ENDPOINT PROTECTOR | by CoSoSys

Quickstart Guide

Protecting the entire network

Quickstart Guide

Endpoint Protector is a Data Loss Prevention (DLP) solution designed for the endpoint systems that are used by your employees. Whether users are accessing data through laptops, desktops, or servers, DLP on these endpoint systems helps your organization to protect against data exfiltration and prevent data loss.

From accidental data loss, to malicious insider activity, protecting your sensitive data is critical to preventing the operational disruptions, regulatory issues, and reputational damage that result from data breaches.

This is why endpoint-based DLP has become a necessity in the ever-evolving cyber threat landscape, and without it, Network Administrators have little chance to prevent data loss from happening, or be able to identify the responsible users.

If you are looking to solve for Regulatory or Compliance needs, such as PCI-DSS, HIPAA, GDPR and more, Endpoint Protector has inbuilt discovery patterns to locate this information and provide response strategies. Alternatively, if the focus is on detecting and protecting Intellectual Property (IP), Patent information, or Client Lists, Endpoint Protector can help there as well.

Endpoint Protector, through its Device Control, Content Aware Protection, eDiscovery, and Enforced Encryption modules, helps companies stop data leakage threats through both internet connections and external storage devices. It not only controls all device activity at the endpoints, but monitors and scans all possible exit points for sensitive content. 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, and encryption can be forced on all content being moved to external USB devices (if permitted). All of this is achieved through Endpoint Protector's single web-based interface.

The following sections will cover the basic deployment, set-up, and configuration actions required to begin protecting your endpoints using Endpoint Protector.

1. Staging the Endpoint Protector Server

To start using Endpoint Protector, a server instance needs to be made available. The server is where all endpoint controls and behavior will be configured, and is the vehicle for delivering the Endpoint Protector agent to endpoint systems.

There are two principal options for server management; Customer-Managed or Provider-Managed.

If Customer-Managed is a desired option, the server can be installed On-Premise or in a Hosted-Cloud Environment.

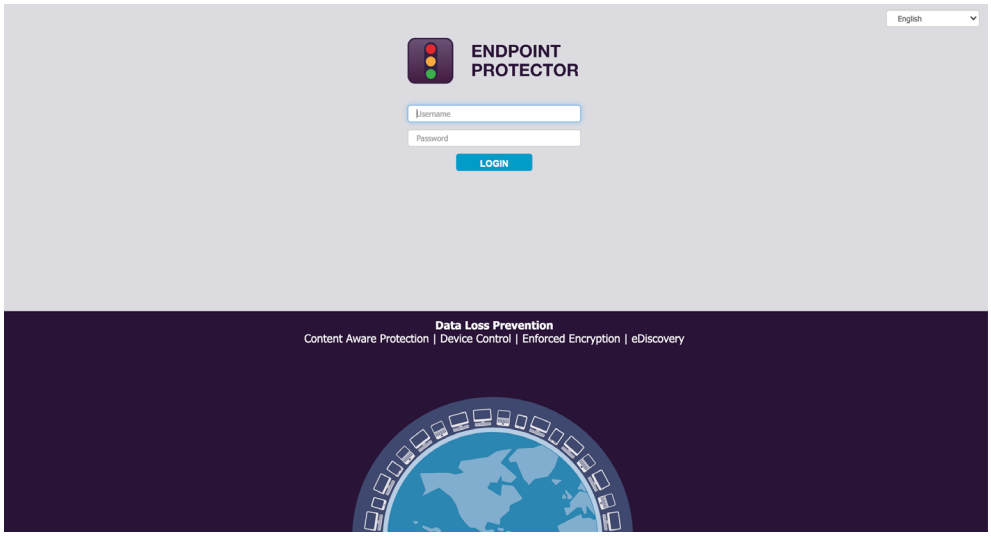
The On-Premise option for a Customer-Managed instance allows for a virtualized image to be set up in a customer's LAN setting. Virtualization options include, but are not limited to: VMware and Hyper-V. The Hosted-Cloud method of deployment allows for use of a customer's Amazon Web Services (AWS), Azure, or Google Cloud Platform (GCP) instance. To obtain more specific information for each of these options, please refer to the resources section on our website: https://www.endpointprotector.com/resources. Here you will find the manuals for 'Virtual and Hardware Appliance Deployment' and 'Cloud Services Deployment'.

Alternatively, if a Provider-Managed setup is required, an instance of Endpoint Protector can be spun up in an isolated cloud environment. To obtain more details on the Provider-Managed option, speak with your CoSoSys Account Manager.

Please note, in order to use the Endpoint Protector Server in a production environment, a License Key is required. After purchasing Endpoint Protector with the necessary module(s), your Account Manager will assign a License that can be installed within the Endpoint Protector Management Console (the configuration interface available on the Endpoint Protector Server). Details on how to access and configure this Management Console can also be found within the manual(s) referenced above.

