



HARMONY

24 February 2025

HARMONY BROWSE

Administration Guide



Check Point Copyright Notice

© 2021 - 2025 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.

Revision History

Date	Description
19 February 2025	Updated "Data Loss Prevention" on page 107 to add Ask action type and Application destination type.
30 October 2024	Added Gen AI Protect to "Data Loss Prevention" on page 107 .
17 October 2024	Added Control Browser Notifications to the Advanced Browser Settings in "Web and Files Protection" on page 57 .
15 October 2024	Added Incognito Mode settings to the Advanced Browser Settings in "Web and Files Protection" on page 57 .
10 October 2024	Added Managing Microsoft Sensitivity Labels for DLP in "Data Loss Prevention" on page 107 .
19 June 2024	Added: <ul style="list-style-type: none"> ▪ "Data Loss Prevention" on page 107. ▪ Data Loss Prevention column in "Introduction to Harmony Browse" on page 14.
19 February 2024	Added "Viewing Dashboard and Reports" on page 33 .
13 February 2024	Added Browser Status to the Table Filters and Column Description. See "Viewing Computer Information" on page 42 .
19 December 2023	Added video tutorials for: <ul style="list-style-type: none"> ▪ "Upload Protection" on page 70. ▪ "Block Upload by Domain" on page 72.
27 November 2023	Added "Custom Settings" on page 70 .
22 November 2023	Added video tutorial for "Upload Emulation " on page 58 .
17 October 2023	Added: <ul style="list-style-type: none"> ▪ "Upload Emulation " on page 58. ▪ "Upload Protection" on page 70. ▪ "Block Upload by Domain" on page 72.

Date	Description
7 August 2023	Added "Schedule Report" on page 172 .
31 July 2023	Added Disable Notifications. See "Credential Protection" on page 74 .
24 July 2023	Added "Upgrading the Harmony Browse Client (Windows only)" on page 27 .
20 June 2023	Added "Override Default File Actions" on page 66 .
23 May 2023	<ul style="list-style-type: none"> ■ Added support for Brave and Edge browsers on macOS. See Browser settings in "Web and Files Protection" on page 57 and the OS, browser, feature compatibility matrix table "Introduction to Harmony Browse" on page 14. ■ Added new features: <ul style="list-style-type: none"> ○ Sending monthly security reports. See "Sending Security Reports" on page 171. ○ "Reports Center" on page 172.
14 February 2023	Added information about the new feature; Policy Mode. See "Configuring the Threat Prevention Policy" on page 51 .
8 February 2023	Added new feature "Sending Security Reports" on page 171 .
7 February 2023	Added a new topic "Uninstalling the Harmony Browse Extension" on page 174 .
31 January 2023	<ul style="list-style-type: none"> ■ Added information about the new feature; Scan local HTML files. See "Credential Protection" on page 74. ■ Added information about the new event; Accessing a local HTML file. See "User Interface - Customized Browser Block Pages" on page 50.
13 December 2022	<ul style="list-style-type: none"> ■ Added information about Localizations supported by the Harmony Browse extension. See "General Information" on page 149. ■ Added a new field Upload and emulate files under to specify the file size limit for Threat Emulation and Extraction. See "Download Emulation and Extraction" on page 57.
05 December 2022	<ul style="list-style-type: none"> ■ Added information about the new feature; Browser Extension Pinning. See "Browser Settings" on page 101. ■ Added a note about how to know the installed Harmony Browse client version. See "Deploying Harmony Browse Clients" on page 22.

Date	Description
04 November 2022	<ul style="list-style-type: none"> ■ Added supported file types for Threat Emulation. See "Download Emulation and Extraction" on page 57. ■ Data residency is now supported for Australia, India and United Kingdom. See Registering to the Infinity Portal.
27 October 2022	<ul style="list-style-type: none"> ■ Added information about the new feature; Malicious Script Protection. See "Malicious Script Protection" on page 65 and "Introduction to Harmony Browse" on page 14. ■ Search reputation is now supported with Bing and Yahoo search engines. See "Web and Files Protection" on page 57.
09 September 2022	Updated "Browser Settings" on page 101 for the Brave browser.
16 August 2022	Added support for the Brave browser on Windows. See "Introduction to Harmony Browse" on page 14 and "Deploying Harmony Browse Clients" on page 22 .
10 August 2022	Added a new topic "Managing IoCs" on page 105 .
25 July 2022	<ul style="list-style-type: none"> ■ Added information about support for Threat Emulation appliance. See "Download Emulation and Extraction" on page 57. ■ Added sk179690 to verify whether the Harmony Browse client can access the Check Point services and the stores of extensions. See "Deploying Harmony Browse Clients" on page 22.
13 July 2022	<ul style="list-style-type: none"> ■ Added information about the new "Web and Files Protection" on page 57. ■ Added three new options for "Web and Files Protection" on page 57.
05 June 2022	Added steps for installing the Harmony Browse extension for Safari. See "Deploying Harmony Browse Clients" on page 22 .
01 June 2022	Added "Browser Settings" on page 101 .
18 May 2022	Updated Adding Exclusions to Rules
04 May 2022	Added "Browser Settings" on page 101

Date	Description
1 February 2022	<p>Updated:</p> <ul style="list-style-type: none"> ▪ Introduction ▪ Creating a New Harmony Browse Management Service ▪ Configuring Harmony Browse Policy ▪ Configuring Client Settings Policy <p>Removed:</p> <ul style="list-style-type: none"> ▪ Configuring Client Settings ▪ Viewing Harmony Browse Logs
30 January 2022	<p>Added:</p> <ul style="list-style-type: none"> ▪ Managing Users in <p>Updated:</p> <ul style="list-style-type: none"> ▪ Introduction ▪ Viewing Computer, Operational and Security Information ▪ Web and Files Protection <p>Removed:</p> <ul style="list-style-type: none"> ▪ Viewing Operational and Security Information
25 January 2022	<p>Updated</p> <ul style="list-style-type: none"> ▪ Viewing Computer Information ▪ Adding Exclusions to Rules ▪ Managing Scanners ▪ Managing Virtual Groups <p>Removed:</p> <ul style="list-style-type: none"> ▪ Active Directory Authentication ▪ Recent Tasks
16 January 2022	<p>Updated:</p> <ul style="list-style-type: none"> ▪ Configuring Harmony Browse Policy
11 January 2022	<p>Updated:</p> <ul style="list-style-type: none"> ▪ Client User Interface Settings

Date	Description
9 January 2022	Added: <ul style="list-style-type: none"> ▪ Harmony Browse Logs Updated: <ul style="list-style-type: none"> ▪ Configuring Threat Prevention Policy ▪ Web and Files Protection ▪ Adding Exclusions to Rules
2 January 2022	Updated: <ul style="list-style-type: none"> ▪ Managing Licenses in the Cloud ▪ Web & Files Protection
12 December 2021	Updated: <ul style="list-style-type: none"> ▪ Introduction ▪ Deploying Endpoint Clients ▪ Configuring Harmony Browse Policy ▪ Configuring Global Policy Settings ▪ Web & Files Protection ▪ Adding Exclusions to Rules Removed: <ul style="list-style-type: none"> ▪ <i>Manual Deployment of Endpoint Clients</i> ▪ <i>Adding a New VPN Site to an Exported Package</i> ▪ Monitoring Deployment and Policy ▪ Performing Push Operations
10 November 2021	Updated: <ul style="list-style-type: none"> ▪ Active Directory Authentication
04 November 2021	Updated: <ul style="list-style-type: none"> ▪ Active Directory Authentication
01 October 2021	Improved formatting and document layout Updated: <ul style="list-style-type: none"> ▪ Adding Exclusions to Rules
15 June 2021	First release of this document

Check Point is engaged in a continuous effort to improve its documentation.

[Please help us by sending your comments to our Technical Writers.](#)

Table of Contents

Revision History	3
Introduction to Harmony Browse	14
Getting Started	16
Creating an Account in the Infinity Portal	16
Accessing the Harmony Browse Administrator Portal	17
Managing Licenses	19
User Center	19
Activating the License	21
Deploying Harmony Browse Clients	22
Upgrading the Harmony Browse Client (Windows only)	27
Creating a New Harmony Browse Management Service	28
Managing Users in Harmony Browse	29
Managing Accounts in the Infinity Portal	32
Viewing Dashboard and Reports	33
Dashboard	33
Custom Dashboard	33
Creating a Custom Dashboard	34
Managing a Custom Dashboard	36
Reports	36
Generate Report	37
Scheduled Reports	38
Announcements	41
Viewing Computer Information	42
Asset Management View	42
Creating a Custom View	42
Status Icon	43
Filters	43

Working with the Computers Table	45
Managing Computers	46
General Actions	46
Configuring Harmony Browse Policy	49
Configuring Client Settings Policy	50
User Interface - Customized Browser Block Pages	50
General - Share Data with Check Point	50
Configuring the Threat Prevention Policy	51
The Parts of the Policy Rule Base	51
The Threat Prevention Policy Toolbar	51
Policy Mode	52
Updating a Predefined Policy Mode	56
Web and Files Protection	57
URL Filtering	57
Files Protection	57
Download Emulation and Extraction	57
Upload Emulation	58
Credential Protection	60
Zero Phishing	60
Password Reuse Protection	60
Safe Search	62
Search Reputation	62
Force Safe Search	63
Advanced Settings	64
URL Filtering	64
Categories	64
Deny List	64
Malicious Script Protection	65
Files Protection	65
General Settings	65

Emulation Environments	65
Override Default File Actions	66
Download Protection	66
Supported Files	67
Download Emulation Actions	69
Unsupported Files	70
Custom Settings	70
Download Emulation and Extraction	70
Upload Protection	70
Upload Emulation Actions	71
Block Upload by Domain	72
Credential Protection	74
Browser Settings	75
Pin Extension	75
Windows	75
macOS	75
Control Browser Notifications	75
Incognito Mode	76
Adding Exclusions to Rules	76
Legacy Exclusions	76
Adding Exclusions to a Specific Rule	76
Adding Global Exclusions	77
Adding Exclusions from Logs	77
Adding a New Exclusion to an Exclusion Category	77
Editing an Exclusion	78
Smart Exclusions	81
Adding Exclusions to a Specific Rule	82
Adding Global Exclusions	90
Migrating Legacy Exclusions	98
Importing and Exporting Exclusions	99

Managing Exclusions	100
Browser Settings	101
Disabling Incognito Mode, BrowserGuest Mode, and InPrivate Mode	101
Overview	101
Chrome on Windows	101
Firefox on Windows	101
Microsoft Edge on Windows	102
Brave on Windows	102
Chrome on macOS	103
Firefox on macOS	103
Microsoft Edge on macOS	103
Enabling the Browser Extension on a Browser with Incognito or InPrivate Mode	104
Ending the Browser Process Running in the Background	104
Browser Extension Pinning	105
Managing IoCs	105
Prerequisite	105
Data Loss Prevention	107
DLP Logs	110
Use Case	111
Known Limitations	111
Sample Data Type	111
Creating a Custom Data Type	113
Creating a Custom Data Type Group	119
Adding an Existing Data Type to a Group	122
Editing a Data Type or Group	123
Duplicating a Data Type or a Group	126
Deleting a Data Type or a Group	128
Managing Microsoft Sensitivity Labels for DLP	130
Step 1 - Copy the Microsoft Sensitivity label names and their UUIDs from Microsoft Purview	130

Step 2 - Creating Microsoft Sensitivity Labels in Harmony Browse	132
Step 3 - Assign Sensitivity Labels to DLP Rules	136
Creating a DLP Rule and Associating with an Event	136
Rule Configuration Logic	142
Scenarios	143
Specific Event	143
Result	143
Specific Event	144
Result	144
Specific Event	144
Result	144
Specific Event	144
Result	145
Specific Event	145
Result	145
Specific Event	145
Result	146
Specific Event	146
Result	146
Specific Event	146
Result	146
Specific Event	147
Result	147
Specific Event	147
Result	147
Specific Event	147
Result	148
Specific Event	148
Result	148
General Information	149

Localization	149
Managing Active Directory Scanners	151
Organization Distributed Scan	151
Full Active Directory Sync	151
Harmony Browse Logs	154
Query Language Overview	156
Criteria Values	156
NOT Values	158
Wildcards	158
Field Keywords	159
Boolean Operators	161
Managing Virtual Groups	162
Exporting Logs	167
Creating Security Certificates for TLS Mutual Authentication	167
Sending Security Reports	171
Reports Center	172
Generate Report	172
Schedule Report	172
Uninstalling the Harmony Browse Extension	174

Introduction to Harmony Browse

Check Point Harmony Browse is a lightweight and easy to deploy solution which enables users to safely access the internet, no matter where they are. It protects organizations and their employees from web-based threats by preventing users from visiting zero-day phishing sites, downloading zero-day malware, accessing non-compliant websites, and reusing corporate passwords for non-business web content.

The product contains an on-cloud management system and a browser extension which provides multi-layer browser protection capabilities.

OS	Browser	URL Filtering	Threat Extraction and Emulation	Upload Emulation	Block Upload by Domain	Zero Phishing	Password Reuse	Safe Search	Search Reputation	Malicious Script Protection	Data Loss Prevention
Windows	Chrome	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Edge Chromium	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Firefox	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
	Brave ³	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Internet Explorer ¹	No	Yes	No	No	Yes	Yes	No	No	No	No
mac OS	Chrome	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Firefox	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
	Safari ²	Yes	No	No	No	Yes	Yes	No	No	No	No
	Brave ³	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Edge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ChromeOS	Chrome	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

 **Notes -**

¹ By default, the extension is disabled. To enable the extension, see [Deploying Harmony Browse Clients](#).

² Browser extension is supported in Safari version 14 and higher.

³ Browser extension is supported in Brave version 1.43.89 and higher.

To set Harmony Browse, follow these steps:

1. Register to the Infinity Portal (see Registering to the Infinity Portal).
2. Register to Harmony Browse (see *"Accessing the Harmony Browse Administrator Portal" on page 17*).
3. Create a new Harmony Browse Management Service (see *"Creating a New Harmony Browse Management Service" on page 28*).
4. Deploy Harmony Browse clients (see *"Deploying Harmony Browse Clients" on page 22*).
5. Create a Harmony Browse Policy (see *"Configuring the Threat Prevention Policy" on page 51*).

Getting Started

To get started with Harmony Browse:

1. [Create an account in Infinity Portal](#)
2. [Accessing the Harmony Browse Administrator Portal](#)
3. [Managing Licenses](#)
4. [Creating a New Harmony Browse Management Service](#)
5. [Deploying Harmony Browse Client](#)
6. [Configuring Harmony Browse Policy](#)

Creating an Account in the Infinity Portal

Check Point Infinity Portal is a web-based interface that hosts the Check Point security SaaS services.

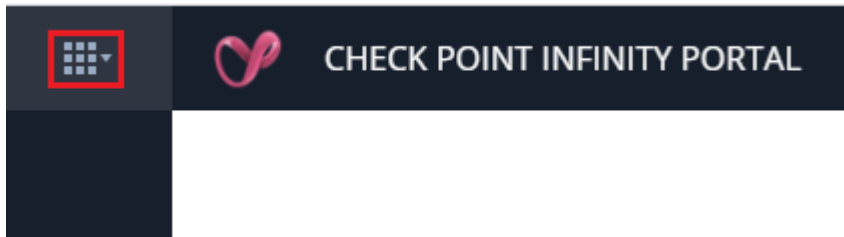
With Infinity Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

To create an Infinity Portal account, see the [Infinity Portal Administration Guide](#).

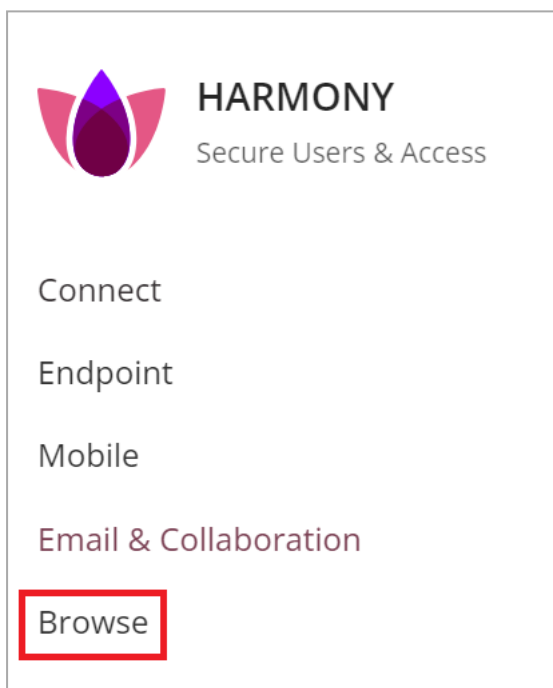
Accessing the Harmony Browse Administrator Portal

To access the Harmony Browse Administrator Portal:

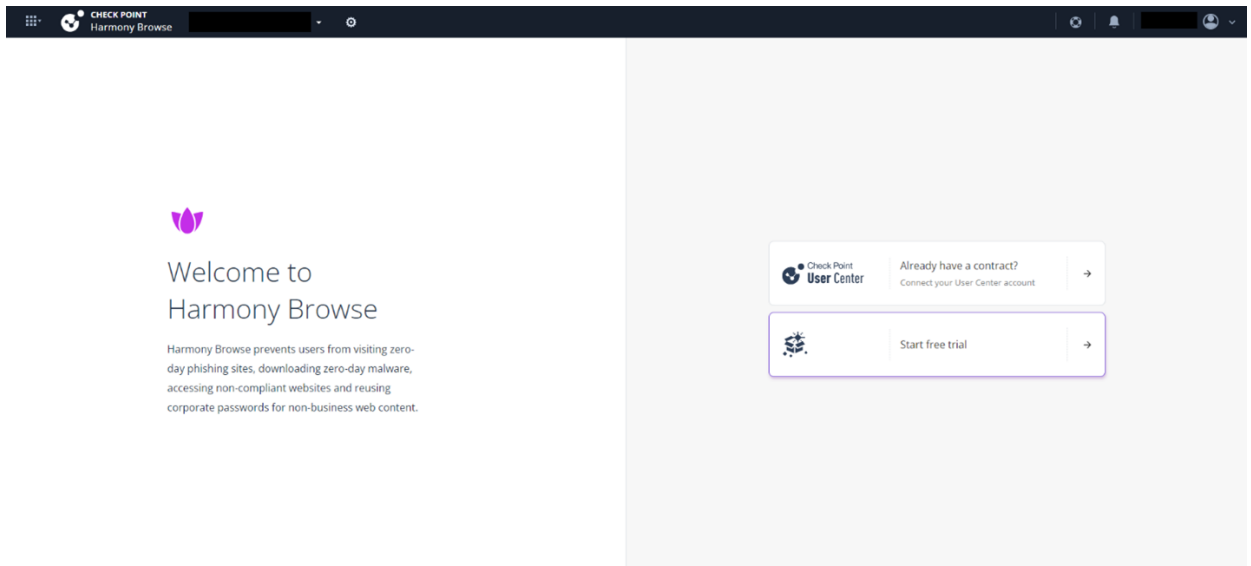
1. Sign in to [Check Point Infinity Portal](#).
2. Click the **Menu** button in the top left corner.



3. Under **Harmony**, click **Browse**.



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 [Infinity 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 **Overview** page appears.

Harmony Browse creates the endpoint management service automatically.

Managing Licenses

User Center

When you create an account in the Infinity 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.

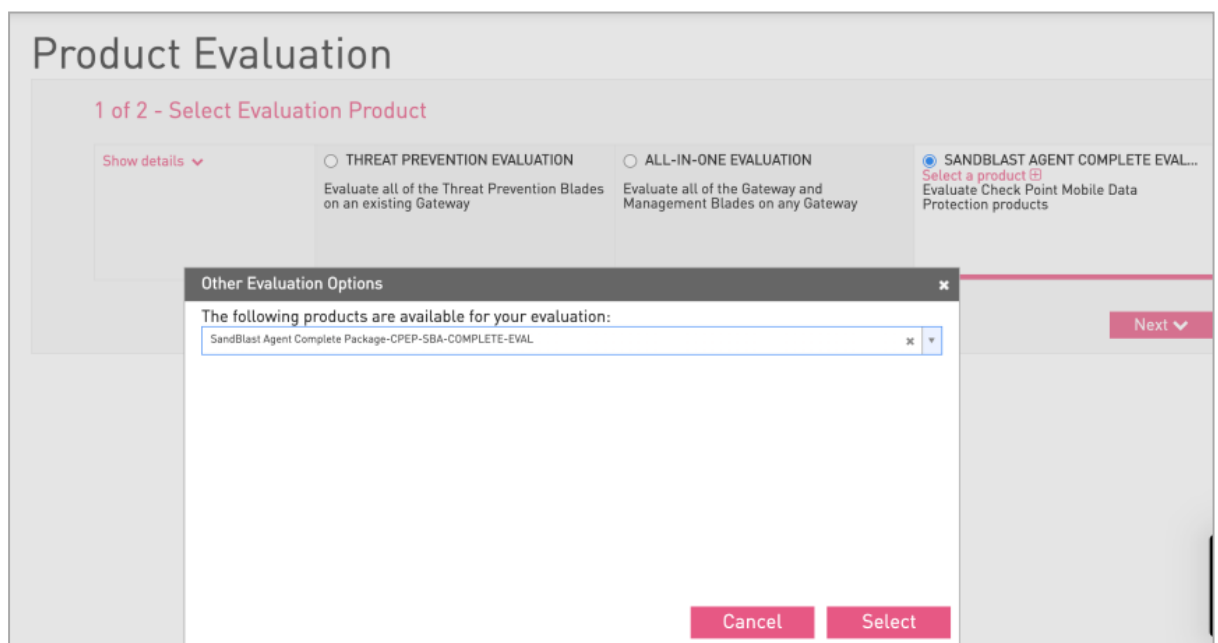
Once you create a User Center account, contact your Check Point sales representative to purchase a license.

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 **Harmony Browse - CP-HAR-BROWSE-EVAL** from the drop-down list and click **Select**.

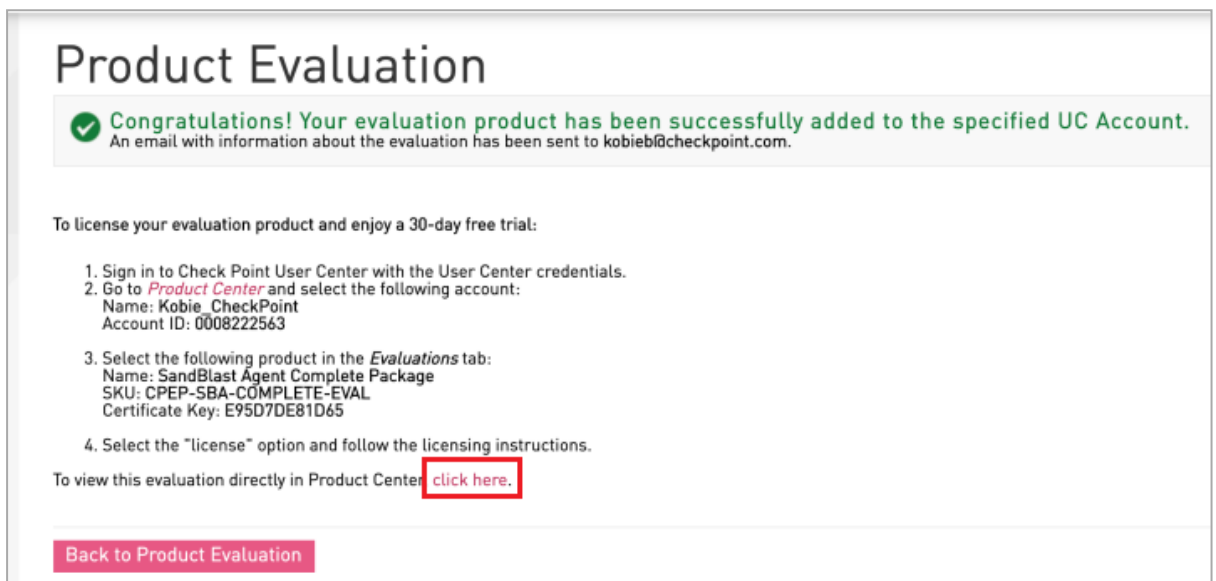


7. Click **Next**
8. In the **Provide Evaluation Info** section that opens, fill in these details:

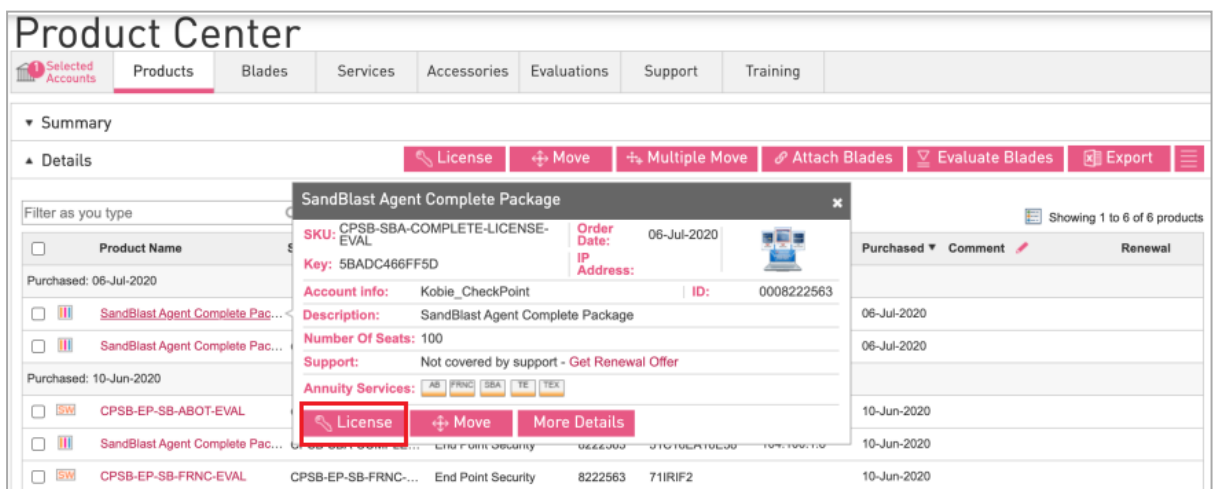
- a. User Center Account
 - b. Email Address
 - c. Evaluation Product will be used by
 - d. Purpose of Evaluation
9. Click **Get Evaluation**.

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.



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 CP-HAR-BROWSE-LICENSE-EVAL
 Certificate Key 4C3602D21A43
 Description Harmony Browsing Security - browser extension security service for one user EVAL

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 NameSelect

• OtherNot relevant.....

• Operating SystemSelect.....

Please select the features you would like to license:

Product/Feature	Description	IP Address
<input checked="" type="checkbox"/> CP-PSB-BROWSE		

* - Required Fields

13. Click License.

Activating the License

To activate a license

1. In Harmony Browse 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**.

Deploying Harmony Browse Clients

Notes -

- Harmony Browse automatically downloads and installs the latest version of the Harmony Browse client on the endpoints. To know the version of the Harmony Browse client installed on the endpoints, go to **Assets Management > Computers** and see the **Endpoint Version** column in the table.
- For Mozilla Firefox users: If a user is accessing the browser for the first time after installing the Harmony Browse extension, a consent page appears that explains how user's personal information is collected, used, and protected. The user must click **Confirm** to provide consent and activate the extension's protection features.

To download the Harmony Browse client:

1. Click **Overview** and then click **Download** on the top banner.
2. To download the file immediately, click **Download** for the relevant OS and transfer the file to the endpoint.

Client	OS	Downloaded file
Browse	Windows	<i>BrowserSetup.exe</i>
	macOS	<i>BrowserSetup.zip</i>
	ChromeOS	<i>BrowserSetup_chromeOS_laptop.txt</i> or <i>BrowserSetup_chromeOS_desktop.txt</i>

To install the Harmony Browse client on Windows using .exe file:

1. Copy the latest `BrowserSetup.exe` to the endpoint.
2. Double click the `BrowserSetup.exe` file to install Harmony Browse.
3. Creating `.msi` file:
 - a. Select **Start** and type **CMD**.
 - b. Right-click **Command Prompt** and select **Run as administrator**.

c. Run:

```
cd <path to BrowseSetup.exe file>
```


d. Run:

```
BrowseSetup.exe /CreateMsi
```

The system creates the `EPS.msi` file.

