6.4.3. Deep Packet Inspection Ports & Settings.. 93
6.4.3.1. Monitor Webmail Json format parser usage......................................96
6.4.3.2. Note on Peer Certificate Validation Usage........................................97
6.4.4. Deep Packet Inspection Applications.. 97
6.4.5. Certificate status matrix........................................... 98
7. eDiscovery............................................................100
7.1. eDiscovery Activation.................................100
7.2. Dashboard......................................................101
7.3. eDiscovery Policies and Scans...............................101
7.3.1. Creating an eDiscovery Policy and Scan... 102
7.4. eDiscovery Scan Result and Actions...............104
7.4.1. Viewing Scan Results and taking Actions. 104
8. Denylists and Allowlists.................................106
8.1. Denylists..................................................107
8.1.1. Custom Content................................107
8.1.2. File Name.......................................108
8.1.3. File Location..................................109
8.1.4. Scan Location................................111
8.1.5. Regex.........................................112
8.1.6. Domain and URL................................113
8.1.7. E-mail Domain.................................115
8.1.8. Applications......................................116
8.2. Allowlists...............................................118
8.2.1. MIME Type..................................118
8.2.2. Allowed Files................................119
8.2.3. File Location................................120
8.2.4. Network Share................................121
8.2.5. E-mail Domain.................................123
8.2.6. Deep Packet Inspection........................124
8.3. URL Categories........................................127
9. Enforced Encryption......................................129
9.1. Enforced Encryption.................................129
9.1.1. Enforced Encryption Deployment..........130
9.1.2. Enforced Encryption Settings.............131
9.1.3. Enforced Encryption Clients...............132
9.1.4. Trusted Device™.............................133
10. Offline Temporary Password............................136
10.1. Generating the Offline Temporary Password... 137
11. Reports and Analysis..................................139
11.1. Logs Report.......................................139
11.2. File Tracing..........................................140
11.2.1. File Tracing Events by Direction........140
11.3. Content Aware Report.............................141
11.3.1. Export Content Aware Reports...........143
11.4. Admin Actions......................................144
11.5. Online Computers.................................145
11.6. Online Users......................................145
11.7. Online Devices....................................146
11.8. Statistics.............................................146
12. Alerts......................................................148
12.1. System Alerts........................................148
12.1.1. Creating a System Alert.....................149
12.1.2. System Alerts History.......................150
12.2. Device Control Alerts............................151
12.2.1. Creating a Device Control Alert..........151
12.2.2. Device Control Alerts History............152
12.3. Content Aware Alerts.............................152
12.3.1. Creating a Content Aware Alert.........153
12.3.2. Content Aware Alerts History............154
12.4. Enforced Encryption Alert.......................155
12.4.1. Creating an Enforced Encryption Alert... 155
12.4.2. Enforced Encryption Alert History........156
13. Directory Services.................................157
13.1. Microsoft Active Directory.........................157
13.2. Azure Active Directory..........................159
13.2.1. Configure Azure Active Directory........159
13.2.1.1. Create the Application on Azure Active Directory..................................................159
13.2.1.2. Create a secret ID for the Application... 161
13.2.1.3. Create Users/Groups using Graph API. 163
13.2.1.4. Add Permissions to the Application.... 166
13.2.1.5. Add Graph Application to Endpoint Protector Server............................170
13.2.1.6. Create a Synchronization Job on the Endpoint Protector Server.................171
14. Appliance...............................................173
14.1. Server Information................................173
14.2. Server Maintenance...............................173
14.2.1. Time Zone......................................174
14.2.2. IP Configuration...............................175
14.2.3. DNS Configuration.............................175
14.2.4. Client Registration Certificate............175
14.2.5. Server Certificate..............................176
14.2.6. Server Certificate Validation...............176
14.2.7. Appliance Operations........................177
14.2.8. SSH Server......................................177
17.6.1. User Remediation Settings .................. 262
17.6.2. Justifications List .............................. 263
17.6.3. Enabling User Remediation ................. 264
17.6.4. User Remediation Usage ....................... 267

18. Endpoint Protector Agent .......................... 270
   18.1. Agent Installation ............................... 270
      18.1.1. Installation on macOS with Deep Packet
               Inspection and VPN Traffic Intercept active .. 271
      18.1.2. Debian based distributions ............... 277
      18.1.3. RedHat based distributions ............... 277

4. Setting the Endpoint Protector Server IP .......... 279

19. Endpoint Protector Server – Client communication 281
   19.1. Endpoint Protector Client ....................... 281
   19.2. Endpoint Protector Server ....................... 281

20. Support .................................................. 283

21. Disclaimer ............................................... 284
1. New features

The latest Endpoint Protector Functional release new features and enhancements, please refer to the Release History section:

https://www.endpointprotector.com/support/endpoint-protector-release-history
2. About this guide

2.1. Scope

This document describes how to set up and configure Endpoint Protector. It provides instructions to complete first-time system deployment, including planning the network topology, and ongoing maintenance.

It also describes how to use the Endpoint Protector user interface and details the lists of default utilized port numbers, configuration limits, and supported standards.

2.2. Intended Audience

This document is intended for system administrators, not end users.

Contact your system administrator if you are accessing a device protected by Endpoint Protector and have any questions that are not covered by this guide.
3. Introduction

Portable storage devices such as USB flash drives, external HDDs, digital cameras, MP3 players and iPods are virtually everywhere and are connected to a Windows, Mac, or Linux computer within seconds. With virtually every computer having internet access applications and collaboration tools, data theft or accidental data loss becomes a mere child’s play.

Data loss and data theft through a simple internet connection or USB device is easy and does not take more than a few seconds. Network Administrators had little chance to prevent this from happening or to identify the responsible users. This was the hard reality until now.

Endpoint Protector, through its Device Control, Content Aware Protection, eDiscovery, and Enforced Encryption modules, helps companies stop these threats. It not only controls all device activity at the endpoint but monitors and scans all possible exit points for sensitive content detection. It ensures critical business data does not leave the internal network either by being copied on devices or sent via the Internet without authorization, reporting all sensitive data incidents. Moreover, data at rest residing on endpoints can be inspected for sensitive content, and remediation actions can be taken. Additionally, enforcing encryption on USB removable devices is also possible. Everything from a single web-based interface.

Endpoint Protector is a complete Data Loss Prevention and the DLP-related features and functionality will be explained below. For detailed information about the Endpoint Protector Server deployment, refer to the Virtual and Hardware Appliance User Manual.
3.1. Main components

Endpoint Protector is designed around several physical entities:

- **Computers** - the Windows, Mac, and Linux workstations that have the Endpoint Protector Client installed
- **Devices** - the devices that are currently supported by Endpoint Protector (USB devices, digital photo cameras, USB memory cards, etc.)
- **Users** - the users who will be handling the devices and the computers

The Server side of Endpoint Protector has different parts, working close together:

- **Endpoint Protector Hardware or Virtual Appliance** – containing Operating System, Database, etc.
- **Web Service** – communicating with the Endpoint Protector Clients and storing the information received from them
- **Endpoint Protector User Interface** – managing the existing devices, computers, users, groups, and their behavior in the entire system
4. Server Functionality

Once the Endpoint Protector Hardware or Virtual Appliance setup is complete, access the User Interface from the assigned IP address.

The default Endpoint Protector Appliance IP address is https://192.168.0.201

**Note:** Always use the IP address with HTTPS (Hypertext Transfer Protocol Secure).

Use the default login credentials for the root account and contact Support to provide the password.

For detailed information on settings change or creating additional administrators, refer to the System Administrators

4.1. Endpoint Protector Configuration Wizard

The Configuration Wizard provides you with several steps to define basic settings. These include setting up the Server Time Zone, importing Licenses, Server Update or uploading
Offline Patches, Global device rights, E-mail Server settings, Main Administrator details, etc. You can change these settings at any time.

The Configuration Wizard is available only if the basic settings for the Endpoint Protector have never been configured.

As an additional security measure, a session timeout is implemented for 300 seconds (5 minutes) of inactivity. If you are not active for this amount of time, you are notified the session will expire and logged out unless you select to continue the session.

**Note:** You can customize the session timeout and timeout counter from the Session Settings sections.

4.2. General Dashboard

In this section, you can view general information as graphics and charts related to the most important activities logged by Endpoint Protector.

You will view more specific dashboards on the Device Control, Content Aware Protection and eDiscovery sections.
4.3. System Status

In this section you can view general information of the system’s functionality, alerts, and backup status.

From the **System Functionality** section, you can enable Endpoint Protector, as well as just specific modules (Device Control, Content Aware Protection, or eDiscovery).
From the **System Status** subsection, you can enable the **HDD Disk Space and Log Rotation**.

*Note:* If this setting is enabled, when the Server’s disk space reaches a certain percentage (starting from 50% up to 90%), old logs will be automatically overwritten by the new ones.

From the **System Alerts** subsection, you can enable important alerts notifying the expiration of the APNS Certificate, Updates, and Support or Passwords.

From the **System Backup** subsection, you can enable the **System Backup**.
4.4. Live Update

From this section, you can check and apply the latest security and Endpoint Protector Server updates.

Note: This feature communicates through port 80. Whitelist the liveupdate.endpointprotector.com (IP: 178.63.3.86) domain.

4.4.1. Software Update

Click **Configure Live Update** to select manual or automatic live updates check, the number of retries, and manage the Automatic Reporting to the LiveUpdate Server.
Click **Check Now** to search for the Endpoint Protector Server updates displayed in the **Available Updates** section. You can select and install an update with **Apply Updates**, or all updates with **Apply all updates**. To view the latest installed updates, click **View Applied Updates**.

You can also schedule an update. Select an entry from the available updates, click **Schedule update** and then use the calendar to select the date and confirm your selection.

Use the **Offline Patch Uploader** option to select the offline patches from your computer and successively install them to the latest Endpoint Protector version.

**Note:** Contact support@endpointprotector.com to request the **Offline Patch**.

**Important:** Before upgrading your Endpoint Protector server to the 5.7.0.0 server version from a pre-5206 version and adjacent OS image, you need to enable database partitions. Please contact **Support** for assistance.

### 4.4.2. Security Updates

You can use this section to check and apply different types of security updates, view information on recent updates checked or installed, and a list of updates available.

**Note:** The security update options will only be available for customer-hosted instances (e.g. AWS, Goggle, etc.) with the exception for Operating System and Kernel upgrades.

**Important:** Updates are not tested beforehand but are pulled from the official Linux repository.

To ensure the updates will not harm the system, follow these actions:

- test the updates in a test environment first
- make a VM snapshot
- make a system backup from the System Maintenance, the System Backup v2 section

CoSoSys Confidential. Copyright © 2004 – 2023 CoSoSys SRL and its licensors. All rights reserved.
Select one of the security updates type available and then click **Check Updates**: 

- **Security** – this will update all security-related updates of installed packages (Critical and High) 
- **Other** – this will download and apply any update available to 3rd party libraries, kernel, OS packages and MySQL database 
- **All Updates** – this will download and apply **Informational** and **Optional/Unclassified** updates 

If there are updates available, click **Apply Updates**. 

![Backend Security Updates](image)

**Note:** For history of applied Backend Updates go to admin action report and choose "Apply Updates" under Activity filter. 

**Important:** Due to patching nature, some updates may automatically restart the Endpoint Protector server or other sub-services in the background.

### 4.5. Effective Rights

In this section you can view currently applied Device Control or Content Aware Protection policies. Based on the options you select from the **Effective Rights Criteria** form, you can view information based on rights, users, computers, device types, specific devices, report type (PDF or XLS), including Outside Hours and Outside Network Policies, and more.

Once the report is generated, from the **Actions** column, you can download or delete it.
5. Device Control

From this section, you can manage all entities in the system, their subsequent rights, and settings. You can also manage other types of settings from the Device Control section such as Endpoint Protector Client and Deep Packet Inspection settings. As the first layer of security within Endpoint Protector, it is activated by default in every configuration provided.

5.1. Dashboard

This section offers a quick overview in the form of graphics and charts related to the Endpoint Protector Entities. You can select the start and end date for the data used in these visual representations from the top-right calendars and view the data in real time.

5.2. Devices

From this section, you can view, sort, and export in Excel, PDF or CSV format any devices from the system. Use the Actions column to edit, manage rights, view device history and delete a specific device.

You can view the right for each device based on the color code from the Status column:

- **Red** indicates the device is blocked in the system
- **Green** indicates the device is allowed on computers or for users
● **Yellow** indicates the device is allowed for some users or computers with restrictions

**Note**: Any new device connected to a protected computer is automatically added to the database and assigned to its first user which can be changed later.

Click **Create** to manually add a new device on the list by providing device information: name, friendly name, type PID, department, description, friendly description, VID, serial number and custom class.

Use **Choose action** to export list of devices, schedule a list export, export or import in JSON format or refresh the device codes.

The Export/Import Devices in JSON format feature allows you to manage device lists from one Endpoint Protector Server to another and aims to correlate the device rights and the Groups.

- If the same Groups exist on both Servers, the imported devices will also maintain the access rights
- If the Groups do not exist, the devices will still be imported but the access rights will be ignored

You can also import the devices directly from Active Directory.

**Note**: For detailed information on Active Directory, refer to the **Directory Services** chapter.

### 5.2.1. Priority order

If you do not configure the devices, the rights are inherited from the default Global Rights that are set per Device Types (USB Storage Device, Digital Camera, iPod, Thunderbolt, Chip Card Device, etc.).

**Note**: For detailed information, refer to the **Device Types** chapter.
If you configure device rights granularly for all entities, the priority order will be the following, starting with the highest:

![Diagram showing priority order: Devices → Computers or Users → Groups → Global]

**Example:** If global rights indicate that no computer on the system has access to a specific device, and for one computer that device has been authorized, then that computer will have access to that device.

### 5.2.2. Device Rights

To manage device rights for specific computers, groups, or users, select **Manage Rights** from the **Actions** column.
After selecting a device, assigning rights to specific users, computers or groups then follow these steps:

1. **Select the Entity and the Device right**

2. **Select the Entities (Computers, Groups, or Users)**
5.2.3. Device History

From this section, you can view the device history by selecting the View Device History action. This will display the Logs Report page filtered for the respective device.

5.3. Computers

From this section, you can filter, create, uninstall or delete a computer and use the Choose action option to create a Settings Report, Export List of Computers and Schedule Export list.

You can download the Settings Report from System Maintenance, the Exported Entities section to view the Deep Packet Inspection status for each entity (Computer/User/Group) and the entity from which Deep Packet Inspection is used.

Any new computer that has the Endpoint Protector Client deployed will be automatically added to the database, thus making it manageable.
The Endpoint Protector Client has a self-registration mechanism. This process is run once after the Client software is installed on a client computer. The Client will then communicate to the Server its existence in the system. The Server will store the information regarding the Computer in the database and it will assign a License.

**Note:** The self-registration mechanism acts whenever a change in the Computer licensing module is made, and also each time the application Client is reinstalled. The owner of the computer is not saved in the process of self-registration.

For more details about Licensing, go to the **System Licensing** chapter.

A Computer is identified by the computer parameters (Main IP, IP List, MAC, Domain, Workgroup, or Computer Serial Number, OS version) but information like Name and Description is also essential.

By default, the computer is assigned to the first user that handles the computer. This can later be changed and is updated automatically based on whoever logs into the computer.

**Note:** Computer Serial Number may not be taken for Virtual Machines due to System Limitations.

You can manually create a new computer at any time by providing the computer parameters and information mentioned above or import computers from Active Directory.

For more details about Active Directory, go to the **Directory Services** chapter.

You can also assign the computers to the following for a better organization:

- **Groups** e.g., several computers within the same office
- **Department** an alternative organization to Groups
5.3.1. Computer Rights

You can manage computer rights from the Actions column for a specific computer by selecting Manage Rights. This section is built around the computers, allowing you to specify which Device Types and Specific Devices can be accessible.

The Standard device control rights include the Device Types and Already Existing Devices sections. These are generally the only device rights used.

In addition to the Standard device control rights, if enabled from the Global Settings, you can create fallback policies for Outside Network and Outside Hours circumstances.

For detailed information on Device Types and Specific Devices (Standard, Outside Network, and Outside Hours), refer to the Device Types chapter.

Note: Use Restore Global Rights to revert to a lower level of rights. Once enabled, all rights on that level will be set to preserve global settings and the system will use the next level of rights.

All Existing Devices that were added on that level will be deleted when the restore is used.

5.3.2. Computer Settings

This section allows you to edit the settings for each computer.

Defining custom settings for all computers is not necessary since a computer is perfectly capable of functioning correctly without any manual settings defined.

It will do this by either inheriting the settings from the group it belongs to or, if not possible, the global settings, which are mandatory and exist in the system with default values from installation.
5.3.3. Computer History

From this section, you can view the computer history by selecting the View Computer History action. This will display the Logs Report page filtered for the respective computer.

5.3.4. Terminal Servers and Thin Clients

The capability to control file transfers on RDP storage between Thin Clients and Windows Terminal Servers can be enforced through Endpoint Protector, as detailed below.
5.3.4.1. Initial Configuration

The process starts with the menu view from Device Control > Computers, namely the action to **Mark as Terminal Server**.

After you selected the computer in the system as a Terminal Server, “Yes” will be displayed for ease of identification, as seen below:

![Device Control - Computers menu view](image)

**Note:** The computers that can be targeted by this action are strictly Windows Servers with Terminal Server roles properly configured.

Make sure that there is at least one Terminal Server license available when the action Mark as Terminal Server is performed.

If the Terminal Server is successfully marked, a new device type will appear when choosing to Edit it under Device Control, Computers, Computer Rights.

The settings for the Terminal Server-specific Device Types are: Preserve Global Settings, Allow Access, Deny Access, and Read-Only Access.

![Terminal Server Specific Device Types](image)

An Allow Access right set to the RDP Storage device type will enable all users that connect to the Terminal Server by RDP to transfer files to and from their local disk volume or shared storage devices such as USBs.

By contrast, a Deny Access right set to the RDP Storage will not allow any user that connects to the Terminal Server by RDP to transfer files to and from their local disk volume or shared storage devices such as USBs.
**Note:** Enable **Use User Rights** in the settings bar from **System Configuration, System Settings, Endpoint Rights Functionality** for the rights policy to apply on user logins with user priority.

Secondly, the menu from **Device Control > Users > Rights** will present an additional device type for all the users in Endpoint Protector, namely Thin Client Storage (RDP Storage).

Multiple users can be recognized as active users on any given Terminal Server, and so, the setting of this right can be used as a powerful tool to create access policies for specific users, as detailed in the use case below.

On a Windows Terminal Server, the Endpoint Protector Client will display RDP Storage disks shared by one or multiple Thin Clients as seen below.
5.4. Users

From this section, you can manage all the users in the system. Users are defined as the end-users who are logged on a computer on which the Endpoint Protector Client software is installed. Any new user will be automatically added to the database, thus making them manageable.
A user is identified by information like Name (Username, First Name, Last Name), Department, Contact Details (Phone, E-mail), and others and is also automatically assigned to a computer.

The Administrator can manually create a new user at any time by providing the user’s parameters and information mentioned above. Users can also be imported into Endpoint Protector from Active Directory.

For detailed information on Active Directory, refer to the Directory Services chapter.

There are two users created by default during the installation process of Endpoint Protector:

- **noUser** is the user linked to all events performed while no user was logged into the computer. Remote users’ names who log into the computer will not be logged and their events will be stored as events of noUser. Another occurrence of noUser events would be to have an automated script/software which accesses a device when no user is logged in to the specific computer.

- **autorunUser** indicates that an installer has been launched by Windows from a specific device. It is the user attached to all events generated by the programs launched from the specific device when Autoplay is enabled in the Operating System.

**Important:** Depending on the OS, additional system users can appear:

- _mbsetupuser (for macOS, during updates)
- 65535, 62624, etc. (for Linux, during locked screens)

The Actions column offers multiple options related to user management like Edit, Manage Rights, History, and Delete.

### 5.4.1. User Rights

The User Rights can be accessed by going to the Actions column for the specific user and selecting Manage Rights.

This section is built around the users, allowing the Administrator to specify what Device Types and also what Specific Devices can be accessible.

The Standard device control rights includes the Device Types and Already Existing Devices sections. These are generally the only device rights used.

In addition to the Standard device control rights, if enabled from the Global Settings, the administrator can create fallback policies for Outside Network and Outside Hours circumstances.

**Note:** The Restore Global Rights button can be used to revert to a lower level of rights. Once this button is pushed all rights on that level will be set to preserve global settings and the system will use the next level of rights.

All Existing Devices that were added on that level will be deleted when the restore is used.
5.4.2. User Settings

From this section, you can edit the settings for each user.

Defining custom settings for all users is not necessary since a user is perfectly capable of functioning correctly without any manual settings defined. It will do this by either inheriting the settings from the group it belongs to or, if not possible, the global settings, which are mandatory and exist in the system with default values from installation.

5.4.3. User History

From this section, you can view the user history by selecting the View User History action. This will display the Logs Report page filtered for the respective user.
5.5. Groups

From this section, you can manage all the groups in the system. Grouping computers and users will help the Administrator manage rights or settings for these entities in a more efficient way.

A group is identified by information like Name and Description, as well as based on the entities (Computers and Users).

You can manually create a new group at any time by providing the group information mentioned above. Groups can also be imported into Endpoint Protector from Active Directory.

*Note:* For detailed information on Active Directory, refer to the Directory Services chapter.
The Actions column offers multiple options related to the group’s management like Edit, Manage Rights, Manage Settings, History, and Delete.

5.5.1. Group Types

5.5.1.1. Regular Groups

Regular Groups are the groups created by the Administrator or are imported from AD and are not created based on a rule. From this section you can add or remove Computers or Users.

5.5.1.2. Smart Groups

Smart Groups are a dynamic category of computers and user groups for which membership can be defined based on element name patterns.

To use Smart Groups, follow these steps:

1. Enable Smart Groups from System Configuration, System Settings, on the Smart Groups section, scroll to the bottom of the page and click Save.

   **Note**: By enabling the Smart Group feature, Computers and Users will not be automatically assigned to the Default Group unless you create a Smart Group.

2. Create a Smart Groups from Device Control, Groups section. Click Create, provide the following and then click Save:
   - Group name, description and Department
   - Enable the Smart Group setting
   - Select the Entity, Computers or Users
   - Set rules for the Computers or Users by inclusion and exclusion

Define the rules Computers or Users are added to the Smart Groups based on the naming pattern rules: XYZ*, *XYZ*, *XYZ.

**Important**: The rules set are key-sensitive!

**Note**: Once created, you can manage the group’s priority by drag and drop actions.
3. Synchronize entities to the Smart Groups

The Smart Groups rule will not remove items from the regular groups to assign them to smart groups. Entities are added to the Smart group through the synchronization process. After you created the Smart Group, click **Sync** to start the synchronization at a given interval every 1 minute.

**Note:** The Synchronization process will not change settings for the regular groups.

If a new Computer is registered and matches one of the rules, the Computer will automatically be assigned to that Group.

If the new Computer does not match the rule, it will be added to the Default Group, if Default Groups are enabled from System Configuration, System Settings, and the Smart Groups section.

4. Delete a Smart Group from the **Actions** column or select the group from the list and then click **Delete**.
Smart Groups have the following **limitations**: 

- Smart Groups do not display assigned computers or users
- You cannot manually add an entity to a Smart Group
- Smart Groups are part of the Default Department but do not use Departments

If you disable Smart Group from System Settings, the Smart Group will be converted into a Regular Group. This will preserve its settings, rights, and other settings but will lose its entities and will remove the Default Group for Computers and the Default Group for Users.

User entities can only be assigned to Smart Groups after the synchronization process, not when a computer is registered, based on how the Endpoint Protector Client relays the user information.

When a Computer is registered, Endpoint Protector only receives information on computers; User information is relayed through events (logs) or regular pings/reprovision requests. User information is volatile: it can change between requests (different users can log in or log out on the same computer; log out events/sleep can also result in default hard coded user entities being marked as active/online).

### 5.5.1.3. Default Groups

Default Groups are groups of Computers and Users that do not belong to Smart Groups. These are Computers and Users that do not follow the name pattern set for Smart Groups.

**Note:** Default Groups are available only if Smart Groups are enabled.

To use Default Groups, follow these steps:

1. Enable Default Groups for Computers and Users from **System Configuration, System Settings**, on the **Smart Groups** section, scroll to the bottom of the page and click **Save**.
Important: You are not required to manually create Default Groups – by enabling them, the Default Groups for Users and Computers will be automatically created.

2. Synchronize entities to the Default Groups
For Computers and Users to be assigned to the Default Groups, on the List of Groups from Device Control the Groups section, from the Actions column select Edit, and then click Sync.

Default Groups have the following limitations:

- You can only edit Default Groups description, not the Default Groups name
- The Default Groups cannot be deleted, but can be disabled from System Configuration, System Settings, on the Smart Groups section
- If Default Groups are disabled, they will be deleted with all their dependencies.
5.5.1.4. Allowlists on Computer Groups

File Location, Network Share Allowlists, and File Location Denylist can be set for groups of Computers.

In the Groups select box, all groups will be displayed.

For a selected group the allowlist/denylist rule will apply only to computers from that group. If the group contains no computer, the rule won’t apply to anything. The Administrator can select additional computers from the select box.

Smart groups are always in sync with all the contained computers for denylists, just like they apply to a policy. Groups selected on allowlists or denylists will be synchronized every 15 minutes.

5.5.2. Group Rights

The Group Rights can be accessed from the Actions column for the specific group and selecting Manage Rights.

This section is built around the group, allowing you to specify what Device Types and also what Specific Devices can be accessible.

This section is similar to the Computer Rights section, the difference being that it applies to all the computers that are part of the group simultaneously.

The Standard device control rights include the Device Types and Already Existing Devices sections. These are generally the only device rights used.

In addition to the Standard device control rights, if enabled from the Global Settings, you can create fallback policies for Outside Network and Outside Hours circumstances.

For detailed information on Device Types and Specific Devices (Standard, Outside Network, and Outside Hours), refer to the Device Types chapter.
Note: Use Restore Global Rights to revert to a lower level of rights. Once enabled, all rights on that level will be set to preserve global settings and the system will use the next level of rights.

Note: All Existing Devices that were added on that level will be deleted when the restore is used.

5.5.3. Group Settings

From this section, you can edit the settings for each group.

Computers and users can be grouped to make editing the settings easier and more logical. Defining custom settings for all groups is not necessary since a computer is perfectly capable of functioning correctly without any granular settings defined. It will do this by either
inheriting the settings from the group it belongs to or, if not possible, the global settings, which are mandatory and exist in the system with default values from installation.

5.6. Global Rights

From this section, you can manage the entire system and specify what rights and settings apply globally, to all Endpoint Protector entities.

**Note:** If device rights or other settings will be configured granularly for entities, the priority order, starting with the highest, will be as follows:

This section relates to the entire system, allowing you to specify what Device Types and Specific Devices can be accessible. While Standard Rights Policies are the default ones, Outside Hours or Outside Network Policies are also available. These are dependent on first activating settings from Global Settings.

5.6.1. Device Types (Standard)

Endpoint Protector supports a wide range of device types, which represent key sources of security breaches. These devices can be authorized, which makes it possible for the users to view, create, or modify their content and for administrators to view the data transferred to and from the authorized devices.

- Removable Storage Devices
- Normal USB Flash Drives, U3 and Autorun Drives, Disk on Key, etc.
- USB 1.1, USB 2.0, USB 3.0
- Memory Cards - SD Cards, MMC Cards, Compact Flash Cards, etc.
- Card Readers - internal and external
- CD/DVD-Player/Burner - internal and external
- Digital Cameras
- Smartphones / Handhelds / PDAs (includes Nokia N-Series, Blackberry, and Windows CE compatible devices, Windows Mobile devices, etc.)
- iPods / iPhones / iPads
- MP3 Player / Media Player Devices
- External HDDs / portable hard disks
- FireWire Devices
- PCMCIA Devices
- Biometric Devices
- Bluetooth
- Printers (applies to serial, USB, and LTP connection methods)
- Express Card (SSD)
- Wireless USB
- LPT/Parallel ports *applies only to storage devices
- Floppy disk drives
- Serial ATA Controllers
- Network Printers

Depending on the device type, besides the Allow and Deny Access rights, additional rights are also available. These include Read-Only Access or multiple combinations of Allow Access but with various limitations, such as Allow access but exclude from CAP scanning or Allow Access if TrustedDevice Level 1 to 4.