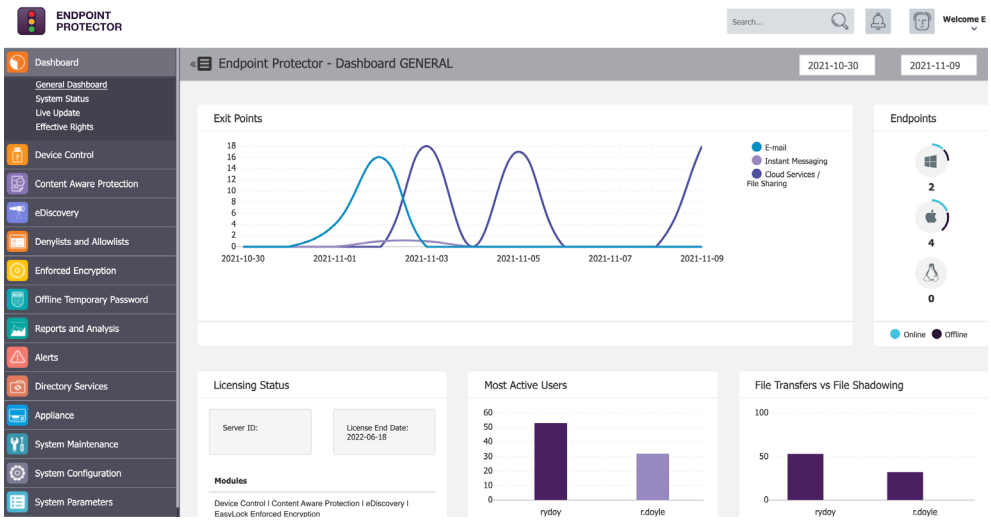
2. Logging in to the Endpoint Protector Server

Once the Endpoint Protector Server has been provisioned, configuration of the feature modules can be performed. To manage policies in preparation for agent deployment, it is necessary to login to the web user interface that was configured during server setup. Generally, this may be a static IP configuration or a namespace. After inputting the address of the Endpoint Protector Server in the address bar, you will be prompted for a user login. Input your assigned username and password if already configured; otherwise, use the default (root, epp2011) if this is a first-time login.



Upon successful login, the **Dashboard > General Dashboard** window will be displayed (see below image). This window is intended to provide a high-level overview of endpoints under management as well as activity, licensing status, and modules licensed.

Your available modules are displayed in the left-side navigation pane. These can be selected to further manage module-specific policies. Ultimately, policies define the actions allowed / disallowed on the endpoint.



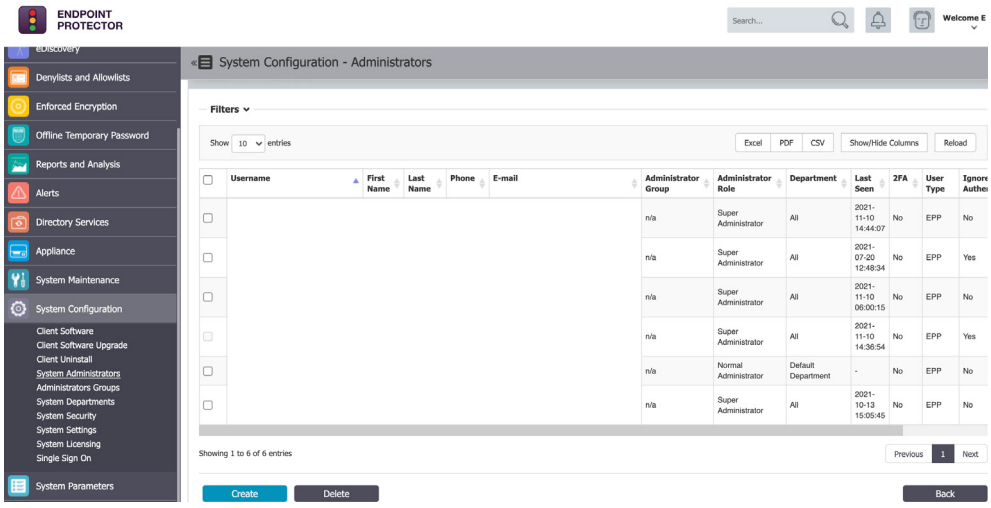
Before deploying any agents, each module's policy should be reviewed. If agents have already been delivered to systems, a review of the configuration(s) can be accomplished by verifying active policy mappings. To clarify, once a policy is built or edited, it would be 'mapped' to a defined target or group of targets. This will be discussed later in the sections for each module.

3. Managing Administrators

Administrators have an important role to play. Not only are they responsible for ensuring Endpoint Protector is kept up to date with the latest releases, but they also play a critical role in deploying and maintaining the DLP policies that will keep your organization safe. That's why, when choosing your Administrators, it's important that they have a complete understanding of how device and content controls should function based on your organizational needs. In this section we will cover the steps required to add Administrators in Endpoint Protector, and how to manage their permissions.

Note - If you have not yet modified the default administrator login, it is recommended that you do so before adding additional Administrators.

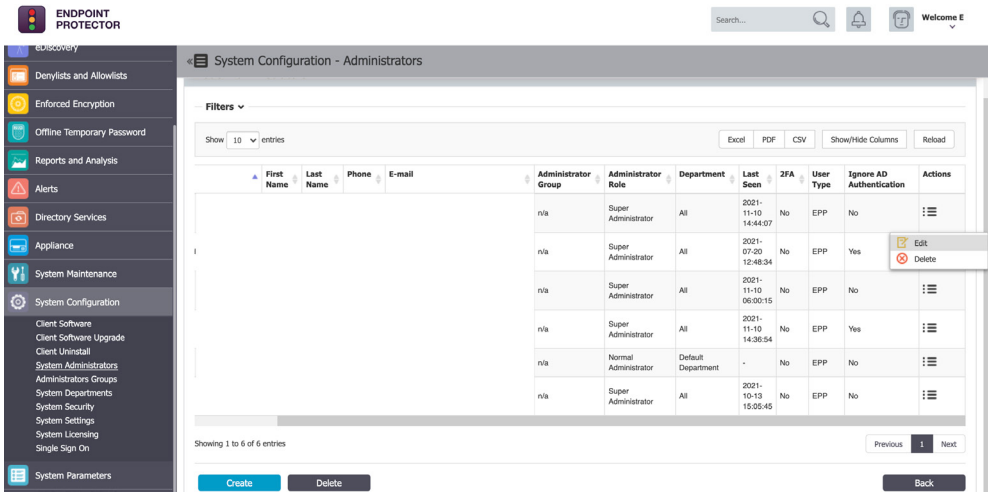
Login and navigate to the System Configuration section of the Endpoint Protector Management console. Next, select 'System Administrators'.