To install the Harmony Browse client on Windows using .msi file:

1. Copy `EPS.msi` to the endpoint.

 **Note** - You can install Harmony Browse extension on the Internet Explorer using the .msi file only.

2. Select **Start** and type **CMD**.

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

4. Do any of these:

- Run:

```
msiexec /i EPS.msi
```

- To install the Windows client with Internet Explorer extension, run:

```
msiexec /i EPS.msi no_ie=false
```

- To install the Windows client without the Brave browser extension, run:

```
msiexec /i EPS.msi brave_extension_disabled=true
```

- To install the Windows client and setting the virtual group of the client, run:

```
msiexec /i EPS.msi virtual_group_name="virtual_group_name"
```

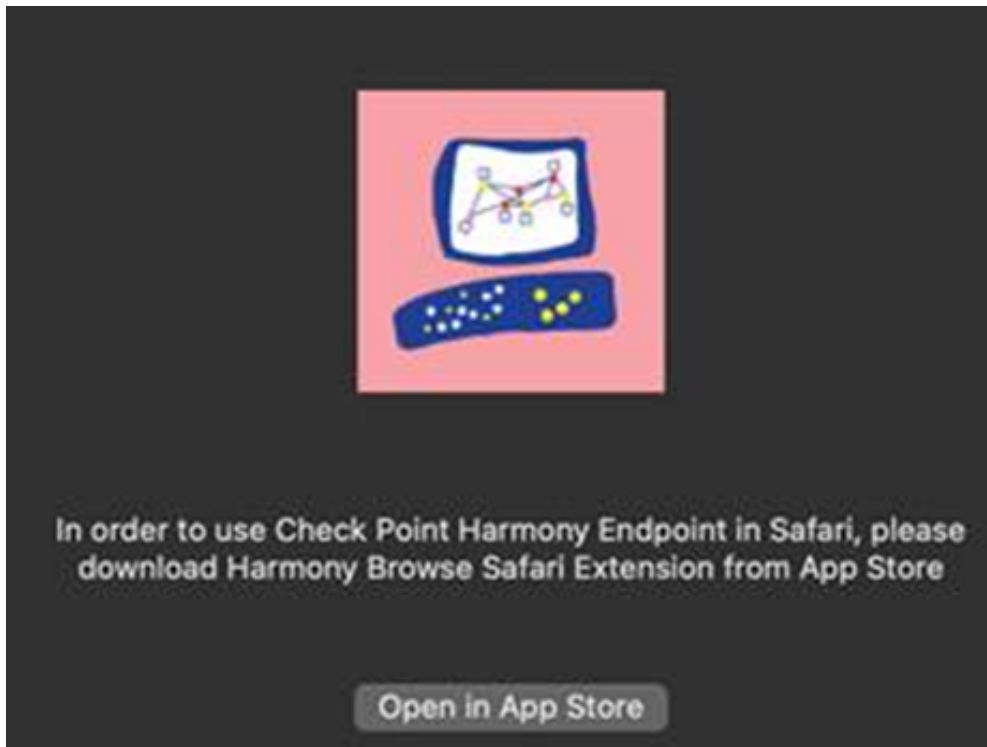
To install the Harmony Browse client on macOS:

1. Copy the zip file to the client.

2. Unzip the file.

3. Run the app file.

4. If you are using Safari, a prompt appears:

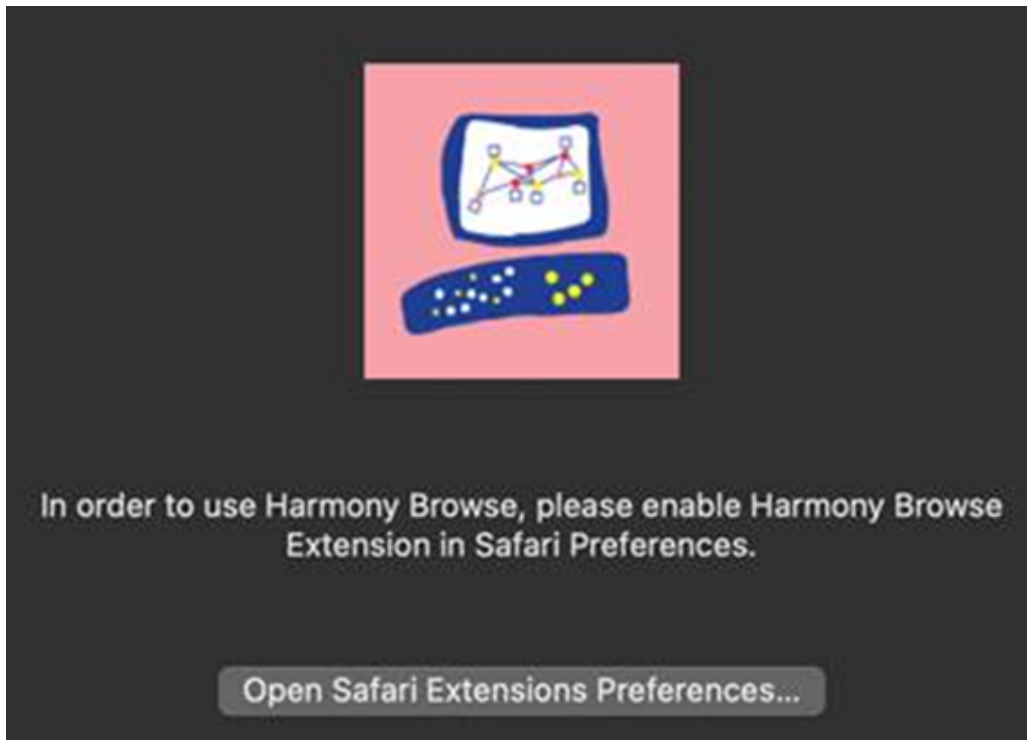


Note - If you do not install the extension, the prompt appears every time you open Safari. If you do not want to install the extension and stop the prompt, in the terminal window, run:

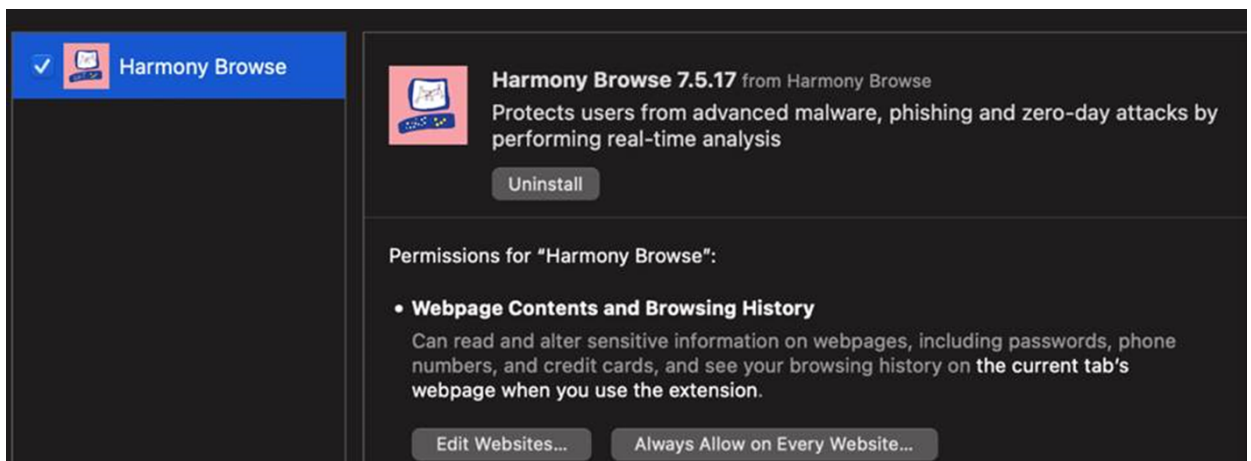
```
sudo defaults write  
/Library/Preferences/com.checkpoint.harmony.browse.helper mute_  
all_prompts -bool YES
```

5. Click **Open in App Store** and install the extension.

After you install the extension, a prompt appears.



6. Click **Open Safari Extensions Preferences**.



7. Select the **Harmony Browse** checkbox and click **Always Allow on Every Website**.
8. Go to **Security & Privacy** and click **Full Disk Access**.



9. Select the **Harmony Browse Helper** checkbox.

Note - To install Harmony Browse on Chromebook, see [sk173974](#).

To verify whether the Harmony Browse client can access the Check Point services and the stores of extensions, see [sk179690](#).

Upgrading the Harmony Browse Client (Windows only)

To upgrade the client:

- Install the .exe file for Windows. See ["Deploying Harmony Browse Clients" on page 22](#).
- Using a *msi* file:
 1. Convert the exe file to *msi* file. See ["Deploying Harmony Browse Clients" on page 22](#).
 2. Run:

```
msiexec /i EPS.msi /qn && timeout /t 30 && msiexec /i  
EPS.msi /qn
```

Creating a New Harmony Browse Management Service

After you register, Harmony Browse automatically creates a new management service.

For existing or old tenants that do not have a management service, you must create a management service manually.

To create a management service manually:

1. In the **Service Management** view, under the **Creating New Browse Management**, enter the information for these fields:

- **Service Identifier** - Select your Endpoint Management Service name for this account.

The Service Identifier:

- 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 Harmony Browse Management Service is deployed. This information is derived from your selection of data residency region when you created the account. See Registering to the Infinity Portal.

2. Click **Create**.

The deployment process initiates.

You can monitor the deployment process in the portal and an email is sent on completion.

Managing Users in Harmony Browse

After you create an account, you can create users who have access to Harmony Browse using this account.

To each user you create, you must assign a user role.

Only **User Admin** can assign roles.

There are two types of user roles:

- **Global** roles.

When creating a new user, you must assign a Global role to the user.

- **Specific Service** roles.

Assigning a Specific Service role to a new user is optional.

Global Roles

Global Roles define the user's permissions to define user roles.

The Global Roles apply to the Infinity Portal platform and to all the services in the Infinity Portal.

Currently, these are the supported Infinity Portal roles:

Role	Description
Admin	Allows Read & Write permissions across all services in your Infinity Portal account. When a new service is activated in your account, an Admin user automatically gets Read & Write permissions in this service.
Read-Only	Allows full Read-Only visibility to all services in your Infinity Portal account. When a new service is activated in your account, a Read-Only user automatically gets read permissions in this service.
User Admin	Allows management of all aspects of users and roles in your Infinity Portal account. Only administrators with User Admin permission can access the Users tab and associate roles with users. Administrators with an Admin role and no User Admin role, cannot access the Users tab.

You can assign multiple Global Roles to each user.

Specific Service Roles

Roles which apply only to a specific service, in this case the role selected here applies only to the Harmony Browse service. You can assign only one Harmony Browse role per user. The Specific Service role selected overrides the assigned Global roles. There are 6 types of specific Harmony Browse 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.

The table below summarizes the permissions of each user type:

Tab on Left Panel	Section	Admin User	Read-Only
Overview	All	Read & Write	Read-Only
Policy	All	Read & Write	Read-Only
	Threat Prevention - Exclusions	Read & Write	Read-Only
Asset Management	All	Read & Write	Read-Only
	Computer Actions (Delete computer data)	Read & Write	Read-Only
Logs	All	Read & Write	Read-Only
Endpoint Settings	All	Read & Write	Read-Only
Service Management	All	Read & Write	Read-Only
	Service Actions (Restart, pause or terminate the service)	Read & Write	Read-Only

To see the list of users and the roles assigned to them, go to the **Global Settings** view > **Users**.

To create a new user:

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**
- **Specific Service Roles**



Note - If the user you wish to add is not registered in Harmony Browse, they receive a registration invitation to establish login credentials for the portal.

5. Click **Add**.



Note: - To edit or delete a user, select the user and click **Edit** or **Delete** from the top toolbar.

Managing Accounts in the Infinity 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 **Harmony Browse**, 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 Harmony Browse, they receive a registration invitation to establish login credentials for the portal.

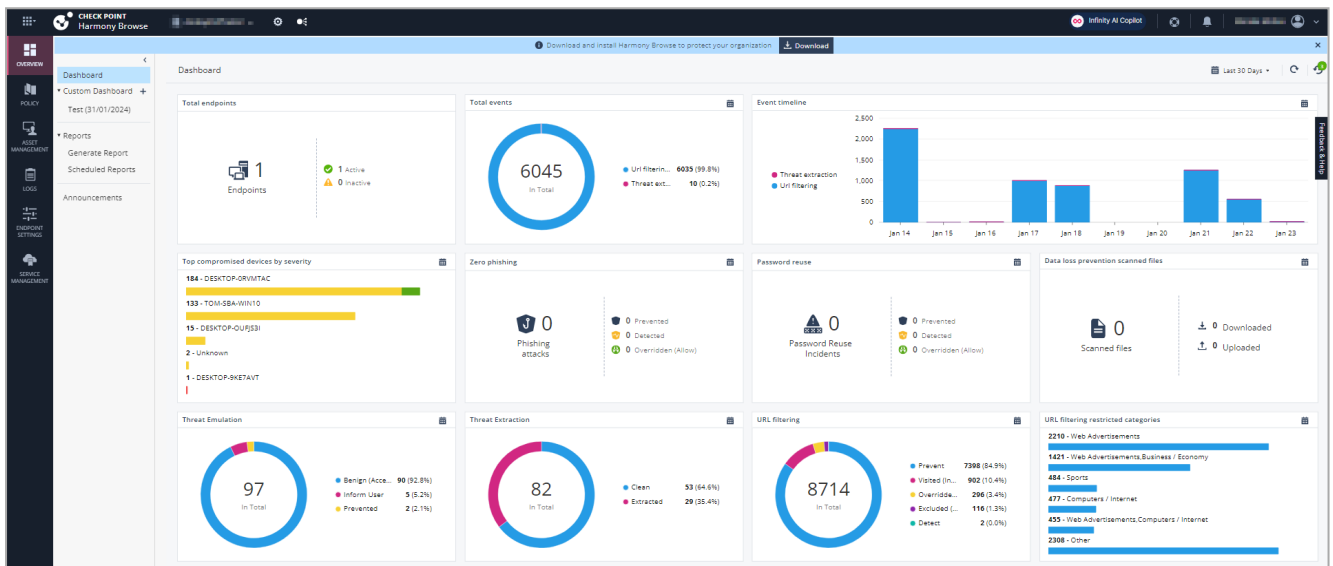
5. Click **Add**.

Viewing Dashboard and Reports

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

Dashboard

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



Custom Dashboard

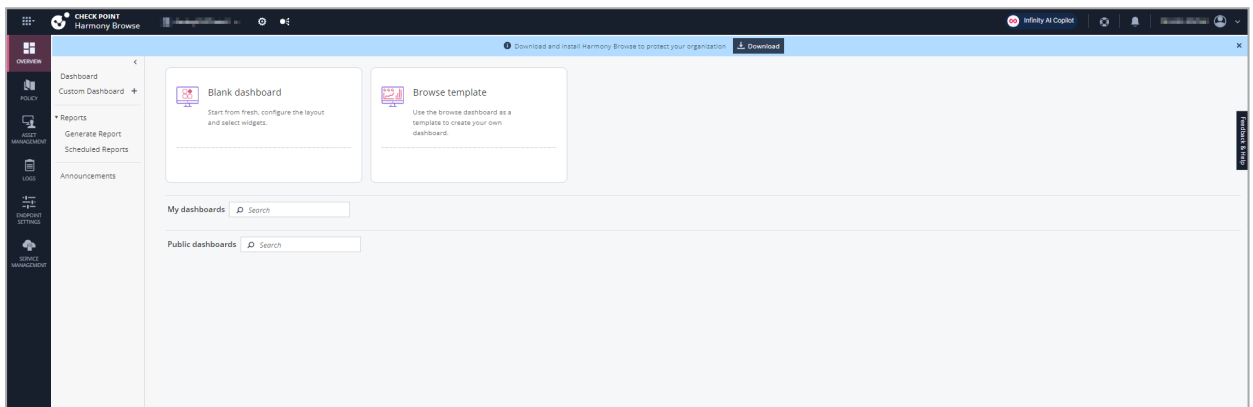
The **Custom Dashboard** allows you to create personalized dashboards with widgets of your preference and specify whether the dashboard should be private or public. **Private** dashboards are available only for you to view whereas, **Public** dashboards are available for all the users with access to 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. **Browse template** allows you to customize the **Dashboard**.

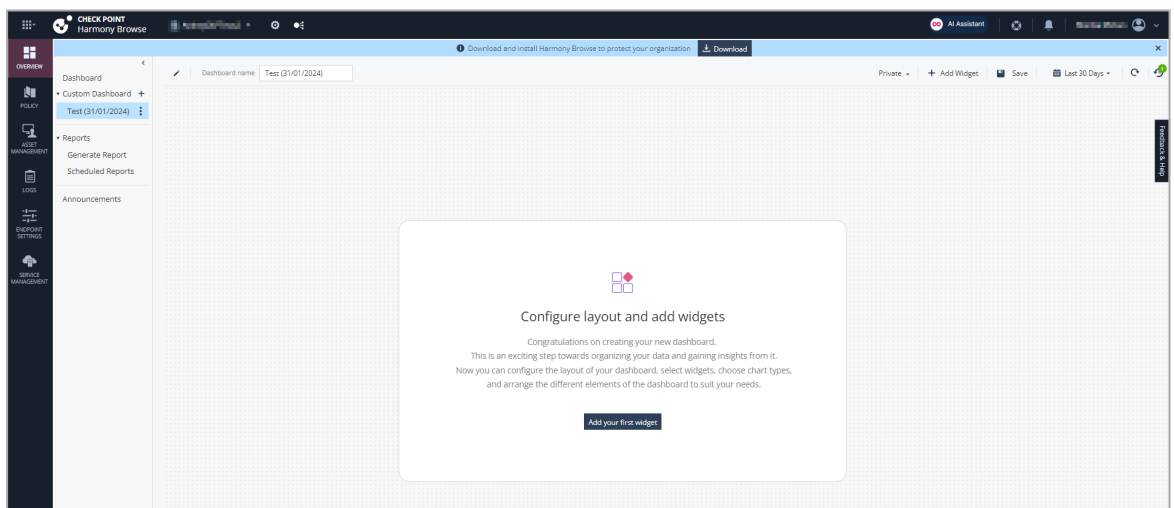
Creating a Custom Dashboard



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**.

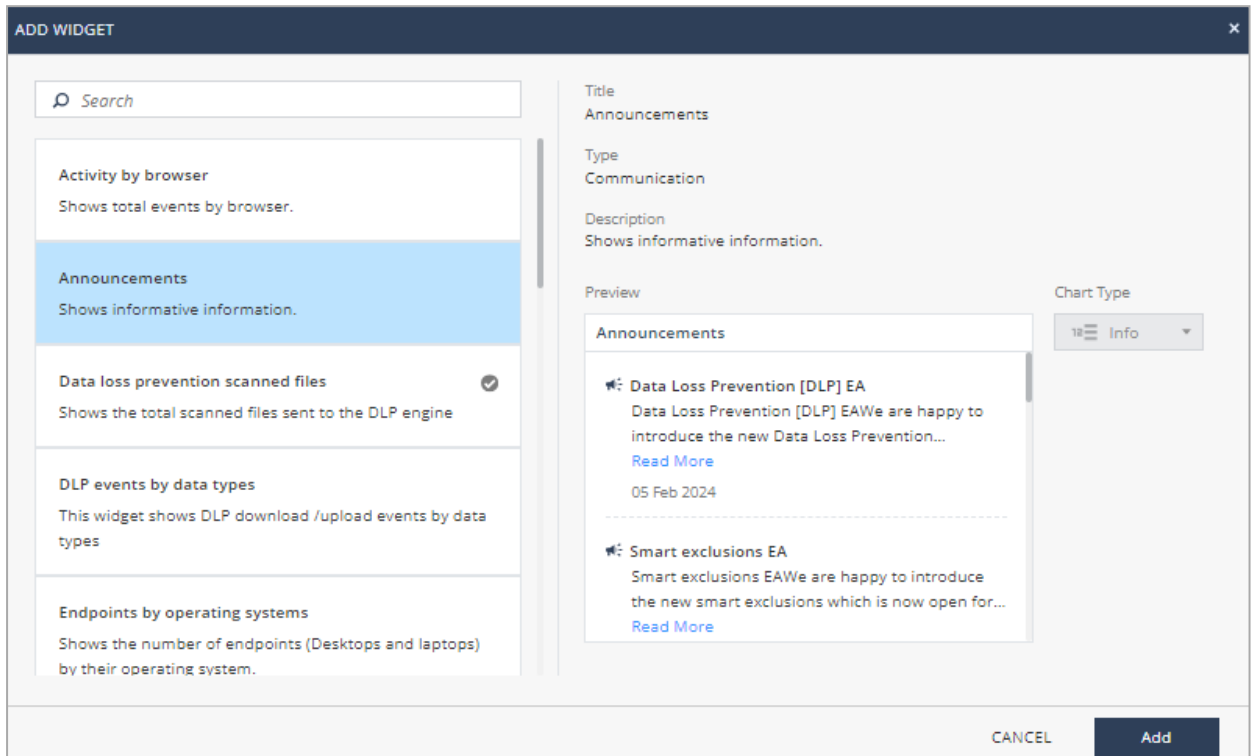
The **Add Widget** window appears.


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


- a. Hover over the **Browse 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**.



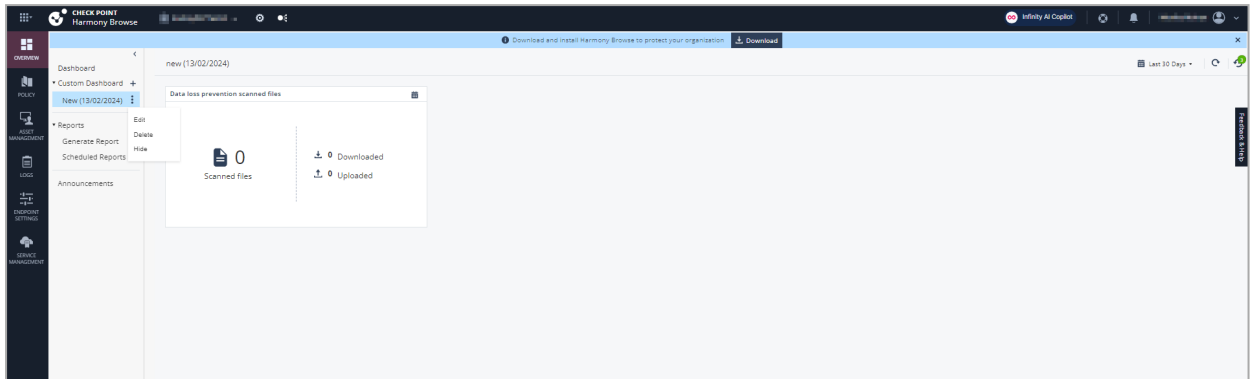
 **Note** - The **Add** button is disabled if the widget is already added to the dashboard.

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**.

Reports

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

- **Security Checkup** - Shows the latest security events.
- **2023 Security Checkup** - Shows a summary of the security events reported by Harmony Browse during 2023.
- **Threat Extraction Report** - Shows the insights on the downloaded files.
- **Check Point Cyber Security Report** - Shows the latest security trends as per Check Point.

Generate Report



To generate a report:

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

The **Export Report** window appears.

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).

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
✕

Name:

Format:


Frequency:

Time: : UTC Now: 08:40

Recipients:

- 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 - 2023 SECURITY CHECKUP
✕

Name:

Format:

Frequency:

Time: : UTC Now: 08:42

Recipients: 

- 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 Harmony Browse.

Viewing Computer Information

Asset Management View

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

Status	Computer Name	Endpoint Version	OS Build	Virtual Group	Device Type	Deploy Time	Last Connection	Last Logged In User	Browser's Status
	BROWSE_90.08.74...	All Desktops+ 1 more	Desktop	04 Feb 2024 07:28 pm	05 Feb 2024 10:30 am	admin	
	BROWSE_90.09.00...	All Desktops+ 1 more	Desktop	01 Feb 2024 06:19 pm	02 Feb 2024 04:12 pm	admin	
	BROWSE_90.09.00...	All Desktops+ 1 more	Desktop	02 Feb 2024 03:50 pm	02 Feb 2024 04:13 pm	admin	
	BROWSE_90.09.00...	All Desktops+ 1 more	Desktop	04 Feb 2024 03:26 pm	05 Feb 2024 12:58 pm	Eli	
	BROWSE_90.09.00...	All Desktops+ 1 more	Desktop	02 Feb 2024 12:30 pm	02 Feb 2024 12:38 pm	user	
	BROWSE_90.09.00...	All Desktops+ 2 more	Desktop	20 Jan 2024 12:10 pm	20 Jan 2024 03:14 pm	admin	
	BROWSE_1_0	All Laptops+ 1 more	Laptop	08 Jan 2024 03:06 pm	08 Jan 2024 04:46 pm	sta	

1 of 7 selected

General

Display Name:

Description:

LDAP

SAM Name:

CN:

Operating System: macOS

OS Version:

Member of

All Windows Laptops

All Laptops


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.

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 44](#).
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 Active Directory scanner.
	Indicates Harmony Browse client.
	Indicates that the client connection is active.
	Indicates that a new computer was discovered that has no client installed.
	Indicates that the computer was deleted from the Active Directory or from the Organizational Tree.

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 the previous page .
Computer Name	Name of the connected computer.
Domain Name	Domain name of the connected computer.
Endpoint version	Harmony Browse installer version.
Operating System	Operating System version installed on the computer.
Device Type	Type of the computer (Desktop or Laptop).
Deploy Time	Time when the client was installed on the computer.
OS Build	Operating System build number of the computer.
Last Connection	Last connection date of the computer.
Last Logged In User	Last logged in user name on the computer.
Virtual Groups	Pre-defined and custom virtual groups of the computer.

Filter/Column Name	Description
Browser Status	<p>Shows the browser and the Harmony Browse extension status on the endpoint.</p> <p>The supported statuses are:</p> <ul style="list-style-type: none"> ▪ Not Installed - <ul style="list-style-type: none"> ○ The browser is not installed. ○ The browser is installed but not used. ○ The browser is used but the extension is disabled by the policy. ▪ Running - 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 browser extension version does not support Browser Status. <p> Note - This is supported only with the Windows browser extension version BROWSE_90.09.0033 and higher.</p>

Working with the Computers Table

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

Managing Computers


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

General Actions

View Computer Logs

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

To view computer logs by it's IP address:

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

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

Create Virtual Group

You can create a virtual group. See [Managing-Virtual-Groups.htm](#).

Create and Add to Virtual Group

You can add computers to a new virtual group. See [Managing-Virtual-Groups.htm](#).

Add to Virtual Group


You can add a computer to a virtual group. See [Managing-Virtual-Groups.htm](#).

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

Directory Scanner

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

Configuring Harmony Browse Policy

The Harmony Browse security policy contains these components:

- Client Settings - including the blocking pages customization and the data sharing with Check Point.
- Threat Prevention - which includes Web & Files Protection. The Threat Prevention policy is unified for all the Threat Prevention components.

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.

In addition, the Browse policy contains the Global Policy Settings (see ["Configuring Client Settings Policy" on page 50](#)) and the Deployment Policy (see ["Deploying Harmony Browse Clients" on page 22](#)).

Configuring Client Settings Policy

User Interface - 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.

General - Share 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.

Configuring the Threat Prevention Policy

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

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 device rules and user rules.

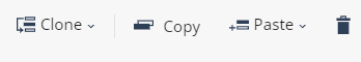

- You can use user objects only in the user policy, and you can use device objects only in the device policy.
- There is no default rule for the user policy.
- User rules override device rules.
- You can use the same group in user and device rules at the same time.
- If a group contains both users and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

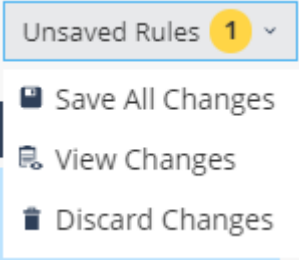
To enable user policy, go to the **Endpoint Settings** view > **Policy Operation Mode**, and select **Mixed mode**.

The 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.
Web & Files Protection	The configurations that applies to URL Filtering , Download Protection , Credential Protection , Safe Search and Advanced Settings .

