ENDPOINT PROTECTOR | by CoSoSys
NOW PART OF netwrix

Endpoint Protector

User Manual

Version: 5.9.3.0

Date: 29 February 2024

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**.

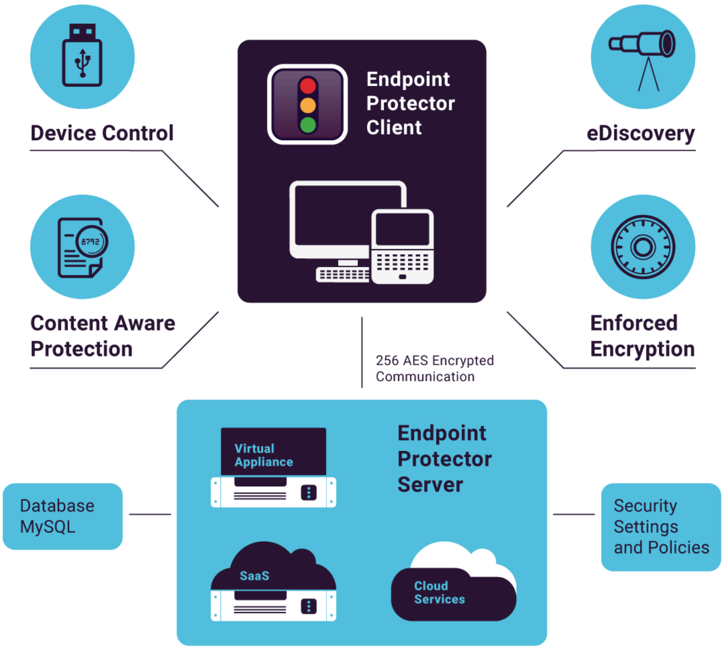
3.1. Main components

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

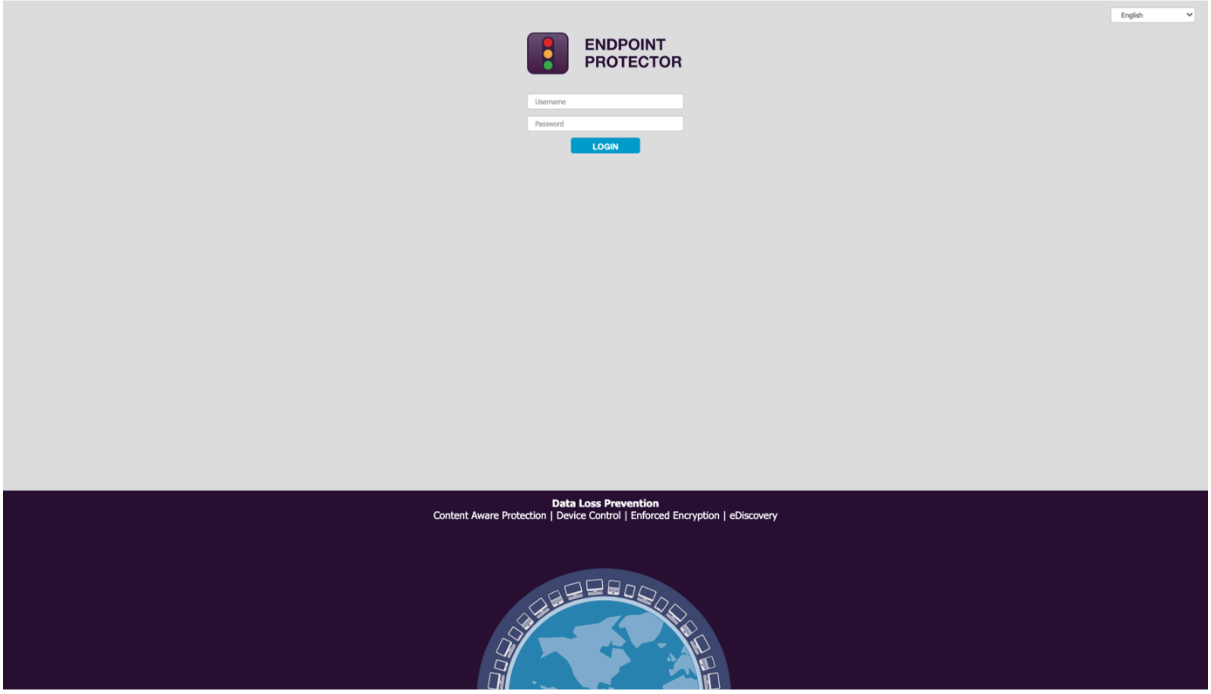
Once the Endpoint Protector Hardware or Virtual Appliance setup is complete, access the User Interface from the assigned IP address.

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**


English
ENDPOINT PROTECTOR
Username
Password
LOGIN
Data Loss Prevention
Content Aware Protection | Device Control | Enforced Encryption | eDiscovery

4.1. Endpoint Protector Configuration Wizard

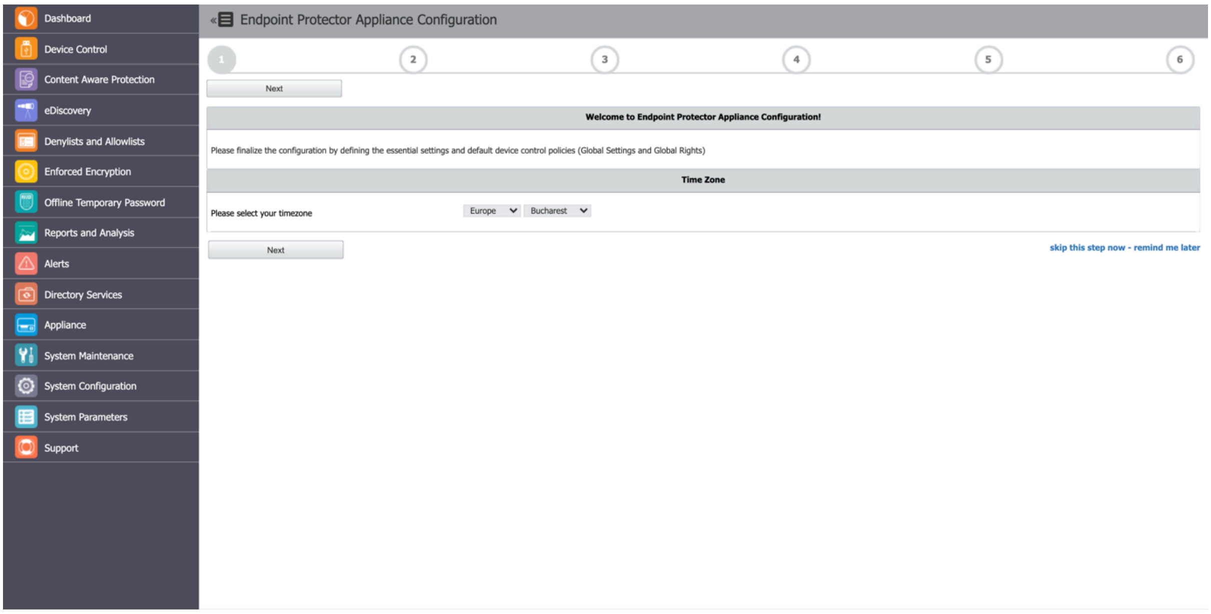
The Configuration Wizard provides you with several steps to define basic settings. These include setting up the Server Time Zone, importing Licenses, Server Update or uploading

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.



Welcome to Endpoint Protector Appliance Configuration!

Please finalize the configuration by defining the essential settings and default device control policies (Global Settings and Global Rights)

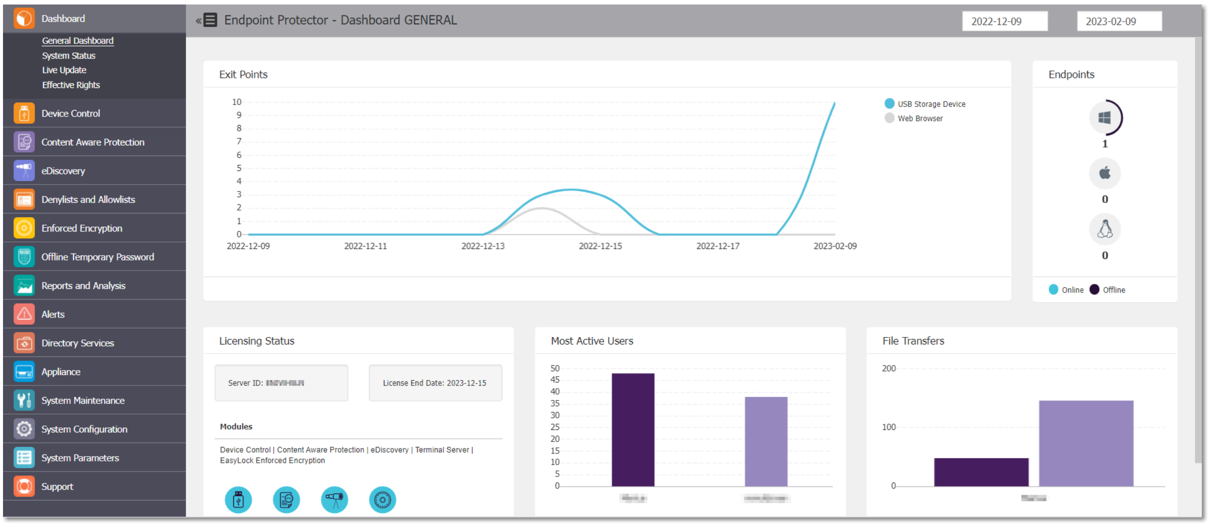
Time Zone

Please select your timezone: Europe, Bucharest

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.



Server ID: [redacted]

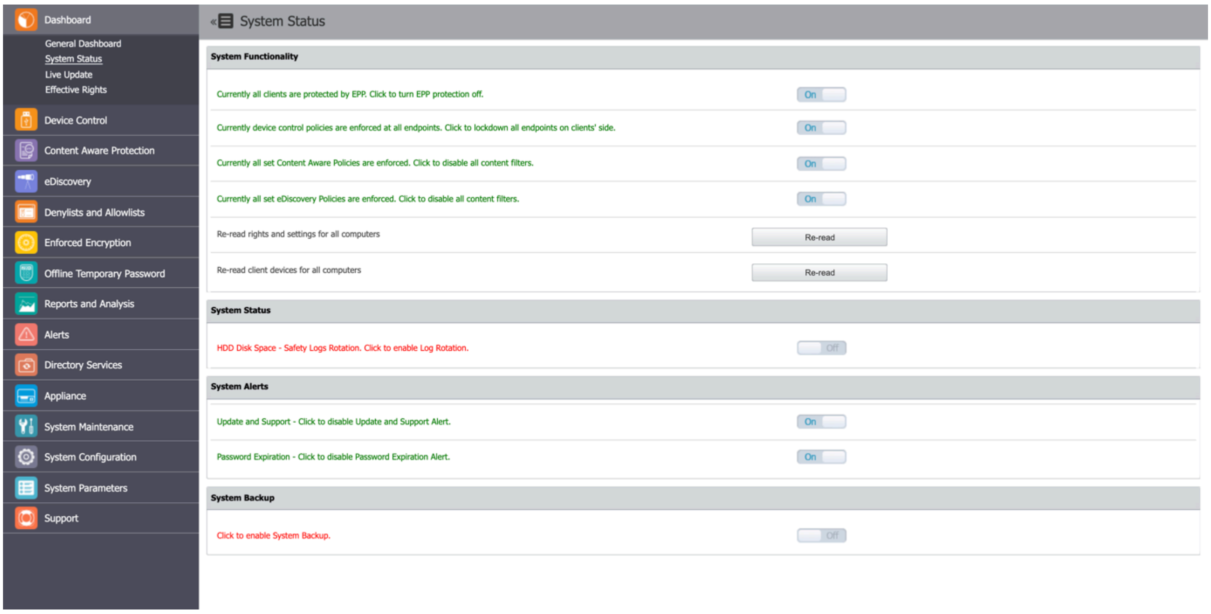
License End Date: 2023-12-15

Modules

Device Control | Content Aware Protection | eDiscovery | Terminal Server | EasyLock Enforced Encryption

4.3. System Status

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



System Functionality

Currently all clients are protected by EPP. Click to turn EPP protection off. On

Currently device control policies are enforced at all endpoints. Click to lockdown all endpoints on clients' side. On

Currently all set Content Aware Policies are enforced. Click to disable all content filters. On

Currently all set eDiscovery Policies are enforced. Click to disable all content filters. On

Re-read rights and settings for all computers Re-read

Re-read client devices for all computers Re-read

System Status

HDD Disk Space - Safety Logs Rotation. Click to enable Log Rotation. Off

System Alerts

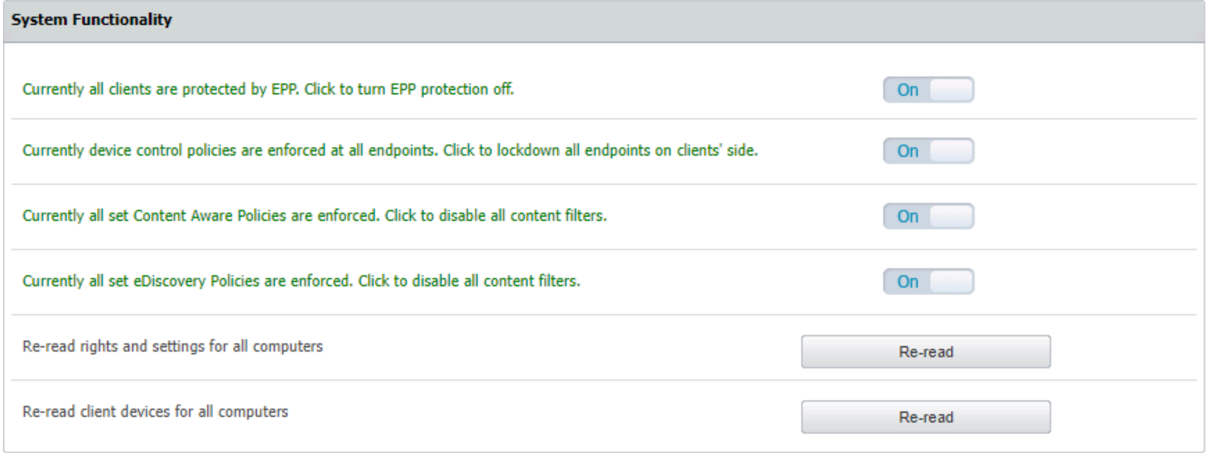
Update and Support - Click to disable Update and Support Alert. On

Password Expiration - Click to disable Password Expiration Alert. On

System Backup

Click to enable System Backup. Off

From the **System Functionality** section, you can enable Endpoint Protector, as well as just specific modules (Device Control, Content Aware Protection, or eDiscovery).



System Functionality

Currently all clients are protected by EPP. Click to turn EPP protection off. On

Currently device control policies are enforced at all endpoints. Click to lockdown all endpoints on clients' side. On

Currently all set Content Aware Policies are enforced. Click to disable all content filters. On

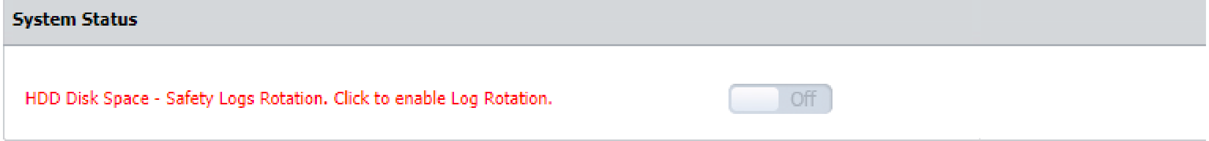
Currently all set eDiscovery Policies are enforced. Click to disable all content filters. On

Re-read rights and settings for all computers — Re-read

Re-read client devices for all computers — Re-read

From the **System Status** subsection, you can enable the **HDD Disk Space and Log Rotation**.

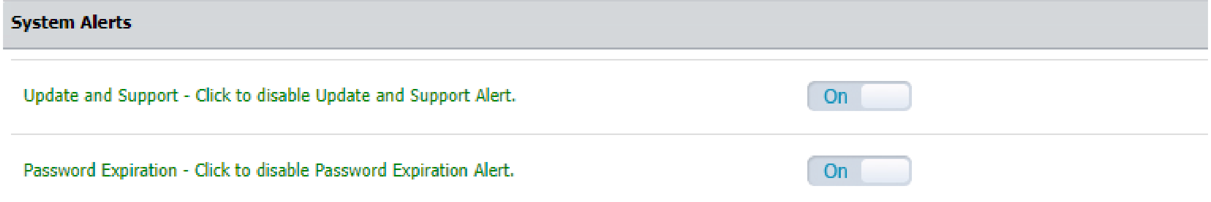
Note: If this setting is enabled, when the Server's disk space reaches a certain percentage (starting from 50% up to 90%), old logs will be automatically overwritten by the new ones.



System Status

HDD Disk Space - Safety Logs Rotation. Click to enable Log Rotation. Off

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

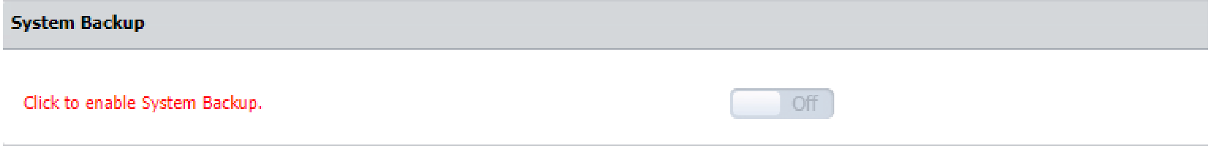


System Alerts

Update and Support - Click to disable Update and Support Alert. On

Password Expiration - Click to disable Password Expiration Alert. On

From the **System Backup** subsection, you can enable the **System Backup**.



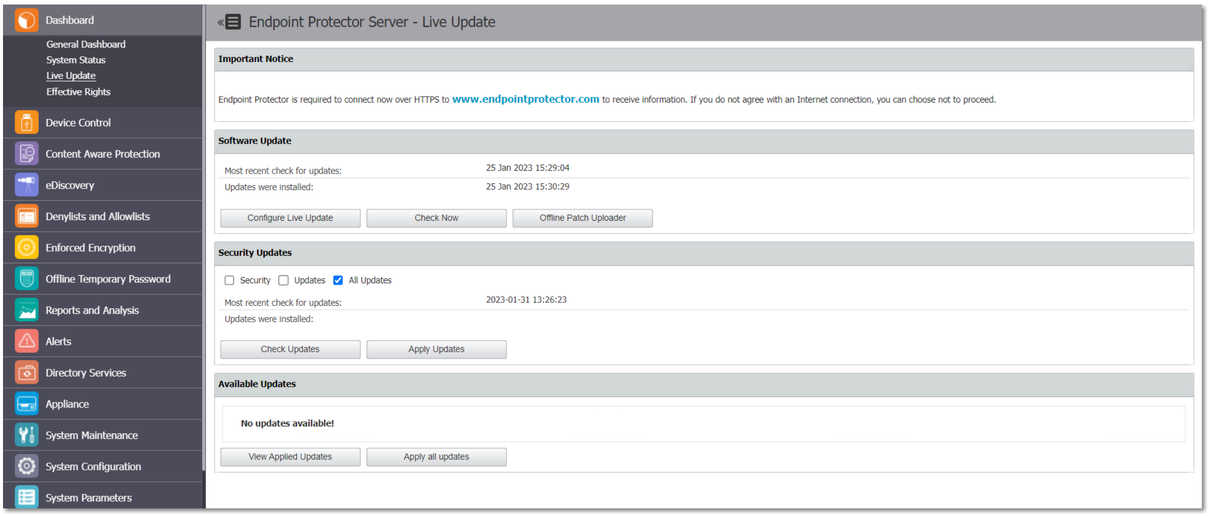
System Backup

Click to enable System Backup. Off

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.



Endpoint Protector Server - Live Update

Important Notice

Endpoint Protector is required to connect now over HTTPS to **www.endpointprotector.com** to receive information. If you do not agree with an Internet connection, you can choose not to proceed.

Software Update

Most recent check for updates:	25 Jan 2023 15:29:04
Updates were installed:	25 Jan 2023 15:30:29

Configure Live Update | Check Now | Offline Patch Uploader

Security Updates

□ Security □ Updates ☑ All Updates

Most recent check for updates:	2023-01-31 13:26:23
Updates were installed:	

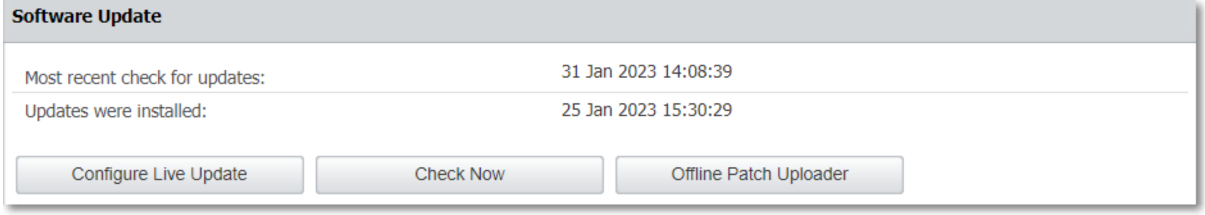
Check Updates | Apply Updates

Available Updates

No updates available!

View Applied Updates | Apply all updates

4.4.1. Software Update

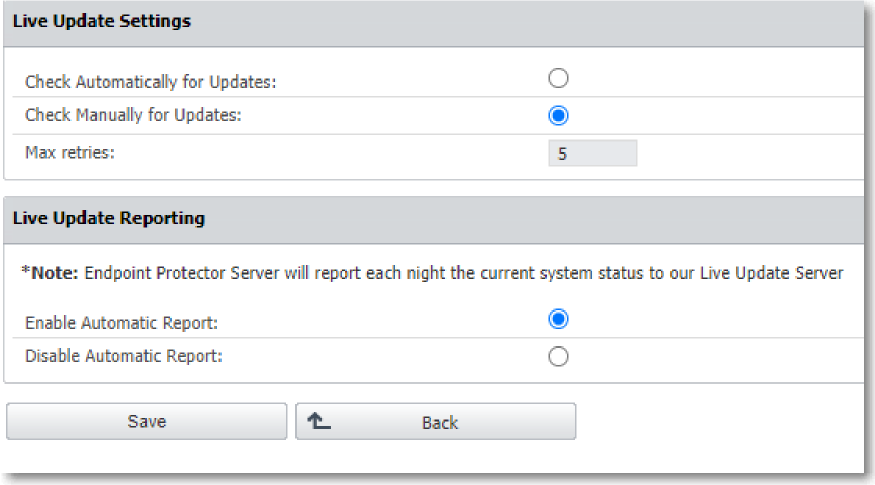


Software Update

Most recent check for updates:	31 Jan 2023 14:08:39
Updates were installed:	25 Jan 2023 15:30:29

Configure Live Update | Check Now | Offline Patch Uploader

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.



Live Update Settings

Check Automatically for Updates:	○
Check Manually for Updates:	●
Max retries:	5

Live Update Reporting

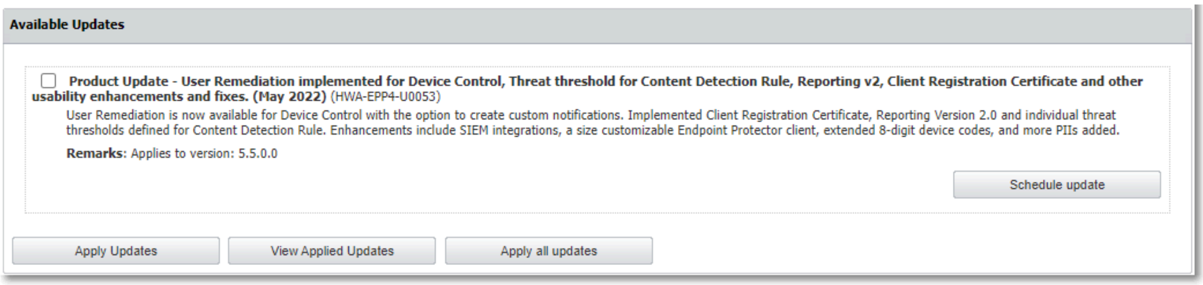
***Note:** Endpoint Protector Server will report each night the current system status to our Live Update Server

Enable Automatic Report:	●
Disable Automatic Report:	○

Save | Back

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.



Available Updates

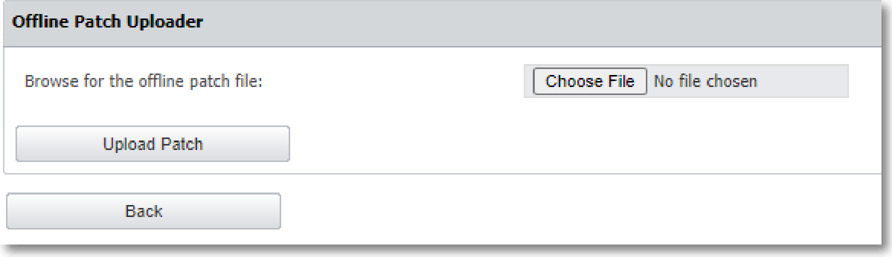
□ **Product Update - User Remediation implemented for Device Control, Threat threshold for Content Detection Rule, Reporting v2, Client Registration Certificate and other usability enhancements and fixes. (May 2022)** (HWA-EPP4-U0053)

User Remediation is now available for Device Control with the option to create custom notifications. Implemented Client Registration Certificate, Reporting Version 2.0 and individual threat thresholds defined for Content Detection Rule. Enhancements include SIEM integrations, a size customizable Endpoint Protector client, extended 8-digit device codes, and more PIIs added.

Remarks: Applies to version: 5.5.0.0

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**.



Offline Patch Uploader

Browse for the offline patch file: No file chosen

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.

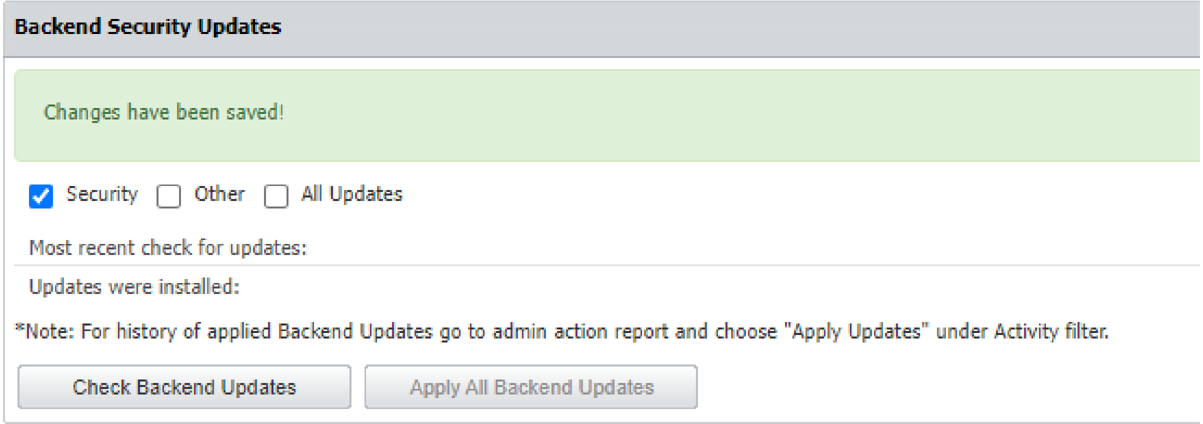
To ensure the updates will not harm the system, follow these actions:

- 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

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

Changes have been saved!

☑ Security □ Other □ All Updates

Most recent check for updates:

Updates were installed:

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

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.

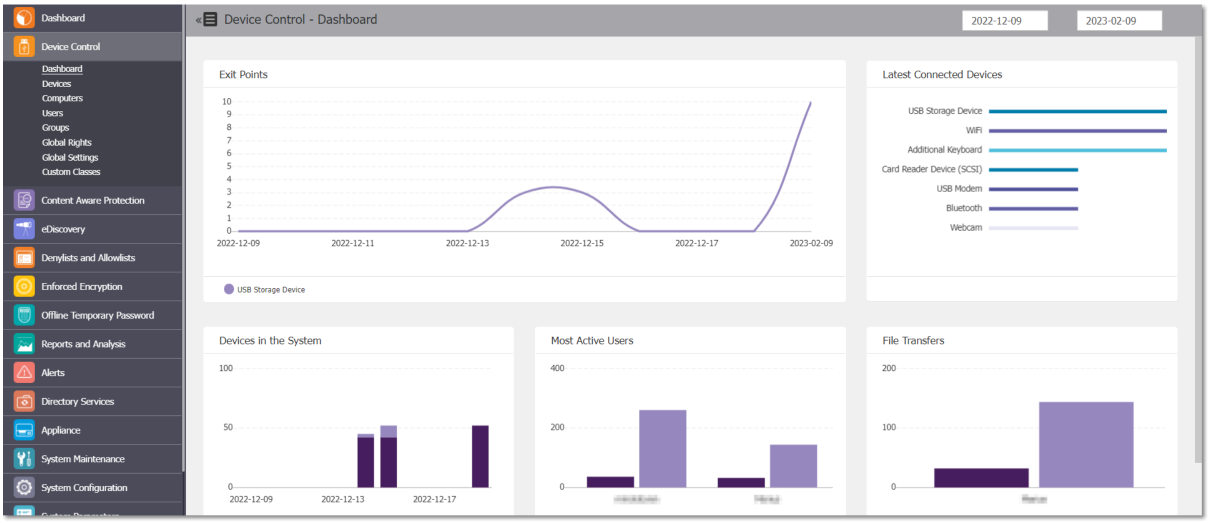
Once the report is generated, from the **Actions** column, you can download or delete it.

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

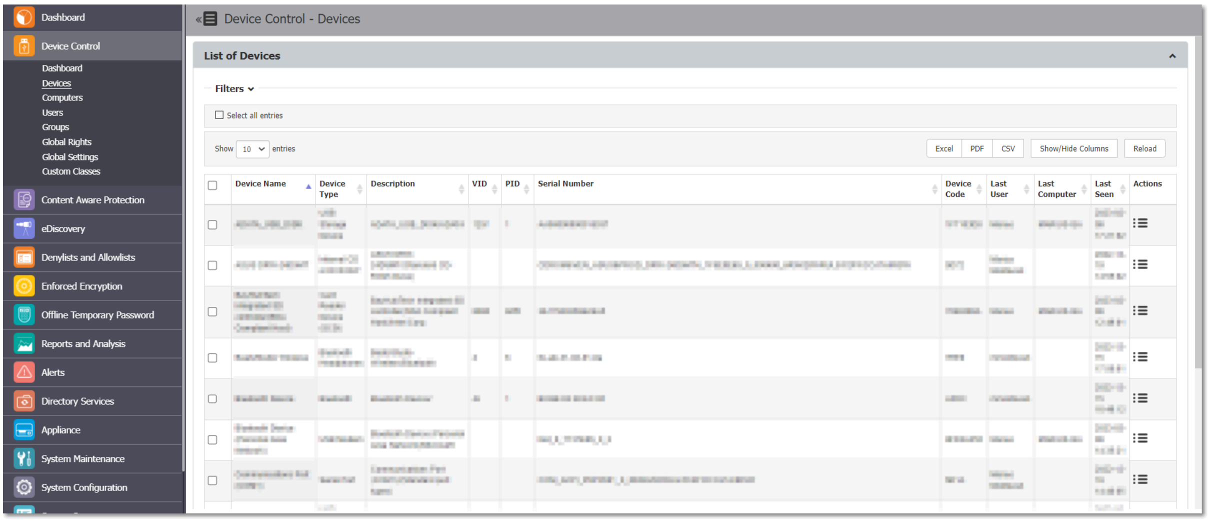
From this section, you can view, sort, and export in Excel, PDF or CSV format any devices from the system. Use the **Actions** column to edit, manage rights, view device history and delete a specific device.

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.

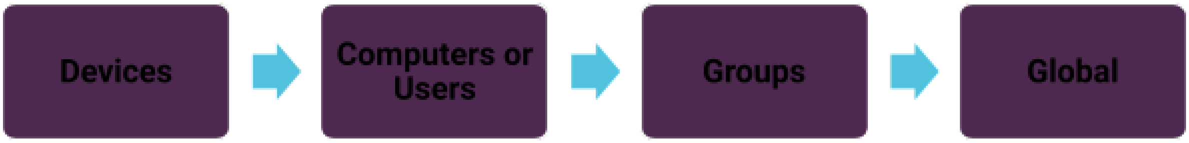
Note: For detailed information on Active Directory, refer to the **Directory Services** chapter.

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.

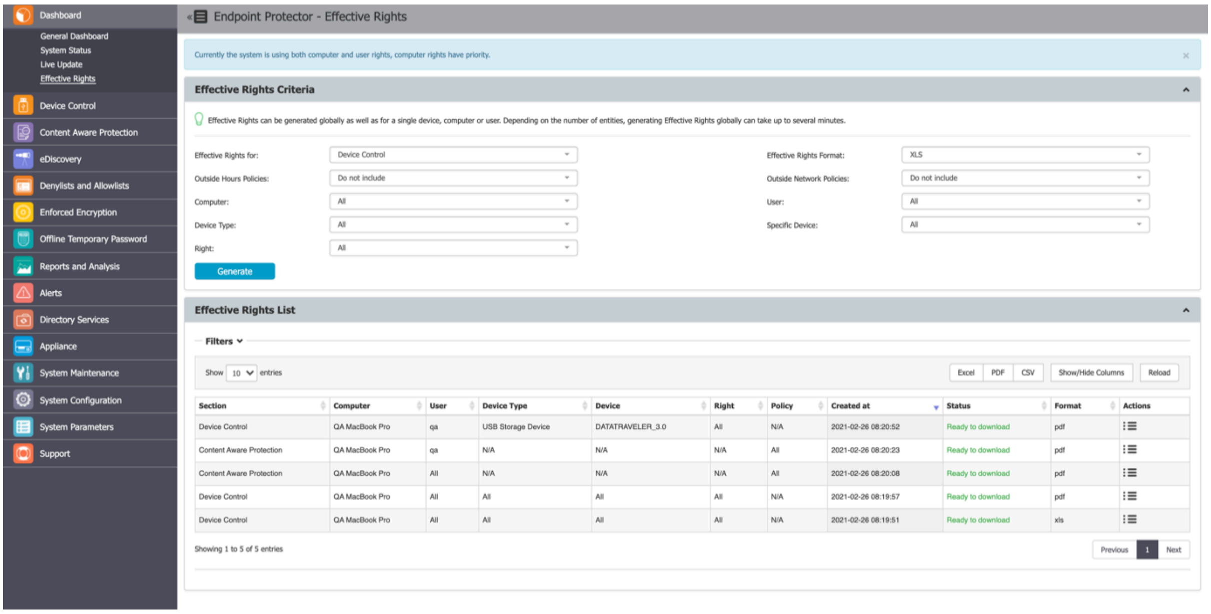
If you configure device rights granularly for all entities, the priority order will be the following, starting with the highest:



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.



Endpoint Protector - Effective Rights

Currently the system is using both computer and user rights, computer rights have priority.

Effective Rights Criteria

Effective Rights can be generated globally as well as for a single device, computer or user. Depending on the number of entities, generating Effective Rights globally can take up to several minutes.

Effective Rights for: Device Control

Outside Hours Policies: Do not include

Computer: All

Device Type: All

Right: All

Effective Rights Format: XLS

Outside Network Policies: Do not include

User: All

Specific Device: All

Generate

Effective Rights List

Filters

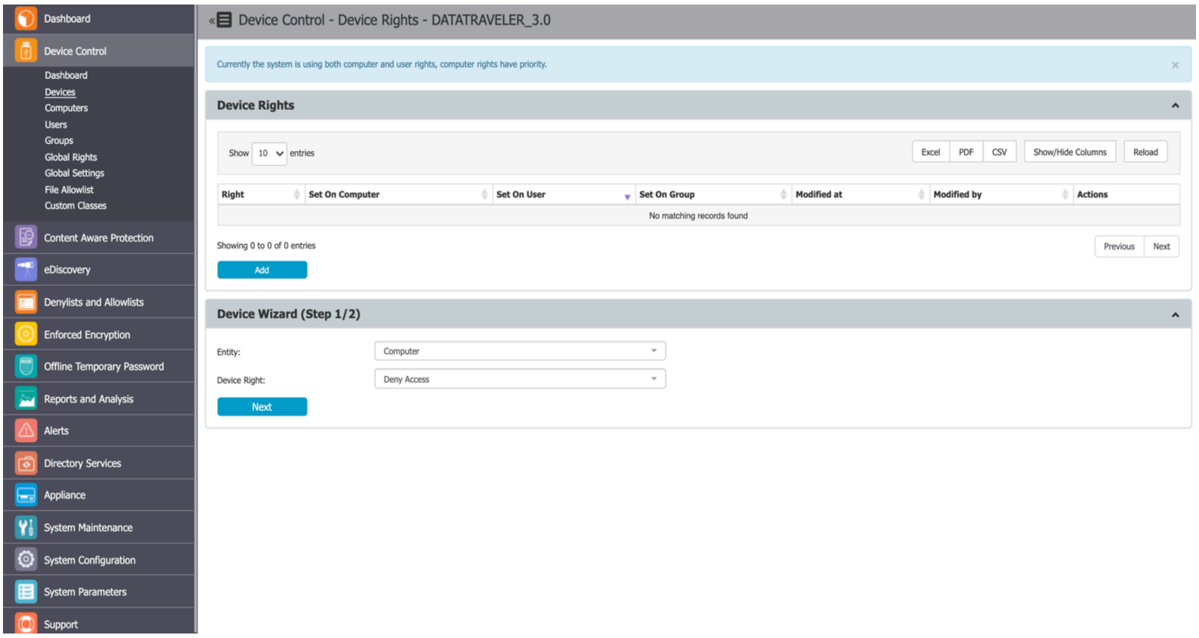
Show 10 entries

Excel PDF CSV Show/Hide Columns Reload

Section	Computer	User	Device Type	Device	Right	Policy	Created at	Status	Format	Actions
Device Control	QA MacBook Pro	qa	USB Storage Device	DATATRAVELER_3.0	All	N/A	2021-02-26 08:20:52	Ready to download	pdf	☰
Content Aware Protection	QA MacBook Pro	qa	N/A	N/A	N/A	All	2021-02-26 08:20:23	Ready to download	pdf	☰
Content Aware Protection	QA MacBook Pro	All	N/A	N/A	N/A	All	2021-02-26 08:20:08	Ready to download	pdf	☰
Device Control	QA MacBook Pro	All	All	All	All	N/A	2021-02-26 08:19:57	Ready to download	pdf	☰
Device Control	QA MacBook Pro	All	All	All	All	N/A	2021-02-26 08:19:51	Ready to download	xls	☰

Showing 1 to 5 of 5 entries

Previous 1 Next



Device Control - Device Rights - DATATRAVELER_3.0

Currently the system is using both computer and user rights, computer rights have priority.

Device Rights

Show 10 entries

Excel PDF CSV Show/Hide Columns Reload

Right	Set On Computer	Set On User	Set On Group	Modified at	Modified by	Actions
No matching records found						

Showing 0 to 0 of 0 entries

Previous Next

Add

Device Wizard (Step 1/2)

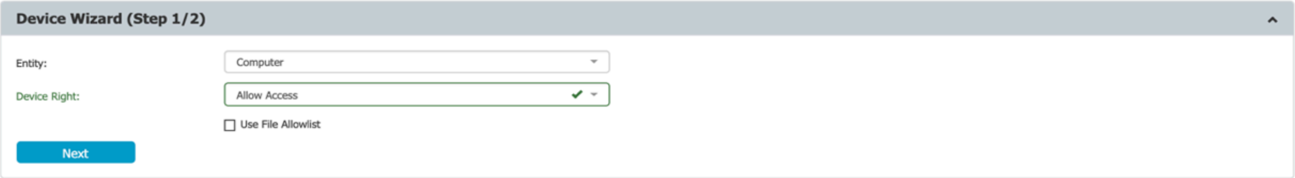
Entity: Computer

Device Right: Deny Access

Next

After selecting a device, assigning rights to specific users, computers or groups then follow these steps:

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



Device Wizard (Step 1/2)

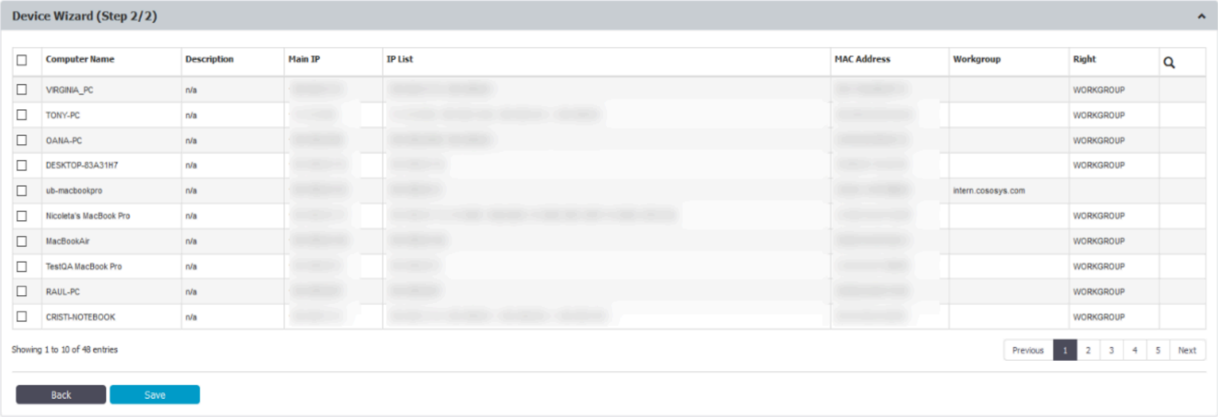
Entity: Computer

Device Right: Allow Access ✓

□ Use File Allowlist

Next

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



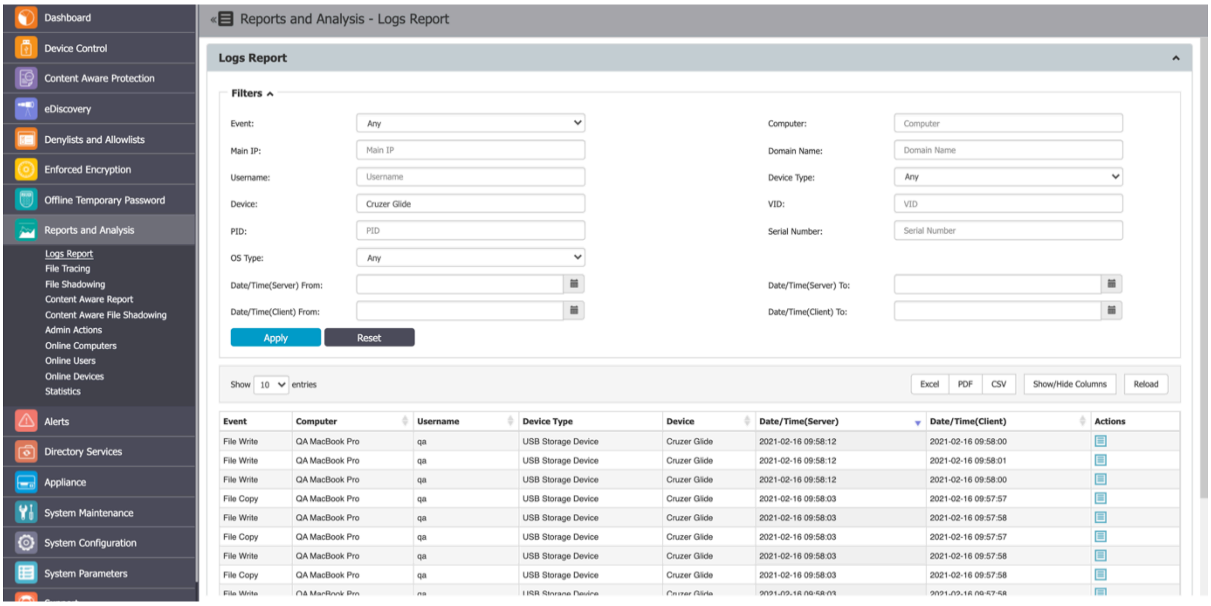
Device Wizard (Step 2/2)

□	Computer Name	Description	Main IP	IP List	MAC Address	Workgroup	Right
□	VIRGINIA_PC	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	TONY-PC	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	OANA-PC	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	DESKTOP-83A31H7	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	ub-macbookpro	n/a	[redacted]	[redacted]	[redacted]	intern.cososys.com	
□	Nicoleta's MacBook Pro	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	MacBookAir	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	TestQA MacBook Pro	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	RAUL-PC	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	CRISTI-NOTEBOOK	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP

Showing 1 to 10 of 48 entries

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.



Reports and Analysis - Logs Report

Logs Report

Filters

Event: Any

Main IP:

Username:

Device: Cruzer Glide

PID:

OS Type: Any

Date/Time(Server) From:

Date/Time(Client) From:

Computer:

Domain Name:

Device Type: Any

VID:

Serial Number:

Date/Time(Server) To:

Date/Time(Client) To:

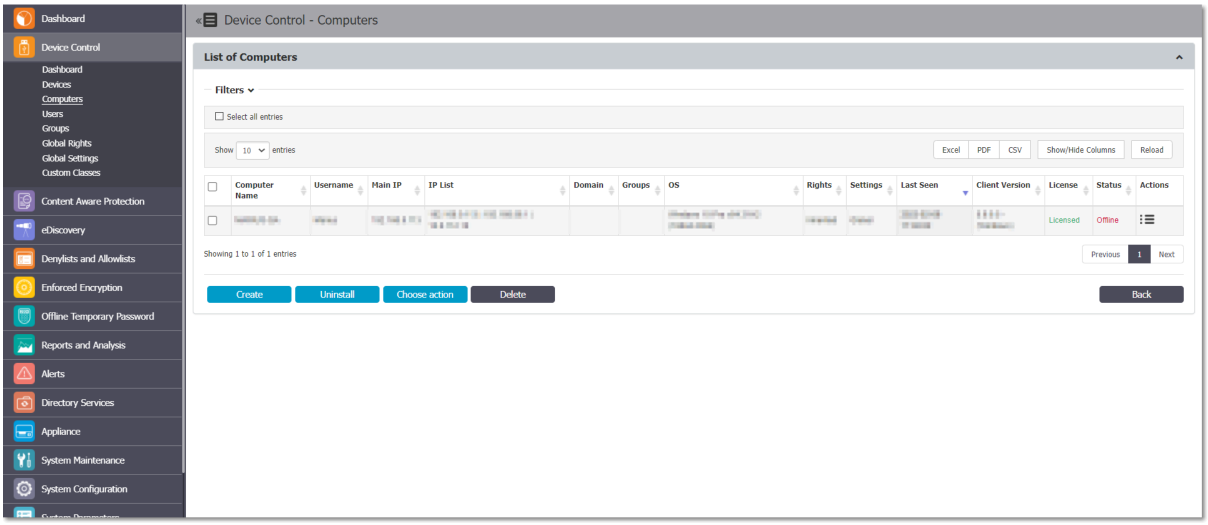
Event	Computer	Username	Device Type	Device	Date/Time(Server)	Date/Time(Client)	Actions
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:12	2021-02-16 09:58:00	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:12	2021-02-16 09:58:01	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:12	2021-02-16 09:58:00	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:57	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:57	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤

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.



☐ Select all entries

Show 10 entries

☐	Computer Name	Username	Main IP	IP List	Domain	Groups	OS	Rights	Settings	Last Seen	Client Version	License	Status	Actions
☐	[redacted]	[redacted]	[redacted]	[redacted]			[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Licensed	Offline	☰

Showing 1 to 1 of 1 entries

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, Computer Serial Number or MachineUUID, 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 MachineUUID 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.

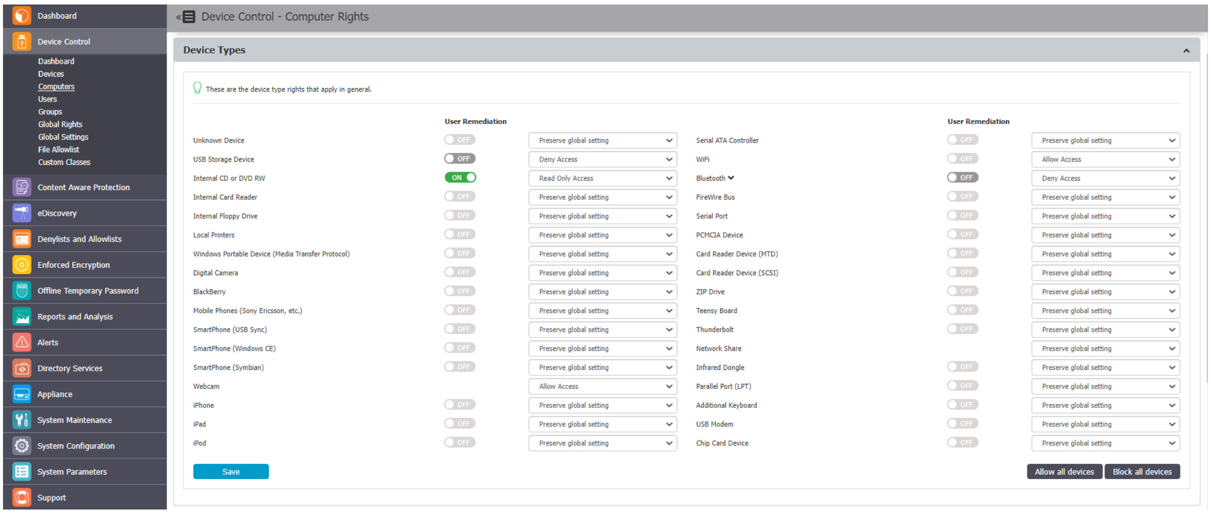
For more details about Active Directory, go to the Directory Services chapter.

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.



These are the device type rights that apply in general.

	User Remediation			User Remediation	
Unknown Device	OFF	Preserve global setting	Serial ATA Controller	OFF	Preserve global setting
USB Storage Device	OFF	Deny Access	WiFi	OFF	Allow Access
Internal CD or DVD RW	ON	Read Only Access	Bluetooth	OFF	Deny Access
Internal Card Reader	OFF	Preserve global setting	FireWire Bus	OFF	Preserve global setting
Internal Floppy Drive	OFF	Preserve global setting	Serial Port	OFF	Preserve global setting
Local Printers	OFF	Preserve global setting	PCMCIA Device	OFF	Preserve global setting
Windows Portable Device (Media Transfer Protocol)	OFF	Preserve global setting	Card Reader Device (MTD)	OFF	Preserve global setting
Digital Camera	OFF	Preserve global setting	Card Reader Device (SCSI)	OFF	Preserve global setting
BlackBerry	OFF	Preserve global setting	ZIP Drive	OFF	Preserve global setting
Mobile Phones (Sony Ericsson, etc.)	OFF	Preserve global setting	Teensy Board	OFF	Preserve global setting
SmartPhone (USB Sync)	OFF	Preserve global setting	Thunderbolt	OFF	Preserve global setting
SmartPhone (Windows CE)	OFF	Preserve global setting	Network Share		Preserve global setting
SmartPhone (Symbian)	OFF	Preserve global setting	Infrared Dongle	OFF	Preserve global setting
Webcam		Allow Access	Parallel Port (LPT)	OFF	Preserve global setting
iPhone	OFF	Preserve global setting	Additional Keyboard	OFF	Preserve global setting
iPad	OFF	Preserve global setting	USB Modem	OFF	Preserve global setting
iPod	OFF	Preserve global setting	Chip Card Device	OFF	Preserve global setting

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.

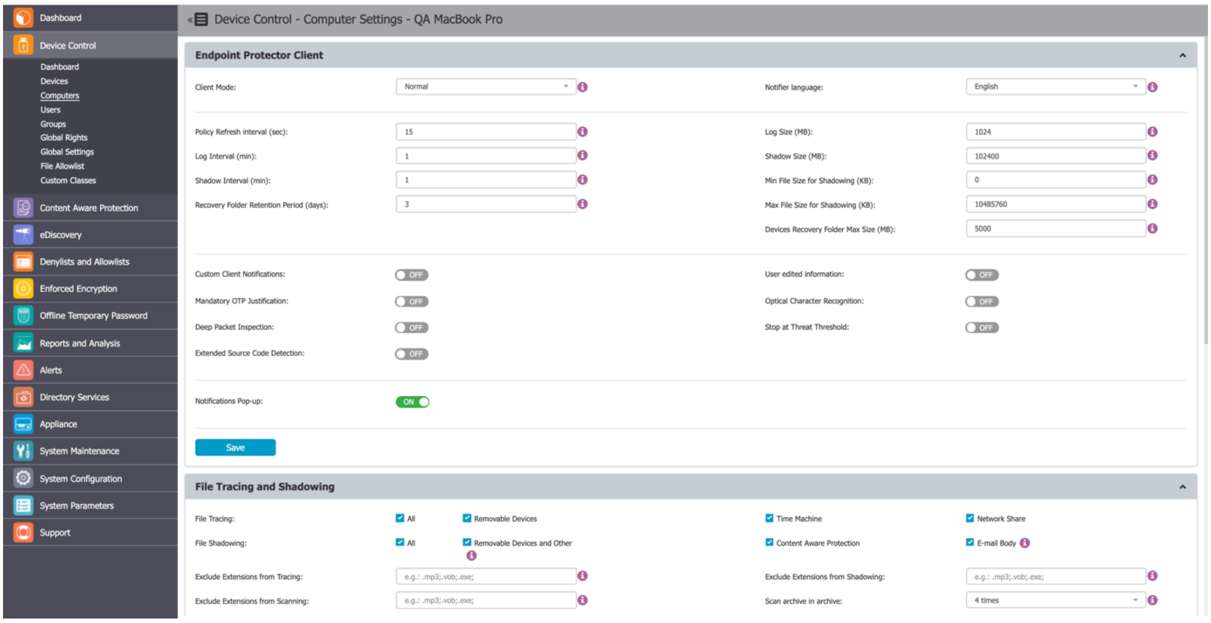
All Existing Devices that were added on that level will be deleted when the restore is used.

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.



Device Control - Computer Settings - QA MacBook Pro

Endpoint Protector Client

Client Mode: Normal

Notifier language: English

Policy Refresh interval (sec): 15

Log Interval (min): 1

Shadow Interval (min): 1

Recovery Folder Retention Period (days): 3

Log Size (MB): 1024

Shadow Size (MB): 102400

Min File Size for Shadowing (KB): 0

Max File Size for Shadowing (KB): 10485760

Devices Recovery Folder Max Size (MB): 5000

Custom Client Notifications: OFF

Mandatory OTP Justification: OFF

Deep Packet Inspection: OFF

Extended Source Code Detection: OFF

User edited information: OFF

Optical Character Recognition: OFF

Stop at Threat Threshold: OFF

Notifications Pop-up: ON

File Tracing and Shadowing

File Tracing: ☑ All ☑ Removable Devices ☑ Time Machine ☑ Network Share

File Shadowing: ☑ All ☑ Removable Devices and Other ☑ Content Aware Protection ☑ E-mail Body

Exclude Extensions from Tracing: e.g.: .mp3;.vob;.exe;

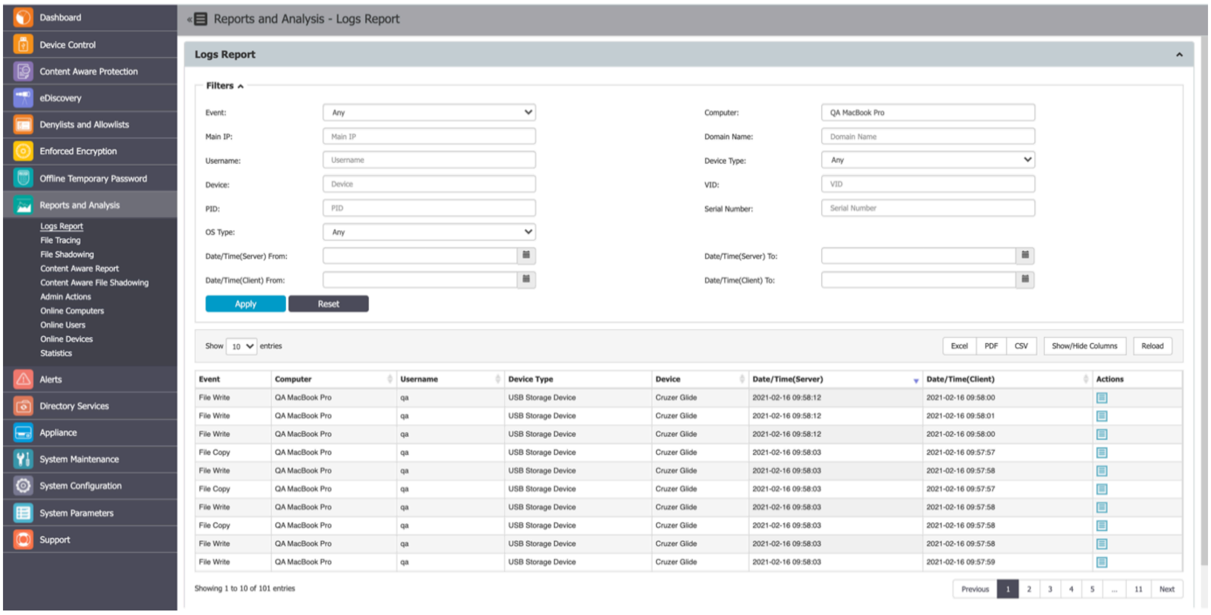
Exclude Extensions from Shadowing: e.g.: .mp3;.vob;.exe;

Exclude Extensions from Scanning: e.g.: .mp3;.vob;.exe;

Scan archive in archive: 4 times

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.



Reports and Analysis - Logs Report

Logs Report

Filters

Event: Any

Computer: QA MacBook Pro

Main IP: Main IP

Domain Name: Domain Name

Username: Username

Device Type: Any

Device: Device

VID: VID

PID: PID

Serial Number: Serial Number

OS Type: Any

Date/Time(Server) From:

Date/Time(Server) To:

Date/Time(Client) From:

Date/Time(Client) To:

Show 10 entries

Event	Computer	Username	Device Type	Device	Date/Time(Server)	Date/Time(Client)	Actions
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:12	2021-02-16 09:58:00	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:12	2021-02-16 09:58:01	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:12	2021-02-16 09:58:00	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:57	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:57	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:59	▤

Showing 1 to 10 of 101 entries

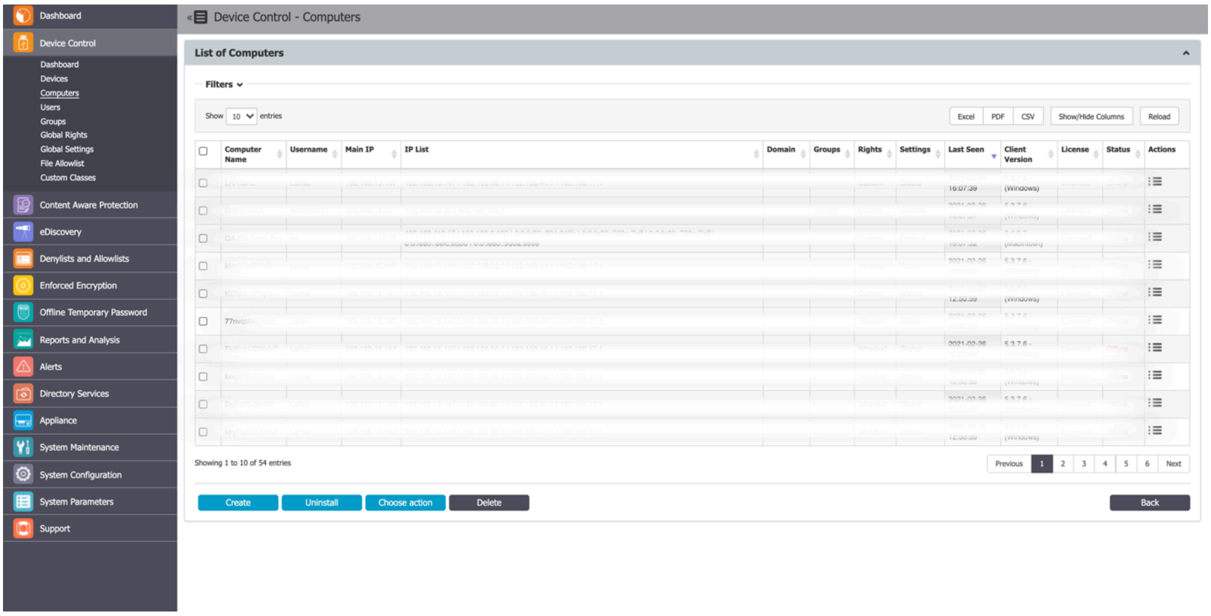
5.3.4. Terminal Servers and Thin Clients

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:

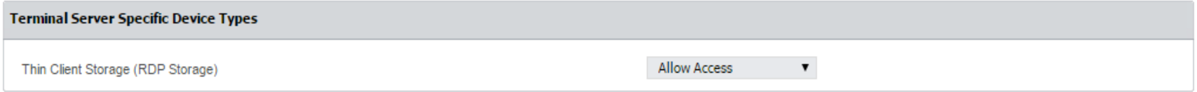


Note: The computers that can be targeted by this action are strictly Windows Servers with Terminal Server roles properly configured

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

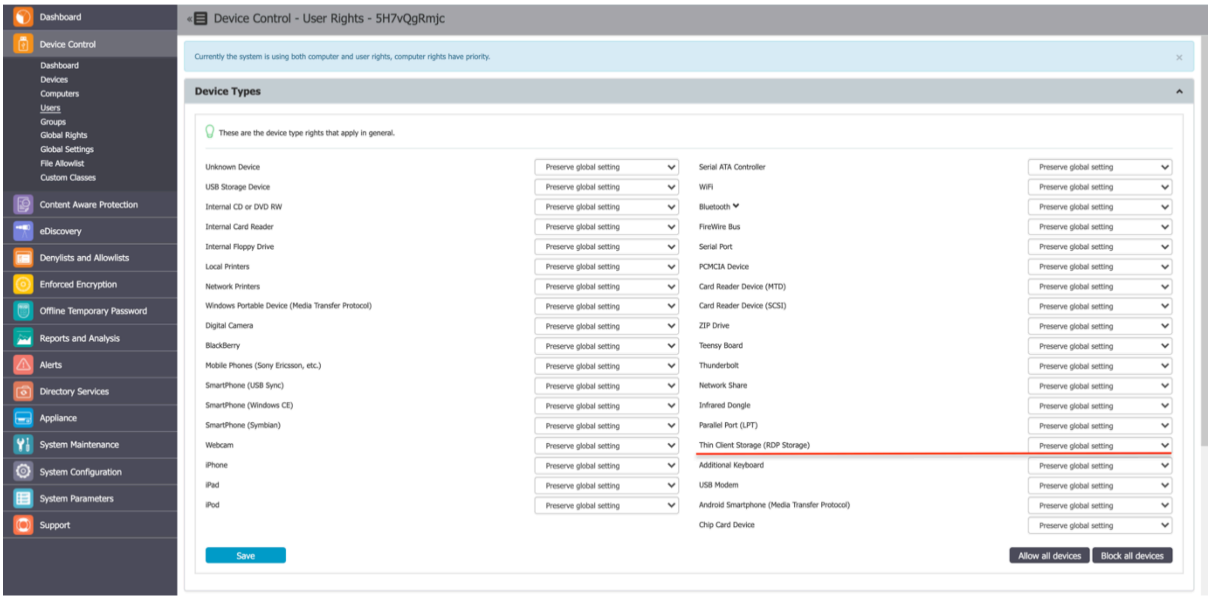
Thin Client Storage (RDP Storage) — Allow Access ▼

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).



Device Control - User Rights - 5H7vQgRmjc

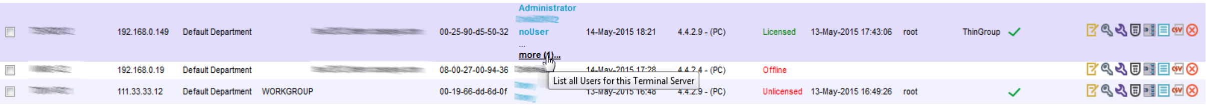
Currently the system is using both computer and user rights, computer rights have priority.

Device Types

These are the device type rights that apply in general.

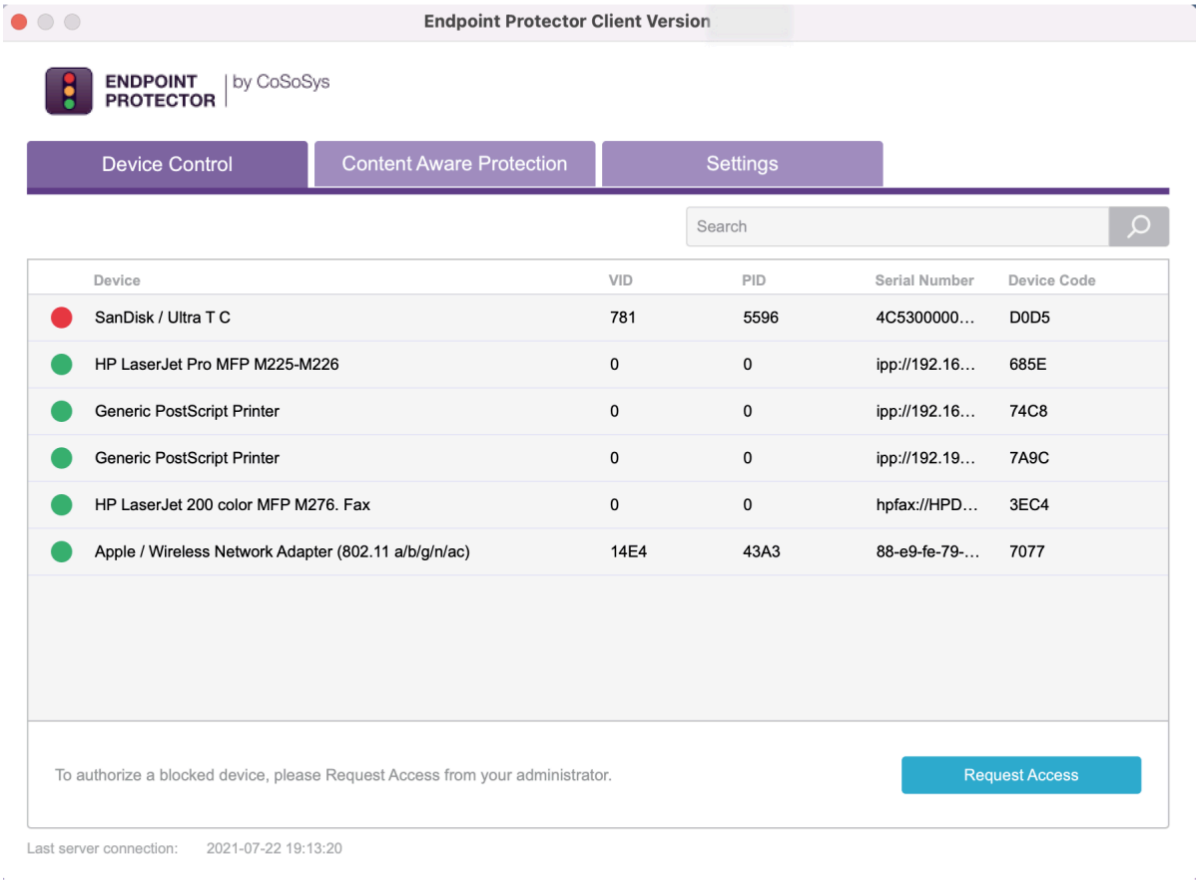
Unknown Device	Preserve global setting	Serial ATA Controller	Preserve global setting
USB Storage Device	Preserve global setting	WiFi	Preserve global setting
Internal CD or DVD RW	Preserve global setting	Bluetooth	Preserve global setting
Internal Card Reader	Preserve global setting	FireWire Bus	Preserve global setting
Internal Floppy Drive	Preserve global setting	Serial Port	Preserve global setting
Local Printers	Preserve global setting	PCMCIA Device	Preserve global setting
Network Printers	Preserve global setting	Card Reader Device (MTD)	Preserve global setting
Windows Portable Device (Media Transfer Protocol)	Preserve global setting	Card Reader Device (SCSI)	Preserve global setting
Digital Camera	Preserve global setting	ZIP Drive	Preserve global setting
BlackBerry	Preserve global setting	Teensy Board	Preserve global setting
Mobile Phones (Sony Ericsson, etc.)	Preserve global setting	Thunderbolt	Preserve global setting
SmartPhone (USB Sync)	Preserve global setting	Network Share	Preserve global setting
SmartPhone (Windows CE)	Preserve global setting	Infrared Dongle	Preserve global setting
SmartPhone (Symbian)	Preserve global setting	Parallel Port (LPT)	Preserve global setting
Webcam	Preserve global setting	Thin Client Storage (RDP Storage)	Preserve global setting
iPhone	Preserve global setting	Additional Keyboard	Preserve global setting
iPad	Preserve global setting	USB Modem	Preserve global setting
iPod	Preserve global setting	Android Smartphone (Media Transfer Protocol)	Preserve global setting
		Chip Card Device	Preserve global setting

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.



☐	[redacted]	192.168.0.149	Default Department	[redacted]	00-25-90-d5-50-32	Administrator [redacted] noUser ... more (1)...	14-May-2015 18:21	4.4.2.9 - (PC)	Licensed	13-May-2015 17:43:06	root	ThinGroup	✓
☐	[redacted]	192.168.0.19	Default Department	[redacted]	08-00-27-00-94-36	[redacted]	14-May-2015 17:28	4.4.2.4 - (PC)	Offline				
☐	[redacted]	111.33.33.12	Default Department	WORKGROUP	00-19-66-dd-6d-0f	[redacted]	13-May-2015 16:48	4.4.2.9 - (PC)	Unlicensed	13-May-2015 16:49:26	root		✓

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


Endpoint Protector Client Version
ENDPOINT PROTECTOR | by CoSoSys
Device Control
Content Aware Protection
Settings
Search

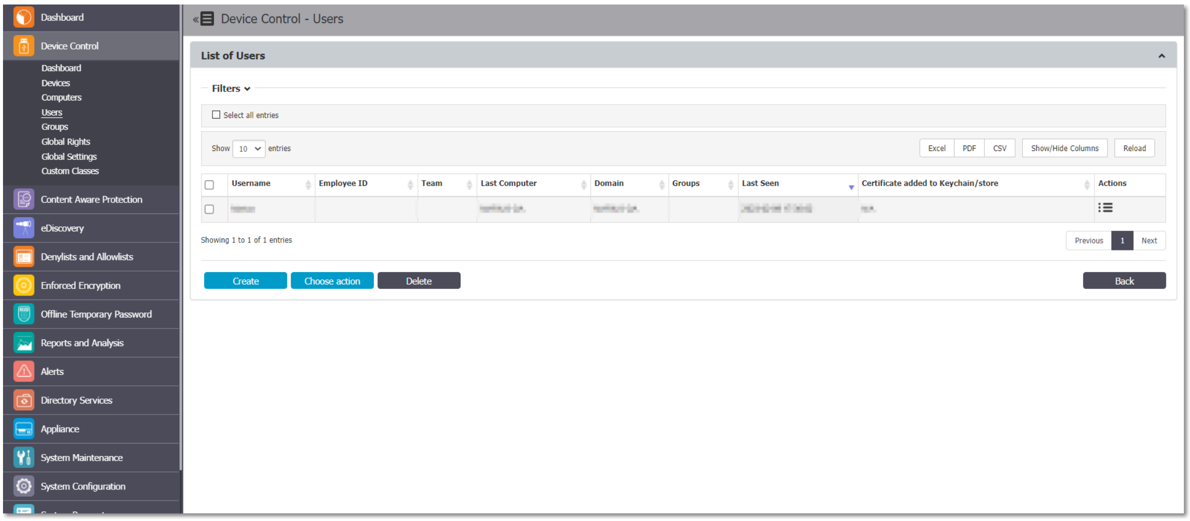
	Device	VID	PID	Serial Number	Device Code
🔴	SanDisk / Ultra T C	781	5596	4C5300000…	D0D5
🟢	HP LaserJet Pro MFP M225-M226	0	0	ipp://192.16…	685E
🟢	Generic PostScript Printer	0	0	ipp://192.16…	74C8
🟢	Generic PostScript Printer	0	0	ipp://192.19…	7A9C
🟢	HP LaserJet 200 color MFP M276. Fax	0	0	hpfax://HPD…	3EC4
🟢	Apple / Wireless Network Adapter (802.11 a/b/g/n/ac)	14E4	43A3	88-e9-fe-79-…	7077

To authorize a blocked device, please Request Access from your administrator.

Last server connection: 2021-07-22 19:13:20

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.



□	Username	Employee ID	Team	Last Computer	Domain	Groups	Last Seen	Certificate added to Keychain/store	Actions
□	[redacted]			[redacted]	[redacted]		[redacted]	[redacted]	☰

Showing 1 to 1 of 1 entries

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.

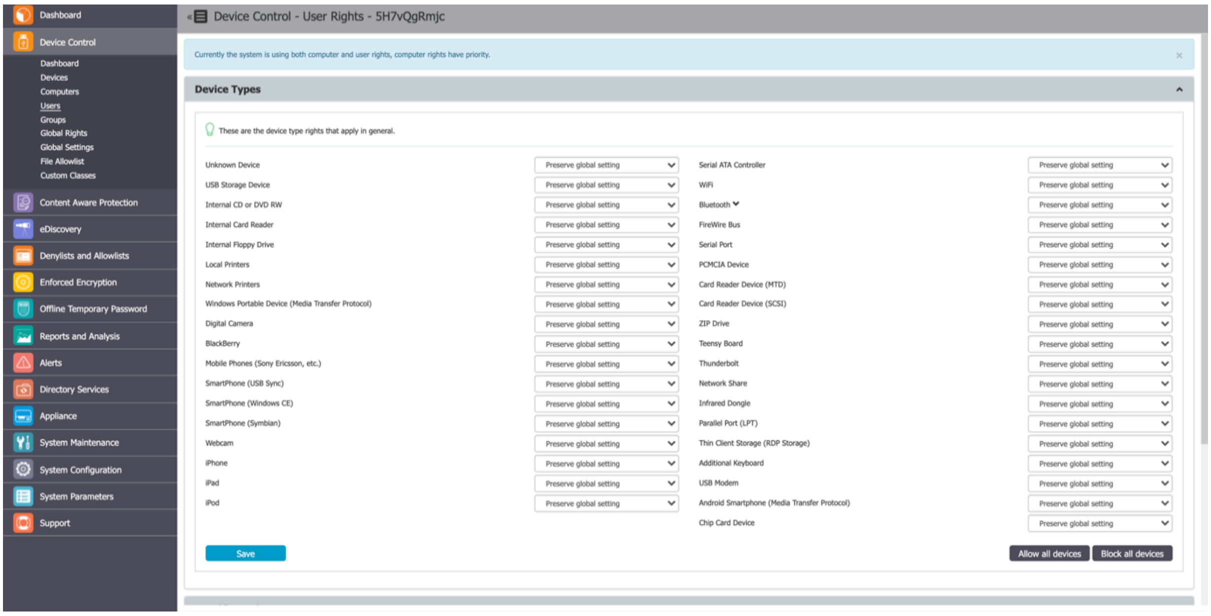
This section is built around the users, allowing the Administrator to specify what Device Types and also what Specific Devices can be accessible.

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.



Device Control - User Rights - 5H7vQgRmjc

Currently the system is using both computer and user rights, computer rights have priority.

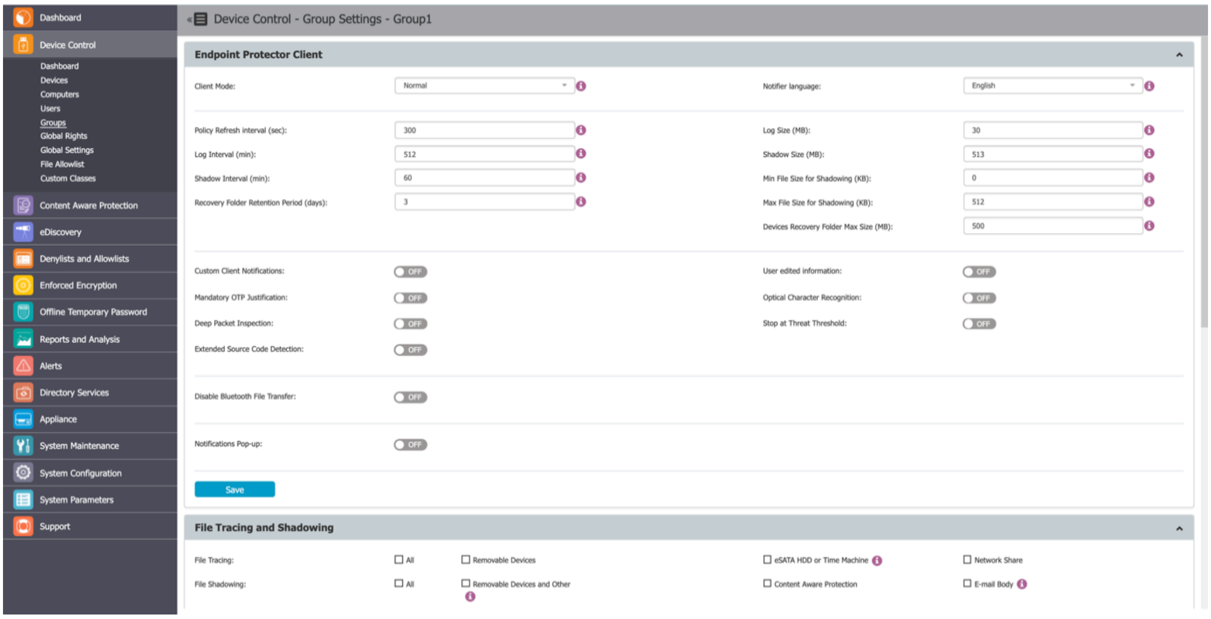
Device Types

These are the device type rights that apply in general.

Unknown Device	Preserve global setting	Serial ATA Controller	Preserve global setting
USB Storage Device	Preserve global setting	WiFi	Preserve global setting
Internal CD or DVD RW	Preserve global setting	Bluetooth	Preserve global setting
Internal Card Reader	Preserve global setting	FireWire Bus	Preserve global setting
Internal Floppy Drive	Preserve global setting	Serial Port	Preserve global setting
Local Printers	Preserve global setting	PCMCIA Device	Preserve global setting
Network Printers	Preserve global setting	Card Reader Device (MTD)	Preserve global setting
Windows Portable Device (Media Transfer Protocol)	Preserve global setting	Card Reader Device (SCSI)	Preserve global setting
Digital Camera	Preserve global setting	ZIP Drive	Preserve global setting
BlackBerry	Preserve global setting	Teensy Board	Preserve global setting
Mobile Phones (Sony Ericsson, etc.)	Preserve global setting	Thunderbolt	Preserve global setting
SmartPhone (USB Sync)	Preserve global setting	Network Share	Preserve global setting
SmartPhone (Windows CE)	Preserve global setting	Infrared Dongle	Preserve global setting
SmartPhone (Symbian)	Preserve global setting	Parallel Port (LPT)	Preserve global setting
Webcam	Preserve global setting	Thin Client Storage (RDP Storage)	Preserve global setting
iPhone	Preserve global setting	Additional Keyboard	Preserve global setting
iPad	Preserve global setting	USB Modem	Preserve global setting
iPod	Preserve global setting	Android Smartphone (Media Transfer Protocol)	Preserve global setting
		Chip Card Device	Preserve global setting

5.4.2. User Settings

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



Device Control - Group Settings - Group1

Endpoint Protector Client

Client Mode:	Normal	Notifier language:	English
Policy Refresh interval (sec):	300	Log Size (MB):	30
Log Interval (min):	512	Shadow Size (MB):	513
Shadow Interval (min):	60	Min File Size for Shadowing (KB):	0
Recovery Folder Retention Period (days):	3	Max File Size for Shadowing (KB):	512
		Devices Recovery Folder Max Size (MB):	500
Custom Client Notifications:	OFF	User edited information:	OFF
Mandatory OTP Justification:	OFF	Optical Character Recognition:	OFF
Deep Packet Inspection:	OFF	Stop at Threat Threshold:	OFF
Extended Source Code Detection:	OFF		
Disable Bluetooth File Transfer:	OFF		
Notifications Pop-up:	OFF		

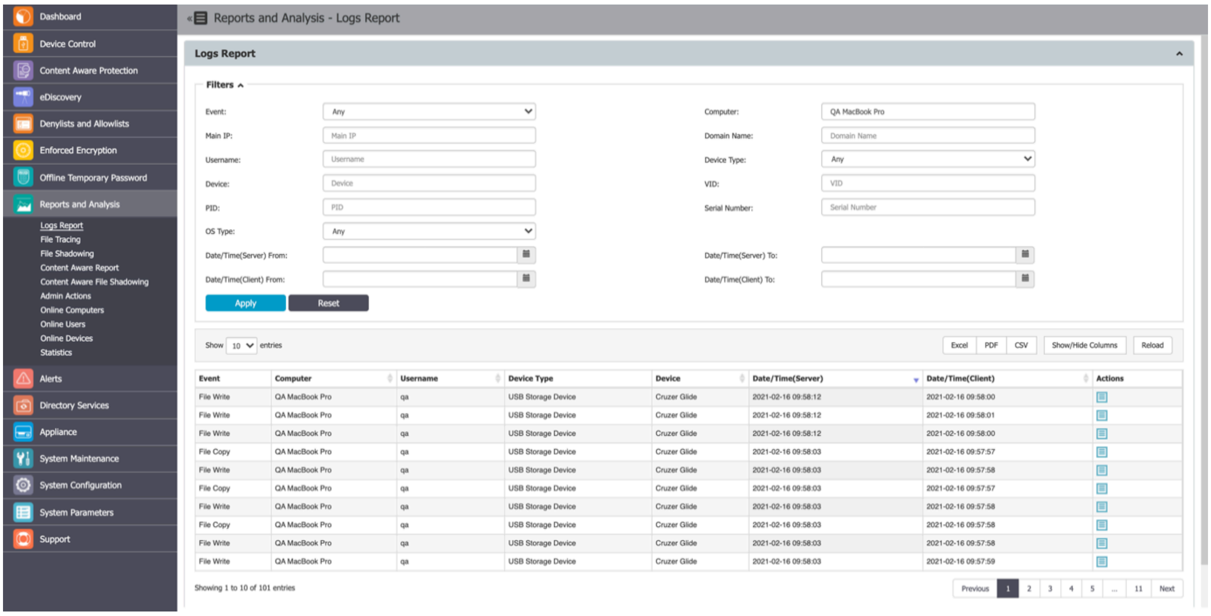
File Tracing and Shadowing

File Tracing:	□ All	□ Removable Devices	□ eSATA HDD or Time Machine	□ Network Share
File Shadowing:	□ All	□ Removable Devices and Other	□ Content Aware Protection	□ E-mail Body

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.



Event: Any
Main IP: Main IP
Username: Username
Device: Device
PID: PID
OS Type: Any
Date/Time(Server) From:
Date/Time(Client) From:
Computer: QA MacBook Pro
Domain Name: Domain Name
Device Type: Any
VID: VID
Serial Number: Serial Number
Date/Time(Server) To:
Date/Time(Client) To:

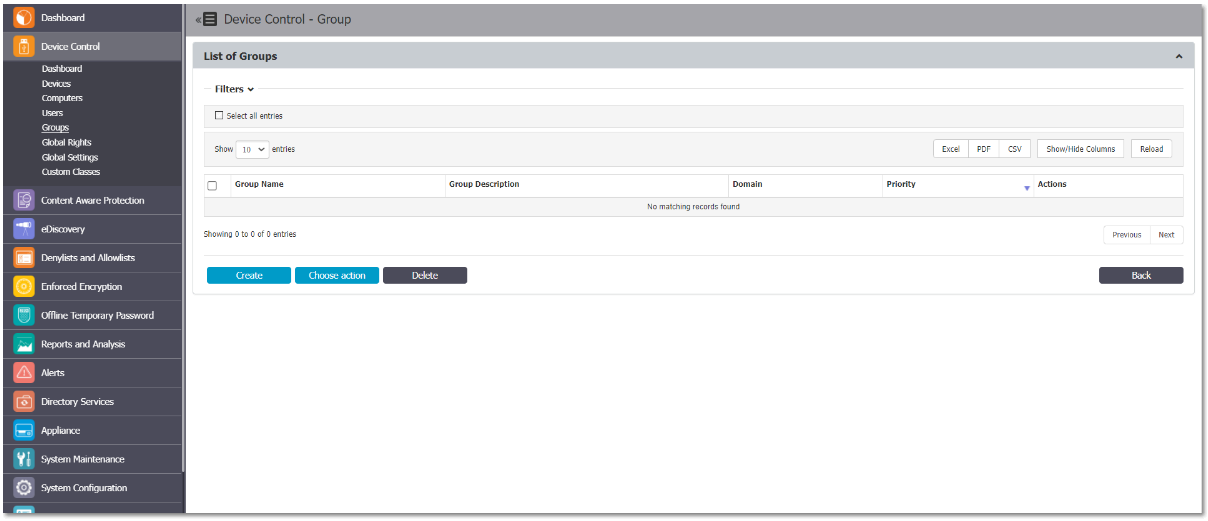
Show 10 entries

Event	Computer	Username	Device Type	Device	Date/Time(Server)	Date/Time(Client)	Actions
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:12	2021-02-16 09:58:00	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:12	2021-02-16 09:58:01	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:12	2021-02-16 09:58:00	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:57	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:57	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:58	▤
File Write	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:58:03	2021-02-16 09:57:59	▤

Showing 1 to 10 of 101 entries

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.



□ Select all entries

Show 10 entries

□	Group Name	Group Description	Domain	Priority	Actions
No matching records found					

Showing 0 to 0 of 0 entries

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.

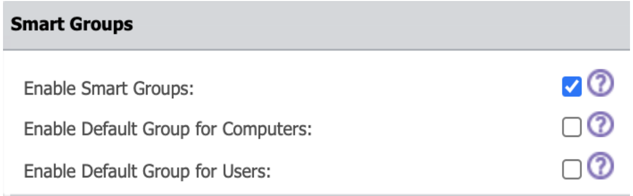
5.5.1.2. Smart Groups

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.



Smart Groups

Enable Smart Groups: ☑

Enable Default Group for Computers: □

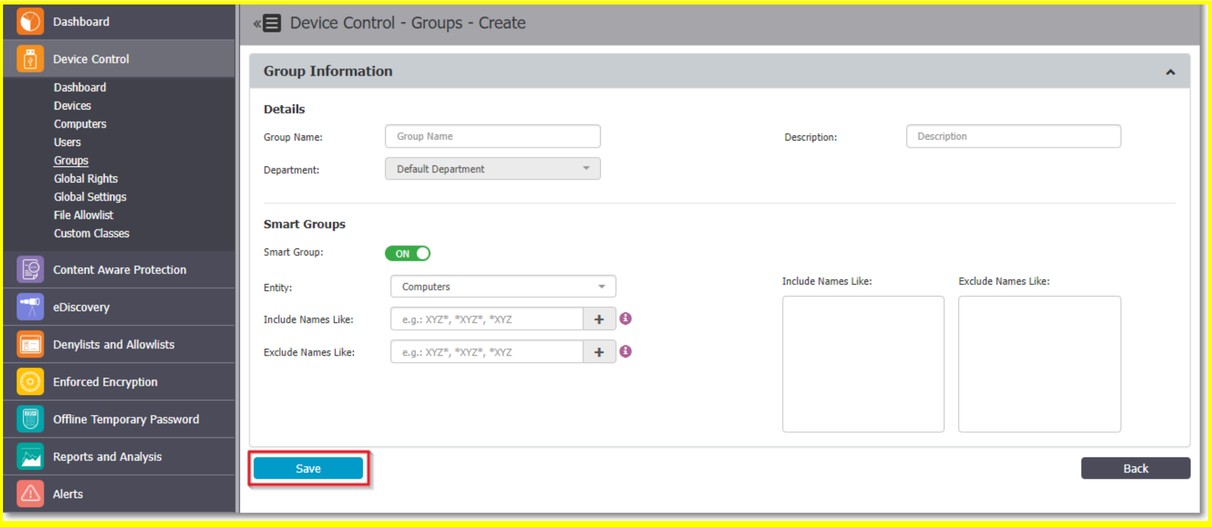
Enable Default Group for Users: □

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.



Device Control - Groups - Create

Group Information

Details

Group Name: Group Name

Description: Description

Department: Default Department

Smart Groups

Smart Group: ON

Entity: Computers

Include Names Like: e.g.: XYZ*, *XYZ*, *XYZ

Exclude Names Like: e.g.: XYZ*, *XYZ*, *XYZ

Include Names Like:

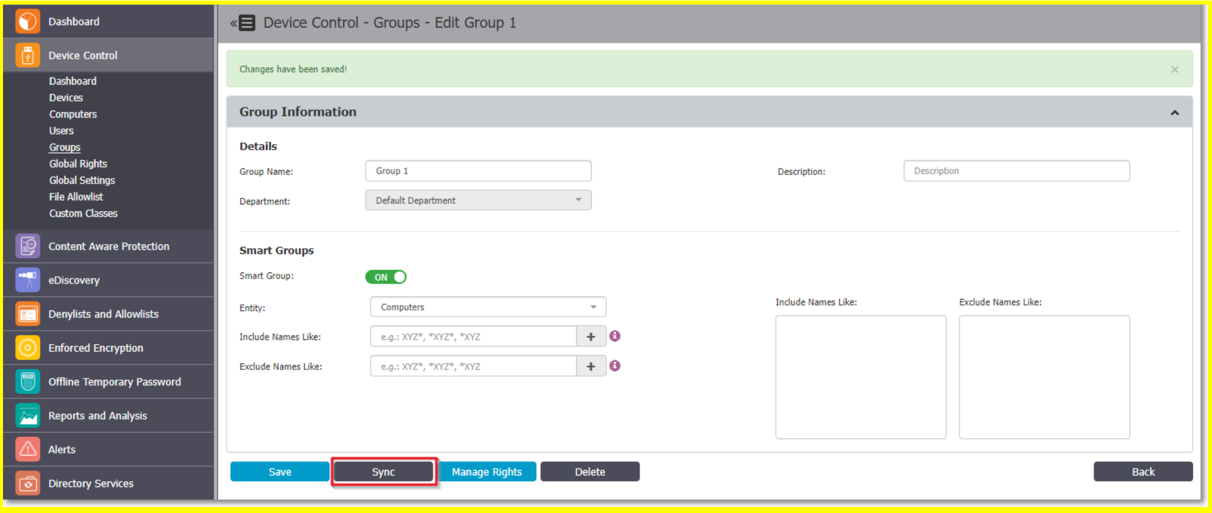
Exclude Names Like:

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.



Device Control - Groups - Edit Group 1

Changes have been saved!

Group Information

Details

Group Name: Group 1

Description: Description

Department: Default Department

Smart Groups

Smart Group: ON

Entity: Computers

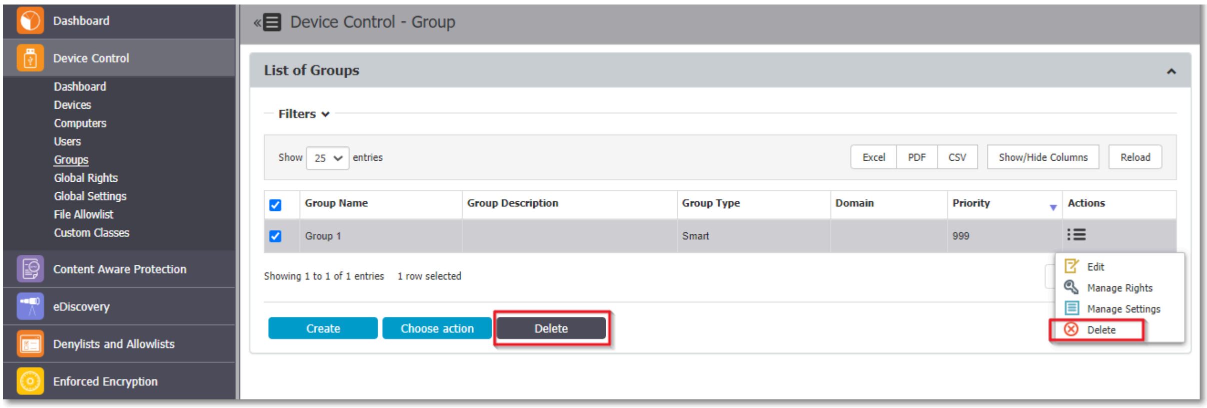
Include Names Like: e.g.: XYZ*, *XYZ*, *XYZ

Exclude Names Like: e.g.: XYZ*, *XYZ*, *XYZ

Include Names Like:

Exclude Names Like:

4. Delete a Smart Group from the **Actions** column or select the group from the list and then click **Delete**.



☑	Group Name	Group Description	Group Type	Domain	Priority	Actions
☑	Group 1		Smart		999	

Showing 1 to 1 of 1 entries 1 row selected

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).

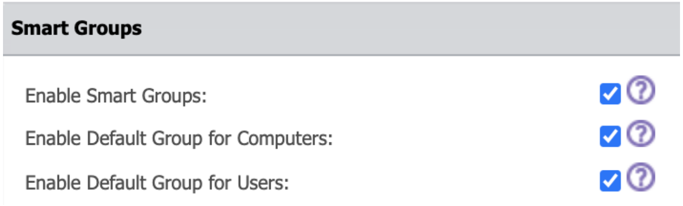
5.5.1.3. Default Groups

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**.



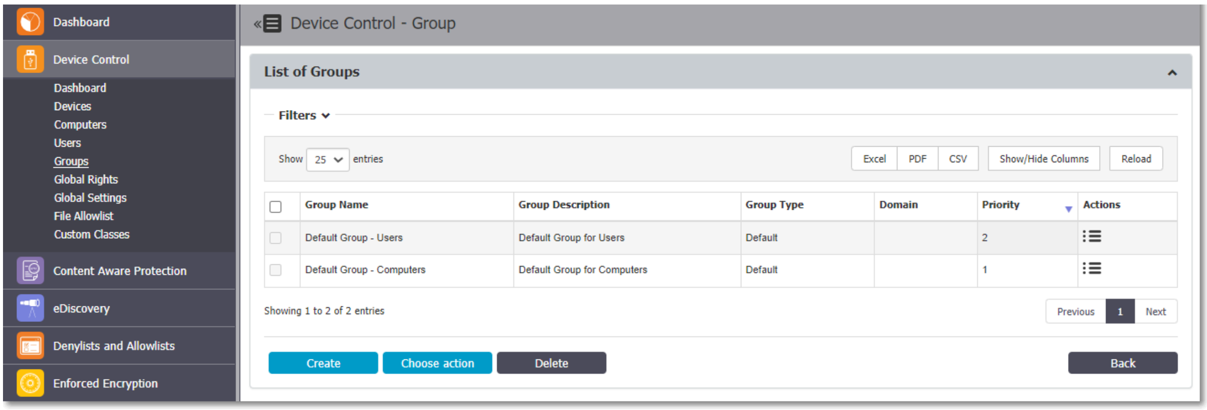
Smart Groups

Enable Smart Groups: ☑

Enable Default Group for Computers: ☑

Enable Default Group for Users: ☑

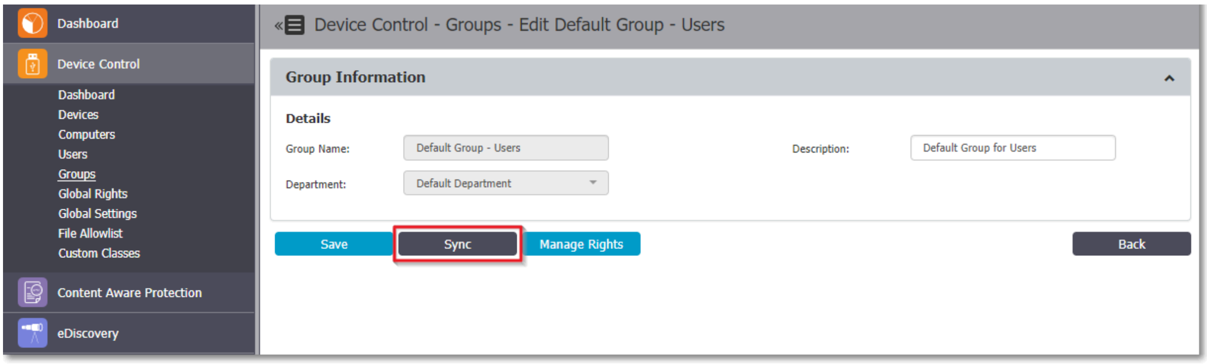
Important: You are not required to manually create Default Groups – by enabling them, the Default Groups for Users and Computers will be automatically created.



□	Group Name	Group Description	Group Type	Domain	Priority	Actions
□	Default Group - Users	Default Group for Users	Default		2	☰
□	Default Group - Computers	Default Group for Computers	Default		1	☰

Showing 1 to 2 of 2 entries

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**.



Details

Group Name: Default Group - Users

Description: Default Group for Users

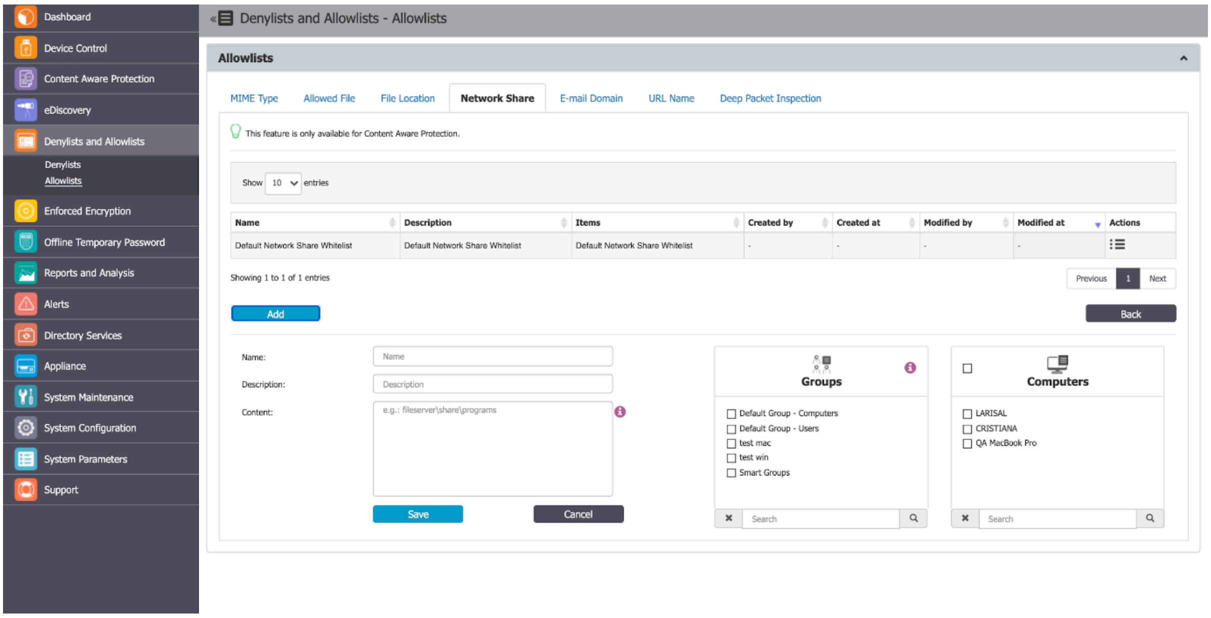
Department: Default Department

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.



This feature is only available for Content Aware Protection.

Show 10 entries

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Default Network Share Whitelist	Default Network Share Whitelist	Default Network Share Whitelist	-	-	-	-	☰

Showing 1 to 1 of 1 entries

Name: Name

Description: Description

Content: e.g.: fileserver\share\programs

Groups

□ Default Group - Computers
□ Default Group - Users
□ test mac
□ test win
□ Smart Groups

□ Computers

□ LARISAL
□ CRISTIANA
□ QA MacBook Pro

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.

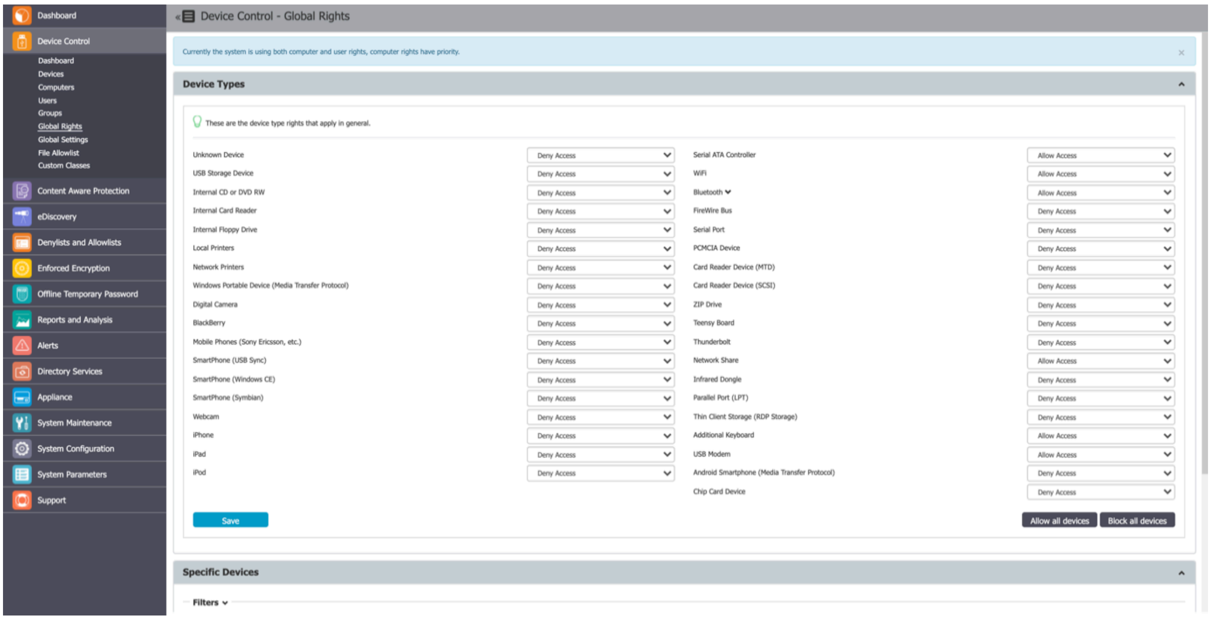
The Standard device control rights include the Device Types and Already Existing Devices sections. These are generally the only device rights used.

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.



Device Control - Global Rights

Currently the system is using both computer and user rights, computer rights have priority.

Device Types

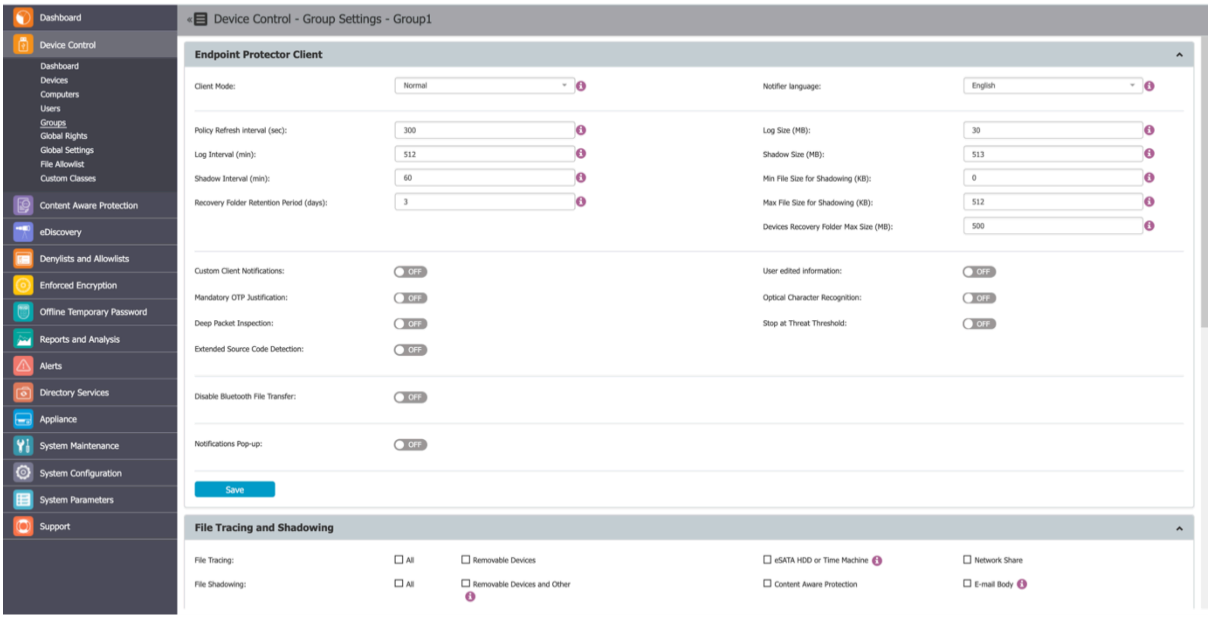
These are the device type rights that apply in general.

Unknown Device	Deny Access	Serial ATA Controller	Allow Access
USB Storage Device	Deny Access	WiFi	Allow Access
Internal CD or DVD RW	Deny Access	Bluetooth	Allow Access
Internal Card Reader	Deny Access	FireWire Bus	Deny Access
Internal Floppy Drive	Deny Access	Serial Port	Deny Access
Local Printers	Deny Access	PCMCIA Device	Deny Access
Network Printers	Deny Access	Card Reader Device (MTD)	Deny Access
Windows Portable Device (Media Transfer Protocol)	Deny Access	Card Reader Device (SCSI)	Deny Access
Digital Camera	Deny Access	ZIP Drive	Deny Access
BlackBerry	Deny Access	Teensy Board	Deny Access
Mobile Phones (Sony Ericsson, etc.)	Deny Access	Thunderbolt	Deny Access
SmartPhone (USB Sync)	Deny Access	Network Share	Allow Access
SmartPhone (Windows CE)	Deny Access	Infrared Dongle	Deny Access
SmartPhone (Symbian)	Deny Access	Parallel Port (LPT)	Deny Access
Webcam	Deny Access	Thin Client Storage (RDP Storage)	Deny Access
iPhone	Deny Access	Additional Keyboard	Allow Access
iPad	Deny Access	USB Modem	Allow Access
iPod	Deny Access	Android Smartphone (Media Transfer Protocol)	Deny Access
		Chip Card Device	Deny Access

Specific Devices

5.5.3. Group Settings

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



Device Control - Group Settings - Group1

Endpoint Protector Client

Client Mode:	Normal	Notifier language:	English
Policy Refresh interval (sec):	300	Log Size (MB):	30
Log Interval (min):	512	Shadow Size (MB):	513
Shadow Interval (min):	60	Min File Size for Shadowing (KB):	0
Recovery Folder Retention Period (days):	3	Max File Size for Shadowing (KB):	512
		Devices Recovery Folder Max Size (MB):	500
Custom Client Notifications:	OFF	User edited information:	OFF
Mandatory OTP Justification:	OFF	Optical Character Recognition:	OFF
Deep Packet Inspection:	OFF	Stop at Threat Threshold:	OFF
Extended Source Code Detection:	OFF		
Disable Bluetooth File Transfer:	OFF		
Notifications Pop-up:	OFF		

File Tracing and Shadowing

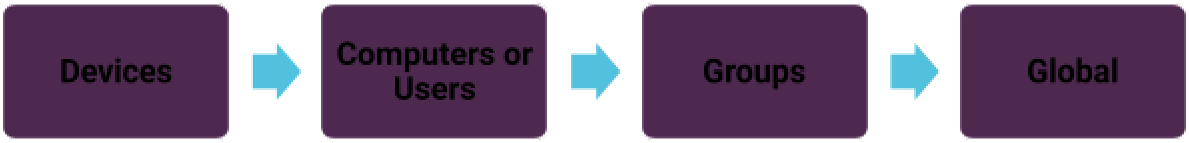
File Tracing:	□ All	□ Removable Devices	□ eSATA HDD or Time Machine	□ Network Share
File Shadowing:	□ All	□ Removable Devices and Other	□ Content Aware Protection	□ E-mail Body

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:

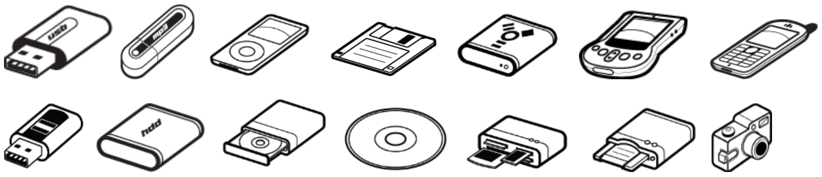


Devices → Computers or Users → Groups → Global

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**

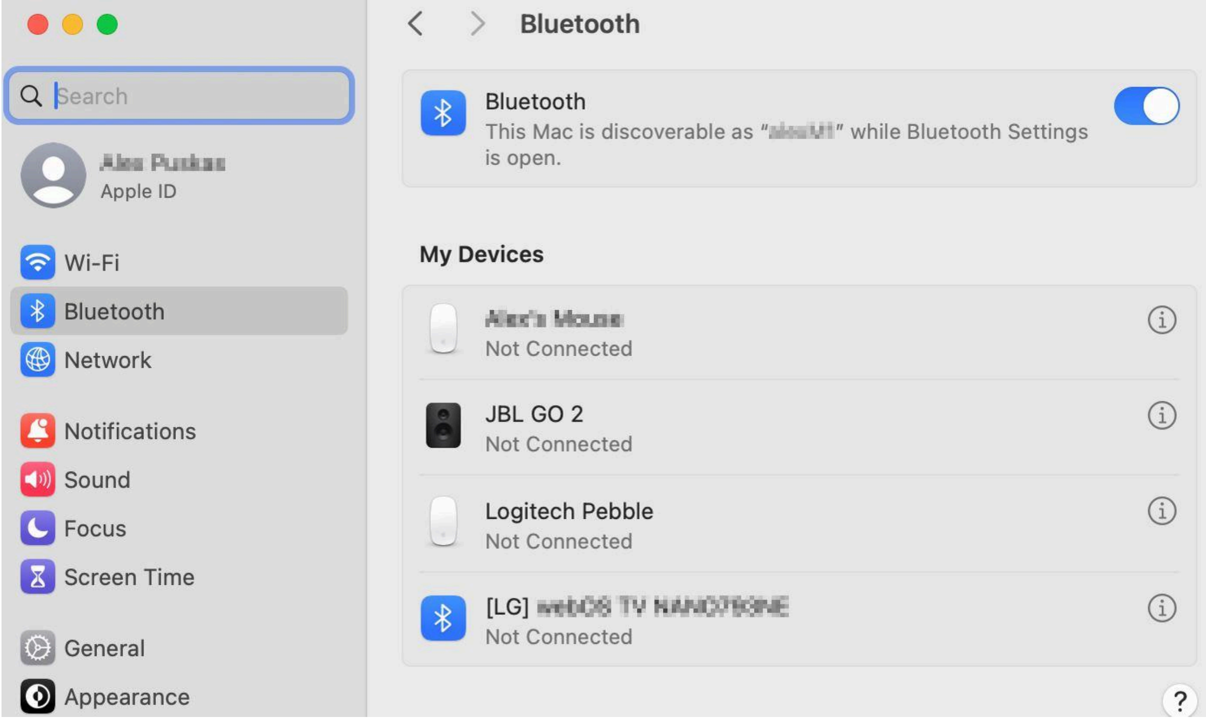
Depending on the device type, besides the Allow and Deny Access rights, additional rights are also available. These include Read-Only Access or multiple combinations of Allow Access but with various limitations, such as Allow access but exclude from CAP scanning or Allow Access if TrustedDevice Level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



Bluetooth

Bluetooth

This Mac is discoverable as "[redacted]" while Bluetooth Settings is open.

