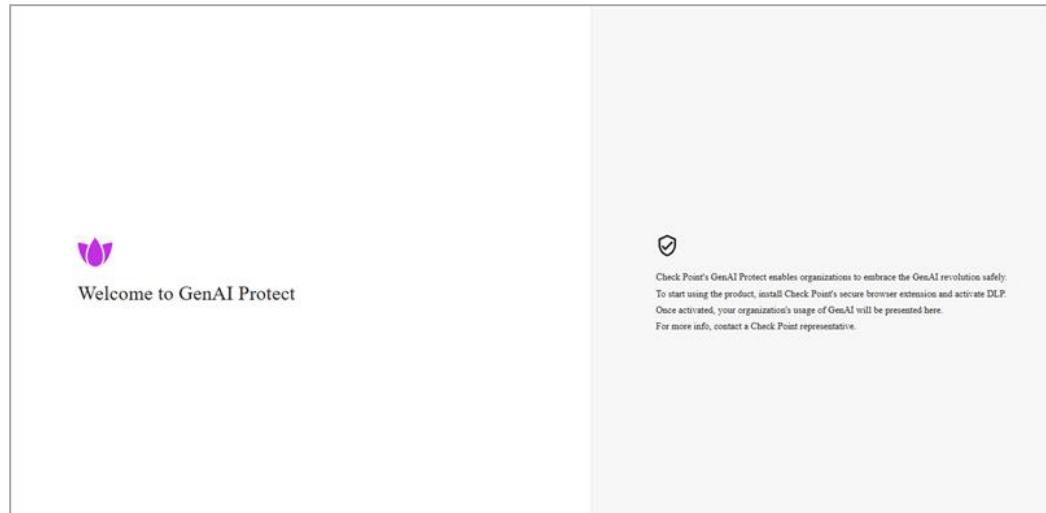
5. Click **Save & Install**.
6. To view the dashboard, from the top right corner of the page, click **GenAI Protect Dashboard**.



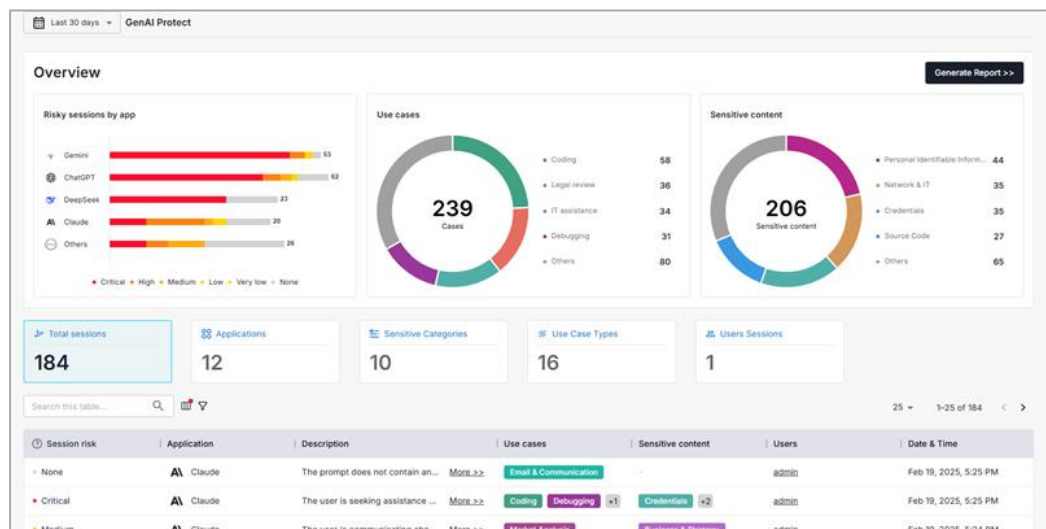
The system redirects you to the SaaS Security Administrator Portal and shows the GenAI Protect Dashboard.

**Notes:**

- If you access the **GenAI Protect** dashboard for the first time, the system might request to activate SaaS Security. Click **Start trial**.
Though GenAI Protect is visible in the SaaS Security Administrator Portal, you do not need additional license to use **GenAI Protect** and it is a part of Endpoint Security Elite license that you have.
- Till the time, the secure browser extension detects events that match the DLP policy rules of GenAI Protect, the system shows the **Welcome** page.



- Once the secure browser extension detects events that match the DLP policy rules of GenAI Protect, the system shows events in the GenAI Protect Dashboard.



For information about how to use GenAI Protect dashboard, see [SaaS Security Administration Guide](#)

Import or Export Policies

Overview

You can import or export all or specific policies in the JSON format for backup purposes or import policies to a new management server.

The supported policies for export and import are:

- Threat Prevention
 - Policy Capabilities
 - Global Exclusions
- Data Protection
 - General
 - OneCheck
- Data Protection
- Access & Compliance
- Client Settings
- Deployment Policy > Software Deployment

Limitations

- We recommend that you avoid modifying policies when you perform this procedure.
- If an export or import fails, you must export or import the file again.
- The import file must be in JSON format.
- If you cancel an import in progress, then the system stops the import but does not revert the files that were imported prior to canceling the import..

Prerequisites

- You must be an Administrator or a Power user to perform this procedure. The Help-desk and Read-only users have read-only access to the Export / Import your policy page. All the other users have no access view the Export / Import your policy page.
- If you are importing policies, ensure that the package or blade version on the target server and in the import file are the same. Otherwise, the system sets the rules as **Do Not Install**.

Exporting Policies

To export all policies:

1. Go to **Policy > Export/Import Policies**.
2. Click **Export**.

The system initiates the export and shows the status of the export. When the export is complete, the system shows the 100% Exported successfully message and downloads the export file to the default downloads folder. The default name of the export file is export_all_DD_MM_YYYY_HH_MM.json.

To export a specific policy:

1. Click **Policy** and go to any one of these pages:
 - **Threat Prevention**
 - Policy Capabilities
 - Global Exclusions
 - **Data Protection**
 - General
 - OneCheck
 - **Access & Compliance**
 - **Client Settings**
 - **Deployment Policy > Software Deployment**

2. Click .

The system initiates the export. When the export is complete, the system downloads the export file to the default downloads folder. The default name of the export file is export_all_DD_MM_YYYY_HH_MM.json.

Importing Policies

To import all policies:

1. Go to **Policy > Export/Import Policies**.
2. Click **Browse To Import** and select the file.



Note - You can edit the file (for example, Notepad++) to import only policies or rules you want..

The system initiates the import and shows the status of the import. When the import is complete, the system shows the 100% Imported successfully message.

To import a specific policy:

1. Click **Policy** and go to any one of these pages:

- **Threat Prevention**
 - Policy Capabilities
 - Global Exclusions
- **Data Protection**
 - General
 - OneCheck
- **Access & Compliance**
- **Client Settings**
- **Deployment Policy > Software Deployment**

2. Click  and select the file.

 **Note** - You can edit the file to import partial policies or rules. You can edit the file (for example, Notepad++) to import only policies or rules you want.

The system initiates the import.

Capabilities of Offline Endpoint Security Client

This table shows the status of capabilities when the Endpoint Security Client is offline, that is, when it is not connected to the Management Server.

Capability	Does it work offline?	Comments
Anti-Malware	Yes	Signatures are not updated.
Anti-Bot and URL Filtering	No	-
Anti-Ransomware, Behavioral Guard, and Forensics	Yes	▪ Signatures are not updated. ▪ The data is not uploaded to Threat Hunting. ▪ The forensic report is not uploaded.

Capability	Does it work offline?	Comments
Threat Emulation and Anti-Exploit	Yes, with the use of a local appliance.	Communication with the Threat Emulation cloud service is blocked.
Remote Access VPN	No	-
Compliance and Posture	Yes	■ The database of vulnerabilities is not updated. ■ Not supported if the client has pre-defined rules that require web access.
Firewall and Application Control	Yes	-
Media Encryption and Port Protection	Yes	Passwords are not updated if the Management Server is not on the same network.
Full Disk Encryption	Yes	■ Self-unlock is not supported if the Management Server is not on the same network. ■ Passwords are not updated if the Management Server is not on the same network.

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, like 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 Full Disk Encryption Drive Slaving Utility and Dynamic Mount Utility that let 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. Smart Card users must use this option for recovery.

To perform full recovery with recovery media

1. Go to **Asset Management > Organization > Computers**.
2. From the top toolbar, click  and select **Remote Help & Recovery > Recovery > Full Disk Encryption Recovery**.

3. Search for the computer which you want to decrypt.

The **OS Name** and **OS version** of the computer are displayed.

4. **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 user or temporary users who can use the recovery media.
 - b. In the window that opens add a username and a password that the users use to access the file.
5. Download the recovery file.
6. Create the recovery media:

Step	Description
1	On the Endpoint Security client, go to folder: C:\Program Files(x86)\CheckPoint\Endpoint Security\Full Disk Encryption\
2	Double-click <code>UseRec.exe</code> 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 R73 and all E80.x versions. You can use the Full Disk Encryption Drive Slaving Utility instead of disk recovery.

 Notes:

- 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 in Windows Command Prompt to start the Full Disk Encryption Drive Slaving Utility:

```
<DISK:>\Program files (x86)\CheckPoint\Endpoint Security\Full  
Disk Encryption\fde_drive_slaving.exe
```

The **Full Disk Encryption - Drive Slaving** window opens.

-  **Note** - To unlock a protected USB connected hard disk drive, you must first start the Drive Slaving Utility, and then connect the disk drive.

2. Select a Full Disk Encryption protected disk to unlock.

The **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 **Asset Management > Organization > Computers**.
2. From the top toolbar, click  and select **Remote Help & Recovery > Recovery > BitLocker Recovery**.

The **BitLocker Management Recovery** window opens.

3. Select **By Recovery Key ID** and 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.

4. 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
```

5. 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 macOS.

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	Description
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	Description
1	Get the serial number of the locked device from the user.
2	Go to Asset Management > Organization > Computers .
3	From the top toolbar, click  and select Remote Help & Recovery > Recovery > FileVault Recovery .
4	In the Computer's Serial Number field, enter the serial number.
5	Click Get Recovery Key .
6	Give the recovery key to the user.

3. User resets their password.

Step	Description
1	Get the Recovery Key from the support representative.
2	Restart the macOS.

Step	Description
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	Enter the recovery key and click the right arrow. A progress bar shows.
5	For Local Users: - In the Reset Password window, the user enters a new password, and optionally, a password hint. - Click Reset Password.

For more information, see [sk138352](#).

A personal key is unique to the client macOS-based computer or device. The key is a string of letters and numbers separated by dashes.

To recover a user's FileVault-encrypted macOS using the personal key, the administrator reads the key to the user, and uses the key to decrypt and unlock the computer.

Decrypting and recovering the user's FileVault-encrypted macOS

■ For a volume formatted as APFS on macOS Mojave 10.14 and higher

1. Show the disk volumes on the macOS:

```
diskutil apfs list
```

The volume to recover is the OS Volume. It has a name similar to `disk2s1`.

2. Unlock the volume:

```
diskutil apfs unlockVolume <Disk Name> -passphrase  
<Personal Recovery Key>
```

3. Get the list of apfs cryptousers:

```
diskutil apfs listcryptousers <Disk Name>
```

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:

```
diskutil apfs decryptVolume <diskname> -user <user  
UUID>
```

5. Enter the password of the local user.

6. Monitor the progress of the decryption:

```
diskutil apfs list
```

■ For a volume formatted as CoreStorage on macOS 10.12 or higher

1. Unlock the volume:

```
diskutil cs unlockVolume <Logical Volume UUID> -  
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:

```
diskutil cs decryptVolume <Logical Volume UUID>
```

4. When prompted, enter the password for the local user.

5. Monitor progress of the decryption:

```
diskutil cs list
```

The user can now reboot the macOS normally. They do not see the FileVault pre-boot screen.

Managing Virtual Groups

Virtual Groups manage groups of users and 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 users and devices assigned to them automatically.

To create a virtual group:

1. Access Endpoint Security and click **Asset Management**.
2. Go to **Organization > Organizational Tree** and select **Virtual Groups**.
3. To create a virtual group for a group, right-click a group.
4. To create a virtual group for a specific device or a user, click the group and right-click the device or user.
5. Select **Create Virtual Group**.

The **Create Virtual Group** window appears.

6. In the **Name** field, enter a group name.
7. (Optional) In the **Comment** field, enter a comment.

 Notes:

- A user or a device can belong to multiple virtual groups.
- Selecting a certain user or 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 users or devices to the group, or select users or devices first and then create a group from them.

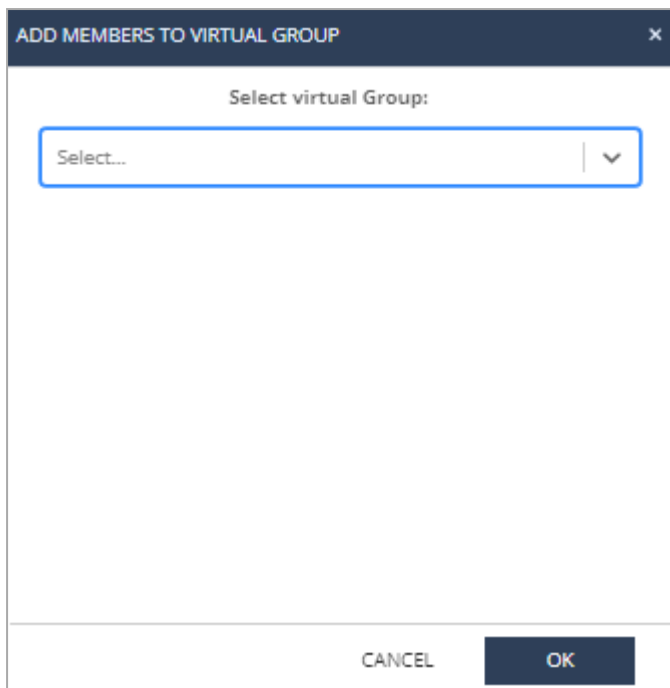
8. Click **OK**.

 **Note** - You can also perform this procedure from **Asset Management > Organization > Computers**. See ["Managing Computers" on page 183](#).

To add a group, device or a user to a virtual group:

1. Access Endpoint Security and click **Asset Management**.
2. Go to **Organization > Organizational Tree** and select **Virtual Groups**.
3. To add a group to a virtual group, right-click a group.
4. To add a specific device or a user to a virtual group, click the group and right-click the device or user.
5. Select **Add to Virtual Group**.

The **Add Members to Virtual Group** window appears.



6. Select the applicable virtual group.
7. Click **OK**.

Note - You can also perform this procedure from **Asset Management > Organization > Computers**. See ["Managing Computers" on page 183](#).

To create and add to virtual group:

1. Access Endpoint Security and click **Asset Management**.
2. Go to **Organization > Organizational Tree** and select **Virtual Groups**.
3. To create and add a group to a virtual group, right-click a group.
4. To create and add a specific device or a user to a virtual group, click the group and right-click the device or user.
5. Select **Create and Add to Virtual Group**.

The **Add Members to Virtual Group** window appears.

ADD MEMBERS TO VIRTUAL GROUP [X]

Name
Group name

Comment
Comment

Members

Search 1 items

Name
CHECKPOINT-TEST

CANCEL OK

6. In the **Name** field, enter a group name.
7. (Optional) In the **Comment** field, enter a comment.
8. In the **Members** section search box, search and select the member.
9. Click **OK**.

Note - You can also perform this procedure from **Asset Management > Organization > Computers**. See ["Managing Computers" on page 183](#).

To move devices from one virtual group to another:

1. In the left navigation panel, click **Asset Management**.
2. In the left pane, click **Organization > Organizational Tree**.
3. Click **Virtual Groups**.
4. Move the devices:
 - To move all the devices from a virtual group, select the virtual group.
 - To move specific devices from a virtual group, click the virtual group, and select the devices.
5. Right-click the virtual group or devices and select **Move to Virtual Group**.

The **Move Members to Virtual Group** window appears.

6. Select the virtual group where you want to move the devices.
7. Click **OK**.

To export the list of devices in a virtual group to an excel file:

1. From the left navigation panel, click **Asset Management > Organization > Organization Tree**.
2. From the list, click **Virtual Group**.
3. Right-click the virtual group and select **Export Virtual Group Report**.

The system exports the list of devices to an excel file. If the virtual group contains child virtual groups, then the devices in those virtual groups are also included in the exported file.

Managing Active Directory Scanners

Endpoint Security can scan and import users, groups, Organizational units (OUs) and computers from multiple supported directory domains. After the objects are imported, you can assign policies.

Notes:

- Endpoint Security does not scan groups of the type Distribution in Microsoft Active Directory.
- If a device belongs to both Microsoft Active Directory and Microsoft Entra ID domains, then the Microsoft Active Directory takes precedence.
- To move a device from the Microsoft Active Directory domain to Microsoft Entra ID domain:
 - a. Disconnect the device from Microsoft Active Directory domain.
 - b. Register the device with Microsoft Entra ID.
- Media Encryption, Remote Help, and automatic access do not work if you install the scanner after installing Media Encryption. To ensure proper operation, install the required scanner (Microsoft Entra ID or Active Directory) before you install Media Encryption.

Supported Directory

- Microsoft Active Directory
- Microsoft Entra ID

Prerequisites

Endpoint Security requires permissions to scan the directory. Ensure that the directory account has the following permissions for each directory scanner:

- The Active Directory root
- Child containers and objects
- Deleted objects container - Deleted objects in directory are stored in the Deleted objects temporarily. Endpoint Security compares the objects in the directory with the Deleted objects container to know the objects that have changed since the last scan.

Managing Microsoft Active Directory Scanner

Organization Distributed Scan

Organization Distributed Scan is enabled by default. You can see its configured settings in the **Endpoint Settings** view > **Default Scanner**.

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 Endpoint Security 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. From the left navigation panel, click **Asset Management**.
2. In the left pane, click **Computers**.
3. From the top toolbar, click  (General Actions) and click **Directory Scanner**.

The **Scanner** window opens.

4. Fill in this information:

Section	Required Information
Connect from computer	▪ Computer name - Select a computer as your AD scanner.
AD Login details	▪ User name (AD) - Enter the user name to access the Active Directory. ▪ Domain name - Enter the domain of the Active Directory. ▪ Password (AD) - Enter the password to access the Active Directory.

Section	Required Information
AD Connection	■ Domain controller - Enter the name of the Domain controller. ■ Port - Enter the number of the listening port on the Domain controller. ■ Use SSL communication (recommended) - Select this checkbox if you want the connection between the AD scanner to the Domain Controller to be over SSL. ■ LDAP Path - The address of the scanned directory server. ■ Search filter - If required, enter search criteria to selectively sync only matching entries from the directory server. For more information, see LDAP syntax. ■ Sync AD every - Specify the time interval in minutes for the system to initiate the scan. Supported range is 5 (min) to 240 (max) minutes.  Notes - • If you set a value outside the supported range (for example 4 or 241), the system resets the value to the closest threshold value. • The recommended time interval is 120 minutes.

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 open the AD scanner configuration pop-up from **Endpoint Settings > AD Scanners > Default Scanner > Setup full Active Directory sync**.

Managing Microsoft Entra ID Scanners

Endpoint Security can scan and import users, groups, administrative units and computers from multiple Microsoft Entra ID into the Endpoint Security. After the objects are imported, you can assign policies.

 **Note** - Endpoint Security does not scan groups of the type Distribution in Microsoft Entra ID.

Limitations

- The Microsoft Entra ID scanner supports Windows only. For macOS devices, use Microsoft Intune.
- User SmartCard is not supported.
- Hybrid mode is not supported.
- The user, device or group can be member of only one Administrative unit.

- The maximum characters supported for **Display Name** is 45.
- Microsoft Entra ID scanner sync stops if the Endpoint Security server is down for a duration of 30 days and above. To restart, contact [Check Point Support](#).
- Microsoft Entra ID does not work if [Full Disk Encryption](#) security blade is enabled.
- If [Full Disk Encryption](#) is enabled and the user changes their password, the user must lock and unlock the device for the new password to take effect.
- Supported only with Endpoint Security Client version E88.50 and higher.
- The Domain Controller (DC) must have sufficient permissions to query LDAP.
- Passwords cannot contain the following special characters:
 , > & ' " \ /
- To view deleted objects, enable the Recycle Bin in AD Admin.
- Querying a Load Balancer is not supported. The query must be sent directly to the DC. For more information, see [SK184794](#).

Configuring the Settings in the Microsoft Entra ID Portal

Before you can add Microsoft Entra ID to Endpoint Security, it is necessary to create the Microsoft Entra ID credentials.

Step 1: Register the Application

1. Log in to the [Microsoft Entra ID](#).
2. From the toolbar select **Azure Active Directory**.
3. Select **App registrations** > click **New Registration**.
4. Below the **Owned applications** tab, enter the application's **Name** > select an **Account**

type > click **Register**.

Home > Check Point | App registrations >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Check Point App ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Check Point only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform ▼ e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Step 2: Add Permissions to the Application

1. Add the necessary permissions to the application.
 - a. Go to the **API permissions** section and click **Add a permission**.

Home > Check Point | App registrations > Check Point App

Check Point App | API permissions

Search << Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission.

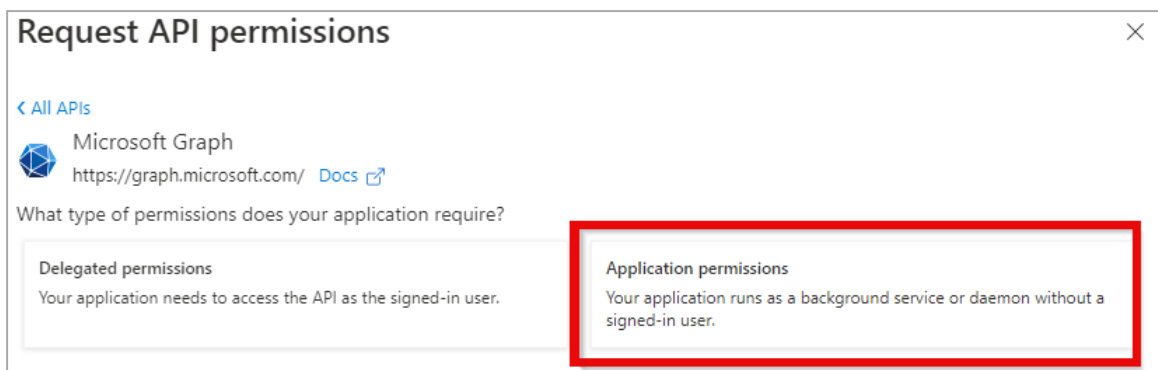
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Check Point

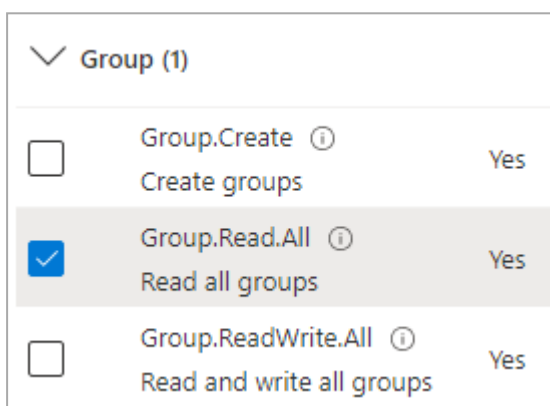
API / Permissions name	Type	Description	Admin consent required
▼ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No

- b. In the window that opens, select **Microsoft Graph > Application permissions**.



2. Select these permissions:

■ **Groups.Read.All**



■ API Permissions:

○ Device.Read.All

▼ Device (1)		
☒	Device.Read.All ⓘ Read all devices	Yes
☐	Device.ReadWrite.All ⓘ Read and write devices	Yes

○ Directory.Read.All

▼ Directory (1)		
☒	Directory.Read.All ⓘ Read directory data	Yes
☐	Directory.ReadWrite.All ⓘ Read and write directory data	Yes
☐	Directory.Write.Restricted ⓘ Manage restricted resources in the directory	Yes

○ GroupMember.Read.All

▼ GroupMember (1)		
☒	GroupMember.Read.All ⓘ Read all group memberships	Yes
☐	GroupMember.ReadWrite.All ⓘ Read and write all group memberships	Yes

○ AdministrativeUnit.Read.All

▼ AdministrativeUnit (1)		
☒	AdministrativeUnit.Read.All ⓘ Read all administrative units	Yes
☐	AdministrativeUnit.ReadWrite.All ⓘ Read and write all administrative units	Yes

- **User.Read.All**

User (1)		
☐	User.EnableDisableAccount.All ⓘ Enable and disable user accounts	Yes
☐	User.Export.All ⓘ Export user's data	Yes
☐	User.Invite.All ⓘ Invite guest users to the organization	Yes
☐	User.ManageIdentities.All ⓘ Manage all users' identities	Yes
☒	User.Read.All ⓘ Read all users' full profiles	Yes
☐	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

3. Give admin consent to the selected permissions.

Home > Check Point | App registrations > Check Point App

Check Point App | API permissions

Overview
Quickstart
Integration assistant

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting
Troubleshooting
New support request

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

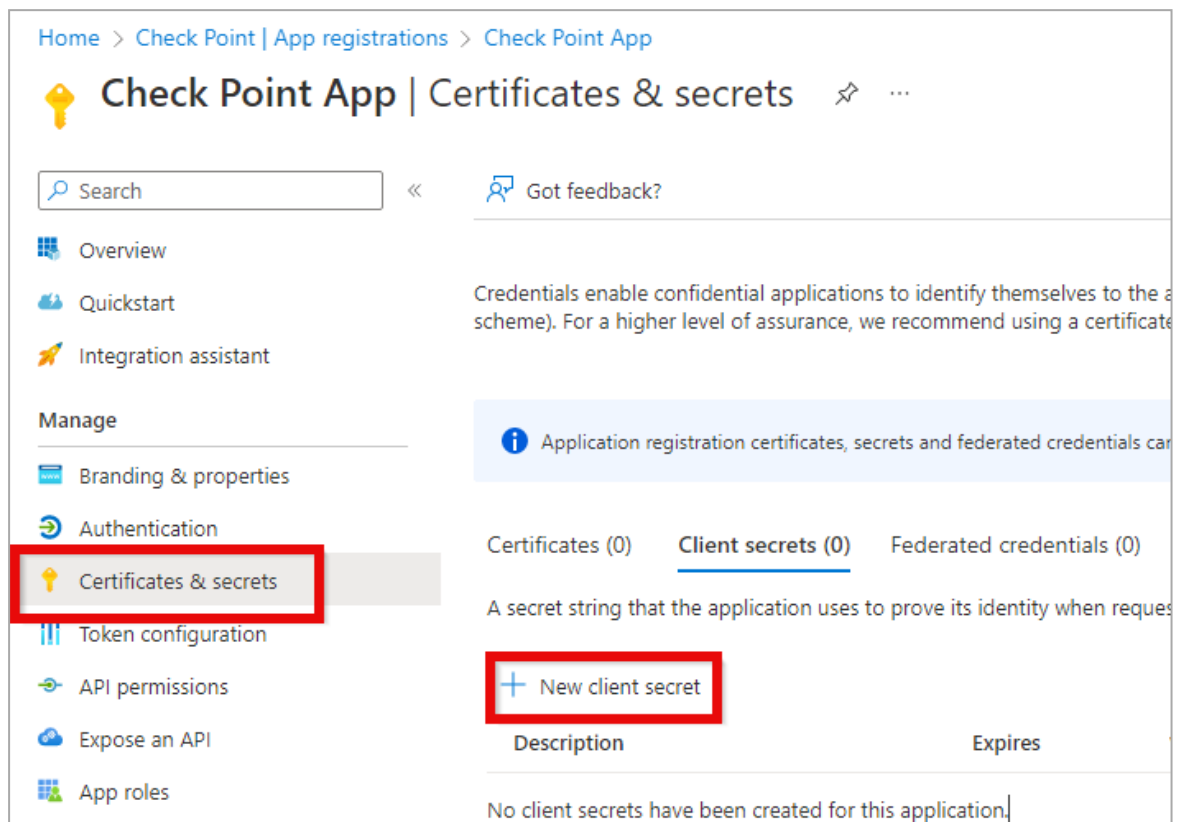
+ Add a permission ☒ Grant admin consent for Check Point

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (6)				
AdministrativeUnit.Read.All	Application	Read all administrative units	Yes	⚠ Not granted for Check P... ***
Device.Read.All	Application	Read all devices	Yes	⚠ Not granted for Check P... ***
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for Check P... ***
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for Check P... ***
GroupMember.Read.All	Application	Read all group memberships	Yes	⚠ Not granted for Check P... ***
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Check P... ***

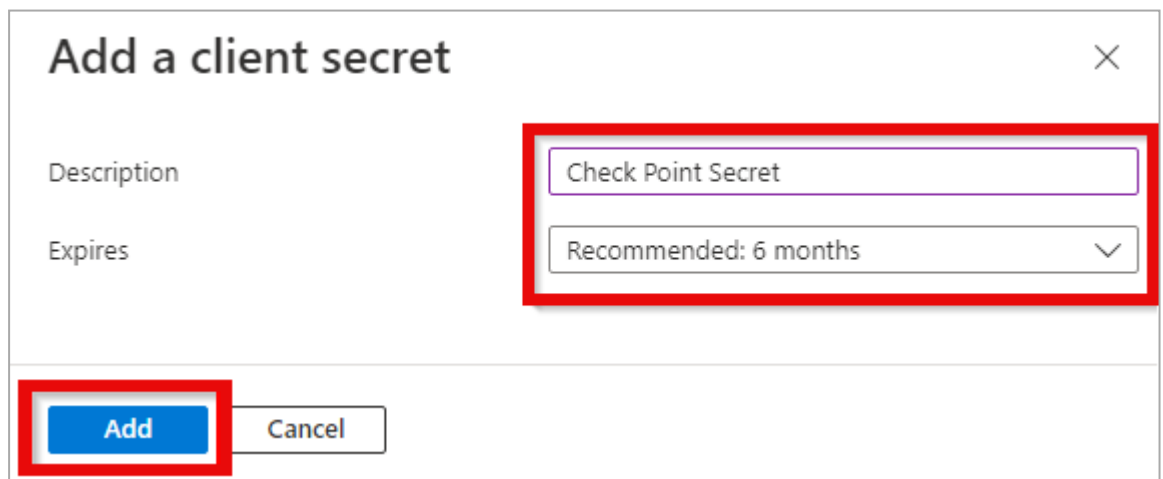
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Step 3: Finish Configuration in Microsoft Entra ID:

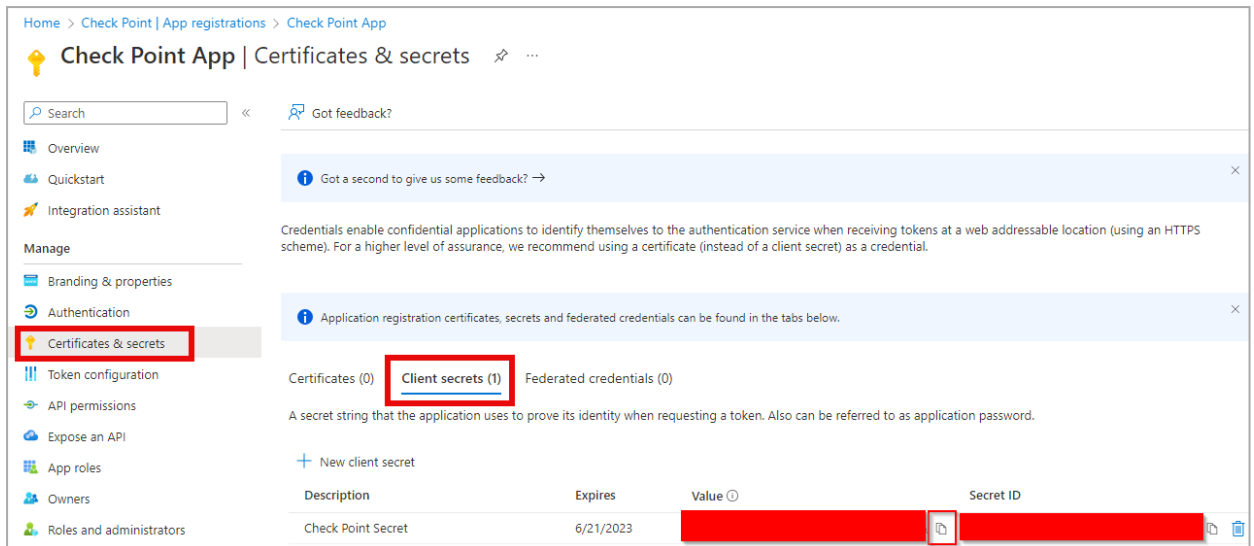
1. Create a secret key for the application.
 - a. Go to the section **Certificates & secrets** > click **New client secret**.



- b. In the **Add a client secret** window, enter a **Description** and the date it **Expires** > click **Add**.

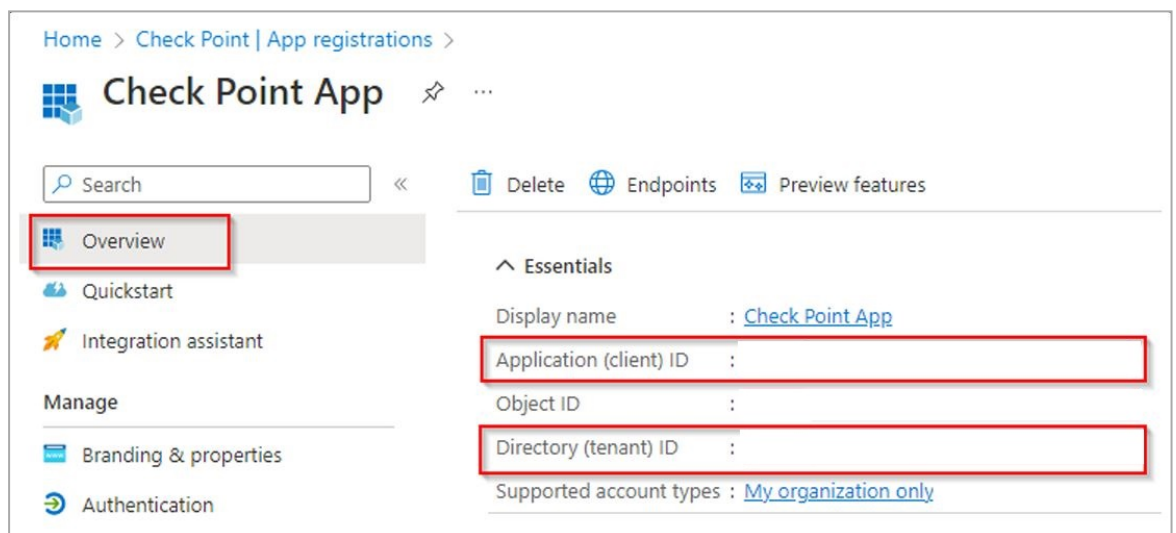


2. Copy the value of the secret key and keep it in a secure place. This key is necessary for the Endpoint Security portal integration with Microsoft Entra ID.



3. Go to the **Overview** section, copy these two values, and keep them in a secure place.

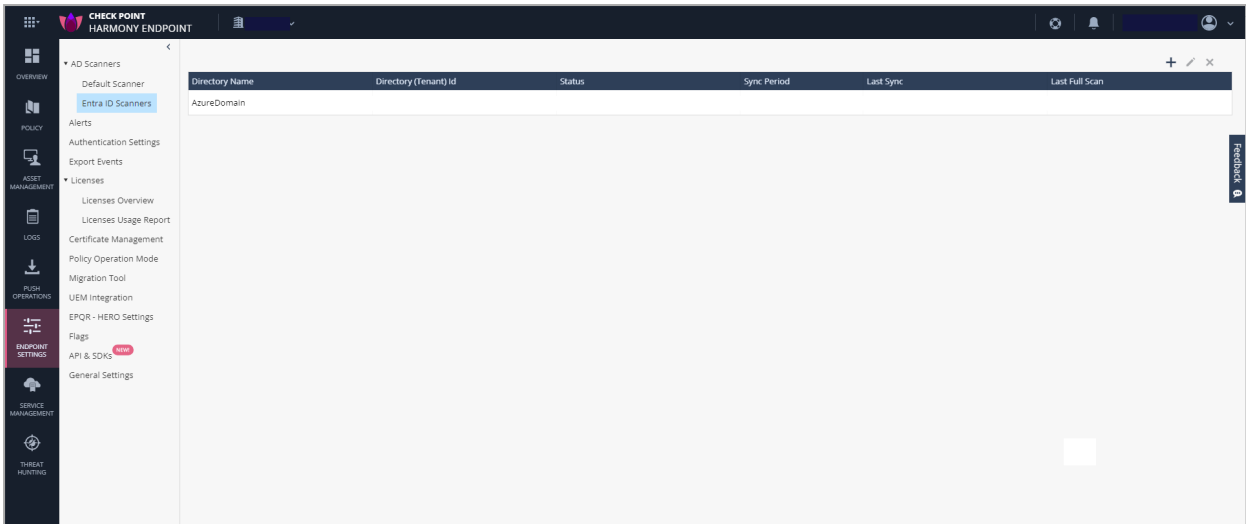
- **Application (client) ID**
- **Directory (tenant) ID**



Importing Objects from Microsoft Entra ID

To import objects from Microsoft Entra ID:

1. Go to **Endpoint Settings**.
2. Expand **AD Scanner** and click **Entra ID Scanners**.



Section	Description
Directory Name	Name of the directory.
Directory (Tenant) ID	Tenant ID from your Microsoft Entra ID portal.
Status	Status of the Microsoft Entra ID directory scan.
Sync Period	Frequency at which Endpoint Security initiates the scan to fetch the data from Microsoft Entra ID.
Last Sync	Date and time when Endpoint Security last synced with Microsoft Entra ID.
Last Full Scan	Date and time of the last full scan of the Microsoft Entra ID.

3. In the top right corner, click **+** .
- The **Add Entra ID Scanner** window appears.

ADD ENTRA ID (AZURE AD) SCANNER

1 INSERT CREDENTIALS

2 INSERT ADDITIONAL CONFIGURATIONS

Enter your credentials. For more information, see the guide [here](#)

Directory (tenant) ID *

Application (client) ID *

Client Secret Key *

4. Enter these:

- a. **Directory (Tenant) ID**
- b. **Application Client ID**

You can obtain these from your [Microsoft Entra ID](#) portal.

Home > Check Point | App registrations >

Check Point App

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Essentials

Display name : [Check Point App](#)

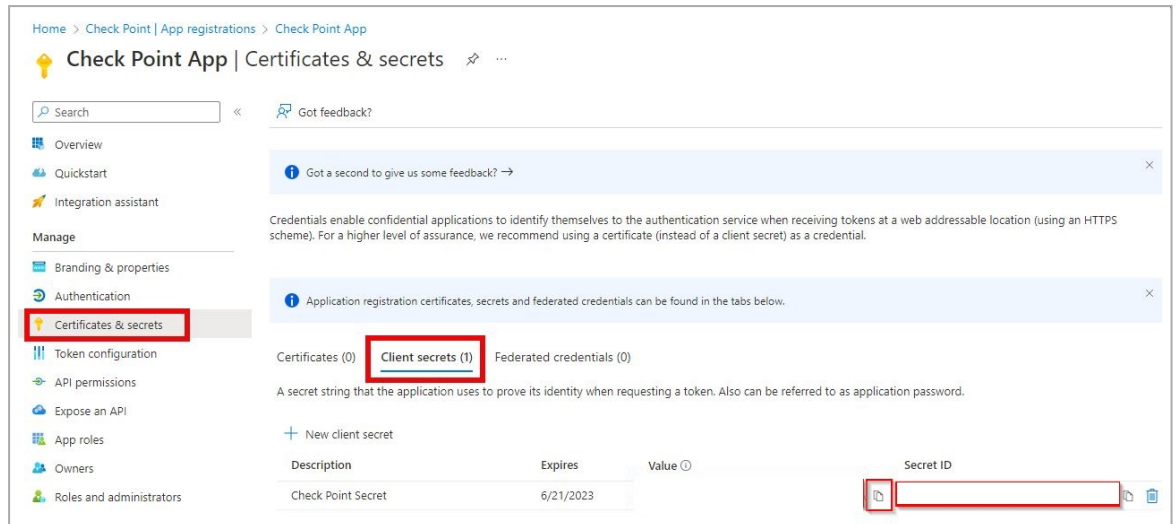
Application (client) ID :

Object ID :

Directory (tenant) ID :

Supported account types : [My organization only](#)

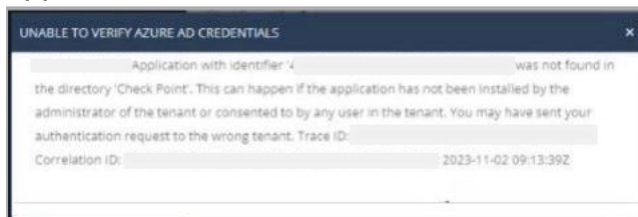
c. Secret ID



You can obtain the **Secret ID** from your [Microsoft Entra ID](#) portal.

5. Click **Verify**.

Note - Make sure that the information you copy from the Microsoft Entra ID portal are entered accurately. If the verification fails, the following dialog box appears:



6. Click **Next**.

7. In the **Root Name** field, enter a name for the root directory.

8. In the **Sync Interval** field, specify the interval (in minutes) for the sync between Endpoint Security and Microsoft Entra ID.