The **Trusted Device™** technology integrated within Endpoint Protector is available in four security levels, depending on the degree of protection offered by a device (trusted devices using Enforced Encryption are TD level 1).

For detailed information on Trusted Device™ and Enforced Encryption, refer to the **Trusted Device™** chapter.

**Note:** With the WiFi – Block if wired network is present option you can disable the WiFi connection, while a wired network connection is present. The WiFi connection will be available when the wired network is not present.

**Note:** On macOS version 14 (Sonoma) and higher, Bluetooth devices are managed only when the device is connected and visible under ‘My Devices’ in the Bluetooth section of ‘System settings’.
By default, the majority of device types are blocked. However, as a working internet connection or wireless keyboards are needed during the configuration process, several devices are set to Allow Access. These include Wi-Fi, Bluetooth, Network Share, Additional Keyboard, and USB Modem.
5.6.1.1. VM USB Device Usage

The VM USB device type extends Endpoint Protector applicability for VMWare and VirtualBox virtual environments.

You can also use this option to manage USB access through the virtual environment.

When using a virtual environment, the USB devices will not be displayed in the Endpoint Protector Notifier with their original names, VID and PID information. Only the original information will remain the serial number.

**Example:** In the below image, you can view the 3 devices detected by Endpoint Protector have different VID, PID and device code, but they all have the same serial number.

**Note:** The Endpoint Protector Client does not distinguish between USB devices (e.g. USB hard drive vs USB Webcam) by Device name/VID/PID.

![Endpoint Protector client interface showing USB devices with serial numbers](image)

5.6.2. Specific Devices (Standard)

From this section, you can manage access rights for a specific device.

Device rights can be set either Globally or, per Group, User, or Computer, by using the Manage Rights action from each section/entity.
To add a new device click **Add** and provide the mandatory information.

There are multiple ways of adding devices:

- **New Device (VID, PID, Serial Number)** – will allow at Step 2 to add new devices based on Vendor ID, Product ID, and Serial Number.

- **Existing Device (Wizard)** – will allow at Step 2 to add devices previously connected to protected computers and already in the Endpoint Protector database.

- **Device Serial Number Range** – will allow at Step 2 to add multiple devices at the same time, by specifying the first and last Serial Number in the range. The recommended use for this feature is for devices that have a consecutive range, with a clear, noticeable pattern.
Note: Although this feature can work in situations where the Serial Number range does not follow a noticeable pattern, this is not recommended. In this type of situation, some devices will be ignored by Endpoint Protector and will not have the expected effect.

- **Bulk List of Devices** – will allow at Step 2 to add up to 1000 devices at the same time. There are two methods to choose from, either importing a list or simply pasting the information.

The File Allowlist feature is also available for USB storage devices that have allowed access. For detailed information on using the File Allowlist, refer to the File Allowlist File chapter.

5.6.3. **Outside Network**

Note: To use this setting, the feature needs to be enabled in the Global Settings section.

From this section, you can define fallback policies that will apply when outside the network. All of the functionalities are identical to the Standard section.

5.6.4. **Outside Hours**

Note: To use this setting, the feature needs to be enabled in the Global Settings section.

From this section, you can define fallback policies that will apply when outside working hours. All of the functionalities are identical to the Standard section.
5.7. Global Settings

From this section, you can apply settings globally to all Endpoint Protector entities.

- If there are no settings defined granularly for a computer, and it does not belong to a group, these are the settings it will inherit.
- If the computer belongs to a group, then it will inherit that group’s settings.

Note: Several settings from this section also relate to other modules apart from the Device Control module (Content Aware Protection, eDiscovery, etc.).

5.7.1. Endpoint Protector Client Settings

From this section, you can manage settings that relate directly to the Endpoint Protector Client and the Client’s behavior for each specific entity (Global, Groups, and Computers).
• **Client Mode** – select a mode to change Endpoint Protector Client behavior.

  **Note:** Learn more from the [Client Mode](#) section.

• **Notifier Language** – Configure the Endpoint Protector Client to automatically match the OS language of the user for notifications. When set to "Automatic," the client adjusts its language to the user's OS language preference without any server interactions, enhancing the user experience and reducing confusion.

To configure the EPP Notifier language selection:

1. Navigate to **DEVICE CONTROL -> GLOBAL SETTINGS** in the Endpoint Protector Console.

2. In the "Notifier language" section, select either "Automatic" or "Default" based on your preferences.

   2.1. "Automatic" means the language will be detected automatically from the OS, without server interaction.

   2.2. "Default" means the language selected on the server will be applied. If the "Automatic" language was selected on the server, the "Automatic" language will be used.

3. Save your settings to apply the chosen language selection.

With this enhanced language selection feature, Endpoint Protector provides a more accommodating experience for users, making notifications and alerts more accessible and user-centric.

• **Tamper Mode** – enable this setting to protect the Endpoint Protector Client from unauthorized termination and modification

  **Important:** A machine or service reboot is mandatory after enabling this setting to work correctly.

• **Policy Refresh Interval (sec)** – enter the time interval at which the Client checks with the Server and updates with the latest settings, rights, and policies.

  **Note:** The policy refresh cycles may be influenced by Azure Active Directory sync intervals (or Active Directory syncs) if Endpoint Protector is configured to sync entities. Please consider the sync intervals of your Azure Active Directory or Active Directory sync processes when determining an appropriate policy refresh interval.

• **Log Interval (min)** – enter the time interval at which the Client attempts to re-send the Logs to the Server.

• **Shadow Interval (min)** – enter a time interval between 0-720 minutes at which the Endpoint Protector Client sends the file Shadows to the Endpoint Protector Server.

  **Note:** Set the interval to 0 to send the file shadows instantly.

• **Recovery Folder Retention Period (days)** – this setting is specific for Mac and Linux computers. It acts as a quarantine folder before a transferred file has been fully
inspected for content, avoiding any potential file loss due to blocked transfers. After the specified time interval, the files are permanently deleted.

- **Log Size (MB)** – enter the largest size of all logs stored on the Client. If the value is reached, new logs will overwrite the oldest ones. These circumstances occur only when the Client and Server do not communicate for a large period of time.

- **Shadow Size (MB)** – enter the largest size of all file shadows on the Client. If the value is reached, new shadows will overwrite the oldest ones. These circumstances occur only when the Client and Server do not communicate for a large period of time.

- **Min File Size for Shadowing (KB)** – enter the smallest size of a file at which a File Shadow is created.

- **Max File Size for Shadowing (KB)** – enter the largest size of a file at which a File Shadow is created.

- **Devices Recovery Folder Max Size (MB)** – this setting is specific for Mac and Linux computers. Maximum size for the quarantine folder. If the value is reached, new files will overwrite the oldest ones.

- **Custom Client Notifications** - if enabled, the Client Notifications can be customized.

- **Mandatory OTP Justification** - if enabled, the Justification a User has to provide when requesting or using an Offline Temporary Password is mandatory.

- **Extend Source Code Detection** - if enabled, this will extend the detection also inside of file type, such as PDF, Docx, etc. With **Monitor Webmail** setting enabled, you can also detect source code in emails in subject and body using web browsers.

  **Note:** Source Code Detection may encounter challenges when dealing with small code snippets. This can occur due to the potential overlap among various programming languages. It's important to consider these limitations when configuring and utilizing Source Code Detection for optimal results.

- **User edited information** - if enabled, the User can edit the user and computer information from within the Endpoint Protector Client.

- **Optical Character Recognition** - if enabled, JPEG, PNG, GIF, BMP, and TIFF file types can be inspected for content. This option will also change the global MIME Type Allowlists.
● **Disable OCR notifications** – if enabled, this will disable all notifications generated by the Optical Character Recognition setting.

● **Limit Reporting Content Aware Protection** - if enabled, this will allow information discovered after reaching the Threat Threshold or after matching the Content Detection Rule that contains AND operator for a Report Only Content Aware Protection policy, to no longer be logged. This considerably reduces the number of logs, therefore, optimizing the allocated storage space.

● **Deep Packet Inspection** - if enabled, network and browser traffic can be inspected for content. This option is required for both the Deep Packet Inspection Allowlists and URL and Domain Denylist.

● **Use stealthy DPI driver** – enable this driver to improve interoperability with independent software vendors

● **Intercept VPN Traffic** – if you enable this setting, you allow the Endpoint Protector Client to intercept VPN traffic on macOS using the network extension framework

  **Note**: Learn more from the **Intercept VPN Traffic** section.

● **Do not scan recently downloaded files** – if enabled, when Deep Packet Inspection is disabled, you can download and upload to a browser a file containing sensitive data

  **Note**: This feature will only work for Windows agents on Endpoint Protect 5710 and later.

● **Block unsecured connection** - if enabled, unsecured access through HTTP will be blocked and user access restricted.

  **Note**: The **Block unsecured connection** feature is only available when the Deep Packet Inspection feature is enabled.

● **EPP behavior when network extension is disabled** – select a behavior type from the available entries

● **Disable Bluetooth File Transfer** - if enabled, this setting will block transfers to Bluetooth Devices, without considering if they are paired or not to the endpoint. **This only applies to Windows endpoints.**
- **Allow formatting/renaming Removable devices in Trusted Device™ Level 1+ (TD1+)** — only available for Windows, enable this setting to allow the user to format or rename a USB device that has TD1-x access permission.

  **Note:** For this setting to work successfully, enable the **Minifilter Driver** setting.

- **User Remediation Pop-up** — this setting is available when the **User Remediation feature** is active and enables User Remediation pop-up notifications for end-users.

- **Enforce User Remediation Pop-up** - this setting is available only if the User Remediation Pop-up setting is enabled. When this setting is enabled, end-users cannot disable User Remediation Pop-up notifications.

- **Notifications Pop-up** — you can select between the traditional notification, system tray, or pop-up notifications.

- **Enable Minifilter driver** — only available for Windows, this setting allows the use of an enhanced driver that provides more reliability and ease of maintenance. You can also enable this setting on the Computers/Users/Groups/Global Rights sections with Manage Settings from the Actions column.

- **User Remediation Notification Template** - you can select from the drop-down list a custom notification.

  **Note:** **User Remediation Pop-up** and **Enforce User Remediation Pop-up** are only available for Premium licenses.

- **Show Request OTP section in EPP Client** — disable this setting to hide the **Request OTP** action from Endpoint Protector Client

- **Show Authorize section in EPP Client** — disable this setting to hide the **Authorize** action from Endpoint Protector Client

### 5.7.1.1. Intercept VPN Traffic

If you enable this setting, the Endpoint Protector Client will intercept VPN traffic on macOS using the network extension framework.
**Note:** The Intercept VPN Traffic feature is only available when the Deep Packet Inspection feature is enabled. It will only work for macOS from version 11.0 onwards and only if Deep Packet Inspection Certificate is also added.

To use this feature, follow these steps:

1. Enable **Deep Packet Inspection**
2. Enable **Intercept VPN Traffic**
3. Select an option for **EPP behavior when network extension is disabled**
   - **Temporary Disable Deep Packet Inspection** – this will disable Deep Packet Inspection temporary
   - **Block Internet Access** - this will block the Internet connection until the user approves the Endpoint Protector Proxy configuration. The user also can allow the configuration after rebooting the PC.
   - **Repeat VPN notification** – this will display the VPN pop-up window multiple times even after the user has previously denied permission
4. Click **Save**;
5. On the pop-up window informing the user that a System Extension is blocked, click **OK** to allow;
6. Go to **System Preferences, Security and Privacy, General**, and then allow the Endpoint Protector Client Extension;
7. On the Endpoint Protector Proxy Configuration pop-up window, click **Allow**;

   ![Endpoint Protector Proxy Configuration](image)

**Note:** When network extension is successfully enabled, a Client Integrity OK log is generated.

8. Go to **System Configuration, System Settings, Deep Packet Inspection Certificate**, and then download the **CA Certificate**;

   ![Deep Packet Inspection Certificate](image)
9. On your macOS, open the **Keychain Access** application and go to **System**;

10. Decompress the **ClientCerts** file;

11. Select the **cascert.pem** file and drag and drop it on **Keychain Access, System**;
12. Double click the X from the newly added certificate and select **Always Trust** from the Trust section;

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Expired Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example Certificate</td>
<td>10 May 2023</td>
</tr>
</tbody>
</table>

13. **Save** the changes.
5.7.1.2. Smart DPI (Log Throttling)

Enable this setting to address the number of excessive false positives for URL Denylists. This improvement provides you with a configuration option to filter out non-relevant information, resulting in a more accurate log that focuses on true false positives and reduces unnecessary noise, saving database storage.

5.7.1.3. Client Mode

You can select from the drop-down list a client mode to define the Endpoint Protector Client behavior.

1. **Normal** – this is the default and recommended setting to use before being fully aware of what the other modes imply.

   **Note:** If the Normal Mode does not suit your needs, consider the **Hidden** or **Silent** modes as the best alternatives.

2. **Transparent** – use this mode to block all devices whilst maintaining users unaware of any restrictions or presence of the Endpoint Protector Client.

   Selecting this mode will:
   - Not display the system tray icon
   - Not display system tray notifications
   - Block everything, regardless of authorized or not
   - Administrator receives alerts for all activities
3. **Stealth** - use this mode to monitor all users and computers whilst maintaining users unaware of any restrictions or presence of the Endpoint Protector Client.

**Note:** As everything is allowed, there will be no disruptions in the daily activities of the users.

Selecting this mode will:
- Not display the system tray icon
- Not display system tray notifications
- Allow everything, regardless of authorized or not
- Enable file shadowing and file tracing to view and monitor all user activity
- Administrator receives alerts for all activities

4. **Panic** – This mode should be selected under extreme situations when a user’s malicious intent or activity is detected by the EPP Admin.

**Important:** It is recommended to use this mode for selected users/groups/computers only, as it will block all devices and generate a high volume of logs!

Selecting this mode will:
- Display the system tray icon
- Display system tray notifications
- Block everything, regardless of authorized or not
- Enable file shadowing and file tracing to view and monitor all user activity
- Administrator receives alerts when computers go in and out of Panic Mode

5. **Hidden Icon** - this mode is similar to Normal mode, except that the Endpoint Protector Client is not visible to the user.

Selecting this mode will:
- Not display the system tray icon
- Not display system tray notifications
- Apply all set rights and settings as per their configuration

6. **Silent** - this mode is similar to Normal mode, except that pop-up notifications are not visible to the user.

Selecting this mode will:
- Display the system tray icon
- Not display system tray notifications
- Apply all set rights and settings as per their configuration
5.7.2. File Tracing and Shadowing

In this section, you can manage the following settings:

- **File Tracing** – this feature allows you to monitor data traffic between protected endpoints and removable devices, internal eSATA HDDs, and Network Shares. It also shows other actions that took place, such as files named, deleted, accessed, modified, etc.

To enable this feature, you can do so from **Device Control, Global Settings**, or granularly for **Groups** or **Computers**.

- **File Shadowing** – this feature extends the information provided by **File Tracing**, creating exact copies of files accessed by users.

The creation of shadow copies can be triggered by the following events: file copy, file write, and file read. Events such as file deleted, file renamed, etc. do not trigger the function.

You can enable File Shadowing on all supported Removable Devices:

  - eSATA HDDs or Time Machines
  - Network Shares
    - Content Aware Protection - file transfers through various exit points such as online applications, printers, clipboards, etc.
  - E-mail Body

**Important**: **File Shadowing** cannot be used without **File Tracing**.

File Shadowing can be delayed due to network traffic and Endpoint Protector Settings for different computers or file sizes. Shadowed files are usually available after a few minutes. Shadow creation may not occur for newly created files; however, the system diligently tracks file activities and generates File Shadowing for subsequent file events as expected.

**Note**: For your deployment, we strongly advise activating File Shadowing for not more than 15% of your total endpoint capacity (e.g., for a 1000 endpoint deployment, File Shadowing should be set to a maximum of 150 endpoints for optimal performance). For more users, please contact customer support for recommended settings.

- **Exclude Extensions from Tracing** – you can disable File Tracing for specific file types.
- **Exclude Extensions from Scanning** – you can disable scanning for specific file types.
- **File Tracing Direction** – this setting enables you to monitor file transfers based on transfer direction:
- **Outgoing File Tracing Direction** is defined by transfers made from the local machine to removable devices.

- **Incoming File Tracing Direction** indicates transfers from the removable devices to the local machine.

- **Both (Outgoing & Incoming)** allows you to monitor all types of transfers that are made between removable devices and the local machine.

**Note**: The File Tracing Direction setting only applies for transfers between removable devices, computers, and network shares and works only on Windows and macOS starting with version 11.0.

- **Exclude Extensions from Shadowing** – use this setting to disable File Shadowing for specific file types.

- **Scan archive in archive** – use this setting to define the archive depth in which content is inspected.

- **Block Time Machine** – if you enable this setting, you will block Time Machine backups on macOS.

- **Metadata Scanning** - if you disable this setting, metadata will not be scanned for PDFs, ZIPs, and Office Files DOCX, XLSX, PPTX, DOC, XLX, PPT).

- **Advanced Printer and MTP Scanning** – if you enable this setting, this will increase accuracy and reduce false positives for File Tracing and File Shadowing. It is available only for Windows and will require a computer restart.

- **Block Print from Browsers** – available only for Windows, enable this setting to restrict the user from printing web pages from various browser types available.

- **File Hash** - if you enable this setting, a file hash will be generated and included in the file transfer logs.

- **Scan Printed Document** – select if you want to be notified a threat was restricted on the whole document or on the specific page.
5.7.2.1. Block Print from Browsers

Enable this setting to restrict the user from printing web pages from various browser types available, define the specific browsers, and create and enforce a Content Aware Policy that includes Printers from the Policy Exit Points section.

**Note:** This setting is available only for Windows.

**Important Note:** After enabling the "Block Print from Browsers" setting and applying the configuration on the Client to enforce it, please be aware that open browser tabs will need to be reloaded, or a browser restart will be required for the changes to take effect.

Users printing from Google Chrome and Microsoft Edge can utilize content-aware detection by enforcing a Content Aware Policy that includes Printers from the Policy Exit Points section. For seamless protection, the EPP Browser Connection extension installs automatically the first time upon enabling the Block Print from Browsers setting. This extension enhances content scanning capabilities during web document printing, integrating seamlessly on both server and client sides.
**Note:** The extension does not function in 'in Private/Incognito' mode. If it fails to load, it reverts to full Block-mode with Printing, providing comprehensive protection.

**Note:** To ensure the extensions’ stability and prevent user interference, use Group Policy Objects (GPO), the exclusive and recommended method for installing on both Google Chrome and Microsoft Edge.

**Important:** Use the Group Policies to set PDF files to be downloaded instead of opened in the web browser for the block print from the browser to function accurately.

**Important:** Group Policy Objects (GPO) are the only supported method to prevent users from disabling or uninstalling the Google Chrome and Microsoft Edge extension.

### 5.7.2.2. Configuring GPO for Browser Extensions

To configure Group Policy Objects (GPO) to deploy a browser extension to Windows machines and prevent users from removing it, follow these steps:

1. **Google Chrome**
   - Refer to the official [Google support guide](#) for detailed instructions.
   - Download Chrome Group Policy Template [here](#).
   - Configure your Group Policy as shown below.
     - EPP Browser Connector ID: `nnnaeanocbmnnjjlicfhcpbpefmlgbcgoi`

2. **Microsoft Edge**
   - Utilize the guide provided by Microsoft: [Configure Microsoft Edge](#).
   - Download the Edge browser extension from this [link](#).
- Configure your Group Policy as shown below.
  - EPP Browser Connector ID: nnaeanocbmnnjjlcfhcbpefmlgbcgoi

**Important:** Make sure to thoroughly test the configuration in a controlled environment to ensure the intended behavior. Always keep endpoint security policies updated and aligned with organizational security standards.

### 5.7.3. Ignore Virtual Printers

We introduced an option to Ignore Virtual Printing events, empowering customers to have control over Content Aware Protection and File Tracing visibility over virtual printers like Microsoft to PDF, PDFCreator, and more. This enhancement not only helps conserve valuable log space but also reduces the workload on your analytics and administration teams. With this option, you can now focus on tracking PDFs only when they exit your organization's environment and not when they have been created, streamlining your monitoring efforts and improving efficiency.

**Note:** This feature only applies for Windows.

### 5.7.4. Configure Max File Size

This section allows customers to tailor Content Aware Protection scanner's file size settings according to their specific needs. By customizing these settings, you can ensure Endpoint Protector meets your organization's requirements. The default maximum file size is set at 40 MB, with a maximum limit of 4096 MB.
Furthermore, you have the flexibility to configure additional file type sizes, which are set as follows by default: PDF (2048 MB) and Archives (256 MB). These file type sizes can be adjusted within the range of 1 KB to 4 GB to accommodate your specific needs.

Additionally, in the Windows environment, a default time-out of 10 seconds is applied. For MacOS, a strict 10-second time-out is enforced due to Apple OS architecture, which terminates processes that do not respond promptly. Linux currently operates without a specific time-out limitation.

**Note:** This setting only applies to Content Aware Protection policies and does not affect eDiscovery Policies and Max File Size for File Shadows.

5.7.5. Outside Hours and Outside Network

From this section, you can manage Outside Network and Outside Hours Policies, for both Device Control and Content Aware modules.

- **Outside Hours policies** – enable the setting and then set the **Working days**, **Business hours start time**, and **end time**.

- **Outside Network policies** – enable the setting and then add the **DNS Fully Qualified Domain Name** and **DNS IP Addresses**.

Once these settings are made, the fallback device type rights can be set Globally, per Groups, Users, or Computers.

**Important:** When triggered, fallback policies supersede the standard device rights. Regarding fallback policies, the Outside Network Policies supersede the Outside Hours Policies.

**Note:** For Content Aware Policies, the Outside Network and Outside Hours Policy Type also needs to be selected.
5.7.6. Transfer Limit

From this section, you can set the transfer limit, within a specific time interval (hours). Once the limit is reached, file transfers to storage devices (Device Control) to control applications (Content Aware Protection) will no longer be possible, until the time interval expires and the count is reset. Similarly, file transfers through Network Shares can also be included in the Transfer Limit.

The mechanism that checks when the Transfer Limit is reached has been designed in such a way that it does not impact the performance of the computer.

Therefore, there might be a slight delay between the exact time the limit is reached and the enforcement of the transfer restrictions. In general, it’s just a few seconds but also depending on the network, it could be up to a few minutes.

There are three actions to choose from when the Transfer Limit is reached:

- **Monitor Only** – this setting reports when the limit is reached
- **Restrict** – this setting blocks the devices and applications that have been defined in the Device Control policies
- **Lockdown** – this setting blocks all devices, regardless if they have been defined within the Device Control policies, including the network interfaces and therefore, any type of transfer

**Note:** To re-establish the Server-Client communication before the Transfer Limit Time Interval expires, a Transfer Limit Reached Offline Temporary Password is available. For detailed information, refer to the **Offline Temporary Password** chapter.

You can enable a Transfer Limit Reached Alert and schedule a Transfer Limit Reached Report on a daily, weekly, or monthly basis.

5.7.7. Debug Logging

You can use this feature to collect logs for a specific issue and send the resulting archive to the Endpoint Protector Server on the Reports and analysis section, the Logs Report page.
By enabling this feature, the Endpoint Protector Client will create the log file (general log file), and if Deep Packet Inspection is enabled, it will collect supplementary Deep Packet Inspection logs along with ssisplit logs.

**Note:** We recommend using the Debug level mode as it contains more than error and warning type information.

![DEBUG Logging](image)

### 5.7.7.1. Debug Logging Usage

#### Manual Logging

To use the debug feature and collect logs, follow these steps:

1. On the **Global/Computer/User Settings** page, enable the following settings:
   - **Debug Mode** from the **DEBUG logging** section
   - Select the logs level (None, Error, Warning, Informational, Debug)
   - For Error, Warning, Informational, and Debug log levels select if you want to obfuscate sensitive data
   - **Save**

**Note:** Read the [Data Obfuscation Rules](#) section for more information.

![Endpoint Protector Client Configuration](image)

0. Right-click the **Endpoint Protector Client** icon and select **Update Policies Now**;
0. Replicate the issue to generate the corresponding logs;
0. Open the Endpoint Protector Client and go to the **Troubleshooting** tab;
0. Click **Upload Logs** - this will upload the logs on the Endpoint Protector Server;
0. Go to the **Global Settings** page and disable Debug Mode.
● Automatic Logging

You can also substitute the user action from the Manual Logging procedure (steps 4 and 5) by using the automatic logging option.

This option is available from Device Control on the Computer page.

Hover over a computer, right-click, and select Collect diagnostic - this will collect logs from a specific computer without input or knowledge from the computer user.

Logs will be sent to the Endpoint Protector Server on the Logs Report page, Artifact Received events are registered when diagnostic data are received.

5.7.7.2. Debug Logging Actions

To view the log actions, go to the Device Control module, on the Computers page and click the Actions column.
● **Collect Diagnostics** - registers an event when diagnostic data are requested (Artifact requested event)

● **Go to Diagnostic data** - this option redirects the user to the Reports and Analysis module on the Logs Report page to Artifact received type events with debug mode logs.
- **Terminate Client** - this option terminates the Endpoint Protector Client

- **Forced Restart Computer** - this option sends a force reboot command to the computer, restarting it in 10 minutes after using the command. The user receives a message warning to avoid losing unsaved documents.

  Are you sure you want to issue a restart computer command to this client machine(s)?

  Use this option with caution. The target machine will receive a forced Reboot command, restarting the endpoint 5 min after receiving the setting. Unsaved documents will get lost!

  ![Diagram of Device Control - Computers]
5.7.7.3. Data Obfuscation Rules

All data is obfuscated according to the following rules:

- the first 4 characters are displayed if the length of the threat is lower than 12 characters

or

- the first 6 characters are displayed if the length of the threat is longer than 12 characters

Specific use cases:

1. For **credit cards**, the PCI Security Standards were implemented
2. For **SSNs**, the last 4 characters are displayed
3. For **Brazil ID** (CPF), the first 3 and the last 2 characters are obfuscated

**Important:** Data is not obfuscated for the file-type threat, file-size threat, and date threat.
5.7.8. Easylock Settings
From this section you can allow EasyLock to be installed and run only on computers that have Endpoint Protector installed or in relation to a list of trusted Endpoint Protector Servers.

5.7.9. Additional Information
From this section you can restore global settings to default and view the name and date when the action was performed.

5.7.10. Display Settings
From this section you can set the maximum number of logs displayed on the Endpoint Protector Server and the number of reports per page.
You can set a maximum number of 10,000 logs to be displayed per report. To export all entries when the log number exceeds the maximum 10,000 limit, use the **Create export** option or narrow the search using filters.

**Note:** The information you set on this setting will also be applied for eDiscovery.

### 5.8. Custom Classes

This section provides you with the option to create new classes of devices for easier management. It is a powerful feature, especially for devices belonging to the same vendor and/or being the same product (same VID and/or PID).

A new Custom Class can be created by clicking on the Create. An existing policy can be edited by double-clicking on it.

You can edit, duplicate or delete a policy after selecting the policy.

Before adding devices to a Custom Class, the Name, Description, Device Type (USB Storage Devices, Cameras, etc.), Device Right (Allow Access, Block Access, etc.) must be provided. Once this is done, there are multiple ways of adding devices to a Custom Class:

- **New Device (VID, PID, Serial Number)** – will allow at Step 2 to add new devices based on Vendor ID, Product ID, and Serial Number.
● **Existing Device (Wizard)** – will allow at Step 2 to add devices previously connected to protected computers and already in the Endpoint Protector database.

![Device Wizard](image)

● **Device Serial Number Range** – will allow at Step 2 to add multiple devices at the same time, by specifying the first and last Serial Number in the range. The recommended use for this feature is for devices that have a consecutive range, with a clear, noticeable pattern.

![Device Wizard](image)

**Note:** Although this feature can work in situations where the Serial Number range does not follow a noticeable pattern, this is not recommended. In this type of situation, some devices will be ignored by Endpoint Protector and the Custom Class will not have the expected effect.

● **Bulk List of Devices** – will allow at Step 2 to add up to 1000 devices at the same time. There are two methods to choose from, either importing a list or simply pasting the information.

![Device Wizard](image)

● **Device Class (Device Type)** – will allow at Step 2 to add a specific right to a Device Type. This option is intended to be used in scenarios when a very fast way to change all device types in the system but specific device rights were granularly added to some users or computers.