My Devices

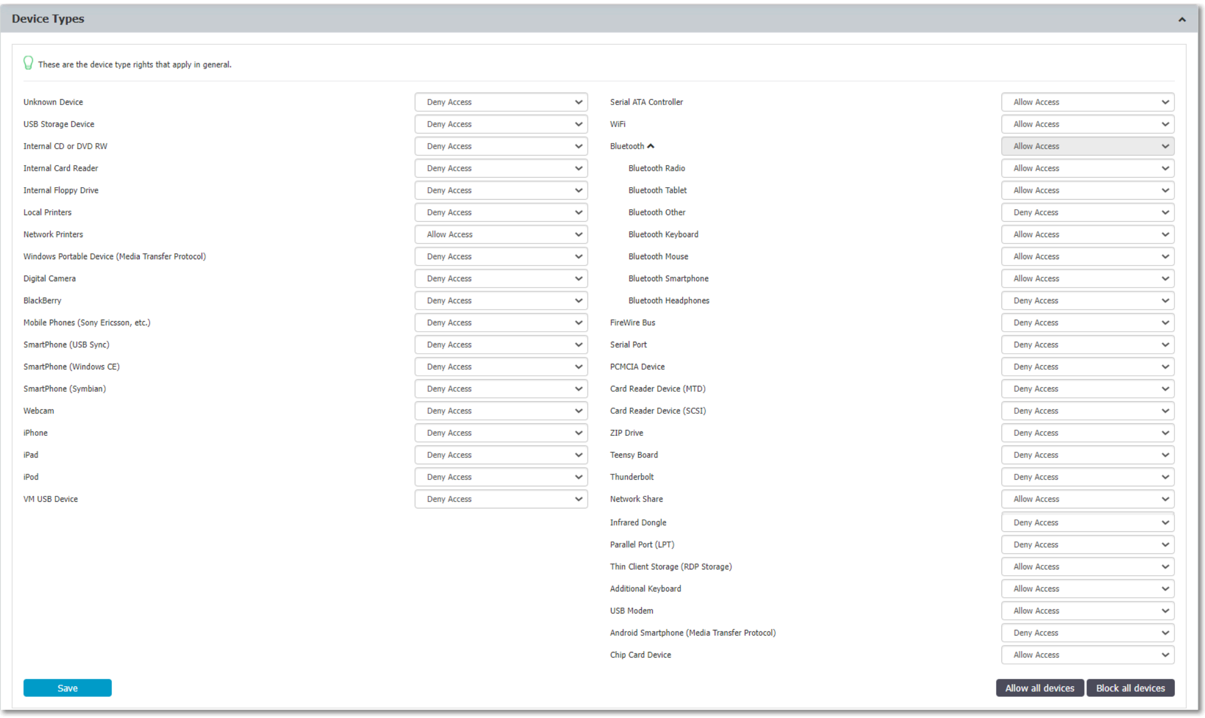
[redacted]
Not Connected

JBL GO 2
Not Connected

Logitech Pebble
Not Connected

[LG] [redacted]
Not Connected

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.



Device Types

These are the device type rights that apply in general.

Unknown Device	Deny Access	Serial ATA Controller	Allow Access
USB Storage Device	Deny Access	WiFi	Allow Access
Internal CD or DVD RW	Deny Access	Bluetooth ^	Allow Access
Internal Card Reader	Deny Access	Bluetooth Radio	Allow Access
Internal Floppy Drive	Deny Access	Bluetooth Tablet	Allow Access
Local Printers	Deny Access	Bluetooth Other	Deny Access
Network Printers	Allow Access	Bluetooth Keyboard	Allow Access
Windows Portable Device (Media Transfer Protocol)	Deny Access	Bluetooth Mouse	Allow Access
Digital Camera	Deny Access	Bluetooth Smartphone	Allow Access
BlackBerry	Deny Access	Bluetooth Headphones	Deny Access
Mobile Phones (Sony Ericsson, etc.)	Deny Access	FireWire Bus	Deny Access
SmartPhone (USB Sync)	Deny Access	Serial Port	Deny Access
SmartPhone (Windows CE)	Deny Access	PCMCIA Device	Deny Access
SmartPhone (Symbian)	Deny Access	Card Reader Device (MTD)	Deny Access
Webcam	Deny Access	Card Reader Device (SCSI)	Deny Access
iPhone	Deny Access	ZIP Drive	Deny Access
iPad	Deny Access	Teensy Board	Deny Access
iPod	Deny Access	Thunderbolt	Deny Access
VM USB Device	Deny Access	Network Share	Allow Access
		Infrared Dongle	Deny Access
		Parallel Port (LPT)	Deny Access
		Thin Client Storage (RDP Storage)	Allow Access
		Additional Keyboard	Allow Access
		USB Modem	Allow Access
		Android Smartphone (Media Transfer Protocol)	Deny Access
		Chip Card Device	Allow Access

5.6.1.1. VM USB Device Usage

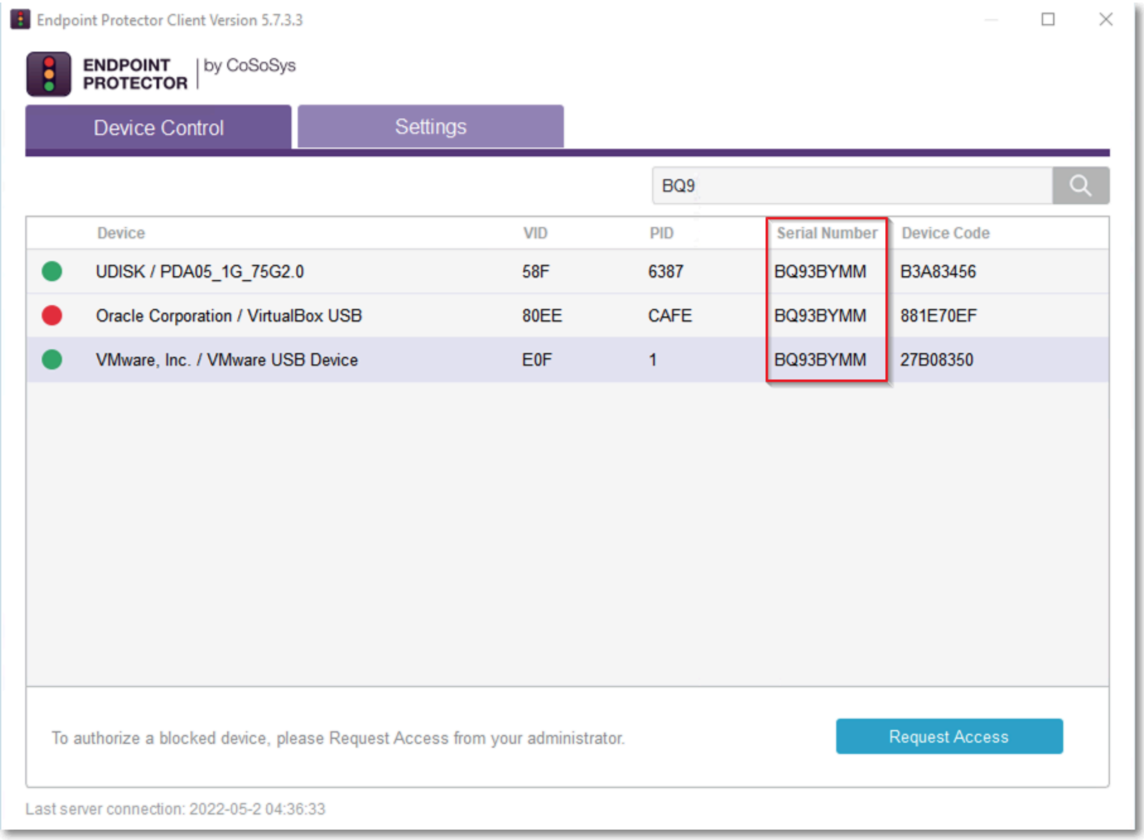
The VM USB device type extends Endpoint Protector applicability for VMWare and VirtualBox virtual environments.

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 Version 5.7.3.3
ENDPOINT PROTECTOR | by CoSoSys
Device Control
Settings
BQ9

	Device	VID	PID	Serial Number	Device Code
🟢	UDISK / PDA05_1G_75G2.0	58F	6387	BQ93BYMM	B3A83456
🔴	Oracle Corporation / VirtualBox USB	80EE	CAFE	BQ93BYMM	881E70EF
🟢	VMware, Inc. / VMware USB Device	E0F	1	BQ93BYMM	27B08350

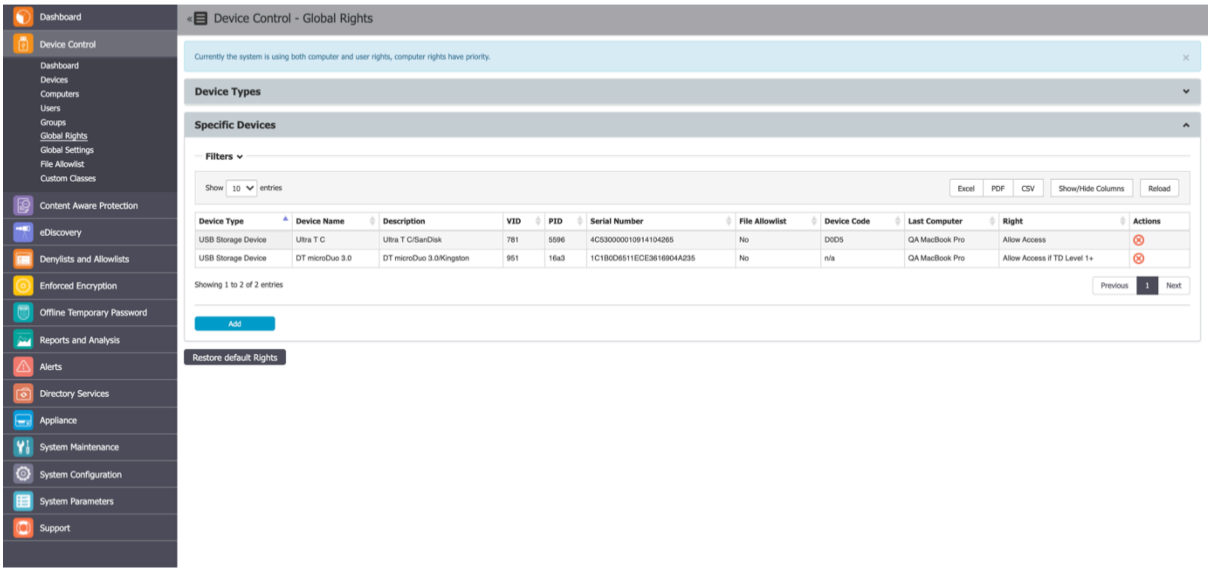
To authorize a blocked device, please Request Access from your administrator.

Last server connection: 2022-05-2 04:36:33

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.



Currently the system is using both computer and user rights, computer rights have priority.

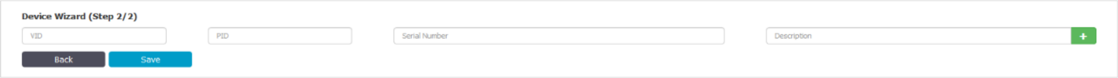
Device Type	Device Name	Description	VID	PID	Serial Number	File Allowlist	Device Code	Last Computer	Right	Actions
USB Storage Device	Ultra T C	Ultra T C/SanDisk	781	5596	4C530000010914104265	No	D0D5	QA MacBook Pro	Allow Access	⊗
USB Storage Device	DT microDuo 3.0	DT microDuo 3.0/Kingston	951	16a3	1C1B0D6511ECE3616904A235	No	n/a	QA MacBook Pro	Allow Access if TD Level 1+	⊗

Showing 1 to 2 of 2 entries

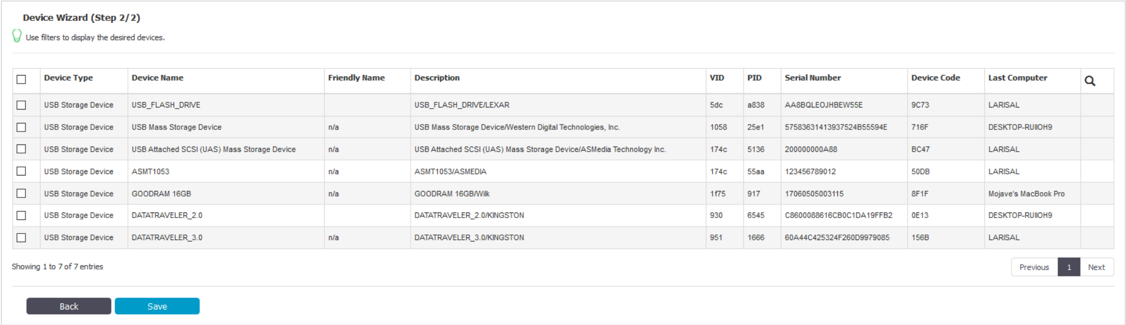
To add a new device click **Add** and provide the mandatory information.

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.

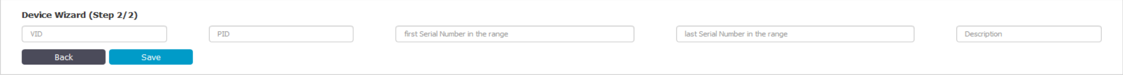


Use filters to display the desired devices.

☐	Device Type	Device Name	Friendly Name	Description	VID	PID	Serial Number	Device Code	Last Computer
☐	USB Storage Device	USB_FLASH_DRIVE		USB_FLASH_DRIVE/LEXAR	5dc	a838	AA8BQLEOJHBEW55E	9C73	LARISAL
☐	USB Storage Device	USB Mass Storage Device	n/a	USB Mass Storage Device/Western Digital Technologies, Inc.	1058	25e1	57583631413937524B55594E	716F	DESKTOP-RUIIOH9
☐	USB Storage Device	USB Attached SCSI (UAS) Mass Storage Device	n/a	USB Attached SCSI (UAS) Mass Storage Device/ASMedia Technology Inc.	174c	5136	200000000A88	BC47	LARISAL
☐	USB Storage Device	ASMT1053	n/a	ASMT1053/ASMEDIA	174c	55aa	123456789012	50DB	LARISAL
☐	USB Storage Device	GOODRAM 16GB	n/a	GOODRAM 16GB/Wilk	1f75	917	17060505003115	8F1F	Mojave's MacBook Pro
☐	USB Storage Device	DATATRAVELER_2.0		DATATRAVELER_2.0/KINGSTON	930	6545	C8600088616CB0C1DA19FFB2	0E13	DESKTOP-RUIIOH9
☐	USB Storage Device	DATATRAVELER_3.0	n/a	DATATRAVELER_3.0/KINGSTON	951	1666	60A44C425324F260D9979085	156B	LARISAL

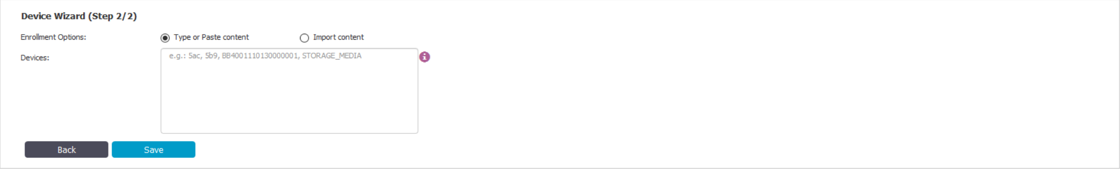
Showing 1 to 7 of 7 entries

- **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 (Step 2/2)
VID
PID
first Serial Number in the range
last Serial Number in the range
Description
Back
Save

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.



Device Wizard (Step 2/2)

Enrollment Options: ● Type or Paste content ○ Import content

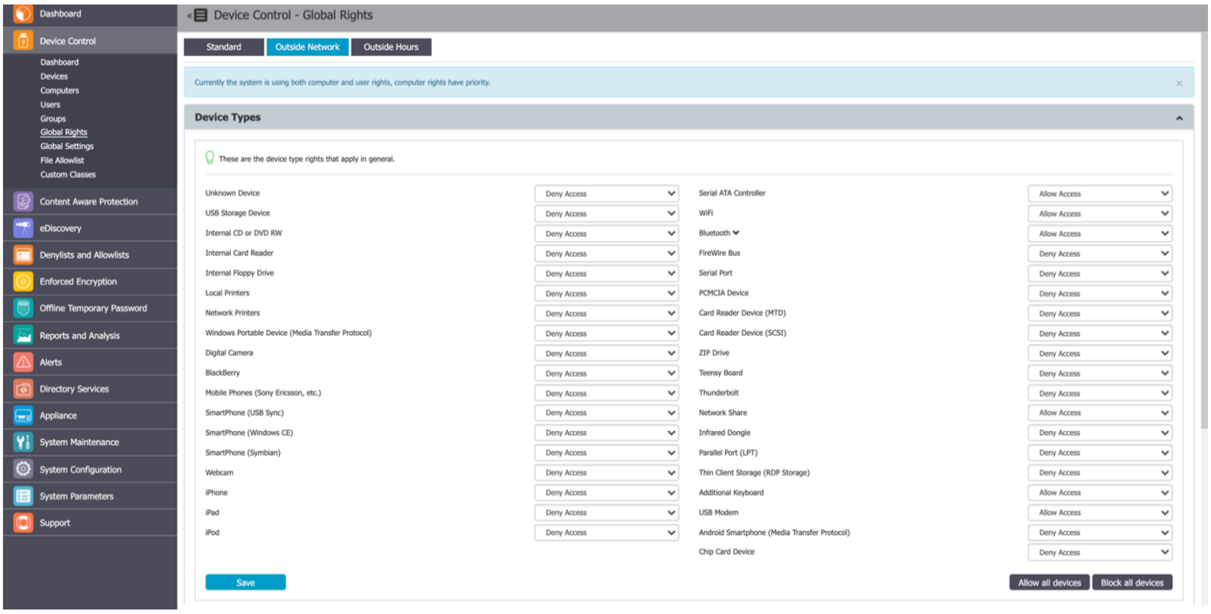
Devices: e.g.: 5ac, 5b9, BB4001110130000001, STORAGE_MEDIA

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.



Device Control - Global Rights

Currently the system is using both computer and user rights, computer rights have priority.

Device Types

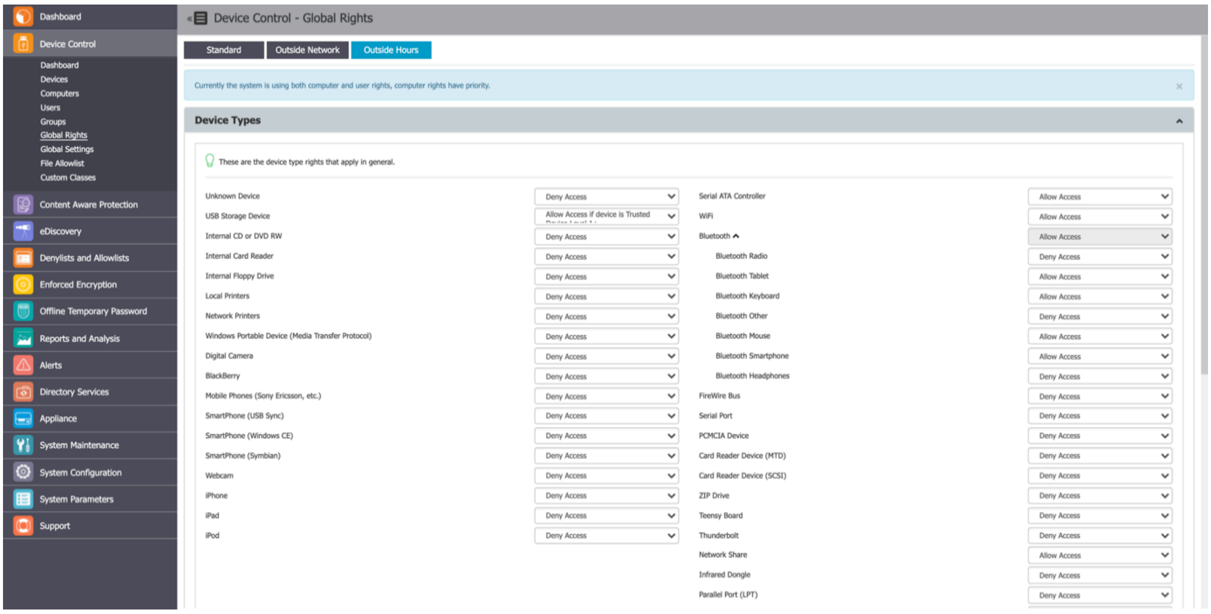
These are the device type rights that apply in general.

Unknown Device	Deny Access	Serial ATA Controller	Allow Access
USB Storage Device	Deny Access	WiFi	Allow Access
Internal CD or DVD RW	Deny Access	Bluetooth	Allow Access
Internal Card Reader	Deny Access	FireWire Bus	Deny Access
Internal Floppy Drive	Deny Access	Serial Port	Deny Access
Local Printers	Deny Access	PCMCIA Device	Deny Access
Network Printers	Deny Access	Card Reader Device (MTD)	Deny Access
Windows Portable Device (Media Transfer Protocol)	Deny Access	Card Reader Device (SCSI)	Deny Access
Digital Camera	Deny Access	ZIP Drive	Deny Access
BlackBerry	Deny Access	Teensy Board	Deny Access
Mobile Phones (Sony Ericsson, etc.)	Deny Access	Thunderbolt	Deny Access
SmartPhone (USB Sync)	Deny Access	Network Share	Allow Access
SmartPhone (Windows CE)	Deny Access	Infrared Dongle	Deny Access
SmartPhone (Symbian)	Deny Access	Parallel Port (LPT)	Deny Access
Webcam	Deny Access	Thin Client Storage (RDP Storage)	Deny Access
iPhone	Deny Access	Additional Keyboard	Allow Access
iPad	Deny Access	USB Modem	Allow Access
iPod	Deny Access	Android Smartphone (Media Transfer Protocol)	Deny Access
		Chip Card Device	Deny Access

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.



Device Control - Global Rights

Currently the system is using both computer and user rights, computer rights have priority.

Device Types

These are the device type rights that apply in general.

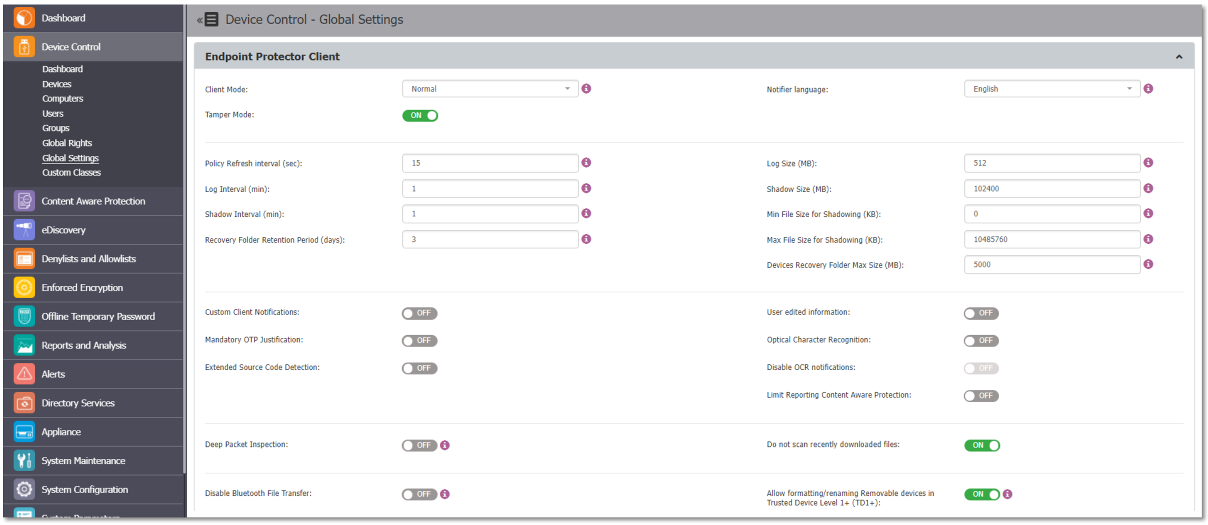
Unknown Device	Deny Access	Serial ATA Controller	Allow Access
USB Storage Device	Allow Access if device is Trusted	WiFi	Allow Access
Internal CD or DVD RW	Deny Access	Bluetooth	Allow Access
Internal Card Reader	Deny Access	Bluetooth Radio	Deny Access
Internal Floppy Drive	Deny Access	Bluetooth Tablet	Allow Access
Local Printers	Deny Access	Bluetooth Keyboard	Allow Access
Network Printers	Deny Access	Bluetooth Other	Deny Access
Windows Portable Device (Media Transfer Protocol)	Deny Access	Bluetooth Mouse	Allow Access
Digital Camera	Deny Access	Bluetooth Smartphone	Allow Access
BlackBerry	Deny Access	Bluetooth Headphones	Deny Access
Mobile Phones (Sony Ericsson, etc.)	Deny Access	FireWire Bus	Deny Access
SmartPhone (USB Sync)	Deny Access	Serial Port	Deny Access
SmartPhone (Windows CE)	Deny Access	PCMCIA Device	Deny Access
SmartPhone (Symbian)	Deny Access	Card Reader Device (MTD)	Deny Access
Webcam	Deny Access	Card Reader Device (SCSI)	Deny Access
iPhone	Deny Access	ZIP Drive	Deny Access
iPad	Deny Access	Teensy Board	Deny Access
iPod	Deny Access	Thunderbolt	Deny Access
		Network Share	Allow Access
		Infrared Dongle	Deny Access
		Parallel Port (LPT)	Deny Access

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.).



Device Control - Global Settings

Endpoint Protector Client

Client Mode:	Normal	Notifier language:	English
Tamper Mode:	ON		
Policy Refresh interval (sec):	15	Log Size (MB):	512
Log Interval (min):	1	Shadow Size (MB):	102400
Shadow Interval (min):	1	Min File Size for Shadowing (KB):	0
Recovery Folder Retention Period (days):	3	Max File Size for Shadowing (KB):	10485760
		Devices Recovery Folder Max Size (MB):	5000
Custom Client Notifications:	OFF	User edited information:	OFF
Mandatory OTP Justification:	OFF	Optical Character Recognition:	OFF
Extended Source Code Detection:	OFF	Disable OCR notifications:	OFF
		Limit Reporting Content Aware Protection:	OFF
Deep Packet Inspection:	OFF	Do not scan recently downloaded files:	ON
Disable Bluetooth File Transfer:	OFF	Allow formatting/renaming Removable devices in Trusted Device Level 1+ (TD1+):	ON

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.

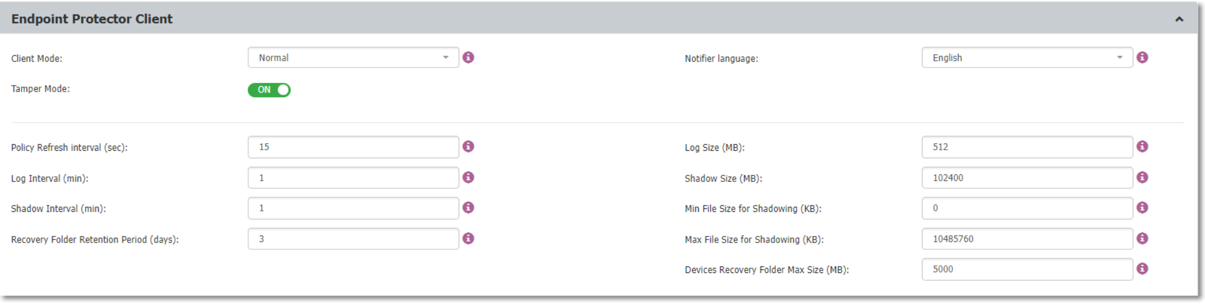
- **Log Interval (min) –** enter the time interval at which the Client attempts to re-send the Logs to the Server.

- **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.



Endpoint Protector Client

Client Mode: Normal

Notifier language: English

Tamper Mode: ON

Policy Refresh interval (sec): 15

Log Interval (min): 1

Shadow Interval (min): 1

Recovery Folder Retention Period (days): 3

Log Size (MB): 512

Shadow Size (MB): 102400

Min File Size for Shadowing (KB): 0

Max File Size for Shadowing (KB): 10485760

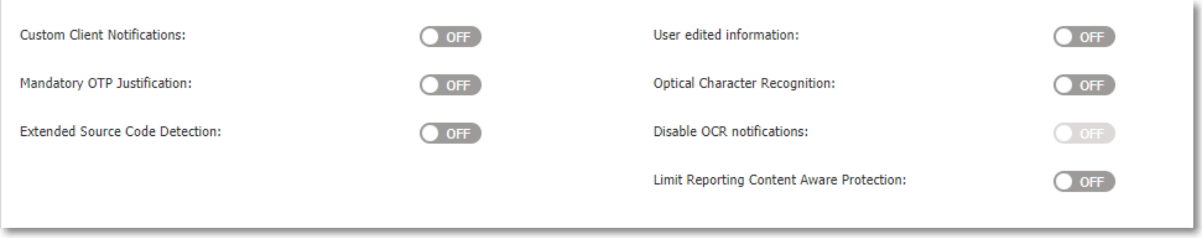
Devices Recovery Folder Max Size (MB): 5000

- **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.



Custom Client Notifications: OFF

Mandatory OTP Justification: OFF

Extended Source Code Detection: OFF

User edited information: OFF

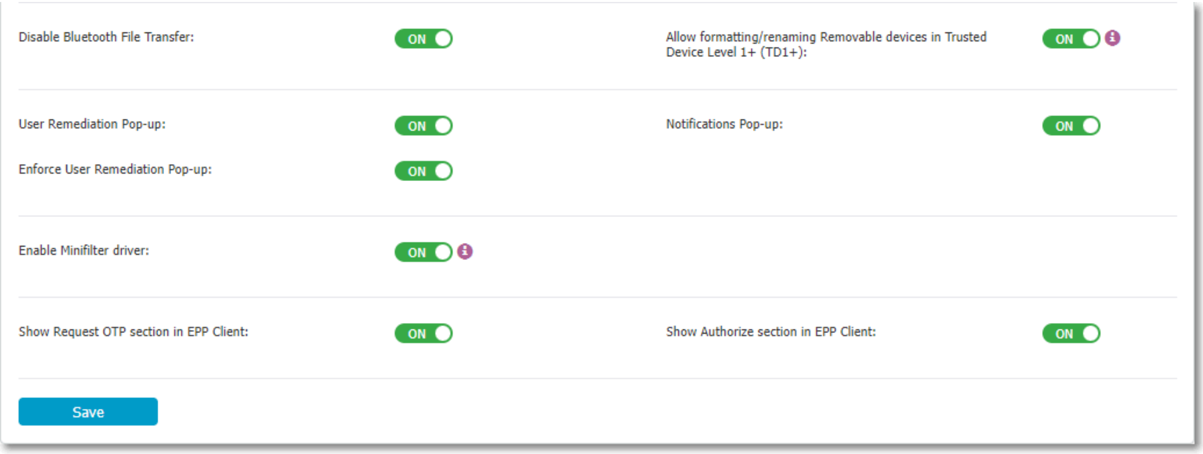
Optical Character Recognition: OFF

Disable OCR notifications: OFF

Limit Reporting Content Aware Protection: OFF

- **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.
- **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



Disable Bluetooth File Transfer: ON

Allow formatting/renaming Removable devices in Trusted Device Level 1+ (TD1+): ON

User Remediation Pop-up: ON

Notifications Pop-up: ON

Enforce User Remediation Pop-up: ON

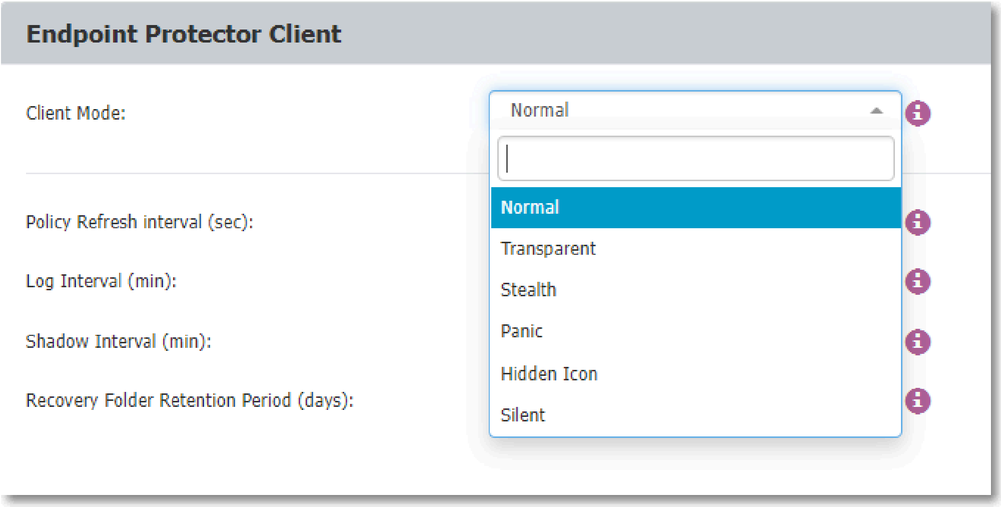
Enable Minifilter driver: ON

Show Request OTP section in EPP Client: ON

Show Authorize section in EPP Client: ON

5.7.1.1. Client Mode

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



Endpoint Protector Client

Client Mode: Normal

Policy Refresh interval (sec):

Log Interval (min):

Shadow Interval (min):

Recovery Folder Retention Period (days):

1. **Normal** – this is the default and recommended setting to use before being fully aware of what the other modes imply. Normal mode does not apply to Content Aware Protection; all other client modes, except Silent mode, are specific to device control.

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. Transparent mode does not apply to Content Aware Protection; all other client modes, except Silent mode, are specific to device control.

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 discreetly monitor users and computers with a focus on device control and file-tracing. Stealth mode does not apply to Content Aware Protection; all other client modes, except Silent mode, are specific to device control.

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. Panic mode does not apply to Content Aware Protection; all other client modes, except Silent mode, are specific to device control.

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. Hidden Icon mode does not apply to Content Aware Protection; all other client modes, except Silent mode, are specific to device control.

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. DPI Configuration

In this section, you can manage the following settings:

- **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.
- **EPP Behavior with Network Extension Off** – select a behavior type from the available entries
- **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.
  - Ignore Expiration Date - when checked, expired certificates will be ignored and traffic will be permitted.
  - Ignore Trust - when checked, certificates will not be validated against the Root Certificate.
  - Ignore Hostname - when checked, the certificate hostname property will not be validated against the server hostname.

Important: Disabling setting '**Peer Certificate Validation**' 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.

- **Display Dialog Boxes for DPI Dropped Connections** - enable this setting to display Dialog windows on endpoint machines, containing more details.
- **Disable DPI Dropped Connections Notifications** - check this setting to suppress notifications shown by the Notification Center nearby the System tray.
- **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.

- **DPI Bypass Traffic** – this setting automatically bypasses non-inspectable traffic and sends an event for allowed traffic.
    - Possible Bypass reasons:
        - Bypass DPI Certificate Rejection by Third-Party Applications
            - Enable this setting, if SSL errors are encountered from the source applications, such as web browsers, like:
                - SSL_R_TLSV1_ALERT_UNKNOWN_CA
                - SSL_R_SSLV3_ALERT_CERTIFICATE_UNKNOWN
            - This signifies that the source application failed to validate the server certificate, which was issued by Endpoint Protector.
            - The absence of the DPI certificate in the system keychain may also contribute to this scenario.
            - ‘Certificate Pinning’ also falls under this category.

Note: Learn more about Using Wireshark for Network Traffic Analysis.

- Bypass Unknown TLS Handshakes
    - Enable this setting, when a secure port connection employs custom encryption instead of TLS, the DPI bypass is activated.
        - This is exemplified by configuring Telegram.app for DPI monitoring, logging into the app, and encountering an unknown TLS handshake.
- Bypass Websites Temporarily Whitelisted (Possible mTLS Connection/SSL Setup Failure/Unsupported TLS Protocol)
    - Enable this setting where an SSL setup failure or an unsupported TLS protocol error occurs on the server side of an SSL connection. EPP temporarily allow-lists the website.
        - While specific examples are infrequent, such instances involve potential mTLS connections.
- Bypass Websockets
    - Enable this setting, when Websites utilize websockets with arbitrary data protocols.
        - EPP passthroughs connections upon the HTTP connection's upgrade to a websocket.

        - Examples are applications, such as WhatsApp Web, Firefox Send etc.

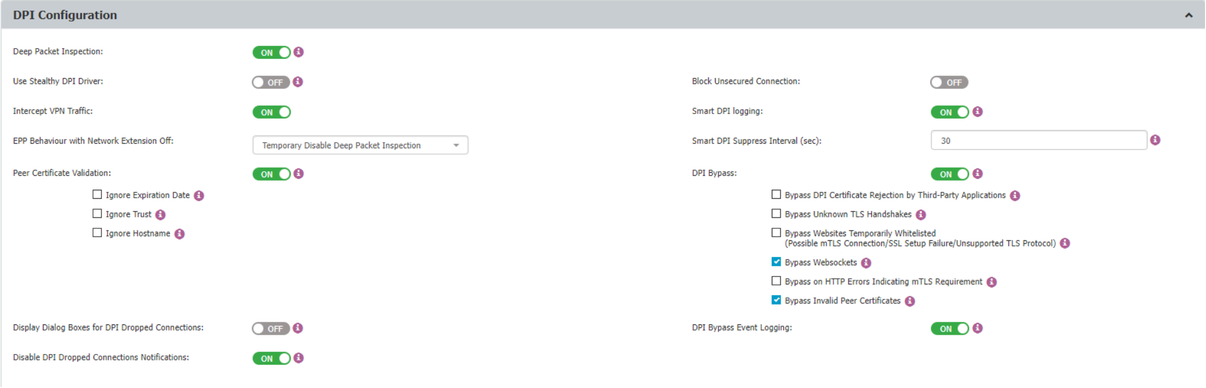
    - Bypass on HTTP Errors Indicating mTLS Requirement
        - Enable this setting, when a server indicates the requirement of a client certificate (mTLS).
            - EPP triggers bypass for HTTP error codes like '*400 Bad Response*' and '*496 SSL Certificate Required*'.
            - Accessing https://client.badssl.com/ from a web browser without providing the necessary client certificate illustrates such situations.
    - Bypass Invalid Peer Certificates
        - Enable this setting, to permit connections with invalid peer certificates when 'Peer Certificate Validation' is enabled.
            - If both 'Bypass Invalid Peer Certificates' and 'Peer Certificate Validation' are enabled, 'Bypass Invalid Peer Certificates' will override setting 'Peer Certificate Validation'.
            - Accessing https://expired.badssl.com/ from a web browser with both settings 'Bypass Invalid Peer Certificates' and 'Peer Certificate Validation' enabled, illustrates such situations (the website will be accessible).

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.

Note: Learn more about Timeout Period for Bypassed Websites, and Handling of Bypassed Domains and Applications.

- **DPI Bypass Event Logging** – this setting will automatically send DPI Bypass events/reasons to EPP Server when connections are being bypassed on endpoints.

  Note: Learn more about Bypass Log Reporting Frequency.



DPI Configuration

Deep Packet Inspection: ON

Use Stealthy DPI Driver: OFF

Intercept VPN Traffic: ON

EPP Behaviour with Network Extension Off: Temporary Disable Deep Packet Inspection

Peer Certificate Validation: ON

- □ Ignore Expiration Date
- □ Ignore Trust
- □ Ignore Hostname

Display Dialog Boxes for DPI Dropped Connections: OFF

Disable DPI Dropped Connections Notifications: ON

Block Unsecured Connection: OFF

Smart DPI logging: ON

Smart DPI Suppress Interval (sec): 30

DPI Bypass: ON

- □ Bypass DPI Certificate Rejection by Third-Party Applications
- □ Bypass Unknown TLS Handshakes
- □ Bypass Websites Temporarily Whitelisted (Possible mTLS Connection/SSL Setup Failure/Unsupported TLS Protocol)
- ☑ Bypass Websockets
- □ Bypass on HTTP Errors Indicating mTLS Requirement
- ☑ Bypass Invalid Peer Certificates

DPI Bypass Event Logging: ON

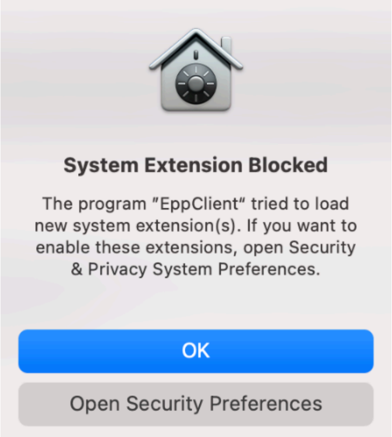
5.7.2.1. Intercept VPN Traffic

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:

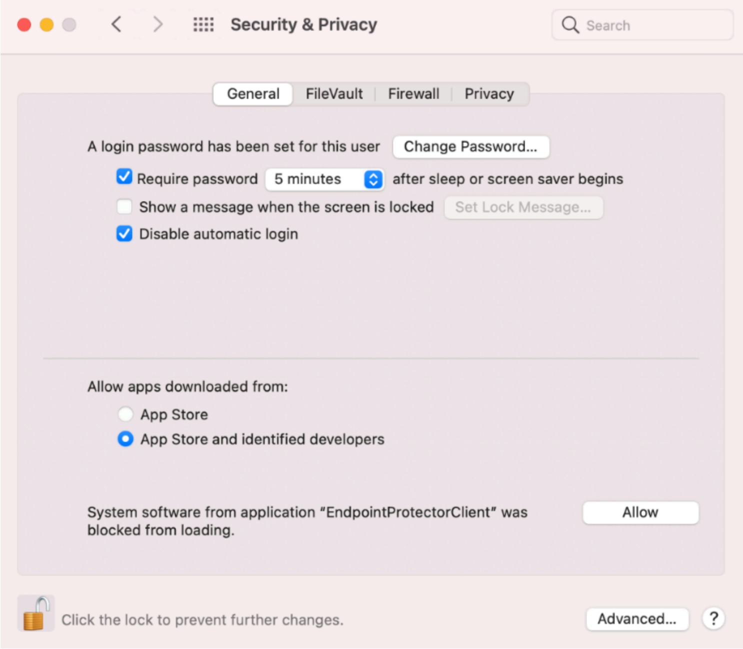
1. Enable **Deep Packet Inspection**
2. Enable **Intercept VPN Traffic**
3. Select an option for **EPP behavior when network extension is disabled**
   - **Temporary Disable Deep Packet Inspection** – this will disable Deep Packet Inspection temporary
   - **Block Internet Access -** this will block 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;



System Extension Blocked

The program "EppClient" tried to load new system extension(s). If you want to enable these extensions, open Security & Privacy System Preferences.

6. Go to **System Preferences**, **Security and Privacy**, **General,** and then allow the Endpoint Protector Client Extension;



A login password has been set for this user

☑ Require password 5 minutes after sleep or screen saver begins

☐ Show a message when the screen is locked

☑ Disable automatic login

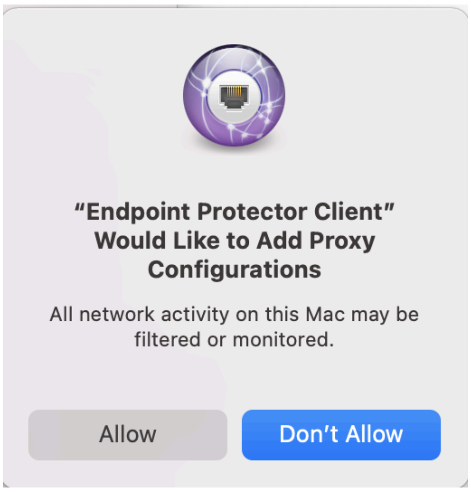
Allow apps downloaded from:

○ App Store

● App Store and identified developers

System software from application "EndpointProtectorClient" was blocked from loading.

7. On the Endpoint Protector Proxy Configuration pop-up window, click **Allow**;

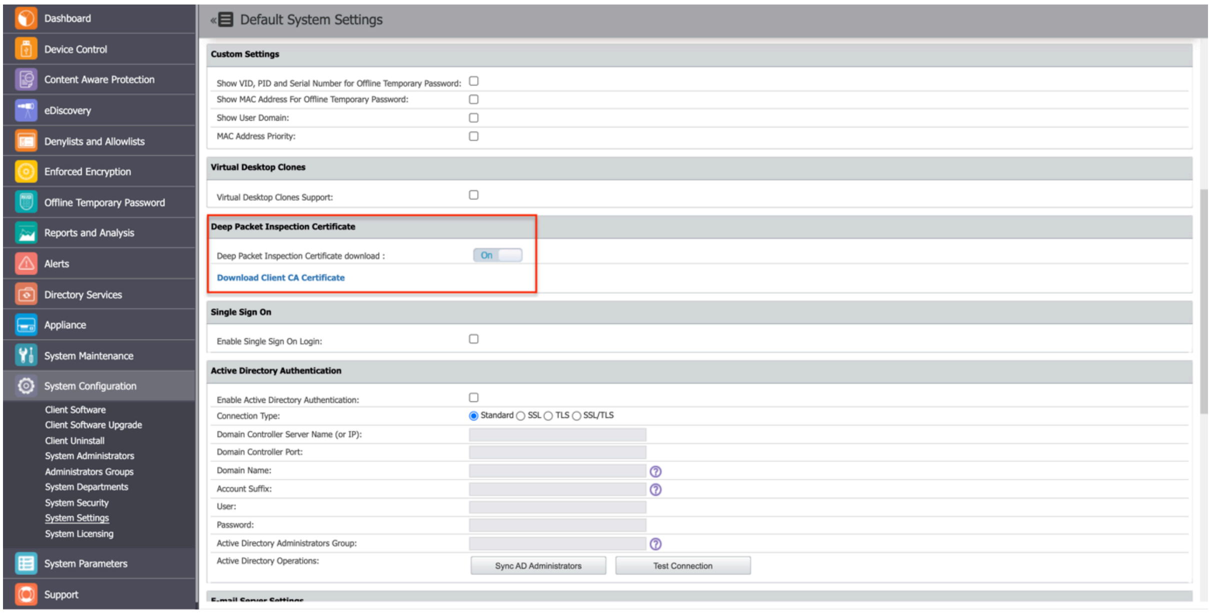


"Endpoint Protector Client" Would Like to Add Proxy Configurations

All network activity on this Mac may be filtered or monitored.

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**;



Default System Settings

Custom Settings

Show VID, PID and Serial Number for Offline Temporary Password: □
Show MAC Address For Offline Temporary Password: □
Show User Domain: □
MAC Address Priority: □

Virtual Desktop Clones

Virtual Desktop Clones Support: □

Deep Packet Inspection Certificate

Deep Packet Inspection Certificate download : On
Download Client CA Certificate

Single Sign On

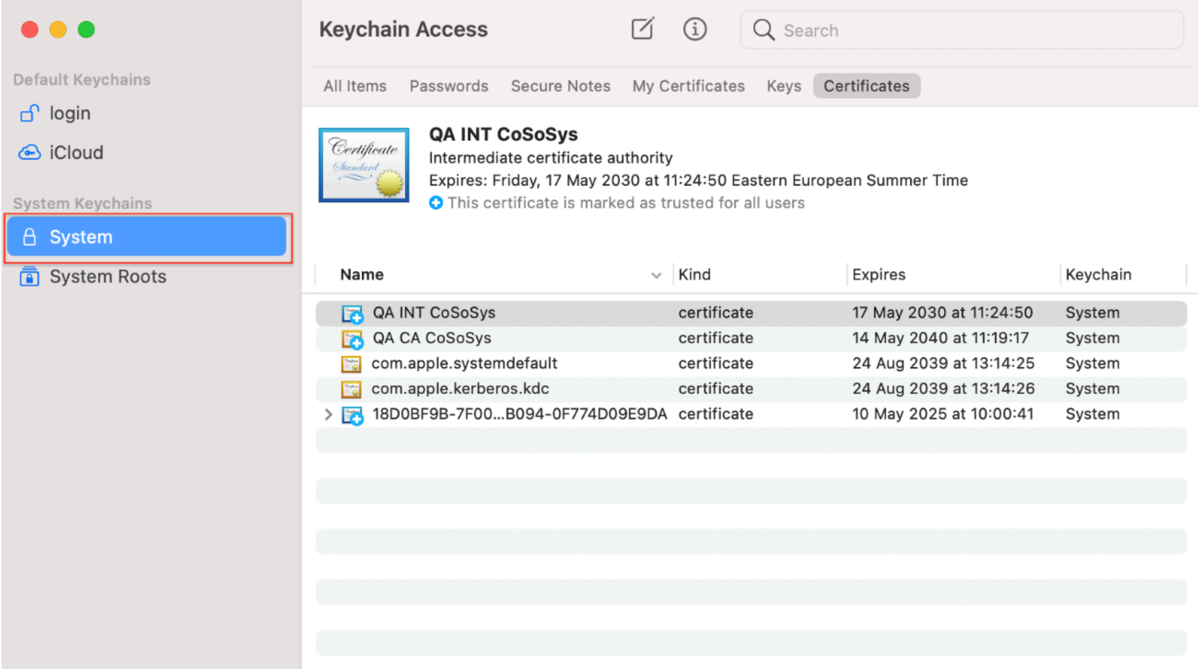
Enable Single Sign On Login: □

Active Directory Authentication

Enable Active Directory Authentication: □
Connection Type: ● Standard ○ SSL ○ TLS ○ SSL/TLS
Domain Controller Server Name (or IP):
Domain Controller Port:
Domain Name:
Account Suffix:
User:
Password:
Active Directory Administrators Group:
Active Directory Operations: Sync AD Administrators | Test Connection

E-mail Server Settings

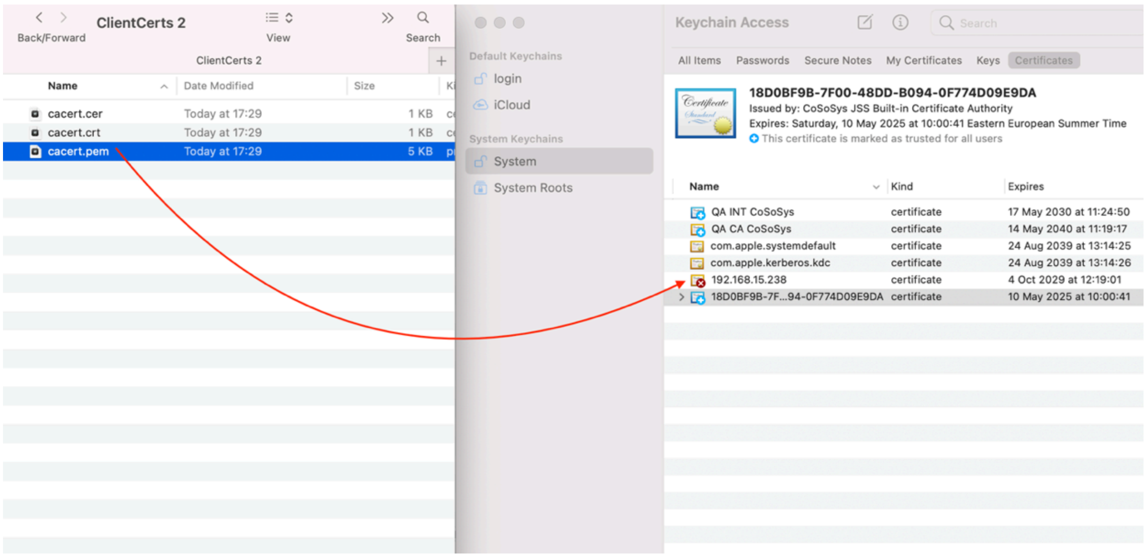
9. On your macOS, open the **Keychain Access** application and go to **System**;



QA INT CoSoSys
Intermediate certificate authority
Expires: Friday, 17 May 2030 at 11:24:50 Eastern European Summer Time
This certificate is marked as trusted for all users

Name	Kind	Expires	Keychain
QA INT CoSoSys	certificate	17 May 2030 at 11:24:50	System
QA CA CoSoSys	certificate	14 May 2040 at 11:19:17	System
com.apple.systemdefault	certificate	24 Aug 2039 at 13:14:25	System
com.apple.kerberos.kdc	certificate	24 Aug 2039 at 13:14:26	System
18D0BF9B-7F00...B094-0F774D09E9DA	certificate	10 May 2025 at 10:00:41	System

10. Decompress the **ClientCerts** file;
11. Select the **cacert.pem** file and drag and drop it on **Keychain Access**, **System;**

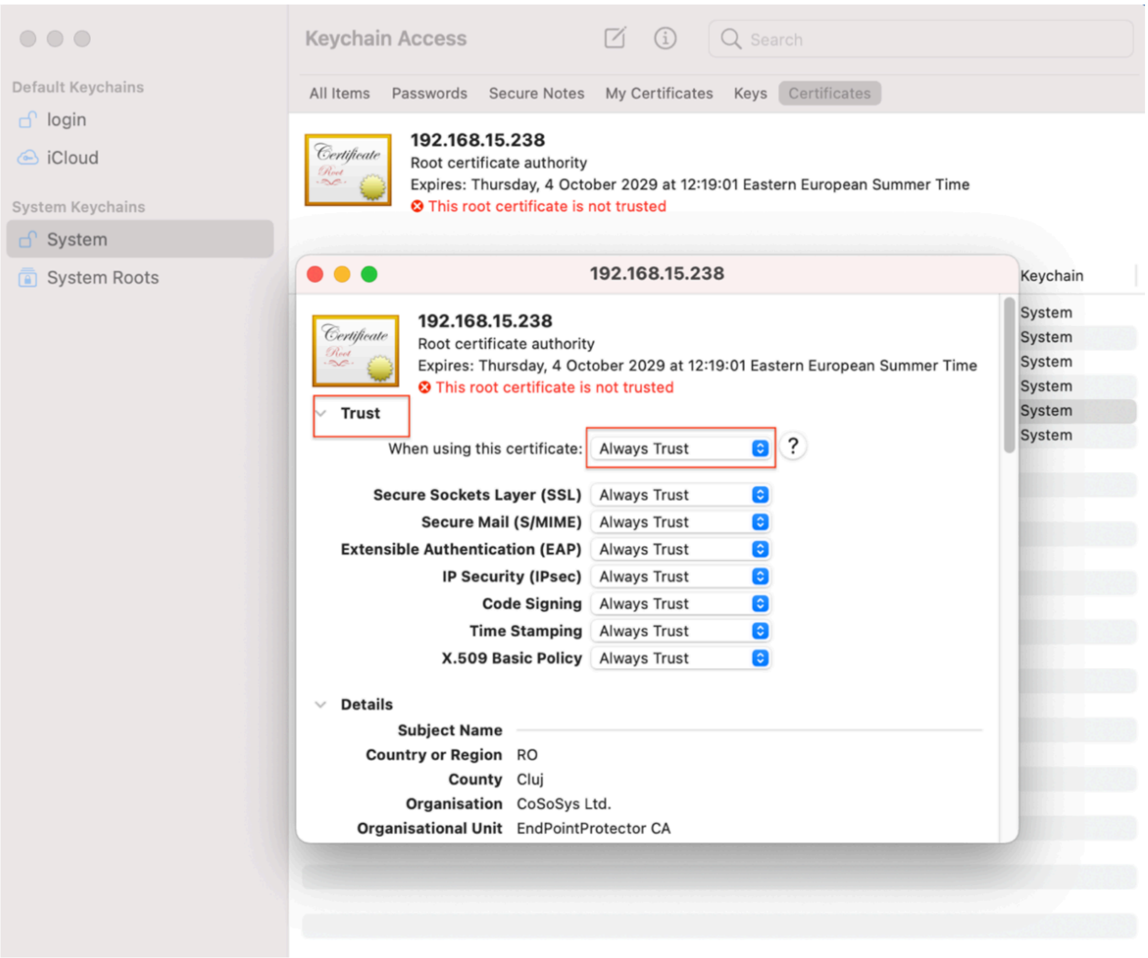


Name	Date Modified	Size
cacert.cer	Today at 17:29	1 KB
cacert.crt	Today at 17:29	1 KB
cacert.pem	Today at 17:29	5 KB

18D0BF9B-7F00-48DD-B094-0F774D09E9DA
Issued by: CoSoSys JSS Built-in Certificate Authority
Expires: Saturday, 10 May 2025 at 10:00:41 Eastern European Summer Time
This certificate is marked as trusted for all users

Name	Kind	Expires
QA INT CoSoSys	certificate	17 May 2030 at 11:24:50
QA CA CoSoSys	certificate	14 May 2040 at 11:19:17
com.apple.systemdefault	certificate	24 Aug 2039 at 13:14:25
com.apple.kerberos.kdc	certificate	24 Aug 2039 at 13:14:26
192.168.15.238	certificate	4 Oct 2029 at 12:19:01
18D0BF9B-7F...94-0F774D09E9DA	certificate	10 May 2025 at 10:00:41

12. Double click the **X** from the newly added certificate and select **Always Trust** from the **Trust** section;



192.168.15.238
Root certificate authority
Expires: Thursday, 4 October 2029 at 12:19:01 Eastern European Summer Time
This root certificate is not trusted

192.168.15.238

192.168.15.238
Root certificate authority
Expires: Thursday, 4 October 2029 at 12:19:01 Eastern European Summer Time
This root certificate is not trusted

Trust

When using this certificate: Always Trust

Secure Sockets Layer (SSL) Always Trust
Secure Mail (S/MIME) Always Trust
Extensible Authentication (EAP) Always Trust
IP Security (IPsec) Always Trust
Code Signing Always Trust
Time Stamping Always Trust
X.509 Basic Policy Always Trust

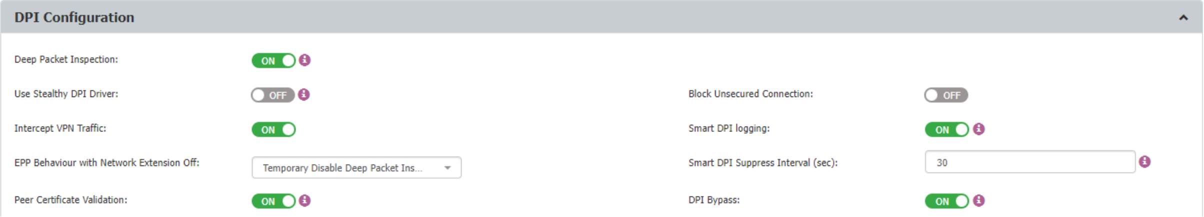
Details

Subject Name
Country or Region RO
County Cluj
Organisation CoSoSys Ltd.
Organisational Unit EndPointProtector CA

13. **Save** the changes.

5.7.2.2. 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.



DPI Configuration

Deep Packet Inspection: ON

Use Stealthy DPI Driver: OFF

Intercept VPN Traffic: ON

EPP Behaviour with Network Extension Off: Temporary Disable Deep Packet Ins...

Peer Certificate Validation: ON

Block Unsecured Connection: OFF

Smart DPI logging: ON

Smart DPI Suppress Interval (sec): 30

DPI Bypass: ON

5.7.2.3. Bypass Log Reporting Frequency

EPP's agent ensures efficient resource utilization by reporting each domain name and application pair at most once every two weeks. This approach prevents an overwhelming influx of logs, which could reach excessive numbers if reported more frequently.

5.7.2.4. Timeout Period for Bypassed Websites

To maintain a streamlined process, EPP enforces a timeout period of two weeks. During this timeframe, the state for bypassed websites is retained. Beyond this period, the bypass state is automatically removed, contributing to effective resource management.

5.7.2.5. Handling of Bypassed Domains and Applications

EPP employs a nuanced approach to handle bypassed domains and applications:

5.7.2.5.1. Memory and Disk Persistence

Bypassed website information is stored in both memory and on disk. This dual storage ensures that the list of skipped websites is readily accessible for efficient future reference. By persisting this information, the frequency of log generation can be controlled to avoid unnecessary strain on resources.

5.7.2.5.2. Clearing Bypass State

To reset the bypass state and clear associated records, administrators can initiate a simple process. Temporarily disabling and subsequently re-enabling the bypass DPI setting on the EPP server achieves this reset.

5.7.2.6. Using Wireshark for Network Traffic Analysis

Prior to a "DPI certificate rejected" event, Wireshark can be instrumental in diagnosing network traffic. The presence of a "TLS alert" error in Wireshark signals the impending event.

5.7.3. 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.

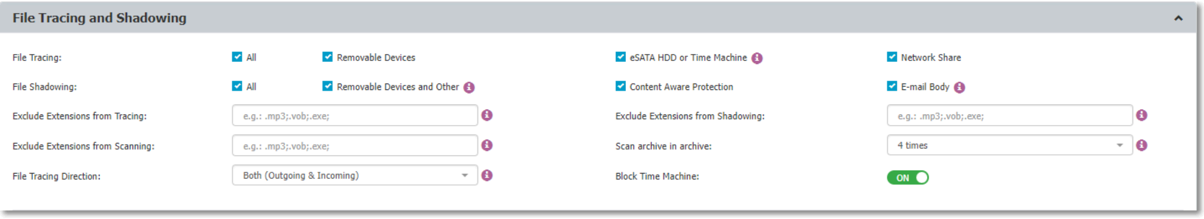
Note: For your deployment, we strongly advise activating File Shadowing for not more than 15% of your total endpoint capacity (e.g., for a 1000 endpoint deployment, File Shadowing should be set to a maximum of 150 endpoints for optimal performance). For more users, please contact customer support for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

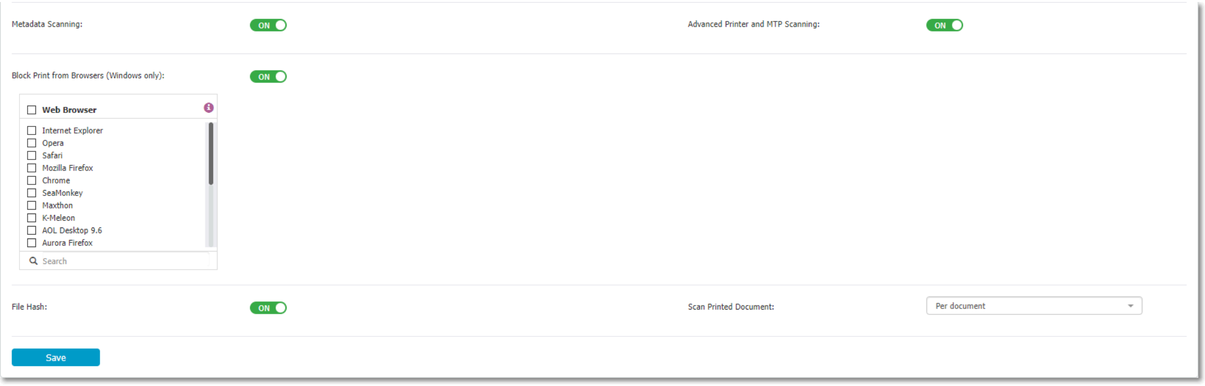
- **Exclude Extensions from Shadowing** – use this setting to disable File Shadowing for specific file types.
- **Scan archive in archive** – use this setting to define the archive depth in which content is inspected.
- **Block Time Machine** – if you enable this setting, you will block Time Machine backups on macOS.



File Tracing and Shadowing

File Tracing:	☑ All	☑ Removable Devices	☑ eSATA HDD or Time Machine	☑ Network Share
File Shadowing:	☑ All	☑ Removable Devices and Other	☑ Content Aware Protection	☑ E-mail Body
Exclude Extensions from Tracing:	e.g.: .mp3;.vob;.exe;		Exclude Extensions from Shadowing:	e.g.: .mp3;.vob;.exe;
Exclude Extensions from Scanning:	e.g.: .mp3;.vob;.exe;		Scan archive in archive:	4 times
File Tracing Direction:	Both (Outgoing & Incoming)		Block Time Machine:	ON

- **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.



Metadata Scanning: ON

Advanced Printer and MTP Scanning: ON

Block Print from Browsers (Windows only): ON

☐ Web Browser

☐ Internet Explorer
☐ Opera
☐ Safari
☐ Mozilla Firefox
☐ Chrome
☐ SeaMonkey
☐ Maxthon
☐ K-Meleon
☐ AOL Desktop 9.6
☐ Aurora Firefox

Search

File Hash: ON

Scan Printed Document: Per document

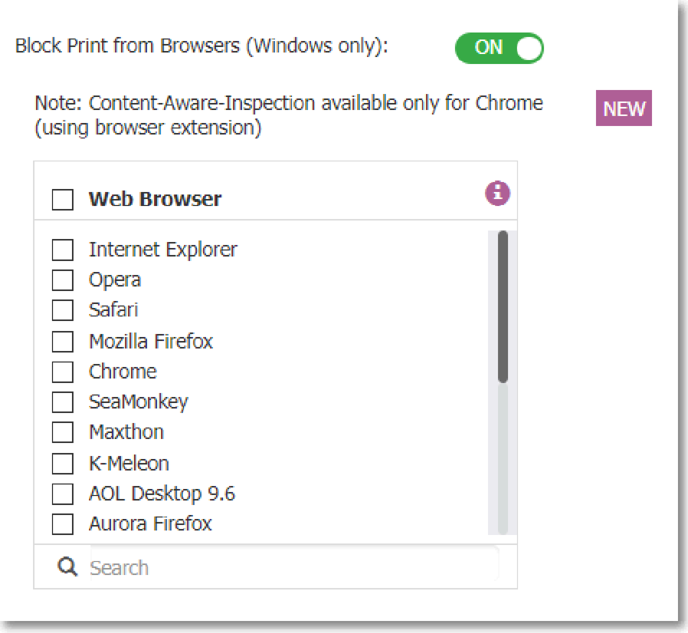
Important: Newer Linux Ubuntu versions have 'snap'-based applications installed by default, affecting EPP Client functionality. This may result in missing file-related events in File Tracing and File Shadow artifacts. The reliance on 'snap'-based applications also affects file-related web browser activities, exacerbating this limitation. Consider non-’snap’-based applications (where possible) as alternative configurations for optimal functionality.

5.7.3.1. 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: 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.



Block Print from Browsers (Windows only): ON

Note: Content-Aware-Inspection available only for Chrome (using browser extension)

☐ Web Browser

☐ Internet Explorer
☐ Opera
☐ Safari
☐ Mozilla Firefox
☐ Chrome
☐ SeaMonkey
☐ Maxthon
☐ K-Meleon
☐ AOL Desktop 9.6
☐ Aurora Firefox

Search

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.

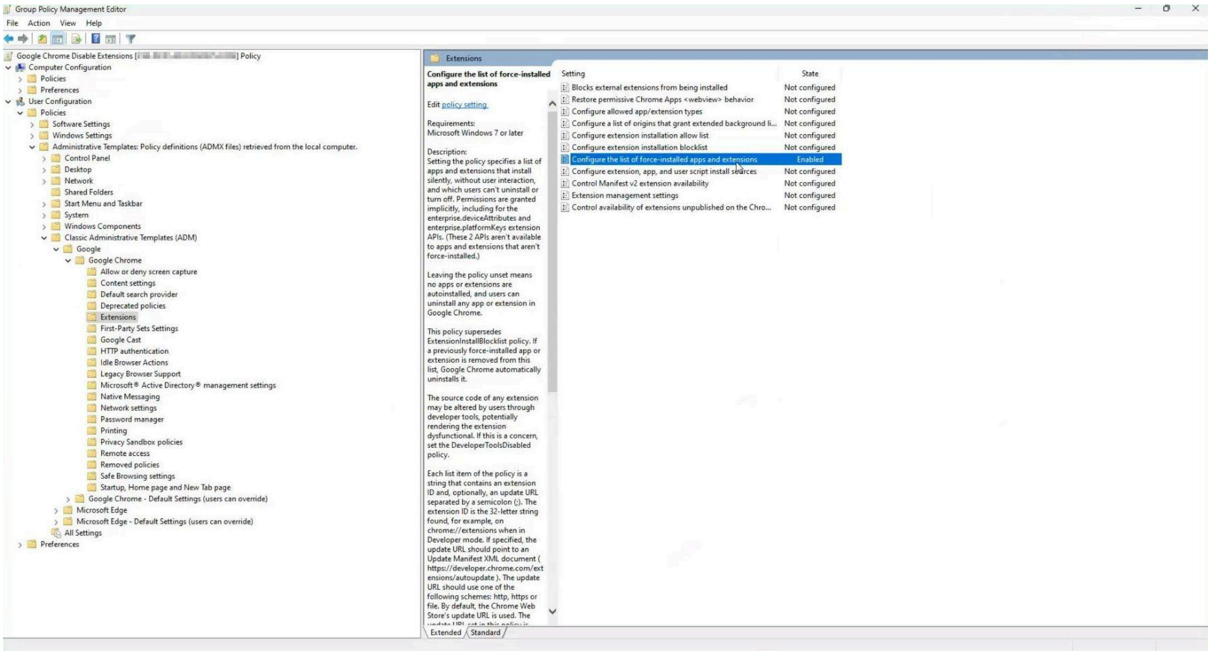
Important: Use the Group Policies to set PDF files to be downloaded instead of opened in the web browser for the block print from the browser to function accurately.

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

5.7.3.2. 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: **nnnaeanocbmnnjjlcfhcbpefmlgbcgoi**



Configure the list of force-installed apps and extensions

Edit policy setting

Requirements:
Microsoft Windows 7 or later

Description:
Setting the policy specifies a list of apps and extensions that install silently, without user interaction, and which users can't uninstall or turn off. Permissions are granted implicitly, including for the enterprise.deviceAttributes and enterprise.platformKeys extension APIs. (These 2 APIs aren't available to apps and extensions that aren't force-installed.)

Leaving the policy unset means no apps or extensions are autoinstalled, and users can uninstall any app or extension in Google Chrome.

This policy supersedes ExtensionInstallBlocklist policy. If a previously force-installed app or extension is removed from this list, Google Chrome automatically uninstalls it.

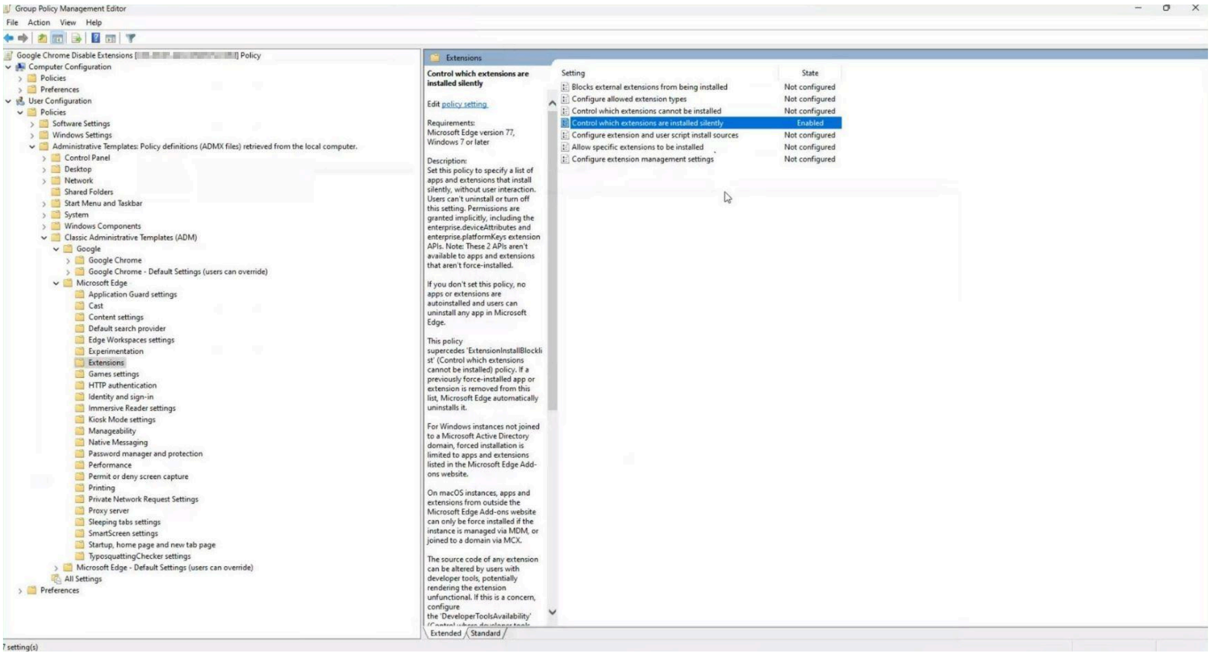
The source code of any extension may be altered by users through developer tools, potentially rendering the extension dysfunctional. If this is a concern, set the DeveloperToolsDisabled policy.

Each list item of the policy is a string that contains an extension ID and, optionally, an update URL separated by a semicolon (;). The extension ID is the 32-letter string found, for example, on chrome://extensions when in Developer mode. If specified, the update URL should point to an Update Manifest XML document (https://developer.chrome.com/extensions/autoupdate). The update URL should use one of the following schemes: http, https or file. By default, the Chrome Web Store's update URL is used. The

Setting	State
Blocks external extensions from being installed	Not configured
Restore permissive Chrome Apps <webview> behavior	Not configured
Configure allowed app/extension types	Not configured
Configure a list of origins that grant extended background li...	Not configured
Configure extension installation allow list	Not configured
Configure extension installation blocklist	Not configured
Configure the list of force-installed apps and extensions	Enabled
Configure extension, app, and user script install sources	Not configured
Control Manifest v2 extension availability	Not configured
Extension management settings	Not configured
Control availability of extensions unpublished on the Chro...	Not configured

2. Microsoft Edge

- Utilize the guide provided by Microsoft: Configure Microsoft Edge.
- Download the Edge Group Policy Template from this link.
- Configure your Group Policy as shown below.
  - EPP Browser Connector ID: **nnnaeanocbmnnjjlcfhcbpefmlgbcgoi**



Control which extensions are installed silently

Edit policy setting

Requirements:
Microsoft Edge version 77, Windows 7 or later

Description:
Set this policy to specify a list of apps and extensions that install silently, without user interaction. Users can't uninstall or turn off this setting. Permissions are granted implicitly, including the enterprise.deviceAttributes and enterprise.platformKeys extension APIs. Note: These 2 APIs aren't available to apps and extensions that aren't force-installed.

If you don't set this policy, no apps or extensions are autoinstalled and users can uninstall any app in Microsoft Edge.

This policy supercedes 'ExtensionInstallBlocklist' (Control which extensions cannot be installed) policy. If a previously force-installed app or extension is removed from this list, Microsoft Edge automatically uninstalls it.

For Windows instances not joined to a Microsoft Active Directory domain, forced installation is limited to apps and extensions listed in the Microsoft Edge Add-ons website.

On macOS instances, apps and extensions from outside the Microsoft Edge Add-ons website can only be force installed if the instance is managed via MDM, or joined to a domain via MCX.

The source code of any extension can be altered by users with developer tools, potentially rendering the extension unfunctional. If this is a concern, configure the 'DeveloperToolsAvailability'

Setting	State
Blocks external extensions from being installed	Not configured
Configure allowed extension types	Not configured
Control which extensions cannot be installed	Not configured
Control which extensions are installed silently	Enabled
Configure extension and user script install sources	Not configured
Allow specific extensions to be installed	Not configured
Configure extension management settings	Not configured

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.

5.7.4. 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.

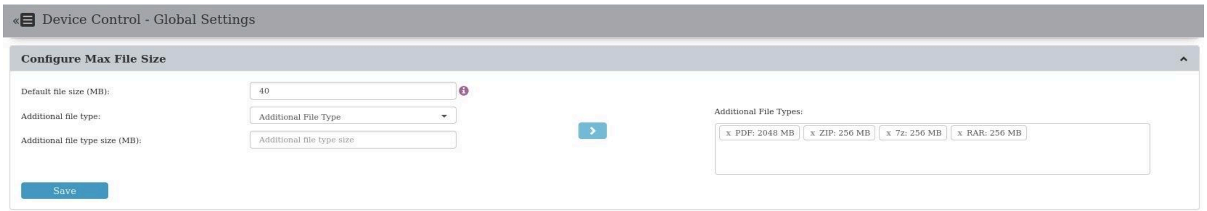
5.7.5. Configure Max File Size

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.



Device Control - Global Settings

Configure Max File Size

Default file size (MB): 40

Additional file type: Additional File Type

Additional file type size (MB): Additional file type size

Additional File Types: x PDF: 2048 MB | x ZIP: 256 MB | x 7z: 256 MB | x RAR: 256 MB

5.7.6. Outside Hours and Outside Network

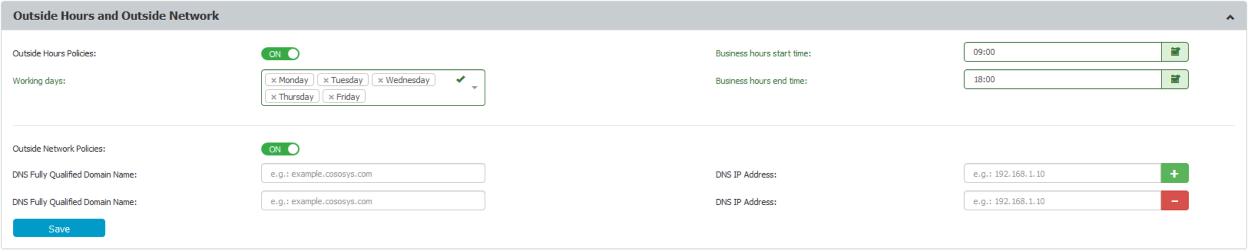
From this section, you can manage Outside Network and Outside Hours Policies, for both Device Control and Content Aware modules.

- **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.



Outside Hours and Outside Network

Outside Hours Policies: ON

Working days: × Monday × Tuesday × Wednesday × Thursday × Friday ✓

Business hours start time: 09:00

Business hours end time: 18:00

Outside Network Policies: ON

DNS Fully Qualified Domain Name: e.g.: example.cososys.com

DNS IP Address: e.g.: 192.168.1.10 +

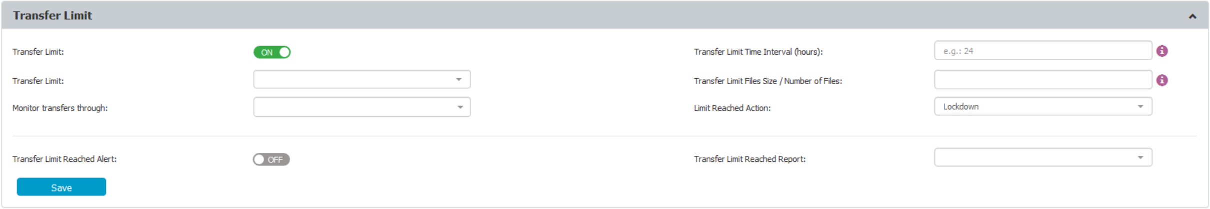
DNS Fully Qualified Domain Name: e.g.: example.cososys.com

DNS IP Address: e.g.: 192.168.1.10 −

Save

5.7.7. 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.



Transfer Limit

Transfer Limit: ON

Transfer Limit:

Monitor transfers through:

Transfer Limit Time Interval (hours): e.g.: 24

Transfer Limit Files Size / Number of Files:

Limit Reached Action: Lockdown

Transfer Limit Reached Alert: OFF

Transfer Limit Reached Report:

Save

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.

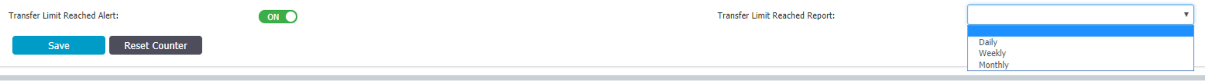
There are three actions to choose from when the Transfer Limit is reached:

- **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.



Transfer Limit Reached Alert: ON

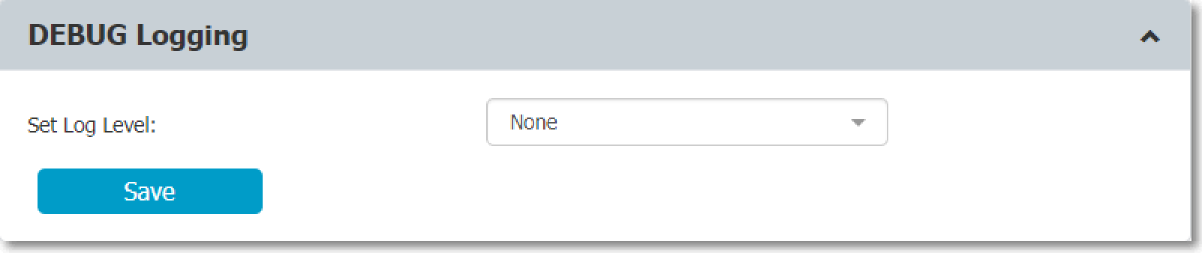
Transfer Limit Reached Report:

5.7.8. 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 sslsplit logs.

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



DEBUG Logging

Set Log Level: None

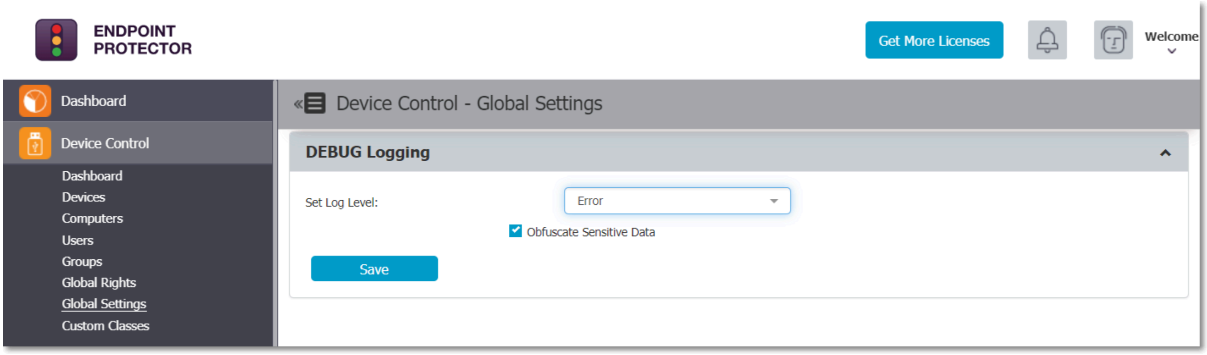
5.7.8.1. Debug Logging Usage

- **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**

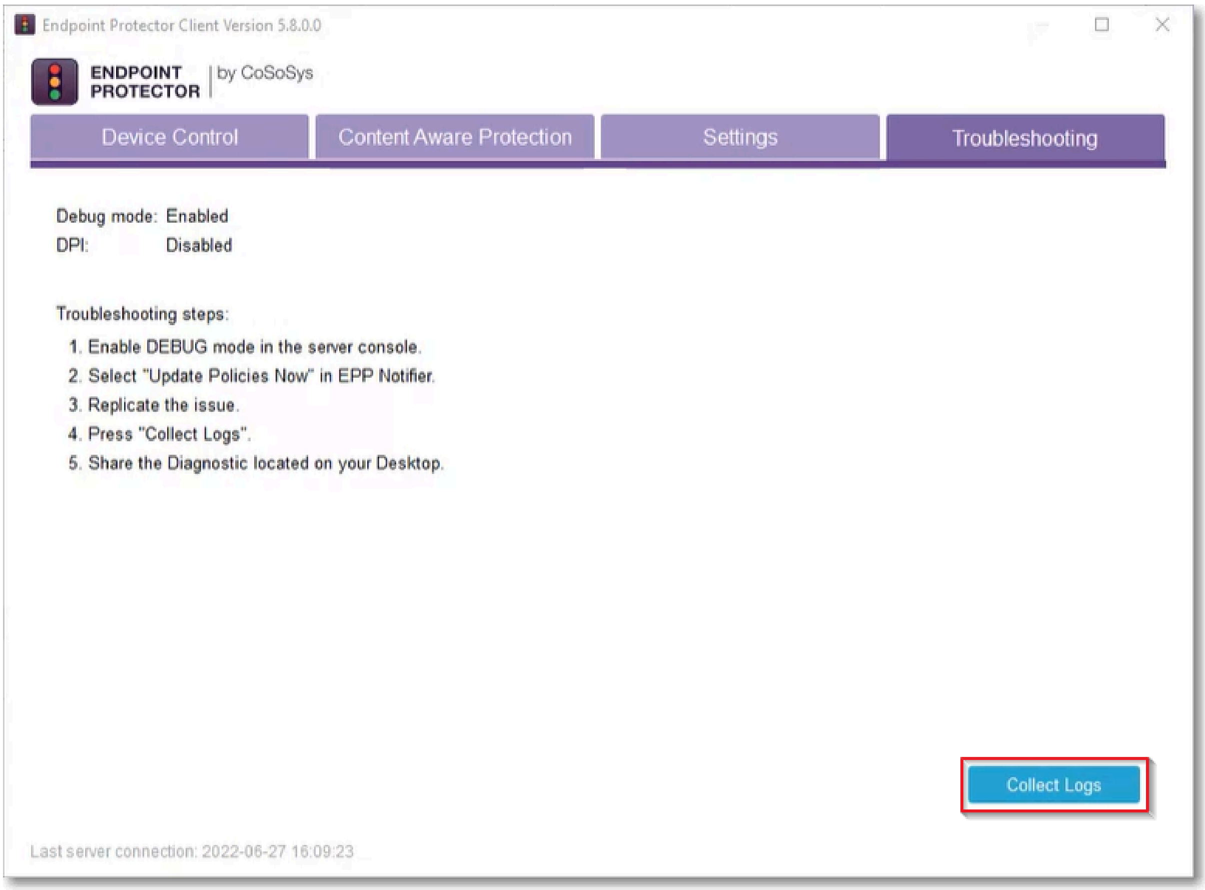
Note: Read the **Data Obfuscation Rules** section for more information.



Set Log Level: Error

☑ Obfuscate Sensitive Data

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.



Debug mode: Enabled
DPI: Disabled

Troubleshooting steps:
1. Enable DEBUG mode in the server console.
2. Select "Update Policies Now" in EPP Notifier.
3. Replicate the issue.
4. Press "Collect Logs".
5. Share the Diagnostic located on your Desktop.

Last server connection: 2022-06-27 16:09:23

- **Automatic Logging**

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

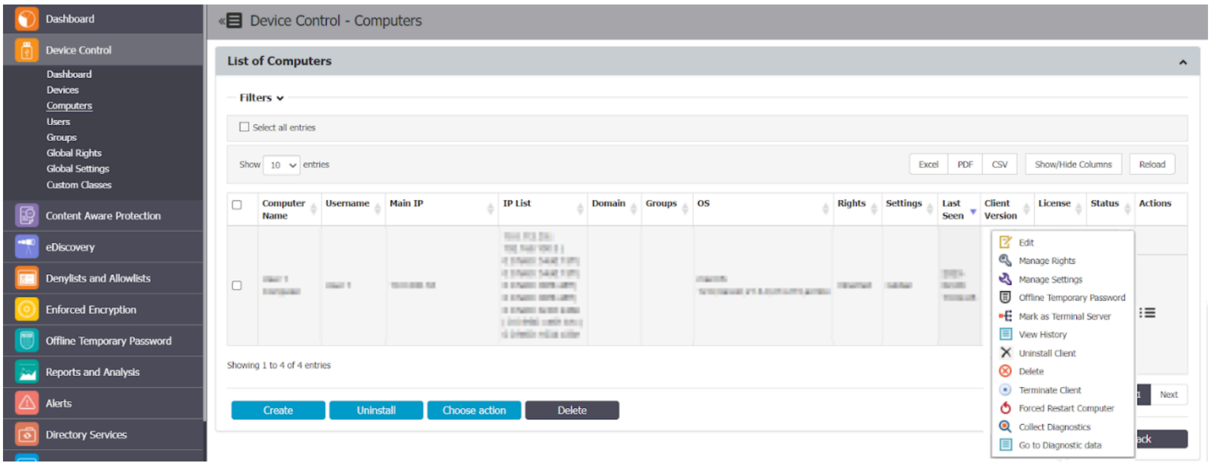
This option is available from **Device Control** on the **Computer** page.

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.

5.7.8.2. Debug Logging Actions

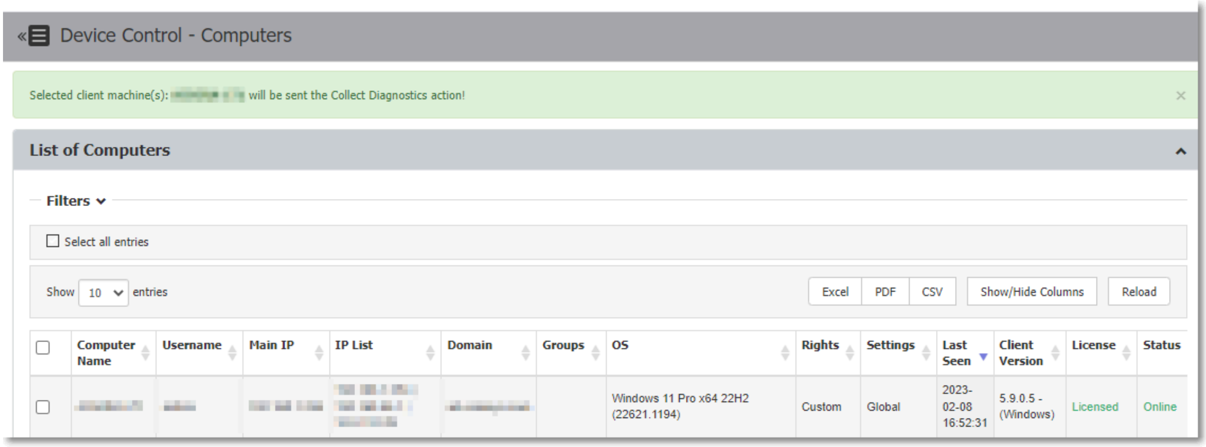
To view the log actions, go to the Device Control module, on the **Computers** page and click the **Actions** column.



☐	Computer Name	Username	Main IP	IP List	Domain	Groups	OS	Rights	Settings	Last Seen	Client Version	License	Status	Actions
☐	[redacted]	[redacted]	[redacted]	[redacted]			[redacted]	[redacted]	[redacted]	[redacted]				☰

Showing 1 to 4 of 4 entries

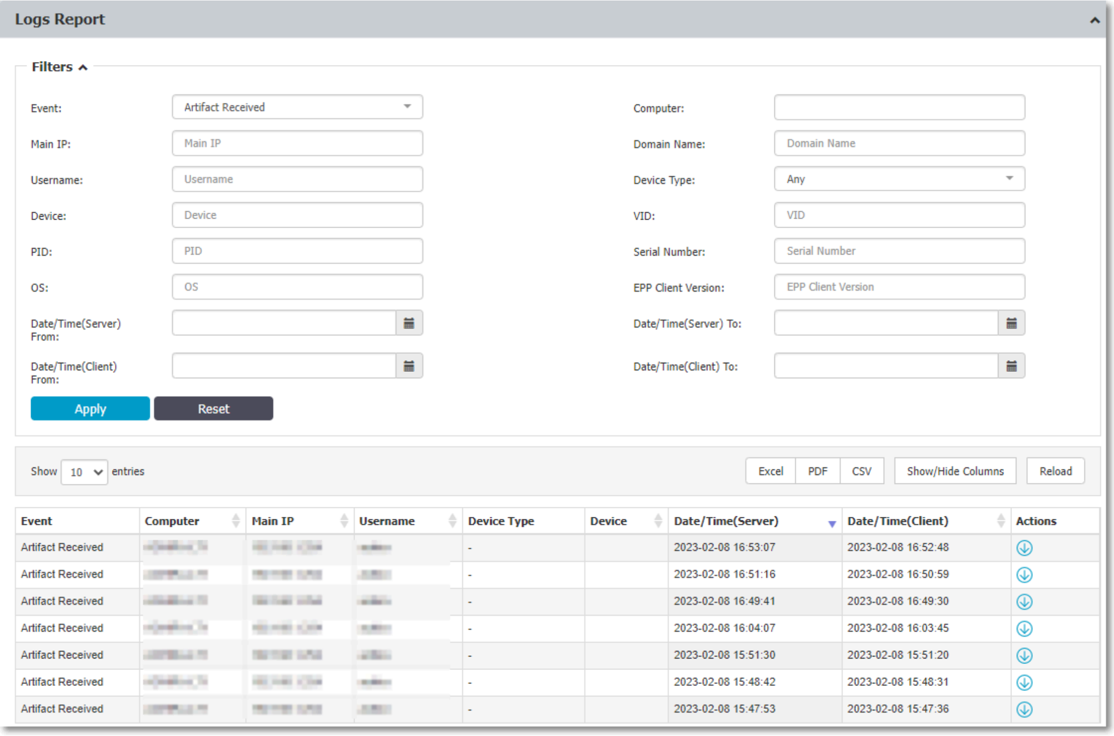
- **Collect Diagnostics** - registers an event when diagnostic data are requested (Artifact requested event)



Selected client machine(s): [redacted] will be sent the Collect Diagnostics action!

☐	Computer Name	Username	Main IP	IP List	Domain	Groups	OS	Rights	Settings	Last Seen	Client Version	License	Status
☐	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		Windows 11 Pro x64 22H2 (22621.1194)	Custom	Global	2023-02-08 16:52:31	5.9.0.5 - (Windows)	Licensed	Online

- **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.



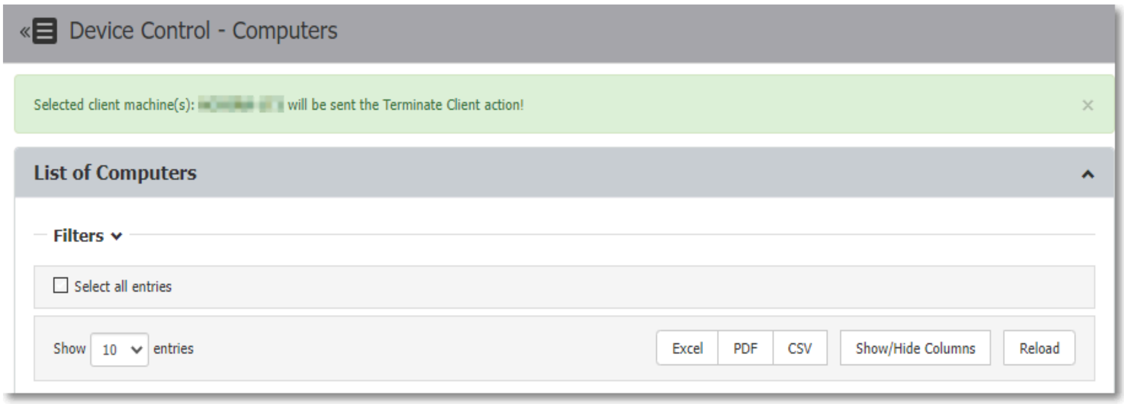
Logs Report

Filters

Event:	Artifact Received	Computer:	
Main IP:	Main IP	Domain Name:	Domain Name
Username:	Username	Device Type:	Any
Device:	Device	VID:	VID
PID:	PID	Serial Number:	Serial Number
OS:	OS	EPP Client Version:	EPP Client Version
Date/Time(Server) From:		Date/Time(Server) To:	
Date/Time(Client) From:		Date/Time(Client) To:	

Event	Computer	Main IP	Username	Device Type	Device	Date/Time(Server)	Date/Time(Client)	Actions
Artifact Received	[redacted]	[redacted]	[redacted]	-		2023-02-08 16:53:07	2023-02-08 16:52:48	ⓘ
Artifact Received	[redacted]	[redacted]	[redacted]	-		2023-02-08 16:51:16	2023-02-08 16:50:59	ⓘ
Artifact Received	[redacted]	[redacted]	[redacted]	-		2023-02-08 16:49:41	2023-02-08 16:49:30	ⓘ
Artifact Received	[redacted]	[redacted]	[redacted]	-		2023-02-08 16:04:07	2023-02-08 16:03:45	ⓘ
Artifact Received	[redacted]	[redacted]	[redacted]	-		2023-02-08 15:51:30	2023-02-08 15:51:20	ⓘ
Artifact Received	[redacted]	[redacted]	[redacted]	-		2023-02-08 15:48:42	2023-02-08 15:48:31	ⓘ
Artifact Received	[redacted]	[redacted]	[redacted]	-		2023-02-08 15:47:53	2023-02-08 15:47:36	ⓘ

- **Terminate Client** - this option terminates the Endpoint Protector Client

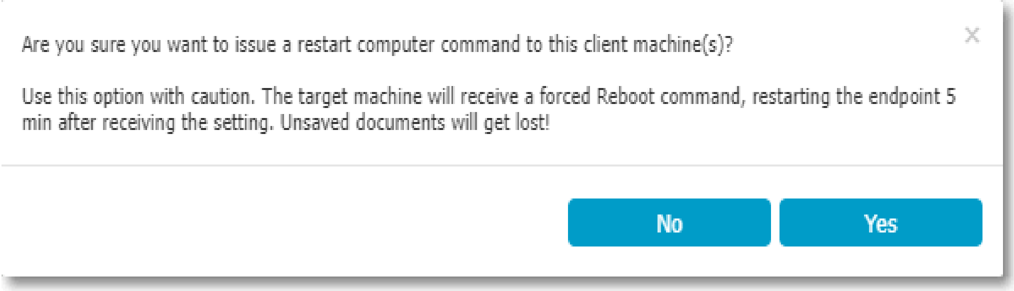


Device Control - Computers

Selected client machine(s): [redacted] will be sent the Terminate Client action!

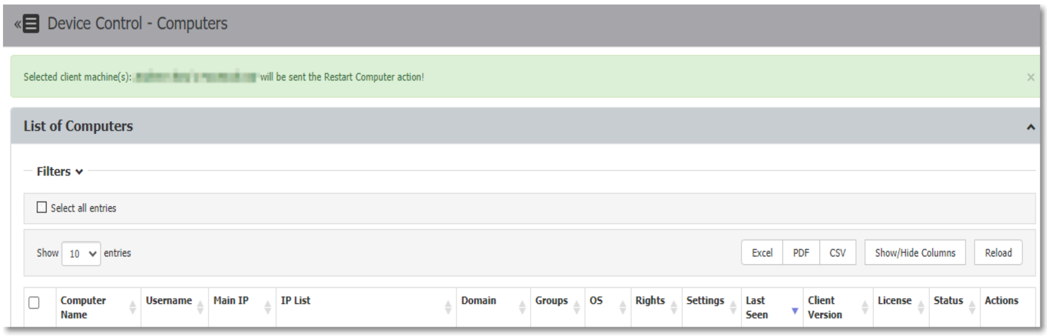
List of Computers

- **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!



Device Control - Computers

Selected client machine(s): [redacted] will be sent the Restart Computer action!

List of Computers

☐	Computer Name	Username	Main IP	IP List	Domain	Groups	OS	Rights	Settings	Last Seen	Client Version	License	Status	Actions

5.7.8.3. 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

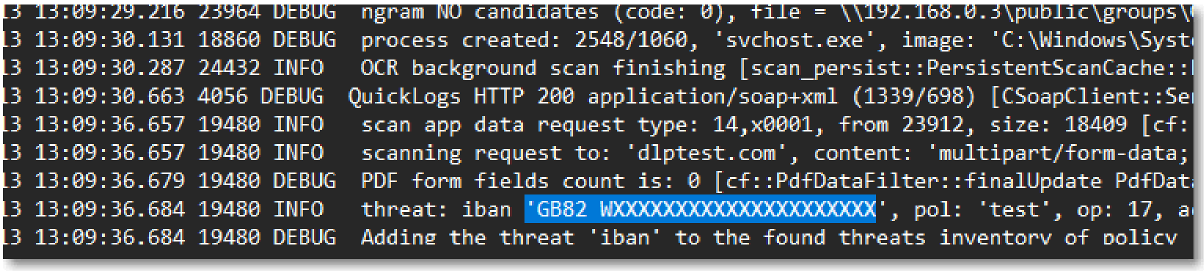
or

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

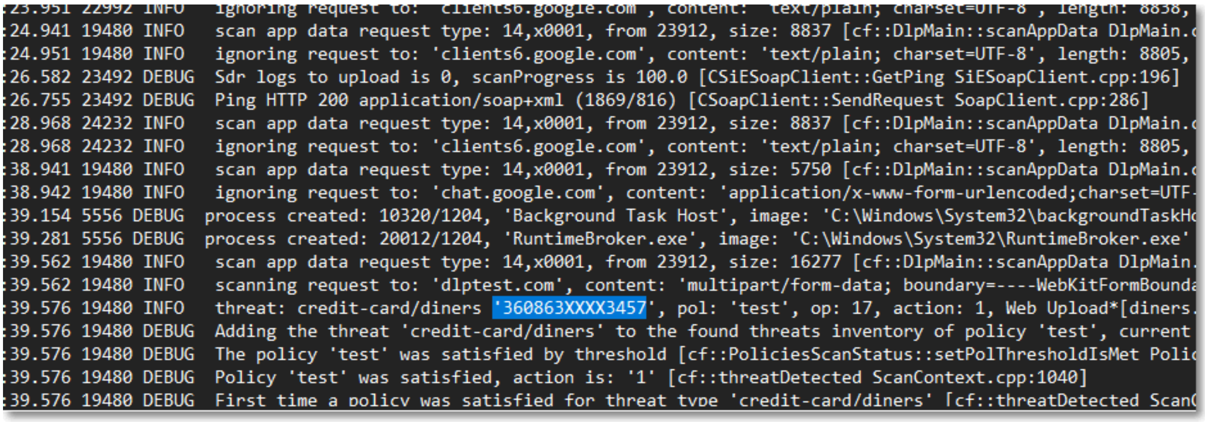
Specific use cases:

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

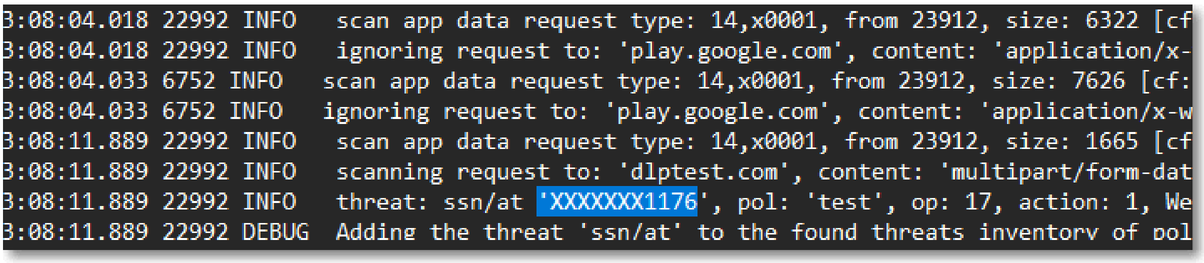
Important: Data is not obfuscated for the file-type threat, file-size threat, and date threat.