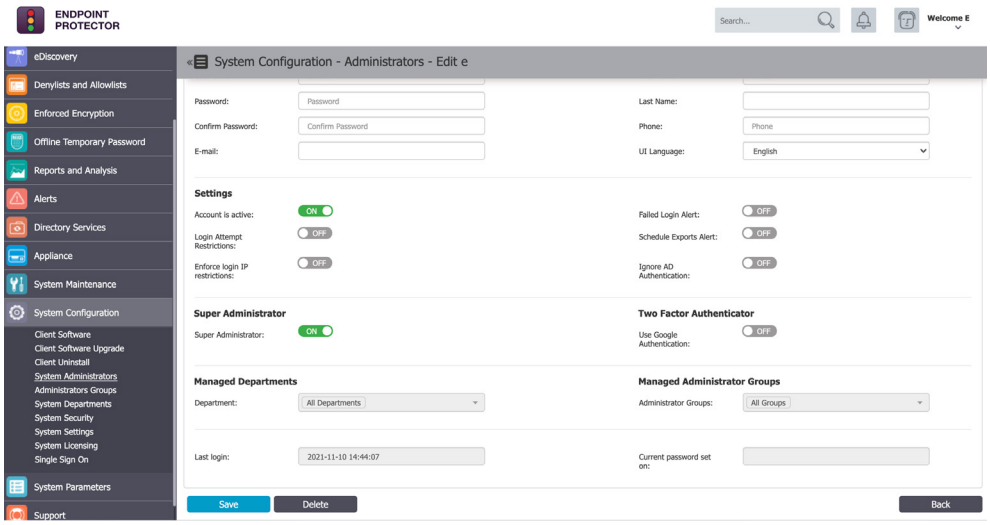
Now, you can begin adding Administrators by using the 'Create' button. If administrative limitations need to exist within the Management Console, when creating the account be sure to define the appropriate 'Administrator Groups'. In general, multiple Administrator Groups can be assigned to an account; unless the 'Read Only' group option is used. To find the group list, locate 'Administrators Groups' under the 'System Configuration' section.

3.1. Editing System Administrators

Editing Administrators is managed through the 'System Administrators' section of the Management Console. To edit an existing account, click the icon in the "Actions" column against the account you want to edit. Select "Edit".



Afterwards, you will see a separate page which allows for any modifications needed; the page will display as seen in the image below. If it is intended for the account to have the highest level of authority within the Management Console, toggle the 'Super Administrator' slider to ON. Once all changes have been made, scroll down and select the 'Save' button. If no changes are intended, use the 'Back' button or simply navigate to another section of the Management Console - either of these actions will behave as a cancel and no changes will be made to the existing account.



4. Configuring Device Control

While it is imperative an agent be deployed to endpoints in order for Endpoint Protector to function, knowledge of how the agents will behave in a given environment is equally important. That is why we typically start by reviewing a Device Control policy, since device control is the heart of the agent and the Endpoint Protector experience.

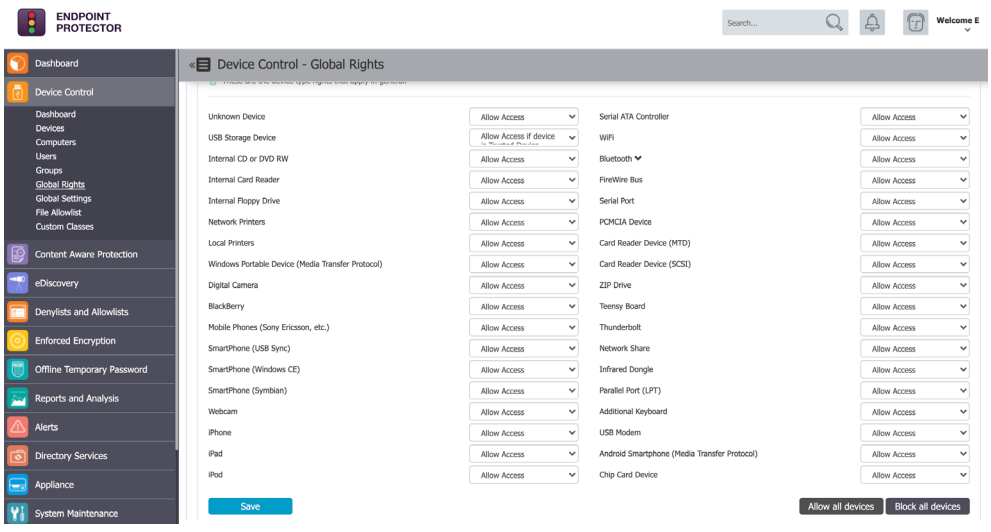
Device Control gives an Administrator the ability to Allow or Deny access to specific peripheral devices. Additionally, this feature set provides functionality around control of unique instances of a given device. This means if an Administrator wants to provide access to a specific brand of USB storage devices, they can do just that. Please note, there are a few inherent functions that provide this support; one being the 'Device Wizard' found under 'Custom Classes'. This will be covered in a later section.