The Threat Prevention Policy Toolbar

To do this	Click this
Clone, copy, paste, and delete rules	
Search	<input type="text" value="Search for entity"/> 

To do this	Click this
<p>Save, view, and discard changes</p> <p>Note - The View Changes functionality shows the policy type that was changed and the date of the change.</p>	

Policy Mode

Policy mode allows you to:

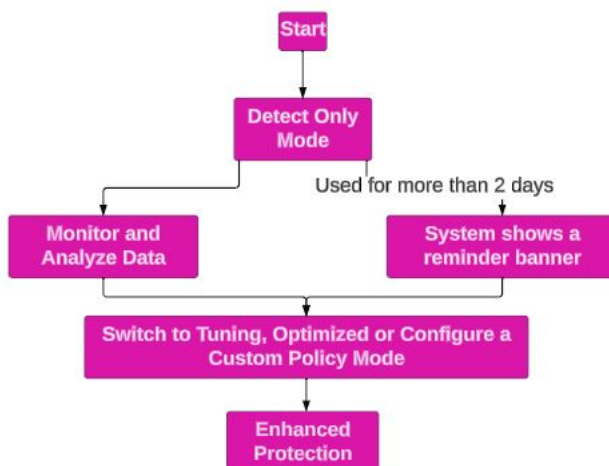
- Quickly configure a Threat Prevention policy by selecting a predefined policy mode (**Detect only**, **Tuning** and **Optimized**). Check Point automatically sets the appropriate operation mode (**Detect**, **Prevent**, **Off**) and **Advanced Settings** options for each capability.
- Manually set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

Capability	Policy Mode		
	Tuning	Detect only	Optimized
URL Filtering	Detect	Detect	Prevent
Download Protection	Detect	Detect	Prevent
Zero Phishing	Detect	Detect	Prevent
Password Reuse	Detect	Detect	Prevent
Search Reputation	Off	Off	On
Force Safe Search	Off	Off	On

Advanced Settings

Capability	Policy Mode		
	Tuning	Detect only	Optimized
URL Filtering	<p>Allow user to dismiss the URL Filtering alert and access the website is disabled.</p> <p>Under Categories, Service is selected.</p> <p>Under Malicious Script Protection:</p> <ul style="list-style-type: none"> ◦ 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. 		<p>Allow user to dismiss the URL Filtering alert and access the website is selected.</p> <p>Under Categories, Service is selected.</p> <p>Under Malicious Script Protection:</p> <ul style="list-style-type: none"> ◦ 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.
Download Protection	<p>Under Supported files, Emulate original file without suspending access is selected.</p> <p>Under Unsupported files, Allow Download is selected.</p>		<p>Under Supported files:</p> <ul style="list-style-type: none"> ◦ Get extracted copy before emulation completes is selected. ◦ Extract potential malicious elements is selected. <p>Under Unsupported files, Allow Download is selected.</p>
Credential Protection	<p>Under Zero Protection, Allow user to dismiss the phishing alert and access the website is disabled.</p> <p>Under Password Reuse, Allow users to dismiss the password reuse alert and access the website is disabled.</p>		<p>Under Zero Protection, Allow user to dismiss the phishing alert and access the website is selected.</p> <p>Under Password Reuse, Allow users to dismiss the password reuse alert and access the website is selected.</p>

- Select **Custom** and set the operation mode manually. For more information, see ["Web and Files Protection" on page 57](#).

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.



- 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 and Files Protection

URL Filtering

URL Filtering rules define which sites can be accessed from within your organization.

To set the URL Filtering mode:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the rule.
3. In the **Web & Files Protection** tab, under **URL Filtering**, select a mode:
 - **Prevent** - The request to enter a site is suspended until a verdict regarding the site is received. Access to the site is blocked if site matches one of the blocked categories or the Deny List.
 - Allows user to dismiss the URL Filtering alert and access the website.
 - This option is selected by default. It provides the user with access to a blocked site if the end user believes the verdict is unjustified. This option can also be turned off through the **Advanced Settings** section.
 - **Detect** - Allows an access if a site is determined as malicious, but logs the traffic.
 - **Off** - **URL Filtering** is turned off.
4. For **Advanced Settings**, see ["URL Filtering" on page 64](#).

Files Protection

Download Emulation and Extraction

Download Protection rules protects users from malicious content.

To set the Download Emulation & Extraction mode:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the rule.
3. In the **Web & Files Protection** tab, under **Download Protection**, select a mode:
 - **Prevent** - Prevents the download if the file is either known to be malicious or detected as malicious by the Threat Emulation.

- **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** - Downloads the file without protection.

4. For **Advanced Settings**, see "[Download Protection](#)" on page 66.

Upload Emulation

Upload Emulation uses Threat Emulation to analyze the files you upload to protected domains to identify threats and mitigate them.



Notes:

- This feature is not supported for Harmony Browse clients managed through the Harmony Endpoint Administrator Portal.
- The domains may support multiple ways to upload a file. For example, clicking a button to browse and upload the file or drag-and-drop the file. If you upload files by drag-and-drop, the **Upload Emulation** feature operates in the **Detect** mode, even if you set to **Prevent** mode.



To enable Upload Emulation:

1. Navigate to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the rule.
3. In the **Web & Files Protection** tab, under **Upload Emulation**, select a mode:
 - **Prevent** - Prevents the upload if the file is either known to be malicious or detected as malicious by the Threat Emulation. To specify additional behaviors for the **Prevent** mode, see *"Upload Protection" on page 70*.
 - **Detect** - Allows the user to upload the files even if it is detected as malicious. The incidents are logged.
 - **Off** - Uploads the file without protection.
4. To specify the protected domains, in the **Upload Emulation** section, click **Edit**.
5. Click **New**.
6. In the **Value** field, enter the domain name or IP address of the protected domain. For example, my-domain or 1.1.1.1.
7. Select the required action for **Upload Emulation**:
 - **Protected** - Enables upload emulation.
 - **Not Protected** - Upload Emulation is disabled.
8. Click **Save**.
9. To delete the domain, select the domain and click **Delete**.

10. To add multiple protected domains, click  :
- To add a list of protected domains and set **Upload Emulation** as **Protected**, click **Import Upload Emulation** and select the CSV file with protected domains.
 - To add a list of protected domains and set both **Password Reuse** and **Upload Emulation** as **Protected**, click **Import All** and select the CSV files with protected domains.
11. To export the list of domains to a CSV file, click  :
- To export only the domains with **Upload Emulation** set as **Protected**, click **Export Upload Emulation**.
 - To export all domains, click **Export All**.
- The system exports the data to a CSV file.
12. Click **OK**.
13. For **Advanced Settings**, see ["Upload Protection" on page 70](#).

Credential Protection

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.

To set the Zero Phishing mode:

1. Go to **Policy > Threat Prevention > Policy Capabilities**.
2. Select the rule.
3. In the **Web & Files Protection** tab, under **Zero Phishing**, select a mode:
 - **Prevent** - If site is scanned and found to be malicious, access to it is blocked and log of the incident is shown in the Harmony Browse web management log section.
 - **Detect** - An incident log is sent but access to the site is not be blocked. Also, the site scan is silent (invisible to the user).
 - **OFF** - Turns off the feature.
4. For **Advanced Settings**, see ["Credential Protection" on page 74](#).


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 **Web & Files Protection** tab, 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 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 Harmony Browse logs.
 - **Off** - Turns off password reuse protection.

4. To add domains to **Password Reuse**, click **New**

 **Note** - Make sure that the endpoint is added to the domain.

5. In the **Value** field, enter the domain name or IP address of the protected domain. For example, my-domain or 1.1.1.1
6. Select the required action for **Password Reuse**:
 - **Protected** - Blocks users from reusing the password of protected domain in other domains.
 - **Not Protected** - Allows users to reuse the password of the protected domain in other domains.
7. Click **Save**.
8. To delete the domain, select the domain and click **Delete**.

9. To add multiple protected domains, click  :
 - To add a list of protected domains and set **Password Reuse** as **Protected**, click **Import Password Reuse**, and select the CSV file with protected domains.
 - To add a list of protected domains and set both **Password Reuse** and **Upload Emulation** as **Protected**, click **Import All** and select the CSV file with protected domain.

10. To export the list of domains to a CSV file, click  :

- To export only the domains with **Password Reuse** set as **Protected**, click **Enable Password Reuse**.
- To export all domains, click **Export All**.

The system exports the data to a CSV file.

11. For **Advanced Settings**, see "[Credential Protection](#)" on page 74.

Safe Search

Search Reputation

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


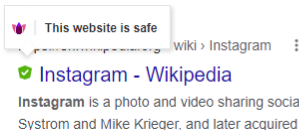
Notes:


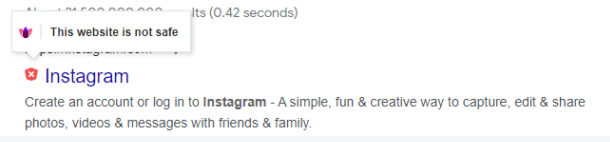

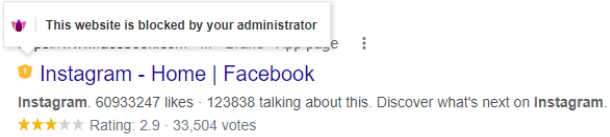
- It is supported only with Google, Bing, and Yahoo search engines.
- To enable this feature, ensure that you set **URL Filtering Mode** to either **Prevent** or **Detect**.


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
	<p>The website is safe.</p> <p>Example:</p>  <p>Instagram - Wikipedia</p> <p>Instagram is a photo and video sharing social networking service founded in 2010 by Kevin Systrom and Mike Krieger, and later acquired by American company ...</p>

Icon	Classification
	<p>The website is not safe.</p> <p>Example:</p> 
	<p>The website is blocked by the Administrator.</p> <p>Example:</p> 

 **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, Harmony Browse 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.

Advanced Settings

URL Filtering

 **Note** - You must set the **URL Filtering Mode** to **Prevent** or **Detect** to set the **Advanced Settings**.

Allow user to dismiss the URL Filtering alert and access the website - Allows user to bypass URL filtering and access the website.

Categories

Harmony Browse categorizes websites and you can specify the categories that must be blocked for the user. When you select a category, the URL Filtering rule applies to all sites in the selected category.

To specify the categories to block:

1. Under **Categories**, select the category. For example, **Bandwidth Consumption**.
2. Click **Show** and then select the sub-category.

Deny List

You can specify specific URLs, domains or IP addresses you want to block or deny access to.

To add a domain or IP address to Deny List, click **Show** and add the URL, domain or IP address.


Notes:

- You can add the domain names manually or upload a CSV file with the domain names you want to add to the Deny List.
- You can use * and ? as wildcards in 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.
- You can export your deny list.
- If you wish to completely block the domain www.test-domain.com, including its sub-domains (sub1.test-domain.com, sub2.test-domain.com, etc') and it is a naked domain (test-domain.com, without the www), you need to add two values to the deny list:
 - *.test_domain.com
 - test_domain.com

Malicious Script Protection

Malicious Script Protection scans **Uncategorized** websites for embedded malicious JavaScripts. If the domain that hosts the script belongs to any one of these categories, then the page is blocked and the event is logged.

- Anonymizer
- Botnets
- Critical Risk
- High Risk
- Medium Risk
- Phishing
- Spam
- Spyware
- Malicious Sites
- Suspicious Content

 **Note** - Ensure that you set **URL Filtering Mode** to either **Prevent** or **Detect**. If it is set to **Prevent**, the page is blocked and the event is logged. If it is set to **Detect**, the page is **not** blocked and the event is logged.

To specify malicious script protection:

- To enable malicious script protection, select **Block websites where Malicious Scripts are found embedded in the HTML**.
- To allow users to dismiss the malicious script security alert and access the website, select **Allow user to dismiss the Malicious Scripts alert and access the website**.


Files Protection

General Settings

Emulation Environments

You can specify the size limit for files that must be sent for Threat Emulation. Files larger than the specified limit are not sent to Threat Emulation.

Upload and emulate files under - Specify the file size limit for Threat Emulation. The default file size limit is 15 MB. The maximum file size limit supported is 100 MB.

 **Note** - Increasing the file size increases the client processing and network traffic required to process large files.




Override Default File Actions

Harmony Browse allows you to override the default file action for the supported and unsupported files.

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 page 70*.
 - **Allow**
 - **Block**
3. Select the **Upload action** for the file:
 - **Default** - The action specified in *"Unsupported Files" on page 70*.
 - **Allow**
 - **Block**
4. (Optional) In the **Comments** field, enter a comment.
5. Click **OK**.

Download Protection

 **Note** - You must set the **Download Emulation & Extraction** to **Prevent** or **Detect** to set the **Advanced Settings**.

Harmony Browse protects against malicious files that you download to your Endpoint. By default, it sends the files for extraction and emulation to Check Point's Threat Emulation on the cloud before they are downloaded to the Endpoint disk. You can also configure Harmony Browse with Threat Emulation on-premise. For more information, see [sk113599](#).

- Threat Emulation: Detects zero-day and unknown attacks. Files are sent to sandbox for emulation to detect evasive zero-day attacks.
- Threat Extraction: Proactively protects users from malicious content. It quickly delivers safe files while the original files are inspected for potential threats.

Supported Files

The supported file types for Threat Emulation are:

Threat Emulation Supported File Types

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

Threat Emulation Supported File Types

img	sldm	xz
iqy		zip
jar		

The supported file types for Threat Extraction are:

Threat Extraction Supported File Types

doc	potm	pptx
docm	potx	xls
docx	ppa	xlsb
dot	ppam	xlsm
dotm	pps	xlsx
dotx	ppsm	xlt
fdf	ppsx	xltm
pdf	ppt	xltx
pot	pptm	xlam
one		



Note - Ignore the files types listed in the Harmony Browse Administrator Portal.

Download Emulation Actions

The options available for supported file types of Threat Extraction are:

- **Get extracted copy before emulation completes**
 - **Extract potential malicious elements** - While a file is tested, receive a copy of the file with all suspicious parts removed. Files that support extraction are available for download after the extraction. Files that do not support extraction are available for download only after the emulation and if it is benign.
 - To specify the elements for Threat Extraction in the downloaded file, click **Elements to extract** and click **+** to add and click **✓** to remove.
 - **Covert to PDF** - For receive the file in a PDF format. If the file is not malicious, users receive the original file when the emulation is finished. Emulation can take up to two minutes.
- **Suspend download until emulation completes** - The original file is downloaded if found to be clean.
- **Emulate original file without suspending access** - Emulates original file without suspending access to the file and logs the incident. If the file is malicious, it is blocked.
- **Allow** - Threat Emulation and Threat Extraction is turned off.

Unsupported Files

The options available for unsupported files types are:

- **Allow Download** - Allows user to access the file.
- **Block Download** - Blocks user from accessing the file.

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.

Upload Protection

Harmony Browse protects against malicious files that you upload to the protected domains. By default, it sends the files to Check Point's Threat Emulation on the cloud before they are uploaded to the domains. You can specify the advanced settings for uploading files that are supported and unsupported by Threat Emulation.

 **Note** - This feature is not supported for Harmony Browse clients managed through the Harmony Endpoint Administrator Portal.



Upload Emulation Actions

- For supported files:
 - **Suspend Upload Until Emulation Completes** - File uploads to the protected domains are suspended until the Threat Emulation analysis of the files is complete and the verdict is benign.
 - **Emulate the file without suspending access and block known malicious files** - Malicious files are blocked and not uploaded to protected domains. Rest of the files are sent to Threat Emulation for analysis without suspending the file upload.
 - **Emulate the file without suspending access** - Files uploaded to the protected domains are logged but not prevented. End user does not receive any notification.
 - **Allow** - Disables the Upload Emulation feature. That is, allows users to upload files to protected domains without Threat Emulation.
- For unsupported files:

- **Allow** - Allows the upload of file types that are not supported by Threat Emulation to the protected domain.
 - **Warning** - Uploading files without Threat Emulation analysis may pose potential security risks.
 - **Block** - Blocks the upload of file types that are not supported by Threat Emulation to the protected domain.
- Note** - File type policy overrides the default file action selected here. For more information, see ["Override Default File Actions" on page 66](#).

Block Upload by Domain

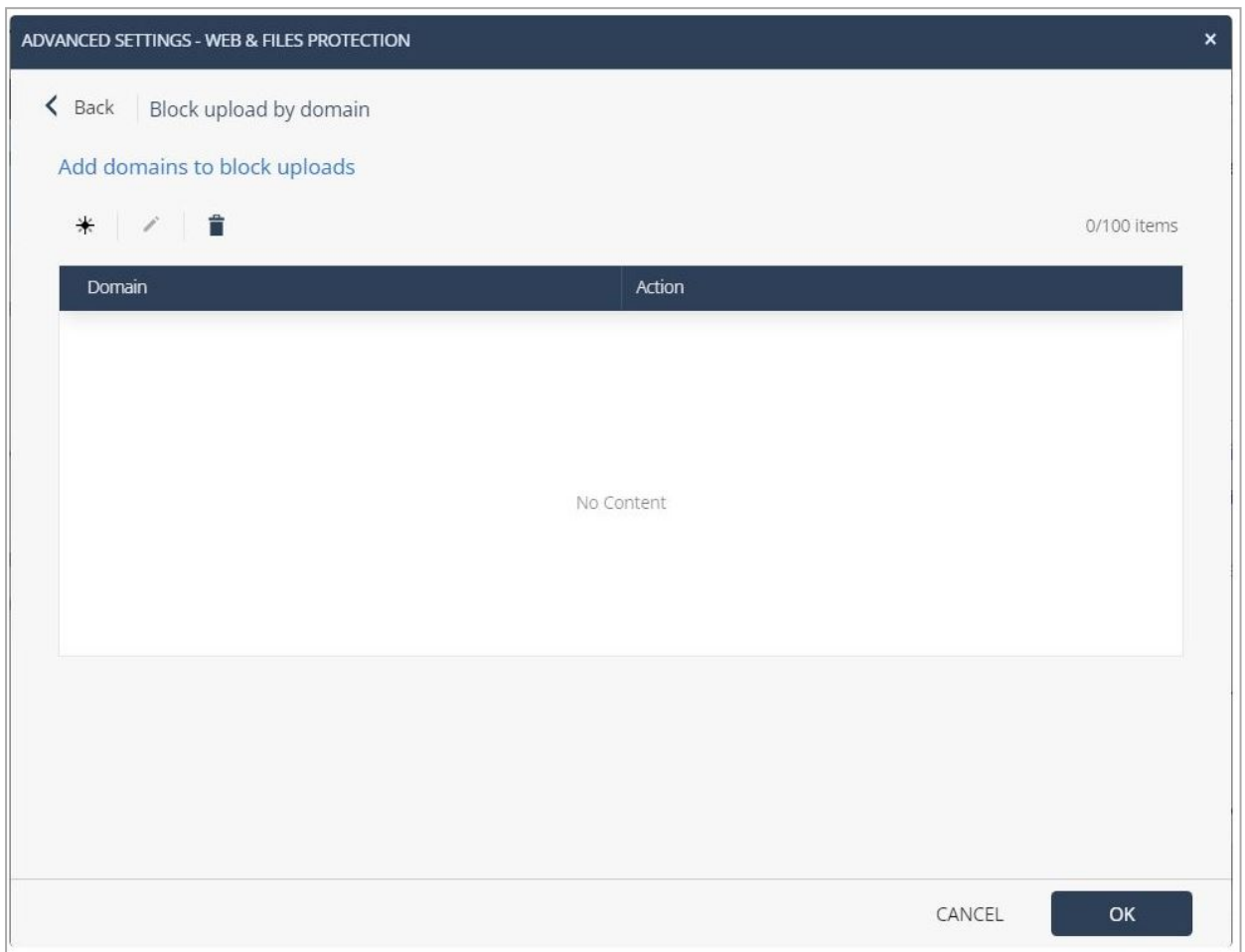
Allows you to specify domains to which you want to either allow or block upload files, regardless of the [Upload Emulation](#) setting.






To block or allow files upload to a domain:

1. Navigate to **Upload Protection**.
2. In the **Block upload by domain** section, click **Edit**.


The **Advanced Settings - Web & Files Protection** window appears.



3. Click .
4. In the **Value** field, enter the domain name or IP address. For example, my-domain.com or 1.1.1.1.
5. From the **Action** list, select the required action:
 - Block
 - Allow
6. Click **OK**.
7. To edit a domain, select the domain and click .

8. To delete a domain, select the domain and click  .
9. Click OK.

Credential Protection

-  **Note** - You must set the **Zero Phishing** and **Password Reuse** to **Prevent** or **Detect** to set the **Advanced Settings**.

User can select any of these settings under **Zero Phishing**:


- **Allow user to dismiss the phishing alert and access the website** - It allows the user to dismiss the blocking page and continue to enter the corporate password.
- **Send log on each scanned site**
- **Allow user to abort phishing scans**
- **Scan local HTML files** - By default, the Harmony Browse 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 ["Configuring Client Settings Policy" on page 50](#)
- This feature is not supported with Safari and Internet Explorer browser extensions.

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

1. When a user opens a local HTML file, the **Harmony Browse 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, Harmony Browse 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.

User can select any of these settings under **Password Reuse Protection**:


- To protect a domain, click **Edit** and enter the domain name or IP address.
- You can also select **Allow users to dismiss the password reuse alert and access the website** setting.

Browser Settings

Pin Extension

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

By default, Harmony Browse extension is pinned to the browser for all users with the Harmony Browse Client version *BROWSE_90.09.0001* and higher (Windows) and latest mac clients.

 **Note** - You can unpin the extension only on Chromium browsers, such as Chrome, Edge and Brave. You cannot unpin an extension in Firefox.

Windows

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

The user must re-login by locking and unlocking the endpoint and either restart the browser or wait for 15 minutes for the changes to reflect. This is not applicable to endpoints with the Harmony Endpoint Security client installed as the browser extension is pinned automatically through the policy update.

macOS

You cannot disable Extension Pinning through a policy in Harmony Browse.

To manually disable Extension Pinning:

1. On the endpoint, navigate to */Library/Application Support/Checkpoint/Threat Emulation/*.
2. Remove these lines from the browser specific script. For example, for Chrome, the script file name is **install_chrome_ext.sh**.

```
<key>$PIN_KEY</key>
```

```
<string>$PIN_VALUE</string>
```

3. Save and run the script.
4. Reload the policy on the browser. For example for Chrome, go to *chrome://policy* and click **Reload policies**.

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.

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.

Legacy Exclusions

You can exclude specific objects from inspection by the protections:

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 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.

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.

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	<ul style="list-style-type: none"> ▪ https://www.domain.com ▪ http://www.domain.com 	<ul style="list-style-type: none"> ▪ https://domain.com ▪ http://domain.com ▪ https://sub.domain.com ▪ http://sub.domain.com
domain.com	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ https://sub.domain.com ▪ http://sub.domain.com 	https://sub2.domain.com

If you enter	It excludes these	It does not exclude these
*.domain.com	Sub-domain of domain.com such as: <ul style="list-style-type: none"> ▪ https://sub1.domain.com ▪ http://sub2.domain.com 	

Threat Emulation, Threat Extraction, and Zero-Phishing Exclusions

You can exclude:

- Domains
- SHA1 hashes from Threat Emulation and Threat Extraction

Domain exclusions

- 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	<ul style="list-style-type: none"> ▪ https://www.domain.com ▪ http://www.domain.com 	<ul style="list-style-type: none"> ▪ https://domain.com ▪ http://domain.com ▪ https://sub.domain.com ▪ http://sub.domain.com
domain.com	<ul style="list-style-type: none"> ▪ 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
sub.domain.com	<ul style="list-style-type: none"> https://sub.domain.com http://sub.domain.com 	https://sub2.domain.com
*.domain.com	Sub-domain of domain.com such as: <ul style="list-style-type: none"> https://sub1.domain.com http://sub2.domain.com 	

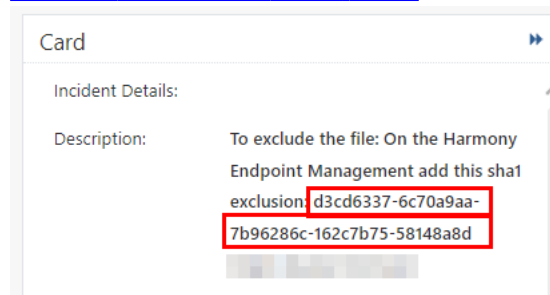
SHA1 exclusions -

- It is not supported with Internet Explorer.
- 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](#).



- Excludes downloaded files from [File Protection](#).
- Excludes local HTML files from [Zero Phishing](#).

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:

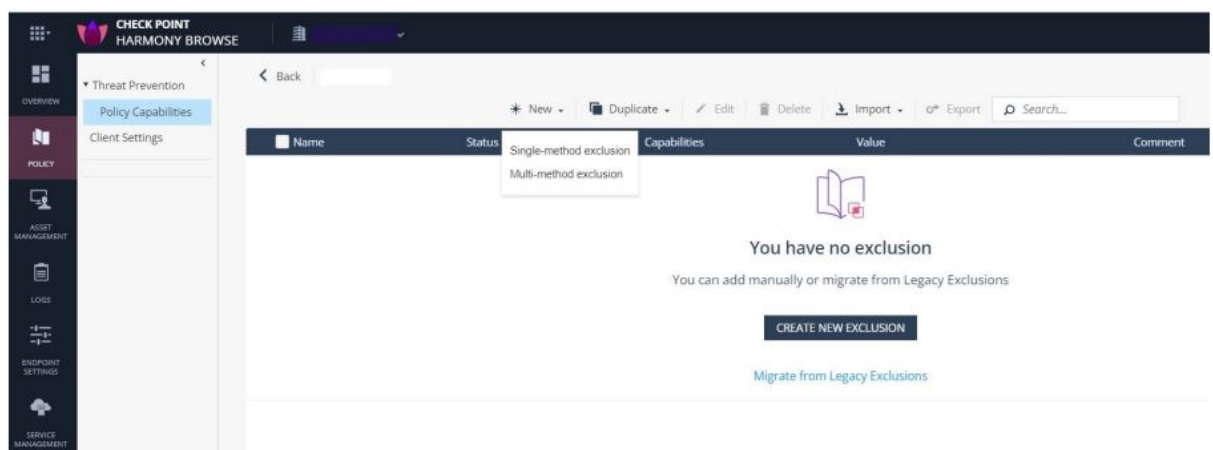
- Set exclusions to all capabilities and operating systems at once.
- Use standard syntax across all exclusion types.
- Use wider range of wildcard characters for nuanced and customized exclusion patterns.
- Easily enable or disable exclusions with a simple toggle button without the need to delete exclusions temporarily.

Adding Exclusions to a Specific Rule



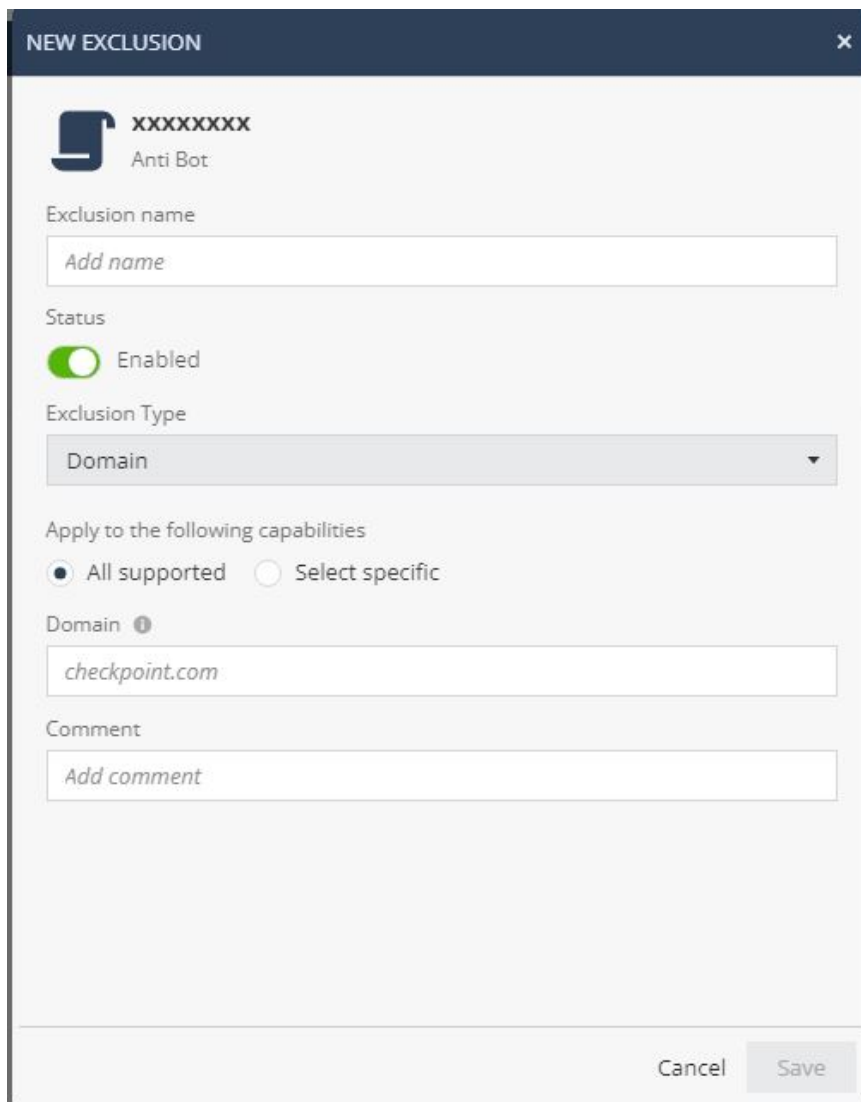
To add a new exclusion to a specific rule:

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 the following fields and options:

- Exclusion name:** A text input field containing the placeholder text 'Add name'.
- Status:** A toggle switch labeled 'Enabled', which is currently turned on.
- Exclusion Type:** A dropdown menu currently set to 'Domain'.
- Apply to the following capabilities:** Two radio buttons: 'All supported' (selected) and 'Select specific'.
- Domain:** A text input field containing the placeholder text 'checkpoint.com'.
- Comment:** A text input field containing 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
File hash	<p>a. From the File hash type list, select the hash type:</p> <ul style="list-style-type: none"> ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) <p>b. In the File hash value, enter the value.</p>
IP Range	<p>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.</p>
Url	In the URL field, enter the URL.
Domain	In the Domain field, enter the domain. For example, checkpoint.com.