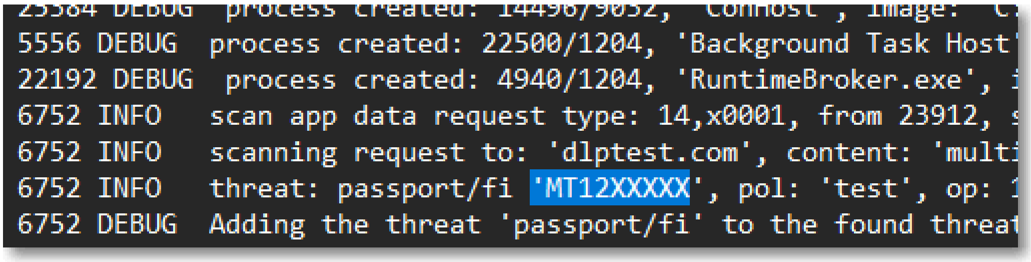
```
13 13:09:29.216 23964 DEBUG  ngram NO candidates (code: 0), file = \\192.168.0.3\public\groups\
13 13:09:30.131 18860 DEBUG  process created: 2548/1060, 'svchost.exe', image: 'C:\Windows\Syst
13 13:09:30.287 24432 INFO   OCR background scan finishing [scan_persist::PersistentScanCache::
13 13:09:30.663 4056 DEBUG  QuickLogs HTTP 200 application/soap+xml (1339/698) [CSoapClient::Se
13 13:09:36.657 19480 INFO   scan app data request type: 14,x0001, from 23912, size: 18409 [cf:
13 13:09:36.657 19480 INFO   scanning request to: 'dlptest.com', content: 'multipart/form-data;
13 13:09:36.679 19480 DEBUG  PDF form fields count is: 0 [cf::PdfDataFilter::finalUpdate PdfDat
13 13:09:36.684 19480 INFO   threat: iban 'GB82 WXXXXXXXXXXXXXXXXXXXXX', pol: 'test', op: 17, a
13 13:09:36.684 19480 DEBUG  Adding the threat 'iban' to the found threats inventorv of policv
```



```
:23.951 22992 INFO   ignoring request to: 'clients6.google.com', content: 'text/plain; charset=UTF-8', length: 8838,
:24.941 19480 INFO   scan app data request type: 14,x0001, from 23912, size: 8837 [cf::DlpMain::scanAppData DlpMain.
:24.951 19480 INFO   ignoring request to: 'clients6.google.com', content: 'text/plain; charset=UTF-8', length: 8805,
:26.582 23492 DEBUG  Sdr logs to upload is 0, scanProgress is 100.0 [CSiESoapClient::GetPing SiESoapClient.cpp:196]
:26.755 23492 DEBUG  Ping HTTP 200 application/soap+xml (1869/816) [CSoapClient::SendRequest SoapClient.cpp:286]
:28.968 24232 INFO   scan app data request type: 14,x0001, from 23912, size: 8837 [cf::DlpMain::scanAppData DlpMain.
:28.968 24232 INFO   ignoring request to: 'clients6.google.com', content: 'text/plain; charset=UTF-8', length: 8805,
:38.941 19480 INFO   scan app data request type: 14,x0001, from 23912, size: 5750 [cf::DlpMain::scanAppData DlpMain.
:38.942 19480 INFO   ignoring request to: 'chat.google.com', content: 'application/x-www-form-urlencoded;charset=UTF-
:39.154 5556 DEBUG  process created: 10320/1204, 'Background Task Host', image: 'C:\Windows\System32\backgroundTaskHo
:39.281 5556 DEBUG  process created: 20012/1204, 'RuntimeBroker.exe', image: 'C:\Windows\System32\RuntimeBroker.exe'
:39.562 19480 INFO   scan app data request type: 14,x0001, from 23912, size: 16277 [cf::DlpMain::scanAppData DlpMain.
:39.562 19480 INFO   scanning request to: 'dlptest.com', content: 'multipart/form-data; boundary=----WebKitFormBounda
:39.576 19480 INFO   threat: credit-card/diners '360863XXXX3457', pol: 'test', op: 17, action: 1, Web Upload*[diners.
:39.576 19480 DEBUG  Adding the threat 'credit-card/diners' to the found threats inventory of policy 'test', current
:39.576 19480 DEBUG  The policy 'test' was satisfied by threshold [cf::PoliciesScanStatus::setPolThresholdIsMet Polic
:39.576 19480 DEBUG  Policy 'test' was satisfied, action is: '1' [cf::threatDetected ScanContext.cpp:1040]
:39.576 19480 DEBUG  First time a policv was satisfied for threat tvpe 'credit-card/diners' [cf::threatDetected Scan(
```



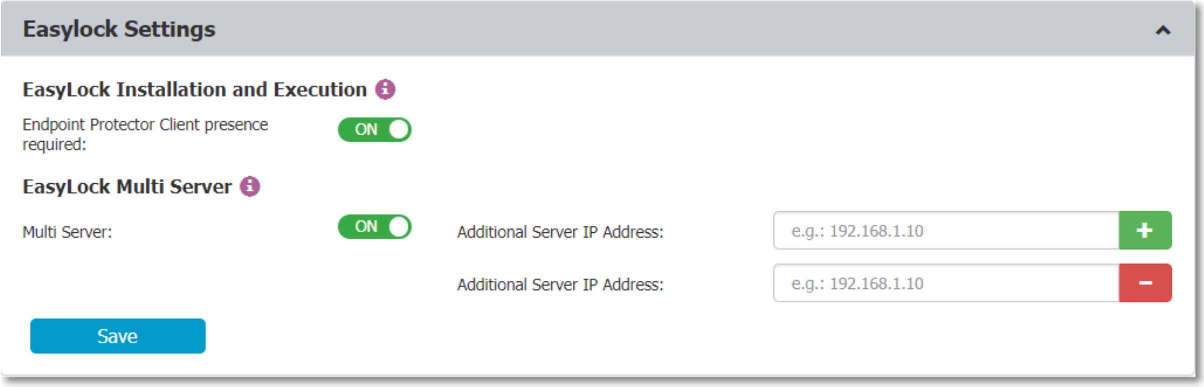
```
3:08:04.018 22992 INFO   scan app data request type: 14,x0001, from 23912, size: 6322 [cf
3:08:04.018 22992 INFO   ignoring request to: 'play.google.com', content: 'application/x-
3:08:04.033 6752 INFO   scan app data request type: 14,x0001, from 23912, size: 7626 [cf:
3:08:04.033 6752 INFO   ignoring request to: 'play.google.com', content: 'application/x-w
3:08:11.889 22992 INFO   scan app data request type: 14,x0001, from 23912, size: 1665 [cf
3:08:11.889 22992 INFO   scanning request to: 'dlptest.com', content: 'multipart/form-dat
3:08:11.889 22992 INFO   threat: ssn/at 'XXXXXXX1176', pol: 'test', op: 17, action: 1, We
3:08:11.889 22992 DEBUG  Adding the threat 'ssn/at' to the found threats inventory of pol
```



```
23584 DEBUG  process created: 14496/9052, 'conhost', image: 'C:
5556 DEBUG  process created: 22500/1204, 'Background Task Host'
22192 DEBUG  process created: 4940/1204, 'RuntimeBroker.exe', i
6752 INFO   scan app data request type: 14,x0001, from 23912, s
6752 INFO   scanning request to: 'dlptest.com', content: 'multi
6752 INFO   threat: passport/fi 'MT12XXXXX', pol: 'test', op: 1
6752 DEBUG  Adding the threat 'passport/fi' to the found threat
```

5.7.9. 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.



Easylock Settings

EasyLock Installation and Execution

Endpoint Protector Client presence required: ON

EasyLock Multi Server

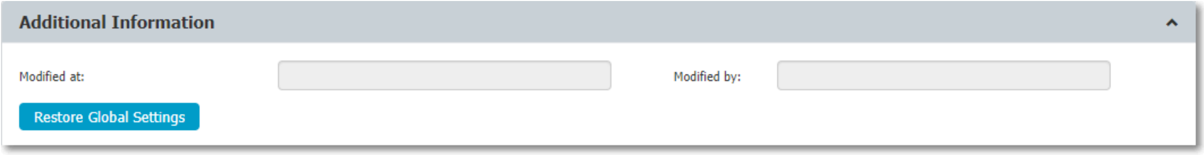
Multi Server: ON

Additional Server IP Address: e.g.: 192.168.1.10 +

Additional Server IP Address: e.g.: 192.168.1.10 −

5.7.10. Additional Information

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



Additional Information

Modified at:

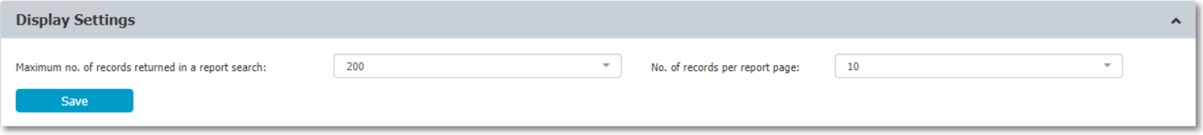
Modified by:

5.7.11. 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.



Display Settings

Maximum no. of records returned in a report search: 200

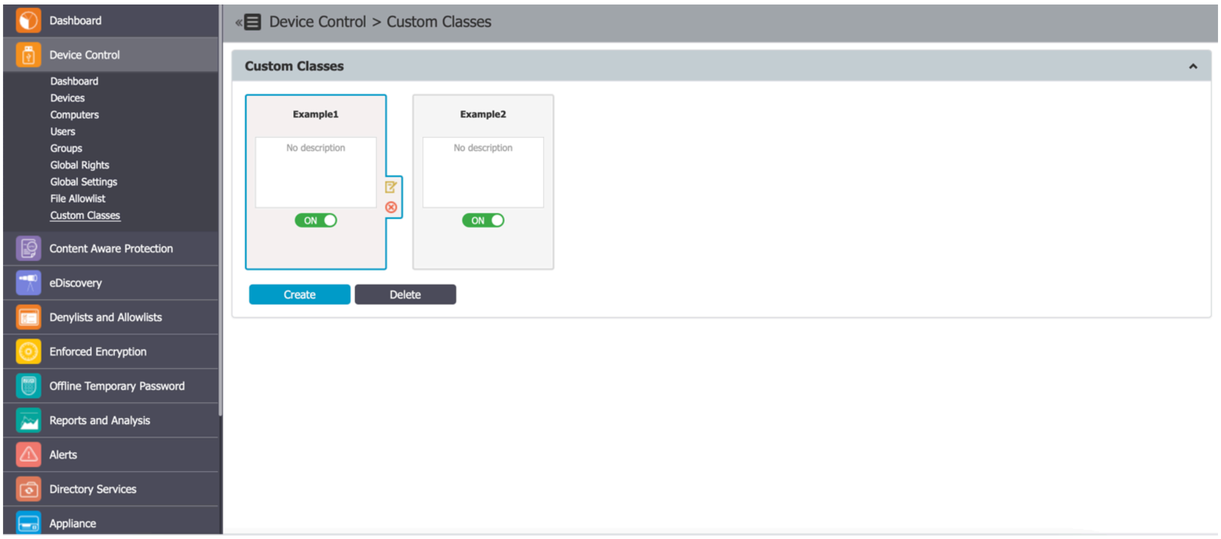
No. of records per report page: 10

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).

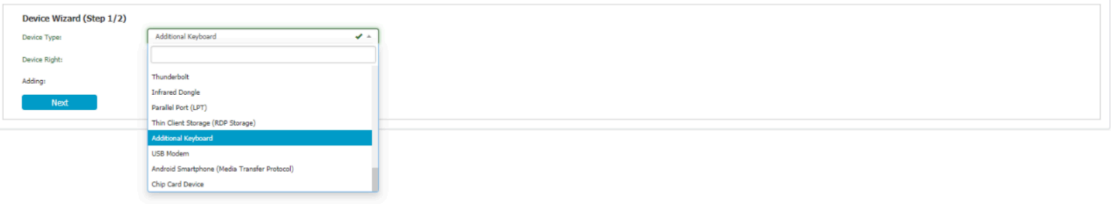
A new Custom Class can be created by clicking on the Create. An existing policy can be edited by double-clicking on it.

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.



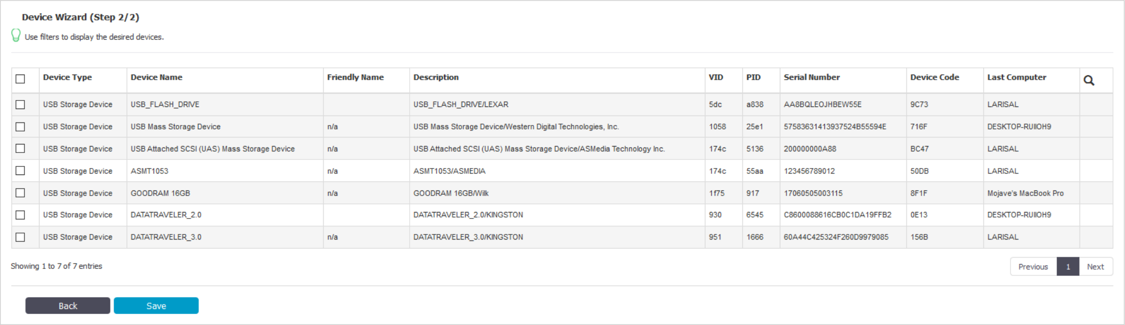
Device Wizard (Step 1/2)

Device Type: Additional Keyboard

Device Right:

Adding:

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



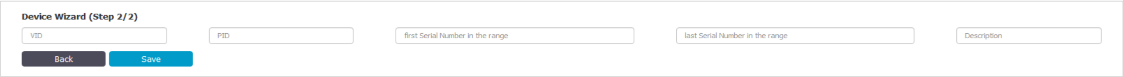
Device Wizard (Step 2/2)

Use filters to display the desired devices.

☐	Device Type	Device Name	Friendly Name	Description	VID	PID	Serial Number	Device Code	Last Computer	🔍
☐	USB Storage Device	USB_FLASH_DRIVE		USB_FLASH_DRIVE/LEXAR	5dc	a838	AA8BQLEOJHBEW55E	9C73	LARISAL	
☐	USB Storage Device	USB Mass Storage Device	n/a	USB Mass Storage Device/Western Digital Technologies, Inc.	1058	25e1	57583631413937524B55594E	716F	DESKTOP-RUIIOH9	
☐	USB Storage Device	USB Attached SCSI (UAS) Mass Storage Device	n/a	USB Attached SCSI (UAS) Mass Storage Device/ASMedia Technology Inc.	174c	5136	200000000A88	BC47	LARISAL	
☐	USB Storage Device	ASMT1053	n/a	ASMT1053/ASMEDIA	174c	55aa	123456789012	50DB	LARISAL	
☐	USB Storage Device	GOODRAM 16GB	n/a	GOODRAM 16GB/Wilk	1f75	917	17060505003115	8F1F	Mojave's MacBook Pro	
☐	USB Storage Device	DATATRAVELER_2.0		DATATRAVELER_2.0/KINGSTON	930	6545	C8600088616CB0C1DA19FFB2	0E13	DESKTOP-RUIIOH9	
☐	USB Storage Device	DATATRAVELER_3.0	n/a	DATATRAVELER_3.0/KINGSTON	951	1666	60A44C425324F260D9979085	156B	LARISAL	

Showing 1 to 7 of 7 entries

- **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.

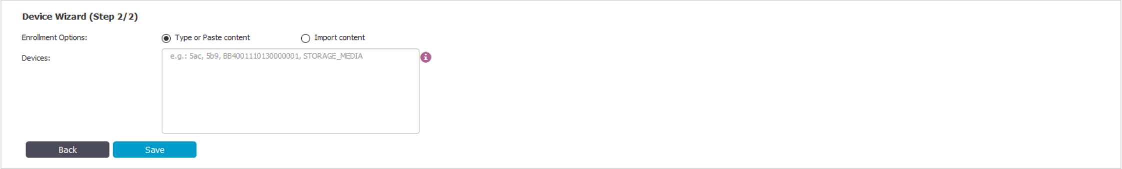


Device Wizard (Step 2/2)

VID
PID
first Serial Number in the range
last Serial Number in the range
Description
Back
Save

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 (Step 2/2)

Enrollment Options: ● Type or Paste content ○ Import content

Devices: e.g.: 5ac, 5b9, BB400111013000001, STORAGE_MEDIA

- **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.

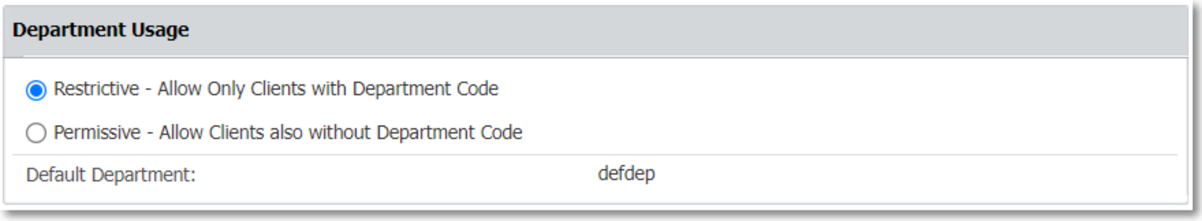
Select an option to grant access for clients based on the Department Code. You can also view the Default Department code – defdep.

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.



Department Usage

● Restrictive - Allow Only Clients with Department Code

○ Permissive - Allow Clients also without Department Code

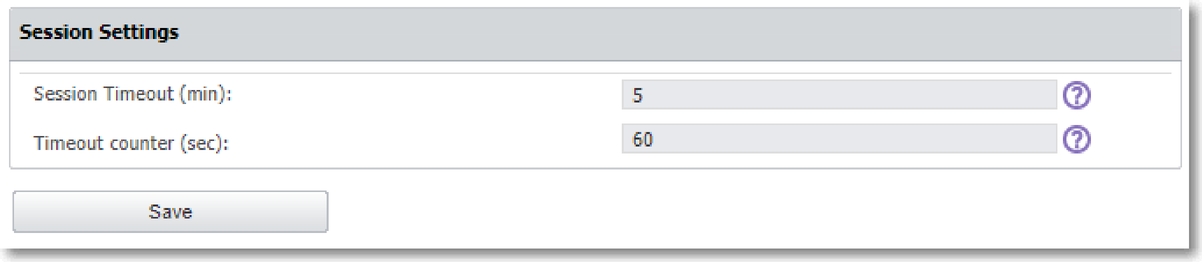
Default Department: defdep

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.



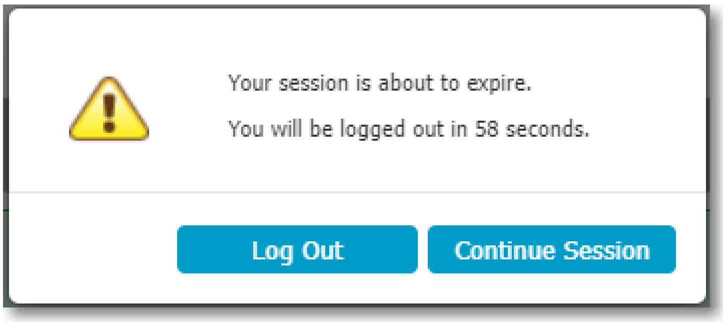
Session Settings

Session Timeout (min): 5

Timeout counter (sec): 60

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.

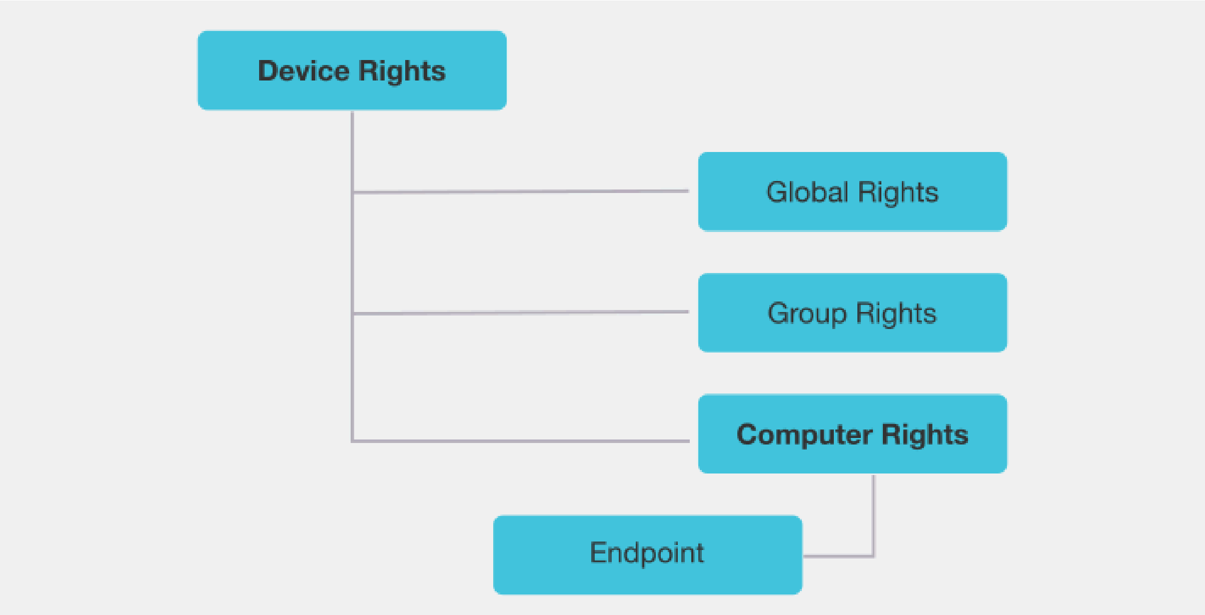


Your session is about to expire.

You will be logged out in 58 seconds.

Endpoint Protector Rights Functionality

Endpoint Protector Rights Functionality



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.

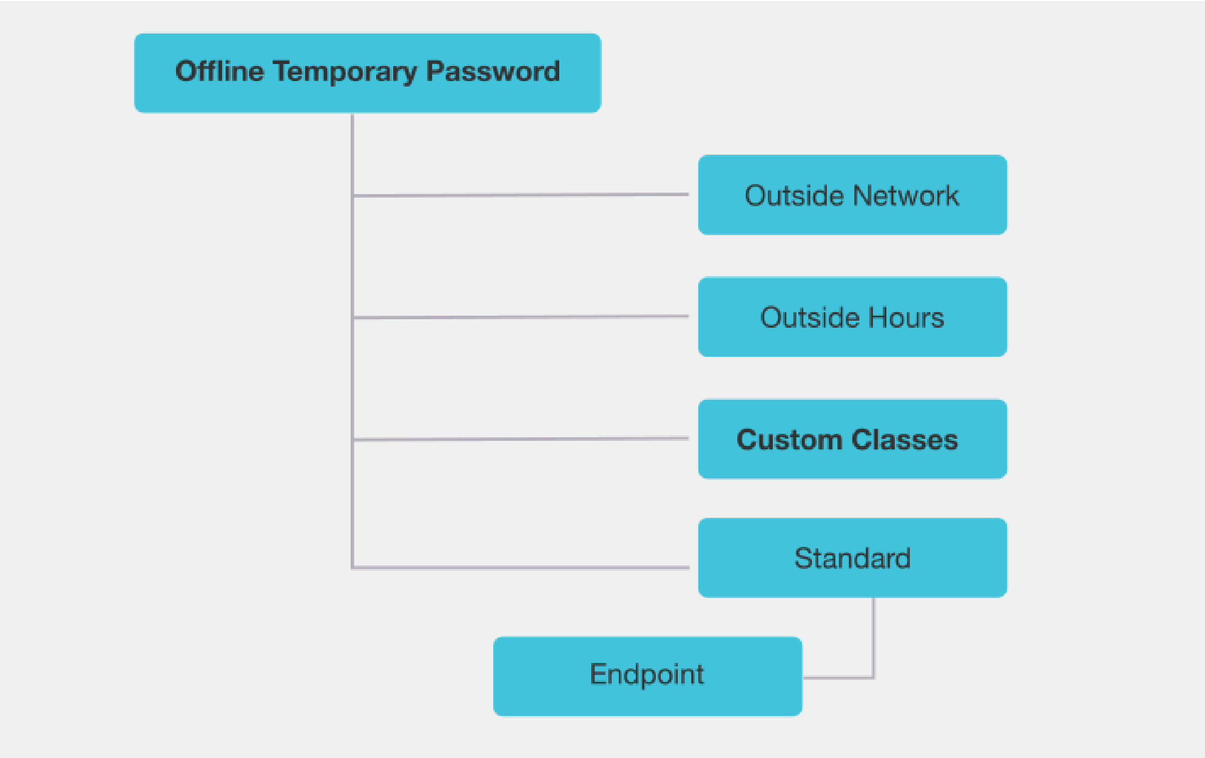
5.9.2. Priorities for Device Control Policies

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.

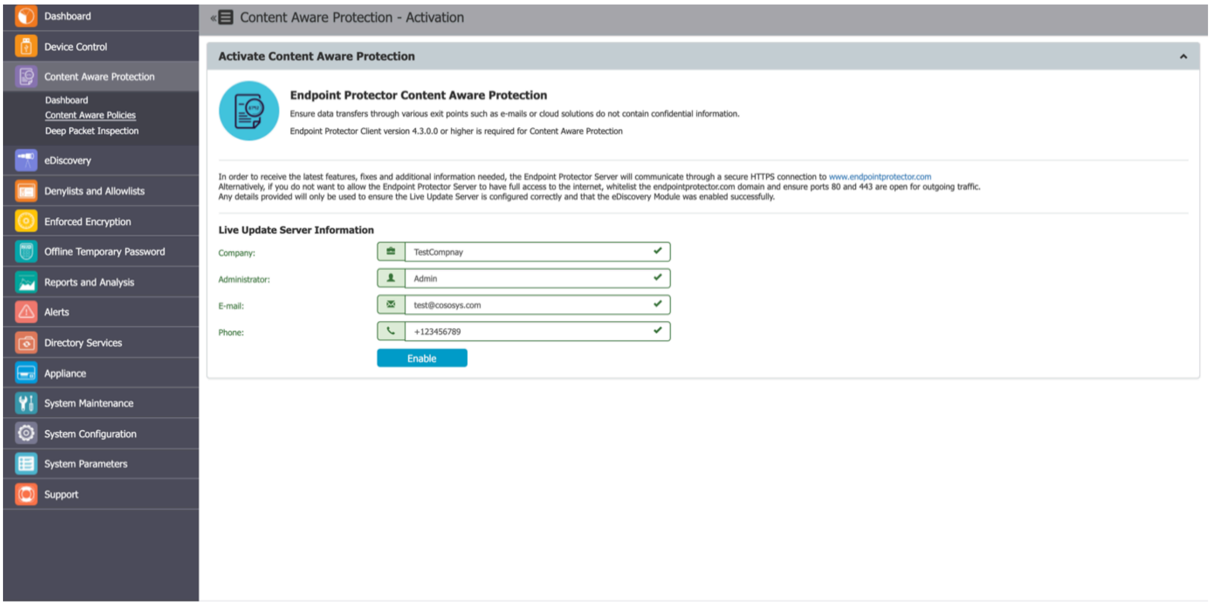
To prevent sensitive data leakage, Endpoint Protector closely monitors all activity at various exit points:

- 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.



Content Aware Protection - Activation

Activate Content Aware Protection

Endpoint Protector Content Aware Protection

Ensure data transfers through various exit points such as e-mails or cloud solutions do not contain confidential information.

Endpoint Protector Client version 4.3.0.0 or higher is required for Content Aware Protection

In order to receive the latest features, fixes and additional information needed, the Endpoint Protector Server will communicate through a secure HTTPS connection to www.endpointprotector.com
Alternatively, if you do not want to allow the Endpoint Protector Server to have full access to the internet, whitelist the endpointprotector.com domain and ensure ports 80 and 443 are open for outgoing traffic.
Any details provided will only be used to ensure the Live Update Server is configured correctly and that the eDiscovery Module was enabled successfully.

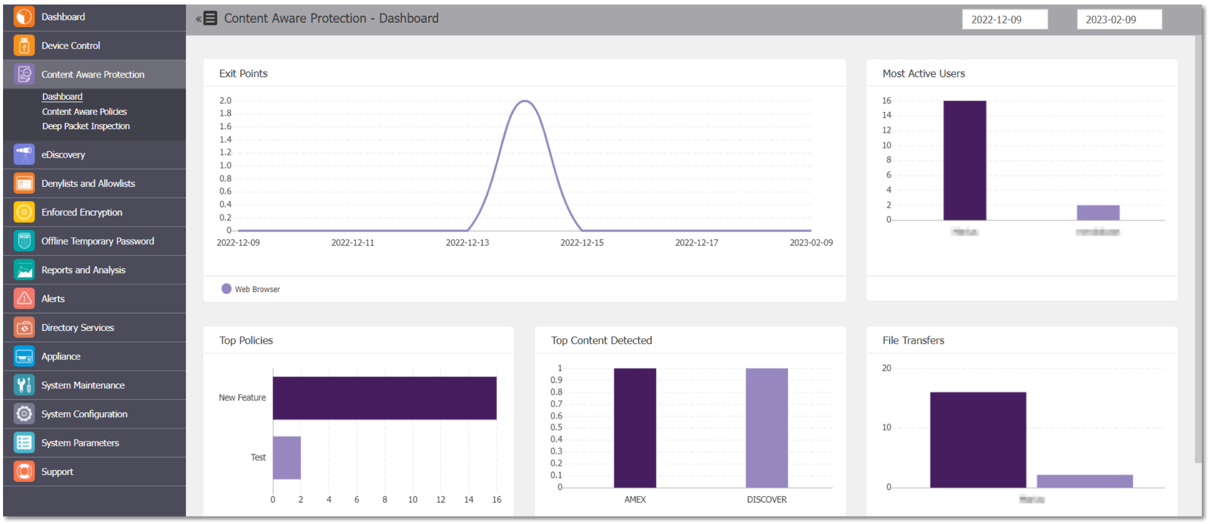
Live Update Server Information

Company: TestCompnay ✓
Administrator: Admin ✓
E-mail: test@cososys.com ✓
Phone: +123456789 ✓

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.).

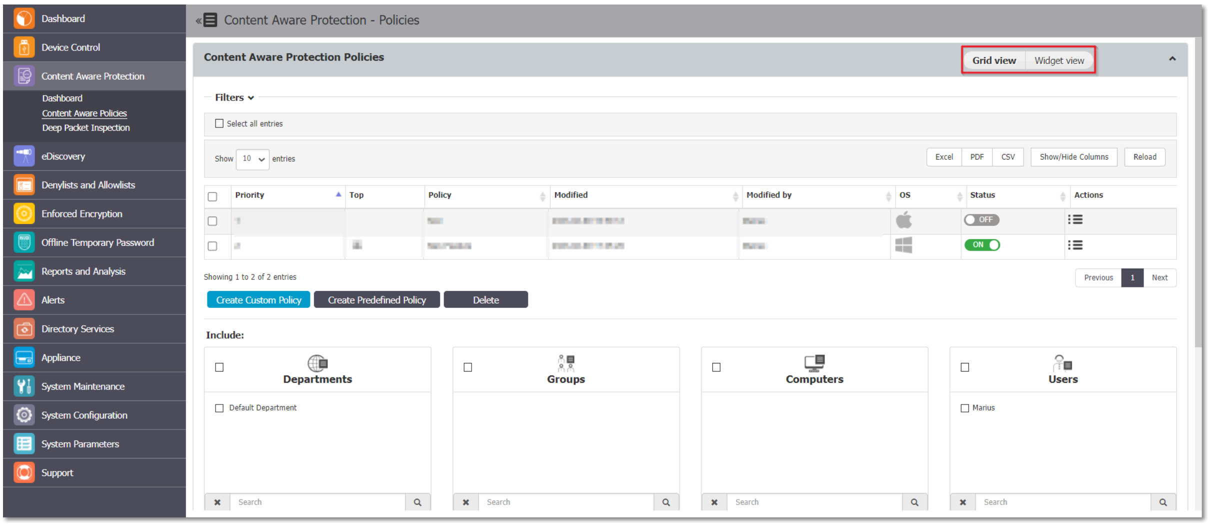
Note: Content Aware Policies also apply to File Allowlist (Device Control > File Allowlist). This means that all files that were previously allowed will be inspected for sensitive content detection, reported, and/or blocked, according to the defined policy.

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



☐	Priority	Top	Policy	Modified	Modified by	OS	Status	Actions
☐	[redacted]		[redacted]	[redacted]	[redacted]		OFF	
☐	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		ON	

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

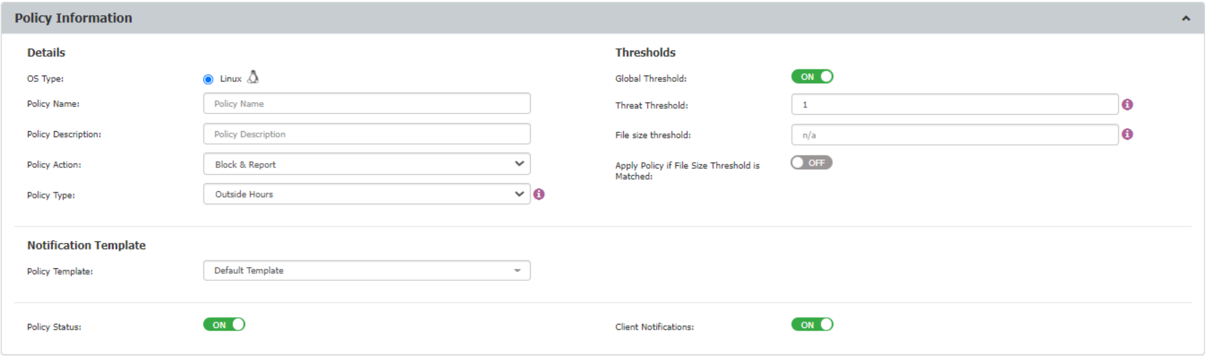
1. Set a Block & Report policy with 4 threats, on the transfer of Social Security Numbers (SSN) for several Internet browsers.

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.



Policy Information

Details

OS Type: ● Linux

Policy Name: Policy Name

Policy Description: Policy Description

Policy Action: Block & Report

Policy Type: Outside Hours

Thresholds

Global Threshold: ON

Threat Threshold: 1

File size threshold: n/a

Apply Policy if File Size Threshold is Matched: OFF

Notification Template

Policy Template: Default Template

Policy Status: ON

Client Notifications: ON

6.3.2. Policy Exit Points

You can monitor transfers from the following exit points:

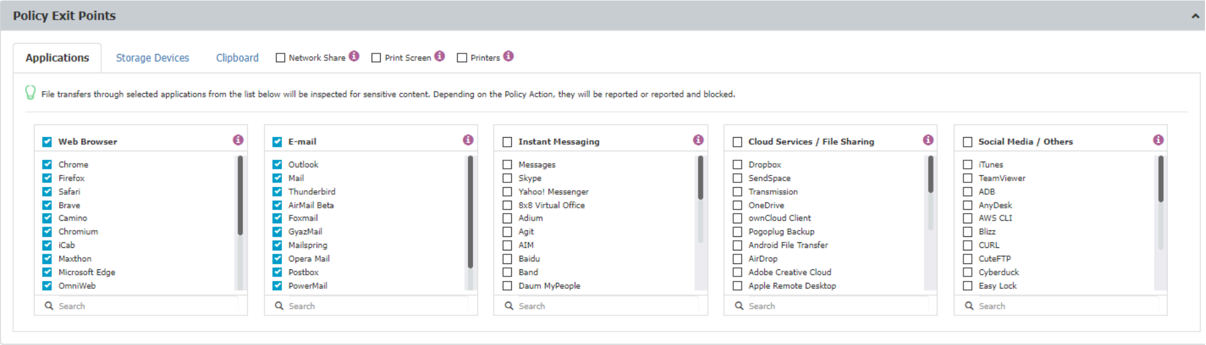
6.3.2.1. Applications

- **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

Applications | Storage Devices | Clipboard | ☐ Network Share | ☐ Print Screen | ☐ Printers

File transfers through selected applications from the list below will be inspected for sensitive content. Depending on the Policy Action, they will be reported or reported and blocked.

☑ **Web Browser**
☑ Chrome
☑ Firefox
☑ Safari
☑ Brave
☑ Camino
☑ Chromium
☑ iCab
☑ Maxthon
☑ Microsoft Edge
☑ OmniWeb

☑ **E-mail**
☑ Outlook
☑ Mail
☑ Thunderbird
☑ AirMail Beta
☑ Foxmail
☑ GyazMail
☑ Mailspring
☑ Opera Mail
☑ Postbox
☑ PowerMail

☐ **Instant Messaging**
☐ Messages
☐ Skype
☐ Yahoo! Messenger
☐ 8x8 Virtual Office
☐ Adium
☐ Agit
☐ AIM
☐ Baidu
☐ Band
☐ Daum MyPeople

☐ **Cloud Services / File Sharing**
☐ Dropbox
☐ SendSpace
☐ Transmission
☐ OneDrive
☐ ownCloud Client
☐ Pogoplug Backup
☐ Android File Transfer
☐ AirDrop
☐ Adobe Creative Cloud
☐ Apple Remote Desktop

☐ **Social Media / Others**
☐ iTunes
☐ TeamViewer
☐ ADB
☐ AnyDesk
☐ AWS CLI
☐ Blizz
☐ CURL
☐ CuteFTP
☐ Cyberduck
☐ Easy Lock

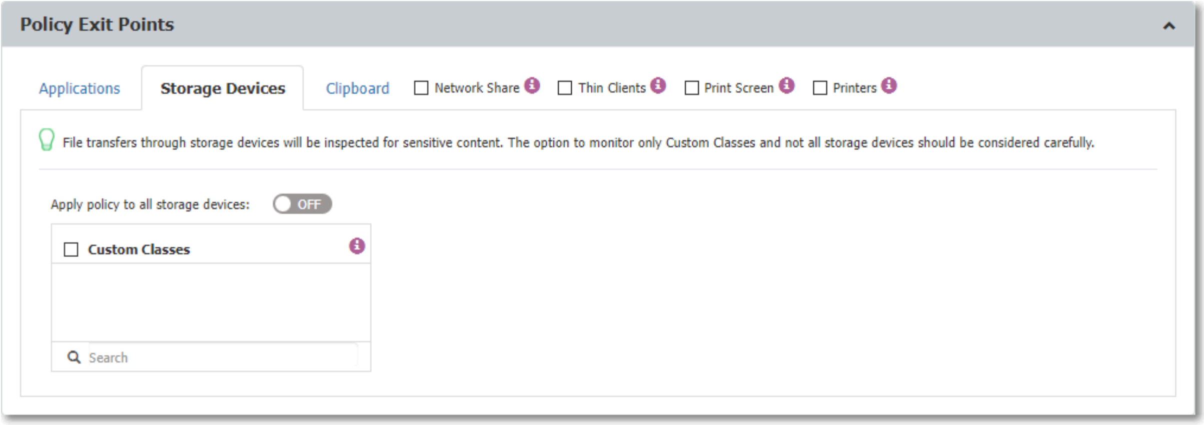
6.3.2.2. Storage Devices

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).



File transfers through storage devices will be inspected for sensitive content. The option to monitor only Custom Classes and not all storage devices should be considered carefully.

Apply policy to all storage devices: OFF

□ Custom Classes

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, i**nstead, 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

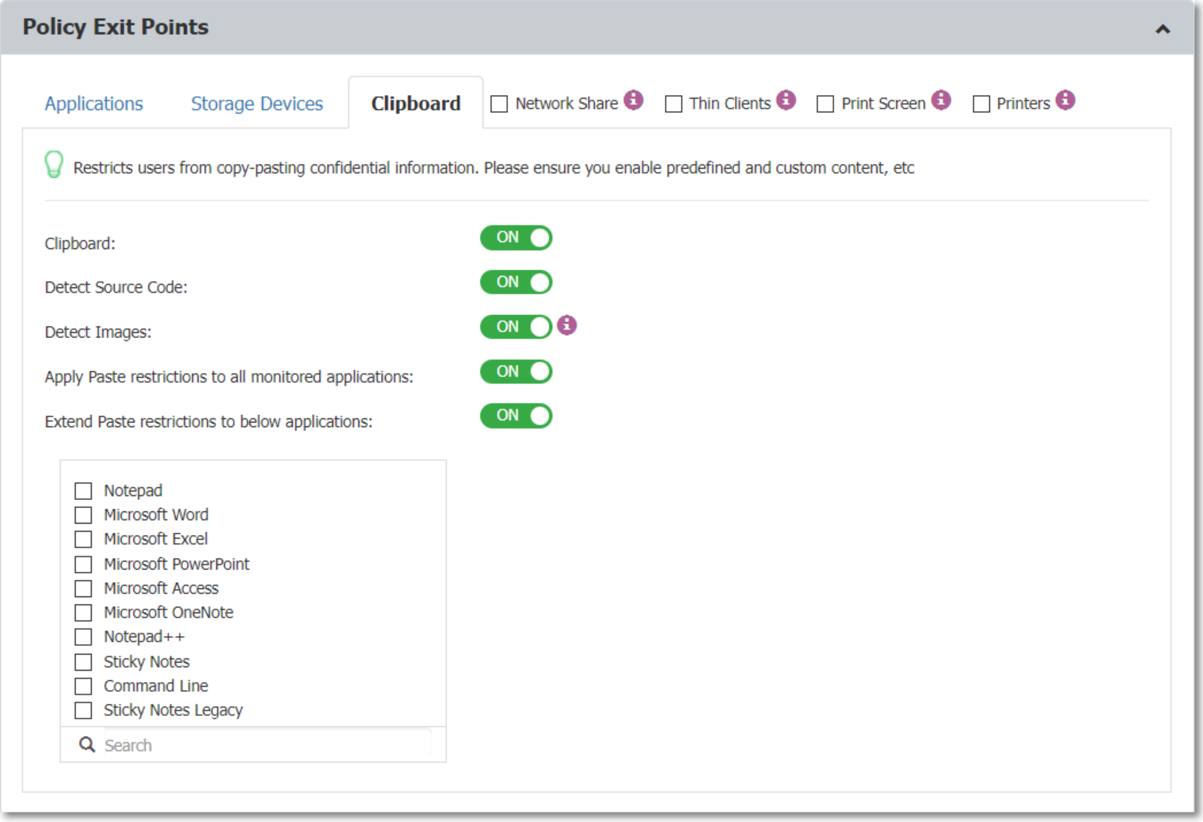
Note: This setting restricts the **Paste** operation for the defined applications.

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.

Important: On certain Linux environments, like those utilizing Wayland protocol by default, paste control is limited due to Wayland's lack of support for detecting the focused window. To ensure security, content blocking occurs during the copy operation.



Policy Exit Points

Applications | Storage Devices | **Clipboard** | □ Network Share | □ Thin Clients | □ Print Screen | □ Printers

Restricts users from copy-pasting confidential information. Please ensure you enable predefined and custom content, etc

Clipboard: ON

Detect Source Code: ON

Detect Images: ON

Apply Paste restrictions to all monitored applications: ON

Extend Paste restrictions to below applications: ON

□ Notepad
□ Microsoft Word
□ Microsoft Excel
□ Microsoft PowerPoint
□ Microsoft Access
□ Microsoft OneNote
□ Notepad++
□ Sticky Notes
□ Command Line
□ Sticky Notes Legacy

Search

Important: Newer Linux Ubuntu versions have 'snap'-based applications installed by default, affecting EPP Client functionality. This may result in missing file-related events in CAP scans. The reliance on 'snap'-based applications also affects file-related web browser activities, exacerbating this limitation. Consider non-'snap'-based applications (where possible) as alternative configurations for optimal functionality.

1. **Network Share** Endpoint Protector will report all the events for Report Only policies for macOS. 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

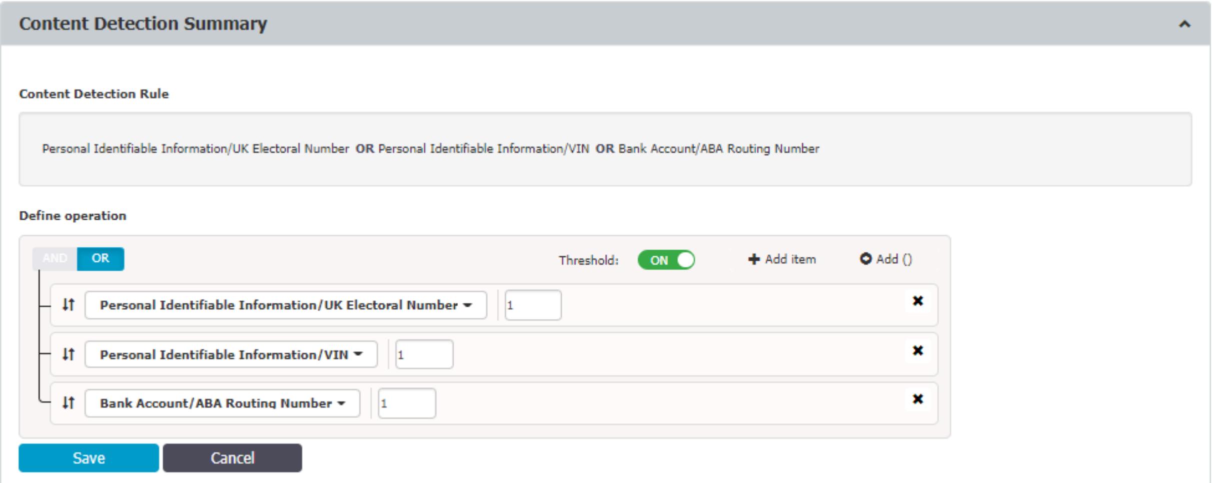
The Custom Detection Summary displays all predefined content, custom content, regular expressions, and HIPAA which were checked in the Content Aware Policy.

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

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 PIIs 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.



Content Detection Summary

Content Detection Rule

Personal Identifiable Information/UK Electoral Number **OR** Personal Identifiable Information/VIN **OR** Bank Account/ABA Routing Number

Define operation

- Personal Identifiable Information/UK Electoral Number: 1
- Personal Identifiable Information/VIN: 1
- Bank Account/ABA Routing Number: 1

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** 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**.**

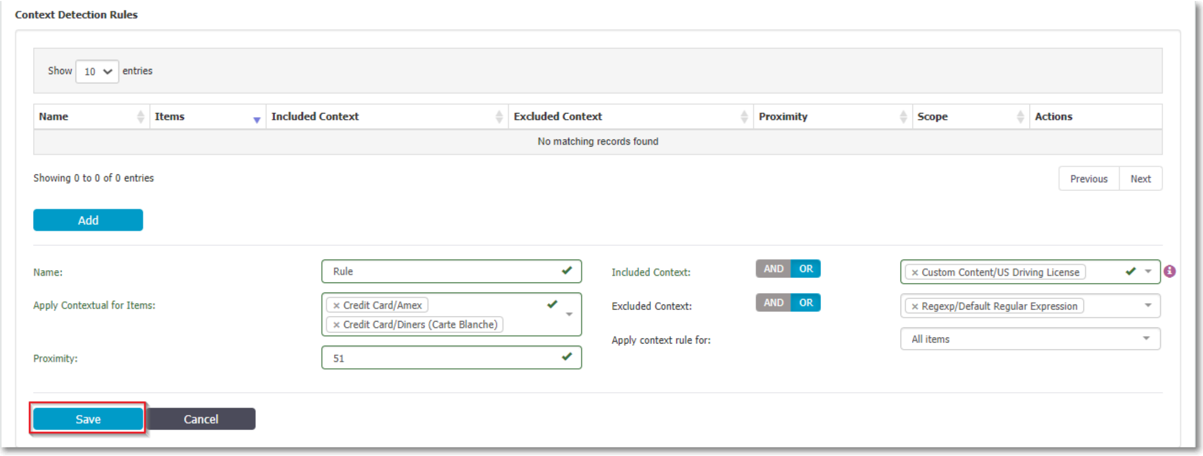
To create a new **Context Detection Rules** click **Add,** fill in the following and then **Save**:

- **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.



Context Detection Rules

Show 10 entries

Name	Items	Included Context	Excluded Context	Proximity	Scope	Actions
No matching records found						

Showing 0 to 0 of 0 entries

Name: Rule

Apply Contextual for Items: × Credit Card/Amex × Credit Card/Diners (Carte Blanche)

Proximity: 51

Included Context: AND OR × Custom Content/US Driving License

Excluded Context: AND OR × Regexp/Default Regular Expression

Apply context rule for: All items

Important: To address conflicts between per-policy and Global Contextual Rules, EPP clients no longer receive Global Contextual Rules if at least one policy has its individual Contextual Rule set. This marks the deprecation of Global Contextual Rules, emphasizing the prioritization of individual policy configurations.

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 PIIs, the SSN will detect the same entity.

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

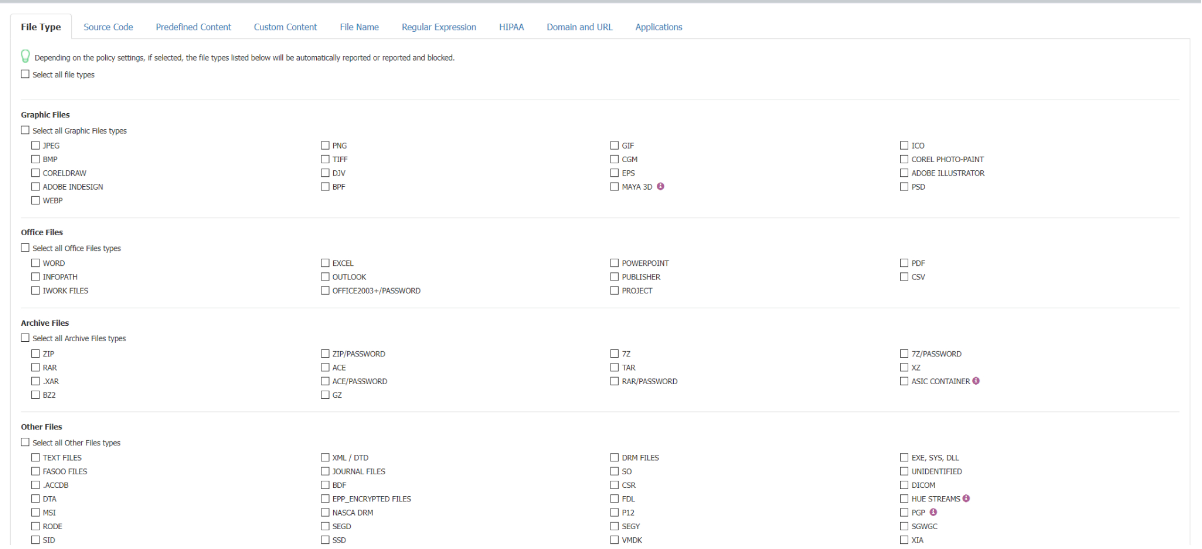
To maintain compatibility with older agent versions after the server upgrade, Italian ID will remain under section ID and server upgrade will retain previous settings, including Italian ID.

  - 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**
- **File Name**
- **File Location**
- **Regular Expressions**
- **HIPAA**
- **Domain and URL**



Depending on the policy settings, if selected, the file types listed below will be automatically reported or reported and blocked.

□ Select all file types

Graphic Files

□ Select all Graphic Files types

□ JPEG	□ PNG	□ GIF	□ ICO
□ BMP	□ TIFF	□ CGM	□ COREL PHOTO-PAINT
□ CORELDRAW	□ DJV	□ EPS	□ ADOBE ILLUSTRATOR
□ ADOBE INDESIGN	□ BPF	□ MAYA 3D	□ PSD
□ WEBP			

Office Files

□ Select all Office Files types

□ WORD	□ EXCEL	□ POWERPOINT	□ PDF
□ INFOPATH	□ OUTLOOK	□ PUBLISHER	□ CSV
□ IWORK FILES	□ OFFICE2003+/PASSWORD	□ PROJECT	

Archive Files

□ Select all Archive Files types

□ ZIP	□ ZIP/PASSWORD	□ 7Z	□ 7Z/PASSWORD
□ RAR	□ ACE	□ TAR	□ XZ
□ .XAR	□ ACE/PASSWORD	□ RAR/PASSWORD	□ ASIC CONTAINER
□ BZ2	□ GZ		

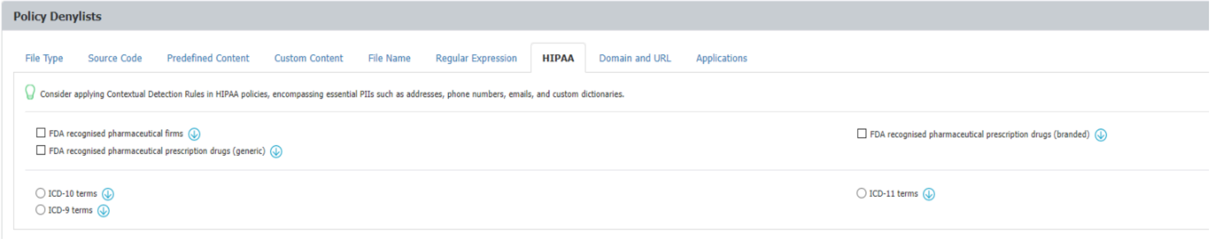
Other Files

□ Select all Other Files types

□ TEXT FILES	□ XML / DTD	□ DRM FILES	□ EXE, SYS, DLL
□ FASOO FILES	□ JOURNAL FILES	□ SO	□ UNIDENTIFIED
□ .ACCDB	□ BDF	□ CSR	□ DICOM
□ DTA	□ EPP_ENCRYPTED FILES	□ FDL	□ HUE STREAMS
□ MSI	□ NASCA DRM	□ P12	□ PGP
□ RODE	□ SEGD	□ SEGY	□ SGWGC
□ SID	□ SSD	□ VMDK	□ XIA

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.



Consider applying Contextual Detection Rules in HIPAA policies, encompassing essential PIIs such as addresses, phone numbers, emails, and custom dictionaries.

□ FDA recognised pharmaceutical firms

□ FDA recognised pharmaceutical prescription drugs (generic)

□ FDA recognised pharmaceutical prescription drugs (branded)

○ ICD-10 terms

○ ICD-9 terms

○ ICD-11 terms

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:

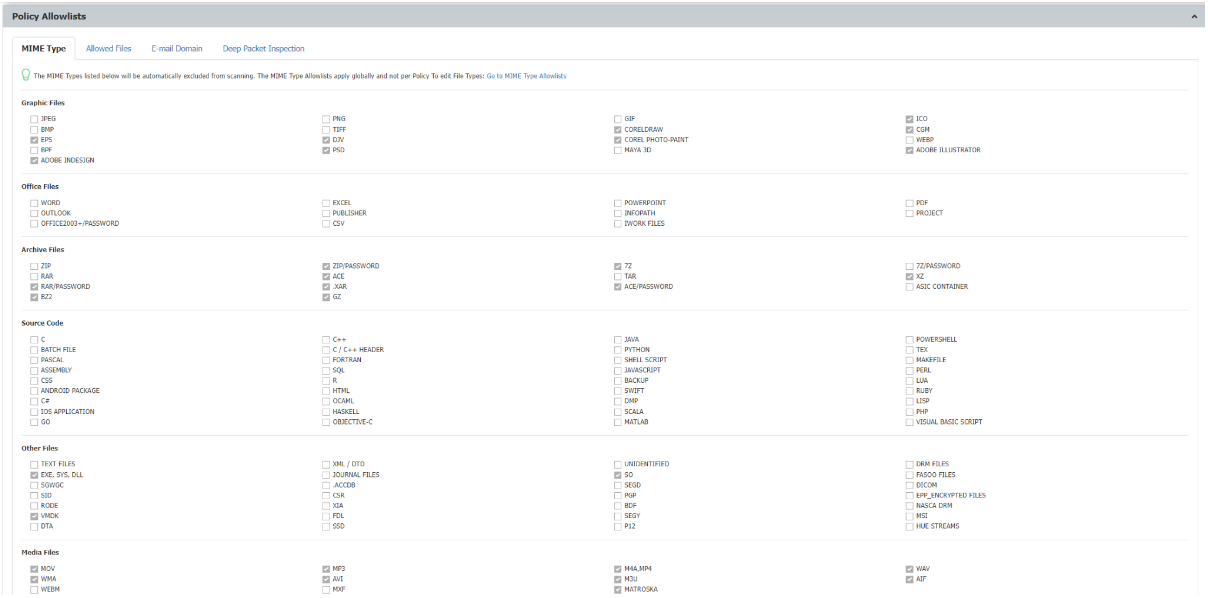
- **MIME Type**
- **Allowed Files**
- **File Location**
- **Network Share**
- **E-mail Domain**

- **URL Name**
- **Deep Packet Inspection**

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.



Policy Allowlists

The MIME Types listed below will be automatically excluded from scanning. The MIME Type Allowlists apply globally and not per Policy To edit File Types: Go to MIME Type Allowlists

Graphic Files

☐ JPEG
☐ BMP
☑ EPS
☐ BPF
☑ ADOBE INDESIGN
☐ PNG
☐ TIFF
☑ DJV
☑ PSD
☐ GIF
☑ CORELDRAW
☑ COREL PHOTO-PAINT
☐ MAYA 3D
☑ ICO
☑ CGM
☐ WEBP
☑ ADOBE ILLUSTRATOR

Office Files

☐ WORD
☐ OUTLOOK
☐ OFFICE2003+/PASSWORD
☐ EXCEL
☐ PUBLISHER
☐ CSV
☐ POWERPOINT
☐ INFOPATH
☐ IWORK FILES
☐ PDF
☐ PROJECT

Archive Files

☐ ZIP
☐ RAR
☑ RAR/PASSWORD
☑ BZ2
☑ ZIP/PASSWORD
☑ ACE
☑ .XAR
☑ GZ
☑ 7Z
☐ TAR
☑ ACE/PASSWORD
☐ 7Z/PASSWORD
☑ XZ
☐ ASIC CONTAINER

Source Code

☐ C
☐ BATCH FILE
☐ PASCAL
☐ ASSEMBLY
☐ CSS
☐ ANDROID PACKAGE
☐ C#
☐ IOS APPLICATION
☐ GO
☐ C++
☐ C / C++ HEADER
☐ FORTRAN
☐ SQL
☐ R
☐ HTML
☐ OCAML
☐ HASKELL
☐ OBJECTIVE-C
☐ JAVA
☐ PYTHON
☐ SHELL SCRIPT
☐ JAVASCRIPT
☐ BACKUP
☐ SWIFT
☐ DMP
☐ SCALA
☐ MATLAB
☐ POWERSHELL
☐ TEX
☐ MAKEFILE
☐ PERL
☐ LUA
☐ RUBY
☐ LISP
☐ PHP
☐ VISUAL BASIC SCRIPT

Other Files

☐ TEXT FILES
☑ EXE, SYS, DLL
☐ SGWGC
☐ SID
☐ RODE
☑ VMDK
☐ DTA
☐ XML / DTD
☐ JOURNAL FILES
☐ .ACCDB
☐ CSR
☐ XIA
☐ FDL
☐ SSD
☐ UNIDENTIFIED
☑ SO
☐ SEGD
☐ PGP
☐ BDF
☐ SEGY
☐ P12
☐ DRM FILES
☐ FASOO FILES
☐ DICOM
☐ EPP_ENCRYPTED FILES
☐ NASCA DRM
☐ MSI
☐ HUE STREAMS

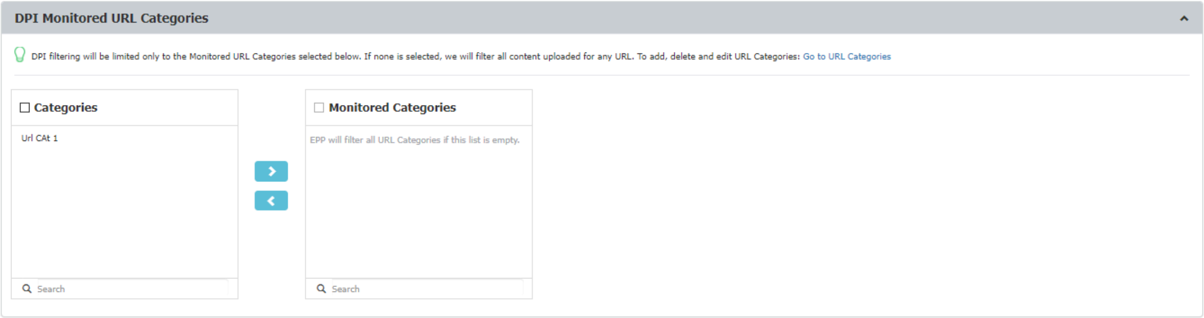
Media Files

☑ MOV
☑ WMA
☐ WEBM
☑ MP3
☑ AVI
☐ MXF
☑ M4A,MP4
☑ M3U
☑ MATROSKA
☑ WAV
☑ AIF

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.



DPI Monitored URL Categories

DPI filtering will be limited only to the Monitored URL Categories selected below. If none is selected, we will filter all content uploaded for any URL. To add, delete and edit URL Categories: Go to URL Categories

☐ Categories

Url CAt 1

☐ Monitored Categories

EPP will filter all URL Categories if this list is empty.

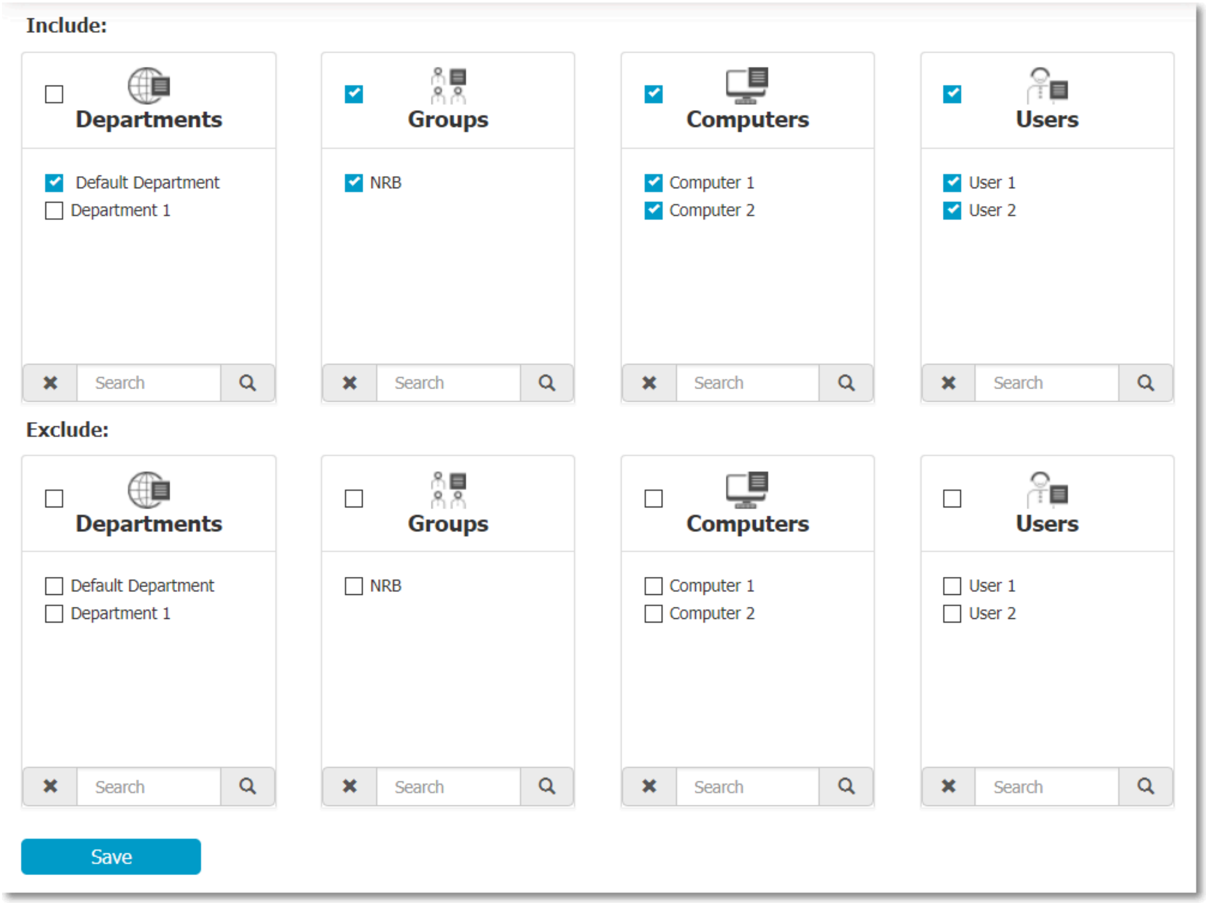
6.3.6. Policy Entities

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.



Include:

□ Departments
☑ Default Department
□ Department 1

☑ Groups
☑ NRB

☑ Computers
☑ Computer 1
☑ Computer 2

☑ Users
☑ User 1
☑ User 2

Exclude:

□ Departments
□ Default Department
□ Department 1

□ Groups
□ NRB

□ Computers
□ Computer 1
□ Computer 2

□ Users
□ User 1
□ User 2

6.3.7. Block and Remediate Policies

Block and Remediate policies are a category of Content Aware Policies. This category of policies gives the end-user the possibility to resolve the Content Aware threats by using justifications.

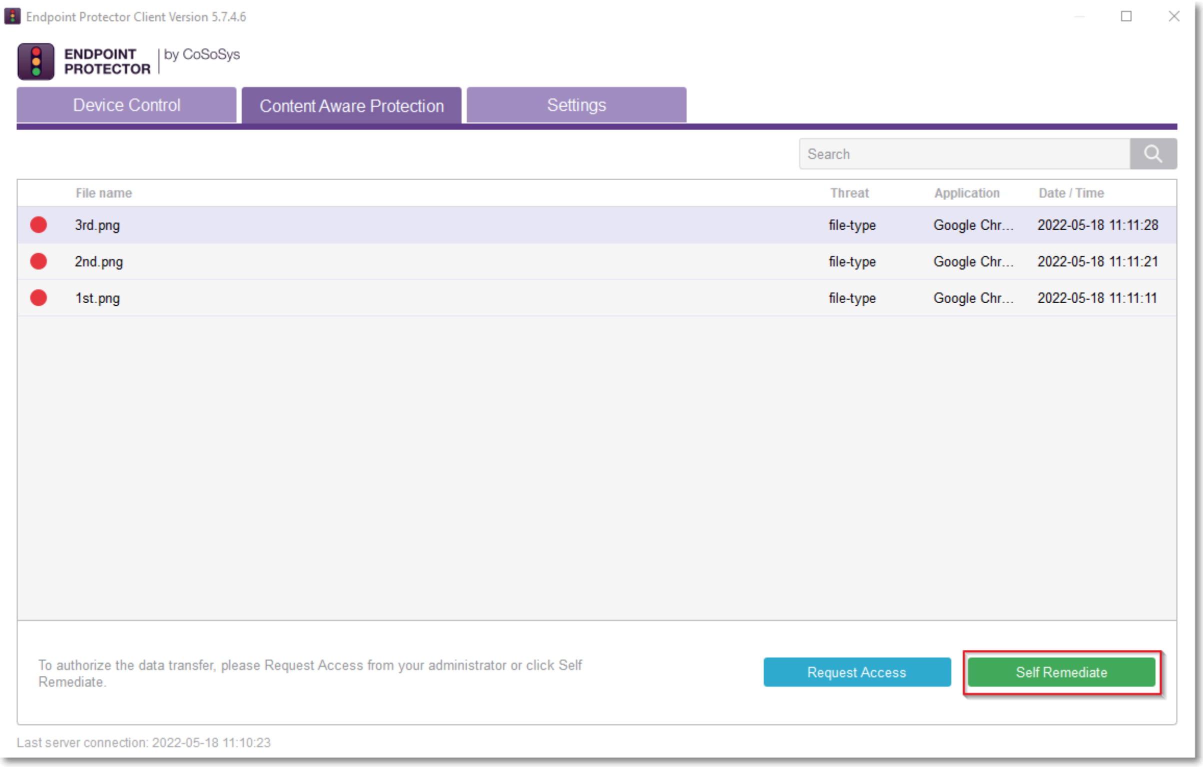
You can create Block and Remediate Content Aware Policies from the Content Aware Protection section, Create Content Aware Policies, Policy Action, Block and Remediate.

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**;



	File name	Threat	Application	Date / Time
●	3rd.png	file-type	Google Chr...	2022-05-18 11:11:28
●	2nd.png	file-type	Google Chr...	2022-05-18 11:11:21
●	1st.png	file-type	Google Chr...	2022-05-18 11:11:11

To authorize the data transfer, please Request Access from your administrator or click Self Remediate.

Last server connection: 2022-05-18 11:10:23

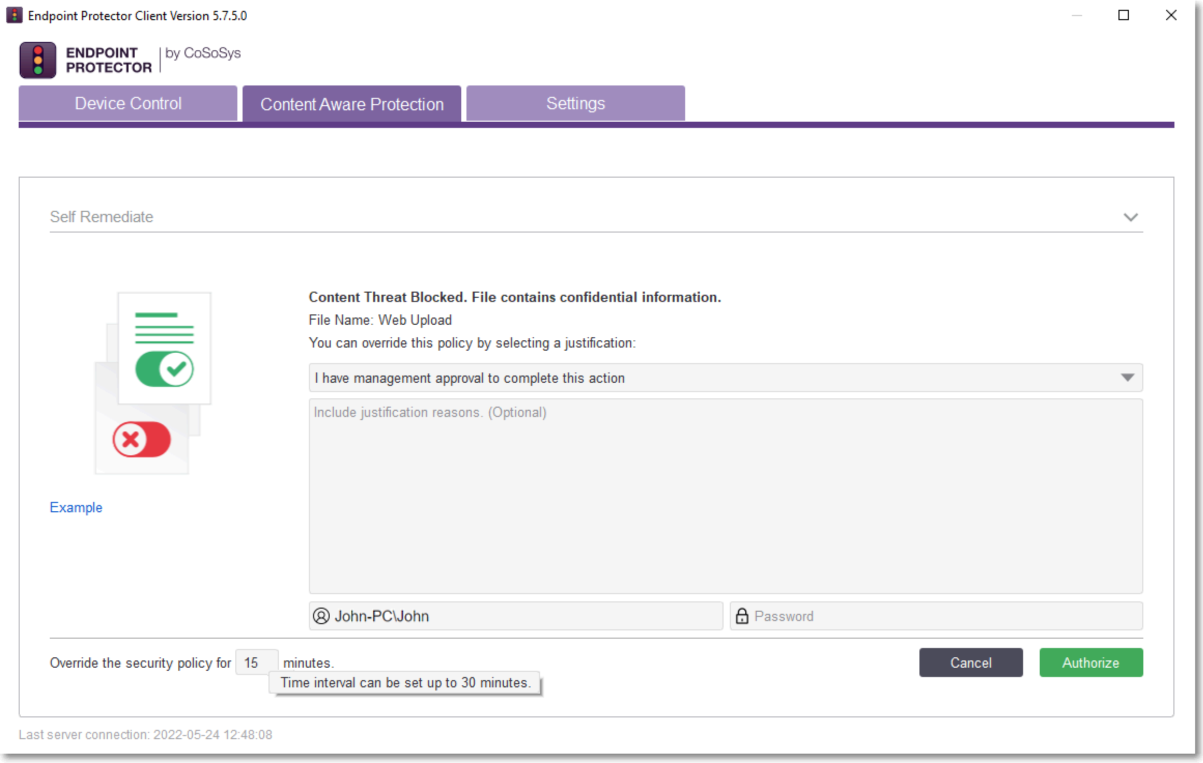
3. On the **Self Remediate** section:
   a. select a **justification** from the drop-down list
   b. add a **reason** for the justification (if required)
   c. navigate to the **custom URL** situated under the logo
   d. add your credentials if the **Require Credentials** setting was enabled (click the 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 Actions column.



Content Threat Blocked. File contains confidential information.

File Name: Web Upload

You can override this policy by selecting a justification:

I have management approval to complete this action

Include justification reasons. (Optional)

John-PC\John

Password

Override the security policy for 15 minutes.

Time interval can be set up to 30 minutes.

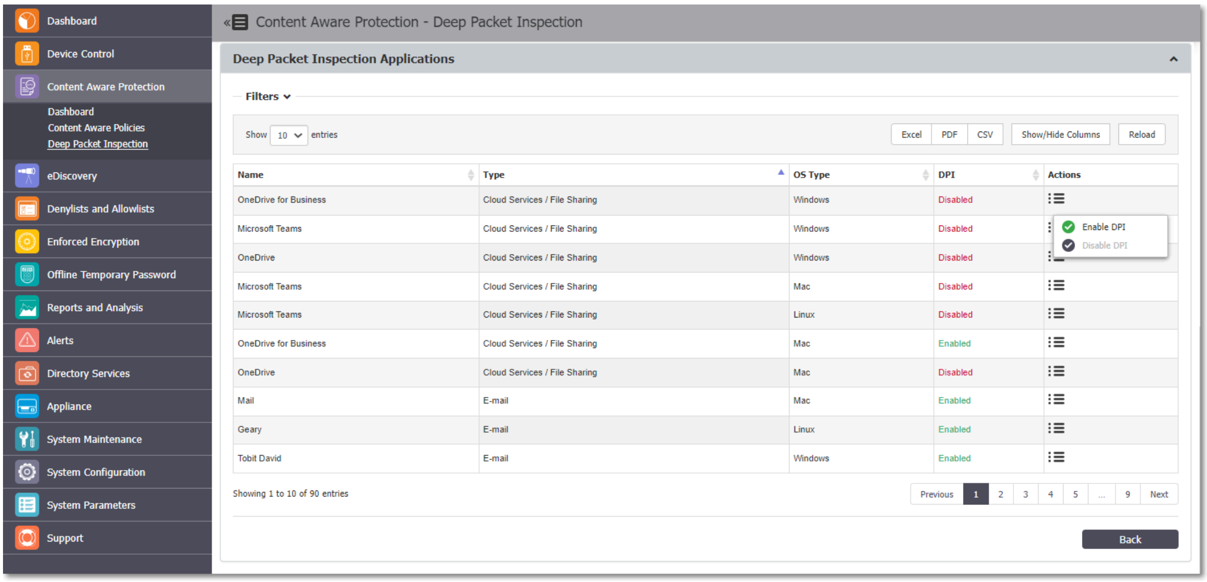
Last server connection: 2022-05-24 12:48:08

- **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.



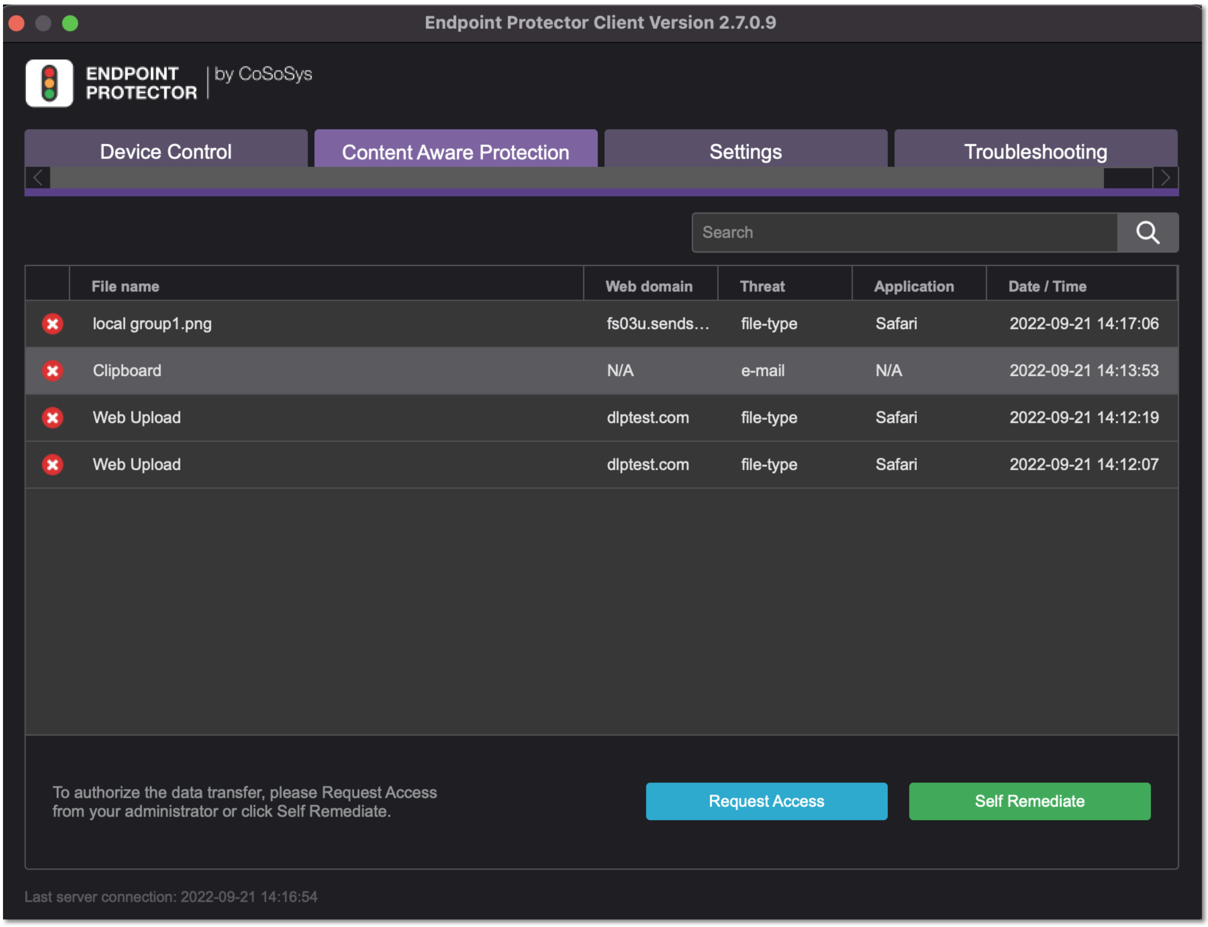
Content Aware Protection - Deep Packet Inspection

Deep Packet Inspection Applications

Name	Type	OS Type	DPI	Actions
OneDrive for Business	Cloud Services / File Sharing	Windows	Disabled	
Microsoft Teams	Cloud Services / File Sharing	Windows	Disabled	Enable DPI Disable DPI
OneDrive	Cloud Services / File Sharing	Windows	Disabled	
Microsoft Teams	Cloud Services / File Sharing	Mac	Disabled	
Microsoft Teams	Cloud Services / File Sharing	Linux	Disabled	
OneDrive for Business	Cloud Services / File Sharing	Mac	Enabled	
OneDrive	Cloud Services / File Sharing	Mac	Disabled	
Mail	E-mail	Mac	Enabled	
Geary	E-mail	Linux	Enabled	
Tobit David	E-mail	Windows	Enabled	

Showing 1 to 10 of 90 entries

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

File name	Web domain	Threat	Application	Date / Time
local group1.png	fs03u.sends…	file-type	Safari	2022-09-21 14:17:06
Clipboard	N/A	e-mail	N/A	2022-09-21 14:13:53
Web Upload	dlptest.com	file-type	Safari	2022-09-21 14:12:19
Web Upload	dlptest.com	file-type	Safari	2022-09-21 14:12:07

To authorize the data transfer, please Request Access from your administrator or click Self Remediate.

Last server connection: 2022-09-21 14:16:54

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.

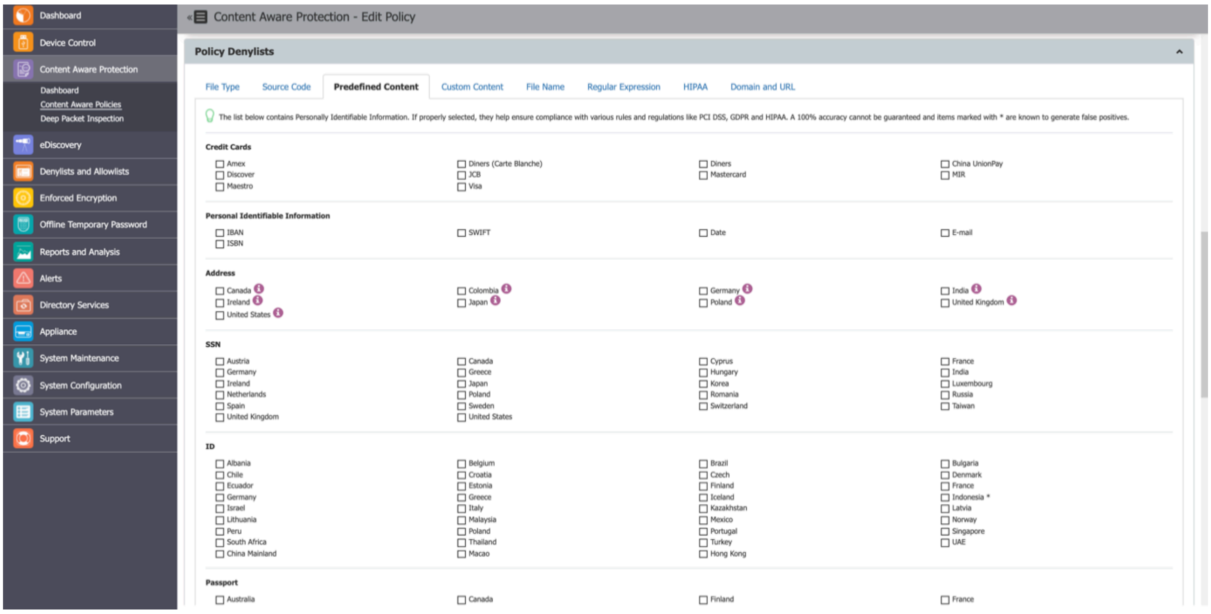
The following rules are used in the application of one or more Content Aware Policies on a computer/user/group/department for each separately selected item (e.g., a specific file type, predefined information, or a custom content dictionary):

Policy A with Priority 1	Policy B with Priority 2	Policy C with Priority 3	Endpoint Protector Action
IGNORED	IGNORED	IGNORED	Information will not be blocked or reported.
IGNORED	IGNORED	*REPORTED*	Information will be reported.
IGNORED	*REPORTED*	*REPORTED*	Information will be reported.
REPORTED	*REPORTED*	*REPORTED*	Information will be reported.
IGNORED	IGNORED	**BLOCKED**	Information will be blocked.
IGNORED	**BLOCKED**	**BLOCKED**	Information will be blocked.
BLOCKED	**BLOCKED**	**BLOCKED**	Information will be blocked.
IGNORED	*REPORTED*	**BLOCKED**	Information will be reported.
IGNORED	**BLOCKED**	*REPORTED*	Information will be blocked.
REPORTED	IGNORED	**BLOCKED**	Information will be reported.
BLOCKED	IGNORED	*REPORTED*	Information will be blocked.

REPORTED	**BLOCKED**	IGNORED	Information will be reported.
BLOCKED	*REPORTED*	IGNORED	Information will be blocked.

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.



The list below contains Personally Identifiable Information. If properly selected, they help ensure compliance with various rules and regulations like PCI DSS, GDPR and HIPAA. A 100% accuracy cannot be guaranteed and items marked with * are known to generate false positives.

Credit Cards

☐ Amex ☐ Discover ☐ Maestro ☐ Diners (Carte Blanche) ☐ JCB ☐ Visa ☐ Diners ☐ Mastercard ☐ China UnionPay ☐ MIR

Personal Identifiable Information

☐ IBAN ☐ ISBN ☐ SWIFT ☐ Date ☐ E-mail

Address

☐ Canada ☐ Ireland ☐ United States ☐ Colombia ☐ Japan ☐ Germany ☐ Poland ☐ India ☐ United Kingdom

SSN

☐ Austria ☐ Germany ☐ Ireland ☐ Netherlands ☐ Spain ☐ United Kingdom ☐ Canada ☐ Greece ☐ Japan ☐ Poland ☐ Sweden ☐ United States ☐ Cyprus ☐ Hungary ☐ Korea ☐ Romania ☐ Switzerland ☐ France ☐ India ☐ Luxembourg ☐ Russia ☐ Taiwan

ID

☐ Albania ☐ Chile ☐ Ecuador ☐ Germany ☐ Israel ☐ Lithuania ☐ Peru ☐ South Africa ☐ China Mainland ☐ Belgium ☐ Croatia ☐ Estonia ☐ Greece ☐ Italy ☐ Malaysia ☐ Poland ☐ Thailand ☐ Macao ☐ Brazil ☐ Czech ☐ Finland ☐ Iceland ☐ Kazakhstan ☐ Mexico ☐ Portugal ☐ Turkey ☐ Hong Kong ☐ Bulgaria ☐ Denmark ☐ France ☐ Indonesia * ☐ Latvia ☐ Norway ☐ Singapore ☐ UAE

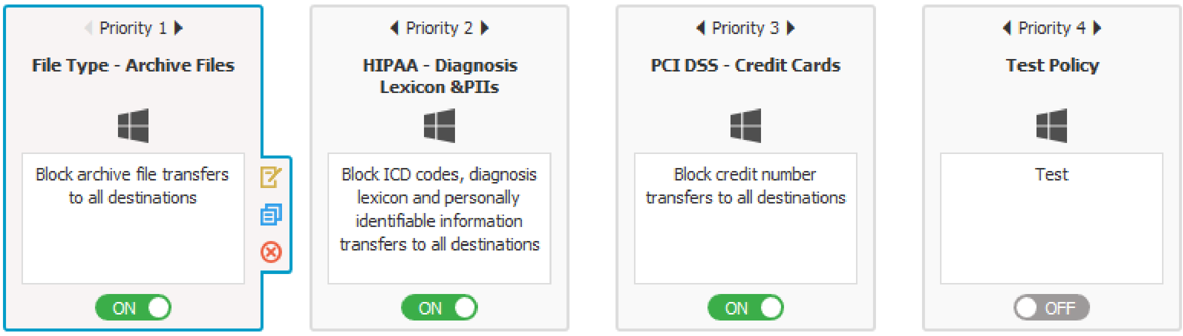
Passport

☐ Australia ☐ Canada ☐ Finland ☐ France

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.



Priority 1
File Type - Archive Files
Block archive file transfers to all destinations
ON

Priority 2
HIPAA - Diagnosis Lexicon &PIIs
Block ICD codes, diagnosis lexicon and personally identifiable information transfers to all destinations
ON

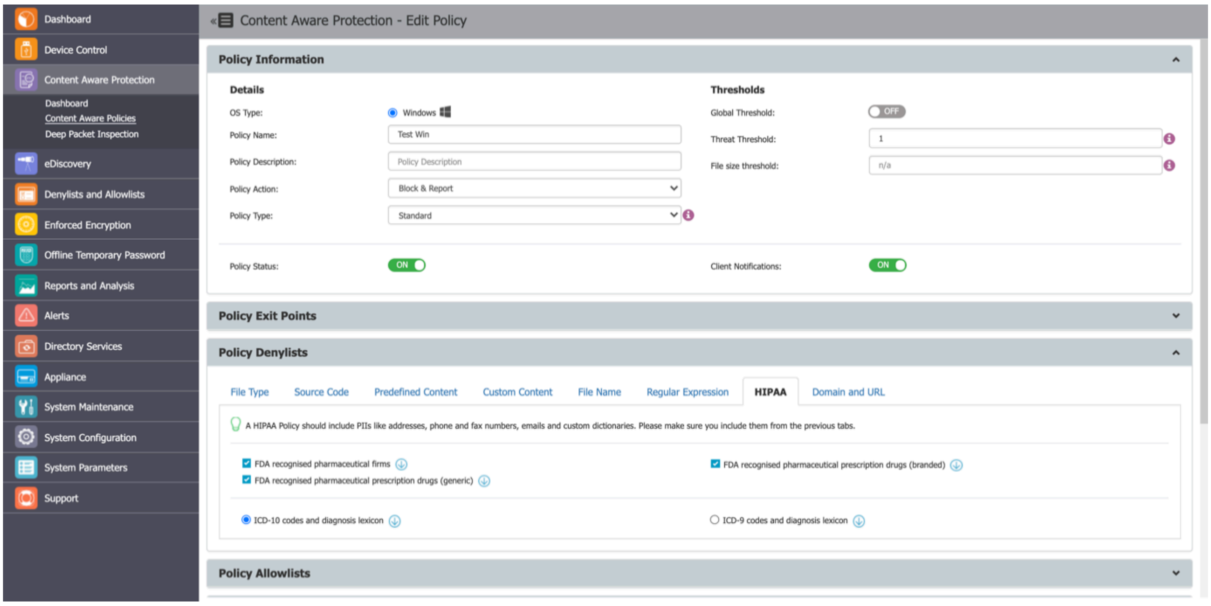
Priority 3
PCI DSS - Credit Cards
Block credit number transfers to all destinations
ON

Priority 4
Test Policy
Test
OFF

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:



Content Aware Protection - Edit Policy

Policy Information

Details

OS Type: ● Windows

Policy Name: Test Win

Policy Description: Policy Description

Policy Action: Block & Report

Policy Type: Standard

Policy Status: ON

Thresholds

Global Threshold: OFF

Threat Threshold: 1

File size threshold: n/a

Client Notifications: ON

Policy Exit Points

Policy Denylists

A HIPAA Policy should include PIIs like addresses, phone and fax numbers, emails and custom dictionaries. Please make sure you include them from the previous tabs.

☑ FDA recognised pharmaceutical firms
☑ FDA recognised pharmaceutical prescription drugs (generic)
☑ FDA recognised pharmaceutical prescription drugs (branded)

● ICD-10 codes and diagnosis lexicon
○ ICD-9 codes and diagnosis lexicon

Policy Allowlists

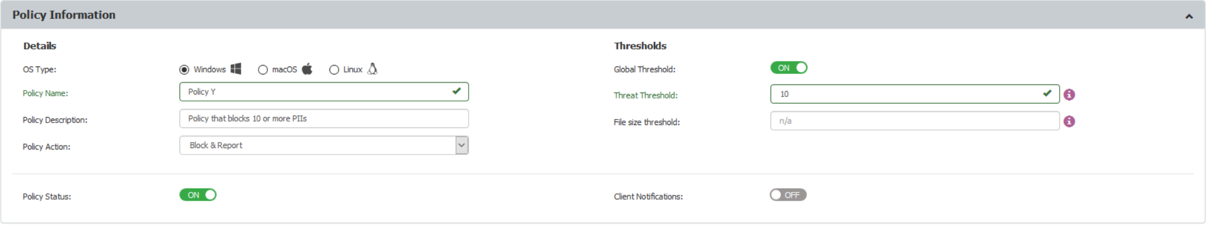
This policy is set on Block & Report with a Global Threshold of 4. It scans the Controlled Storage Device Types (which can be inspected from the System Parameters > Device Types), the Clipboard, and the Network Share as well as all the database of applications recognized by Endpoint Protector. This policy 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:



Policy Information

Details

OS Type: ● Windows ○ macOS ○ Linux

Policy Name: Policy Y ✓

Policy Description: Policy that blocks 10 or more PIIs

Policy Action: Block & Report

Policy Status: ON

Thresholds

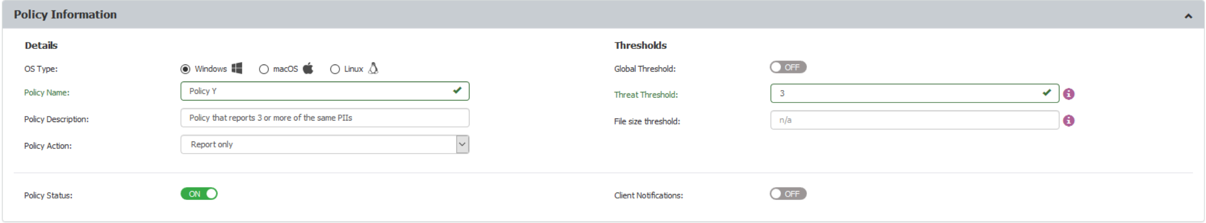
Global Threshold: ON

Threat Threshold: 10 ✓

File size threshold: n/a

Client Notifications: OFF

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

Details

OS Type: ● Windows ○ macOS ○ Linux

Policy Name: Policy Y ✓

Policy Description: Policy that reports 3 or more of the same PIIs

Policy Action: Report only

Policy Status: ON

Thresholds

Global Threshold: OFF

Threat Threshold: 3 ✓

File size threshold: n/a

Client Notifications: OFF

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).

Important: Newer Linux Ubuntu versions have 'snap'-based applications installed by default, affecting EPP Client functionality. This may result in missing file-related events in DPI file resolution. The reliance on 'snap'-based applications also affects file-related web browser activities, exacerbating this limitation. Consider non-'snap'-based applications (where possible) as alternative configurations for optimal functionality.

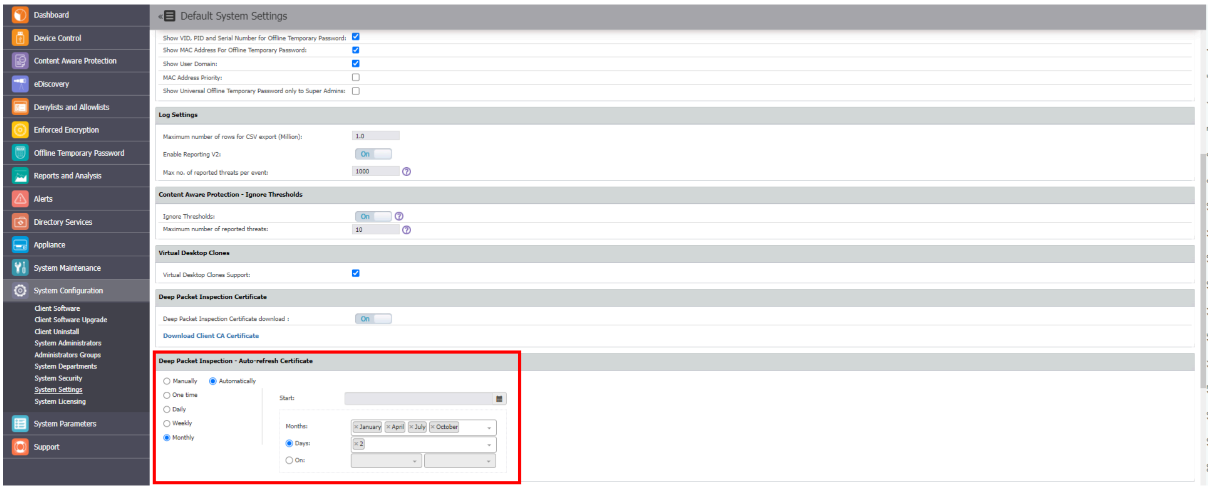
6.4.1. Deep Packet Inspection Certificate

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.



Default System Settings

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: ☐

Log Settings

Maximum number of rows for CSV export (Million): 1.0
Enable Reporting V2: On
Max no. of reported threats per event: 1000

Content Aware Protection - Ignore Thresholds

Ignore Thresholds: On
Maximum number of reported threats: 10

Virtual Desktop Clones

Virtual Desktop Clones Support: ☑

Deep Packet Inspection Certificate

Deep Packet Inspection Certificate download : On
Download Client CA Certificate

Deep Packet Inspection - Auto-refresh Certificate

○ Manually ● Automatically
○ One time
○ Daily
○ Weekly
● Monthly

Start:
Months: January, April, July, October
● Days: 2
○ On:

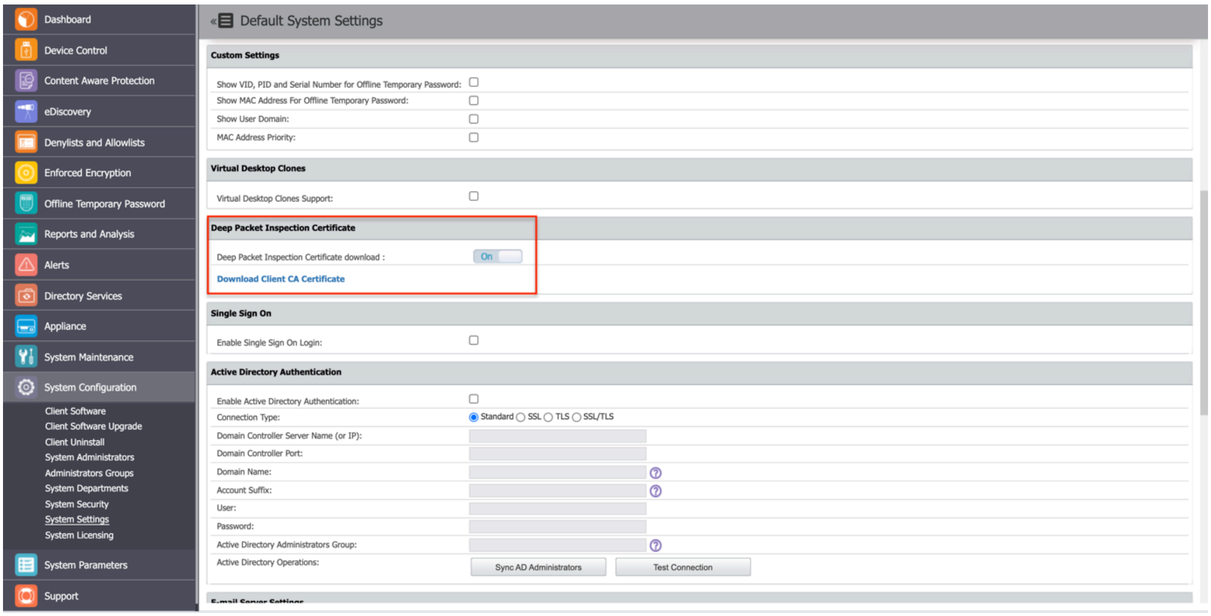
6.4.2. Deep Packet Inspection Certificate on macOS

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**.



Default System Settings

Custom Settings

Show VID, PID and Serial Number for Offline Temporary Password: □

Show MAC Address For Offline Temporary Password: □

Show User Domain: □

MAC Address Priority: □

Virtual Desktop Clones

Virtual Desktop Clones Support: □

Deep Packet Inspection Certificate

Deep Packet Inspection Certificate download : On

Download Client CA Certificate

Single Sign On

Enable Single Sign On Login: □

Active Directory Authentication

Enable Active Directory Authentication: □

Connection Type: ● Standard ○ SSL ○ TLS ○ SSL/TLS

Domain Controller Server Name (or IP):

Domain Controller Port:

Domain Name:

Account Suffix:

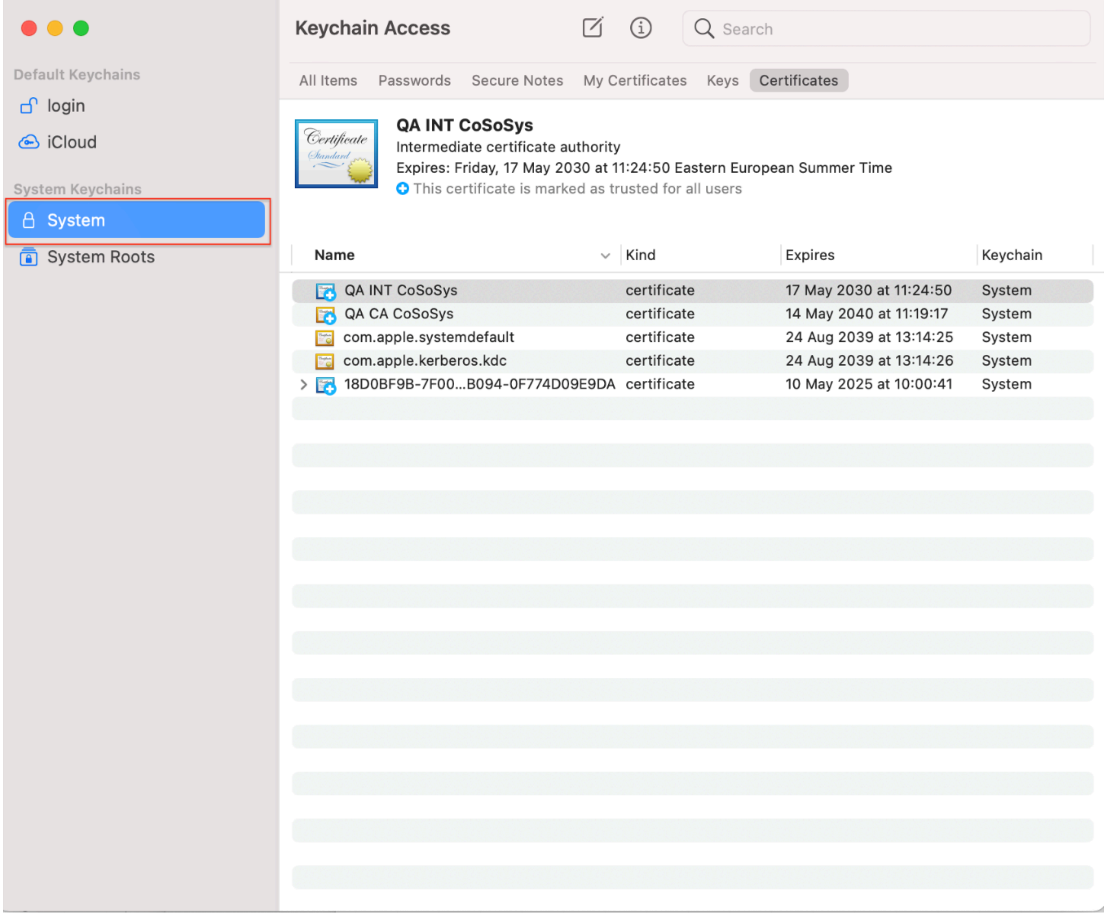
User:

Password:

Active Directory Administrators Group:

Active Directory Operations: Sync AD Administrators | Test Connection

2. Open the **Keychain Access** application from your macOS and select **System**.

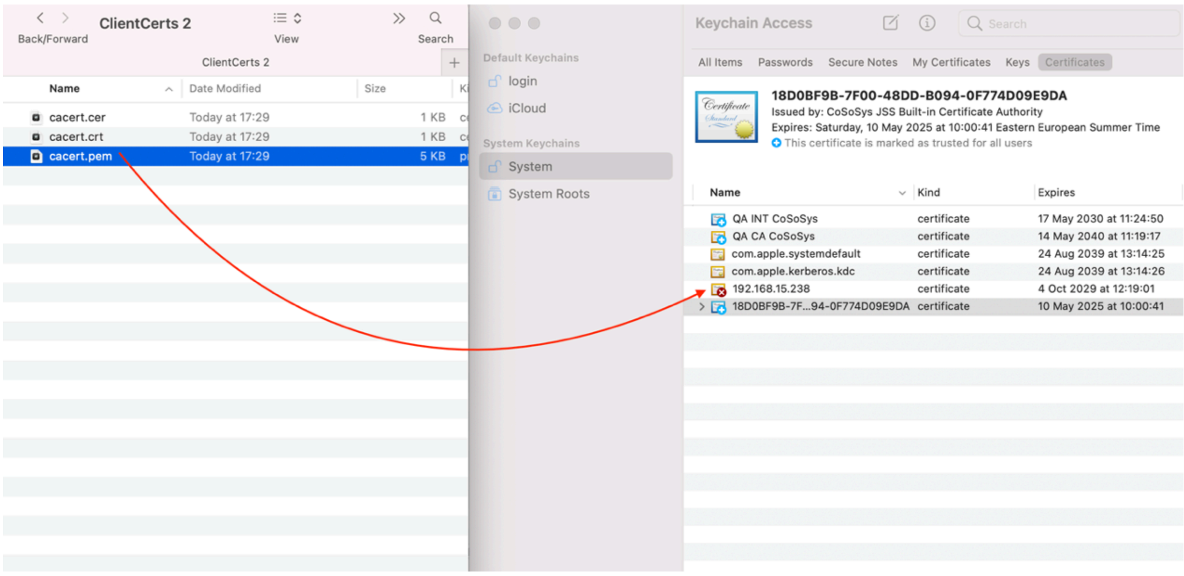


QA INT CoSoSys
Intermediate certificate authority
Expires: Friday, 17 May 2030 at 11:24:50 Eastern European Summer Time
This certificate is marked as trusted for all users

Name	Kind	Expires	Keychain
QA INT CoSoSys	certificate	17 May 2030 at 11:24:50	System
QA CA CoSoSys	certificate	14 May 2040 at 11:19:17	System
com.apple.systemdefault	certificate	24 Aug 2039 at 13:14:25	System
com.apple.kerberos.kdc	certificate	24 Aug 2039 at 13:14:26	System
18D0BF9B-7F00...B094-0F774D09E9DA	certificate	10 May 2025 at 10:00:41	System

3. Decompress the downloaded **ClientCerts** file.

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

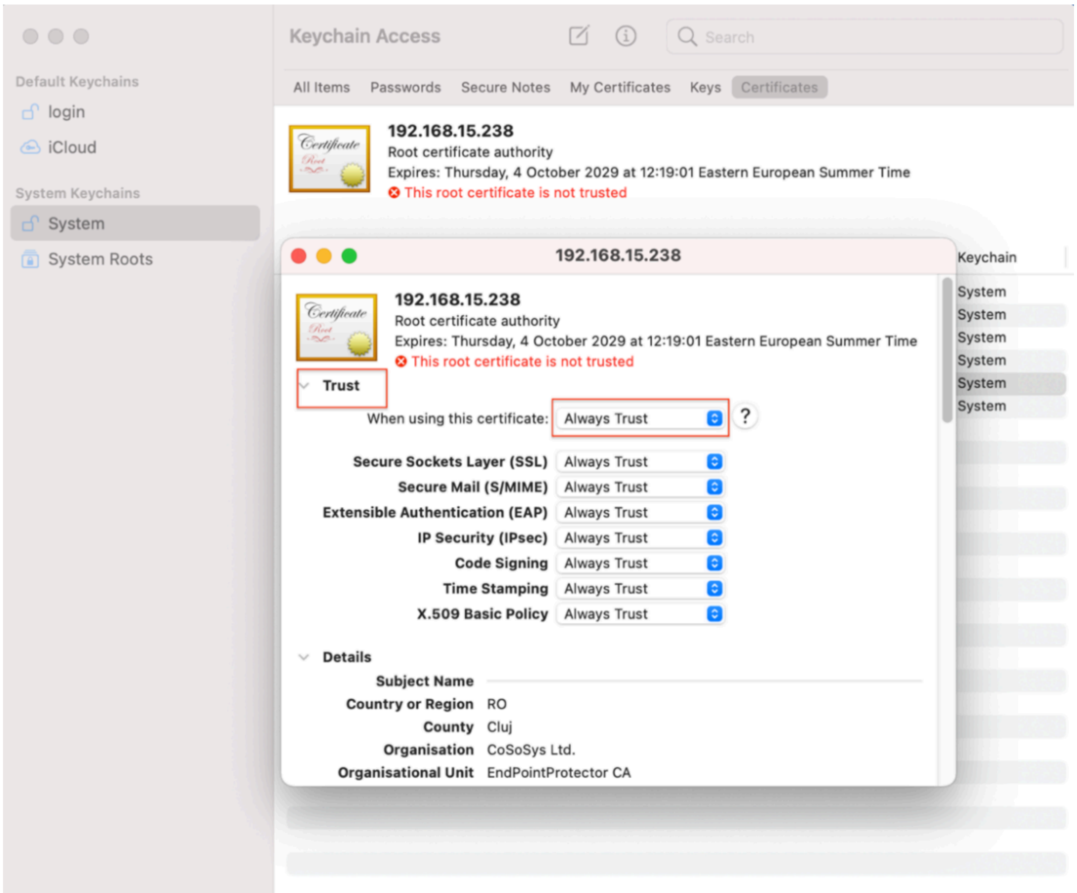


Name	Date Modified	Size
cacert.cer	Today at 17:29	1 KB
cacert.crt	Today at 17:29	1 KB
cacert.pem	Today at 17:29	5 KB

18D0BF9B-7F00-48DD-B094-0F774D09E9DA
Issued by: CoSoSys JSS Built-in Certificate Authority
Expires: Saturday, 10 May 2025 at 10:00:41 Eastern European Summer Time
This certificate is marked as trusted for all users

Name	Kind	Expires
QA INT CoSoSys	certificate	17 May 2030 at 11:24:50
QA CA CoSoSys	certificate	14 May 2040 at 11:19:17
com.apple.systemdefault	certificate	24 Aug 2039 at 13:14:25
com.apple.kerberos.kdc	certificate	24 Aug 2039 at 13:14:26
192.168.15.238	certificate	4 Oct 2029 at 12:19:01
18D0BF9B-7F...94-0F774D09E9DA	certificate	10 May 2025 at 10:00:41

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



192.168.15.238
Root certificate authority
Expires: Thursday, 4 October 2029 at 12:19:01 Eastern European Summer Time
This root certificate is not trusted

192.168.15.238

192.168.15.238
Root certificate authority
Expires: Thursday, 4 October 2029 at 12:19:01 Eastern European Summer Time
This root certificate is not trusted

Trust

When using this certificate: Always Trust

Secure Sockets Layer (SSL): Always Trust
Secure Mail (S/MIME): Always Trust
Extensible Authentication (EAP): Always Trust
IP Security (IPsec): Always Trust
Code Signing: Always Trust
Time Stamping: Always Trust
X.509 Basic Policy: Always Trust

Details

Subject Name
Country or Region: RO
County: Cluj
Organisation: CoSoSys Ltd.
Organisational Unit: EndPointProtector CA

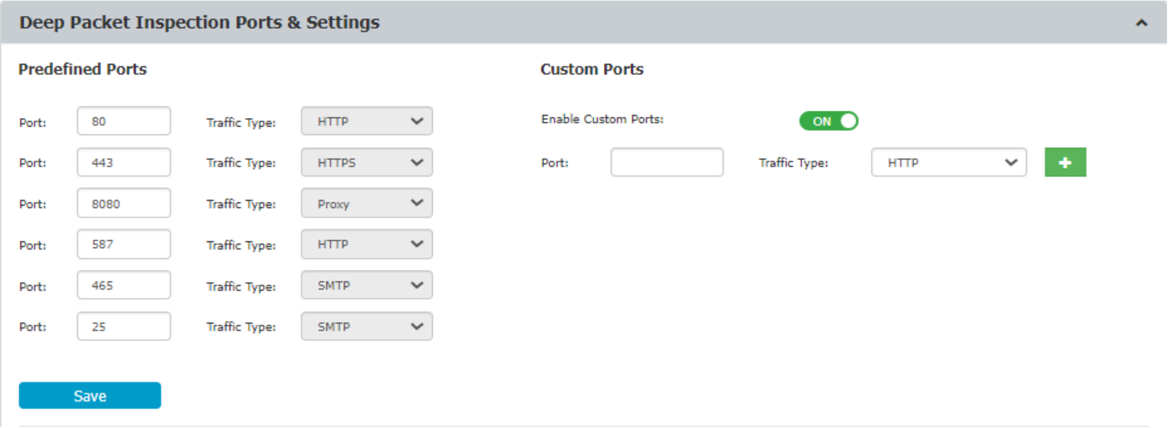
6. **Save** the changes.

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.



Deep Packet Inspection Ports & Settings

Predefined Ports

Port:	80	Traffic Type:	HTTP
Port:	443	Traffic Type:	HTTPS
Port:	8080	Traffic Type:	Proxy
Port:	587	Traffic Type:	HTTP
Port:	465	Traffic Type:	SMTP
Port:	25	Traffic Type:	SMTP

Custom Ports

Enable Custom Ports: ON

Port: Traffic Type: HTTP

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: For comprehensive visibility while using **'Teams over web'** in a MS Edge browser, make sure to enable **'Edge'** under **'Policy Exits Points -> Applications -> Web Browser'** in the CAP policy.

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.

- **Detailed Slack Reporting** – to access this setting, ensure **Text Inspection** is enabled and use **Reporting V2** from System Configuration -> System Settings. Once enabled, you can view Destination Details for Slack on the Content Aware Report page in the **Reports and Analysis** section.