**Example:** For the case above, we created a Custom Class CD-ROM Allow and set Allow access rights to devices of type CD-ROM /DVD-ROM. Let’s say that CD-ROMs have Deny access rights set on Client PC CIP0. Once the custom class CD-ROM Allow is created and
Custom Classes is enabled, all the CD-ROMs/DVD-ROMs will have access, even if on the Client PC CIP0 they have Deny access.

5.9. Priorities for device rights

Computer Rights, Group Rights, and Global Rights form a single unit and they inherit each-others settings. This means that changes to any one of these entities affect the other ones.

There are three levels of hierarchy: Global Rights, Group Rights, and Computer Rights, the latter being the deciding factor in rights management.

The device rights surpass all computer, group, and global rights.

The user rights are on the same level as the computer rights. The priority can be set from the System Settings section.

**Note:** For detailed information, refer to the **Department Usage** chapter.

Select an option to grant access for clients based on the Department Code. You can also view the Default Department code - defdep.

**Note:** For detailed information, refer to the **System Departments** chapter. Department Usage

Select an option to grant access for clients based on the Department Code.

You can also view the **Default Department** code - defdep.

**Note:** For detailed information, refer to the **System Departments** chapter.

5.9.1. Session Settings

You can modify the following session timeout settings:

- **Session Timeout** – set the amount of time the user is inactive until the session expires between 5 and 60 minutes
- **Timeout counter** – set the amount of time for the session timeout countdown between 5 seconds and Session Timeout minus one minute

**Example:** If you define the Session Timeout to 5 minutes and the Timeout counter to 60 seconds, then after 4 minutes of inactivity you will be notified by the pop-up window that in 60 seconds you will be logged out.
If you remain idle for the defined amount of time, then Endpoint Protector stops responding and displays a message that indicates the session will expire in the predefined countdown.

You can choose to log out or continue your session, resetting the session timeout interval.

**Example:** Device X is allowed from Global Rights. If in the Computer Rights section, the same device does not have permission to be used, the device will not be usable. Same applies vice-versa: if the device lacks access permission globally, and has permission set per computer, the device will be allowed. The same applies for Global Rights and Group Rights: if
globally the device does not have permission to be used, and group permission exists, the device will be allowed.

5.9.2. Priorities for Device Control Policies

By default, only the Standard Device Control Rights are available. They include the Device Types and the Already Existing Devices sections.

Custom Classes can be defined. They represent a group of devices that have particular access right across the entire network. Custom Classes surpass the Standard rights.

If enabled, Outside Network and Outside Hours device rights can be configured. These surpass the Custom Classes rights.

The Offline Temporary Password rights allow the creation of exceptions from applied rules. These rights surpass all others.
6. Content Aware Protection

This module allows the Administrator to set up and enforce strong content filtering policies for selected users, computers, groups, or departments and take control over the risks posed by accidental or intentional file transfers of sensitive company data, such as:

- **Personal Identifiable Information (PII):** social security numbers (SSN), driving license numbers, E-mail addresses, passport numbers, phone numbers, addresses, dates, etc.

- **Financial and credit card information:** credit card numbers for Visa, MasterCard, American Express, JCB, Discover Card, Diners Club, bank account numbers, etc.

- **Confidential files:** sales and marketing reports, technical documents, accounting documents, customer databases, etc.

**Important:** Endpoint Protector cannot scan encrypted files or applications that use encryption to secure communication.

To prevent sensitive data leakage, Endpoint Protector closely monitors all activity at various exit points:

- Transfers on portable storage and other media devices (USB Drives, external HDDs, CDs, DVDs, SD cards, etc.), either directly or through encryption software (e.g., Enforced Encryption)

- Transfers on local networks (Network Share)

- Transfers via the Internet (E-mail Clients, File Sharing Application, Web Browsers, Instant Messaging, Social Media, etc.)

- Transfers to the cloud (iCloud, Google Drive, Dropbox, Microsoft SkyDrive, etc.)

- Transfers through Copy & Paste / Cut & Paste

- Print screens

- Printers and others
6.1. Content Aware Protection Activation

Content Aware Protection comes as the second level of data protection available in Endpoint Protector. The module is displayed but requires a simple activation by pressing the Enable button. If not previously provided, the contact details of the Main Administrator will be required.

**Note:** Any details provided will only be used to ensure the Live Update Server is configured correctly and that the Content Aware Protection module was enabled successfully.

**Important:** The Content Aware Protection module is separate from Device Control or eDiscovery modules, and requires separate licensing.
6.2. Dashboard

This section offers a quick overview in the form of graphics and charts related to the Content Aware Protection module.

6.3. Content Aware Policies

Content Aware Policies are sets of rules for sensitive content detection that enforce file transfers management on selected entities (users, computers, groups, departments).

From this section, you can create a new policy, edit or delete an existing policy or create and apply a predefined policy.

**Example:** A Content Aware Policy can be set to only block Credit Cards AND Email Addresses. In this case, a file that contains a Credit Card AND an email address will be blocked, but if transferring a file that only contains Credit Cards, it will not be blocked.

Each company can define its sensitive content data lists as Custom Content Dictionaries corresponding to their specific domain of activity, targeted industry, and roles.

To ease this task, the Content Aware Protection module comes with a Predefined Content Dictionary that covers the most used sets of confidential terms and expressions.

**Example:** A policy can be set up for the Financial Department of the company to block Excel reports sent via E-mail or to report all transfers of files containing personally identifiable and financial information (e.g., credit card numbers, E-mail, phone numbers, social security numbers etc.).

**Note:** Content Aware Policies also apply to File Allowlist (Device Control > File Allowlist). This means that all files that were previously allowed will be inspected for sensitive content detection, reported, and/or blocked, according to the defined policy.
Exactly like Device Control policies, the Content Aware policies continue to be enforced on a computer even after it is disconnected from the company network.

One or more Content Aware Policy can be enforced on the same computer, user, group, or department. To avoid any conflicts between the applied rules, a prioritization of policies is performed through a left-to-right ordering. The leftmost policy has the highest priority (Priority 1), while the rightmost policy has the lowest priority. Changing priorities for one or more policies can be performed by moving the policy to the right or the left with a simple click on the left arrow for higher priority or on the right arrow for lower priority.

To manage the Content Aware Protection policies more easily, use the following options:

- switch between the Grid or Widget view options from the top-right corner
- use the Top button to assign the highest priority to a policy
- double-click on a policy from the Priority column to edit its priority
6.3.1. Policy Information

You can create up to 48 Content Aware policies.

To create a Content Aware Policy, provide the following information:

**Note:** Depending on the specific application and OS, some limitations may apply.

- **OS Type** - select the operating system to which the policy applies, Windows, macOS, or Linux
- **Policy Name** – add a name for the policy
- **Policy Description** – add a description for the policy
- **Policy Action** - select the type of action you want the policy to perform
  - **Block & Report** – this policy will deny all transfers of data that include sensitive content and report the action
  - **Report only** – this policy will allow all transfers of data that include sensitive content and will only report the action
  - **Block only** - this policy will deny all transfers of data that include sensitive content but not report the action
  - **Block and Remediate** - this policy will deny all transfers of data that include sensitive content but allow the user to remediate the action by using a justification

**Note:** Initially, we recommend using the **Report only** action to gain a better view of data use across your network and not interrupt your activity.

- **Policy Type** - select the policy type, Standard, Outside Hours, or Outside Network

**Note:** To enforce the Outside Hours and Outside Network options, after you save the policy, enable the setting on the specific device from **Device Control, Global settings, Group or Computers**.

- **Policy Template** – select a custom notification from the drop-down list or create one from **System Parameters, Device Types and Notification, Custom Content Aware Protection Notifications** section
- **Policy Status** – enable to set policy status to active
- **Client Notifications** – enable this setting to send notifications to clients
- **Global Thresholds** – if disabled, the threshold can be considered a Regular Threshold
- **Threat Threshold** – type the number of maximum allowed content violations for a file transfer
- **File size threshold** – enter the file size (in MB) starting from which the file transfer is either blocked or reported
Note: If a File Size Threshold is set, it will be applied to the whole policy, regardless of what file types or custom contents are checked inside the policy. The value used in the File Size Threshold must be a positive, whole number.

- **Apply Policy if File Size Threshold is Matched** – enable this setting to apply the policy in combination with the threshold. The content selected from the Denylist will be blocked taking into consideration the threshold.

**Important:** This setting does not apply for **File Name and File Location**.

Note: The Threshold option applies only to multiple filters, including Predefined Content, Custom Content, and Regular Expressions. As a general rule, it is recommended that Block & Report policies that use the Threshold should be placed with higher priority than Report Only policies.

6.3.1.1. **Regular and Global Threshold Use Cases**

1. Set a Block & Report policy with 4 threats, on the transfer of Social Security Numbers (SSN) for several Internet browsers.

The **Regular Threshold** set to 4 threats will block all transfers on the selected browsers which contain four or more individual SSN numbers, but it will not block the transfers with 1, 2, 3 x SSN instances.

In contrast to the Regular Threshold which blocks 4 or more threats of the same type, the **Global Threshold** blocks 4 or more threats of different types combined.

2. Set a Block & Report policy with 2 threats, on the transfer of a Social Security Number (SSN) and a Phone number.

The 2 threats will not be blocked by a Regular Threshold policy, only by one with a Global Threshold. On the other hand, 2 Social Security Numbers will be blocked by policies with both types of thresholds set at 2.
6.3.2. Policy Exit Points
You can monitor transfers from the following exit points:

6.3.2.1. Applications
- **Web Browsers** (e.g., Internet Explorer, Chrome, Firefox, Safari, etc.)
- **E-mail** (e.g., Outlook, Thunderbird, Lotus Notes, etc.)

**Important**: Universal Windows Platform applications, including the Windows 10 Mail application, run in an isolated environment, restraining the use of add-ons. This will prevent Content Aware policies with Windows Mail set as Exit Point to block restricted file transfers.

- **Instant Messaging** (e.g., Skype, Pidgin, Google Talk, etc.)
- **Cloud Services / File Sharing** (e.g., Google Drive Client, iCloud, Dropbox, DC++, etc.)
- **Social Media / Others** (e.g., iTunes, Total Commander, GoToMeeting, etc.)

**Note**: Select Adobe Flash Player from the Web Browser category to block sites that use Adobe Flash Active X.

![Policy Exit Points screenshot](image)

6.3.2.2. Storage Devices
From the storage devices tab, you can select to monitor transfers:

- **only to Custom Classes**
- **for all Storage Devices** - enable the Apply policy to all storage devices setting to enforce content policies on all storage devices, regardless of Custom Classes.

**Note**: For Windows, file transfers will be monitored both to and from removable media.

**Important**: On Linux the paste functionality only works when the default gnome session is Xorg. On other gnome sessions the paste functionality is disabled (ex: wayland).
Block CD/DVD Burning

This feature is only available for Windows, built-in or third-party burning features.

To restrict the user from saving sensitive content on a CD or DVD using the built-in Windows features, follow these steps:

1. Create a Content Aware Policy;
2. From the Policy Exit Points section, on the Storage Devices tab, enable the Apply policy to all storage devices setting;
3. From the Policy Denylist section, select the threats you want the policy to detect.

To restrict the user from saving sensitive content on a CD or DVD using third-party applications, follow these steps:

1. Create a Content Aware Policy;
2. From the Policy Exit Points section, on the Storage Devices tab, enable the Apply policy to all storage devices setting;
3. On the Applications tab, from the Social Media/Others options, select the following:
   - CDBurnerXP
   - ImgBurn CD/DVD
   - InfraRecorder CD - DVD
4. From the Policy Denylist section, select the threats you want the policy to detect

**Note:** The feature will apply to CD/DVD burning options Like a USB flash drive and With a CD/DVD player, using either Drag and Drop or Copy and Paste actions.

### 6.3.2.3. Clipboard

The Clipboard functionality enables you to monitor all content captured through Copy & Paste or Cut & Paste operations.

**Note:** The Clipboard functionality applies only to confidential content that is defined inside the Policy Denylists section for the Source Code tab, Predefined Content, Custom Content, or Regular Expressions.
The Clipboard functionality provides a certain degree of granularity and can be enabled:

- **Clipboard** – enable this setting to monitor all content from a computer, regardless of the defined exit points.

**Note:** This setting only applies to **Copy** operations.

When performing a **Copy** operation, the Endpoint Protector Client will inspect the clipboard content and if confidential information is detected, the content **will be deleted**. As such, the **Paste** operation will not work because the clipboard content was deleted.

- **Source code** – enable this setting to detect the defined in the policy.

**Note:** This setting applies to **Copy** or **Paste** operations.

The Endpoint Protector Client will inspect the clipboard content for source codes and if source code is detected and monitored in a Content Aware policy (e.g., C++ is selected in a Content Aware policy, and the detected clipboard content is C++) the content **will be blocked** on a **Copy** or **Paste** operation (depending if the **Apply Paste restrictions to all monitored applications** settings is enabled)

- **Detect Images** – enable this setting to detect copying images to clipboard

The following image types will be targeted:

1. print screen type images - the content is automatically blocked
2. image files copied with CTRL+C shortcut and pasted to clipboard (this will paste the file URL to clipboard)

**Note:** If multiple files are copied and the content contains at least one image, the file content **will be blocked**.

Similar to code source detection, the Detect images setting applies if the file type is blocked in Content Aware Protection policy (if the user will copy a PNG file, the file will be blocked if the PNG file type is checked in the Content Aware Protection policy).

The Endpoint Protector notifier will save the content of an image in a temporary location, which will be moved if shadow is enabled or deleted if not after scan.

- **To inspect certain applications and set Paste restrictions, enable the **Apply Paste restrictions to all monitored applications** setting**

**Note:** This setting restricts the **Paste** operations for the defined Policy Exit Points.

When performing a **Copy** operation, the Endpoint Protector Client will inspect the clipboard content and if confidential information is detected, the content **will be allowed, instead**, it will **block** a **Paste** operation if the application is monitored in a Content Aware policy.

**Important:** The **Paste** operation is allowed when the user changes the window to other applications.
**Example:** In a Content Aware policy, Firefox is monitored, Chrome is not monitored and the Apply Paste restrictions to all monitored applications setting is enabled. The user performs a Copy operation from Notepad which contains confidential information, then:

- The Paste operation on Firefox is blocked
- The Paste operation on Chrome is allowed

- To inspect extended applications and set Paste restrictions, enable the **Extend Paste restrictions to bellow applications** setting

**Note:** This setting restricts the Paste operation for the defined applications.

Use this setting to extend the applications not listed in a Content Aware policy and **block** the Paste operations.

**Example:** Microsoft Word is not listed in a Content Aware policy, but you can select the application from the list to monitor the Paste operation on the Microsoft Word app.

On-demand, Endpoint Protector can add other applications.

1. **Network Share**
   For Network Share for macOS, Endpoint Protector will report all the events for Report Only policies. For Block & Report policies the transfer from a Local Share towards the Local Disk, Controlled Storage Device Types, and Controlled Applications are blocked.

2. **Thin Clients** applies to file transfers to thin clients drives.

3. **Print Screen** applies to the screen capture options.
4. **Printers** apply to both local and network shared printers.

**Note:** When enabled, it is recommended to enable the **Advanced Printer and MTP Scanning** option in **Settings** (Global, Groups, Computers, etc.)

### 6.3.3. Content Detection Summary

The Custom Detection Summary displays all predefined content, custom content, regular expressions, and HIPAA which were checked in the Content Aware Policy.

You can use the **Content Detection Rule** to define the policy by combining multiple criteria using the operators **AND**, **OR**.

**Note:** The feature is available for **Premium** licenses and also enables **Restrict Content Detection** to specific file types and the **Context Detection Rules**.

To edit a Content Detection Rule, click **Edit** and then, on the **Define operation** section, provide the following information:

- Select **operator** - **OR** (default), **AND**
- Enable **Threshold** and type the number adjacent to each entry from 1 to 1000; this will disable the **Global Threshold** setting from the **Policy Information** section.
- **Add item** and select from the drop-down a PII; before saving the operation, you can change PII by selecting from the drop-down list. To delete an entry from the list, click **x** adjacent to each PII.
- **Add group**

Use the up and down arrows or drag and drop an entry from the list to change the order from the operation.

To **Restrict Content Detection**, select from the drop-down list the file types you want to apply the Content Detection Rule to.

If no file type is set, the content defined in the content Detection Rule will be searched in all the file types that are not blocked by this policy.
The **Context Detection Rules** is a **Premium** feature that allows you to specify the minimum or maximum number of contexts matches for one or more threat types previously defined in the Content Detection Rule and reducing false positive detections.

**Important:** You can create Context Detection Rules only if you define a **Content Detection Rule** using an **OR** operator.

To create a new **Context Detection Rules** click **Add**, fill in the following and then **Save**:

- **Name** – add a name for the context detection rule
- **Apply Contextual for Items** – select from the drop-down list the predefined content selected in the Content Detection Rule
- **Proximity** – add a number between 50 and 3000
- **Included Context** – select the AND/OR operator and then select from the drop-down list the custom content, RegEx or HIPPA you want to be included in the rule
- **Excluded Context** – select the AND/OR operator and then select from the drop-down list the custom content, RegEx or HIPPA you want to be excluded from the rule

**Note:** Custom content used in Content Detection rules will not be displayed in the included and excluded context drop-down lists.

- **Apply context rule for** - select if you want to apply the rule to **All items** or **At least 1 item**.

**Note:** You can create a maximum number of 15 Context Detection Rules.

6.3.4. **Policy Denylists and Allowlists**

The policy denylist and allowlist specify the content to be detected – it includes file type filtering, predefined content filtering, custom content filtering, file allowlists, regular expressions and domain allowlists, deep packet inspection, etc.

6.3.4.1. **Policy Denylists**

You can use the following Denylists:
● **File Type** - since many files (e.g.: Programming Files) are actually .TXT files, we recommend more precaution when selecting this file type to avoid any unexpected effects.

**Note:** File type detection will not always work accurately for some very large password-protected Microsoft Office files.

● **Source Code** - An N-gram based detection method is used to increase the accuracy of these file types. However, as various source code is closely linked together (e.g.: C, C++, etc.), these also are checked. To make things easier, Endpoint Protector automatically marks these correlations.

When the Deep Packet Inspection is enabled an extended way to monitor Git is available. If Git is selected from the Restricted Apps, Git-related actions (fetch, clone, push, pull) will be blocked, regardless of the git application used. This will result in completely blocking Git. However, Deep Packet Inspection Allowlists can be used to allow a specific Git, linked to a specific domain (e.g.: internalgit.mydomain.com).

**Note:** All Git traffic is encrypted therefore, allowing a specific domain will result in any file transfers to be allowed, regardless of content or other policy restrictions defined.

If Git is selected from Restricted Apps, no Endpoint Protector client notifications and logs will be generated for the Git-related actions (fetch, clone, push, pull).

● **Predefined Content** - the majority of the Predefined Content items are country-specific (e.g. Australia, Canada, Germany, Korea, United Kingdom, United States, etc.). To avoid a large number of logs or potential false positives, only enable the Passports that apply to your region or sensitive data.

### Italian SSN and ID usage

Starting with Endpoint Protector server version 5.7.0.0, Italian SSN is added to the PII list. Similar to Italian ID, if selected from the list of PII's, the SSN will detect the same entity.

When using Italian SSN and ID, we recommend you upgrade to the latest Endpoint Protector agent version.

To maintain compatibility with older agent versions after the server upgrade, Italian ID will remain under section ID and server upgrade will retain previous settings, including Italian ID.

- Use Italian SSN when deploying to agent versions xxx and later
- Use Italian ID when deploying to agent versions xxx and earlier
- Use both Italian SSN and ID for a mixed environment of new and older agent versions

Because the Italian SSN and ID detect the same entity, do not select Italian ID to avoid multiple reporting results.

The new Endpoint Protector agent versions will report on both Italian ID and SSN.

● **Custom Content**
6.3.4.2. HIPAA compliance

Any Content Aware Protection policy automatically becomes a HIPAA policy if any options from the HIPAA tab are selected. The available options refer to FDA-approved lists and ICD terms. These will automatically report or block transfer files containing PII like Health Insurance Numbers, Social Security Numbers, Addresses, and much more.

Note: For a HIPAA policy to be effective and more accurate, it is recommended to utilize Contextual Detection Rules in conjunction with Predefined Content and Custom Content filters. To enhance precision, users should also enable 'Whole Word Only' under Custom Content. The ICD-11 dictionary focuses solely on specific terms, not insurance codes.

Note: It is advisable to set appropriate thresholds and combinations of arguments to minimize false positives for shorter disease descriptions.

6.3.4.3. Policy Allowlists

You can use the following Allowlists:
Note: For detailed information on Denylists and Allowlist, refer to the Denylists and Allowlists chapter.

Important: The Content Aware Protection Policies continue to report and/or block sensitive data transfers from protected computers even after they are disconnected from the company network.

Logs will be saved within the Endpoint Protector Client and will be sent to the Server once the connection has been reestablished.

6.3.5. DPI Monitored URL Categories

You can define the monitored URL categories the Deep Packet Inspection will filter. If none is selected, Deep Packet Inspection will filter all content uploaded for any URL.

You can add, delete and edit URL Categories from the Denylists and Allowlists section.
6.3.6. Policy Entities

The final step in creating a policy is selecting the entities that it will apply to from the available ones:

- Departments
- Groups
- Computers
- Users

**Note:** If a Content Aware Policy was already enforced on a computer, user, group, or department, when clicking on it, the corresponding network entities on which it was applied will be highlighted.

You can also define a list of entities that will be excluded from the policy by selecting from the Excluded section.
6.3.7. Block and RemEDIATE Policies

Block and RemEDIATE policies are a category of Content Aware Policies only available if Premium licenses are available.

This category of policies gives the end-user the possibility to resolve the Content Aware threats by using justifications.

You can create Block and RemEDIATE Content Aware Policies from the Content Aware Protection section, Create Content Aware Policies, Policy Action, Block and RemEDIATE.

When detected, Content Aware threats are displayed:

- in the Endpoint Protector notifier, the Content Aware tab
- as pop-up notifications if this option is enabled from the Settings section

To remediate the threat, the user has to follow these steps:

1. Open the **Endpoint Protector notifier** and go to the **Content Aware Protection** tab;
2. Select the file for remediation and click **Self Remediate**;
3. On the **Self Remediate** section:
   a. select a **justification** from the drop-down list
   b. add a **reason** for the justification (if required)
   c. navigate to the **custom URL** situated under the logo
   d. add your credentials if the **Require Credentials** setting was enabled (click the username icon to refresh your current username)
   e. add the **number of minutes** needed to remediate the device (you can hover over the default number to view the maximum time interval)
   f. click **Authorize**

**Note:** You can manage more settings for the Self Remediate feature from System Preferences and **User Remediation** sections.

User Remediation for Content Aware Protection can remediate file transfers via web domains.

To apply User Remediation on specific web domains, enable Deep Packet Inspection from Global/Computers/Users/Group. This feature will then be enabled by default for Browsers and Desktop Email applications.

For other applications, you need to manually enable Deep Packet Inspection from the Content Aware Protection module, the Deep Packet Inspection section, on the Act
ions column.

- **When Deep Packet Inspection is enabled** – you can apply User Remediation for files transferred on a specific web domain.

  E.g., If you upload a file on uploadsite.com and apply User Remediation, you can only upload on uploadsite.com, not on otheruploadsite.com.

- **When Deep Packet Inspection is disabled** – you can only apply User Remediation for files transferred on a specific application.

  E.g., If you upload a file on Chrome and apply User Remediation, you can upload the file on any URL from Chrome.
You can view the web domains used for the User Remediation in the Endpoint Protector Client, the Content Aware Protection tab on the Web Domains column.

![Endpoint Protector Client Version 2.7.0.9](image)

### 6.3.8. Applying multiple Content Aware Policies

Content Aware Protection is a very versatile tool, where you can perform the granular implementation of actions regarding the report and/or block and report of files.

A Content Aware Policy is a set of rules for reporting or blocking & reporting the selected information. All the other options left unchecked will be considered as Ignored by Endpoint Protector.

When applying two policies to the same PC, it is possible to block one type of file, for example, PNG files, when they are uploaded through Mozilla Firefox, while a second policy is to report only PNG files when they are uploaded through Internet Explorer. In the same way, it is possible to report only files that contain confidential words from a selected dictionary that are sent through Skype, while the second policy is to block the same files if they are sent through Yahoo Messenger. Similarly, it is possible to create combinations that block a file type or a file that contains predefined content/custom content/regular expression for one application, while letting it through reporting it only for another.
The following rules are used in the application of one or more Content Aware Policies on a computer/user/group/department for each separately selected item (e.g., a specific file type, predefined information, or a custom content dictionary):

<table>
<thead>
<tr>
<th>Policy A with Priority 1</th>
<th>Policy B with Priority 2</th>
<th>Policy C with Priority 3</th>
<th>Endpoint Protector Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGNORED</td>
<td>IGNORED</td>
<td>IGNORED</td>
<td>Information will not be blocked or reported.</td>
</tr>
<tr>
<td>IGNORED</td>
<td>IGNORED</td>
<td>REPORTED</td>
<td>Information will be reported.</td>
</tr>
<tr>
<td>IGNORED</td>
<td>REPORTED</td>
<td>REPORTED</td>
<td>Information will be reported.</td>
</tr>
<tr>
<td>REPORTED</td>
<td>REPORTED</td>
<td>REPORTED</td>
<td>Information will be reported.</td>
</tr>
<tr>
<td>IGNORED</td>
<td>IGNORED</td>
<td>BLOCKED</td>
<td>Information will be blocked.</td>
</tr>
<tr>
<td>IGNORED</td>
<td>BLOCKED</td>
<td>BLOCKED</td>
<td>Information will be blocked.</td>
</tr>
<tr>
<td>BLOCKED</td>
<td>BLOCKED</td>
<td>BLOCKED</td>
<td>Information will be blocked.</td>
</tr>
<tr>
<td>IGNORED</td>
<td>REPORTED</td>
<td>BLOCKED</td>
<td>Information will be reported.</td>
</tr>
<tr>
<td>IGNORED</td>
<td>BLOCKED</td>
<td>REPORTED</td>
<td>Information will be blocked.</td>
</tr>
<tr>
<td>REPORTED</td>
<td>IGNORED</td>
<td>BLOCKED</td>
<td>Information will be reported.</td>
</tr>
<tr>
<td>BLOCKED</td>
<td>IGNORED</td>
<td>REPORTED</td>
<td>Information will be blocked.</td>
</tr>
<tr>
<td>REPORTED</td>
<td>BLOCKED</td>
<td>IGNORED</td>
<td>Information will be reported.</td>
</tr>
<tr>
<td>BLOCKED</td>
<td>REPORTED</td>
<td>IGNORED</td>
<td>Information will be blocked.</td>
</tr>
</tbody>
</table>

**Important:** The information left unchecked when creating a policy will be considered as Ignored by Endpoint Protector and not as Allowed.

The deep packet inspection feature has been expanded to e-mail scanning based on domain allowing.
A recommended HIPAA should be considered a Content Aware Policy that, besides the options in the HIPAA tab, also has the below configuration:

- All the File Types recognized should be included.
- All Personal Identifiable Information should be Country Specific to the United States (Address, Phone/Fax, and Social Security Numbers)
- Both Internet Protocol Addresses Access should be selected
- The URL and Domain Allowlists options should also be checked

HIPAA policies can be created and used on their own or in combination with regular policies, for better control of the data inside the network. These policies are available for Windows, Mac OS X, or Linux computers.

6.3.8.1. Example: Use Case Nr. 1

Suppose that Company X handles patient medical records that come in electronic formats and which contain general information such as Patient Name, Address, Birthdate, Phone number, Social Security Number, and E-Mail address. The company would like to block the transfer of this data through all the common Windows desktop applications.
Knowing that the sensitive data comes in the format of a profile per patient, the administrator can create a HIPAA policy like the one shown below:

This policy is set on Block & Report with a Global Threshold of 4. It scans the Controlled Storage Device Types (which can be inspected from the System Parameters > Device Types), the Clipboard, and the Network Share as well as all the database of applications recognized by Endpoint Protector. This policy will ONLY block the transfer of those files which contain 4 or more of the PII’s selected inside the policy. All the files which happen to contain just 1 Address or 2 Phone Numbers or 2 E-mails will be transferred.

6.3.8.2. Example: Use Case Nr. 2

Company Y has a large database of patients’ sensitive information. This information is stored in individual office files which contain ten (10) or even more Personal Identifiable Information (PII) items per patient. Other than these files, the company's staff regularly uses some file that contains three (3) of the same PIIs per file. Company Y would like to block the leakage of the files database from its database that contains 10 or more items yet only report the transfer of the files containing 3 items.