- 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.

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. *"Smart Exclusions" on page 81*


 **Notes:**

- Capabilities not relevant to the selected group are not available.
- Anti-Exploit capability supports only **Process path** and **Infection/Protection** exclusions.

g. (Optional) In the **Comment** field, enter comments.

h. Click **Next**.

 **Note** - For supported syntax and capabilities for exclusion types, see [sk181679](#).

If the Exclusion Group is	Exclusion Type	Then
System	Process path	<p>a. In the Process path field, enter the path of the process. For example, C:\windows\system\cmd.exe.</p> <p>b. To specify additional criteria, expand Process path options, and select:</p> <ul style="list-style-type: none"> ▪ Case sensitive ▪ Trusted process ▪ Argument and if required, select Regex, and in the Argument value field, enter the value.
	Process original name ¹	<p>Enter the process original name. For example, Cmd.exe. Supported only for Windows-based endpoints.</p> <p> Notes -</p> <ul style="list-style-type: none"> ▪ To find the original name of the process: <ul style="list-style-type: none"> i. Right-click on the executable file. ii. Go to Properties > Details > Original filename. ▪ Process original name is case-sensitive.
	Process hash	<p>a. From the Process hash type list, select the hash type:</p> <ul style="list-style-type: none"> ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) <p>b. In the Process hash value, enter the value.</p>
	Process signer ¹	<p>In the Process signer value field, enter the process signer value. For example, Check Point Ltd.</p>

If the Exclusion Group is	Exclusion Type	Then
	File path	<ol style="list-style-type: none"> In the File path field, enter the path of the file. For example, C:\windows\system\. To specify additional criteria, expand File path options, and select Case sensitive.
	File hash	<ol style="list-style-type: none"> From the File hash type list, select the hash type: <ul style="list-style-type: none"> ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) 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
	Url	In the URL field, enter the URL.
	Domain	In the Domain field, enter the domain. For example, checkpoint.com.


¹ It is mandatory to provide either `Process original name` or the `Process signer` parameter. All the other parameters are optional.

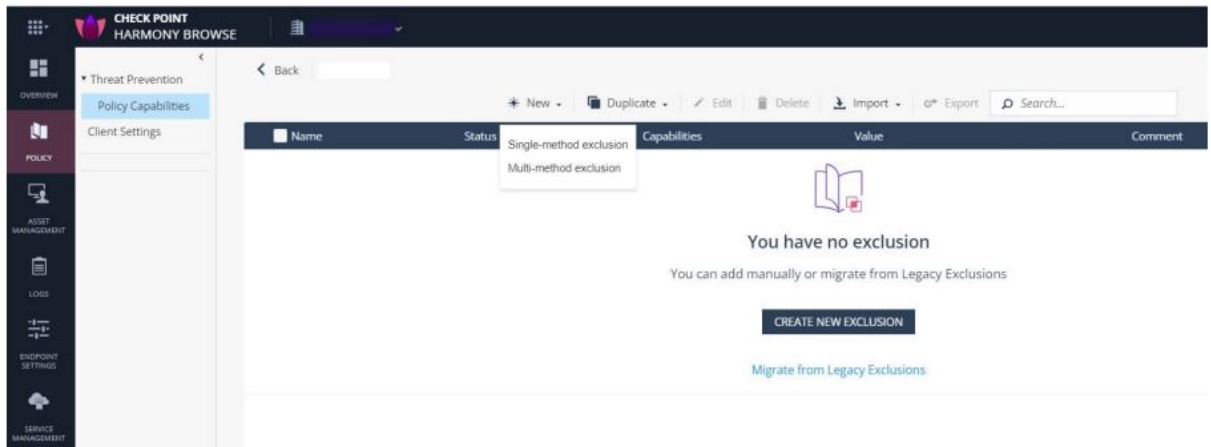
- i. Click **Finish**.
8. Click **OK**.
 9. Click **Save & Install**.

 **Note** - You can change **Single-method exclusion** to **Multi-method exclusion**. See [Managing Exclusions](#).

Adding Global Exclusions

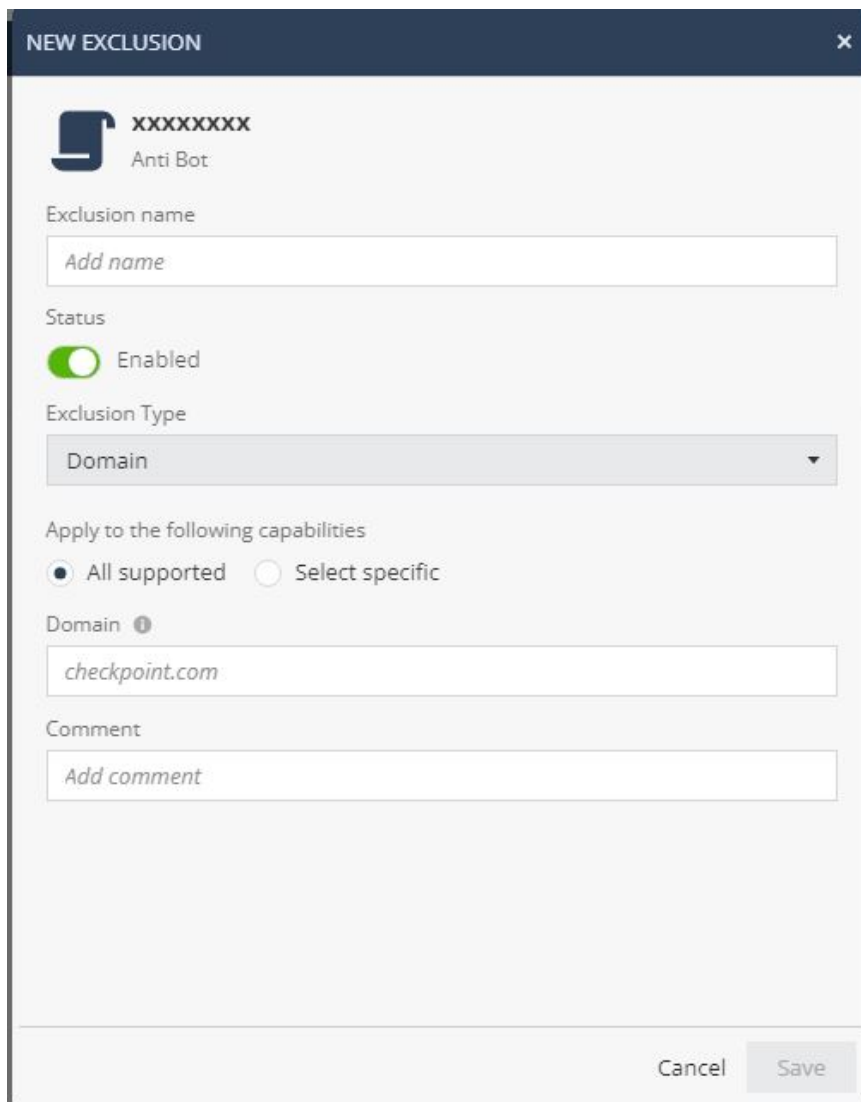
To add global exclusions that apply to all the rules:

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 the following fields and options:

- Exclusion name:** A text input field containing the placeholder text 'Add name'.
- Status:** A toggle switch labeled 'Enabled', which is currently turned on.
- Exclusion Type:** A dropdown menu with 'Domain' selected.
- Apply to the following capabilities:** Two radio buttons: 'All supported' (selected) and 'Select specific'.
- Domain:** A text input field containing 'checkpoint.com'.
- Comment:** A text input field containing 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
File hash	<p>a. From the File hash type list, select the hash type:</p> <ul style="list-style-type: none"> ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) <p>b. In the File hash value, enter the value.</p>
IP Range	<p>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.</p>
Url	In the URL field, enter the URL.
Domain	In the Domain field, enter the domain. For example, checkpoint.com.

- 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.

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. ["Smart Exclusions" on page 81](#)


 **Notes:**

- Capabilities not relevant to the selected group are not available.
- Anti-Exploit capability supports only **Process path** and **Infection/Protection** exclusions.

g. (Optional) In the **Comment** field, enter comments.

h. Click **Next**.

 **Note** - For supported syntax and capabilities for exclusion types, see [sk181679](#).

If the Exclusion Group is	Exclusion Type	Then
System	Process path	<p>a. In the Process path field, enter the path of the process. For example, C:\windows\system\cmd.exe.</p> <p>b. To specify additional criteria, expand Process path options, and select:</p> <ul style="list-style-type: none"> ▪ Case sensitive ▪ Trusted process ▪ Argument and if required, select Regex, and in the Argument value field, enter the value.
	Process original name ¹	<p>Enter the process original name. For example, Cmd.exe. Supported only for Windows-based endpoints.</p> <p> Notes -</p> <ul style="list-style-type: none"> ▪ To find the original name of the process: <ul style="list-style-type: none"> i. Right-click on the executable file. ii. Go to Properties > Details > Original filename. ▪ Process original name is case-sensitive.
	Process hash	<p>a. From the Process hash type list, select the hash type:</p> <ul style="list-style-type: none"> ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) <p>b. In the Process hash value, enter the value.</p>
	Process signer ¹	<p>In the Process signer value field, enter the process signer value. For example, Check Point Ltd.</p>

If the Exclusion Group is	Exclusion Type	Then
	File path	<ol style="list-style-type: none"> In the File path field, enter the path of the file. For example, C:\windows\system\. To specify additional criteria, expand File path options, and select Case sensitive.
	File hash	<ol style="list-style-type: none"> From the File hash type list, select the hash type: <ul style="list-style-type: none"> ▪ MD5 ▪ SHA1 ▪ SHA2 ▪ cdhash (for macOS only) 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.

¹ It is mandatory to provide either `Process original name` or the `Process signer` parameter. All the other parameters are optional.


- Click **Finish**.

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 82](#) 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.

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	REG ADD HKLM\SOFTWARE\Policies\Mozilla\Firefox /v DisablePrivateBrowsing /t REG_DWORD /d 1

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

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

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	defaults write /Library/Preferences/org.mozilla.firefox DisablePrivateBrowsing -bool TRUE

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.

To disable	Run
BrowserGuest mode	<pre>defaults write com.microsoft.edge BrowserGuestModeEnabled -integer 0</pre>
InPrivate mode	<pre>defaults write com.microsoft.edge InPrivateModeAvailability -integer 1</pre>

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

You can enable Harmony Browse extension on your browser in Incognito or InPrivate mode.

To enable the Harmony Browse extension on Chrome in the Incognito mode:

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

To enable the Harmony Browse extension on Edge in the InPrivate mode:

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

To enable the Harmony Browse extension on Firefox in the InPrivate mode:

1. In your browser's address bar, type `about:addons` and select **Extensions**.
2. Click the **Harmony Browse 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 Harmony Browse 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 and Files Protection" on page 57](#) .


Managing IoCs

Indicator of Compromise (IoC) is an indicator to cyber security professionals about an unusual activity or an attack. Harmony Browse allows you to add IoCs for domains, IP addresses, URLs, MD5 Hash keys and SHA1 Hash keys that are automatically blocked by File Protection (Threat Emulation and Threat Extraction) and URL Filtering without the need to install the policy.

Prerequisite

- For the IoCs domain, IP address and URL, activate (Prevent or Detect) the URL Filtering capability.
- For the IoCs MD5 Hash and SHA1 Hash, activate (Prevent or Detect) the Download Protection capability.

To add IoCs:

1. Click **Policy > Threat Prevention**.
2. Click **Manage IoCs**.
3. Click  .

The **New IoC** window appears.

4. Select a **Type** and enter a **Value** and **Comment** (optional).
5. Click **OK**.

The IoC is added to the table.

To import IoCs from an excel sheet:

You can import IoCs from an excel sheet containing up to 10000 entries in the format:

	A	B	C
1	Domain	checkpoint.com	This is your comment
2	IP	192.168.1.1	This is your comment
3	URL	http://checkpoint.com/test.htm	This is your comment
4	MD5	2eb040283b008eee17aa2988ece13152	This is your comment
5	SHA1	5c528ebc85c151361dc02ed08a25eb25f665fd8f	This is your comment
6	Domain	test.com	This is your comment
7	IP	192.168.1.2	This is your comment
8	URL	http://mytest.com/test.htm	This is your comment
9	MD5	2eb040283b008eee17aa2988ece13153	This is your comment
10	SHA1	5c528ebc85c151361dc02ed08a25eb25f665fd8k	This is your comment

1. Click **Policy > Threat Prevention**.
2. Click **Manage IoCs**.
3. Click  .

The **Import IoCs** window appears.


4. Click **Upload** and select the excel sheet.

Note - The system verifies the entries in the excel and discards invalid entries.

5. Click **Import**.

The IoCs are added to the table.


To edit an IoC:

1. Click **Policy > Threat Prevention**.
2. Click **Manage IoCs**.
3. Select the IoC.
4. Click  .

The **Edit IoC** window appears.

5. Make the required changes.
6. Click **OK**.

To delete IoCs:

1. Click **Policy > Threat Prevention**.
2. Click **Manage IoCs**.
3. Select the IoCs.
4. Click  .

A prompt appears.

5. Click **OK**.

To export IoCs to an excel sheet:

1. Click **Policy > Threat Prevention**.
2. Click **Manage IoCs**.
3. Click  .

The system exports the IoCs to an excel sheet.

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:

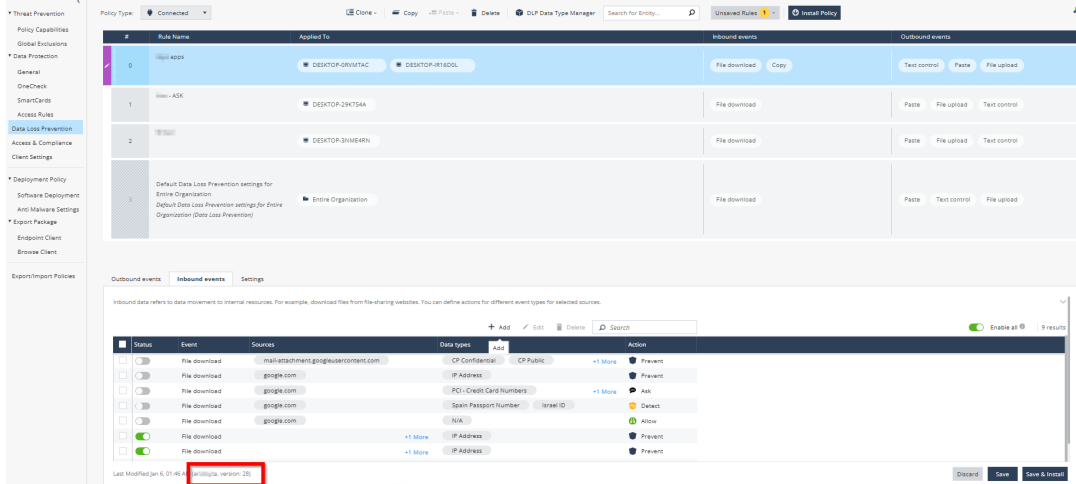
- **Detect** - Performs the DLP scan but does not block the data.
- **Prevent** - Performs the DLP scan and prevents data transfer if it finds a match to a data type.
- **Allow** - Acts as exclusions, allowing data transfer in certain events.

- **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.

The Data Loss Prevention tab allows the administrator to enable and install the Gen AI Protect feature on the endpoints. Gen AI Protect monitors the use of various Gen AI tools 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.

Notes:

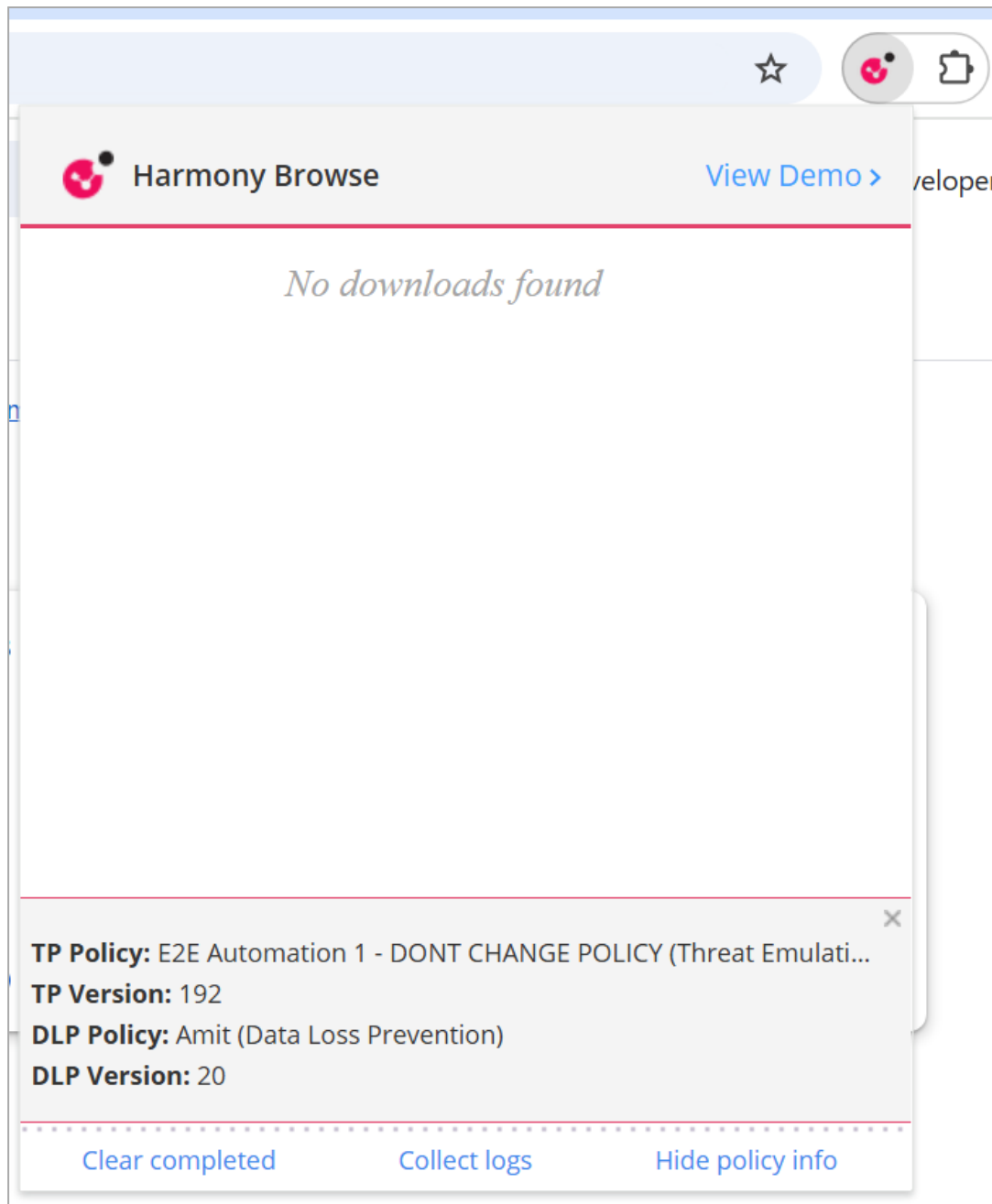
- You can find the policy version number in the bottom left corner of the page.



The screenshot displays the 'Data Loss Prevention' policy configuration. The 'Inbound events' section is active, showing a table of data types and their corresponding actions. The table includes columns for Status, Event, Sources, Data types, and Action. The 'Policy version: 02' is highlighted in a red box at the bottom left of the console.

Status	Event	Sources	Data types	Action
<input type="checkbox"/>	File download	mail-attachment.googleusercontent.com	CP Confidential, CP Public	Prevent
<input type="checkbox"/>	File download	google.com	IP Address	Prevent
<input type="checkbox"/>	File download	google.com	PCI - Credit Card Numbers	Ask
<input type="checkbox"/>	File download	google.com	Spain Passport Number, Israel ID	Detect
<input type="checkbox"/>	File download	google.com	N/A	Allow
<input type="checkbox"/>	File download		IP Address	Prevent
<input type="checkbox"/>	File download		IP Address	Prevent

- You can find both policy name and policy version number in the browser extension.



DLP Logs

- [Logs](#) are sent for **Block**, **Prevent**, **Detect**, and **Ask** 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 in EU and US regions only.
- 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.

Sample Data Type

For supported data and file types, see [sk181662](#).

The screenshot displays the 'DLP Data Type Manager' interface. On the left, a list of data types is shown, with 'Canada Passport Number' selected. The main panel shows the configuration for this data type, including its name, date modified, description, tags, type, matching threshold, where used, and groups. Red circles with numbers 1 through 14 highlight specific elements in the interface.

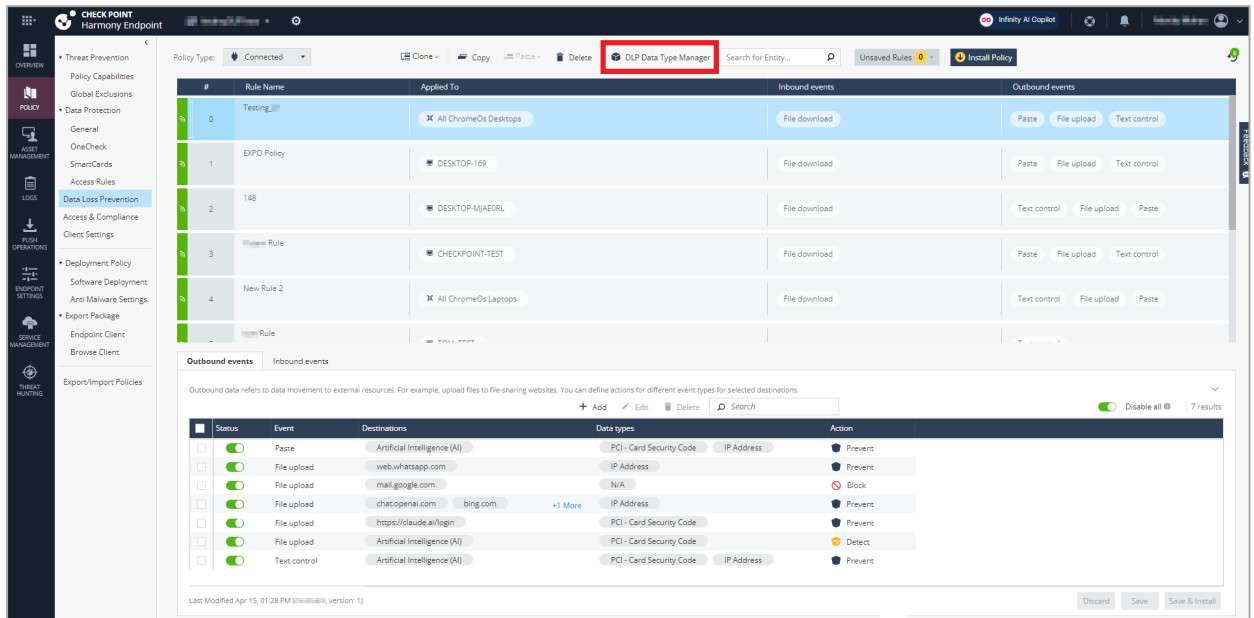
Legends	Description
1	Name of the data type.
2	Date and time (in MM/DD/YY, HH:MM:SS XM format) when the data type was last modified.
3	Brief description of the data type.

Legends	Description
4	Custom tags (category) for the data type. Helps in searching for data types.
5	Matching criteria: <ul style="list-style-type: none"> ▪ 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.
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.

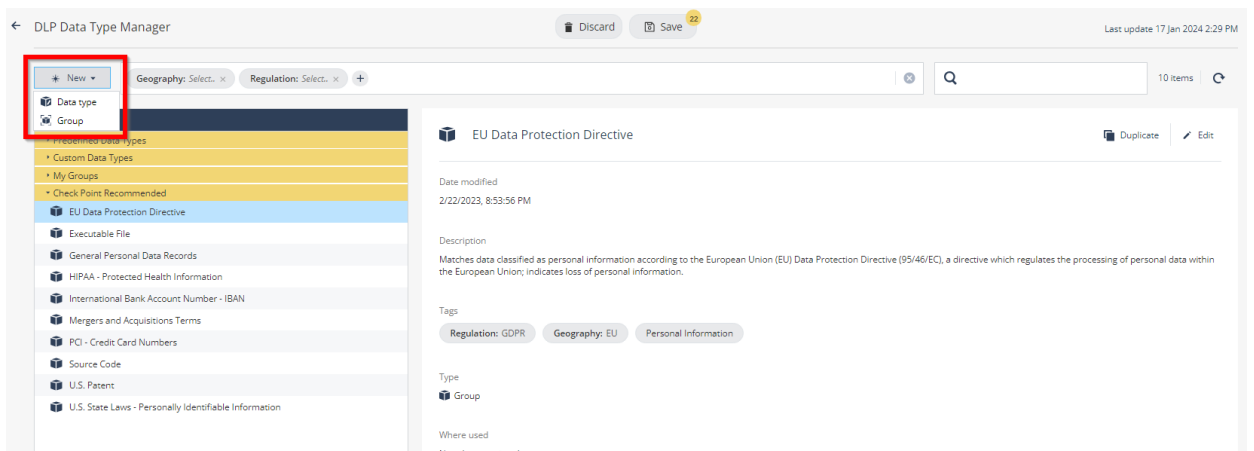
Creating a Custom Data Type

To create a custom data type:

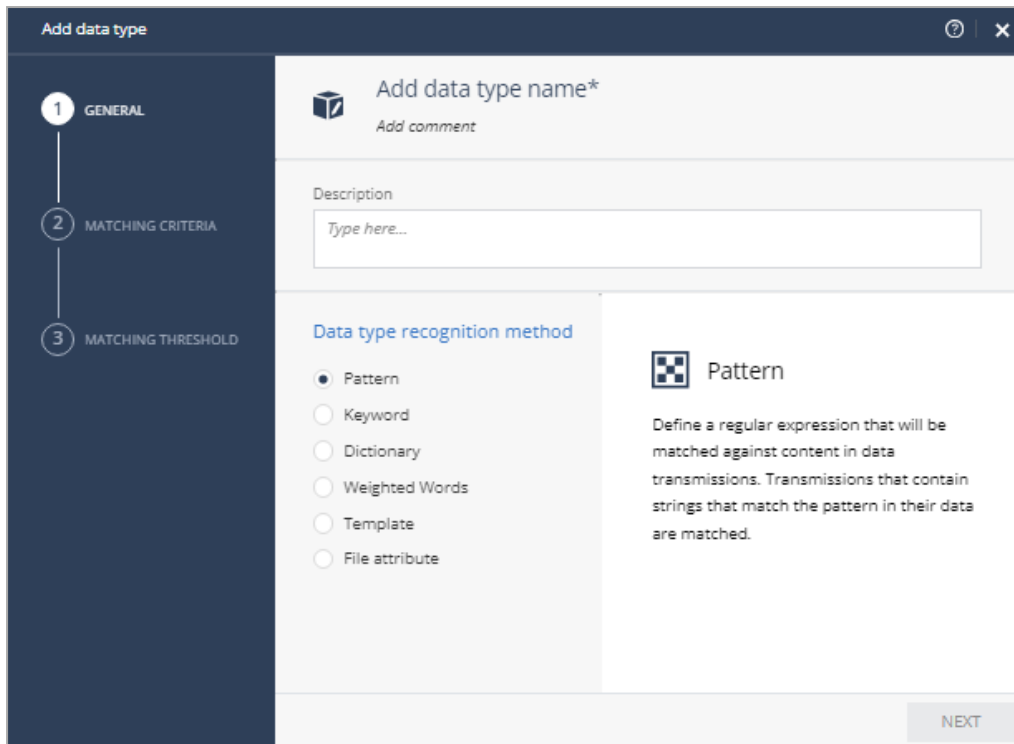
1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.