You should consider 'Global Rights' to be the highest tier for the assignment of configurations. Below Global Rights, the next entity is Groups, then Computers and/or Users, and then Computers. There is an option under System Configuration > System Settings that allows an Administrator to define if computer rights, user rights, or both is to be used.

Generally, the way to understand overall prioritization is to consider that the lowest tier will always take precedence. In this example, consider that you have configured a 'Deny Access' restriction at a computer level for **SystemA**. In the event that you modify your Global Rights (policy) to Allow Access to everything, all systems other than **SystemA** will have no denied access (assuming no other restrictions have been made elsewhere).

4.1 Setting up an "Allow All" Device Control Policy

In a strategy to achieve minimum user disruptions in the initial deployment of Endpoint Protector, a first best practice is to modify the 'Global Rights' configuration so that everything is given 'Allow Access'. Later, if Device Control is intended to be used for denied access, Global Rights or Groups is the best place to create restrictions to keep administrative efficiency in place.



5. Configuring Content Aware Protection

To best understand Content Aware Protection (CAP), consider this module similar in behavior to an Antivirus' Active Scan feature. CAP is looking at active files to determine the properties of those files. Files are made 'active' in a system when they are in use and more specifically, when an attempt is made to transmit them beyond the user's endpoint.

Data exfiltration prevention is a key component of any good DLP solution, and as such the detection or classification that occurs through data property determination is what makes this module essential. By using the 'Predefined Policy' option, you can focus attention on specific file types or specific regulatory items (such as HIPAA, PII, PCI-DSS, etc.). Depending on the Operating System type(s) in a given environment, policies can be built for each of your Windows, macOS, and/or Linux systems. If there is a need to look at specific items such as list files, 'Custom Content' can be entered or imported within the 'Denylists and Allowlists' node of the Management Console. Once the 'Custom Content' is added, this can be linked to the policy under the 'Custom Content' tab within the relevant entry.

After a policy is created, it needs to be assigned to a target. The target can be either Departments, Groups, Computers and/or Users. To see the assigned targets of a Content Aware Protection policy, select the policy within the Content Aware Policies section of the Management Console, then scroll to the bottom of the page. Should there be a need to make an edit in an assignment, be sure to click the 'Save' button found just below the section for defining the target of the policy.

5.1. Setting up a "Report only" Content Aware Protection Policy

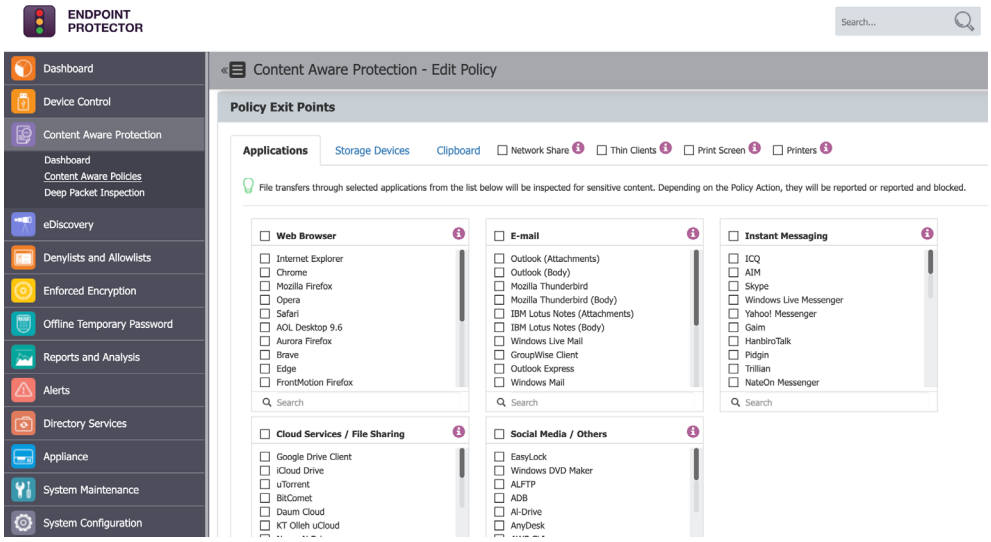
To complement the "Allow All" Device Control Policy, it is recommended that you next create a "Report only" Content Aware Protection Policy. This is your first step in understanding the movement of files across your endpoints.

Create a "Report only" CAP policy by navigating to **Content Aware Protection** > 'Content Aware Policies' within the Endpoint Protector Management Console. Click the 'Create Custom Policy' button, define the OS Type, provide a Policy Name (it is suggested to include "Reporting" or "Report only" within the Name or Description), and be sure to select **Report only** for the 'Policy Action:' field. Scroll to the bottom of this page and choose the **Save** button - this action will return you to the Policies viewing window. If you are managing more than one Operating System type in the environment, follow this same procedure to create the Policy framework(s) for the other platform(s).

After your **Report only** policy framework(s) has been established, select your first policy within the window and choose the icon for edit. This 'Edit' icon can be found on the right-hand side of the policy (look for the pen and paper icon). This will bring you back to the 'Edit Policy' page where you will select the Exit Points of focus, and the items which you may later deliver blocking restrictions against.

Although the terminology used in this policy is 'Denylists', by setting the policy to Report only you are implementing no restrictions. In a later section, you will be guided through creating locking actions for your policies so that automatic remediation occurs. Additionally, since the CAP feature module focuses on in-motion objects solely, it consumes minimal endpoint resources. With this said, it is best to set within the policy only the variables which are found in a given environment where agents are to be installed. This will ensure no unnecessary processing takes place at the point of detection.