You can set up a policy that will block the transfer of files containing 10 PIIs by using a Global Threshold of 10, like in the policy shown below:
Another HIPAA policy can be used to report the transfer of files that contain 3 items of the same kind by using a Regular Threshold set at 3, like the below-shown example:

![Policy Information](image)

The Block & Report policy will have the priority while the Report Only policy will be the second.

### 6.4. Deep Packet Inspection

The Deep Packet Inspection functionality provides a certain degree of granularity, allowing you to fine-tune the content inspection functionality to the network specifications.

**Note:** Enabling Deep Packet inspection could impact upload speed of inspected files. Use our network extension instead of Packet Filter as a possible workaround (i.e., turn Intercept VPN Traffic on).

#### 6.4.1. Deep Packet Inspection Certificate

The Deep Packet Inspection functionality uses Certificates generated from Endpoint Protector Root Certificate Authority to intercept network traffic by Deep Packet Inspection and for Client-Endpoint Protector Server communication.

Endpoint Protector offers the option to automatically refresh Certificates with various scheduling alternatives. After a new Certificate is generated, it will be sent in to the Client and replace the existing one.

To configure **Deep Packet Inspection - Auto-refresh Certificate** feature, please reference the following steps:

1. Go to **System Configuration, System Settings, Deep Packet Inspection - Auto-refresh Certificate** and chose **Automatically** option
2. Choose one of available scheduling options and Save changes.
3. New Certificate will be distributed automatically to the endpoints after it is generated.
4. Reboot of the endpoint is required to enforce a new Certificate.
6.4.2. Deep Packet Inspection Certificate on macOS

Due to the latest changes in the macOS 11.0 that affect Deep Packet Inspection, a new Root Certificate is needed in order for the Deep Packet Inspection feature to work on the mentioned macOS version.

**Note:** Deep Packet Inspection will only work on macOS 11.0 and newer if Deep Packet Inspection Certificate is added for the Endpoint Protector Client.

This certificate can be downloaded from System Configuration, System Settings, and Deep Packet Inspection Certificate and added manually or automatically through deployment solutions.

To add it manually, follow these steps:

1. Go to **System Configuration, System Settings, Deep Packet Inspection Certificate**, and download the **CA Certificate**.

2. Open the **Keychain Access** application from your macOS and select **System**.
3. Decompress the downloaded ClientCerts file.

4. Select cacert.pem file and drag and drop it on Keychain Access, System

5. Double click the x from the newly added certificate and from the Trust section, select Always Trust.
6. **Save** the changes.

**Important**: Please beware, that Regenerating the Server Certificate Stack will force MacOS users to add the new Certificate into the Keychain (on Windows it will be updated automatically).

6.4.3. **Deep Packet Inspection Ports & Settings**

From this section, you can correlate the monitored applications with the ports used in each network, manage settings and add allowed domains for the Gmail provider.

By default, the Deep Packet Inspection functionality comes with a list of predefined ports (80, 443, 8080, etc.). You can add ports from this section, if custom ports are used in a specific network, particularly by one of the monitored applications defined as an Exit Point within a Content Aware Protection Policy.
In this section you can also manage the following settings:

- **Text Inspection** - enable this setting to monitor confidential content typed in Teams, Skype, Slack, Mattermost or Google Spreadsheet, Facebook Post, Facebook Comment, and Instagram Comment online applications.

  **Note:** You need to enable Deep Packet Inspection for Teams, Skype, Slack, and Mattermost to apply the text inspection setting. The list cannot be granularly managed.

  **Important:** In blocking mode, Instant Messaging events related to platforms such as Slack and Google Chat might be generated multiple times. This behavior is attributed to the tools’ inherent retry mechanisms when a message is blocked. Endpoint Protector is designed to block all such retry attempts for enhanced security.

- **DPI Bypass Traffic** – this setting automatically bypasses non-inspectable traffic and sends an event for allowed traffic.
  - Possible Bypass reasons:
    - DPI certificate rejected by third party application
      - e.g. this can happen when certificate pinning is used
    - Unknown TLS handshake
      - e.g. for applications which use custom encryption such as Telegram
    - Website temporarily white listed - possible mTLS connection (SSL setup failure/unsupported TLS protocol).
      - e.g. an SSL error occurred on the destination side
    - Websocket passthrough
      - e.g. upgrade to WebSocket was allowed, e.g. when using WhatsApp Web, Firefox Send etc.
    - Website temporarily whitelisted - Possible mTLS connection (HTTP error code 4xx).
      - e.g. error codes include: "400 Bad Response" or "496 SSL Certificate Required"

  **Important:** Please be aware that the current Default DPI list and the new Default DPI bypass list are exclusively utilized when manually checked within CAP (Content Aware Protection) policies.

- **Detailed Slack Reporting** – available only with Text Inspection enabled and Reporting V2 from System Configuration, System Settings, use this setting to report Destination Details for Slack on the Content Aware Report page from the Reports and Analysis section.
Note: This setting requires an active Internet connection for the Endpoint Protector Client.

- **Peer Certificate Validation** – enable this setting to turn on the Endpoint Protector certificate validation of the websites that are accessed by the user when DPI is active.

**Important**: Disabling this setting will not impact EPP functionality. It should only be disabled when an alternative network traffic inspection product, such as a Secure Web Gateway Solution, is validating website certificates.

- **Monitor webmail** – enable this setting to scan subject and body for Gmail, Outlook and Yahoo on the browser. Attachments will be monitored regardless of this setting.

**Important**: When using Yahoo, the email recipients whitelist for attachments will work only if the attachment is uploaded after the recipients are added. If the recipients are modified after the attachment has been added, the file will not be scanned again and validated against the new recipients list. Inconsistent behavior may be experienced on Linux machines.

You can also use the Monitor webmail feature to detect source code for web browsers emails in subject and body. For email applications, source code can be detected in subject, and for the body, source code cannot be enabled for detection without breaking other functionality.

**Note**: Always use Monitor webmail with Extended Source Code Detection setting enabled.

- **Block unsupported protocols in New Outlook** – enable this setting to block send email functionality in New Outlook without interacting with Outlook legacy functionality.

- **Allowed domains for Google Business accounts** - You can use this setting to allow the users to access specific Google domains for professional usage when Deep Packet Inspection is enabled.

To specify the allowed business accounts, type an entry on the **Add allowed Business accounts** and then click +

The new entry will be displayed on the **Allowed Business accounts** list, from where you can delete by clicking x.

**Important**: Endpoint Protector will block access to all Google domains (business and private) used for Gmail, Google Drive, Google Docs, etc. that are not listed here. If the list remains empty, no Google domain will be blocked.
To use this setting, you need to be familiarized with JSON concepts and structures.

Go over the following Syntax examples considering the values used are the default values from the Endpoint Protector Server UI:

- You can specify multiple paths, separated by a comma ‘,’ inside the curly brackets. The paths will then be parsed and used, in the specified order, one by one, until the information is successfully extracted.

- `[]` takes all entries from the array and parses the result, and can be used with both of the following examples.

1. **Subject extraction example for Yahoo:**

   `subject={requests[0].payloadParts[0].payload.message.headers.subject}`

   - Uses named key-value pairs and arrays ([{}])

   - **Example:** If the array located at the requests key has 3 elements, the path will be expanded for each element:

   - `requests[0].payloadParts[0].payload.message.headers.subject`
   - `requests[1].payloadParts[0].payload.message.headers.subject`
   - `requests[2].payloadParts[0].payload.message.headers.subject`

   The process is then repeated for the payloadParts array.

0. **Subject extraction example for Gmail:**

   `subject={[[1]0][0][1][13][0][7]}`

   - Uses only nested arrays

   - The subject here is located at a specific path inside nested arrays without having to go through all elements of a specific array and use `[]`. 
Important: It is advised, that due to recent changes applied by cloud providers, to not apply any changes in the JSON parser, unless Monitor Webmail is not working

6.4.3.2. Note on Peer Certificate Validation Usage

- If Deep Packet Inspection is ON and Peer Certificate Validation is enabled then you cannot access unsecured websites and a certificate warning message is displayed.

- If Deep Packet Inspection is ON and Peer Certificate Validation is disabled then you can access unsecured websites and no certificate warning messages are displayed.

Example: Your organization uses an SSL inspection proxy or gateway. The certificates injected by the proxy or gateway cannot be validated on the endpoint because they are either invalid or the issuer CA certificate is not installed in the "Trusted Root Certification Authorities" in the computer certificate store.

To allow Deep Packet Inspection to work in this case you must skip peer certificates validation. Endpoint Protector Client assumes that in this case the peer certificate validation is performed by the proxy or gateway so that security is not compromised.

6.4.4. Deep Packet Inspection Applications

From this section, you can enable or disable the Deep Packet Inspection functionality for each application that is subject to this functionality.

Note: Only the applications that support Deep Packet Inspection are available in the list below.
**Important:** The Deep Packet Inspection functionality needs to be first enabled from Device Control, Settings (Global, Groups, Computers, etc.).

**Note:** For detailed information on, refer to the [Global Settings] chapter.

### 6.4.5. Certificate status matrix

The following table lists when Endpoint Protector Server reports specific states:

<table>
<thead>
<tr>
<th>OS</th>
<th>is Available</th>
<th>isTrusted</th>
<th>Server Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>MacOS</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>N/A</td>
<td>Not added</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>Not added</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>Not added</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>N/A</td>
<td>Not trusted</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>Not trusted</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>Trusted</td>
</tr>
<tr>
<td>Linux</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

CoSoSys Confidential. Copyright © 2004 – 2023 CoSoSys SRL and its licensors. All rights reserved.
<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>0</td>
<td></td>
<td>Not added</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
<td>Trusted</td>
</tr>
</tbody>
</table>

**Note:** Linux has dedicated certificate stores.

**Note:** On Windows, if the certificate is added, it is automatically trusted.
This module allows you to create policies that inspect data residing on protected Windows, Macs, and Linux computers. The company’s data protection strategy can be enforced and risks posed by accidental or intentional data leaks can be managed. You can mitigate problems posed by data at rest by discovering sensitive data, such as:

- **Personal Identifiable Information (PII):** social security numbers (SSN), driving license numbers, E-mail addresses, passport numbers, phone numbers, addresses, dates, etc.
- **Financial and credit card information:** credit card numbers for Visa, MasterCard, American Express, JCB, Discover Card, Diners Club, bank account numbers, etc.
- **Confidential files:** sales and marketing reports, technical documents, accounting documents, customer databases, etc.

### 7.1. eDiscovery Activation

eDiscovery comes as the third level of data protection available in Endpoint Protector. The module is displayed but requires a simple activation by pressing the Enable button. If not previously provided, the contact details of the Main Administrator will be required.

*Note:* Any details provided will only be used to ensure the Live Update Server is configured correctly and that the eDiscovery module was enabled successfully.

*Important:* The eDiscovery module is separate from Device Control or Content Aware Protection modules, and requires separate licensing.
7.2. Dashboard

This section offers a quick overview in the form of graphics and charts related to the eDiscovery module.

7.3. eDiscovery Policies and Scans

eDiscovery Policies are sets of rules for sensitive content detection for data stored on protected computers.

An eDiscovery Policy is made up of five main elements:

- **OS Type**: the OS it applies to (Windows, Mac, or Linux)
- **Thresholds**: the number of acceptable violations
Policy Denylists: the content to be detected
Policy Allowlists: the content that can be ignored
Entities: the departments, groups, or computers it applies to

Note: Once the eDiscovery Policies are created, select the type of eDiscovery Scan.

eDiscovery Scans are sets of rules for Policies, defining when to start the data discovery. There are several types of scans:

- Clean scan: starts a new discovery (from scratch)
- Incremental scan: continues the discovery (skipping the previously scanned files)

eDiscovery Automatic Scanning is also available, allowing you to set an Incremental Scan:

- One time – a scan will run once, at the specific date and time
- Weekly – a scan will run every 7 days, from the set date and time
- Monthly – a scan will run every 30 days, from the set date and time

An eDiscovery Scan can be stopped at any time as results can also be automatically cleared. This can be done by using:

- Stop scan: stops the scan (but does not affect the logs)
- Stop scan and clear scan: stops the scan and clears the logs

Note: Use Global Stop and Clear in situations where all the eDiscovery Scans need to be stopped and all the Logs cleared.

7.3.1. Creating an eDiscovery Policy and Scan

You can easily create and manage eDiscovery Policies and Scans from the eDiscovery, Policies and Scans section.
To create a new policy click Create Custom Policy and to edit an available policy, double-click it. You need to select a policy to edit, duplicate or delete a policy.

When creating a new policy, select the following:

- **Policy Information** (OS Type, Policy name, description, action, and type)
- **Policy Exit points**
- **Policy Denylists, Policy Allowlists**
- **Policy Entities** (Departments, Groups, and Computers)

You can use the following thresholds:

- **Limit Reporting eD**
- **Threat Threshold value**
- **File Size Threshold**

You can find more details about Thresholds directly in the Endpoint Protector User Interface.

For detailed information on Denylists and Allowlist, refer to the **Denylists and Allowlists** chapter.

After the eDiscovery Policy has been created, Scanning Actions can be assigned. These include **Start clean scan, Start incremental scan, Stop scan**, and **Clear logs**.
**Note:** Exactly like Content Aware Protection Policies, the eDiscovery Policies and Scans continue to detect sensitive data stored on protected computers even after they are disconnected from the company network. Logs will be saved within the Endpoint Protector Client and will be sent to the Server once the connection has been reestablished.

### 7.4. eDiscovery Scan Result and Actions

After an eDiscovery Scan starts, you can inspect the items found and apply actions to remediate (e.g., delete on target, encrypt on target, decrypt on target, etc.). All results are displayed in the eDiscovery, Scan Results, and Actions section.

You can also access the Scan Results and Actions section directly from eDiscovery > Policies and Scans by selecting a computer from the eDiscovery Scans list and choosing the Inspect found items action. This will automatically filter the Scan Results list and display the items only for that specific computer.

#### 7.4.1. Viewing Scan Results and taking Actions

From this section, you can manage the scan results. A list of all the computers that were scanned can be viewed and actions such as deleting, encrypting or decrypting files can be taken.
You can apply an action to each item individually or, can select multiple items and apply the action simultaneously by using the Choose action button.
8. Denylists and Allowlists

From this section, you can create Denylists and Allowlists that can be used in both the Content Aware Protection and eDiscovery modules. Once defined, these lists can be enabled for a specific policy.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Platform</th>
<th>Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Windows</td>
<td>macOS</td>
</tr>
<tr>
<td>Denylists</td>
<td>Custom Content</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>File Name</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>File Location</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Scan Location</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Regex</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Domain and URL</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>E-mail Domain</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>MIME Type</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Allowed Files</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>File Location</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Allowlists</td>
<td>Network Share</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>E-mail Domain</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>URL Name</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Deep Packet Inspection</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>URL Categories</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
8.1. Denylists

8.1.1. Custom Content

Custom Content denylists are custom-defined lists of terms and expressions detected as sensitive content by Endpoint Protector, available for both Content Aware Protection and eDiscovery modules.

From this section, you can view and add e-mail custom content denylists and from the Actions column, you can edit, delete or export an existing denylist.

To create a new denylist, under the list of available denylists, click Add, provide a name and description and then type or paste items at least three characters separated by a new line, comma, or semicolon. You can import content using the sample file provided on the form and then select the option based on the number of uploaded items.

**Note:** Dictionaries of under 100 items can be edited, while larger dictionaries have to be uploaded again.

Once the denylist is created, it will be displayed on the Custom Content list and will be available when creating or editing a Content Aware Protection or eDiscovery policy.
8.1.2. File Name

File Name Denylists are custom-defined lists of file names detected by Endpoint Protector, available for both Content Aware Protection and eDiscovery modules.

From this section, you can view and add filename denylists and from the **Actions** column, you can edit, delete or export an existing denylist.
To create a new denylist, under the list of available denylists, click Add, provide a name and description and then type or paste the file names separated by a new line, comma, or semicolon. You can import content using the sample file provided on the form.

You can define the content by adding the file name, file name and extension, or just the extension.

- example.pdf filename - all files that end in example.pdf will be blocked (e.g. example.pdf, myexample.pdf, test1example.pdf).
- .epp extension - all files that have the .epp extension will be blocked (e.g. test.epp, mail.epp, 123.epp).

Once the denylist is created, it will be displayed on the File Name list and will be available when creating or editing a Content Aware Protection or eDiscovery policy.

Important: For Content Aware Protection, the File Name Denylists work only for Block & Report type Policies. The Case Sensitive and Whole Words Only features do not apply.

8.1.3. File Location

File Location Denylists are custom-defined lists of locations identified by Endpoint Protector. File transfers within this location are automatically blocked, regardless of the content inspection rules or permissions defined in various Policies.

File Location Denylists are available for both Content Aware Protection and eDiscovery modules.
Enabling the option to **Include subfolders for File Location Denylists** will affect all other File Location Denylists and Allowlists throughout the system. By default, the File Location Denylists apply to all files located in the specific folder but also to any other files located in containing subfolders.

**Note:** In addition to defining the File Location Denylist, the browser or application used to transfer files also needs to be selected from within the Content Aware Protection Policy.

From this section, you can view and add file location denylists and from the **Actions** column, you can edit, delete or export an existing denylist.

To create a new denylist, under the list of available denylists, click **Add**, provide a **name** and **description**, add the items separated by a new line, comma, or semicolon and then select the **groups** and **computers**.

**Important:** File Location Denylist will not apply to groups of users, only to groups of computers. File Location Denylist will only apply for the selected computer groups after 15 minutes.
You can use wildcard patterns in the File Location Denylists to specify wildcard matching. To match a desktop folder on Windows, use the pattern "?:\Users\Desktop".

<table>
<thead>
<tr>
<th>Wildcards Type</th>
<th>File Location</th>
<th>Results matched</th>
<th>Results not matched</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implicit</td>
<td>C:\temp</td>
<td>C:\temp\file.txt</td>
<td>C:\temp1\file.txt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C:\temp\test\file2.txt</td>
<td>C:\Windows\file.txt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C:\tempfile.txt</td>
<td></td>
</tr>
<tr>
<td>Explicit</td>
<td>C:\Windows*</td>
<td>C:\Windows\regedit.exe</td>
<td>C:\Windows.old\regedit.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C:\Windows\system32\notepad.exe</td>
<td>C:\Windows.old\system32\notepad.exe</td>
</tr>
</tbody>
</table>

8.1.4. Scan Location

Scan Location Denylists are custom-defined lists of locations identified by the eDiscovery module. Data at rest within this location are automatically inspected for content, depending on the rules defined in various Policies.
From this section, you can view and add scan location denylists and from the **Actions** column, you can edit or delete an existing denylist.

To create a new denylist, under the list of available denylists, click **Add**, provide a **name** and **description**, add the scan locations separated by a new line, comma, or semicolon or select from the **Predefined Scan Locations** and then **Add to Content**.

When defining a Scan Location, use these special characters to define the path:
- `*` - to replace any word
- `?` - to replace any character

### 8.1.5. Regex

Regular Expressions are sequences of characters that form a search pattern, mainly for use in pattern matching with strings.

You can create a regular expression to find a certain recurrence in the data that is transferred across the protected network. **Regex Denylists are available for both the Content Aware Protection and eDiscovery modules.**

**Important:** If possible, avoid using Regular Expressions, as their complexity typically increases the resources usage. Using a large number of regular expressions as filtering criteria typically increases CPU usage. Also, improper regular expressions or improper use can have negative implications.

From this section, you can view and add regex expressions and from the **Actions** column, you can edit or delete an existing denylist.

To create a new denylist, under the list of available denylists, click **Add**, provide a **name** and **description** and then add the regex expression.
You can **test** a regular expression for accuracy using the right-side option. Add the content and then click Test. If the Regular Expression has no errors, then the same content should appear into the Matched content box, as shown below:

**To match an E-mail:** `[-0-9a-zA-Z.+_]\[@[-0-9a-zA-Z.+_]\](\[a-zA-Z])(\[2,4])`

**To match an IP:** `(25\[0-5]\[2-4][0-9][0-9]?)(\cdot(25\[0-5]\[2-4][0-9][0-9]?)(\cdot(25\[0-5]\[0-9][0-9][0-9][0-9]?))\{3\})`

**Note:** This feature is provided “as is” and requires advanced knowledge of the Regular Expression syntax. No direct support is offered and it is the responsibility of the customers to learn and implement regular expressions and to thoroughly test.

### 8.1.6. Domain and URL

Domain and URL Denylists are custom-defined lists of web addresses identified by Endpoint Protector. Access to domains and URLs from these lists will be denied.

**Note:** Domain and URL Denylists are available only for the Content Aware Protection module.
From this section, you can view and add domain and URL denylists and from the **Actions** column, you can edit, delete or export an existing denylist.

To create a new denylist, under the list of available denylists, click **Add**, provide a **name** and **description** and then **type or paste** items separated by a new line, comma, or semicolon. You can **import content** using the **sample file** provided on the form.

You can create or import up to 100 lists of dictionaries, each dictionary comprising up to 50000 web domains.

**Note**: Dictionaries comprising up to 100 web domains can be edited, but for more extensive dictionaries, you will need to import them again.

You can define the content by adding the file name, file name and extension, or just the extension - **pdf**, **test1example.pdf**. **example.endpointprotector.com**, ***example.com**, ***example*example**, **https://website.com**

Once the denylist is created, it will be displayed on the Domain and URL list and will be available when creating or editing a Content Aware Protection policy.
8.1.7. E-mail Domain

E-mail Domain Denylists are custom-defined e-mail addresses and domains applicable to groups and computers that block the user from sending emails.

**Important**: This feature blocks the user from sending emails regardless of content and type. As the denylist applies to the computer, not the policy, it blocks emails sent from the applications you select that have Report Only or Block and Remediate policies with no remediation possible.

**Note**: This feature is only available for Content Aware Protection when Deep Packet Inspection is enabled and only impacts applications that retrieve the email recipients and are selected on Content Aware Protection Policy.

From this section, you can view and add e-mail domain denylists and from the Actions column, you can edit, delete or export an existing e-mail domain denylist.

To create a new denylist, under the list of available denylists, click Add, provide a name and description, add the items separated by a new line, comma, or semicolon and then select the groups and computers. You can import content using the sample file provided on the form.
8.1.8. Applications

This section introduces the documentation related to CLI (Command Line Interface) commands denylists usage. CLI commands denylists empower customers with greater control over application start events and offer the capability to scrutinize command line arguments used to launch specific applications. This functionality enhances the precision of CAP (Content Aware Protection) policies, enabling users to gain visibility and control over the usage of particular applications.

Example: Consider the scenario of controlling the startup mode of an application, as illustrated by the example below for Google Chrome:

```
chrome.exe --incognito
```

With CLI commands denylists, you can define criteria for command line arguments that match specific application behaviors. This allows you to create CAP policies tailored to your organization's needs, ensuring that the launch and behavior of applications align with your security and compliance requirements.

**Important:** certain native command line utilities such as `ls`, `md`, `cd`, which are embedded in the Operating System Core, may not be captured by CAP visibility. These commands are integral to the functioning of the operating system and are typically excluded from CAP policies, and are not an egress channel.

To define CLI command denylist policies, follow these steps:

1. Navigate to Denylists -> Application tab in the Endpoint Protector Console.
2. Define your criteria based on the command line arguments used by the applications you want to control.
3. Incorporate these criteria into your CAP policies as arguments to ensure precise control and monitoring of application usage.

Follow these steps and leverage CLI commands denylists to enhance your organization's security posture and ensure that applications are used in compliance with your policies and
regulations.

Note: Currently, the EPP Client's visibility is restricted when it comes to PowerShell and PowerShell ISE.

Note: At the moment, we do not offer visibility for basic command line operations on MacOS and Linux, including actions such as touch, cp, cd, mv, and mkdir.

8.2. Allowlists

8.2.1. MIME Type

The content inspection functionally within Endpoint Protector identifies multiple file types. While some files (e.g. Word, Excel, PDFs, etc.) can contain confidential information (e.g. PII,
SSNs, Credit Cards, etc.), other files are highly unlikely to contain such data (e.g. .dll, .exe, .mp3, .avi, etc.).

The purpose of the MIME Type Allowlists is to eliminate the use of resources to inspect redundant and unnecessary files for content, as well as reducing false positives due to information detected in the metadata of files where the risk of data loss is extremely low.

**Example:** As songs or video files cannot contain lists of credit card numbers, there is no need to inspect them using content filters.

MIME Type Allowlists are available for both the Content Aware Protection and eDiscovery modules and apply to Custom Content, Predefined Content, and Regular Expressions.

**Note:** By default, graphic files, media files, some password-protected archive files and some system files are automatically defined within the MIME Type Allowlists. While this can be changed, we recommend only doing so after gaining a deeper understanding of the type of data transferred, used, or stored by the users in your system, and the subsequent logs increase in the Endpoint Protector Server.

8.2.2. **Allowed Files**

Allowed Files Allowlists are custom groups of files you exclude from Endpoint Protector sensitive content detection, available for both Content Aware Protection and eDiscovery modules.
You can add a new allowlist or edit and delete from the **Actions** column.

To create a new allowlist, under the list of available allowlists, click **Add**, provide a **name** and **description** and then select a file from the list or upload a new file you can use in multiple allowlists.

Once the allowlist is created, it will be displayed on the Allowed File list and will be available when creating or editing a Content Aware Protection or eDiscovery policy.

### 8.2.3. File Location

File Location Allowlists are custom-defined lists of locations identified by Endpoint Protector. File transfers within this location are automatically allowed, regardless of the content inspection rules or permissions defined in various Policies.

**File Location Allowlists** are available for both Content Aware Protection and eDiscovery modules.
Enable the **Include subfolders for File Location Allowlists** option to affect all other File Location Denylists and Allowlists throughout the system. By default, the File Location Allowlists apply to all files located in the specific folder but also to any other files located in containing subfolders.

**Important:** In addition to defining the File Location Allowlist, the browser or application used to transfer files also needs to be selected from within the Content Aware Protection Policy.

You can use wildcard patterns in the file location allow list, to specify wildcard matching.

To match a desktop folder on Windows use the pattern "?:\Users\*/Desktop".

<table>
<thead>
<tr>
<th>Wildcards Type</th>
<th>File Location</th>
<th>Results matched</th>
<th>Results not matched</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implicit</td>
<td><code>\file-share\public</code></td>
<td><code>\file-share\public\jdoe\file.txt</code></td>
<td><code>\file-share\c$\file.txt</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>\file-share\public\user512\file2.txt</code></td>
<td><code>\file-server\public\jdoe\file.txt</code></td>
</tr>
<tr>
<td>Explicit</td>
<td><code>*\public*</code></td>
<td><code>\localhost\public\payslip.xlsx</code></td>
<td><code>\localhost\c$\system32\notepad.exe</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>\192.168.20.2\public\Windows\system32\notepad.exe</code></td>
<td><code>\Windows.old\system32\notepad.exe</code></td>
</tr>
</tbody>
</table>

You can add a new allowlist or edit, delete or export from the **Actions** column.
From this section, you can view and add file location denylists and from the Actions column, you can edit, delete or export an existing denylist.

To create a new denylist, under the list of available denylists, click Add, provide a name and description, add the items separated by a new line, comma, or semicolon and then select the groups and computers.

File Location Allowlists will not apply to groups of users, only to groups of computers. File Location Allowlists will only apply for the selected computer groups after 15 minutes.

8.2.4. Network Share

Network Share Allowlists are custom-defined lists of network share addresses where transfers of confidential information will be allowed by Endpoint Protector.

**Note:** Network Share Allowlists are available only for the Content Aware Protection module.

You can use wildcard patterns in the Network Share Allowlist to specify wildcard matching. The Network Share Allowlist can perform matching the whole file name, not only on the directory name, when wildcard patterns are used.

**Important:** The Network Share must be set to Allow Access and Scan Network Share must be checked inside a Content Aware Protection Policy.
You can add a new allowlist or edit, delete or export from the **Actions** column.

To create a new allowlist, under the list of available allowlists, click **Add**, provide a **name** and **description**, add server name or IP address to define a network share path separated by a new line, comma, or semicolon and then select the **groups** and **computers**.

Network Share Allowlists will not apply to groups of users, only to groups of computers. Network Share Allowlists will only apply for the selected computer groups after 15 minutes.