2. Click **New** and select **Data type**.

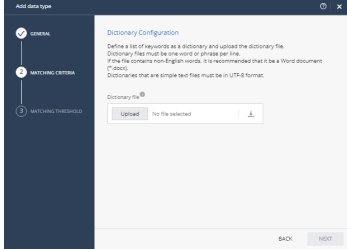


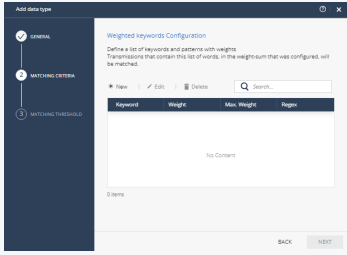
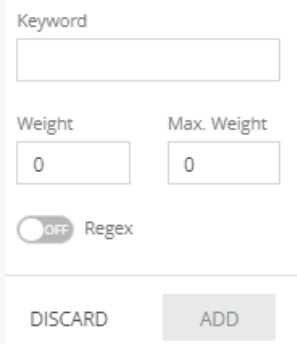
The **Add data type** wizard appears.

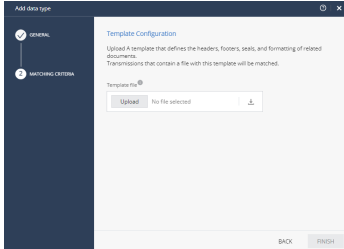
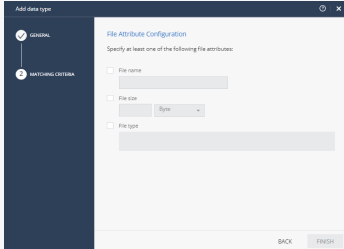


3. Enter the data type name, object comment (optional) and description.
4. From the **Data type recognition method** list, select a recognition method:

Recognition method	Description	Action
<p>Pattern</p>	<p>Applies the action specified in the policy capability rule if the file contents match the threshold for the pattern. For example, <i>5523-2342</i>.</p>	<p>In the Patterns section, enter the pattern and click +.</p>
<p>Keyword</p>	<p>Applies the action specified in the policy capability rule if the file contents match the threshold for the keyword. For example, <i>Confidential, Secret</i>.</p>	<p>In the Keywords section, enter the keywords and click +.</p>

Recognition method	Description	Action
<p>Dictionary</p> 	<p>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, China, United Kingdom</i>.</p> <p>Each keyword must be specified in a single line in the UTF-8 format.</p> <p>Note - The recommended file formats are Microsoft Word and <i>.txt</i>.</p>	<p>Upload the dictionary file.</p>

Recognition method	Description	Action
<p>Weighted Words</p> 	<p>Applies the action specified in the policy capability rule if the file contains keywords and the cumulative weight matches or exceeds the threshold.</p> <p>Use this method to specify multiple keywords.</p> <p>For example, consider two keywords:</p> <ul style="list-style-type: none"> ▪ credit with Weight=1 and Max. Weight=3 ▪ transaction with Weight=2 and Max. Weight=30 <p>and Matching Threshold=15.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<ol style="list-style-type: none"> a. Click New.  b. Enter these: <ul style="list-style-type: none"> ▪ 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.

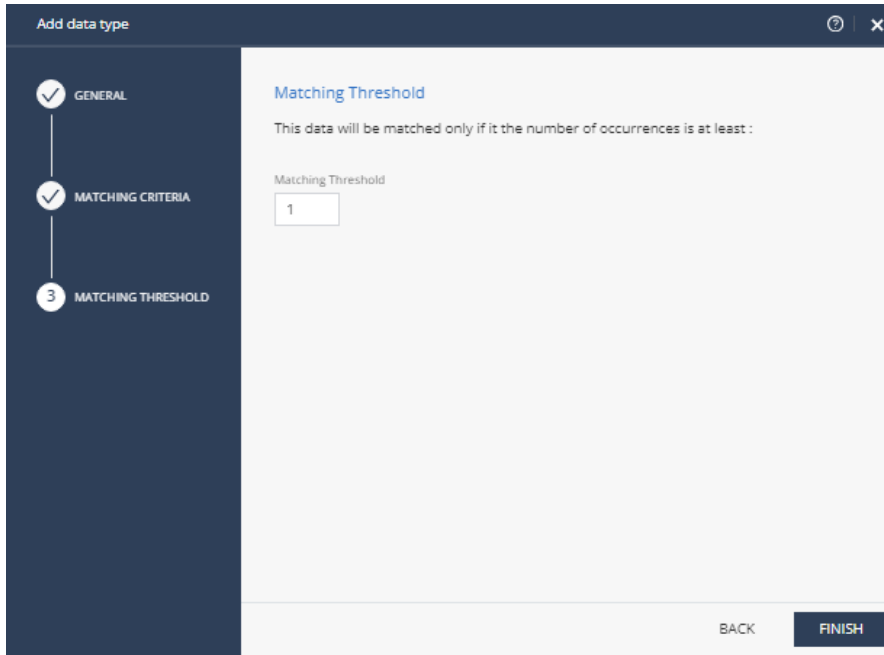
Recognition method	Description	Action
	<p>If the sum of the final weights of the keywords is less than the Matching Threshold, then the file is uploaded or downloaded.</p>	
<p>Template</p> 	<p>Applies the action specified in the policy capability rule if the file contents match the threshold for the terms in the template. For example, a template with a set header, footer and logo.</p> <p>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.</p>	<p>Upload the template file.</p>
<p>File attribute</p> 	<p>Applies the action specified in the policy capability rule if the file:</p> <ul style="list-style-type: none"> ■ Matches the specified file name. ■ Size is equal to or greater than the specified file size. ■ Type matches the specified file type. 	<p>Select any of these and enter a value:</p> <ul style="list-style-type: none"> ■ File name. For example, <i>Account Numbers, Employee Details</i>. ■ File size. File size in Byte, KB, MB or GB. ■ File type. <ul style="list-style-type: none"> • 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.



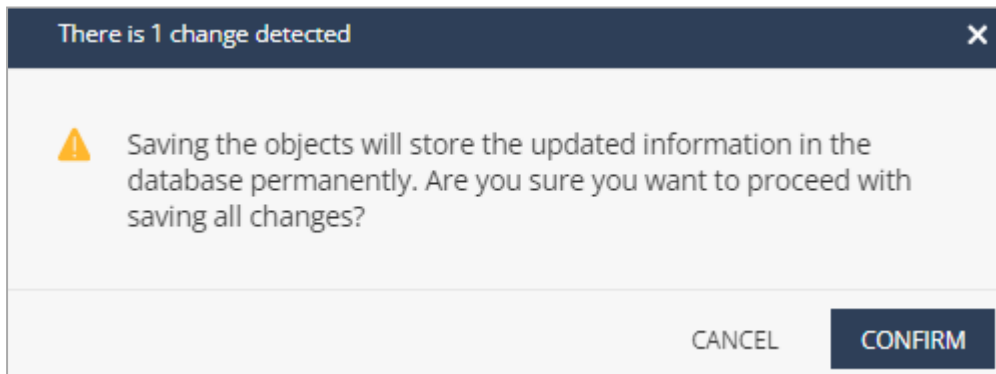
 **Note** - This step does not apply to **Template** and **File attribute** recognition methods.

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.

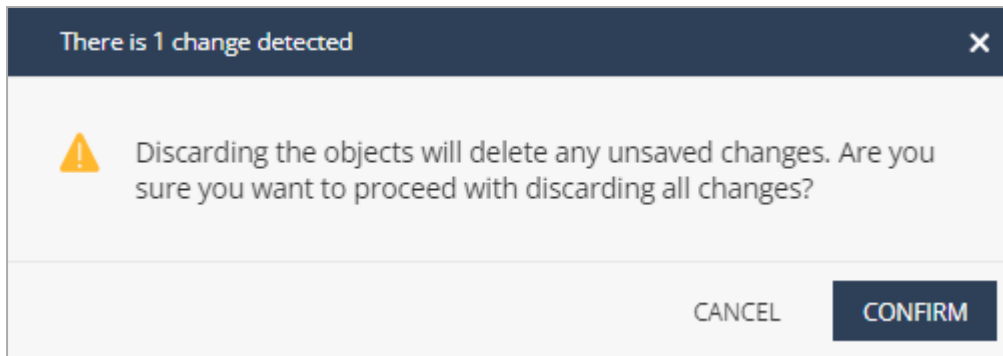
The **change detected** window appears.



9. Click **Confirm**.

10. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.

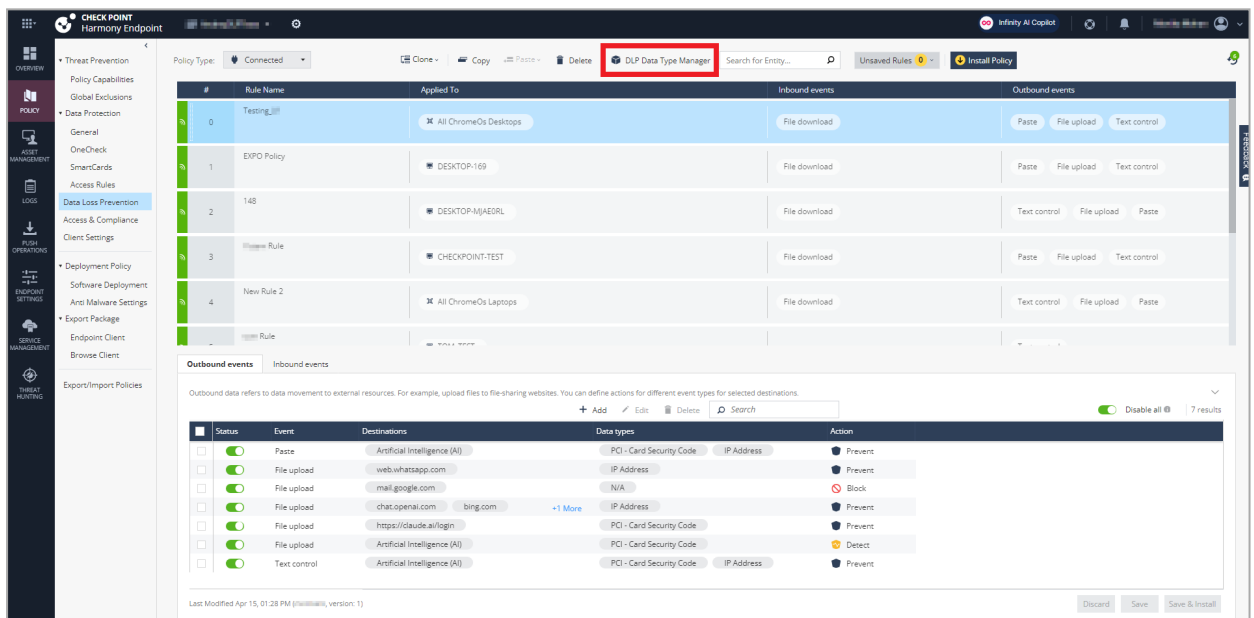


11. Click **Confirm**.

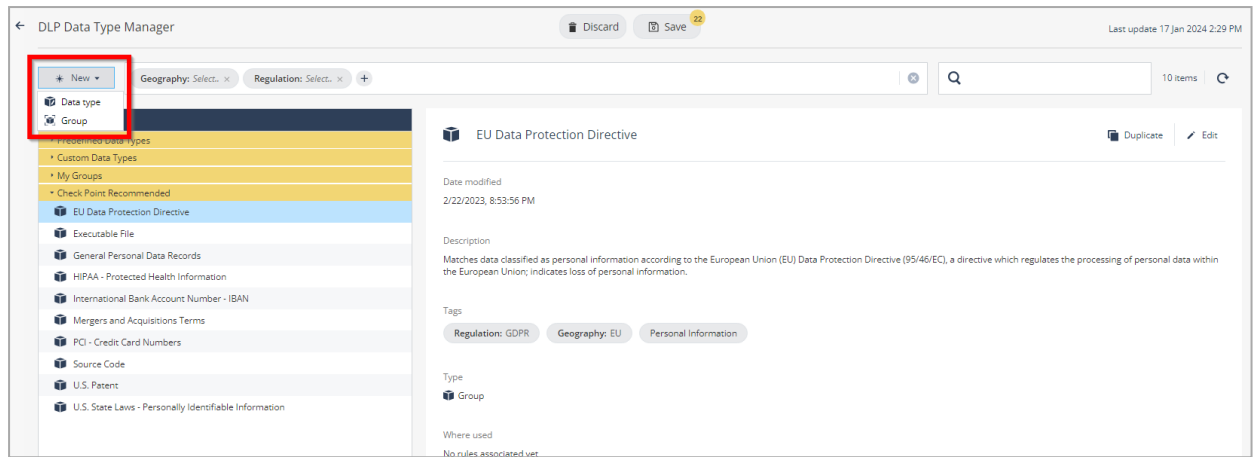
Creating a Custom Data Type Group

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**.



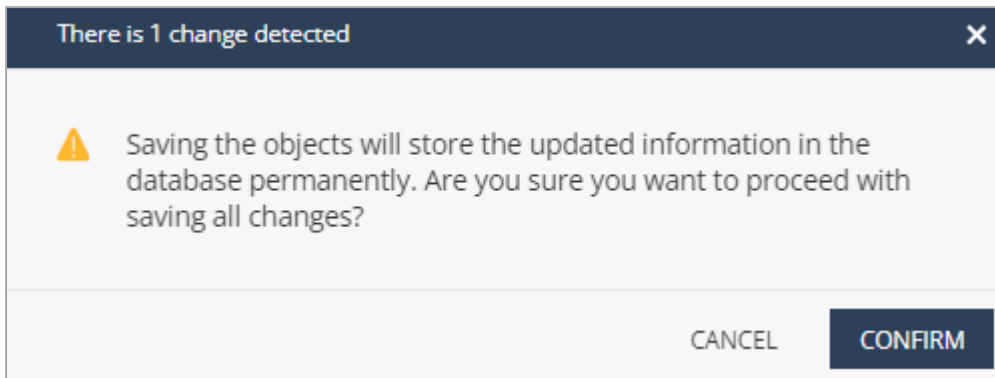
The **New Data type Group** window appears.

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**.

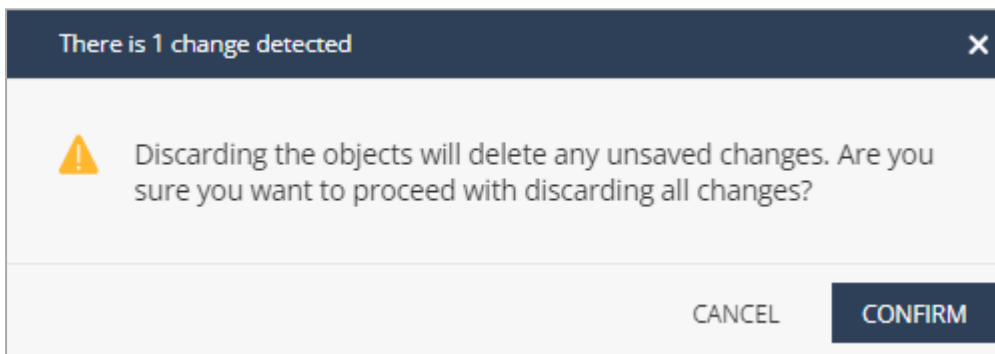
7. To permanently save all the changes to the database, click **Save** at the top.

The **change detected** window appears.



8. Click **Confirm**.
9. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.

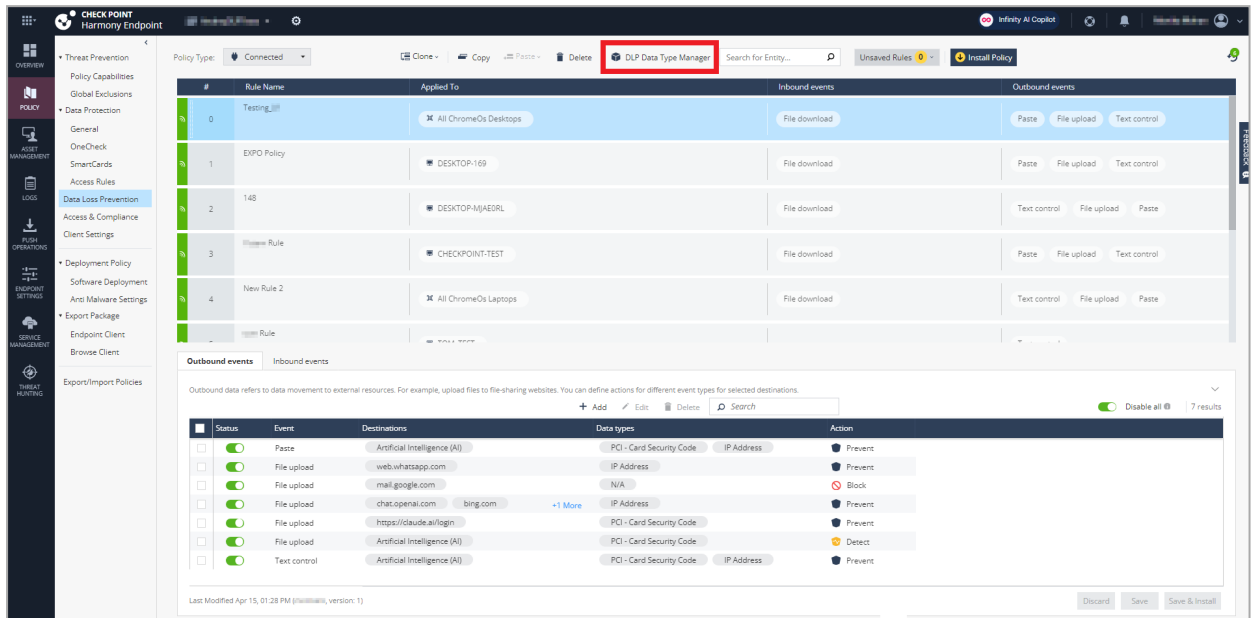


10. Click **Confirm**.

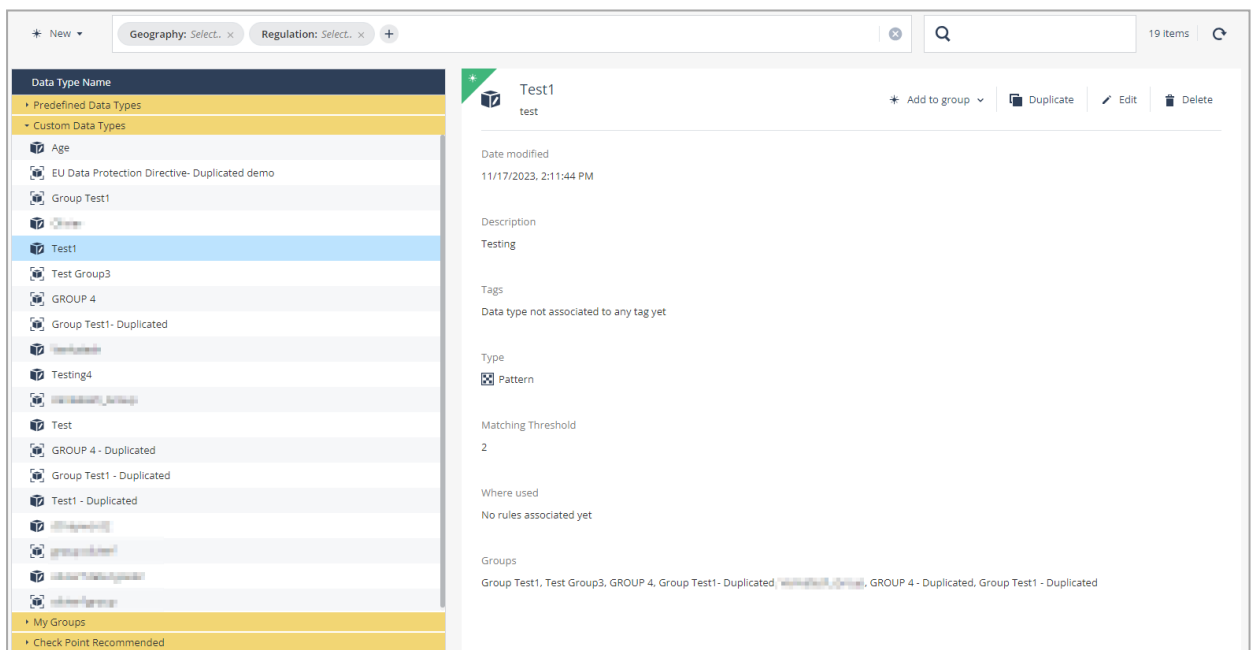
Adding an Existing Data Type to a Group

To add an existing data type to a group:

1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.



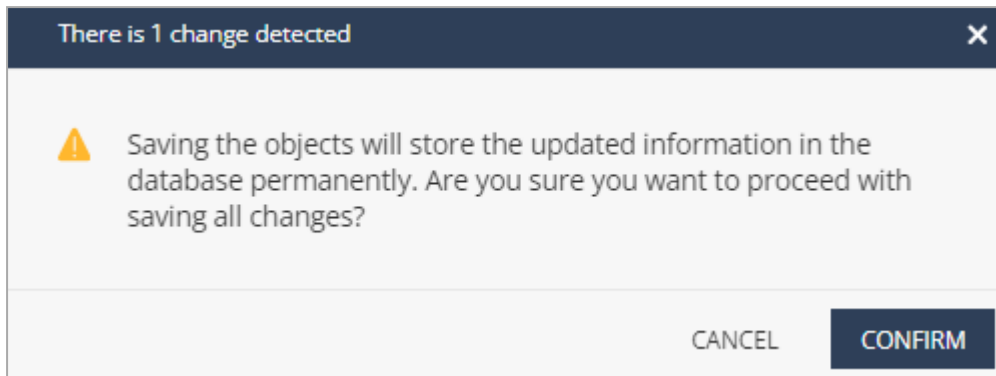
2. In the **Data Type Name** list, expand **Custom Data Types** or **Predefined Data Types** and select the data type.



3. Click **Add to group**.
4. Select the group(s) from the list.
5. Click **Add**.

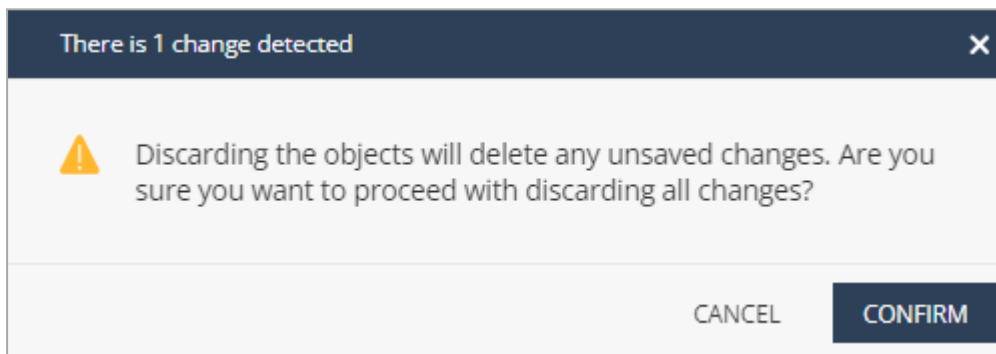
- To permanently save all the changes to the database, click **Save** at the top.

The **change detected** window appears.



- Click **Confirm**.
- To discard all the changes, click **Discard** at the top.

The **change detected** window appears.



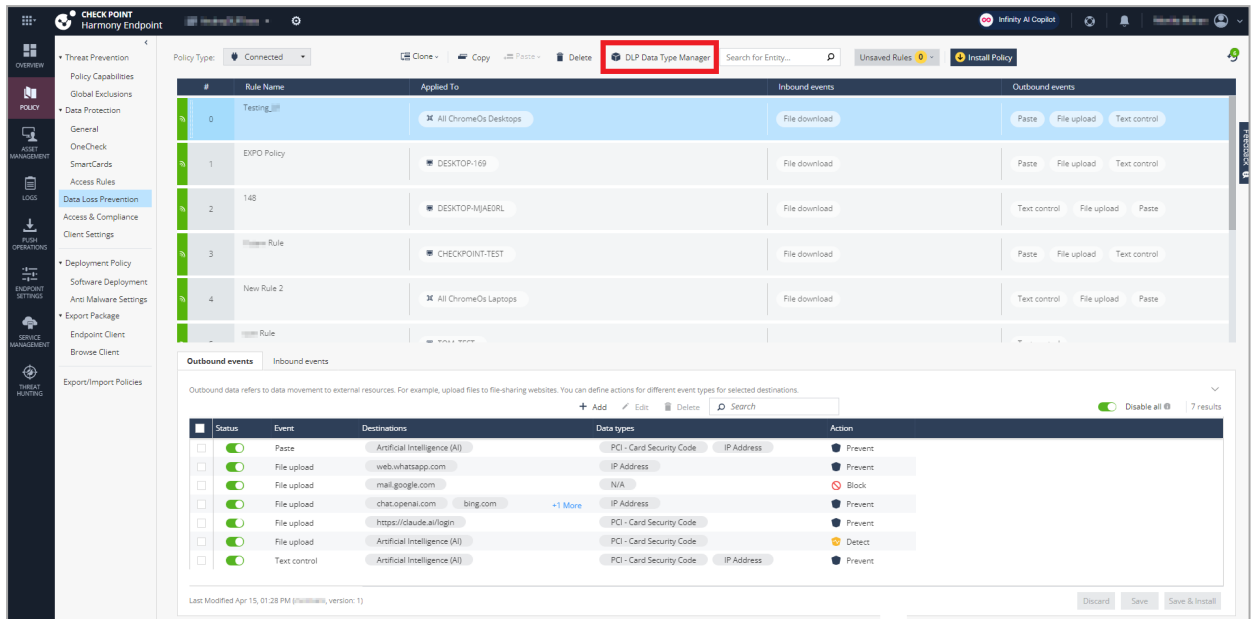
- Click **Confirm**.