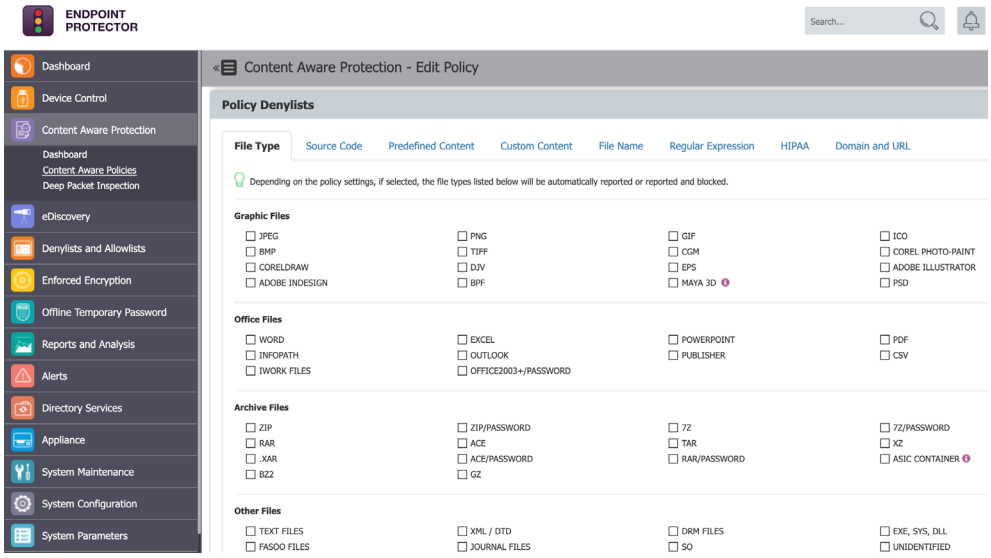
Most commonly, the **Applications** tab under 'Exit Points' is used for common email clients and/or web browsers in a given environment. Alongside this, the **Storage Devices** tab can be used if you intend to later restrict the transfer of sensitive files to storage media.



The Denylists section provides methods for determining which objects to focus classification and determination on. If it is desired to audit activity around given files, the 'File Type' tab will provide several options for common files types in systems. If the focus is more regulatory-bound, using the 'Predefined Content' tab may be more appropriate.

If true customization is required the 'Custom Content' tab allows for mapping of items such as list file entries, or the Regular Expression tab allows for the use of logical operators.

A best practice with regards to your Denylists selection may include Credit Card Numbers (CCN), Social Security Numbers (SSN), or even Personal Identifiable Information (PII). Sample entries or files can be found at the site:
DLPTest.com (https://dlptest.endpointprotector.com), under the Sample Data section.



At this point, you are able to scroll to the bottom of the Policy edit page and choose to **Save** again - do this for each "Report only" policy created. Once you have progressed through the section for Deploying Agents (Section 8), you will return to the policies created here and select the target Client Systems that will utilize these policies.

6. Configuring an eDiscovery Scan

Supporting the Content Aware Protection (CAP) feature module, eDiscovery provides greater insight into the information found (at-rest) within a given environment. To reuse a reference made earlier, think of eDiscovery much like an Antivirus scan. The difference being that eDiscovery provides for passive scanning rather than active scanning. Just like a 'Full Scan' with an Antivirus, passive scanning looks for data at rest and allows those objects to be classified according to content. Therefore, eDiscovery provides a broader view of the data residing on user endpoints that an organization is responsible for, and that may breach compliance requirements.

It is imperative that an organization knows where its most critical data rests so that it can be well governed and protected. By understanding where this sensitive data is, better permissioning can take place and tighter boundaries may be established. Ultimately, allowing for more responsible management from a cybersecurity perspective.

Even though configuring eDiscovery scans is similar to making a new Content Aware Protection Policy (discussed earlier), there are a few distinctions to consider. Firstly, since eDiscovery is broader in terms of how it scans, and it naturally consumes more processing resources on the endpoint. Therefore, despite Endpoint Protector offering the industry's most light-weight and efficient agent, it is recommended to run scans outside of prime working hours.

Secondly, a policy with more scan variables configured will have greater intensity when scanning takes place. As a best practice, restrict scans to defined data types. If you want to scan for multiple data types, consider creating seperate policies and run scans in staggered intervals.

Finally, in an effort to appear consistent with Content Aware Protection policies, the terminology and variables used by eDiscovery are very similar. Although Denylists and Allowlists are the terms used, consider the 'Denylists' section to be an area for items of focus where the 'Allowlists' section is intended to solve for items which are not concerning. This will have later relevance when we discuss remediation options for results of an eDiscovery scan(s).

6.1. Creating and triggering an eDiscovery scan

Begin by navigating to **eDiscovery** > 'Policies and Scans'. Click the Create Custom Policy button, choose the OS Type of focus, provide a Policy Name, select items of focus, then scroll to the bottom and click the Save button. Later, after deployment of the Endpoint Protector Agents, you will return to this Policy section and choose your scan targets within the Policy.

Additionally, once Agents have been deployed there will be a section under 'Policies and Scans' for defined scans. 'Manual Scanning' or 'Automatic Scanning' may be defined by selecting the defined scan, and if Automatic Scanning is chosen a window will appear to configure interval details. A scan can either be run as a 'clean scan' or 'incremental scan. Generally you would run an incremental scan following an initial full assessment (clean scan). When scan results complete, you can choose the 'Action' to 'Inspect found items' or simply navigate to the 'Scan Results and Actions' section within the eDiscovery expansion tree on the left of the Management Console. In section 10 we will discuss the review of scan results and remediation options.