**Important:** Do not type the network share path with backslashes (\) 192.168.0.1\public\users\test; fileserver\documents\example

### 8.2.5. E-mail Domain

E-mail Domain Allowlists are custom-defined e-mail addresses to which sending of confidential information will be allowed by Endpoint Protector.

**Note:** E-mail Domain Allowlists are available only for the Content Aware Protection module.
You can add a new allowlist or edit, delete or export from the **Actions** column.

To create a new allowlist, under the list of available allowlists, click **Add**, provide a **name** and **description** and then **type or paste** items at least three characters separated by a new line, comma, or semicolon. You can **import content** using the **sample file** provided on the form.

Once the allowlist is created, it will be displayed on the E-mail Domain list and will be available when creating or editing a Content Aware Protection policy.

You can use wildcard patterns in the e-mail domain to specify wildcard matching as displayed in the following example.
### 8.2.6. Deep Packet Inspection

Available only for the Content Aware Protection module, Deep Packet Inspection Allowlists are custom-defined lists or dictionaries with web domains Endpoint Protector will allow confidential information uploads.

<table>
<thead>
<tr>
<th>E-mail name</th>
<th>Domain</th>
<th>Results matched</th>
<th>Results not matched</th>
</tr>
</thead>
<tbody>
<tr>
<td>@epp.com</td>
<td><a href="mailto:Robert@epp.com">Robert@epp.com</a>; <a href="mailto:jdoe@epp.com">jdoe@epp.com</a>; <a href="mailto:james@epp.com.ca">james@epp.com.ca</a></td>
<td><a href="mailto:sara@epp.com">sara@epp.com</a>; <a href="mailto:jeff@ccs.com">jeff@ccs.com</a></td>
<td></td>
</tr>
</tbody>
</table>

You can add a new allowlist or edit, delete or export from the **Actions** column.

You can create or import up to 100 lists of dictionaries, each dictionary comprising up to 50000 web domains.

**Note:** Dictionaries comprising up to 100 web domains can be edited, but for more extensive dictionaries, you will need to import them again.

To create a new allowlist, under the list of available allowlists, click **Add**, provide a **name** and **description** and then **type or paste** items at least three characters separated by a new line, comma, or semicolon. You can import content using the **sample file** provided on the form.

**Example:** example.endpointprotector, *example.com, *example*, https://website.com, etc.

**Important:** “?” cannot be used to replace a character.
**Note:** Due to Gmail usage, take the following into consideration:

- You need to allow `mail.google.com` for adding e-mail attachments or files using the drag and drop option
- You need to allow `doc.google.com` to add images in the email body

Once the allowlist is created, it will be displayed on the Deep Packet Inspection list and will be available when creating or editing a Content Aware Protection policy.

<table>
<thead>
<tr>
<th>Name:</th>
<th>Description:</th>
<th>Content Options:</th>
<th>Content:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><img src="content-choices" alt="Content Options" /></td>
<td><img src="content-example" alt="Content Example" /></td>
</tr>
</tbody>
</table>

![Add Button](add-button)

![Save Button](save-button)

![Cancel Button](cancel-button)
# Wildcards usage examples for Deep Packet Inspection

<table>
<thead>
<tr>
<th>Domain name</th>
<th>Results matched</th>
<th>Results not matched</th>
</tr>
</thead>
<tbody>
<tr>
<td>box.com</td>
<td>box.com</td>
<td>Sub.box.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>box1.com</td>
</tr>
<tr>
<td>*.box.com</td>
<td>Sub.box.com</td>
<td>Fakebox.com</td>
</tr>
<tr>
<td></td>
<td>bad.box.com</td>
<td>mybox.com</td>
</tr>
<tr>
<td>box.*.com</td>
<td>Box.co.com</td>
<td>Sub.box.co.com</td>
</tr>
<tr>
<td></td>
<td>box.bad.com</td>
<td>Box1.co.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>box.co.uk</td>
</tr>
<tr>
<td>box.com.*</td>
<td>Box.com.co</td>
<td>Sub.box.com.us</td>
</tr>
<tr>
<td></td>
<td>box.com.us</td>
<td>box1.com.us</td>
</tr>
<tr>
<td></td>
<td>ftp://cisco.com/drives/downloads/</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Using wildcards will search for domain names, not URLs.

## 8.3. URL Categories

URL Categories are custom-defined lists of web domains that can be set on Content Aware Policies to limit the Deep Packet Inspection monitoring of the web traffic. If no Deep Packet Inspection Monitored URL Category is set on a policy, the Endpoint Protector Client will monitor all web domains by default.

**Important:** URL Categories only apply when the Deep Packet Inspection feature is active.

Blocking content based on URL categories can lead to data loss if not used correctly because it will restrict a policy to a few domain names. Policies must be constantly updated as new URLs need to be added to the categories lists.
You can add a new URL category or edit, delete or export from the Actions column.

To create a new URL category, under the list of available URL categories, click Add, provide a name and description and then type or paste items at least three characters separated by a new line, comma, or semicolon. You can import content using the sample file provided on the form and then select the option based on the number of uploaded items.

Once the URL category is created, it will be displayed on the URL category list and will be available when creating or editing a Content Aware Protection policy.
9. Enforced Encryption

9.1. Enforced Encryption

Enforced Encryption is a cross-platform solution that protects data with government-approved 256 bit AES CBC-mode encryption. For USB devices, it needs to be deployed on the root of the device. With the intuitive Drag & Drop interface, files can be quickly copied to and from the device.

![Enforced Encryption Interface](image)

**Note:** For detailed information on Enforced Encryption, refer to the Enforced Encryption User Manual.

Used in combination with Endpoint Protector, Enforced Encryption allows USB storage devices to be identified as Trusted Device™ Level 1. This can ensure that USB Enforced Encryption is used on protected computers. Accessing data stored on the device can be done via the password the user configured or via a Master Password set by the Endpoint

---

1 Formerly known as Easylock
Protector administrator. The encrypted data can be opened by any user only after it is decrypted, therefore requiring the user to copy the information out of Enforced Encryption.

**Important:** Enforced Encryption is not compatible with devices that have a write-protection mechanism in place, preventing the modification or deletion of data. The write-protection mechanism can be enforced using a hardware component (for example a switch on the USB device) or a software component.

**Note:** While Endpoint Protector can detect any Enforced Encryption USB encrypted device as a Trusted Device™ Level 1, to use the Enforced Encryption feature, a specific Enforced Encryption version must be used. This is available for the Endpoint Protector User Interface.

Enforced Encryption works on read-only mode if the device was formatted on Windows, the Enforced Encryption configured on Windows or some files were encrypted on Windows. On macOS, these files can be decrypted, except for NTFS due to incompatibility with Enforced Encryption.

### 9.1.1. Enforced Encryption Deployment

Enforced Encryption is supported for both Mac and Windows computers.

Deployment can be done automatically if **Allow Access if Trusted Device™ Level 1+** is selected for the USB Storage Devices. This can be done by going to Device Control, Global Rights section, or using the quick links provided, as per the image above.

Manual deployment is also available. Download links for both Windows and Mac are available in this section. The downloaded Enforced Encryption file must be copied onto the USB storage device and executed from the root of the device. Due to extended security features for manual deployment, Enforced Encryption will have to be redownloaded from the Endpoint Protector interface each time it will be used to encrypt a new USB storage device.

**Note:** Starting with Endpoint Protector 5.2.0.0, manual deployment can also be made by the user if the device is set on Allow Access, by pressing the small USB icon- Encrypt Device with Enforced Encryption.

Both Enforced Encryption deployments are straightforward and require the user only to configure a password.
**Note:** On Macs, USB storage devices with multiple partitions are not supported by Enforced Encryption and Trusted Device™ Level 1.

### 9.1.2. Enforced Encryption Settings

This section allows you to remotely manage Enforced Encryption encrypted devices. Before being able to take advantage of these features, you must configure a Master Password.

In the **Settings** section, the **Master Password** can be configured, the Enforced Encryption File Tracing enabled, as well as defining the installation and execution of Enforced Encryption only on computers where the Endpoint Protector Client is present.

For both the Master Password and the User Password, complex rules can be enforced. If these are enabled, the password lengths, minimum characters, validity, history, and other settings can be set.

Endpoint Protector allows tracing of files copied and encrypted on portable devices using Enforced Encryption. This option can be activated from inside the Settings windows located under the Enforced Encryption tab.
By checking the File Tracing option, all data transferred to and from devices using Enforced Encryption is recorded and logged for later auditing. The logged information is automatically sent to the Endpoint Protector Server if the Endpoint Protector Client is present on that computer. This action takes place regardless of the File Tracing option being enabled or not for that specific computer through the Device Control module.

In case the Endpoint Protector Client is not present, the information is stored locally in an encrypted format on the device and it will be sent at a later time from any other computer with the Endpoint Protector Client installed.

The additional Offline File Tracing option is an extension to the first option, offering the possibility to store information directly on the device, before being sent to the Endpoint Protector Server. The list of copied files is sent only the next time the device is plugged in and only if the Endpoint Protector Client is present and communicates with the Endpoint Protector Server.

Additionally, Easy Lock performs File Shadowing for the files that are transferred if the Endpoint Protector Client is present and the File Shadowing option is enabled on the computer on which the events occur – through the Device Control module. This is a real-time event and no shadowing information is stored on the device at any given time.

**Note:** Enabling global File Tracing will not automatically activate the File Tracing option on Enforced Encryption Trusted Device™ and vice versa.

### 9.1.3. Enforced Encryption Clients

In the Clients list section, all Enforced Encryption enforced devices are listed. By selecting the Manage Client Action a list of Actions History is displayed, as well as the option to manage them by sending a message, changing the user's password, resetting the device, resending the master password, and more.
9.1.4. **Trusted Device™**

Protecting Data in Transit is essential to ensure no third party has access to data in case a device is lost or stolen. The Enforced Encryption solution gives administrators the possibility to protect confidential data on portable devices in case of loss or theft. Ensuring only encrypted devices can be used on computers where Endpoint Protector is present can be done by utilizing Trusted Device™. Trusted Device™ must receive authorization from the Endpoint Protector Server, otherwise, they will be unusable. There are four levels of security for Trusted Device™:

- **Level 1** - Minimum security for office and personal use with a focus on software-based encryption for data security. Any USB Flash Drive and most other portable storage devices can be turned into a Trusted Device™ Level 1. It does not require any specific hardware but it does need an encryption solution such as Enforced Encryption on [http://www.endpointprotector.com/en/index.php/products/easylock](http://www.endpointprotector.com/en/index.php/products/easylock)

- **Level 2** - Medium security level with biometric data protection or advanced software-based data encryption. It requires special hardware that includes security software and has been tested for Trusted Device™ Level 2.

- **Level 3** - High-security level with strong hardware-based encryption that is mandatory for regulatory compliance such as SOX, HIPAA, GBLA, PIPED, Basel II, DPA, or PCI 95/46/EC. It requires special hardware that includes advanced security software and hardware-based encryption that has been tested for Trusted Device™ Level 3.

- **Level 4** - Maximum security for military and government use. Level 4 Trusted Device™ include strong hardware-based encryption for data protection and are independently certified (e.g., FIPS 140). These devices have successfully undergone rigorous testing for software and hardware. It requires special hardware that is available primarily through security-focused resellers.

- **Level 1+** - Derived from Level 1, it will ensure that Enforced Encryption 2 with Master Password will be automatically deployed on USB storage devices plugged into computers where the Endpoint Protector Client is present.

**Note:** If a Trusted Device™ Level 1 right is enabled and a Trusted Device™ level 2, 3 or 4 is connected, the right will apply accordingly.

The table below provides a list of Trusted Device™:

<table>
<thead>
<tr>
<th>Device Names</th>
<th>Trusted Device™ Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforced Encryption Encrypted devices</td>
<td>1</td>
</tr>
<tr>
<td>AT1177</td>
<td>2</td>
</tr>
</tbody>
</table>

CoSoSys Confidential. Copyright © 2004 – 2023 CoSoSys SRL and its licensors. All rights reserved.
<table>
<thead>
<tr>
<th>Device</th>
<th>Encryption Type</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>UT169</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>UT176</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Trek ThumbDrive</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>BitLocker Encrypted devices</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>FileVault Encrypted devices</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Buffalo Secure Lock</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>CTWO SafeXs</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Integral Crypto</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Integral Crypto Dual</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Integral Courier Dual</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IronKey Secure Drive</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>iStorage datAshur</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Kanguru Bio Drive</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Kanguru Defender</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Kanguru Elite (30, 200 &amp; 300)</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Kanguru Defender Elite</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Kingston DataTraveler Locker+</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Lexar 1 (Locked I Device)</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Lexar Gemalto</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>SaferZone Token</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>ScanDisk Enterprise</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Verbatim Professional</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Verbatim Secure Data</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Verbatim V-Secure</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>iStorage datAshur Pro</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Kanguru Defender (2000 &amp; 3000)</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>SafeStick BE</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Stealth MXP Bio</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
10. Offline Temporary Password

In this section, you can generate Offline Temporary Passwords (or OTPs) and grant temporary access rights. In addition to situations when only temporary access is needed, it can also be used when there is no network connection between the protected computers and the Endpoint Protector Server.

The Offline Temporary Password can be generated for the below entities:

- **Device** (a specific device)
- **Computer and User** (all devices)
- **Computer and User** (all file transfers)

A password is linked to a time period and is unique for a certain device and computer. This means the same password cannot be used for a different device or computer. It also cannot be used twice (except for Universal Offline Temporary Password).

The time intervals available are 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 1 day, 2 days, 5 days, 14 days, and 30 days or Custom.

The Offline Temporary Password Duration offers a customized option, allowing the generation of time-based OTP Codes, with a Start Date/Time and an End Date/Time.

For large companies or multinationals that have the Endpoint Protector Server and the protected endpoints in different time zones, taking into consideration how the Server Time and Client Time work is essential.

**Example:** The Endpoint Protector Server is located in Germany, making the Server Time UTC+01:00.

The protected endpoints are located in Romania, making the Client Time UTC+02:00.

When generating an OTP Code that should take effect tomorrow, from 16:00 on the endpoint time, it should actually be generated for tomorrow, from 15:00 (to adjust for the 1h difference in the time zone).

For the predefined duration, the above adjustment is not necessary. The OTP Code will be valid for that specific amount of time, starting with the moment it was redeemed. The only thing to consider is that the OTP Code needs to be redeemed the same day it was generated.
**Note:** The Universal Offline Temporary Password feature can also be turned on. If enabled, it can be used by any user, on any computer, for any device or file transfers – it eliminates security restrictions for one hour. It can be used multiple times, by any user that knows it.

The **Universal Offline Temporary Password** can be made visible only for Super Administrators. If this setting is enabled, Normal and Offline Temporary Password Administrators will not be able to see and use it. Enable this setting from System Configuration, System Settings, and Custom settings.

You have the option to add a justification, mentioning the reason why the password was created. This can later be used for a better overview or various audit purposes.

Once an Offline Temporary Password has been authorized, any other rights and settings saved afterwards on the Endpoint Protector Server will not take immediate effect. The Offline Temporary Password has to expire and the connection with the Server re-established.

**Note:** The Transfer Limit Reset Offline Temporary Password is only available if the feature is enabled. The main purpose of this type of Offline Temporary Password is to re-establish the Server-Client communication before the Transfer Limit Reset Time Interval has expired.

### 10.1. Generating the Offline Temporary Password

Depending on the options selected from the drop-down menus, the Offline Temporary Password (or OTP) can be generated for an exact device, all devices, or all file transfers.

When generating an Offline Temporary Password for a Device, you can either introduce the Device Code communicated by the user or search the Endpoint Protector database for an existing device. Alternatively, you can generate an Offline Temporary Password directly from
the Device Control, Computers section, by selecting the Offline Temporary Password option from the Actions column.

When generating an OTP Code for a device, either the Device Code or the Device Name has to be entered (one of them will automatically fill in the other field).

The Computer Name and the Username fields do not need to be both filled in. The OTP Code is perfectly valid if only one of them is provided. However, if the OTP Code needs to be valid for an exact device, on an exact computer, for an exact user, all of the relevant fields need to be filled in.

Once the OTP Code has been generated, it will be displayed on the right side of the image above.

As it needs to be provided to the person that made the request, Endpoint Protector offers two quick ways of doing this, either by sending a direct e-mail or by printing it out.

**Note:** You can edit the Administrator contact information that is displayed to a user from System Configuration, System Settings, as the Main Administrator Contact Details.

Similar to generating an Offline Temporary Password for a specific device, when generating one for all devices or all file transfers, the Computer Name and the Username fields are not both mandatory. The OTP Code is perfectly valid if only one of them is provided. However, if the OTP Code needs to be valid for an exact computer and an exact user, all of the relevant fields need to be filled in.
11. Reports and Analysis

This section offers an overview of the System Logs, Device Control Logs and Shadows, Content Aware Logs and Shadows, Admin Actions, Statistics, and other helpful information.

Details regarding eDiscovery Scans and Enforced Encryption can be viewed in their specific sections and not in the Reports and Analysis section.

As an additional security measure, this section may be protected by an additional password set by the Super Administrator, from System Configuration, System Security.

For detailed information on System Security, refer to the System Security chapter.

11.1. Logs Report

From this section, you can view, sort, and export the main logs in the system. There are several event types such as User Login, User Logout, AD Import, AD Synchronization, Uninstall Attempt, etc., included in this section. Additionally, the main Device Control logs can be viewed in this section.

Note: Use the Filters option to view and sort different log types and then export the result list.
11.2. File Tracing

This section offers an overview of trace files that have been transferred from a protected computer to a portable device or another computer on the network, and vice versa.

A special mention is given here to the "File Hash" column. Endpoint Protector computes an MD5 hash for most of the files to which the File Tracing feature applies to. This way, mitigating threats coming from changing the file content is ensured.

You can export the search results (as an Excel, PDF, or CSV) or Create and Export containing the entire log report as a .CSV file.

11.2.1. File Tracing Events by Direction

The "File Tracing Events Matrix by Direction" table is a valuable reference for understanding how Endpoint Protector categorizes file tracing events based on data transfer directions. It offers insight into event handling and helps users customize data protection policies effectively. Whether tracking local transfers or interactions with removable devices and network shares, this table provides a clear overview. It’s an essential resource for configuring data protection policies in the Endpoint Protector environment, ensuring strong security and compliance.

**Note:** This matrix refers to clients from the 5.9.0.0 release and higher.

Please see the table below for a detailed view of the events.
### File Tracing Events Matrix by Direction

<table>
<thead>
<tr>
<th>Direction</th>
<th>Windows</th>
<th>macOS</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local -&gt; Local (Partition 0)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Local -&gt; Removable</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
</tr>
<tr>
<td>Local -&gt; Network share</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Local -&gt; Partition 1</td>
<td>Src &amp; Dest</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Removable -&gt; Local (Partition 0)</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Removable -&gt; Removable</td>
<td>Src &amp; Dest</td>
<td>Dest</td>
<td>Src &amp; Dest</td>
</tr>
<tr>
<td>Removable -&gt; Network share</td>
<td>Src &amp; Dest</td>
<td>Dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Removable -&gt; Partition 1</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
</tr>
<tr>
<td>Network share -&gt; Local (Partition 0)</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Network share -&gt; Removable</td>
<td>Src &amp; Dest</td>
<td>Dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Network share -&gt; Network share</td>
<td>Src &amp; Dest</td>
<td>Dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Network share -&gt; Partition 1</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Partition 1 -&gt; Local (Partition 0)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Partition 1 -&gt; Removable</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Partition 1 -&gt; Network share</td>
<td>Src &amp; Dest</td>
<td>Src &amp; Dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Partition 1 -&gt; Partition 0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Legend:
- Partition 0 -> Boot Partition (OS)
- Partition 1 -> 2nd Partition (e.g., 2nd OS or Data Partition)

### 11.3. Content Aware Report

From this section, you can view Content Aware Logs in the system and detect data incidents corresponding to the Content Aware Policies applied.

When using the latest Endpoint Protector client, you can view log details structured per file scanned.
Expand each entry from the log report list to view the Log Details expanded section, providing the following information:

- **Policy** – select an active policy from the drop-down list
- **Policy name** – the name of the selected policy
- **Policy type** – the type of the selected policy
- **Items type** – the Policy Denylist category selected
- **Matched type** – the Policy Denylist type selected
- **Matched items** – click the link to view a pop-up window with the list of matched items

- **Count** – the number of matched items
From the Filters section, check the Include old logs prior to 5.7 upgrade option from the filter section to include all logs in your searches. If the option is not selected, the filters will apply only to the new structure of logs.

**Note:** For Mac users, when the DPI (Deep Packet Inspection) feature is enabled on the EPP agent for Mac, there might be certain scenarios where the agent does not provide full destination details for files being transferred from a network share through monitored applications, such as browsers. In such cases, the destination information may not be fully captured in the monitoring process.

**Note:** For Linux users, it's important to note that the EPP agent does not currently support network share visibility, except in situations where files are being transferred from a network share through DPI monitored applications, like browsers. In other scenarios, network share visibility might not be available.

### 11.3.1. Export Content Aware Reports

You can export Content Aware Logs as an Excel, PDF, or CSV or create and export the entire log report as a CSV or XLSX file.

- **Excel/PDF/CSV** – situated above the Content Aware Reports list, this will export only the default columns
• **Create Export** – situated below the Content Aware Reports list, this will create an export containing all data, including the expanded Logs Details section with columns Policy Type, Policy Name, Item type, Matched type, Matched items and Count.

After the message that is displayed that **A new export has been made and is available on Export List**, click **View Export List** to open the list of Reports, where you can download or delete a report.

11.4. Admin Actions

This section offers an overview of every important action performed in the interface. From the Action column, you can view additional information.
11.5. Online Computers

This section offers an overview of computers registered on the system which have an established connection with the server.

If the Refresh Interval for computer X is 1 minute, then computer X was communicating with the server in the last 1 minute.

11.6. Online Users

This section offers an overview of users registered on the system which have an established connection with the server.
11.7. Online Devices

This section provides an overview of devices registered on the system which have an established connection with the server.

11.8. Statistics

The Statistics module allows you to view system activity regarding data traffic and device connections. The integrated filter makes generating reports easy and fast. Simply select the field of interest and click Apply Filter.
## Statistics

<table>
<thead>
<tr>
<th>Results</th>
<th>Status</th>
<th>Action</th>
<th>Data Traffic</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Search Criteria

- **Username**: 
- **First Name**: 
- **Last Name**: 
- **Email**: 
- **Time Since Last**: 
  - **Time**: 
  - **Last**: 

---

CoSoSys Confidential. Copyright © 2004 – 2023 CoSoSys SRL and its licensors. All rights reserved.
12. Alerts

From this section, you can define E-mail Alerts for the main events detected by Endpoint Protector: System Alerts, Device Control Alerts, Content Aware Alerts, and Enforced Encryption Alerts.

**Note:** Before creating alerts, make sure the Endpoint Protector E-mail Server Settings have been configured from the System Configuration, System Settings section. You also have the option to verify these settings by sending a test E-mail.

For each Administrator to appear in the list of recipients for the Alerts, this has to be provided under the Administrator details from the System Configuration, System Administrators section.

### 12.1. System Alerts

From this section, you can create system alerts, including APNS certificate expiry, updates and support expiry, endpoint licenses used, etc.
12.1.1. Creating a System Alert

To add a new Alert, click **Create**, provide the required information and then click **Save**.

1. **Event** – select the type of event that generates the alert

   - **Updates and Support** – set an alert regarding each module's maintenance status (Device Control, Content Aware Protection, and eDiscovery);

   **Note**: You can disable the Update and Support system alert from General Dashboard, System Status.

   - **Endpoint Licenses** – set an alert to be notified of the percentage of used Endpoint Licenses and eliminate the risks of having unprotected endpoints as each network is constantly growing. Define alerts when the percentage of used Endpoint Licenses reaches 70%, 80%, or 90%.

   - **Client Uninstall** – set an alert each time an Endpoint Protector Client is uninstalled for better management of an extensive network. This is particularly helpful when there are several assigned Administrators.

   - **Server Disk Space** – set an alert to be notified of the Server Disk Space status and ensure Server Disk Space remains available for logs to be stored and policies are correctly applied.

   Define alerts when disk space reaches 70%, 80%, or 90% and then select the monitored partitions from the available root, epp and boot.

   - **Device Control – Logs Amount** – set an alert each time the Number of Device Control Logs Stored reaches a specific amount. Select from the available intervals or define a custom value.

   - **Content Aware – Logs Amount** – set an alert each time the Number of Content Aware Logs Stored reaches a specific amount. Select from the available intervals or define a custom value.
12.1.2. **System Alerts History**

From this section, you can view a history of the System Alerts. Alerts that are no longer needed for auditing purposes can later be deleted.
12.2. Device Control Alerts

From this section, you can create Device Control alerts, for events such as Connected, File Read, File Write, Enforced Encryption – successfully deployed, etc.

12.2.1. Creating a Device Control Alert

To add a new Alert, click Create, provide the required information, and then click Save.

1. **Event** – select the event type that generates the alert;
2. **Alerts Name** – add a name for the alert;
3. **Device Type** – select the device type from the drop-down list of available devices;
4. **Devices** – select the specific device already available in the system;
5. **Monitored Entities** – select the Groups, Computers, or Users that generate the event;
6. **Administrators** - select the Administrators that will receive the alerts.
12.2.2. Device Control Alerts History

From this section, you can view a history of the Device Control Alerts. Alerts that are no longer needed for auditing purposes can later be deleted.

12.3. Content Aware Alerts

From this section, you can create Content Aware alerts, for events such as Content Threat Detected or Content Threat Blocked.
12.3.1. Creating a Content Aware Alert

To add a new Alert, click **Create**, provide the information required and then click **Save**.

1. **Event** - the event type that generates the alert (Content Threat Detected or Content Threat Blocked)
   - Content Threat Detected DPI bypass whitelist
   - Content Threat Blocked
   - Content Remediation Session Active
   - Content Remediation Request Canceled by User
   - DPI Bypassed Traffic

2. **Alerts Name** – add a name for the alert

3. **Content Policy** – select a policy to apply the alert (this field is not available if you select DPI Bypass Traffic event)

4. **Administrators** - select the Administrators that will receive the alerts.

5. **Monitored Entities** – select the Groups, Computers, or Users that generate the event

The alert sent on the email will also include a CSV file with a report of the threats found.

**Note**: Before creating the alert, ensure the selected Content Aware Policy is enabled on the chosen Computer, User, Group, or Department.
12.3.2. Content Aware Alerts History

From this section, you can view a history of the Content Aware Alerts. Alerts that are no longer needed for auditing purposes can later be deleted.
12.4. Enforced Encryption Alert

From this section, you can create Enforced Encryption alerts, for events such as password changes, messages sent, etc.

12.4.1. Creating an Enforced Encryption Alert

To add a new Alert click Create, provide the required information and then click Save.

1. **Event** – select the type of event that generates the alert
   - Send Message
   - Change Master Password
   - Change User’s Password
   - Reset Device
   - Change Settings – Installation and Execution
   - Re-deploy Client
   - Master Password Login Success
155 | Endpoint Protector 5.9.1.0 User Manual

- **Password Login Failure**
- **Password Login Exceeded**

2. **Alerts Name** – add a name for the alert

3. **Administrators** - select the Administrators that will receive the alerts.

12.4.2. **Enforced Encryption Alert History**

From this section, you can view the history of the Enforced Encryption Alerts. Alerts that are no longer needed for auditing purposes can later be deleted.
13. Directory Services

From this section, you can import and synchronize the entities (Users, Computers, and Groups) from the company's Active Directories.

13.1. Microsoft Active Directory

You can create and manage connections from the Directory Services, Microsoft Active Directory section. The required information includes the Connection Type, Server, Port, Username, and Password.

Note: When having to import a very large number of entities, we recommend using the Base Search Path to get only the relevant information displayed. Due to browser limitations, importing the whole AD structure may impede the display of the import tree if it contains a very large number of entities.
To ensure the information is correct, click Test to test the new connection.

Once a new connection has been created, it is available in the synchronization list and can be further edited, to include the required entities.

For the defined connections, several synchronization options are available. From this section, the connection credentials and synchronization interval can also be changed.

The Advanced Groups Filter can be used to import and synchronize only specific groups, ignoring all other entities.

From the Directory Browser section, you can select the entities that need to be synced.

**Note:** You can view only Organizational units (OU) and Groups in the Directory Browser.

Once the entities have been selected, they can be saved to sync.
13.2. Azure Active Directory

You can create and manage connections from the Directory Services, Azure Active Directory. From this section, Groups from the Azure Active Directory will have their users synchronized with the Endpoint Protector Server. Group membership will be retrieved recursively by the API platform itself.