Note: This setting requires an active Internet connection for the Endpoint Protector Client.

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

- **Monitor webmail –** Enable this setting to scan the 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.

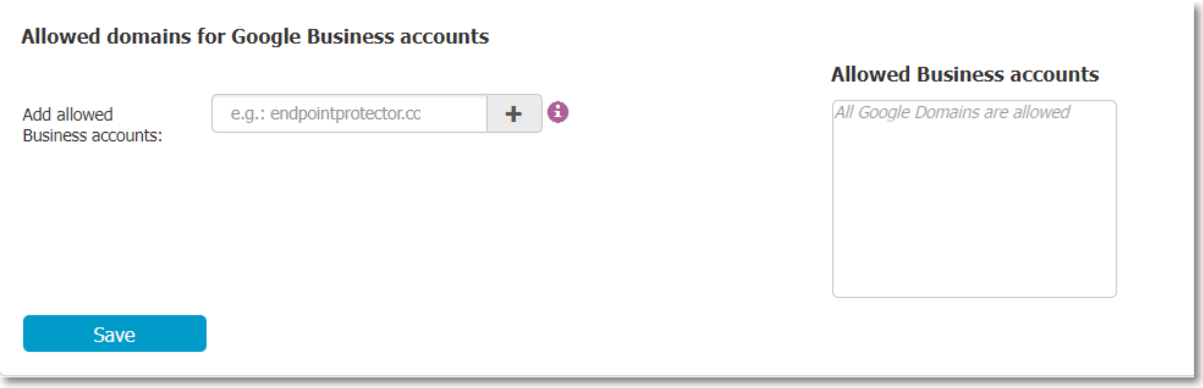
Note: Always use **Monitor webmail** with **Extended Source Code Detection** setting enabled.

- **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.


Allowed domains for Google Business accounts
Add allowed Business accounts:
e.g.: endpointprotector.cc
+
Allowed Business accounts
All Google Domains are allowed
Save

6.4.3.1. Monitor Webmail Json format parser usage

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[:].payloadParts[:].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:

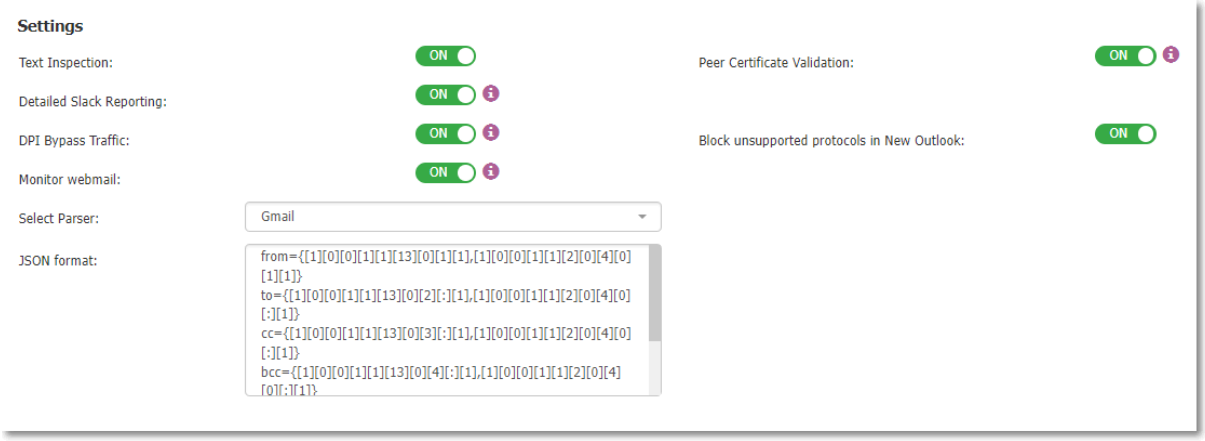
  - requests[0].payloadParts[:].payload.message.headers.subject
  - requests[1].payloadParts[:].payload.message.headers.subject
  - requests[2].payloadParts[:].payload.message.headers.subject

  The process is then repeated for the payloadParts array,

0. Subject extraction example for Gmail:

   subject={[1][0][0][1][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 [:]



Settings

Text Inspection:	ON	Peer Certificate Validation:	ON
Detailed Slack Reporting:	ON		
DPI Bypass Traffic:	ON	Block unsupported protocols in New Outlook:	ON
Monitor webmail:	ON		
Select Parser:	Gmail		

JSON format:

```
from={[1][0][0][1][1][13][0][1][1],[1][0][0][1][1][2][0][4][0][1][1]}
to={[1][0][0][1][1][13][0][2][:][1],[1][0][0][1][1][2][0][4][0][:][1]}
cc={[1][0][0][1][1][13][0][3][:][1],[1][0][0][1][1][2][0][4][0][:][1]}
bcc={[1][0][0][1][1][13][0][4][:][1],[1][0][0][1][1][2][0][4][0][:][1]}
```

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.

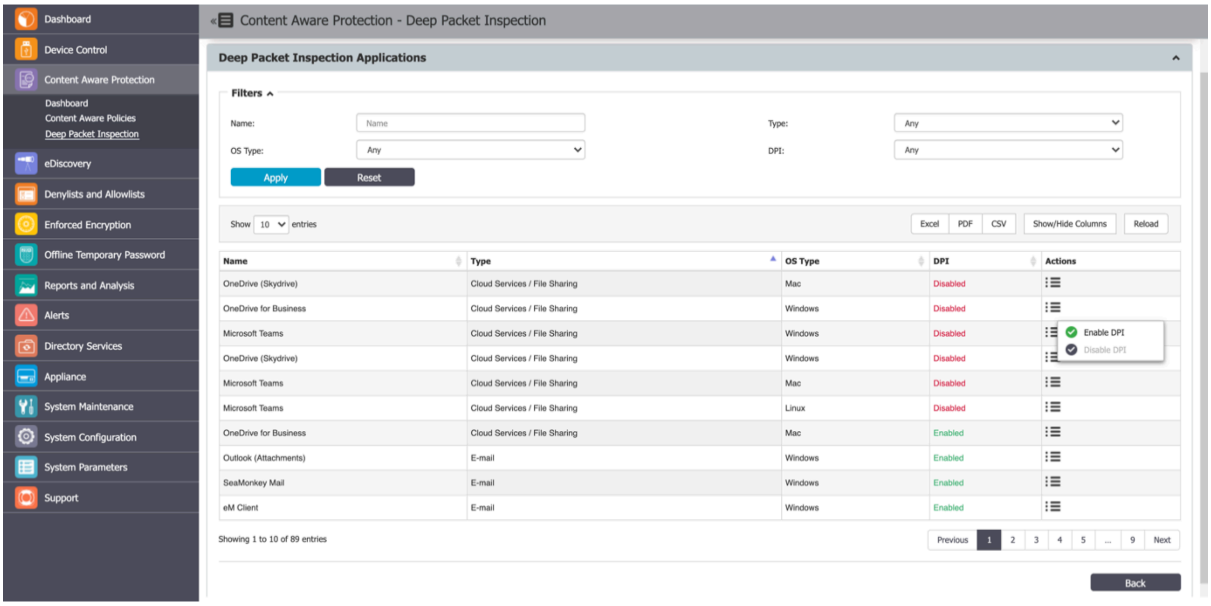
Example: Your organization uses an SSL inspection proxy or gateway. The certificates injected by the proxy or gateway cannot be validated on the endpoint because they are either invalid or the issuer CA certificate is not installed in the "Trusted Root Certification Authorities" in the computer certificate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



Content Aware Protection - Deep Packet Inspection

Deep Packet Inspection Applications

Filters

Name: Name

Type: Any

OS Type: Any

DPI: Any

Show 10 entries

Name	Type	OS Type	DPI	Actions
OneDrive (Skydrive)	Cloud Services / File Sharing	Mac	Disabled	☰
OneDrive for Business	Cloud Services / File Sharing	Windows	Disabled	☰
Microsoft Teams	Cloud Services / File Sharing	Windows	Disabled	☰
OneDrive (Skydrive)	Cloud Services / File Sharing	Windows	Disabled	☰
Microsoft Teams	Cloud Services / File Sharing	Mac	Disabled	☰
Microsoft Teams	Cloud Services / File Sharing	Linux	Disabled	☰
OneDrive for Business	Cloud Services / File Sharing	Mac	Enabled	☰
Outlook (Attachments)	E-mail	Windows	Enabled	☰
SeaMonkey Mail	E-mail	Windows	Enabled	☰
eM Client	E-mail	Windows	Enabled	☰

Showing 1 to 10 of 89 entries

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:

OS	is Available	isTrusted	Server Side
macOS	N/A	N/A	N/A
	N/A	0	N/A
	N/A	1	N/A

	0	N/A	Not added
	0	0	Not added
	0	1	Not added
	1	N/A	Not trusted
	1	0	Not trusted
	1	1	Trusted
Linux	N/A	N/A	N/A
	N/A	0	N/A
	N/A	1	N/A
	0	N/A	N/A
	0	0	N/A
	0	1	N/A
	1	N/A	N/A
	1	0	N/A
	1	1	N/A
Windows	N/A		N/A
	0		Not added
	1		Trusted

Note: Linux has dedicated certificate stores.

Note: On Windows, if the certificate is added, it is automatically trusted.

7. eDiscovery

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:

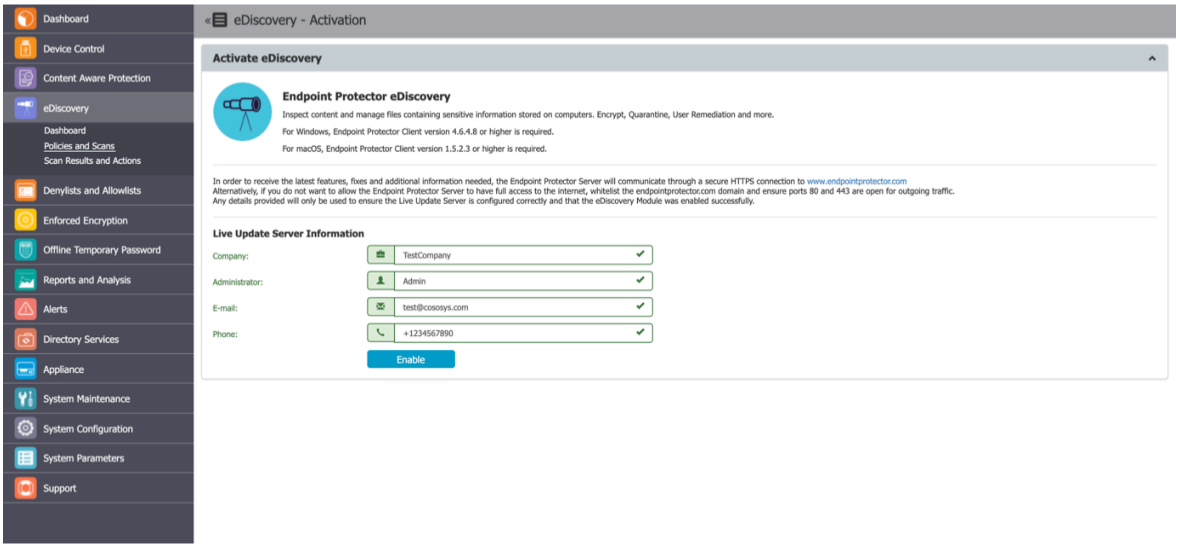
- **Personal Identifiable Information (PII):** social security numbers (SSN), driving license numbers, E-mail addresses, passport numbers, phone numbers, addresses, dates, etc.
- **Financial and credit card information**: credit card numbers for Visa, MasterCard, American Express, JCB, Discover Card, 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.



eDiscovery - Activation

Activate eDiscovery

Endpoint Protector eDiscovery

Inspect content and manage files containing sensitive information stored on computers. Encrypt, Quarantine, User Remediation and more.

For Windows, Endpoint Protector Client version 4.6.4.8 or higher is required.

For macOS, Endpoint Protector Client version 1.5.2.3 or higher is required.

In order to receive the latest features, fixes and additional information needed, the Endpoint Protector Server will communicate through a secure HTTPS connection to www.endpointprotector.com
Alternatively, if you do not want to allow the Endpoint Protector Server to have full access to the internet, whitelist the endpointprotector.com domain and ensure ports 80 and 443 are open for outgoing traffic.
Any details provided will only be used to ensure the Live Update Server is configured correctly and that the eDiscovery Module was enabled successfully.

Live Update Server Information

Company: TestCompany ✓

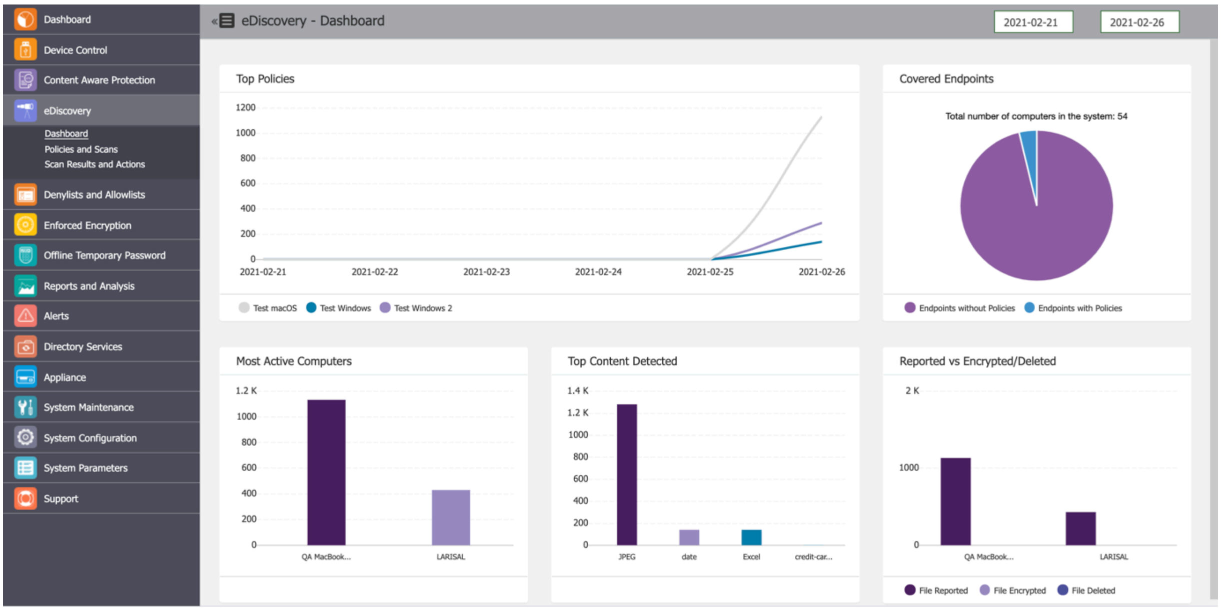
Administrator: Admin ✓

E-mail: test@cososys.com ✓

Phone: +1234567890 ✓

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

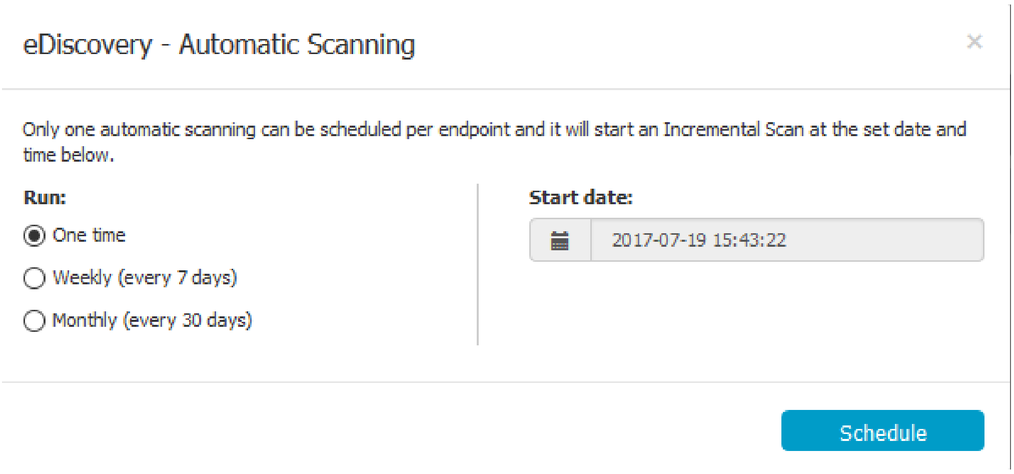
Note: Once the eDiscovery Policies are created, select the type of eDiscovery Scan.

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

- **Clean scan**: stars 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



eDiscovery - Automatic Scanning

Only one automatic scanning can be scheduled per endpoint and it will start an Incremental Scan at the set date and time below.

Run:

● One time

○ Weekly (every 7 days)

○ Monthly (every 30 days)

Start date: 2017-07-19 15:43:22

An eDiscovery Scan can be stopped at any time as results can also be automatically cleared.

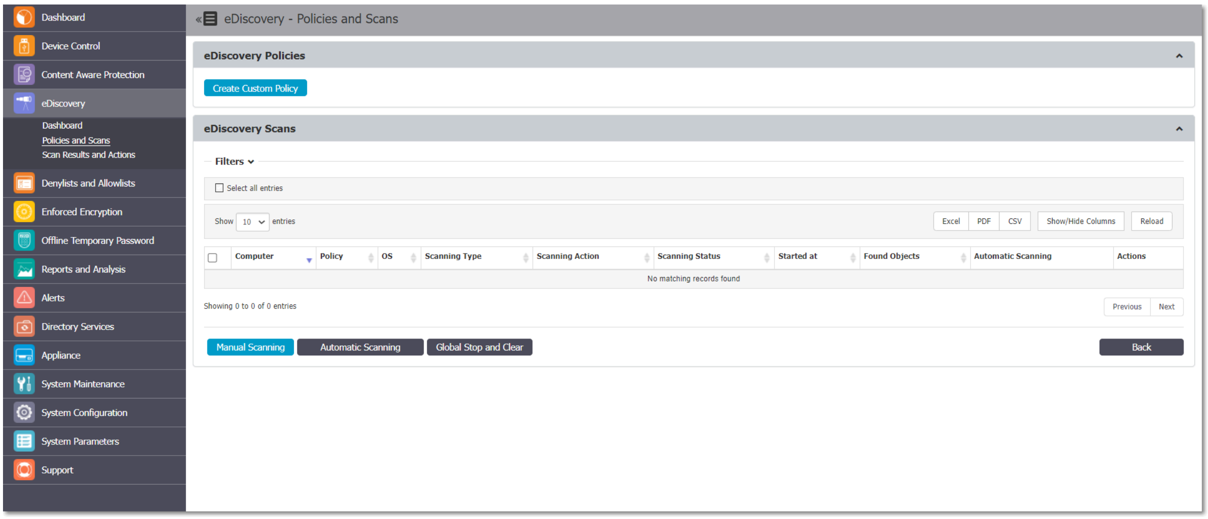
This can be done by using:

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

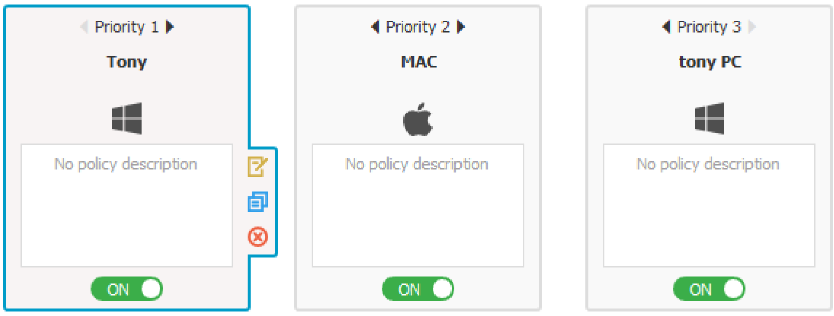
Note: Use Global Stop and Clear in situations where all the eDiscovery Scans need to be stopped and all the Logs cleared.

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.

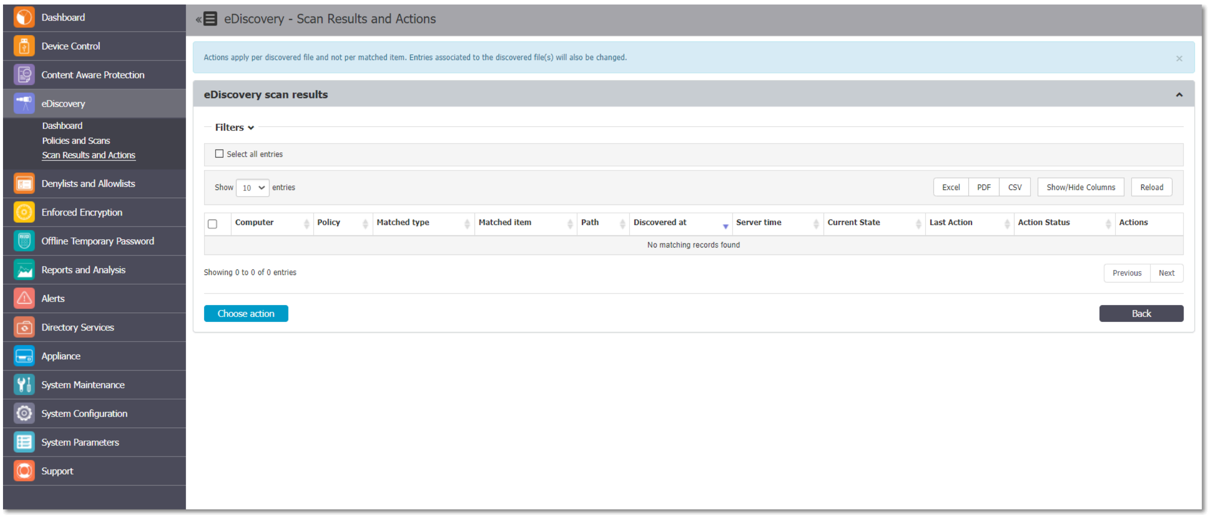
For detailed information on Denylists and Allowlist, refer to the Denylists and Allowlists chapter.

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.



eDiscovery - Scan Results and Actions

Actions apply per discovered file and not per matched item. Entries associated to the discovered file(s) will also be changed.

eDiscovery scan results

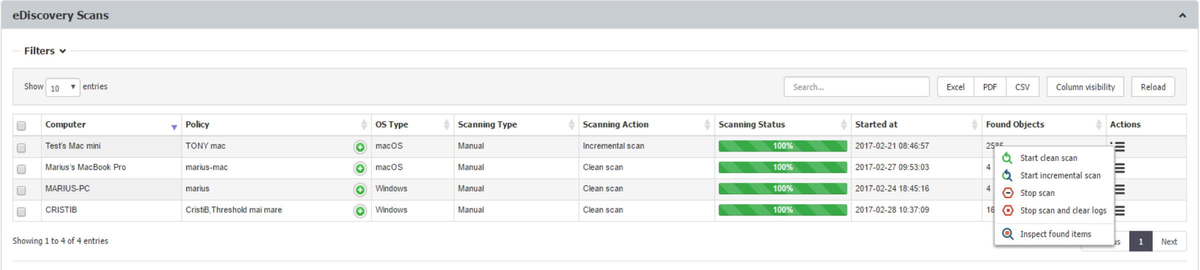
□ Select all entries

Show 10 entries

□	Computer	Policy	Matched type	Matched item	Path	Discovered at	Server time	Current State	Last Action	Action Status	Actions
No matching records found											

Showing 0 to 0 of 0 entries

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.



eDiscovery Scans

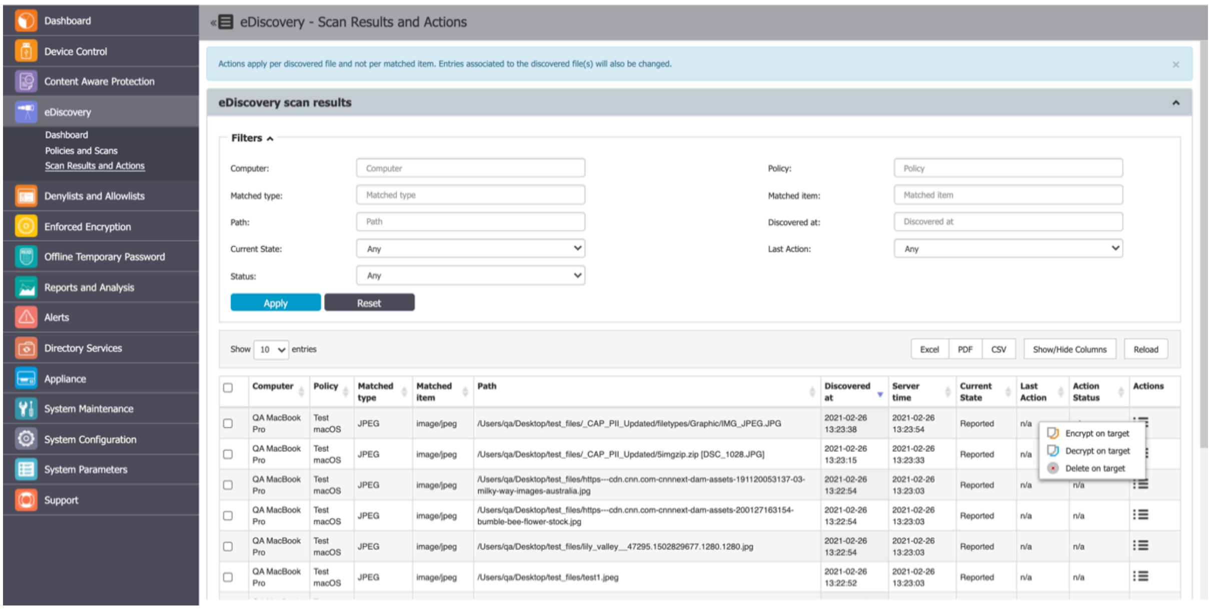
Show 10 entries

□	Computer	Policy	OS Type	Scanning Type	Scanning Action	Scanning Status	Started at	Found Objects	Actions
□	Test's Mac mini	TONY mac	macOS	Manual	Incremental scan	100%	2017-02-21 08:46:57	25	☰
□	Marius's MacBook Pro	marius-mac	macOS	Manual	Clean scan	100%	2017-02-27 09:53:03	4	☰
□	MARIUS-PC	marius	Windows	Manual	Clean scan	100%	2017-02-24 18:45:16	4	☰
□	CRISTIB	CristiB,Threshold mai mare	Windows	Manual	Clean scan	100%	2017-02-28 10:37:09	16	☰

Showing 1 to 4 of 4 entries

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.



eDiscovery - Scan Results and Actions

Actions apply per discovered file and not per matched item. Entries associated to the discovered file(s) will also be changed.

eDiscovery scan results

Filters

Computer: Computer

Matched type: Matched type

Path: Path

Current State: Any

Status: Any

Policy: Policy

Matched item: Matched item

Discovered at: Discovered at

Last Action: Any

□	Computer	Policy	Matched type	Matched item	Path	Discovered at	Server time	Current State	Last Action	Action Status	Actions
□	QA MacBook Pro	Test macOS	JPEG	image/jpeg	/Users/qa/Desktop/test_files/_CAP_PII_Updated/filetypes/Graphic/IMG_JPEG.JPG	2021-02-26 13:23:38	2021-02-26 13:23:54	Reported	n/a		☰
□	QA MacBook Pro	Test macOS	JPEG	image/jpeg	/Users/qa/Desktop/test_files/_CAP_PII_Updated/5imgzip.zip [DSC_1028.JPG]	2021-02-26 13:23:15	2021-02-26 13:23:33	Reported	n/a		☰
□	QA MacBook Pro	Test macOS	JPEG	image/jpeg	/Users/qa/Desktop/test_files/https---cdn.cnn.com-cnnnext-dam-assets-191120053137-03-milky-way-images-australia.jpg	2021-02-26 13:22:54	2021-02-26 13:23:03	Reported	n/a	n/a	☰
□	QA MacBook Pro	Test macOS	JPEG	image/jpeg	/Users/qa/Desktop/test_files/https---cdn.cnn.com-cnnnext-dam-assets-200127163154-bumble-bee-flower-stock.jpg	2021-02-26 13:22:54	2021-02-26 13:23:03	Reported	n/a	n/a	☰
□	QA MacBook Pro	Test macOS	JPEG	image/jpeg	/Users/qa/Desktop/test_files/lily_valley__47295.1502829677.1280.1280.jpg	2021-02-26 13:22:54	2021-02-26 13:23:03	Reported	n/a	n/a	☰
□	QA MacBook Pro	Test macOS	JPEG	image/jpeg	/Users/qa/Desktop/test_files/test1.jpeg	2021-02-26 13:22:52	2021-02-26 13:23:03	Reported	n/a	n/a	☰

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.

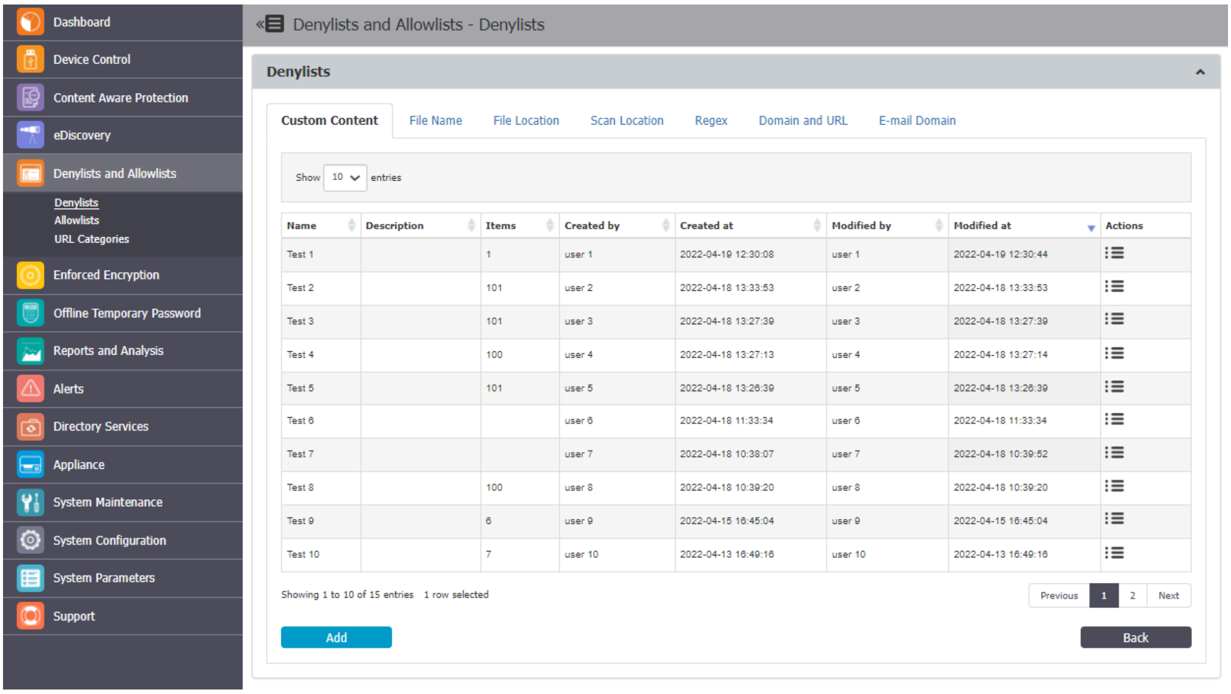
Denylists and Allowlists Availability

Type	Name	Platform			Modules	
		Windows	macOS	Linux	Content Aware Protection	eDiscovery
Denylists	Custom Content	✔	✔	✔	✔	✔
	File Name	✔	✔	✔	✔	✔
	File Location	✔	✔	✔	✔	✔
	Scan Location	✔	✔	✔	✘	✔
	Regex	✔	✔	✔	✔	✔
	Domain and URL	✔	✔	✔	✔	✘
	E-mail Domain	✔	✔	✔	✔	✘
Allowlists	MIME Type	✔	✔	✔	✔	✔
	Allowed Files	✔	✔	✔	✔	✔
	File Location	✔	✔	✔	✔	✔
	Network Share	✔	✔	✘	✔	✘
	E-mail Domain	✔	✔	✔	✔	✘
	URL Name	✔ only on Internet Explorer	✘	✘	✔	✘
	Deep Packet Inspection	✔	✔	✔	✔	✘
URL Categories		✔	✔	✔	✔	✘

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.



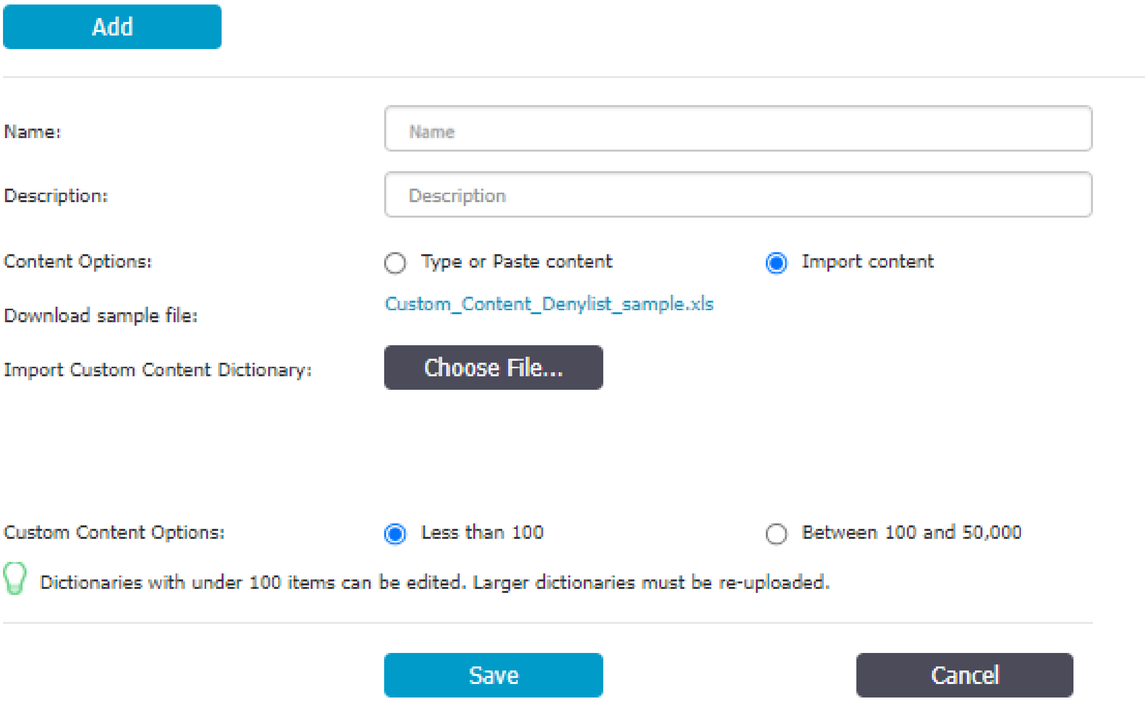
Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Test 1		1	user 1	2022-04-19 12:30:08	user 1	2022-04-19 12:30:44	☰
Test 2		101	user 2	2022-04-18 13:33:53	user 2	2022-04-18 13:33:53	☰
Test 3		101	user 3	2022-04-18 13:27:39	user 3	2022-04-18 13:27:39	☰
Test 4		100	user 4	2022-04-18 13:27:13	user 4	2022-04-18 13:27:14	☰
Test 5		101	user 5	2022-04-18 13:26:39	user 5	2022-04-18 13:26:39	☰
Test 6			user 6	2022-04-18 11:33:34	user 6	2022-04-18 11:33:34	☰
Test 7			user 7	2022-04-18 10:38:07	user 7	2022-04-18 10:39:52	☰
Test 8		100	user 8	2022-04-18 10:39:20	user 8	2022-04-18 10:39:20	☰
Test 9		6	user 9	2022-04-15 16:45:04	user 9	2022-04-15 16:45:04	☰
Test 10		7	user 10	2022-04-13 16:49:16	user 10	2022-04-13 16:49:16	☰

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.



Name: Name

Description: Description

Content Options: ○ Type or Paste content ● Import content

Download sample file: Custom_Content_Denylist_sample.xls

Import Custom Content Dictionary:

Custom Content Options: ● Less than 100 ○ Between 100 and 50,000

Dictionaries with under 100 items can be edited. Larger dictionaries must be re-uploaded.

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 filename and extension, or just the extension.

Examples: Matching and Non-Matching for File Names like "**example.pdf**":

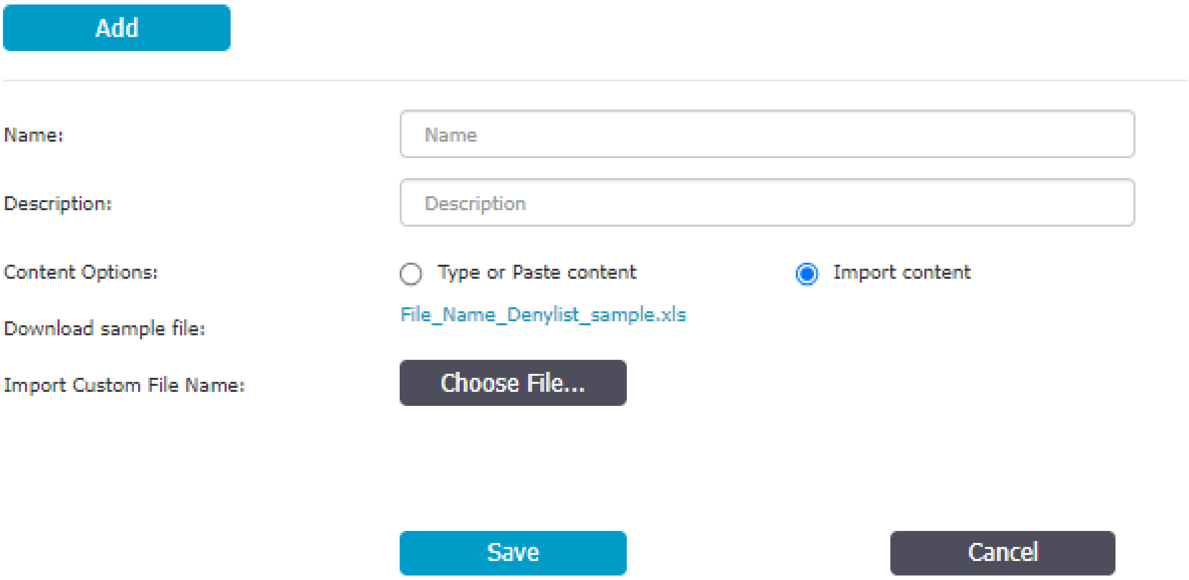
- **Matching**: example.pdf, my_example.pdf
- **Non-Matching**: example.txt, myexample.txt, test.pdf, example.pdf.txt, test_example.pdf_test.zip

Examples: Matching and Non-Matching for File Extensions like "**.epp**":

- **Matching**: test.epp, mail.epp, 123.epp
- **Non-Matching**: 123.epp.zip, mail.epp.txt

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.



Name: Name

Description: Description

Content Options: ○ Type or Paste content ● Import content

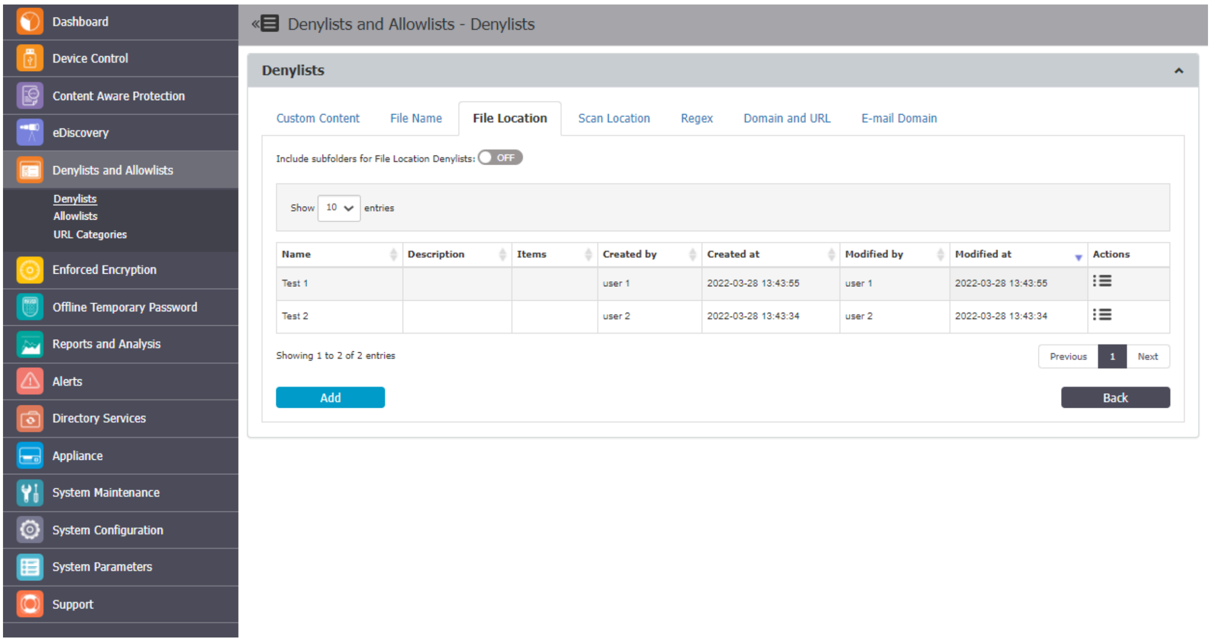
Download sample file: File_Name_Denylist_sample.xls

Import Custom File Name: Choose File...

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.



Include subfolders for File Location Denylists: OFF

Show 10 entries

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Test 1			user 1	2022-03-28 13:43:55	user 1	2022-03-28 13:43:55	☰
Test 2			user 2	2022-03-28 13:43:34	user 2	2022-03-28 13:43:34	☰

Showing 1 to 2 of 2 entries

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

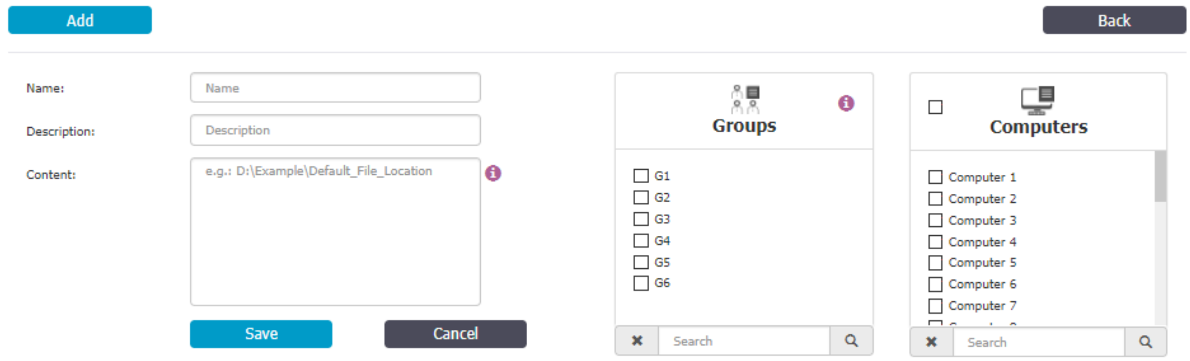
Denylists apply to all files located in the specific folder but also to any other files located in containing subfolders.

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\"**.

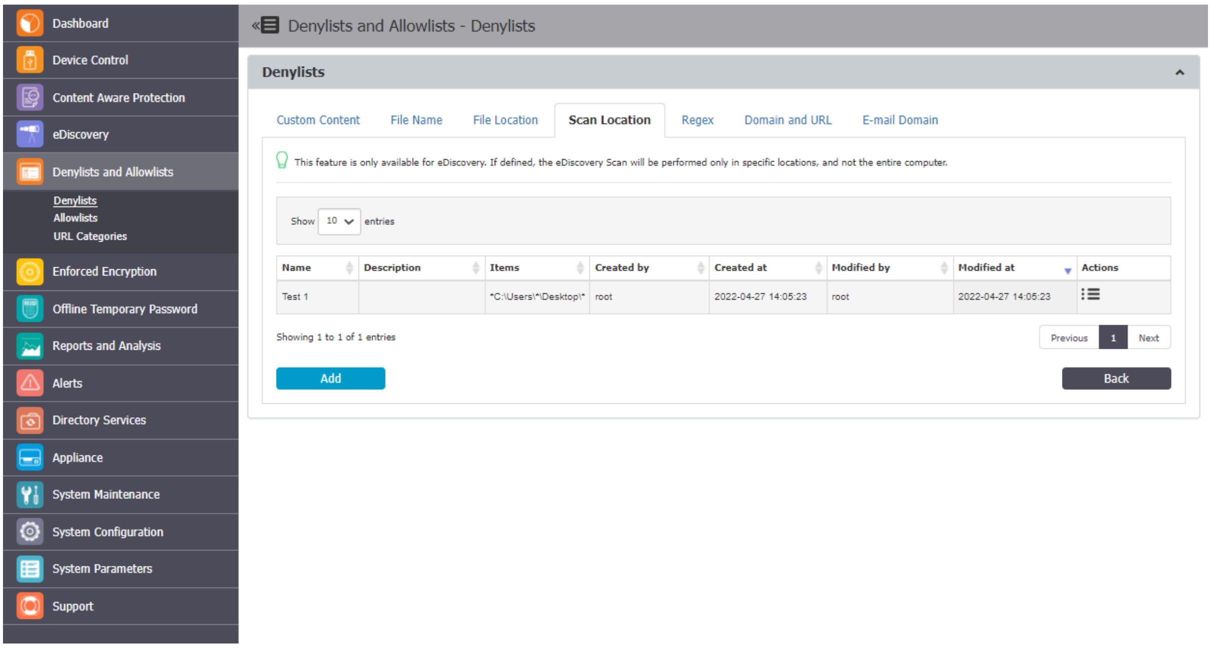
Wildcards usage examples for File Location

Wildcards Type	File Location	Results matched	Results not matched
Implicit	C:\temp	C:\temp\file.txt C:\temp\test\file2.txt C:\tempfile.txt	C:\temp1\file.txt C:\Windows\file.txt

Explicit	C:\Windows\*	C:\Windows\regedit.exe C:\Windows\system32\notepad.exe	C:\Windows.old\regedit.exe C:\Windows.old\system32\notepad.exe

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.



This feature is only available for eDiscovery. If defined, the eDiscovery Scan will be performed only in specific locations, and not the entire computer.

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Test 1		*C:\Users\*\Desktop\*	root	2022-04-27 14:05:23	root	2022-04-27 14:05:23	☰

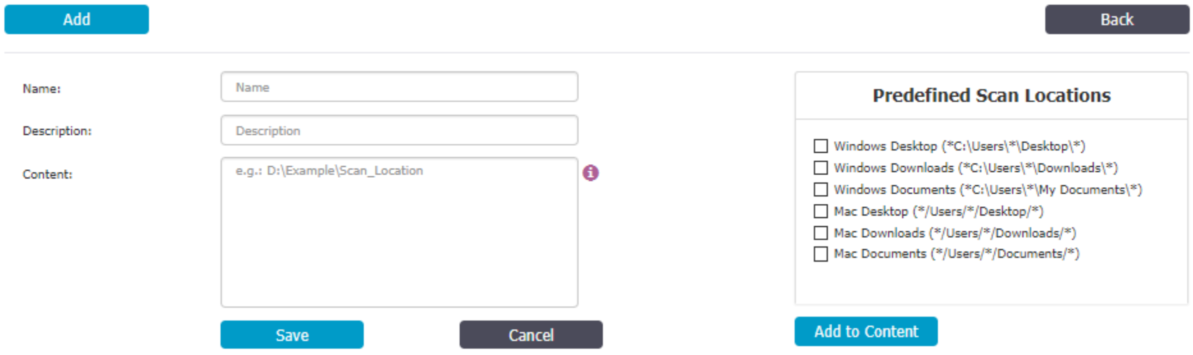
Showing 1 to 1 of 1 entries

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



Name: Name

Description: Description

Content: e.g.: D:\Example\Scan_Location

Predefined Scan Locations

- □ Windows Desktop (*C:\Users\*\Desktop*)
- □ Windows Downloads (*C:\Users\*\Downloads*)
- □ Windows Documents (*C:\Users\*\My Documents*)
- □ Mac Desktop (*/Users/*/Desktop/*)
- □ Mac Downloads (*/Users/*/Downloads/*)
- □ Mac Documents (*/Users/*/Documents/*)

8.1.5. Regex

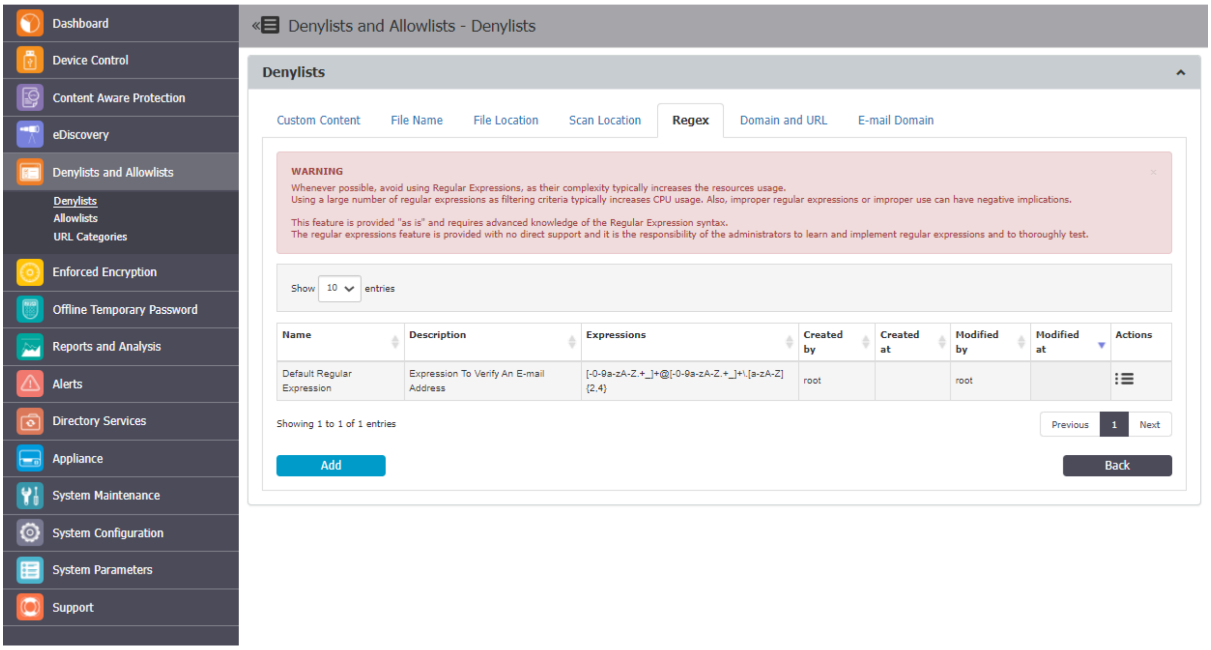
Regular Expressions are sequences of characters that form a search pattern, mainly for use in pattern matching with strings.

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.



WARNING
Whenever 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.

This feature is provided "as is" and requires advanced knowledge of the Regular Expression syntax.
The regular expressions feature is provided with no direct support and it is the responsibility of the administrators to learn and implement regular expressions and to thoroughly test.

Show 10 entries

Name	Description	Expressions	Created by	Created at	Modified by	Modified at	Actions
Default Regular Expression	Expression To Verify An E-mail Address	[-0-9a-zA-Z.+_]+@[-0-9a-zA-Z.+_]+\.[a-zA-Z]{2,4}	root		root		☰

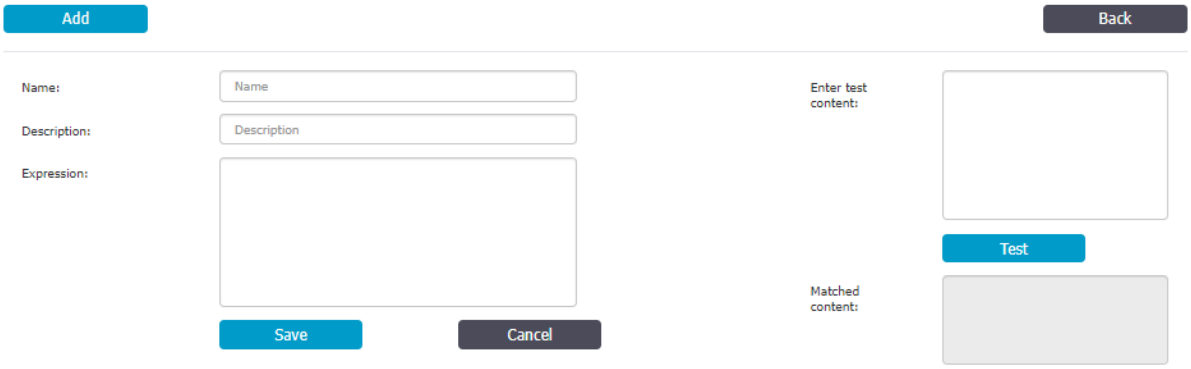
Showing 1 to 1 of 1 entries

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[0-4][0-9]|[01]?[0-9][0-9]?)(\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)){3}

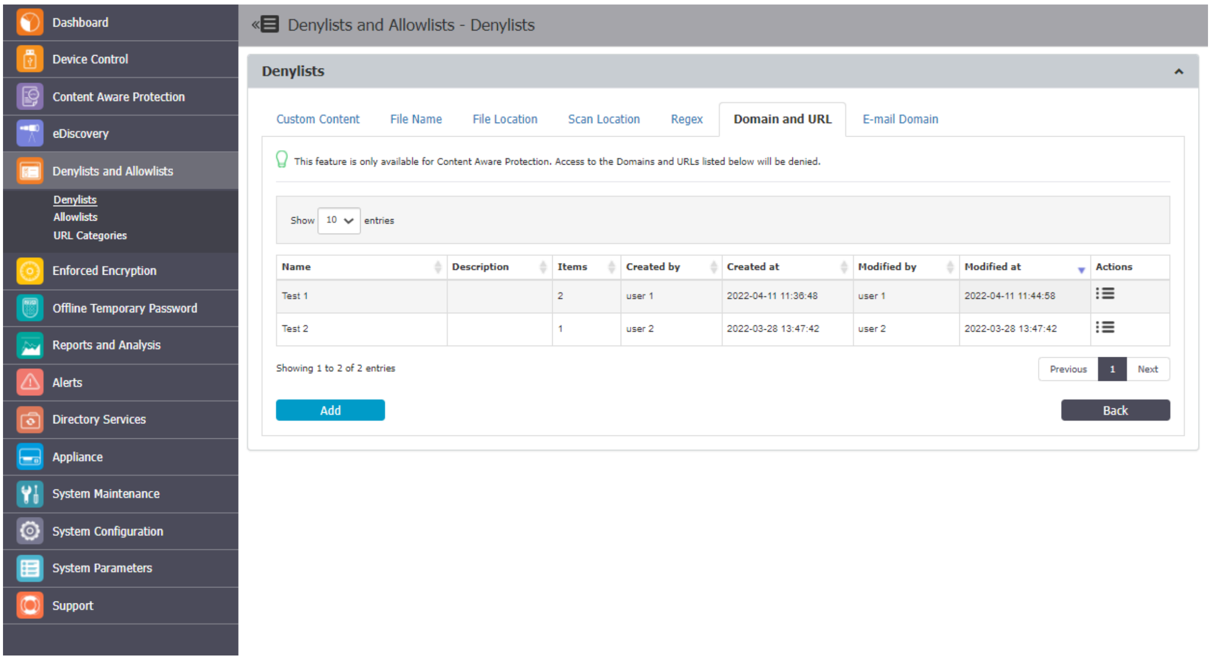
Note: This feature is provided “as is” and requires advanced knowledge of the Regular Expression syntax. No direct support is offered and it is the responsibility of the customers to learn and implement regular expressions and to thoroughly test.



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.



This feature is only available for Content Aware Protection. Access to the Domains and URLs listed below will be denied.

Show 10 entries

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Test 1		2	user 1	2022-04-11 11:36:48	user 1	2022-04-11 11:44:58	☰
Test 2		1	user 2	2022-03-28 13:47:42	user 2	2022-03-28 13:47:42	☰

Showing 1 to 2 of 2 entries

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.

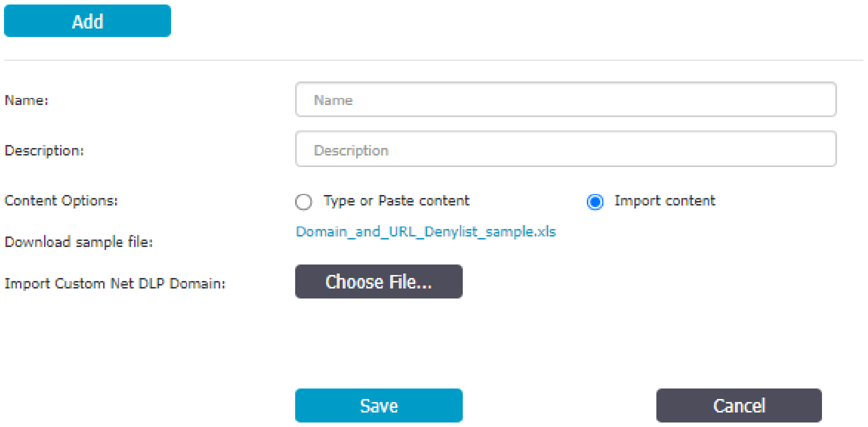
To create a new denylist, under the list of available denylists, click **Add**, provide a **name** and **description** and then **type or paste** items separated by a new line, comma, or semicolon. You can **import content** using the **sample file** provided on the form.

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.



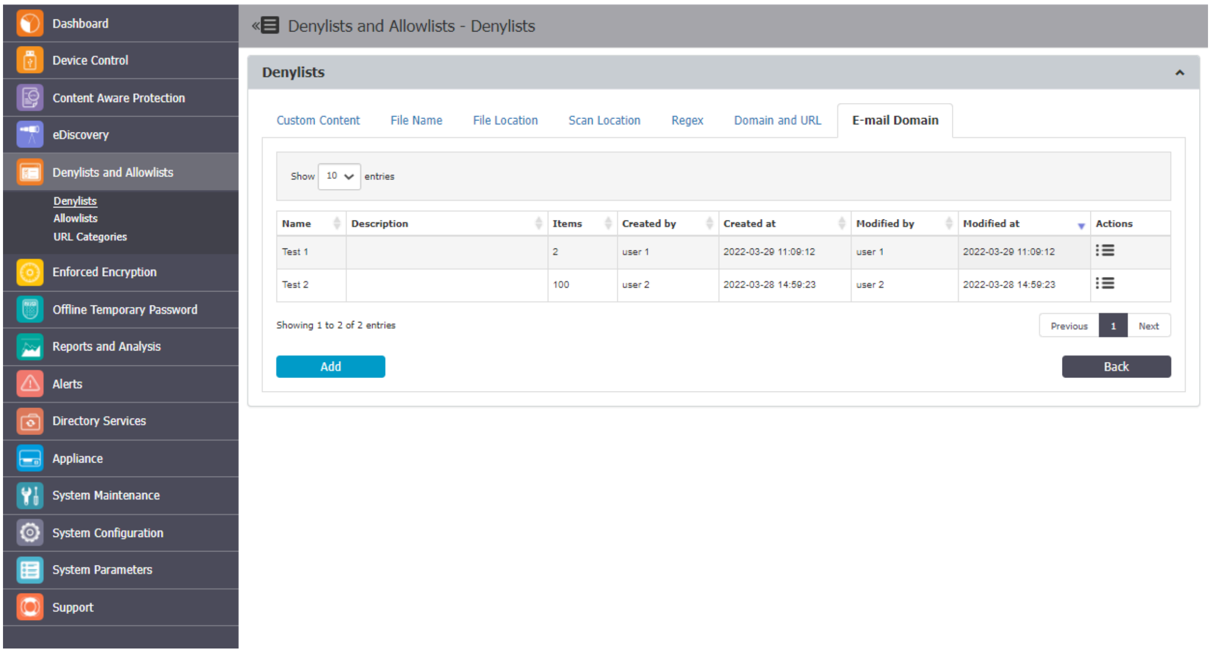
Name:	Name
Description:	Description
Content Options:	○ Type or Paste content ● Import content
Download sample file:	Domain_and_URL_Denylist_sample.xls
Import Custom Net DLP Domain:	Choose File...

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**.



Denylists and Allowlists - Denylists

Denylists

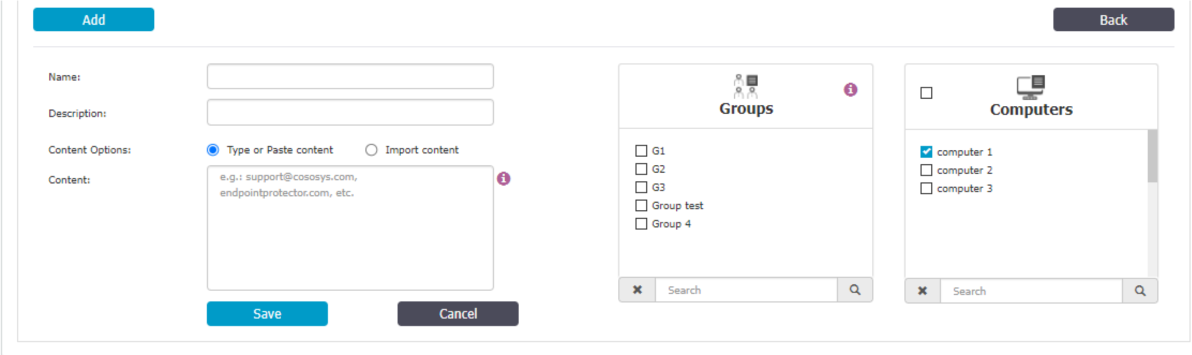
Show 10 entries

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Test 1		2	user 1	2022-03-29 11:09:12	user 1	2022-03-29 11:09:12	☰
Test 2		100	user 2	2022-03-28 14:59:23	user 2	2022-03-28 14:59:23	☰

Showing 1 to 2 of 2 entries

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.



Name:

Description:

Content Options: ● Type or Paste content ○ Import content

Content: e.g.: support@cososys.com, endpointprotector.com, etc.

Groups

□ G1
□ G2
□ G3
□ Group test
□ Group 4

□ Computers

☑ computer 1
□ computer 2
□ computer 3

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.

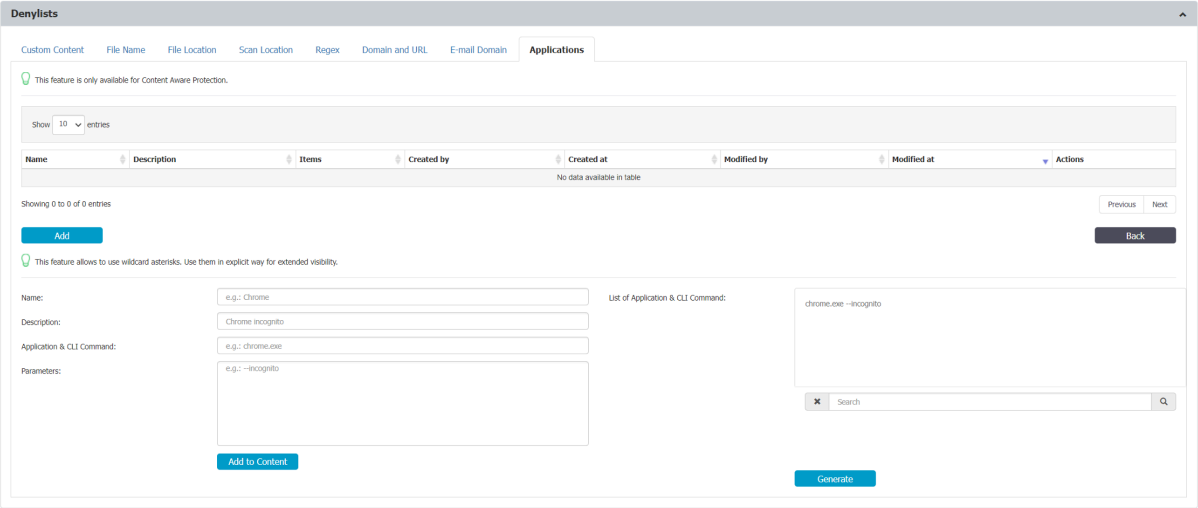
To define CLI command denylist policies, follow these steps:

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.



This feature is only available for Content Aware Protection.

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
No data available in table							

Showing 0 to 0 of 0 entries

This feature allows to use wildcard asterisks. Use them in explicit way for extended visibility.

Name: e.g.: Chrome

Description: Chrome incognito

Application & CLI Command: e.g.: chrome.exe

Parameters: e.g.: --incognito

List of Application & CLI Command: chrome.exe --incognito

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

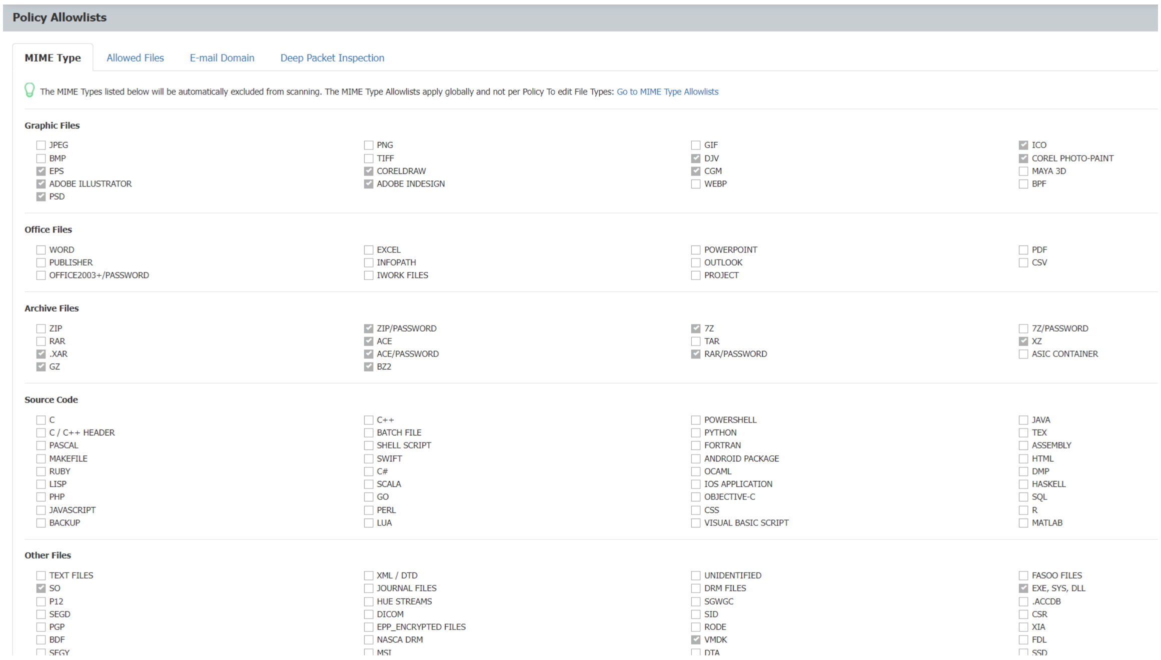
The content inspection functionally within Endpoint Protector identifies multiple file types. While some files (e.g. Word, Excel, PDFs, etc.) can contain confidential information (e.g. PIIs, SSNs, Credit Cards, etc.), other files are highly unlikely to contain such data (e.g. .dll, .exe, .mp3, .avi,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



Policy Allowlists

The MIME Types listed below will be automatically excluded from scanning. The MIME Type Allowlists apply globally and not per Policy To edit File Types: Go to MIME Type Allowlists

Graphic Files

☐ JPEG
☐ BMP
☑ EPS
☑ ADOBE ILLUSTRATOR
☑ PSD
☐ PNG
☐ TIFF
☑ CORELDRAW
☑ ADOBE INDESIGN
☐ GIF
☑ DJV
☑ CGM
☐ WEBP
☑ ICO
☑ COREL PHOTO-PAINT
☐ MAYA 3D
☐ BPF

Office Files

☐ WORD
☐ PUBLISHER
☐ OFFICE2003+/PASSWORD
☐ EXCEL
☐ INFOPATH
☐ IWORK FILES
☐ POWERPOINT
☐ OUTLOOK
☐ PROJECT
☐ PDF
☐ CSV

Archive Files

☐ ZIP
☐ RAR
☑ .XAR
☑ GZ
☑ ZIP/PASSWORD
☑ ACE
☑ ACE/PASSWORD
☑ BZ2
☑ 7Z
☐ TAR
☑ RAR/PASSWORD
☐ 7Z/PASSWORD
☑ XZ
☐ ASIC CONTAINER

Source Code

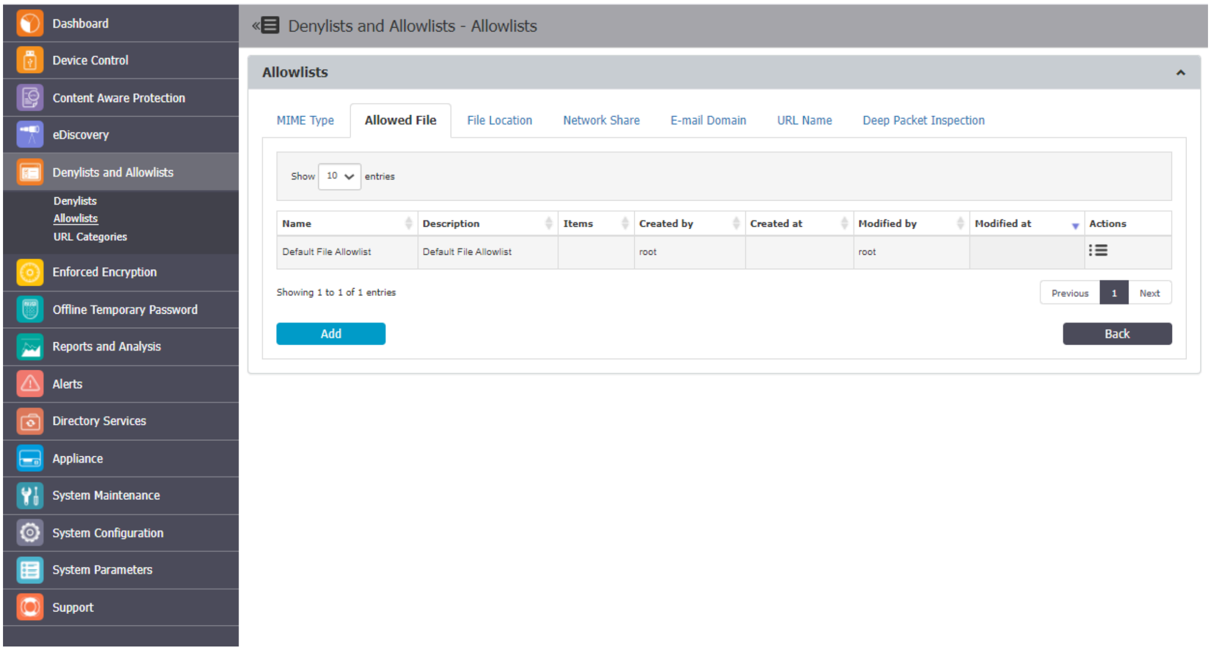
☐ C
☐ C / C++ HEADER
☐ PASCAL
☐ MAKEFILE
☐ RUBY
☐ LISP
☐ PHP
☐ JAVASCRIPT
☐ BACKUP
☐ C++
☐ BATCH FILE
☐ SHELL SCRIPT
☐ SWIFT
☐ C#
☐ SCALA
☐ GO
☐ PERL
☐ LUA
☐ POWERSHELL
☐ PYTHON
☐ FORTRAN
☐ ANDROID PACKAGE
☐ OCAML
☐ IOS APPLICATION
☐ OBJECTIVE-C
☐ CSS
☐ VISUAL BASIC SCRIPT
☐ JAVA
☐ TEX
☐ ASSEMBLY
☐ HTML
☐ DMP
☐ HASKELL
☐ SQL
☐ R
☐ MATLAB

Other Files

☐ TEXT FILES
☑ SO
☐ P12
☐ SEGD
☐ PGP
☐ BDF
☐ SEGY
☐ XML / DTD
☐ JOURNAL FILES
☐ HUE STREAMS
☐ DICOM
☐ EPP_ENCRYPTED FILES
☐ NASCA DRM
☐ MSI
☐ UNIDENTIFIED
☐ DRM FILES
☐ SGWGC
☐ SID
☐ RODE
☑ VMDK
☐ DTA
☐ FASOO FILES
☑ EXE, SYS, DLL
☐ .ACCDB
☐ CSR
☐ XIA
☐ FDL
☐ SSD

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.



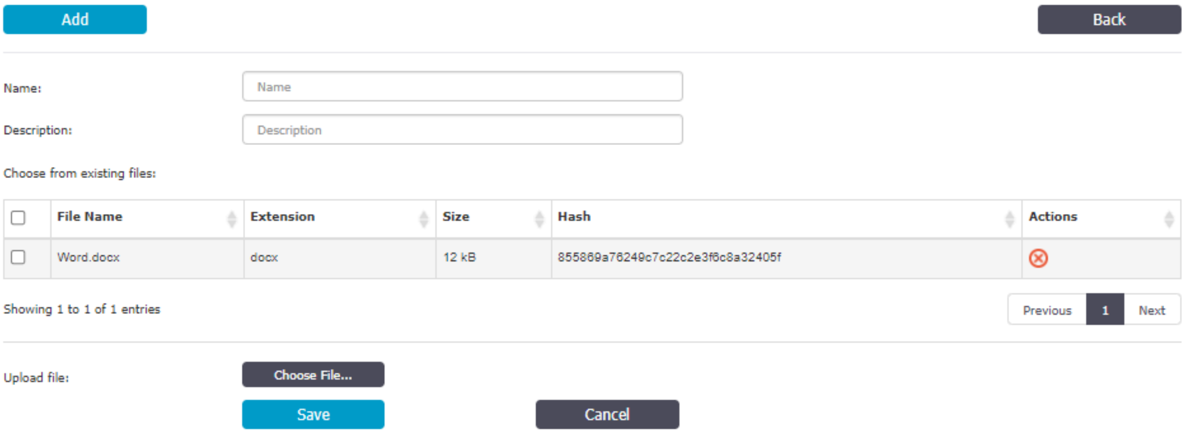
Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Default File Allowlist	Default File Allowlist		root		root		☰

Showing 1 to 1 of 1 entries

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.



Add

Back

Name: Name

Description: Description

Choose from existing files:

□	File Name	Extension	Size	Hash	Actions
□	Word.docx	docx	12 kB	855869a76249c7c22c2e3f6c8a32405f	⊗

Showing 1 to 1 of 1 entries

Previous 1 Next

Upload file: Choose File...

Save

Cancel

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.

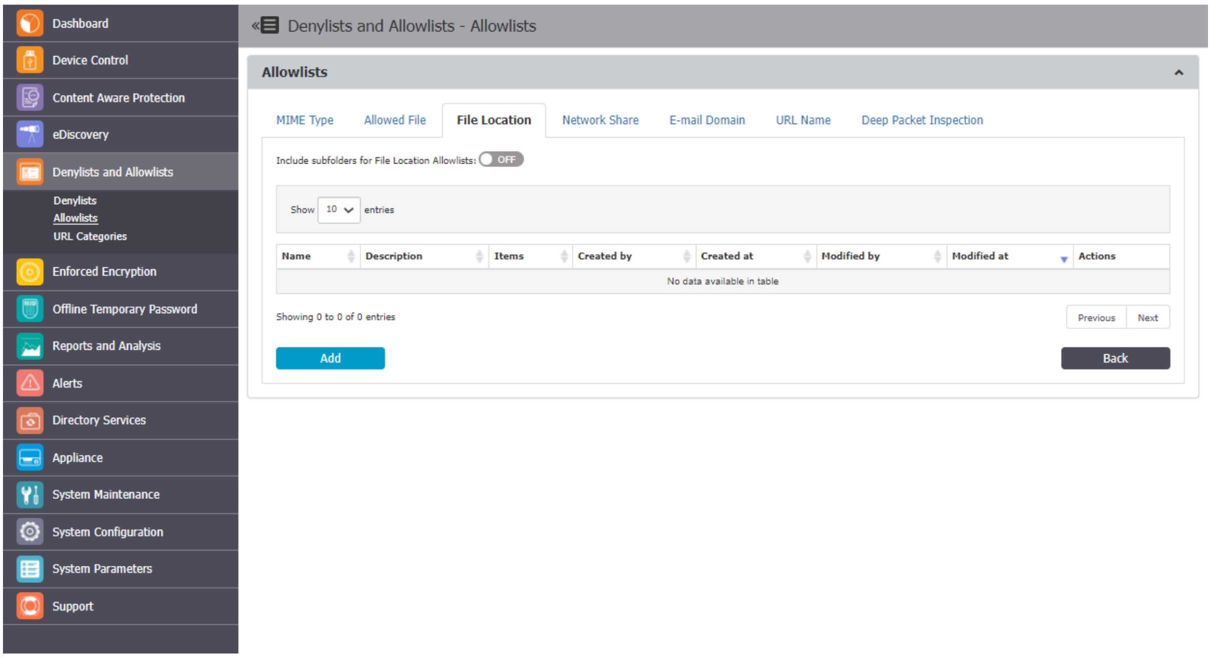
Important: In addition to defining the File Location Allowlist, the browser or application used to transfer files also needs to be selected from within the Content Aware Protection Policy.

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\".**

Wildcards usage examples for File Location			
Wildcards Type	**File Location**	**Results matched**	**Results not matched**

Implicit	\\file-share\public	\\file-share\public\jdoe\file.txt \\file-share\public\user512\file2.txt	\\file-share\c$\file.txt \\file-server\public\jdoe\file.txt
Explicit	*\public*	\\localhost\public\payslip.xlsx \\192.168.20.2\public\Windows\system32\notepad.exe	\\localhost\c$\system32\notepad.exe C:\Windows.old\system32\notepad.exe



Include subfolders for File Location Allowlists: OFF

Show 10 entries

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
No data available in table							

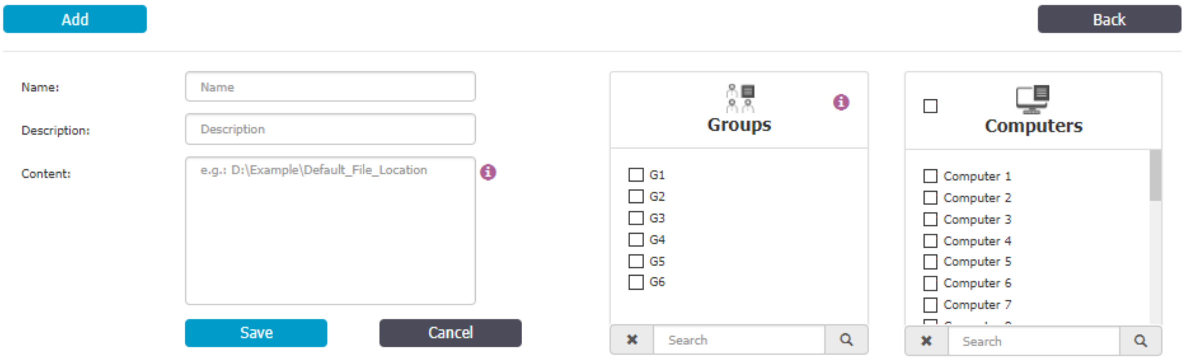
Showing 0 to 0 of 0 entries

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.



Name: Name

Description: Description

Content: e.g.: D:\Example\Default_File_Location

□ G1
□ G2
□ G3
□ G4
□ G5
□ G6

□ Computer 1
□ Computer 2
□ Computer 3
□ Computer 4
□ Computer 5
□ Computer 6
□ Computer 7

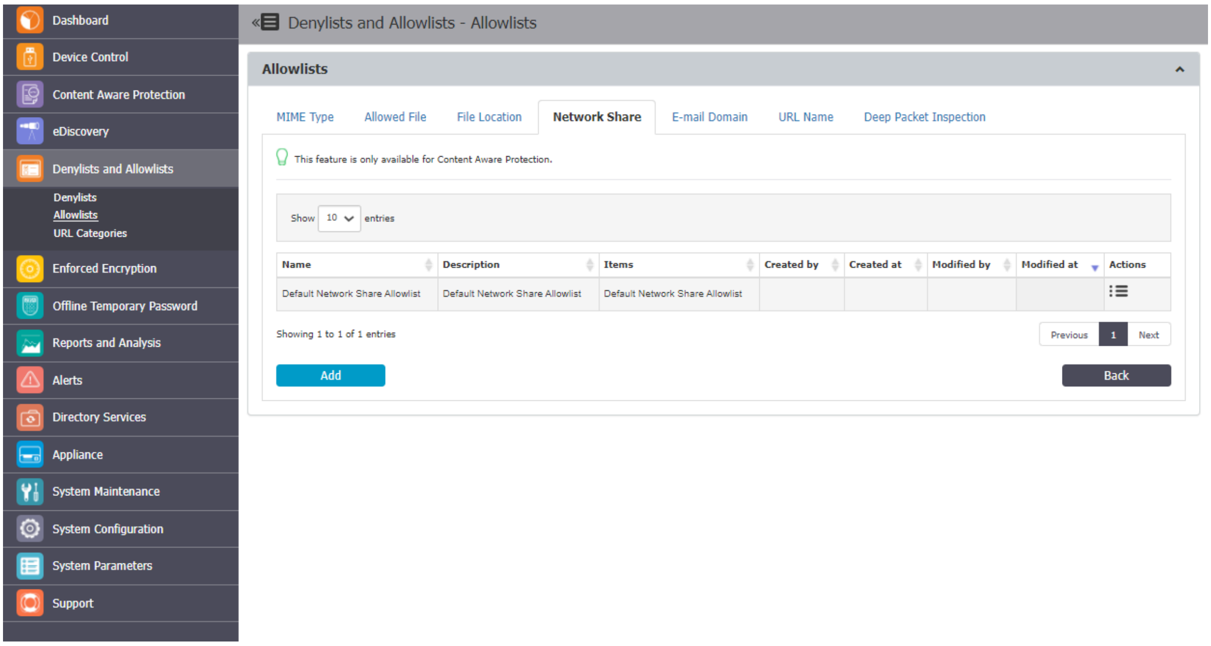
8.2.4. Network Share

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.



This feature is only available for Content Aware Protection.

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Default Network Share Allowlist	Default Network Share Allowlist	Default Network Share Allowlist					☰

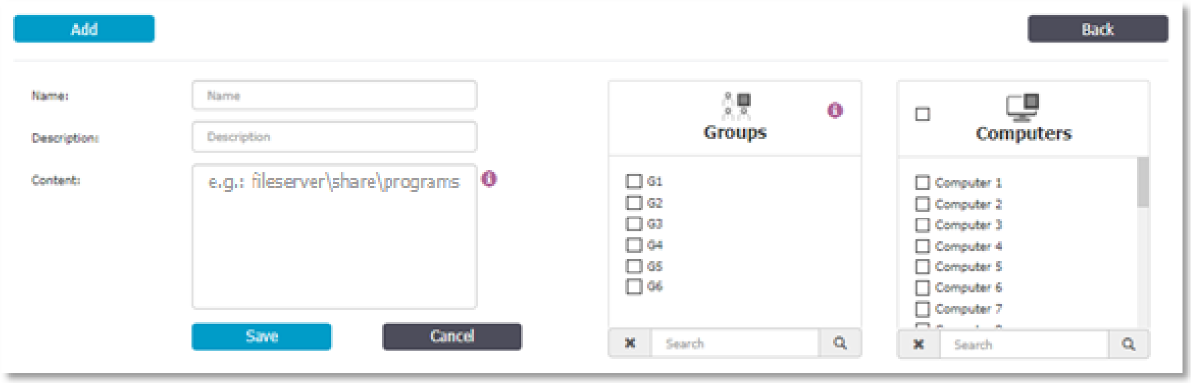
Showing 1 to 1 of 1 entries

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.

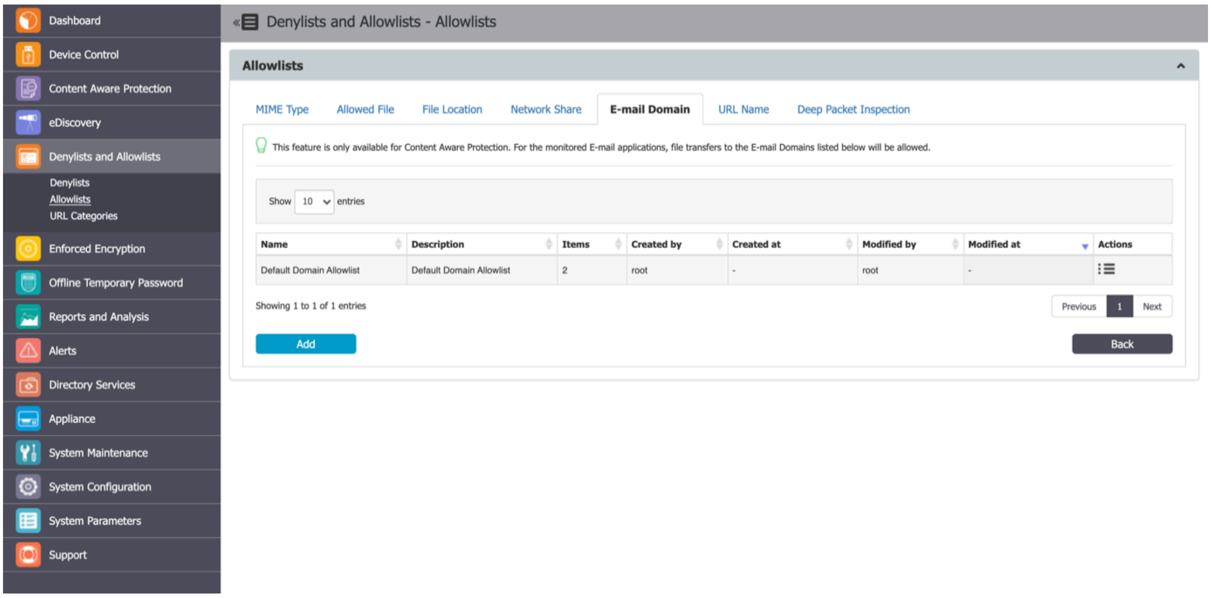
Important: Do not type the network share path with backslashes (\\) 192.168.0.1\public\users\test; fileserver\documents\example



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.



This feature is only available for Content Aware Protection. For the monitored E-mail applications, file transfers to the E-mail Domains listed below will be allowed.

Show 10 entries

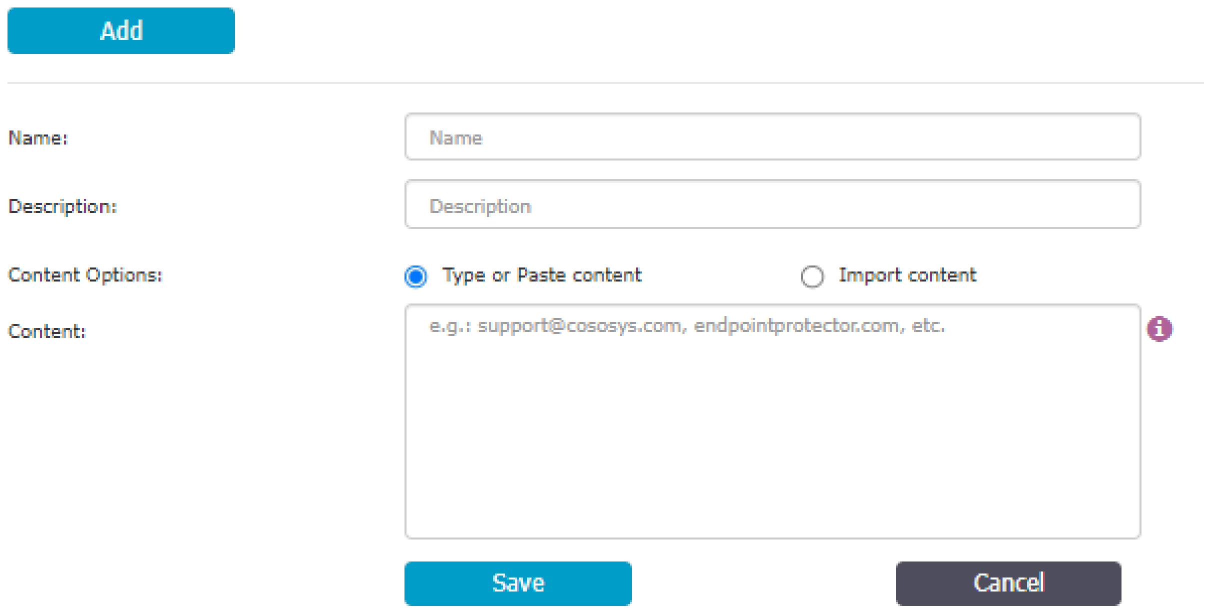
Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Default Domain Allowlist	Default Domain Allowlist	2	root	-	root	-	☰

Showing 1 to 1 of 1 entries

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.



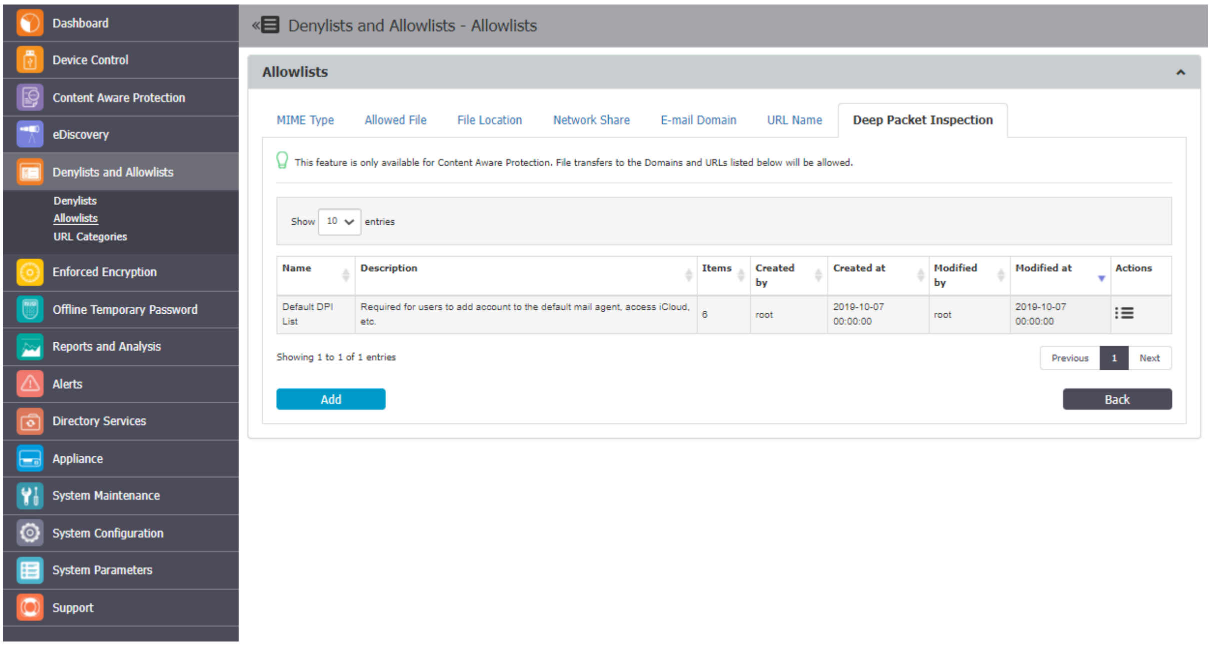
Name:	Name
Description:	Description
Content Options:	● Type or Paste content ○ Import content
Content:	e.g.: support@cososys.com, endpointprotector.com, etc.

You can use wildcard patterns in the e-mail domain to specify wildcard matching as displayed in the following example.

Wildcards usage examples for E-mail Domain		
E-mail Domain name	Results matched	Results not matched
@epp.com	robert@epp.com jdoe@epp.com james@epp.com.ca	sara@epp.com jeff@ccs.com

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.



This feature is only available for Content Aware Protection. File transfers to the Domains and URLs listed below will be allowed.

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Default DPI List	Required for users to add account to the default mail agent, access iCloud, etc.	6	root	2019-10-07 00:00:00	root	2019-10-07 00:00:00	☰

Showing 1 to 1 of 1 entries

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.

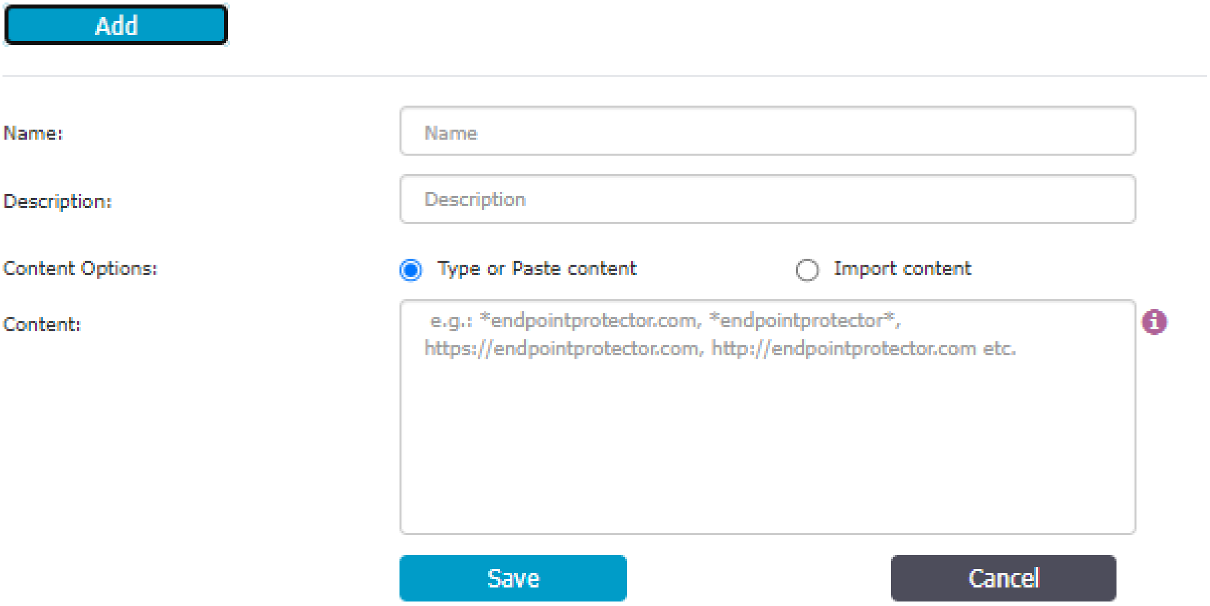
Example: example.endpointprotector, *example.com, *example*, https://website.com, etc.

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.



Add

Name:	Name	
Description:	Description	
Content Options:	● Type or Paste content	○ Import content
Content:	e.g.: *endpointprotector.com, *endpointprotector*, https://endpointprotector.com, http://endpointprotector.com etc.	

Wildcards usage examples for Deep Packet Inspection

Domain name	Results matched	Results not matched
box.com	box.com	Sub.box.com box1.com
*.box.com	Sub.box.com bad.box.com	Fakebox.com mybox.com
box.*.com	Box.co.com box.bad.com	Sub.box.co.com Box1.co.com box.co.uk
box.com.*	Box.com.co box.com.us	Sub.box.com.us box1.com.us
https://cisco.com	https://cisco.com/drives/downloads/ http://cisco.com/drives/downloads/ ftp://cisco.com/drives/downloads/	https://sub.cisco.com/drives/downloads/ https://cisco.com.ca/downloads/
https://cisco.com*	https://cisco.com.ca/downloads/ http://cisco.com.ca/downloads/	https://sub.cisco.com.ca/downloads/ https://bad.cisco.com/downloads/

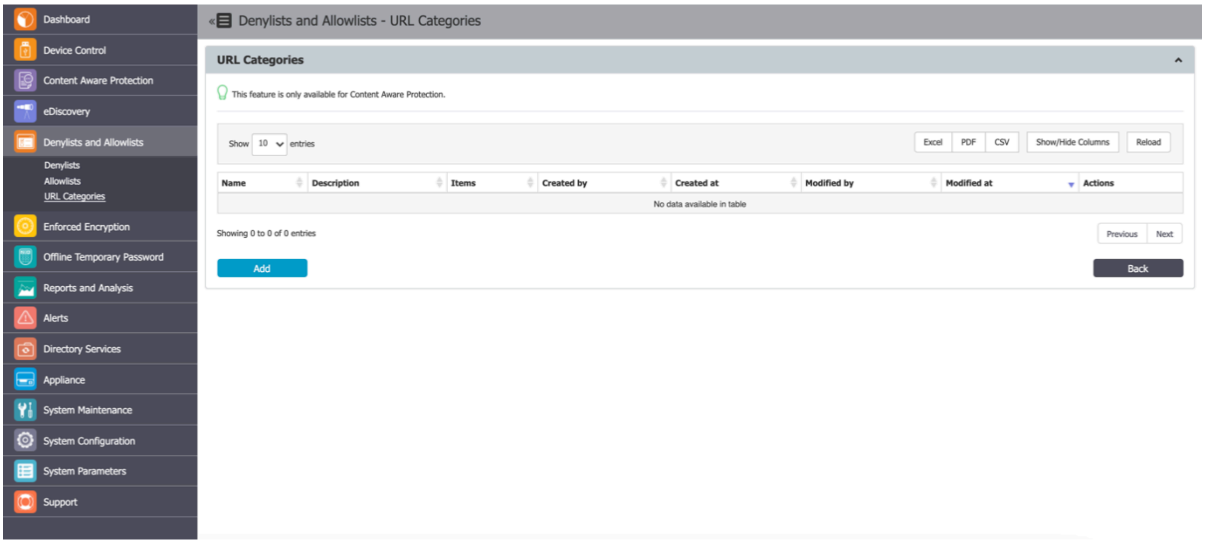
Note: Using wildcards will search for domain names, not URLs.

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.



Denylists and Allowlists - URL Categories

URL Categories

This feature is only available for Content Aware Protection.

Show 10 entries

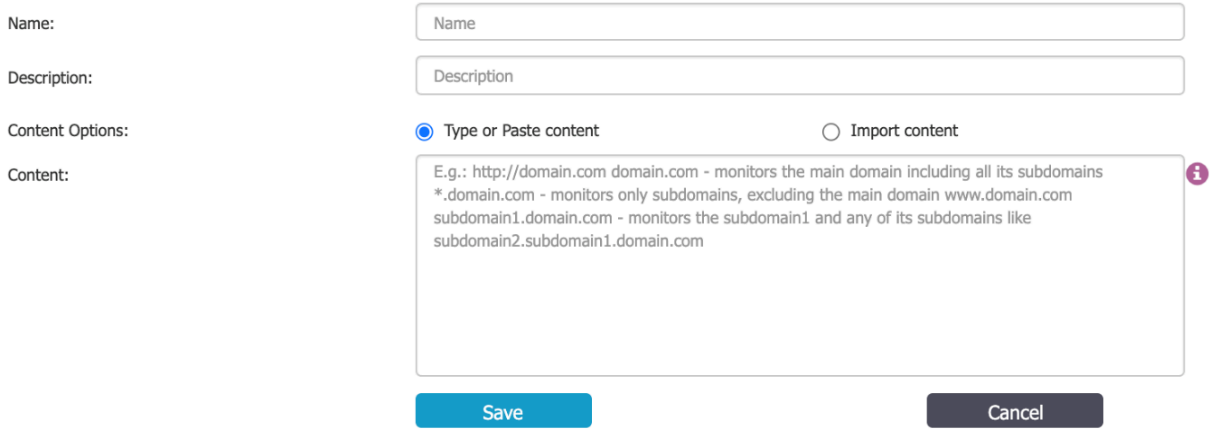
Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
No data available in table							

Showing 0 to 0 of 0 entries

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.



Name: Name

Description: Description

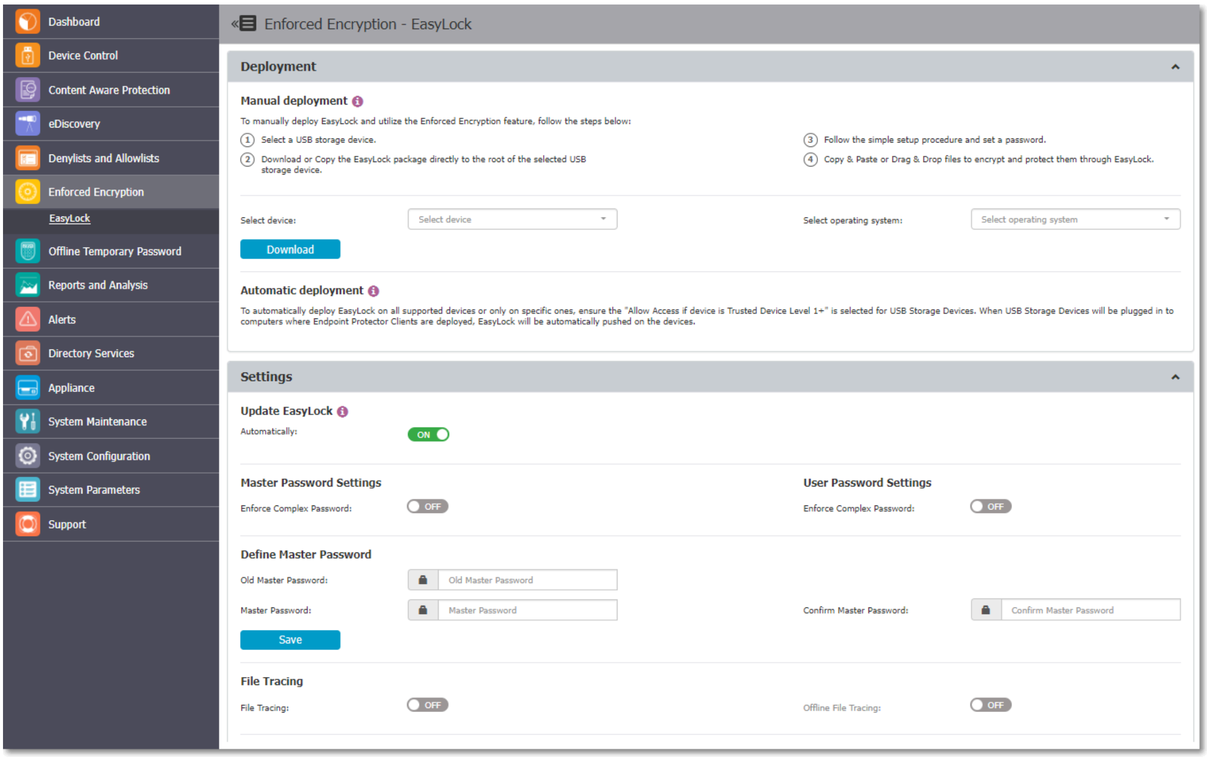
Content Options: ● Type or Paste content ○ Import content

Content: E.g.: http://domain.com domain.com - monitors the main domain including all its subdomains *.domain.com - monitors only subdomains, excluding the main domain www.domain.com subdomain1.domain.com - monitors the subdomain1 and any of its subdomains like subdomain2.subdomain1.domain.com

9. Enforced Encryption

9.1. Enforced Encryption[1]

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 - EasyLock

Deployment

Manual deployment

To manually deploy EasyLock and utilize the Enforced Encryption feature, follow the steps below:

1. Select a USB storage device.
2. Download or Copy the EasyLock package directly to the root of the selected USB storage device.
3. Follow the simple setup procedure and set a password.
4. Copy & Paste or Drag & Drop files to encrypt and protect them through EasyLock.

Select device: Select device

Select operating system: Select operating system

Automatic deployment

To automatically deploy EasyLock on all supported devices or only on specific ones, ensure the "Allow Access if device is Trusted Device Level 1+" is selected for USB Storage Devices. When USB Storage Devices will be plugged in to computers where Endpoint Protector Clients are deployed, EasyLock will be automatically pushed on the devices.

Settings

Update EasyLock

Automatically: ON

Master Password Settings

Enforce Complex Password: OFF

User Password Settings

Enforce Complex Password: OFF

Define Master Password

Old Master Password: Old Master Password

Master Password: Master Password

Confirm Master Password: Confirm Master Password

File Tracing

File Tracing: OFF

Offline File Tracing: OFF

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.

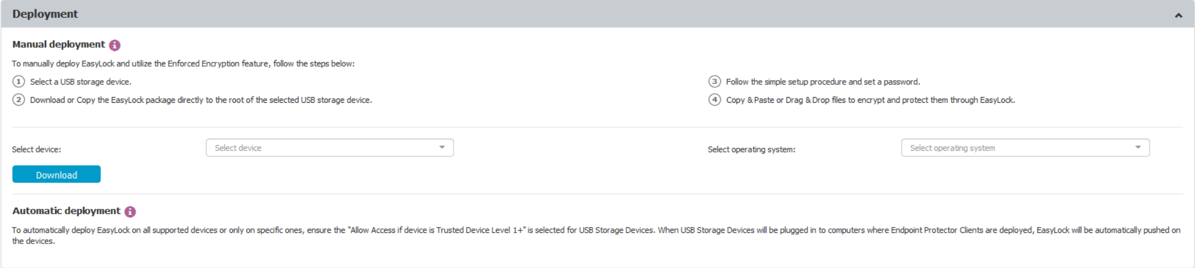
Important: Enforced Encryption is not compatible with devices that have a write-protection mechanism in place, preventing the modification or deletion of data. The write-protection mechanism can be enforced using a hardware component (for example a switch on the USB device) or a software component.

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

Manual deployment

To manually deploy EasyLock and utilize the Enforced Encryption feature, follow the steps below:

1. Select a USB storage device.
2. Download or Copy the EasyLock package directly to the root of the selected USB storage device.
3. Follow the simple setup procedure and set a password.
4. Copy & Paste or Drag & Drop files to encrypt and protect them through EasyLock.

Select device: Select device

Select operating system: Select operating system

Automatic deployment

To automatically deploy EasyLock on all supported devices or only on specific ones, ensure the "Allow Access if device is Trusted Device Level 1+" is selected for USB Storage Devices. When USB Storage Devices will be plugged in to computers where Endpoint Protector Clients are deployed, EasyLock will be automatically pushed on the devices.

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.

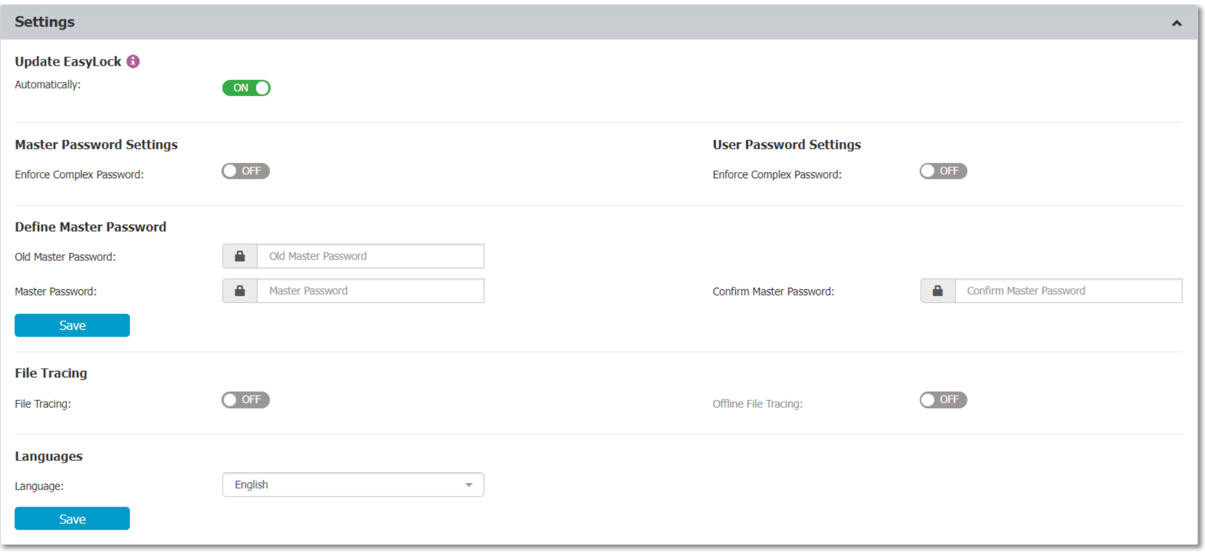
Note: Starting with Endpoint Protector 5.2.0.0, manual deployment can also be made by the user if the device is set on Allow Access, by pressing the small USB icon- Encrypt Device with Enforced Encryption.

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.