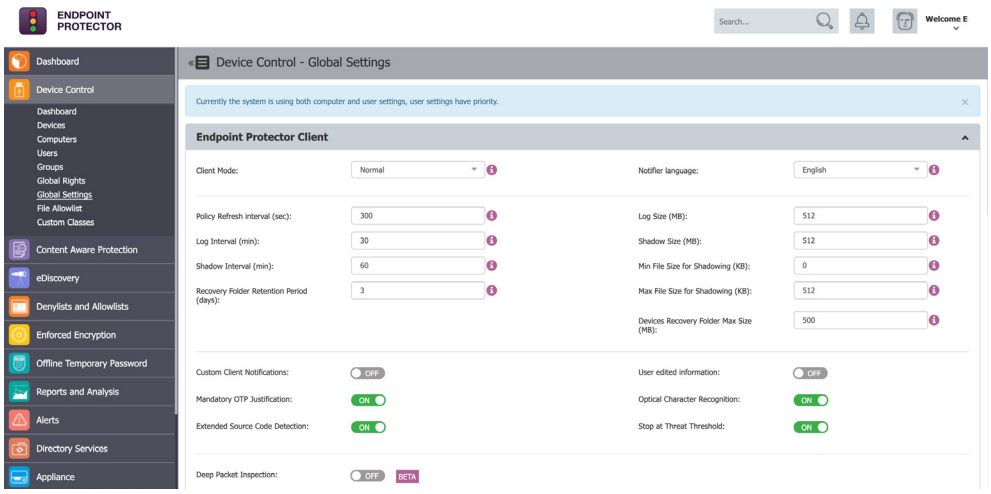
7. Configuring the User Experience

Many organizations have unique requirements and may need to have varied end user experiences based on the role or function of an employee within the organization. With this in mind, Endpoint Protector allows for customization of the Endpoint Protector Client to accommodate these unique needs. In this section we will discuss the Client Settings available and review how to implement these settings at specific tier levels within the Endpoint Protector Management Console.

7.1. Client Settings

There are several settings which relate directly to the Endpoint Protector Client. These settings establish the client's behavior, and can be configured for specific entity mapping. Specific entity mappings include: Global, Groups, Computers, and Users.

Client Settings are located and configured within the Device Control section of the Endpoint Protector Management Console. Within Device Control you will see a section specifically for 'Global Settings'. If settings are intended to be configured at a lower tier level, there are 'Actions' available which allow for the 'Manage Settings' functionality. Precedence levels of these settings function much like Device Control rights, which was described earlier in the Device Control section of this guide.



7.1.1. Client Modes

The Endpoint Protector Client offers several modes that define its behavior on an end user's system. There are six modes to choose from, and they can be changed at any given time. Below is a quick summary of each mode available for configuration by an Endpoint Protector Administrator.

Normal

The default deployment mode for the Endpoint Protector Agent. We recommend that you do not change from Normal mode to another mode without being fully aware of what the other modes imply. If the Normal mode behavior does not suit your needs, Hidden or Silent modes are usually the best alternatives to consider.

Panic

This mode can be utilized under extreme situations, such as when a user has malicious intent or rogue activity is detected. With these special circumstances the Administrator may toggle to this configuration in order to block all devices. It is recommended to exercise extreme caution if using this mode.

- System tray icon is displayed
- System tray notifications are shown
- Everything is blocked, regardless if authorized or not
- File shadowing and file tracing are enabled to see and monitor all user activity
- Administrator receives alerts when computers go in and out of Panic Mode

Transparent

This mode is useful to block all devices, but users remain unaware of any restrictions or presence of the Endpoint Protector Client and its activity.

- No system tray icon is displayed
- No system tray notifications are shown
- Everything is blocked, regardless if authorized or not
- Administrator receives alerts for all activities

Hidden Icon

This mode is very similar to the Normal mode option. The difference is that the Endpoint Protector Client is not visible to the user.

- No system tray icon is displayed
- No system tray notifications are shown
- All configured rights and settings are applied as per their configuration

Stealth

This mode is useful to monitor all users and computers, but users remain unaware of any restrictions or presence of the Endpoint Protector Client and its activity. Since everything is configured to allow, there will be no disruptions in the day-to-day activities of the users.

- No system tray icon is displayed
- No system tray notifications are shown
- Everything is allowed, regardless if authorized or not
- File shadowing and file tracing are enabled to see and monitor all user activity
- Administrator receives alerts for all activities

Silent

This mode is very similar to the Normal mode option. The difference is that the pop-up notifications are not visible to the user.

- System tray icon is displayed
- No system tray notifications are shown
- All configured rights and settings are applied as per their configuration

7.1.2. Client Modes

Notifier Language

The Endpoint Protector Client Notifier language.

Policy Refresh Interval (sec)

The time interval at which the Endpoint Protector Client checks in with the Endpoint Protector Server and updates with the latest settings, rights, and policies.

Notifications Pop-up

The Administrator has the option to select between traditional (system tray) and pop-up notifications. This setting relates directly to an end user's experience once blocking is set to take place within policy.

7.2. Configuring User Remediation Settings

User Remediation is an optional feature, designed to allow for a bypass when an employee is attempting to transmit sensitive information. Instead of having a block message displayed to that employee (which would require further Administrative intervention), 'User Remediation' gives the ability for specific personnel to transmit information that may be necessary for the role, function or duty. Rather than following an 'ask for permission' model, this feature allows for an 'ask for forgiveness' approach. While this bypass can allow for more timely delivery of content, justification details can be requested which are then transmitted to an Administrator so that further scrutiny and due diligence may take place.