Example

- Group 1 - User 1, User 2, User 3;
- Group 2 - Group 1, User 4;
- Group 3 - Group 2, User 5;

If Group 3 is selected for the synchronization operation, only Group 3 will be imported and created in the Endpoint Protector Server. User 5 will also be imported and will be added as a member of Group 3. Group 2 and all subsequent groups will be parsed and only the Users will be retrieved and the actual groups will not be added to the server.

After the synchronization is done, it will look like that on the Endpoint Protector server:

- Group 3 - User 5, User 4, User 3, User 2, User 1;

13.2.1. Configure Azure Active Directory

13.2.1.1. Create the Application on Azure Active Directory

1. Log in to Azure Portal.

2. Go to Azure Active Directory.

3. Click App Registrations from the Manage section on the Active Directory menu on the left side, then on New Registration.
4. On the **Registration** page enter your **Name**

5. On the Supported account type select **Default Directory**

**Important**: Do not fill in the **Redirect URI** field!

6. Click **Register**.

7. On the **Essentials** section save the following information:

   - Application (client) ID will be needed for adding it in the Application (client) ID field on the Endpoint Protector Server.
   - Directory (tenant) ID will be needed for adding it in the Tenant ID field on the Endpoint Protector Server.
13.2.1.2. Create a secret ID for the Application

The secret ID will be used as an authentication method to gain access to the application via Graph API.

1. Click **Certificates & Secrets** on the side menu from the **Manage** section.

2. Click **New client secret** on the **Certificates & secrets** page.
3. **Enter a Description** for the secret ID.

4. **Click Add** and **Add a client secret** section.
Take note of the Secret ID value and make sure to copy it to the clipboard and also to store it safely because it will be needed further on.

**Note:** Notice that when navigating back, the secret ID will be hidden.

13.2.1.3. **Create Users/Groups using Graph API**

1. Click **Home** and then **Azure Active Directory**.
2. Click **Add** from the Default **Directory** Overview page
3. Click Add User.

- Select Create User
- Enter the Username and select the Domain
- Enter the Name
- Either click Auto-generate password or create one on your own
- Add the Department
- Click Create
13.2.1.4. **Add Permissions to the Application**

Permission to be added to our application:

- **Directory.Read.All**
- **Group.Read.All**
- **User.Read.All**

Make sure the created application is open then:
1. Click API Permissions.

2. Click Add a Permission

3. Click Microsoft Graph.
4. Click Application Permissions.

5. Search for the permissions mentioned above and check each of the permissions. (Directory.Read.All, Group.Read.All, User.Read.All)
6. Click Add Permissions.

7. Click Grant admin consent for Default Directory from the API Permission page.
13.2.1.5. Add Graph Application to Endpoint Protector Server

1. Go to **Endpoint Protector Server, Directory Services, Azure Active Directory**.

2. Click **Add** to add an API Consumer - One API Consumer can be used for multiple synchronization jobs.

3. Provide the following details:
   - **Name**
   - **Description**
   - **Directory (tenant) ID** saved earlier on the Tenant ID field
   - **Application (client) ID** saved earlier on the Application (Client) ID field
   - **Secret ID** saved earlier in the Client Secret Value field

CoSoSys Confidential. Copyright © 2004 – 2023 CoSoSys SRL and its licensors. All rights reserved.
4. Click Test and then Save.

13.2.1.6. Create a Synchronization Job on the Endpoint Protector Server

1. Click Create Sync Job.
2. Provide Synchronization information:

- Name
- Description
- Select the created API Consumer
- Select Sync Interval
- Click Save

The "Map on-premises users" switch in the Azure Active Directory connector controls how Endpoint Protector (EPP) retrieves user names in hybrid environments with both a local Active Directory and Azure Active Directory (Azure AD). This switch has two states:

- **Unmarked** (feature disabled): EPP uses the "userPrincipalName" Azure AD attribute to retrieve user names. This attribute is the primary source for user identification and account mapping.
- **Marked** (feature enabled): EPP uses the "onPremisesSamAccountName" Azure AD attribute to retrieve user names, ensuring accurate synchronization between the local Active Directory and Azure AD.

By utilizing this feature, EPP ensures seamless synchronization of user names, preventing duplicate usernames. Enable or disable the "Map on-premises users" feature based on your specific hybrid environment setup and requirements.
14. Appliance

14.1. Server Information

From this section you can view general information about the Server, the System Fail/Over status, information on Disk Space usage and Database, and the Server Uptime.

14.2. Server Maintenance

In this section, you can set up a preferential time zone and NTP synchronization server, configure the IP and DNS, register the client certificate, set up a self-signing certificate, perform routine operations and manage the SSH access.
14.2.1. Time Zone

In this section you can set a preferential time zone and/or sync the appliance to an NTP source.

- **Time zone** - select from the drop-down lists the zone and location
- **NTP Server** – type the server or go with the default entry
- **How often to synchronize** – select from the drop-down a time interval when to synchronize of go with the default selection

**Note:** The appliances are prefigured to sync once a week with pool.ntp.org.

- **Current server time** – the field displays the current server time
- **Automatic NTP Synchronization** – opt in or out to trigger the NTP synchronization automatically
- Click **Save** to keep all modifications without triggering the synchronization process.
- Click **Synchronize Time** to trigger the synchronization, which will occur in the next 5 minutes. The Alerts and Logs will be reported after the 5 minutes in a format of your choice.
- Click **Refresh Current Time** to update the **Current server time** field.
14.2.2. IP Configuration

In this section you can change the network settings for the appliance to communicate correctly in your network.

**Important:** Once you change the IP address, close and open again the Internet browser and then access the Endpoint Protector Administration and Reporting Tool with the new IP address.

![IP Configuration](image)

14.2.3. DNS Configuration

In this section you can modify or add a DNS server address and then **Save** your changes.

![DNS Configuration](image)

14.2.4. Client Registration Certificate

From this section, you can register and then verify the Endpoint Protector Client certificate signature. The client registration certificate is an additional security measure enabling certificate-based authentication.

**Important:** The Client Registration Certificate feature is not available for Linux!

1. Enable the custom certificate setting and then upload the certificate chain, Root CA and Intermediate;

   When the custom certificate is **enabled** then:
   - **Endpoint Protector Server** will validate the client certificate at the registration phase
   - **Endpoint Protector Client** will not validate the server certificate

   When the custom certificate is **disabled** then:
   - **Endpoint Protector Server** will not validate the client certificate at the registration phase
   - **Endpoint Protector Client** will not validate the server certificate
2. Enable the test certificate setting and then upload a **certificate signed by root CA just for testing the signature** (for example the Endpoint Protector Client certificate);

3. Click **Save** and allow 2 minutes for the information to be validated. You will view a successful message confirming the custom certificate was added and the test certificate is valid.

**Important**: The client registration authentication certificate and the Endpoint Protector server certificate must be issued by the same CA.

For this feature to work, there must be cryptographic identities signed by the root CA deployed on the endpoints.

- On **macOS** these identities should be added to System Keychain in the "My Certificates" section.
- On **Windows** they should be placed in the Certificate Manager’s Local Computer\Certificates\Personal section.

14.2.5. **Server Certificate**

In this section you can set up a custom certificate.

To do so, copy and paste the content from the **.pem** certificate in the **body** and **key** text boxes and then **Save** your modifications.

14.2.6. **Server Certificate Validation**

From this section, you can configure Server Certificate Validation, which ensures that certificates used for all communication requests on EPP clients are validated. This feature is crucial for maintaining secure communication between various Endpoint Protector (EPP) products.
**Note:** All certificate validation statuses will be reported to the EPP Server and stored for debugging purposes in EPP Client logs.

**Important:** Please use this feature responsibly, as improper certificate usage with certification validation might disrupt EPP Client to EPP Server communication.

**Important:** Starting from the 5.9.0.0 release (for Windows: 6.0.x.x; for MacOS: 2.8.3.x; for Linux: 2.2.0.x) or higher, enabling this option activates EPP Server Certificate Validation for all communication requests on EPP clients. This enhances the security of your EPP environment by ensuring that certificates used for communication are valid and trusted.

### 14.2.7. Appliance Operations

In this section you can perform appliance operations such as Reboot or Shutdown.

![Appliance Operations](image)

### 14.2.8. SSH Server

In this section you can manage user access to the Appliance through the SSH protocol.

**Note:** We recommended you set this option to Enable before requesting Support access.
14.3 SIEM Integration

SIEM are a third-party security information and event management tools that allow logging and analyzing logs generated by network devices and software. The integration with SIEM technology enables Endpoint Protector to transfer activity events to a SIEM server for analysis and reporting.

In this section, you can add, edit or delete an existing SIEM Server integration. To edit or delete a SIEM Server you need to select an available SIEM server integration.

**Important:** You can configure a maximum number of 4 SIEM Server integrations.

To create a SIEM Server click **Add New** and provide the following information:

- **SIEM Status** – toggle switch to enable/disable the SIEM server
- **Disable Logging** – toggle switch to enable/disable logging
  
  **Note:** If you disable logging, logs will be stored on the Endpoint Protector Server or on the SIEM Server when SIEM is enabled.
- **Server Name** – add a server name
- **Server Description** – add a description
- **Server IP or DNS** – add the IP or DNS
- **Server Protocol** – select the UDP or TCP server protocol
  
  **Note:** Based on the protocol you select you can enable **SIEM Encryption**.
- **Server Port** – add a port
- **Exclude Headers** - toggle switch to enable/disable log headers
  
  **Note:** If you disable log headers, you will only export data to SIEM.
● **Log Types** – select from the available options the logs to send to the SIEM Server

---

**Important**: Please be aware that the SIEM integration feature in Endpoint Protector comes with certain limitations. To make use of the latest features of this SIEM integration, your environment must meet specific criteria. It should have been installed from image version 5.6.0.0 or a more recent version, and maintain an active HTTPS connection. Please note that SIEM integration is only accessible in environments that meet these stringent prerequisites.

### 14.3.1. SIEM Encryption

When using the TCP protocol, you have the option to encrypt communication to each SIEM server. In order to do so, enable the **Encryption** setting and then upload the root **CA** that was used to sign the server certificate for the SIEM server in .pem format.

**Important**: The certificate used on the SIEM server must be signed by the same CA as the one uploaded to the EPP Server. Endpoint Protector will check the following:

- the SIEM certificate is signed by the CA, and the CN or SAN matches the name for the SIEM machine
- the Root CA has the Basic Constraint CA set to true

When validating a certificate, the entire certificate chain must be valid, including the CA certificate; if any certificate of the chain is invalid, the connection will be rejected.

Make sure you update the certificate files when they expire.

**Note**: If you applied the latest patch using the **Live Update** option, and cannot view the SIEM encryption setting, please contact [Customer Support](mailto:customersupport@cososys.com).
15. System Maintenance

15.1. File Maintenance

This module allows you to retrieve, organize and clean-up files used by the Endpoint Protector Server.

You have the following options:

- **Shadow Files**: allows archiving and deleting shadowed files from a selected client computer
- **Log Backup Files**: allows archiving and deleting previously backed up log files

To archive a previously selected set of files click **Save as Zip** and to permanently remove a set of files from the Endpoint Protector Server click **Delete**.

15.2. Exported Entities

From this section, you can view the list of exported entities, download or delete them, and view the scheduled export in the system and reschedule them accordingly.
You can initiate the manual generation of the scheduled export from the Device Control, List of Devices / List of Computers / List of Users / List of Groups sections.

The scheduled exports can be sent automatically via e-mail to all the Administrators that have the Scheduled Export Alert setting enabled.

The Scheduled Exports are recurring (Daily / Weekly or Monthly), and, as such, will continuously take up more and more storage on the Endpoint Protector Server.
To maintain performance and, since these exports can also be sent automatically via e-mail to specific Administrators, the Scheduled Exports already generated are automatically deleted from the Server after 14 days.

For performance reasons, the Scheduled Exports and Disable Logging option allows you to also keep the logs on the Endpoint Protector Server or only have them in the SIEM Server.

15.3. System Snapshots

The System Snapshots module allows you to save all device control rights and settings in the system and restore them later if needed.

**Important:** After installing the Endpoint Protector Server, we strongly recommend that you create a System Snapshot before modifying anything. In this case, you can revert back to the original settings if you configure the server incorrectly.

To create a System Snapshot, go to System Configuration and click **Make Snapshot**.

Enter a name for the snapshot and a description. Select the items to store in the snapshot, **Only Rights**, **Only Settings**, or **Both** and then click **Save**.

The snapshot will appear in the list of System Snapshots.

To restore a previously created snapshot, click **Restore** next to the snapshot, and then confirm your action.
15.4. Audit Log Backup

Similar to the Log Backup and Content Aware Log Backup, this section allows old logs to be saved and exported. The options to select the number of logs to be exported, period and file size are available, as well as the option to view a Backup List or set a Backup Scheduler.

Both the Audit Log Backup and Audit Backup Scheduler offer several options like what type of logs to backup, how old should the included logs be, to keep or delete them from the server, to include file shadows or not, etc.

However, the main difference comes from the fact that the exported logs come in an improved visual model, making things easier to audit or to create reports for executives.

The Backup export CSV file will differ based on the Endpoint Protector Server version used:
● For Endpoint Protector 5.6.0.0 or older, the CSV file reports a file for each threat discovered
● For Endpoint Protector 5.7.0.0, reports, only one file containing all threats discovered, separated by an underscore

15.4.1. Audit Log Backup Scheduler

While the Audit Log Backup starts the backup instantly, the Audit Log Backup Scheduler provides the option to set the procedure for a specific time and the frequency of the backup (every day, every week, every month, every year, etc.).
15.5. External Storage

From this section, you can externalize files generated by Endpoint Protector to a particular storage disk from the network. Files such as Shadows, Audit Log Backups and System Backups can be saved to an FTP, SFTP or Samba / Network Share server.

You can enable the option to keep a copy of the files on the Endpoint Protector Server for all External Storage Types.
15.5.1. FTP Server

To configure an FTP Server, provide the following information:

- **Externalize Files** – the Endpoint Protector files: Shadows, Audit Log Backup or System Backups
- **Server IP Address** – the IP of the external server
- **Remote Directory** – a specific location on the external directory
- **Username** – the username of the external server
- **Password** – the associated password
- **Enable Storage**
- **Server Port**
- **Passive Connection**
- **Anonymous Login**

15.5.2. SFTP Server

To configure an SFTP Server, provide the following information:

- **Externalize Files** – the Endpoint Protector files: Shadows, Audit Log Backups or System Backups
- **Server IP Address** – the IP of the external server
- **Remote Directory** – a specific location on the external directory
- **Server Port** – the port of the external storage server
- **Username** – the username of the external server
- **Password** – the associated password
15.5.3. Samba / Network Share Server

To configure a Samba / Network Share Server, provide the following information:

- **Enable Storage**
- **Keep copy on EPP Server** — enable this setting to create; a backup of the storage on the Endpoint Protector Server
- **Externalize Files** — select the Endpoint Protector files: Shadows, Audit Log Backup or System Backups
- **Authentication Security** — select the security protocol: Default, NTLM, NTLMv2, NTLMSSP
- **Domain or Workgroup** — only where applicable
- **Mount Point**
- **Remote Directory** — a specific location on the external directory
- **Protocol Version**
- **Username** — the username of the external server
- **Password** — the associated password
15.6. System Backup

15.6.1. From the Web Interface

This module allows you to make complete system backups.

To view the list of current backups, go to System Maintenance, System Backup v2.

To restore the system to an earlier state, click Restore next to the entry and then confirm your action.

**Important:** Once deleted, a backup cannot be recovered.

The Download button will prompt you to save the .eppb backup file on the local drive. It is recommended to keep a good record of where these files are saved.

**Important:** When using the Restore Backup feature, we recommend requesting assistance from support@endpointprotector.com.

On the Make Backup section, you have the following options:
- Save the **Database content** - the backup file will contain all the devices, rights, logs, settings and policies present on the EPP server at the making of the backup.

- Save the **Application sources** - the backup will contain files such as the EPP clients and others related to the proper functioning of the server.

**Note:** The System Backup will not contain nor preserve the IP Address, File Shadowing copies or the Temporary Logs Files.

The second section, **Status**, returns the state of the system. If a backup creation is in progress, it will be reported as seen below.

![System Backup Status](image)

If the system is idle, the button will return the last known status, which by default is set at 100% done.

The next menu, **Upload**, allows you to populate the backup list with .eppb files from the local filesystem. This functionality is useful in cases of server migration or crash recovery.

**Important:** Endpoint Protector Backup Files (.eppb) larger than **200 MB** can only be uploaded from the console of the appliance. We recommend that you contact Support when a created .eppb file exceeds this 200 MB limit.

![Upload System Backup](image)

From this section, you can schedule an automatic backup routine by setting a trigger condition, the **System Backup time interval**. The routine can be set to run daily, weekly, monthly and so forth.
The Scheduler will also prompt the administrator with the **Last Automatic System Backup reminder**.

**Note:** A scheduled routine is recommended in order to prevent unwanted loss.
15.6.2. From the Console

Endpoint Protector offers the option to revert the system to a previous state from the administrative console on which the initial configuration occurs.

The #2 menu presents you with the following options:

1. **System Restore** – can be performed if a system backup has been performed prior to the event, using the web interface
2. **Import** – can be performed if a `.eppb` file has been downloaded and saved on an FTP server
3. **Export** – can be performed in order to save existing backups on an existent FTP server

To either import or export the `.eppb` files, an administrator will need to provide the system a valid FTP IP address and the path inside its filesystem to the `.eppb` file.

An example is shown below:
15.7. System Backup v2

From this section, you can migrate the database (entities, rights, settings, policies, configurations, etc.) from an older Endpoint Protector Server to a newer one.

**Note:** This feature is not intended as a replacement for the System Backup functionality but rather as a migration tool from older Endpoint Protector images to the ones starting with version 5.2.0.6.

The version of the old Server and the new Server will have to be the same. Before starting the migration process, make sure both Servers have the same version (e.g.: update the old server to 5206, aligning it with the new server that is about to be deployed).

It does not include logs, Audits or System Backups. If needed, these should be downloaded before proceeding.

**Example**

The initial Endpoint Protector deployed was version 4.4.0.7. Over time, updates were applied though the Live Update section, bringing the appliance to Endpoint Protector version 5.2.0.6. While these constantly included patches and security updates, they did not include a full rollout of a new core OS version (e.g.: the appliance is still running on Ubuntu 14.04 LTS).

As Ubuntu 14.04 no longer receives security patches since 2019, those that want to migrate to a Server running on the latest Ubuntu LTS version should take advantage of this functionality.
15.7.1. Creating a System Backup v2 (Migration)

You can create a new migration backup from the System Maintenance, System Backup v2 section.

**Note:** For security purposes, the System Backup Key will not be stored by the Endpoint Protector. Before proceeding, make sure it is properly saved.

15.7.2. Importing and Restore (Migrate)

A backup can be restored on the same Endpoint Protector Server. However, the main use case would be to import and restore the backup on a newer Endpoint Protector Server (e.g.: version higher than 5.2.0.6).

The migration process of a System Backup requires the backup file and System Backup Key.
**Note:** If needed, previous System Backups or Audit Log Backups should be downloaded prior to this step, as they will not be kept in process.

After the Import and Restore (Migration) has been made to the new Appliance, the old Appliance should be turned off. Its IP would then have to be reassigned to the new Appliance in order for the deployed Endpoint Protector Clients to start communicating with the new Appliance.

![System Backup - Import and Restore](image)

15.8. File Shadow Repository

From this section, you can enable the Endpoint Protector Client to send File Shadows directly and at a global level to an externalized location, the File Shadows Repositories.

You can create multiple File Shadow Repositories and define how each endpoint manages the File Shadows based on department and repository type.

**Note:** In Endpoint Protector, the Department defines a collection of entities with the same attributes. It should not be confused with the department from an organizational chart.

Starting with Endpoint Protector Server version 5.8.0.0, file shadowing was made more reliable on macOS and Linux by first relying on OS features to transfer the files.

1. on Mac/Linux:
   - primary: LDAP (as-is)
   - fallback: curl (as-is)

2. on Windows:
   - primary: LDAP
   - fallback: curl

To create a File Shadow Repository, click **Add** and then provide the following information:
Department – assign one or more departments to the File Shadow Repository

Repository Type – select the type of repository, FTP, Samba (smbv1), Azure File Storage and Samba (smbv2) or S3 Bucket

Note: If you select S3 Bucket type, the information required to create a File Shadow Repository will differ. Read more on S3 Buckets File Shadow Repository in the following section.

Note: The minimum permissions required for Samba shares is 750 (case owner has full access and the Group has only Read and Execute).

Repository IP Address – add the File Shadow Repository IP address

Port – add the port used by the File Shadow Repository

Note: You are not required to define the port for Samba (smbv1) or Azure File Storage and Samba (smbv2) repositories.

Folder Path – add the folder path where File Shadows will be saved

Username and Password – add the repository credentials

15.8.1. S3 Bucket File Shadow Repository

The Amazon S3 bucket is a public cloud object storage resource available from Amazon Web Services (AWS) Simple Storage Service (S3).

S3 Bucket type File Shadow Repository supports large files up to 5TB (AWS specification).

To create an S3 Bucket type File Shadow Repository on Endpoint Protector, provide the following information:

- Repository Type – select S3 Bucket as the type of repository
- Department – assign one or more departments to the File Shadow Repository
● **S3 Bucket Region** – depending on the artifacts retrieval method, select one of the options from the drop-down list or add a bucket region corresponding with the AWS S3 Bucket settings

● **S3 Bucket Name** – add a name for the bucket repository corresponding with the AWS S3 Bucket settings

● **S3 Location** – add a specific sub-folder location in the AWS S3 Bucket

● **Access Key ID** – add the Key for S3 Bucket corresponding with the AWS S3 Bucket settings

● **Secret Access Key** – add the Token Key generated for a user corresponding with the AWS S3 Bucket settings

Select the artifacts retrieval method:

1. **Indirect Artefact retrieval** – this is the recommended and most secure option to retrieve artifacts via the Endpoint Protector Server.

   **Note:** The system administrator will request artifact retrieval using the Endpoint Protector Server UI. The Endpoint Protector Server will retrieve artifacts from the S3 Bucket Repository and provide an artifact file to the system administrator.

You can download or delete an object using SDK, which limits the regions available to the following:

- us-west1 - Northern California
- us-west2 - Oregon
- eu-west1 - EU (Ireland)
- ap-southeast-1 - Asia Pacific (Singapore)
- ap-southeast-2 - Asia Pacific (Sydney)
- ap-northeast-1 - Asia Pacific (Japan)
- sa-east-1 - South America (São Paulo)
- us-gov1-west-1 - United States GovCloud
- fips-us-gov-west-1 - United States GovCloud FIPS 140-2

2. **Direct artifact retrieval** – this option is dedicated to globally distributed Endpoint Protector deployment. This method will establish a direct connection from the system administrator’s computer to the S3 Bucket Repository and initiate direct artifact download.

   **Note:** To use the direct artifact retrieval method, add the Endpoint Protector Server IP in the S3 Bucket whitelist as detailed below.

You can download or delete file shadows from the Reports and Analysis section, the Logs Report page, and the Content Aware Report page using the Actions column.
When a file is uploaded, an External Repository Upload log will be displayed.

**Important:** File shadows contained in the S3 Bucket (File Shadow Repository) will not be included in the Audit.

**Note:** In the scenario where there may be an unreliable network, the Client will attempt to upload the artifact 10 times before the guard-rail will stop upload attempts. This will delete the File Shadow from the queue to ensure endpoint performance, disk space utilization, and mobile transfer limits are not affected.

### 15.8.1.1. Domain whitelisting

To add the Endpoint Protector Server IP to the S3 Bucket whitelist, follow these steps:

1. Log in to AWS;
2. Click on an entry from the S3 Bucket list;
3. On the S3 Bucket, select the **Permission** tab, scroll down to the **Bucket** policy section, and then click **Edit**;
4. On the Bucket Policy, add the following IPs:
   - Static IP address of the Administrator endpoint for download
   - EPP External Server IP address to delete

5. Use the Policy generator from the top-right corner to help you edit or create a new Bucket policy – this will open a new page with the AWS Policy Generator.

On the AWS Policy Generator, provide the following information:

- **Select Type of Policy** – S3 Bucket Policy
- **Effect** – select to Allow
- **Principal** – add *
- **Actions** – select **DeleteObject** and **GetObject**
- **Amazon Resource Name (ARN)** – add the ARN name
- **Click Add Conditions** and then select from the drop-down lists **IpAddress** as the **Condition**, **aws:SourceIp** as the **Key** and add the two **IPs** separated by a comma to the **Value** field.

Add the Statement, click **Generate Policy**, and then use the **Bucket Policy**.
15.8.1.2. Internet Connectivity Requirements

When using S3 Bucket as the File Shadows Repository type, you will need a direct internet connection in the following situations:

- For the Endpoint Protector Client to deliver File Shadows to the AWS S3 Bucket repository
- For the Endpoint Protector Server to retrieve File Shadows from the AWS S3 Bucket repository using the indirect artifact retrieval method
- For the Administrator endpoint to retrieve File Shadows from the AWS S3 Bucket repository using the direct artifact retrieval method

15.8.1.3. File naming and structure

1. File name convention

The file names will be uploaded to the S3 Bucket with URLs encoded to avoid issues with special characters. The Endpoint Protector Server will then decode to display the original name.
Example:

File name
canada_&$@=+/.,(?%>]~<&_/山人é口ō刀ã木ù日ì月è女ū子ｉ馬/鸟niǎ目ǜ水 .txt

File name displayed in AWS S3 Bucket

ln4w7yuqax-dev-client-bucket/2022-11-23/ComputerName/canada_26%24%40%3D%3B%3A%2B%20%2C%3F%5C%7B%5E%7D%25%60%5D%3E%5B~%3C%23%7C%5E%B1%B1%E4%B A%BAe%CC%81%E5%8F%A3o%CC%86%E5%88%80a%CC%84%E6%9C%A8u%CC%80%E6%9 7%A5i%CC%80%E6%9C%88e%CC%80%E5%A5%B3u%CC%88%CC%8C%E5%AD%90i%CC%86 %E9%A6%AC%3A%E9%A9%AC%E9%B3%A5%3A%E9%B8%9Fnia%CC%8C%E7%9B%AEu%CC %80%E6%B0%B4%20.txt

Important: File name and special characters from the computer name and location will also be encoded.

2. File name structure

Default file name structure:

bucketName/CurrentDate/ComputerName

- bucket name (ln4w7yuqax-dev-client-bucket)
- current date in YYYY-MM-DD format (2022-11-23)
- computer name URL encoded

File name structure with S3 Bucket location field specified:

bucketName/location/CurrentDate/ComputerName
This section contains the Endpoint Protector Clients, System Licensing and other advanced settings, which influence the functionality and stability of the system.

16.1. Client Software

From this section, you can download and install the Endpoint Protector Client corresponding to your operating system.

**Note:** The Server and Client communicate through port 443.

When using a custom WebUI port, please contact CoSoSys Support to assist in configuring the Nginx configuration file.

The Windows Client installers allow the option to download the package with or without add-ons. This option fixes any incompatibility that may arise between Endpoint Protector and the specific solutions.

**Important:** Only the latest Endpoint Protector Clients are available for download. You cannot set another default Endpoint Protector Client version from the Client Software Upgrade section.

To improve the Endpoint Protector installation process, use the Endpoint Protector tool that allows you to run installation-related actions, identify your current Linux distribution, and view Endpoint Protector Release Notes.

Use the following commands:

- `i` - install
- `u` - uninstall
- `rn` - release notes
- `l` - distribution list

**Note:** Contact Customer Support to provide the tool as well as assistance.
16.1.1. Bypass Proxy Settings

You have the ability to bypass proxy settings for all operating systems.