Settings

Update EasyLock

Automatically: ON

Master Password Settings

Enforce Complex Password: OFF

User Password Settings

Enforce Complex Password: OFF

Define Master Password

Old Master Password: Old Master Password

Master Password: Master Password

Confirm Master Password: Confirm Master Password

Save

File Tracing

File Tracing: OFF

Offline File Tracing: OFF

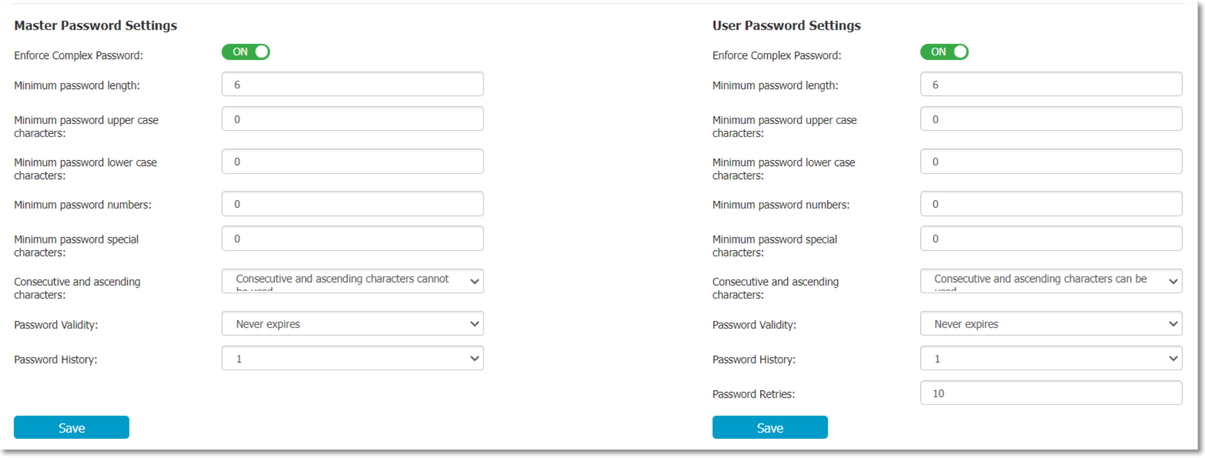
Languages

Language: English

Save

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.



Master Password Settings

Enforce Complex Password: ON

Minimum password length: 6

Minimum password upper case characters: 0

Minimum password lower case characters: 0

Minimum password numbers: 0

Minimum password special characters: 0

Consecutive and ascending characters: Consecutive and ascending characters cannot be used

Password Validity: Never expires

Password History: 1

Save

User Password Settings

Enforce Complex Password: ON

Minimum password length: 6

Minimum password upper case characters: 0

Minimum password lower case characters: 0

Minimum password numbers: 0

Minimum password special characters: 0

Consecutive and ascending characters: Consecutive and ascending characters can be used

Password Validity: Never expires

Password History: 1

Password Retries: 10

Save

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.

File Tracing

File Tracing: OFF

Offline File Tracing: OFF

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.

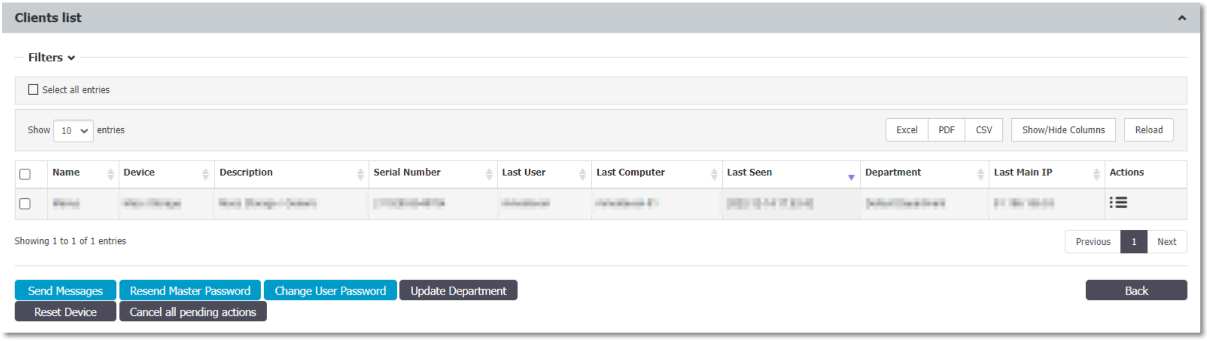
The additional Offline File Tracing option is an extension to the first option, offering the possibility to store information directly on the device, before being sent to the Endpoint Protector Server. The list of copied files is sent only the next time the device is plugged in and only if the Endpoint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



Clients list

Filters

□ Select all entries

Show 10 entries

□	Name	Device	Description	Serial Number	Last User	Last Computer	Last Seen	Department	Last Main IP	Actions
□	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	☰

Showing 1 to 1 of 1 entries

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
  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™:

Device Names	Trusted Device™ Level
Enforced Encryption Encrypted devices	1
AT1177	2

UT169	2
UT176	2
Trek ThumbDrive	2
BitLocker Encrypted devices	3
FileVault Encrypted devices	3
Buffalo Secure Lock	3
CTWO SafeXs	3
Integral Crypto	3
Integral Crypto Dual	3
Integral Courier Dual	3
IronKey Secure Drive	3
iStorage datAshur	3
Kanguru Bio Drive	3
Kanguru Defender	3
Kanguru Elite (30, 200 & 300)	3
Kanguru Defender Elite	3
Kingston DataTraveler Locker+	3
Lexar 1 (Locked I Device)	3
Lexar Gemalto	3
SaferZone Token	3
ScanDisk Enterprise	3
Verbatim Professional	3
Verbatim Secure Data	3
Verbatim V-Secure	3
iStorage datAshur Pro	4
Kanguru Defender (2000 & 3000)	4

SafeStick BE	4
Stealth MXP Bio	4

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.

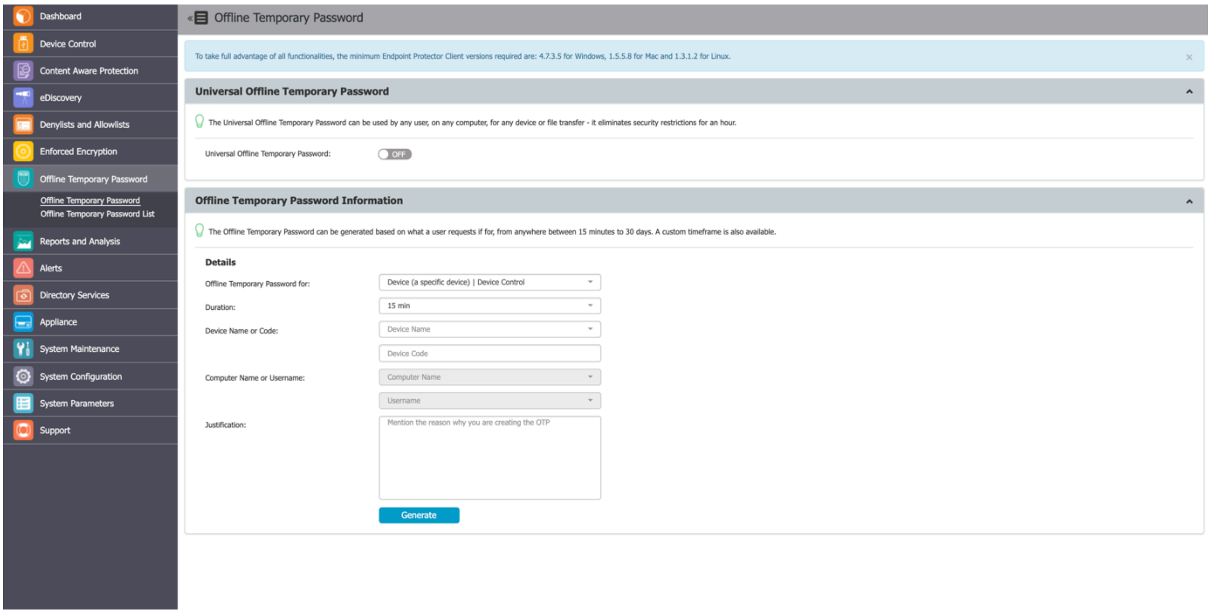
You have the option to add a justification, mentioning the reason why the password was created. This can later be used for a better overview or various audit purposes.

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.



To take full advantage of all functionalities, the minimum Endpoint Protector Client versions required are: 4.7.3.5 for Windows, 1.5.5.8 for Mac and 1.3.1.2 for Linux.

Universal Offline Temporary Password

The Universal Offline Temporary Password can be used by any user, on any computer, for any device or file transfer - it eliminates security restrictions for an hour.

Universal Offline Temporary Password: OFF

Offline Temporary Password Information

The Offline Temporary Password can be generated based on what a user requests if for, from anywhere between 15 minutes to 30 days. A custom timeframe is also available.

Details

Offline Temporary Password for: Device (a specific device) | Device Control

Duration: 15 min

Device Name or Code: Device Name

Device Code

Computer Name or Username: Computer Name

Username

Justification: Mention the reason why you are creating the OTP

Generate

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

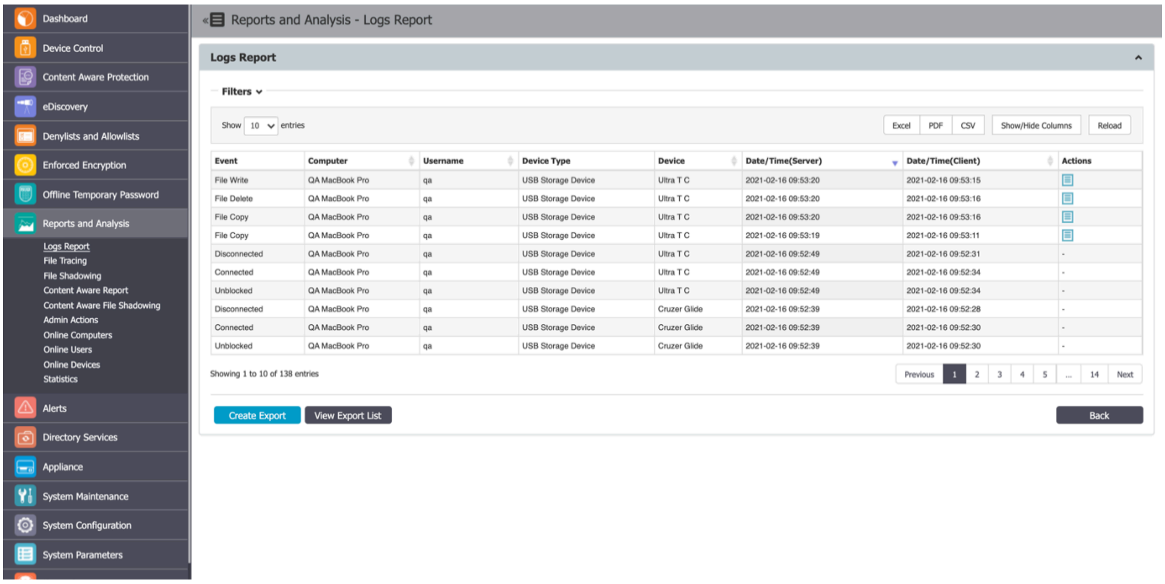
This section offers an overview of the System Logs, Device Control Logs and Shadows, Content Aware Logs and Shadows, Admin Actions, Statistics, and other helpful information.

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.



Event	Computer	Username	Device Type	Device	Date/Time(Server)	Date/Time(Client)	Actions
File Write	QA MacBook Pro	qa	USB Storage Device	Ultra T C	2021-02-16 09:53:20	2021-02-16 09:53:15	▤
File Delete	QA MacBook Pro	qa	USB Storage Device	Ultra T C	2021-02-16 09:53:20	2021-02-16 09:53:16	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Ultra T C	2021-02-16 09:53:20	2021-02-16 09:53:16	▤
File Copy	QA MacBook Pro	qa	USB Storage Device	Ultra T C	2021-02-16 09:53:19	2021-02-16 09:53:11	▤
Disconnected	QA MacBook Pro	qa	USB Storage Device	Ultra T C	2021-02-16 09:52:49	2021-02-16 09:52:31	-
Connected	QA MacBook Pro	qa	USB Storage Device	Ultra T C	2021-02-16 09:52:49	2021-02-16 09:52:34	-
Unblocked	QA MacBook Pro	qa	USB Storage Device	Ultra T C	2021-02-16 09:52:49	2021-02-16 09:52:34	-
Disconnected	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:52:39	2021-02-16 09:52:28	-
Connected	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:52:39	2021-02-16 09:52:30	-
Unblocked	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	2021-02-16 09:52:39	2021-02-16 09:52:30	-

Showing 1 to 10 of 138 entries

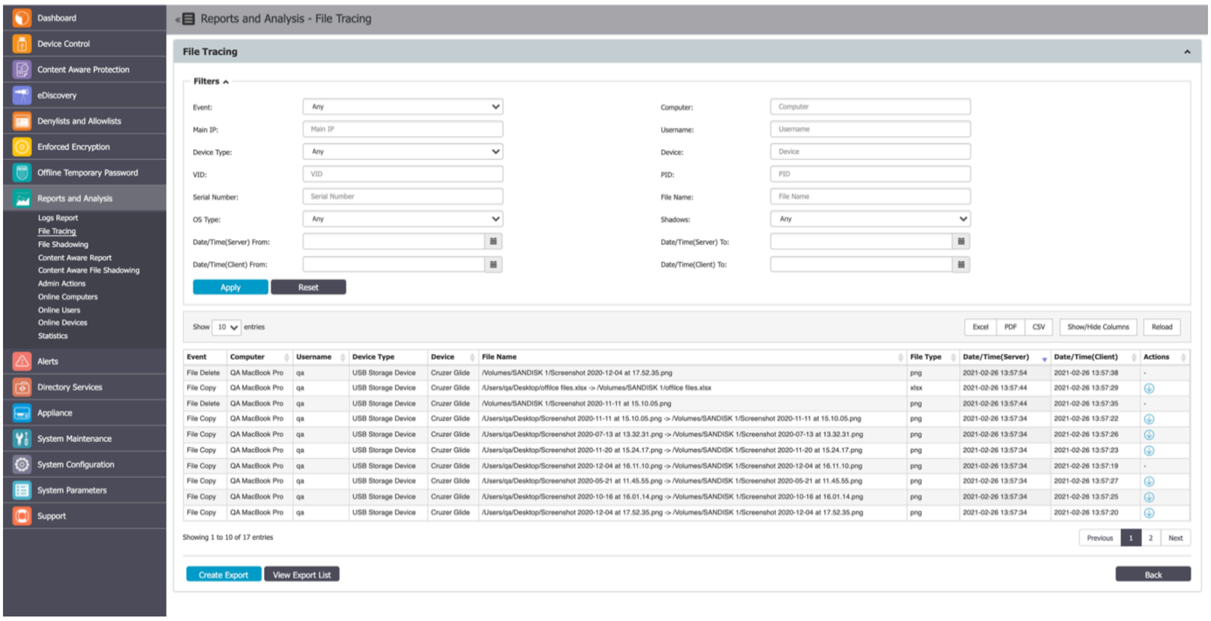
Note: Use the Filters option to view and sort different log types and then export the result list.

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.



Event: Any

Computer: Computer

Main IP: Main IP

Username: Username

Device Type: Any

Device: Device

VID: VID

PID: PID

Serial Number: Serial Number

File Name: File Name

OS Type: Any

Shadows: Any

Date/Time(Server) From:

Date/Time(Server) To:

Date/Time(Client) From:

Date/Time(Client) To:

Show 10 entries

Event	Computer	Username	Device Type	Device	File Name	File Type	Date/Time(Server)	Date/Time(Client)	Actions
File Delete	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Volumes/SANDISK 1/Screenshot 2020-12-04 at 17.52.35.png	png	2021-02-26 13:57:54	2021-02-26 13:57:38	-
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Users/qa/Desktop/offiice files.xlsx -> /Volumes/SANDISK 1/office files.xlsx	xlsx	2021-02-26 13:57:44	2021-02-26 13:57:29	↓
File Delete	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Volumes/SANDISK 1/Screenshot 2020-11-11 at 15.10.05.png	png	2021-02-26 13:57:44	2021-02-26 13:57:35	-
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Users/qa/Desktop/Screenshot 2020-11-11 at 15.10.05.png -> /Volumes/SANDISK 1/Screenshot 2020-11-11 at 15.10.05.png	png	2021-02-26 13:57:34	2021-02-26 13:57:22	↓
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Users/qa/Desktop/Screenshot 2020-07-13 at 13.32.31.png -> /Volumes/SANDISK 1/Screenshot 2020-07-13 at 13.32.31.png	png	2021-02-26 13:57:34	2021-02-26 13:57:26	↓
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Users/qa/Desktop/Screenshot 2020-11-20 at 15.24.17.png -> /Volumes/SANDISK 1/Screenshot 2020-11-20 at 15.24.17.png	png	2021-02-26 13:57:34	2021-02-26 13:57:23	↓
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Users/qa/Desktop/Screenshot 2020-12-04 at 16.11.10.png -> /Volumes/SANDISK 1/Screenshot 2020-12-04 at 16.11.10.png	png	2021-02-26 13:57:34	2021-02-26 13:57:19	-
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Users/qa/Desktop/Screenshot 2020-05-21 at 11.45.55.png -> /Volumes/SANDISK 1/Screenshot 2020-05-21 at 11.45.55.png	png	2021-02-26 13:57:34	2021-02-26 13:57:27	↓
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Users/qa/Desktop/Screenshot 2020-10-16 at 16.01.14.png -> /Volumes/SANDISK 1/Screenshot 2020-10-16 at 16.01.14.png	png	2021-02-26 13:57:34	2021-02-26 13:57:25	↓
File Copy	QA MacBook Pro	qa	USB Storage Device	Cruzer Glide	/Users/qa/Desktop/Screenshot 2020-12-04 at 17.52.35.png -> /Volumes/SANDISK 1/Screenshot 2020-12-04 at 17.52.35.png	png	2021-02-26 13:57:34	2021-02-26 13:57:20	↓

Showing 1 to 10 of 17 entries

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.

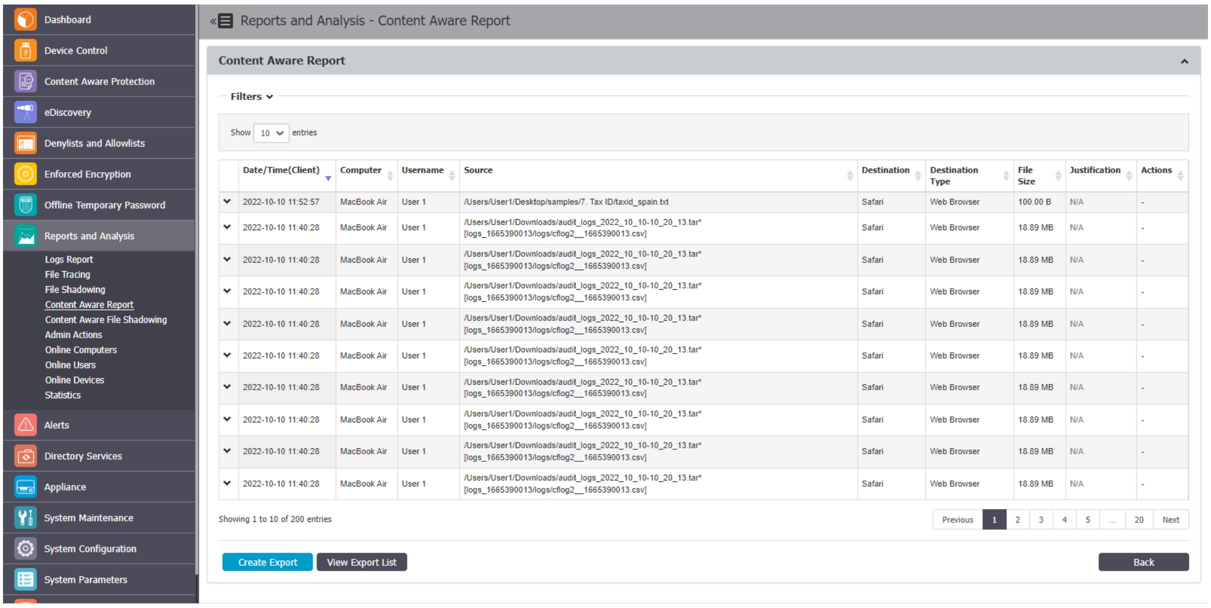
File Tracing Events Matrix by Direction			
Direction	Windows	macOS	Linux
Local -> Local (Partition 0)	N/A	N/A	N/A
Local -> Removable	Src & Dest	Src & Dest	Src & Dest
Local -> Network share	Src & Dest	Src & Dest	N/A
Local -> Partition 1	Src & Dest	N/A	N/A
Removable -> Local (Partition 0)	Src & Dest	Src & Dest	Src & Dest
Removable -> Removable	Src & Dest	Dest	Src & Dest
Removable -> Network share	Src & Dest	Dest	N/A
Removable -> Partition 1	Src & Dest	Src & Dest	Src & Dest
Network share -> Local (Partition 0)	Src & Dest	Src & Dest	N/A
Network share -> Removable	Src & Dest	Dest	N/A
Network share -> Network share	Src & Dest	Dest	N/A
Network share -> Partition 1	Src & Dest	Src & Dest	N/A
Partition 1 -> Local (Partition 0)	N/A	N/A	N/A
Partition 1 -> Removable	Src & Dest	Src & Dest	Src & Dest
Partition 1 -> Network share	Src & Dest	Src & Dest	N/A
Partition 1 -> Partition 0	N/A	N/A	N/A

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.



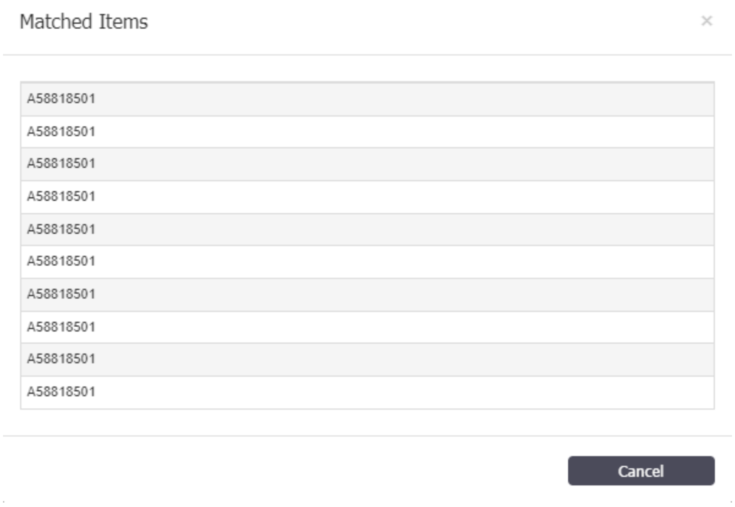
Date/Time(Client)	Computer	Username	Source	Destination	Destination Type	File Size	Justification	Actions
2022-10-10 11:52:57	MacBook Air	User 1	/Users/User1/Desktop/samples/7. Tax ID/taxid_spain.txt	Safari	Web Browser	100.00 B	N/A	-
2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-

Showing 1 to 10 of 200 entries

When using the latest Endpoint Protector client, you can view log details structured per file scanned.

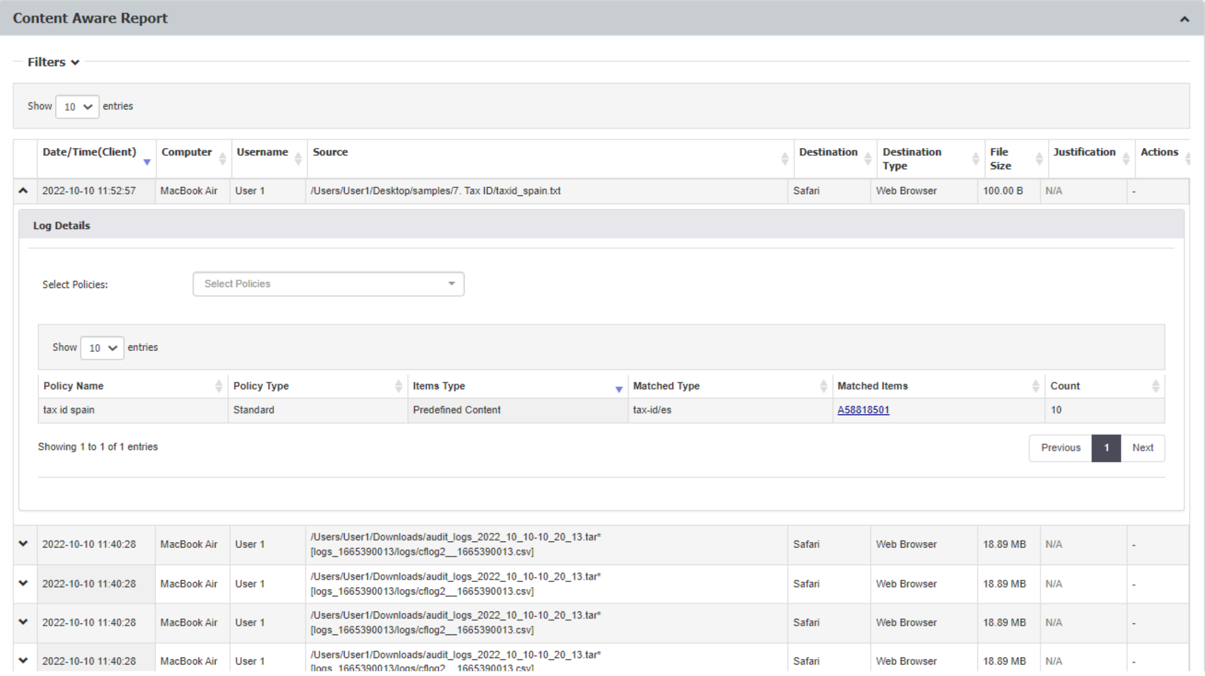
Expand each entry from the log report list to view the Log Details expanded section, providing the following information:

- **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


Matched Items

A58818501
A58818501
A58818501
A58818501
A58818501
A58818501
A58818501
A58818501
A58818501
A58818501

- **Count** – the number of matched items


Content Aware Report

Filters

Show 10 entries

	Date/Time(Client)	Computer	Username	Source	Destination	Destination Type	File Size	Justification	Actions
^	2022-10-10 11:52:57	MacBook Air	User 1	/Users/User1/Desktop/samples/7. Tax ID/taxid_spain.txt	Safari	Web Browser	100.00 B	N/A	-

Log Details

Select Policies: Select Policies

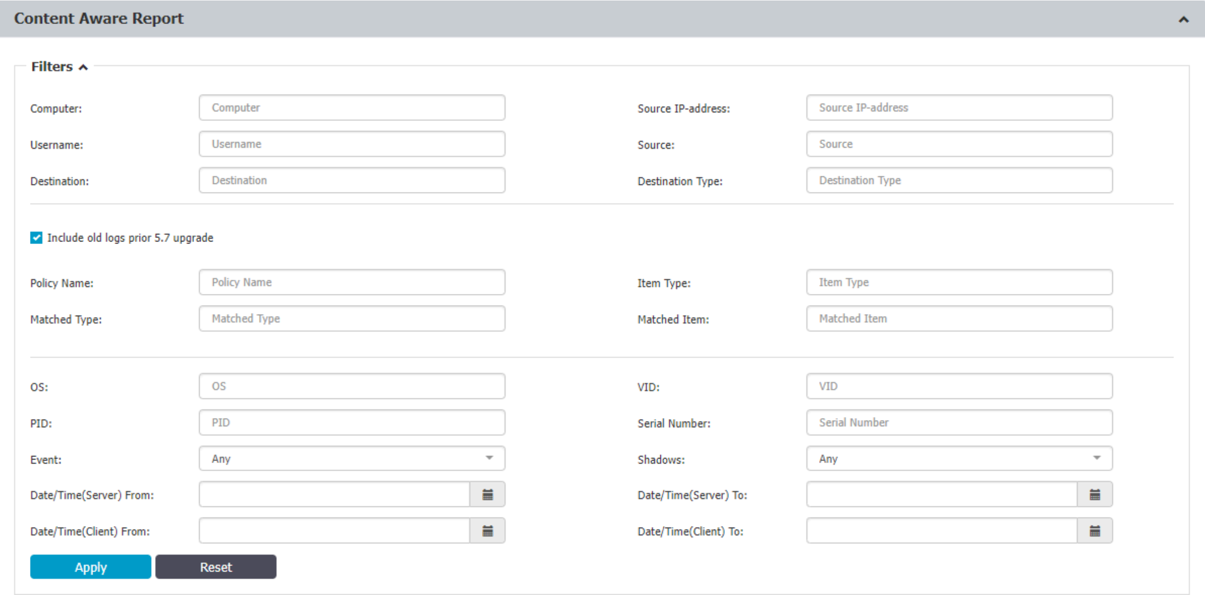
Show 10 entries

Policy Name	Policy Type	Items Type	Matched Type	Matched Items	Count
tax id spain	Standard	Predefined Content	tax-id/es	A58818501	10

Showing 1 to 1 of 1 entries

	Date/Time(Client)	Computer	Username	Source	Destination	Destination Type	File Size	Justification	Actions
v	2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
v	2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
v	2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-
v	2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]	Safari	Web Browser	18.89 MB	N/A	-

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.



Content Aware Report

Filters

Computer:	Computer	Source IP-address:	Source IP-address
Username:	Username	Source:	Source
Destination:	Destination	Destination Type:	Destination Type

☑ Include old logs prior 5.7 upgrade

Policy Name:	Policy Name	Item Type:	Item Type
Matched Type:	Matched Type	Matched Item:	Matched Item
OS:	OS	VID:	VID
PID:	PID	Serial Number:	Serial Number
Event:	Any	Shadows:	Any
Date/Time(Server) From:		Date/Time(Server) To:	
Date/Time(Client) From:		Date/Time(Client) To:	

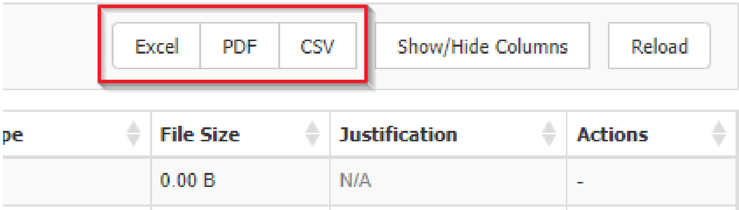
Note: For Mac users, when the DPI (Deep Packet Inspection) feature is enabled on the EPP agent for Mac, there might be certain scenarios where the agent does not provide full destination details for files being transferred from a network share through monitored applications, such as browsers. In such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

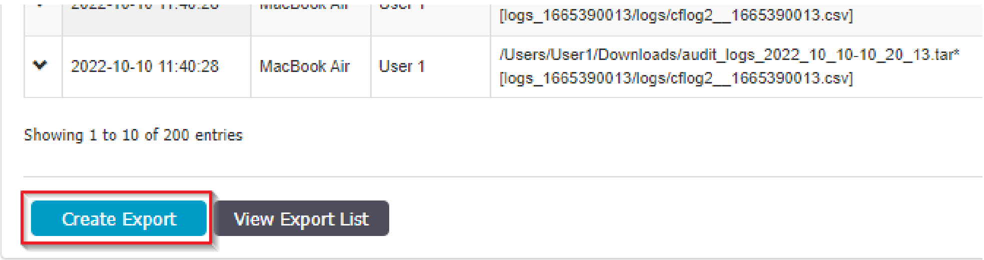
You can export Content Aware Logs as an Excel, PDF, or CSV or create and export the entire log report as a CSV or XLSX file.

- **Excel/PDF/CSV** – situated above the Content Aware Reports list, this will export only the default columns



pe	File Size	Justification	Actions
	0.00 B	N/A	-

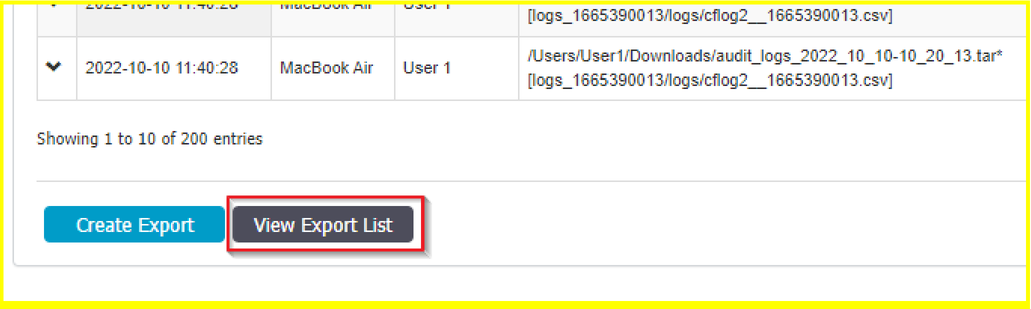
- **Create Export** – situated below the Content Aware Reports list, this will create an export containing all data, including the expanded Logs Details section with columns Policy Type, Policy Name, Item type, Matched type, Matched items and Count.



				[logs_1665390013/logs/cflog2__1665390013.csv]
⌄	2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]

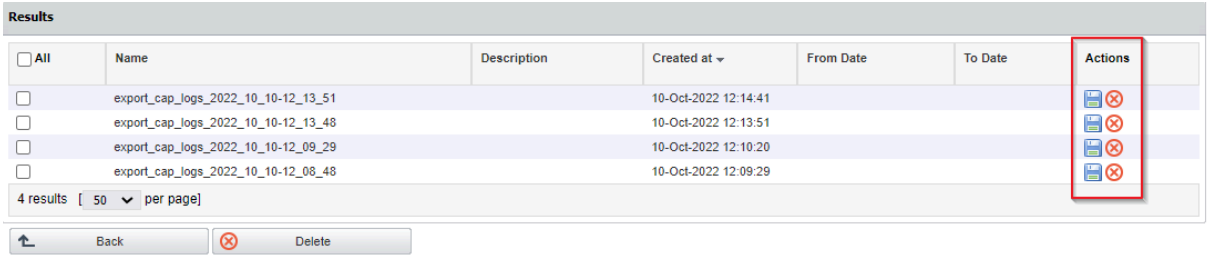
Showing 1 to 10 of 200 entries

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.



				[logs_1665390013/logs/cflog2__1665390013.csv]
⌄	2022-10-10 11:40:28	MacBook Air	User 1	/Users/User1/Downloads/audit_logs_2022_10_10-10_20_13.tar* [logs_1665390013/logs/cflog2__1665390013.csv]

Showing 1 to 10 of 200 entries



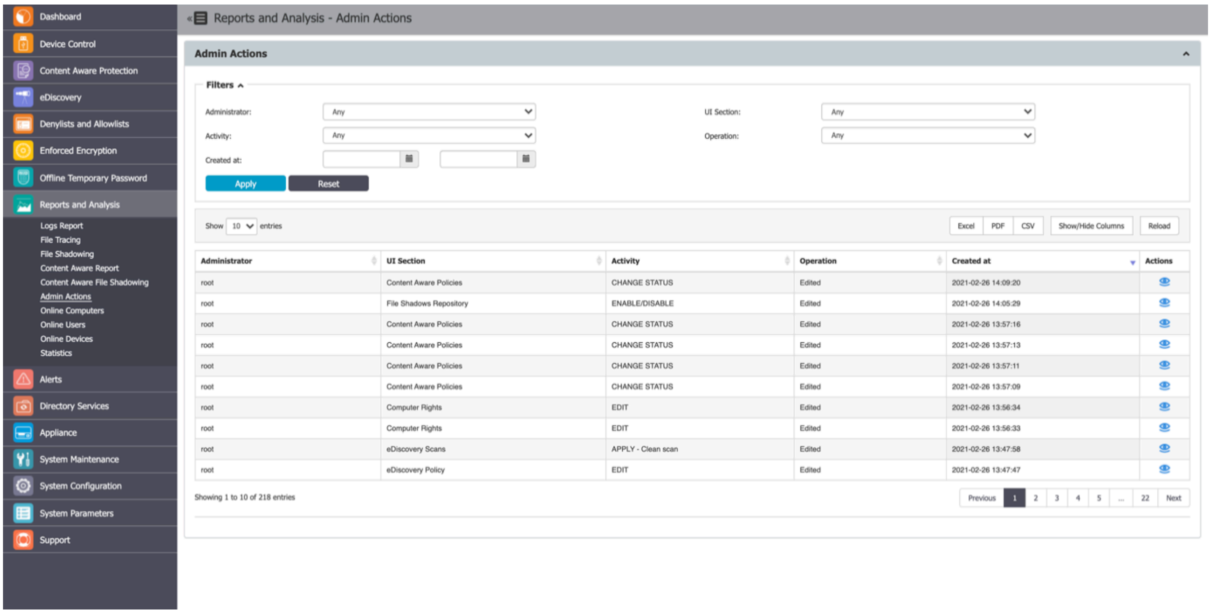
Results

□ All	Name	Description	Created at ▾	From Date	To Date	Actions
□	export_cap_logs_2022_10_10-12_13_51		10-Oct-2022 12:14:41			💾 ⊗
□	export_cap_logs_2022_10_10-12_13_48		10-Oct-2022 12:13:51			💾 ⊗
□	export_cap_logs_2022_10_10-12_09_29		10-Oct-2022 12:10:20			💾 ⊗
□	export_cap_logs_2022_10_10-12_08_48		10-Oct-2022 12:09:29			💾 ⊗

4 results [50 ⌄ per page]

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.



Admin Actions

Filters

Administrator: Any
UI Section: Any
Activity: Any
Operation: Any
Created at:

Show 10 entries

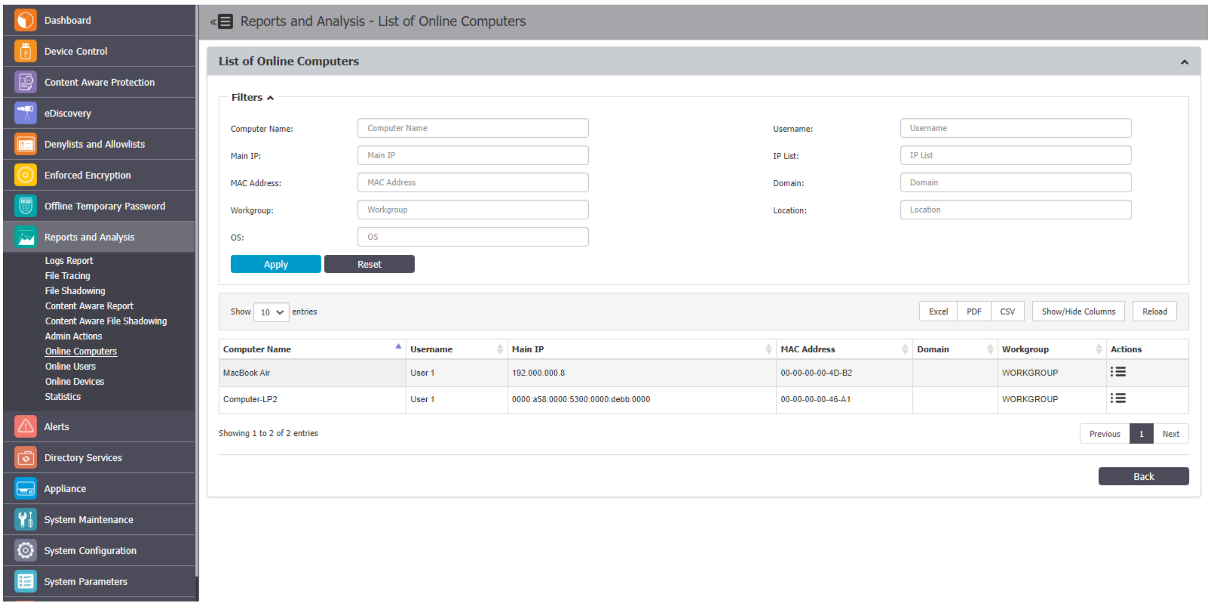
Administrator	UI Section	Activity	Operation	Created at	Actions
root	Content Aware Policies	CHANGE STATUS	Edited	2021-02-26 14:09:20	👁
root	File Shadows Repository	ENABLE/DISABLE	Edited	2021-02-26 14:05:29	👁
root	Content Aware Policies	CHANGE STATUS	Edited	2021-02-26 13:57:16	👁
root	Content Aware Policies	CHANGE STATUS	Edited	2021-02-26 13:57:13	👁
root	Content Aware Policies	CHANGE STATUS	Edited	2021-02-26 13:57:11	👁
root	Content Aware Policies	CHANGE STATUS	Edited	2021-02-26 13:57:09	👁
root	Computer Rights	EDIT	Edited	2021-02-26 13:56:34	👁
root	Computer Rights	EDIT	Edited	2021-02-26 13:56:33	👁
root	eDiscovery Scans	APPLY - Clean scan	Edited	2021-02-26 13:47:58	👁
root	eDiscovery Policy	EDIT	Edited	2021-02-26 13:47:47	👁

Showing 1 to 10 of 218 entries

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.



List of Online Computers

Filters

Computer Name: Computer Name
Username: Username
Main IP: Main IP
IP List: IP List
MAC Address: MAC Address
Domain: Domain
Workgroup: Workgroup
Location: Location
OS: OS

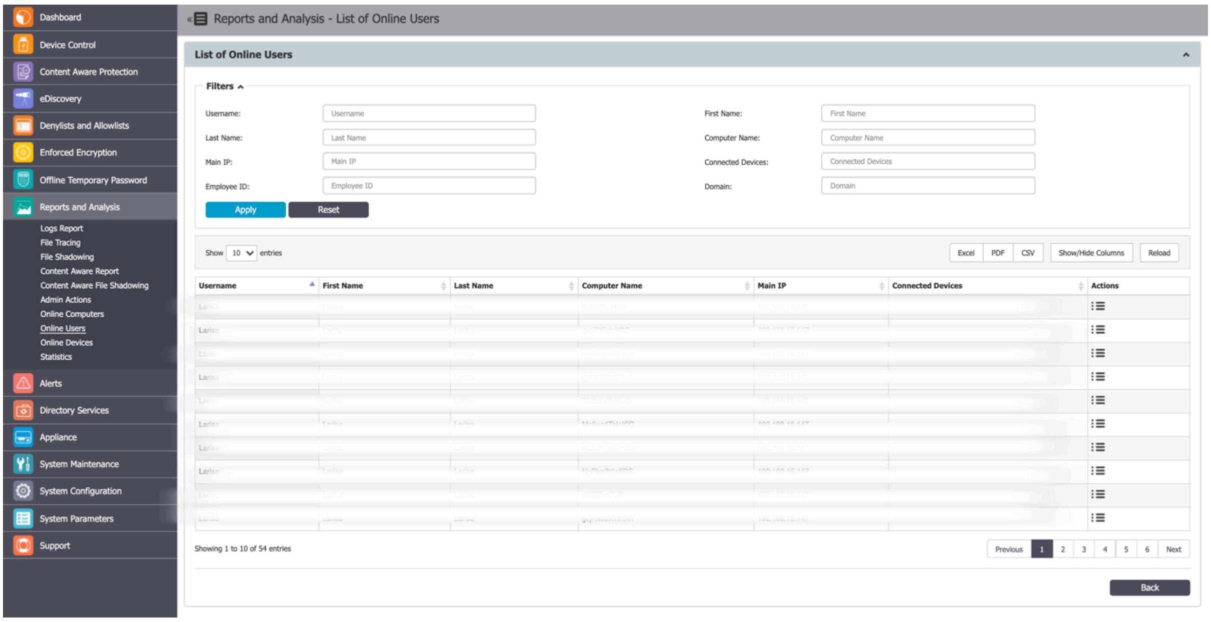
Show 10 entries

Computer Name	Username	Main IP	MAC Address	Domain	Workgroup	Actions
MacBook Air	User 1	192.000.000.8	00-00-00-00-4D-B2		WORKGROUP	☰
Computer-LP2	User 1	0000:a58:0000:5300:0000:debb:0000	00-00-00-00-46-A1		WORKGROUP	☰

Showing 1 to 2 of 2 entries

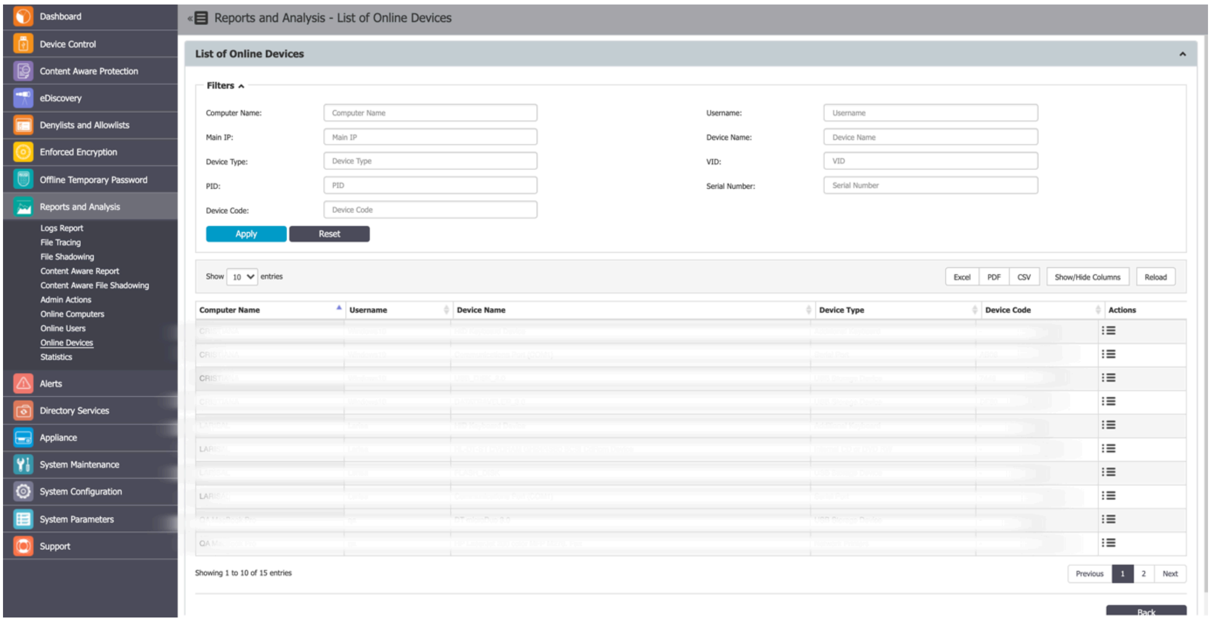
11.6.Online Users

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



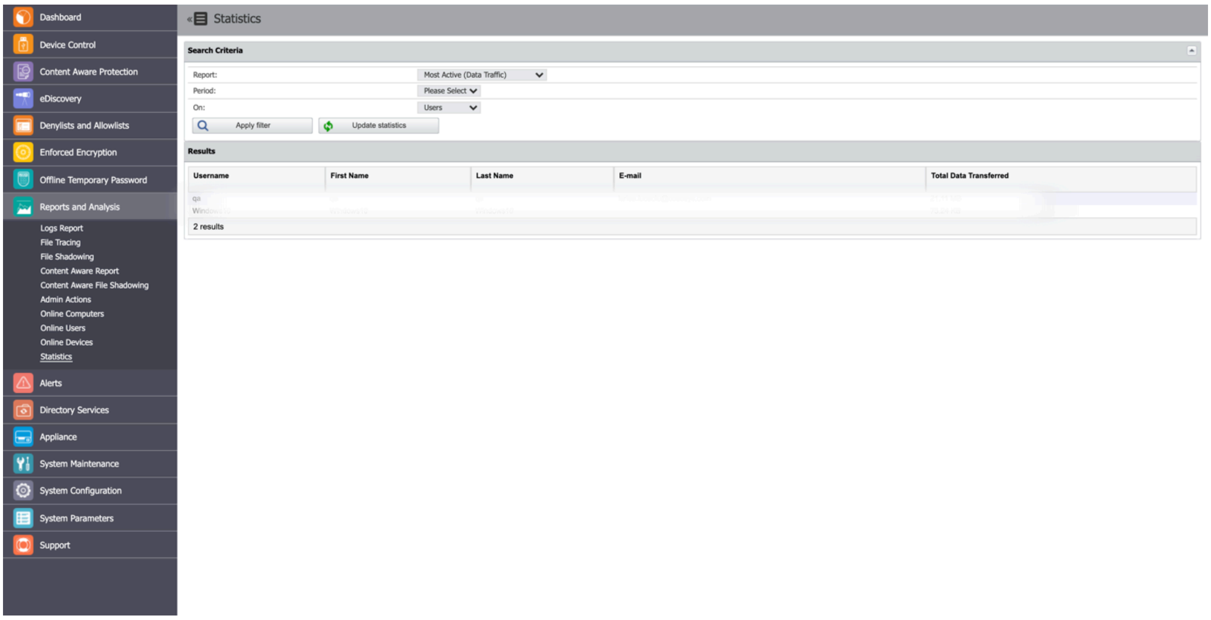
11.7. Online Devices

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.



Search Criteria

Report: Most Active (Data Traffic)

Period: Please Select

On: Users

Results

Username	First Name	Last Name	E-mail	Total Data Transferred
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

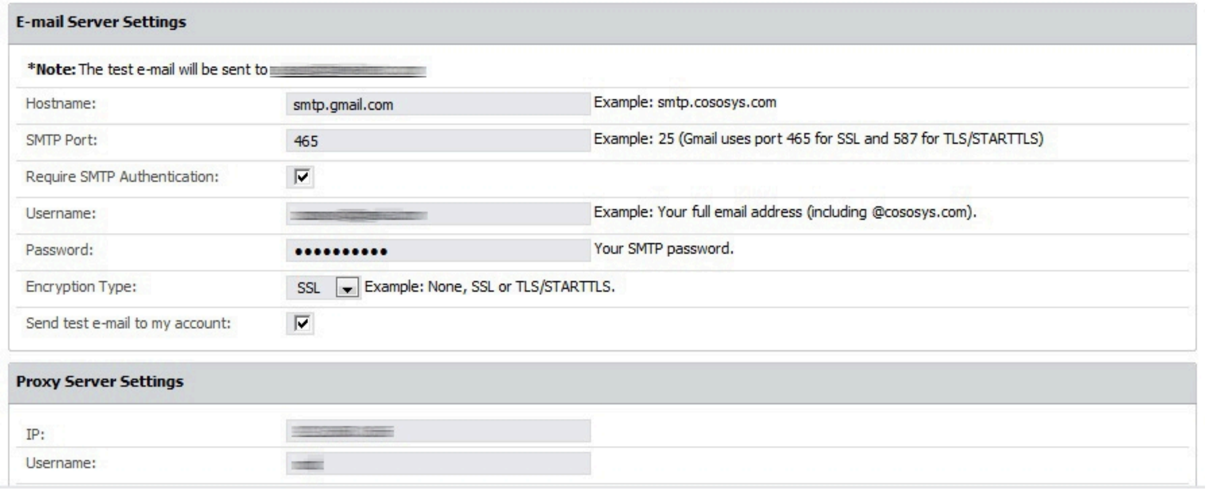
2 results

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.



E-mail Server Settings

***Note:** The test e-mail will be sent to [redacted]

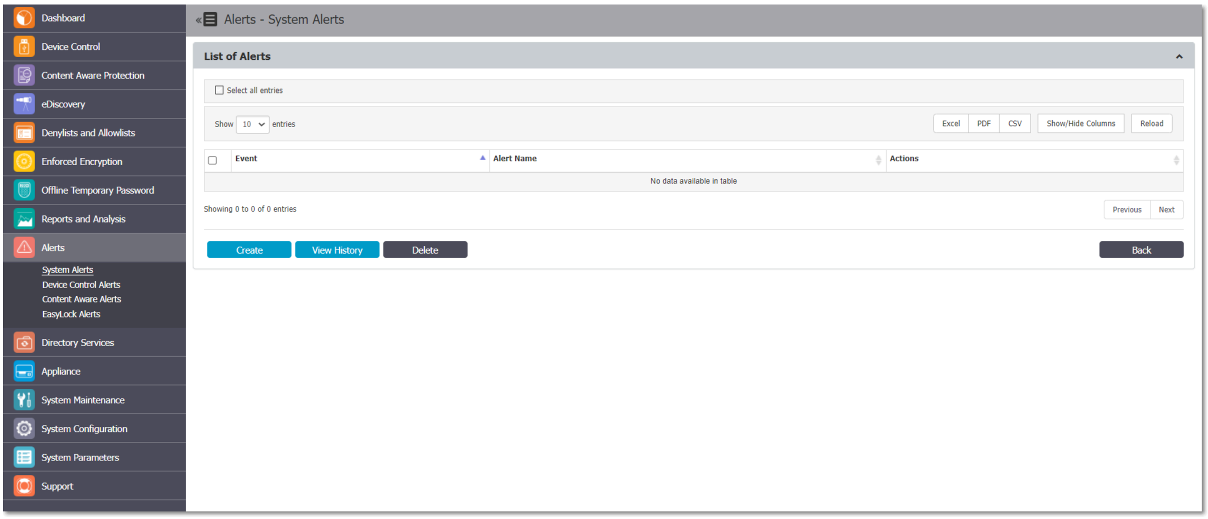
Hostname:	smtp.gmail.com	Example: smtp.cososys.com
SMTP Port:	465	Example: 25 (Gmail uses port 465 for SSL and 587 for TLS/STARTTLS)
Require SMTP Authentication:	☑	
Username:	[redacted]	Example: Your full email address (including @cososys.com).
Password:	••••••••••	Your SMTP password.
Encryption Type:	SSL ▾	Example: None, SSL or TLS/STARTTLS.
Send test e-mail to my account:	☑	

Proxy Server Settings

IP:	[redacted]
Username:	[redacted]

12.1.System Alerts

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



□	Event	Alert Name	Actions
		No data available in table	

Showing 0 to 0 of 0 entries

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.

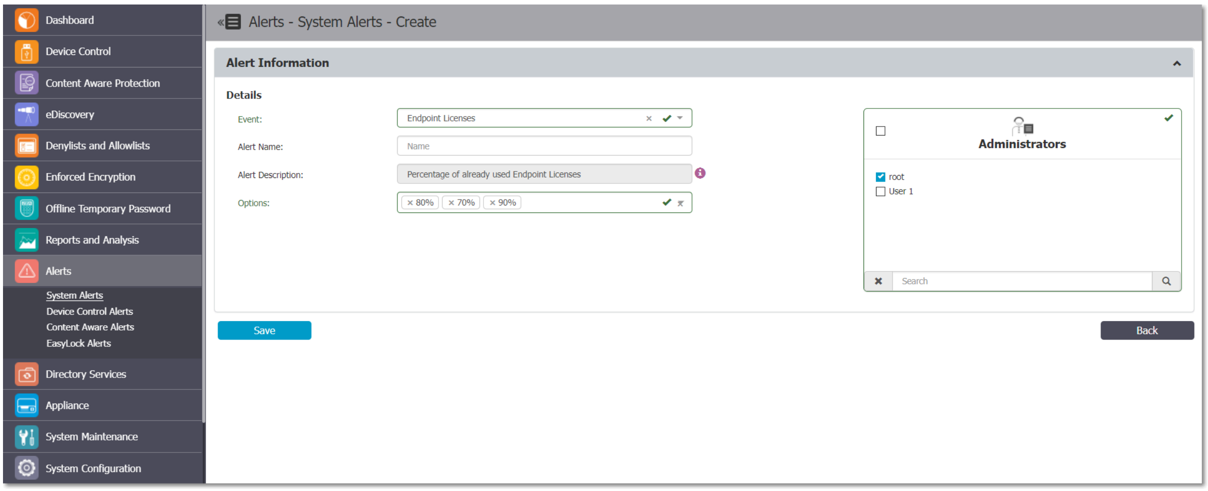
  Define alerts when disk space reaches 70%, 80%, or 90% and then select the monitored partitions from the available root, epp and boot.
- **Device Control – Logs Amount –** set an alert each time the Number of Device Control Logs Stored reaches a specific amount. Select from the available intervals or 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.

- **Password Expiration** – set an alert to be notified when a password is about to expire. Define the alert using the 10, 5, or 1 day options.
- **Not Seen Online –** set an alert each time a protected endpoint has not been seen online in the specific timeframe. Select an option from the available intervals or define a custom interval. This alert can also identify computers where the Endpoint Protector Client might have been uninstalled.
- **Unplanned Client Termination** – set an alert to identify when a user tries to terminate the Endpoint Protector process.

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

3. **Options** – based on the type of alert you selected, define the alert using the additional options

4. **Administrators** - select the Administrators that will receive the alerts.



Alerts - System Alerts - Create

Alert Information

Details

Event: Endpoint Licenses

Alert Name: Name

Alert Description: Percentage of already used Endpoint Licenses

Options: × 80% × 70% × 90%

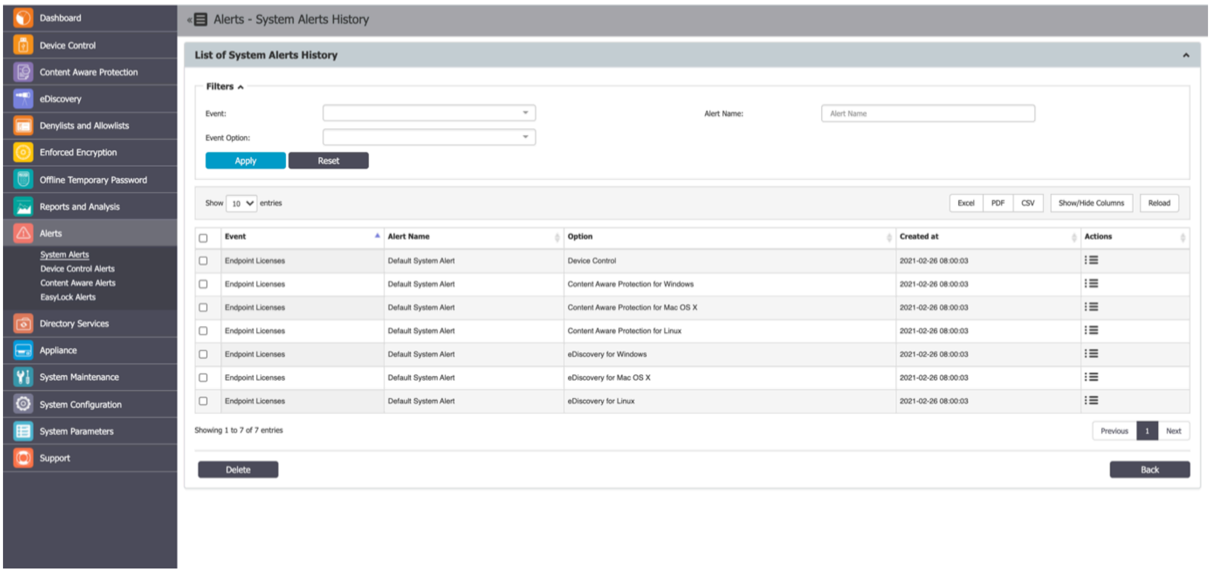
Administrators

☑ root

☐ User 1

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.



Alerts - System Alerts History

List of System Alerts History

Filters

Event:

Event Option:

Alert Name: Alert Name

Apply Reset

Show 10 entries

Excel PDF CSV Show/Hide Columns Reload

☐	Event	Alert Name	Option	Created at	Actions
☐	Endpoint Licenses	Default System Alert	Device Control	2021-02-26 08:00:03	☰
☐	Endpoint Licenses	Default System Alert	Content Aware Protection for Windows	2021-02-26 08:00:03	☰
☐	Endpoint Licenses	Default System Alert	Content Aware Protection for Mac OS X	2021-02-26 08:00:03	☰
☐	Endpoint Licenses	Default System Alert	Content Aware Protection for Linux	2021-02-26 08:00:03	☰
☐	Endpoint Licenses	Default System Alert	eDiscovery for Windows	2021-02-26 08:00:03	☰
☐	Endpoint Licenses	Default System Alert	eDiscovery for Mac OS X	2021-02-26 08:00:03	☰
☐	Endpoint Licenses	Default System Alert	eDiscovery for Linux	2021-02-26 08:00:03	☰

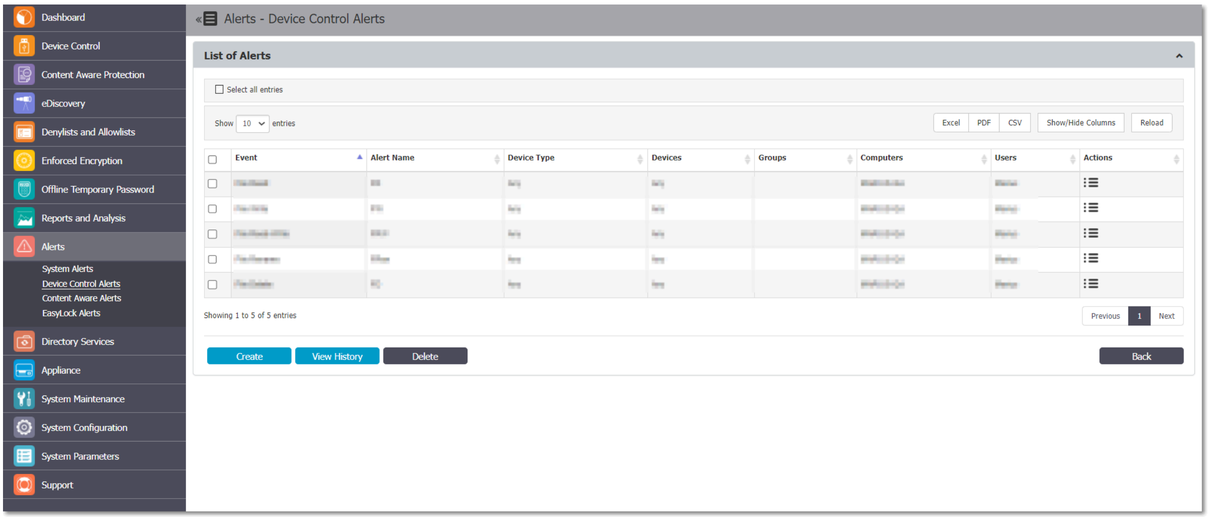
Showing 1 to 7 of 7 entries

Previous 1 Next

Delete Back

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.



Alerts - Device Control Alerts

List of Alerts

☐ Select all entries

Show 10 entries

Excel PDF CSV Show/Hide Columns Reload

☐	Event	Alert Name	Device Type	Devices	Groups	Computers	Users	Actions
☐	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	☰
☐	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	☰
☐	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	☰
☐	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	☰
☐	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	☰

Showing 1 to 5 of 5 entries

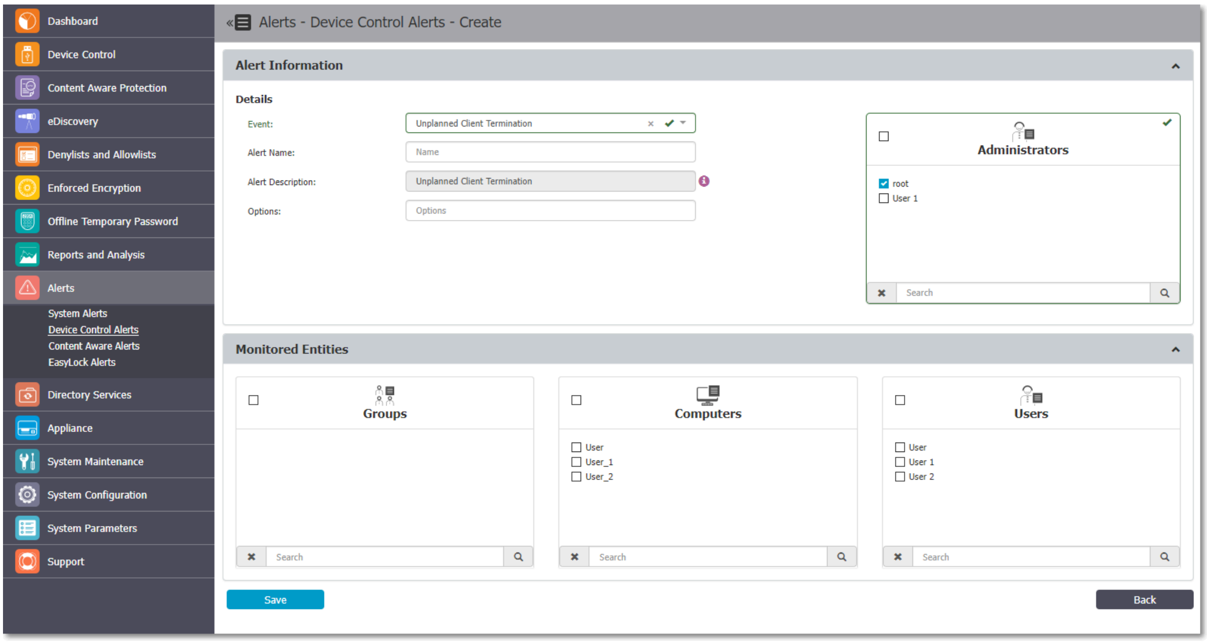
Previous 1 Next

Create View History Delete Back

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.



Alerts - Device Control Alerts - Create

Alert Information

Details

Event: Unplanned Client Termination

Alert Name: Name

Alert Description: Unplanned Client Termination

Options: Options

□ Administrators

☑ root
□ User 1

Monitored Entities

□ Groups

□ Computers

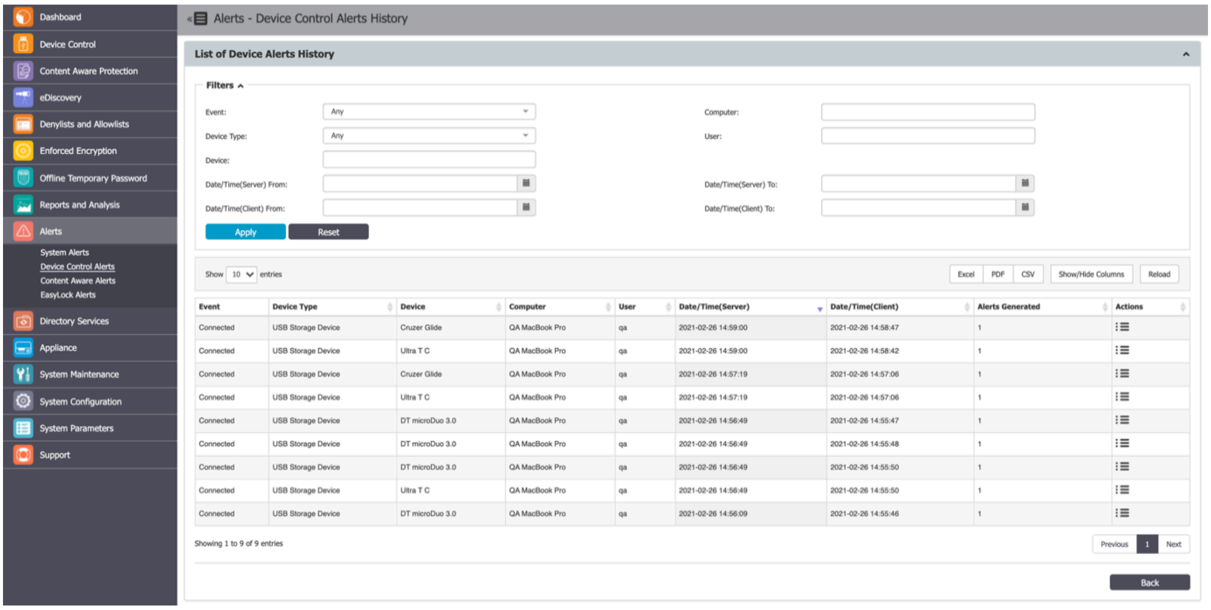
□ User
□ User_1
□ User_2

□ Users

□ User
□ User 1
□ User 2

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.



Alerts - Device Control Alerts History

List of Device Alerts History

Filters

Event: Any

Device Type: Any

Device:

Date/Time(Server) From:

Date/Time(Client) From:

Computer:

User:

Date/Time(Server) To:

Date/Time(Client) To:

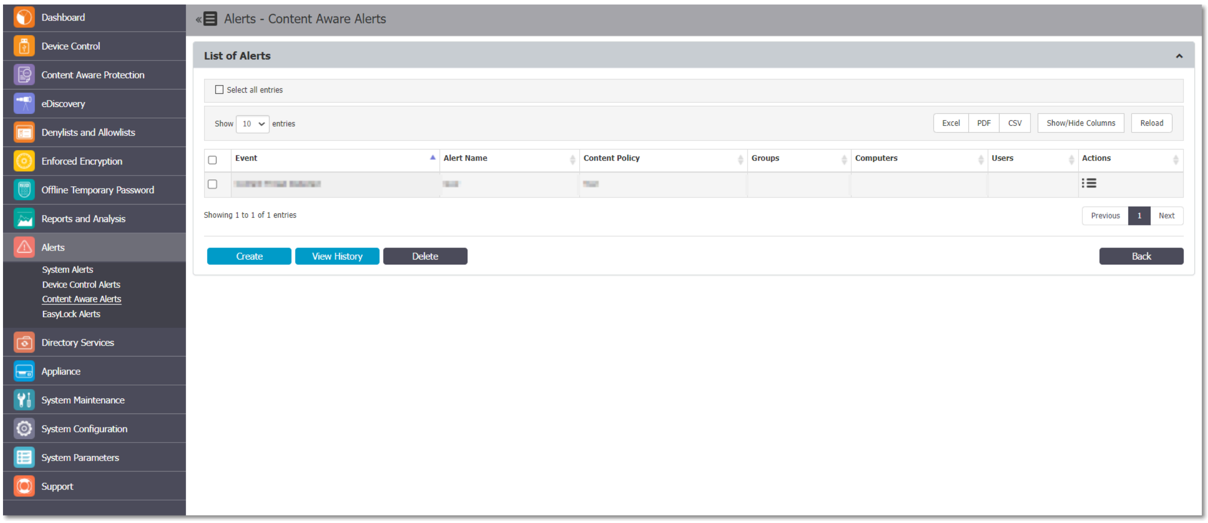
Show 10 entries

Event	Device Type	Device	Computer	User	Date/Time(Server)	Date/Time(Client)	Alerts Generated	Actions
Connected	USB Storage Device	Cruzer Glide	QA MacBook Pro	qa	2021-02-26 14:59:00	2021-02-26 14:58:47	1	☰
Connected	USB Storage Device	Ultra T C	QA MacBook Pro	qa	2021-02-26 14:59:00	2021-02-26 14:58:42	1	☰
Connected	USB Storage Device	Cruzer Glide	QA MacBook Pro	qa	2021-02-26 14:57:19	2021-02-26 14:57:06	1	☰
Connected	USB Storage Device	Ultra T C	QA MacBook Pro	qa	2021-02-26 14:57:19	2021-02-26 14:57:06	1	☰
Connected	USB Storage Device	DT microDuo 3.0	QA MacBook Pro	qa	2021-02-26 14:56:49	2021-02-26 14:55:47	1	☰
Connected	USB Storage Device	DT microDuo 3.0	QA MacBook Pro	qa	2021-02-26 14:56:49	2021-02-26 14:55:48	1	☰
Connected	USB Storage Device	DT microDuo 3.0	QA MacBook Pro	qa	2021-02-26 14:56:49	2021-02-26 14:55:50	1	☰
Connected	USB Storage Device	Ultra T C	QA MacBook Pro	qa	2021-02-26 14:56:49	2021-02-26 14:55:50	1	☰
Connected	USB Storage Device	DT microDuo 3.0	QA MacBook Pro	qa	2021-02-26 14:56:09	2021-02-26 14:55:46	1	☰

Showing 1 to 9 of 9 entries

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.



□	Event	Alert Name	Content Policy	Groups	Computers	Users	Actions
□	[redacted]	[redacted]	[redacted]				☰

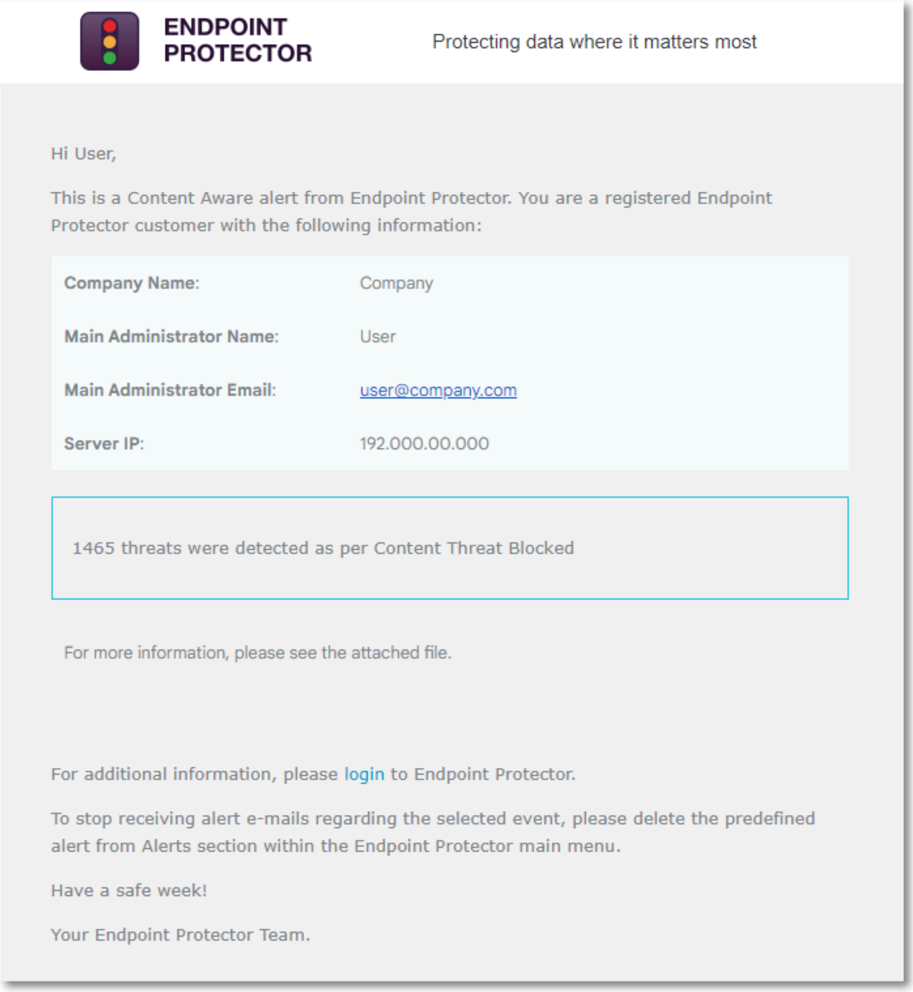
12.3.1. Creating a Content Aware Alert

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 DetectedDPI bypasswhitelist**
   - **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.



ENDPOINT PROTECTOR

Protecting data where it matters most

Hi User,

This is a Content Aware alert from Endpoint Protector. You are a registered Endpoint Protector customer with the following information:

Company Name:	Company
Main Administrator Name:	User
Main Administrator Email:	user@company.com
Server IP:	192.000.00.000

1465 threats were detected as per Content Threat Blocked

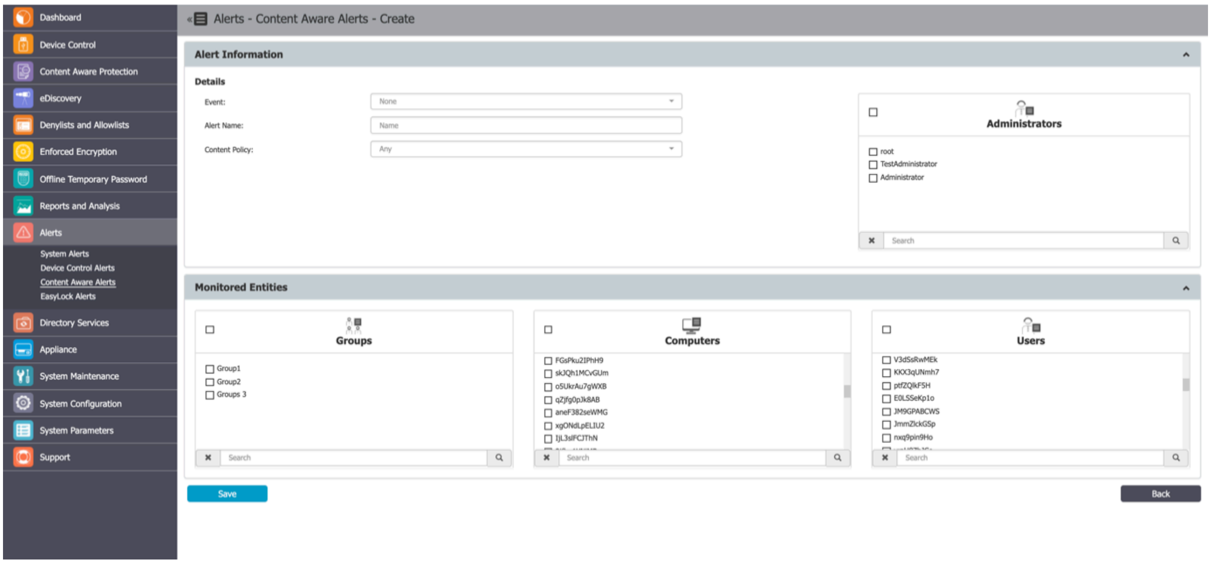
For more information, please see the attached file.

For additional information, please login to Endpoint Protector.

To stop receiving alert e-mails regarding the selected event, please delete the predefined alert from Alerts section within the Endpoint Protector main menu.

Have a safe week!

Your Endpoint Protector Team.



Alerts - Content Aware Alerts - Create

Alert Information

Details

Event: None

Alert Name: Name

Content Policy: Any

□ Administrators

□ root
□ TestAdministrator
□ Administrator

Search

Monitored Entities

□ Groups

□ Group1
□ Group2
□ Groups 3

□ Computers

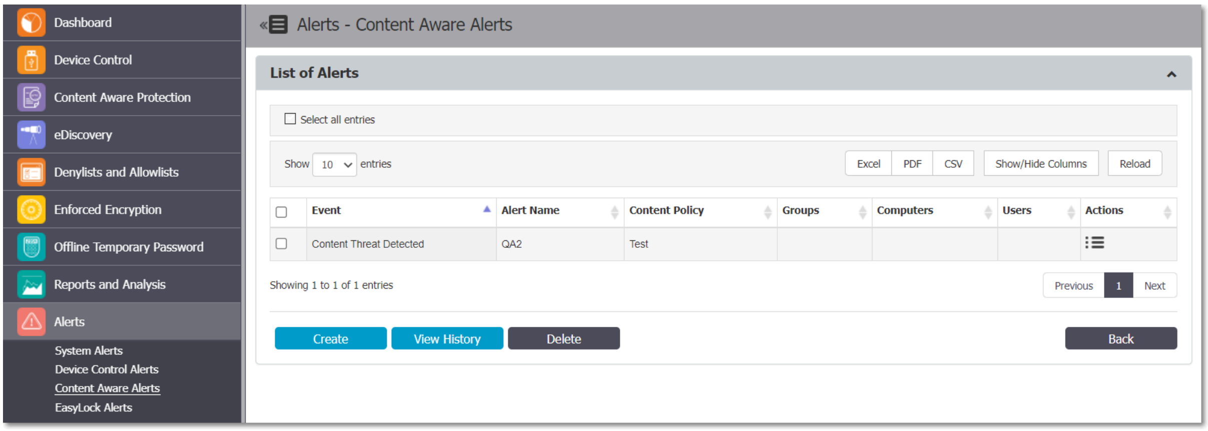
□ FGsPku2IPhH9
□ skJQh1MCvGUm
□ o5UkrAu7gWXB
□ qZjfg0pJk8AB
□ aneF382seWMG
□ xgONdLpELIU2
□ IjL3slFCJThN

□ Users

□ V3dSsRwMEk
□ KKX3qUNmh7
□ ptfZQlkF5H
□ E0LSSeKp1o
□ JM9GPABCWS
□ JmmZlckGSp
□ nxq9pin9Ho

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.

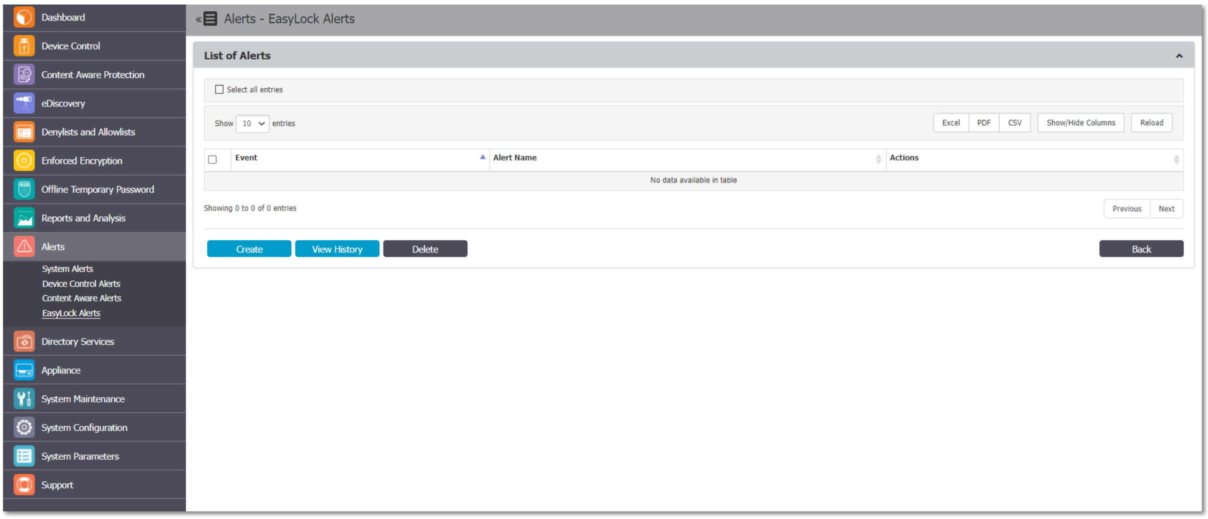


□	Event	Alert Name	Content Policy	Groups	Computers	Users	Actions
□	Content Threat Detected	QA2	Test				☰

Showing 1 to 1 of 1 entries

12.4. Enforced Encryption Alert

From this section, you can create Enforced Encryption alerts, for events such as password changes, messages sent, etc.



□	Event	Alert Name	Actions
	No data available in table		

Showing 0 to 0 of 0 entries

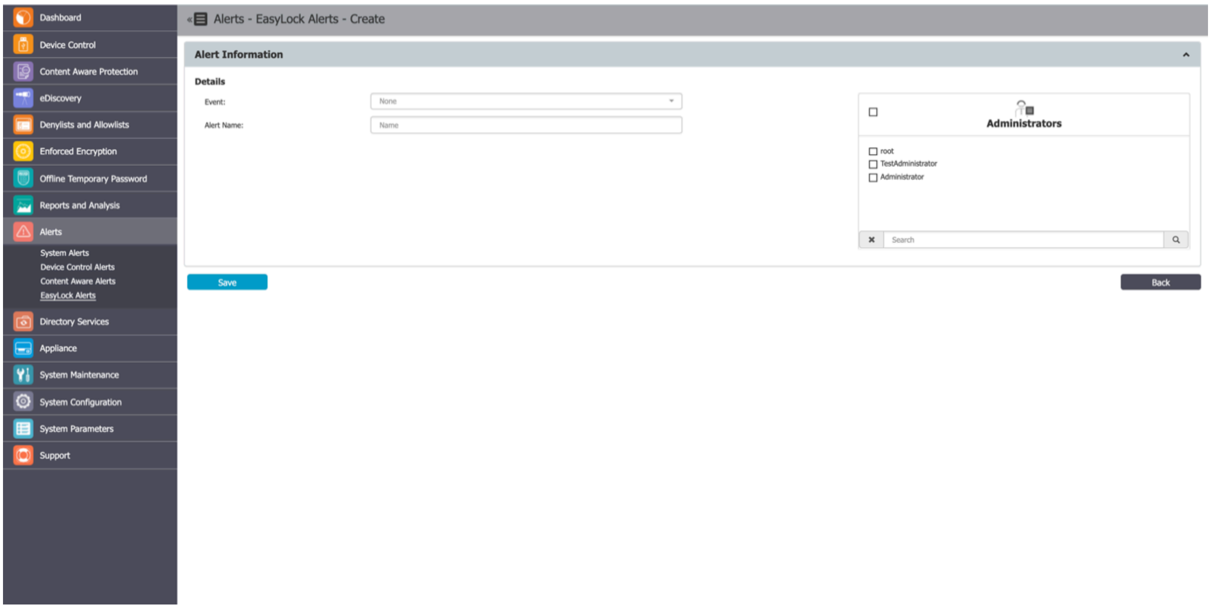
12.4.1. Creating an Enforced Encryption Alert

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**

- **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.



Alerts - EasyLock Alerts - Create

Alert Information

Details

Event: None

Alert Name: Name

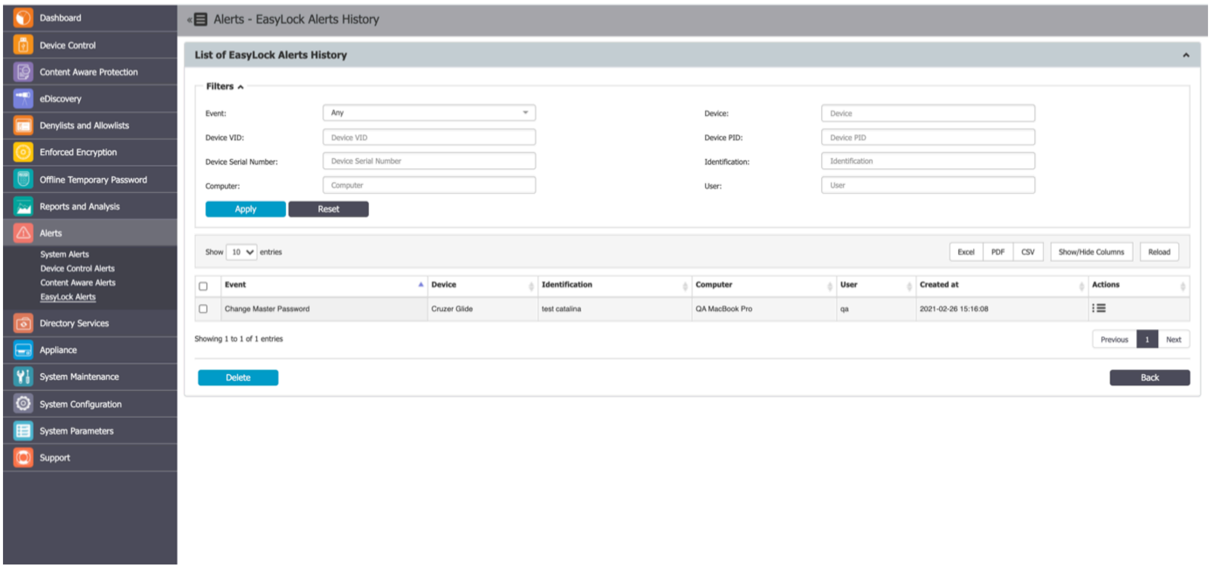
□ Administrators

□ root
□ TestAdministrator
□ Administrator

Search

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.



Alerts - EasyLock Alerts History

List of EasyLock Alerts History

Filters

Event: Any

Device: Device

Device VID: Device VID

Device PID: Device PID

Device Serial Number: Device Serial Number

Identification: Identification

Computer: Computer

User: User

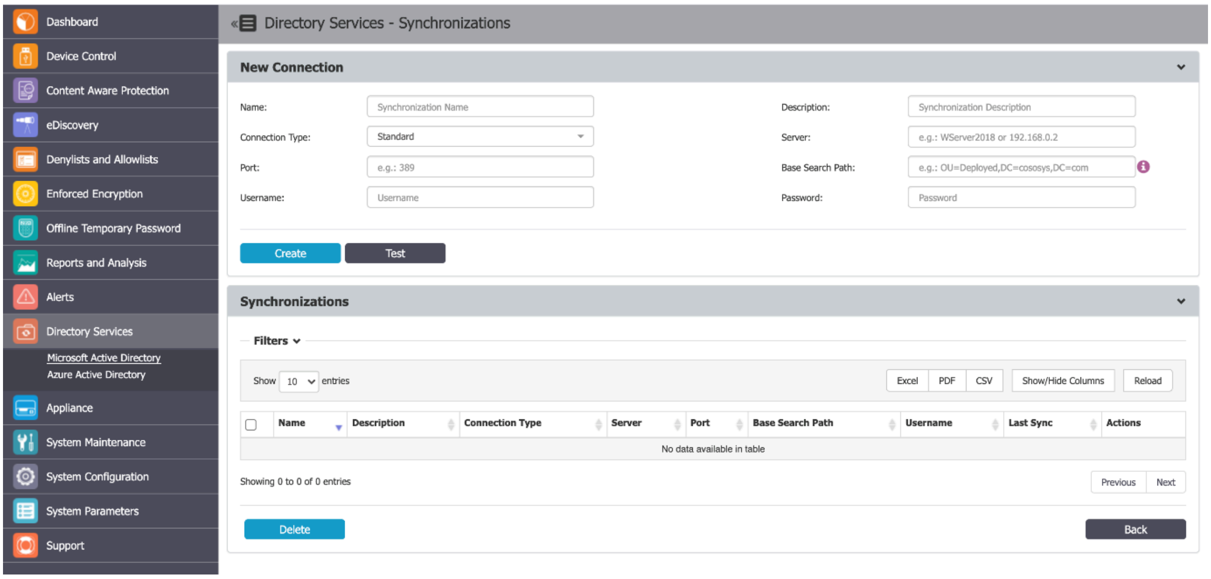
Show 10 entries

□	Event	Device	Identification	Computer	User	Created at	Actions
□	Change Master Password	Cruzer Glide	test catalina	QA MacBook Pro	qa	2021-02-26 15:16:08	☰

Showing 1 to 1 of 1 entries

13. Directory Services

From this section, you can import and synchronize the entities (Users, Computers, and Groups) from the company's Active Directories.



New Connection

Name:	Synchronization Name	Description:	Synchronization Description
Connection Type:	Standard	Server:	e.g.: WServer2018 or 192.168.0.2
Port:	e.g.: 389	Base Search Path:	e.g.: OU=Deployed,DC=cososys,DC=com
Username:	Username	Password:	Password

Synchronizations

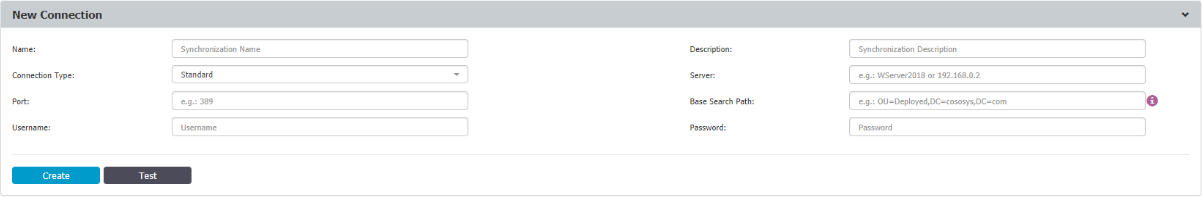
Show 10 entries

☐	Name	Description	Connection Type	Server	Port	Base Search Path	Username	Last Sync	Actions
				No data available in table					

Showing 0 to 0 of 0 entries

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.



New Connection

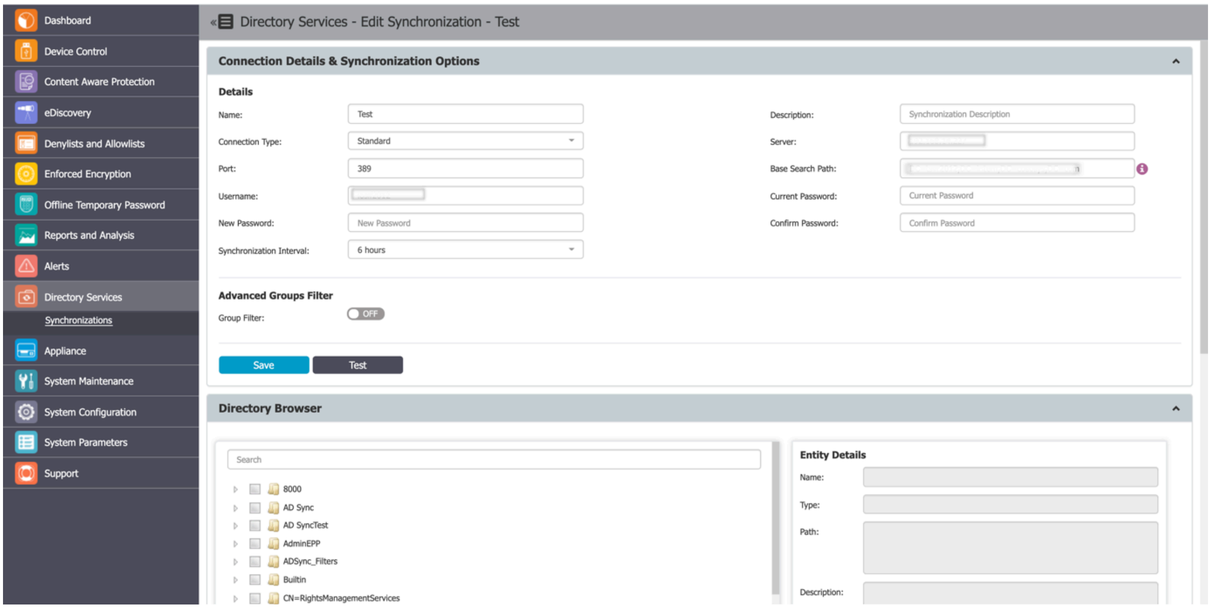
Name:	Synchronization Name	Description:	Synchronization Description
Connection Type:	Standard	Server:	e.g.: WServer2018 or 192.168.0.2
Port:	e.g.: 389	Base Search Path:	e.g.: OU=Deployed,DC=cososys,DC=com
Username:	Username	Password:	Password

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.



Directory Services - Edit Synchronization - Test

Connection Details & Synchronization Options

Details

Name:	Test
Connection Type:	Standard
Port:	389
Username:	[redacted]
New Password:	New Password
Synchronization Interval:	6 hours
Description:	Synchronization Description
Server:	[redacted]
Base Search Path:	[redacted]
Current Password:	Current Password
Confirm Password:	Confirm Password

Advanced Groups Filter

Group Filter: OFF

Directory Browser

Search

- 8000
- AD Sync
- AD SyncTest
- AdminEPP
- ADSync_Filters
- Builtin
- CN=RightsManagementServices

Entity Details

Name:

Type:

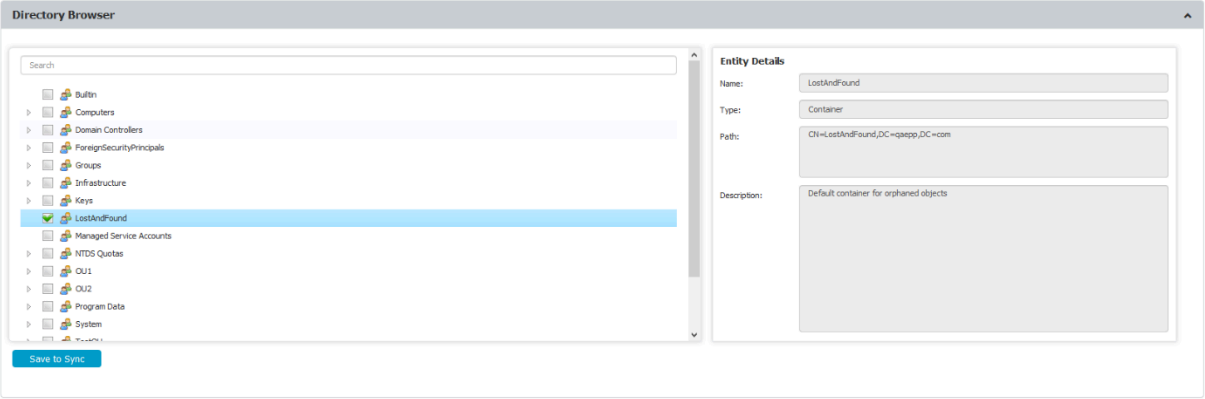
Path:

Description:

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.



Directory Browser

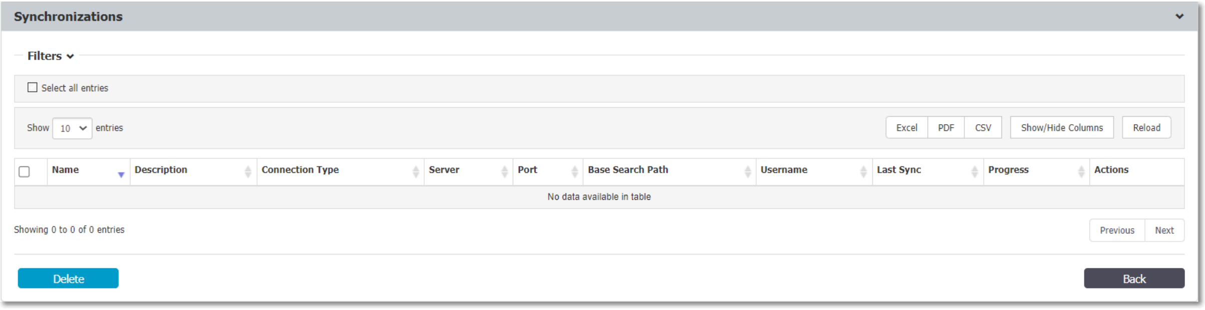
Search

- □ Builtin
- □ Computers
- □ Domain Controllers
- □ ForeignSecurityPrincipals
- □ Groups
- □ Infrastructure
- □ Keys
- ☑ LostAndFound
- □ Managed Service Accounts
- □ NTDS Quotas
- □ OU1
- □ OU2
- □ Program Data
- □ System

Entity Details

Name:	LostAndFound
Type:	Container
Path:	CN=LostAndFound,DC=qaepp,DC=com
Description:	Default container for orphaned objects

Once the entities have been selected, they can be saved to sync.



☐	Name	Description	Connection Type	Server	Port	Base Search Path	Username	Last Sync	Progress	Actions
No data available in table										

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;**

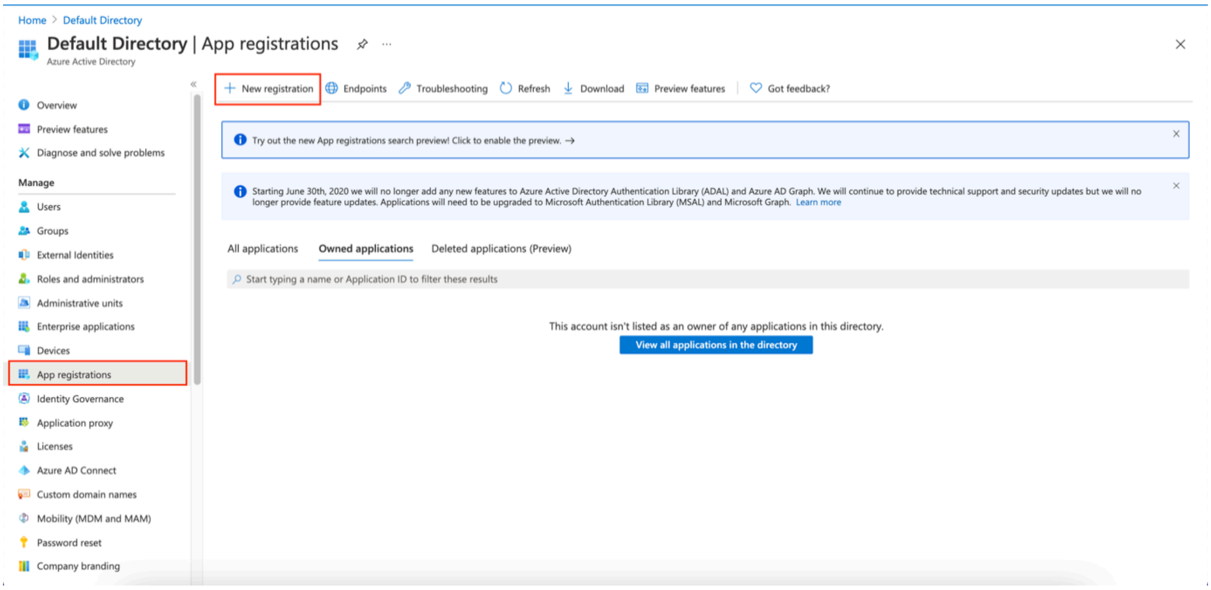
13.2.1. Configure Azure Active Directory

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**.



Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

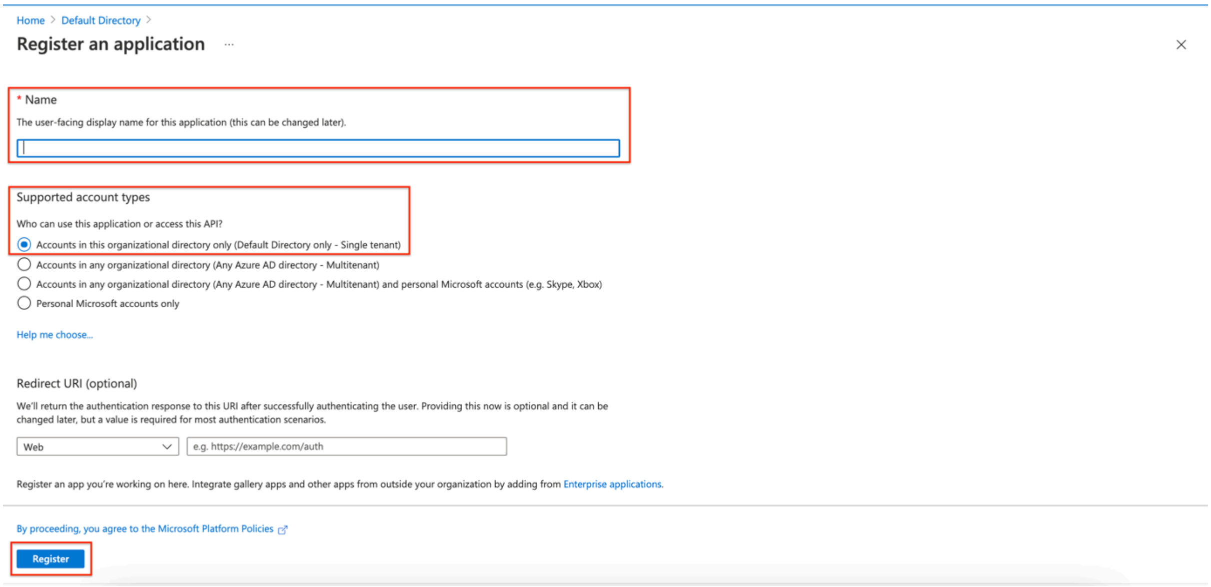
This account isn't listed as an owner of any applications in this directory.

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**.



* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Redirect URI (optional)

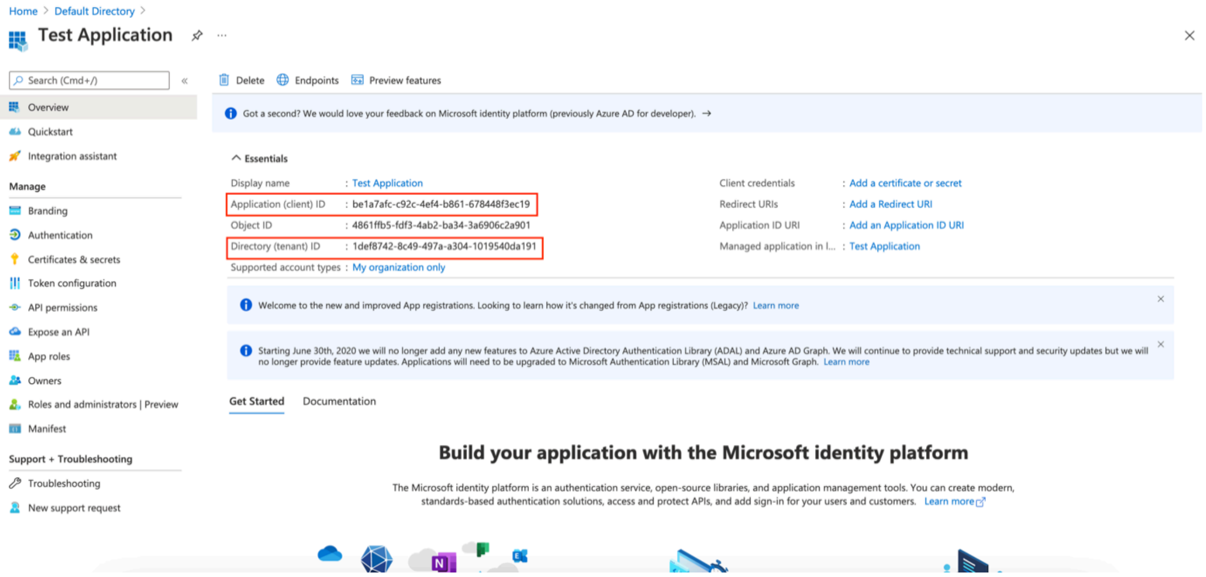
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

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.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Test Application
Application (client) ID : be1a7afc-c92c-4ef4-b861-678448f3ec19
Object ID : 4861ffb5-fdf3-4ab2-ba34-3a6906c2a901
Directory (tenant) ID : 1def8742-8c49-497a-a304-1019540da191
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : Test Application

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

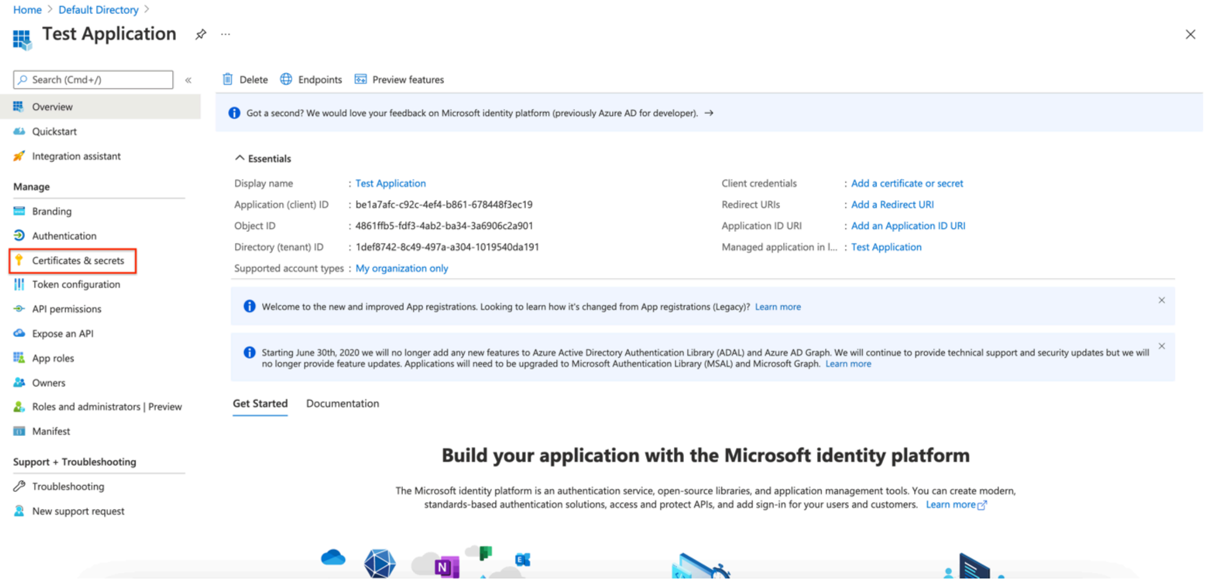
Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

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.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Test Application
Application (client) ID : be1a7afc-c92c-4ef4-b861-678448f3ec19
Object ID : 4861ffb5-fdf3-4ab2-ba34-3a6906c2a901
Directory (tenant) ID : 1def8742-8c49-497a-a304-1019540da191
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : Test Application

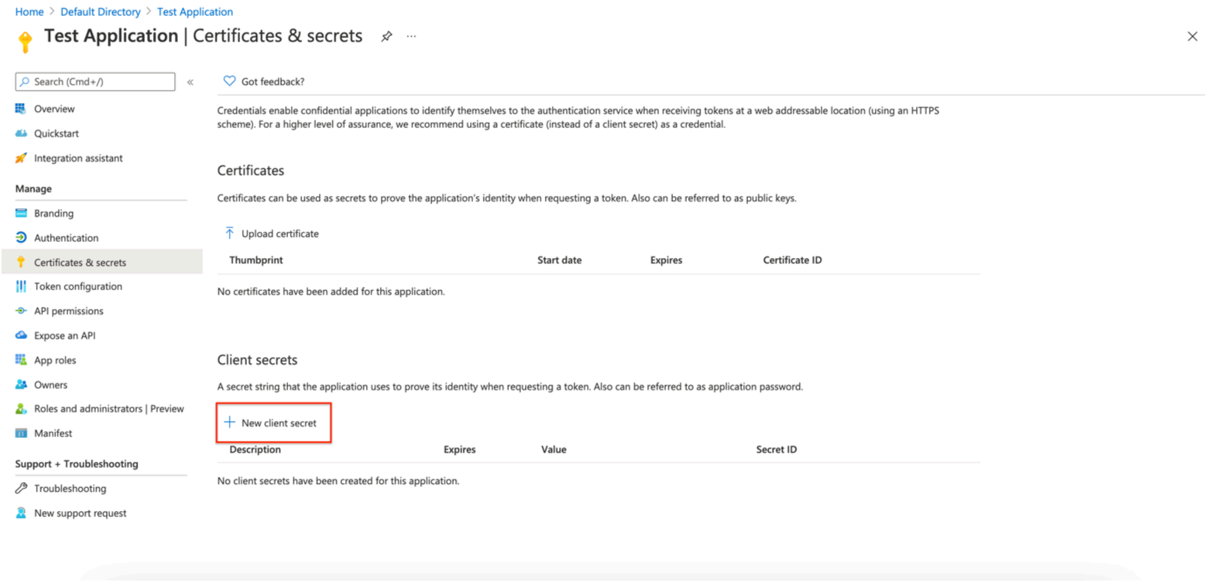
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

2. Click **New client secret** on the **Certificates & secrets** page.



Home > Default Directory > Test Application

Test Application | Certificates & secrets

- Search (Cmd+/)
- Overview
- Quickstart
- Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	Certificate ID
No certificates have been added for this application.			