Note - User Remediation is a premium feature. As such, this section is only available if Premium licenses are present on the Endpoint Protector Server.

User Remediation Pop-up

This setting is available when the 'User Remediation' feature is active. The Administrator has the option to enable User Remediation pop-up notifications for the end users.

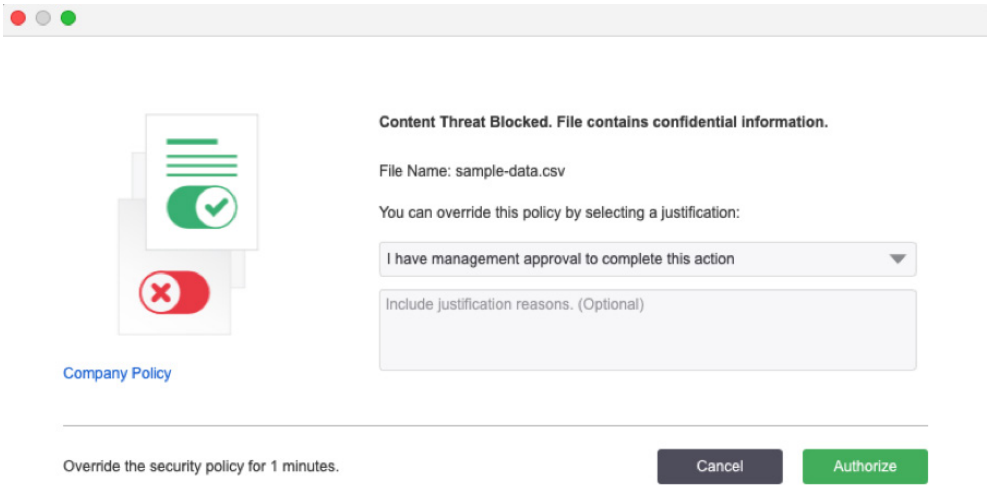
Enforce User Remediation Pop-up

This setting is available only if the 'User Remediation' Pop-up setting is enabled. When this setting is enabled, the end user does not have the ability to disable User Remediation Pop-up notifications.

7.2.1. Configuring User Remediation Settings

Within the Endpoint Protector Management Console, under System Parameters > 'User Remediation', variables for this feature can be seen. Variables found here may include, but are not limited to: Custom Logo, Custom URL, and time interval. One note to consider is that the 'Time Interval' determines how long the window will remain open for the transmission of the individual object (relative to an individual transmit channel). More specifically, if a user attempts to send out a document containing PII information via an email attachment, an authorized action would allow a defined amount of minutes for that item to be sent via email after the action is selected.

See the following image for a sample 'User Remediation' Pop-up message.

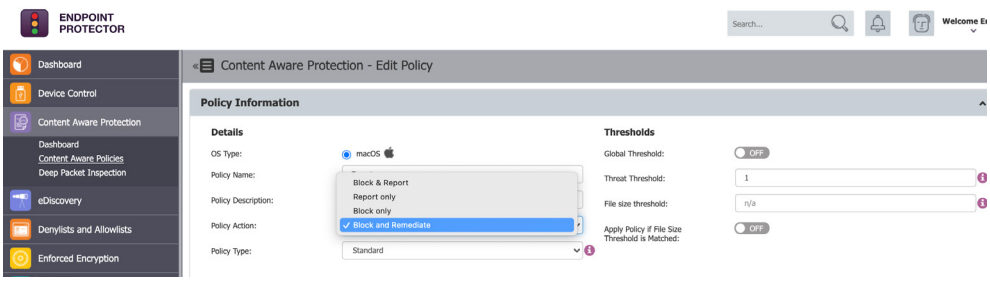


7.2.3. User Remediation Reporting

Logs (or details) of an end user's response to a User Remediation intervention can be found in the Endpoint Protector Management Console under Reports and Analysis > 'Content Aware Report'. If User Remediation has been utilized to authorize a bypass and transmit of sensitive content, the Justification field will provide any user submitted messaging.

7.2.4. Implementing User Remediation

Although it is recommended to turn on User Remediation after configuring a Blocking Policy for Content Aware Protection, we will cover this item here. To turn on User Remediation, navigate to the Content Aware Protection Policy(s) where restriction is intended and choose to edit the 'Policy Action:' field. By selecting 'Block and Remediate', the User Remediation feature will be enabled the next time the endpoint connects to the Endpoint Protector Server.



7.3. Setting up an "Offline Temporary Password"

In environments where the 'User Remediation' feature is not able to be utilized, "Offline Temporary Passwords" offers another means for the bypassing of a policy.

Within the Management Console of Endpoint Protector, this section allows the Administrator to generate Offline Temporary Passwords (or OTPs) and grant temporary access rights to users. 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 (i.e. where User Remediation would be unable to function).

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)

More specific examples supporting Multinational instances or instances with several time-zones can be found within the User Manual defined at the beginning of this guide.

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 in the case of Universal Offline Temporary Passwords). 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.

8. Deploying Endpoint Protector Agents

Congratulations, you are now ready to begin deploying your Endpoint Protector Agents. It is recommended that you deploy agents to your endpoint systems before modifying the policies to perform blocking. This will give a chance to further discover any system variables which may need allowances, as well as give a window for end user feedback.

The Endpoint Protector Client package(s) can be retrieved from the Endpoint Protector Management Console under **System Configuration** > 'Client Software'. Locate the section for either Windows, Mac, or Linux and follow the instructions to "Download" the relative package. The Windows package will offer add-ons, so based on your desired blocking strategy you may want to choose none, one, or several add-ons Once you have downloaded the package, begin deployment through your chosen deployment tool.