Editing a Data Type or Group

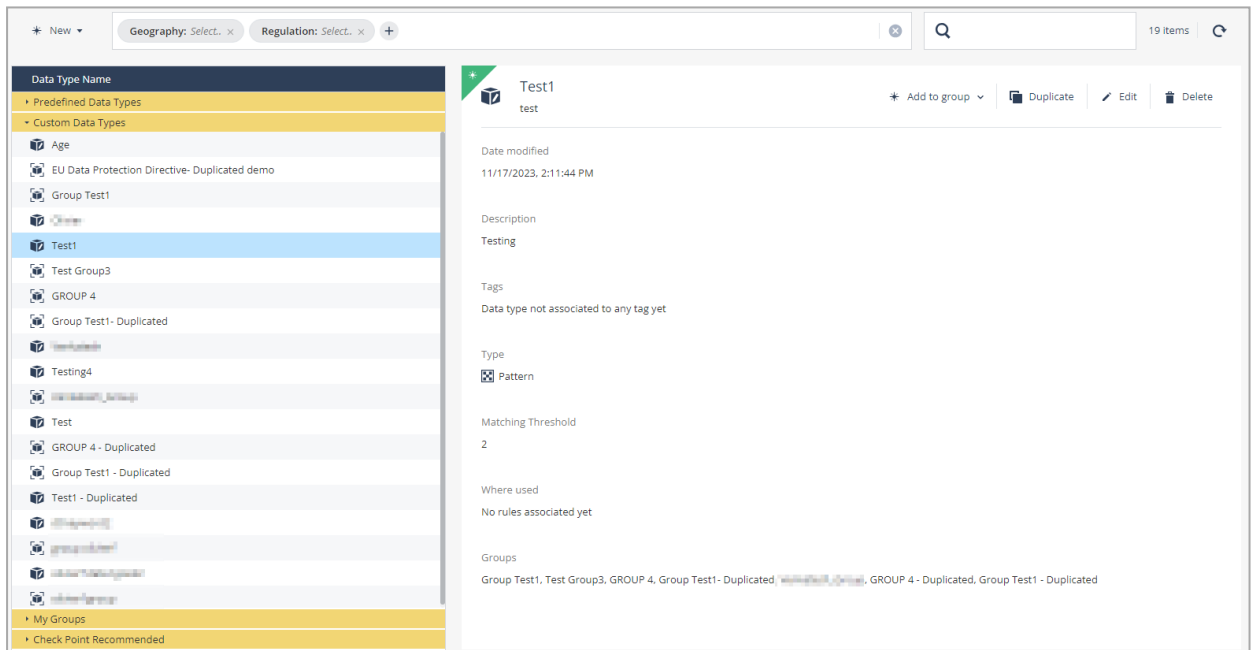
- Note** - If you edit a data type, the changes are reflected in all the groups that contain this data type.

To edit a data type or group:

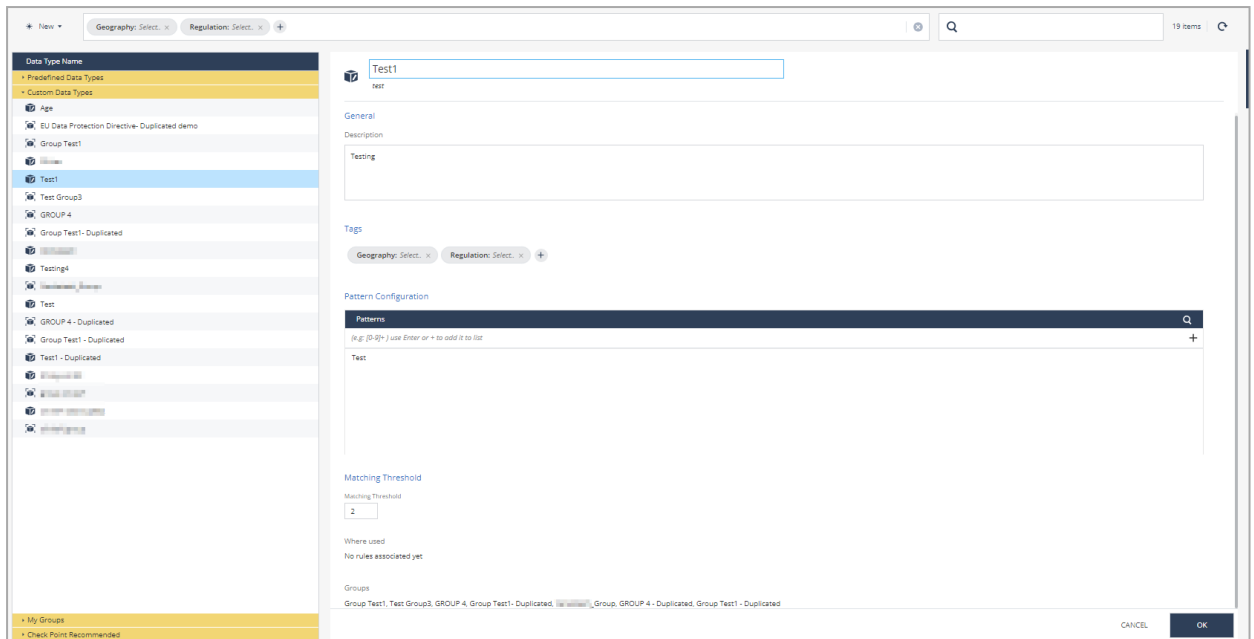
1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.



2. In the **Data Type Name** list, expand the DLP group and select the data type or the group.



3. Click **Edit**.



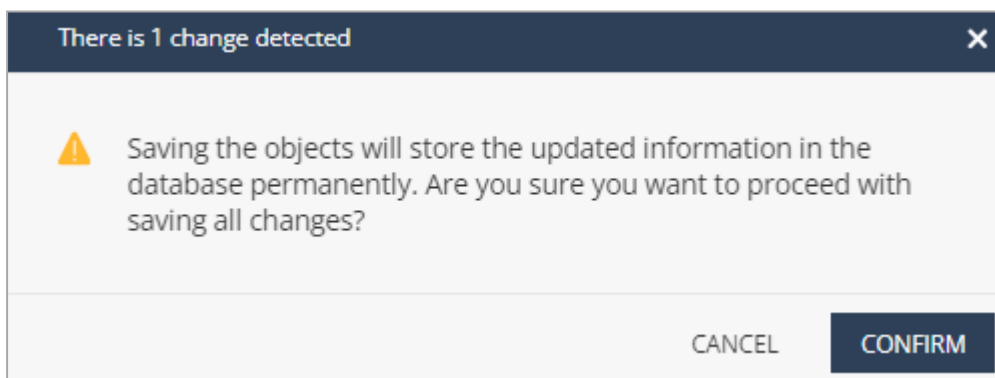
4. Make the required changes.

 **Note** - In the **Check Point Recommended** and **Predefined Data Types** DLP groups, you can edit only **Matching level** and **Add object comment**.

5. Click **OK**.

6. To permanently save all the changes to the database, click **Save** at the top.

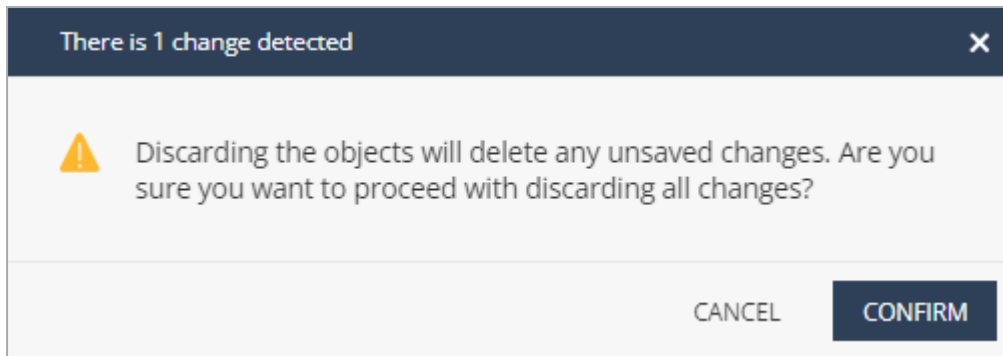
The **change detected** window appears.



7. Click **Confirm**.

8. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.

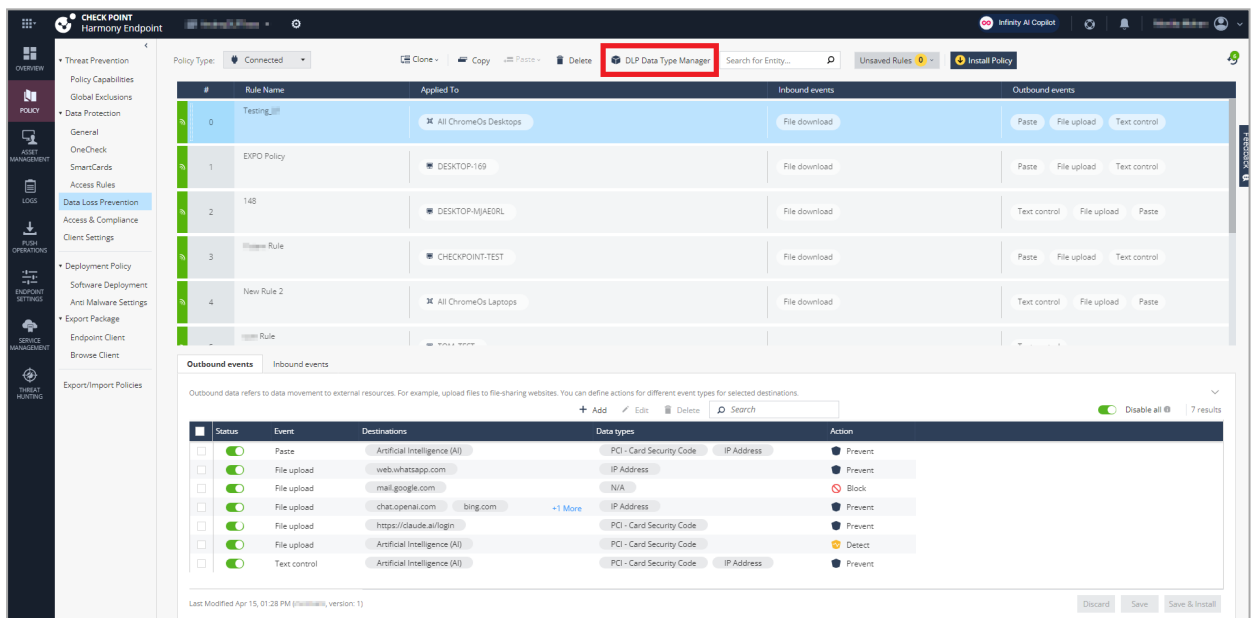


9. Click **Confirm**.

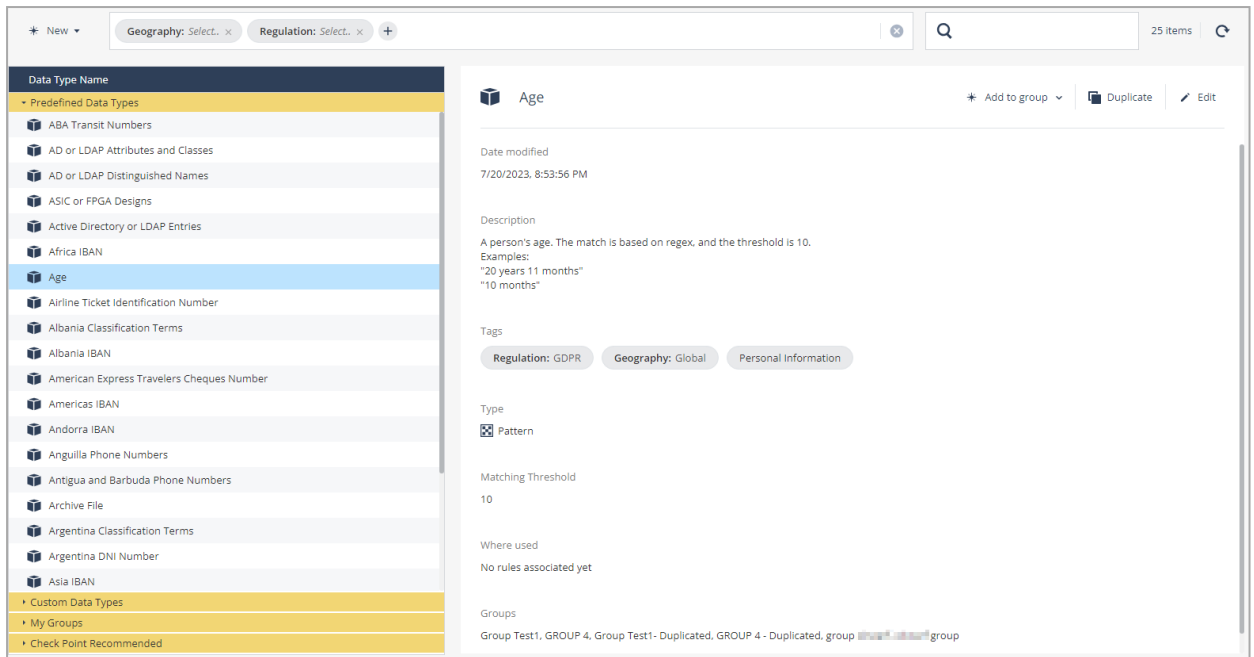
Duplicating a Data Type or a Group

To duplicate a data type or group:

1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.

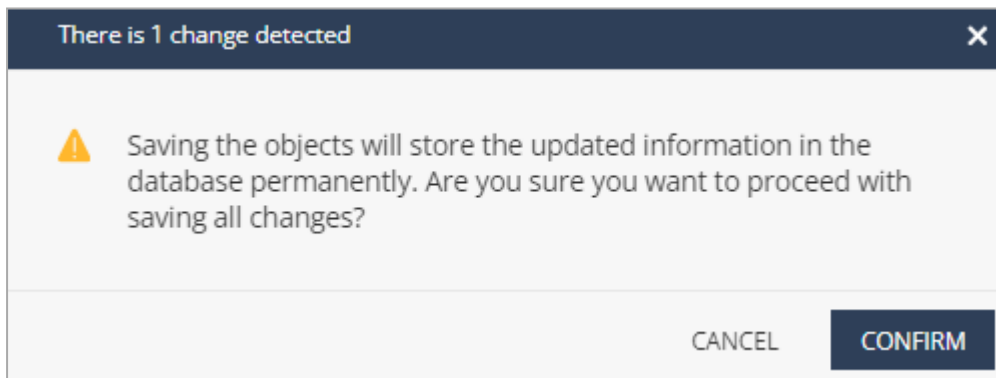


2. In the **Data Type Name** list, expand the DLP group and select the data type or the group within.



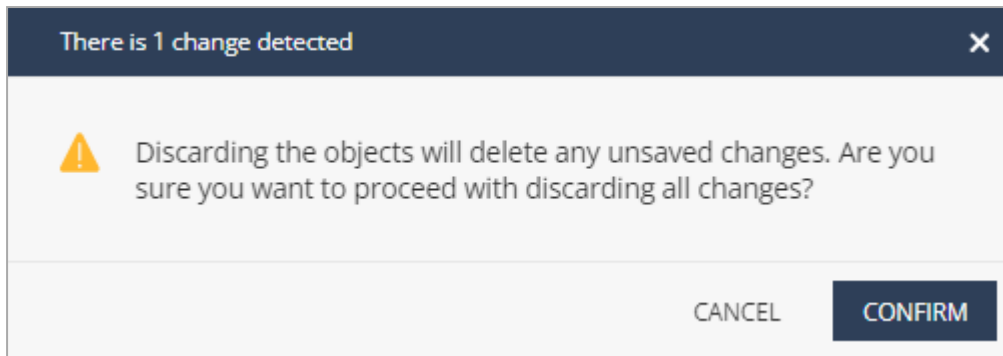
3. Click **Duplicate**.
4. Make the required changes.
5. Click **OK**.
6. To permanently save all the changes to the database, click **Save** at the top.

The **change detected** window appears.



7. Click **Confirm**.
8. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.



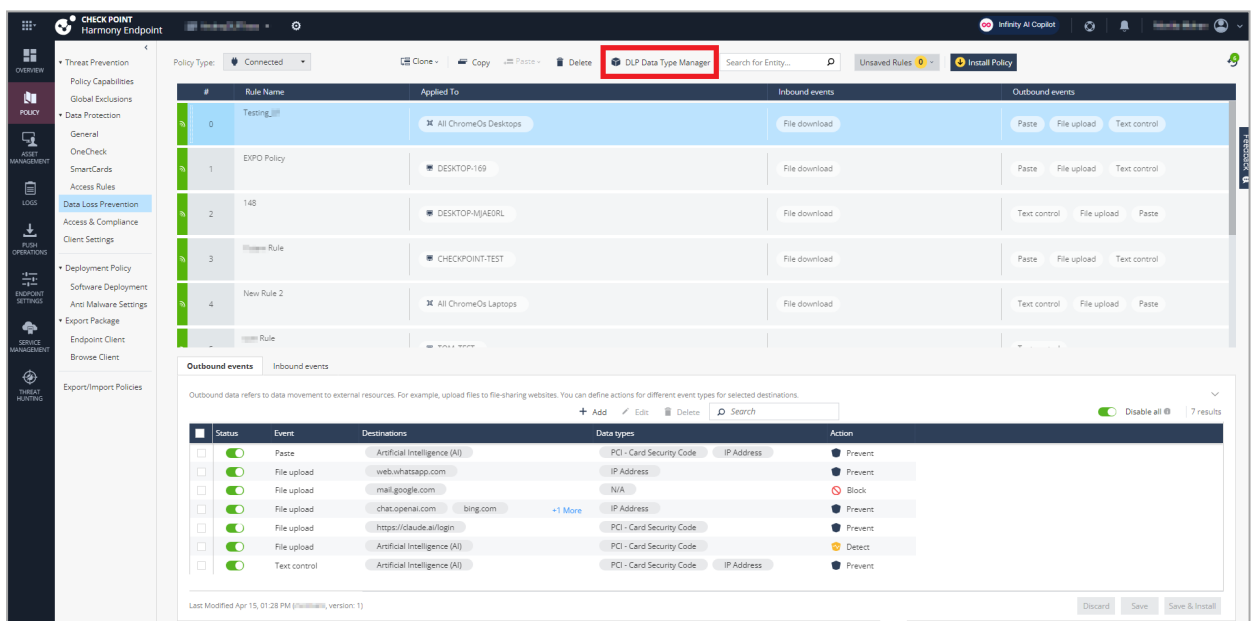
9. Click **Confirm**.

Deleting a Data Type or a Group

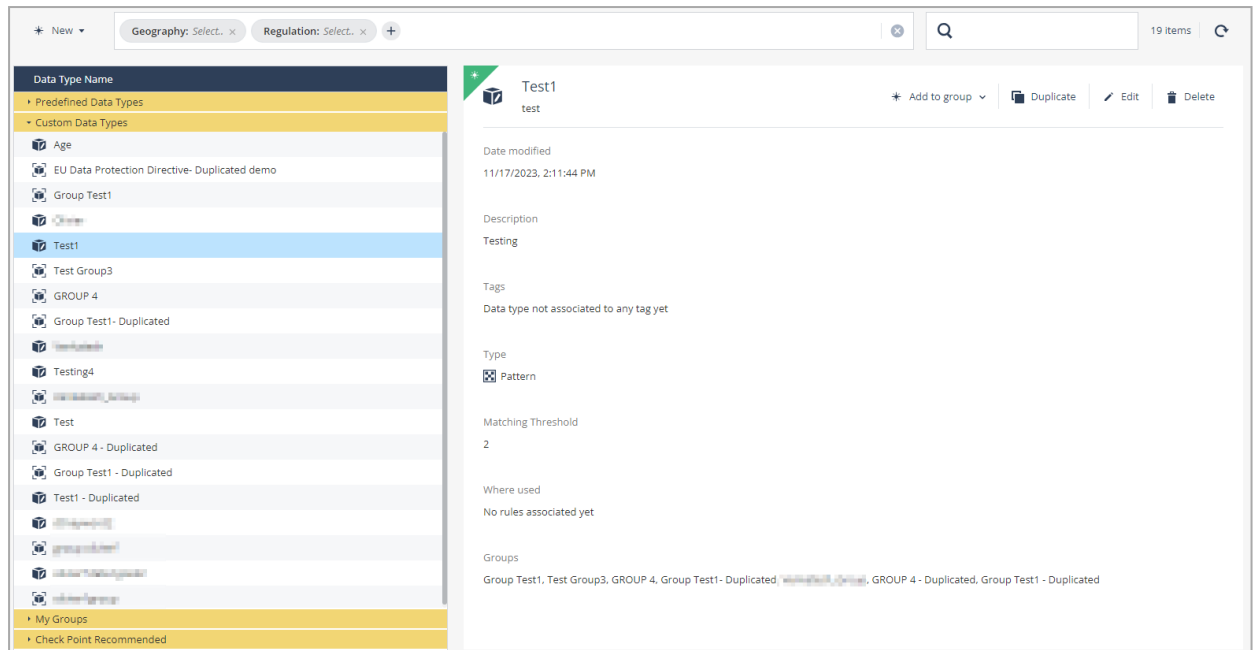
- Note** - Before you delete a data type, make sure to remove the data type from the group(s) and policy capability rules.

To delete a data type or group:

1. Go to **Policy > Data Loss Prevention** and click **DLP Data Type Manager**.

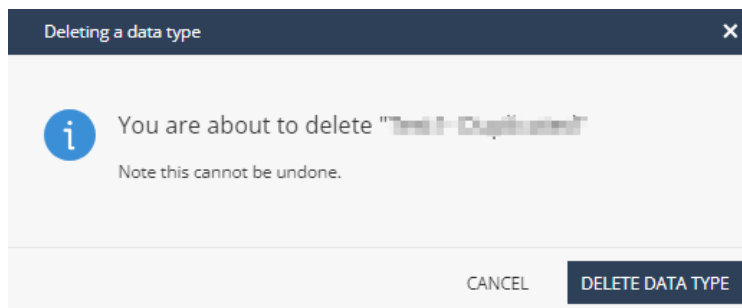


2. In the **Data Type Name** list, expand the DLP group and select the data type or the group within.



3. Click **Delete**.

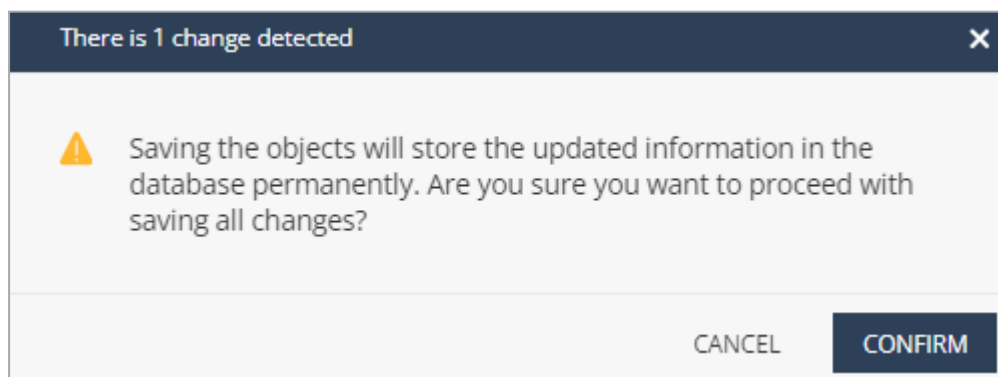
The **Deleting a data type** window appears.



4. Click **Delete Data Type**.

5. To permanently save all the changes to the database, click **Save** at the top.

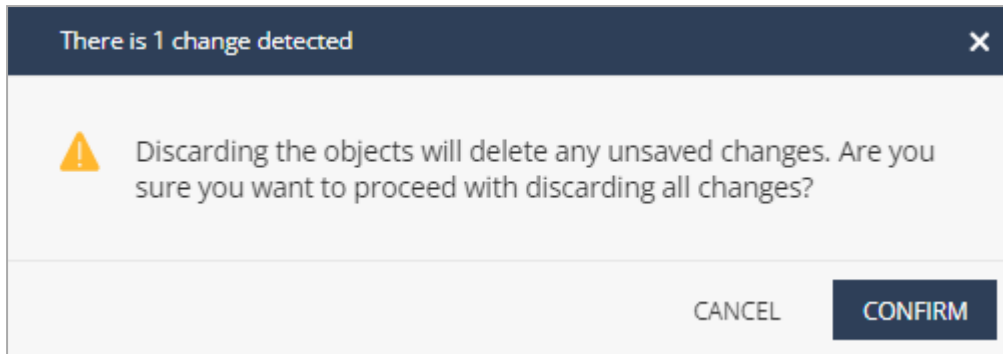
The **change detected** window appears.



6. Click **Confirm**.

7. To discard all the changes, click **Discard** at the top.

The **change detected** window appears.



8. Click **Confirm**.

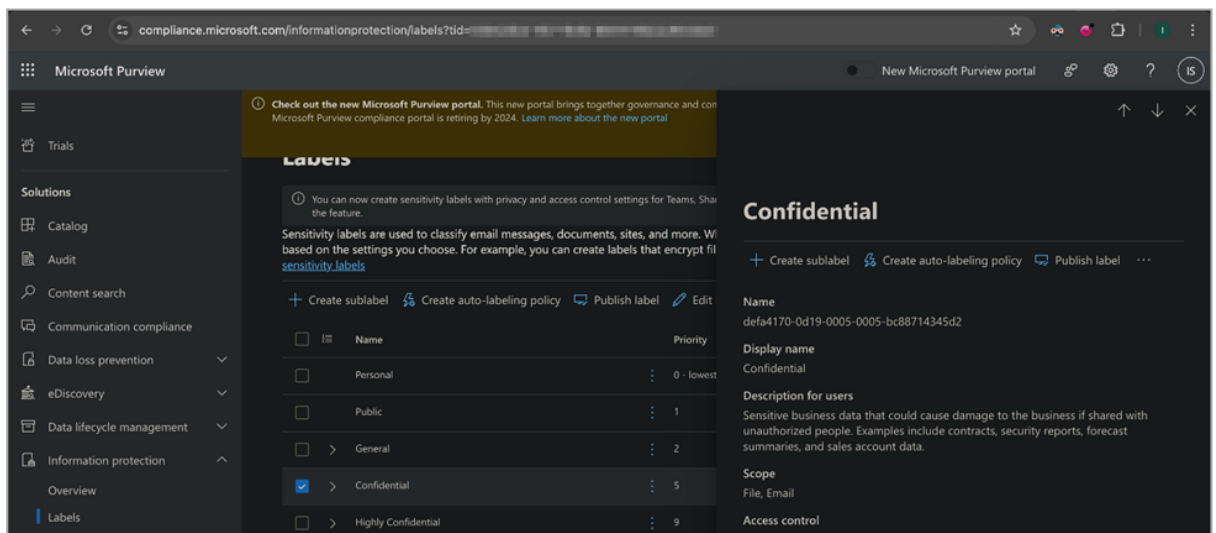
Managing Microsoft Sensitivity Labels for DLP

Harmony Browse 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-IPSSession
```

- 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
```

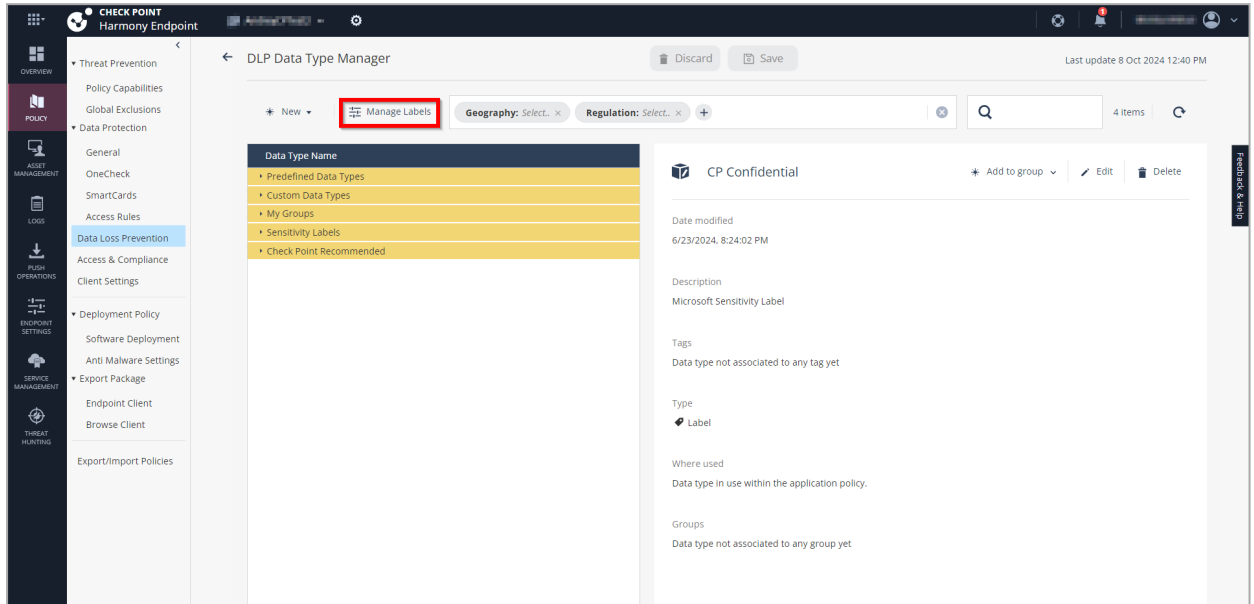
DisplayName	Name	Guid
Personal	defa170-8d19-0000-0000-bc8874345d2	defa170-8d19-0000-0000-bc8874345d2
Public	defa170-8d19-0000-0001-bc8874345d2	defa170-8d19-0000-0001-bc8874345d2
General	defa170-8d19-0000-0002-bc8874345d2	defa170-8d19-0000-0002-bc8874345d2
Unknown (unrestricted)	defa170-8d19-0000-0003-bc8874345d2	defa170-8d19-0000-0003-bc8874345d2
All Employees (unrestricted)	defa170-8d19-0000-0004-bc8874345d2	defa170-8d19-0000-0004-bc8874345d2
Out of Office	defa170-8d19-0000-0005-bc8874345d2	defa170-8d19-0000-0005-bc8874345d2
Unknown (unrestricted)	defa170-8d19-0000-0006-bc8874345d2	defa170-8d19-0000-0006-bc8874345d2
All Employees	defa170-8d19-0000-0007-bc8874345d2	defa170-8d19-0000-0007-bc8874345d2
Trusted People	defa170-8d19-0000-0008-bc8874345d2	defa170-8d19-0000-0008-bc8874345d2
Highly Confidential	defa170-8d19-0000-0009-bc8874345d2	defa170-8d19-0000-0009-bc8874345d2

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 Harmony Browse

1. Log in to Infinity Portal and access the Harmony Browse 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

🔍

Name	UUID
[?] Confidential	88479d74-8251-4268-b102-4d7459719631
[?] Public	2201f24c-4e01-41d0-b108-2f1401260100
[?] Restricted/Confidential	c1014715-4012-4128-b102-4d7459719631
[?] Top Secret	88479d74-8251-4268-b102-4d7459719631

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

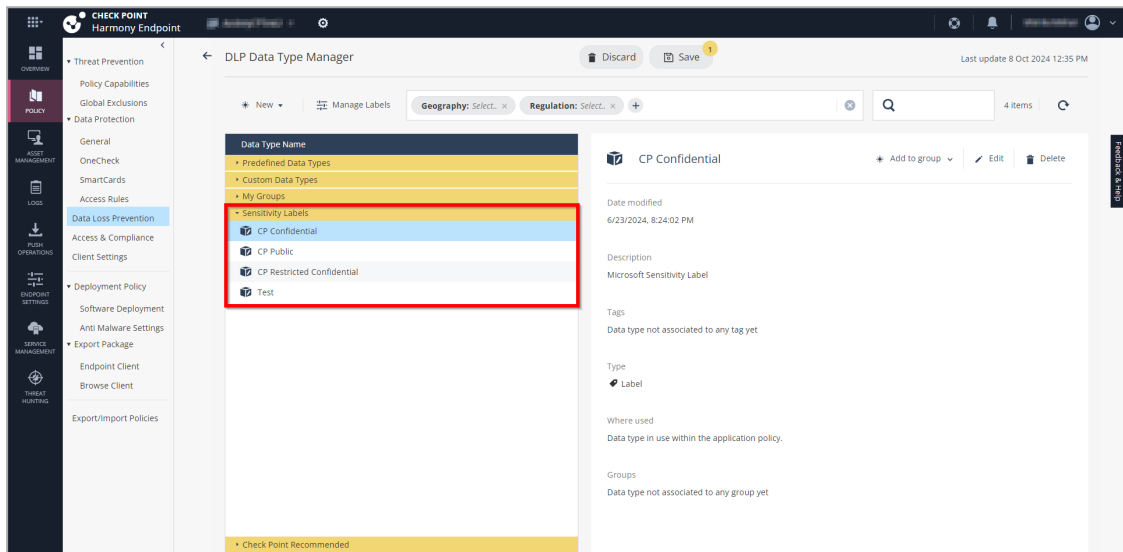
5. In the **Name** field, enter a name for the label. For example, MIP_EXAMPLE.
6. In the **UUID** field, enter the label UUID. For more information, see ["Step 1 - Copy the Microsoft Sensitivity label names and their UUIDs from Microsoft Purview"](#) on page 130.
7. Click **Add**.
8. Click **OK**.