9. Click **Add**.

ADD ENTRA ID (AZURE AD) SCANNER

1 ☒ INSERT CREDENTIALS

2 ☐ INSERT ADDITIONAL CONFIGURATIONS

Root Name *

Choose your Directory root name

Sync Interval

120

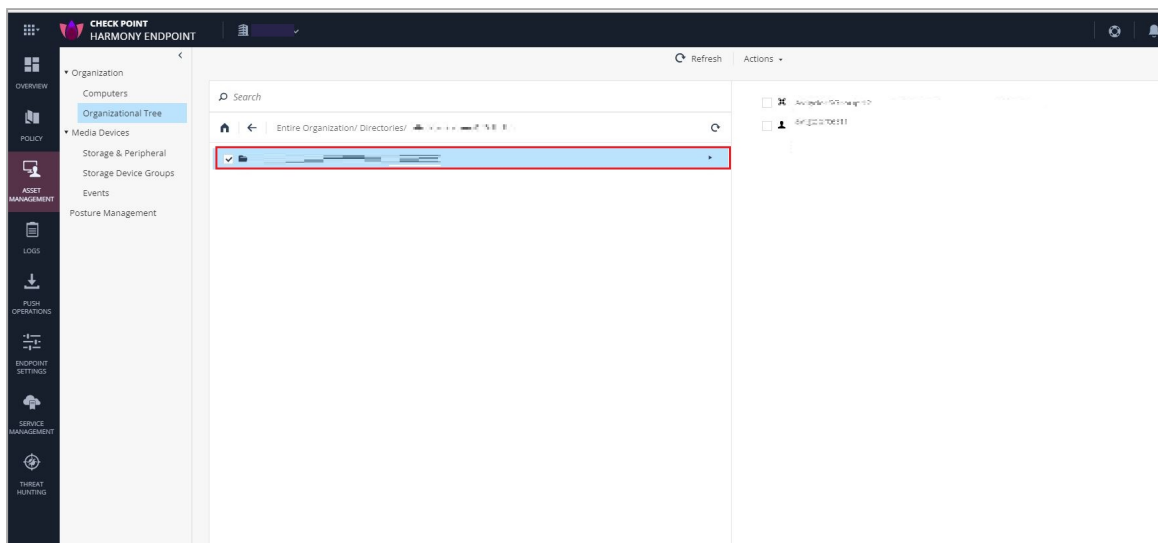
BACK ADD

The Microsoft Entra ID directory is added to the table.

10. To edit a directory, select the directory and at the top right pane, click .
11. To delete a directory, select the directory and at the top right pane, click .
12. To verify whether the Microsoft Entra ID is successfully imported:

- a. Go to **Asset Management**.
- b. Expand **Organization > Organizational Tree > Directories**.

The root Microsoft Entra ID should be listed in the table.



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 **Asset Management > Organization > Computers**.
2. Click  and select **Remote Help & Recovery > Full Disk Encryption**.
3. Select the type of assistance the end-user needs:
 - **One-Time Logon** - Provides 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.
4. Search for the locked computer.
5. Select the applicable user from the list (this step is not applicable in the case of Pre-Boot Bypass Remote Help).
6. Tell the user to enter the **Response one** text string in the Remote Help window on the locked computer.

The endpoint computer shows a challenge code.
7. In the **Challenge (from user)** field, enter the challenge code that the user gives you.
8. Click **Generate Response**.

Remote Help authenticates the challenge code and generates a response code.
9. Tell the user to enter the **Response Two (to user)** text string in the Remote Help window on the locked computer.
10. Make sure that the user changes the password or has one-time access to the computer before ending the Remote Help session.

Active Directory Authentication

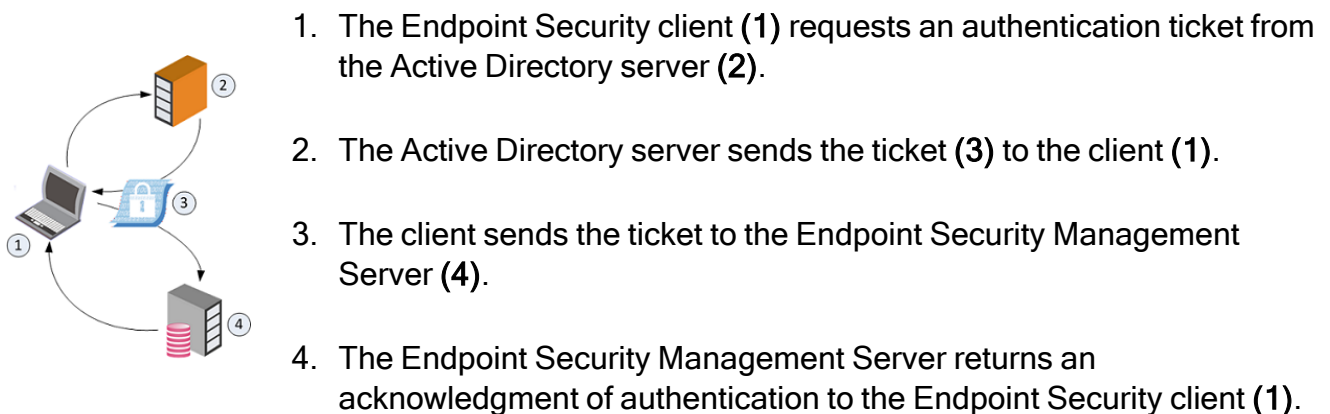
Endpoint Security Active Directory Authentication

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:



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 Endpoint Security.

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/nacl.com@NAC1.COM mapuser auth-
user@NAC1.COM pass 123456 out outfile.keytab
```

Parameters:

Syntax	Example Value	Explanation
<code><Service Name></code>	tst	Name of the service.
<code><realm name></code> <code><REALM NAME></code>	nacl.com NAC1.COM	Domain name of the Active Directory server. The first instance is in lower case. The second instance in upper case.
<code><Username></code>	auth-user	The Active Directory domain user.
<code><Password></code>	123456	Password for user.
<code><Name of Output File></code>	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: nacl-dc.nacl.com
Successfully mapped tst/nacl.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/nacl.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 Endpoint Security 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 Endpoint Security, go to the **Endpoint Settings** view > the **Authentication Settings** tab.
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 561](#):

Field	Description
Domain name	Active Directory domain name. For example: <code>nacl.com</code>
Principle Name	Authentication service name in the format: <code>ServiceName/realm@REALM</code> This value must match the name that was configured in Active Directory > New Object . For example: <code>tst/nacl.com@NACL.COM</code>
Version Key	Enter the version number according to the Active Directory output in the <code>vno</code> field. For example: 7
Encryption method	Select the encryption method according to the Active Directory output in the <code>etype</code> field. For example: <code>RC4-HMAC</code>

Field	Description
Password	Enter (and confirm) the password of the Active Directory Domain Admin user you created for Endpoint Security use. For example: 123456

- Click **Add**.
- When you are ready to work in Strong Authentication mode, select **Work in authenticated mode** in the **Authentication Settings** tab.

 **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 544](#)).

Step 3 of 3: Save Changes

After you finished configuring strong authentication for Active Directory, save your changes.

- In Endpoint Security, go to the **Policy** tab.
- On 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 Endpoint Security, go to **Endpoint Settings > Authentication Settings**.
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 `nacl.com` add an alternative domain name such as `ad.nacl.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 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.

Endpoint Security Logs

Endpoint Security Logs menu allows you to customize logs and views to effectively monitor all your systems from one location.



From the New Tab Catalog, select what you want to show in this tab:

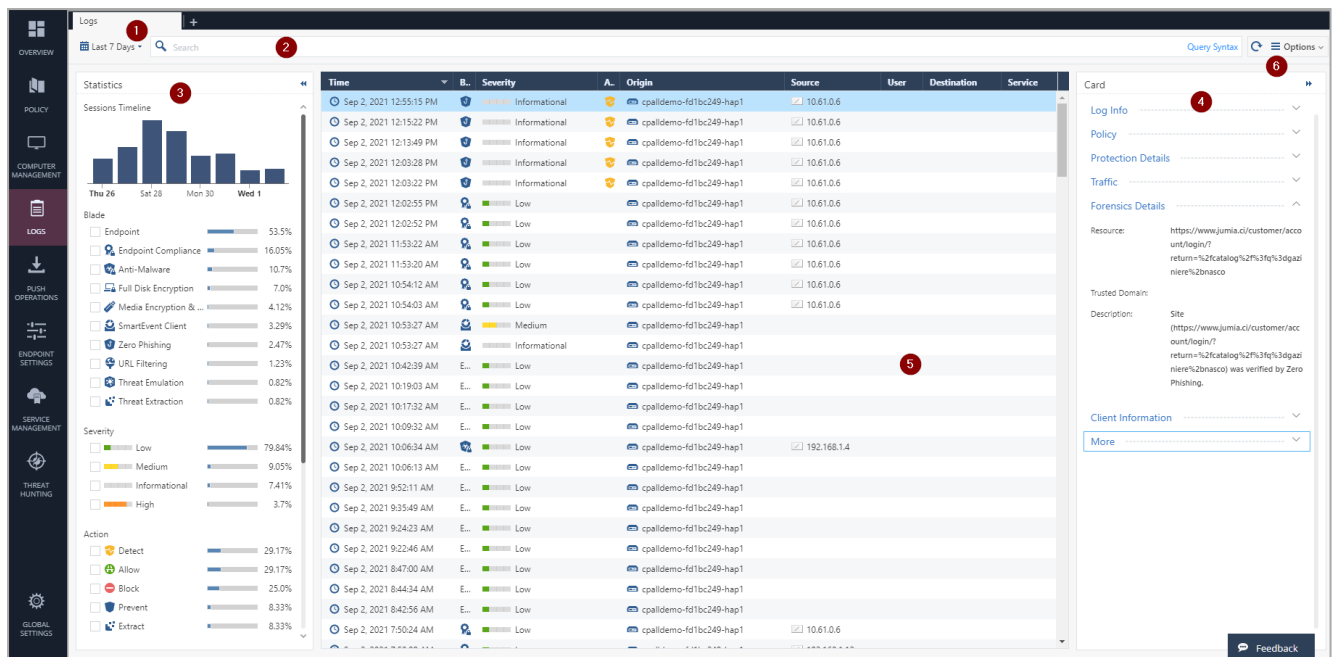
Catalog Item	Description
Favorites	Select one of the Logs or View that you marked with the Favorite icon (★)
Recent	Select one of the Logs or Views that you opened recently
Shared	Select a view that was shared with you
Logs	Select one of the widgets with logs collected from all Endpoint Security clients Note - Though the interface shows support to export up to one million logs, you can export a maximum of 10000 entries to a .csv file.
Views	Select one of the Views with data from all available blades, services, and applications
Reports	Select one of the available reports

Note - For custom views and reports through SmartView, see the [Logging and Monitoring Administration Guide](#).

You can open as many tabs as you want providing they show different views.

Use the toolbar on the top to open views, create new views and reports, export them to PDF and perform relevant actions.

See all collected logs in the Endpoint Security Logs view:



Use the time filter (1) and select the relevant options on the Statistics pane (3) to set specific criteria and customize the search results. Alternatively, you can enter your query in the search bar. For more details about the Query Language, see ["Query Language Overview" on page 570](#).

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 other parameters.
4	Card - Log information and other details.
5	Results pane - Shows log entries for the most recent query.
6	Options - Hide or show a client identity in the Card, and export the log details to CSV.

The information recorded in logs can be useful in these cases:

- To identify the cause of technical problems.
- To monitor traffic more closely.
- To make sure that all features function properly.

Note - You can forward logs to expansion (SIEM). For more information, see [Event Forwarding](#).

Data Storage and Retention

- Threat Hunting and Endpoint Data Retention is 90 days by default.
- Ingestion limit is 110MB, per seat, per day.
- Additional Data Retention is available for 1 year, by using the Threat Hunting Data Retention SKU/ Events & AI Ops SKUs.

For more information, see [sk182394](#).

Static Signatures (YARA) Logs

Anti-Malware Mode	Static Signatures (YARA) Mode	Action	Outcome
Detect	Detect	YARA detects the malicious file	Endpoint Security logs the action as Anti-Malware Detect.
	Prevent	YARA blocks the malicious file	Endpoint Security logs the action as Anti-Malware Prevent even though the Anti-Malware is in Detect mode.
Prevent	Detect	YARA detects the malicious file	Endpoint Security logs the action as Anti-Malware Detect even though the Anti-Malware is in Prevent mode.
	Prevent	YARA blocks the malicious file	Endpoint Security logs the action as Anti-Malware Prevent.
Off	Off	No protection	No logs as Anti-Malware protection is disabled.

Query Language Overview

A powerful query language lets you show only selected records from the log files, according to your criteria.

To create complex queries, use Boolean operators, wildcards, fields, and ranges.

This section refers in detail to the query language.

When you use Endpoint Security to create a query, the applicable criteria appear in the **Query search bar**.

The basic query syntax is:

```
[<Field>:] <Filter Criterion>
```

To put together many criteria in one query, use Boolean operators:

```
[<Field>:] <Filter Criterion> {AND | OR | NOT} [<Field>:] <Filter Criterion> ...
```

Most query keywords and filter criteria are not case sensitive, but there are some exceptions.

For example, "source:<X>" is case sensitive ("Source:<X>" does not match).

If your query results do not show the expected results, change the case of your query criteria, or try upper and lower case.

When you use queries with more than one criteria value, an **AND** is implied automatically, so there is no need to add it. Enter **OR** or other boolean operators if needed.

Criteria Values

Criteria values are written as one or more text strings.

You can enter one text string, such as a word, IP address, or URL, without delimiters.

Phrases or text strings that contain more than one word must be surrounded by quotation marks.

One-word string examples

- John
- inbound
- 192.168.2.1
- some.example.com

- `dns_udp`

Phrase examples

- `"John Doe"`
- `"Log Out"`
- `"VPN-1 Embedded Connector"`

IP Addresses

IPv4 and IPv6 addresses used in log queries are counted as one word.

Enter IPv4 address with dotted decimal notation and IPv6 addresses with colons.

Example:

- `192.0.2.1`
- `2001:db8::f00:d`

You can also use the *wildcard* '*' character and the *standard network suffix* to search for logs that match IP addresses within a range.

Examples:

- `src:192.168.0.0/16`

Shows all records for the source IP 192.168.0.0 to 192.168.255.255 inclusive

- `src:192.168.1.0/24`

Shows all records for the source IP 192.168.1.0 to 192.168.1.255 inclusive

- `src:192.168.2.*`

Shows all records for the source IP 192.168.2.0 to 192.168.2.255 inclusive

- `192.168.*`

Shows all records for 192.168.0.0 to 192.168.255.255 inclusive

NOT Values

You can use **NOT** *<field>* values with **Field Keywords** in log queries to find logs for which the value of the field is not the value in the query.

Syntax:

```
NOT <field>: <value>
```

Example:

```
NOT src:10.0.4.10
```

Wildcards

You can use the standard wildcard characters (* and ?) in queries to match variable characters or strings in log records.

You can use more than the wildcard character.

Wildcard syntax:

- The ? (question mark) matches one character.
- The * (asterisk) matches a character string.

Examples:

- Jo? shows Joe and Jon, but not Joseph.
- Jo* shows Jon, Joseph, and John Paul.

If your criteria value contains more than one word, you can use the wildcard in each word.

For example, 'Jo* N*' shows Joe North, John Natt, Joshua Named, and so on.



Note - Using a single '*' creates a search for a non-empty value string. For example asset name:*

Field Keywords

You can use predefined field names as keywords in filter criteria.

The query result only shows log records that match the criteria in the specified field.

If you do not use field names, the query result shows records that match the criteria in all fields.

This table shows the predefined field keywords. Some fields also support keyword aliases that you can type as alternatives to the primary keyword.

Keyword	Keyword Alias	Description
severity		Severity of the event
app_risk		Potential risk from the application, of the event
protection		Name of the protection
protection_type		Type of protection
confidence_level		Level of confidence that an event is malicious
action		Action taken by a security rule
blade	product	Software Blade
destination	dst	Traffic destination IP address, DNS name or Check Point network object name
origin	orig	Name of originating Security Gateway
service		Service that generated the log entry
source	src	Traffic source IP address, DNS name or Check Point network object name
user		User name

Syntax for a field name query:

```
<field name>:<values>
```

Where:

- **<field name>** - One of the predefined field names
- **<values>** - One or more filters

To search for rule number, use the **Rule** field name.

For example:

```
rule:7.1
```

If you use the rule number as a filter, rules in all the Layers with that number are matched.

To search for a rule name, you must not use the **Rule** field. Use free text.

For example:

```
"Block Credit Cards"
```



Best Practice - Do a free text search for the rule name. Make sure rule names are unique and not reused in different Layers.

Examples:

- `source:192.168.2.1`
- `action:(Reject OR Block)`

You can use the OR Boolean operator in parentheses to include multiple criteria values.



Important - When you use fields with multiple values, you must:

- Write the Boolean operator, for example **AND**.
- Use parentheses.

Boolean Operators

You can use the Boolean operators **AND**, **OR**, and **NOT** to create filters with many different criteria.

You can put multiple Boolean expressions in parentheses.

If you enter more than one criteria without a Boolean operator, the **AND** operator is implied.

When you use multiple criteria without parentheses, the **OR** operator is applied before the **AND** operator.

Examples:

- `blade:"application control" AND action:block`

Shows log records from the Application and URL Filtering Software Blade where traffic was blocked.

- `192.168.2.133 10.19.136.101`

Shows log entries that match the two IP addresses. The **AND** operator is presumed.

- `192.168.2.133 OR 10.19.136.101`

Shows log entries that match one of the IP addresses.

- `(blade: Firewall OR blade: IPS OR blade:VPN) AND NOT action:drop`

Shows all log entries from the Firewall, IPS or VPN blades that are not dropped.

The criteria in the parentheses are applied before the **AND NOT** criterion.

- `source:(192.168.2.1 OR 192.168.2.2) AND destination:17.168.8.2`

Shows log entries from the two source IP addresses if the destination IP address is 17.168.8.2.

This example also shows how you can use Boolean operators with field criteria.

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 Endpoint Security:

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.
- **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, the log exporter needs these certificates:
 - A *.pem Certificate Authority certificate (must 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	Description
1	Generate the self-signed root CA key: <pre>openssl genrsa -out ca.key 2048</pre>
2	Generate the root CA certificate file in the PEM format: <pre>openssl req -x509 -new -nodes -key ca.key -days 2048 -out ca.pem</pre> 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	Description
1	Generate a client key: <pre>openssl genrsa -out cp_client.key 2048</pre>
2	Generate a client certificate sign request: <pre>openssl req -new -key cp_client.key -out cp_client.csr</pre>
3	Sign the certificate using the CA certificate files: <pre>openssl x509 -req -in cp_client.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out cp_client.crt -days 2048 -sha256</pre>

Step	Description
4	Convert the certificate to the P12 format: <pre>openssl pkcs12 -inkey cp_client.key -in cp_client.crt -export -out cp_client.p12</pre>  Note - The challenge phrase used in this conversion is required in the <code>cp_client</code> TLS configuration.

3. Create a server (target) certificate

Step	Description
1	Generate a server key: <pre>openssl genrsa -out server.key 2048</pre>
2	Generate a server certificate sign request: <pre>openssl req -new -key server.key -out server.csr</pre>
3	Sign the certificate using the CA certificate files: <pre>openssl x509 -req -in server.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out server.crt -days 2048 -sha256</pre>

 **Note** - Some SIEM applications require the server certification to be in a specific format. For more information, refer to SIEM Specific Instructions section ([sk122323](#)).

Sending Security Reports

You can send weekly and monthly security report to all the administrators by email. The security report contains a summary of events detected and prevented by Endpoint Security.

To send weekly and monthly security reports to all administrators by email:

1. Click **Endpoint Settings > General Settings**:
 - To send weekly reports, toggle **Send weekly security report by email to all administrators** to **ON**.
 - To send monthly reports, toggle **Send monthly security report by email to all administrators** to **ON**.

Performing Push Operations (Old User Interface)

Note - To make the user interface clear and helpful, there is a new interface available. See ["Push Operations" on page 611](#).

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
Forensics and Remediation	Analyze by Indicator	Yes	Yes	No
	File Remediation	Yes	Yes	Yes
	Isolate Computer	Yes	Yes	No
	Release Computer	Yes	Yes	No

Category	Push Operations	Windows	macOS	Linux
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
	Search and Fetch files	Yes	Yes	No
	Registry Actions	Yes	No	No
	File Actions	Yes	Yes	No
	VPN Site	Yes	Yes	No
	Collect Processes	Yes	No	No
	Run Diagnostics	Yes	Yes	No
	Enable / Disable Self Protection	Yes	Yes	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, <code>c:\temp\eicar.txt</code> 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: - Click + and select the organization. - Click Update Selection. - Select the device and click Next. - Add Comment, optional comment about the action. - To move the files to quarantine, select Move the following files to quarantine. - To restore the files from quarantine, select Restore the following files from quarantine. - Click +. - From the drop-down: - Select Full file path or Incident ID: - In the Element field, enter the incident ID from the Endpoint Security client or enter the incident UID for the corresponding incident from the Logs menu in the Endpoint Security Administrator Portal. To obtain the incident UID, open the log entry and expand the More section to view the incident UID. - Click OK - Select MD5 Hash: - Enter or upload the Element. - Click OK. - 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

Push Operations	Description	2FA Required								
Deploy New Endpoints	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.	No								
	<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 Endpoint Security Client version to install on the target device.  Note - Only Endpoint Security client versions with a corresponding exported package ("<i>Manual Deployment of Endpoint Clients</i>" on page 106) are showed here. You can only push a client version if the package exists in the export packages.</td></tr></table>		Field	Description	Comment	Optional comment about the action.	Select the deployment endpoint	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.	Endpoint version	Select the Endpoint Security Client version to install on the target device.  Note - Only Endpoint Security client versions with a corresponding exported package (" <i>Manual Deployment of Endpoint Clients</i> " on page 106) are showed here. You can only push a client version if the package exists in the export packages.
	Field		Description							
	Comment		Optional comment about the action.							
Select the deployment endpoint	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.									
Endpoint version	Select the Endpoint Security Client version to install on the target device.  Note - Only Endpoint Security client versions with a corresponding exported package (" <i>Manual Deployment of Endpoint Clients</i> " on page 106) are showed here. You can only push a client version if the package exists in the export packages.									

Push Operations	Description	2FA Required						
Collect Client Logs	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 <i>C:\ProgramData\CheckPoint\Endpoint Security\Temp</i>. • For Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory <i>C:\Windows\SysWOW64\config\systemprofile\CPIInfo</i>. ■ For macOS, client logs are stored in the directory <i>/Users/Shared/cplogs</i>. <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></table>	Field	Description	Comment	Optional comment about the action.	Log set to collect	Select the scope of information for the logs.	No
Field	Description							
Comment	Optional comment about the action.							
Log set to collect	Select the scope of information for the logs.							

Push Operations	Description	2FA Required				
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Debug Info upload</td><td> Select the location to upload the logs: ▪ Upload CPInfo reports to AWS S3 - If the push operation is successful, the administrator will receive a download link in the Endpoint Security Administrator Portal to download the logs.  Notes - • This option is supported only with the Endpoint Security client for Windows version E88.30 and higher and for macOS version E88.50 and higher. • To enable this option, select a single user. • You can create and copy the link to download the logs using the copy to clipboard icon in the Operation output section of the Push Operation Endpoint Details. The copied link will be valid for 30 minutes. ▪ Upload CPInfo reports to Check Point servers ▪ Upload CPInfo reports to Corporate server - Update the relevant corporate server information. </td></tr></table>	Field	Description	Debug Info upload	Select the location to upload the logs: ▪ Upload CPInfo reports to AWS S3 - If the push operation is successful, the administrator will receive a download link in the Endpoint Security Administrator Portal to download the logs.  Notes - • This option is supported only with the Endpoint Security client for Windows version E88.30 and higher and for macOS version E88.50 and higher. • To enable this option, select a single user. • You can create and copy the link to download the logs using the copy to clipboard icon in the Operation output section of the Push Operation Endpoint Details. The copied link will be valid for 30 minutes. ▪ Upload CPInfo reports to Check Point servers ▪ Upload CPInfo reports to Corporate server - Update the relevant corporate server information.	
Field	Description					
Debug Info upload	Select the location to upload the logs: ▪ Upload CPInfo reports to AWS S3 - If the push operation is successful, the administrator will receive a download link in the Endpoint Security Administrator Portal to download the logs.  Notes - • This option is supported only with the Endpoint Security client for Windows version E88.30 and higher and for macOS version E88.50 and higher. • To enable this option, select a single user. • You can create and copy the link to download the logs using the copy to clipboard icon in the Operation output section of the Push Operation Endpoint Details. The copied link will be valid for 30 minutes. ▪ Upload CPInfo reports to Check Point servers ▪ Upload CPInfo reports to Corporate server - Update the relevant corporate server information.					
Repair Client	Repairs the Endpoint Security client installation. This requires a computer restart.  Note - This push operation applies only to Endpoint Security clients that have been upgraded to a newer version at least once after the installation.	No				

Push Operations	Description	2FA Required
Shutdown Computer	Shuts down the computer or computers based on the configured settings.	No
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 Security 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 Endpoint Security Windows clients running version E85.30 and above	Yes

Push Operations	Description	2FA Required				
Search and Fetch files	Searches and uploads files to a server.	Yes				
	Supported fields are:					
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr></table>		Field	Description	Comment	Optional comment about the action.
	Field		Description			
	Comment		Optional comment about the action.			
	Search and Fetch files					
	Locate the following files in the specific folders		Searches for the files in the specified folders. a. In the File table, click + . b. Enter the file name. For example, <i>test.txt</i> or <i>test.zip</i> 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.			
	Locate the following files by exact path		Searches for the files in the specified path. a. In the File table, click + . b. Enter the path where you want to search for the file and click OK. c. Repeat the steps for additional paths.			
	Files upload					
	Select the Upload files to		Select the checkbox to upload the files to a server.			

Push Operations	Description	2FA Required				
	<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>	Field	Description	Corporate Server Info	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.	
Field	Description					
Corporate Server Info	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.					

Push Operations	Description	2FA Required						
Registry Actions	Add or remove a registry key.	No						
	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></table>		Field	Description	Comment	Optional comment about the action.	Action	Select an action. ■ Add Key to Registry ■ Remove Key From Registry  Caution - Removing a registry might impact the endpoint's operating system.
	Field		Description					
	Comment		Optional comment about the action.					
	Action		Select an action. ■ Add Key to Registry ■ Remove Key From Registry  Caution - Removing a registry might impact the endpoint's operating system.					
	Add Key to Registry							
	Key		Full path where you want to add the registry key. For example, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>					
	Subkey		Enter the key name to add in the registry. For example, ProductVersion .					
	Value Type		Select the registry type.					
Value	Enter the registry value.							
Is redirected	Indicates that virtualization is enabled and add the registry to 32-bit. By default, the registry is added for 64-bit.							
Remove Key From Registry								

Push Operations	Description	2FA Required								
	<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, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>  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.	Field	Description	Key	Full path of registry key that you want to delete. For example, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>  Caution - Removing a registry might impact the endpoint's operating system.	Subkey	Enter the key name to remove from the registry. For example, ProductVersion .	Is redirected	Indicates that virtualization is enabled and delete the registry in 32-bit. By default, the registry is deleted for 64-bit.	
Field	Description									
Key	Full path of registry key that you want to delete. For example, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>  Caution - Removing a registry might impact the endpoint's operating system.									
Subkey	Enter the key name to remove from the registry. For example, ProductVersion .									
Is redirected	Indicates that virtualization is enabled and delete the registry in 32-bit. By default, the registry is deleted for 64-bit.									

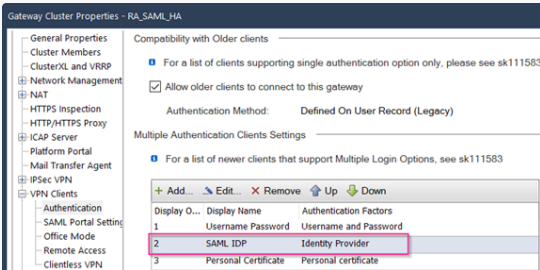
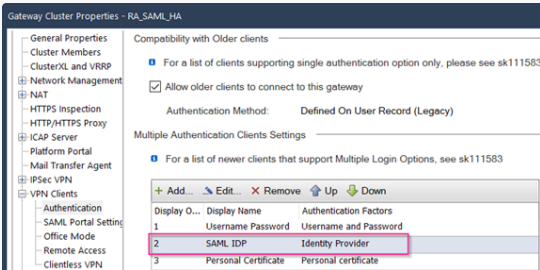
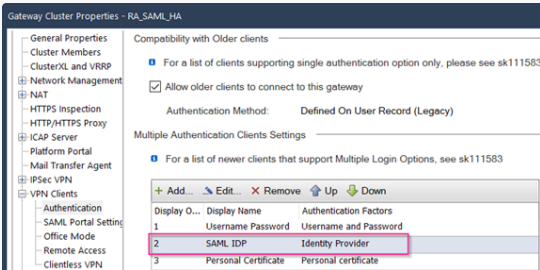
Push Operations	Description	2FA Required						
File Actions	Copy, move or delete the file or folder. Supported fields:	No						
	 Note - The folder actions are supported only with the Endpoint Security Client version 87.20 and higher.							
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</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 Endpoint Security's protected files. </td></tr></table>		Field	Description	Comment	Optional comment about the action.	Action	Select an action. ▪ Copy File ▪ Move File ▪ Delete File  Caution - Deleting a file might impact Endpoint Security's protected files.
	Field		Description					
	Comment		Optional comment about the action.					
Action	Select an action. ▪ Copy File ▪ Move File ▪ Delete File  Caution - Deleting a file might impact Endpoint Security's protected files.							
Copy File								
File path	Full path of the file or folder you want to copy, including the file or folder name. Example: ▪ For File - <i>C:\Users\<user_name>\Desktop\test.doc</i> ▪ For Folder - <i>C:\Users\Username\Desktop\</i>							

Push Operations	Description	2FA Required				
	<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 - <i>C:\Users\<user_name>\Documents</i> - For Folder - <i>C:\Users\Username2\</i>  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></table>	Field	Description	Target file path	Full path where you want to paste the file or folder. Example: - For File - <i>C:\Users\<user_name>\Documents</i> - For Folder - <i>C:\Users\Username2\</i>  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.	
Field	Description					
Target file path	Full path where you want to paste the file or folder. Example: - For File - <i>C:\Users\<user_name>\Documents</i> - For Folder - <i>C:\Users\Username2\</i>  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.					
	Move File <table><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 - <i>C:\Users\<user_name>\Desktop\test.doc</i> - For Folder - <i>C:\Users\Username>\Desktop\</i> </td></tr></table>	File path	Full path of the file or folder you want to move, including the file or folder name. Example: - For File - <i>C:\Users\<user_name>\Desktop\test.doc</i> - For Folder - <i>C:\Users\Username>\Desktop\</i>			
File path	Full path of the file or folder you want to move, including the file or folder name. Example: - For File - <i>C:\Users\<user_name>\Desktop\test.doc</i> - For Folder - <i>C:\Users\Username>\Desktop\</i>					

Push Operations	Description	2FA Required				
	<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 - <i>C:\Users\<user_name>\Documents</i> - For Folder - <i>C:\Users\Username1\Documents\</i>  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></table>	Field	Description	Target file path	Path where you want to move the file or folder. Example: - For File - <i>C:\Users\<user_name>\Documents</i> - For Folder - <i>C:\Users\Username1\Documents\</i>  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.	
	Field	Description				
	Target file path	Path where you want to move the file or folder. Example: - For File - <i>C:\Users\<user_name>\Documents</i> - For Folder - <i>C:\Users\Username1\Documents\</i>  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.				
Delete File						
File path	Full path of the file you want to delete, including the file name. For example, <i>C:\Users\<user_name>\Desktop\test.doc</i>  Caution - Deleting a file might impact Endpoint Security's protected files.  Note - Delete folder action is not supported.					

Push Operations	Description	2FA Required				
VPN Site	Adds or removes a VPN site. Limitations: ■ This is not supported with Linux operating system. ■ You cannot create separate VPN sites for each user that access the endpoint. The same VPN site applies to all users. ■ SoftID and challenge-response authentication methods are not tested. ■ The system does not validate the entries (for example, Server Name or Fingerprint) that you specify. ■ Only one fingerprint operation is supported at a time. ■ You cannot add a new VPN site or remove a VPN site if a VPN site is already connected in the Endpoint Security client. Disconnect the VPN site before you add a new VPN site. ■ This operation is not supported if the firewall policy for the client is configured through the on-premise Security Gateway (Policy > Data Protection > Access & Compliance > Firewall > When using Remote Access, enforce Firewall Policy from is Remote Access Desktop Security Policy). To enable the operation on such a client: a. In the Security Gateway, change the parameter <i>allow_disable_firewall</i> to true in the <i>\$FWDIR/conf/trac_client_1.ttm</i> file. b. Install the policy on the Security Gateway. c. Reboot the Endpoint Security client. d. Perform the push operation. Note - If the operation fails with timeout, see sk179798 for troubleshooting instructions. Supported fields: <table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr></table>	Field	Description	Comment	Optional comment about the action.	No
Field	Description					
Comment	Optional comment about the action.					

Push Operations	Description	2FA Required														
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Action</td><td>Select an action: ■ Add VPN Site ■ Remove VPN Site </td></tr><tr><td colspan="2">Add VPN Site</td></tr><tr><td>Server Name</td><td>Enter the IP address or FQDN of the remote access gateway. Note - Ensure the endpoint can resolve the FQDN to the IP address of the gateway.</td></tr><tr><td>Use Custom Display Name</td><td>Select the checkbox if you want to change the display name of the server in the Endpoint Security client.</td></tr><tr><td>Display Name</td><td>Server name displayed in the Endpoint Security client. By default, it uses the Server Name. To change the display name ,select the Use Custom Display Name checkbox and enter a display name.</td></tr><tr><td>Use Custom Login Option</td><td>Select the checkbox if you want to use a custom login option.</td></tr></table>	Field	Description	Action	Select an action: ■ Add VPN Site ■ Remove VPN Site	Add VPN Site		Server Name	Enter the IP address or FQDN of the remote access gateway. Note - Ensure the endpoint can resolve the FQDN to the IP address of the gateway.	Use Custom Display Name	Select the checkbox if you want to change the display name of the server in the Endpoint Security client.	Display Name	Server name displayed in the Endpoint Security client. By default, it uses the Server Name . To change the display name ,select the Use Custom Display Name checkbox and enter a display name.	Use Custom Login Option	Select the checkbox if you want to use a custom login option.	
Field	Description															
Action	Select an action: ■ Add VPN Site ■ Remove VPN Site															
Add VPN Site																
Server Name	Enter the IP address or FQDN of the remote access gateway. Note - Ensure the endpoint can resolve the FQDN to the IP address of the gateway.															
Use Custom Display Name	Select the checkbox if you want to change the display name of the server in the Endpoint Security client.															
Display Name	Server name displayed in the Endpoint Security client. By default, it uses the Server Name . To change the display name ,select the Use Custom Display Name checkbox and enter a display name.															
Use Custom Login Option	Select the checkbox if you want to use a custom login option.															

Push Operations	Description	2FA Required				
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Login Option</td><td> Login option for the server. By default, Standard login option is selected. To use a custom login option, select Use Custom Login Option checkbox, and enter the login option. This must match the Display Name specified in the GW properties > VPN Clients > Authentication > Multiple Authentication Clients Settings in the SmartConsole. For example, SAML IDP.  For the Standard login option, make sure that the Authentication Method is Defined on User Record (Legacy). Otherwise, Standard: does not need authentication method error appears. </td></tr></table>	Field	Description	Login Option	Login option for the server. By default, Standard login option is selected. To use a custom login option, select Use Custom Login Option checkbox, and enter the login option. This must match the Display Name specified in the GW properties > VPN Clients > Authentication > Multiple Authentication Clients Settings in the SmartConsole. For example, SAML IDP.  For the Standard login option, make sure that the Authentication Method is Defined on User Record (Legacy). Otherwise, Standard: does not need authentication method error appears.	
Field	Description					
Login Option	Login option for the server. By default, Standard login option is selected. To use a custom login option, select Use Custom Login Option checkbox, and enter the login option. This must match the Display Name specified in the GW properties > VPN Clients > Authentication > Multiple Authentication Clients Settings in the SmartConsole. For example, SAML IDP.  For the Standard login option, make sure that the Authentication Method is Defined on User Record (Legacy). Otherwise, Standard: does not need authentication method error appears.					

Push Operations	Description	2FA Required						
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Authentication Method</td><td> Select an authentication method. The options displayed depend on the Login Option. Authentication methods for the Standard login option: ▪ username-password ▪ certificate (for a certificate stored in the CAPI store) ▪ p12-certificate ▪ securityIDKeyFob ▪ securityIDPinPad ▪ SoftID (not tested) ▪ challenge-response (not tested) Authentication methods for the custom login option: ▪ Select certificate from hardware or software token (CAPI) ▪ Use certificate from Public-Key Cryptographic Standard (PKCS #12) file ▪ Other Note - Select the relevant certificate authentication method if your custom login uses a certificate. Otherwise, select Other. </td></tr><tr><td>Fingerprint</td><td> Enter the fingerprint key. For information about how to collect fingerprint details, see "Collecting Fingerprint details for a VPN Site:" on page 606. </td></tr></table>	Field	Description	Authentication Method	Select an authentication method. The options displayed depend on the Login Option. Authentication methods for the Standard login option: ▪ username-password ▪ certificate (for a certificate stored in the CAPI store) ▪ p12-certificate ▪ securityIDKeyFob ▪ securityIDPinPad ▪ SoftID (not tested) ▪ challenge-response (not tested) Authentication methods for the custom login option: ▪ Select certificate from hardware or software token (CAPI) ▪ Use certificate from Public-Key Cryptographic Standard (PKCS #12) file ▪ Other Note - Select the relevant certificate authentication method if your custom login uses a certificate. Otherwise, select Other.	Fingerprint	Enter the fingerprint key. For information about how to collect fingerprint details, see "Collecting Fingerprint details for a VPN Site:" on page 606.	
Field	Description							
Authentication Method	Select an authentication method. The options displayed depend on the Login Option. Authentication methods for the Standard login option: ▪ username-password ▪ certificate (for a certificate stored in the CAPI store) ▪ p12-certificate ▪ securityIDKeyFob ▪ securityIDPinPad ▪ SoftID (not tested) ▪ challenge-response (not tested) Authentication methods for the custom login option: ▪ Select certificate from hardware or software token (CAPI) ▪ Use certificate from Public-Key Cryptographic Standard (PKCS #12) file ▪ Other Note - Select the relevant certificate authentication method if your custom login uses a certificate. Otherwise, select Other.							
Fingerprint	Enter the fingerprint key. For information about how to collect fingerprint details, see "Collecting Fingerprint details for a VPN Site:" on page 606.							

Push Operations	Description	2FA Required												
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Remote Access Gateway Name</td><td>Enter the remote access gateway name. For information about how to get the remote access gateway name, see "Collecting Remote Access Gateway Name" on page 609.</td></tr><tr><td colspan="2">Remove VPN Site</td></tr><tr><td>Display Name</td><td>Enter the display name for the server.</td></tr></table>	Field	Description	Remote Access Gateway Name	Enter the remote access gateway name. For information about how to get the remote access gateway name, see "Collecting Remote Access Gateway Name" on page 609 .	Remove VPN Site		Display Name	Enter the display name for the server.					
Field	Description													
Remote Access Gateway Name	Enter the remote access gateway name. For information about how to get the remote access gateway name, see "Collecting Remote Access Gateway Name" on page 609 .													
Remove VPN Site														
Display Name	Enter the display name for the server.													
Collect Processes	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>	Field	Description	Comment	Optional comment about the action.	Collect all processes	Collects information about all the processes running on the endpoint.	Collect process by name	Collects information about a specific process on the endpoint.	Process name	Enter the process name. Case-sensitive.	Additional output fields	Select the additional information you want to view in the collected information.	No
Field	Description													
Comment	Optional comment about the action.													
Collect all processes	Collects information about all the processes running on the endpoint.													
Collect process by name	Collects information about a specific process on the endpoint.													
Process name	Enter the process name. Case-sensitive.													
Additional output fields	Select the additional information you want to view in the collected information.													

Push Operations	Description	2FA Required
Run Diagnostics	Runs diagnostics on an endpoint to collect this information: ■ Total CPU and RAM usage in the last 12 hours. ■ CPU usage by processes initiated in the last 12 hours. For example, the CPU used by Anti-Malware to scan files. You can review the CPU usage data to identify processes (scans) that consume CPU more than the specified threshold and exclude such processes from future scans.  Note - This is supported with Endpoint Security client version E86.80 and higher.  Warning - Only exclude a process if you are sure that the file is not malicious and is not vulnerable to cyber-attacks. To view the latest diagnostics report, see "Show Last Diagnostics Report" on page 217.	
Enable / Disable Self Protection	This Push Operation allows the administrator to enable or disable the self protection capabilities on endpoints. Supported fields: ■ Enable - Enables the self protection capabilities. ■ Disable - Disables the self protection capabilities. ■ Timeout Command Expiration - Select the expiration time for the command.  Note - After the timeout, the command expires, and the self protection capabilities will be enabled automatically.	

Push Operations	Description	2FA Required						
Collect Memory Dump	Collects Memory Dump from an endpoint based on the configured settings. Memory dump is a snapshot of system memory at specific instance of the active process and the operating system.  Note - This push operation can be executed on one device at an instance.							
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Comment</td><td>Optional comment about the action.</td></tr><tr><td>Type</td><td> Select the type of memory dump to be collected. ▪ Process - Captures memory dumps for one or more processes using process name or PID.  Notes: • The system generates multiple memory dumps if several processes share the same name. • Memory dumps are not supported for Protected Process Light (PPL) processes. ▪ Kernel - Collects a kernel memory dump without requiring a system reboot.  Note - Kernel memory dump is not supported on Windows 7 devices. ▪ Full - Initiates a BSOD to collect a full or active memory dump (requires prior configuration on the target device). For more information, see Dell documentation.  Note - It is optional to reboot the endpoint to collect the Full memory dump. </td></tr></table>	Field	Description	Comment	Optional comment about the action.	Type	Select the type of memory dump to be collected. ▪ Process - Captures memory dumps for one or more processes using process name or PID.  Notes: • The system generates multiple memory dumps if several processes share the same name. • Memory dumps are not supported for Protected Process Light (PPL) processes. ▪ Kernel - Collects a kernel memory dump without requiring a system reboot.  Note - Kernel memory dump is not supported on Windows 7 devices. ▪ Full - Initiates a BSOD to collect a full or active memory dump (requires prior configuration on the target device). For more information, see Dell documentation.  Note - It is optional to reboot the endpoint to collect the Full memory dump.	
	Field	Description						
Comment	Optional comment about the action.							
Type	Select the type of memory dump to be collected. ▪ Process - Captures memory dumps for one or more processes using process name or PID.  Notes: • The system generates multiple memory dumps if several processes share the same name. • Memory dumps are not supported for Protected Process Light (PPL) processes. ▪ Kernel - Collects a kernel memory dump without requiring a system reboot.  Note - Kernel memory dump is not supported on Windows 7 devices. ▪ Full - Initiates a BSOD to collect a full or active memory dump (requires prior configuration on the target device). For more information, see Dell documentation.  Note - It is optional to reboot the endpoint to collect the Full memory dump.							

Push Operations	Description	2FA Required								
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Process name</td><td>Enter the process name of the process memory dump.</td></tr><tr><td>Process PID</td><td>Enter the process PID of the process memory dump.</td></tr><tr><td>Dump info upload</td><td> Select the location to upload the memory dump: ▪ Upload Memory Dump to AWS S3 - After the push operation is successful, the system shows a download option in the Operation output column of the Push Operation Endpoint Details section. ▪ Upload Memory Dump to Check Point servers - After the push operation is successful, the system uploads the memory dump to this location: • For Windows Endpoint Security Client versions E88.31 and higher, client logs are stored in the directory <i>C:\ProgramData\CheckPoint\EndpointSecurity\Temp</i>. • For Windows Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory <i>C:\Windows\SysWOW64\config\systemprofile\CPIInfo</i>. • For macOS, client logs are stored in the directory <i>/Users/Shared/cplogs</i>. ▪ Upload Memory Dump to Corporate server - Enter your corporate server details. After the push operation is successful, the system uploads the memory dump to the configured location in the corporate server. </td></tr></table>	Field	Description	Process name	Enter the process name of the process memory dump.	Process PID	Enter the process PID of the process memory dump.	Dump info upload	Select the location to upload the memory dump: ▪ Upload Memory Dump to AWS S3 - After the push operation is successful, the system shows a download option in the Operation output column of the Push Operation Endpoint Details section. ▪ Upload Memory Dump to Check Point servers - After the push operation is successful, the system uploads the memory dump to this location: • For Windows Endpoint Security Client versions E88.31 and higher, client logs are stored in the directory <i>C:\ProgramData\CheckPoint\EndpointSecurity\Temp</i>. • For Windows Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory <i>C:\Windows\SysWOW64\config\systemprofile\CPIInfo</i>. • For macOS, client logs are stored in the directory <i>/Users/Shared/cplogs</i>. ▪ Upload Memory Dump to Corporate server - Enter your corporate server details. After the push operation is successful, the system uploads the memory dump to the configured location in the corporate server.	
Field	Description									
Process name	Enter the process name of the process memory dump.									
Process PID	Enter the process PID of the process memory dump.									
Dump info upload	Select the location to upload the memory dump: ▪ Upload Memory Dump to AWS S3 - After the push operation is successful, the system shows a download option in the Operation output column of the Push Operation Endpoint Details section. ▪ Upload Memory Dump to Check Point servers - After the push operation is successful, the system uploads the memory dump to this location: • For Windows Endpoint Security Client versions E88.31 and higher, client logs are stored in the directory <i>C:\ProgramData\CheckPoint\EndpointSecurity\Temp</i>. • For Windows Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory <i>C:\Windows\SysWOW64\config\systemprofile\CPIInfo</i>. • For macOS, client logs are stored in the directory <i>/Users/Shared/cplogs</i>. ▪ Upload Memory Dump to Corporate server - Enter your corporate server details. After the push operation is successful, the system uploads the memory dump to the configured location in the corporate server.									

Push Operations	Description	2FA Required
	 Notes: ■ Automated packaging and upload of memory dump - All memory dumps are automatically zipped, segmented if necessary, and uploaded to the designated destination (Check Point FTP, Amazon S3, or custom FTP servers). ■ On 32-bit Windows systems, the ZIP file name is not displayed when uploading full memory dumps to an FTP server. ■ The Memory Dump feature is supported only on Endpoint Security for Windows client version E89.05 and later.	

6. Under **User Notification:**

- To notify the user about the push operation, select the **Inform user with notification** checkbox.
- To allow the user to postpone 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. Specify the duration after which the system automatically terminates the unexecuted push operation (For example, if the Endpoint client is offline):

- **7 days**
- **Custom**
- **Never**

9. 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 [Check Point Portal Administration Guide](#).
- To enable 2FA authentication for the current tenant, click **Global Settings**, and follow the instructions. For more information, see [Check Point Portal Administration Guide](#).

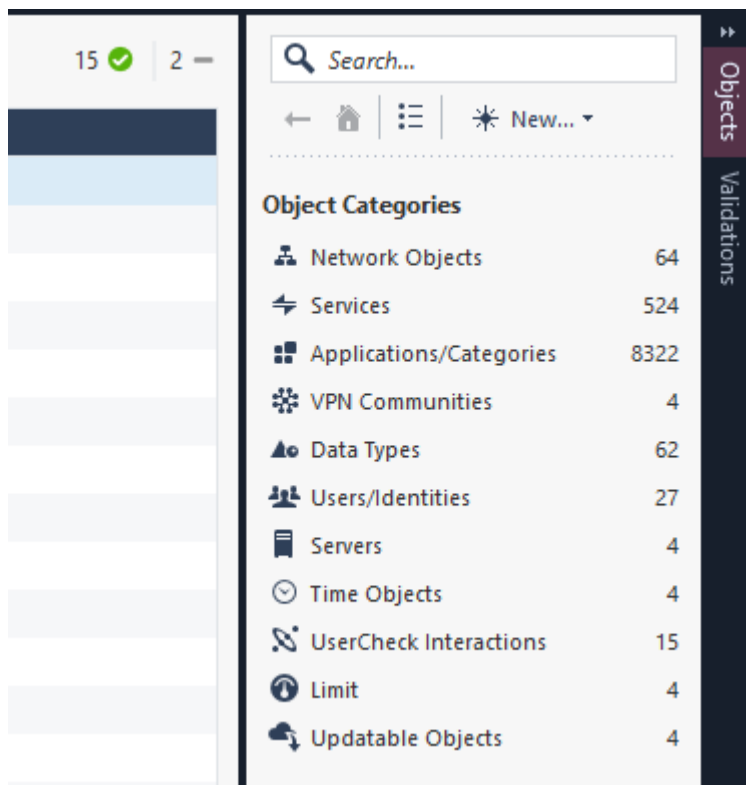
10. Click **Finish**.

11. 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.

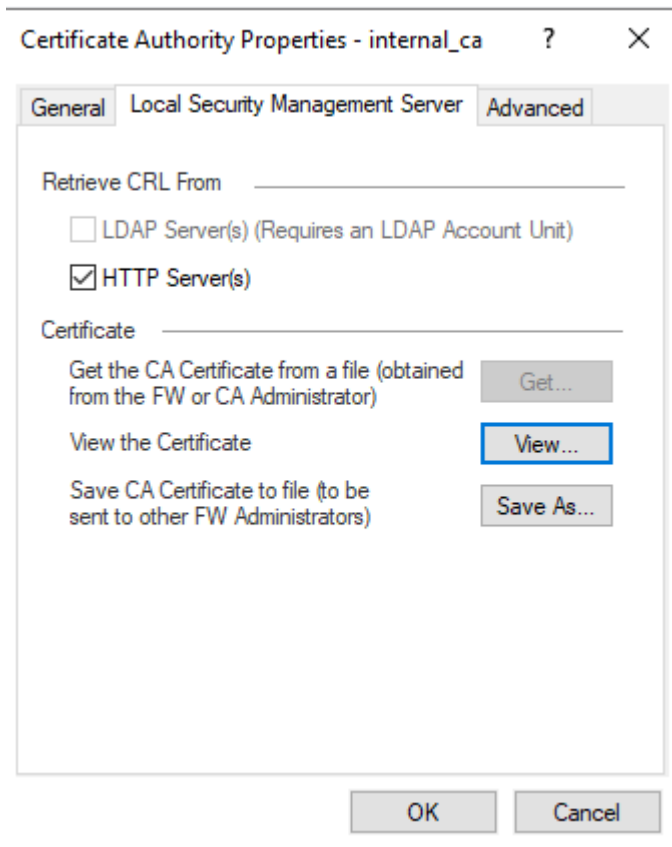
Collecting Fingerprint details for a VPN Site:

To get the fingerprint from SmartConsole

- In SmartConsole, in the right pane, under **Object Categories**, click **Servers > Trusted CA > internal ca**.

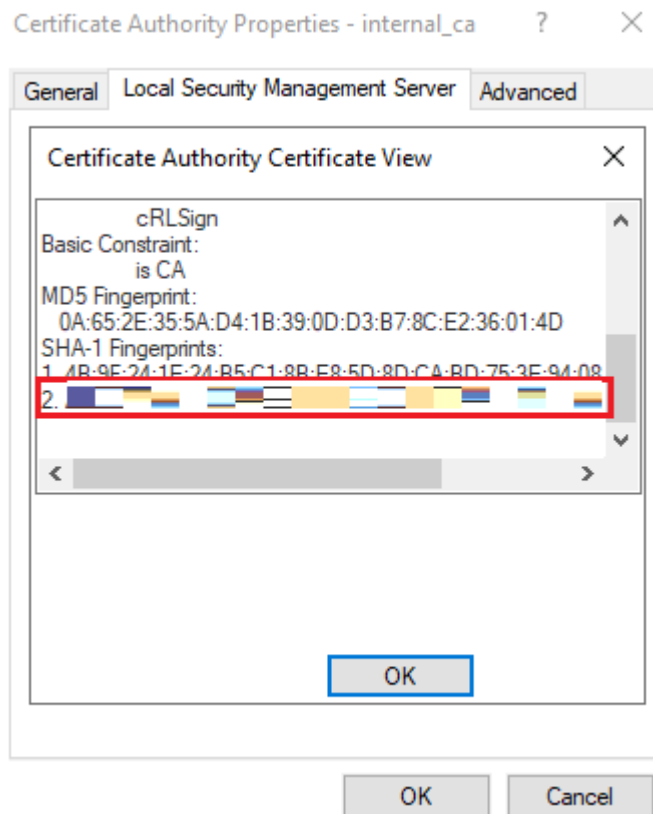


The **Certificate Authority Properties** window appears.



- b. Click the **Local Security Management** tab.
- c. Under **Certificate**, click **View**.

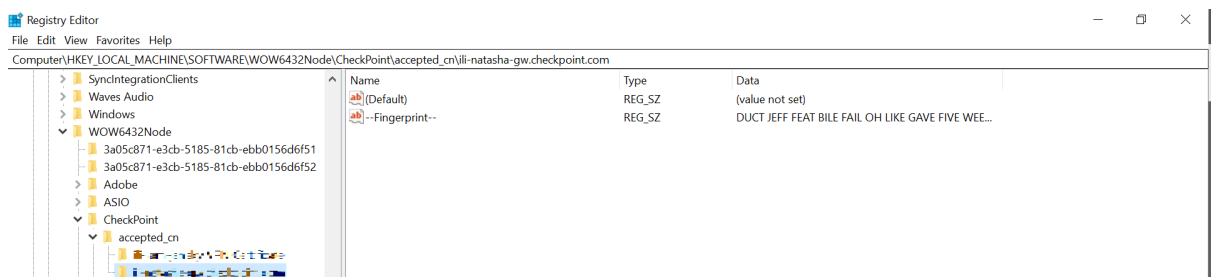
The **Certificate Authority Certificate View** window appears.



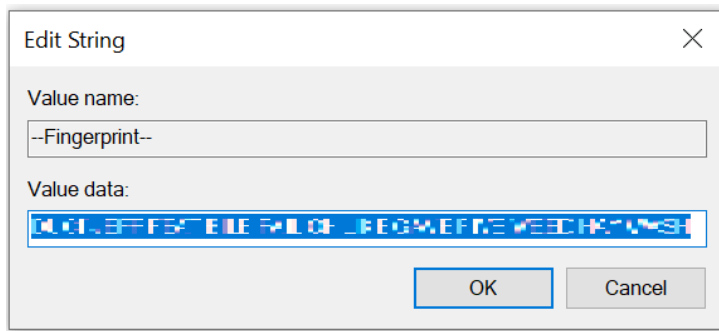
- d. Scroll down to **SHA-1 Fingerprints**. The fingerprint is on line number 2.

To get the fingerprint from the device

- Manually add the VPN site in the client. For more information, see *Endpoint Security Clients User Guide*.
- After you add and connect to the VPN site successfully, In **Registry Editor**, go to *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\accepted_cn*.
- It displays a folder with the display name of your VPN site.



- Double-click the folder.
- In the right pane, under **Name**, double-click **--Fingerprint--**.
The **Edit String** window appears.



- f. Copy the fingerprint key from the **Value** data field.
- g. Click **Cancel** to close the window.
- h. Paste the fingerprint key in the **Fingerprint** field.

Collecting Remote Access Gateway Name

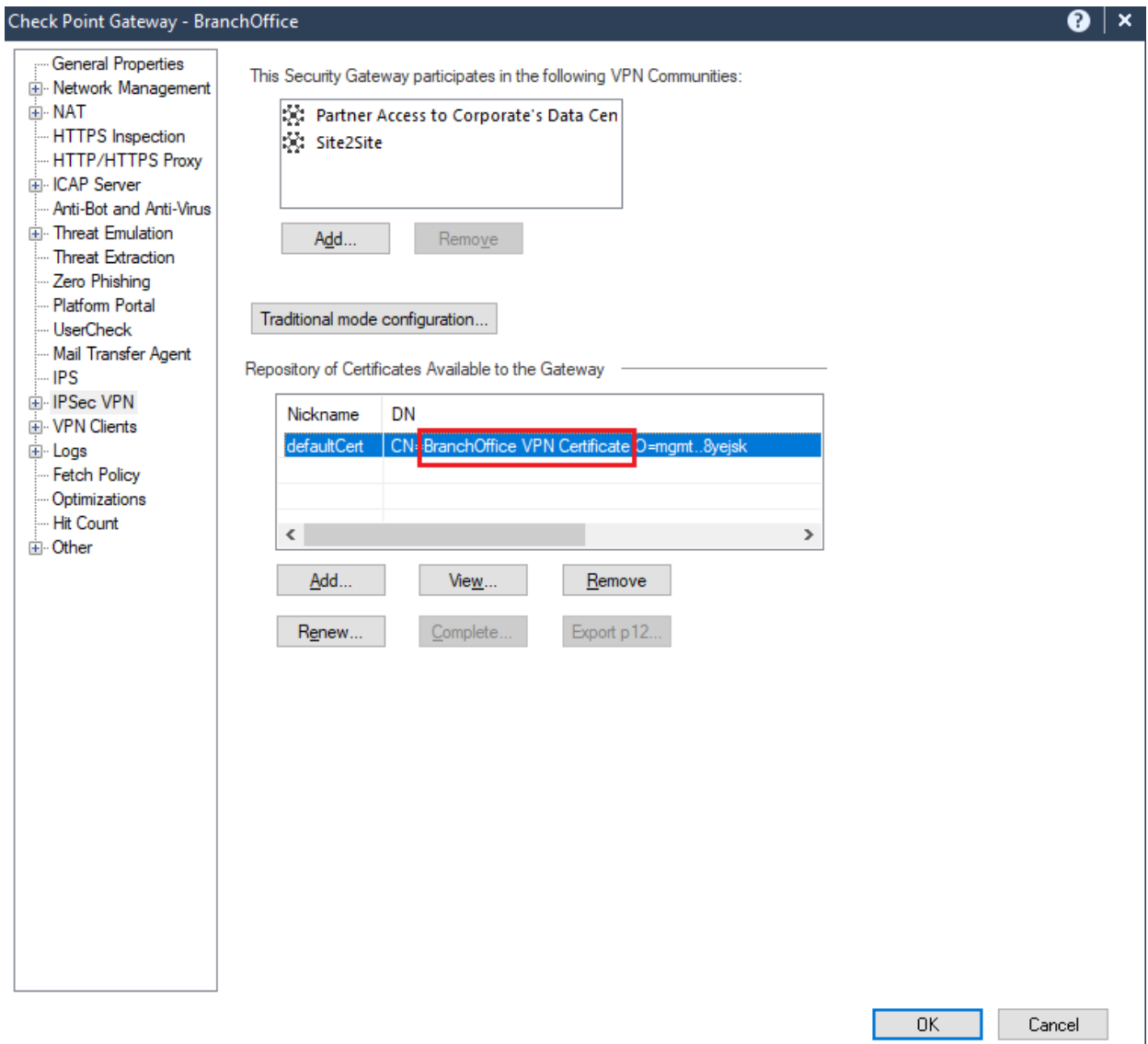
To get the Remote Access Gateway name from SmartConsole:

- In SmartConsole, go to **Gateways and Servers**.
- Double-click the gateway.

The **Check Point Gateway** window appears.

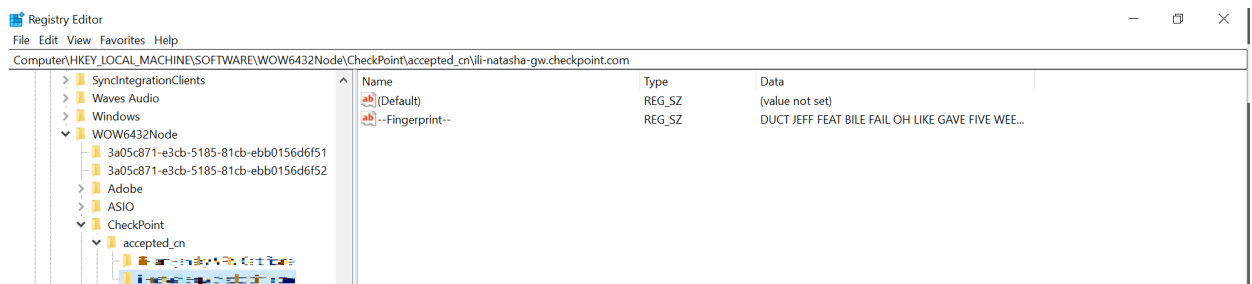
- c. Double-click **IPSec VPN**.
- d. Under **Repository of Certificates Available to the Gateway**, in the table, expand the DN

column. The value after **CN=** indicates the remote access gateway name.



To get the remote access gateway name from the device:

- In **Registry Editor**, go to *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\accepted_cn*.
- It shows a folder with the display name of your VPN site. Copy the folder name and paste it in the **Remote Access Gateway Name** field.



Push Operations

The Push Operations feature in Endpoint Security enables you to run predefined tasks remotely on managed endpoint devices. These tasks support automation, diagnostics, enforcement, and recovery workflows.

Accessing Push Operations

By default, the **Push Operations** page shows the list of all the push operations created and their statuses in the last 30 days.

To view the Push Operations page, click **Asset Management > Push Operations**.

Push Operation	Pushed to	Deployment status	Run date	Created by	Created on	Expires on
Application Scan	DESKTOP-FVVHBJ5	Scheduled	08 Sep 2025 03:51 pm	sahar@checkpoint.com	08 Sep 2025 03:52 pm	15 Sep 2025 03:52 pm
Application Scan	DESKTOP-FVVHBJ5	Scheduled	08 Sep 2025 03:51 pm	sahar@checkpoint.com	08 Sep 2025 03:52 pm	15 Sep 2025 03:52 pm
Scan for Malware	DESKTOP-FVVHBJ5	Scheduled	19 Aug 2025 06:54 pm	rafiel@checkpoint.com	27 Aug 2025 02:09 pm	03 Sep 2025 02:09 pm
Scan for Malware	DESKTOP-FVVHBJ5	Scheduled	27 Aug 2025 02:08 pm	rafiel@checkpoint.com	27 Aug 2025 02:08 pm	03 Sep 2025 02:08 pm
Copy File	3 Devices	Scheduled	27 Aug 2025 02:05 pm	rafiel@checkpoint.com	27 Aug 2025 02:05 pm	03 Sep 2025 02:05 pm
Remote Command	2 Devices	Partially completed	12 Aug 2025 06:03 pm	orenel@checkpoint.com	19 Aug 2025 06:59 pm	26 Aug 2025 06:59 pm
Remote Command	DESKTOP-FVVHBJ5	Failed	13 Aug 2025 06:43 pm	sahar@checkpoint.com	13 Aug 2025 06:43 pm	20 Aug 2025 06:43 pm
Remote Command	DESKTOP-FVVHBJ5	Failed	13 Aug 2025 06:42 pm	sahar@checkpoint.com	13 Aug 2025 06:42 pm	20 Aug 2025 06:42 pm
Scan for Malware	ABOXKOWNWOC-PC	Scheduled	12 Aug 2025 11:16 pm	oliverf@checkpoint.com	12 Aug 2025 11:16 pm	19 Aug 2025 11:16 pm
Remote Command	AANSBVJZES-PC	Scheduled	12 Aug 2025 06:58 pm	oliverf@checkpoint.com	12 Aug 2025 06:58 pm	19 Aug 2025 06:58 pm

Extending the Time Frame of Push Operations

To view push operations created in a specific period, select the time frame from the drop-down at the top right corner of the page.

- Last 30 days
- Last 7 days
- Last day

Push Operations Dashboard Widgets

Widget Name	Description
Total	Shows the total number of push operations created within the selected time frame.
Scheduled	Shows the total number of push operations configured and scheduled within the selected time frame.

Widget Name	Description
In Progress	Shows the total number of push operations running on one or more endpoint devices within the selected time frame.
Completed	Shows the total number of push operations that ran successfully on all targeted endpoint devices within the selected time frame.
Partially Completed	Shows the total number of push operations that ran on some endpoint devices but failed or timed out within the selected time frame.
Failed	Shows the total number of push operations that failed on all targeted endpoint devices within the selected time frame.

Push Operations Table

Column	Description
Push operation	Shows the type of action performed.
Pushed to	Shows the list of devices.
Deployment status	Shows the status of the deployment. ■ Scheduled ■ In progress ■ Partially completed ■ Completed ■ Failed
Run date	Shows the date and time when the push operation was executed.
Created by	Shows the user's email address that initiated the push operation.
Created on	Shows the date and time when the push operation was created.
Expire on	Shows the date and time when the push operation is going to expire.
Comment	Shows the comments associated with the push operation.

Available Actions from Push Operations

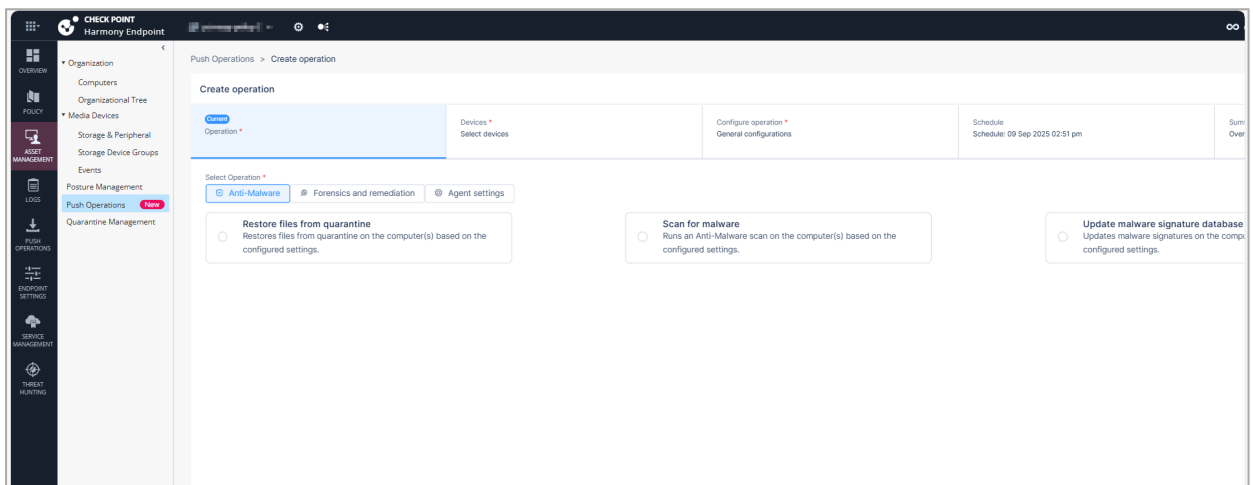
- **Run Again:** Re-executes a previously completed push operation on the selected devices.
- **Clone:** Duplicates an existing push operation.
- **Delete:** Removes a push operation.
- **Cancel:** Stops a scheduled or in-progress push operation.
- **Export:** Downloads a push operation data for reporting.

Creating a Push Operation

To create a new push operation:

1. Log in to the Endpoint Security Administrator Portal.
2. Navigate to **Asset Management > Push Operations**.
3. Click **Create operation**.

The **Create operation** page appears. You need to select the required operation and the required actions.



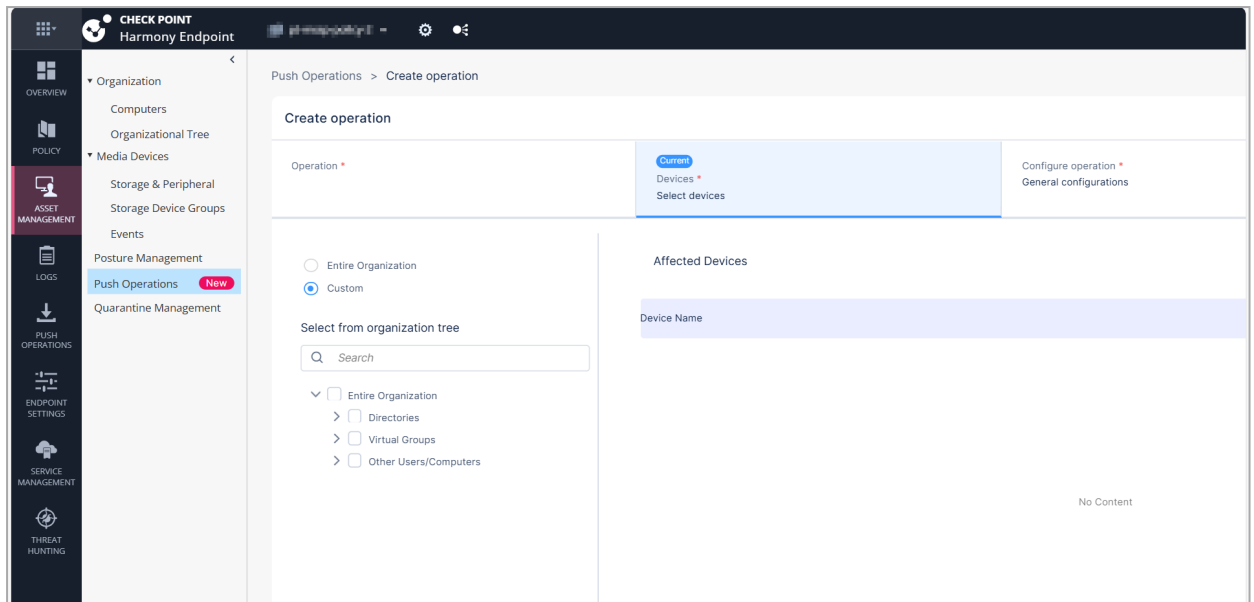
4. In the **Operation** tab, select the required operation.

Here are the supported operations:

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
Forensics and Remediation	Analyze by Indicator	Yes	Yes	No
	File Remediation	Yes	Yes	Yes
	Isolate Computer	Yes	Yes	No
	Release Computer	Yes	Yes	No

Category	Push Operations	Windows	macOS	Linux
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
	Search and Fetch files	Yes	Yes	No
	Registry Actions	Yes	No	No
	File Actions	Yes	Yes	No
	VPN Site	Yes	Yes	No
	Collect Processes	Yes	No	No
	Run Diagnostics	Yes	Yes	No
	Enable / Disable Self Protection	Yes	Yes	No
	Collect Memory Dump	Yes	Yes	No

5. Click **Next**.
6. In the **Devices** tab, configure the required devices.



- To perform a push operation for all organizational assets, select **Entire organization**.
- To perform a push operation for specific affected assets, select **Custom** and choose the affected devices.

7. Click **Next**.

8. 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: - In the Full Path field, enter the path to file before it was quarantined including the file name. For example, <code>c:\temp\eicar.txt</code> - 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: - Click + and select the organization. - Click Update Selection. - Select the device and click Next. - Add Comment, optional comment about the action. - To move the files to quarantine, select Move the following files to quarantine. - To restore the files from quarantine, select Restore the following files from quarantine. - Click +. - From the drop-down: - Select Full file path or Incident ID: - In the Element field, enter the incident ID from the Endpoint Security Security client or enter the incident UID for the corresponding incident from the Logs menu in the Endpoint Security portal. To obtain the incident UID, open the log entry and expand the More section to view the incident UID. - Click OK - Select MD5 Hash: - Enter or upload the Element. - Click OK. - 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

• Deploy New Endpoints

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.

 **Note** - The **Deploy New Endpoints** operation does not need Two-Factor Authentication (2FA).

Field	Description
Comment	Optional comment about the action.
Select the deployment endpoint	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.
Endpoint version	Select the Endpoint Security Client version to install on the target device.  Note - Only Endpoint Security client versions with a corresponding exported package ("Manual Deployment of Endpoint Clients" on page 106) are showed here. You can only push a client version if the package exists in the export packages.

- **Collect Client Logs**

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.*

Field	Description
Comment	Optional comment about the action.
Log set to collect	Select the scope of information for the logs.
Debug Info upload	Select the location to upload the logs: ◦ Upload CPInfo reports to AWS S3 - If the push operation is successful, the administrator will receive a download link in the Endpoint Security Administrator Portal to download the logs.  Notes - ◦ This option is supported only with the Endpoint Security client for Windows version E88.30 and higher and for macOS version E88.50 and higher. ◦ To enable this option, select a single user. ◦ You can create and copy the link to download the logs using the copy to clipboard icon in the Operation output section of the Push Operation Endpoint Details. The copied link will be valid for 30 minutes. ◦ Upload CPInfo reports to Check Point servers ◦ Upload CPInfo reports to Corporate server - Update the relevant corporate server information.

 **Note** - The **Collect Client Logs** operation does not need Two-Factor Authentication (2FA).

- **Repair Client**

Repairs the Endpoint Security client installation. This requires a computer restart.

 Notes:

- This push operation applies only to Endpoint Security clients that have been upgraded to a newer version at least once after the installation.
- The **Repair Client** operation does not need Two-Factor Authentication (2FA).

- **Shutdown Computer**

Shuts down the computer or computers based on the configured settings.

 **Note** - The **Shutdown Computer** operation does not need Two-Factor Authentication (2FA).

- **Restart Computer**

Shuts down the computer or computers based on the configured settings.

 **Note** - The **Restart Computer** operation does not need Two-Factor Authentication (2FA).

- **Uninstall Client**

Uninstalls the Endpoint Security client remotely on the selected devices. This feature is supported for E84.30 client and above.

 **Note** - The **Uninstall Client** operation needs Two-Factor Authentication (2FA).

- **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.

 **Note** - The **Application Scan** operation does not need Two-Factor Authentication (2FA).

- **Kill Process**

Remotely kills/ terminate the processes.

 **Note** - The **Kill Process** operation does not need Two-Factor Authentication (2FA).

- **Remote Command**

- Allows administrators to run both signed (introduced by CP) and unsigned (ones the customer creates) scripts on the Endpoint Security 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.

 Notes:

- The **Remote Command** operation needs Two-Factor Authentication (2FA).
- The Remote Command feature is supported only in Windows clients running version E85.30 and above.

- **Registry Actions**

Add or remove a registry key.

Field	Description
Comment	Optional comment about the action.
Action	Select an action. ◦ Add Key to Registry ◦ Remove Key From Registry  Caution - Removing a registry might impact the endpoint's operating system.

Add Key to Registry

Key	Full path where you want to add the registry key. For example, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>
Subkey	Enter the key name to add in the registry. For example, ProductVersion .
Value Type	Select the registry type.
Value	Enter the registry value.
Is redirected	Indicates that virtualization is enabled and add the registry to 32-bit. By default, the registry is added for 64-bit.

Remove Key From Registry

Key	Full path of registry key that you want to delete. For example, <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Endpoint Analysis</i>  Caution - Removing a registry might impact the endpoint's operating system.

Field	Description
Subkey	Enter the key name to remove from the registry. For example, ProductVersion .
Is redirected	Indicates that virtualization is enabled and delete the registry in 32-bit. By default, the registry is deleted for 64-bit.

To change the working hours to allow the Anti-Malware signature updates on a DHS compliant Endpoint Security client, see [sk180559](#).



Note - The **Registry Actions** operation does not need Two-Factor Authentication (2FA).

- **File Actions**

Copy, move or delete the file or folder.



Notes:

- The **File Actions** operation does not need Two-Factor Authentication (2FA).
- The folder actions are supported only with the Endpoint Security Client version 87.20 and higher.

Field	Description
Comment	Optional comment about the action.
Action	Select an action. ◦ Copy File ◦ Move File ◦ Delete File Caution - Deleting a file might impact Endpoint Security's protected files.

Copy File

File path	Full path of the file or folder you want to copy, including the file or folder name. Example: ◦ For File - <i>C:\Users\<user_name>\Desktop\test.doc</i> ◦ For Folder - <i>C:\Users\Username\Desktop\</i>
Target file path	Full path where you want to paste the file or folder. Example: ◦ For File - <i>C:\Users\<user_name>\Documents</i> ◦ For Folder - <i>C:\Users\Username2\</i> 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.

Move File

Field	Description
File path	Full path of the file or folder you want to move, including the file or folder name. Example: - For File - <i>C:\Users\<user_name>\Desktop\test.doc</i> - For Folder - <i>C:\Users\Username>\Desktop\</i>
Target file path	Path where you want to move the file or folder. Example: - For File - <i>C:\Users\<user_name>\Documents</i> - For Folder - <i>C:\Users\Username1\Documents\</i>  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.

Delete File

File path	Full path of the file you want to delete, including the file name. For example, <i>C:\Users\<user_name>\Desktop\test.doc</i>  Caution - Deleting a file might impact Endpoint Security's protected files.  Note - Delete folder action is not supported.

- **VPN Site**

Adds or removes a VPN site.



Notes:

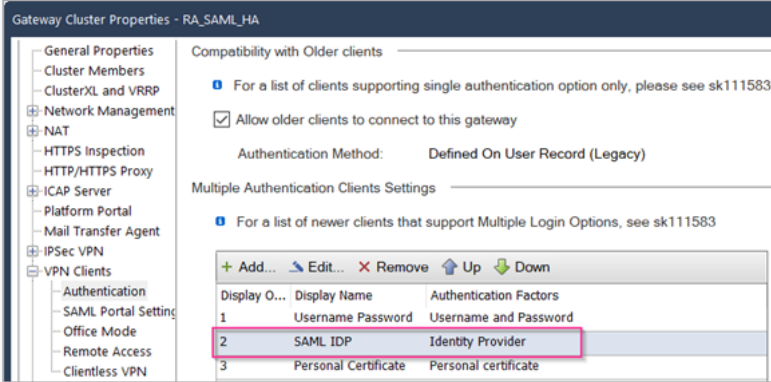
- The **VPN Site** operation does not need Two-Factor Authentication (2FA).
- If the operation fails with timeout, see [sk179798](#) for troubleshooting instructions.

Limitations:

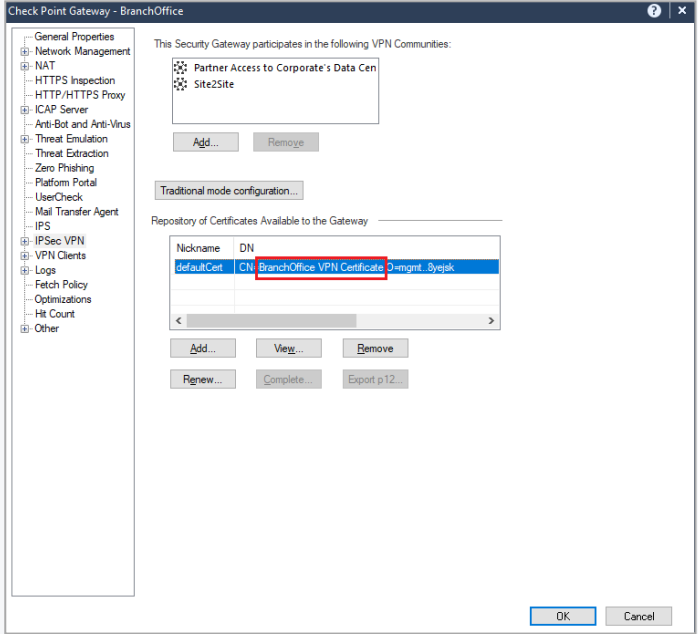
- This is not supported with Linux operating system.
- You cannot create separate VPN sites for each user that access the endpoint. The same VPN site applies to all users.
- **SoftID** and **challenge-response** authentication methods are not tested.
- The system does not validate the entries (for example, **Server Name** or **Fingerprint**) that you specify.
- Only one fingerprint operation is supported at a time.
- You cannot add a new VPN site or remove a VPN site if a VPN site is already connected in the Endpoint Security client. Disconnect the VPN site before you add a new VPN site.
- This operation is not supported if the firewall policy for the client is configured through the on-premise Security Gateway (**Policy > Data Protection > Access & Compliance > Firewall > When using Remote Access, enforce Firewall Policy from is Remote Access Desktop Security Policy**). To enable the operation on such a client:
 - a. In the Security Gateway, change the parameter *allow_disable_firewall* to **true** in the *\$FWDIR/conf/trac_client_1.ttm* file.
 - b. Install the policy on the Security Gateway.
 - c. Reboot the Endpoint Security client.
 - d. Perform the push operation.

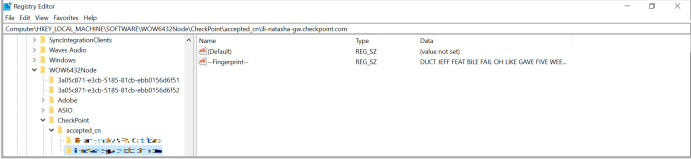
Field	Description
Comment	Optional comment about the action.

Field	Description
Action	Select an action: ◦ Add VPN Site ◦ Remove VPN Site
Add VPN Site	
Server Name	Enter the IP address or FQDN of the remote access gateway. Note - Ensure the endpoint can resolve the FQDN to the IP address of the gateway.
Use Custom Display Name	Select the checkbox if you want to change the display name of the server in the Endpoint Security client.
Display Name	Server name displayed in the Endpoint Security client. By default, it uses the Server Name . To change the display name ,select the Use Custom Display Name checkbox and enter a display name.
Use Custom Login Option	Select the checkbox if you want to use a custom login option.

Field	Description
Login Option	Login option for the server. By default, Standard login option is selected. To use a custom login option, select Use Custom Login Option checkbox, and enter the login option. This must match the Display Name specified in the GW properties > VPN Clients > Authentication > Multiple Authentication Clients Settings in the SmartConsole. For example, SAML IDP.  For the Standard login option, make sure that the Authentication Method is Defined on User Record (Legacy). Otherwise, Standard: does not need authentication method error appears.

Field	Description
Authentication Method	Select an authentication method. The options displayed depend on the Login Option. Authentication methods for the Standard login option: ◦ username-password ◦ certificate (for a certificate stored in the CAPI store) ◦ p12-certificate ◦ securityIDKeyFob ◦ securityIDPinPad ◦ SoftID (not tested) ◦ challenge-response (not tested) Authentication methods for the custom login option: ◦ Select certificate from hardware or software token (CAPI) ◦ Use certificate from Public-Key Cryptographic Standard (PKCS #12) file ◦ Other Note - Select the relevant certificate authentication method if your custom login uses a certificate. Otherwise, select Other.

Field	Description
Remote Access Gateway Name	Enter the remote access gateway name. To get the remote access gateway name from SmartConsole: - In SmartConsole, go to Gateways and Servers. - Double-click the gateway. The Check Point Gateway window appears. - Double-click IPSec VPN. - Under Repository of Certificates Available to the Gateway, in the table, expand the DN column. The value after CN= indicates the remote access gateway name.  To get the remote access gateway name from the device: - In Registry Editor, go to <i>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Check Point\accepted_cn</i>.

Field	Description
	b. It shows a folder with the display name of your VPN site. Copy the folder name and paste it in the Remote Access Gateway Name field. 

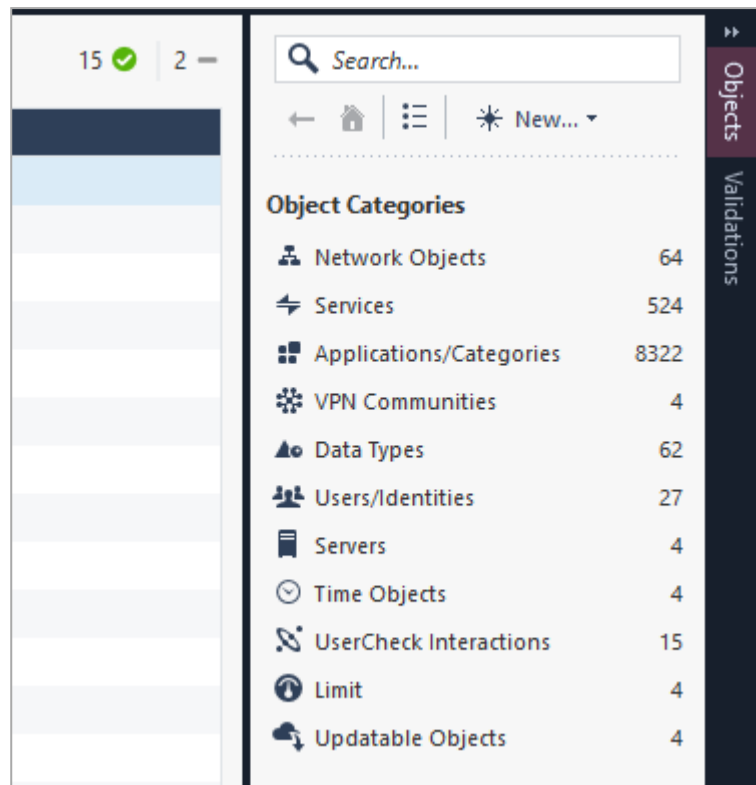
Remove VPN Site

Display Name	Enter the display name for the server.

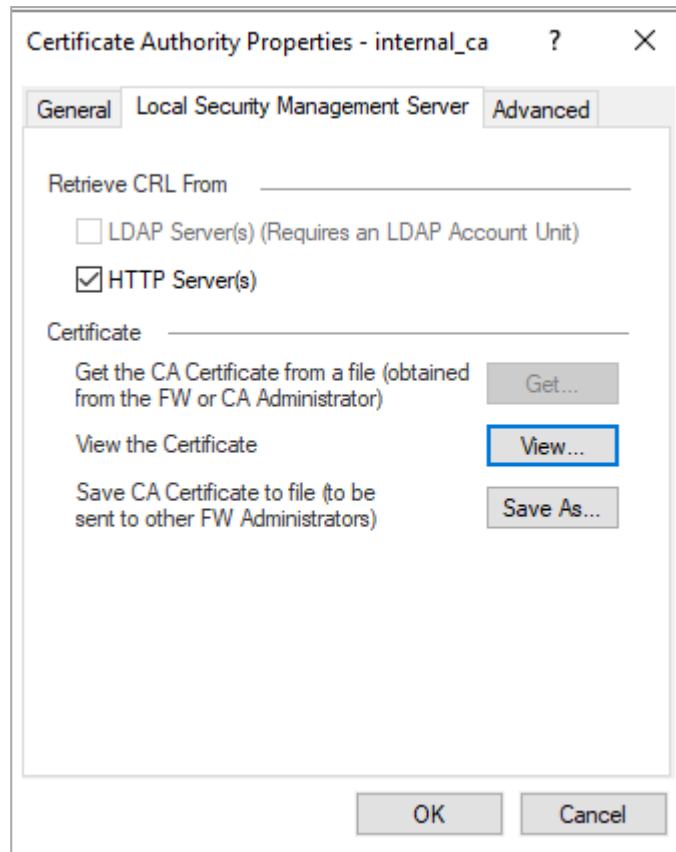
- **Collecting Fingerprint details for a VPN Site:**

To get the fingerprint from SmartConsole

- a. In SmartConsole, in the right pane, under **Object Categories**, click **Servers > Trusted CA > internal ca**.



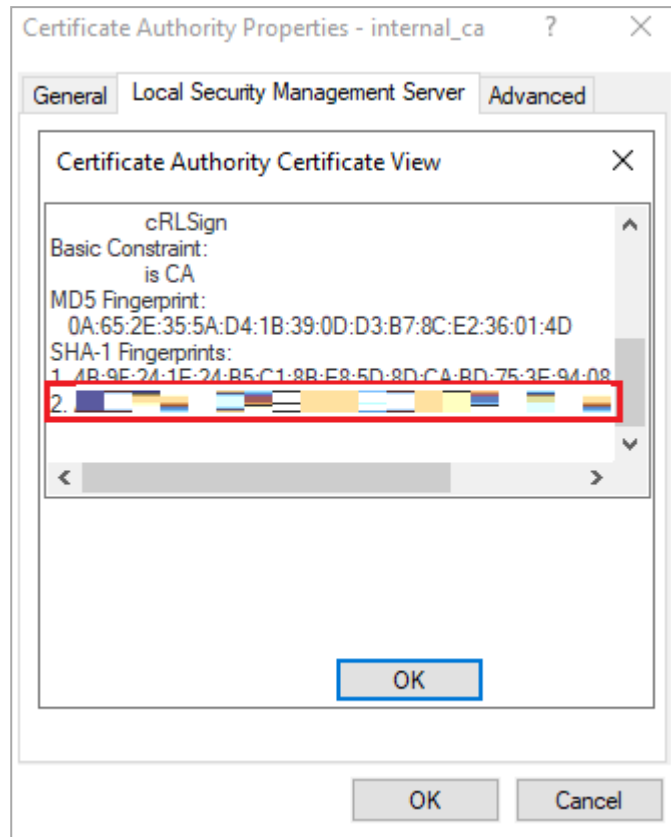
The **Certificate Authority Properties** window appears.



- b. Click the **Local Security Management** tab.

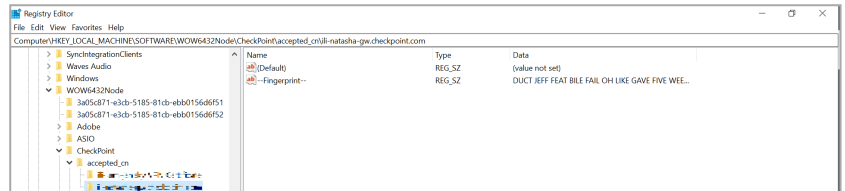
- c. Under **Certificate**, click **View**.

The **Certificate Authority Certificate View** window appears.



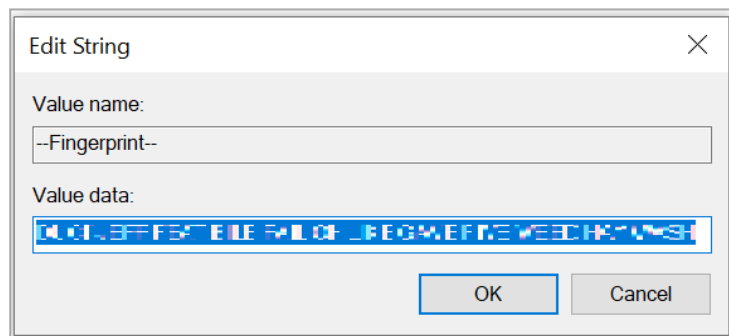
- d. Scroll down to **SHA-1 Fingerprints**. The fingerprint is on line number 2.

- To get the fingerprint from the device
 - a. Manually add the VPN site in the client. For more information, see *Endpoint Security Clients User Guide*.
 - b. After you add and connect to the VPN site successfully, In **Registry Editor**, go to *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\accepted_cn*.
 - c. It displays a folder with the display name of your VPN site.



- d. Double-click the folder.
- e. In the right pane, under **Name**, double-click **-- Fingerprint--**.

The **Edit String** window appears.



- f. Copy the fingerprint key from the **Value** data field.
- g. Click **Cancel** to close the window.
- h. Paste the fingerprint key in the **Fingerprint** field.

- **Collect Processes**

Collects information about the process running on the endpoint.

Field	Description
Comment	Optional comment about the action.
Collect all processes	Collects information about all the processes running on the endpoint.
Collect process by name	Collects information about a specific process on the endpoint.
Process name	Enter the process name. Case-sensitive.
Additional output fields	Select the additional information you want to view in the collected information.

 **Note** - The **Collect Processes** operation does not need Two-Factor Authentication (2FA).

- **Run Diagnostics**

Runs diagnostics on an endpoint to collect this information:

- Total CPU and RAM usage in the last 12 hours.
- CPU usage by processes initiated in the last 12 hours. For example, the CPU used by Anti-Malware to scan files.

You can review the CPU usage data to identify processes (scans) that consume CPU more than the specified threshold and exclude such processes from future scans.

 **Note** - This is supported with Endpoint Security client version E86.80 and higher.

 **Warning** - Only exclude a process if you are sure that the file is not malicious and is not vulnerable to cyber-attacks.

To view the latest diagnostics report, see ["Show Last Diagnostics Report" on page 217](#).

- **Enable / Disable Self Protection**

The **Enable / Disable Self Protection** push operation allows the administrator to enable or disable the self protection capabilities on endpoints.

Limitations:

- **Enable** - Enables the self protection capabilities.
- **Disable** - Disables the self protection capabilities.
- **Timeout Command Expiration** - Select the expiration time for the command.

 **Note** - After the timeout, the command expires, and the self protection capabilities will be enabled automatically.

- **Collect Memory Dump**

Collects Memory Dump from an endpoint based on the configured settings. Memory dump is a snapshot of system memory at specific instance of the active process and the operating system.

 **Note** - The **Collect Memory Dump** push operation can be executed on one device at an instance.

Limitations:

- **Enable** - Enables the self protection capabilities.
- **Disable** - Disables the self protection capabilities.
- **Timeout Command Expiration** - Select the expiration time for the command.

 **Note** - After the timeout, the command expires, and the self protection capabilities will be enabled automatically.

Field	Description
Comment	Optional comment about the action.
Type	Select the type of memory dump to be collected. ◦ Process - Captures memory dumps for one or more processes using process name or PID.  Notes: ◦ The system generates multiple memory dumps if several processes share the same name. ◦ Memory dumps are not supported for Protected Process Light (PPL) processes. ◦ Kernel - Collects a kernel memory dump without requiring a system reboot.  Note - Kernel memory dump is not supported on Windows 7 devices. ◦ Full - Initiates a BSOD to collect a full or active memory dump (requires prior configuration on the target device). For more information, see Dell documentation.  Note - It is optional to reboot the endpoint to collect the Full memory dump.

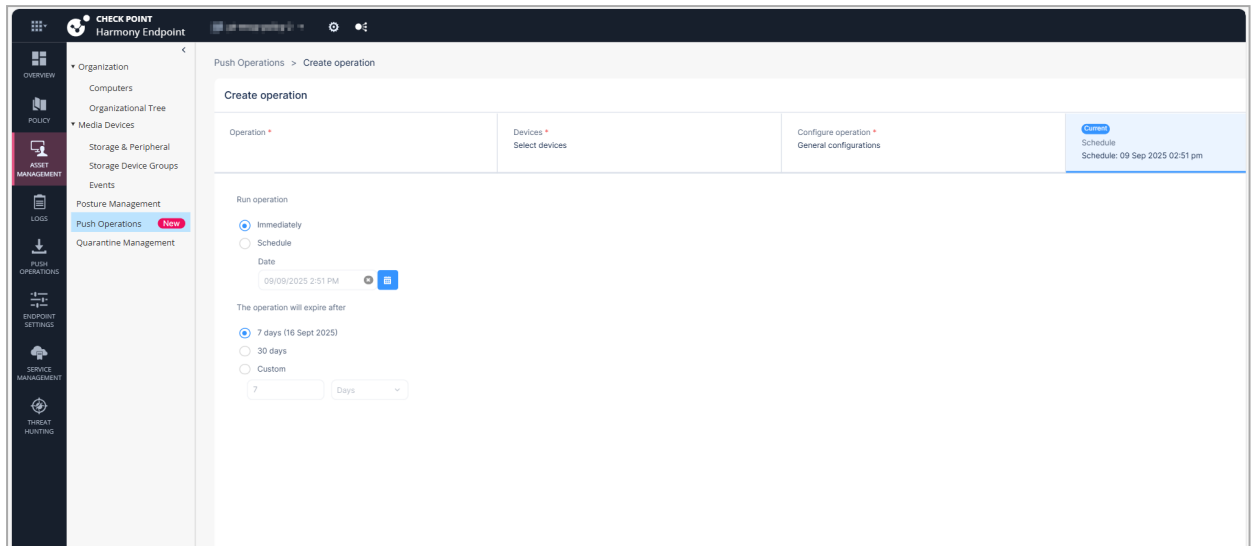
Field	Description
Process name	Enter the process name of the process memory dump.
Process PID	Enter the process PID of the process memory dump.
Dump info upload	Select the location to upload the memory dump: ◦ Upload Memory Dump to AWS S3 - After the push operation is successful, the system shows a download option in the Operation output column of the Push Operation Endpoint Details section. ◦ Upload Memory Dump to Check Point servers - After the push operation is successful, the system uploads the memory dump to this location: ◦ For Windows Endpoint Security Client versions E88.31 and higher, client logs are stored in the directory <i>C:\ProgramData\CheckPoint\EndpointSecurity\Temp</i>. ◦ For Windows Endpoint Security Client versions E88.30 and lower, client logs are stored in the directory <i>C:\Windows\SysWOW64\config\systemprofile\CPInfo</i>. ◦ For macOS, client logs are stored in the directory <i>/Users/Shared/cplogs</i>. ◦ Upload Memory Dump to Corporate server - Enter your corporate server details. After the push operation is successful, the system uploads the memory dump to the configured location in the corporate server.

**Notes:**

- Automated packaging and upload of memory dump - All memory dumps are automatically zipped, segmented if necessary, and uploaded to the designated destination (Check Point FTP, Amazon S3, or custom FTP servers).
- On 32-bit Windows systems, the ZIP file name is not displayed when uploading full memory dumps to an FTP server.
- The Memory Dump feature is supported only on Endpoint Security for Windows client version E89.05 and later.

9. Click **Next**.

10. (Optional) In the **Schedule** tab, configure the schedule to run the operation.



a. In the **Run Operation** section:

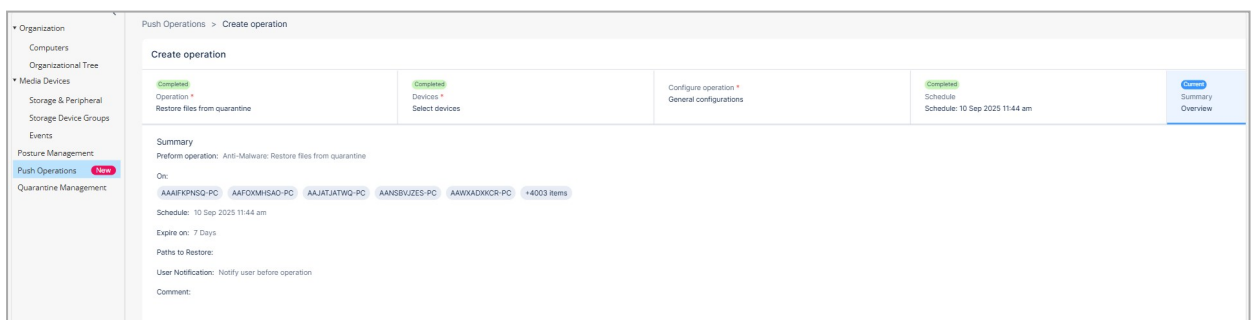
- To execute the operation immediately, select **Immediately**.
- To schedule the date and time to run the operation, select **Schedule** and in the **Date** section, select the required date and time.

b. In the **Expire on** section, select the expiration time frame.

- 7 days
- 30 days
- Custom

11. Click **Next**.

12. The **Summary** tab shows a summary of the selected operation.



13. Click **Create**.

Affected Devices Table

Column	Description
Devices	Lists the selected devices.
Operation status	Displays the status of each device: ■ Succeeded: Operation completed successfully. ■ Blade not installed: Endpoint lacks the required blade for this operation. ■ Agent not installed: The Endpoint Security Agent is not on the device. ■ Timed out: The operation did not complete in time.
Status received on	Displays the date and time when the operation was initiated on that device.
Sent to device on	Displays the date and time when the operation was sent to the device.
Operation output	Path or file location related to the operation. The Copy  icon allows you to copy the output path quickly.

Filtering the Push Operations

To filter push operations, use one of the following ways:

- Click on the **Search** bar on the top-right corner and enter the required text.
- Click the **Filter**  icon next to the **Search** bar and select the required options.

Certificate Management

Certificate Management allows you to use your certificates to sign the [export package](#). By default, Check Point certificate is used.

To add a new certificate:

1. Go to **Endpoint Settings > Certificate Management**.
2. Click **+**.

The **New Certificate** window appears.

3. Click **Browse** and select the certificate.
4. (Optional) In the **Comments** field, enter a comment.
5. Click **Save**.
6. To delete a certificate, click  and then **Delete**.

Forensics Data

Endpoint Security collects forensics data from endpoints that you can export to a data analytics tool for analysis and create policies accordingly to prevent attacks. For more information on forensics, see [Automated Attack analysis](#).

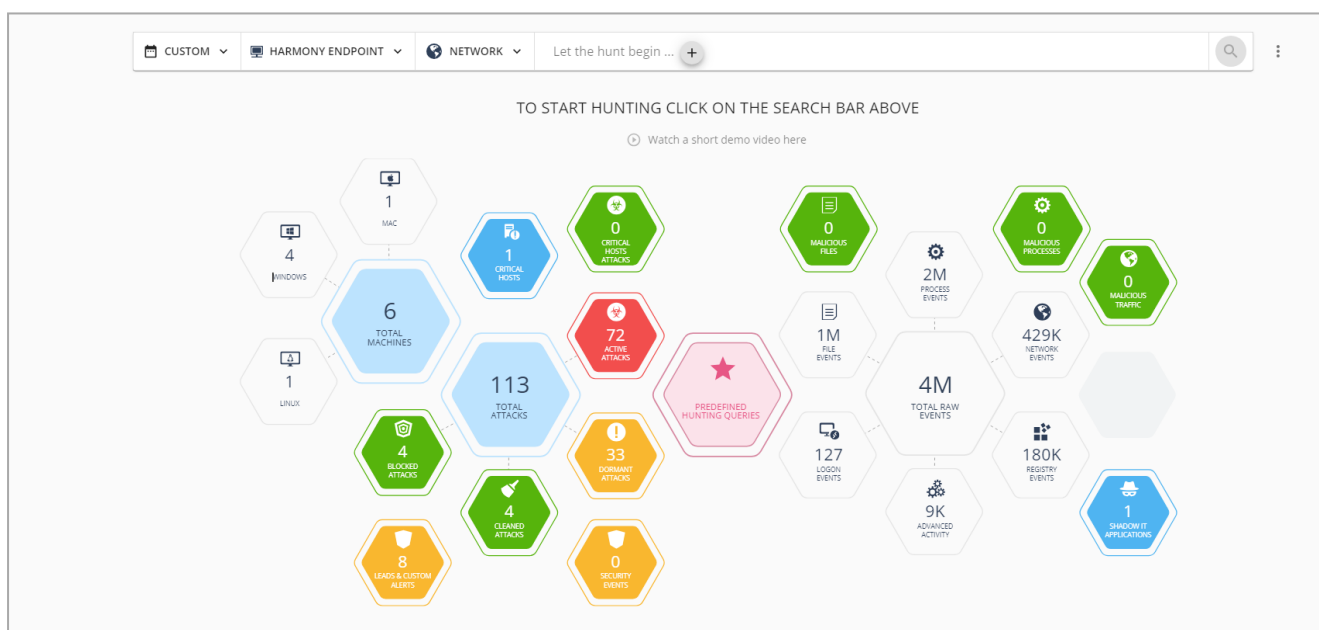
You can perform following actions with the forensics data:

- Exporting to Check Point's *"Threat Hunting" below*.
- *"Sending Forensics Data to Third-Party Analytics Tool" on page 656*
- *"Downloading Forensics Reports" on page 656*

Note - Endpoint Security exports the forensic data only in the JSON format. Make sure that the third-party data analytics tool accepts the data in the JSON format.

Threat Hunting

Threat Hunting is an investigative tool which allows for advanced querying on all malicious and benign forensics events collected from the organization's endpoints with Check Point Endpoint Security installed.



The information collected lets you to:

- Investigate the full scope of an attack.
- Discover stealth attack by observation of a suspicious activity.
- Remediate the attack before it causes further damage.
- Proactively hunt for advanced attacks by searching for anomalies, and using hunting leads and enrichment.

Threat Hunting supports:

- Data collection and enrichment - All events are collected through multiple sensors and sent to a unified repository and enhanced by ThreatCloud, MITRE mapping and alerts from all the prevention engines.
- Rich toolset for custom queries, drill down and pivoting to suspicious activity.
- Predefined queries and a MITRE dashboard which map all activity and allow a quick start to proactive hunting.
- Remediation actions per result or a bulk operation integrated in the Threat Hunting flow (such as file quarantine and kill process).

Supported Regions

Threat Hunting is supported only for the Check Point Portal tenants (accounts) residing in these regions:

- Australia
- EU
- India
- United Kingdom
- United Arab Emirates
- US

Supported Versions

- Endpoint Security Client version E84.10 and higher.
- Management version:
 - Cloud-only, web management.

Enabling Threat Hunting

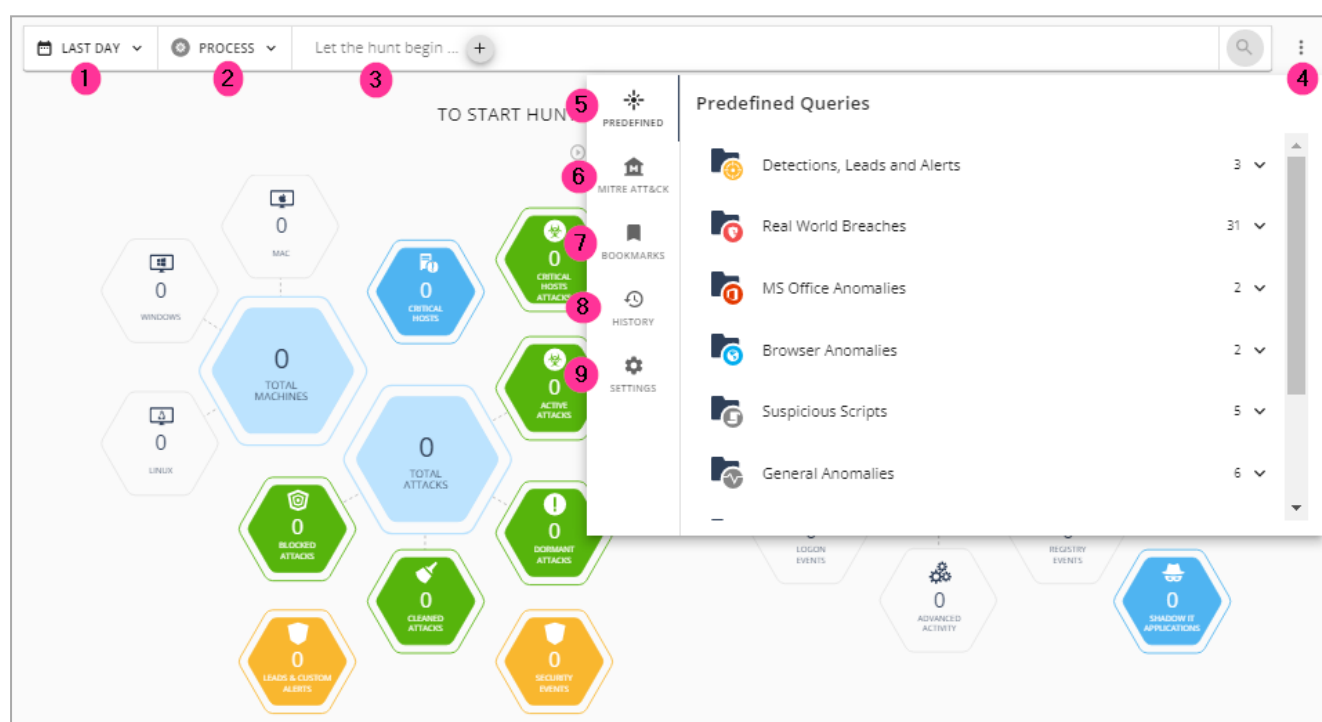
By default, Threat Hunting is disabled in Endpoint Security.

To enable Threat Hunting:

1. Go to **Policy > Policy Capabilities**.
2. Click the **Analysis & Remediation** tab.
3. From the **Enable Threat Hunting** list, select **On**.
4. Click **Save & Install**.
5. After the policy is pushed to the agents, wait a few minutes until data is sent by the agents.

Then you can go to the **Threat Hunting** view to start searching through events.

Using Threat Hunting



Item	Description
1	Last Day - Time filter for the query. Users can choose between Last Day , Last 2 Days , Last Week and a Custom time period.
2	Process - Refine your query results according to the activity type.
3	Let the hunt begin - Click + and define the values to search in the logs. You can add multiple values and fields at a time.
4	Menu for predefined queries.

Item	Description
5	Predefined - Check Point's predefined queries, divided by category.  Note - Leads in Detections, Leads and Alerts are lead detections or signatures. If an incident is raised under this category, the term Lead. is prefixed to its protection name. For example, Lead.Win.BrwsrPassThft.B. It does NOT indicate an attack and we recommend that you ignore these incidents. This is used by Check Point to analyze if a protection has to be developed. For example, create a new signature.
6	MITRE ATT&CK - Shows the MITRE ATT&CK framework of tactics and techniques. Each technique includes one or more queries, pre-defined by Check Point Research.
7	Bookmarks - Shows the custom queries saved as bookmarks, either as global (available for all users in the account) or private (available only for the user). Users can also define email notifications for these saved queries, currently limited to 10. For more information, see "Saving a Query as a Bookmark" on page 653.
8	History - See all the queries that you used.
9	Settings - Change the UI look and feel.

To hunt for threats, you can use predefined queries or by proactively creating your own queries.

- To use predefined queries:

1. Go to **Predefined Hunting Queries** or

Click the  icon next to the search box and select **Predefined**.

You can quickly find all active attacks and browse through different malicious events detected by Endpoint clients.

2. Click the  icon next to the search box and select **MITRE ATT&CK**.

The **MITRE ATT&CK** dashboard provides real-time visibility on all the techniques observed by Endpoint Security across your endpoints. It maps all raw events to MITRE Tactics, Techniques, and Procedures (TTPs) regardless of status.

The **MITRE ATT&CK** dashboard is divided into 12 categories and each category is a stage in an attack. Each category includes multiple attack techniques.

MITRE ATT&CK											
INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
Valid Accounts T1078	Software Deployment Tools T1027	Accessibility Features T1023	DLL Search Order Hijacking T1028	File System Logical Offsets T1026	Credential Dumping T1003	System Service Discovery T1027	Application Deployment Software T1028	Data from Local System T1028	Commonly Used Port T1043	Data Compressed T1022	Data Destruction T1045
Replication Through Removable Media T1029	Windows Remote Management T1029	Shortcut Modification T1023	Process Injection T1055	Obfuscated Files or Information T1027	Input Capture T1056	Query Registry T1012	Windows Remote Management T1029	Input Capture T1056	Application Layer Protocol T1027	Data Encrypted T1022	Service Stop T1049
External Remote Services T1132	Service Detection T1035	Modify Existing Service T1023	Bypass User Access Control T1028	DLL Search Order Hijacking T1028	Brute Force T1110	System Network Configuration Discovery T1026	Remote Desktop Protocol T1029	Email Collection T1134	Multilayer Encryption T1027	Exfiltration Over Command and Control Channel T1040	Inhibit System Recovery T1045
Drive-by Compromise T1189	Windows Management Instrumentation T1047	Path Interception T1024	Access Token Manipulation T1134	Process Injection T1055	Private Keys T1142	Remote System Discovery T1026	Windows Admin Shares T1027	Screen Capture T1133	Remote File Copy T1135		Resource Hijacking T1045
Spearphishing Attachment T1193	Scheduled Task/Job T1057	Logon Scripts T1057	Sudo T1109	Indicator Removal on Host T1027	Credentials in Registry T1134	System Owner/User Discovery T1027	Remote File Copy T1135		Multi-hop Proxy T1138		
Spearphishing Link T1132	Command Line Interface T1059	DLL Search Order Hijacking T1028		BundleID T1028	Credentials from Web Browsers T1134	System Network Connections Discovery T1026	Remote Services T1027		Remote Access Tools T1133		
	Scripting T1059	New Service T1035		Disabling Security Tools T1027		Process Discovery T1027			Standard Cryptographic Protocol T1022		

When you click a technique, a window opens with an explanation about the technique and a list of predefined queries. Run a query to get a list of the events in which the specific technique implementation was used.

Brute Force - Technique T1110

★ 0
Total Events

 0
Total Machines

i Adversaries may use brute force techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained.

[Official Mitre™ page](#)

Query 1  0  0

Logon Event ID **IS** 4625

Connection Count **IS NOT** 1




CLOSE

■ To search for specific events by proactively creating your own queries:

1. Go to **Threat Hunting**.
2. Click the + sign next to **Let the hunt begin**.
3. From the **Indicator** list, select the filter.

The screenshot shows a modal window titled '+ Add Filter'. It contains two dropdown menus: 'Indicator' with 'Process Name' selected, and 'Operator' with 'Is' selected. Below these is a text input field with the placeholder text 'Add a single value...' and a small 'x' icon. Below the input field, the text 'Process name' is visible. At the bottom right of the modal are two buttons: 'CANCEL' and 'ADD'.

4. From the **Operator** list, select the condition.
5. In the **Add a single value** field, enter a value for the indicator.
6. Click **Add**.

It shows the search results in a timeline. The timeline provides behavioral insights that indicate anomalies or attacks.

7. To add another filter to the same query, repeat steps 2 to 6.

 **Note** - If you have multiple filters, the system applies the logical **AND** operator between the filters.

8. To filter events based on the timeline, click the required hexagon.

It shows detailed information about the event, together with intelligent enrichment, such as attack classification, malware family and MITRE technique details.

9. To create a bookmark for a query, see ["Saving a Query as a Bookmark" on the next page](#).
10. You can also filter the results by date and process.

11. To take remediation action for the filtered results, click **Actions** and choose any of these:
 - **Terminate Process**
 - **Quarantine File**
 - **Trigger Forensic Analysis**
 - **Isolate Machine**
12. To export the results to a CSV file, click **Actions > Export to CSV**.

Saving a Query as a Bookmark

You can add filters to a query and save it as a bookmark. You can also send email notifications to users if Threat Hunting activity matches the query.

To save a query as a bookmark:

1. Create a [query](#).
2. Click ☆ from the top right corner of the page.

The **Create Shared/Private Bookmark** pop-up appears.

+ Create Shared Bookmark

☒ Shared - available to all system users
☐ Private - available only to you

Name:
 Importance:

Select or create tag name

Description

Max. characters: 500

☐ Send E-mail notifications to mailing list for any new hits

CANCEL SAVE

3. To make the bookmark public, select **Shared - available to all system users**.
4. To make the bookmark private, select **Private - available only to you**.
5. In the **Name** field, enter a query name.
6. From the **Importance** list, select an importance level for the query detection.
7. In the **Select or create tag name** field, enter the tag name or select the tag name if available.

Tags create folders to store bookmarked queries.

8. In the **Description** field, enter a description for the bookmark.
9. To send email notifications if new activity matches the bookmarked query, select **Send E-mail notifications to mailing list for any new hits** checkbox.

Endpoint Security sends email notifications to the recipients added to the **Threat Hunting Notifications** page.

10. Click **Save**.

To add recipients to Threat Hunting email notifications:

1. Go to **Threat Hunting**.
2. Click the  icon next to the search box and select **Notifications**.
3. From the **Recipients** list, select the users or enter the email address.

Use Case - Maze Ransomware Threat Hunting

You want to investigate the maze ransomware attack. You read about it in the internet and you are afraid it may already have infiltrated your organization.

1. In the MITRE ATT&CK website: Search for Maze ransomware.
2. From the list of techniques that Maze ransomware uses, select the applicable technique.
For example: Windows Management Instrumentation
3. From the Check Point Portal, access **Threat Hunting**
4. Click the  icon on the right side of the search box, and go to **MITRE ATT&CK**.
5. In the **MITRE ATT&CK** dashboard, search for the technique you copied from the Maze website.
6. Click the technique to see all the events in your organization in which this technique was used.

Sending Forensics Data to Third-Party Analytics Tool

You can send the forensics data to a third-party data analytics tool, such as Elastic that accepts the data in the JSON format.

To send forensics report to the Third-Party analytics tool:

1. Navigate to **Threat Prevention > Manage > Manage Data Tube**.
2. In the **URL** field, enter the URL of the third-party data analytics tool.

 **Note** - Endpoint Security does not support to enter user credentials for the third-party analytics tool for authentication.

3. Click **Save**.

The system applies the policy to all endpoints.

Endpoints send the forensic data in JSON format to the third-party data analytics tool.

Downloading Forensics Reports

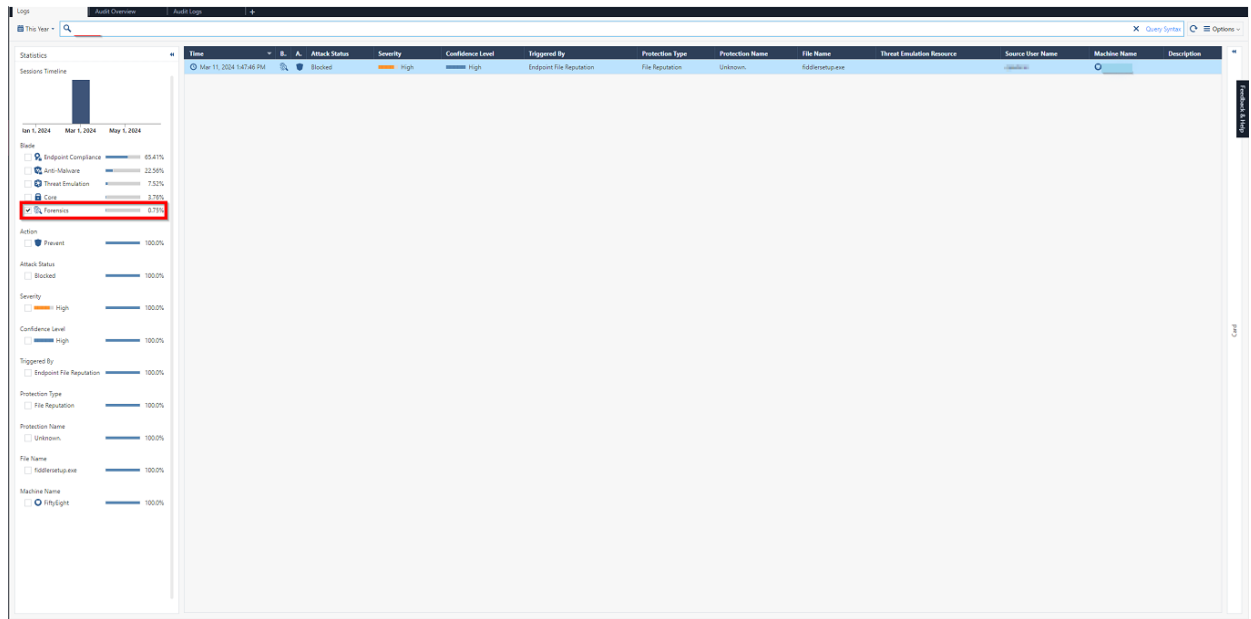
The Forensic Report shows a comprehensive analysis of the entire sequence of an attack, as analyzed by the Forensics software blade in Endpoint Security.

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.

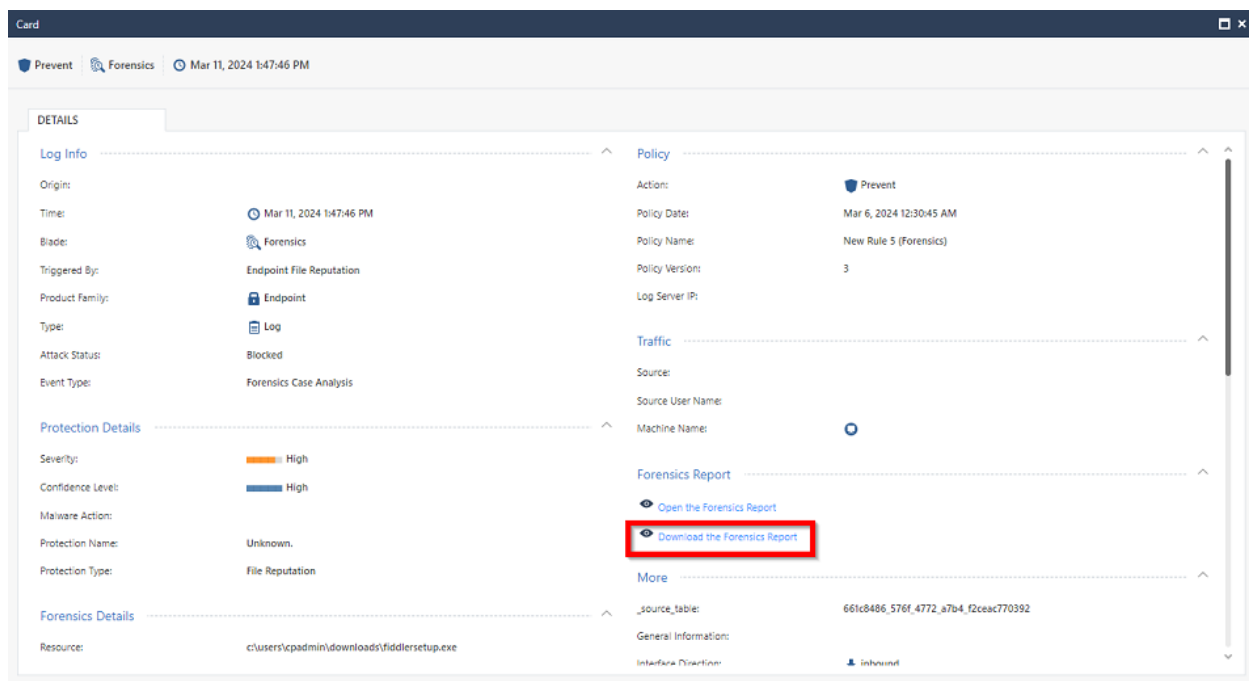
To download the forensics report of an event:

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 ["Endpoint Security Logs" on page 567](#) .



Note - To search the Forensics event using the machine name, enter the machine name in the search field and click **Enter**.

- From the list, double-click the event for which you want to download the report.
The **Card** window with the log details appears.
- 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.

Two-Factor Authentication

Check Point recommends you to configure two-factor authentication for Endpoint Security. To configure, see [Two-Factor Authentication](#).

Endpoint Security for Linux

This chapter describes the installation and use of Endpoint Security in Linux operating systems.

- [*"Endpoint Security for Linux Overview" on page 660*](#)
- [*"Deploying Endpoint Security for Linux" on page 678*](#)
- [*"Endpoint Security for Linux Runtime Configurations" on page 680*](#)
- [*"Endpoint Security for Linux CLI Commands" on page 684*](#)
- [*"Endpoint Security for Linux Additional Information" on page 687*](#)

Endpoint Security for Linux Overview

 **Note** - Starting in R81, the on-premises Endpoint Security Server supports Endpoint Security for Linux. To enable Endpoint Security 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](#).
- Ensure these directories reside on a file system mounted with executable permissions. Avoid using the `noexec` option when mounting these file systems.
 - `/var/lib`
 - `/tmp`
- The Linux Kernel Headers package for the installed kernel must be available. This package is typically installed during the Linux distribution installation.

Key Threat Prevention Technologies

Anti-Malware

- The Anti-Malware security engine detects trojans, viruses, malware, and other malicious threats.
- The engine is implemented as a multi-threaded flexible scanner daemon. It is managed centrally through a web-console.
- In addition, it supports command line utilities for on-demand file scans, access functionality, and automatic signature updates.
- Managed centrally through a web-console and also supports Command Line Utilities for on-demand file/folder scans, detection lists and file restorations

Endpoint Detection and Response (EDR) / Threat Hunting

- Endpoint Security for Linux, updates ThreatCloud with Indicator of Compromise (IoC) and Indicator of Attack (IoA) events.
- Threat Hunting technology lets the administrators proactively search for cyber threats that made it through the first line of defense to the Linux Endpoint device.

- Threat Hunting uses advanced detection capabilities, such as queries and automation, to find malicious activities and extract hunting leads of data.
- Supporting events:
 - Process - start / stop
 - Files - create / delete / rename / open
 - Network - local connections, ports, DNS

Behavioral Guard

- Dynamic analysis of malware executed on the Endpoint Client is performed based on the behavioral patterns of various attack types, including ransomware, cryptominers, and trojans.
- Centrally managed via the web management platform.
- Leverages a large set of constantly updated signatures to detect, prevent, and remediate modern attacks.
- Features automatic signature updates powered by the latest intelligence, ensuring adaptation to emerging threats

Anti-Ransomware

Monitors the endpoint for signs of ransomware activity and helps prevent file encryption by malicious actors.

Forensics

Generates detailed analytics and interactive reports from threats and incidents, providing a comprehensive view of attack flows and actionable insights for effective remediation.

 **Note** - Starting from version 1.22.x, the Forensics security blade is installed by default when the Behavioral Guard security blade is installed.

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

Supported Linux Versions

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Ubuntu 25.10	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Ubuntu 24.04 (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–
Ubuntu 22.04 (64-bit) (Supported versions: 22.04 - 22.04.3)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Distribution / OS Version	1.28.12	1.28.11	1.26.8	1.24.02	1.22.18	1.22.16	1.22.12	1.20.7	1.18.16	1.18.12	1.15.10	1.13.7	1.13.3	1.13.2
Ubuntu 20.04 (64-bit) (Supported versions: 20.04 - 20.04.6)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Ubuntu 18.04* (64-bit) (Supported versions: 18.04 - 18.04.6)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Ubuntu 16.04 (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Alma Linux 10.1	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Alma Linux 10	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Alma Linux 9.7	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Alma Linux 9.6	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Alma Linux 9.5	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
Alma Linux 9 (64-bit) (Supported versions: 9.0 - 9.3)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Alma Linux 8 (64-bit) (Supported versions: 8.9 and 8.10)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
Amazon Linux 2023	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
Amazon Linux 2 (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Cent OS 8* (64-bit) (Supported versions : 8.0 - 8.5)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Distri butio n / OS Versi on	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Cent OS 7 (64- bit) (Sup porte d versi ons: 7.8 - and 7.9)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	—	—
Debi an Linux 13.3	✓	✓	—	—	—	—	—	—	—	—	—	—	—	—
Debi an Linux 13.2	✓	✓	—	—	—	—	—	—	—	—	—	—	—	—
Debi an Linux 13 (64- bit)	✓	✓	✓	—	—	—	—	—	—	—	—	—	—	—

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
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)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 39 ¹	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Fedora 38 ¹	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 37	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 36	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 35	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Fedora 34	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Mint 22.3	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Mint 22.2	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Mint 22.1	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
Mint 22	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–
Mint 21.3	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
OpenSUSE Leap 16.0	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
OpenSUSE Leap 15.6	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
OpenSUSE 15.4 and OpenSUSE 15.5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
OpenSUSE 42.3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Oracle Linux 10.1	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Oracle Linux 10	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
Oracle Linux 9.7	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Oracle Linux 9.6	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Oracle Linux 9.5	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Oracle Linux 9.4	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
Oracle Linux 8 (64-bit) (Supported versions: 8.0 - 8.10)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Oracle Linux 7.9 (64-bit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Red Hat Enterprise Linux (RHEL) 10 (64-bit)	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Red Hat Enterprise Linux (RHEL) 9.7 (64-bit)	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Red Hat Enterprise Linux (RHEL) 9.6 (64-bit)	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
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	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	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)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Rocky 10.1	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Rocky 10	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–
Rocky 9.7	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
Rocky 9.5	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
Rocky 8.10	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
SUSE Linux Enterprise Server (SLES) 16 (64-bit)	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
SUSE Linux Enterprise Server (SLES) 15 (64-bit) (Supported versions: 15S P7)	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–

Distribution / OS Version	1.2 8.1 2	1.2 8.1 1	1. 26 .8	1.2 4.0 2	1.2 2.1 8	1.2 2.1 6	1.2 2.1 2	1. 20 .7	1.1 8.1 6	1.1 8.1 2	1.1 5.1 0	1. 15 .7	1. 13 .3	1. 13 .2
SUSE Linux Enterprise Server (SLES) 15 (64-bit) (Supported versions: 15S P2 and 15S P3)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SUSE Linux Enterprise Server (SLES) 12 (64-bit) (Supported versions: 12S P5)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

¹ Only Anti-Malware support.

Linux Kernel Support

Endpoint Security for Linux supports the general-purpose Linux kernels included in standard Linux distributions. These kernels come by default with Linux distribution.

This excludes kernels that are:

- Non default kernels
- Unbreakable kernels
- Appliance, for example, Exadata
- Community based, for example, ELRepo
- Custom Compiled kernels
- Desktop and Gaming kernels

Installation on Semi-Isolated Environments with Super Node Proxy

Prerequisite

1. Make sure that Endpoint Security for Linux version 1.22.12 or higher is installed on client devices.
2. Make sure that Endpoint Security for Windows version E88.70 or higher is installed on super node devices.
3. The Linux devices must be able to resolve the Fully Qualified Domain Name (FQDN) of the Windows super node machine. This can be achieved through an organizational name server.



Notes:

- Before exporting the package, make sure that a Windows super-node is properly configured in the server policy for each virtual group of Linux devices. For more information, see ["General" on page 353](#).

Installation Procedure

1. **Export and Download the Offline Package:** Download the appropriate universal offline package (rpm or deb) that matches your distribution. Transfer the package to all endpoint devices.
2. For Red Hat Enterprise Linux (RHEL), run this command before installing the package:

```
subscription-manager config --rhsm.manage_repos=0
```


3. Run the installation package.
4. **Verify communication with the Management Server:**

- a. To verify the status, run:

```
cpla info
```

```
(venv) root@fedora:~# cpla info
CPLA version: 1.22.3
Operating system: Fedora Linux 39
Management server URL: 172.23.123.209
Connection status: Connected - Supernode
Enabled engines:
Anti Malware: Installed
```

The output displays:

```
Connection status: Connected - Supernode
```

The client appears in the server's asset information.

Note - If communication is not established, perform these:

1. Verify Windows device FQDN is resolvable from the Linux device and that super-node device proxy functionality is working, for example, `curl --proxy http://<super-node fqdn>:3128 https://www.checkpoint.com`
2. Verify super-node policy is configured and installed prior to exporting a package.
3. Verify `SBA_SEMI_ISOLATED_ENV` environment variable is correctly applied: The file `/etc/checkpoint/cpla/env` should contain the line `SBA_SEMI_ISOLATED_ENV=1`
4. Verify that the default policy is detected during installation. If not, contact [Check Point Support](#) and verify that the support for semi-isolated environment is active. See **step 4** in [Prerequisites](#):

If the default policy is processed correctly, these lines should appear in `/var/log/checkpoint/common/sbalinux-install.log`:

```
super_node: found default policies
super_node: extracted default policies to /tmp/tmp.PM0DcS0Lav
super_node: processing policy - type: 401 pac: 1 id: 6be2fbae-1b28-4e52-9192-e50e499b6e73 mod_date: 10
super_node: PAC_1_Pol_CPEPS_SID401_ID_6be2fbae-1b28-4e52-9192-e50e499b6e73_content.cppol -> 401_1.dat
super_node: processing policy - type: 51 pac: 1 id: 770d1b19-2262-423a-b29a-9d2d70197d6a mod_date: 1737458621360
super_node: PAC_1_Pol_CPEPS_SID51_ID_770d1b19-2262-423a-b29a-9d2d70197d6a_content.cppol -> 51_1.dat
super_node: created registry file
```

Deploying Endpoint Security for Linux

This section explains how to install Endpoint Security on Linux operating systems for Endpoint cloud users.

To install Endpoint Security for Linux for Endpoint Cloud Users:

1. Navigate to **Policy > Export Package**
2. Download the Linux installation script:
3. Copy/Download the installation script to the target device. Run one of these options:

- To allow execution permission to the file, run:

```
chmod +x ./<Name of Install Script>
```

- If the Linux host uses HTTP or HTTPS proxy, install the client using the proxy details:

```
sudo ./<Name of Install Script> install --http_proxy  
http://username:password@proxy_address:port
```

- 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 --productedr
```

- To deploy Behavioral Guard only, run:

```
sudo ./<Name of Install Script> install --  
product bg
```

- To enable the Threat Hunting function, make sure that Threat Hunting is enabled in the applicable policy rule. Navigate to **Policy > Threat Prevention > Analysis & Remediation** and ensure Threat Hunting is set to ON.