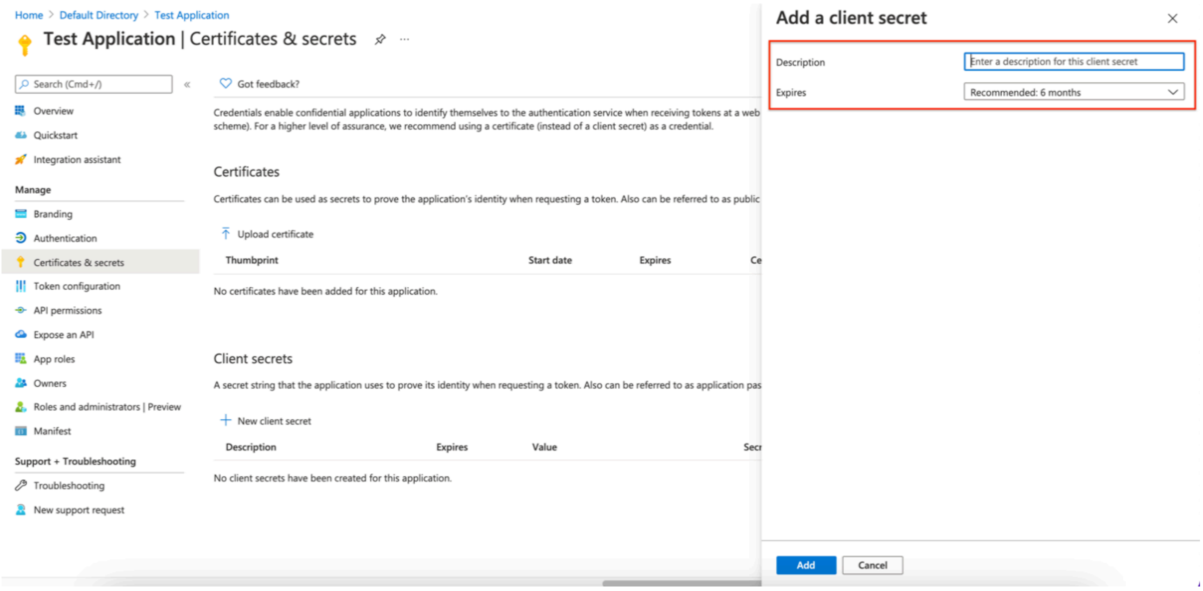
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

3. Enter a **Description** for the secret ID.



Home > Default Directory > Test Application

Test Application | Certificates & secrets

- Search (Cmd+/)
- Overview
- Quickstart
- Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public

Upload certificate

Thumbprint	Start date	Expires	Ce
No certificates have been added for this application.			

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application pas

+ New client secret

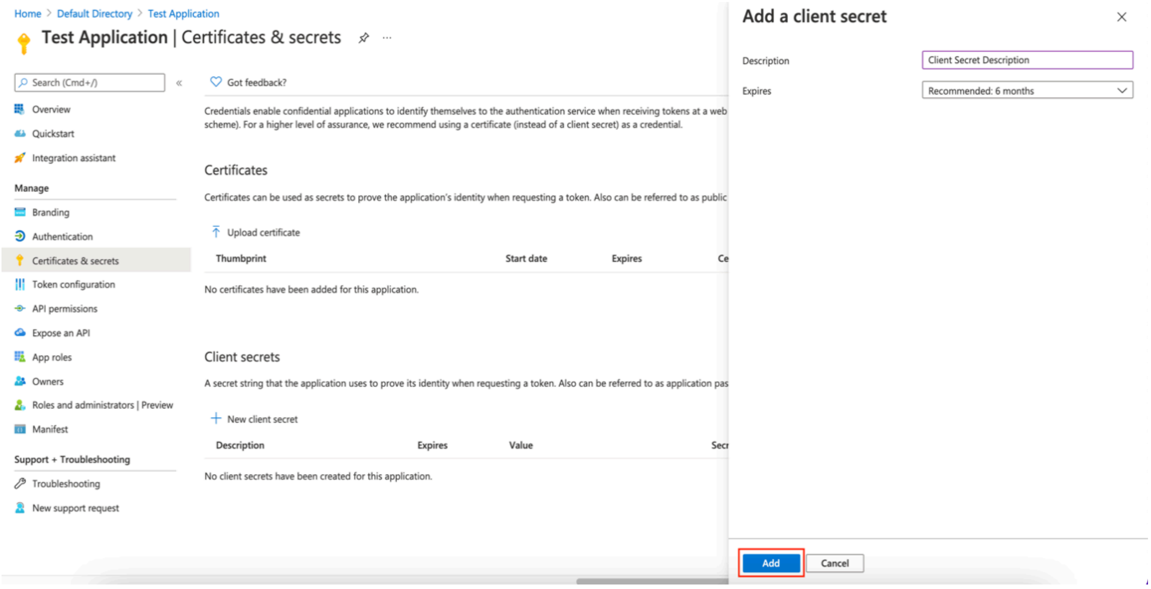
Description	Expires	Value	Secr
No client secrets have been created for this application.			

Add a client secret

Description	Enter a description for this client secret
Expires	Recommended: 6 months

Add | Cancel

4. Click **Add** and **Add a client secret** section.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public

Thumbprint	Start date	Expires	Ce

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application pas

Description	Expires	Value	Secr

No client secrets have been created for this application.

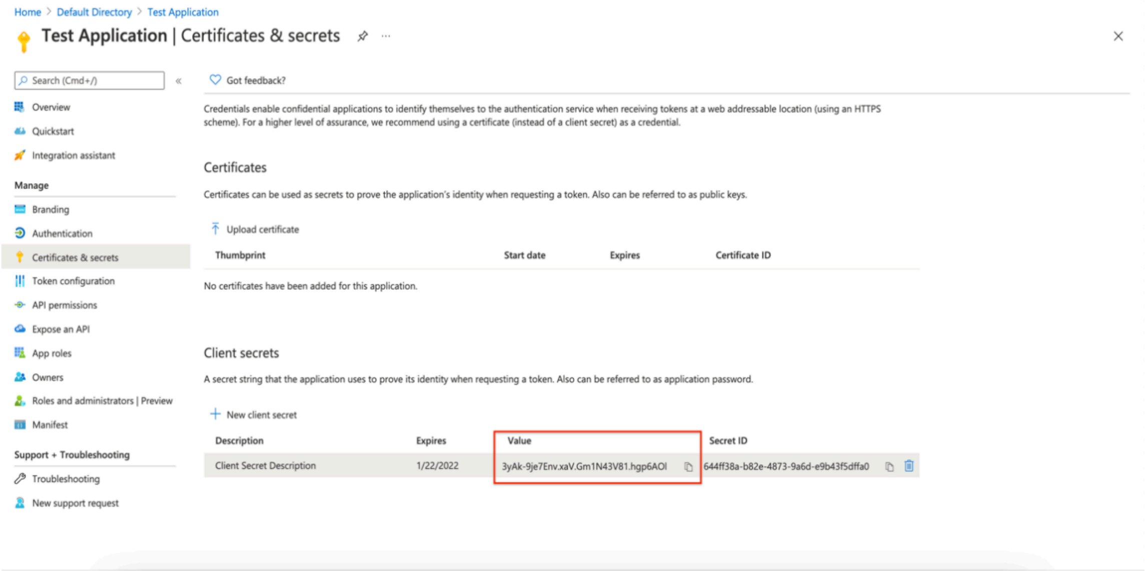
Add a client secret

Description: Client Secret Description

Expires: Recommended: 6 months

5. 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.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	Certificate ID

No certificates have been added for this application.

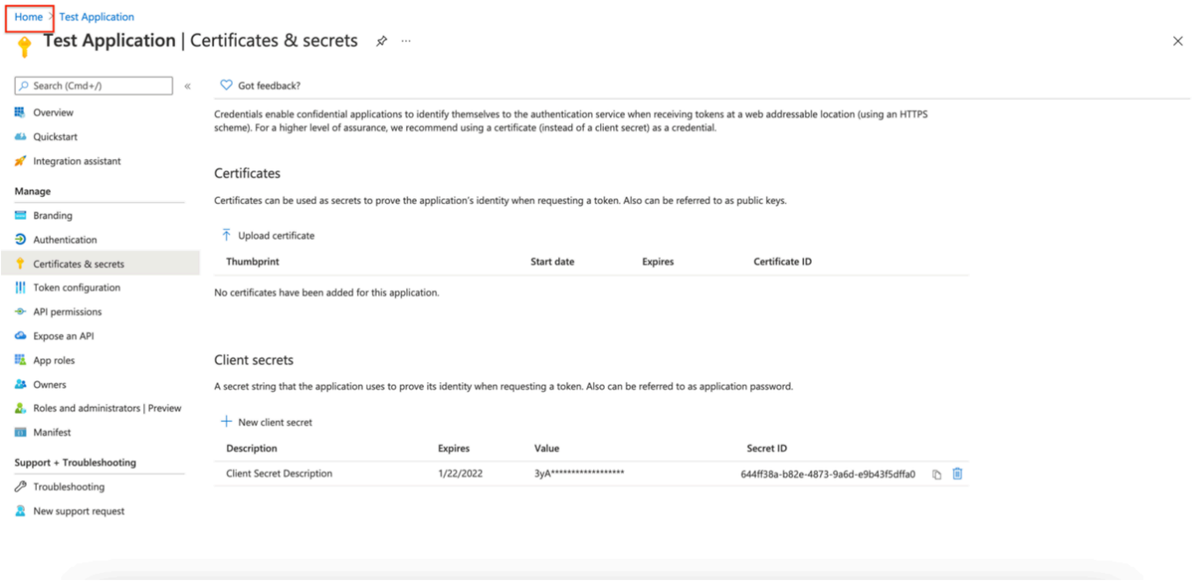
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Client Secret Description	1/22/2022	3yAk-9je7Env.xaV.Gm1N43V81.hgp6AOl	644ff38a-b82e-4873-9a6d-e9b43f5dffa0

13.2.1.3. Create Users/Groups using Graph API

1. Click **Home** and then **Azure Active Directory**.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	Certificate ID

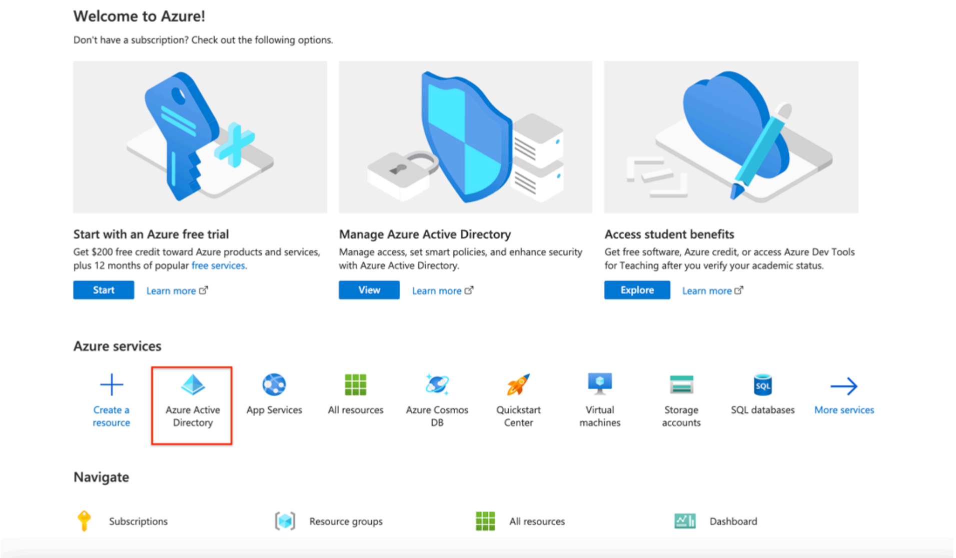
No certificates have been added for this application.

Client secrets

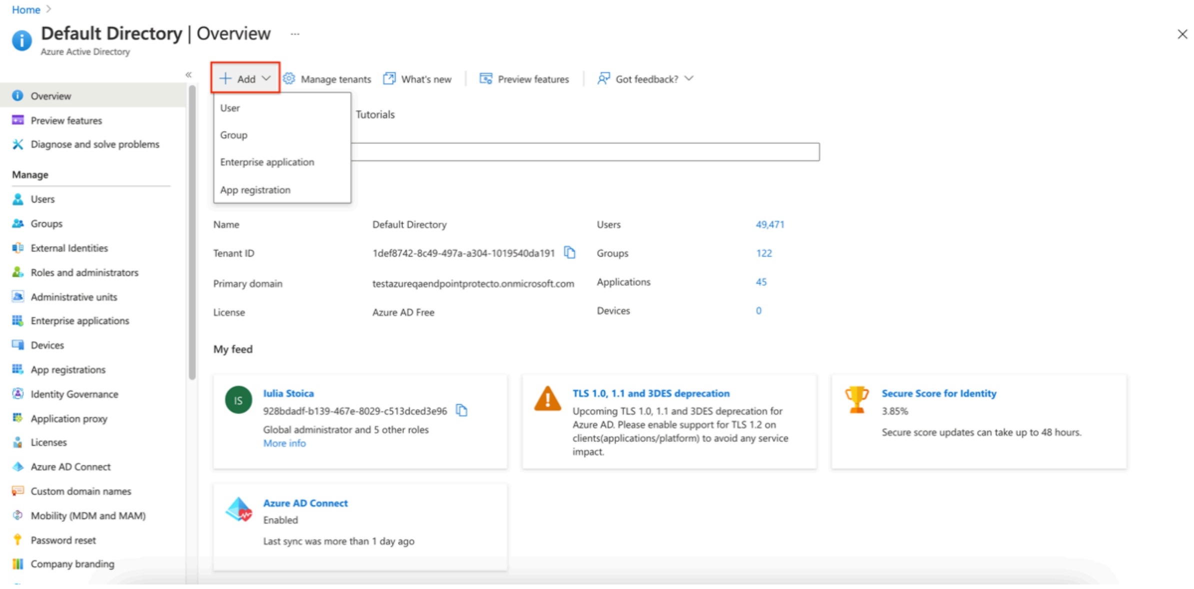
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value	Secret ID
Client Secret Description	1/22/2022	3yA******************	644ff38a-b82e-4873-9a6d-e9b43f5dffa0


Welcome to Azure!
Don't have a subscription? Check out the following options.
Start with an Azure free trial
Get $200 free credit toward Azure products and services, plus 12 months of popular free services.
Start
Learn more
Manage Azure Active Directory
Manage access, set smart policies, and enhance security with Azure Active Directory.
View
Learn more
Access student benefits
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.
Explore
Learn more
Azure services
Create a resource
Azure Active Directory
App Services
All resources
Azure Cosmos DB
Quickstart Center
Virtual machines
Storage accounts
SQL databases
More services
Navigate
Subscriptions
Resource groups
All resources
Dashboard

2. Click **Add** from the Default **Directory| Overview** page



Name	Default Directory	Users	49,471
Tenant ID	1def8742-8c49-497a-a304-1019540da191	Groups	122
Primary domain	testazureqaendpointprotecto.onmicrosoft.com	Applications	45
License	Azure AD Free	Devices	0

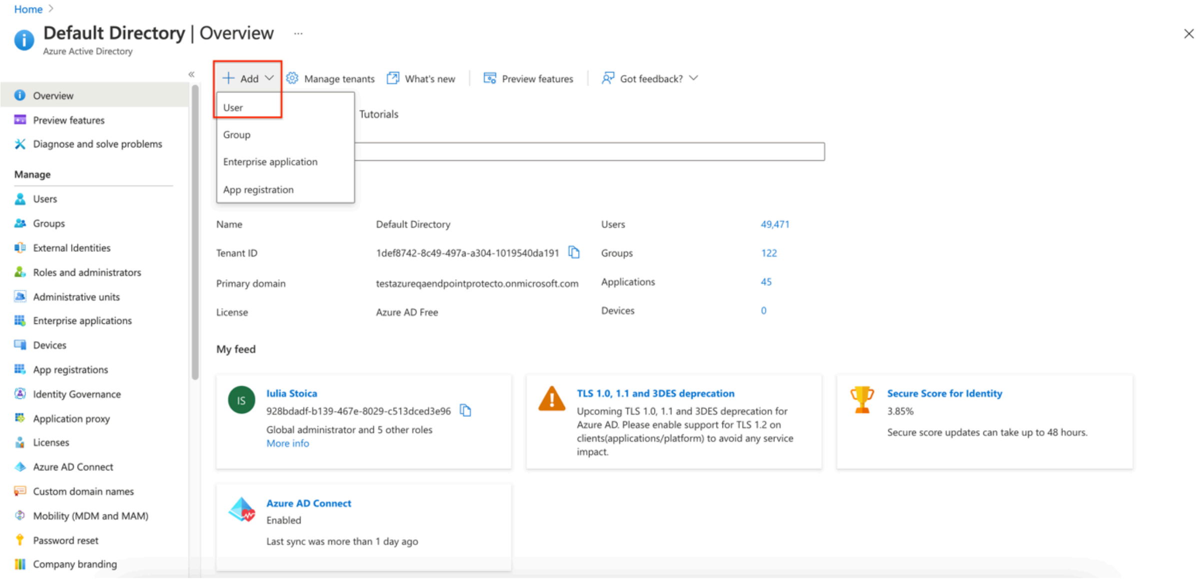
Iulia Stoica
928bdadf-b139-467e-8029-c513dced3e96
Global administrator and 5 other roles
More info

TLS 1.0, 1.1 and 3DES deprecation
Upcoming TLS 1.0, 1.1 and 3DES deprecation for Azure AD. Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

Secure Score for Identity
3.85%
Secure score updates can take up to 48 hours.

Azure AD Connect
Enabled
Last sync was more than 1 day ago

3. Click **Add User**.



Name	Default Directory	Users	49,471
Tenant ID	1def8742-8c49-497a-a304-1019540da191	Groups	122
Primary domain	testazureqaendpointprotecto.onmicrosoft.com	Applications	45
License	Azure AD Free	Devices	0

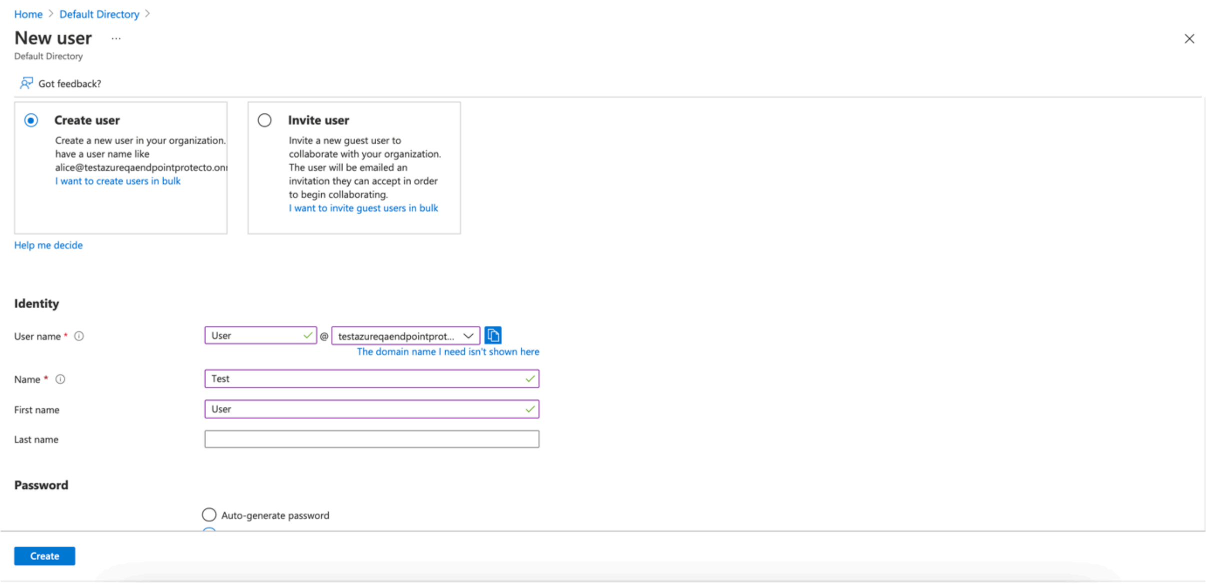
Iulia Stoica
928bdadf-b139-467e-8029-c513dced3e96
Global administrator and 5 other roles
More info

TLS 1.0, 1.1 and 3DES deprecation
Upcoming TLS 1.0, 1.1 and 3DES deprecation for Azure AD. Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

Secure Score for Identity
3.85%
Secure score updates can take up to 48 hours.

Azure AD Connect
Enabled
Last sync was more than 1 day ago

- 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**



Home > Default Directory >

New user ···

Default Directory

Got feedback?

● Create user

Create a new user in your organization. have a user name like alice@testazureqaendpointprotecto.onl

I want to create users in bulk

○ Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

I want to invite guest users in bulk

Help me decide

Identity

User name * : User @ testazureqaendpointprot...

The domain name I need isn't shown here

Name * : Test

First name: User

Last name:

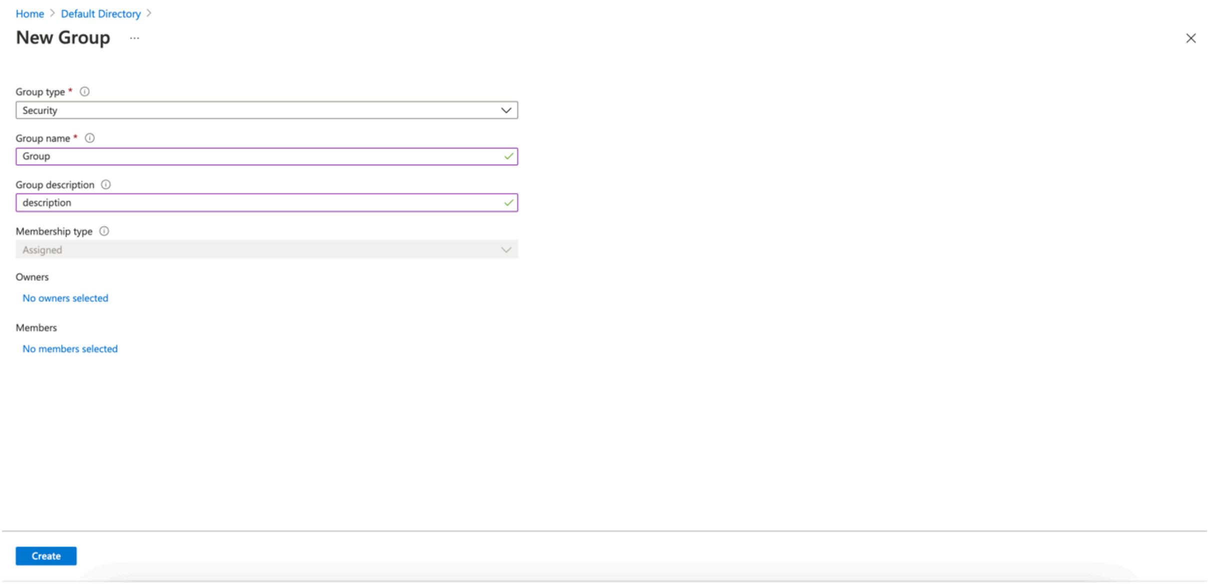
Password

○ Auto-generate password

Create

4. Repeat Steps 1 and 2, then click **Group**.

- Select **group type security**
- Enter a **name** for the group
- Click **No members selected** to add membership
- Search for the newly created user and click **Select**



Home > Default Directory >

New Group ···

Group type * : Security

Group name * : Group

Group description: description

Membership type: Assigned

Owners

No owners selected

Members

No members selected

Create

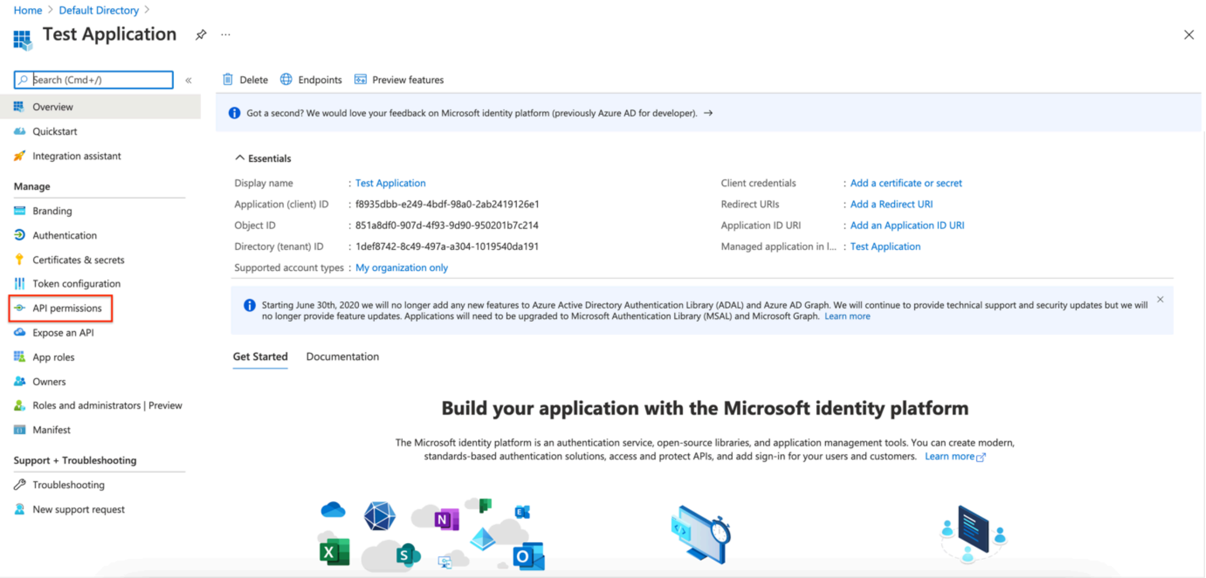
13.2.1.4. Add Permissions to the Application

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**.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

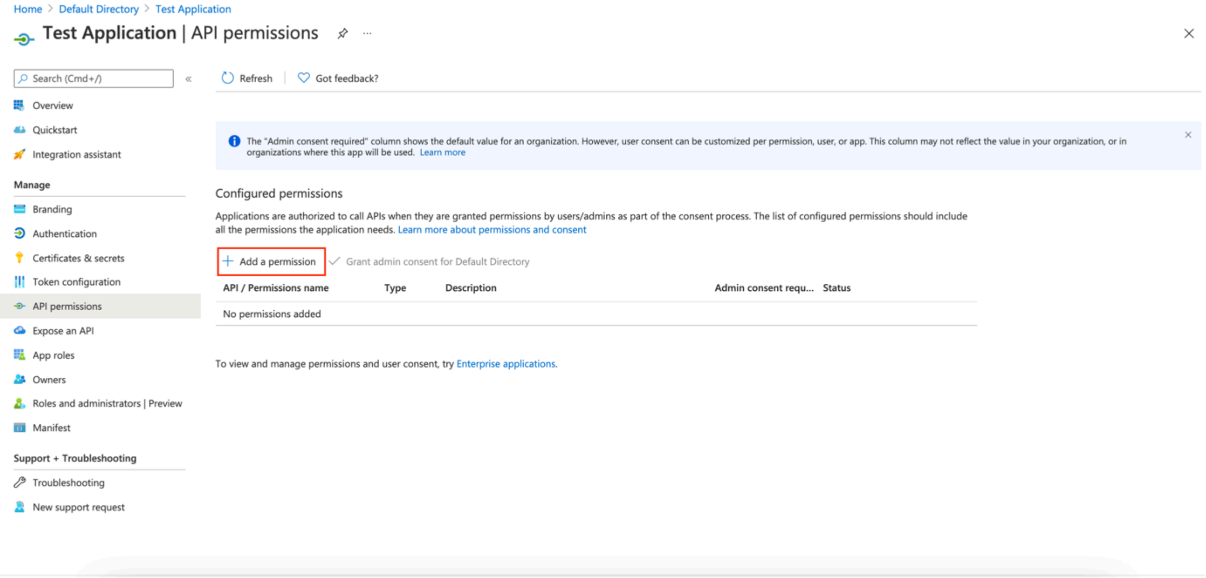
Display name : Test Application
Application (client) ID : f8935dbb-e249-4bdf-98a0-2ab2419126e1
Object ID : 851a8df0-907d-4f93-9d90-950201b7c214
Directory (tenant) ID : 1def8742-8c49-497a-a304-1019540da191
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : Test Application

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

2. Click **Add a Permission**



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

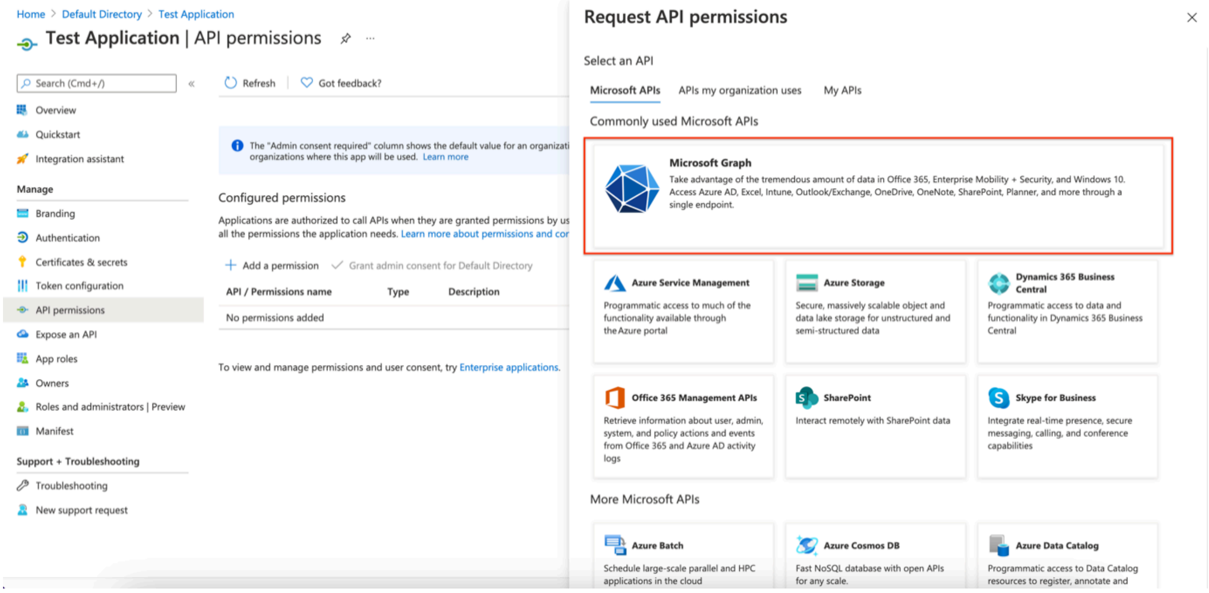
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

To view and manage permissions and user consent, try Enterprise applications.

3. Click **Microsoft Graph**.



The "Admin consent required" column shows the default value for an organizati organizations where this app will be used. Learn more

Applications are authorized to call APIs when they are granted permissions by us all the permissions the application needs. Learn more about permissions and cor

To view and manage permissions and user consent, try Enterprise applications.

Microsoft Graph: Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Service Management: Programmatic access to much of the functionality available through the Azure portal

Azure Storage: Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Dynamics 365 Business Central: Programmatic access to data and functionality in Dynamics 365 Business Central

Office 365 Management APIs: Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

SharePoint: Interact remotely with SharePoint data

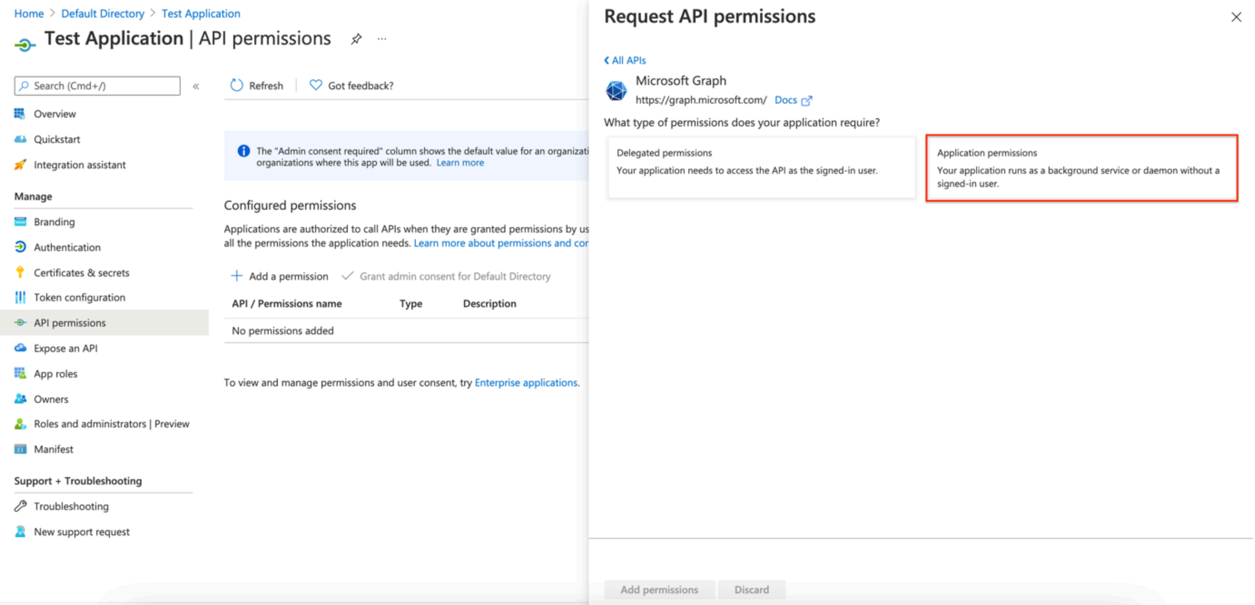
Skype for Business: Integrate real-time presence, secure messaging, calling, and conference capabilities

Azure Batch: Schedule large-scale parallel and HPC applications in the cloud

Azure Cosmos DB: Fast NoSQL database with open APIs for any scale.

Azure Data Catalog: Programmatic access to Data Catalog resources to register, annotate and

4. Click **Application Permissions**.



The "Admin consent required" column shows the default value for an organizati organizations where this app will be used. Learn more

Applications are authorized to call APIs when they are granted permissions by us all the permissions the application needs. Learn more about permissions and cor

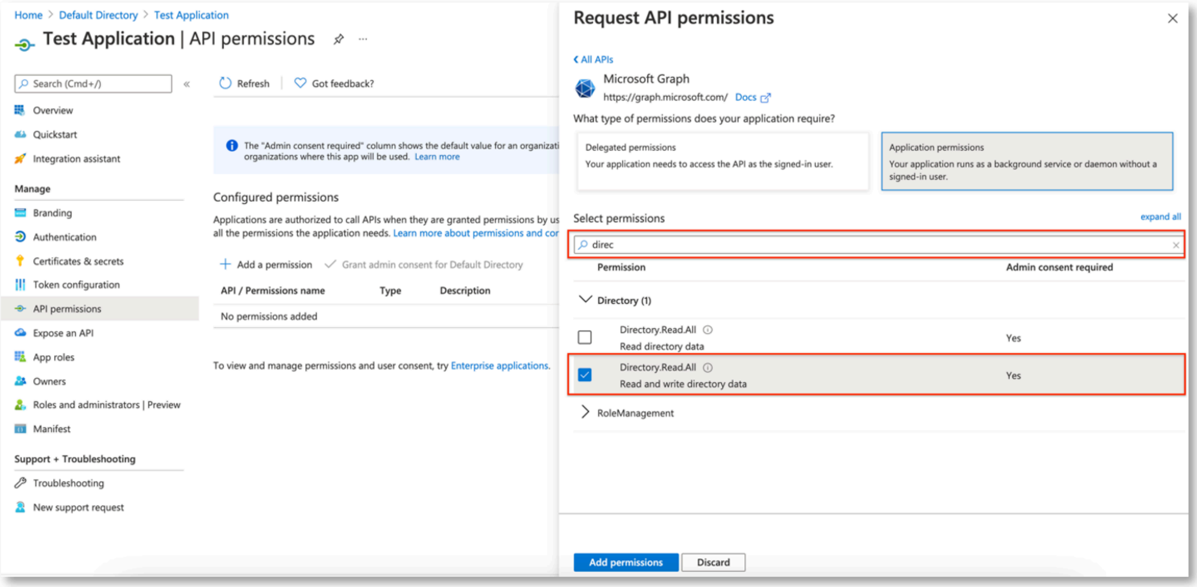
To view and manage permissions and user consent, try Enterprise applications.

What type of permissions does your application require?

Delegated permissions: Your application needs to access the API as the signed-in user.

Application permissions: Your application runs as a background service or daemon without a signed-in user.

5. Search for the permissions mentioned above and check each of the permissions. (Directory.Read.All, Group.Read.All, User.Read.All)



The "Admin consent required" column shows the default value for an organizati organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by us all the permissions the application needs. Learn more about permissions and cor

API / Permissions name	Type	Description
No permissions added		

To view and manage permissions and user consent, try Enterprise applications.

Request API permissions

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

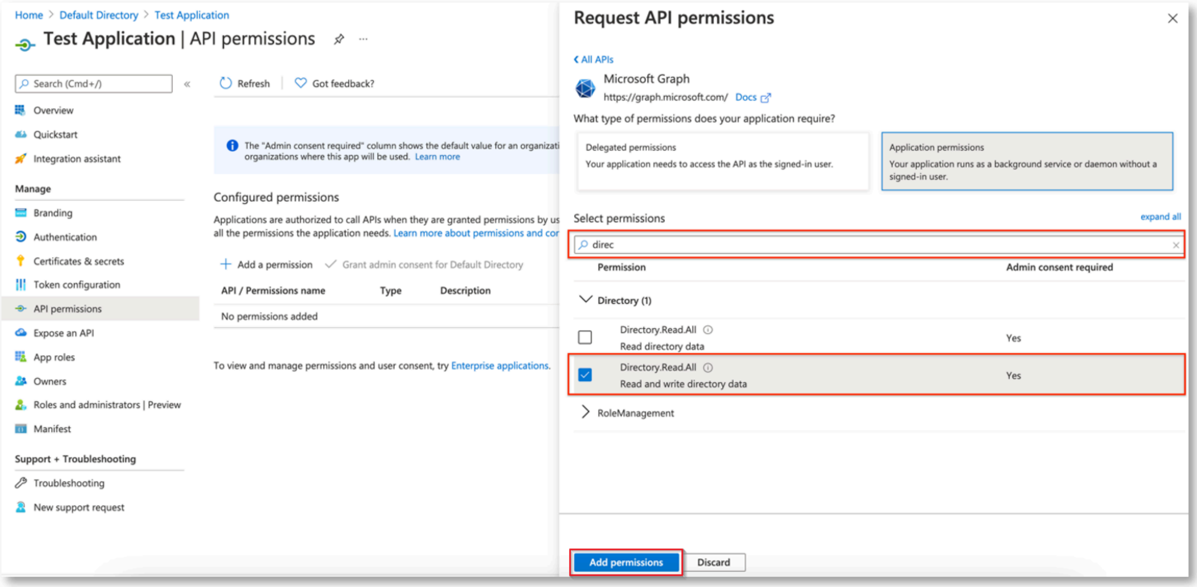
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

direc

Permission	Admin consent required
Directory (1)	
□ Directory.Read.All Read directory data	Yes
☑ Directory.Read.All Read and write directory data	Yes
RoleManagement	

6. Click **Add Permissions**.


Home > Default Directory > Test Application
Test Application | API permissions

The "Admin consent required" column shows the default value for an organizati organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by us all the permissions the application needs. Learn more about permissions and cor

API / Permissions name | Type | Description
No permissions added

To view and manage permissions and user consent, try Enterprise applications.

Request API permissions

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

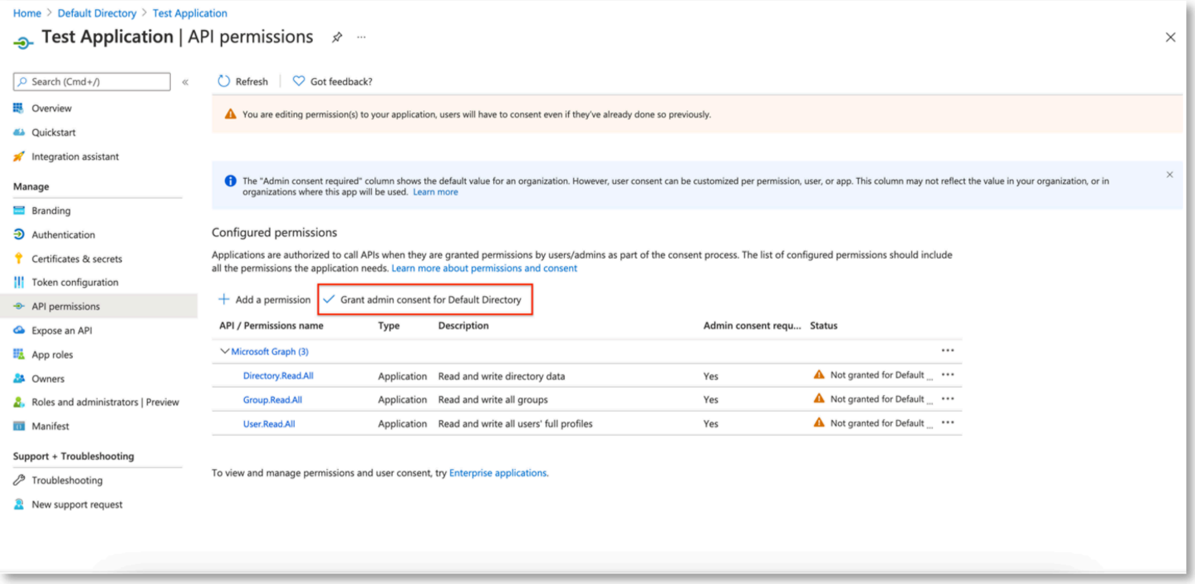
Select permissions

direc

Permission | Admin consent required
Directory (1)
□ Directory.Read.All Read directory data | Yes
☑ Directory.Read.All Read and write directory data | Yes
RoleManagement

Add permissions Discard

7. Click **Grant admin consent for Default Directory** from the **API Permission** page.



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

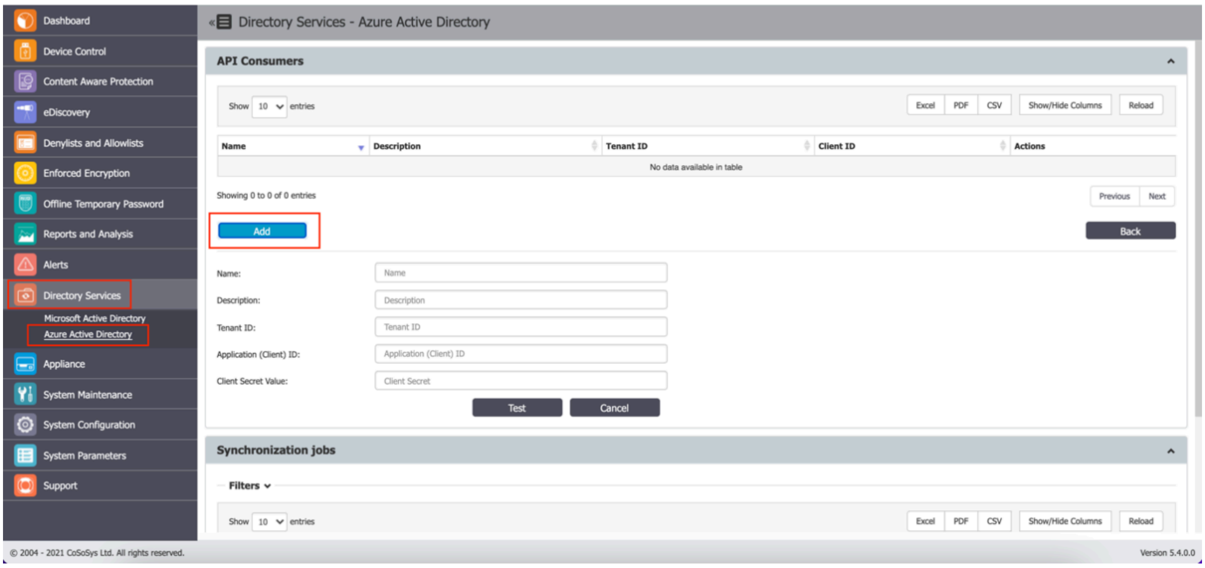
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Directory.Read.All	Application	Read and write directory data	Yes	Not granted for Default ...
Group.Read.All	Application	Read and write all groups	Yes	Not granted for Default ...
User.Read.All	Application	Read and write all users' full profiles	Yes	Not granted for Default ...

To view and manage permissions and user consent, try Enterprise applications.

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.



Name	Description	Tenant ID	Client ID	Actions
No data available in table				

Showing 0 to 0 of 0 entries

Name: Name

Description: Description

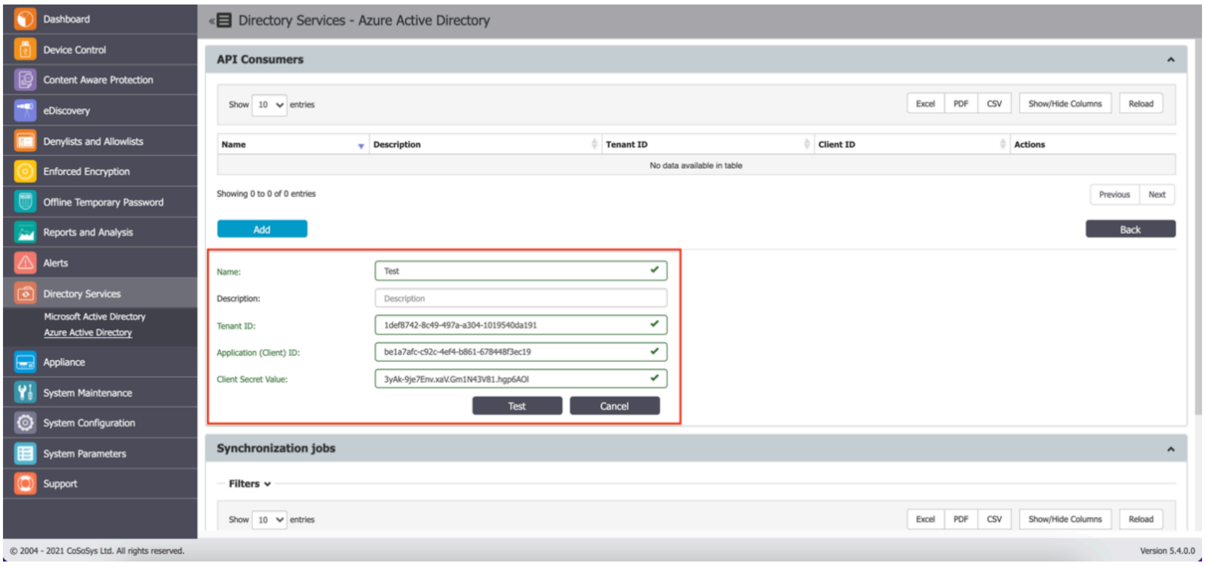
Tenant ID: Tenant ID

Application (Client) ID: Application (Client) ID

Client Secret Value: Client Secret

© 2004 - 2021 CoSoSys Ltd. All rights reserved. Version 5.4.0.0

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



Name	Description	Tenant ID	Client ID	Actions
No data available in table				

Showing 0 to 0 of 0 entries

Name: Test

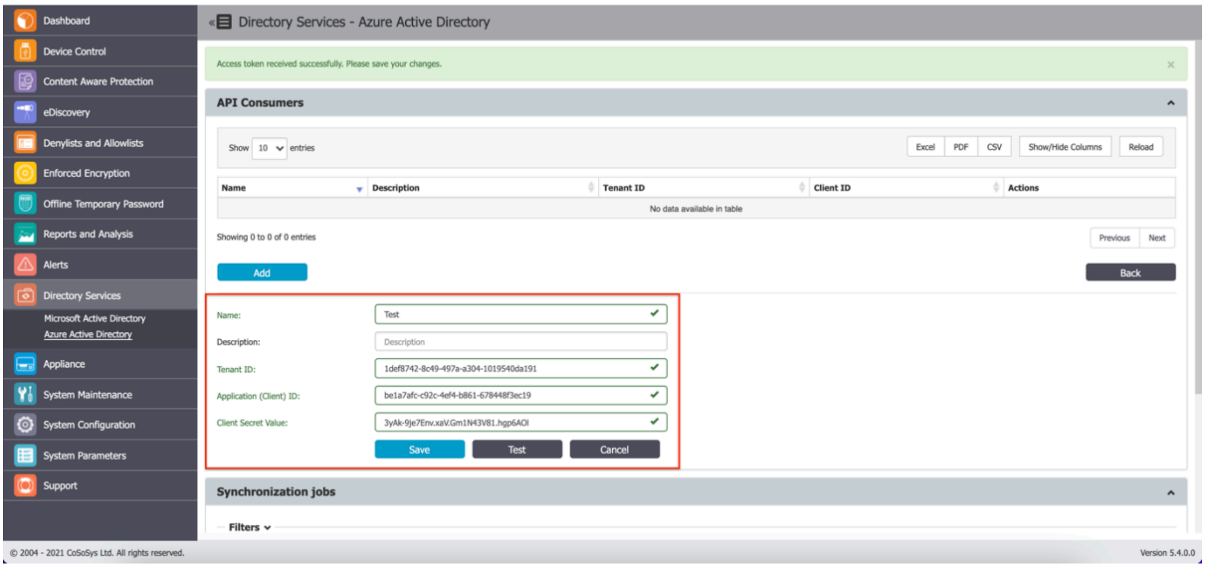
Description: Description

Tenant ID: 1def8742-8c49-497a-a304-1019540da191

Application (Client) ID: be1a7afc-c92c-4ef4-b861-678448f3ec19

Client Secret Value: 3yAk-9je7Env.xaV.Gm1N43V81.hgp6AOl

4. Click **Test** and then **Save**.



Access token received successfully. Please save your changes.

Name	Description	Tenant ID	Client ID	Actions
No data available in table				

Showing 0 to 0 of 0 entries

Name: Test

Description: Description

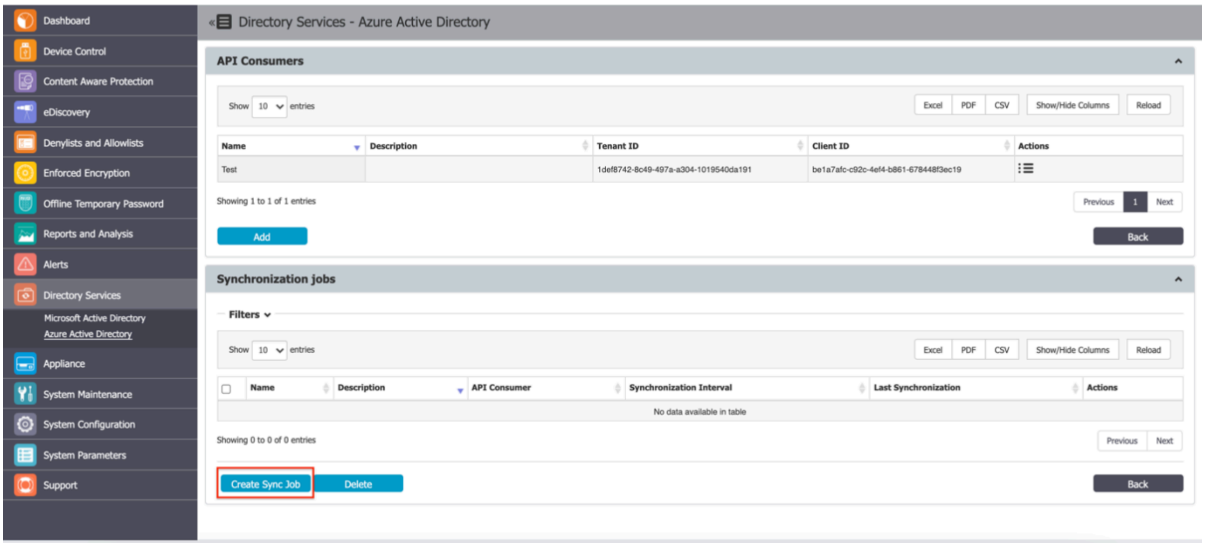
Tenant ID: 1def8742-8c49-497a-a304-1019540da191

Application (Client) ID: be1a7afc-c92c-4ef4-b861-678448f3ec19

Client Secret Value: 3yAk-9je7Env.xaV.Gm1N43V81.hgp6AOl

13.2.1.6. Create a Synchronization Job on the Endpoint Protector Server

1. Click **Create Sync Job**.



Directory Services - Azure Active Directory

API Consumers

Name	Description	Tenant ID	Client ID	Actions
Test		1def8742-8c49-497a-a304-1019540da191	be1a7afc-c92c-4ef4-b861-678448f3ec19	☰

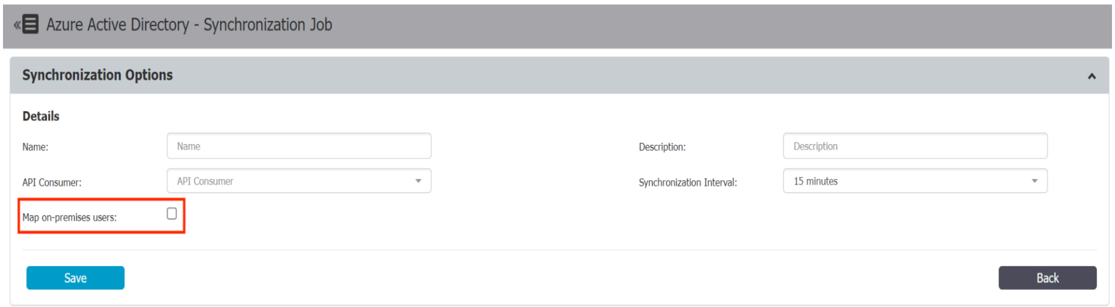
Showing 1 to 1 of 1 entries

Synchronization jobs

☐	Name	Description	API Consumer	Synchronization Interval	Last Synchronization	Actions
			No data available in table			

Showing 0 to 0 of 0 entries

2. Provide Synchronization information:
   - **Name**
   - **Description**
   - Select the created API Consumer
   - Select **Sync Interval**
   - Click **Save**



Azure Active Directory - Synchronization Job

Synchronization Options

Details

Name:	Name	Description:	Description
API Consumer:	API Consumer	Synchronization Interval:	15 minutes
Map on-premises users:	☐		

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:

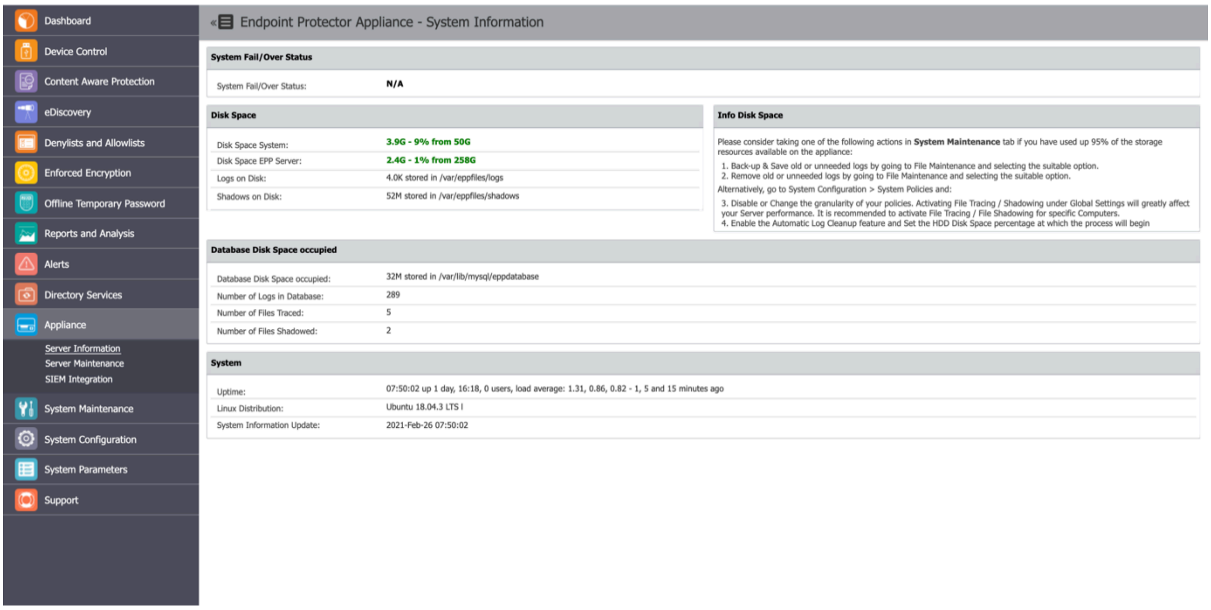
- **Unmarked** (feature disabled): EPP uses the "userPrincipalName" Azure AD attribute to retrieve user names. This attribute is the primary source for user identification and account mapping.
- **Marked** (feature enabled): EPP uses the "onPremisesSamAccountName" Azure AD attribute to retrieve user 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.



Endpoint Protector Appliance - System Information

System Fail/Over Status

System Fail/Over Status:	**N/A**

Disk Space

Disk Space System:	**3.9G - 9% from 50G**
Disk Space EPP Server:	**2.4G - 1% from 258G**
Logs on Disk:	4.0K stored in /var/eppfiles/logs
Shadows on Disk:	52M stored in /var/eppfiles/shadows

Info Disk Space

Please consider taking one of the following actions in **System Maintenance** tab if you have used up 95% of the storage resources available on the appliance:

1. Back-up & Save old or unneeded logs by going to File Maintenance and selecting the suitable option.
2. Remove old or unneeded logs by going to File Maintenance and selecting the suitable option.

Alternatively, go to System Configuration > System Policies and:

3. Disable or Change the granularity of your policies. Activating File Tracing / Shadowing under Global Settings will greatly affect your Server performance. It is recommended to activate File Tracing / File Shadowing for specific Computers.
4. Enable the Automatic Log Cleanup feature and Set the HDD Disk Space percentage at which the process will begin

Database Disk Space occupied

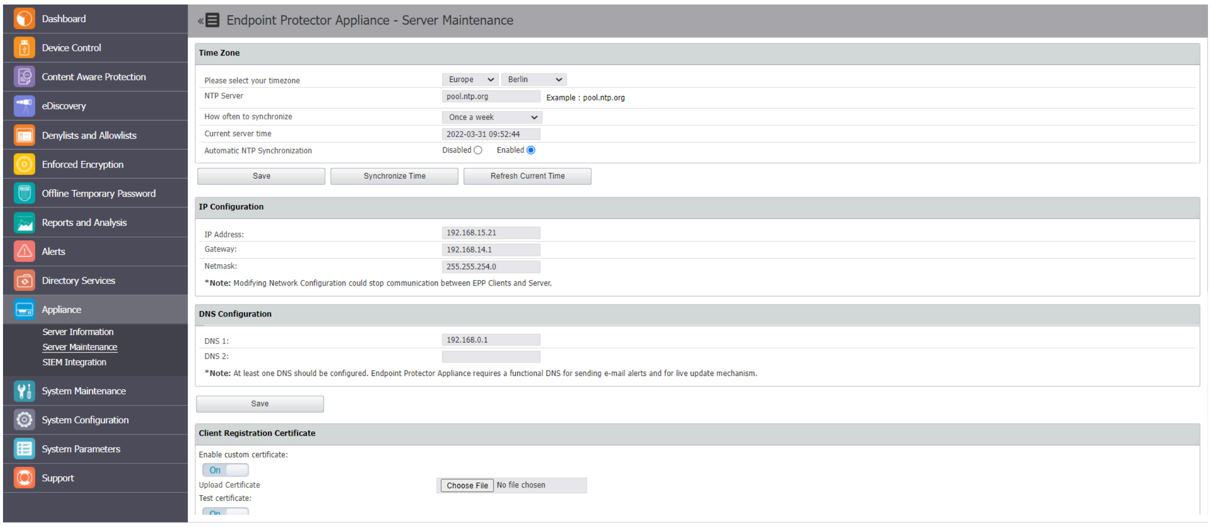
Database Disk Space occupied:	32M stored in /var/lib/mysql/eppdatabase
Number of Logs in Database:	289
Number of Files Traced:	5
Number of Files Shadowed:	2

System

Uptime:	07:50:02 up 1 day, 16:18, 0 users, load average: 1.31, 0.86, 0.82 - 1, 5 and 15 minutes ago
Linux Distribution:	Ubuntu 18.04.3 LTS l
System Information Update:	2021-Feb-26 07:50:02

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.



Endpoint Protector Appliance - Server Maintenance

Time Zone

Please select your timezone	Europe, Berlin
NTP Server	pool.ntp.org Example : pool.ntp.org
How often to synchronize	Once a week
Current server time	2022-03-31 09:52:44
Automatic NTP Synchronization	Disabled ○ Enabled ●

IP Configuration

IP Address:	192.168.15.21
Gateway:	192.168.14.1
Netmask:	255.255.254.0

***Note:** Modifying Network Configuration could stop communication between EPP Clients and Server.

DNS Configuration

DNS 1:	192.168.0.1
DNS 2:	

***Note:** At least one DNS should be configured. Endpoint Protector Appliance requires a functional DNS for sending e-mail alerts and for live update mechanism.

Client Registration Certificate

Enable custom certificate: On

Upload Certificate No file chosen

Test certificate:

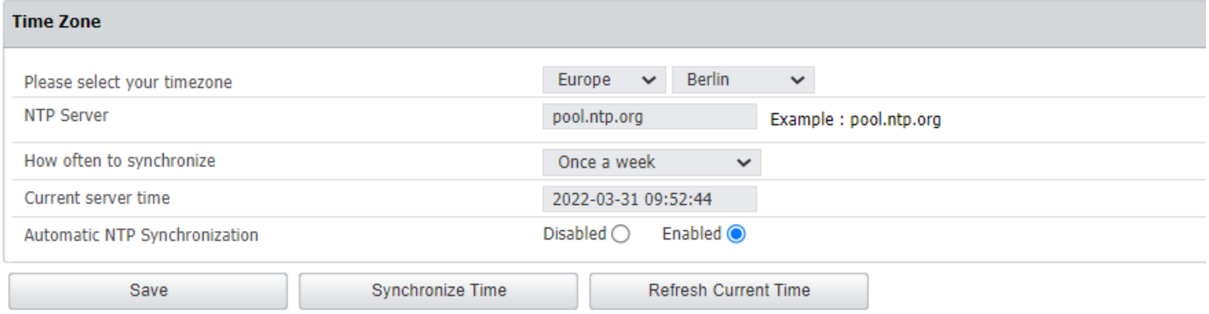
14.2.1. Time Zone

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.



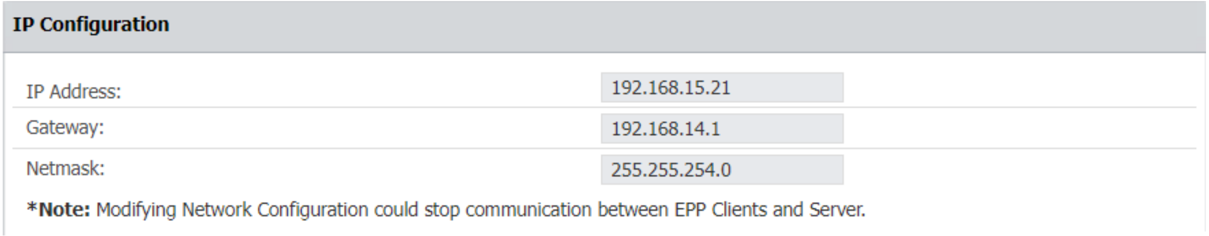
Time Zone

Please select your timezone	Europe, Berlin
NTP Server	pool.ntp.org Example : pool.ntp.org
How often to synchronize	Once a week
Current server time	2022-03-31 09:52:44
Automatic NTP Synchronization	Disabled ○ Enabled ●

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

IP Address: 192.168.15.21

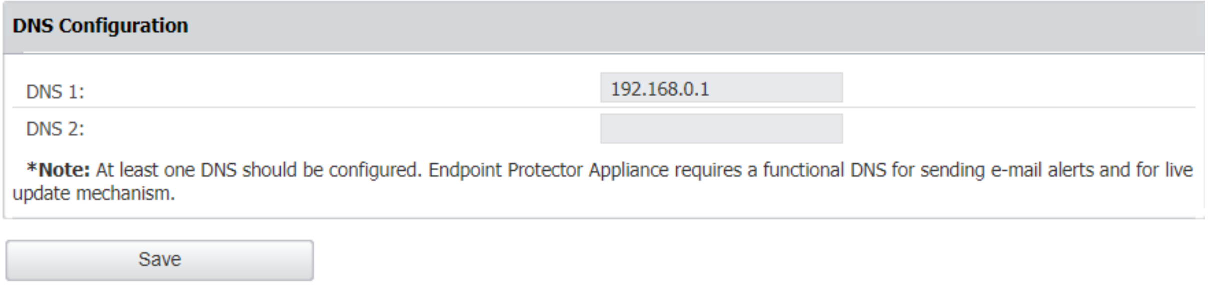
Gateway: 192.168.14.1

Netmask: 255.255.254.0

***Note:** Modifying Network Configuration could stop communication between EPP Clients and Server.

14.2.3. DNS Configuration

In this section you can modify or add a DNS server address and then **Save** your changes.



DNS Configuration

DNS 1: 192.168.0.1

DNS 2:

***Note:** At least one DNS should be configured. Endpoint Protector Appliance requires a functional DNS for sending e-mail alerts and for live update mechanism.

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:

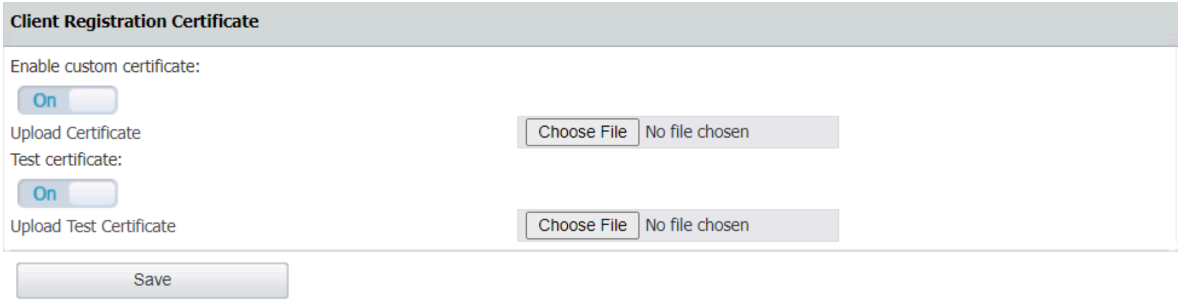
   - **Endpoint Protector Server** will not validate the client certificate at the registration phase
   - **Endpoint Protector Client** will not validate the server certificate

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.



Client Registration Certificate

Enable custom certificate: On

Upload Certificate: Choose File No file chosen

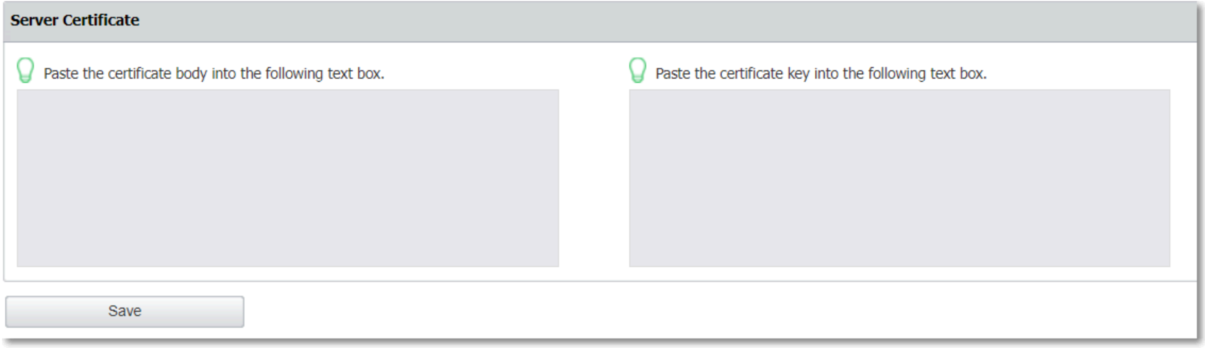
Test certificate: On

Upload Test Certificate: Choose File No file chosen

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.



Server Certificate

Paste the certificate body into the following text box.

Paste the certificate key into the following text box.

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.

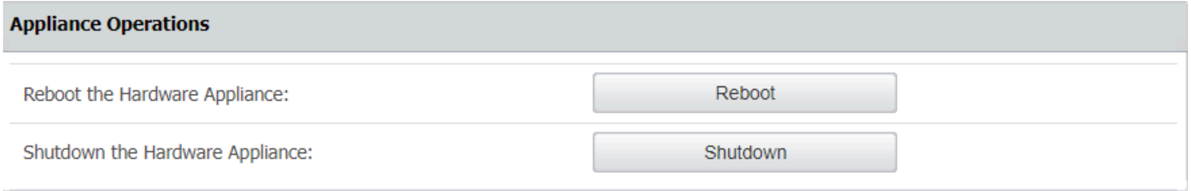
Note: All certificate validation statuses will be reported to the EPP Server and stored for debugging purposes in EPP Client logs.

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.



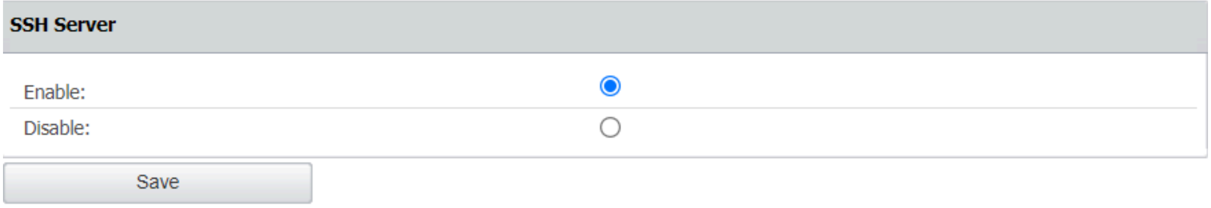
Appliance Operations

Reboot the Hardware Appliance:	Reboot
Shutdown the Hardware Appliance:	Shutdown

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.



SSH Server

Enable:	●
Disable:	○

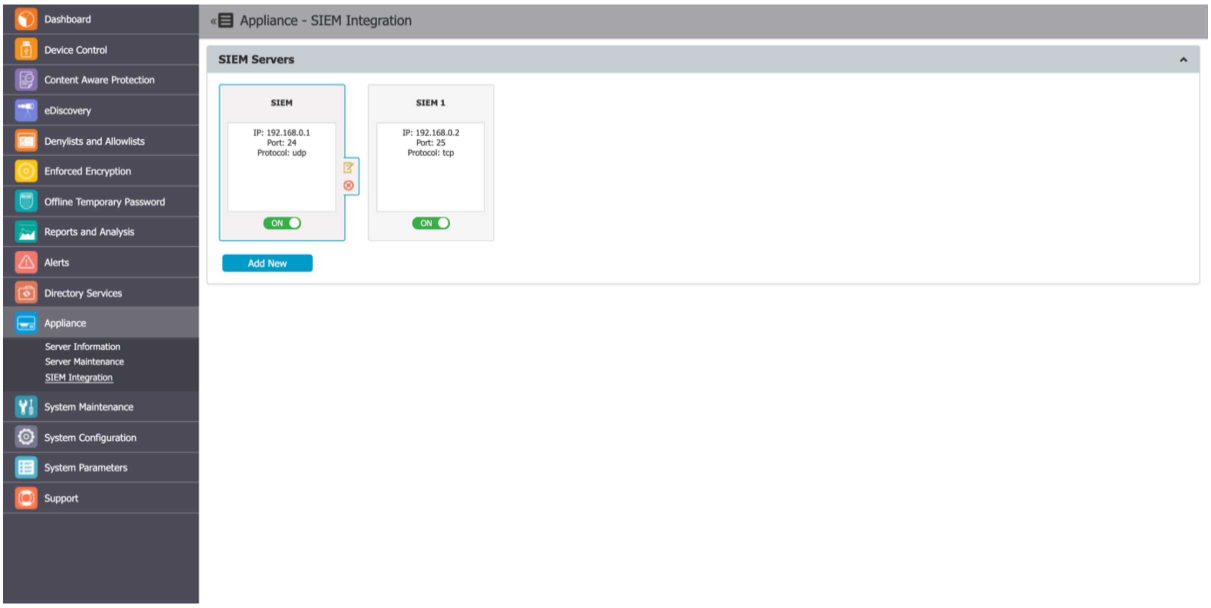
Save

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.



SIEM
IP: 192.168.0.1
Port: 24
Protocol: udp

SIEM 1
IP: 192.168.0.2
Port: 25
Protocol: tcp

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.

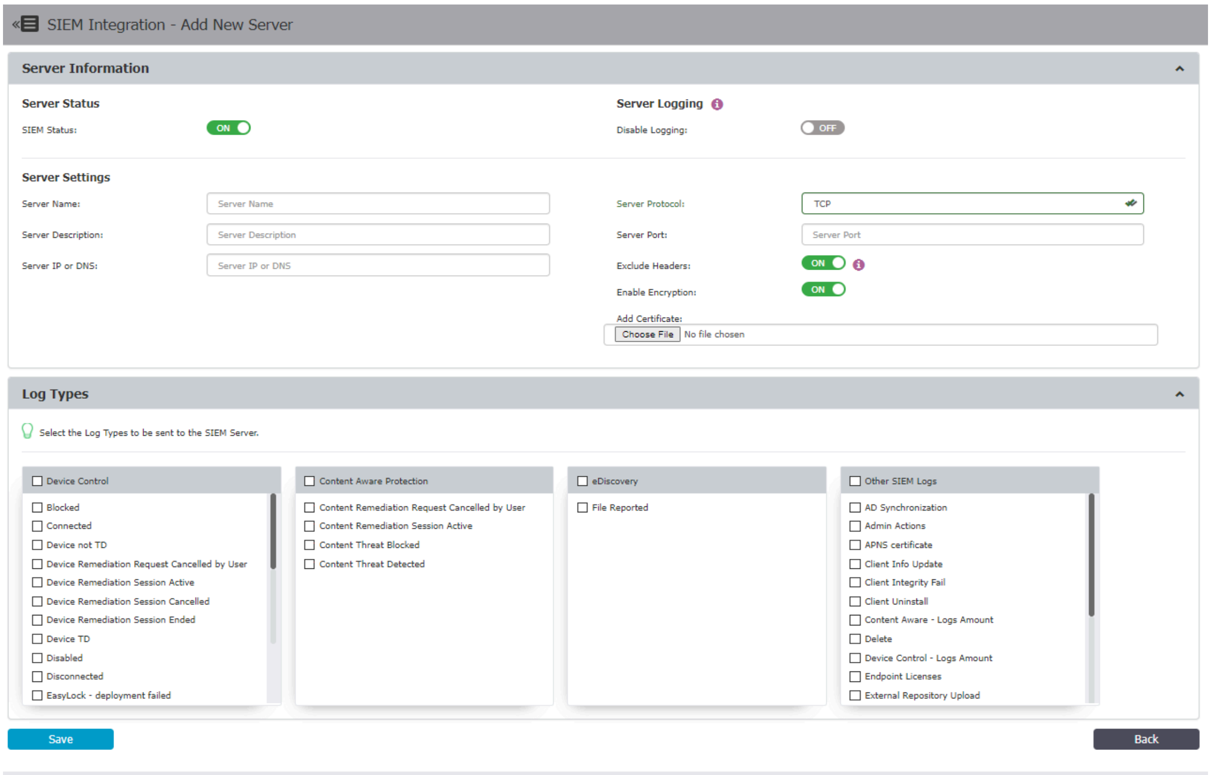
- **Server Name** – add a server name
- **Server Description** – add a description
- **Server IP or DNS** – add the IP or DNS
- **Server Protocol** – select the UDP or TCP server protocol

  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



SIEM Integration - Add New Server

Server Information

Server Status

SIEM Status: ON

Server Logging

Disable Logging: OFF

Server Settings

Server Name: Server Name

Server Description: Server Description

Server IP or DNS: Server IP or DNS

Server Protocol: TCP

Server Port: Server Port

Exclude Headers: ON

Enable Encryption: ON

Add Certificate: Choose File No file chosen

Log Types

Select the Log Types to be sent to the SIEM Server.

□ Device Control	□ Content Aware Protection	□ eDiscovery	□ Other SIEM Logs
□ Blocked	□ Content Remediation Request Cancelled by User	□ File Reported	□ AD Synchronization
□ Connected	□ Content Remediation Session Active		□ Admin Actions
□ Device not TD	□ Content Threat Blocked		□ APNS certificate
□ Device Remediation Request Cancelled by User	□ Content Threat Detected		□ Client Info Update
□ Device Remediation Session Active			□ Client Integrity Fail
□ Device Remediation Session Cancelled			□ Client Uninstall
□ Device Remediation Session Ended			□ Content Aware - Logs Amount
□ Device TD			□ Delete
□ Disabled			□ Device Control - Logs Amount
□ Disconnected			□ Endpoint Licenses
□ EasyLock - deployment failed			□ External Repository Upload

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.

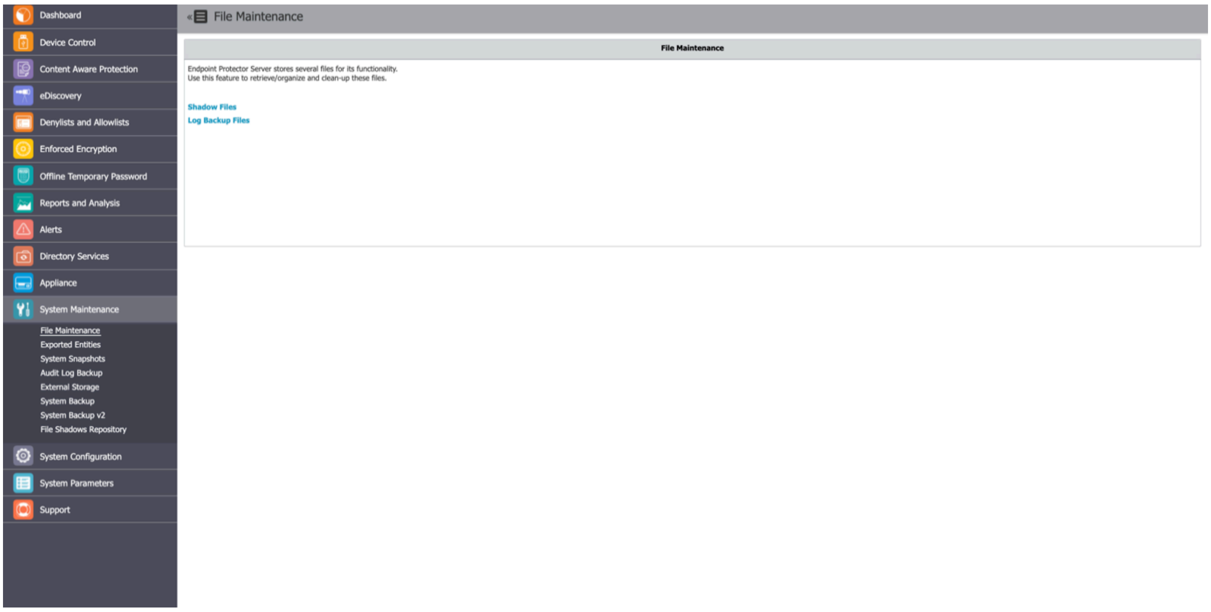
Make sure you update the certificate files when they expire.

Note: If you applied the latest patch using the **Live Update** option, and cannot view the SIEM encryption setting, please contact **Customer Support**.

15. System Maintenance

15.1. File Maintenance

This module allows you to retrieve, organize and clean-up files used by the Endpoint Protector Server.



Endpoint Protector Server stores several files for its functionality.
Use this feature to retrieve/organize and clean-up these files.

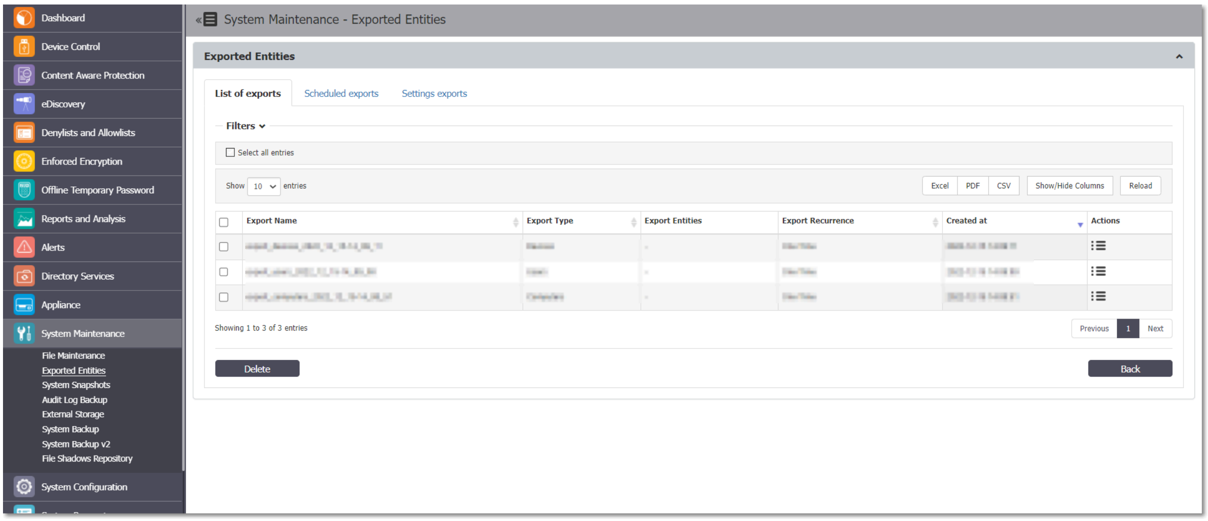
You have the following options:

- **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.



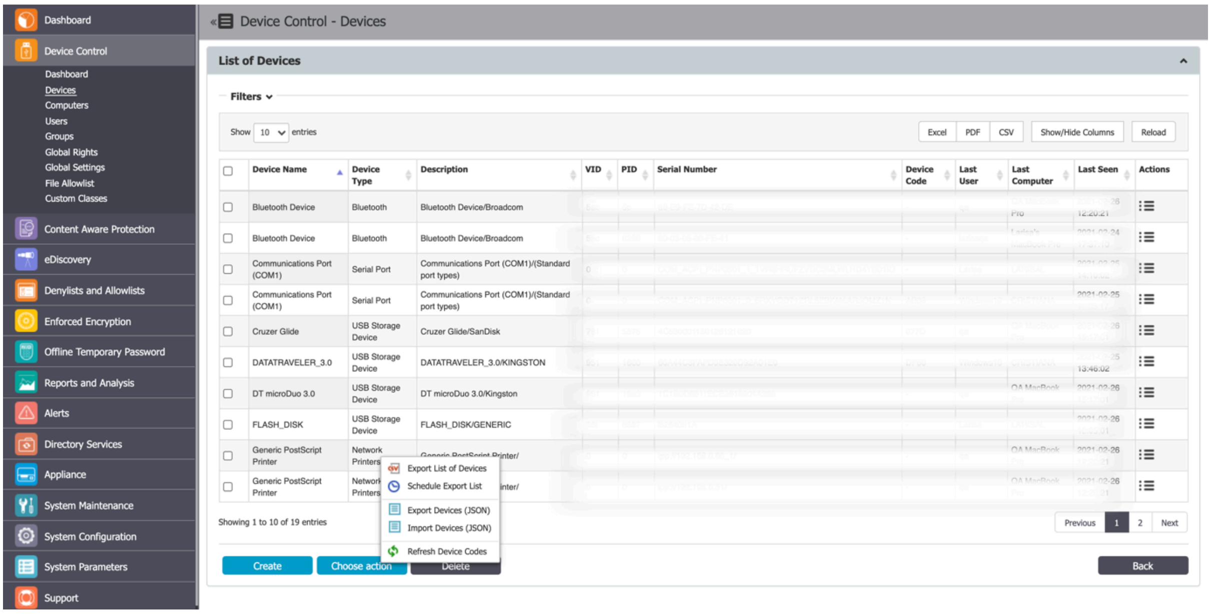
□ Select all entries

Show 10 entries

□	Export Name	Export Type	Export Entities	Export Recurrence	Created at	Actions
□			-			☰
□			-			☰
□			-			☰

Showing 1 to 3 of 3 entries

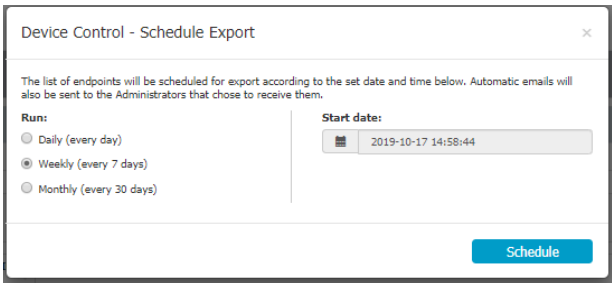
You can initiate the manual generation of the scheduled export from the Device Control, List of Devices / List of Computers / List of Users / List of Groups sections.



Show 10 entries

□	Device Name	Device Type	Description	VID	PID	Serial Number	Device Code	Last User	Last Computer	Last Seen	Actions
□	Bluetooth Device	Bluetooth	Bluetooth Device/Broadcom						Pro	12:20:21	☰
□	Bluetooth Device	Bluetooth	Bluetooth Device/Broadcom								☰
□	Communications Port (COM1)	Serial Port	Communications Port (COM1)/(Standard port types)								☰
□	Communications Port (COM1)	Serial Port	Communications Port (COM1)/(Standard port types)							2021-02-25	☰
□	Cruzer Glide	USB Storage Device	Cruzer Glide/SanDisk								☰
□	DATATRAVELER_3.0	USB Storage Device	DATATRAVELER_3.0/KINGSTON							13:46:02	☰
□	DT microDuo 3.0	USB Storage Device	DT microDuo 3.0/Kingston						QA MacBook	2021-02-26	☰
□	FLASH_DISK	USB Storage Device	FLASH_DISK/GENERIC							2021-02-26	☰
□	Generic PostScript Printer	Network Printers	Generic PostScript Printer/						QA MacBook	2021-02-26	☰
□	Generic PostScript Printer	Network Printers	inter/						QA MacBook	2021-02-26	☰

Showing 1 to 10 of 19 entries



The list of endpoints will be scheduled for export according to the set date and time below. Automatic emails will also be sent to the Administrators that chose to receive them.

Run:

○ Daily (every day)

● Weekly (every 7 days)

○ Monthly (every 30 days)

Start date: 2019-10-17 14:58:44

The scheduled exports can be sent automatically via e-mail to all the Administrators that have the **Scheduled Export Aler**t setting enabled.

The Scheduled Exports are reoccurring (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.

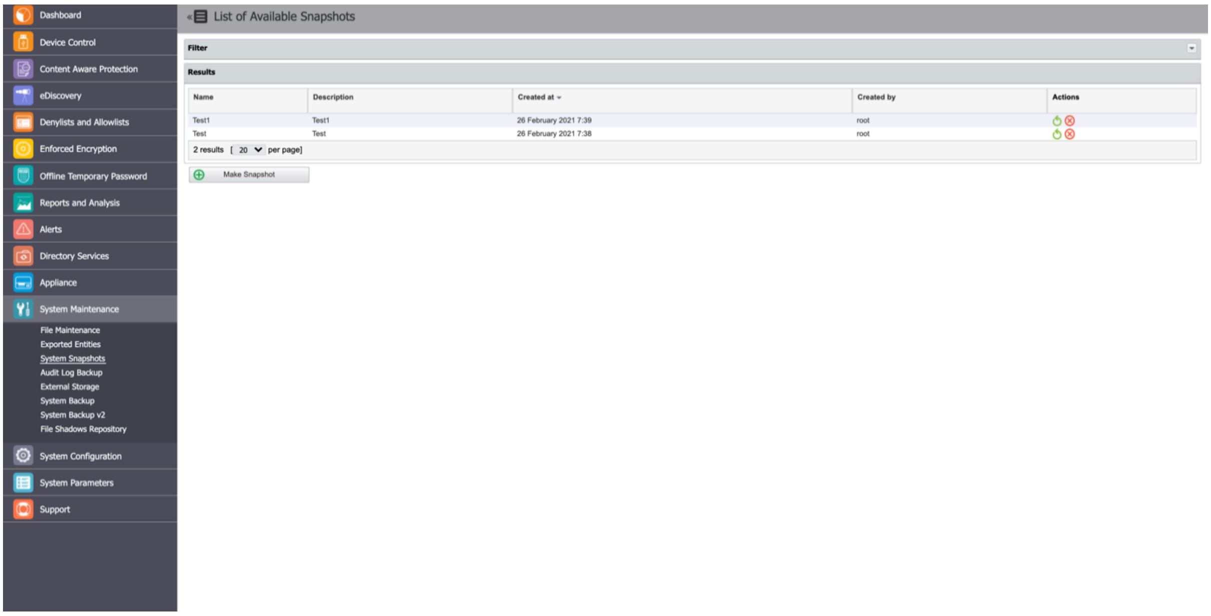
For performance reasons, the Scheduled Exports and Disable Logging option allows you to also keep the logs on the Endpoint Protector Server or only have them in the SIEM Server.

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**.



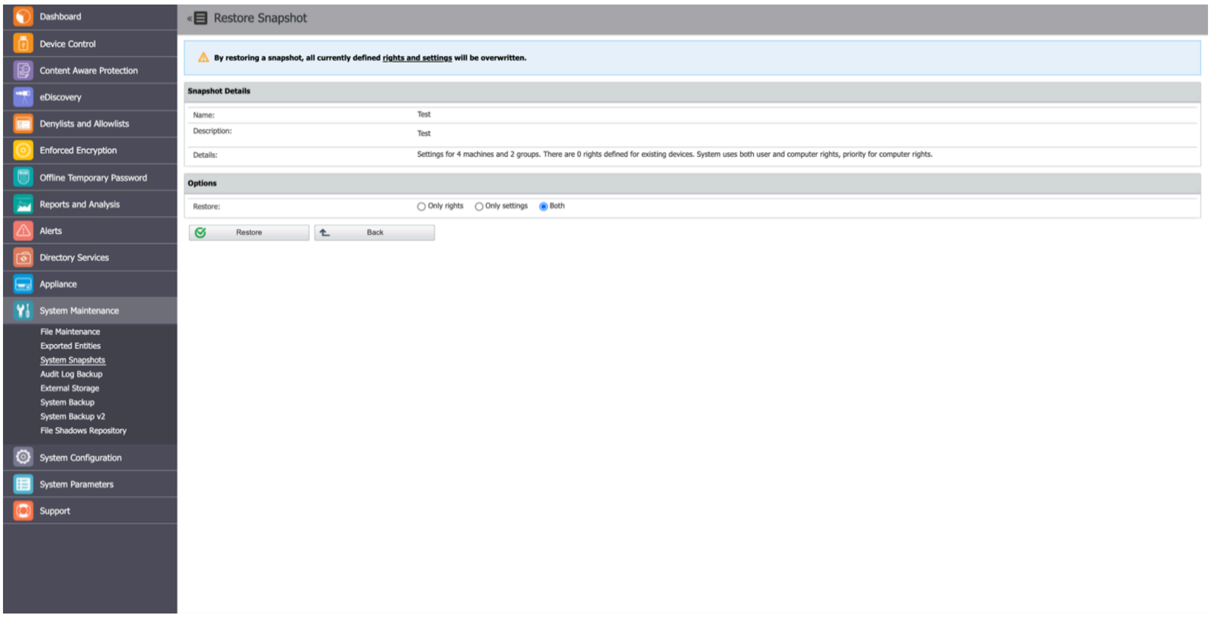
Name	Description	Created at	Created by	Actions
Test1	Test1	26 February 2021 7:39	root	
Test	Test	26 February 2021 7:38	root	

2 results [20 per page]

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.



Restore Snapshot

By restoring a snapshot, all currently defined rights and settings will be overwritten.

Snapshot Details

Name:	Test
Description:	Test
Details:	Settings for 4 machines and 2 groups. There are 0 rights defined for existing devices. System uses both user and computer rights, priority for computer rights.

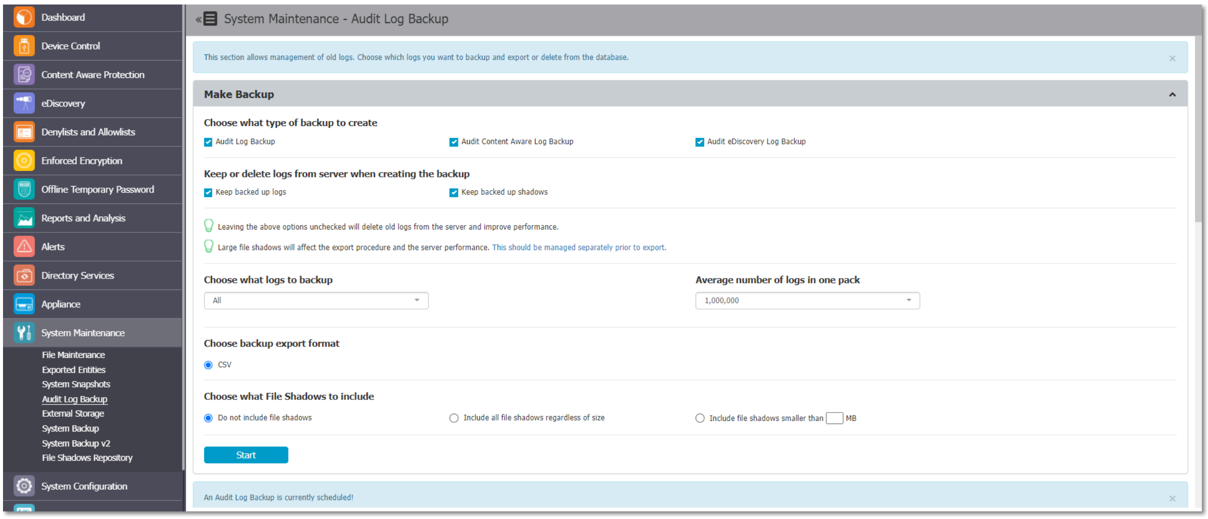
Options

Restore: ○ Only rights ○ Only settings ● Both

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.



System Maintenance - Audit Log Backup

This section allows management of old logs. Choose which logs you want to backup and export or delete from the database.

Make Backup

Choose what type of backup to create

☑ Audit Log Backup ☑ Audit Content Aware Log Backup ☑ Audit eDiscovery Log Backup

Keep or delete logs from server when creating the backup

☑ Keep backed up logs ☑ Keep backed up shadows

Leaving the above options unchecked will delete old logs from the server and improve performance.

Large file shadows will affect the export procedure and the server performance. This should be managed separately prior to export.

Choose what logs to backup: All

Average number of logs in one pack: 1,000,000

Choose backup export format

● CSV

Choose what File Shadows to include

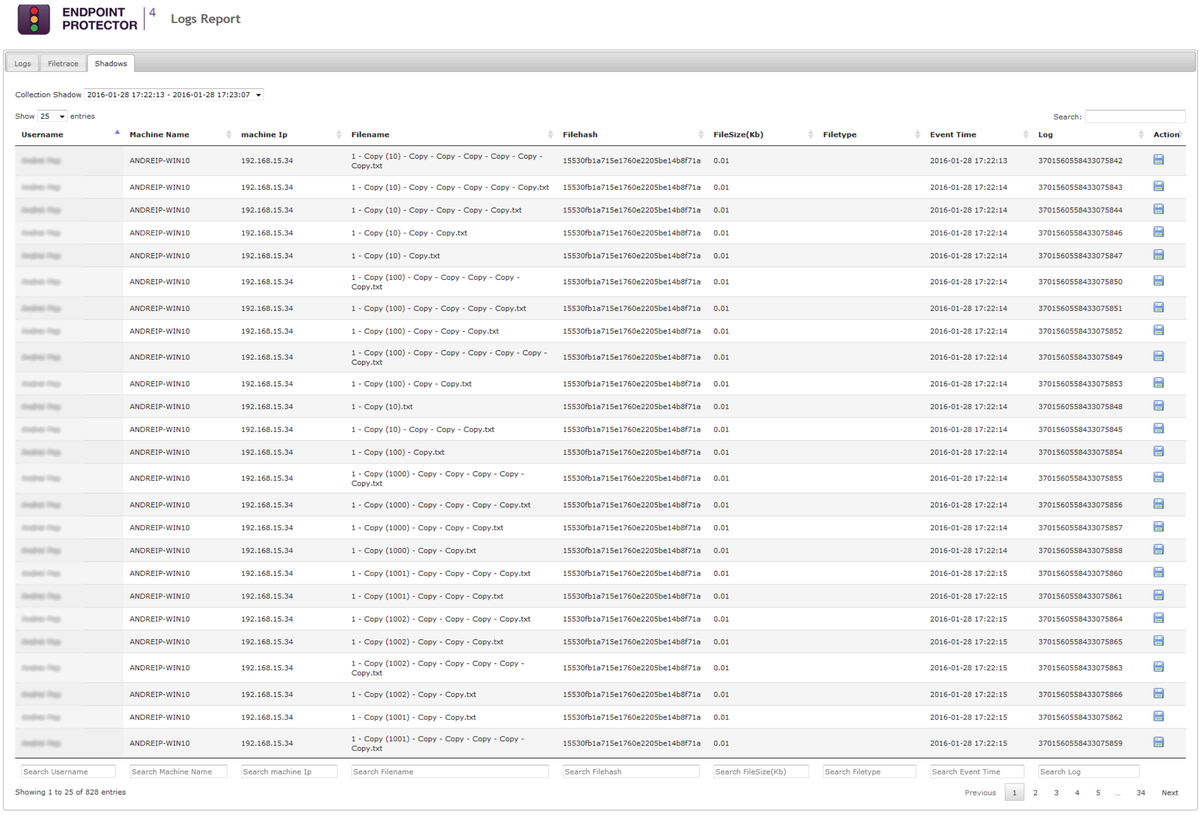
● Do not include file shadows ○ Include all file shadows regardless of size ○ Include file shadows smaller than ☐ MB

An Audit Log Backup is currently scheduled!

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



Collection Shadow 2016-01-28 17:22:13 - 2016-01-28 17:23:07

Show 25 entries

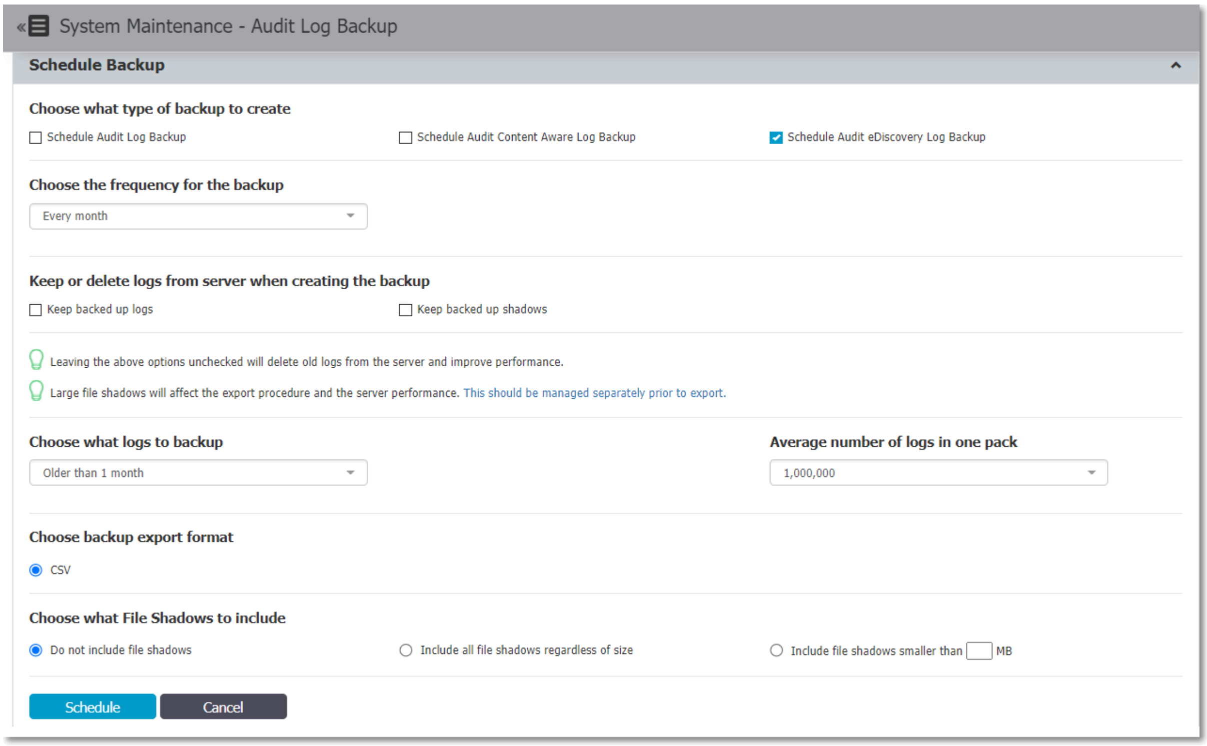
Search:

Username	Machine Name	machine Ip	Filename	Filehash	FileSize(Kb)	Filetype	Event Time	Log	Action
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:13	3701560558433075842	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075843	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075844	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075846	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075847	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075850	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075851	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075852	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075849	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075853	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10).txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075848	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075845	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075854	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075855	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075856	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075857	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075858	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075860	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075861	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075864	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075865	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075863	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075866	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075862	💾
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075859	💾
Search Username	Search Machine Name	Search machine Ip	Search Filename	Search Filehash	Search FileSize(Kb)	Search Filetype	Search Event Time	Search Log	

Showing 1 to 25 of 828 entries

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.).



System Maintenance - Audit Log Backup

Schedule Backup

Choose what type of backup to create

□ Schedule Audit Log Backup □ Schedule Audit Content Aware Log Backup ☑ Schedule Audit eDiscovery Log Backup

Choose the frequency for the backup

Every month

Keep or delete logs from server when creating the backup

□ Keep backed up logs □ Keep backed up shadows

Leaving the above options unchecked will delete old logs from the server and improve performance.

Large file shadows will affect the export procedure and the server performance. This should be managed separately prior to export.

Choose what logs to backup: Older than 1 month

Average number of logs in one pack: 1,000,000

Choose backup export format

● CSV

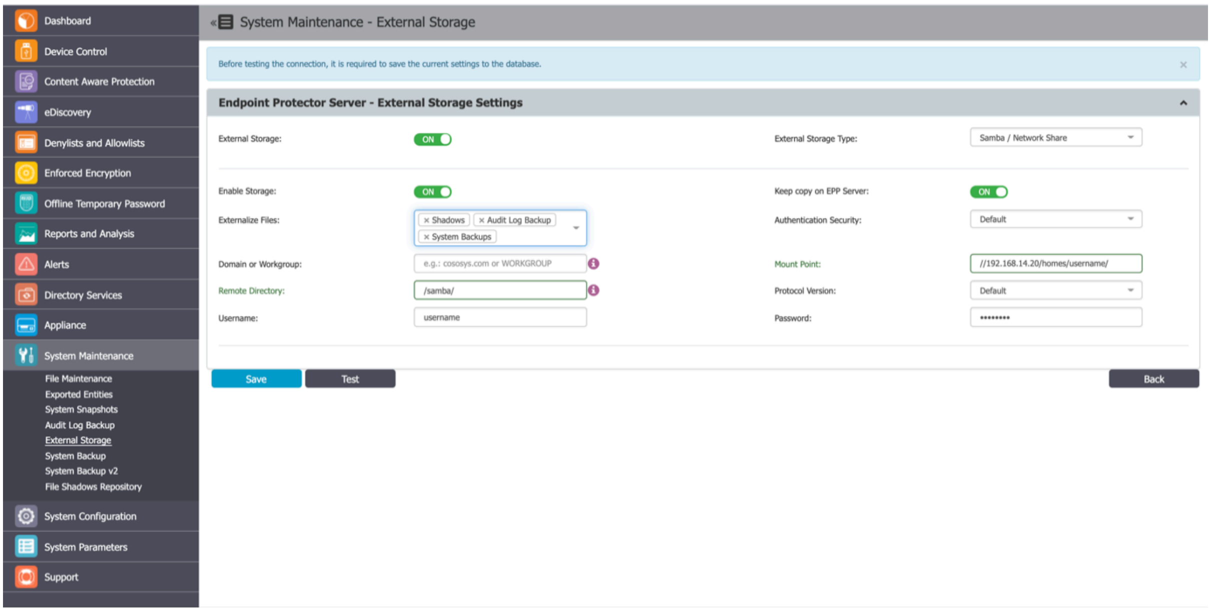
Choose what File Shadows to include

● Do not include file shadows ○ Include all file shadows regardless of size ○ Include file shadows smaller than ___ MB

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.



System Maintenance - External Storage

Before testing the connection, it is required to save the current settings to the database.

Endpoint Protector Server - External Storage Settings

External Storage: ON

External Storage Type: Samba / Network Share

Enable Storage: ON

Keep copy on EPP Server: ON

Externalize Files: × Shadows × Audit Log Backup × System Backups

Authentication Security: Default

Domain or Workgroup: e.g.: cososys.com or WORKGROUP

Mount Point: //192.168.14.20/homes/username/

Remote Directory: /samba/

Protocol Version: Default

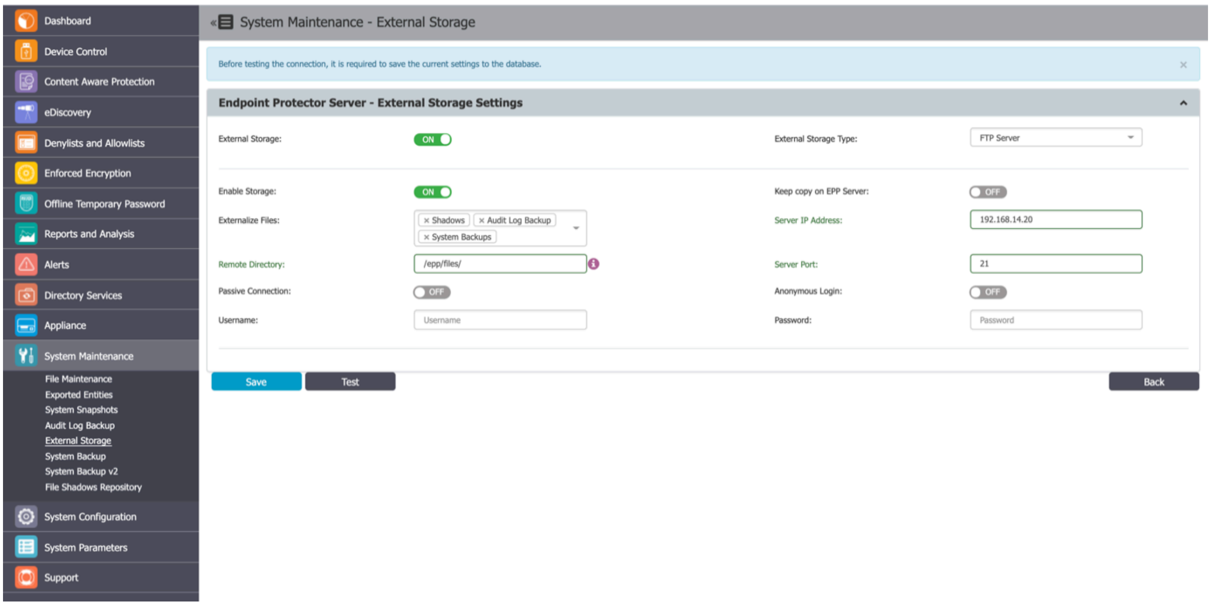
Username: username

Password: ••••••••

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**



System Maintenance - External Storage

Before testing the connection, it is required to save the current settings to the database.