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.



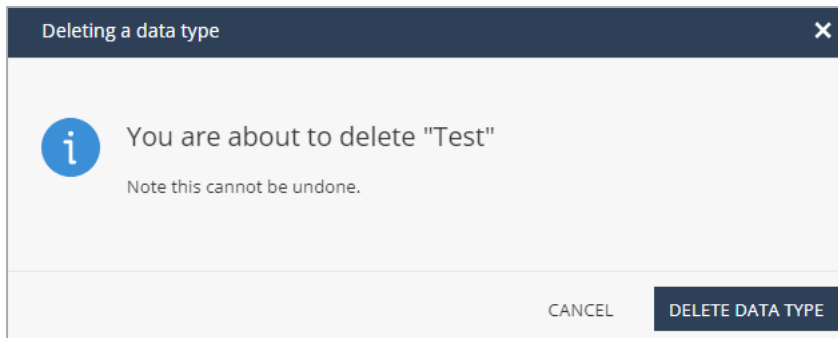
9. To edit a label, select the label you want to edit, click **Edit**, update the field and then click **Apply**.

Name

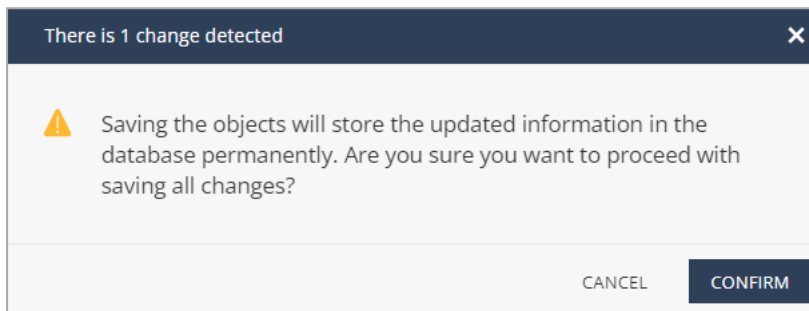
UUID

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

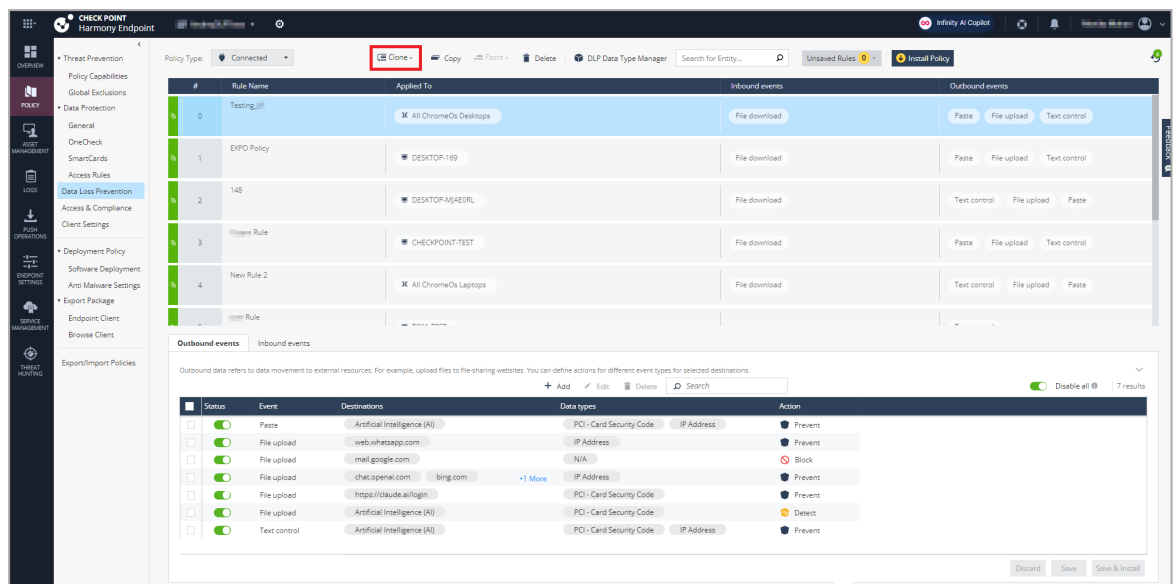
After creating Sensitivity labels in Harmony Browse, you must assign them to the DLP rules to enforce data protection based on these sensitivity labels.

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

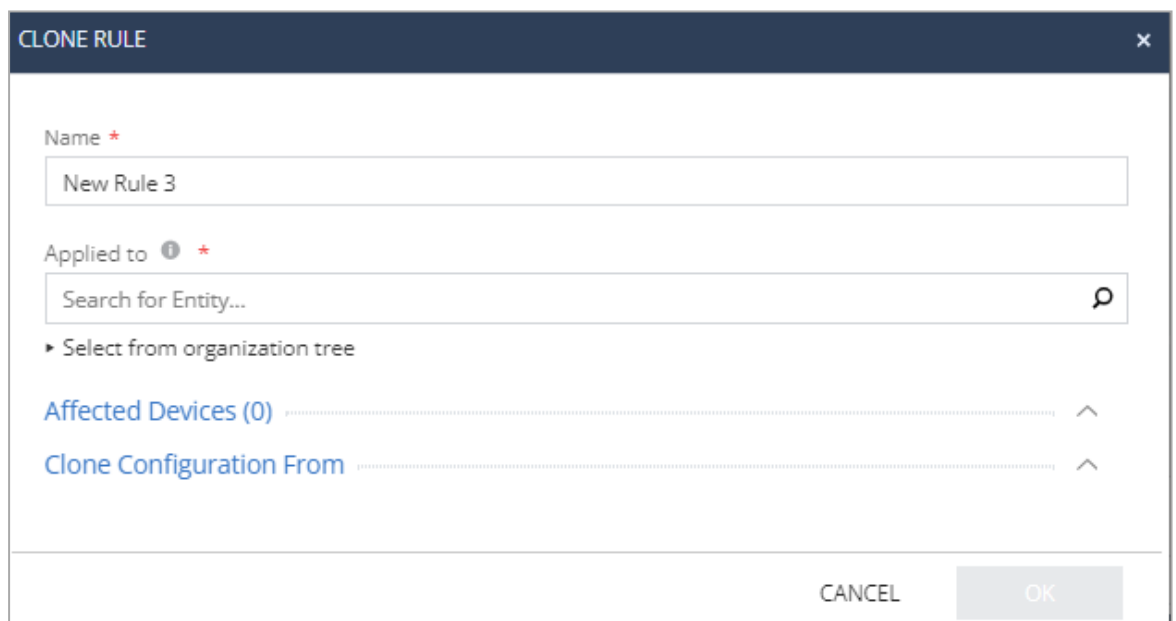
1. Go to **Policy > Data Loss Prevention**.
2. Add a rule:

- 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:

- a. Select the rule to which the Gen AI protection must be associated.
- b. From the list of tabs, select **Settings** tab.
- c. Select **Enable GenAI protect**.
- d. Click **Save & Install**, to apply the rule on the applicable endpoints.

4. Click one of these tabs:

- **Outbound events** - Outbound data refers to transferring content to external resources.

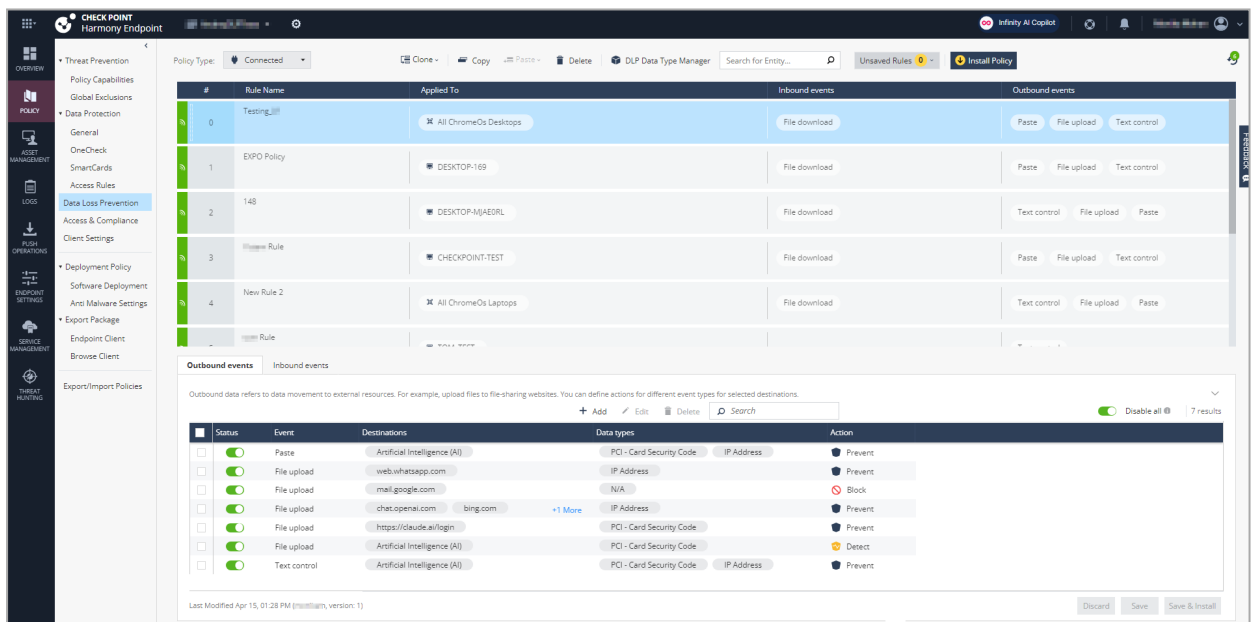
Examples:

- 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.



The screenshot shows the Checkpoint Harmony Endpoint console. The main window is titled "Data Protection - New Event" and displays a table of outbound events. The table has the following columns: Status, Event, Destinations, Data types, and Action. The table contains several rows of events, including Paste, File upload, and Text control, with various destinations and data types. The table is currently showing 7 results.

Status	Event	Destinations	Data types	Action
<input checked="" type="checkbox"/>	Paste	Artificial Intelligence (AI)	PCI - Card Security Code, IP Address	Prevent
<input checked="" type="checkbox"/>	File upload	web.whatsapp.com	IP Address	Prevent
<input checked="" type="checkbox"/>	File upload	mail.google.com	N/A	Block
<input checked="" type="checkbox"/>	File upload	chat.openai.com, bing.com	IP Address	Prevent
<input checked="" type="checkbox"/>	File upload	https://cloud.ai/login	PCI - Card Security Code	Prevent
<input checked="" type="checkbox"/>	File upload	Artificial Intelligence (AI)	PCI - Card Security Code	Detect
<input checked="" type="checkbox"/>	Text control	Artificial Intelligence (AI)	PCI - Card Security Code, IP Address	Prevent

5. Click **Add**.

The **Data Protection - New Event** window appears.

The screenshot shows the 'data protection - New event' configuration window. It includes the following fields and options:

- Status:** A toggle switch is turned 'On'.
- Event type:** A dropdown menu is set to 'File upload'.
- Destination type:** A dropdown menu is set to 'Category'.
- Categories & sub categories:** A search bar contains 'Security', with a close button and a dropdown arrow.
- Action:** A dropdown menu is set to 'Prevent'.
- Data types:** A search bar with a magnifying glass icon and the text 'Search' is present. Below it, a list shows '1 Results' with a header 'Data types' and one entry: 'Age-Duplicated'.
- Buttons:** 'Cancel' and 'Save' buttons are located at the bottom right.

- By default, the event is enabled. To disable, turn off the **Status** toggle button.
- 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	<ul style="list-style-type: none"> ▪ File upload ▪ File download ▪ Copy 	In the URL field, enter the web addresses to which you want to apply the rule.
Application	<ul style="list-style-type: none"> ▪ Text control ▪ Paste 	In the Applications field, select the application(s) to which you want to apply the rule.
Domain	<ul style="list-style-type: none"> ▪ File upload ▪ File download ▪ Copy 	In the Domain field, enter the domain to which you want to apply the rule.
Category	<ul style="list-style-type: none"> ▪ 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:

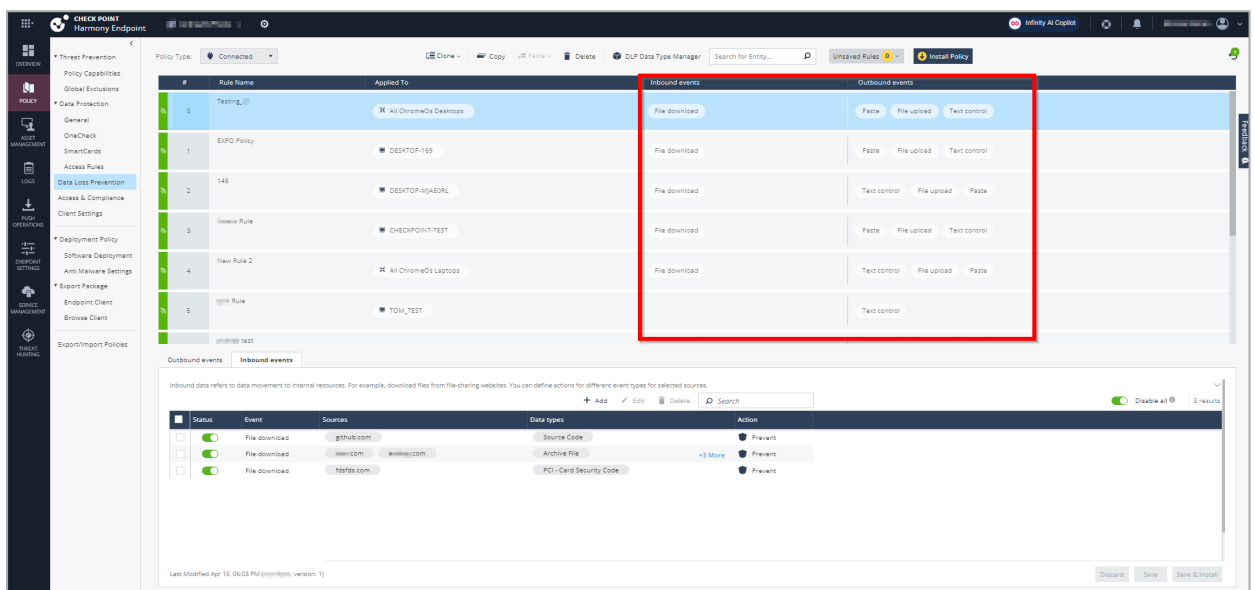
- **Detect** - Performs the DLP scan but does not block the data.
- **Prevent** - Performs the DLP scan and prevents data transfer if it finds a match to a data type.
- **Allow** - Acts as exclusions, allowing data transfer in certain events.
- **Block** - Blocks the data without the DLP scan.

- **Ask** - Asks the user to provide justification before allowing data transfer based on the DLP scan results.
10. To associate data types with an event, in the **Data types** section, click **+** and select the data type or a group.

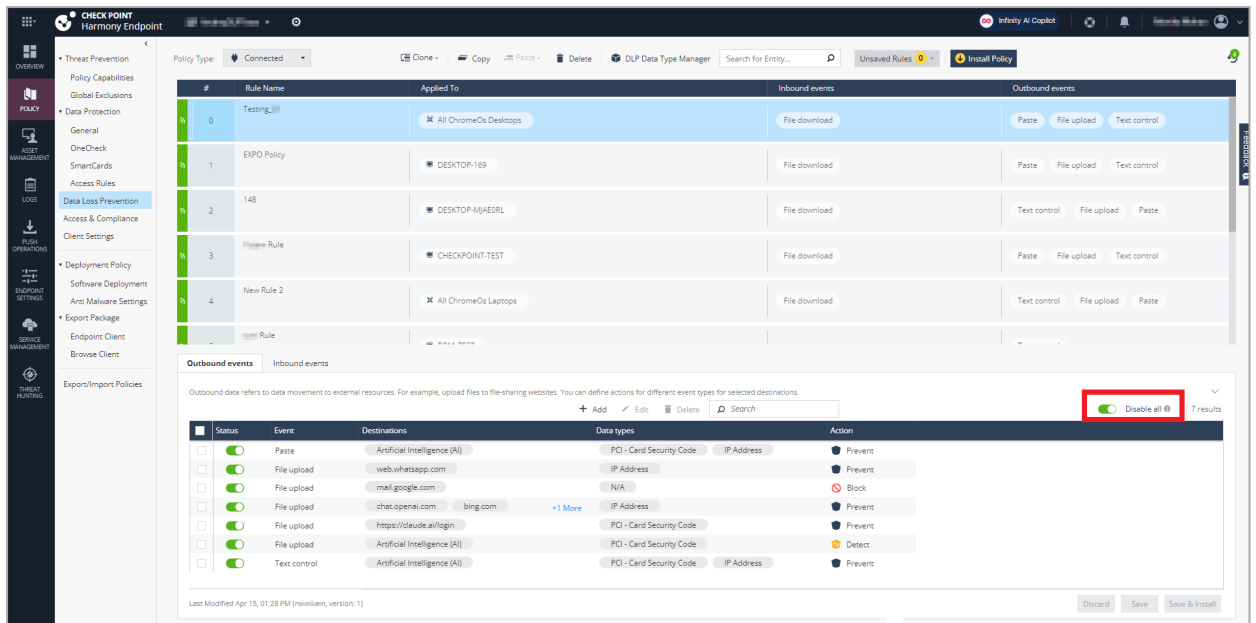
Note - This step is applicable only if the **Action** is **Ask**, **Detect** or **Prevent**.

11. Click **Save**.

The events are displayed in the **Outbound events** and **Inbound events** columns in the DLP rule.

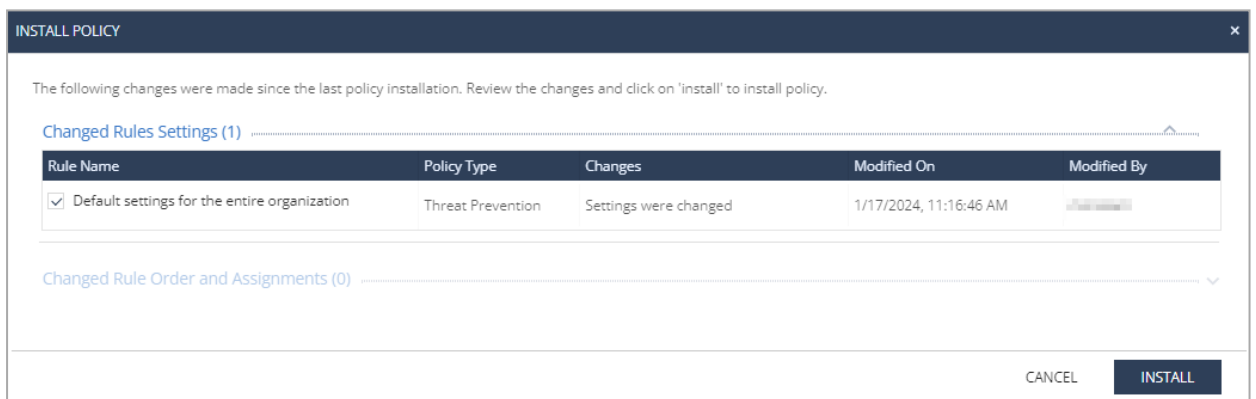


12. To delete an event, select the event that you want to delete and click **Delete**.
13. To edit an event, select the event that you want to edit, click **Edit**, make the required changes and click **OK**.
14. To disable all events, turn off the **Disable all** toggle button.



15. Click **Save & Install**.

The **Install Policy** window appears.

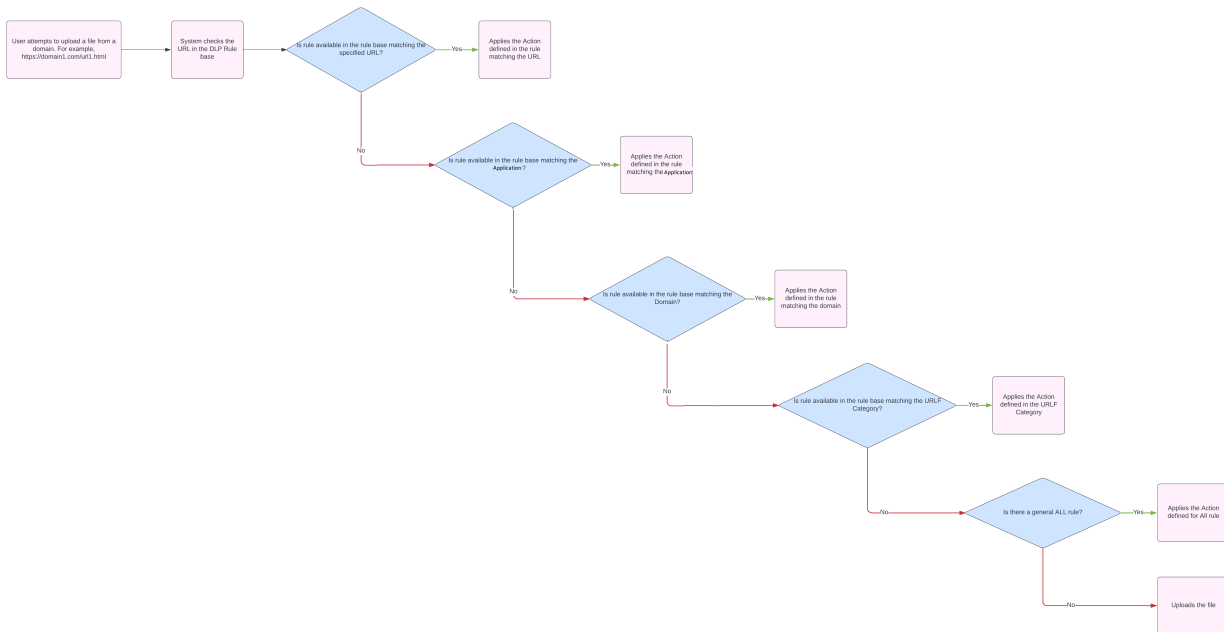


16. Click **Install**.

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

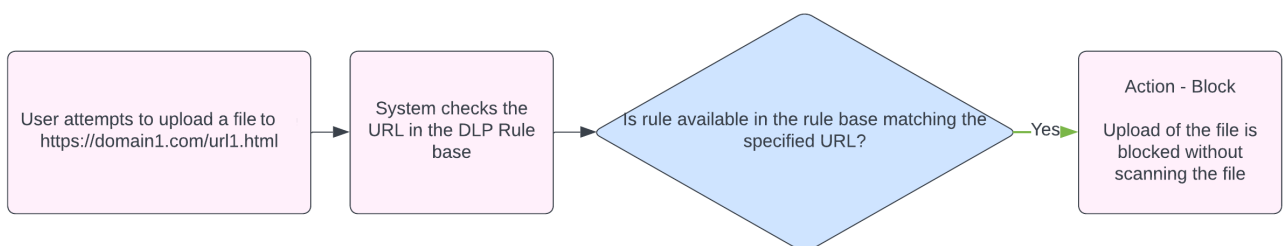
Status	Event	Destinations	Data types	Action
<input type="checkbox"/>	<input checked="" type="checkbox"/> File upload	All	ABA Transit Numbers	Detect
<input type="checkbox"/>	<input checked="" type="checkbox"/> File upload	https://domain1.com/url1.html	N/A	Block
<input type="checkbox"/>	<input checked="" type="checkbox"/> File upload	https://domain1.com/url2.html	N/A	Allow
<input type="checkbox"/>	<input checked="" type="checkbox"/> File upload	domain1.com	PCI - Card Security Code	Prevent
<input type="checkbox"/>	<input checked="" type="checkbox"/> File upload	Computers / Internet	N/A	Allow
<input type="checkbox"/>	<input checked="" type="checkbox"/> File upload	Education	N/A	Block
<input type="checkbox"/>	<input checked="" type="checkbox"/> Paste	ChatGPT	IP Address	Prevent
<input type="checkbox"/>	<input checked="" type="checkbox"/> Paste	Artificial Intelligence (AI)	N/A	Block
<input type="checkbox"/>	<input checked="" type="checkbox"/> 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

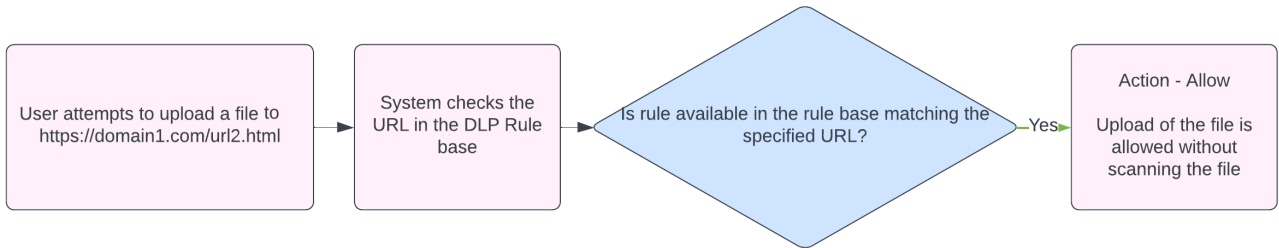


Scenario 2: User attempts to upload a file to `https://domain1.com/ur12.html`

Specific Event

Most specific event is the **URL** `https://domain1.com/ur12.html`.