Notes:

- If Strong/Kerberos authentication is enabled, then HTTP 401 is in the `/var/log/checkpoint/cpla/cpla.log`.
- It is necessary to put the keytab file used for authentication set up in the file `/var/lib/checkpoint/cpmgmt/auth.keytab` (the file is generated by the *ktpass* utility).

```
sudo ./<install script name> install --product edr
```

Endpoint Security for Linux Runtime Configurations

Overview

The CPLA component monitors applications running inside Linux containers and associates security events with the correct container context.

By retrieving metadata from the container runtime, CPLA improves event accuracy and supports investigation of container-based activity.

Limitations

- Default configuration works for most environments.
- The CRI-O socket path cannot be modified.
- Kubernetes distributions may require runtime-specific configuration.

How Container Runtime Monitoring Works

When container runtime monitoring is enabled:

1. An application running inside a container generates a security event.
2. CPLA identifies the container associated with the event.
3. CPLA queries the container runtime API.
4. The container runtime returns container metadata.
5. CPLA enriches the event with container context information.

Supported Container Runtimes

CPLA supports the following container runtimes:

- Docker
- containerd
- CRI-O

Default configuration settings are provided for all supported runtimes and are suitable for most environments. In certain deployments, configuration customization may be required to align with the infrastructure or runtime setup.

Prerequisites

Before configuring container runtime integration, verify that:

- The CPLA service is installed and running
- A supported container runtime (Docker, containerd, or CRI-O) is installed.

Configuring Container Runtime Settings

CPLA container runtime settings are configured using environment variables in the CPLA environment file.

To configure container runtime settings:

1. Stop the CPLA service:

```
systemctl stop cpla.service
```

2. Edit the file:

```
/etc/checkpoint/cpla/env
```

Add or modify the required environment variables. (See, [Runtime-Specific Configuration](#)).

3. Start the CPLA service:

```
systemctl start cpla.service
```

Path Configuration Requirements

CPLA runs in a sandbox and accesses the host filesystem through a `/host` mount.

- If a configured path is outside `/run` or `/var/run`, the path must be prefixed with `/host`
- Paths under `/run` or `/var/run` do not require the `/host` prefix

For example,

Host path	Configured path
<code>/var/lib/containerd/containerd.sock</code>	<code>/host/var/lib/containerd/containerd.sock</code>

Runtime-Specific Configuration

Docker

CPLA connects to Docker using the standard `DOCKER_HOST` environment variable.

Environment Variable	Description	Default Value
<code>DOCKER_HOST</code>	Docker API socket URL	<code>unix:///var/run/docker.sock</code>

Note - If the Docker daemon uses a non-default API socket, update the value in the CPLA environment file.

containerd

When using containerd, configure the following environment variables as required:

Environment Variable	Description	Default Value
SBA_CONTAINERD_SOCK	Path to containerd API unix socket	/run/containerd/containerd.sock
SBA_CONTAINERD_V2_TASK_PATH	Path to containerd state directory	/run/containerd/io.containerd.runtime.v2.task
SBA_CONTAINERD_NAMESPACE	Containerd namespace for containers	default

CRI-O

CPLA supports API version configuration for CRI-O.

Environment Variable	Description	Default Value
SBA_CRI_API_VERSION	API version (v1alpha2 or v1)	Auto-detected

Notes -

- If not configured, CPLA automatically detects the API version.
- CPLA always uses the default socket:
/var/run/crio/crio.sock
- The CRI-O socket path cannot be changed.

Kubernetes-Specific Configuration

Some Kubernetes distributions use non-default container runtime paths. In these environments, CPLA must be configured accordingly.

MicroK8s

MicroK8s is a Kubernetes distribution from Canonical that installs as a snap package. As a result, runtime paths are prefixed with the snap installation location. MicroK8s uses containerd as the underlying container runtime. When installed with default settings and in the default location, the following configuration applies.

```
SBA_CONTAINERD_
SOCK=/host/var/snap/microk8s/common/run/containerd.sock

SBA_CONTAINERD_V2_TASK_
PATH=/host/var/snap/microk8s/common/run/containerd/io.containerd.run
time.v2.task

SBA_CONTAINERD_NAMESPACE=k8s.io
```

 **Note** - These paths are outside `/run` or `/var/run`; therefore the `/host` prefix is required.

K3s

K3s is a Kubernetes distribution commonly used with Rancher, but it can also be deployed independently. By default, it uses containerd as the underlying container runtime with a custom runtime directory.

Use the following configuration.

```
SBA_CONTAINERD_SOCK=/run/k3s/containerd/containerd.sock

SBA_CONTAINERD_V2_TASK_
PATH=/run/k3s/containerd/io.containerd.runtime.v2.task

SBA_CONTAINERD_NAMESPACE=k8s.io
```

 **Note** - These paths are under `/run`, `/host` prefix is not required.

Verification

After configuration, verify that CPLA communicates with the container runtime.

1. The CPLA service is running.
2. Confirm that container-related events include metadata.

Endpoint Security 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 bg --help
```

To show information about the installed EDR, run:

```
cpla edr info
```

To show the help for available Behavioral Guard commands, run:

```
cpla bg--help
```

To show information about the installed Behavioral Guard, run:

```
cpla bg 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 detections of Anti-Malware, run:

```
cpla am detections
```

 **Note** - To limit the number of detections displayed, use the parameter `--limit <number_of_detections>`. Default is 100.

To show the latest detections of Behavioral Guard, run:

```
cpla bg detections
```

 **Note** - To limit the number of detections displayed, use the parameter `--limit <number_of_detections>`. Default is 100.

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 Endpoint Security for Linux

To uninstall Endpoint Security from Linux, run:

```
sudo ./ <install script name> uninstall
```

To uninstall EDR only, run:

```
sudo ./ <install script name> uninstall --product edr
```

To uninstall BG only, run:

```
sudo ./ <install script name> uninstall --  
product bg
```

Endpoint Security 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 Endpoint Securityfor Linux.

Endpoint Security 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 700](#) 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 703](#).

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 Endpoint Security to randomize the **Periodic Scan** according to the scanning period. For example, if the **Scan Periodic** is set as **Every Week**, Endpoint Security 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

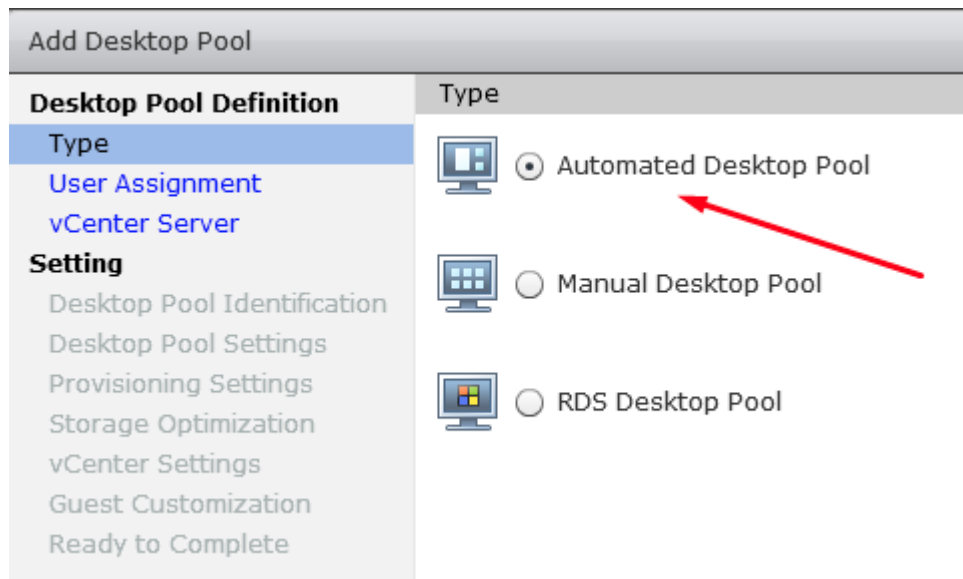
 **Best Practice** - We recommend to use a different naming pattern for each machine in each pool.

VMware Horizon Key Points

This procedure is mandatory to create supported Horizon pools for **Persistent Virtual Desktops**.

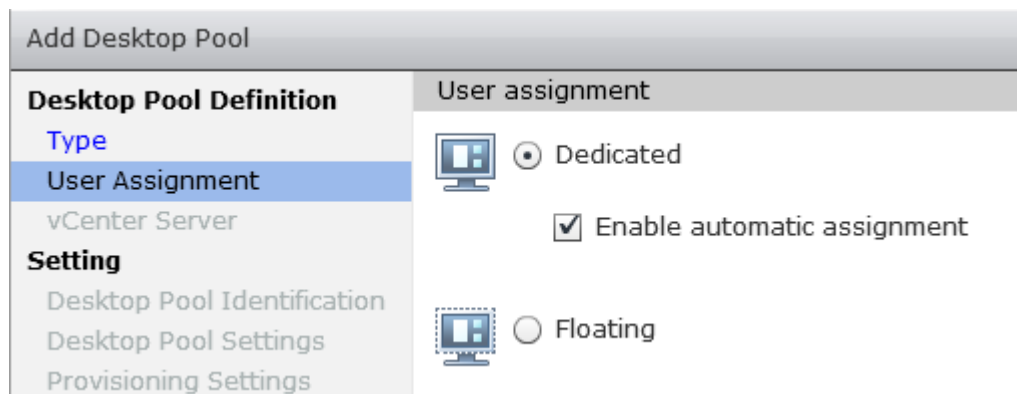
Procedure

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.

Add Desktop Pool

Desktop Pool Definition

- Type
- User Assignment
- vCenter Server**

Setting

- Desktop Pool Identification
- Desktop Pool Settings
- Provisioning Settings
- Storage Optimization
- vCenter Settings
- Guest Customization
- Ready to Complete

vCenter Server

☐ Instant clones
 ☐ View Composer linked clones
 ☐ Full virtual machines

vCenter Server

viewlab-vc.Viewcp.local(administrator@vsphere.local)

4. In **Guest Customization** panel, select **Allow reuse of pre-existing computer account**.

Add Desktop Pool - vdi-pool

Guest Customization

Domain: viewcp.local(Administrator)

AD container: CN=Computers Browse...

☒ Allow reuse of pre-existing computer accounts ?

☐ Use QuickPrep

Power-off script name: ?

Power-off script parameters: Example: p1 p2 p3

Post-synchronization script name: ?

Post-synchronization script parameters: Example: p1 p2 p3

☐ Use a customization specification (SysPrep)

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.

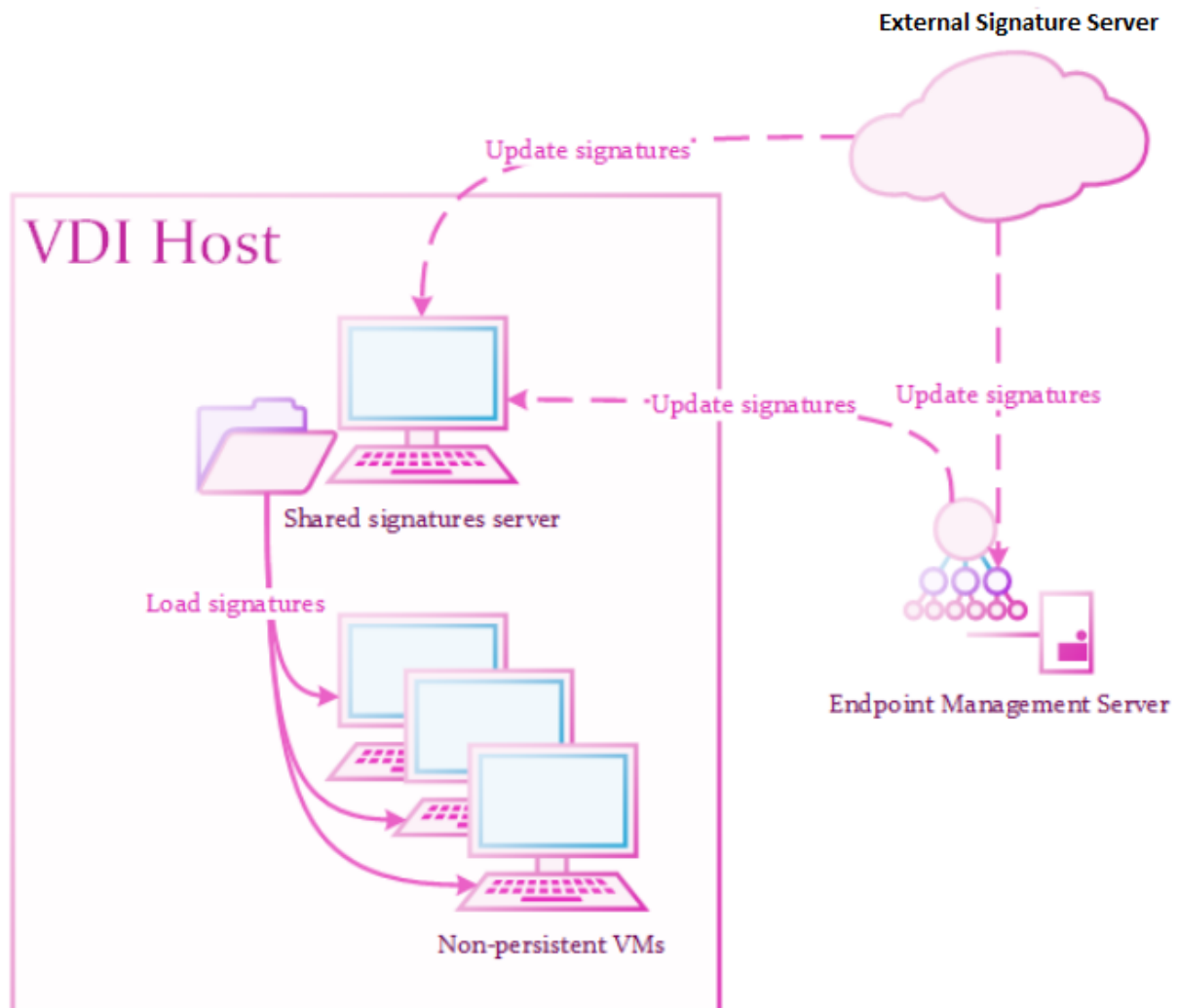
Configuring Clients for Non-Persistent Desktops

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 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 700 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 703.

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

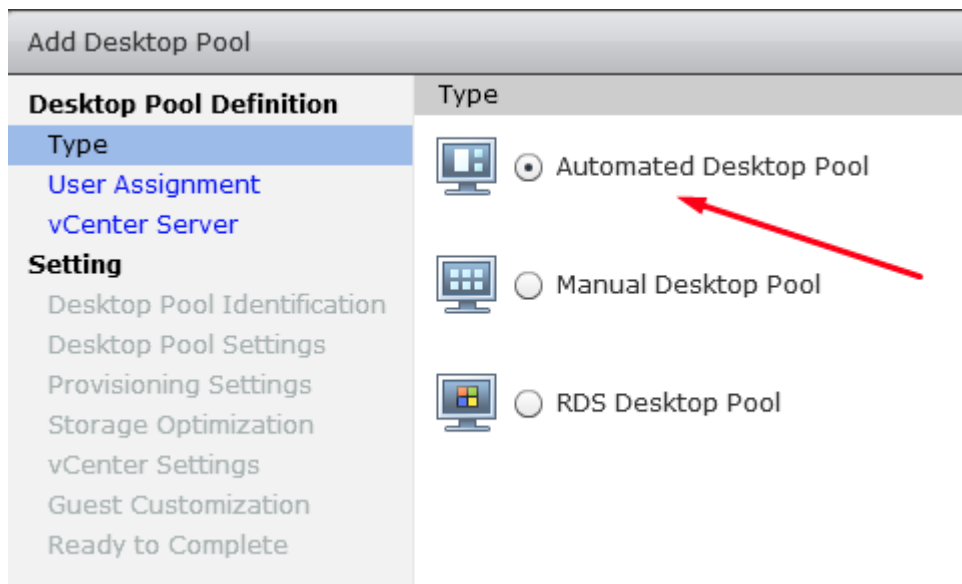
Note - Check Point recommends that each created pool will use a different machine naming pattern. This will prevent situations where Management Server has duplicate machine entries from different pools.

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**.

The screenshot shows the 'Add Desktop Pool' dialog with the 'User assignment' tab selected. In the left sidebar, 'User Assignment' is highlighted. The main area shows two options: 'Dedicated' (unselected) and 'Floating' (selected). A red arrow points to the 'Floating' radio button. The 'Enable automatic assignment' checkbox is checked.

3. In the **vCenter Server** panel, choose **Instant Clones** or **Linked Clones**.

The screenshot shows the 'Add Desktop Pool' dialog with the 'vCenter Server' tab selected. In the left sidebar, 'vCenter Server' is highlighted. The main area shows three options: 'Instant clones' (selected), 'View Composer linked clones', and 'Full virtual machines'. Red arrows point to the 'Instant clones' and 'View Composer linked clones' radio buttons. Below, the 'vCenter Server' field contains the text '172.23.15.11(administrator@vsphere.local)'.

4. In the **Guest Customization** panel, select **Allow reuse of pre-existing computer account**.

The screenshot shows the 'Add Desktop Pool - vdi-pool' dialog with the 'Guest Customization' tab selected. In the left sidebar, 'Guest Customization' is highlighted. The main area shows fields for 'Domain' (Viewcp.local(administrator)), 'AD container' (CN=Computers), and a checked checkbox 'Allow reuse of pre-existing computer accounts' which is highlighted with a red box. Below this are fields for 'Power-off script name', 'Power-off script parameters', 'Post-synchronization script name', and 'Post-synchronization script parameters', each with a help icon. The 'Ready to Complete' button is at the bottom.

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 Endpoint Security client version E86.40 and higher.
- Fully supported with Citrix Provisioning Services (PVS) running the Endpoint Security 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 Virtual 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 **Virtual Group**.
2. Export the applicable packages.

From the left navigation panel, click **Policy**.

In the **Deployment Policy** section, click **Export Package**.

3. Assign the new **Virtual Group** to a relevant policy.
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

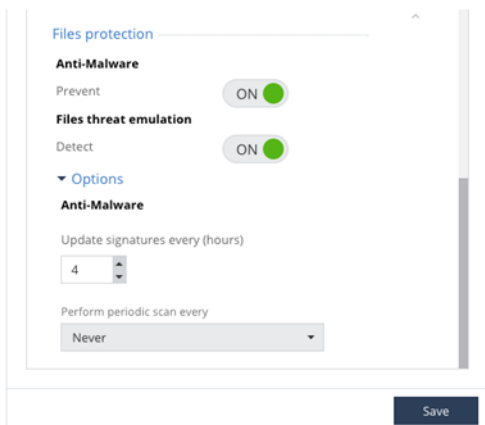
"Anti-Malware Scan Storms" can occur when anti-virus scans run at the same time on multiple virtual machines on the same physical server.

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 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.

Endpoint Security 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 Endpoint Security 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 456](#).
- 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 Endpoint Security 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 352*.

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 91*.
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](#).

Configuring Threat Emulation (TE) Appliance for Endpoint Security

Prerequisites

For TE Appliances:

- TE Appliance running on R81.10 or later.
- TE Appliance has a valid Check Point license.
- Internet connection for the TE Appliance.

For Device:

Use a Windows or a macOS machine with Endpoint Security Client connected to the Endpoint Security Management Server.

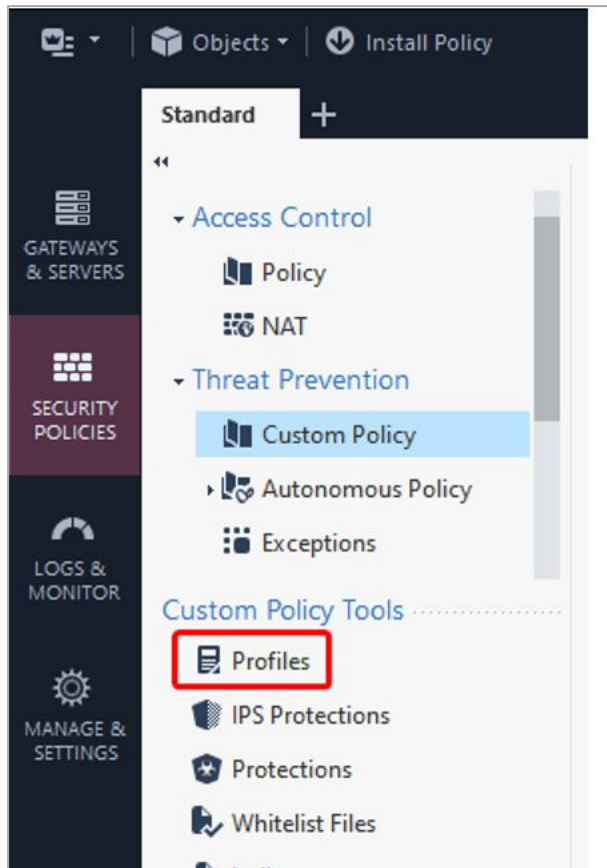
Step 1 - Configure the TE Appliance on SmartConsole

1. Configure the Security Policies

Configure the Firewall **Rulebase** as **Accept** to enable communication during the initial configuration.

2. Add a new profile

- a. Go to the **Security Policies** tab.

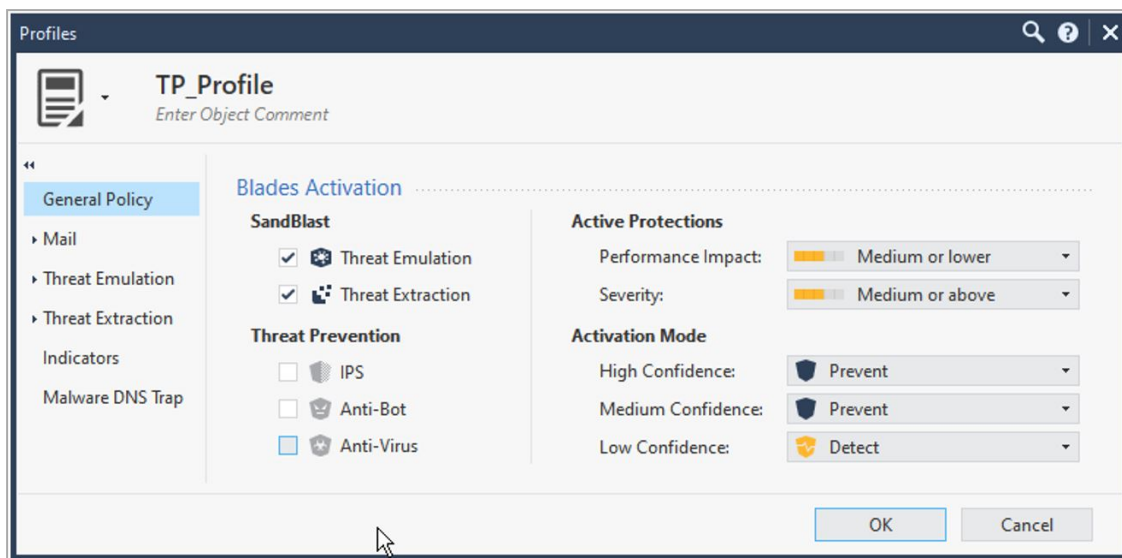


- b. In the **Custom Policy Tools** section, click **Profiles**.
- c. Click **New**.



- d. Enter a name for the profile . For example, **TP_Profile**.

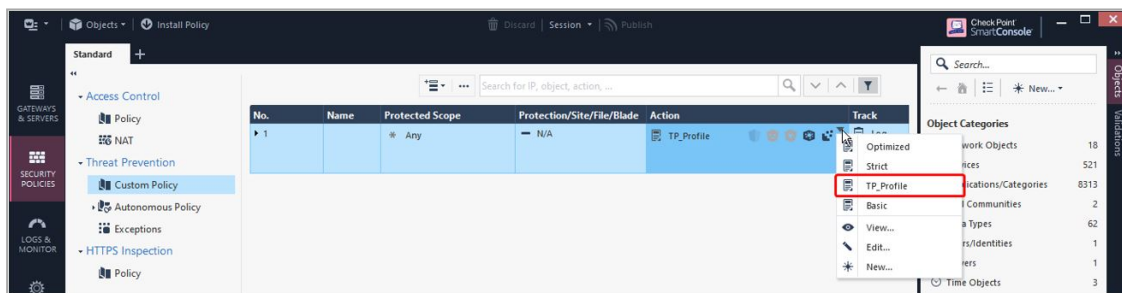
- e. Enable **Threat Emulation** and **Threat Extraction**. Ensure that all other features are disabled.



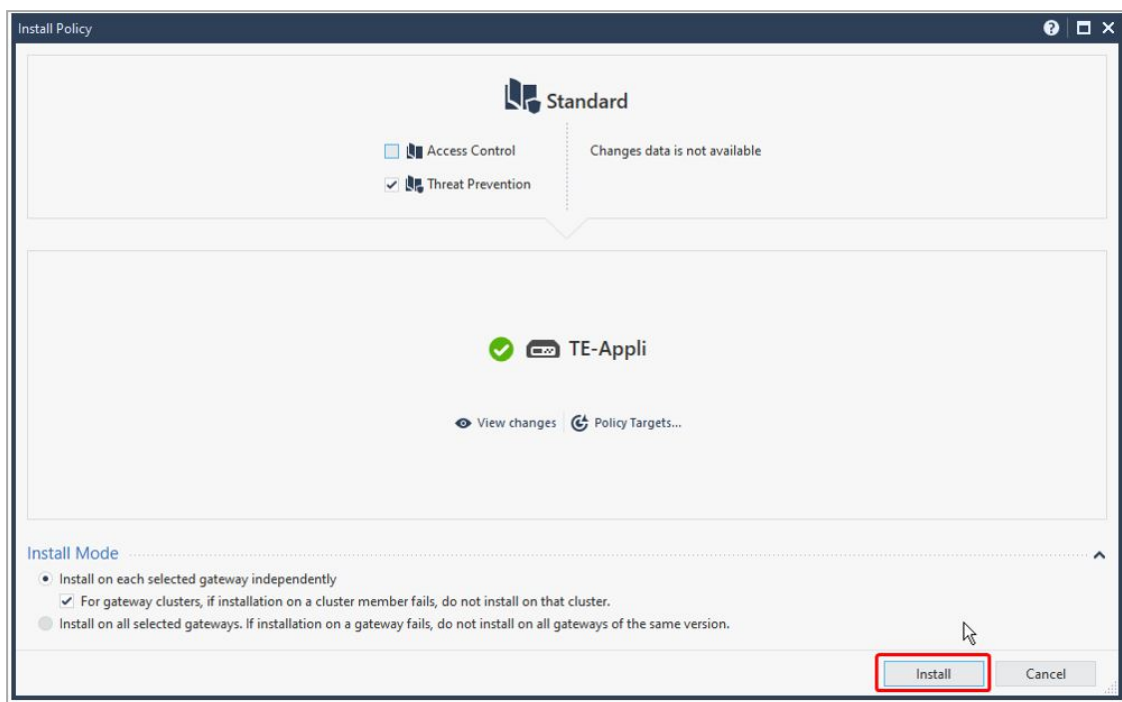
- f. Click **OK**.

3. Set up a profile for Threat Prevention policy

- a. Navigate to **Threat Prevention > Custom Policy**.
- b. Select the profile name you created while creating the new profile.



- c. Click **Install** to apply the changes to the TE Appliance.



4. Configure the Gateway Object for TE Appliance

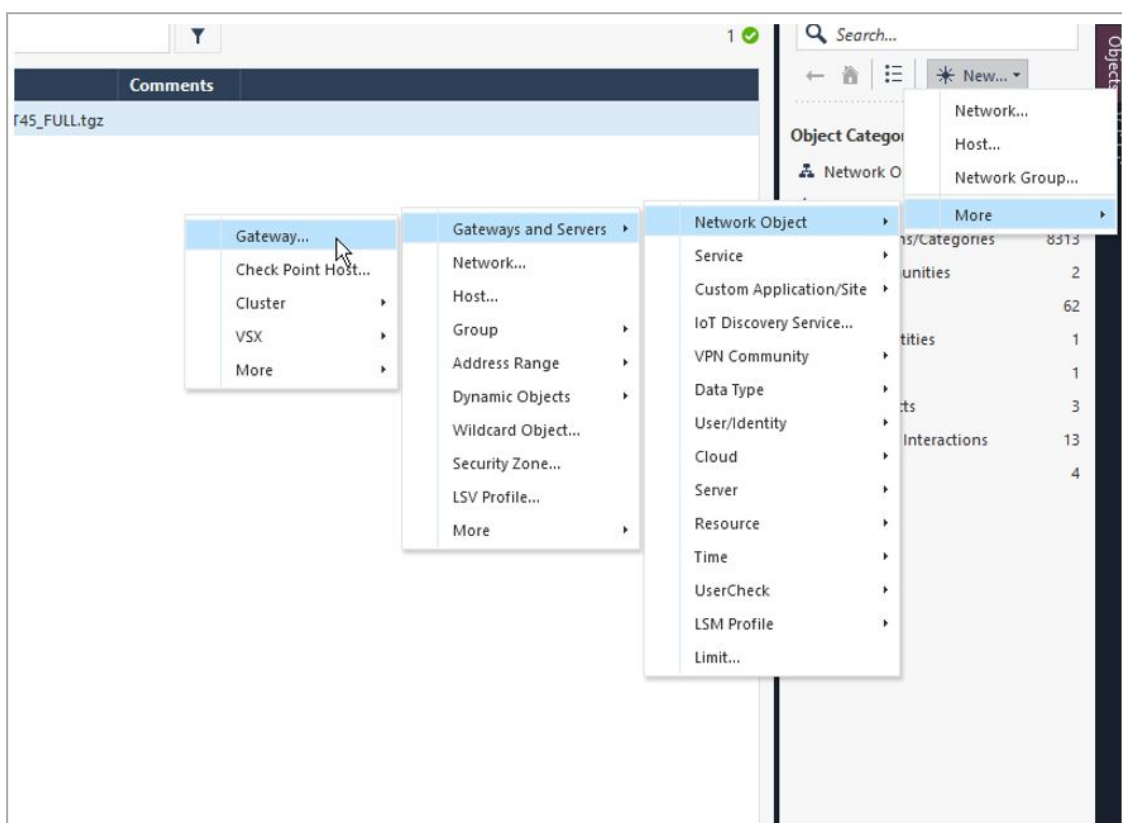
Set up the Secure Internal Communication (SIC)

- Note** - SIC is auto-configured during the initial configuration. To reset the password, following these steps:
- Open SSH Client and type **Expert** mode.
 - Enter `cpconfig` in the command line.
 - Select **Secure Internal Communication** from the menu.
 - Once prompted, set a new SIC password.

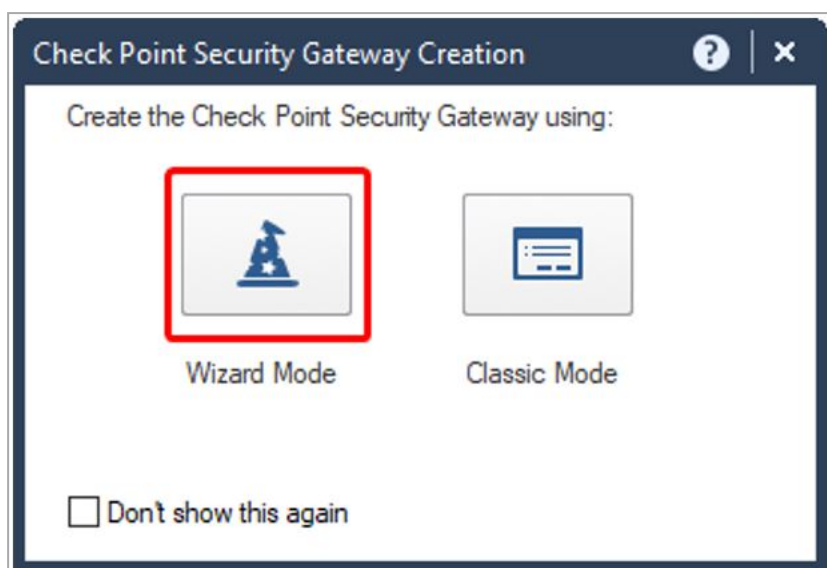
Step 2 - Create a TE Appliance Object in the SmartConsole

1. Define a Gateway Object

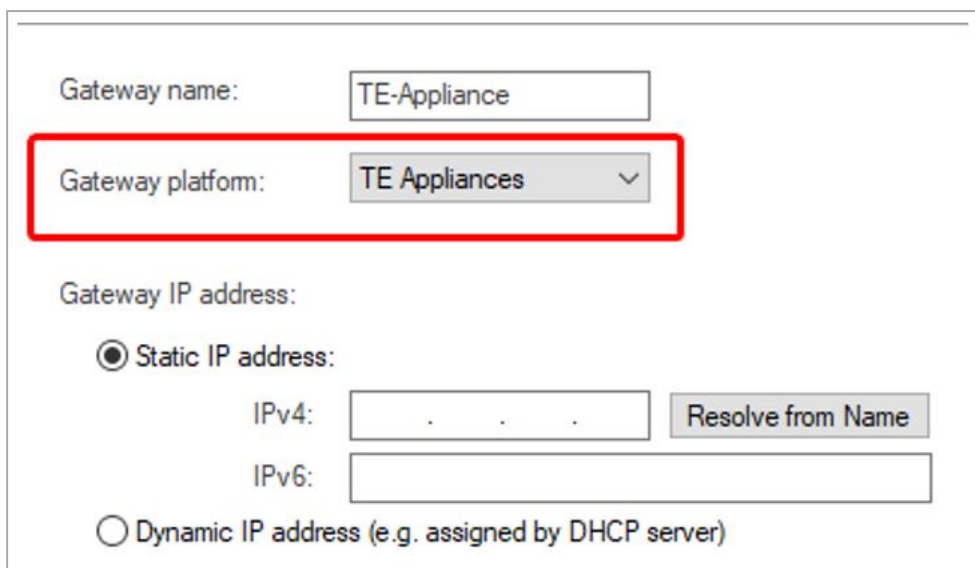
- a. Open **SmartConsole**.
- b. Go to **Gateway > Gateways and Servers > Network Object > New Gateway**.



- c. Select **Wizard Mode**.



- d. In the **Gateway platform**, select **TE Appliances** and enable **Static IP address**.



Gateway name:

Gateway platform: TE Appliances ▼

Gateway IP address:

☒ Static IP address:

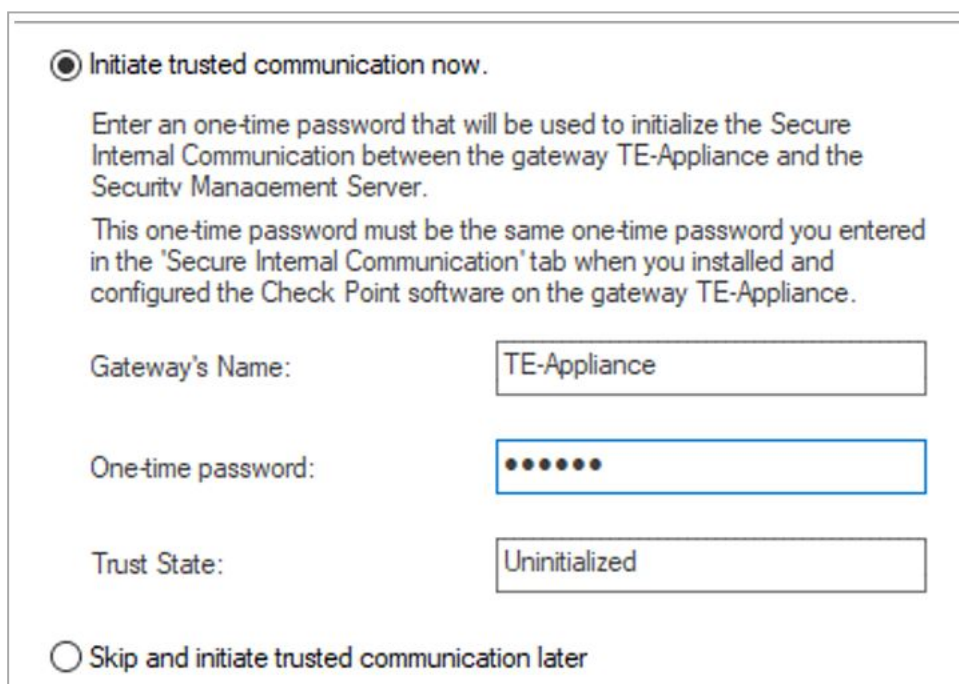
IPv4: . . Resolve from Name

IPv6:

☐ Dynamic IP address (e.g. assigned by DHCP server)

- i. Enter the SIC password.