Endpoint Protector Server - External Storage Settings

External Storage: ON

External Storage Type: FTP Server

Enable Storage: ON

Keep copy on EPP Server: OFF

Externalize Files: × Shadows × Audit Log Backup × System Backups

Server IP Address: 192.168.14.20

Remote Directory: /epp/files/

Server Port: 21

Passive Connection: OFF

Anonymous Login: OFF

Username: Username

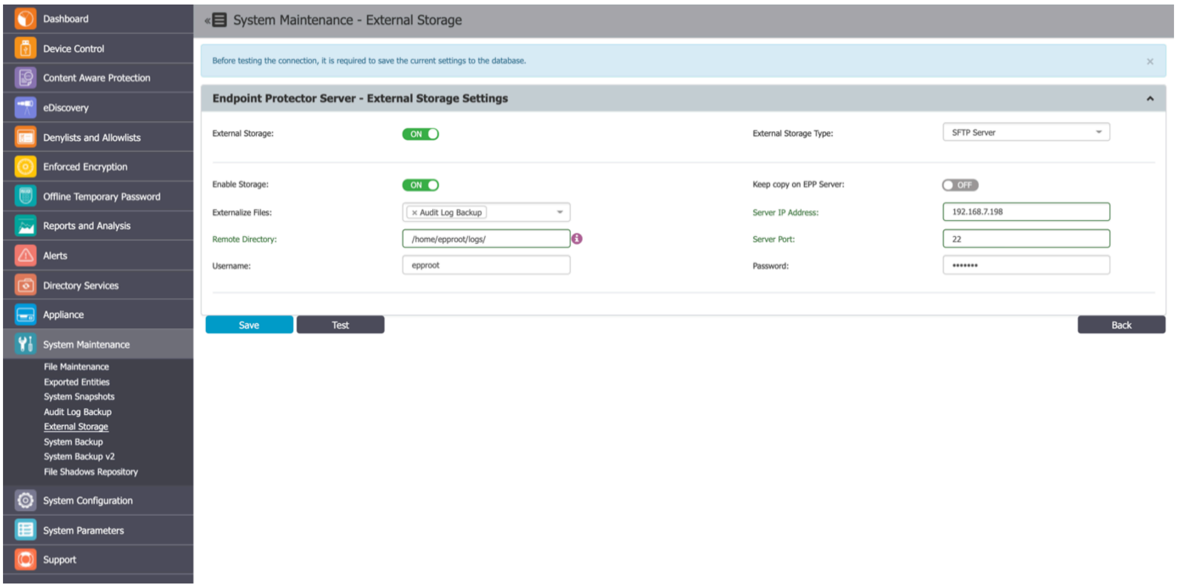
Password: Password

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

- **Enable storage**



System Maintenance - External Storage

Before testing the connection, it is required to save the current settings to the database.

Endpoint Protector Server - External Storage Settings

External Storage: ON

External Storage Type: SFTP Server

Enable Storage: ON

Keep copy on EPP Server: OFF

Externalize Files: × Audit Log Backup

Server IP Address: 192.168.7.198

Remote Directory: /home/epproot/logs/

Server Port: 22

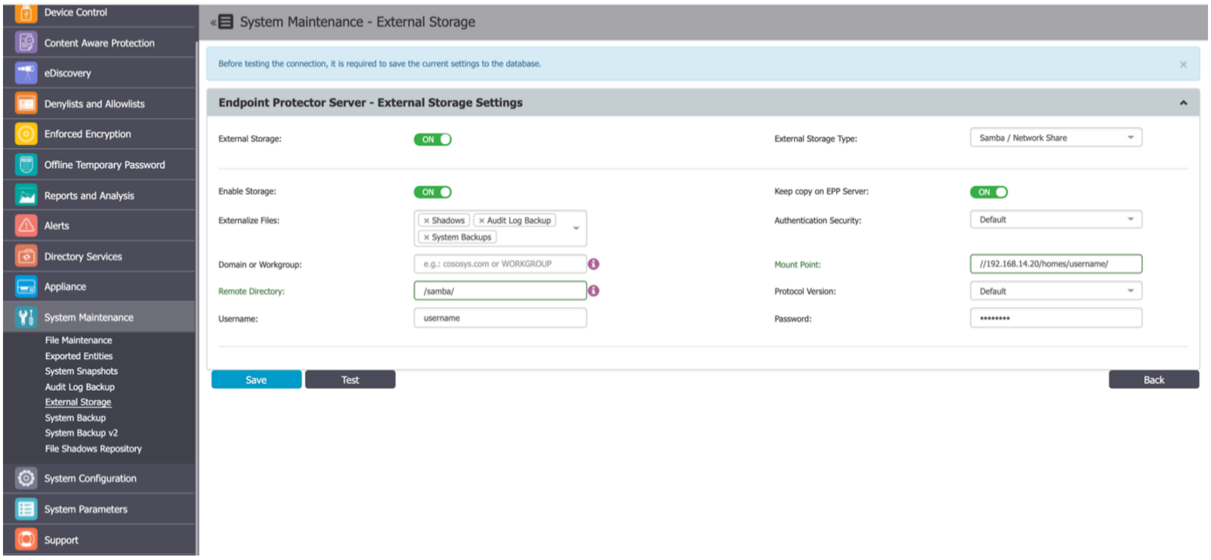
Username: epproot

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



System Maintenance - External Storage

Before testing the connection, it is required to save the current settings to the database.

Endpoint Protector Server - External Storage Settings

External Storage: ON

External Storage Type: Samba / Network Share

Enable Storage: ON

Keep copy on EPP Server: ON

Externalize Files: × Shadows × Audit Log Backup × System Backups

Authentication Security: Default

Domain or Workgroup: e.g.: cososys.com or WORKGROUP

Mount Point: //192.168.14.20/homes/username/

Remote Directory: /samba/

Protocol Version: Default

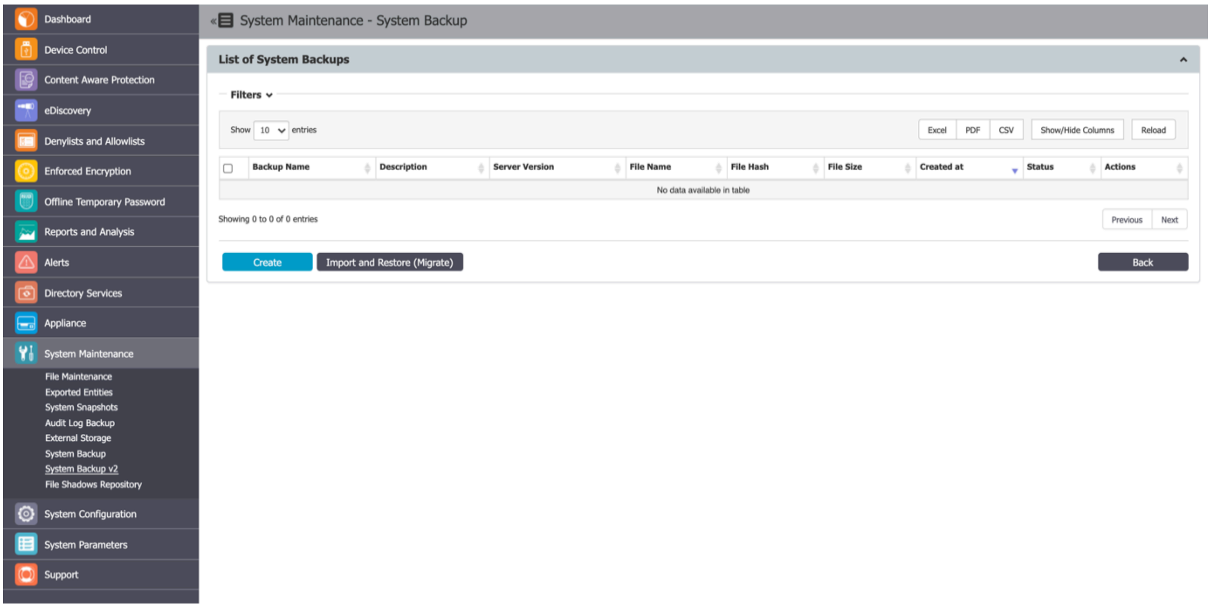
Username: username

Password: ••••••••

15.6.System Backup

15.6.1. From the Web Interface

This module allows you to make complete system backups.



System Maintenance - System Backup

List of System Backups

☐	Backup Name	Description	Server Version	File Name	File Hash	File Size	Created at	Status	Actions
					No data available in table				

Showing 0 to 0 of 0 entries

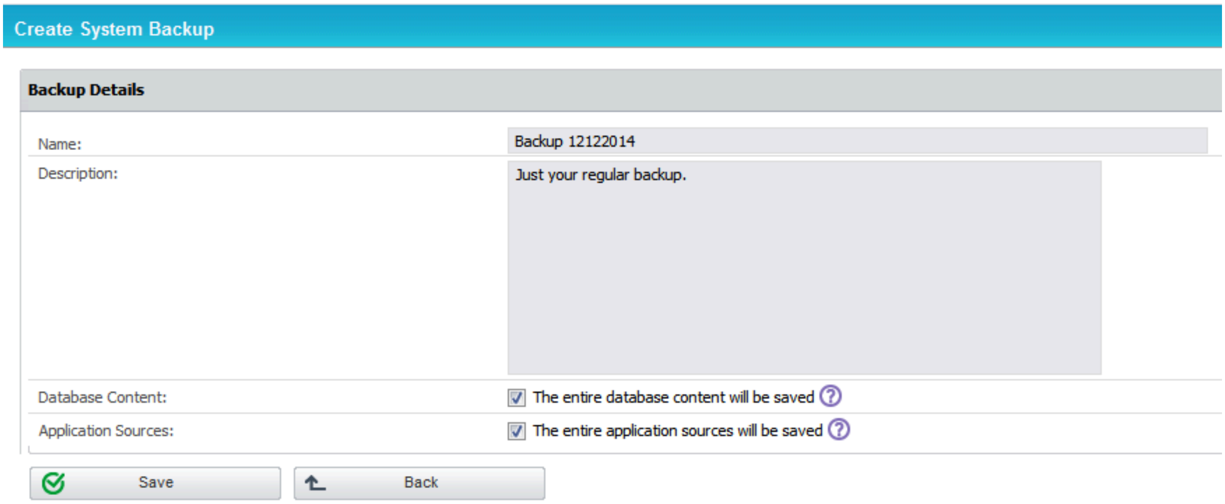
To view the list of current backups, go to **System Maintenance, System Backup v2**.

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**.



Create System Backup

Backup Details

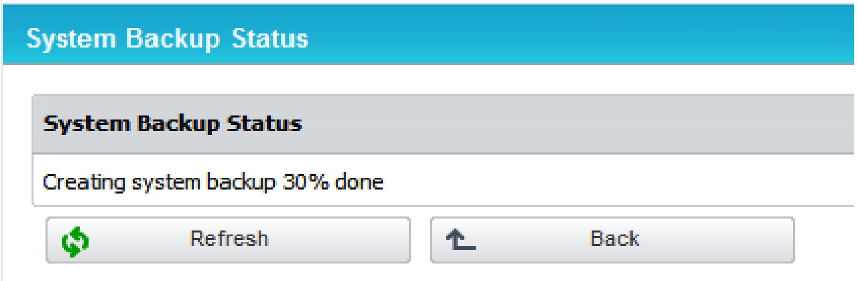
Name:	Backup 12122014
Description:	Just your regular backup.
Database Content:	☑ The entire database content will be saved
Application Sources:	☑ The entire application sources will be saved

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

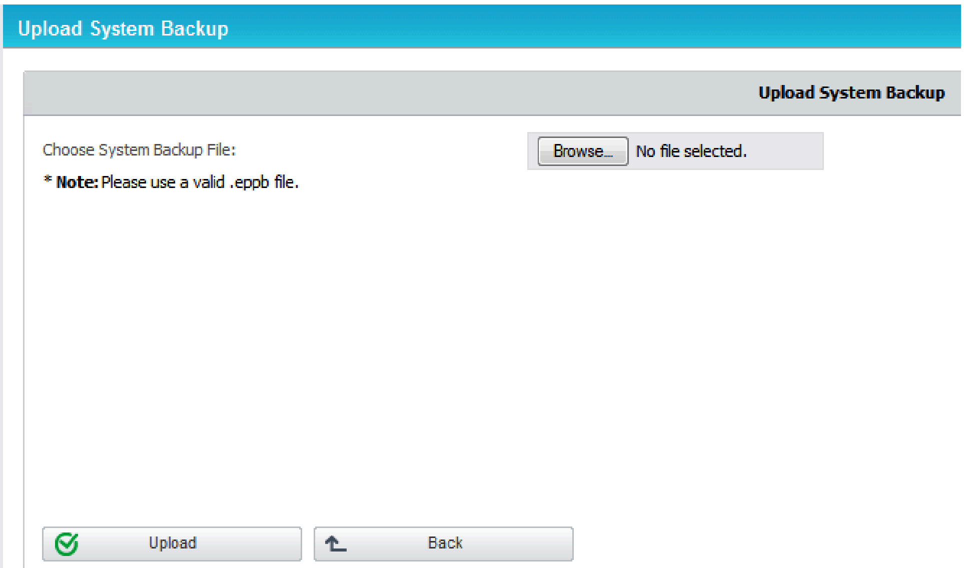
System Backup Status

Creating system backup 30% done

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

Upload System Backup

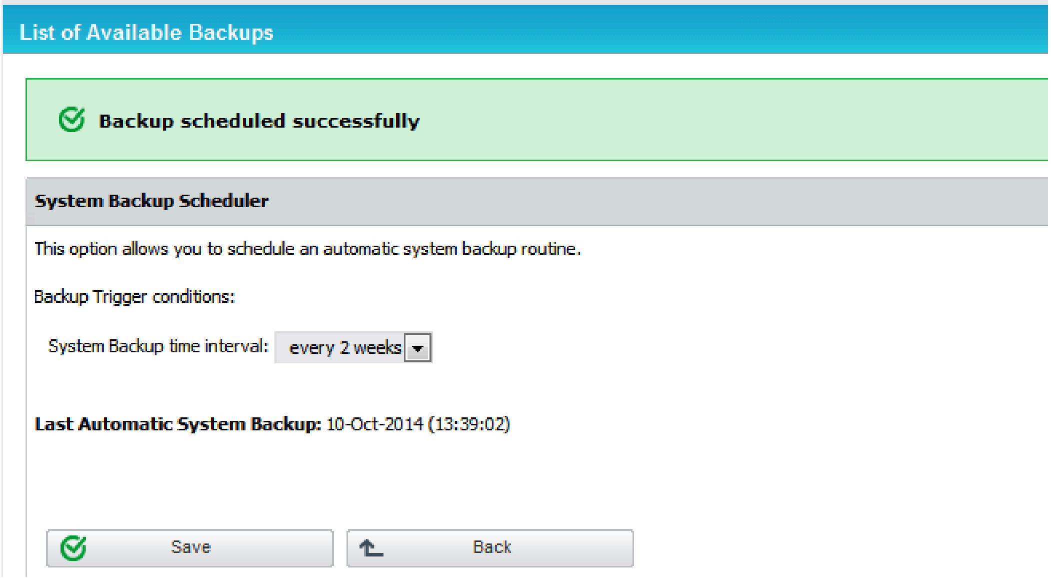
Choose System Backup File: Browse... No file selected.

* **Note:** Please use a valid .eppb file.

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.



List of Available Backups

Backup scheduled successfully

System Backup Scheduler

This option allows you to schedule an automatic system backup routine.

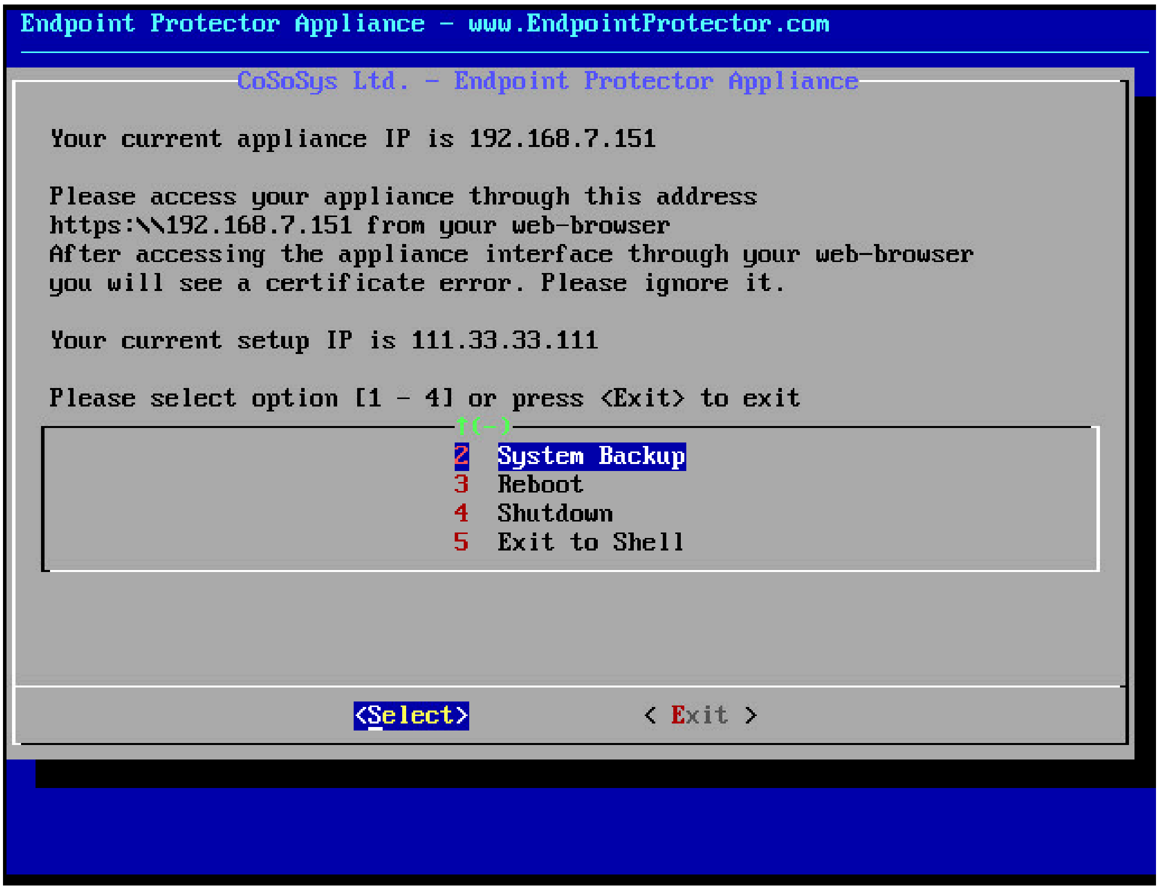
Backup Trigger conditions:

System Backup time interval: every 2 weeks

Last Automatic System Backup: 10-Oct-2014 (13:39:02)

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.



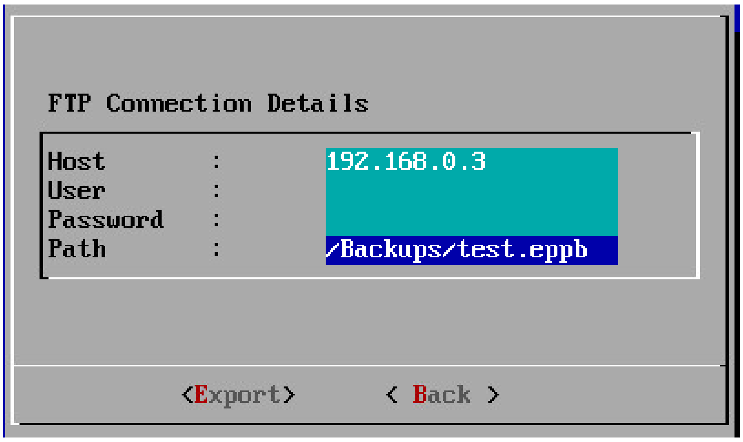
```
Endpoint Protector Appliance - www.EndpointProtector.com

CoSoSys Ltd. - Endpoint Protector Appliance

Your current appliance IP is 192.168.7.151

Please access your appliance through this address
https:\\192.168.7.151 from your web-browser
After accessing the appliance interface through your web-browser
you will see a certificate error. Please ignore it.

Your current setup IP is 111.33.33.111

Please select option [1 - 4] or press <Exit> to exit
```

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:



FTP Connection Details

```
Host       :      192.168.0.3
User       :
Password   :
Path       :      /Backups/test.eppb
```

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.

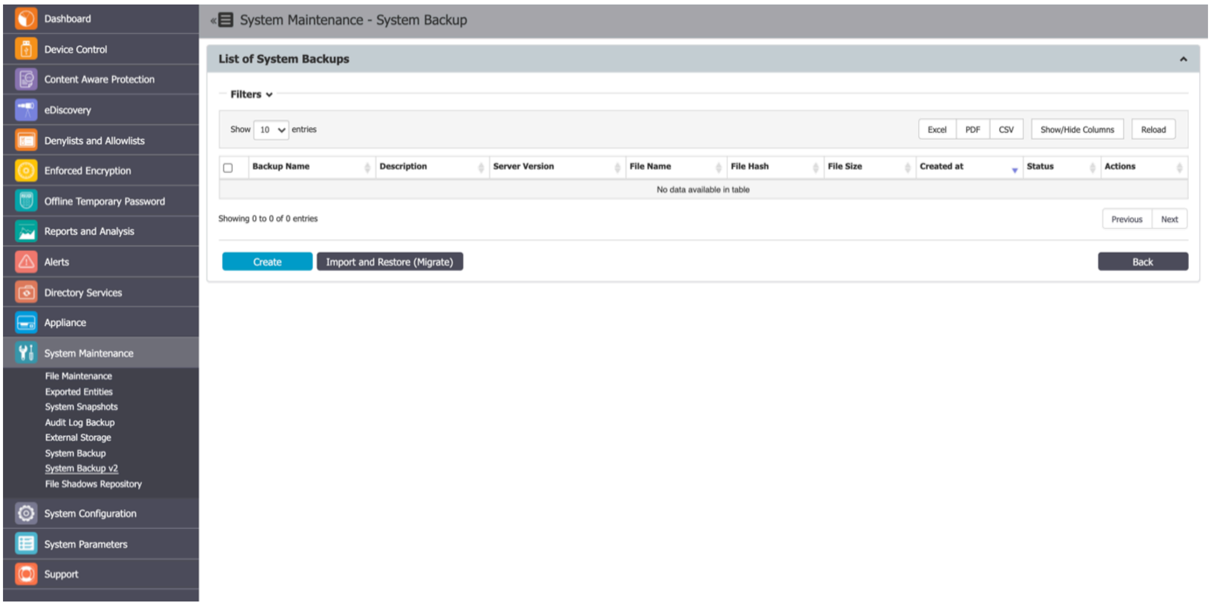
The version of the old Server and the new Server will have to be the same. Before starting the migration process, make sure both Servers have the same version (e.g.: update the old server to 5206, aligning it with the new server that is about to be deployed).

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.

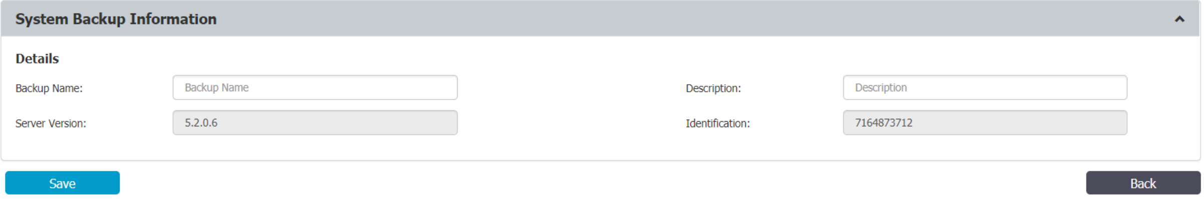


□	Backup Name	Description	Server Version	File Name	File Hash	File Size	Created at	Status	Actions
No data available in table									

Showing 0 to 0 of 0 entries

15.7.1. Creating a System Backup v2 (Migration)

You can create a new migration backup from the **System Maintenance**, **System Backup v2** section.



Details

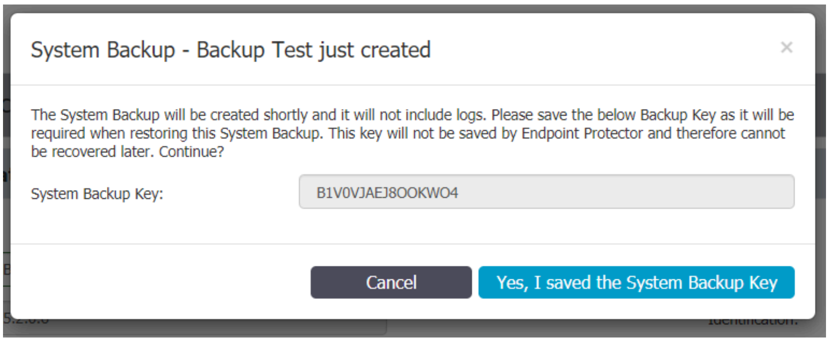
Backup Name: Backup Name

Description: Description

Server Version: 5.2.0.6

Identification: 7164873712

Note: For security purposes, the **System Backup Key** will not be stored by the Endpoint Protector. Before proceeding, make sure it is properly saved.



System Backup - Backup Test just created

The System Backup will be created shortly and it will not include logs. Please save the below Backup Key as it will be required when restoring this System Backup. This key will not be saved by Endpoint Protector and therefore cannot be recovered later. Continue?

System Backup Key: B1V0VJAEJ8OOKWO4

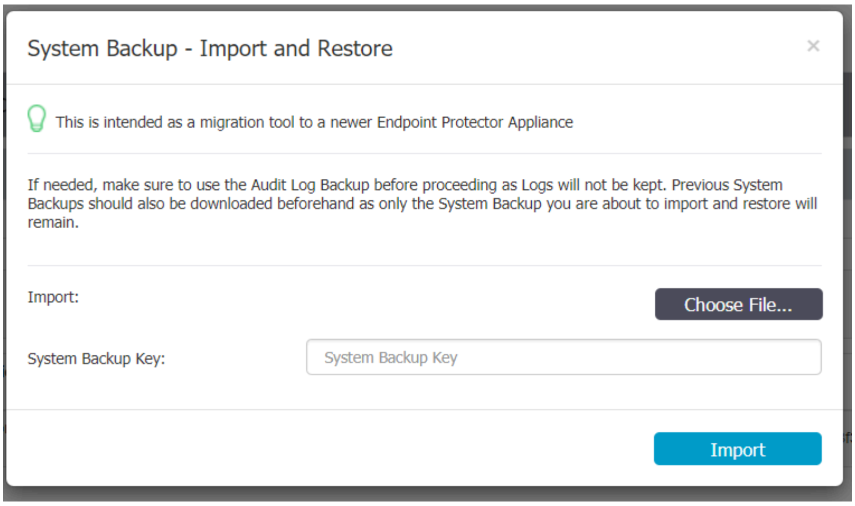
15.7.2. Importing and Restore (Migrate)

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

This is intended as a migration tool to a newer Endpoint Protector Appliance

If needed, make sure to use the Audit Log Backup before proceeding as Logs will not be kept. Previous System Backups should also be downloaded beforehand as only the System Backup you are about to import and restore will remain.

Import:

System Backup Key: System Backup Key

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

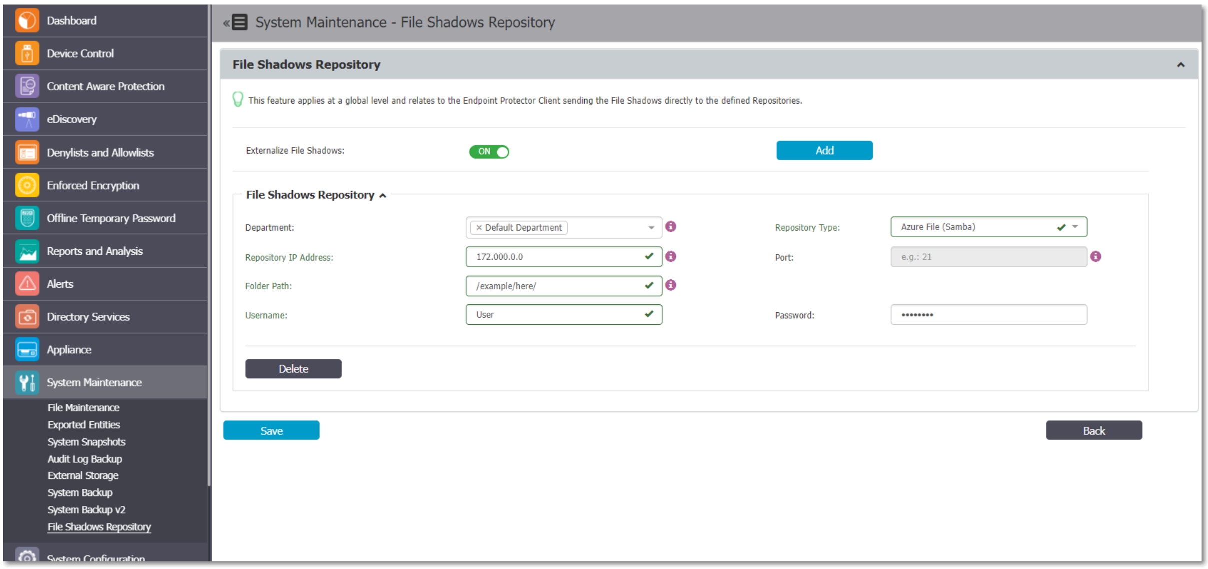
Note: If you select S3 Bucket type, the information required to create a File Shadow Repository will differ. Read more on S3 Buckets File Shadow Repository in the following section.

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



This feature applies at a global level and relates to the Endpoint Protector Client sending the File Shadows directly to the defined Repositories.

Externalize File Shadows: ON

File Shadows Repository

Department: × Default Department

Repository Type: Azure File (Samba)

Repository IP Address: 172.000.0.0

Port: e.g.: 21

Folder Path: /example/here/

Username: User

Password: ••••••••

15.8.1. Test Connection

The "Test" button facilitates the verification process for FTP and S3 bucket repositories (Indirect artifact retrieval). This functionality enables you to authenticate and execute a dummy file upload using the provided credentials.

1. **FTP Repository:** The "Test" button verifies authentication and file upload.
2. **S3 Bucket Repository (Indirect Artefact Retrieval):** The "Test" button checks key, secret_key, and validates bucket region and name if authentication response was successful.

Note: The Test Connection for S3 Bucket (Direct Artefact Retrieval), Samba v1, Samba v2, and Azure File Storage Repository is not supported due to additional 3rd Party requirements, such as IP Whitelisting, smbclient, etc..

This enhancement aims to make the testing process more transparent and efficient for FTP and S3 bucket repositories while considering the specific requirements of each repository type.

15.8.2. 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.

In this approach, when the download button is pressed, a request is sent to AWS to verify the file's presence in the bucket. If the file is not found, the EPP server responds with a message: **"The object object_name does not exist in the S3 Bucket Repository."** In the case of the file's existence, a subsequent request to AWS is made to obtain a pre-assigned URL for the shadow, which is then used to initiate the shadow download.

Note: The EPP server does not acquire a copy of the shadow at any point during this transaction. It only receives confirmation that the shadow exists in the S3 Bucket repository.

Users then download the shadows directly from the S3 bucket using a preassigned URL provided by AWS.

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.

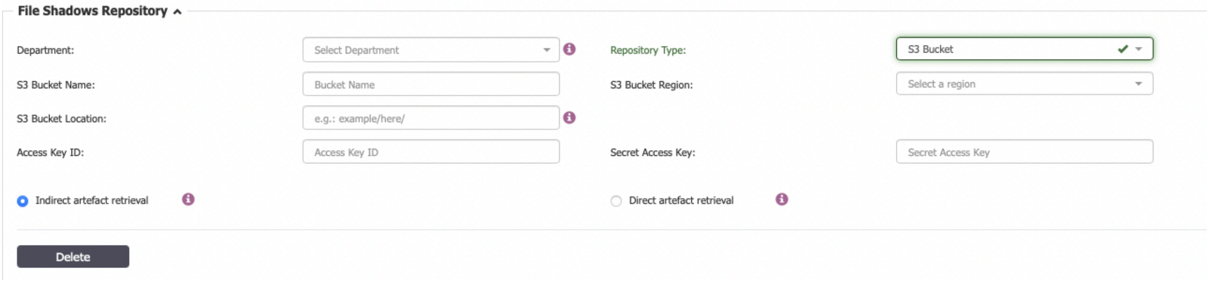
Important: To set up the S3 bucket repository using both the Direct and Indirect methods, administrators are required to specify the 'Bucket Name' and generate the 'Access Key ID' and 'Secret Access Key' through AWS administration.

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.



File Shadows Repository

Department: Select Department

Repository Type: S3 Bucket

S3 Bucket Name: Bucket Name

S3 Bucket Region: Select a region

S3 Bucket Location: e.g.: example/here/

Access Key ID: Access Key ID

Secret Access Key: Secret Access Key

● Indirect artefact retrieval

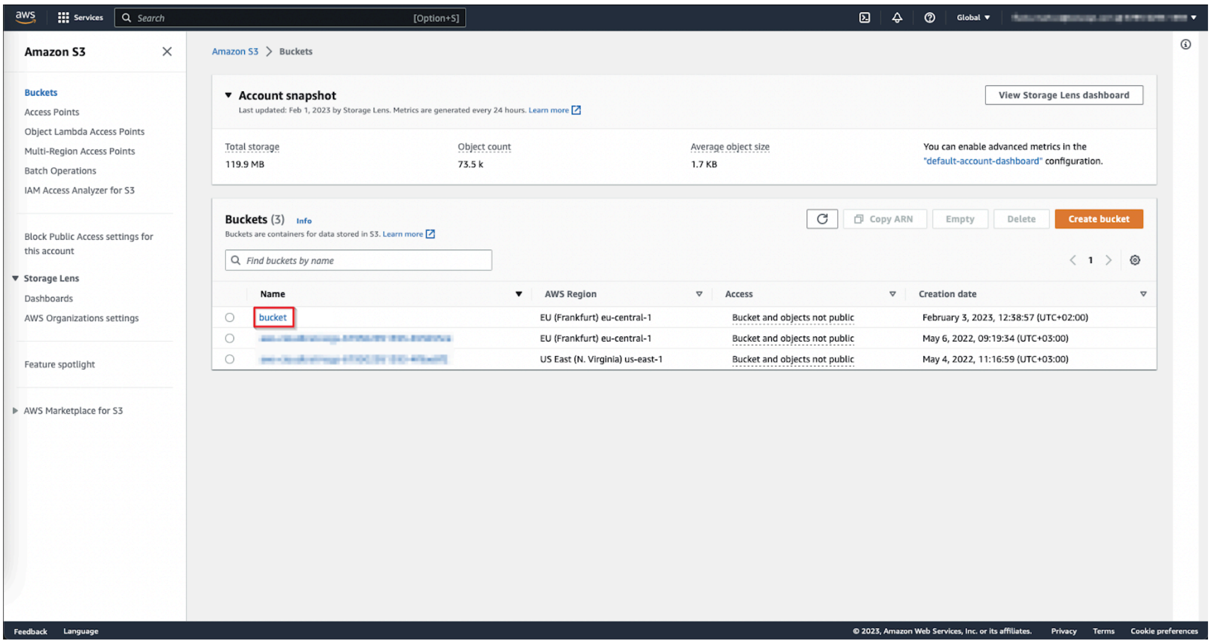
○ Direct artefact retrieval

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.

15.8.2.1. 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;**



▾ Account snapshot

Last updated: Feb 1, 2023 by Storage Lens. Metrics are generated every 24 hours. Learn more

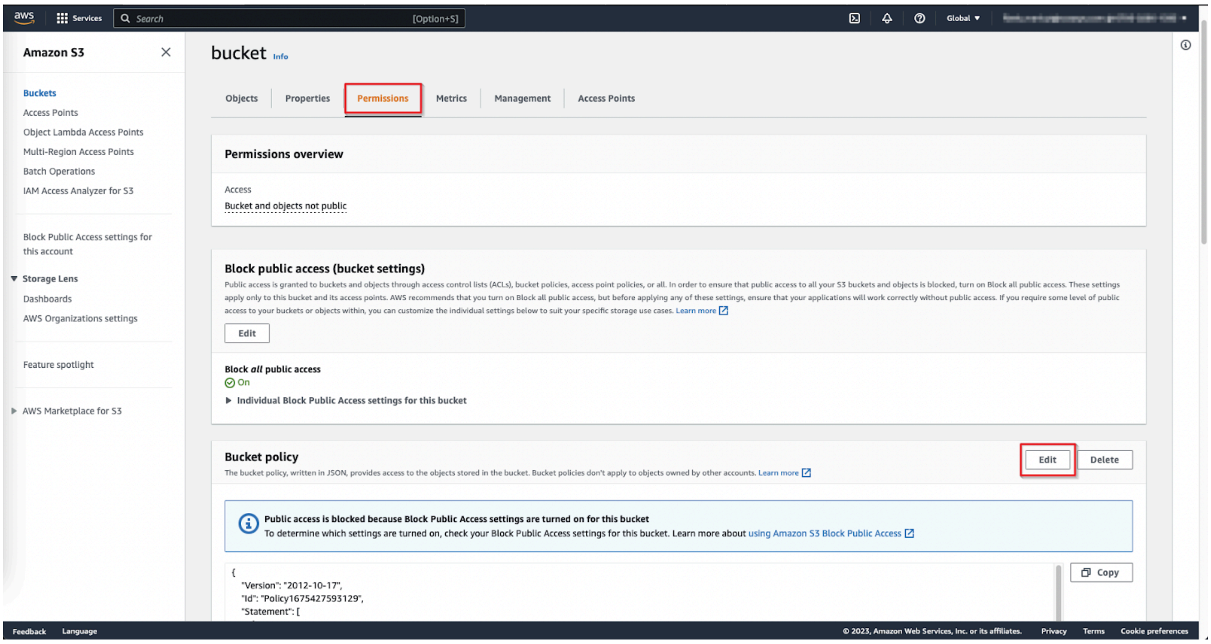
Total storage	Object count	Average object size	
119.9 MB	73.5 k	1.7 KB	You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets (3) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	bucket	EU (Frankfurt) eu-central-1	Bucket and objects not public	February 3, 2023, 12:38:57 (UTC+02:00)
○	[redacted]	EU (Frankfurt) eu-central-1	Bucket and objects not public	May 6, 2022, 09:19:34 (UTC+03:00)
○	[redacted]	US East (N. Virginia) us-east-1	Bucket and objects not public	May 4, 2022, 11:16:59 (UTC+03:00)

3. On the S3 Bucket, select the **Permission** tab, scroll down to the **Bucket** policy section, and then click **Edit**;



Permissions overview

Access: Bucket and objects not public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block *all* public access: ✓ On

▸ Individual Block Public Access settings for this bucket

Bucket policy

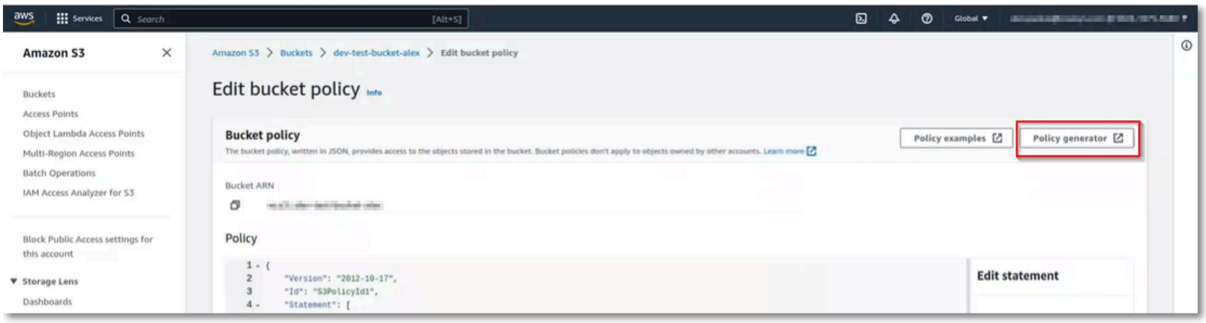
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

```
{
  "Version": "2012-10-17",
  "Id": "Policy1675427593129",
  "Statement": [
```

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.



The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Bucket ARN: [redacted]

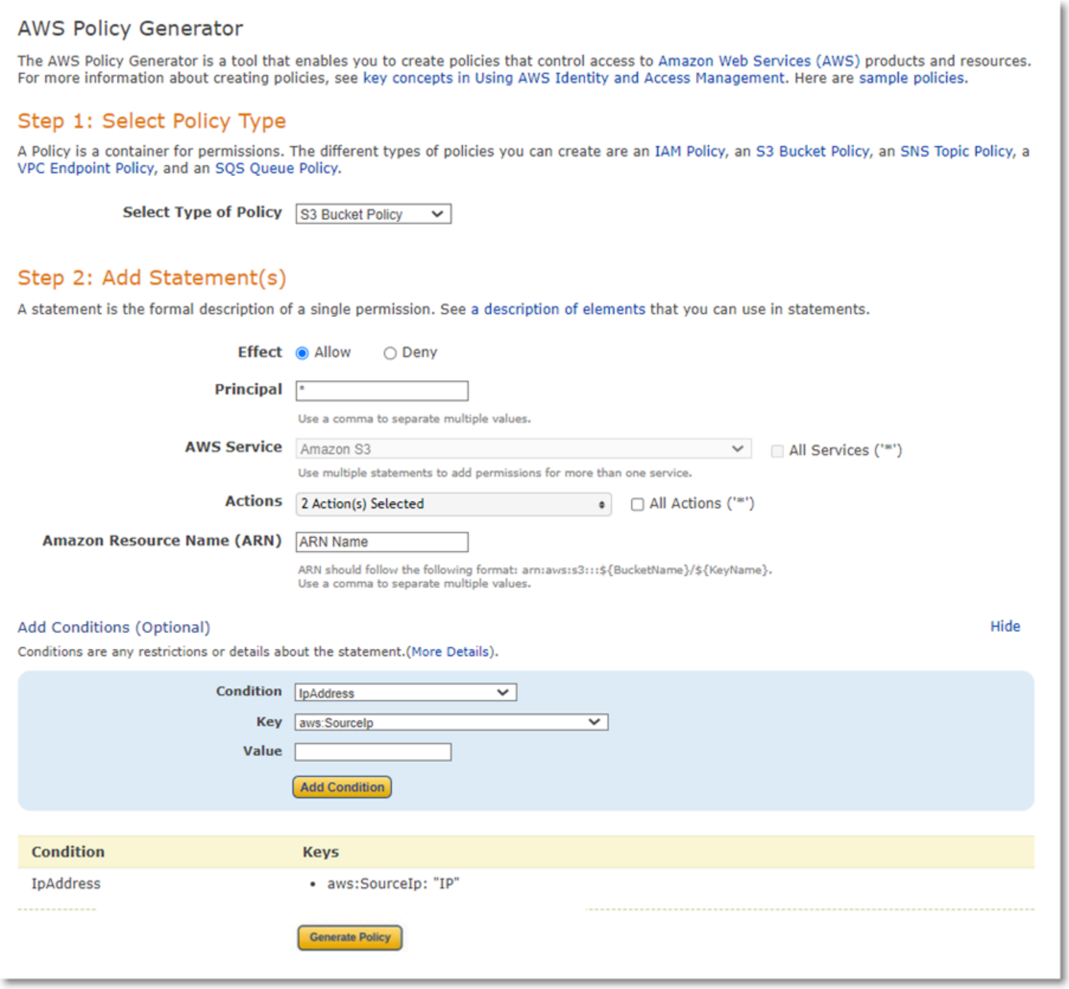
```
{
    "Version": "2012-10-17",
    "Id": "S3PolicyId1",
    "Statement": [
```

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**.

Note: For more information on this procedure, read the AWS documentation.



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect: ● Allow ○ Deny

Principal: *

Use a comma to separate multiple values.

AWS Service: Amazon S3 □ All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions: 2 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN): ARN Name

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

Conditions are any restrictions or details about the statement.(More Details).

Condition: IpAddress

Key: aws:SourceIp

Value:

Condition	Keys
IpAddress	• aws:SourceIp: "IP"

Example: S3 Bucket Policy (JSON)