Most commonly Active Directory and JAMF are utilized for Agent deployment. Deployment guides are available at https://www.endpointprotector.com/resources. If you intend to deploy with another utility, as long as installation switches for packages are supported, there should be no concerns.

Within a small group deployment, using the Agent packages downloaded from the Management Console and running interactively should be sufficient. When installing in a Mac environment, be sure to provide local disk access after performing the installation. This is done by navigating on the macOS system to: System Preferences > Security & Privacy > Privacy Tab > Full Disk Access > Search for the Endpoint Protector Client and check the application, then save the changes.

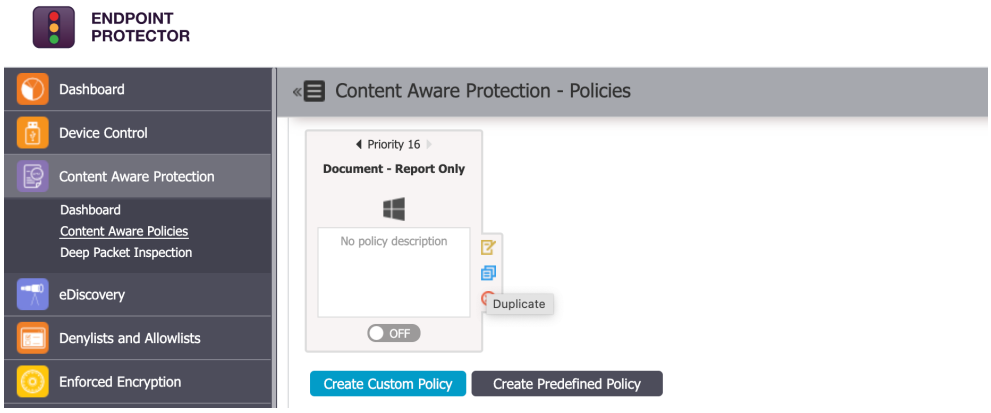
8.1. Assigning target systems to Policy(s)

Once your initial Endpoint Protector Agents have been delivered to systems, be sure to review the policies discussed in section 4.1 and section 5, and map these systems within the policies. This will allow for proper analysis through the Reports built into the Endpoint Protector Management Console so that after activity has occurred, all variables within the environment are fully accounted for.

9. Setting up a "Blocking" Content Aware Protection Policy

The "Blocking" policy will be used to transition from the "Report Only" Content Aware Policy(s) created previously. Once review of the "Content Aware Report" has occurred, following interactive testing to several Client systems in an environment, It is best to create a copy of the "Report only" Policy(s).

To create the "Blocking" Policy(s), a duplication feature is delivered at the Policy Management page. You will find this in the Endpoint Protector Management Console under **Content Aware Protection** > 'Content Aware Policies'. Locate each "Report only" policy and choose the 'Duplicate' icon found on the right-hand side of the policy. It is the second icon seen in the three displayed icons column which appears upon policy selection.



After creating each of the policies intended for Blocking, choose to edit these policies by using the 'Edit' icon found just above the 'Duplicate' icon. Within each policy modify the 'Policy Action:' selection to the desired Blocking method. Keep in mind that "Block and Remediate" requires a Premium License package. Scroll to the bottom of each Policy page and verify all intended Policy Entities are selected, then click the Save button. After review of each new "Blocking" Policy, toggle the "Report only" policies to OFF.

10. Performing Remediation within eDiscovery

As discussed in the latter portion of Section 6, there are remediation options available upon an eDiscovery scan completion. These options are 'Encrypt on target', 'Decrypt on target', 'Delete on target', and can be found under the "Actions" column of **eDiscovery** > 'Scan Results and Actions' within the Endpoint Protector Management Console.

These actions are present to help mitigate potential risks in the event that sensitive data is found on the endpoint. For example, holding customer PII data on user endpoints may breach one or more privacy laws (such as GDPR).

11. Configuring Enforced Encryption

Protecting data in transit is essential to ensure no third party has access to confidential information. When data needs to be saved on USB storage devices, encryption can be the best solution to prepare for when a device is lost, misplaced, or stolen. EasyLock is a cross-platform, enterprise-grade, data encryption solution designed to keep confidential data safe.

There are several EasyLock versions available. Although they are very similar and both offer the same encryption capabilities and ease of use, there are some things to consider when choosing the right version, based on your scenarios.

• **EasyLock** – a stand-alone application that does not require any installation on the computer itself. It protects data on USB storage devices with government-approved 256bit AES CBC-mode encryption.

• **EasyLock Enforced Encryption** – also a stand-alone application, offering the same functionalities for USB storage devices. The difference is that it does require a small installation on the computer itself. The application allows USB storage devices to be identified in TrustedDevices 1+. It can only be used in combination with Endpoint Protector as it provides enforced encryption options for any USB storage device that connects to the protected computer, and remote management of those devices (resetting passwords, sending messages, resetting devices, etc.)

With the intuitive Drag & Drop interface, files can be quickly copied to and from the device for fast, secure and efficient workflow.

For more details on using EasyLock and Enforced Encryption see our User manual found here:
https://www.endpointprotector.com/support/pdf/manual/EasyLock_2_User_Manual.pdf

EndpointProtector.com

COSOSYS

HQ (Romania)

sales@cososys.com
+40 264 593 110 / ext. 103
+40 264 593 113 / ext. 202

Germany

vertrieb@endpointprotector.de
+49 7541 97826730
+49 7541 97826734 / ext. 202

North America

sales.us@endpointprotector.com
+1 888 271 9349
+1 877 377 6475