16.1.1.1. Windows and macOS

1. Endpoint Protector Wizard Installer

Select the option to **Use Manual Proxy Settings** from the Endpoint Protector Wizard installer and then provide the following information:

- **Proxy IP**: IP of the proxy server
- **Proxy Port**: Port of the proxy
- **Select the Use authentication checkbox**
- **Username**: add proxy server username
- **Password**: add proxy server password

2. CLI commands

You can also apply manual proxy settings using CLI commands:

**Example**: 

```
msiexec.exe /i "C:\Work\Tools\EPPClientSetup.5.7.1.5_x86_64.msi" /q
REBOOT=ReallySuppress RUNNOTIFIER=0 /log "C:\Windows\TEMP\epp-upgrade.log"
WSIP="192.168.18.125" WSPORT="8080" DEPT_CODE="defdep" PROXYIP="127.0.0.1" PROXYPORT="80" AUTHUSR="user_name" AUTHPASS="password"
```

Where:

- **PROXY_IP** - IP of the proxy
- **PROXY_PORT** - Port of the proxy
- **AUTHUSR** - Username (if authentication for proxy is needed)
- **AUTHPASS** - Password (if authentication for proxy is needed)
You can also use CLI Commands below to install EPP Client in specific mode of working.

- **WSIP** - server address
- **WSPORT** - server port number
- **DEPT_CODE** - department code
- **IPV6MAPPING** - IPV6 Mapping IPv4 addresses
- **SUPPRESSRD** - suppress FileRead/FileDelete events for NS and Removable devices
- **DISABLECAP** - disabling loading of CAP drivers (CAP will not work)

### 16.1.1.2. Linux

For Linux, you can only use CLI arguments in the options to bypass proxy settings.sh file. To do so, follow these steps:

1. Access the installation folder, open a Terminal, and run the following command:
   ```bash
   <cd pathToLinuxClientFolder>
   ```
2. To run commands as root, run the following command and type your password:
   ```bash
   <sudo su>
   ```
3. Open the options.sh configuration file with the following command:
   ```bash
   <gedit options.sh>
   ```
4. In the configuration file, you will view the following fields for the proxy setup:
   ```
   ● #EPPCLIENT_HTTPS_PROXY=
   ● #export EPPCLIENT_HTTPS_PROXY
   ```
5. Remove the `#` before each entry to apply the proxy setups;
6. For the first proxy setup, `EPPCLIENT_HTTPS_PROXY`, add the proxy server information in the `address:port:user:password` format.

**Example:**
```
EPPCLIENT_HTTPS_PROXY=address:port:user:password
```

3. Save the changes, and then run the installation without having a VPN connection:
   ```bash
   <bash install.sh>
   ```

Additional CLI commands for Linux in specific mode:

- **#EPPCLIENT_SUPRESSRW** - suppress FileRead/FileDelete events for NS and Removable devices
- **#EPPCLIENT_DISABLECAP** - disabling loading of CAP drivers (CAP will not work)

### 16.2. Client Software Upgrade

From this section, you can upgrade the Endpoint Protector Client and manage the upgraded jobs. The Client Software Upgrade feature is only available for Windows and macOS Clients.

To upgrade your Linux Clients, submit a request using the [online form](#).
Note: When updating your operating system to the latest macOS Ventura, eppclient.log and eppsslsplit.log will be deleted from private/var/log.

Important: The feature is not compatible for Endpoint Protector instances that are running on 32-bit versions of Windows.

16.2.1. Create new Upgrade Job

To upgrade your Endpoint Protector Client, you need to create a new upgrade job, following these steps:

1. Select the OS version from the drop-down list and then click Next;

2. Select the groups and/or computers to perform or exclude from the upgrade and then click Next. You will view a summary of your selection above the table with endpoints.

Note: Only computers that use the operating system you previously selected will be upgraded. If you selected a group that has an endpoint using a different operating system, it will not be upgraded. If you selected a mixed group, with both computers and users, only the computers will be upgraded.
3. Edit the default job title, add a description and confirm the upgrade job details by clicking **Start Upgrade job**. You will view the upgrade as an entry on the **Upgrade jobs** section.

**Important:** The upgrade process for the Endpoint Protector Client is impacted by a dedicated cron. Running every 5 minutes, the cron sets the upgrade process status to **Pending** and every 15 minutes checks and updates process status to **Completed** or **Completed with failures**.
16.2.2. Manage Upgrade Jobs
From this section you can view the upgraded jobs and use the **Actions** column to view job details, cancel, pause, retry, archive or delete an entry on the list.

To continue upgrading canceled Client Upgrade jobs, use the **Retry** option from the **Actions** column.

**Note:** If you deleted or archived a Client Upgrade job, then the endpoints become available for selection in other jobs.

![Upgrade Jobs screenshot](image1)

16.3. Client Uninstall
From this section, you can perform a remote uninstall of the Endpoint Protector Client. The computers will receive the uninstall command at the same time they receive the next set of commands from the server.

If the computer is offline, it will receive the uninstall command the first time it will come online. When the uninstall button is pressed the computer(s) will be grayed out until the action will be performed.

The uninstall command can be canceled if it was not already executed.

![Client Uninstall screenshot](image2)
**Note:** If the server and EPP client can't communicate due to missing server certification validation (when the certification validation setting is enabled), uninstall commands can't be executed from the EPP Server. In such cases, if you're unable to manually install the certificate on the EPP Client computer, you can temporarily disable the certification validation setting on the EPP Server and synchronize the EPP Client to retrieve an uninstall command.

### 16.4. System Administrators

From this section you can view, create, manage and delete administrators.

To create a new Administrator, under the table with existing administrators, click **Create** and then provide the following information:

1. **Administrator details** – add the username and password, email, first and last name, phone number and then select the UI language

2. **Account settings**
   - **Account is active** – manage the account status
   - **Login Attempt Restrictions** – enforce a 5 to 10 minutes timeout for 5 to 10 unsuccessful login attempts before a new login attempt can be made
   - **Enforce login IP restrictions** – restrict login attempts from specific IP addresses
   - **Require password change at next login** – request the administrator to change password at first login; once the password is changed, this setting is automatically disabled.

**Important:** The **Require password change at next login** setting is ignored in the following situations:

a) When the **Enforce all administrator password security at next login** setting is also enabled from System Configuration, **System Security**, then **Require password change at next login** is ignored and disabled once the password is changed.
b) For Active Directory imported users

c) For SSO users (Azure and OKTA) the setting is hidden

- Failed Login Alert – receive alerts for any failed login
- Schedule Exports Alert – receive alerts on any scheduled exports
- Ignore AD Authentication – allow using AD credentials to login Endpoint Protector

3. Super Administrator details

- Super Administrator – enable this section to grant the Administrator access to all Departments and Endpoint Protector sections
- Two Factor Authentication – enforce 2FA (Two-Factor Authentication) by using the Google Authenticator previously installed on your device
- Managed Departments – assign the Administrator to one or more departments
- Managed Administrators Groups – assign the Administrator to one or more Administrators Group

16.5. Administrator Types

The Super Administrator has complete control over the entire system. By enabling the Import users as super administrators settings in the Single Sign On section, you can grant Super Administrator privilege to all Azure Single Sign On imported users.

Super Administrators have access to the General Dashboard, can control Live Updates, can run Effective Rights reports, can manage Device Control, can manage Content Aware Protection (CAP) including Deep Packet Inspection (DPI), can manage eDiscovery, can manage Denylists, Allowlists, and URL Categories, can manage Enforced Encryption (EE), can manage Offline Temporary Password (OTP), can view Reporting and Statistics, manage
and view Administrative Actions, manage and view Alerts, manage and view Directory Services, manage and view Appliance Configuration and SIEM Integration, manage and view System Maintenance, manage and view Systems Configuration, download and view Client Software (including Upgrade), manage system parameters, and download and view Client Software (including Upgrade).

The Normal Administrator is a system user with normal privileges but some limitations. They can only manage entities belonging to the system departments for which they are responsible for. Normal Administrators can be allocated to certain responsibilities inside Administrators Groups to further restrict access. They can, for example, be assigned to a Helpdesk group with specific duties such as Offline Temporary Password and Enforced Encryption, or their permissions restricted to specific modules such as Content Aware and Device Control.

Despite these restrictions, Normal Administrators have access to a variety of system management tools, such as Manage Device Control, Manage Content Aware Protection (CAP) (including Deep Packet Inspection (DPI)), Manage eDiscovery, Manage Denylists, Manage Allowlists, Manage Offline Temporary Password (OTP), Manage Enforced Encryption (EE), View Reporting and Statistics, View and Manage Alerts, and Download and View Client Software (including Upgrade). They can also control system parameters.

By assigning Normal Administrators specific roles and groups, an organization can ensure that sensitive data and tools are only accessible to those who need them, while still providing their team members with the tools they need to efficiently manage the system.

16.6. Administrators Groups

From this section you can create and manage Administrators Groups, granting Normal Administrators with access to specific Endpoint Protector sections.

The Administrators added to these groups will only be able to view and manage the sections assigned by the selected roles.

By default, the following Administrators Groups are created:

- **Offline Temporary Password Administrators** – grants access only to the Offline Temporary Password section
- **Reports and Analysis Administrators** – grants access to the Reports and Analysis section
- **Enforced Encryption (EE) Administrators** – grants access only to the Enforced Encryption section
- **Maintenance Administrators** – grants access only to the Directory Services, as well as Appliance Configuration, SIEM Integration and System Maintenance.
● **Helpdesk** - grants access only to the Enforced Encryption and Offline Temporary Password sections

● **Device Control Administrators** – grants access only to the Device Control section

● **Read Only Administrators** – grants read only access to all Endpoint Protector sections

● **Content Aware Protection (CAP) Administrators** – grants access to Content Aware Protection (CAP) (including Deep Packet Inspection (DPI)) as well as Denylists, Allowlists, and URL Categories.

● **eDiscovery Administrators** – grants access only to the eDiscovery section

To create a new Administrators Group, click **Create** and then provide the following information:

- **Name** – add a name for the new Administrators Group
- **Roles** – select one or more roles from the list

**Important:** The Read Only role cannot be combined with any other roles!

- **Description** - add a description of the new Administrators Group
- **Select Administrators** – add one or more Administrators to this group

You can also add Administrators to an Administrator Group when creating an Administrator from System Configuration, Systems Administrators section, on the Managed Administrators Groups field.

**Note:** The Support section will always be available in Endpoint Protector regardless of the role you assign to the Administrator Group.

16.6.1. User Role Matrix

The EPP User Role Matrix defines the many capabilities and permissions that Administrators have based on their role. This matrix ensures that users only have access to the features
they need to fulfill their duties, boosting security and lowering the chance of unintentional changes or data breaches.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Super Admin</th>
<th>Normal Admin</th>
<th>Reports &amp; Analyst Admin</th>
<th>OAT Admin</th>
<th>IE Admin</th>
<th>Maintenance Admin</th>
<th>HelpDesk (OIT &amp; EIT)</th>
<th>Device Control Admin</th>
<th>CAP Admin</th>
<th>eDiscovery Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the General Dashboard</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Live Updates</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run Effective Rights reports</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Device Control</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Content-Aware Protection (CAP) including Deep Packet Inspection</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage eDiscovery</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Sensitive, Allowlists, and URL Categories</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Enforced Encryption (EE)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Offline Temporary Password (OTP)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Reporting and Statistics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage and View Administrative Actions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and Manage Alerts</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage and View Directory Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage and View Appliance Configuration and GEM Integration</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage and View System Maintenance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage and View System Configuration</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Download and View Client Software (Including Upgrade)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage System Parameters</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Except for items, Manage System Parameters</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Within the EPP, there are several different user roles, each with their own set of permissions. The **Super Administrator** role is the most powerful and has access to all features, whilst other roles have more restricted access based on their job tasks.

**Note:** Each of the aforementioned roles can be assigned to a department. When in read-only mode, users are only given viewing options. This guarantees that they can obtain essential information but are unable to alter the system.

### 16.7. Two Factor Authentication

The Two Factor Authentication (2FA) allows the login process to include an extra step requesting a temporary code generated via the Google Authenticator app. With the Two Factor Authentication on, once the user creation or edit is saved, the administrator will be redirected to a verification screen.
The Google Authenticator app will ask you to register using a unique code or QR Code. Following the registration process, your account will be added to the list with a validity timer for the unique code that will be used for the second authentication factor.

16.8. System Departments

This section allows you to create and manage System Departments.

Using System Departments is optional. Endpoint Protector works perfectly well with just the Default Department (defdep). Moreover, most scenarios are best covered by simply using Devices, Computers, Users, and Groups (the entities also available in AD).

The functionality becomes useful mainly in large installations, with a high number of Administrators and, where strict regulatory compliance rules are in place. Under these circumstances, departments can be created, allowing each Normal Administrators to only manage their own entities.
**Important:** This functionality should not be confused with Groups of computers and users, nor with administrators’ roles.

To create a new department click **Create** and then provide a name, description and unique code.

**Note:** If you provide a wrong department code or none at all, the department code is considered invalid and that computer will be assigned to the default department (defdep).

In terms of terminology, a similarity between Endpoint Protector and Active Directory (or any other Director Service software) would make the Department equivalent to an Organization Unit. Of course, the Organization Unit is not identical to the Department, and again Endpoint Protector leaves the power to the actual Super Administrator to virtually link one or more Organization Units to an Endpoint Protector Department.

Each entity (e.g.: computer) must belong to a department. When deploying the Endpoint Protector Client, if a department having the given code is found, then the computer will register, and it will belong to that department.

**Example:** Computer Test-PC is registered to the department “developers”. In this case, the user Test logged on that computer will be assigned to the same department together with the devices connected on the computer Test-PC.
Super Administrators (e.g.: root) will have access to all the main entities regardless of their departments. They will also be able to create departments, as well as Normal Administrators or Administrators with other roles. Super Administrators will also be responsible for assigning administrators to manage departments.

A regular administrator can only manage the departments it was assigned to. It cannot see entities relating to other departments.

16.9. System Security

From this section, you can configure several security settings such as client uninstalling passwords, restricting access to sensitive information only to super administrators, protecting sensitive data, and enforcing all administrators’ password security at the next login and password expiration options.

16.9.1. Security Password for Uninstall Protection

From this section, you can set a password that will be required when the user performs an Endpoint Protector Client uninstall action.

**Note:** At the top of the page, you will view a message informing you if a password is set for this action.
16.9.2. Data Security Privileges
From this section, you can allow access to sensitive data only to super administrators.

16.9.3. Additional Security Password for Sensitive Data Protection
From this section, you can set a password for sensitive data to provide additional security.

**Note:** At the top of the page, you will view a message informing you if a password is set for this action.

16.9.4. Security Password for System Administrator
From this section, you can require all administrators to use their security password at the next login session.

**Note:** Once you have enabled the “Enforce all administrator password security at next login” setting, the feature cannot be disabled.

If enabled, only complex passwords can be defined, complying with the below rules:

- the minimum length is 9 characters
- must contain small and capital letters, numbers and special characters
- consecutive characters and numbers in ascending order cannot be used

**Important:** The Enforce all administrator password security at next login setting will have priority over Advanced User Password Settings as this setting also applies to non-admin, such as Reporter, Read-only users, etc.
16.9.5. Advanced User Password Settings

From this section, you can set advanced user password settings for all users.

Enable the Complex Password setting and then provide the following information:

- Minimum password length: 8
- Minimum password uppercase characters: 1
- Minimum password lowercase characters: 1
- Minimum password numbers: 1
- Minimum password special characters: 1
- Select if consecutive and ascending characters can be used

If you enforce a password that expires, provide the following information:

- Set **password validity** up to 30 day(s)
- Select if the new **password must be different** from the previous 4 entries

These are mandatory requirements when creating a new Administrator from the **System Administrators** section.

**Important**: After you provide all information for the Advanced User Password Settings section, all users are required to change their passwords at the next login, not only admins.

![Advanced User Password Settings](image)

16.10. System Settings

From this section, you can manage general settings that apply to the entire system, several having already been configured from the initial Endpoint Protector Configuration Wizard.

16.10.1. Department Usage

Select an option to grant access for clients based on the **Department Code**.
You can also view the Default Department code - defdep.

**Note:** For detailed information, refer to the System Departments chapter.

### 16.10.2. Session Settings

You can modify the following session timeout settings:

- **Session Timeout** – set the amount of time the user is inactive until the session expires between 5 and 60 minutes
- **Timeout counter** – set the amount of time for the session timeout countdown between 5 seconds and Session Timeout minus one minute

**Example:** If you define the Session Timeout to 5 minutes and the Timeout counter to 60 seconds, then after 4 minutes of inactivity you will be notified by the pop-up window that in 60 seconds you will be logged out.

If you remain idle for the defined amount of time, then Endpoint Protector stops responding and displays a message that indicates the session will expire in the predefined countdown.

You can choose to log out or continue your session, resetting the session timeout interval.
16.10.3. Endpoint Protector Rights Functionality
Set functionality rights for computer, user, or both, in which case you can prioritize user rights or computer rights.

16.10.4. Smart Groups
Manage settings related to Smart Groups, Default Groups for Computers or Users.

**Note:** Smart Groups are dynamic groups for which membership can be defined based on element name pattern.

- **Enable Smart Groups** – when this setting is disabled, it will convert Smart Groups to regular groups with no entities assigned and will remove the Default Group for Computers and the Default Group for Users.

- **Enable Default Group for Computers** - this will create a default group for computers containing all computers that are not part of a Smart Group.

**Note:** By disabling this setting, you will delete the Default Group for Computers.

- **Enable Default Group for Users** - this will create a default group for users containing all users that are not part of a Smart Group.

**Note:** By disabling this setting, you will delete the Default Group for Users.

16.10.5. Client Update Mechanism
Enable the **Client Update V2** setting to improve the client update performance and add custom hostname and port.

**Note:** The custom port you define in this section will be used when generating the client update download link instead of the default 443.
16.10.6. Custom Settings

To display more information in Endpoint Protector, enable the following:

- Show VID, PID and Serial Number for Offline Temporary Password
- Show MAC Address for Offline Temporary Password
- Show User Domain
- MAC Address Priority
- Show Universal Offline Temporary Password only to Super Admins

16.10.7. Log Settings

Manage the following log settings:

- Set the Maximum number of rows in millions to export the Logs Report in .csv format.

**Note:** By setting the maximum number of rows to 1.0, you will export 1 million logs in the Logs Report .csv export as one row corresponds with one log.

When having partitions for logs on the server, make sure the dates are also selected when making the export.

- Reporting V2 – enabled by default, use this setting to modify the **Content Aware Report** log structure and display information in **Destination details, Email sender,** and **Email subject** columns.

**Note:** For Endpoint Protector Server versions older than 5.7.0.0, the Reporting V2 setting is not enabled by default.

The structure enabled by this setting will also be reflected in SIEM.
Set the **Maximum number of reported threats per event** that will be displayed in the **Content Aware Report** log structure, the expanded Log Details section, on the Count column.

**Note:** You can set a number of reported threats between 100 and 1000.

16.10.7.1. Log settings use case and terminology

**Log request** - sent by the Endpoint Protector Client

**Event** - scan result of a scanned document

**Threat** - matched item (e.g. US SSN)

Log request:
- event1.0 (scan result of a scanned document) => 1000 threats before splitting events
- event1.1 => 500 threats
- event2.0 => 200 threats
- up to 100 events

**Example:** Value set to 500. 3 documents containing 1,500; 600; and 200 threats are subject to Content Aware Protection policies.

The Endpoint Protector Client will send a single log request.

Log request:
- event1.0 (scan result of a scanned document) => 500 threats => splitting event
- event1.1 (scan result of a scanned document) => 500 threats => splitting event (second log entry in the reports)
- event1.2 (scan result of a scanned document) => 500 threats (third log entry in the reports)
- event2.0 (scan result of a scanned document) => 500 threats => splitting event
- event2.1 (scan result of a scanned document) => 100 threats (second log entry in the reports)
- event3.0 (scan result of a scanned document) => 200 threats
- up to 100 events
16.10.8. Content Aware Protection – Ignore Thresholds

Enable the Ignore Thresholds setting to allow Endpoint Protector to log all sensitive information from scanned files from 1 to 100,000 threats limit set in the Maximum number of reported threats field, for the Content Aware Protection Block policies applied.

**Note:** This will increase the amount of logging and potentially affect client and server performance.

**Important:** The Limit Reporting CAP setting has priority over Ignore Thresholds setting. If Limit Reporting CAP is enabled, the reporting will stop when the threshold is reached.

The maximum number of reported threats will be automatically modified as follows:

<table>
<thead>
<tr>
<th>User Input</th>
<th>Input Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

16.10.9. Virtual Desktop Clones

Enable the Virtual Desktop Clones Support setting to allow the Endpoint Protector server to identify the virtual desktop clone and interact accordingly with the Endpoint Protector client.

16.10.10. Deep Packet Inspection Certificate

Disable the Deep Packet Inspection certificate download to require the Endpoint Protector clients to use the legacy certificate. You can also download the Client CA Certificate.

For detailed information, refer to the Deep Packet Inspection chapter.
16.10.11. Server Certificate Stack

Use this section to regenerate a custom server certificate.

Enable the option and then provide the following information:

- **FQDN** (Fully Qualified Domain Name) - used in certificates and **Regenerate Server Certificate Stack** and CA Certificate used for Deep Packet Inspection on macOS
- **Country name** – add the first two letters of the country
- **State or Province name** – add the state or province name
- **Locality Name** – add locality name

Once you’ve set all the mandatory information, scroll to the bottom of the settings page, click **Save** and then return to the Server Certificate Stack section and click **Regenerate Server Certificate Stack**.

The Server certificate will be regenerated in a couple of minutes, and the user will be logged out.

**Important:** Download the Deep Packet Inspection certificate again on macOS and trust it into the keychain.

**Note:** This setting is valid for macOS 12.0 or higher, but when regenerating the CA certificate, also replace it on macOS 11.0 - download certificate and add to **System > Keychain Access**.

**Important:** Do not use this setting if no instance of macOS 12.0 (or higher) is registered on the Endpoint Protector server.

16.10.12. Single Sign On

Enable the **Single Sign On Login** setting to log into Endpoint Protector and then select a **Failover Login User** to use when single sign on is not functional.
16.10.13. Active Directory Authentication

Enable the **Active Directory Authentication** setting to import an Active Directory group of administrators into Endpoint Protector as Super Administrators.

**Note:** By enabling the Active Directory Authentication, you allow the administrators to use their Active Directory credentials to log into Endpoint Protector.

To import an Active Directory group of administrators, follow these steps:

1. Fill in the fields with the required information, considering:
   a. In some cases, you need to add the domain in front of the `username` (domain\username)
   b. **Active Directory Administrators Group** can be synchronized with any other groups of users except for "primary groups" which is limited from this action by Microsoft
2. Scroll to the bottom of the page and save the changes – you will view a successful message at the top of the page;
3. Return to the **Active Directory Authentication** section and click **Test Connection** to confirm the process was successful;
4. Click **Sync AD Administrators**.

**Important:** Once the Active Directory Administrators Group has been defined, only users that are part of this AD group will be synced and imported as Super Administrators for Endpoint Protector. Any additional administrators (with different access control levels) can be created manually from the **System Administrators** section.
16.10.14. **E-mail Server Settings**

Manage **Email server** settings based on the email type you use - **native** or **SMTP**.

**Note:** To enable this feature, you need an Internet connection.

16.10.15. **Proxy Server Settings**

Configure **Proxy server** settings by managing the following:

- **Proxy Type**
- **Authentication Type**
- **IP and Port**
- **Proxy access credentials** (username/password)

Once you provide all the information, click **Test** to confirm the settings are working successfully.

**Note:** If a Proxy Server is not configured, Endpoint Protector will connect directly to liveupdate.endpointprotector.com.

16.10.16. **Main Administrator Contact Details**

Edit contact details for the main administrator and then click **Save** to keep all modifications.

16.11. **System Licensing**

From this section, you can manage and have a complete overview of the Endpoint Protector licensing status.
Note: As of Endpoint Protector Version 5.9.0.0, a new subscription-based licensing system has been introduced. This change removes the licensing restrictions on Premium features, granting unrestricted access to features like Contextual Detection for all customers. This adjustment aligns with the revised licensing model, categorizing all features as standard and accessible to all users.

Endpoint Protector Licensing is based on two main aspects:

- **Modules** – all modules are licensed separately (Content Aware Protection, eDiscovery, etc.) and require the Device Control module
- **Endpoints** – refers to the Windows, Mac or Linux computers that need to be protected, by having the Endpoint Protector Client installed on them

Based on the selected Modules and Endpoints, a licensing file will be provided by your Endpoint Protector Representative.

The Endpoint Protector **Server ID** uniquely identifies each server and is linked to the license file. This needs to be provided to the Endpoint Protector Representative before purchasing the licenses.

The **License End Date** displays the Validity of the Licenses in the system.

The **Support** represents the level of purchased Support (Standard or Premium)

16.11.1. Free Trial

Endpoint Protector provides a one-time free, 30-day trial period.

By enabling the **Free Trial** option, you will automatically enable all modules for 50 computers. The endpoint licenses will be assigned on a **first-in-first-served** basis.

If one or more licensed endpoints become inactive and need to be reassigned, you can release those licenses, which will automatically be reassigned to other online computers.
16.11.2. Import and manage Licenses

Click **Import Licenses** to allow browsing for the license file. It contains all the relevant information in a single file (modules, number of endpoints, expiry date, type of Support, etc.).

Click **View Licenses** to allow the management of the endpoint licenses.

If one or more licensed endpoints become inactive and need to be reassigned, you can release those licenses, which will automatically be reassigned to other online computers.

By using the **Automatic Release Licenses** functionality, licenses will be released automatically for endpoints that have not been seen online in a specific number of days (15 days, 30 days, 90 days, etc. or a custom value).
16.12. Single Sign On

Single Sign On allows you to log in the Endpoint Protector Server with Azure AD. If Premium license is enabled, Single Sign On with OKTA credentials is also available.

The Single Sign On section includes the following:

- **Provider** – select a provider to start the configuration

- **Failover Login URL** - enter or generate a link to a page where login locally with Endpoint Protector Super Administrator is allowed. This will bypass Azure Single Sign On login in the situation when it stops working. To view the URL, enable the Display Failover Login URL setting.

**Note:** You can provide Super Administrator status to all imported users by enabling the Import users as super administrators setting.

- **Service Provider** represents the identity of the Endpoint Protector Server. The information is required when configuring the Endpoint Protector application in Azure. Select if the login is based on **IP or Domain**, provide an **Entity ID** as well as **Login** and **Logout URL**.

- **Identity Provider** represents Azure side. It includes the fields where data generated from Azure should be filed so you will be able to login to Endpoint Protector Server.

16.12.1. Single Sign On configuration with Azure AD

To activate Single Sign on with Azure AD, follow these steps:

1. Go to **System Configuration, System Settings, Single Sign On**.
2. Upon the activation, select a Failover Login User from the drop-down; root user will be selected by default.
After the above steps have been completed, a Single Sign On subsection is displayed in the System Configuration section.

**Note:** The Failover Login User you selected cannot be deleted from Endpoint Protector Server while it is selected. Single Sign On cannot be activated without a Failover Login User.

3. Select the **Provider** to view Single Sign On subsections.

4. Go to portal.azure.com and login.

5. Go to **Azure Active Directory**.

6. Create a **New Enterprise Application**:
   a. Add a **New Application**;
   b. Click **Create your own application**;
   c. Give the application a name;
d. Select **Integrate any other application you don’t find in the gallery**;
e. Click **Create**.
7. From the left-hand menu go to **Single Sign On** and then select the **SAML** method.
8. To edit **Basic SAML Configuration**, open the Single Sign On page from the Endpoint Protector Server and copy/paste the data from the Single Sign On page on Basic SAML Configuration page.

9. On the **Basic SAML Configuration** page, delete the data that is by default completed for Identifier (Entity Edit).

10. From the **Single Sign On** page on the **Endpoint Protector Server**
a. copy the data from **Service Provider**, the **Entity ID** field and paste it on the Identifier (Entity ID) field and on **Reply URL** (Assertion Consumer Service URL) from Basic SAML Configuration page and check it as **Default**.

b. Copy **Login URL** from **Service Provider, Single Sign On** page from **Endpoint Protector Server** and paste it on **Sign on URL** from Basic SAML Configuration page.

c. Copy **Logout URL** from **Service Provider, Single Sign On** page from **Endpoint Protector Server** and paste it on **Logout URL** from Basic SAML Configuration page.
11. Save the settings without testing Single Sign On yet.

12. Go to Step 3 from the page, **SAML Signing Certificate** and click **Edit**.

13. Change **Signing Algorithm** to **SHA-1** and click **Save**.
14. From Step 3, **SAML Signing Certificate**, download **Certificate (Base64)**.
15. Open the downloaded certificate with a text editor and copy the content inside it.

16. Paste the content in the **Endpoint Protector Server, System Configuration** section, **Single Sign On, Identity Provider, Security Certificate**.