 **Note** - Ensure that the **Trust State** is **Initialized**



☒ Initiate trusted communication now.

Enter an one-time password that will be used to initialize the Secure Internal Communication between the gateway TE-Appliance and the Security Management Server.

This one-time password must be the same one-time password you entered in the 'Secure Internal Communication' tab when you installed and configured the Check Point software on the gateway TE-Appliance.

Gateway's Name:

One-time password:

Trust State:

☐ Skip and initiate trusted communication later

- e. Complete the Wizard setup.

2. Install the Security Policy

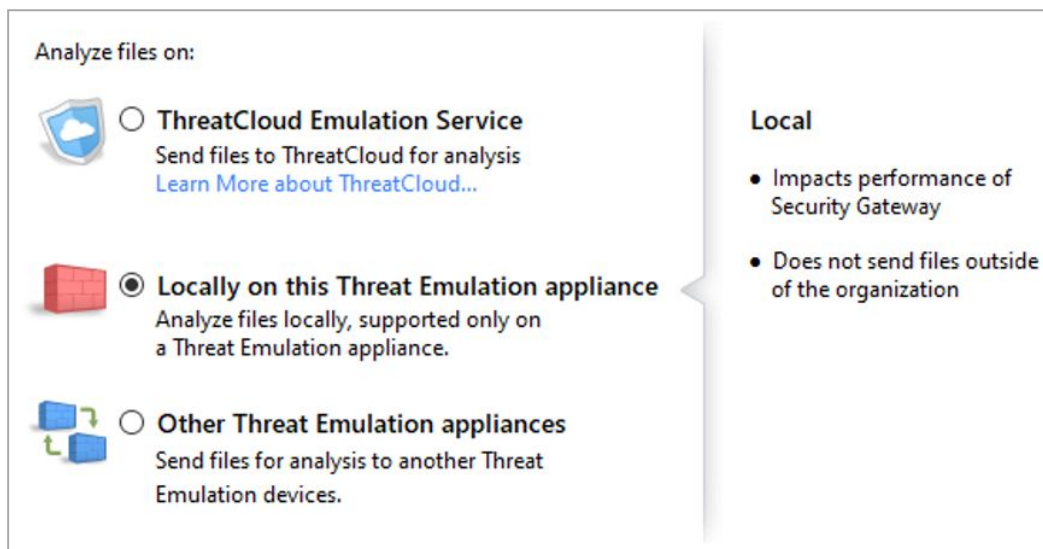
- a. In the **Gateway Object Properties**, navigate to the **Threat Prevention** tab.

- b. In the **Blades** section, do these:

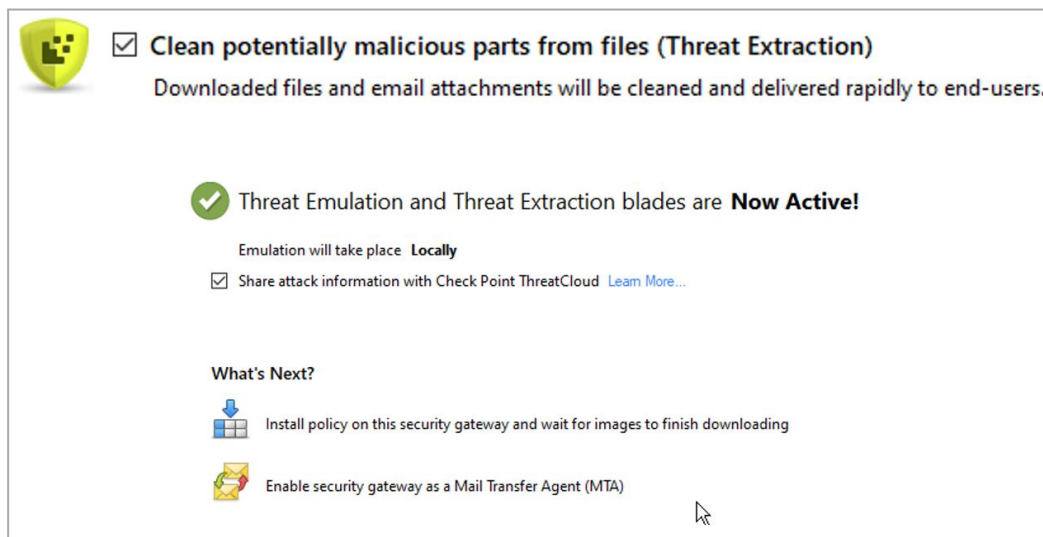
Navigate to the **Main Menu** in the SmartConsole and click **Install Policy** for the changes to appear.

To enable Threat Prevention Features:

- a. In the **Custom Threat Prevention** section, enable **Threat Emulation Blade**.
- b. Set the **Threat Emulation** location to **Locally on this Threat Emulation Appliance**



- c. Enable **Threat Extraction**.



- d. Save and close the settings.

3. Configure UserCheck Settings on the TE Appliance

- a. To enable HTTPS for the UserCheck Portal, go to **TE Appliance Object > UserCheck > Settings**

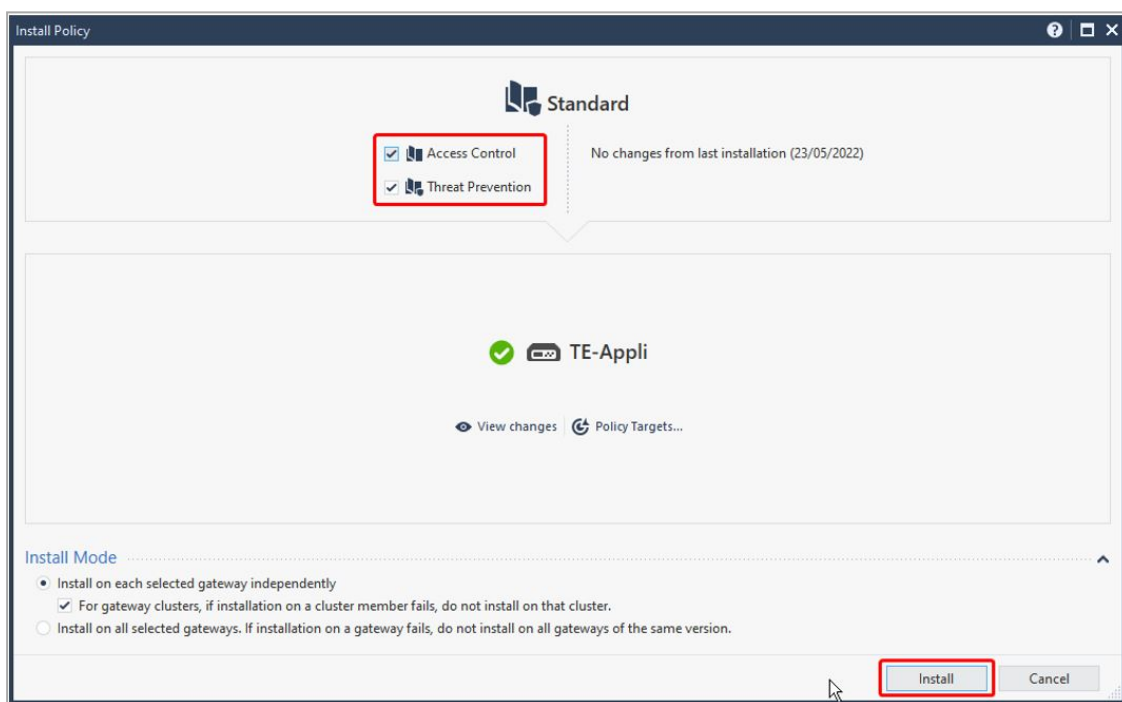
Ensure that the URL starts with either an IP address or an FQDN.

- b. By default, the system uses the built-in SSL certificates in SmartConsole. If you want to use your own SSL certificates, navigating to the **Certificates** section, click **Import** and upload the valid SSL certificate.
- c. Ensure that the UserCheck portal is enabled to be accessible to all interfaces by navigating to **UserCheck settings > Accessibility > Accessible from all interfaces**.



Note - This setting enables the Security Gateway to receive requests from the Security Management Server via internet. To ensure secure communication, check the configuration of the **Threat Prevention API**.

- d. Install both policies on the **TE Appliance** to apply the changes.



Step 3 - Enable Threat Prevention API

1. To modify API Settings using the GuiDBedit tool, close all the active SmartConsole sessions.
2. Launch the GuiDBedit tool and connect to the **Security Management Server**.
3. Press **CTRL+F** and search for the `enable_scrub_web_service` field.
4. Change the value of all the matching entries to **true**.

5. Save the configuration by navigating to **File> Save All** and close the GuiDBedit Tool.

 **Note** - For the API to properly function, set the `enable_scrub_web_service` entry to **true**.

6. In the SmartConsole, open **TE Appliance Object Properties**
7. Navigate to the **Threat Extraction** tab.
8. Enable **Web API**.
9. Connect to the SSH Client and switch to **Expert** mode to enable API access and logging.
10. Open the `/opt/CPUserCheckPortal/phpincs/conf/TPAPI.ini` file in a text editor. For example, **VI editor**.
11. Locate `logs_api_enabled` and change its value to **TRUE**.

 **Note** - When Threat Prevention is used, you can retrieve the original **File** by allowing logging for Zero Phishing.

12. Execute the following commands to configure and enable the web service.

- a. `[Expert@HostName:0]# killall scrubd`
- b. `[Expert@HostName:0]#
/opt/CPUserCheckPortal/scripts/configure_scrub_web_
service.sh enable`

 **Note** - If no API key has been set, the script will auto-generate a random key. This key can be viewed and modified in the `/opt/CPUserCheckPortal/phpincs/conf/TPAPI.ini` file.

- c. `[Expert@HostName:0]# mpclient restart UserCheck`

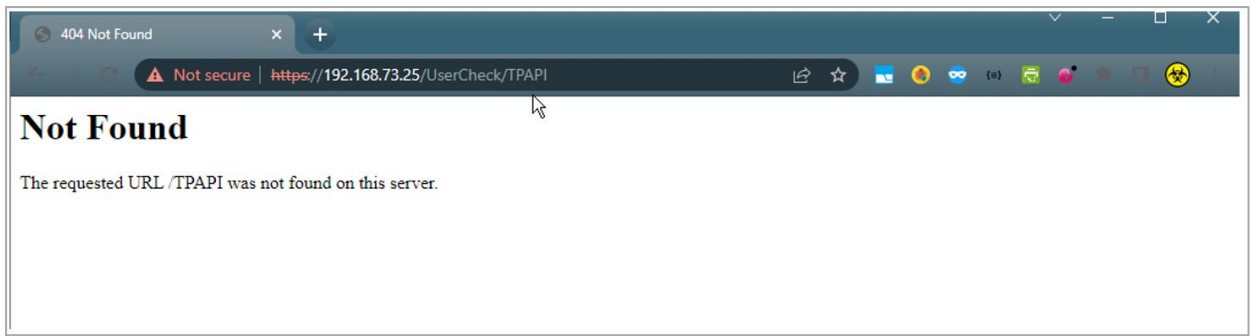
13. Run the following command on TE Appliance to enable Logging for Threat Emulation.

```
[Expert@HostName:0]# tecli advanced remote emulator logs enable
```

 **Note** - This requires a Threat Emulation Engine Update 6 or later. For more information about upgrade instructions and version details, see [sk95235](#).

14. To check the configuration of the TE Appliance and to respond to the Threat Emulation API, enter `https://<IP_Address_of_TE_Appliance>/UserCheck/TPAPICheck` in a browser.

A **404 Page Not Found** message indicates that the API endpoint is reachable and active.



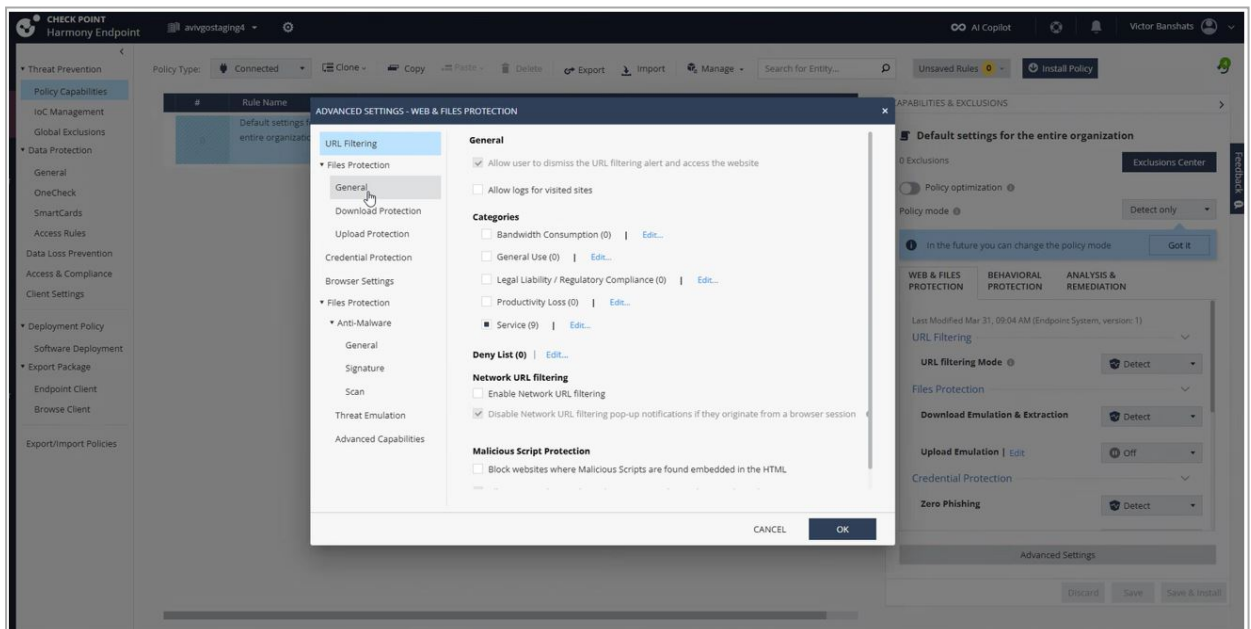
Note - If you receive an **Insecure Response** or face certificate error in your browser, it may be caused by one of the following:

- The certificate is issued to a different FQDN/IP than the one used in the URL.
- The certificate uses a SHA-1 hash algorithm, which most browsers do not comply with.
- The client system does not trust the certificate.

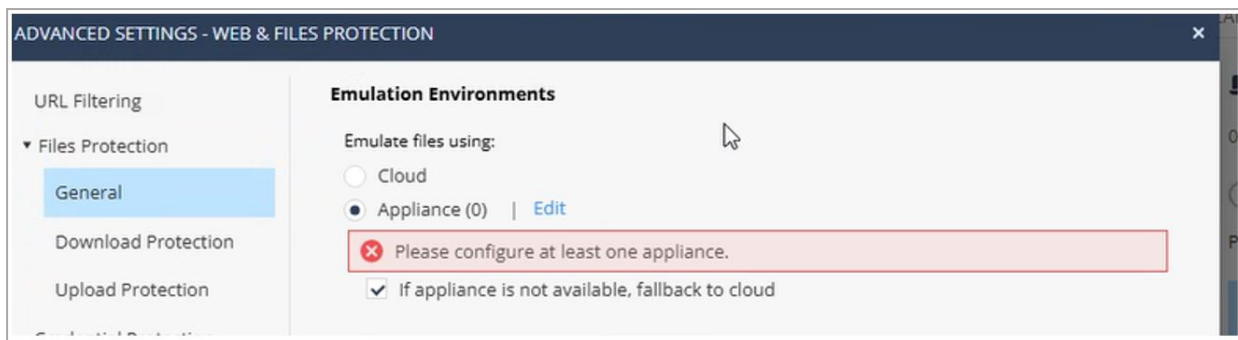
If you use the Firefox browser, note that the browser has a certificate store and importing the certificate from the Windows store is not recommended.

Step 4 - Threat Emulation Configuration in Check Point Portal

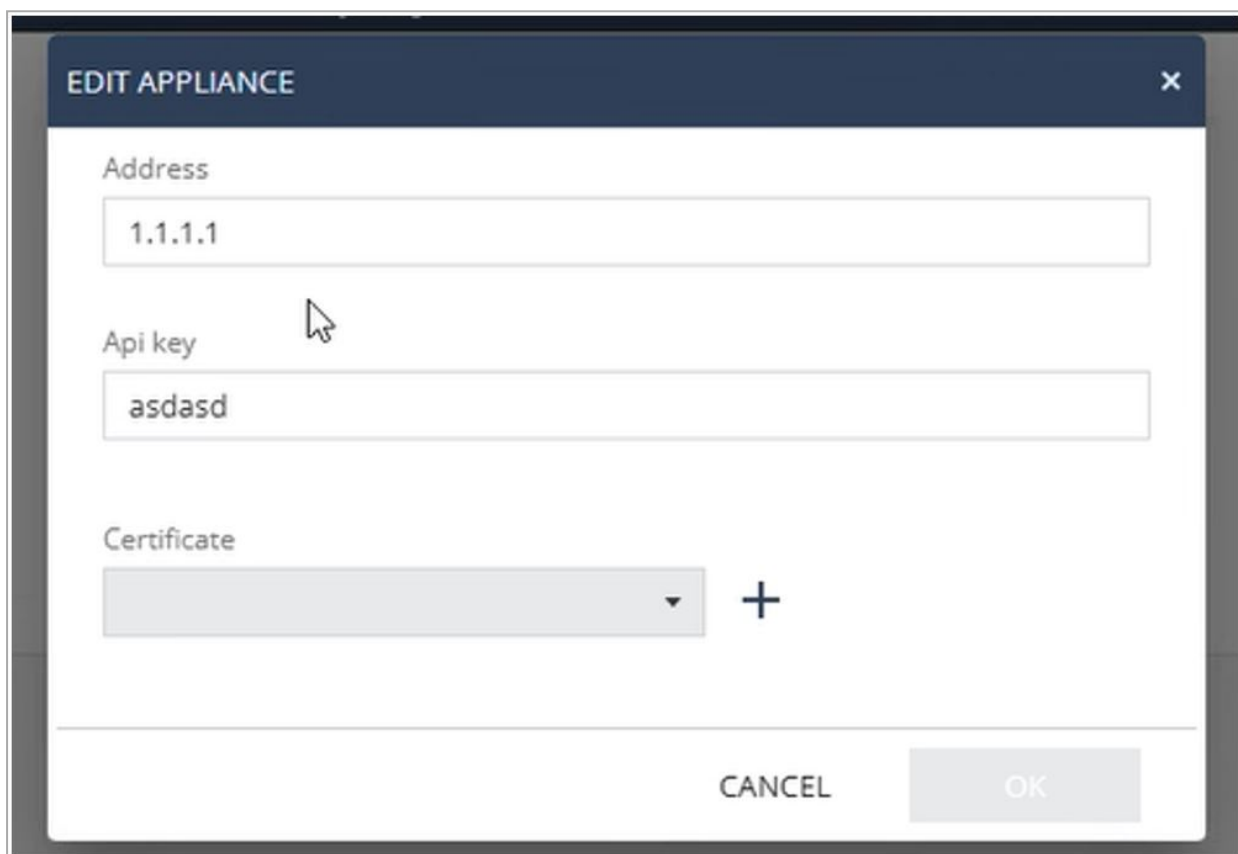
- Navigate to **Policy Capabilities > Threat Prevention > Web & Files Protection > Advanced Settings > Files Protection > General**.



- Change the **Cloud** option to **Appliance**.



3. Enable the **If Appliance is not available, fallback to cloud** checkbox.
4. Click **Edit**.



5. In the **Address** field, enter the FQDN or IP address of the Appliance.
6. Enter the **API key**.
 -  **Note** - For instructions on generating and handling API key, see [Check Point Portal Administration Guide](#).
7. You can use the default SSL certificate from the Check Point Portal or add your own SSL certificate.
 -  **Note** - If you use your own SSL certificate, ensure that you install and distribute the SSL certificate to all the endpoint clients (Windows and macOS).
8. Click **OK**.

9. Click **Save** and then **Install Policy**.

Known Limitations

1. Secure Internal Communication (SIC) must be successfully established between SmartConsole and the on-premises TE appliance. This is the same SIC trust mechanism used between Management Servers or between Management and Gateways. As SIC relies on specific TCP ports for trust communication, these ports must remain open and reachable between the Endpoint Cloud server and the TE appliance.
2. Certain backend configuration values require modification through Check Point internal tools (for example, GuiDBEdit). If such changes are required, contact [Check Point Support](#) for assistance.
3. Using a TE appliance with an Endpoint Cloud server in a fully air-gapped environment is not supported.

Managed Security Service Providers (MSSP)

Viewing Statistics for MSSP

Endpoint Security provides an interface for Managed Security Service Providers (MSSP) to:

- Create and manage (pause, stop, start and restart) the service of their child accounts
- View general statistics about their child accounts
- View operational statistics about their child accounts
- View contract details of their child accounts

 **Important** - MSSP View is only available for customers who are part of the Early Availability program.

Service Management

On the **Service Management** page, you can view and manage the service of the MSSP and their child accounts.

To view the **Service Management** page, click **Overview > MSSP View > Service Management**.

To refresh the information, click **Refresh**.

Accounts Info



The **Accounts Info** widget shows:

- Total number of accounts (includes MSSP accounts and child accounts).
- Number of deployed accounts (accounts with valid license).

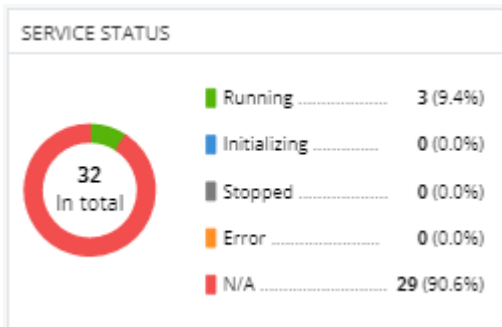
Click **Deployment** to view the deployed accounts in the ["Account Details Table" on the next page](#).

- Number of accounts under evaluation (accounts with evaluation license).

Click **Evaluation** to view the accounts under evaluation in the ["Account Details Table" on the next page](#).

- Number of active endpoints. It also shows the change in the number of active endpoints by percentage in the last 24 hours.

Service Status

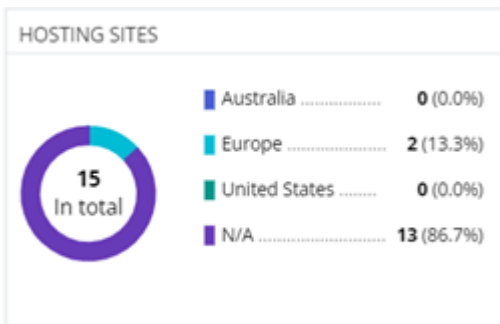


The **Service Status** widget shows the service status of the accounts:

- Running
- Initializing
- Stopped
- Error
- N/A

To sort the accounts by status, click Status. For more details, see ["Account Details Table" on the next page](#).

Hosting Sites



The **Hosting Sites** widget shows the number of accounts residing in different data regions.

Account Details Table

The **Account Details** table shows the details of the account.

Item	Description
 Create Service	Create a new service (a new Endpoint Security Management Server).
 Start	Starts the service for the account selected in the table.
 Restart	Restarts the service for the accounts selected in the table.
Actions	Perform these actions: ▪ Export to CSV - Exports the data to an excel file in CSV format. ▪ Manage account - Opens the General Settings page. For more information on managing an account, see the Check Point Portal Administration Guide.
Search	Enter the account name to search.
 Toggle Filters	Opens the Filters widget. Specify the filter criteria.
Account Name	Name of the account.
Service Status	Service status of the accounts: ▪ Running ▪ Initializing ▪ Stopped ▪ Error ▪ N/A
Purpose	Purpose of the child account: ▪ Product Evaluation ▪ Product Deployment ▪ N/A

Item	Description
Connection Token	Token used for the connection. The token is automatically generated when the service is created. You can use this token to connect to the tenant from the SmartConsole.
Hosting Site	Data region where the account is hosted.
Launch Time	Date and time the service was created.

MSSP Essentials

The **MSSP Essentials** page shows the essential details about the MSSP and child accounts.

To view the **MSSP Essentials** page, click **Overview > MSSP View > MSSP Essentials**.

To view the details specific to a child account, on the right pane, click , select the account and click **OK**.

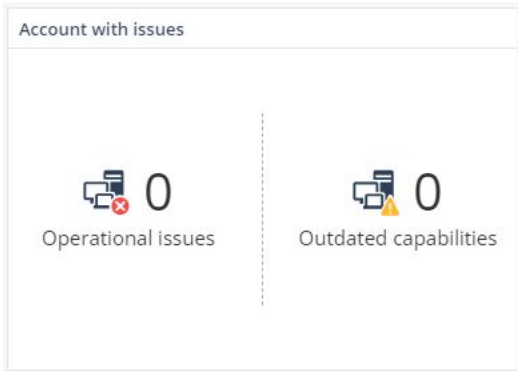
MSSP Total Endpoints



The **MSSP total endpoints** widget shows the total number of accounts, including MSSP accounts, child accounts and active / inactive endpoints.

Click **View Accounts** to view the MSSP and child account information. For more information, see ["Accounts Info" on page 746](#).

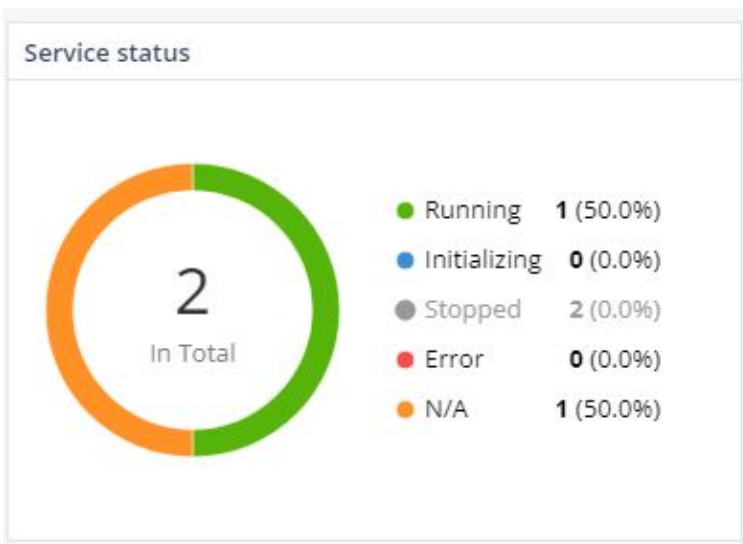
Account with Issues



The **Account with issues** widget shows the total number of **Operational issues** and **Outdated capabilities** across accounts that have at least one device.

Hover over the widget, click **View Accounts** to view the details of the account, and their issues. For more information, see ["Issues by Accounts" on page 746](#).

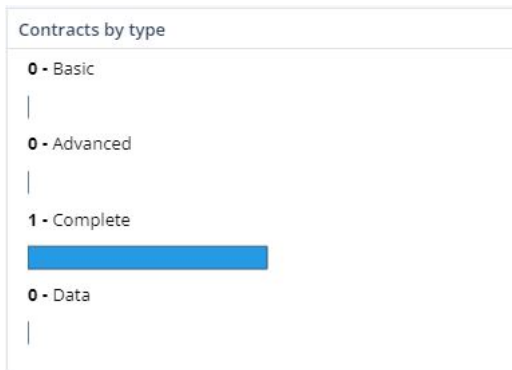
Service Status



The **Service Status** widget shows the number of accounts categorized by their Endpoint Security client service status.

To view the account by status, click the status. For more information, see ["Service Status" on page 747](#).

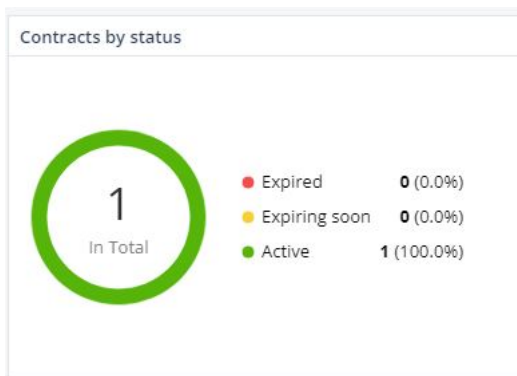
Contracts by Type



The **Contracts by type** widget shows the number of contracts categorized by their type.

Click the widget to view the number of contracts for each account.

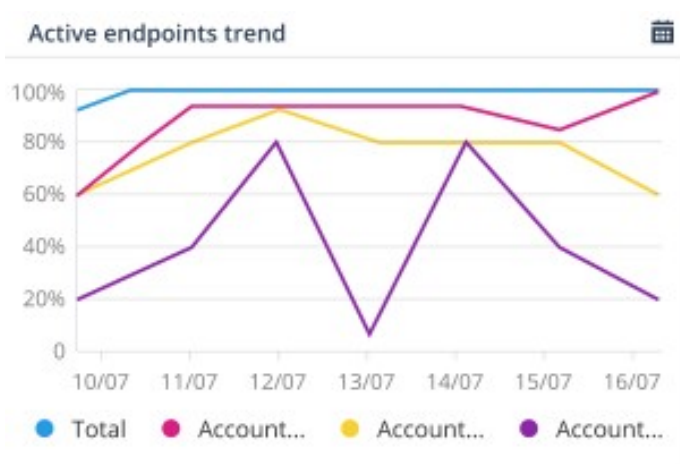
Contracts by Status



The **Contracts by status** widget shows the number of contracts categorized by their status.

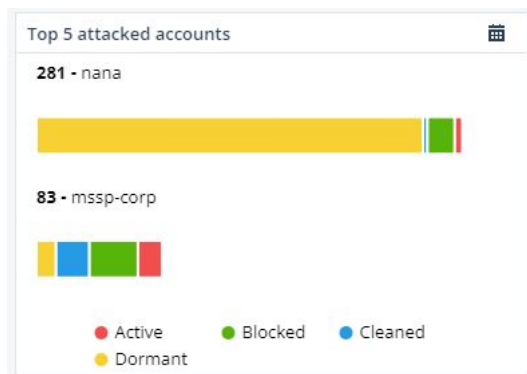
Click the widget to see the validity status of the contracts.

Active Endpoints Trend



The **Active endpoints trend** widget shows the line graph of active Endpoint Security clients for each account (up to five) over time.

Top 5 Attacked Accounts

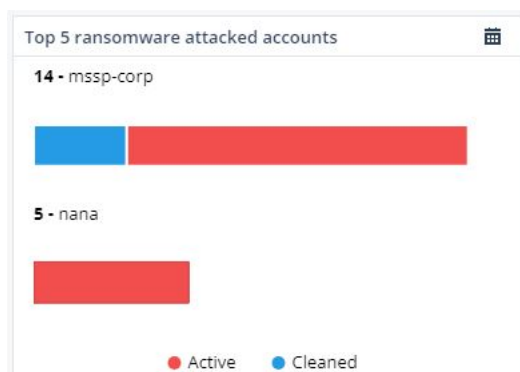


The **Top 5 attacked accounts** widget shows the top five attacked accounts categorized by their status.

The statuses are:

- **Active** - A malicious process attacked and infected the device. Termination and quarantine of the process or other elements of the attack is failed or disabled in the [policy](#).
- **Blocked** - A malicious process does not attack the device as all the infected files are blocked immediately and quarantined.
- **Cleaned** - A malicious process attacked and infected the device. The device is cleaned as the infected files are terminated and quarantined.
- **Dormant** - A malicious process does not attack, but the device is infected as the quarantine of one of the infected file fails.

Top 5 Ransomware Attacked Accounts



The **Top 5 ransomware attacked accounts** widget shows the top five accounts targeted by ransomware attacks.

The statuses are:

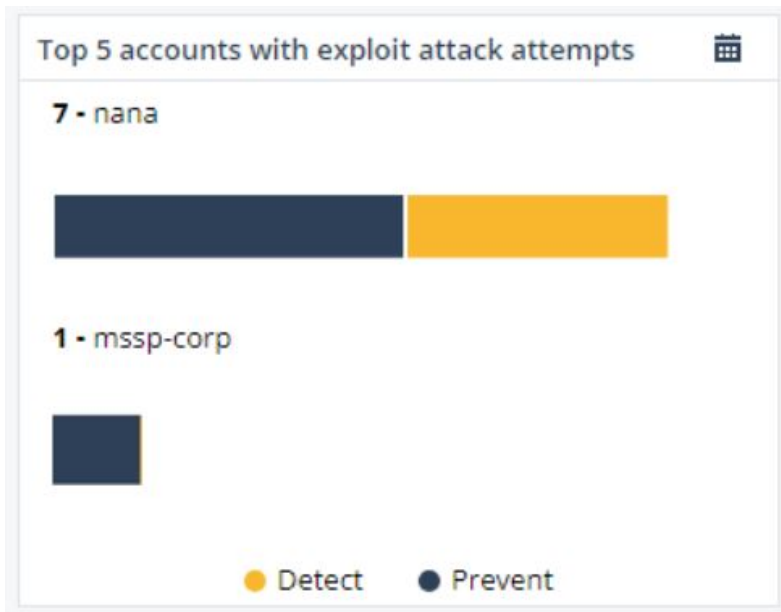
- **Active** - A malicious process attacked and infected the device. Termination and quarantine of the process or other elements of the attack is failed or disabled in the [policy](#).
- **Cleaned** - A malicious process attacked and infected the device. The device is cleaned as the infected files are terminated and quarantined.

Top 5 Phishing Attacked Accounts



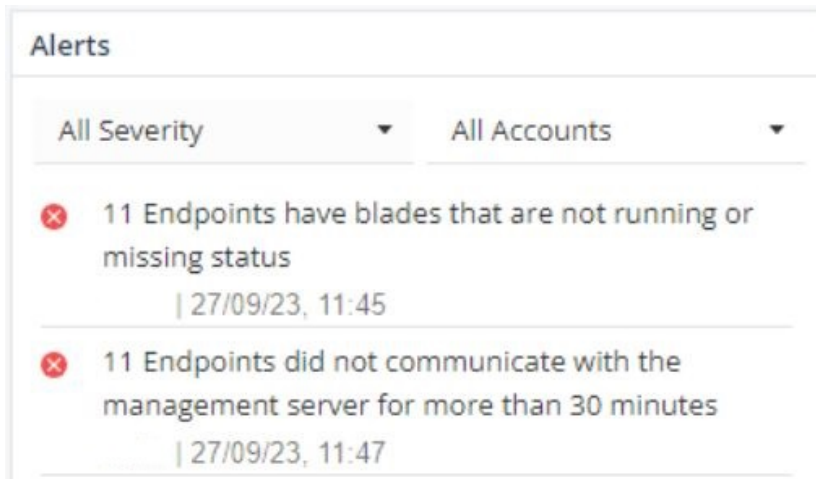
The **Top 5 phishing attacked accounts** widget shows the top five accounts targeted by phishing attacks.

Top 5 Accounts with Exploit Attack Attempts



The **Top 5 accounts with exploit attack attempts** widget shows the top five accounts that have been subject to exploit attack attempts.

Alerts



The **Alerts** widget shows the active alerts on all the endpoints in the account.

MSSP Custom Dashboard

The **MSSP Custom Dashboard** allows you to create personalized dashboards for child accounts and MSSP accounts with widgets of your preference and specify whether the dashboard should be private or public. **Private** dashboards are available only for you to view, whereas **Public** dashboards are available for all the users with access to the **MSSP View** page. However, only the owner of the dashboard can edit it.

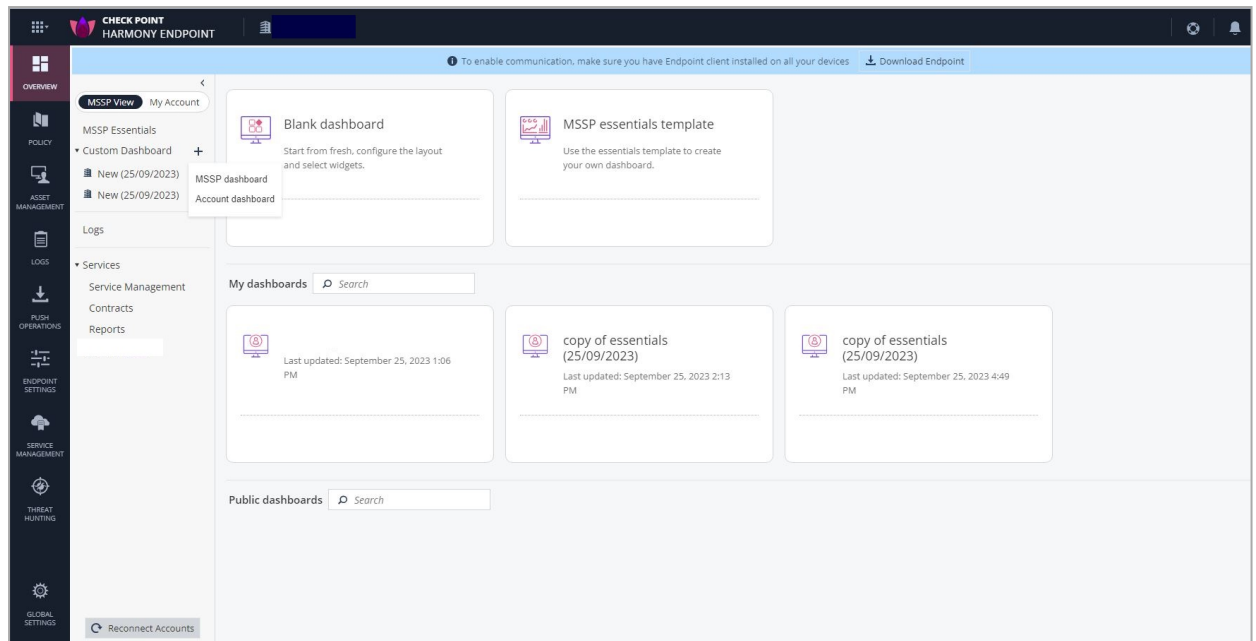
MSSP Dashboard

The MSSP dashboard allows you to create personalized dashboards for the MSSP and child accounts.

- The **Blank dashboard** allows you to create a new dashboard with the available widgets.
- The **MSSP Essentials template** dashboard allows you to customize the ["MSSP Essentials" on page 732](#) dashboard.

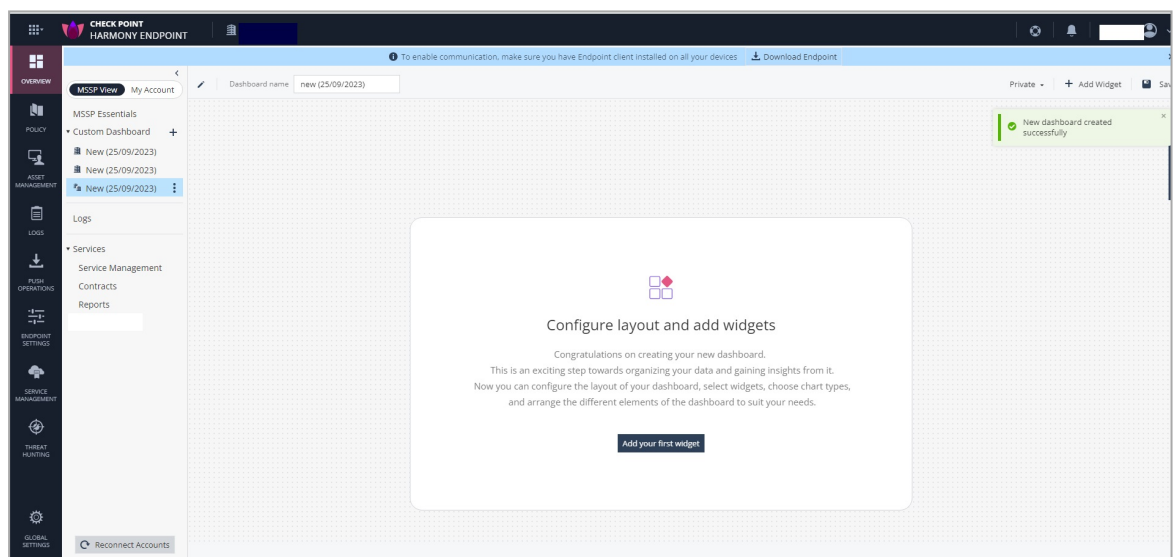
To create a MSSP dashboard:

1. Go to **Overview > MSSP View**, click **+** next to **Custom Dashboard** and click **MSSP dashboard**.



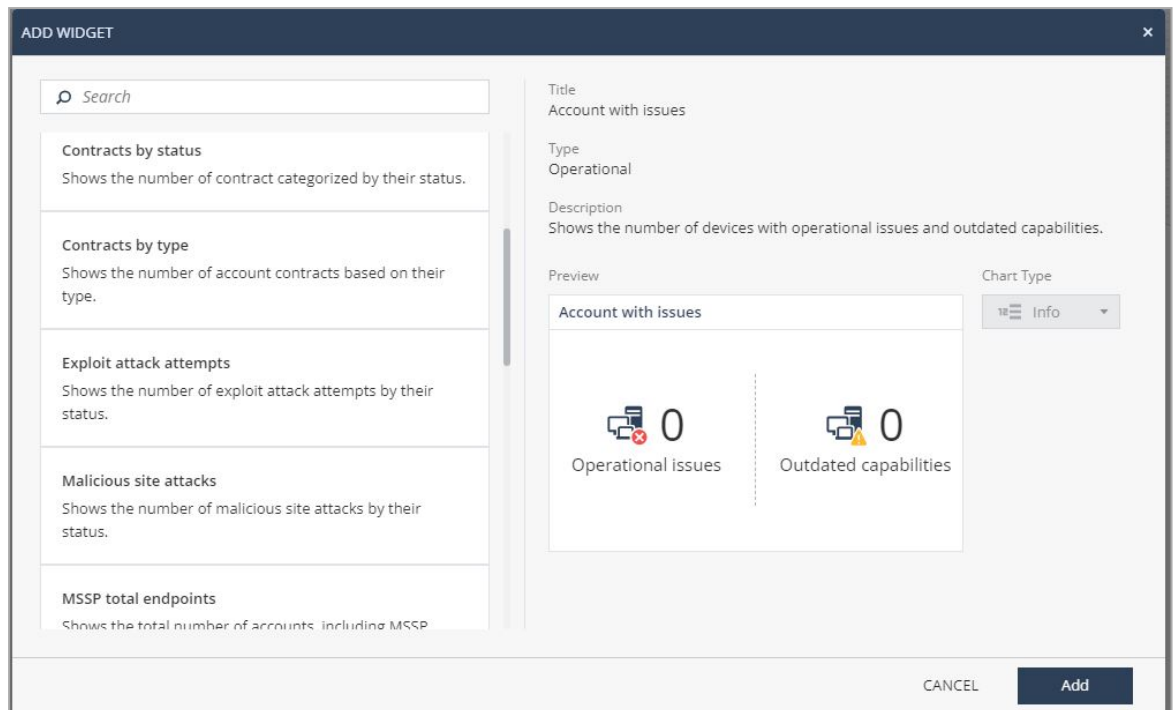
2. To create a new custom dashboard from scratch:

- a. Hover over the **Blank dashboard** widget and click **Add**.
- b. Click **Add Your First Widget**.