Result

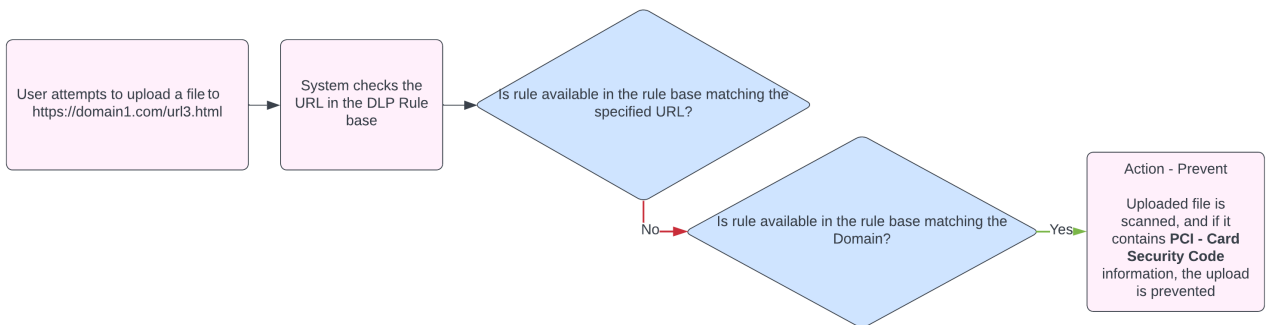


Scenario 3: User attempts to upload a file to `https://domain1.com/ur13.html`

Specific Event

Most specific event is the **Domain** `domain1.com`.

Result



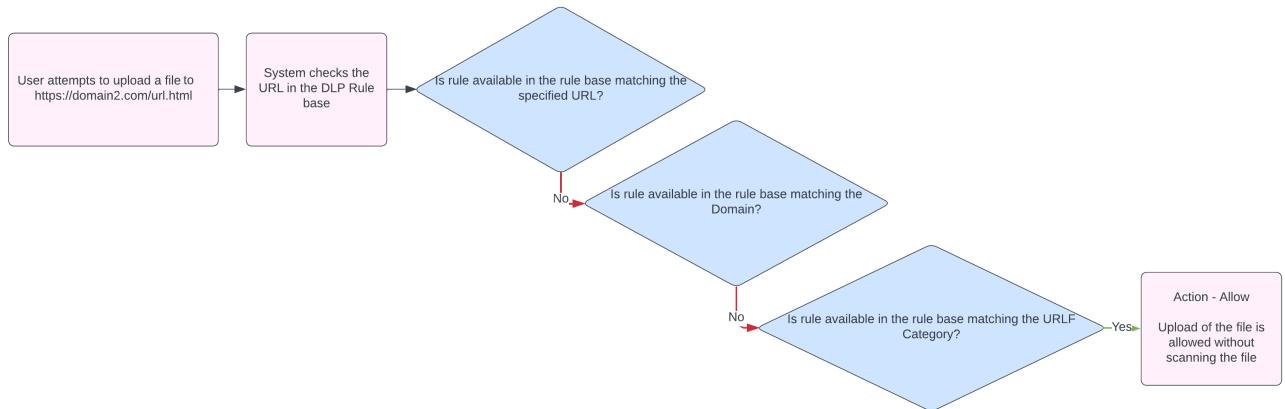
Scenario 4: User attempts to upload a file to `https://domain2.com/ur1.html`

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



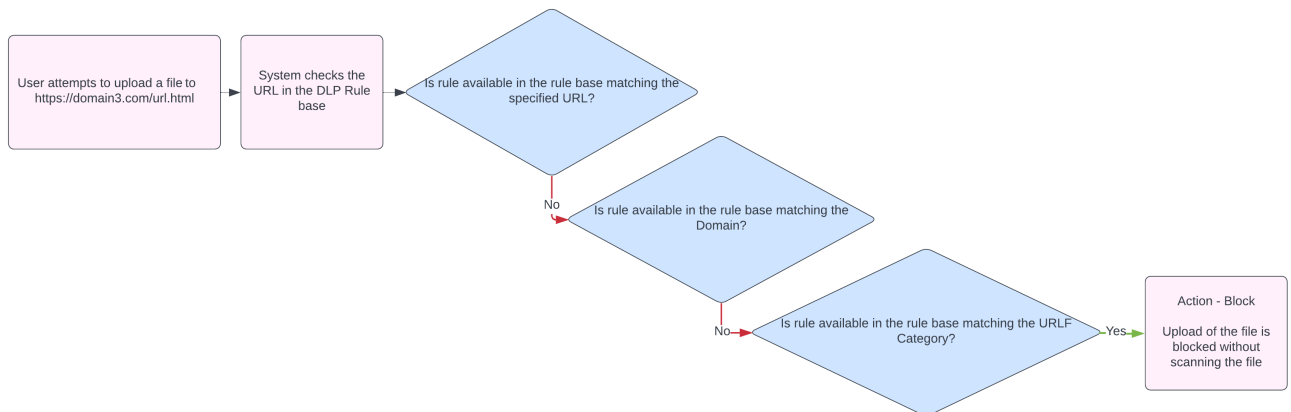
Scenario 5: User attempts to upload a file to https://domain3.com/url.html

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

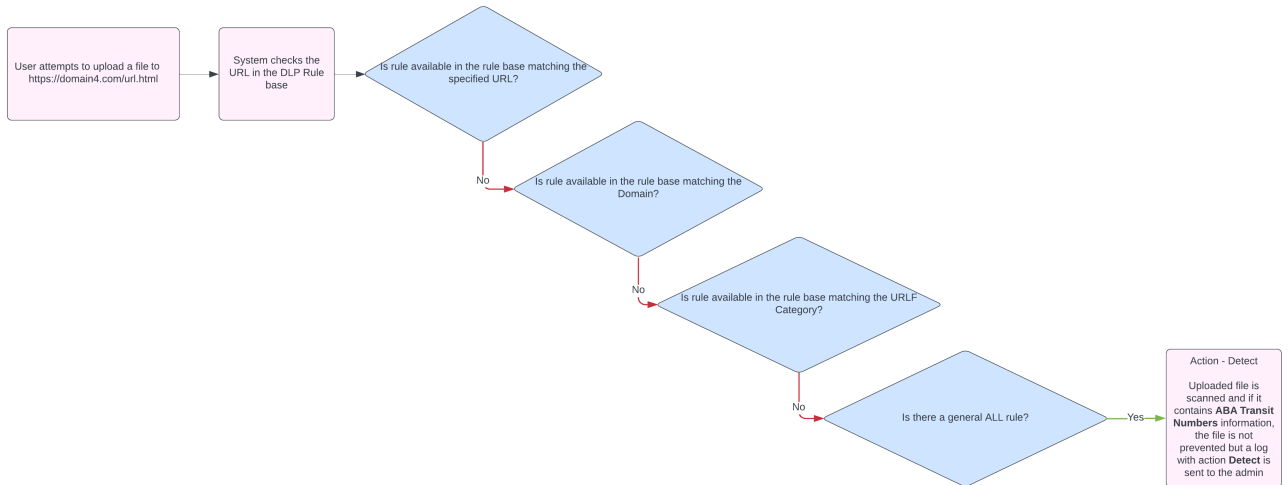


Scenario 6: User attempts to upload a file to https://domain4.com/url.html

Specific Event

Since there are no specific events for the URL, Domain, or Category, the event with the destination **All** is selected.

Result

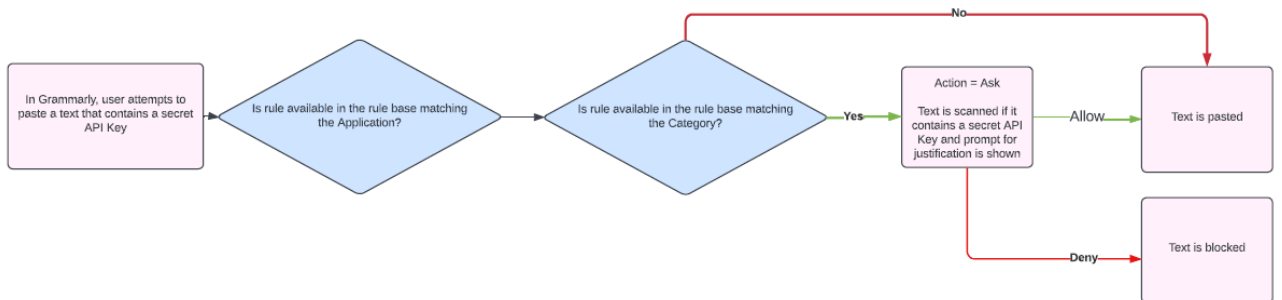


Scenario 7: In Grammarly, user attempts to paste a secret API Key

Specific Event

Most specific event is the **Application Grammarly**.

Result

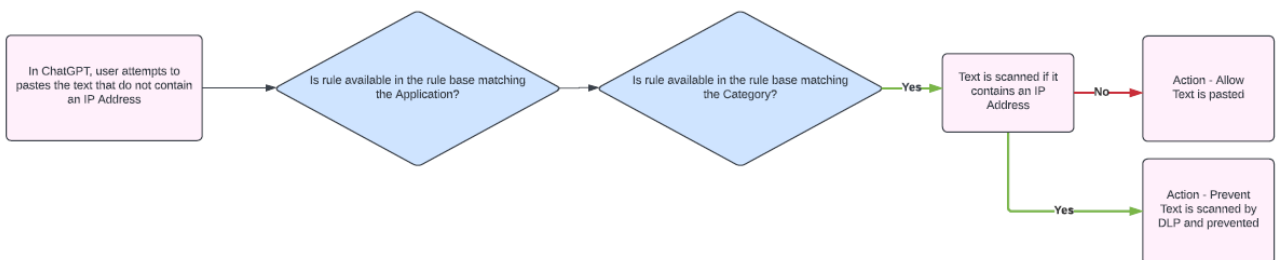


Scenario 8: In ChatGPT, user attempts to paste the text that do not contain an IP address

Specific Event

Most specific event is the **Application ChatGPT**.

Result

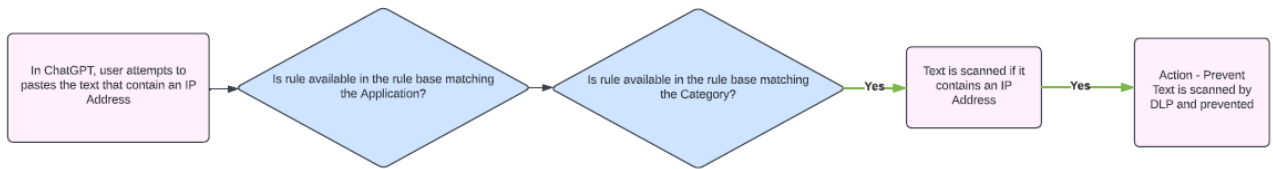


Scenario 9: In ChatGPT, user attempts to paste the text that contain an IP address

Specific Event

Most specific event is the **Application ChatGPT**.

Result

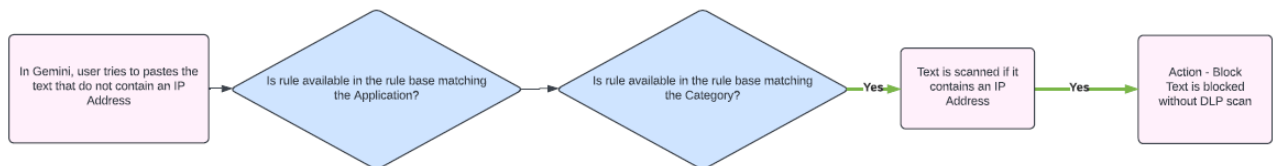


Scenario 10: In Gemini, user attempts to paste the text that do not contain an IP address

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
<input type="checkbox"/>	File upload	domain1.com	PCI - Card Security Code	Prevent
<input type="checkbox"/>	File upload	Computers / Internet	N/A	Allow
<input type="checkbox"/>	File upload	Education	N/A	Block
<input type="checkbox"/>	File upload	doamin1.com	IP Address	Detect

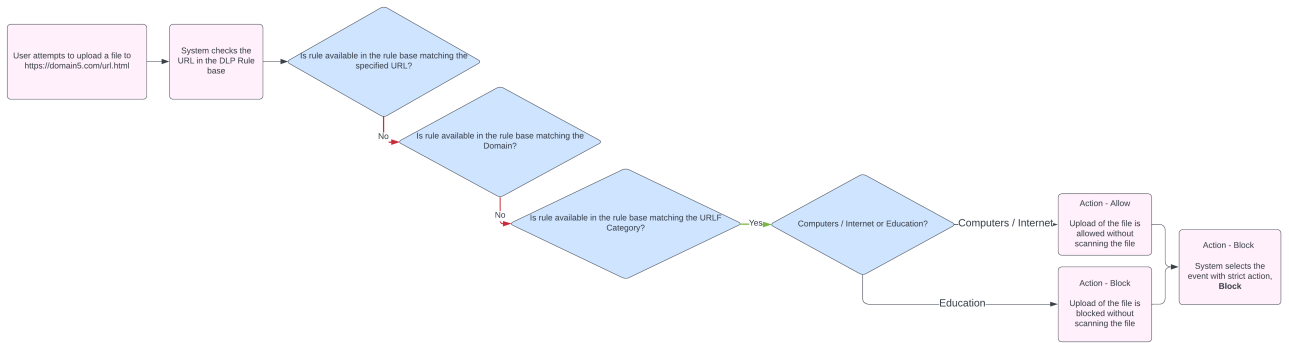
Scenario 11: User attempts to upload a file to https://domain5.com/ur1.html

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

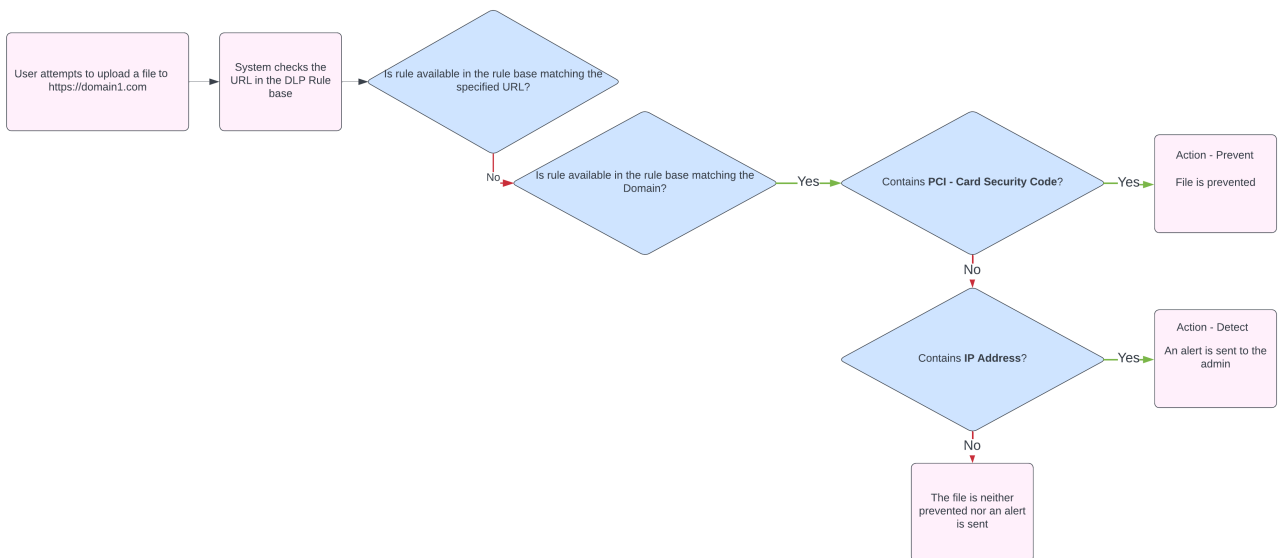


Scenario 12: User attempts to upload a file to https://domain1.com

Specific Event

Since there are no events for the URL, only two events for the **Domain domain1.com** are relevant.


Result



General Information

Localization

The Harmony Browse extension automatically detects the language of the browser and translates the following to the detected language:

- Pop-up and associated notifications
- Block pages
-  **Note** - The customized parts of a block page are not translated. For more information, see "[Configuring Client Settings Policy](#)" on page 50.
- OS notifications

The supported languages for localization are:

- Czech
- Danish
- German
- Greek
- English
- Spanish (European and Latin American)
- Finnish
- French
- Italian
- Japanese
- Norwegian Bokmål
- Dutch
- Norwegian Nynorsk
- Norwegian
- Polish
- Portuguese (European and Brazilian Portuguese)
- Romanian

- Russian
- Swedish

Managing Active Directory Scanners

If your organization uses Microsoft Active Directory (AD), you can import users, groups, Organizational units (OUs) and computers from multiple AD domains into the Harmony Browse. After the objects are imported, you can assign policies.

When you first log in to Harmony Browse, the AD tree is empty. To populate the tree with computers from the Active Directory, you must configure the Directory Scanner.

The Directory Scanner scans the defined Active Directory and fills the AD table in the **Asset Management** view, copying the existing Active Directory structure to the server database.

Harmony Browse supports the use of multiple AD scanners per Active Directory domain, and multiple domains per service.

Required Permissions to Active Directory:

For the scan to succeed, the user account related to each Directory Scanner instance requires full read permissions to:

- The Active Directory root.
- All child containers and objects.
- The deleted objects container.

An object deleted from the Active Directory is not immediately erased, but moved to the Deleted Objects container.

Comparing objects in the AD with those in the Deleted objects container gives a clear picture of network resources (computers, servers, users, groups) that have changed since the last scan.

The Active Directory Scanner does not scan Groups of type "Distribution".

Organization Distributed Scan

Organization Distributed Scan is enabled by default. You can see its configured settings in the **Endpoint Settings** view > **AD Scanners**.

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 download Endpoint client to be defined as an AD scanner:

1. Go to the Overview tab.
2. Click on the Download button in the blue bar.
3. Click on the Download button under the Client for AD integration.

To configure the AD scanner:

1. In the left navigation panel, click **Asset Management**.
2. In the left pane, click **Computers**.
3. In the top toolbar, click **Computer Actions** > in the section **General Actions**, click **Directory Scanner**.


The **Scanner** window opens.

4. Fill in this information:

SECTION	REQUIRED INFORMATION
Connect from computer	<ul style="list-style-type: none"> ▪ Computer name - Select the computer name which the AD integration client was installed on. This computer will be used as your AD scanner.
AD Login details	<ul style="list-style-type: none"> ▪ 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.
AD Connection	<ul style="list-style-type: none"> ▪ 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. ▪ Sync AD every - Configure the interval at which the scanning will be performed

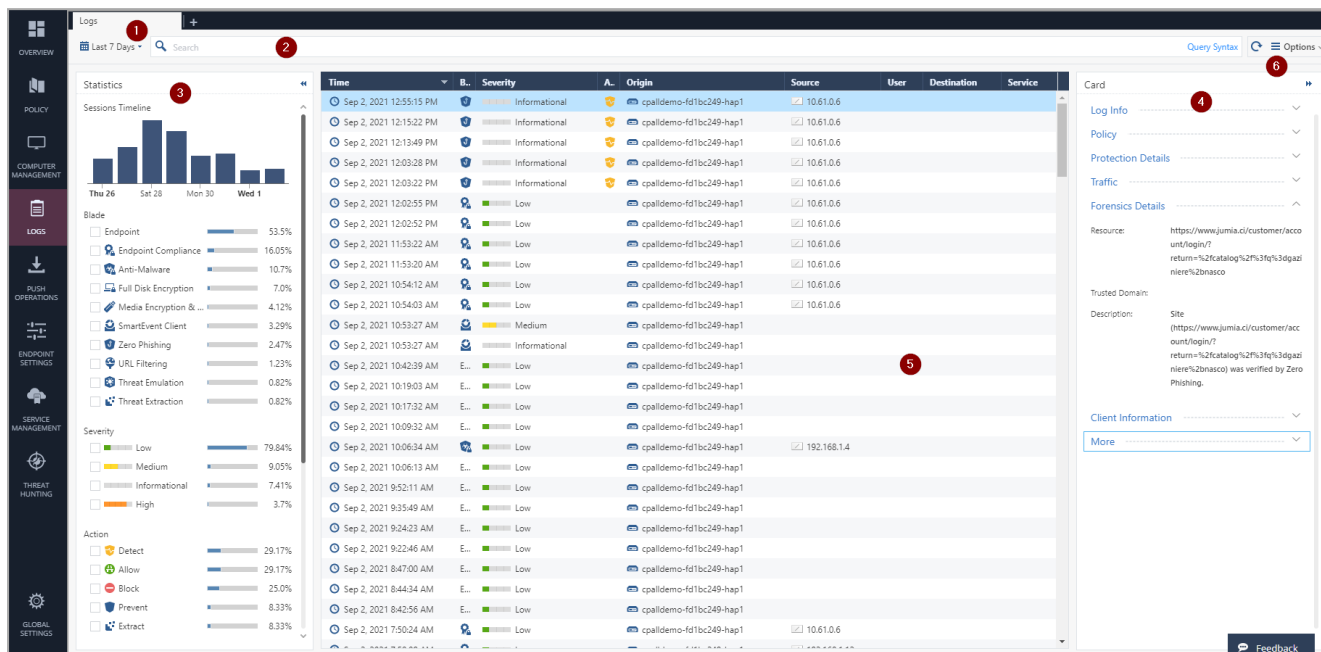
When you create a new AD scanner, the Organization Directory Scan is automatically disabled.

To see information on your activated AD scanners, go to the **Endpoint Settings** view.

 **Note** - You can also reach scanner configuration form through the **Endpoint Settings** view > **Setup full Active Directory sync**.

Harmony Browse Logs

See all collected logs in the Harmony Browse 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 156](#).

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](#).

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 Harmony Browse 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:

-

Shows all records for the source IP 192.168.0.0 to 192.168.255.255 inclusive

-

Shows all records for the source IP 192.168.1.0 to 192.168.1.255 inclusive

-

Shows all records for the source IP 192.168.2.0 to 192.168.2.255 inclusive

-

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.

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 Harmony Browse 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.

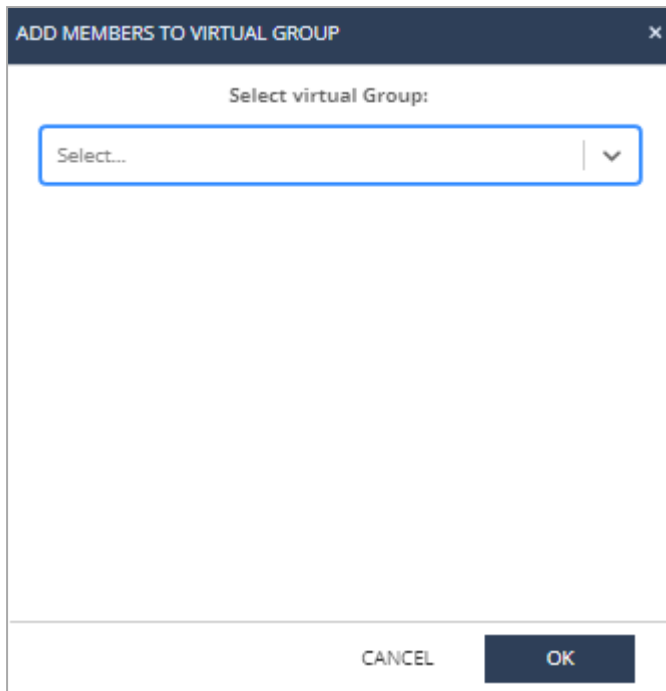
8. Click **OK**.

Note - You can also perform this procedure from **Asset Management > Organization > Computers**. See ["Managing Computers" on page 46](#).


To add a group, device or a user to a virtual group:

1. Access Harmony Browse 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 46](#).

To create and add to virtual group:

1. Access Harmony Browse 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.

The screenshot shows a dialog box titled "ADD MEMBERS TO VIRTUAL GROUP". It features three input fields: "Name" (placeholder: "Group name"), "Comment" (placeholder: "Comment"), and a "Members" section. The "Members" section includes a search box with a magnifying glass icon and the text "Search", and a list of members. The list has a header "Name" and one item "CHECKPOINT-TEST". At the bottom are "CANCEL" and "OK" buttons.

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 46](#).

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.

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 Harmony Browse:

1. Go to **Endpoint Settings > Export Events**.
2. Click **Add**.

The **New Logging Service** window opens.

3. Fill in the export details:
 - **Name** - Enter a name for the exported information.
 - **IP Address** - Enter the IP Address of the target to which the logs are exported.
 - **Protocol** - Select the protocol over which to export the logs: TCP or UDP.
 - **Format** - Select the export format.
 - **Port** - Select the port over which to export the logs. Only these ports are supported for outgoing communication: 514, 6514, 443.
 - **TLS/SSL** - Select this checkbox if you want log information to be TLS/SSL encrypted. The only allowed authentication method through TLS is mutual authentication. For mutual authentication, 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> <p>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.</p> <p> Best Practice - Use the device IP address as the Common Name.</p>

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	<p>Convert the certificate to the P12 format:</p> <pre>openssl pkcs12 -inkey cp_client.key -in cp_client.crt -export -out cp_client.p12</pre> <p> Note - The challenge phrase used in this conversion is required in the cp_client TLS configuration.</p>

3. Update the security parameters on the Check Point exporting server

Step	Description
1	<p>On a Multi-Domain Server or Multi-Domain Log Server, go to the context of the applicable Domain Management Server or Domain Log Server: If you run on a Multi-Domain Log Server/Multi-Domain Log Server, run this command to switch to the required domain:</p> <pre>mdsend <Name or IP Address of Domain Management Server or Domain Log Server></pre>
2	<p>Go to the deployment directory:</p> <pre>cd \$EXPORTERDIR/targets/<Deployment Name>/</pre>
3	<p>Create a directory for the certificate files:</p> <pre>mkdir -v certs</pre>
4	<p>Copy the ca.pem and cp_client.p12 certificate files to the \$EXPORTERDIR/targets/<Deployment Name>/certs/ directory.</p> <p> Note - The ca.key must <i>not</i> be published.</p>
5	<p>Assign the read permissions to the ca.pem and cp_client.p12 certificate files:</p> <pre>chmod -v +r ca.pem chmod -v +r cp_client.p12</pre>
6	<p>Update the secured target:</p> <pre>cp_log_export set name <Name> domain-server <Domain-Server> encrypted true ca-cert <Full Path to CA Certificate *.pem File> client-cert <Full Path to *.p12 Certificate File> client-secret <Challenge Phrase for the *.p12 File></pre>

4. 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 Harmony Browse.

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**.

Reports Center

The Reports Center provides you with the insights of the security analysis detected by the endpoint. These reports can be generated and scheduled.

Generate Report

To view predefined reports, navigate to **Endpoint Settings > Reports Center > Generate Report**.

You can download these reports in the pdf format:

- **Security Checkup** - A comprehensive report on security events.
- **Threat Extraction** - Shows the insights on the downloaded files.
- **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. Click **Export**.

Schedule Report

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

Notes:

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

To schedule a report:

1. Navigate to **Endpoint Settings > Reports Center > Schedule Report**.

2. Click **Add**.

The Schedule Report window appears.

3. From the **Name** list, select the report.

4. From the **Time Frame** list, select the period for the report:

- **Last day**
- **Last 7 days**
- **Last 30 days**

5. 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.

6. 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.

7. In the **Recipients** field, enter the recipients for the report.

8. Click **Schedule**.

The schedule is added to the table. The report becomes effective 24 hours after you schedule it.

9. To edit a scheduled report, select the report in the table and click **Edit**.

10. To delete a scheduled report, select the report in the table and click **Delete**.

Uninstalling the Harmony Browse Extension

For more information, see [sk180608](#).