17. Return to **Azure SAML-based Sign On** page and reach Step 4, Set up “your application” and copy Azure AD Identifier.
18. Go to Endpoint Protector Server, System Configuration, Single Sign On, Identity Provider, Azure AD Identifier and paste the data from the previous step.

19. Return to Azure SAML-based Sign On page and reach Step 4, Set up “your application” and copy Login URL.

20. Switch to Endpoint Protector Server, System Configuration, Single Sign On, Identity Provider, Login URL and paste the data from the previous step.

21. Return to Azure SAML-based Sign On page and reach Step 4 -> Set up “your application” and copy Logout URL.

22. Switch to Endpoint Protector Server, System Configuration, Single Sign On, Identity Provider, Logout URL and paste the data from the previous step.
23. Generate Failover Login URL from Endpoint Protector Server, System Configuration, Single Sign On, Failover Login URL and Save the URL.


25. Switch to Azure, Select Users and groups from the left menu.
26. Go to Add user/group, none Selected, search for the Azure User, Select, Assign.
27. The User is assigned to the application and login in Endpoint Protector with Azure is now possible.


**Single Sign On Configuration with OKTA**

1. To activate Single Sign On, go to System Configuration, System Settings, Single Sign On.

Upon the activation, select a Failover Login User from the drop-down. Root user will be selected by default.

![Default System Settings](default_system_settings.png)

After the above steps have been completed, a Single Sign On subsection is displayed in the System Configuration section.

2. Select the Provider in order for Single Sign On subsection to be displayed.
3. Go to yourcompany.okta.com, Applications and then Create App Integration.
4. On the following screen, select **SAML 2.0** and click **Next**.

5. Set a **Name** for the Application and click **Next**.

6. Open the **Configure SAML** tab.

7. Go to your Endpoint Protector Server, System Configuration, Single Sign On.
8. Copy the information from:

- **Audience URI (SP Entity ID)** and paste it on the field with the same name from OKTA, Configure SAML.

- **Login URL OKTA** and paste it on the field **Single sign on URL** from OKTA page, Configure SAML.

9. On the OKTA page, click **Show Advanced Settings**.
10. Edit the following fields:

- **Signature Algorithm**, select RSA-SHA1
- **Digest Algorithm**, select SHA1

11. Hide **Advanced Settings** and click **Next**.

12. At step 3, select an answer for each question and click **Finish**.
13. Go to Applications, the Endpoint Protector application, Assignments and assign People to this application.
14. After assigning the accounts, click **Done**.

15. Go to **Applications**, open the created app and click **Sign On, View Setup Instructions**.

16. From the new opened section, copy the needed information and paste it on your **Endpoint Protector Server**:

   - Identity Provider Single Sign-On URL to Endpoint Protector Server, System configuration, Single Sign On, Identity Provider Single Sign-on URL.
- Identity Provider Issuer to Endpoint Protector Server, System configuration, Single Sign On, Identity Provider Issuer

17. Save the settings on your Endpoint Protector Server and click **Test** to confirm configuration settings are correct.
17. System Parameters

17.1. Device Types and Notifications

From this section you can view and manage device types and notifications, view and enable default notifications and their translations and define custom notifications for Content Aware Protection policies and Device Control User Remediation.

17.1.1. List of Device Types and Notifications

On the List of Device Types and Notifications, you can view the Device Types available in the system along with their availability for each operating system and if those devices can be inspected by the Content Aware Protection module.

You can enable and edit the notification messages that appear on the Endpoint Protector Client from the Actions column.
17.1.2. List of Default Notifications

You can view and enable/disable a message from the list of Default Notifications or edit the custom notifications translations.

Note: You can enable Custom Client Notifications globally from Device Control, Global Settings or individually for computers or groups, from their specific Settings sections.

17.1.3. Custom Content Aware Protection Notifications

On this section, you can create custom notifications and set them per Content Aware Policies so specific Content Aware Policies can have specific client notifications.

To add a new notification, follow these steps:

1. Click Create
2. Set a Template Name, Title and Body text.
Use these parameters to create your custom message:

- `{fileName}` - the blocked/reported file name;
- `{type}` - will be replaced with blocked or reported, depending on the policy type;
- `{threatName}` - will be replaced with the threat name;
- `{threatMatch}` - will be replaced with the matched text;

3. **Click Save**

**Example:** "{fileName}" was "{type}" because it contains confidential data.

Once the notification was created, you can select the custom notification from the Notification Template drop-down of a specific Content Aware Policy.

17.1.4. Custom Device Control User Remediation Notifications

**Note:** This section is available only if the Device Control User Remediation setting is enabled from the User Remediation section.

In this section you can add, edit and delete custom notifications for Device Control User Remediation.

You can add a maximum of 100 custom notifications but you cannot delete the default entry.

To add a new custom notification, follow these steps:

1. **Click Create**
2. Use these parameters to create your custom message:
3. Click **Save**

**Example:** USB Driver({deviceName}) is blocked({action})

Once the notification was created, you can select the custom notification from the **User Remediation Notification Template** drop-down located in the **Device Control** section, **Global Setting, Users, Computers** and **Groups**.

17.2. **Contextual Detection**

From this section, you can manage the contextual detection for the entire system. If enabled, the confidential information detected by Endpoint Protector will be inspected for both content and context.

In addition to the function that detects sensitive information (e.g.: Credit Cards, IDs, Passports, Driving Licenses, etc.), the context will also be taken into consideration (e.g.: proximity to other relevant keywords, other related functions, regular expressions, etc.).

In addition to providing context to the detected sensitive information, this functionality also helps decrease false positives.

**Note:** This feature applies at a global level, for both **Content Aware Protection** and **eDiscovery Policies**. If enabled, the context detection will supersede the content only detection through the system.
Please ensure the accuracy of the rules and the relevance for your scenarios before enabling this functionality.

Once the Contextual Detection feature is enabled, it will apply at a global level, based on the rules defined in the Contextual XML (but also linked to the configured Content Aware Protection and eDiscovery policies).

There are two options to create the Contextual rules:

- creating it directly from the Endpoint Protector Server
- manually editing the Contextual XML and then uploading it to the Endpoint Protector Server

17.2.1. Creating the XML

This method is recommended for general use as it is the easiest method and it can cover most use cases.
For each category of Predefined Content (e.g.: Credit Cards, IDs, Passports, Driving Licenses, etc.), contextual detection can be configured by clicking on the **Add** button and selecting things like:

- **Category and Type** – the content aware detection function.
- **Surrounding text** – the number of characters of the search interval to determine the context.
- **Related Dictionary** – a set of keywords related to the PII.
- **Related Regular Expression** – an additional way of adding a related rule that is not among the content aware detection functions.
- **Related File Type** – the related file type.
- **Related File Size (MB)** – the related file size, in megabytes.
- **Minimum Matches** – the minimum number of items to match to validate the detection rule.
- **Unrelated Dictionary** – a set of keywords not related to the PII.
- **Unrelated Regular Expression** – an additional way of adding a non-related rule that is not among the content aware detection functions.
- **Unrelated File Type** – the unrelated file type.
- **Unrelated File Size (MB)** – the unrelated file size, in megabytes.
- **Maximum Matches** – the value above which the rule will not be validated (recommended value is 0).

**Important:** Do not forget to Generate the Contextual XML after creating or making changes to contextual rules!
17.2.2. Uploading the XML

This method is recommended for advanced Administrators as it offers extended functionalities but it also requires a deeper understanding of the XML syntax. Advanced contextual functionalities are also available. For this method, the Contextual XML file has to be edited manually by the Administrator and then uploaded to the Endpoint Protector Server.

**Proximity, Dictionaries, Regex**, etc. have to be defined within the XML document. In addition to the functionalities described in the previous chapter, there are more complex options available like: **Confidence Level**, additional **Functions** to consider when determining the Main Function, etc.

Study the examples provided within Endpoint Protector Server to understand the syntax needed in the Contextual XML.

**Example**

```xml
<Rules>
<!-- SSN / Canada this is an example with multiple patterns -->
<Entity id="ssn/canada" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="75">
    <Any minMatches="2">
      <Match idRef="keywords_Canada_SSN_1"/>
      <Match idRef="keywords_Canada_SSN_2"/>
      <Match idRef="validate_date_fct"/>
      <Match idRef="regex_email_id"/> <!-- This is just an example -->
    </Any>
    <Any maxMatches="0">
      <Match idRef="keywords_exclude_Canada_SSN"/>
    </Any>
  </Pattern>
</Entity>

<Function id="validate_date_fct" name="SEARCH_DATE_INTRL"/> <!-- name should be the same with the one on the client -->
  <Function id="func_dlp_is_valid_ssn" name="SEARCH_SSN_Canada"/> <!-- name should be the same with the one on the client -->

**Example**

```xml
<Keyword id="keywords_Canada_SSN_1">
  <Group matchStyle="word">
    <Term>sin</Term>
    <Term>social insurance</Term>
  </Group>
</Keyword>
```
<Term>numero d'assurance sociale</Term>
<Term>sins</Term>
<Term>ssn</Term>
<Term>ssns</Term>
<Term>social security</Term>
<Term>numero d'assurance sociale</Term>
<Term>national identification number</Term>
<Term>national id</Term>
<Term>sin#</Term>

</Group>
</Keyword>

<Keyword id="keywords_Canada_SSN_2">
<Group matchStyle="word">
   <Term>driver's license</Term>
   <Term>drivers license</Term>
   <Term>DOB</Term>
   <Term>Birthdate</Term>
</Group>
</Keyword>

<Keyword id="keywords_exclude_Canada_SSN">
<Group matchStyle="word">
   <Term>random word</Term>
</Group>
</Keyword>

<Regex id="regex_email_id">[0-9a-zA-Z.+]@[-0-9a-zA-Z.+]\.[a-zA-Z]{2,4}</Regex>

</Rules>
</RulePackage>
17.3. Advanced Scanning Detection

The Windows environment is subject to constant OS and security updates and the installed applications are in a constant loop of continuous development. To avoid eventual changes that interfere with the Endpoint Protector Client, the ability to allow applications and processes is available.

The Advanced Scanning Exceptions feature allows applications to be excluded from scanning, for endpoints that have the Advanced Printing and MTP scanning feature enabled.

**Note:** This feature applies at a global level, for all Windows endpoints that have the Advanced Printing and MTP Scanning features enabled.
17.4. Rights

This subsection displays a list with all access rights that can be assigned to devices.

17.5. Events

In this section you can view, manage and export the events list logged by Endpoint Protector.

You can edit event name and description or enable/disable logging for specific events from the Actions column.
17.5.1. Events Types and Descriptions

This subsection displays a comprehensive list of events, and ensures that administrators can effectively manage and monitor their data protection policies. Additionally, there are more specific events, such as those related to EasyLock deployment, printer activity, user information updates, transfer limits, external repository uploads, content remediation, forced uninstall attempts, device remediation sessions, certificate management, unplanned client terminations, artifact receipts, and DPI bypassed traffic. These events provide granular insight into various system activities, ensuring that organizations can maintain robust security and compliance measures. For a detailed view of all events and their descriptions, please see the table below.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>Device Connected</td>
</tr>
<tr>
<td>Disconnected</td>
<td>Device Disconnected</td>
</tr>
<tr>
<td>File Read</td>
<td>File read from device</td>
</tr>
<tr>
<td>File Write</td>
<td>File written to device</td>
</tr>
<tr>
<td>File Read-Write</td>
<td>File read and write from device</td>
</tr>
<tr>
<td>File Rename</td>
<td>File from device renamed</td>
</tr>
<tr>
<td>File Delete</td>
<td>File deleted from device</td>
</tr>
<tr>
<td>Device TD</td>
<td>Trusted Device™ connected</td>
</tr>
<tr>
<td>Deleted</td>
<td>File deleted from device</td>
</tr>
<tr>
<td>Enable Read-Only</td>
<td>Device Read-Only Enabled</td>
</tr>
<tr>
<td>Enable if TD Level 1</td>
<td>Allows access when a Trusted Device™ is connected (e.g., a USB stick with EasyLock installed, which is automatically launched)</td>
</tr>
<tr>
<td>Enable if TD Level 2</td>
<td>Allows access when Trust Level 2 device is connected</td>
</tr>
<tr>
<td>Enable if TD Level 3</td>
<td>Allows access when Trust Level 3 device is connected</td>
</tr>
<tr>
<td>Enable if TD Level 4</td>
<td>Allows access when Trust Level 4 device is connected</td>
</tr>
<tr>
<td>AD Synchronization</td>
<td>AD Synchronization</td>
</tr>
<tr>
<td>Blocked</td>
<td>Device or port blocked</td>
</tr>
<tr>
<td>Unblocked</td>
<td>Device or port unblocked</td>
</tr>
<tr>
<td>Offline Temporary Password Used</td>
<td>Offline Temporary Password Used</td>
</tr>
<tr>
<td>User Login</td>
<td>User Login</td>
</tr>
<tr>
<td>File Encrypt</td>
<td>File encrypted using EasyLock</td>
</tr>
<tr>
<td>File Decrypt</td>
<td>File decrypted using EasyLock</td>
</tr>
<tr>
<td>File Encrypt (offline)</td>
<td>File encrypted using EasyLock when not communicating with the Endpoint Protector Server</td>
</tr>
<tr>
<td>File Decrypt (offline)</td>
<td>File decrypted using EasyLock when not communicating with the Endpoint Protector Server</td>
</tr>
<tr>
<td>Content Threat Detected</td>
<td>Content Aware Protection - Threat Detected</td>
</tr>
<tr>
<td>Content Threat Blocked</td>
<td>Content Aware Protection - Threat Blocked</td>
</tr>
<tr>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>File Copy</td>
<td>A file was copied to or from a removable device</td>
</tr>
<tr>
<td>Content Threat Discovered</td>
<td>eDiscovery - Threat Discovered</td>
</tr>
<tr>
<td>eDiscovery Client Action</td>
<td>eDiscovery - Action received successfully</td>
</tr>
<tr>
<td>User Logout</td>
<td>User Logout</td>
</tr>
<tr>
<td>Client Integrity OK</td>
<td>Endpoint Protector Client Integrity ok</td>
</tr>
<tr>
<td>Client Integrity Fail</td>
<td>Endpoint Protector Client Integrity failed</td>
</tr>
<tr>
<td>Policies Received</td>
<td>Endpoint Protector Client received policy successfully</td>
</tr>
<tr>
<td>Uninstall Attempt</td>
<td>Endpoint Protector Client uninstall attempt</td>
</tr>
<tr>
<td>EasyLock - successfully deployed</td>
<td>EasyLock - successfully deployed</td>
</tr>
<tr>
<td>EasyLock - deployment failed</td>
<td>EasyLock - deployment failed</td>
</tr>
<tr>
<td>File Printed</td>
<td>File sent to printer successfully</td>
</tr>
<tr>
<td>User Information Updated</td>
<td>User information updated successfully</td>
</tr>
<tr>
<td>Transfer Limit Reached</td>
<td>Transfer Limit Reached</td>
</tr>
<tr>
<td>External Repository Upload</td>
<td>File Shadow uploaded to Repository successfully</td>
</tr>
<tr>
<td>External Repository Upload Fail</td>
<td>File Shadow uploaded to Repository failed</td>
</tr>
<tr>
<td>Content Remediation Session Active</td>
<td>Content Aware Protection - Threat Remediated</td>
</tr>
<tr>
<td>Content Remediation Request Canceled by User</td>
<td>Content Aware Protection - User Remediation dialog was closed by the user</td>
</tr>
<tr>
<td>Forced Uninstall Attempt</td>
<td>Endpoint Protector Client forced uninstall attempt</td>
</tr>
<tr>
<td>Device Remediation Request Canceled by User</td>
<td>Device Control - User Remediation dialog was closed by the user</td>
</tr>
<tr>
<td>Device Remediation Session Canceled</td>
<td>Device Temporarily Unlock with User Remediation canceled</td>
</tr>
<tr>
<td>Device Remediation Session Active</td>
<td>Device Temporarily Unlocked with User Remediation</td>
</tr>
<tr>
<td>Device Remediation Session Ended</td>
<td>Device Temporarily Unlock with User Remediation ended</td>
</tr>
<tr>
<td>Certificate added to Keychain/store</td>
<td>Certificate added to Keychain/store successfully</td>
</tr>
<tr>
<td>Unplanned Client Termination</td>
<td>Unplanned Client Termination</td>
</tr>
<tr>
<td>Artifact Received</td>
<td>Artifact Received</td>
</tr>
<tr>
<td>DPI Bypassed Traffic</td>
<td>DPI Bypassed Traffic</td>
</tr>
</tbody>
</table>
17.6. User Remediation

User remediation is a feature that allows the end-users to apply a justification and self-remediate a policy violation or a restricted-access device.

**Note:** This feature is only available for **Premium** licenses.

![User Remediation Settings](image)

17.6.1. User Remediation Settings

In this section, you can customize the User Remediation notification, manage settings and enable User Remediation for Device Control.

- **Display Custom Logo** – select a 200x200 pixels image to be displayed on the pop-up notification

- **Display Custom URL** – add a URL to direct the end-user to a specific web page, and then add a label for the URL

  **Note:** The following URL formats are accepted:

  - `http://endpointprotector.com`
  - `https://endpointprotector.com`
  - `http://www.endpointprotector.com`
  - `https://www.endpointprotector.com`

- **Require Credentials** – request the end-user to use their local account or Active Directory credentials

  **Note:** The following credential formats are accepted for login:

  - **Local user** - computer_name\username *(John-PC\John)*
  - **LDAP/AD user**
- domain_name\username (epp.com\John)
- ip\username (192.168.14.140\John)

- **Time Interval** – enter the time interval in which the end-user can remediate a Block and Remediated threat or a restricted-access device

- **Maximum Time Interval** – enter the maximum time interval in which the end-user can remediate a Block and Remediated threat or restricted-access device

**Note:** The maximum time interval you can enter is **1440 minutes (24 hours)**.

- **Enable User Remediation for Device Control** – enable the setting to use the user remediation feature for the Device Control module.

  **Important:** The Enable User Remediation for Device Control setting is disabled by default. By enabling this feature, all the settings regarding User Remediation will be applied to both Content Aware Protection and Device Control modules.

17.6.2. **Justifications List**

In this section, you can view, add, edit, export, and remove justifications. The justification represents the reason selected by the end-user to justify the threat or device remediation.

To add a new justification, click **Add**, fill in the mandatory fields and then click **Save**. You can add up to a maximum of 10 justifications. By default, several justifications are already added, but make sure that at least one justification is enabled all the time.

To enable and enforce the end-user to view User Remediation pop-up notifications, manage the option from Device Control, Global Settings, **Endpoint Protector Client Settings**.
17.6.3. Enabling User Remediation

To use User Remediation for Device Control, follow these steps:

1. Enable the **User Remediation for Device Control** feature from **User Remediation Settings**;

2. Customize the User Remediation notifications for Device Control.

   To do so, go to the **Devices Types and Notifications**, Custom Device Control User Remediation section, click **Create**, fill in the mandatory fields and **Save**;
3. Enable the **User Remediation Pop-up** setting from the [Endpoint Protector Client settings](#) section and then select the customized notification from the **User Remediation Notification Template** drop-down list;
4. Navigate to **Global Rights**, Device Types section and enable **User Remediation** for devices with limited access – devices that have full access permission cannot benefit from the User Remediation feature.

**Note:** For built-in devices, such as Webcam and Network share, the User Remediation feature is not available.
17.6.4. User Remediation Usage

To remediate the device, the end-user has to follow these steps:

1. Open the **Endpoint Protector notifier** and go to the **Device Control** tab;
2. Select the device for remediation and click **Self Remediate**;
3. On the **Self Remediate** section:
   a. select a **justification** from the drop-down list
   b. add a **reason** for the justification (if required)
   c. navigate to the **custom URL** situated under the logo
   d. add your credentials if the **Require Credentials** setting was enabled (click the username icon to refresh your current username)
      i. Note: When reopening the dialog, if a different username was used for authentication, EPP Notifier will automatically switch back to the username of the currently logged-in user.
      ii. Note: Usernames are not case sensitive.
   e. add the **number of minutes** needed to remediate the device (you can hover over the default number to view the maximum time interval)
   f. click **Authorize**

**Note:** You can manage more settings for the Self Remediate feature from System Preferences and **User Remediation** sections.
To stop the device remediation session at any time during the time interval, select the device from the Device Control tab in the Endpoint Protector notifier and then click Revoke Remediation.
18. Endpoint Protector Agent

The Endpoint Protector Agent enforces the Rights and Settings received from the Endpoint Protector Server on the protected endpoints (Windows, Mac, and Linux).

You can download the Endpoint Protector Agent directly from the Endpoint Protector UI. For detailed information about downloading the Endpoint Protector Agent, refer to the Client Software chapter.

**Note:** You can use tools like Active Directory or JAMF to deploy the Endpoint Protector Agent in large networks.

**Important:** Starting with Endpoint Protector Server version 5.8.0.0, you benefit from an additional security measure that safeguards the Agent integrity, available from Device Control, Global Settings page, the Tamper Mode setting - to prevent the Endpoint Protector Agent from unauthorized termination or alteration.

18.1. Agent Installation

For Windows and Mac, your input in installing the Endpoint Protector Agent is minimal. The Installation folder and Server information are already preconfigured, and downloadable from the Endpoint Protector Server.

For Linux installation instructions, read the readmeLinux.txt file available under the Read this before installing link.

**Note:** You can also install the Agent from a repository for Endpoint Protector Linux Agents starting with version 1.4.0.4., as described in the chapter below.

The following are several examples of supported distributions:

- Ubuntu 14.04+
- Mint 18.X
- CentOS 7.x
- Fedora 29
- OpenSUSE 42.2 and 42.3
18.1.1. Installation on macOS with Deep Packet Inspection and VPN Traffic Intercept active

1. Open the Endpoint Protector Server.
2. Go to the System configuration section, select Client Software and then download the macOS Endpoint Protector Agent.
3. Decompress the downloaded file.
4. Open the .pkg file and follow the installation steps and give the requested permissions.
5. After the installation was successfully made, go to System Preferences, Security & Privacy, Privacy tab, Full Disk Access, search for Endpoint Protector Client, select the checkbox and then save the changes.

7. Go to the System Configuration section, System Settings, Deep Packet Inspection Certificate, and download the CA Certificate.
8. Open the **Keychain Access** application from your macOS and select **System**.

9. Decompress the downloaded **ClientCerts** file.

10. Select **cacert.pem** file and drag and drop it on **Keychain Access, System**
11. Double-click the x on the newly added certificate and on the Trust section, select Always Trust.

12. Save the changes.


14. Select one option for EPP behavior when network extension is disabled.
● **Temporary Disable Deep Packet Inspection** – this option will temporary disable Deep Packet Inspection

● **Block Internet Access** – this option will end the Internet connection until the end-user approves the Endpoint Protector Proxy Configuration once the computer is rebooted.

15. Save the changes.

16. The following pop-up will be displayed informing the end-user that a System Extension is blocked and needs to be allowed.

17. Go to **System Preferences, Security and Privacy**, select the **General** tab and allow the Endpoint Protector Client Extension.
18. Allow the Endpoint Protector Proxy Configuration from the pop-up window.

At this point, the macOS Endpoint Protector Client installation is completed.

**Note:** If EPPNotifier is not visible or notifications do not display after the installation or upgrade of the EPP client on macOS, please resolve this issue by restarting your machine.

In situations where the EPP client is installed and then uninstalled on macOS, you may still see EPPNotifier in the Notification settings. To remove it from the list, simply right-click and select "Reset notifications."
18.1.2. Debian based distributions

While the installation process is similar, each distribution and version have their own particularities.

The following are several examples of supported distributions:

- Ubuntu 14.04
- Ubuntu 15.04
- Ubuntu 16.04
- Ubuntu 17.04
- Ubuntu 18.04
- Ubuntu 19.04
- Ubuntu 20.04
- Ubuntu 21.04
- Ubuntu 21.10
- Ubuntu 22.04
- LinuxMint
- Debian

```bash
sudo apt update
sudo apt upgrade
wget https://download.endpointprotector.com/linux_agent/EPPClient_v[X.X.X]/[Filename]
cd /Download
# unpack the archive
tar xvf [Filename.tar.xz]
# edit the options.ini file to contain the correct server address
cd [Extracted filename]
gedit options.ini
# run the installation script
bash install.sh
```

18.1.3. RedHat based distributions

While the installation process is similar, each distribution and version have their own particularities.

The following are several examples of supported distributions:
- CentOS 7.x
- RedHat 8.x
- Fedora 32, 33, 34, 35
- AWS Linux 2

```bash
sudo yum update
sudo yum upgrade
wget https://download.endpointprotector.com/linux_agent/EPPClient_v[X.X.X]/[Filename]
cd /Download
# unpack the archive
tar xvf [Filename.tar.xz]
# edit the options.ini file to contain the correct server address
cd [Extracted filename]
gedit options.ini
# run the installation script
sudo bash install.sh
```

- OpenSuse 15.2
- SUSE 15+
- SLED Linux Enterprise Server 15 SP1
- SLED Linux Enterprise Server 15 SP2
- SLED Linux Enterprise Server 15 SP3
4. Setting the Endpoint Protector Server IP

For all RedHat-based distributions, you need to follow an additional step after executing the above commands in order to set the Endpoint Protector Server IP.

Based on each distribution, follow the corresponding method:

**Method 1**

1. Define the Endpoint Protector Server IP
   
   EPPCLIENT_WS_SERVER=[**the desired IP**]
   
   export EPPCLIENT_WS_SERVER

2. Install the Endpoint Protector Client
   
   · for SUSE and openSUSE: #zypper install epp-client
   
   · for CentOS, RedHat, Fedora: #yum install epp-client
**Method 2**

1. Install the Endpoint Protector Client
   - for SUSE and openSUSE: `zypper install epp-client`
   - for CentOS, RedHat, Fedora: `yum install epp-client`

2. Run bash file to define the Endpoint Protector Server IP
   `bash `/opt/cososys/share/apps/epp-client/scripts/set_epp_client_server.sh'`
This section details the communication between the Endpoint Protector Server and Client encrypted by the TLS protocol.

- On Endpoint Protector Server version 5.7.0.0 TLSv1.2 is enabled by default and TLSv1.1 could be enabled upon request (backwards compatibility to older agents/appliances) in 5.7.0.0.
- On Endpoint Protector Server version 5.8.0.0 TLSv1.2 and TLSv1.3 will be enabled by default. TLSv1.1 could be enabled upon request (backwards compatibility to older agents/appliances) in 5.8.0.0.

### 19.1. Endpoint Protector Client

<table>
<thead>
<tr>
<th>OS</th>
<th>Older version</th>
<th>Newer version</th>
<th>Endpoint Protector Particularities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>❌/Windows 7, XP, and versions older than Windows 10</td>
<td>✔/Windows 10 and higher</td>
<td>Uses Windows’ built-in TLS encryption engine (Schannel).</td>
</tr>
<tr>
<td>macOS</td>
<td>✔</td>
<td>✔</td>
<td>Uses a custom bundled OpenSSL package shipped with the Endpoint Protector Client.</td>
</tr>
<tr>
<td>Linux</td>
<td>❌</td>
<td>✔</td>
<td>Uses Linux’s built-in OpenSSL engine.</td>
</tr>
</tbody>
</table>

### 19.2. Endpoint Protector Server
<table>
<thead>
<tr>
<th>Older than 5.7.0.0</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 5.7.0.0 or higher</td>
<td>For <strong>in-place upgrades via Live Update</strong>, the Linux OS libraries must be upgraded by Customer Support</td>
</tr>
</tbody>
</table>
20. Support

For additional support resources, please visit our website where you can read manuals, FAQs, watch videos and tutorials, direct e-mail support and much more.

Our Technical Support Department can also be contacted from Endpoint Protector, the Support section by using the Open Support Ticket option. One of our team members will contact you in the shortest time possible.
This document is provided on an “AS IS” basis. To the maximum extent permitted by law, we disclaim all liability, as well as any and all representations and warranties, whether express or implied, as to the fitness for a particular purpose, title, non-infringement, merchantability, interoperability and performance, in relation to this document. Nothing herein shall be deemed to constitute any warranty, representation or commitment in addition to those expressly provided in the terms and conditions that apply to the Customer's use of Endpoint Protector.

Each Endpoint Protector Server has the default SSH Protocol (22) open for Support Interventions and there is one (1) System Account enabled (epproot) protected with a password. The SSH Service can be disabled at customers’ request.

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.