The **Add Widget** window appears.

- c. From the left pane, select the widget and click **Add**.



Note - The **Add** button is disabled if the widget is already added to the dashboard.

- d. To add more widgets, click **Add Widget** and repeat step c.
3. To create a new custom **MSSP essentials template** dashboard:
- a. Hover over the **MSSP essentials template** widget and click **Duplicate**.

The dashboard appears under **Custom Dashboard** on the left navigation pane, and it is also listed under **My dashboards** in the **MSSP Dashboard** page.

4. In the **Dashboard name** field, enter a name.
5. Click **Save**.
6. To delete a widget, on the widget, click  and click **Delete**.
7. By default, all custom dashboards you create in **MSSP Account** are set as **Private**. To make the custom dashboard available to all users with access to the **MSSP Account** page, from the **Private** list on the upper-right corner, click **Public**. The system adds the dashboard under **Public dashboards** for other users.

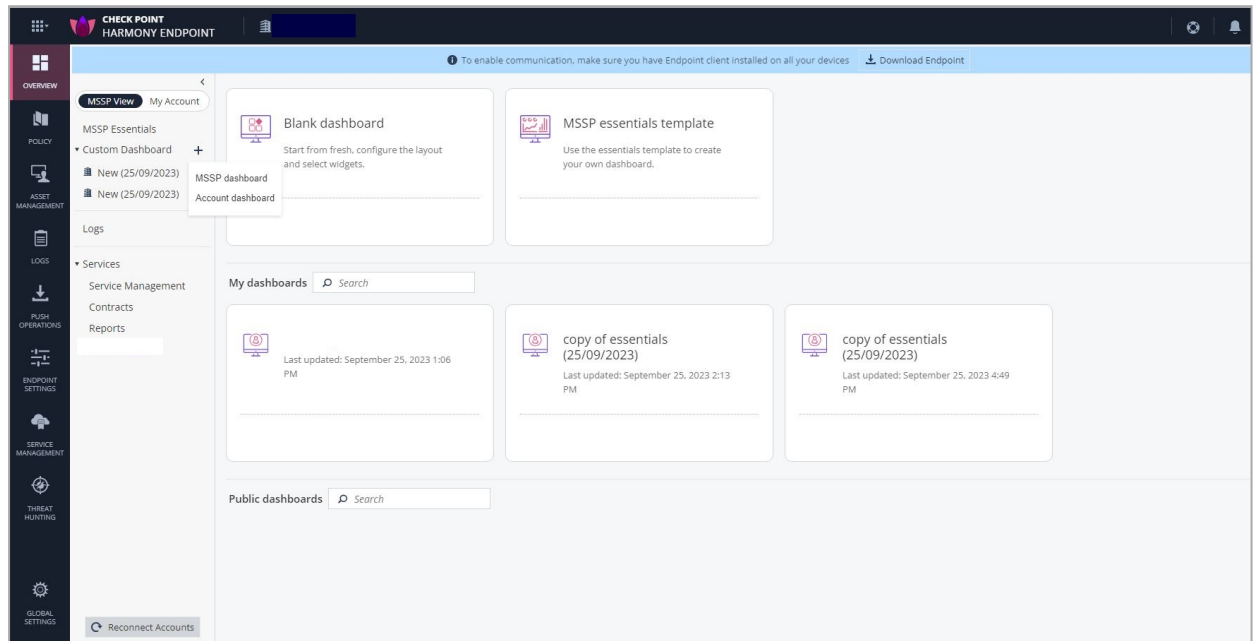
Account Dashboard

The Account dashboard allows you to create personalized dashboards for the MSSP account.

- **Blank dashboard** allows you to create a new dashboard with available widgets.
- **Unified template** allows you to customize the Unified Dashboard. For more information, see **Unified Dashboard** in *"Viewing Operational Overview, Security Overview and Reports" on page 149*.

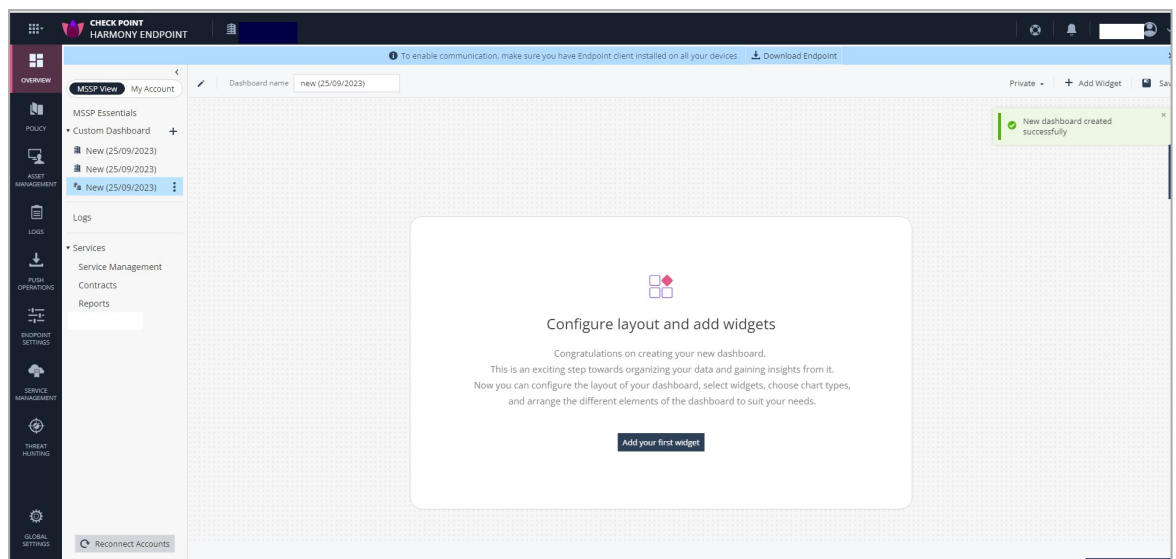
To create an account dashboard:

1. Go to **Overview > MSSP View**, click **+** next to **Custom Dashboard** and click **Account dashboard**.



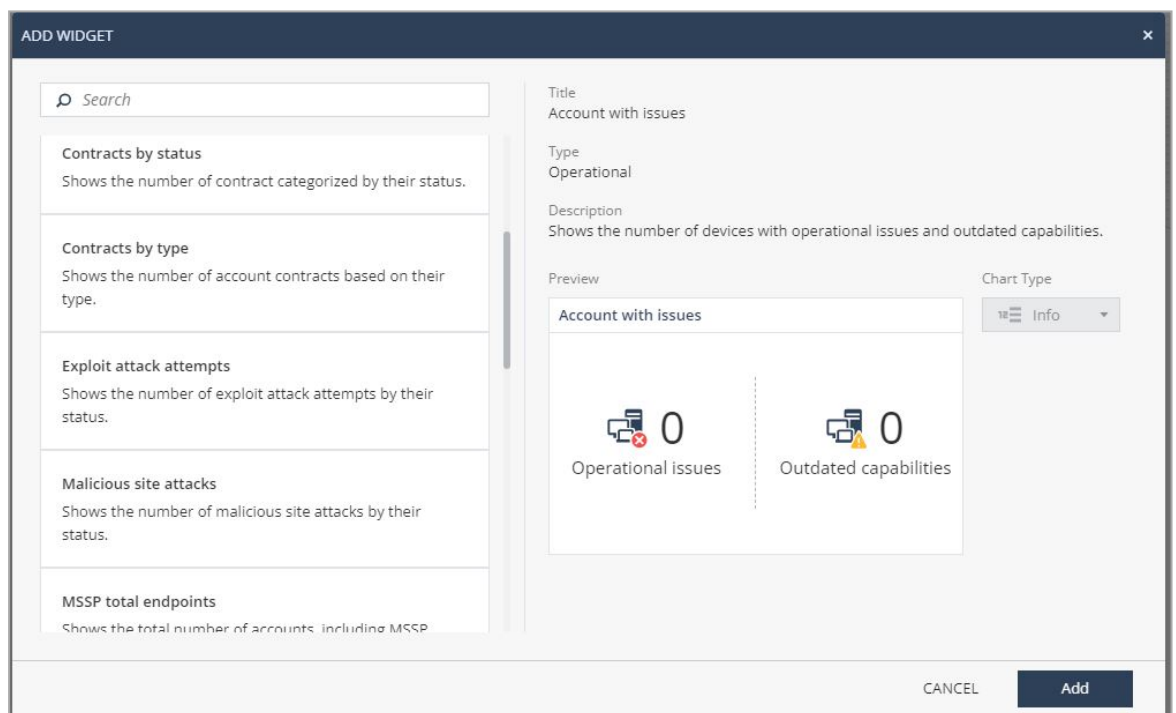
2. To create a new custom dashboard from scratch:

- a. Hover over the **Blank dashboard** widget and click **Add**.
- b. Click **Add Your First Widget**.



The **Add Widget** window appears.

- c. From the left pane, select the widget and click **Add**.



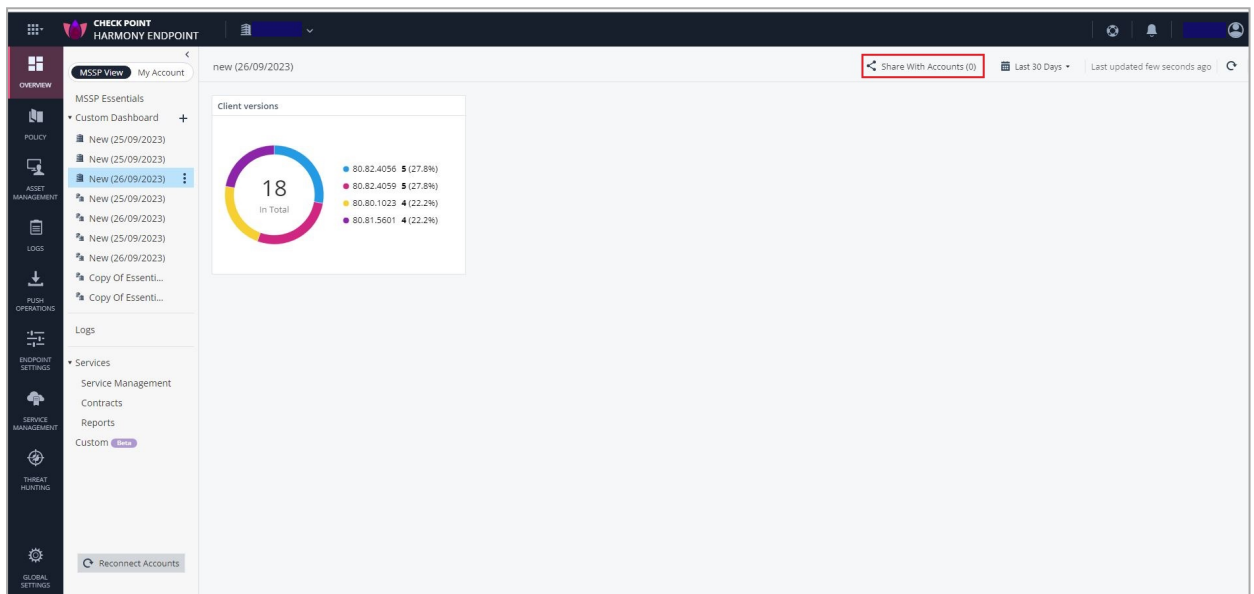
Note - The **Add** button is disabled if the widget is already added to the dashboard.

- d. To add more widgets, click **Add Widget** and repeat step c.
3. To create a custom **Unified template** dashboard:

- a. Hover over the **Unified template** widget and click **Duplicate**.

The dashboard appears under **Custom Dashboard** on the left navigation pane, and it is also listed under **My dashboards** in the **Account Dashboard** page.

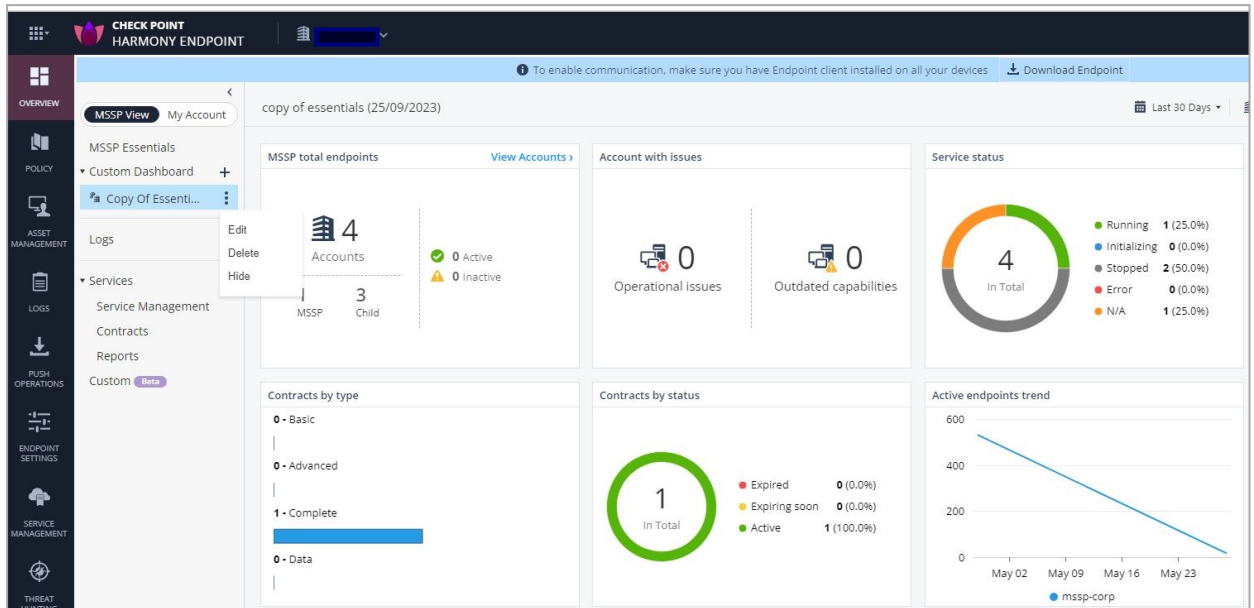
4. In the **Dashboard name** field, enter a name.
5. To delete a widget, on the widget, click  and click **Delete**.
6. Click **Save**.
7. To share the **Account dashboard** with other child accounts, on the right pane, click **Share With Accounts**, select the account and click **Share**



The dashboard appears in the **Public Dashboard** of the child account.

Managing a Custom Dashboard

1. Go to **Overview > MSSP View**.



2. To edit a dashboard:

- a. Expand **Custom Dashboard**.
- b. Click  for the dashboard you want to edit and click **Edit**.
- c. Make the necessary changes and click **Save**.

 **Note** - You cannot edit dashboards created by other users.

3. To delete a dashboard, expand **Custom Dashboard**, click  for the dashboard you want to delete and click **Delete**.

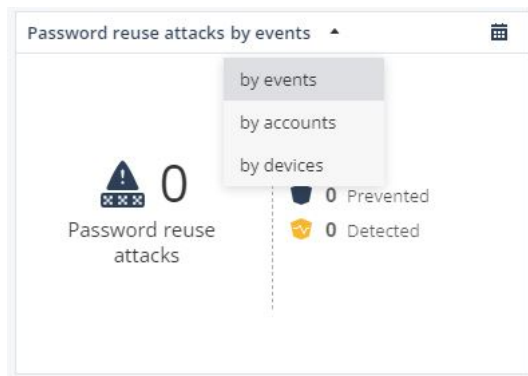
 **Note** - You cannot delete dashboards created by other users.

4. To hide a dashboard, expand **Custom Dashboard**, click  for the dashboard you want to hide and click **Hide**. The dashboard is removed from the list under **Custom Dashboard** on the left navigation pane.
5. To unhide a dashboard, click , hover over the dashboard you want to unhide and click **Add**. The dashboard is added to the list under **Custom Dashboard** on the left navigation pane.
6. To duplicate a dashboard, click , hover over the dashboard and click **Duplicate**.

Optional Widgets

You can customize the **Custom dashboard** by adding these widgets:

Password Reuse Attacks



The **Password reuse attacks by events** widget shows the number of password reuse attacks by their status.

Use the drop down to view the attacks by events, accounts or devices.

Phishing Attacks



The **Phishing attacks by events** widget shows the number of phishing attacks by their status.

Use the drop down to view the attacks by events, accounts or devices.

Ransomware Attacks



The **Ransomware attacks by events** widget shows the number of ransomware attacks by their status.

Use the drop down to view the attacks by events, accounts or devices.

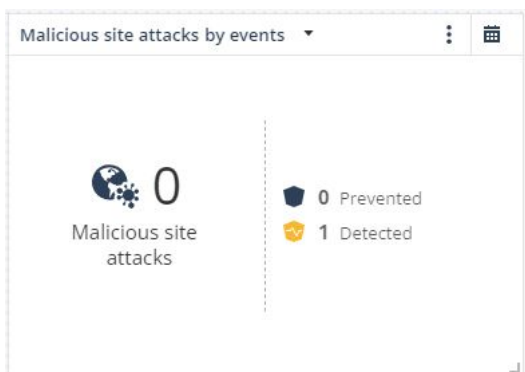
Exploit Attacks



The **Exploit attack attempts by events** shows the number of exploit attack attempts by their status.

Use the drop down to view the attacks by events, accounts or devices.

Malicious Site Attacks



The **Malicious site attacks by events** widget shows the number of malicious site attacks by their status.

Use the drop down to view the attacks by events, accounts or devices.

Service Management

You can use the **Service Management** page to view the overall status of your accounts.

To view the **Service Management** page, click **Overview > MSSP View > Services > Service Management**.

Accounts Info



The **Accounts Info** widget shows:

- Total number of accounts (includes MSSP accounts and child accounts).
- Number of deployed accounts (accounts with valid license).

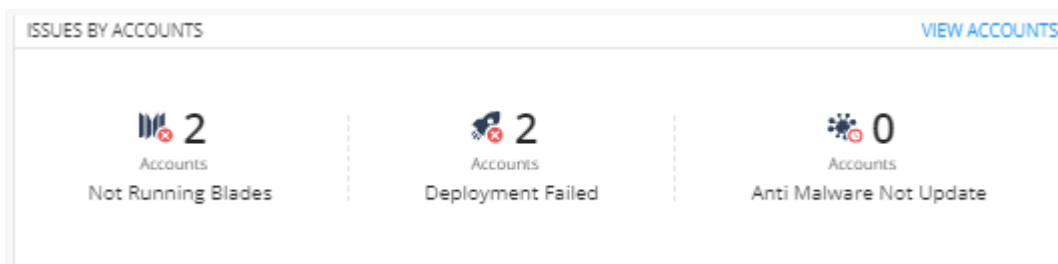
Click **Deployment** to view the deployed accounts in the ["Account Details Table" on page 731](#).

- Number of accounts under evaluation (accounts with evaluation license).

Click **Evaluation** to view the accounts under evaluation in the ["Account Details Table" on page 731](#).

- Number of active endpoints. It also shows the change in the number of active endpoints by percentage in the last 24 hours.

Issues by Accounts



The **Issues by Accounts** widget shows the:

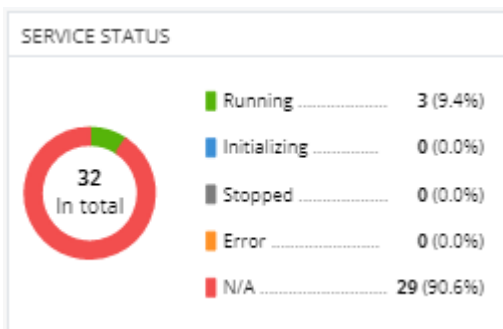
- Number of accounts with endpoints with blades that are not running or are inactive in the Endpoint Security client.
- Number of accounts with endpoints where Endpoint Security client deployment failed.
- Number of accounts with endpoints where the Anti-Malware signature is not updated in the last 72 hours.

To view more information, click **View Accounts**. A new page appears that shows the details of issues in a table.

Item	Description
Search	Enter the account name to search.
 Toggle Filters	Opens the Filters widget. Specify the filter criteria.
Account Name	Name of the account.
Protected Endpoints	Number of endpoints protected.
Failed	Number of failed Endpoint Security client deployments.
On Over 72h Ago	Number of accounts whose last Anti-Malware signature update was more than 72 hours ago.
Not Running Blades	Number of blades that are not running on the Endpoint Security client.

To export the issues to an Excel file, click **Export to CSV**.

Service Status

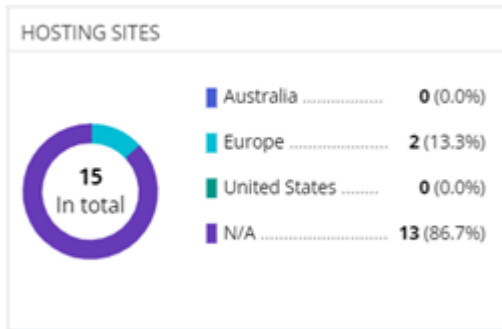


The **Service Status** widget shows the service status of the accounts:

- Running
- Initializing
- Stopped
- Error
- N/A

To sort the accounts by status, click Status. For more details, see ["Account Details Table" on page 731](#).

Hosting Sites



The **Hosting Sites** widget shows the number of accounts residing in different data regions.

Account Details Table

The **Account Details** table shows the details of the account.

Item	Description
 Create Service	Create a new service (a new Endpoint Security Management Server).
 Start	Starts the service for the account selected in the table.
 Restart	Restarts the service for the accounts selected in the table.
Actions	Perform these actions: ▪ Export to CSV - Exports the data to an excel file in CSV format. ▪ Manage account - Opens the General Settings page. For more information on managing an account, see the Check Point Portal Administration Guide.
Search	Enter the account name to search.
 Toggle Filters	Opens the Filters widget. Specify the filter criteria.
Account Name	Name of the account.

Item	Description
Service Status	Service status of the accounts: - Running - Initializing - Stopped - Error - N/A
Purpose	Purpose of the child account: - Product Evaluation - Product Deployment - N/A
Connection Token	Token used for the connection. The token is automatically generated when the service is created. You can use this token to connect to the tenant from the SmartConsole.
Hosting Site	Data region where the account is hosted.
Launch Time	Date and time the service was created.

Contracts

You can use the **Contracts** page to view the contract details of the MSSP and the child accounts.

To view the **Contracts** page, click **Overview > MSSP View > Contracts**.

To refresh the information, click **Refresh**.

Accounts Info



The **Accounts Info** widget shows:

- Total number of accounts (includes MSSP accounts and child accounts).
- Number of deployed accounts (accounts with valid license).

Click **Deployment** to view the deployed accounts in the ["Account Details Table" on page 731](#).

- Number of accounts under evaluation (accounts with evaluation license).

Click **Evaluation** to view the accounts under evaluation in the ["Account Details Table" on page 731](#).

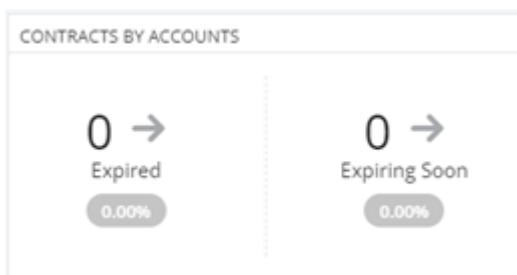
- Number of active endpoints. It also shows the change in the number of active endpoints by percentage in the last 24 hours.

Accounts Contracts Distribution



The **Accounts Contract Distribution** widget shows the number of contracts of each type.

Contracts by Accounts



The **Contracts by Accounts** widget shows the accounts that expired or expire soon.

Click the links to see the related accounts in the ["Contract Details Table" below](#).

Contract Details Table

The **Contract Details** table shows the contract details of all the accounts:

Item	Description
Action	Perform any of these actions: ▪ Export to CSV - Exports the data to an Excel file in CSV format. ▪ Send Email - Sends an email to the account owner about the contract expiration status. To customize the email, see "Sending an Email to Account on Contract Status" on the next page. ▪ Manage account - Opens the General Settings page. For more information on managing an account, see <i>Global Settings > Account Management</i> in the Check Point Portal Administration Guide.
Search	Enter the account name to search.
Renew	Renew an expired contract.
 Toggle Filters	Opens the Filters widget. Specify the filter criteria.
Account Name	Name of the account.
Total Endpoint	Number of endpoints in the account.
Max Endpoint	Maximum number of endpoints allocated to the account in the contract.
Active Contracts	Number of active contracts.
About to Expire Contracts	Number of contracts that are about to expire.
Expired Contracts	Number of contracts that expired.
Exceeded Accounts	Number of accounts that exceeded the maximum number of seats allocated in all the contracts for the account.

Contract Status Report

The **Contract Status Report** shows the type of contracts, number of seats (licenses) available per blade, the number of seats used, and their expiration dates. To see the contract status report of an account, click the account name in the ["Contract Details Table" on the previous page](#).

← Back | Contract Status Report

ACCOUNT DETAILS

 **XXXXXXXXXX** Total/Max Endpoints
0/100

Contracts

Type	Active	About To Expire	Expired
Basic	N/A	N/A	N/A
Advanced	N/A	N/A	N/A
Complete	1	N/A	N/A
Data	N/A	N/A	N/A

OVERVIEW

Agent		0 / 100
Firewall		0 / 100
Full Disk Encryption		0 / 100
Data Leak Prevention		0 / 100
Anti Malware		0 / 100
Anti Bot		0 / 100
Forensics		0 / 100
Threat Emulation		0 / 100

Contract Type: Complete | Status: ● Active | Expiration Time: 

Blade Name	Seats In Use/ Total Seats	Percentage Of Usage
Anti Bot	0/100	0 %
Anti Malware	0/100	0 %
Agent	0/100	0 %
Data Leak Prevention	0/100	0 %
Firewall	0/100	0 %

Sending an Email to Account on Contract Status

You can send an email alert to accounts on their contract status.

To send an email alert:

1. Select the account from the ["Contract Details Table" on page 750](#).
2. Click **Action > Send Email**.
3. Under **Type**, select the contract type.
 - All Contracts
 - Contracts Expiring Soon
 - Contracts Expire
 - Contracts Exceeded
 - Custom
4. Enter the **Recipients**, **Subject**, and **Body** of the email.
5. Click **Ok**.

The system sends the email to the recipients.

SEND EMAIL

Account Name

Type

first - child

All Contracts

Email Details

Recipients *

Search...

Subject *

Your Endpoint contract/s details

Body *

This is an automated message from the Endpoint Security Management Server.

Your account first - child has 1 contracts:

- Complete: Active Dec 27, 2024

CANCEL

OK

Reports for MSSP

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

- **Threat Analysis Report** - A comprehensive report with the latest security events.
- **Threat Analysis Report Anonymized** - A comprehensive report with the latest security events without specific user names.
- **High Risks Cyber Attack Report** - Shows the analysis of all the Endpoint Security events by statuses of the attack pillars.
- **Web Activity Checkup** - Shows the web activity in the organization.
- **Threat Emulation Report** - A comprehensive report about scanned and malicious files.
- **Threat Extraction** - Shows the insights on the downloaded files.
- **Software Deployment** - Shows the deployment status in the organization.

- **Vulnerability Management** - A comprehensive report of vulnerabilities detected by Endpoint Security.
-  **Note** - Available only to customer subscribed to this feature and with server version R81.10.x and higher.
- **Posture Management** - Shows Vulnerability Management and patches information.
- Note** - Available only to customer subscribed to this feature and with server version R81.10.x and higher.
- **Policies Reports** - A comprehensive report on Threat Prevention capabilities.
- **Operational Report** - Shows the insights about the operational status of the deployed endpoints.
- **Compliance Report** - Shows the compliance status in the organization.
- **Check Point Cyber Security Report 2023** - Shows the insights to help your organization stay secure.

To download a report:

1. Select the report and click **Export Report**.
The **Export Report** window appears.
2. In the **Time Frame** list, select **Last day**, **Last 7 days**, or **Last 30 days**.
3. From the **Tenant** list, select the required tenant for which you want to download the report.
4. Click **Export**.

Global Exclusions

With Global Exclusions in a Managed Security Service Provider (MSSP) account, you can create exclusions (using Legacy or Smart Exclusions) at one place and sync them with the child accounts.

To access Global Exclusions, go to **Overview > MSSP View > Global Exclusions**.

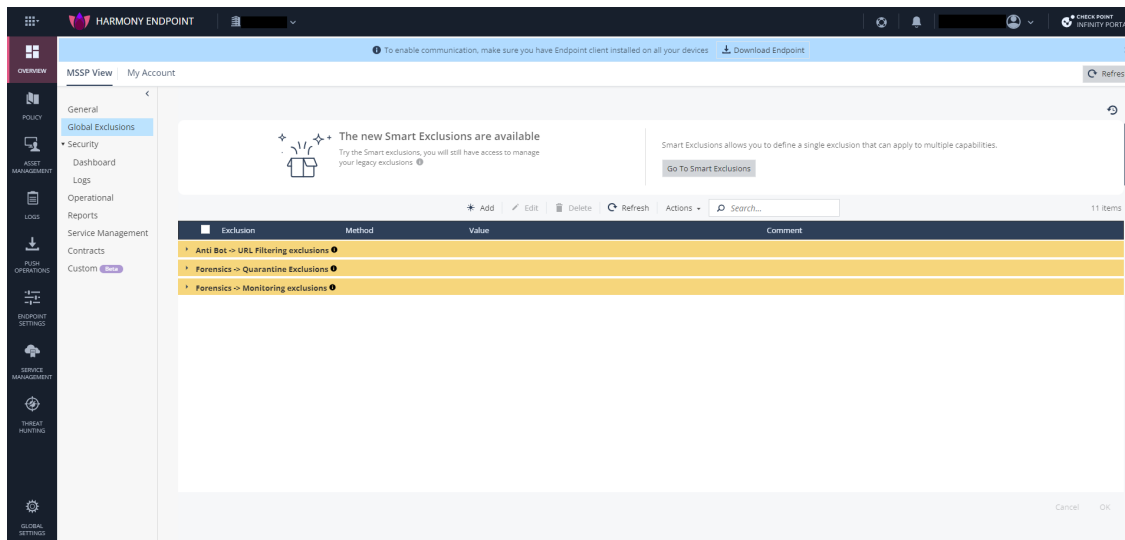
Adding Global Exclusions using Legacy Exclusion

For information on how to add exclusions using Legacy Exclusion, see [Adding Global Exclusions](#) "Adding Global Exclusions" on page 295

After you add exclusions, click **Save**. The exclusions are installed on the Endpoint Security Management Server and enforced on the endpoint through the Endpoint Security Client.



Caution - When you click **Save**, in addition to the exclusion changes, all the policy changes that have been saved for the corresponding capability in the child accounts are also installed on the Endpoint Security Management Server. For example, if you have added **Anti-Malware** exclusions, then all the saved changes related to the Anti-Malware policy in the child accounts are installed to the Endpoint Security Management Server.



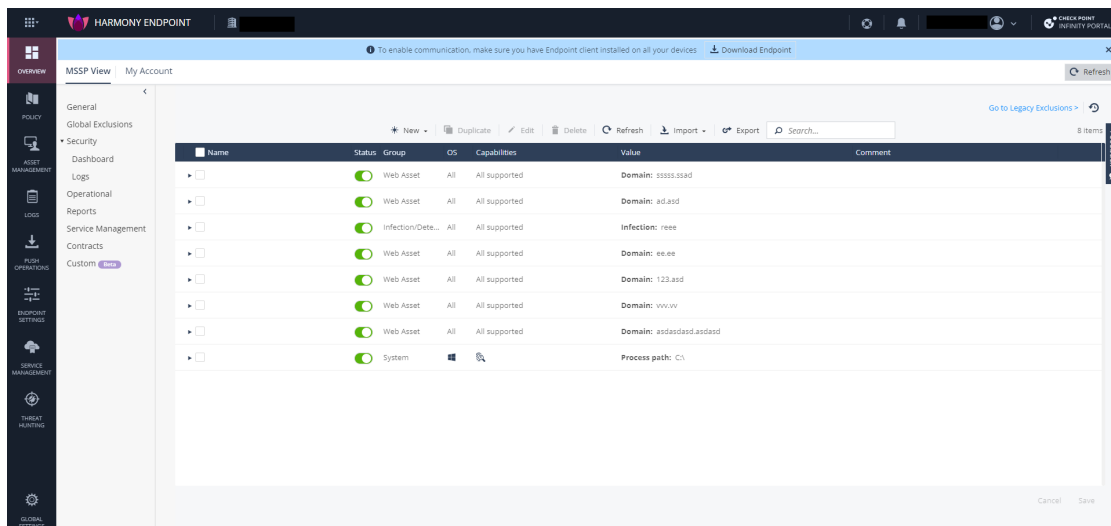
Adding Global Exclusions using Smart Exclusion

For information on how to add exclusions using Smart Exclusion, see ["Adding Global Exclusions" on page 322](#).

After you add exclusions, click **Save**. The exclusions are installed on the Endpoint Security Management Server and enforced on the endpoint through the Endpoint Security Client.



Caution - When you click **Save**, in addition to the exclusion changes, all the policy changes that have been saved for the corresponding capability in the child accounts are also installed on the Endpoint Security Management Server. For example, if you have added **Anti-Malware** exclusions, then all the saved changes related to the Anti-Malware policy in the child accounts are installed to the Endpoint Security Management Server.



Syncing Exclusions with Child Accounts

If the Endpoint Security service status in child accounts is **Running**, then the exclusions are automatically synchronized with the Global Exclusions configured in the MSSP server. If the service status is **Stopped** or **Paused**, then the system shows a banner notification when the service in the child accounts is **Running** again.



Click **Sync All** to sync the exclusions with the child accounts.

Templates for Child Accounts

Endpoint Security allows Managed Security Service Providers (MSSP) to create custom templates and attach them to child accounts. The template consists of predefined settings, for example, for Threat Prevention policy. The supported templates are:

- ["Threat Prevention Policy Template" on the next page](#)
- ["Software Deployment Policy Template" on page 762](#)

Use Case

You are an MSSP with several child accounts that require unique policy settings and frequent updates:

- You want to assign these unique policy settings to child accounts easily without having to manually define them for each child account.
- You want to manage policy updates from the parent account and propagate the updates to child accounts automatically.

Benefits

- Centralized policy management
- Consistent enforcement in policy settings
- Customized policy settings for unique requirements
- Ensures all child accounts are compliant.

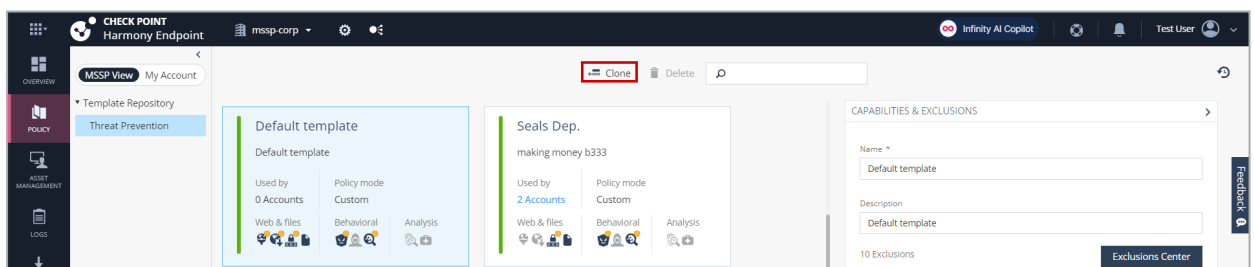
Threat Prevention Policy Template

The template consists of predefined settings for Threat Prevention policy capabilities, such as Web & Files Protection, Behavioral Protection and so on.

Creating a Threat Prevention Policy Template



1. [Access the Endpoint Security Administrator Portal](#) with the MSSP account.
2. Click **Policy > MSSP View > Template Repository > Threat Prevention**.
3. Select the **Default template** and click **Clone**.



4. Select the cloned template and in the **Capabilities and Exclusions** pane, do these:

CAPABILITIES & EXCLUSIONS

Name *
Test-Template

Description
Clone of the default template

10 Exclusions **Exclusions Center**

EndPoint for Server Optimization ⓘ OFF

WEB & FILES PROTECTION **BEHAVIORAL PROTECTION** **ANALYSIS & REMEDIATION**

Last Modified (, version: 2)

URL Filtering

URL Filtering Mode ⓘ Detect

Download Protection

Advanced Settings

Discard Save

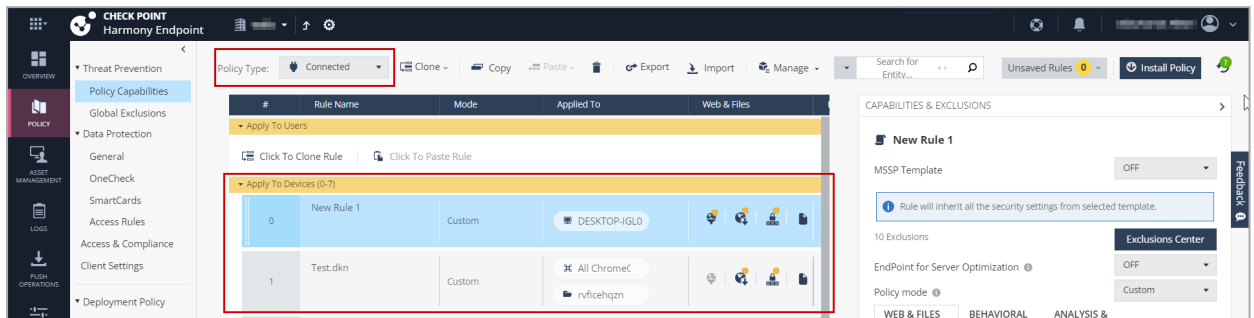
- In the **Name** field, edit the name. For example, *Default Settings for All Customers*.
- (Optional) In the **Description** field, enter a description.
- To add exclusions, click **Exclusions Center**. See ["Adding Exclusions to Rules" on page 294](#).
- Configure these capabilities, including **Advanced Settings**:
 - ["Web & Files Protection" on page 259](#)
 - ["Behavioral Protection" on page 286](#)
 - ["Analysis & Remediation" on page 293](#)

5. Click **Save**.

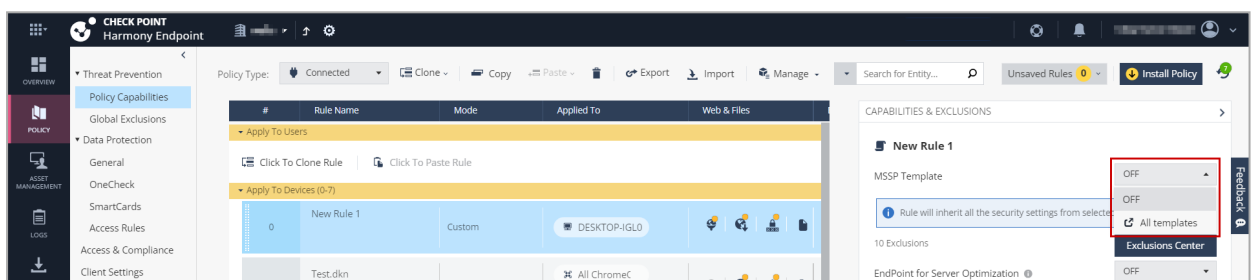
Attaching the Threat Prevention Policy Template to a Child Account

- [Access the Endpoint Security Administrator Portal](#) with child account.
- Go to **Policy > Threat Prevention > Policy Capabilities**.
- Select the policy in the table.

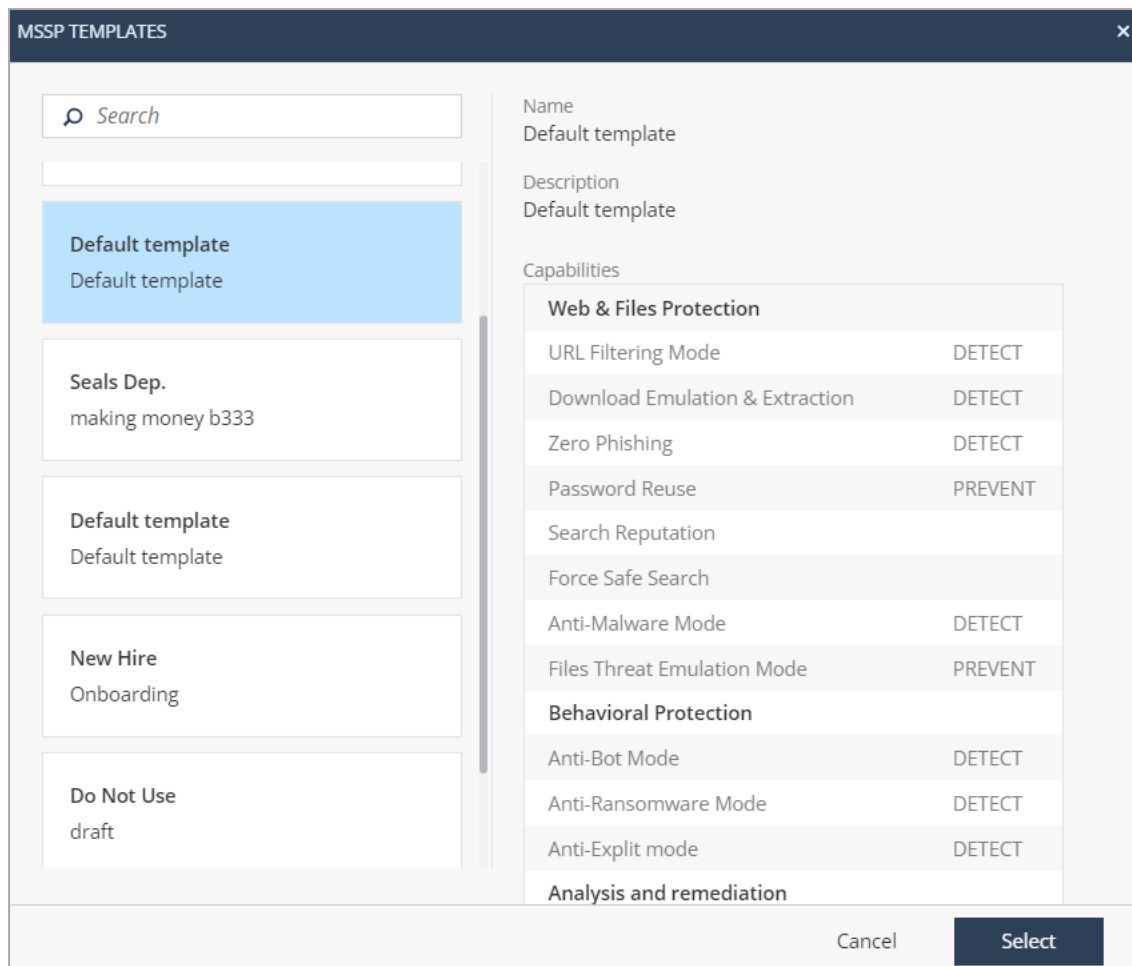
Note - Make sure the rule is for devices only and it is **Connected**. To view device specific rules, change the policy operation mode to **Mixed**. For more information, see *"Unified Policy" on page 248*.



4. In the **Capabilities and Exclusion** pane, from the **MSSP template** list, select **All templates**.



The **MSSP Templates** window appears.



5. Select the template from the left pane and click **Select**.

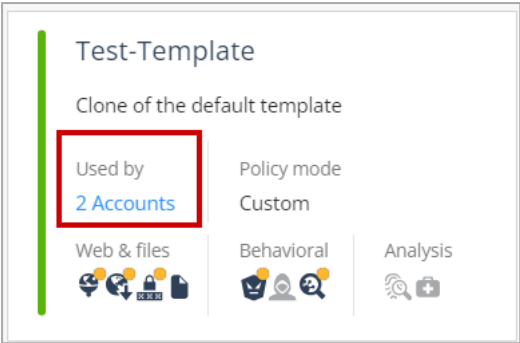
6. Click **Save & Install**.

After the policy is installed, the policy capability settings are disabled (Read-only) and the changes to the template from the MSSP account are automatically applied to the child account.

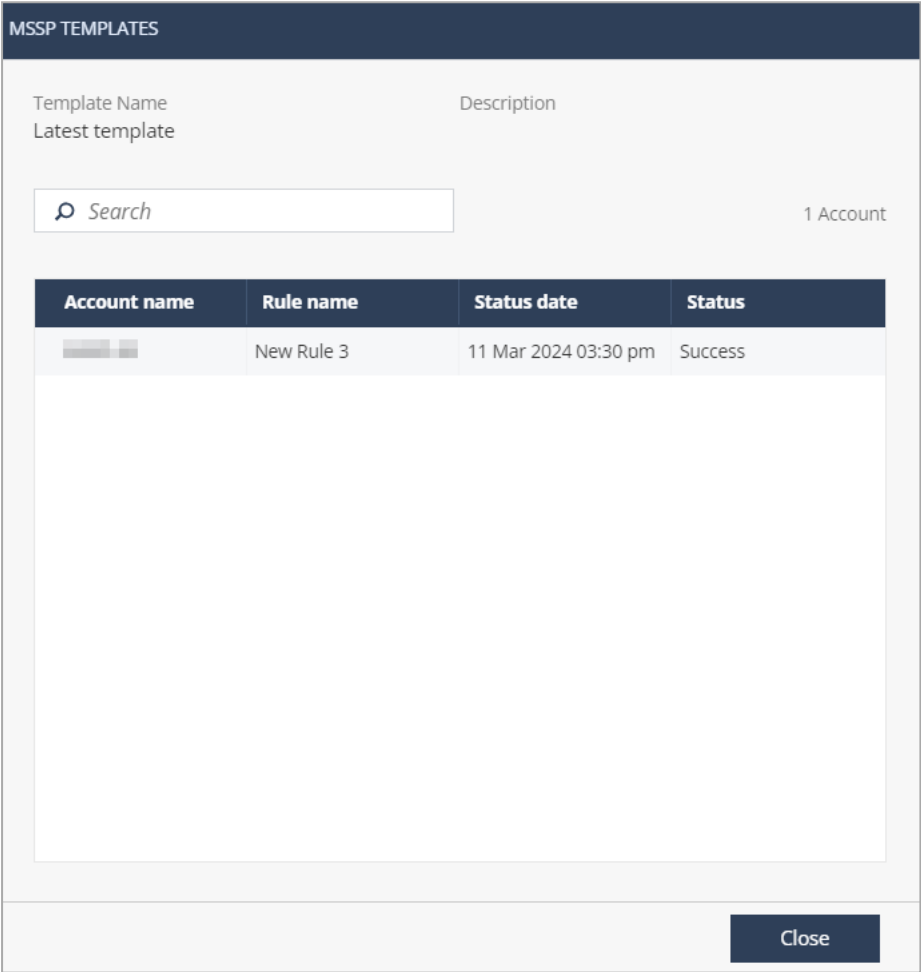
Viewing the Accounts Attached to a Template

1. [Access the Endpoint Security Administrator Portal](#) with the MSSP account.
2. Click **Policy > MSSP View > Template Repository > Threat Prevention**.

Used by shows the number of child accounts attached to the template.



3. To view the child accounts, click the number. The **MSSP Templates** pop-up appears and shows the details:



Column Name	Description
Account name	Child account name.
Rule name	Policy rule name that uses the template in the child account.

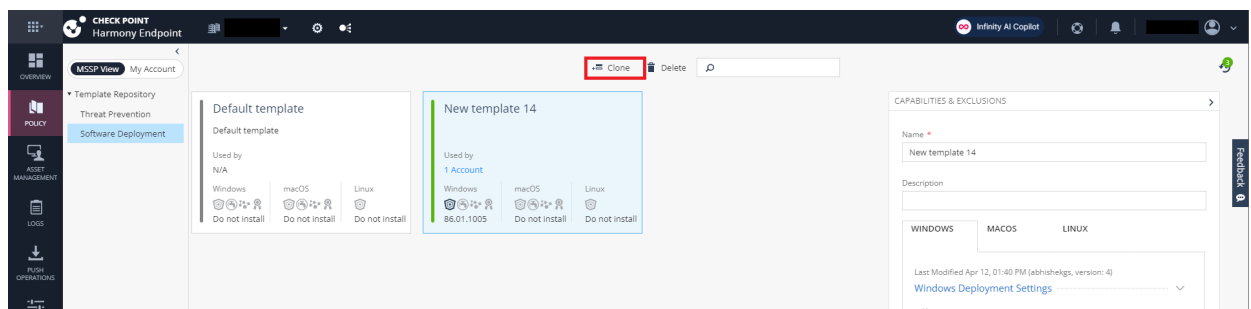
Column Name	Description
Status date	Last date and time in the server when the child account checked for the template updates.
Status	Status of the last update. ■ Success - The child account received the latest updates from the template. ■ Failed - The child account failed to receive the latest updates from the template.

Software Deployment Policy Template

The template consists of predefined settings for Software Deployment policy.

Creating a Software Deployment Policy Template

1. [Access the Endpoint Security Administrator Portal](#) with the MSSP account.
2. Click **Policy > MSSP View > Template Repository > Software Deployment**.
3. Select the **Default template** and click **Clone**.



4. Select the cloned template and in the **Capabilities and Exclusions** pane, do these:

The screenshot shows a configuration window titled 'CAPABILITIES & EXCLUSIONS'. It has three tabs: 'WINDOWS', 'MACOS', and 'LINUX'. The 'WINDOWS' tab is selected. Inside the tab, there is a 'Name' field with the text 'New template 14' and a red asterisk indicating it is required. Below it is a 'Description' field. Further down, there is a section for 'Last Modified' showing 'Apr 12, 01:40 PM (abhishekgs, version: 4)' and a link 'Windows Deployment Settings'. Below this is a 'Version' dropdown menu currently set to '86.01.1005'. Underneath is a 'Capabilities' section with a tree view. The root is 'All' (selected). It has four sub-items: 'Threat Prevention' (checked), 'Data Protection', 'Remote Access VPN', and 'Access'. At the bottom of the window are 'Discard' and 'Save' buttons.

- a. In the **Name** field, edit the name. For example, *Default Settings for All Customers*.
- b. (Optional) In the **Description** field, enter a description.
- c. Configure the deployment for **WINDOWS**, **MACOS**, and **LINUX**:
 - i. **Version** - From the list, select the necessary version that must be deployed on the endpoints.
 - ii. **Capabilities** - From the tree, select the necessary capabilities that must be deployed in the endpoints.



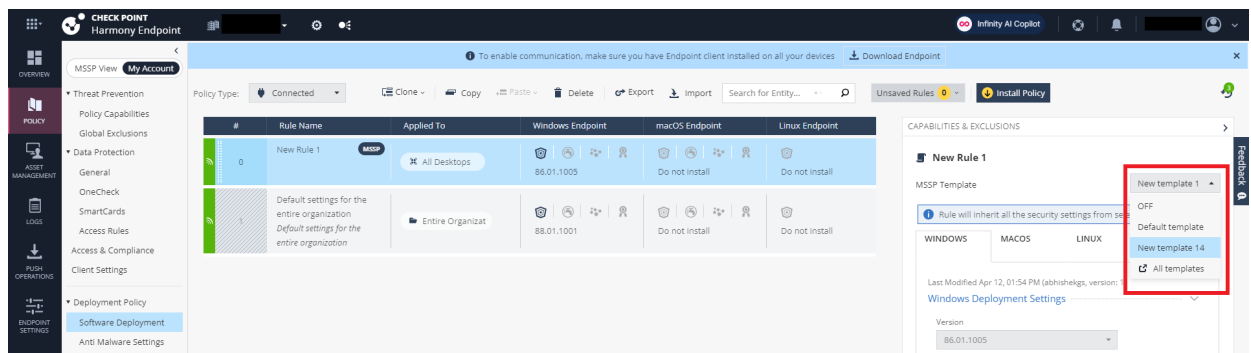
Note - Select **All** to deploy all the capabilities.

5. Click **Save**.

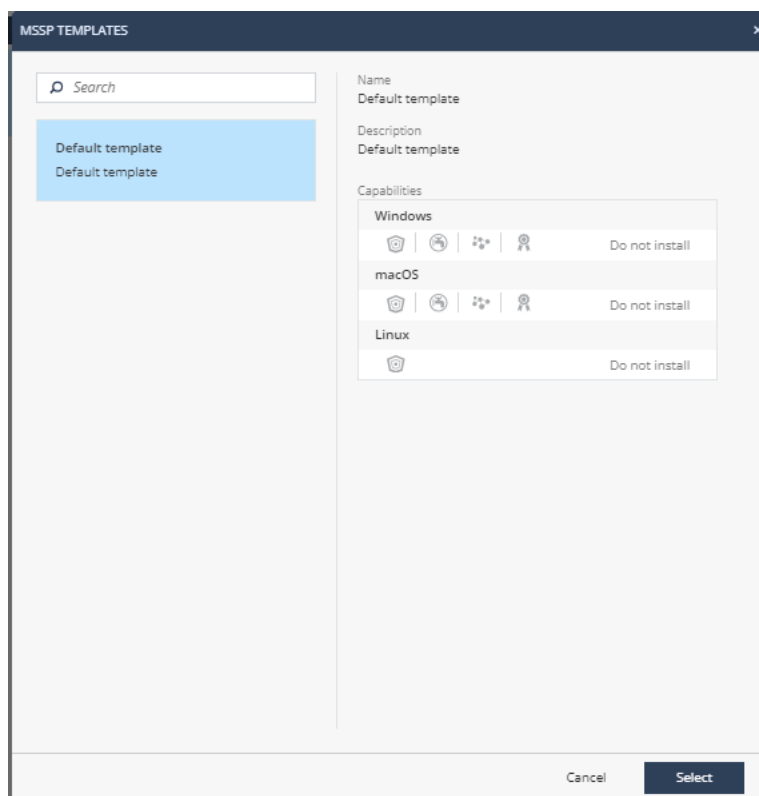
Attaching the Software Deployment Policy Template to a Child Account

1. [Access the Endpoint Security Administrator Portal](#) with the child account.
2. Go to **Policy > Deployment Policy > Software Deployment**.
3. Select the policy in the table.

4. In the **Capabilities and Exclusion** pane, from the **MSSP template** list, select **All templates**.



The **MSSP Templates** window appears.



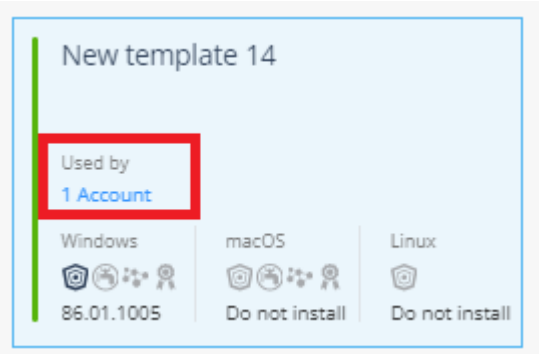
5. Select the template from the left pane and click **Select**.
6. Click **Save & Install**.

After the policy is installed, the policy capability settings are disabled (Read-only) and the changes to the template from the MSSP account are automatically applied to the child account.

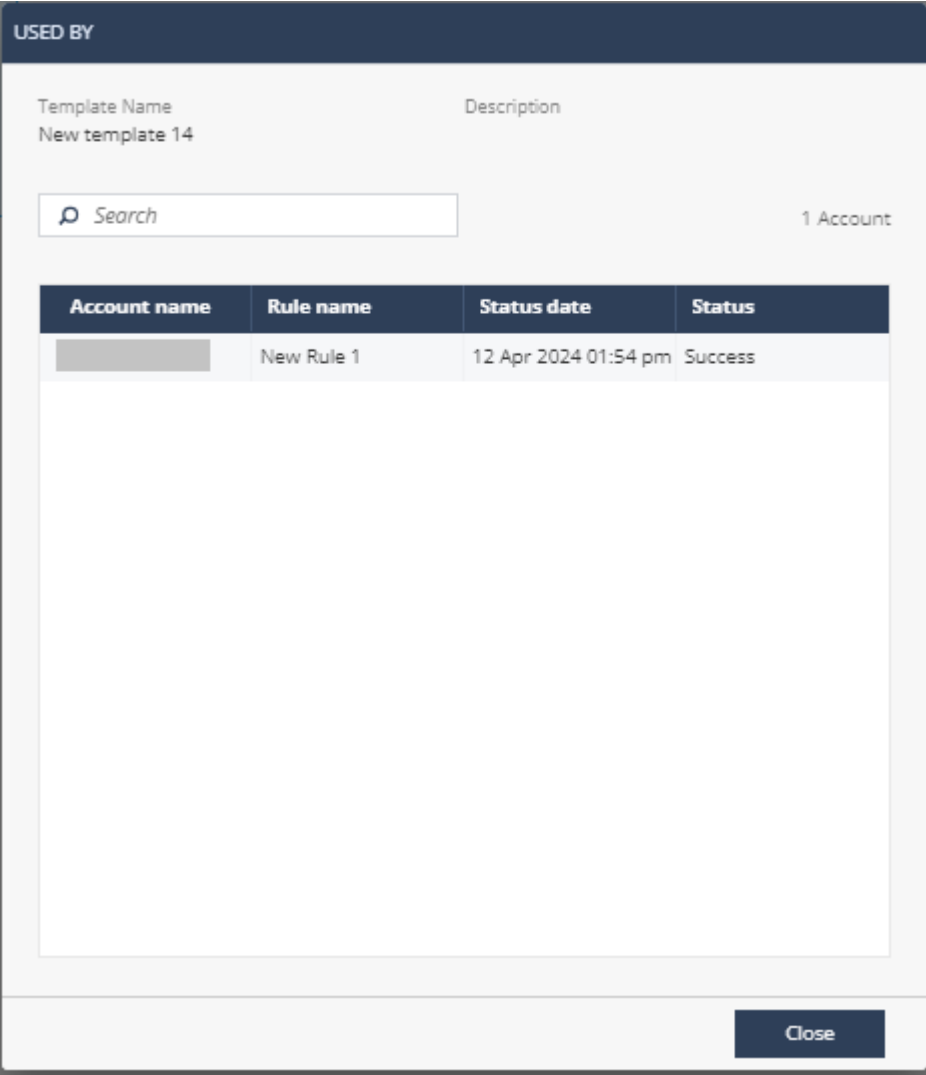
Viewing the Accounts Attached to a Template

1. [Access the Endpoint Security Administrator Portal](#) with the MSSP account.
2. Click **Policy > MSSP View > Template Repository > Software Deployment**.

Used by shows the number of child accounts attached to the template.



3. To view the child accounts, click the number. The **MSSP Templates** pop-up appears and shows the details:



Column Name	Description
Account name	Child account name.

Column Name	Description
Rule name	Policy rule name that uses the template in the child account.
Status date	Last date and time in the server when the child account checked for the template updates.
Status	Status of the last update. ■ Success - The child account received the latest updates from the template. ■ Failed - The child account failed to receive the latest updates from the template.

Smart App Control

Smart App Control is a Windows 11 native feature that blocks malicious, untrusted, or potentially unwanted apps from running on your device. For more information, see [Smart App Control](#).

The Smart App Control feature is compatible only with the Check Point Endpoint Security Client E87.50 and higher, with these limitations:

- Only these installations are supported:
 - [Tiny Agent](#)
 - [Vanilla Client](#)
 - [Export Package](#)
- Reconnect Tool - Perform steps 1 to 7 for Windows in the ["Reconnect Tool" on page 65](#) topic and then do one of these steps to use the Reconnect tool:
 - Sign the *reconnect_utility.exe* file with your certificate and then continue with step 8 for Windows in the ["Reconnect Tool" on page 65](#) topic.
 - Run the *reconnect_utility.exe* file.

It creates the **reconnect_tool** folder.

- a. Transfer the **reconnect_tool** folder to the endpoints.
- b. On the endpoint, open the **reconnect_tool** folder, and run the *ReRegister.exe* file.

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 Endpoint Security:

- Capsule Docs and Endpoint URL Filtering are not supported.
- When you create a new administrator, you cannot use the "**Change password on next login**" option.
- Distributed Active Directory Scanner: The deletion of a user from an Active Directory is not detected by the automatic scan and it is not reflected in the organizational tree.
- Unlock On LAN is not working. During Pre-boot, the client device cannot communicate correctly with the server.
- When you create a new AD scanner, you cannot scan user certificates from Active Directory.
- In order to use WSL2 on Windows 10 and 11 with Endpoint Security installed you must alter your firewall configuration. These changes apply only when you use the firewall blade. For additional information please see [sk177207](#).

Appendix

- ["Appendix A - Deploying Endpoint Security Client using SCCM" below](#)
- ["Appendix B - Uninstalling the Endpoint Security Client \(For macOS and Windows\)" on the next page](#)
- ["Appendix C - Deploying Endpoint Security Client Using Microsoft Intune" on page 772](#)
- ["Appendix D - Microsoft Intune Wipe and Windows Reset with Full Disk Encryption" on page 779](#)

Appendix A - Deploying Endpoint Security Client using SCCM

Use the Microsoft System Center Configuration Manager (SCCM) to install and deploy Endpoint Security Client.

Use Case

If you already use SCCM to manage your organization's endpoints, you can use it to deploy Check Point Endpoint Security on these managed endpoints.

Prerequisites

A System Center Configuration Manager (SCCM) account.

Step 1: Create the Endpoint Security Windows Application in SCCM

Follow these steps to create and upload Endpoint Security application to the SCCM service.

1. Open the Microsoft Endpoint Configuration Manager (SCCM).
2. From the top toolbar, select **Create Application**.
3. Click **Browse**.
 - a. Upload the `EPS.MSI` file created in ["Preparing the Endpoint Security Client Windows Package for Deployment" on page 772](#).
 - b. Click **Open**.
 - c. Click **Next**.

4. In the **General Information** window, enter the **Name**, **Additional Comments**, and **Publisher** information.
5. Click **Next**.
6. Review the **Summary** information and click **Next**.

Step 2: Deploy the Endpoint Security Windows Application in SCCM

Follow these steps to install and deploy the Endpoint Security application created in Step 1.

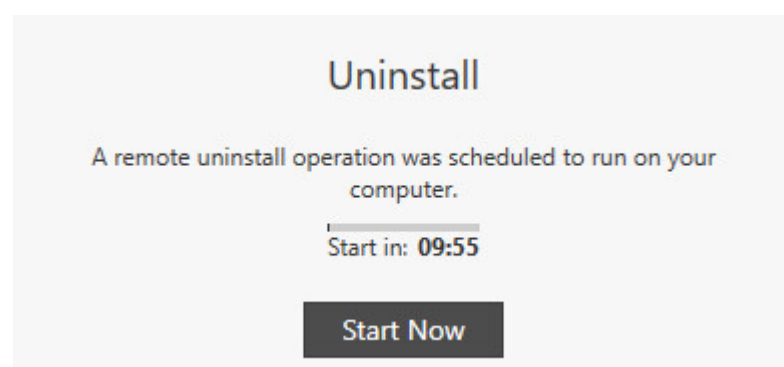
1. Open SCCM and from the top toolbar, click **Deploy**.
2. Go to the **General** page > select **Collection** > click **Browse**.
3. Click **Device Collections** and select the collection of devices > click **Next**.
4. Select **Content**, click **Add** > **Next**.
5. In **Deployment** settings, set the **Action** to **Install** and set **Purpose** to **Required**.
6. Go to **User Experience** and set your preferences > click **Next**.
7. Select **Alerts** and set your alerts > click **Next**.
8. Review the information and click **Next**.

The number of deployments is updated in the SCCM application.

9. To make sure the deployment is successful, open the **Software Center** on the target device.

Appendix B - Uninstalling the Endpoint Security Client (For macOS and Windows)

To uninstall the Endpoint Security Client, perform the **Uninstall Client** Push Operation. The system sends the uninstall request to the endpoint. The operation is executed automatically after the scheduled duration or the end-user can click **Start Now** to start the operation immediately.



 Notes -

- The system automatically reboots the endpoint after uninstalling the client successfully.
- The system deletes the client information on the Endpoint Security Management Server after the configured period of time (default is 30 days).

For more information on the Uninstall Client Push Operation, see ["Performing Push Operations \(Old User Interface\)" on page 580](#).

Appendix C - Deploying Endpoint Security Client Using Microsoft Intune

You can use Microsoft Intune or Microsoft Endpoint Manager to deploy Endpoint Security Client on Windows-based endpoints.

Use Case

If you already use Microsoft Intune or Microsoft Endpoint Manager to manage your organization's endpoints, you can also use the same Microsoft Intune or Microsoft Endpoint Manager to deploy Endpoint Security Client on these managed endpoints.

Prerequisites

- A Microsoft 365 account/subscription. for Microsoft Intune or Microsoft Endpoint Manager.
- You must be a Global Administrator or an Intune Service Administrator (Intune Administrator) to deploy the Endpoint Security Client. For more information on roles and permissions, see [Role-based access control \(RBAC\) with Microsoft Intune](#).
- You must have enrolled Windows endpoints to Microsoft Intune or Microsoft Endpoint Manager. For more information, see [Set up enrollment for Windows endpoints](#).
- Before you deploy Endpoint Security Client, make sure all your enrolled endpoints are contained in a single group. If you do not have such a group, create a new group and assign your endpoints and users to it.

Preparing the Endpoint Security Client Windows Package for Deployment

1. Log in to Check Point Portal and access the Endpoint Security Administrator Portal.
2. Go to **Overview** and click **Download Endpoint** on the top banner.

You can also click **Policy > Deployment Policy > Software Deployment** and click **Download Endpoint** on the top banner.

3. Select the required **Download version** and **Virtual group** for Windows.
4. Click **Download**.

The *EndpointSetup.exe* file downloads.

5. Create an MSI file from the downloaded *EndpointSetup.exe* file by running this command.

```
EndpointSetup.exe /CreateMSI
```

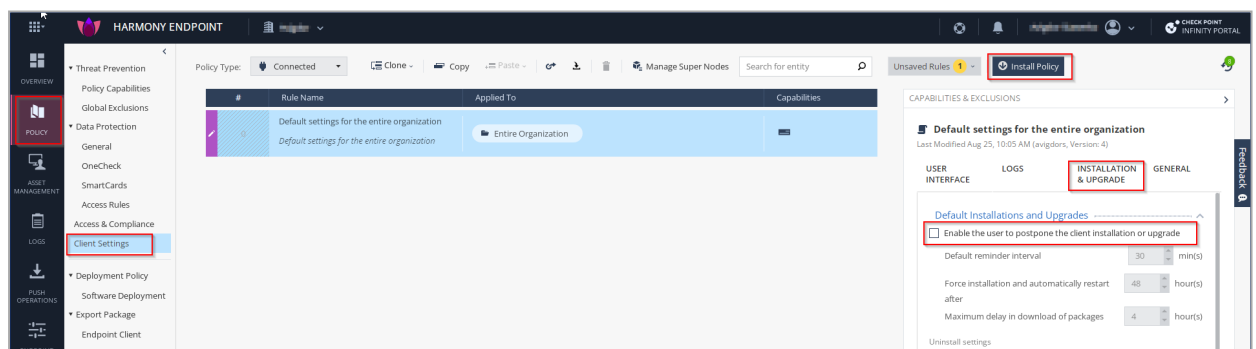
The **EPS.msi** file is created.

Endpoint Security Configuration

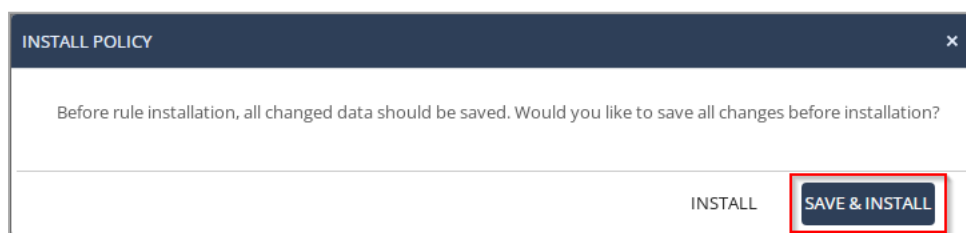
After you deploy the Endpoint Security Client, the installation does not start immediately. The user can postpone the installation for up to 48 hours.

To start the Endpoint Security Client installation immediately, before ["Creating the Endpoint Security Windows App in Microsoft Intune"](#) on the next page, do these:

1. Log in to Check Point Portal and access the Endpoint Security Administrator Portal.
2. Go to **Policy > Client Settings**.
3. In the right section **Capabilities & Exclusions**, click the **Installation & Upgrade** tab.
4. Clear the **Enable the user to postpone the client installation or upgrade** checkbox and click **Save**.



5. Click **Install Policy** to deploy the rule to the endpoints.
6. In the **Install Policy** pop-up screen, click **Save & Install**.

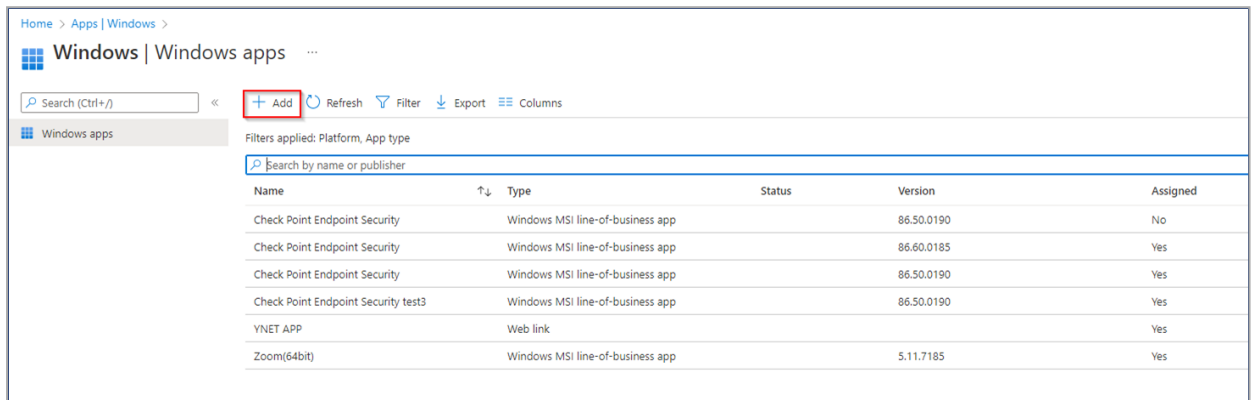


Creating the Endpoint Security Windows App in Microsoft Intune

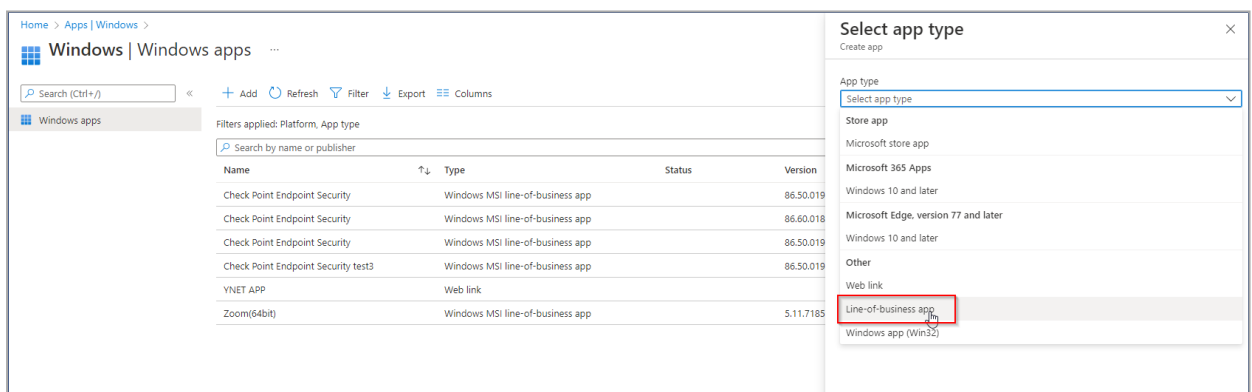
1. Log in to Microsoft Intune or Microsoft Endpoint Manager admin center.
2. Go to **Apps**. In the section **By Platforms**, select **Windows**.

The **Windows apps** page opens.

3. Click **Add**.

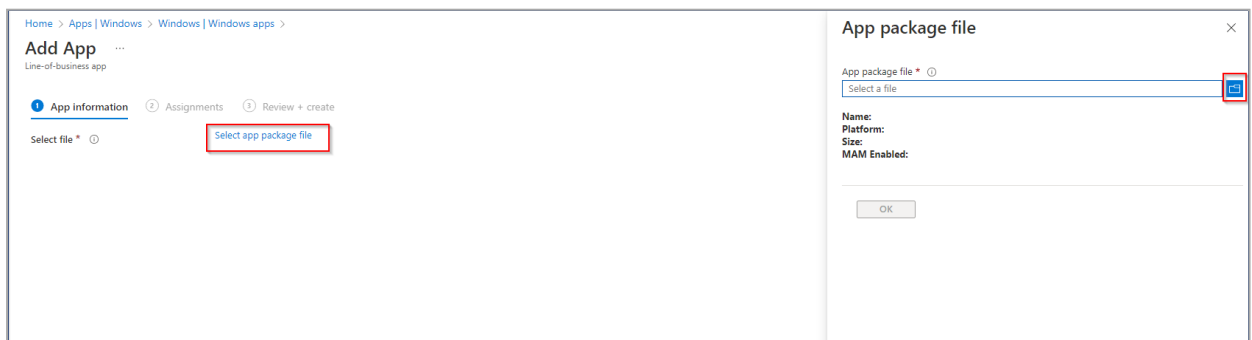


4. In the **Select app type** pane, select **Line-of-business app**, and click **Select** at the bottom.



The **Add app** page appears.

5. Under the **App information**, click **Select app package file**.



6. In the **App package file** pane, upload the **EPS.msi** file you created in ["Preparing the Endpoint Security Client Windows Package for Deployment" on page 772](#) and click **OK**.
7. Enter the **Name**, **Description**, and **Publisher** information.
8. Select **Yes** for **Ignore app version** and click **Next**.

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows MSI line-of-business app

Name * ⓘ

Description * ⓘ

[Edit Description](#)

Publisher * ⓘ

App install context ⓘ ☐ User ☐ Device

Ignore app version ⓘ ☐ Yes ☒ No

Command-line arguments

Category ⓘ

Show this as a featured app in the Company Portal ⓘ ☐ Yes ☒ No

Information URL ⓘ

Privacy URL ⓘ

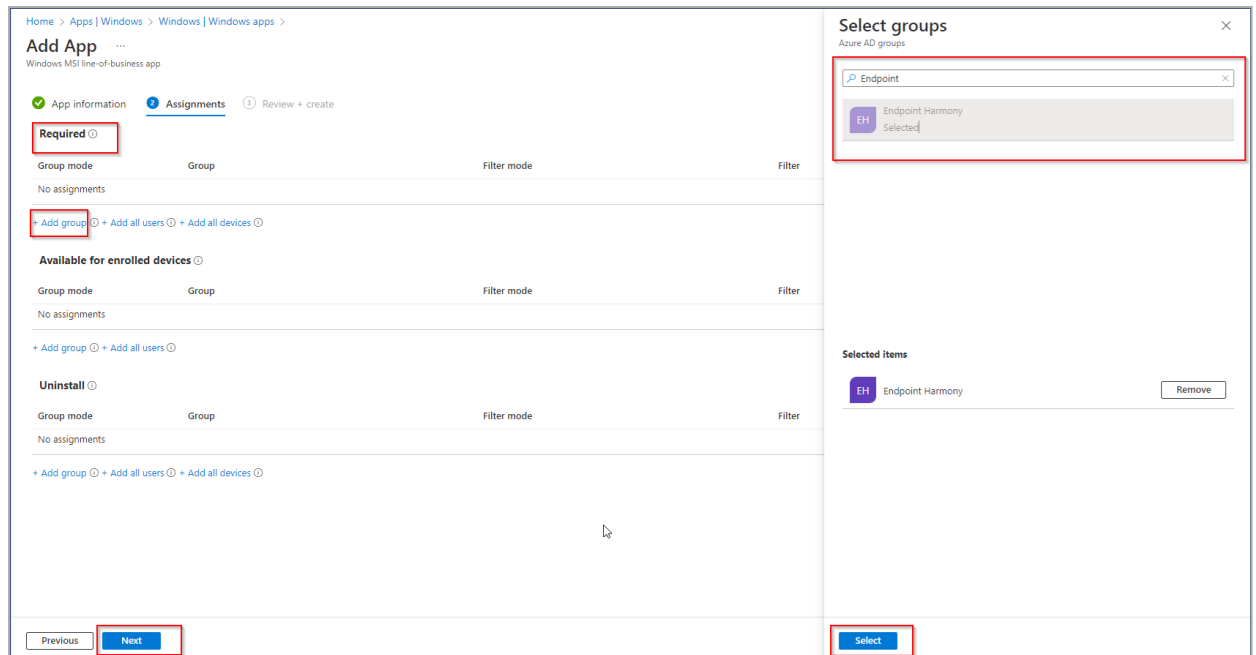
Developer ⓘ

Owner ⓘ

Notes ⓘ

Logo ⓘ [Select image](#)

9. Go to **Assignments** tab and assign the app to the groups that you want to deploy Endpoint Security Client. For more information, see [Assign apps to groups with Microsoft Intune](#).
10. In the **Assignments** tab, under **Required**, click **Add group**.
11. In the **Select groups** pane, select the relevant group and click **Select**.



12. In the **Add app** page, click **Next**.
13. Review the information and click **Create**.

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows MSI line-of-business app

App information

App package file	EPS.msi
Name	Check Point Endpoint Security
Description	Check Point Endpoint Security
Publisher	Check Point
App install context	Device
Ignore app version	No
Command-line arguments	--
Category	--
Show this as a featured app in the Company Portal	No
Information URL	--
Privacy URL	--
Developer	--
Owner	--
Notes	--
Logo	--

Assignments

Group mode	Group	Filter mode	Filter	Install
> Required				
Available for enrolled devices				
Uninstall				

Previous **Create**

After the **EPS.msi** file is uploaded, you can see information about the newly created app.

The screenshot displays the 'Check Point Endpoint Security' interface for 'Client Apps'. The left sidebar contains navigation links: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area shows the 'Check Point Endpoint Security' header with a search bar and a 'Delete' button. Below this, the 'Overview' tab is selected, showing 'Manage' and 'Monitor' sections. The 'Properties' section lists: Publisher: Check Point, Operating system: Windows, Version: 86.60.0185, Created: 8/16/2022, 2:18:46 PM, Assigned: Yes, and App package file: EPS.msi. The 'Device status' section features a donut chart showing 3 installed devices, with 0 not installed, 0 failed, 0 install pending, and 0 not applicable. The 'User status' section features a donut chart showing 1 installed user, with 0 not installed, 0 failed, 0 install pending, and 0 not applicable.

Home > Apps > Windows > Windows apps >

Check Point Endpoint Security

Client Apps

Search (Ctrl+/) Delete

Overview

Manage

Properties

Monitor

Device install status

User install status

Publisher : Check Point

Operating system : Windows

Version : 86.60.0185

Created : 8/16/2022, 2:18:46 PM

Assigned : Yes

App package file : EPS.msi

Device status

3 TOTAL

Installed: 3
Not Installed: 0
Failed: 0
Install Pending: 0
Not Applicable: 0

User status

1 TOTAL

Installed: 1
Not Installed: 0
Failed: 0
Install Pending: 0
Not Applicable: 0

Appendix D - Microsoft Intune Wipe and Windows Reset with Full Disk Encryption

Overview

Microsoft Intune Wipe and Windows Reset this PC are operating system-level reset mechanisms. When Check Point Full Disk Encryption (FDE) is enabled, encryption and authentication operate below the operating system, in the pre-boot environment.

Because of this separation, Windows reset and wipe operations do not remove or manage FDE.

Notes and Limitations

- Windows reset and wipe operations do not manage Full Disk Encryption.
- The required encryption state must be planned before performing a reset.
- Unsupported reset methods can result in inaccessible devices.

Reset Behavior with Full Disk Encryption

When Full Disk Encryption is enabled:

- Disk encryption remains enabled after a reset or wipe
- The pre-boot authentication environment is preserved
- Encryption keys and policies are not modified by reset operations

Windows reset and wipe mechanisms cannot:

- Remove Full Disk Encryption
- Remove the pre-boot authentication environment
- Change the encrypted disk state

Supported Reset and Wipe Configurations

The following table shows supported and unsupported reset and wipe configurations for devices protected with FDE.

Operation	Configuration	Supported
Reset this PC	Keep my files - Restore preinstalled apps = Yes	Yes
Reset this PC	Keep my files - Restore preinstalled apps = No	No

Operation	Configuration	Supported
Reset this PC	Remove everything - Clean data = Yes	Yes
Reset this PC	Remove everything - Clean data = No	Yes
Intune Wipe	Keep enrollment state	Yes
Intune Wipe	Continue wipe if device loses power	Yes
Autopilot Reset		No
Intune Wipe	Remove enrollment state	No
Windows Fresh Start		No

Reset Without Full Disk Encryption

Use this reset approach when the device must not remain encrypted after the reset or wipe.

In this case:

- Full Disk Encryption must be uninstalled
- All encrypted disks must be fully decrypted

After decryption:

- Microsoft Intune Wipe is supported
- Windows Reset this PC is supported

 **Note** - If Full Disk Encryption is not removed before the reset, the device can become inaccessible.

Reset with Full Disk Encryption Enabled

Use this reset approach when the device must remain encrypted after the reset or wipe.

In this case:

- Disk encryption remains enabled throughout the reset
- Pre-boot authentication remains enabled
- The Full Disk Encryption blade must be redeployed after the reset

After redeployment, the same Full Disk Encryption policy must be applied.

Autopilot Reset (Not Supported)

Autopilot Reset is not supported on devices protected with Full Disk Encryption.

Autopilot Reset performs device reprovisioning that assumes full control of disk state and platform security configuration. Because Full Disk Encryption operates below the operating system, Autopilot Reset cannot manage or remove FDE components.

Using Autopilot Reset on an encrypted device can result in:

- Boot failures
- Inaccessible encrypted disks
- Pre-boot authentication issues

Intune Wipe with Enrollment Removal (Not Supported)

Intune Wipe with enrollment removal is not supported on devices protected with Full Disk Encryption.

When enrollment is removed:

- The device management context is lost
- Full Disk Encryption components remain active
- The encryption state cannot be managed or recovered automatically

This can prevent access to the encrypted disk after the wipe.

Trusted Platform Module (TPM) Considerations

If the reset operation clears the TPM, TPM usage must be disabled in the Full Disk Encryption policy before the reset

If TPM usage is not disabled:

- SafeBoot authentication may fail
- Password-based authentication may fail