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
            "s3:GetObject",
            "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::your-bucket-name/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            “IP1”, //the external  IP of the server; it’s need it for Delete action
            “IP2”, //public IP address; It’s needed for the download method
          ]
        }
      }
    }
  ]
}
```

Explanation:

- "**Effect**": "Allow" signifies permission granted.
- "**Principal**": "*" extends access to anyone (you can substitute * with an AWS account ID for limiting access to a specific account).
- "**Action**": [“s3:DeleteObject”, “s3:DeleteObject”]" permits both the "GetObject" action and the "DeleteObject" action (Download and Delete methods).
- "**Resource**": arn:aws:s3:::your-bucket-name/"" designates the ARN (Amazon Resource Name) of objects in your bucket. Replace "your-bucket-name" with your actual bucket name.
  - Important: It is crucial to append / at the end of the bucket ARN, as the AWS generator does not include it by default.
- "**Condition**" is where you specify the IP address condition.
- For the **“GetObject”** method (Download action from EPP) – this method requires the **public IP address**. To download the shadow, a proper AWS URL is constructed based on the Bucket Name, Bucket location, region, and shadow name.
- For the **“DeleteObject”** method (Delete action from EPP) - this method requires the server's external IP.

In this approach, a cURL request is employed to dispatch the DELETE request to AWS S3, facilitating the removal of the object from the bucket. This request is initiated from the EPP server, necessitating the whitelisting of its external IP in the Bucket Policy.

15.8.2.2. 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

15.8.2.3. 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ŏ刀ā木ù日ì月è女ǔ子ǐ馬/马鳥/鸟niǎ目ù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*_%E5%B1%B1%E4%BA%BAe%CC%81%E5%8F%A3o%CC%86%E5%88%80a%CC%84%E6%9C%A8u%CC%80%E6%97%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

16. System Configuration

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.

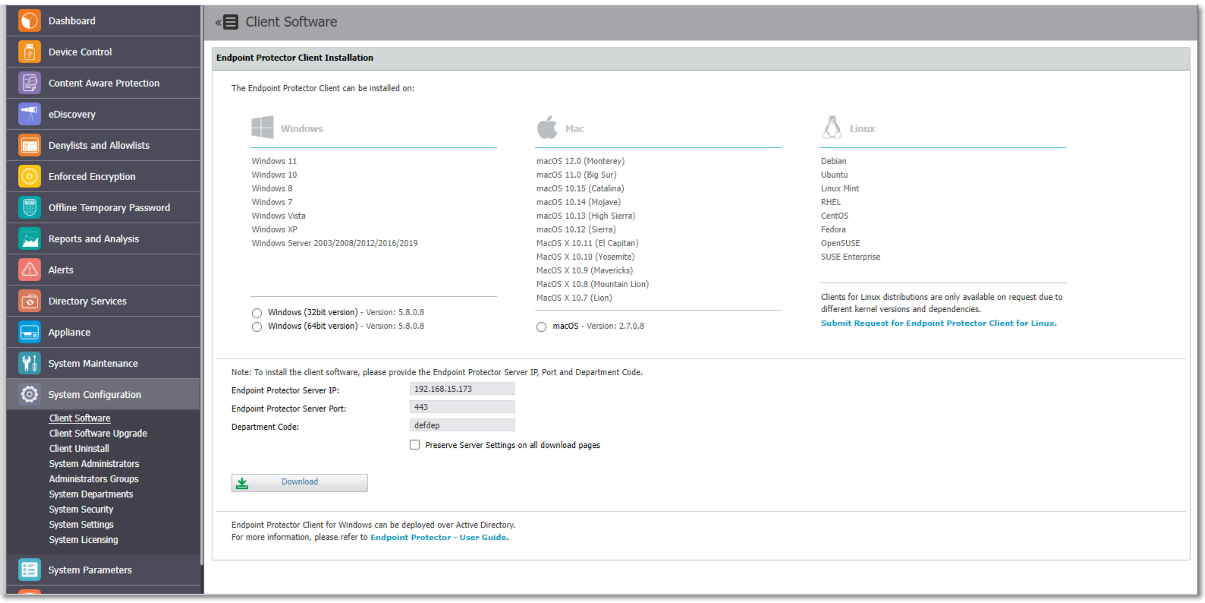
Important: Only the latest Endpoint Protector Clients are available for download. You cannot set another default Endpoint Protector Client version from the Client Software Upgrade section.

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.



Endpoint Protector Client Installation

The Endpoint Protector Client can be installed on:

Windows	Mac	Linux
Windows 11	macOS 12.0 (Monterey)	Debian
Windows 10	macOS 11.0 (Big Sur)	Ubuntu
Windows 8	macOS 10.15 (Catalina)	Linux Mint
Windows 7	macOS 10.14 (Mojave)	RHEL
Windows Vista	macOS 10.13 (High Sierra)	CentOS
Windows XP	macOS 10.12 (Sierra)	Fedora
Windows Server 2003/2008/2012/2016/2019	MacOS X 10.11 (El Capitan)	OpenSUSE
	MacOS X 10.10 (Yosemite)	SUSE Enterprise
	MacOS X 10.9 (Mavericks)	
	MacOS X 10.8 (Mountain Lion)	
	MacOS X 10.7 (Lion)	
○ Windows (32bit version) - Version: 5.8.0.8 ○ Windows (64bit version) - Version: 5.8.0.8	○ macOS - Version: 2.7.0.8	Clients for Linux distributions are only available on request due to different kernel versions and dependencies. Submit Request for Endpoint Protector Client for Linux.

Note: To install the client software, please provide the Endpoint Protector Server IP, Port and Department Code.

Endpoint Protector Server IP: 192.168.15.173

Endpoint Protector Server Port: 443

Department Code: defdep

□ Preserve Server Settings on all download pages

Endpoint Protector Client for Windows can be deployed over Active Directory.
For more information, please refer to Endpoint Protector - User Guide.

Note: EPP Client versions are displayed in the format X.X.X.XXXX on endpoints. This version will be saved in the EPP Server database, although the web console will truncate the last 3 digits.

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:
   <cd pathToLinuxClientFolder>
2. To run commands as root, run the following command and type your password;
   <sudo su>
3. Open the options.sh configuration file with the following command:
   <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 install.sh>

Additional CLI commands for Linux in specific mode:

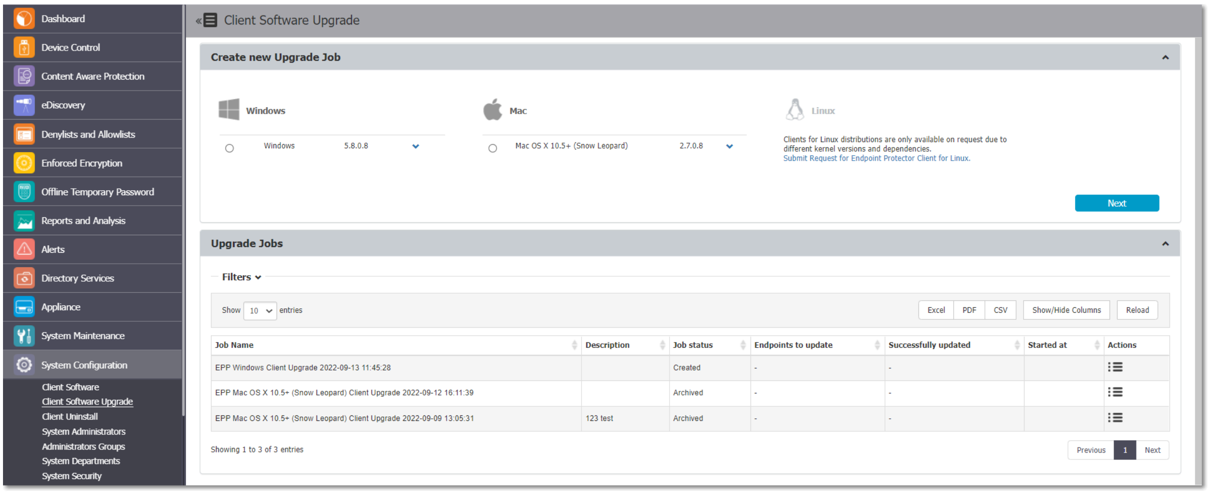
- #EPPCLIENT_SUPRESSRW - suppress FileRead/FileDelete events for NS and Removable devices
- #EPPCLIENT_DISABLECAP - disabling loading of CAP drivers (CAP will not work)

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.



○ Windows 5.8.0.8

○ Mac OS X 10.5+ (Snow Leopard) 2.7.0.8

Clients for Linux distributions are only available on request due to different kernel versions and dependencies.
Submit Request for Endpoint Protector Client for Linux.

Show 10 entries

Job Name	Description	Job status	Endpoints to update	Successfully updated	Started at	Actions
EPP Windows Client Upgrade 2022-09-13 11:45:28		Created	-	-		☰
EPP Mac OS X 10.5+ (Snow Leopard) Client Upgrade 2022-09-12 16:11:39		Archived	-	-		☰
EPP Mac OS X 10.5+ (Snow Leopard) Client Upgrade 2022-09-09 13:05:31	123 test	Archived	-	-		☰

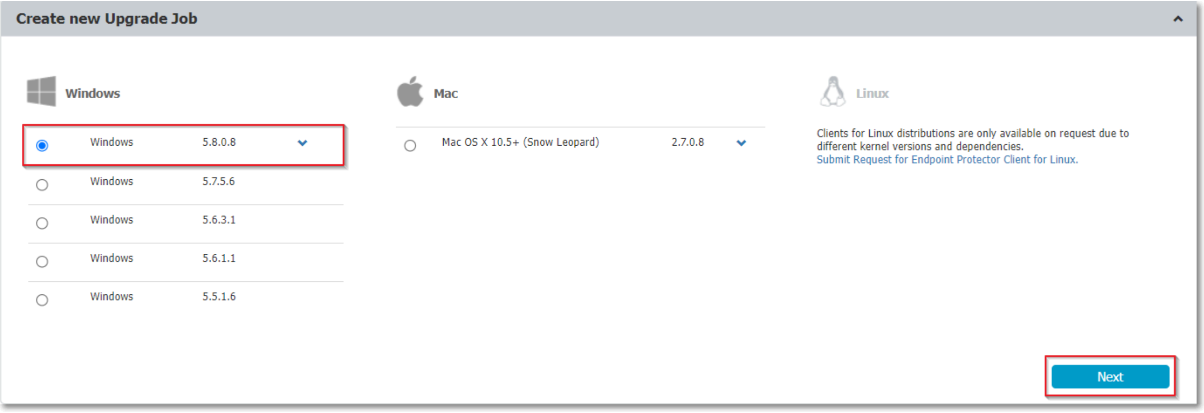
Showing 1 to 3 of 3 entries

Note: EPP Client versions are displayed in the format X.X.X.XXXX on endpoints. This version will be saved in the EPP Server database, although the web console will truncate the last 3 digits. In case EPP Client versions are identical (first 4-digits), EPP Server will still compare the full version number against each other, identifying the most recent version.

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**;



● Windows 5.8.0.8

○ Windows 5.7.5.6

○ Windows 5.6.3.1

○ Windows 5.6.1.1

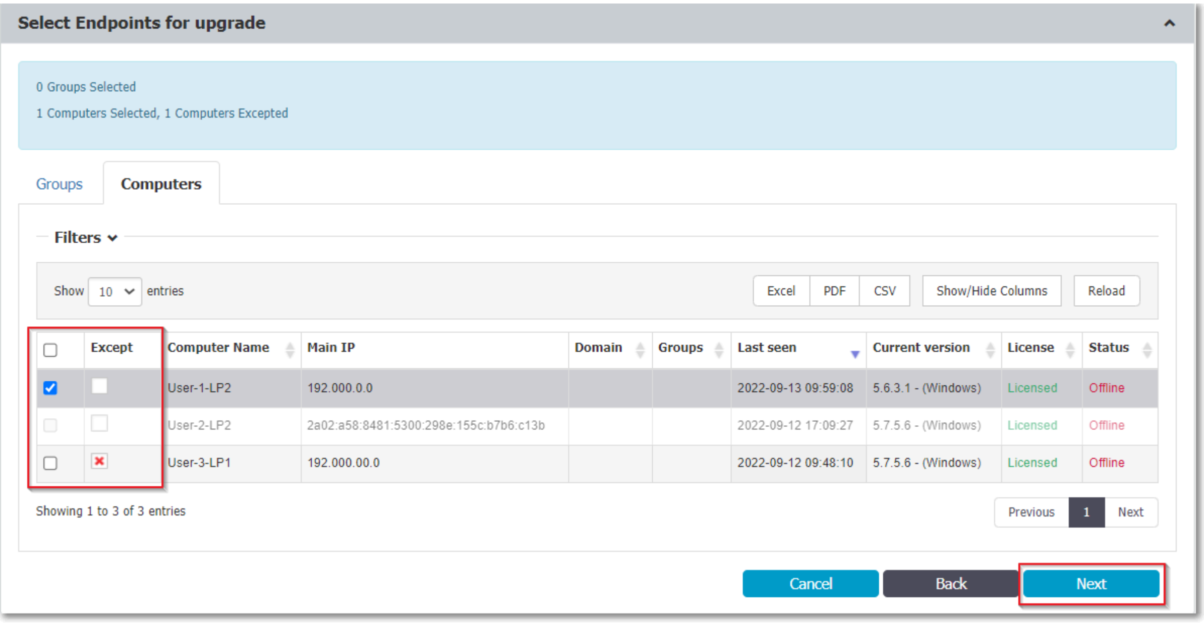
○ Windows 5.5.1.6

○ Mac OS X 10.5+ (Snow Leopard) 2.7.0.8

Clients for Linux distributions are only available on request due to different kernel versions and dependencies.
Submit Request for Endpoint Protector Client for Linux.

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.



Select Endpoints for upgrade

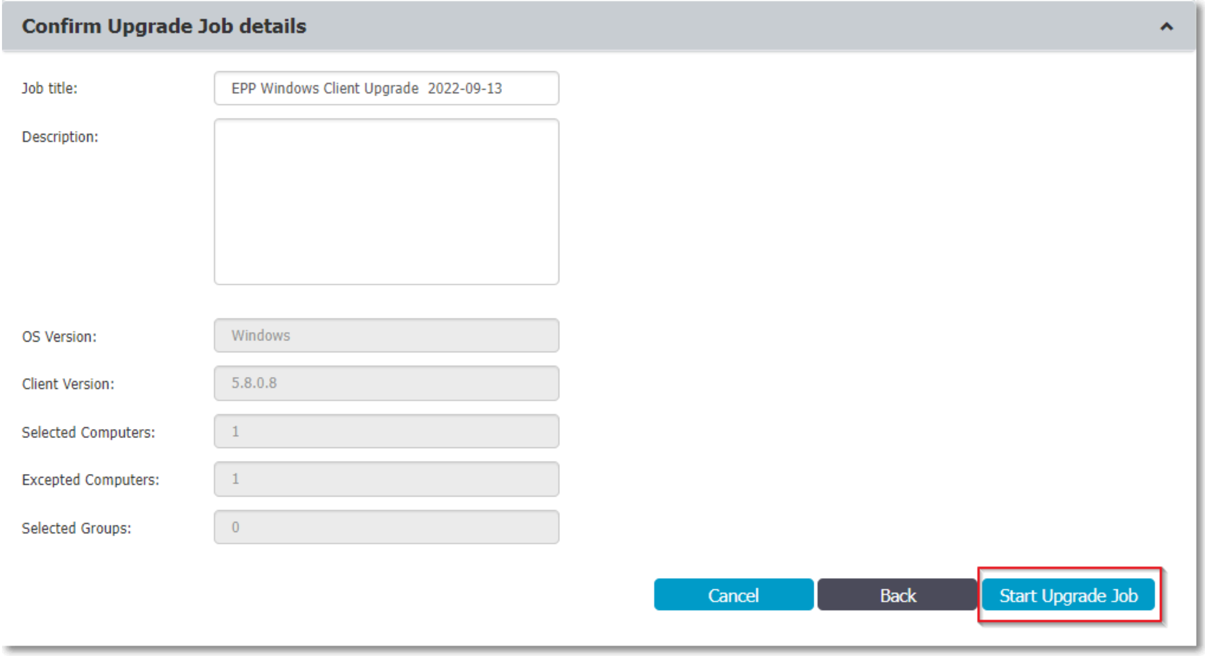
0 Groups Selected
1 Computers Selected, 1 Computers Excepted

□	Except	Computer Name	Main IP	Domain	Groups	Last seen	Current version	License	Status
☑	□	User-1-LP2	192.000.0.0			2022-09-13 09:59:08	5.6.3.1 - (Windows)	Licensed	Offline
□	□	User-2-LP2	2a02:a58:8481:5300:298e:155c:b7b6:c13b			2022-09-12 17:09:27	5.7.5.6 - (Windows)	Licensed	Offline
□	☒	User-3-LP1	192.000.00.0			2022-09-12 09:48:10	5.7.5.6 - (Windows)	Licensed	Offline

Showing 1 to 3 of 3 entries

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**.



Confirm Upgrade Job details

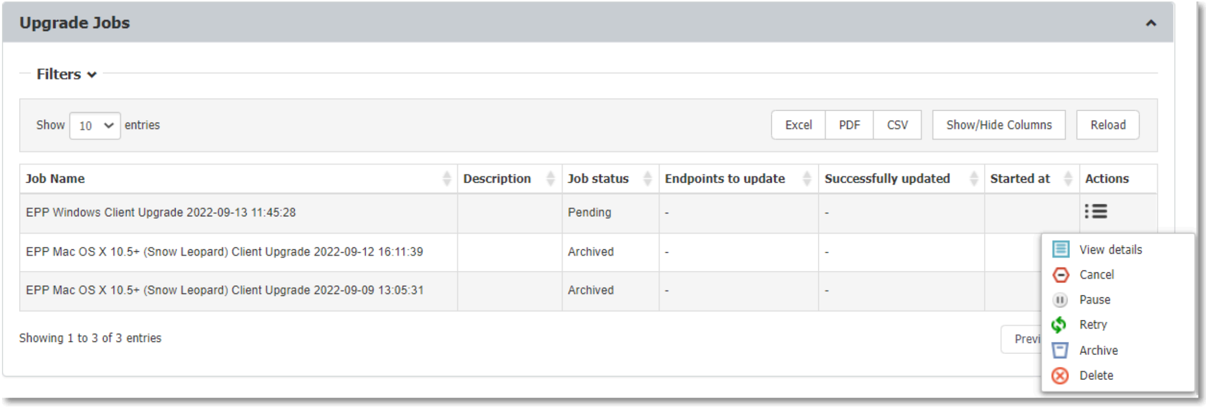
Job title:	EPP Windows Client Upgrade 2022-09-13
Description:	
OS Version:	Windows
Client Version:	5.8.0.8
Selected Computers:	1
Excepted Computers:	1
Selected Groups:	0

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

Job Name	Description	Job status	Endpoints to update	Successfully updated	Started at	Actions
EPP Windows Client Upgrade 2022-09-13 11:45:28		Pending	-	-		
EPP Mac OS X 10.5+ (Snow Leopard) Client Upgrade 2022-09-12 16:11:39		Archived	-	-		
EPP Mac OS X 10.5+ (Snow Leopard) Client Upgrade 2022-09-09 13:05:31		Archived	-	-		

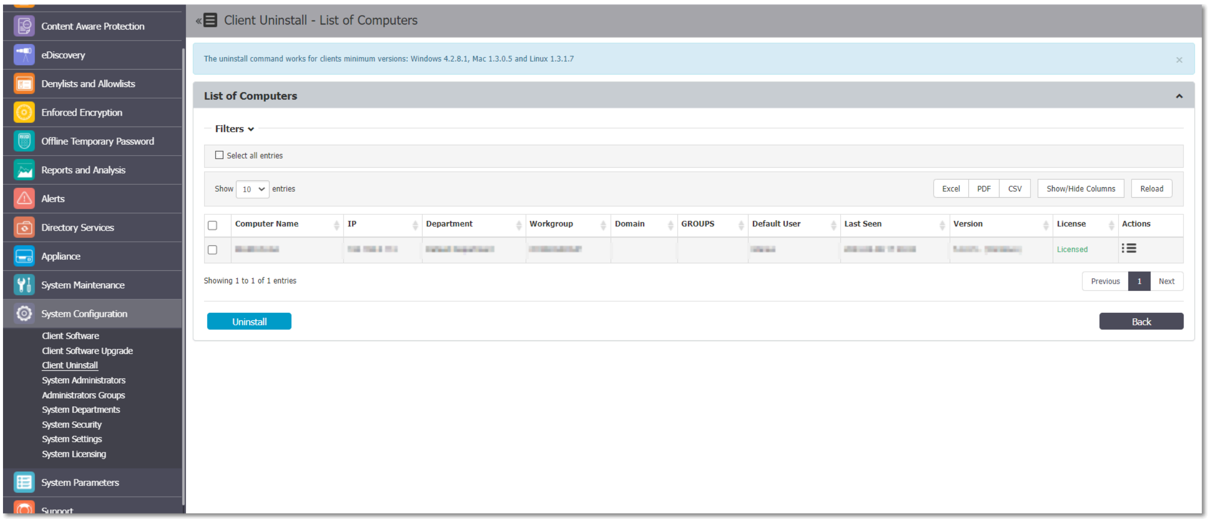
Showing 1 to 3 of 3 entries

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 - List of Computers

The uninstall command works for clients minimum versions: Windows 4.2.8.1, Mac 1.3.0.5 and Linux 1.3.1.7

List of Computers

□ Select all entries

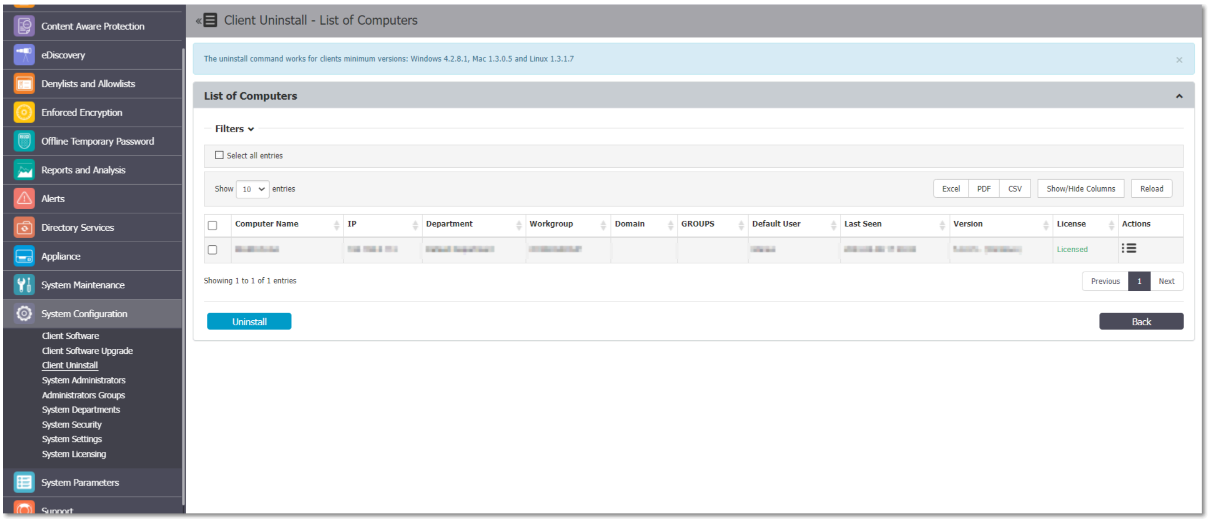
□	Computer Name	IP	Department	Workgroup	Domain	GROUPS	Default User	Last Seen	Version	License	Actions
□	[redacted]	[redacted]	[redacted]	[redacted]			[redacted]	[redacted]	[redacted]	Licensed	☰

Showing 1 to 1 of 1 entries

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.


Client Uninstall - List of Computers

The uninstall command works for clients minimum versions: Windows 4.2.8.1, Mac 1.3.0.5 and Linux 1.3.1.7

List of Computers

□ Select all entries

□	Computer Name	IP	Department	Workgroup	Domain	GROUPS	Default User	Last Seen	Version	License	Actions
□	[redacted]	[redacted]	[redacted]	[redacted]			[redacted]	[redacted]	[redacted]	Licensed	☰

Showing 1 to 1 of 1 entries

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:

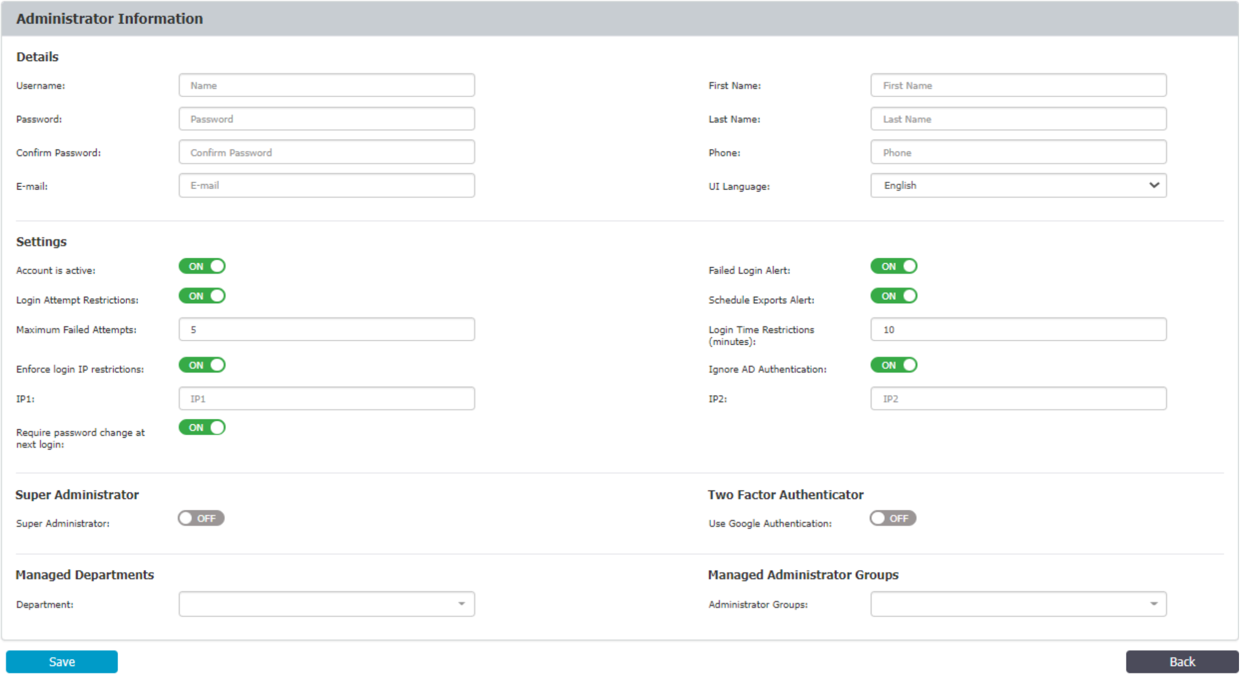
a) When the **Enforce all administrator password security at next login** setting is also enabled from System Configuration, System Security, then **Require password change at next login** is ignored and disabled once the password is changed.

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



Administrator Information

Details

Username:	Name	First Name:	First Name
Password:	Password	Last Name:	Last Name
Confirm Password:	Confirm Password	Phone:	Phone
E-mail:	E-mail	UI Language:	English

Settings

Account is active:	ON	Failed Login Alert:	ON
Login Attempt Restrictions:	ON	Schedule Exports Alert:	ON
Maximum Failed Attempts:	5	Login Time Restrictions (minutes):	10
Enforce login IP restrictions:	ON	Ignore AD Authentication:	ON
IP1:	IP1	IP2:	IP2
Require password change at next login:	ON		

Super Administrator		Two Factor Authenticator	
Super Administrator:	OFF	Use Google Authentication:	OFF

Managed Departments		Managed Administrator Groups	
Department:		Administrator Groups:	

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 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

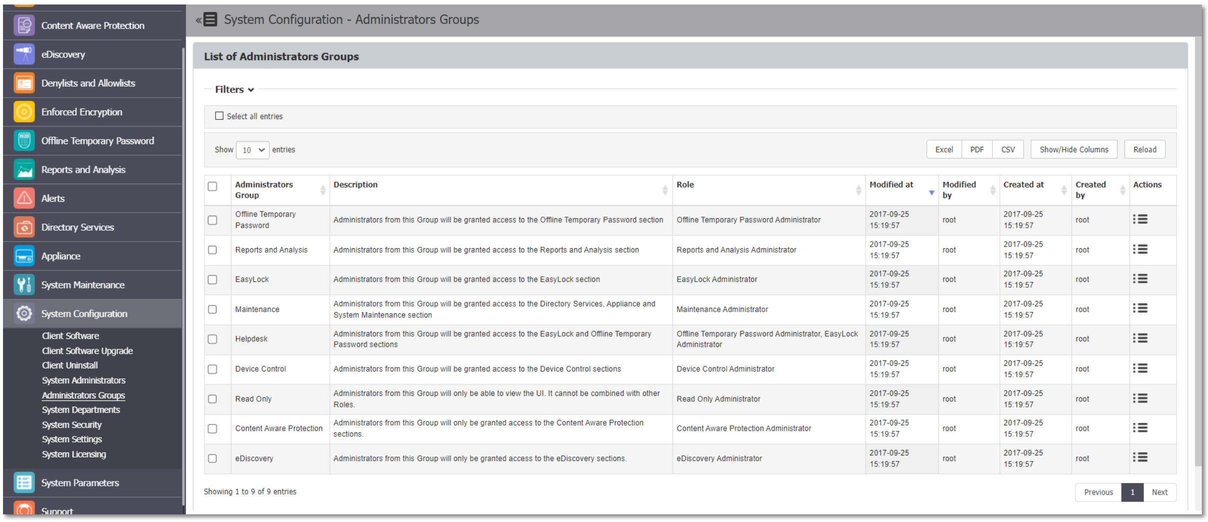
Important: The **Read Only** role cannot be combined with any other roles!

- **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.



System Configuration - Administrators Groups

List of Administrators Groups

□ Select all entries

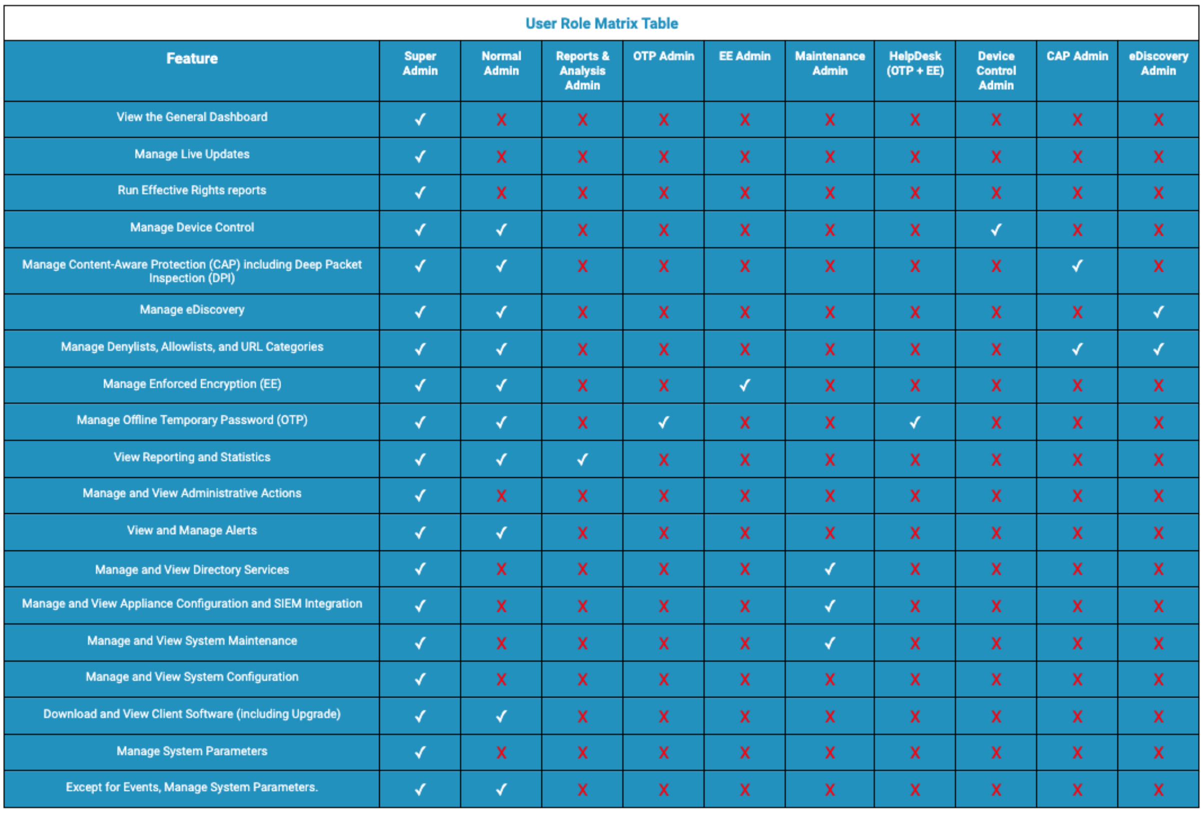
Show 10 entries

□	Administrators Group	Description	Role	Modified at	Modified by	Created at	Created by	Actions
□	Offline Temporary Password	Administrators from this Group will be granted access to the Offline Temporary Password section	Offline Temporary Password Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Reports and Analysis	Administrators from this Group will be granted access to the Reports and Analysis section	Reports and Analysis Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	EasyLock	Administrators from this Group will be granted access to the EasyLock section	EasyLock Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Maintenance	Administrators from this Group will be granted access to the Directory Services, Appliance and System Maintenance section	Maintenance Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Helpdesk	Administrators from this Group will be granted access to the EasyLock and Offline Temporary Password sections	Offline Temporary Password Administrator, EasyLock Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Device Control	Administrators from this Group will be granted access to the Device Control sections	Device Control Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Read Only	Administrators from this Group will only be able to view the UI. It cannot be combined with other Roles.	Read Only Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Content Aware Protection	Administrators from this Group will only be granted access to the Content Aware Protection sections.	Content Aware Protection Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	eDiscovery	Administrators from this Group will only be granted access to the eDiscovery sections.	eDiscovery Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰

Showing 1 to 9 of 9 entries

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.



User Role Matrix Table

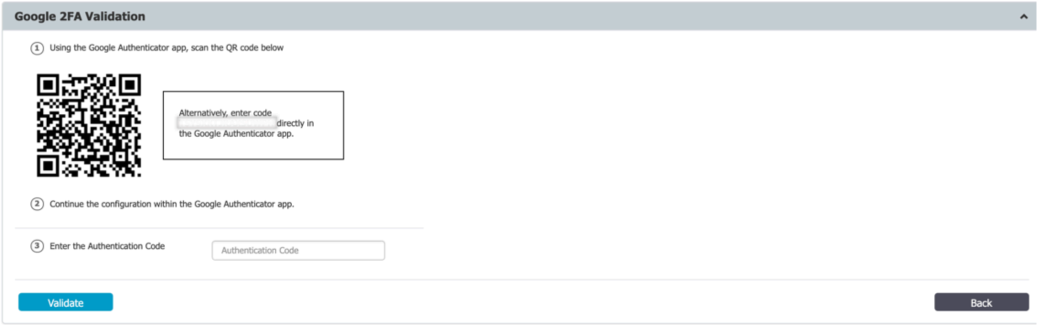
Feature	Super Admin	Normal Admin	Reports & Analysis Admin	OTP Admin	EE Admin	Maintenance Admin	HelpDesk (OTP + EE)	Device Control Admin	CAP Admin	eDiscovery Admin
View the General Dashboard	✓	X	X	X	X	X	X	X	X	X
Manage Live Updates	✓	X	X	X	X	X	X	X	X	X
Run Effective Rights reports	✓	X	X	X	X	X	X	X	X	X
Manage Device Control	✓	✓	X	X	X	X	X	✓	X	X
Manage Content-Aware Protection (CAP) including Deep Packet Inspection (DPI)	✓	✓	X	X	X	X	X	X	✓	X
Manage eDiscovery	✓	✓	X	X	X	X	X	X	X	✓
Manage Denylists, Allowlists, and URL Categories	✓	✓	X	X	X	X	X	X	✓	✓
Manage Enforced Encryption (EE)	✓	✓	X	X	✓	X	X	X	X	X
Manage Offline Temporary Password (OTP)	✓	✓	X	✓	X	X	✓	X	X	X
View Reporting and Statistics	✓	✓	✓	X	X	X	X	X	X	X
Manage and View Administrative Actions	✓	X	X	X	X	X	X	X	X	X
View and Manage Alerts	✓	✓	X	X	X	X	X	X	X	X
Manage and View Directory Services	✓	X	X	X	X	✓	X	X	X	X
Manage and View Appliance Configuration and SIEM Integration	✓	X	X	X	X	✓	X	X	X	X
Manage and View System Maintenance	✓	X	X	X	X	✓	X	X	X	X
Manage and View System Configuration	✓	X	X	X	X	X	X	X	X	X
Download and View Client Software (including Upgrade)	✓	✓	X	X	X	X	X	X	X	X
Manage System Parameters	✓	X	X	X	X	X	X	X	X	X
Except for Events, Manage System Parameters.	✓	✓	X	X	X	X	X	X	X	X

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.



Google 2FA Validation

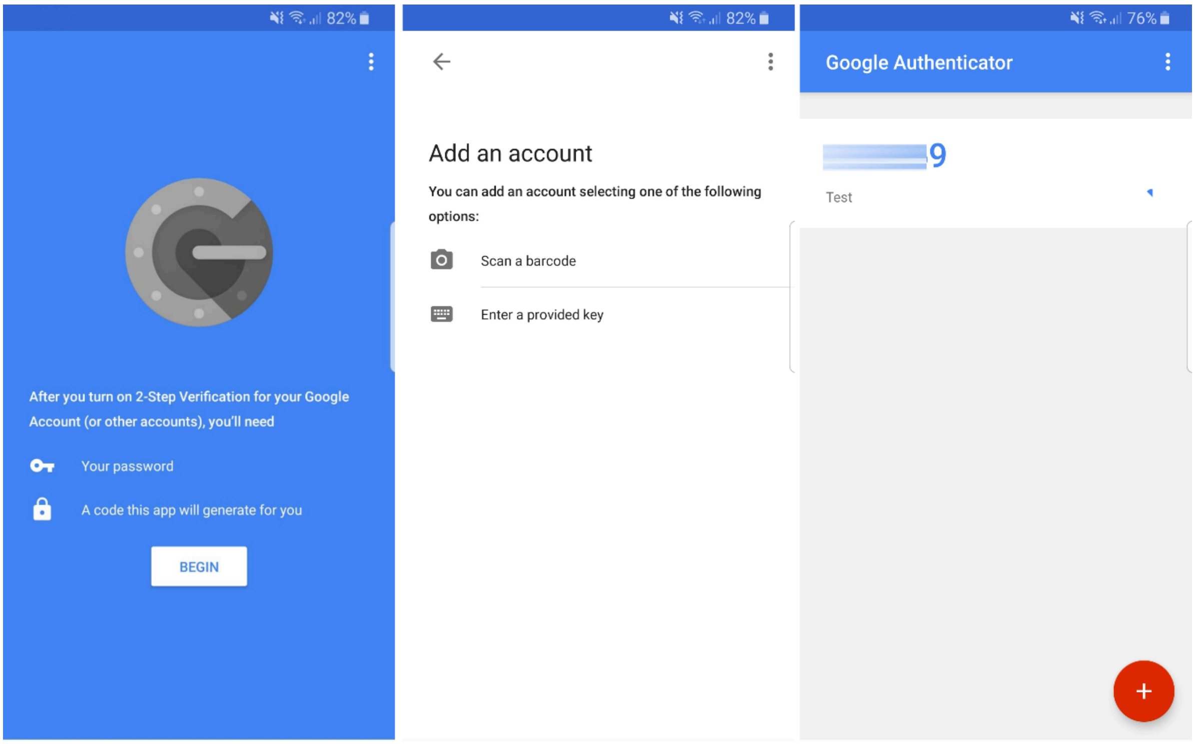
1. Using the Google Authenticator app, scan the QR code below

Alternatively, enter code [redacted] directly in the Google Authenticator app.

2. Continue the configuration within the Google Authenticator app.

3. Enter the Authentication Code

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.



After you turn on 2-Step Verification for your Google Account (or other accounts), you'll need

Your password

A code this app will generate for you

Add an account

You can add an account selecting one of the following options:

Scan a barcode

Enter a provided key

[redacted]

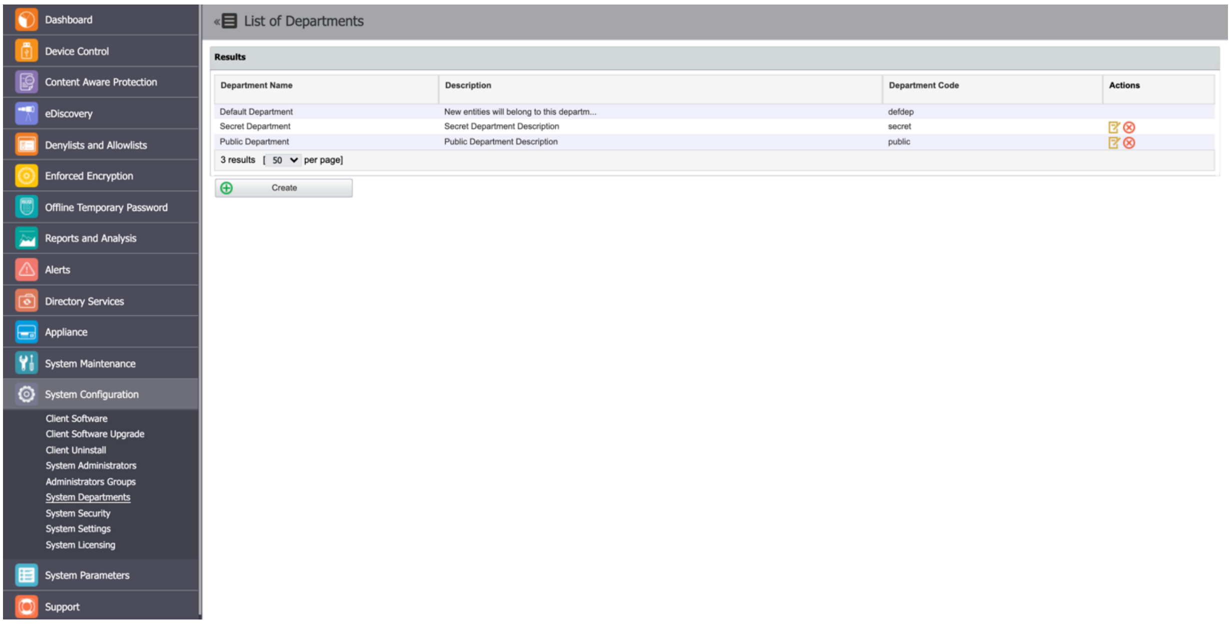
16.8.System Departments

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.



List of Departments

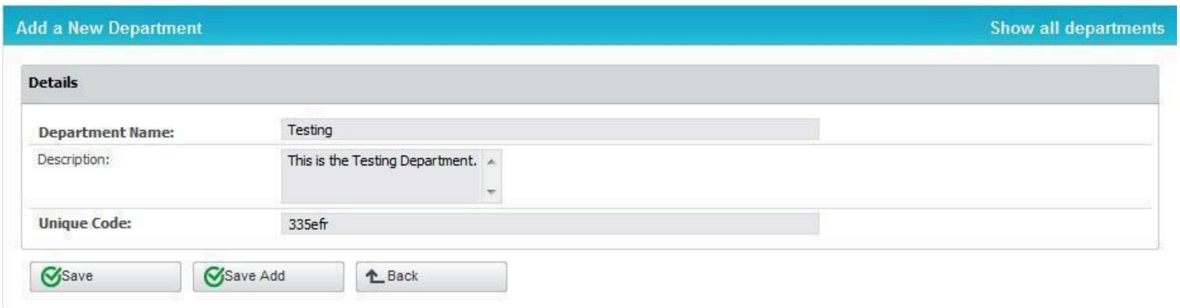
Results

Department Name	Description	Department Code	Actions
Default Department	New entities will belong to this departm...	defdep	
Secret Department	Secret Department Description	secret	📝 ⊗
Public Department	Public Department Description	public	📝 ⊗

3 results [50 per page]

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).



Add a New Department

Details

Department Name:	Testing
Description:	This is the Testing Department.
Unique Code:	335efr

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.

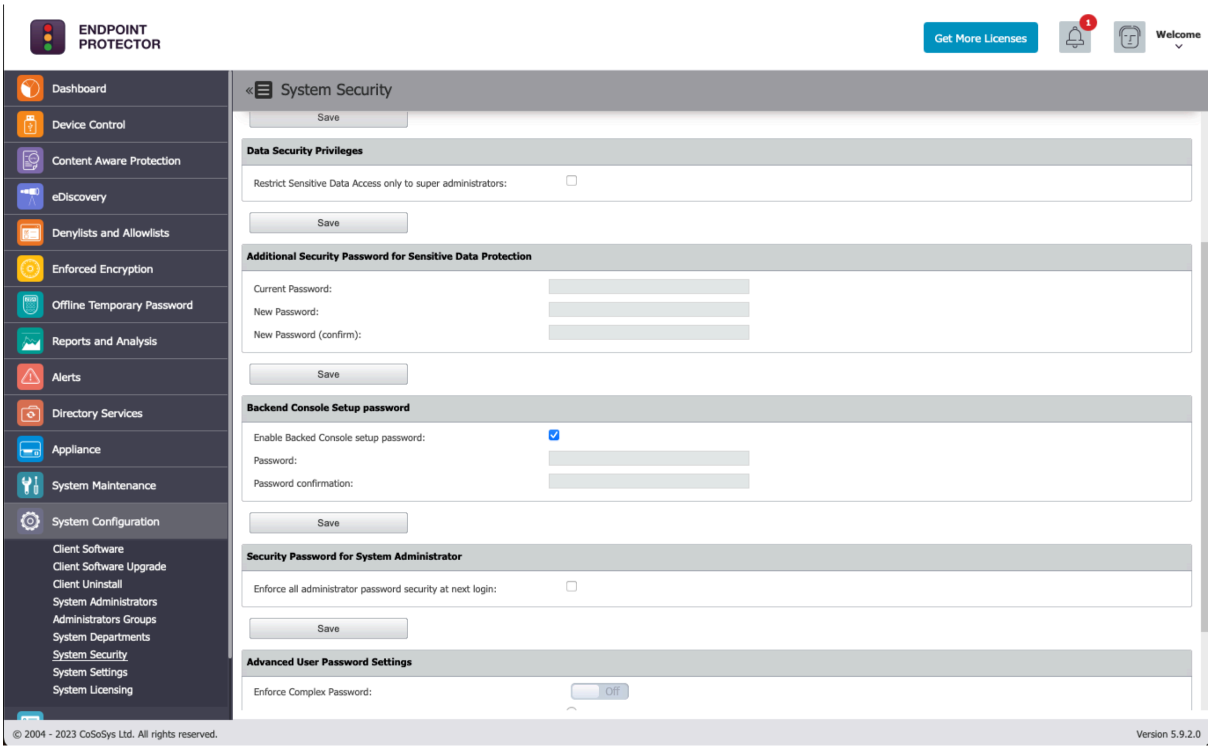
Example: Computer Test-PC is registered to the department "developers". In this case, the user Test logged on that computer will be assigned to the same department together with the devices connected on the computer Test-PC.

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.



Data Security Privileges

Restrict Sensitive Data Access only to super administrators: □

Save

Additional Security Password for Sensitive Data Protection

Current Password:

New Password:

New Password (confirm):

Save

Backend Console Setup password

Enable Backed Console setup password: ☑

Password:

Password confirmation:

Save

Security Password for System Administrator

Enforce all administrator password security at next login: □

Save

Advanced User Password Settings

Enforce Complex Password: Off

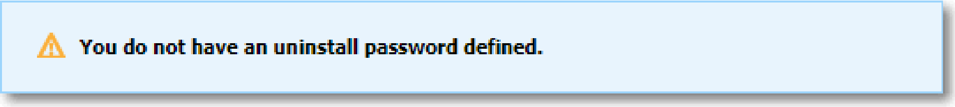
© 2004 - 2023 CoSoSys Ltd. All rights reserved.

Version 5.9.2.0

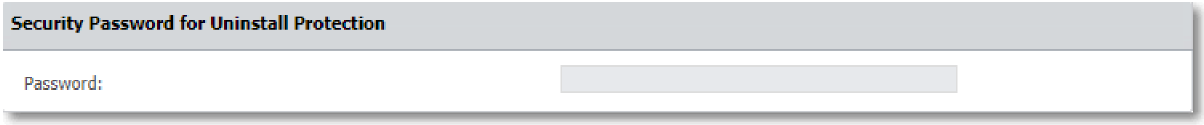
16.9.1. Security Password for Uninstall Protection

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.



⚠ You do not have an uninstall password defined.

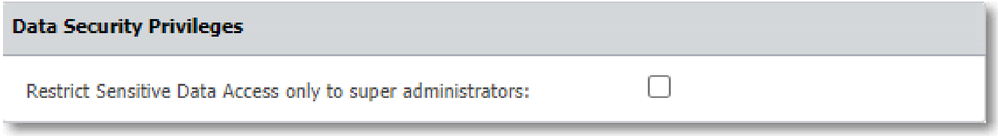


Security Password for Uninstall Protection

Password:

16.9.2. Data Security Privileges

From this section, you can allow access to sensitive data only to super administrators.



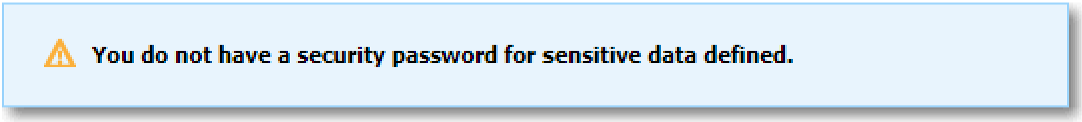
Data Security Privileges

Restrict Sensitive Data Access only to super administrators: □

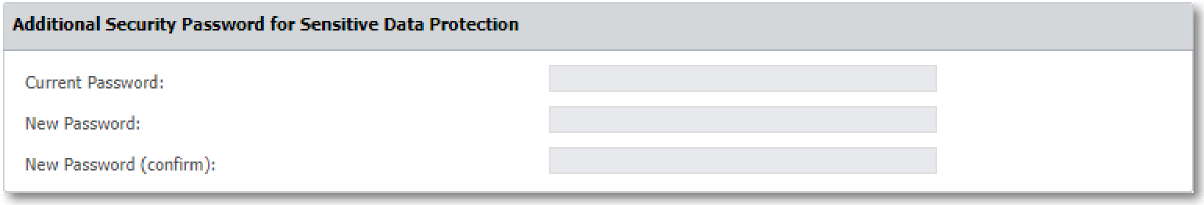
16.9.3. Additional Security Password for Sensitive Data Protection

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.



⚠ **You do not have a security password for sensitive data defined.**



Additional Security Password for Sensitive Data Protection

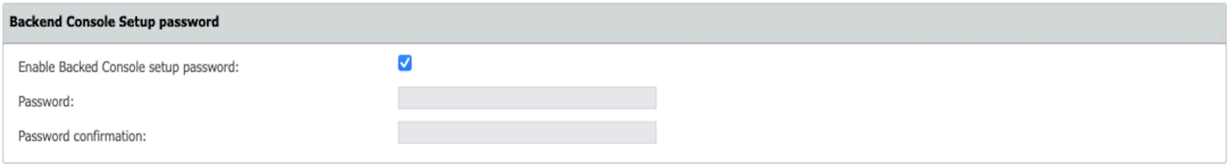
Current Password:

New Password:

New Password (confirm):

16.9.4. Backend Console Setup Password

This feature enhances security by allowing only authorized users to configure critical settings in the Backend Console. To activate this safeguard, navigate to **Security Configuration**, select **System Security**, and enable **Backend Console Setup Password** under the Backend Console Setup section. Save your changes to add an extra layer of security, for a more secure and controlled environment.



Backend Console Setup password

Enable Backed Console setup password: ☑

Password:

Password confirmation:

Important: This feature is designed for Ubuntu 22. With backend password settings enabled and applied:

- On Ubuntu 14 and Ubuntu 18, pressing 'Exit' refreshes the menu without requiring the password again.

- On Ubuntu 22, pressing 'Exit' prompts for the password again.

Note: To enforce password protection, a reboot of the EPP Server appliance is required. Please be aware of this when changing passwords.

Note: ASCII character set is supported for passwords.

16.9.5. Security Password for System Administrator

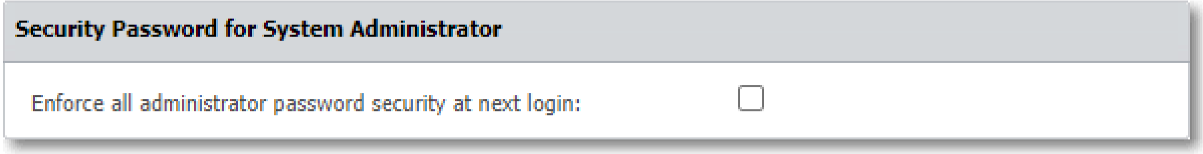
From this section, you can require all administrators to use their security password at the next login session.

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.



Security Password for System Administrator

Enforce all administrator password security at next login: □

16.9.6. 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

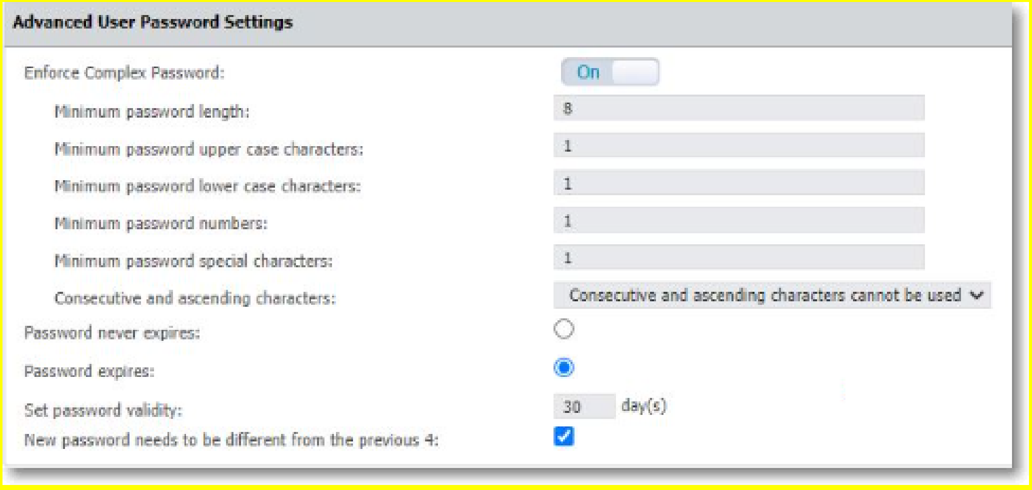
If you enforce a password that expires, provide the following information:

- 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

Enforce Complex Password:	On
Minimum password length:	8
Minimum password upper case characters:	1
Minimum password lower case characters:	1
Minimum password numbers:	1
Minimum password special characters:	1
Consecutive and ascending characters:	Consecutive and ascending characters cannot be used
Password never expires:	○
Password expires:	●
Set password validity:	30 day(s)
New password needs to be different from the previous 4:	☑

16.10. System Settings

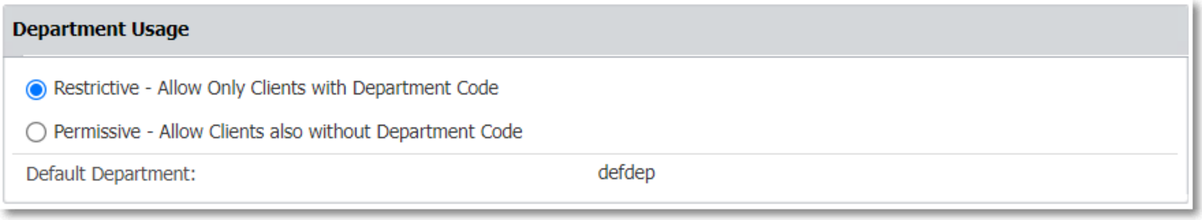
From this section, you can manage general settings that apply to the entire system, several having already been configured from the initial Endpoint Protector Configuration Wizard.

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.



Department Usage

● Restrictive - Allow Only Clients with Department Code

○ Permissive - Allow Clients also without Department Code

Default Department: defdep

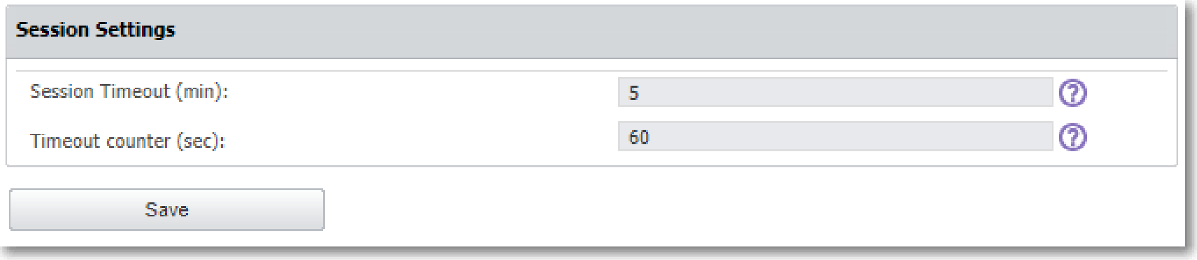
16.10.2. Session Settings

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.



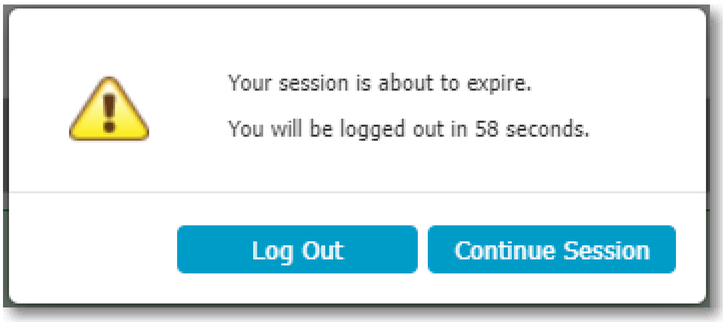
Session Settings

Session Timeout (min): 5

Timeout counter (sec): 60

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.

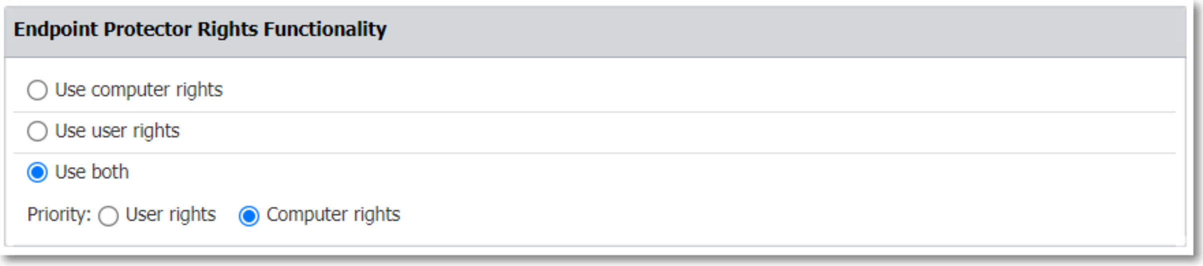


Your session is about to expire.

You will be logged out in 58 seconds.

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.



Endpoint Protector Rights Functionality

○ Use computer rights

○ Use user rights

● Use both

Priority: ○ User rights ● 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.

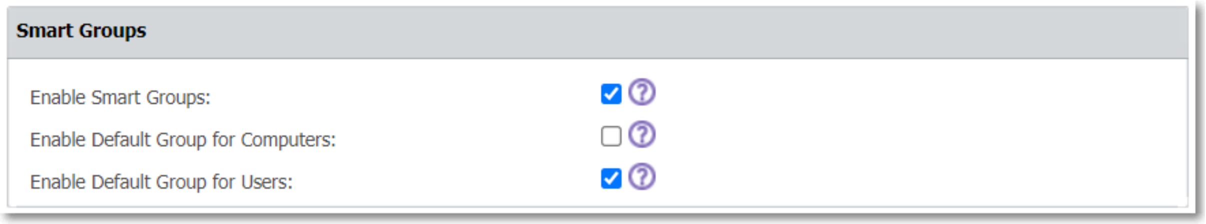
- **Enable Smart Groups** – when this setting is disabled, it will convert Smart Groups to regular groups with no entities assigned and will remove the Default Group for Computers and the Default Group for Users.

- **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.



Smart Groups

Enable Smart Groups: ☑

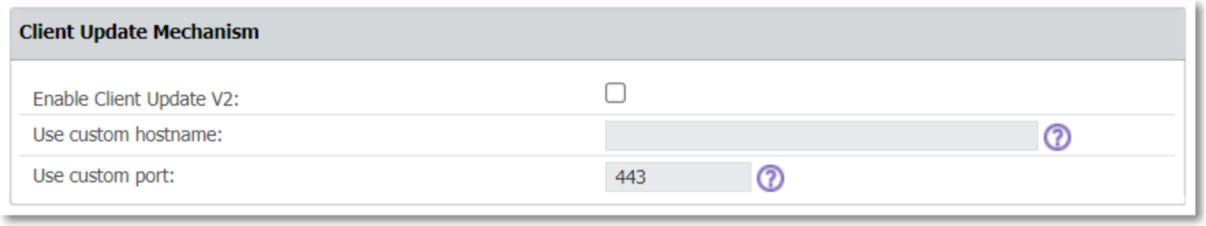
Enable Default Group for Computers: □

Enable 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.



Client Update Mechanism

Enable Client Update V2: □

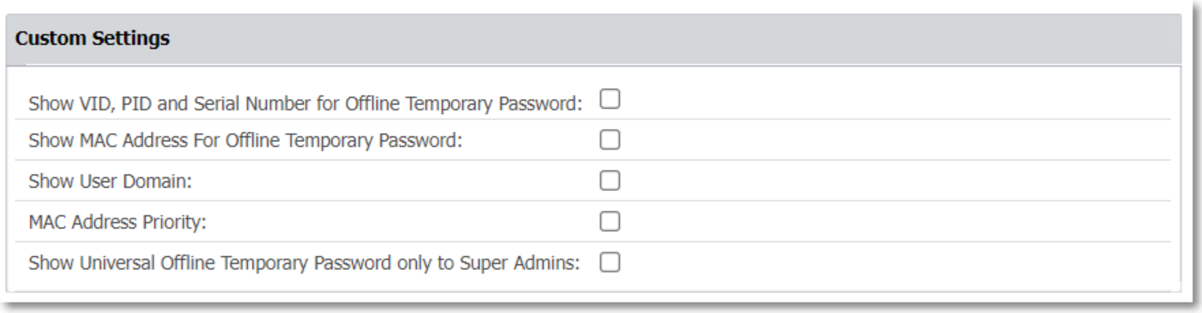
Use custom hostname:

Use custom port: 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**



Custom Settings

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.

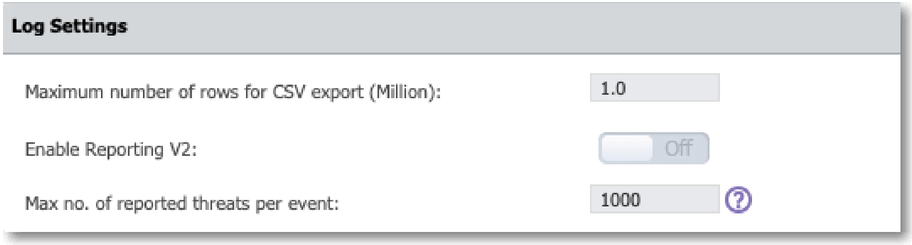
- **Reporting V2** – enabled by default, use this setting to modify the Content Aware Report log structure and display information in **Destination details**, **Email sender,** and **Email subject** columns.

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.



Log Settings

Maximum number of rows for CSV export (Million): 1.0

Enable Reporting V2: Off

Max no. of reported threats per event: 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.

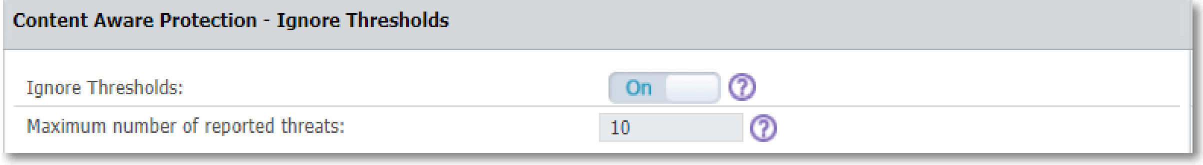
Note: This will increase the amount of logging and potentially affect client and server performance.

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:

User Input	Input Updated

0	1



Content Aware Protection - Ignore Thresholds

Ignore Thresholds: On

Maximum number of reported threats: 10

Limit Reporting Content Aware Protection refers to Report Only policies.

- If enabled, the EPP client will stop reporting threats for a Report Only policy once it finds enough threats to conclude it is satisfied.

The "Content Aware Protection - Ignore Thresholds" toggle refers to Block & Report policies.

- When this toggle is On, scanning will not stop when a block verdict is determined, but will continue to report further threats found in a transfer.
- To limit the number of reported threats in this case, the value of the "*Maximum number of reported threats*" setting can be set to a value greater than zero. The set value is only indicative for the number of reported threats, the actual number reported can be slightly larger.

The '**Global/Threat Threshold**' values in CAP policies will be ignored/overridden by the setting '**Ignore Thresholds**' when the Boolean logic of the CAP policy contains at least one "**AND**" operator. A policy will be satisfied when the Boolean logic (example: see below) is met with one or more matches per identifier.

Eg. (E-mail AND SSN US) OR CC Visa

Example - Scenario 1:

- CAP Policy:
  - Block & Report
  - Threat Threshold: 4
  - Content Detection Rule: (E-mail AND SSN US) OR CC Visa
- Ignore Thresholds: ON
  - Maximum number of reported threats: 10
- Limit Reporting: OFF
- Test File contains
  - E-mail: 2
  - SSN US: 3
  - CC Visa: 6

  - IBAN: 22

In our example, the policy will trigger when the policy is satisfied (Boolean logic), no matter if the ‘**Threat Threshold**’ is met or not due to the ‘**AND**’ operator in the policy. Depending on the data structure in our test file, EPP Client may report different 10 threats to EPP Server

- 2 E-mails + 2 SSN US + 6 CC Visa
- or 1 E-mail + 3 SSN US + 6 CC Visa
- Etc.

Note: Identifiers which are not part of the Boolean logic in a CAP policy will not be reported!

Generally, a CAP policy (Block & Report) will trigger when the Boolean logic of the policy is satisfied. However, with ‘**Ignore Thresholds**’ enabled and with 1+ ‘**AND**’ operator(s) in the policy, the scan engine will ignore the ‘**Threat Threshold**’ setting and continue the scan until the total threat of 10 is reached, no matter if “**Limit Reporting**” (under DEVICE CONTROL - Global Settings) is being enabled or disabled.

Generally, a CAP policy (Report only) will trigger when the Boolean logic of the policy is satisfied. However, with ‘**Ignore Thresholds**’ enabled and with 1+ ‘**AND**’ operator(s) in the policy, the scan engine will ignore the ‘**Threat Threshold**’ setting. If “**Limit Reporting**” (under DEVICE CONTROL - Global Settings) is enabled, the scan continues until the total threat of 10 from setting ‘**Maximum number of reported threats**’ under ‘**Ignore Thresholds**’ is reached.

Generally, a CAP policy (Report only) will trigger when the Boolean logic of the policy is satisfied. However, with ‘**Ignore Thresholds**’ enabled and with 1+ ‘**AND**’ operator(s) in the policy, the scan engine will ignore the ‘**Threat Threshold**’ setting. If “**Limit Reporting**” (under DEVICE CONTROL - Global Settings) is disabled, the scan engine will continue the scan until the entire file is scanned, but will only report 10 threats, set with ‘**Maximum number of reported threats**’ under ‘**Ignore Thresholds**’.

Example - Scenario 2:

- CAP Policy:
  - Block & Report
  - Threat Threshold: 4
  - Content Detection Rule: (E-mail AND SSN US) OR CC Visa
- Ignore Thresholds: ON
  - Maximum number of reported threats: 4
- Limit Reporting: OFF
- Test File contains
  - E-mail: 2
  - SSN US: 3
  - CC Visa: 6

    - IBAN: 22

In our example, the policy will trigger when the policy is satisfied (Boolean logic), no matter if the '**Threat Threshold'** is met or not due to the '**AND**' operator in the policy. Depending on the data structure in our test file, EPP Client may report different 4 threats to EPP Server

- 1 E-mail + 1 SSN US + 2 CC Visa
- or 2 E-mails + 1 SSN US + 1 CC Visa
- Or 1 E-mail + 2 SSN US + 1 CC Visa

Generally, a CAP policy (Block & Report) will trigger when the Boolean logic of the policy is satisfied. However, with '**Ignore Thresholds**' enabled and with 1+ '**AND**' operator(s) in the policy, the scan engine will ignore the '**Threat Threshold**' setting and continue the scan until the total threat of 4 from setting '**Maximum number of reported threats**' is reached, no matter if "**Limit Reporting**" (under DEVICE CONTROL - Global Settings) is being enabled or disabled.

Generally, a CAP policy (Report only) will trigger when the Boolean logic of the policy is satisfied. However, with '**Ignore Thresholds**' enabled and with 1+ '**AND**' operator(s) in the policy, the scan engine will ignore the '**Threat Threshold**' setting. If "**Limit Reporting**" (under DEVICE CONTROL - Global Settings) is enabled, the scan continues until the total threat of 4 from setting **'Maximum number of reported threats**' under '**Ignore Thresholds**' is reached.

Generally, a CAP policy (Report only) will trigger when the Boolean logic of the policy is satisfied. However, with '**Ignore Thresholds**' enabled and with 1+ '**AND**' operator(s) in the policy, the scan engine will ignore the '**Threat Threshold**' setting. If "**Limit Reporting**" (under DEVICE CONTROL - Global Settings) is disabled, the scan engine will continue the scan until the entire file is scanned, but will only report 4 threats, set with **'Maximum number of reported threats**' under '**Ignore Thresholds**'.

Example - Scenario 3:

- CAP Policy:
    - Report Only
    - Threat Threshold: 4
    - Content Detection Rule: (E-mail AND SSN US) OR CC Visa
- Ignore Thresholds: ON
    - Maximum number of reported threats: 10
- Limit Reporting: ON
- Test File contains
    - E-mail: 2
    - SSN US: 3
    - CC Visa: 6

  - IBAN: 22

In our example, the policy will trigger when the policy is satisfied (Boolean logic), meaning that all identifiers reach a '**Threat Threshold**' of at least 1, ignoring setting **'Maximum number of reported threats**' under '**Ignore Thresholds**'. Depending on the data structure in our test file, EPP Client may report the single threats to EPP Server differently

- 1 E-mails + 1 SSN US
- or 1 CC Visa

Generally, a CAP policy (Report only) will trigger when the Boolean logic of the policy is satisfied, meaning that all identifiers reach a '**Threat Threshold**' of at least 1. The scan engine will ignore the '**Maximum number of reported threats**' under '**Ignore Thresholds**', when "**Limit Reporting**" (under DEVICE CONTROL - Global Settings) is <u>enabled.</u> Reporting stops as soon as the policy is satisfied.

Generally, a CAP policy (Report only) will trigger when the Boolean logic of the policy is satisfied, meaning that all identifiers reach a '**Threat Threshold**' of at least 1. The scan engine will consider the '**Maximum number of reported threats**' under '**Ignore Thresholds**', when "**Limit Reporting**" (under DEVICE CONTROL - Global Settings) is <u>disabled.</u> Reporting stops when 10 threats are found.

Example - Scenario 4:

- CAP Policy:
  - Block & Report
  - Threat Threshold: 4
  - Content Detection Rule: E-mail OR SSN US OR CC Visa
- Ignore Thresholds: ON
  - Maximum number of reported threats: 10
- Limit Reporting: OFF
- Test File contains
  - E-mail: 2
  - SSN US: 3
  - CC Visa: 6
  - IBAN: 22

In our example, the policy will trigger when the policy is satisfied (Boolean logic), meaning when at least one identifier (eg. E-mail) reaches a '**Threat Threshold**' of 4, but the scan engine will continue to scan until the total threat of 10 from setting **'Maximum number of reported threats**' under '**Ignore Thresholds**' is reached. Depending on the data structure in our test file, EPP Client may report different 10 threats to EPP Server

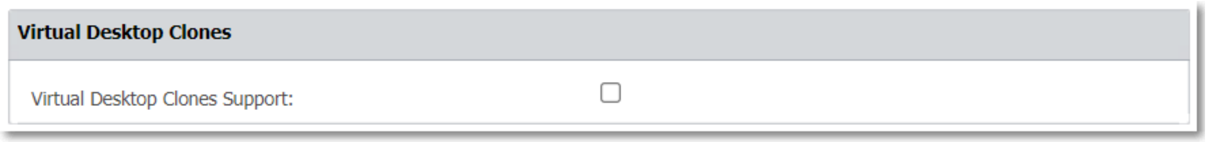
- 2 E-mails + 2 SSN US + 6 CC Visa

- or 1 E-mail + 3 SSN US + 6 CC Visa
- Etc.

Generally, a CAP policy (Block & Report) will trigger when the Boolean logic of the policy is satisfied. However, with ‘**Ignore Thresholds**’ enabled and no ‘**AND**’ operator(s) in the policy, the scan engine will search until the total threat of 10 from setting ‘**Maximum number of reported threats**’ under ‘**Ignore Thresholds**’ is reached.

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.



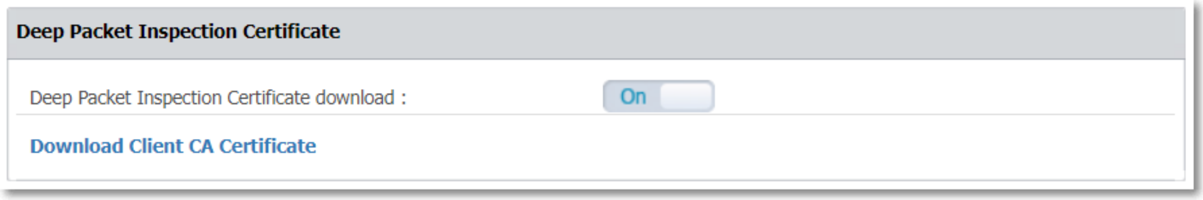
Virtual Desktop Clones

Virtual Desktop Clones Support: □

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.



Deep Packet Inspection Certificate

Deep Packet Inspection Certificate download : On

Download Client CA Certificate

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

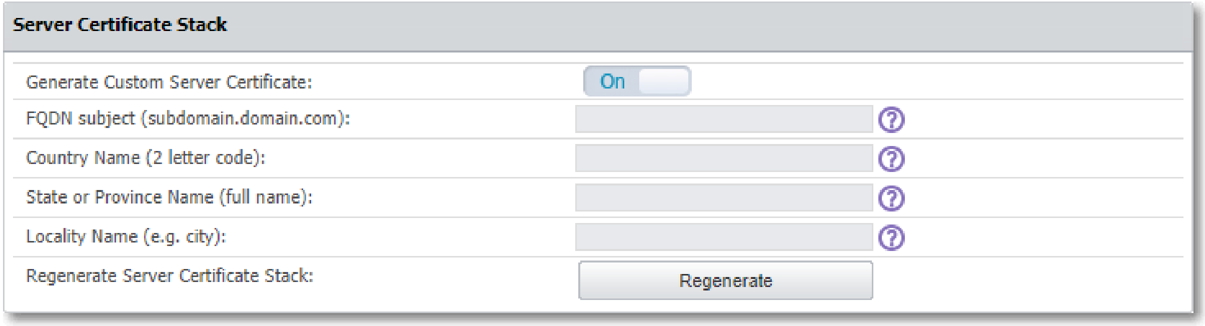
Once you’ve set all the mandatory information, scroll to the bottom of the settings page, click **Save** and then return to the Server Certificate Stack section and click **Regenerate Server Certificate Stack**.

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.

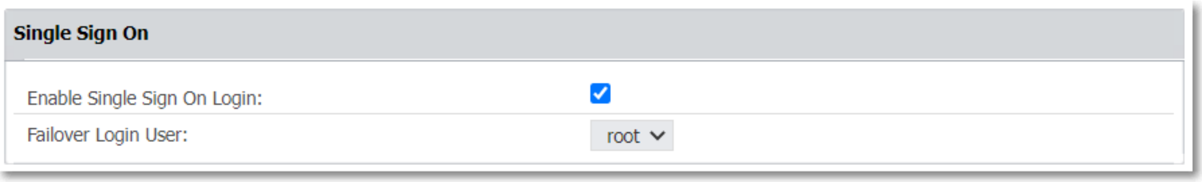


Server Certificate Stack

Generate Custom Server Certificate:	On
FQDN subject (subdomain.domain.com):	
Country Name (2 letter code):	
State or Province Name (full name):	
Locality Name (e.g. city):	
Regenerate Server Certificate Stack:	Regenerate

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.



Single Sign On

Enable Single Sign On Login:	☑
Failover Login User:	root

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:

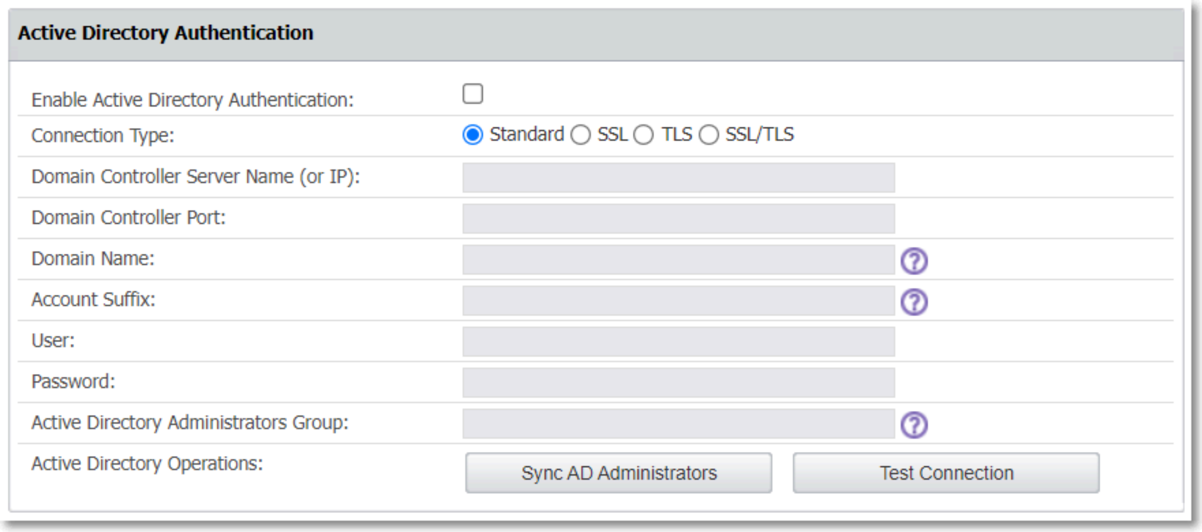
1. Fill in the fields with the required information, considering:
    a. In some cases, you need to add the domain in front of the **username** (domain\username)
    b. **Active Directory Administrators Group** can be synchronized with any other groups of users except for "**primary groups**" which is 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.



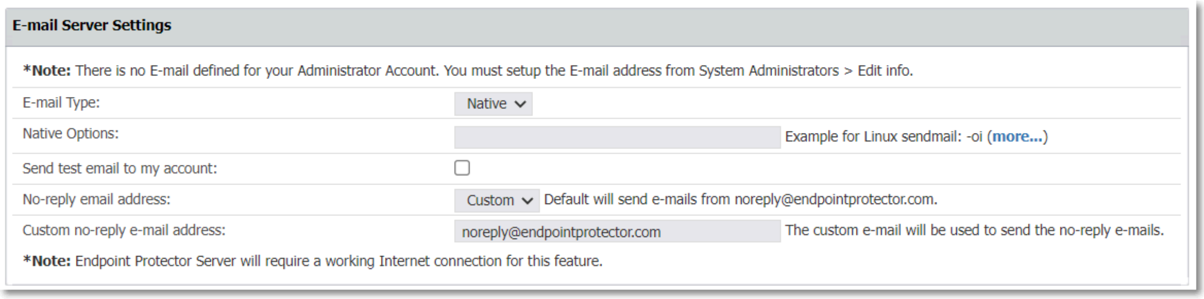
Active Directory Authentication

Enable Active Directory Authentication:	□
Connection Type:	● Standard ○ SSL ○ TLS ○ SSL/TLS
Domain Controller Server Name (or IP):	
Domain Controller Port:	
Domain Name:	
Account Suffix:	
User:	
Password:	
Active Directory Administrators Group:	
Active Directory Operations:	Sync AD Administrators · Test Connection

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.



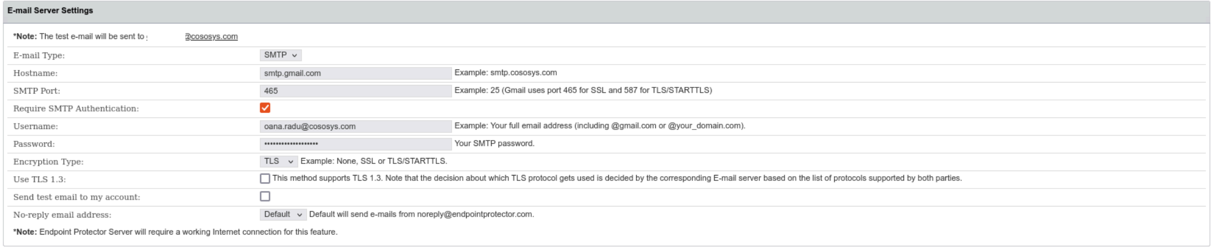
E-mail Server Settings

***Note:** There is no E-mail defined for your Administrator Account. You must setup the E-mail address from System Administrators > Edit info.

E-mail Type:	Native	
Native Options:		Example for Linux sendmail: -oi (**more...**)
Send test email to my account:	□	
No-reply email address:	Custom	Default will send e-mails from noreply@endpointprotector.com.
Custom no-reply e-mail address:	noreply@endpointprotector.com	The custom e-mail will be used to send the no-reply e-mails.

***Note:** Endpoint Protector Server will require a working Internet connection for this feature.

Manage email server settings based on your email type—native or SMTP, with support for TLS 1.3.

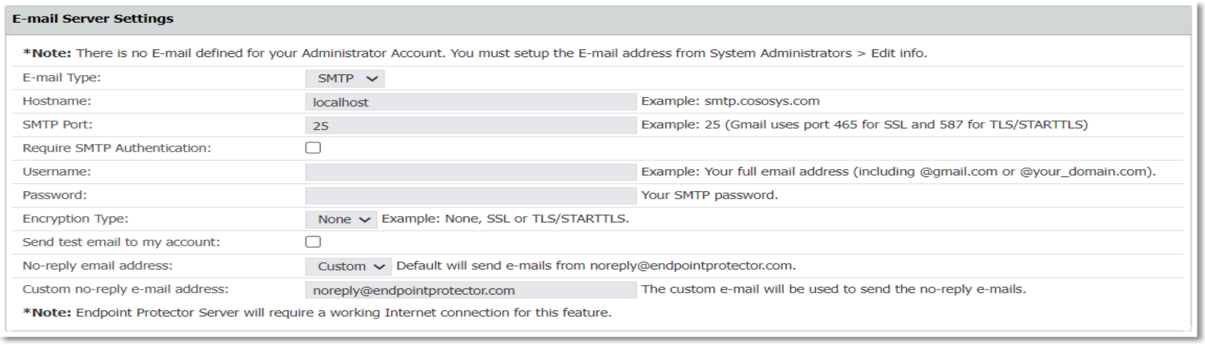


E-mail Server Settings

***Note:** The test e-mail will be sent to @cososys.com

E-mail Type:	SMTP ⌄	
Hostname:	smtp.gmail.com	Example: smtp.cososys.com
SMTP Port:	465	Example: 25 (Gmail uses port 465 for SSL and 587 for TLS/STARTTLS)
Require SMTP Authentication:	☑	
Username:	oana.radu@cososys.com	Example: Your full email address (including @gmail.com or @your_domain.com).
Password:	•••••••••••••••••••	Your SMTP password.
Encryption Type:	TLS ⌄	Example: None, SSL or TLS/STARTTLS.
Use TLS 1.3:	☐	This method supports TLS 1.3. Note that the decision about which TLS protocol gets used is decided by the corresponding E-mail server based on the list of protocols supported by both parties.
Send test email to my account:	☐	
No-reply email address:	Default ⌄	Default will send e-mails from noreply@endpointprotector.com.

***Note:** Endpoint Protector Server will require a working Internet connection for this feature.



E-mail Server Settings

***Note:** There is no E-mail defined for your Administrator Account. You must setup the E-mail address from System Administrators > Edit info.

E-mail Type:	SMTP ⌄	
Hostname:	localhost	Example: smtp.cososys.com
SMTP Port:	25	Example: 25 (Gmail uses port 465 for SSL and 587 for TLS/STARTTLS)
Require SMTP Authentication:	☐	
Username:		Example: Your full email address (including @gmail.com or @your_domain.com).
Password:		Your SMTP password.
Encryption Type:	None ⌄	Example: None, SSL or TLS/STARTTLS.
Send test email to my account:	☐	
No-reply email address:	Custom ⌄	Default will send e-mails from noreply@endpointprotector.com.
Custom no-reply e-mail address:	noreply@endpointprotector.com	The custom e-mail will be used to send the no-reply e-mails.

***Note:** Endpoint Protector Server will require a working Internet connection for this feature.

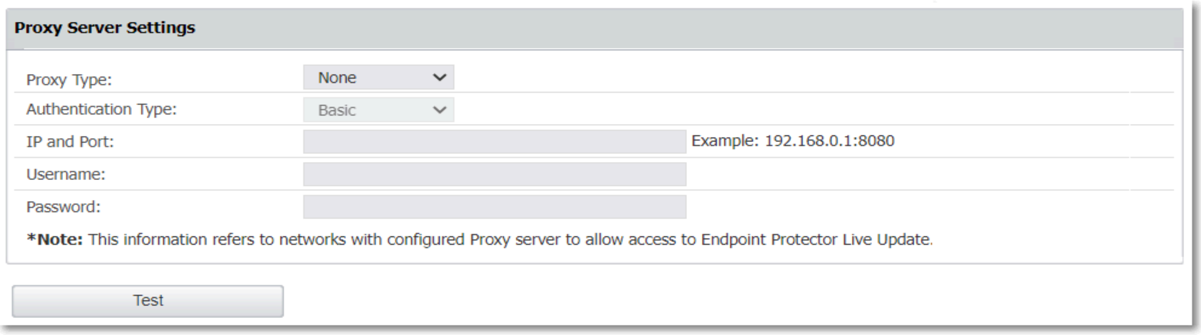
16.10.15. Proxy Server Settings

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.



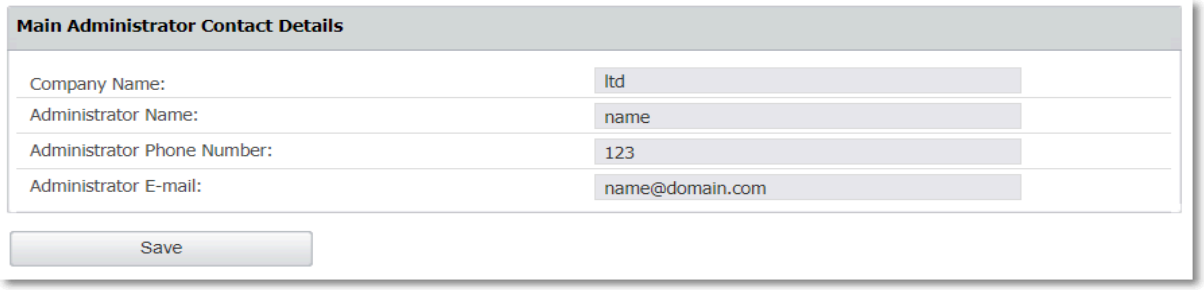
Proxy Server Settings

Proxy Type:	None ⌄	
Authentication Type:	Basic ⌄	
IP and Port:		Example: 192.168.0.1:8080
Username:		
Password:		

***Note:** This information refers to networks with configured Proxy server to allow access to Endpoint Protector Live Update.

16.10.16. Main Administrator Contact Details

Edit contact details for the main administrator and then click **Save** to keep all modifications.

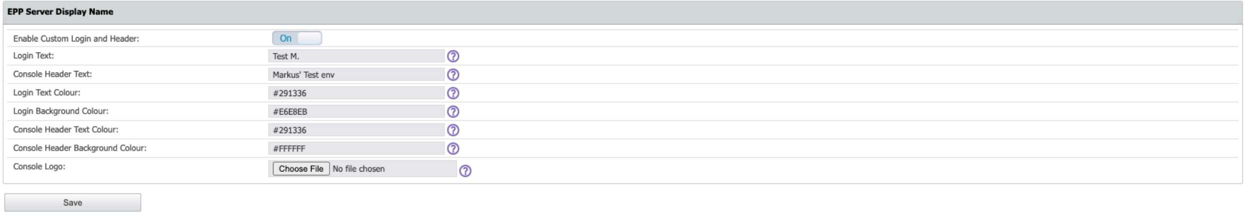


Main Administrator Contact Details

Company Name:	ltd
Administrator Name:	name
Administrator Phone Number:	123
Administrator E-mail:	name@domain.com

16.10.17. EPP Server Display Name

EPP users have the capability to visually differentiate environments within the Endpoint Protector UI. This feature enables users to add custom text above the Endpoint Protector logo on the login page and alongside the logo in the Endpoint Protector header. You can customize text and upload a custom logo for further personalization. These visual cues are designed to prevent incidents like unintentional modifications on the wrong environment

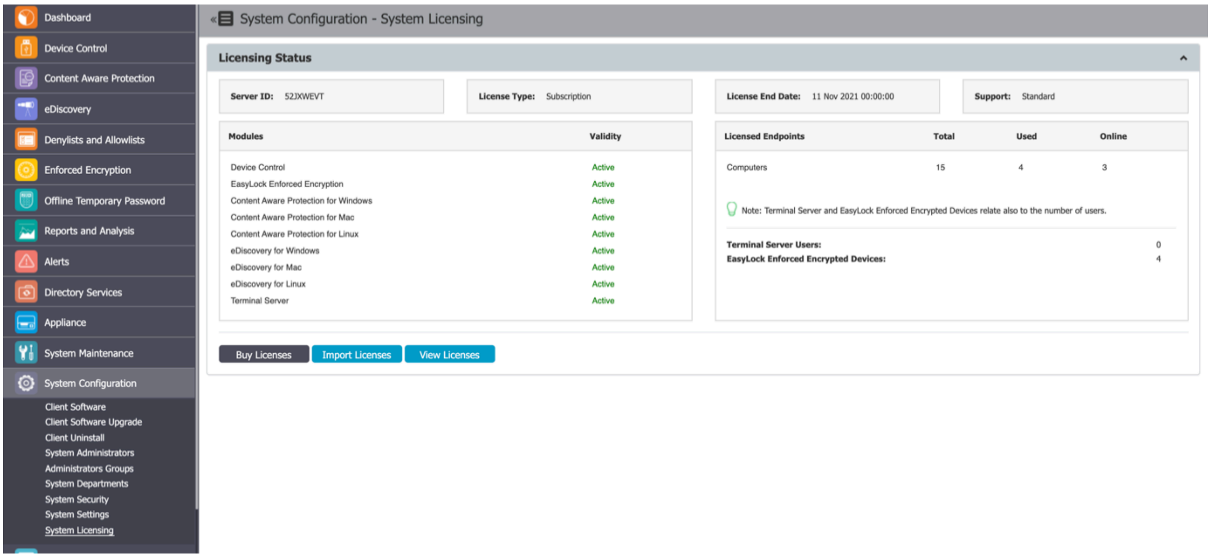


EPP Server Display Name

Enable Custom Login and Header:	On
Login Text:	Test M.
Console Header Text:	Markus' Test env
Login Text Colour:	#291336
Login Background Colour:	#E6E8EB
Console Header Text Colour:	#291336
Console Header Background Colour:	#FFFFFF
Console Logo:	Choose File No file chosen

16.11. System Licensing

From this section, you can manage and have a complete overview of the Endpoint Protector licensing status.



System Configuration - System Licensing

Licensing Status

Server ID: 52JXWEVT

License Type: Subscription

License End Date: 11 Nov 2021 00:00:00

Support: Standard

Modules	Validity
Device Control	Active
EasyLock Enforced Encryption	Active
Content Aware Protection for Windows	Active
Content Aware Protection for Mac	Active
Content Aware Protection for Linux	Active
eDiscovery for Windows	Active
eDiscovery for Mac	Active
eDiscovery for Linux	Active
Terminal Server	Active

Licensed Endpoints	Total	Used	Online
Computers	15	4	3

Note: Terminal Server and EasyLock Enforced Encrypted Devices relate also to the number of users.

Terminal Server Users:	0
EasyLock Enforced Encrypted Devices:	4

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.

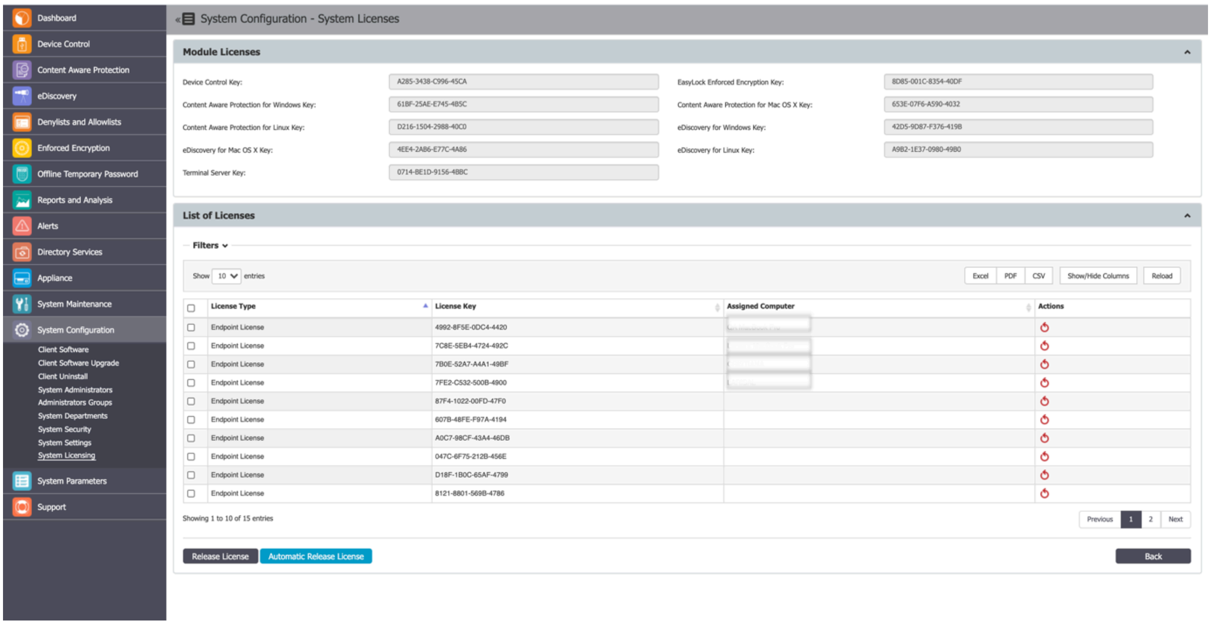
By enabling the **Free Trial** option, you will automatically enable all modules for 50 computers. The endpoint licenses will be assigned on a **first-in-first-served** basis.

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.



Module Licenses

Device Control Key:	A285-3438-C996-45CA	EasyLock Enforced Encryption Key:	8D85-001C-8354-40DF
Content Aware Protection for Windows Key:	61BF-25AE-E745-4B5C	Content Aware Protection for Mac OS X Key:	653E-07F6-A590-4032
Content Aware Protection for Linux Key:	D216-1504-2988-40C0	eDiscovery for Windows Key:	42D5-9D87-F376-419B
eDiscovery for Mac OS X Key:	4EE4-2AB6-E77C-4A86	eDiscovery for Linux Key:	A9B2-1E37-0980-49B0
Terminal Server Key:	0714-BE1D-9156-4BBC		

List of Licenses

Filters

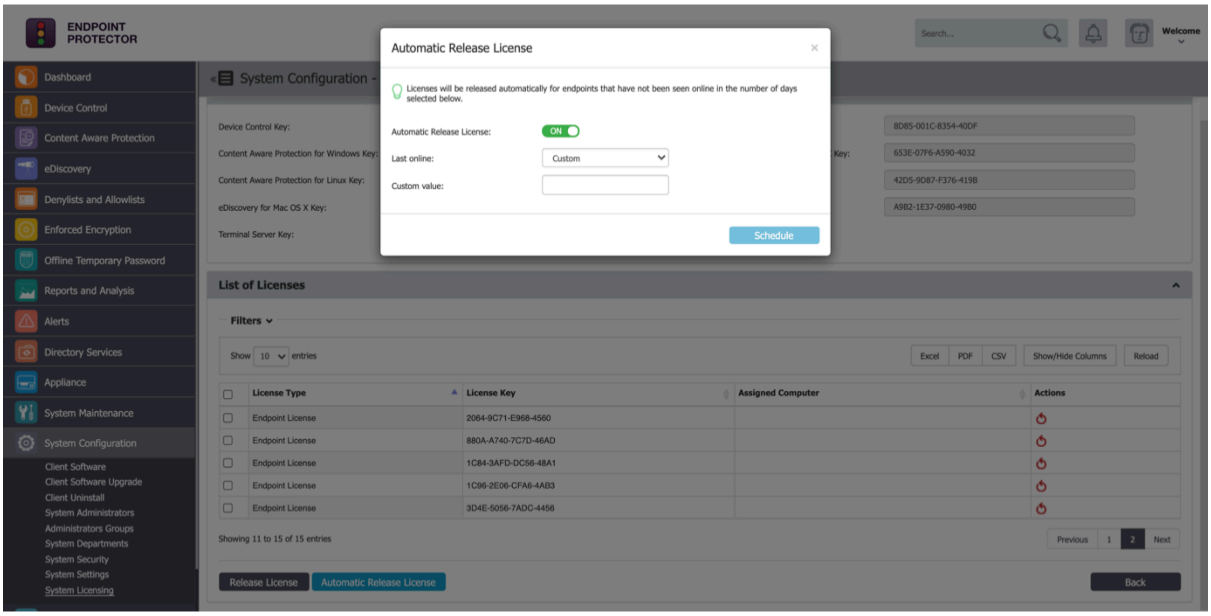
Show 10 entries — Excel | PDF | CSV | Show/Hide Columns | Reload

☐	License Type	License Key	Assigned Computer	Actions
☐	Endpoint License	4992-8F5E-0DC4-4420	[redacted]	⥀
☐	Endpoint License	7C8E-5EB4-4724-492C	[redacted]	⥀
☐	Endpoint License	7B0E-52A7-A4A1-49BF	[redacted]	⥀
☐	Endpoint License	7FE2-C532-500B-4900	[redacted]	⥀
☐	Endpoint License	87F4-1022-00FD-47F0		⥀
☐	Endpoint License	607B-48FE-F97A-4194		⥀
☐	Endpoint License	A0C7-98CF-43A4-46DB		⥀
☐	Endpoint License	047C-6F75-212B-456E		⥀
☐	Endpoint License	D18F-1B0C-65AF-4799		⥀
☐	Endpoint License	8121-8801-569B-4786		⥀

Showing 1 to 10 of 15 entries — Previous 1 2 Next

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).



Automatic Release License ×

Licenses will be released automatically for endpoints that have not been seen online in the number of days selected below.

Automatic Release License: ON

Last online: Custom

Custom value:

Device Control Key:
Content Aware Protection for Windows Key:
Content Aware Protection for Linux Key:
eDiscovery for Mac OS X Key:
Terminal Server Key:

8D85-001C-8354-40DF
653E-07F6-A590-4032
42D5-9D87-F376-419B
A9B2-1E37-0980-49B0

List of Licenses

Filters

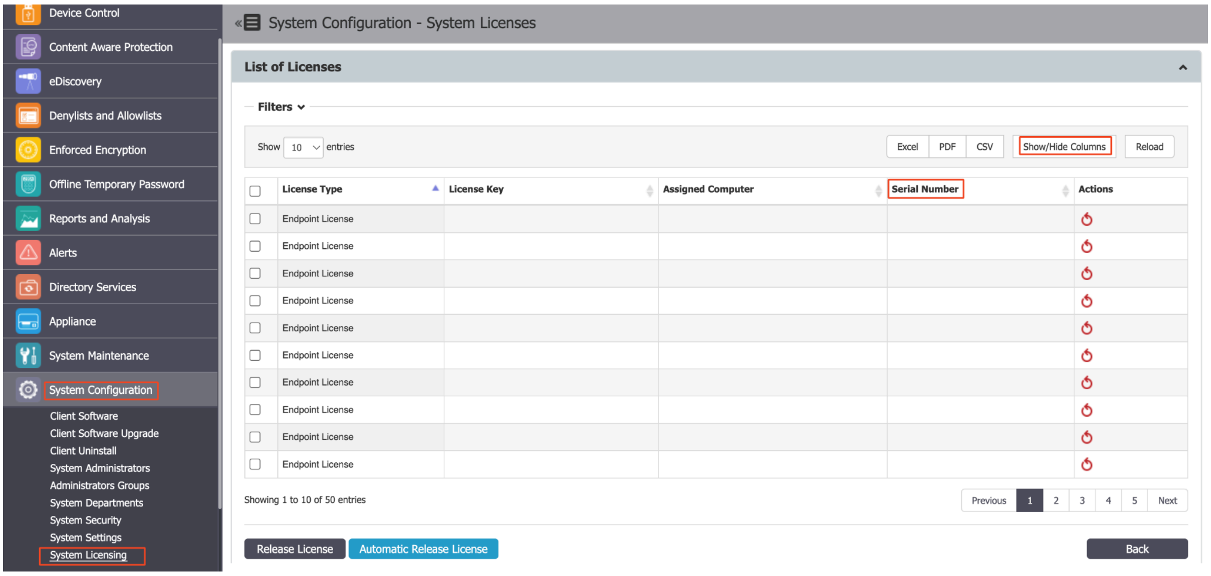
Show 10 entries — Excel | PDF | CSV | Show/Hide Columns | Reload

☐	License Type	License Key	Assigned Computer	Actions
☐	Endpoint License	2064-9C71-E968-4560		⥀
☐	Endpoint License	880A-A740-7C7D-46AD		⥀
☐	Endpoint License	1C84-3AFD-DC56-48A1		⥀
☐	Endpoint License	1C96-2E06-CFA6-4AB3		⥀
☐	Endpoint License	3D4E-5056-7ADC-4456		⥀

Showing 11 to 15 of 15 entries — Previous 1 2 Next

To streamline license management within **System Configuration**, navigate to **System Licensing** and discover the **Serial Number** field under the **View Licenses** section. In the licensing table, you will find a **Serial Number** column. To customize your view, use the **Show/Hide Columns** button, including a checkbox for "Serial Number" (defaulted to 'show'). This resolves issues with identical computer names and facilitates more effective management via Serial Number integration, reinforced by MachineUUIDs.

Note: If a computer's Serial Number is absent, it will be substituted with MachineUUID to ensure endpoint machine reliability, now featuring in the license page column across all OS platforms.

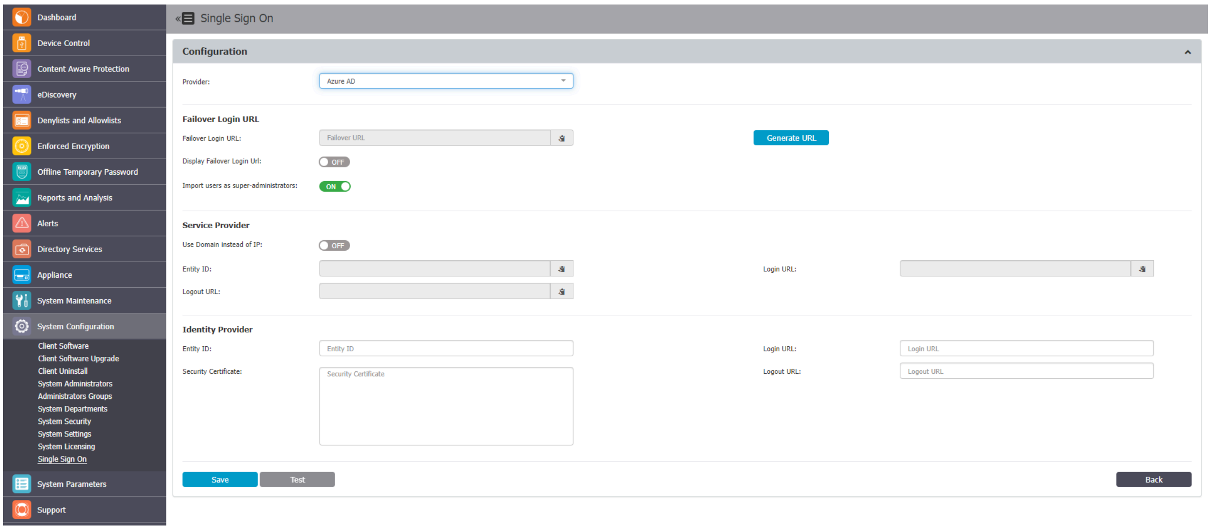


☐	License Type	License Key	Assigned Computer	Serial Number	Actions
☐	Endpoint License				⏻
☐	Endpoint License				⏻
☐	Endpoint License				⏻
☐	Endpoint License				⏻
☐	Endpoint License				⏻
☐	Endpoint License				⏻
☐	Endpoint License				⏻
☐	Endpoint License				⏻
☐	Endpoint License				⏻
☐	Endpoint License				⏻

Showing 1 to 10 of 50 entries

16.12. Single Sign On

Single Sign On allows you to log in the Endpoint Protector Server with Azure AD and OKTA.



Provider: Azure AD

Failover Login URL

Failover Login URL: Failover URL

Display Failover Login Url: OFF

Import users as super-administrators: ON

Service Provider

Use Domain instead of IP: OFF

Entity ID:

Login URL:

Logout URL:

Identity Provider

Entity ID: Entity ID

Login URL: Login URL

Security Certificate: Security Certificate

Logout URL: Logout URL

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.

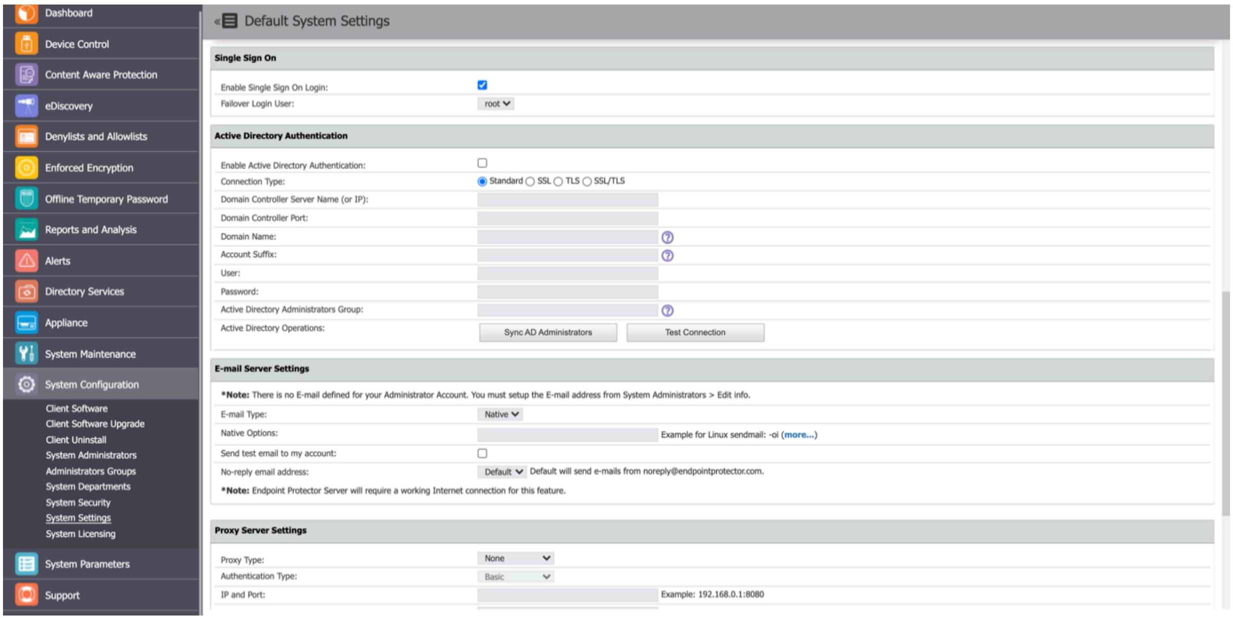
Note: You can provide Super Administrator status to all imported users by enabling the **Import users as super administrators** setting.

- **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.



Default System Settings

Single Sign On

Enable Single Sign On Login: ☑
Failover Login User: root

Active Directory Authentication

Enable Active Directory Authentication: □
Connection Type: ● Standard ○ SSL ○ TLS ○ SSL/TLS
Domain Controller Server Name (or IP):
Domain Controller Port:
Domain Name:
Account Suffix:
User:
Password:
Active Directory Administrators Group:
Active Directory Operations:

E-mail Server Settings

***Note:** There is no E-mail defined for your Administrator Account. You must setup the E-mail address from System Administrators > Edit info.

E-mail Type: Native
Native Options: Example for Linux sendmail: -oi (more...)
Send test email to my account: □
No-reply email address: Default Default will send e-mails from noreply@endpointprotector.com.

***Note:** Endpoint Protector Server will require a working Internet connection for this feature.

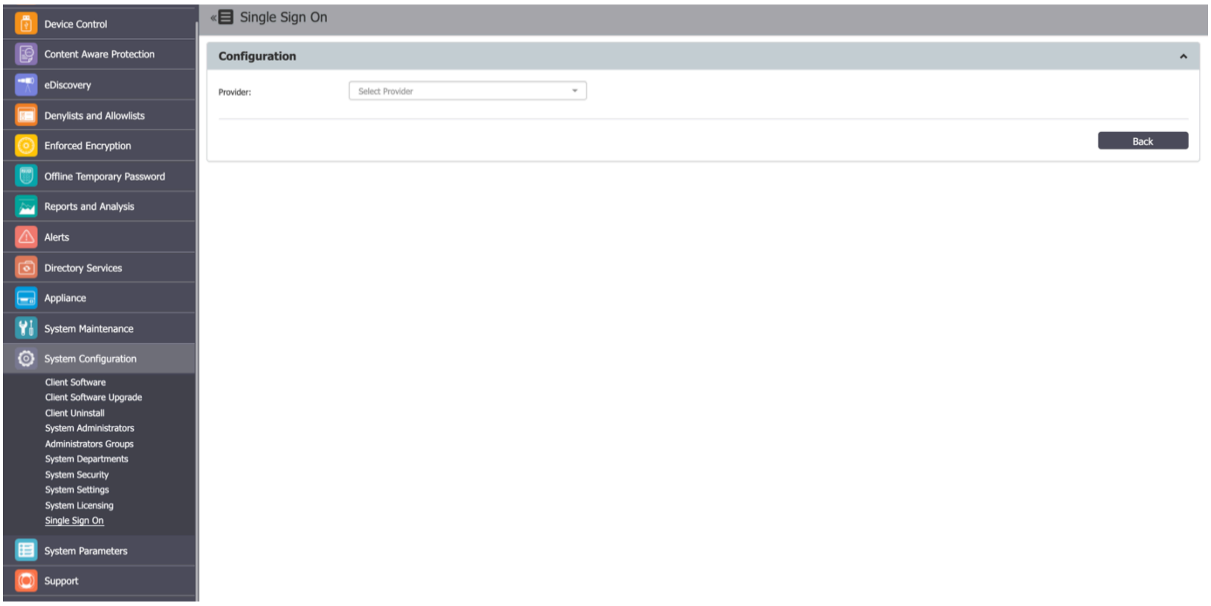
Proxy Server Settings

Proxy Type: None
Authentication Type: Basic
IP and Port: Example: 192.168.0.1:8080

After the above steps have been completed, a Single Sign On subsection is displayed in the System Configuration section.

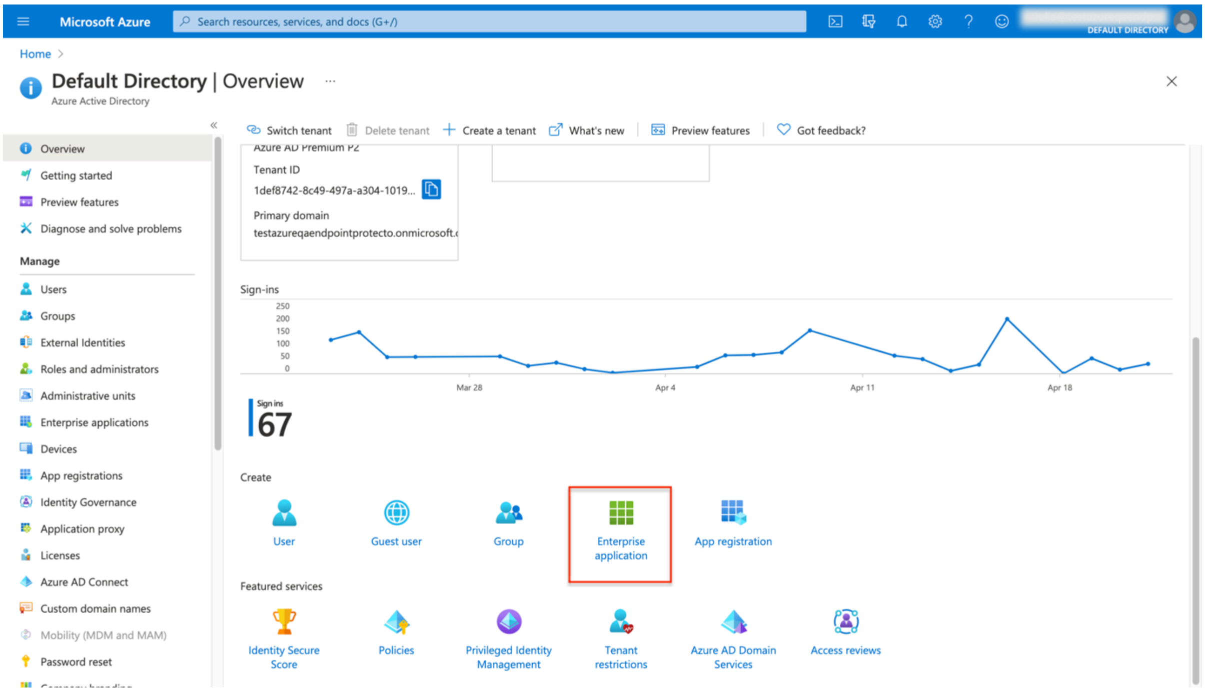
Note: The Failover Login User you selected cannot be deleted from Endpoint Protector Server while it is selected. Single Sign On cannot be activated without a Failover Login User.

3. Select the **Provider** to view Single Sign On subsections.



Provider: Select Provider

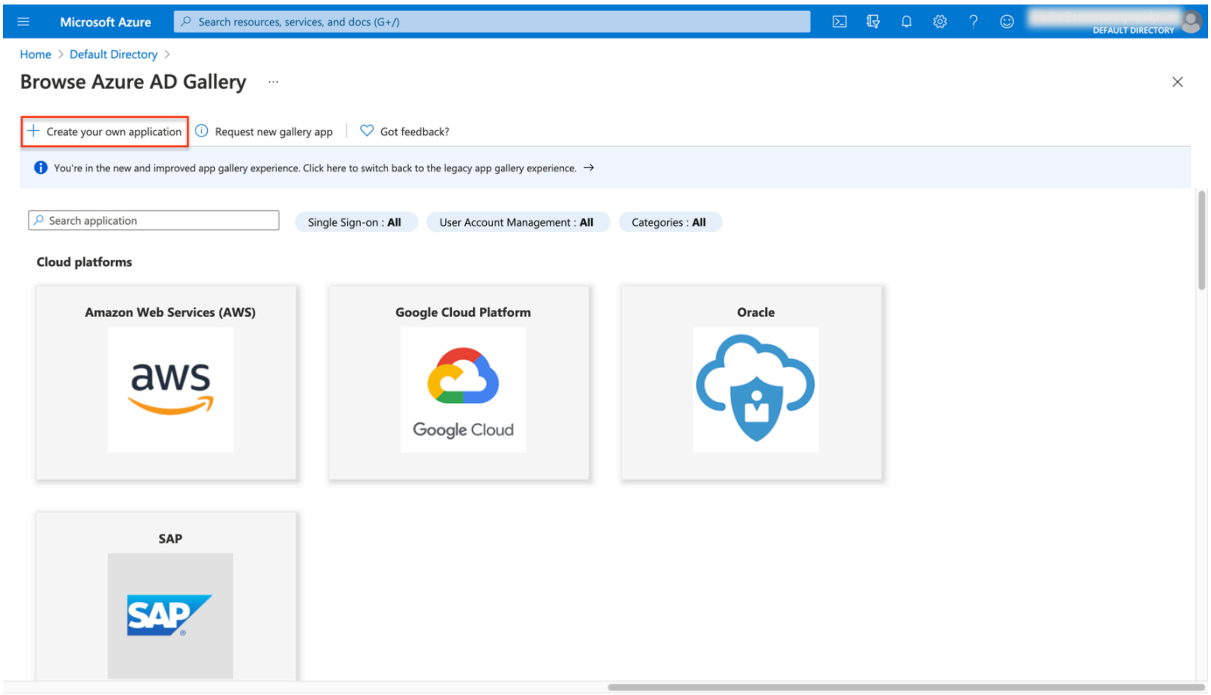
4. Go to **portal.azure.com** and login.
5. Go to **Azure Active Directory**.
6. Create a **New Enterprise Application**:
   a. Add a **New Application;**
   b. Click **Create your own application**;
   c. Give the application a name;
   d. Select **Integrate any other application you don’t find in the gallery**;
   e. Click **Create**.



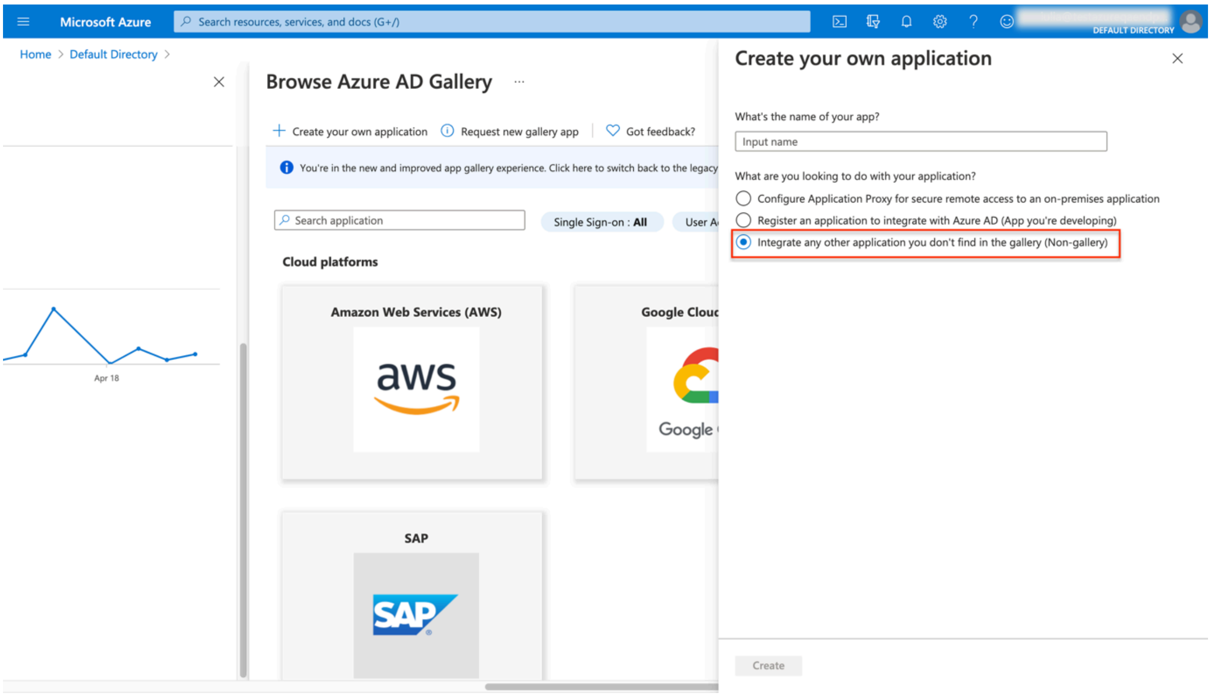
Azure AD Premium P2

Tenant ID
1def8742-8c49-497a-a304-1019...

Primary domain
testazureqaendpointprotecto.onmicrosoft.c



You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →



Create your own application

What's the name of your app?

Input name

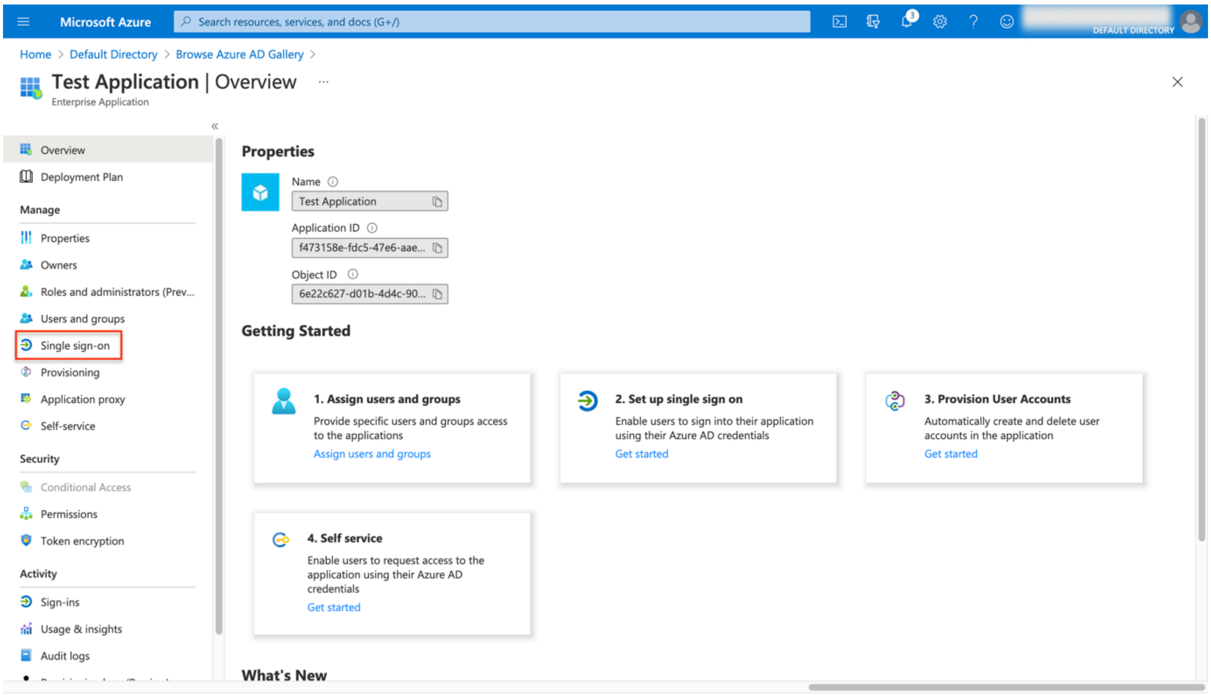
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

7. From the left-hand menu go to **Single Sign On** and then select the **SAML** method.



Test Application | Overview

Enterprise Application

Properties

Name: Test Application

Application ID: f473158e-fdc5-47e6-aae...

Object ID: 6e22c627-d01b-4d4c-90...

Getting Started

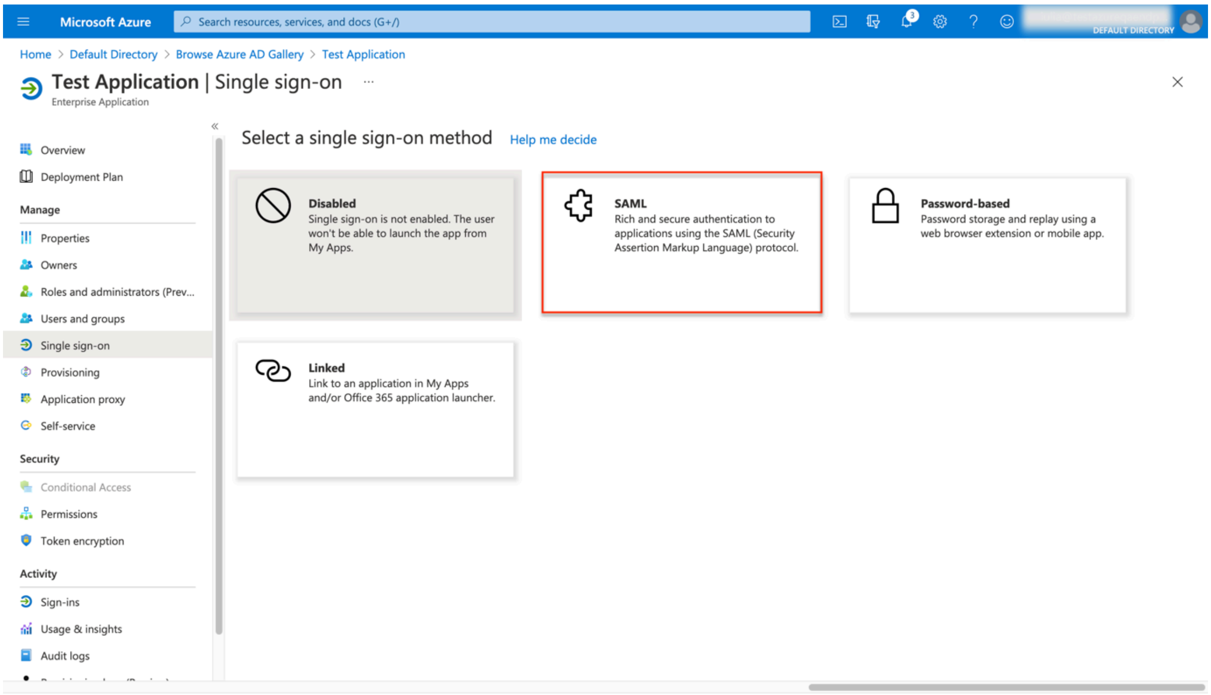
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

What's New



Test Application | Single sign-on

Enterprise Application

Select a single sign-on method   Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

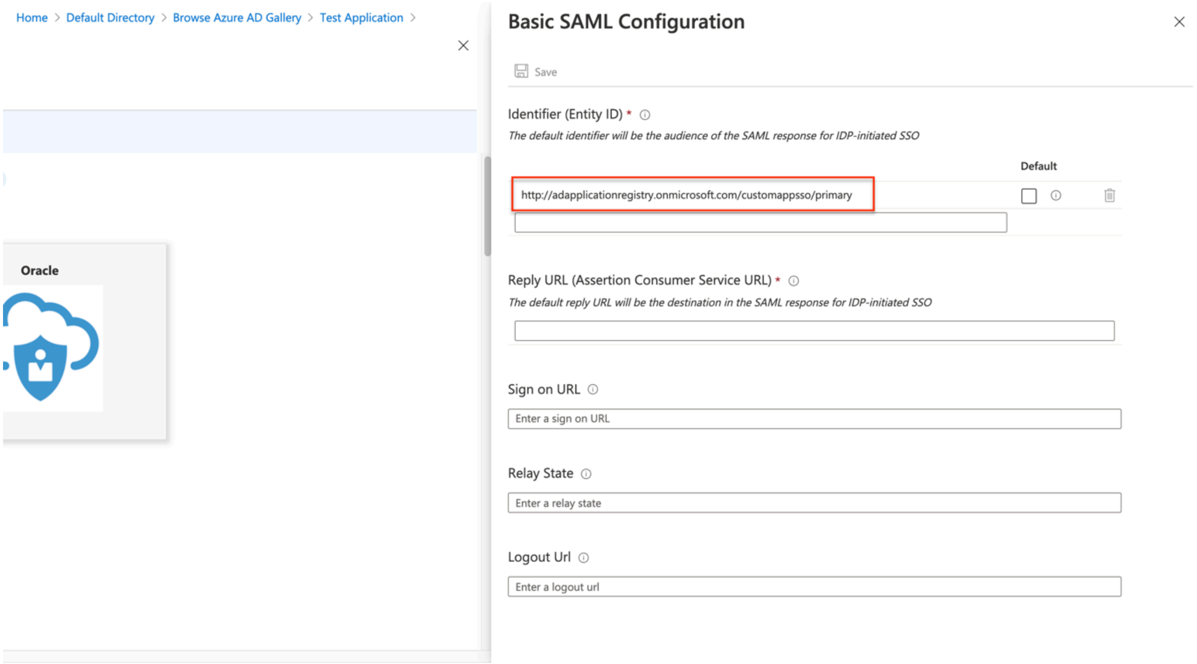
SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

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).



Home > Default Directory > Browse Azure AD Gallery > Test Application >
Oracle

Basic SAML Configuration

Save

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

http://adapplicationregistry.onmicrosoft.com/customappsso/primary □

Reply URL (Assertion Consumer Service URL) *

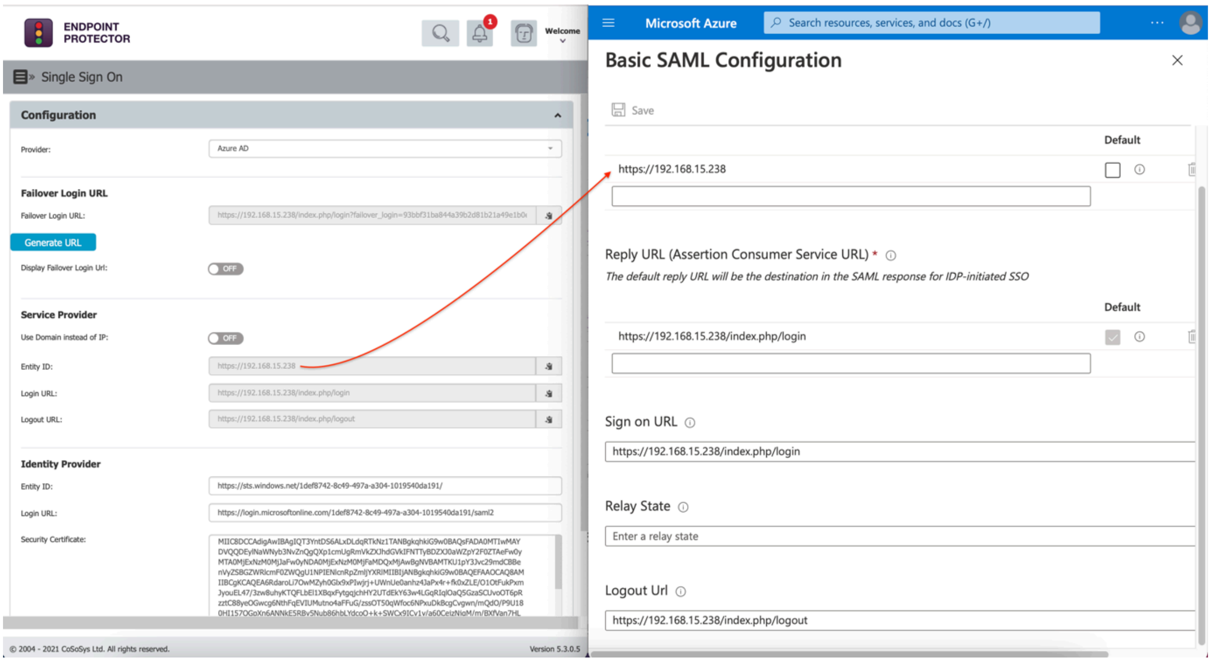
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Sign on URL: Enter a sign on URL

Relay State: Enter a relay state

Logout Url: Enter a logout url

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**.



Configuration

Provider: Azure AD

Failover Login URL

Failover Login URL: https://192.168.15.238/index.php/login?failover_login=93bbf31ba844a39b2d81b21a49e1b0

Generate URL

Display Failover Login Url: OFF

Service Provider

Use Domain instead of IP: OFF

Entity ID: https://192.168.15.238

Login URL: https://192.168.15.238/index.php/login

Logout URL: https://192.168.15.238/index.php/logout

Identity Provider

Entity ID: https://sts.windows.net/1def8742-8c49-497a-a304-1019540da191/

Login URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2

Security Certificate:

```
MIIC8DCCAdigAwIBAgIQT3YntDS6ALxDLdqRTkNz1TANBgkqhkiG9w0BAQsFADA0MTIwMAY
DVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0y
MTA0MjExNzM0MjJaFw0yNDA0MjExNzM0MjFaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBe
nVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM
IIBCgKCAQEA6RdaroLi7OwMZyh0Glx9xPIwjrj+UWnUe0anhz4JaPx4r+fk0xZLE/O1OtFukPxm
JyouEL47/3zw8uhyKTQFLbEl1XBqxFytgqjchHY2UTdEkY63w4LGqRIqlOaQ5GzaSCUvoOT6pR
zztC88yeOGwcg6NthFqEVIUMutno4aFFuG/zssOT50qWfoc6NPxuDkBcgCvgwn/mQdO/P9U18
0HI157OGoXn6ANNkE5RBv5Nub86hbLYdcoO+k+SWCx9ICv1v/a60CeizNioM/m/BXfVan7HL
```

© 2004 - 2021 CoSoSys Ltd. All rights reserved. Version 5.3.0.5

Basic SAML Configuration

Save

Default

https://192.168.15.238 □

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

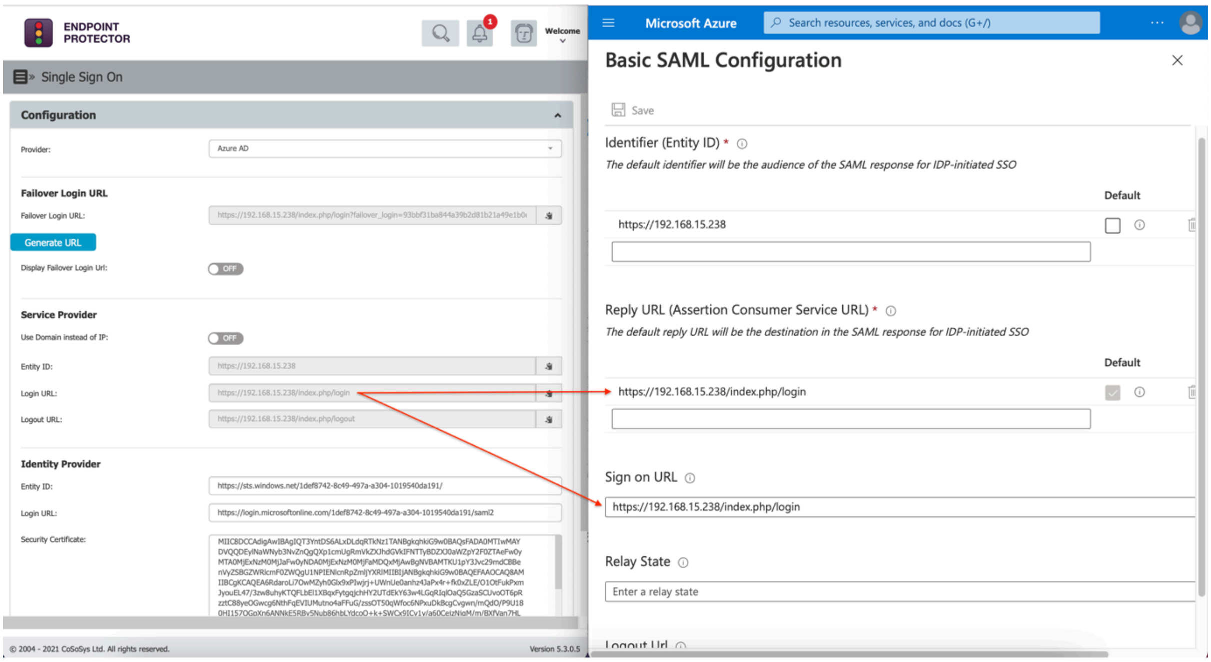
https://192.168.15.238/index.php/login ☑

Sign on URL: https://192.168.15.238/index.php/login

Relay State: Enter a relay state

Logout Url: https://192.168.15.238/index.php/logout

    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.



Configuration

Provider: Azure AD

Failover Login URL

Failover Login URL: https://192.168.15.238/index.php/login?failover_login=93bbf31ba844a39b2d81b21a49e1b0

Display Failover Login Url: OFF

Service Provider

Use Domain instead of IP: OFF

Entity ID: https://192.168.15.238

Login URL: https://192.168.15.238/index.php/login

Logout URL: https://192.168.15.238/index.php/logout

Identity Provider

Entity ID: https://sts.windows.net/1def8742-8c49-497a-a304-1019540da191/

Login URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2

Security Certificate:

```
MIIC8DCCAdigAwIBAgIQT3YntDS6ALxDLdqRTkNz1TANBgkqhkiG9w0BAQsFADA0MTIwMAY
DVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0y
MTA0MjExNzM0MjJaFw0yNDA0MjExNzM0MjFaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBe
nVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM
IIBCgKCAQEA6RdaroLi7OwMZyh0Glx9xPIwjrj+UWnUe0anhz4JaPx4r+fk0xZLE/O1OtFukPxm
JyouEL47/3zw8uhyKTQFLbEl1XBqxFytgqjchHY2UTdEkY63w4LGqRIqlOaQ5GzaSCUvoOT6pR
zztC88yeOGwcg6NthFqEVIUMutno4aFFuG/zssOT50qWfoc6NPxuDkBcgCvgwn/mQdO/P9U18
0HI157OGoXn6ANNkE5RBv5Nub86hbLYdcoO+k+SWCx9ICv1v/a60CeizNioM/m/BXfVan7HL
```

© 2004 - 2021 CoSoSys Ltd. All rights reserved.
Version 5.3.0.5
Microsoft Azure
Search resources, services, and docs (G+/)

Basic SAML Configuration

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

	Default
https://192.168.15.238	☐

Reply URL (Assertion Consumer Service URL) *

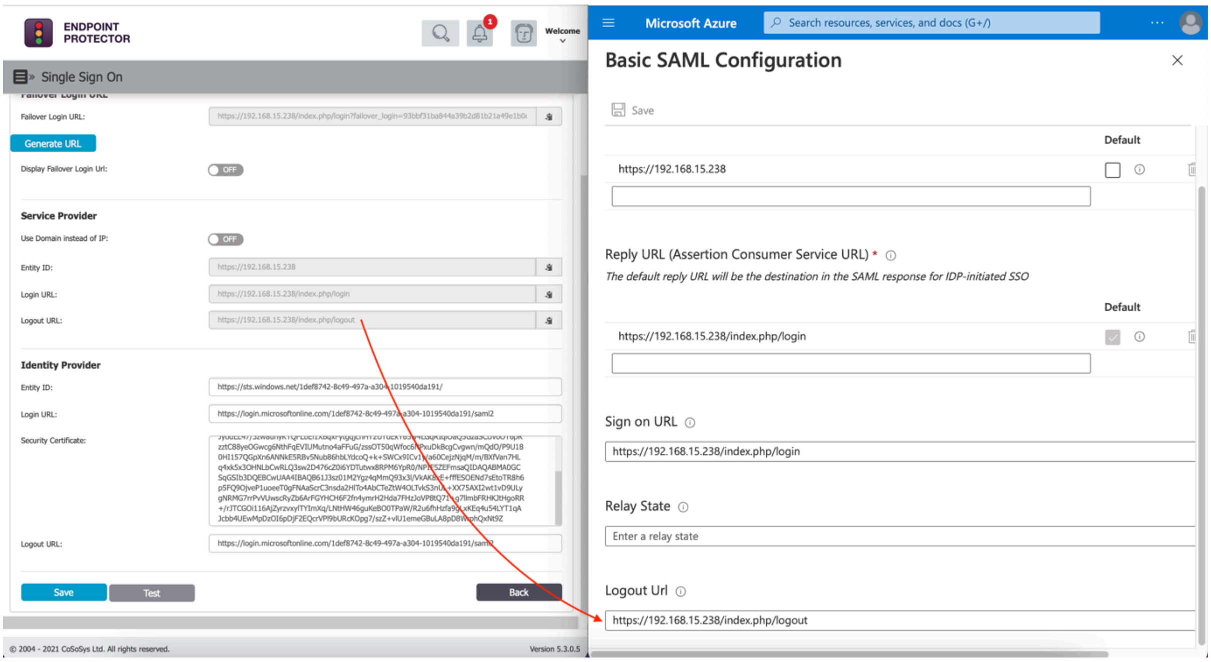
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default
https://192.168.15.238/index.php/login	☑

Sign on URL: https://192.168.15.238/index.php/login

Relay State: Enter a relay state

Logout Url



Failover Login URL: https://192.168.15.238/index.php/login?failover_login=93bbf31ba844a39b2d81b21a49e1b0

Display Failover Login Url: OFF

Service Provider

Use Domain instead of IP: OFF

Entity ID: https://192.168.15.238

Login URL: https://192.168.15.238/index.php/login

Logout URL: https://192.168.15.238/index.php/logout

Identity Provider

Entity ID: https://sts.windows.net/1def8742-8c49-497a-a304-1019540da191/

Login URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2

Security Certificate:

Logout URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2

Save
Test
Back
© 2004 - 2021 CoSoSys Ltd. All rights reserved.
Version 5.3.0.5
Microsoft Azure
Search resources, services, and docs (G+/)

Basic SAML Configuration

	Default
https://192.168.15.238	☐

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

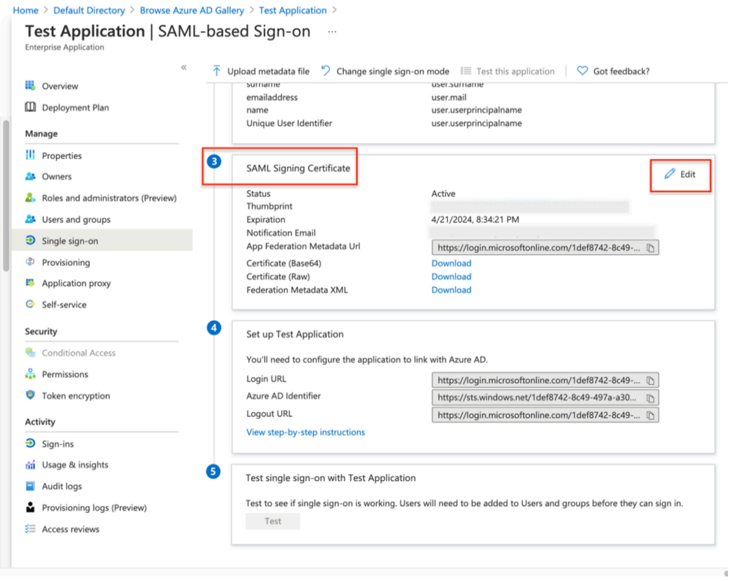
	Default
https://192.168.15.238/index.php/login	☑

Sign on URL: https://192.168.15.238/index.php/login

Relay State: Enter a relay state

Logout Url: https://192.168.15.238/index.php/logout

11. Save the settings without testing Single Sign On yet.
12. Go to Step 3 from the page, **SAML Signing Certificate** and click **Edit**.



Home > Default Directory > Browse Azure AD Gallery > Test Application >

Test Application | SAML-based Sign-on ···

Enterprise Application

surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	[redacted]
Expiration	4/21/2024, 8:34:21 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/1def8742-8c49-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Test Application

You'll need to configure the application to link with Azure AD.

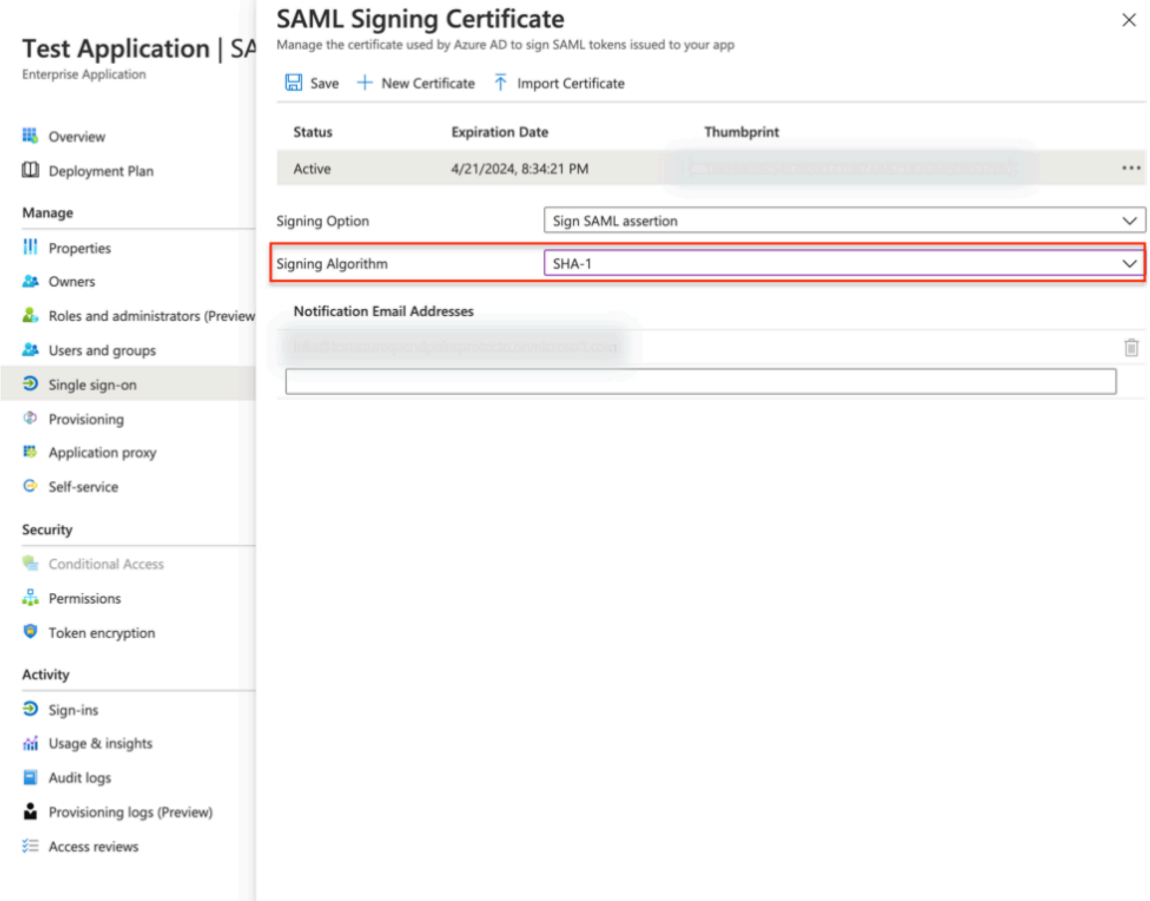
Login URL	https://login.microsoftonline.com/1def8742-8c49-...
Azure AD Identifier	https://sts.windows.net/1def8742-8c49-497a-a30...
Logout URL	https://login.microsoftonline.com/1def8742-8c49-...

View step-by-step instructions

5 Test single sign-on with Test Application

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

13. Change **Signing Algorithm** to **SHA-1** and click **Save**.



SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Status	Expiration Date	Thumbprint
Active	4/21/2024, 8:34:21 PM	[redacted]

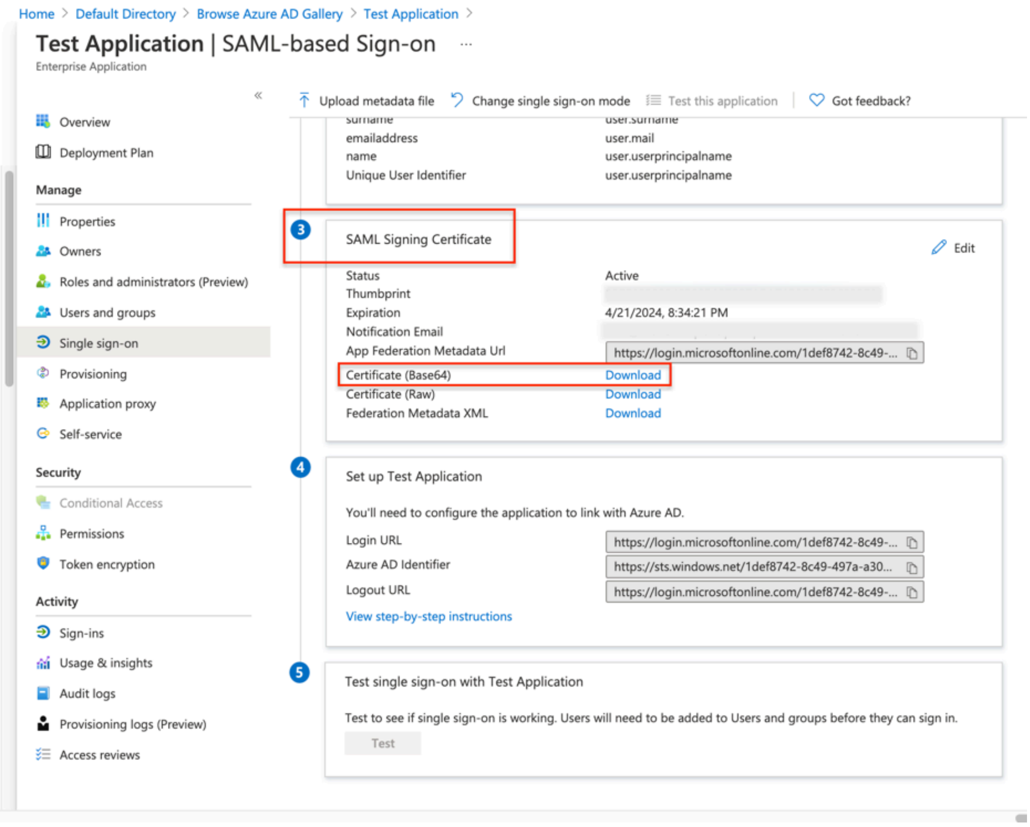
Signing Option: Sign SAML assertion

Signing Algorithm: SHA-1

Notification Email Addresses

[redacted]

14. From Step 3, **SAML Signing Certificate**, download **Certificate (Base64).**



surname user.surname
emailaddress user.mail
name user.userprincipalname
Unique User Identifier user.userprincipalname

SAML Signing Certificate

Status: Active
Thumbprint: [redacted]
Expiration: 4/21/2024, 8:34:21 PM
Notification Email: [redacted]
App Federation Metadata Url: https://login.microsoftonline.com/1def8742-8c49-...
Certificate (Base64): Download
Certificate (Raw): Download
Federation Metadata XML: Download

Set up Test Application

You'll need to configure the application to link with Azure AD.

Login URL: https://login.microsoftonline.com/1def8742-8c49-...
Azure AD Identifier: https://sts.windows.net/1def8742-8c49-497a-a30...
Logout URL: https://login.microsoftonline.com/1def8742-8c49-...

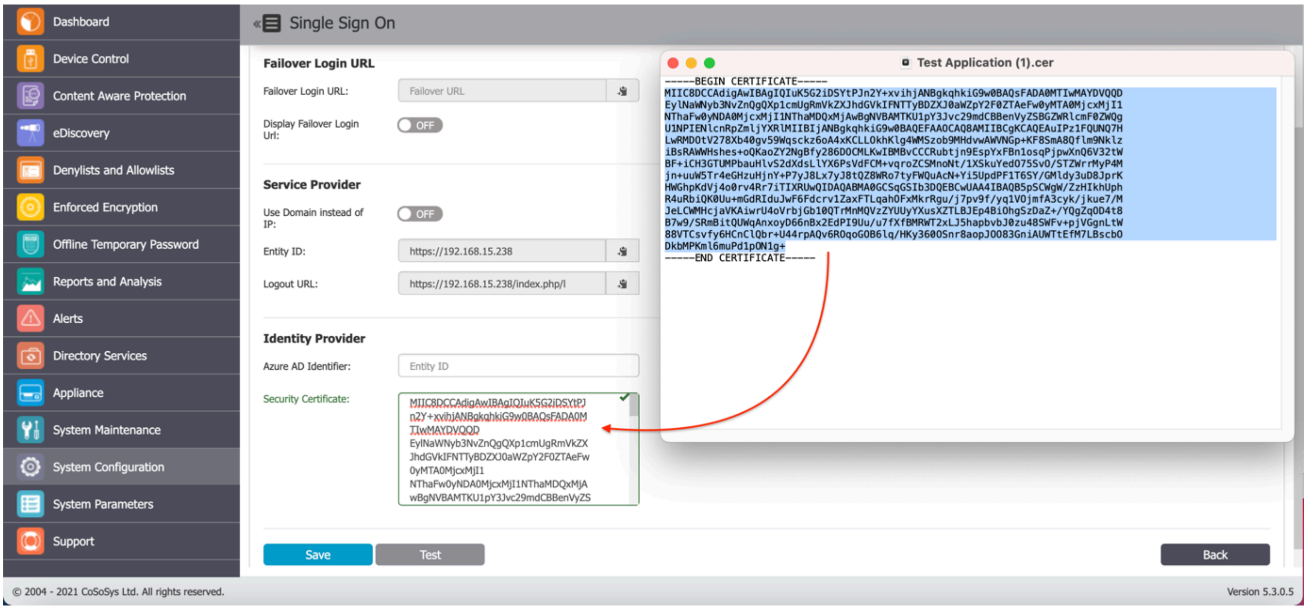
View step-by-step instructions

Test single sign-on with Test Application

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

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.



Failover Login URL

Failover Login URL: Failover URL
Display Failover Login Url: OFF

Service Provider

Use Domain instead of IP: OFF
Entity ID: https://192.168.15.238
Logout URL: https://192.168.15.238/index.php/l

Identity Provider

Azure AD Identifier: Entity ID
Security Certificate:

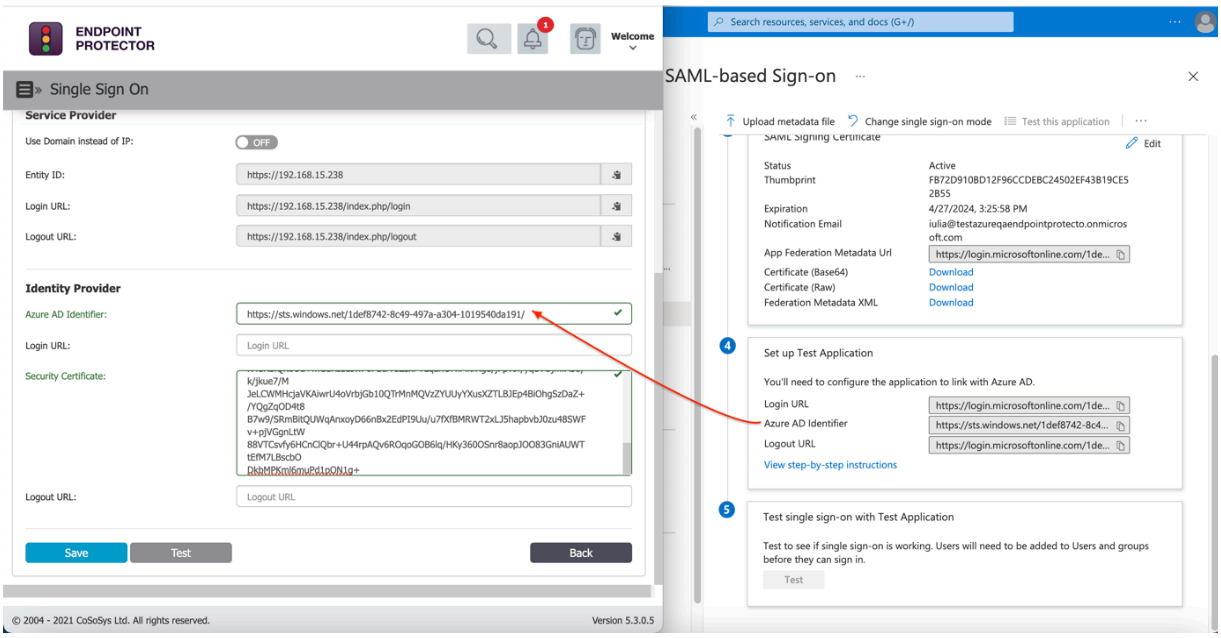
MIIC8DCCAdigAwIBAgIQIuK5G2iDSYtPJ
n2Y+xvihjANBgkqhkiG9w0BAQsFADA0M
TIwMAYDVQQD
EylNaWNyb3NvZnQgQXp1cmUgRmVkZX
JhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw
0yMTA0MjcxMjI1
NThaFw0yNDA0MjcxMjI1NThaMDQxMjA
wBgNVBAMTKU1pY3Jvc29mdCBBenVyZS

Test Application (1).cer

-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQIuK5G2iDSYtPJn2Y+xvihjANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD
EylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA0MjcxMjI1
NThaFw0yNDA0MjcxMjI1NThaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQg
U1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuIPz1FQUNQ7H
LwRMDOtV278Xb40gv59Wqsckz6oA4xKCLLOkhKlg4WMSzob9MHdvwAWVNGp+KF8SmA8Qflm9Nklz
iBsRAWWHshes+oQKaoZY2NgBfy286DOCMLKwIBMBvCCCRubtjn9EspYxFBn1osqPjpwXnQ6V32tW
BF+iCH3GTUMPbauHlvS2dXdsLlYX6PsVdFCM+vqroZCSMnoNt/1XSkuYedO75SvO/STZWrrMyP4M
jn+uuW5Tr4eGHzuHjnY+P7yJ8Lx7yJ8tQZ8WRo7tyFWQuAcN+Yi5UpdPF1T6SY/GMldy3uD8JprK
HWGhpKdVj4o0rv4Rr7iTIXRUwQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB5pSCWgW/ZzHIkhUph
R4uRbiQK0Uu+mGdRIduJwF6Fdcrv1ZaxFTLqahOFxMkrRgu/j7pv9f/yq1VOjmfA3cyk/jkue7/M
JeLCWMHcjaVKAiwrU4oVrbjGb10QTrMnMQVzZYUUyYXusXZTLBJEp4BiOhgSzDaZ+/YQgZqOD4t8
B7w9/SRmBitQUWqAnxoyD66nBx2EdPI9Uu/u7fXfBMRWT2xLJ5hapbvbJ0zu48SWFv+pjVGgnLtW
88VTCsvfy6HCnClQbr+U44rpAQv6ROqoGOB6lq/HKy360OSnr8aopJOO83GniAUWTtEfM7LBscbO
DkbMPKml6muPd1pON1g+
-----END 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.



Single Sign On

Service Provider

Use Domain instead of IP: OFF

Entity ID: https://192.168.15.238

Login URL: https://192.168.15.238/index.php/login

Logout URL: https://192.168.15.238/index.php/logout

Identity Provider

Azure AD Identifier: https://sts.windows.net/1def8742-8c49-497a-a304-1019540da191/ ✓

Login URL: Login URL

Security Certificate: k/jkue7/M JeLCWMHcjaVKAiwrU4oVrbjGb10QTrMnMQVzZYUUyYXusXZTLBJEp4BiOhgSzDaZ+ /YQgZqOD4t8 B7w9/SRmBitQUWqAnxoyD66nBx2EdPI9Uu/u7fXfBMRWT2xLJ5hapbvbJ0zu48SWF v+pjVGgnLtW 88VTCsvfy6HCnClQbr+U44rpAQv6ROqoGOB6lq/HKy360OSnr8aopJOO83GniAUWT tEfM7LBscbO DkbMPKml6muPd1pON1g+ ✓

Logout URL: Logout URL

© 2004 - 2021 CoSoSys Ltd. All rights reserved. Version 5.3.0.5

SAML-based Sign-on

SAML Signing Certificate

Status: Active

Thumbprint: FB72D910BD12F96CCDEBC24502EF43B19CE5 2B55

Expiration: 4/27/2024, 3:25:58 PM

Notification Email: iulia@testazureqaendpointprotecto.onmicrosoft.com

App Federation Metadata Url: https://login.microsoftonline.com/1de...

Certificate (Base64): Download

Certificate (Raw): Download

Federation Metadata XML: Download

4 Set up Test Application

You'll need to configure the application to link with Azure AD.

Login URL: https://login.microsoftonline.com/1de...

Azure AD Identifier: https://sts.windows.net/1def8742-8c4...

Logout URL: https://login.microsoftonline.com/1de...

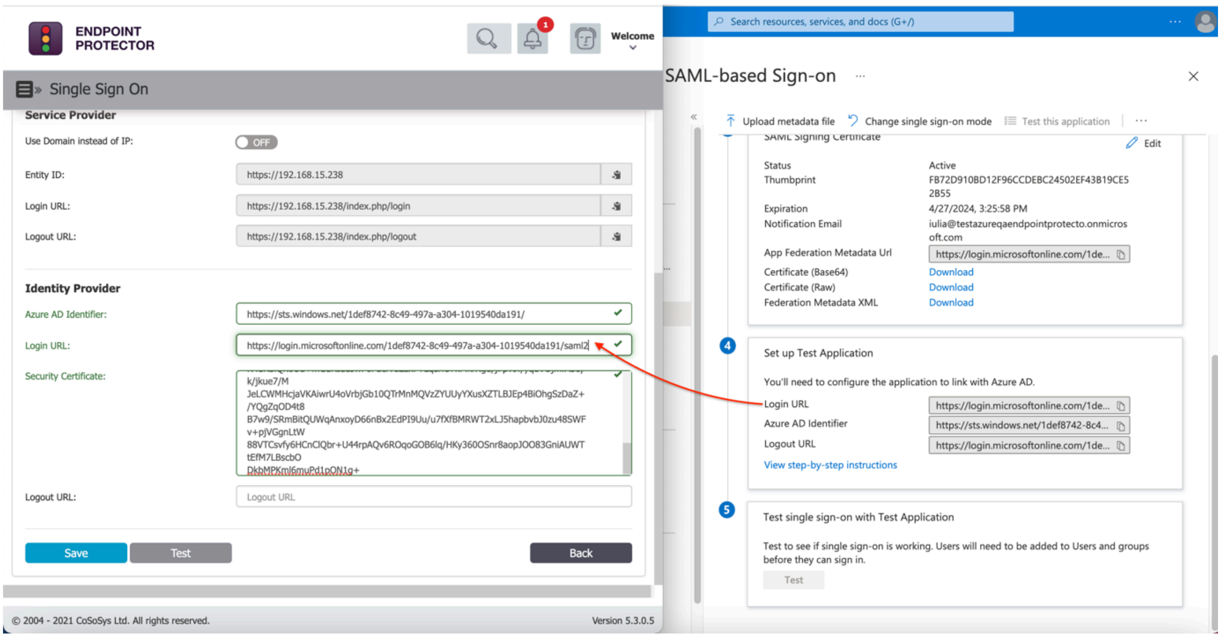
View step-by-step instructions

5 Test single sign-on with Test Application

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

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.



Single Sign On

Service Provider

Use Domain instead of IP: OFF

Entity ID: https://192.168.15.238

Login URL: https://192.168.15.238/index.php/login

Logout URL: https://192.168.15.238/index.php/logout

Identity Provider

Azure AD Identifier: https://sts.windows.net/1def8742-8c49-497a-a304-1019540da191/ ✓

Login URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2 ✓

Security Certificate: k/jkue7/M JeLCWMHcjaVKAiwrU4oVrbjGb10QTrMnMQVzZYUUyYXusXZTLBJEp4BiOhgSzDaZ+ /YQgZqOD4t8 B7w9/SRmBitQUWqAnxoyD66nBx2EdPI9Uu/u7fXfBMRWT2xLJ5hapbvbJ0zu48SWF v+pjVGgnLtW 88VTCsvfy6HCnClQbr+U44rpAQv6ROqoGOB6lq/HKy360OSnr8aopJOO83GniAUWT tEfM7LBscbO DkbMPKml6muPd1pON1g+ ✓

Logout URL: Logout URL

© 2004 - 2021 CoSoSys Ltd. All rights reserved. Version 5.3.0.5

SAML-based Sign-on

SAML Signing Certificate

Status: Active

Thumbprint: FB72D910BD12F96CCDEBC24502EF43B19CE5 2B55

Expiration: 4/27/2024, 3:25:58 PM

Notification Email: iulia@testazureqaendpointprotecto.onmicrosoft.com

App Federation Metadata Url: https://login.microsoftonline.com/1de...

Certificate (Base64): Download

Certificate (Raw): Download

Federation Metadata XML: Download

4 Set up Test Application

You'll need to configure the application to link with Azure AD.

Login URL: https://login.microsoftonline.com/1de...

Azure AD Identifier: https://sts.windows.net/1def8742-8c4...

Logout URL: https://login.microsoftonline.com/1de...

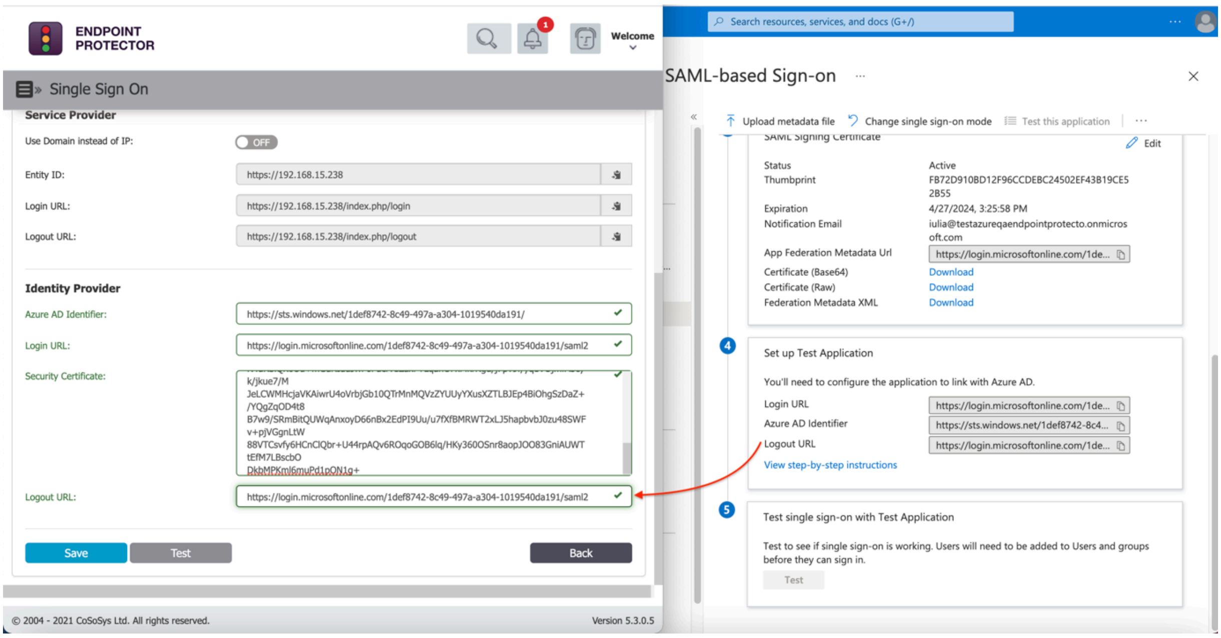
View step-by-step instructions

5 Test single sign-on with Test Application

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

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.


ENDPOINT PROTECTOR
Welcome
Search resources, services, and docs (G+/)
Upload metadata file
Change single sign-on mode
Test this application
Edit
Save
Test
Back
© 2004 - 2021 CoSoSys Ltd. All rights reserved.
Version 5.3.0.5

Single Sign On

Service Provider

Use Domain instead of IP: OFF

Entity ID: https://192.168.15.238

Login URL: https://192.168.15.238/index.php/login

Logout URL: https://192.168.15.238/index.php/logout

Identity Provider

Azure AD Identifier: https://sts.windows.net/1def8742-8c49-497a-a304-1019540da191/ ✓

Login URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2 ✓

Security Certificate: ✓

```
k/jkue7/M
JeLCWMHcjaVKAiwrU4oVrbjGb10QTrMnMQVzZYUUyYXusXZTLBJEp4BiOhgSzDaZ+
/YQgZqOD4t8
B7w9/SRmBitQUWqAnxoyD66nBx2EdPI9Uu/u7fXfBMRWT2xLJ5hapbvbJ0zu48SWF
v+pjVGgnLtW
88VTCsvfy6HCnClQbr+U44rpAQv6ROqoGOB6lq/HKy360OSnr8aopJOO83GniAUWT
tEfM7LBscbO
DkbMPKml6muPd1pON1g+
```

Logout URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2 ✓

SAML-based Sign-on

SAML Signing Certificate

Status	Active
Thumbprint	FB72D910BD12F96CCDEBC24502EF43B19CE5 2B55
Expiration	4/27/2024, 3:25:58 PM
Notification Email	iulia@testazureqaendpointprotecto.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/1de...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Test Application

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/1de...
Azure AD Identifier	https://sts.windows.net/1def8742-8c4...
Logout URL	https://login.microsoftonline.com/1de...

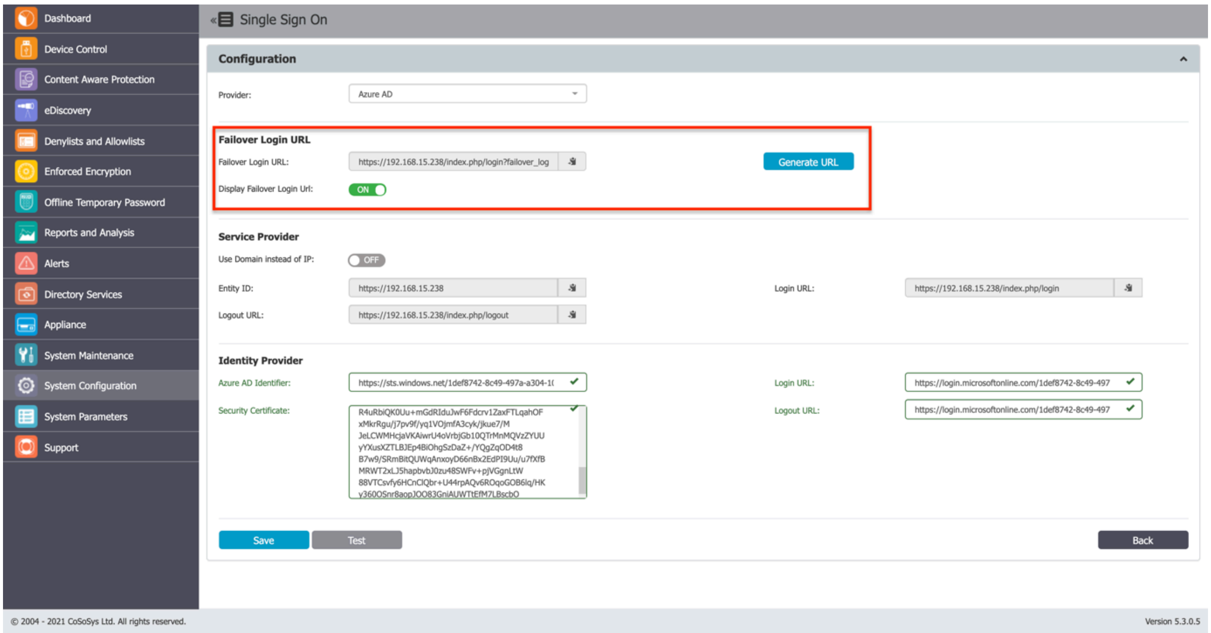
View step-by-step instructions

5 Test single sign-on with Test Application

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Test

23. Generate Failover Login URL from Endpoint Protector Server, System Configuration, Single Sign On, Failover Login URL and Save the URL.



Single Sign On

Configuration

Provider: Azure AD

Failover Login URL

Failover Login URL: https://192.168.15.238/index.php/login?failover_log

Display Failover Login Url: ON

Service Provider

Use Domain instead of IP: OFF

Entity ID: https://192.168.15.238

Login URL: https://192.168.15.238/index.php/login

Logout URL: https://192.168.15.238/index.php/logout

Identity Provider

Azure AD Identifier: https://sts.windows.net/1def8742-8c49-497a-a304-1(✓

Login URL: https://login.microsoftonline.com/1def8742-8c49-497 ✓

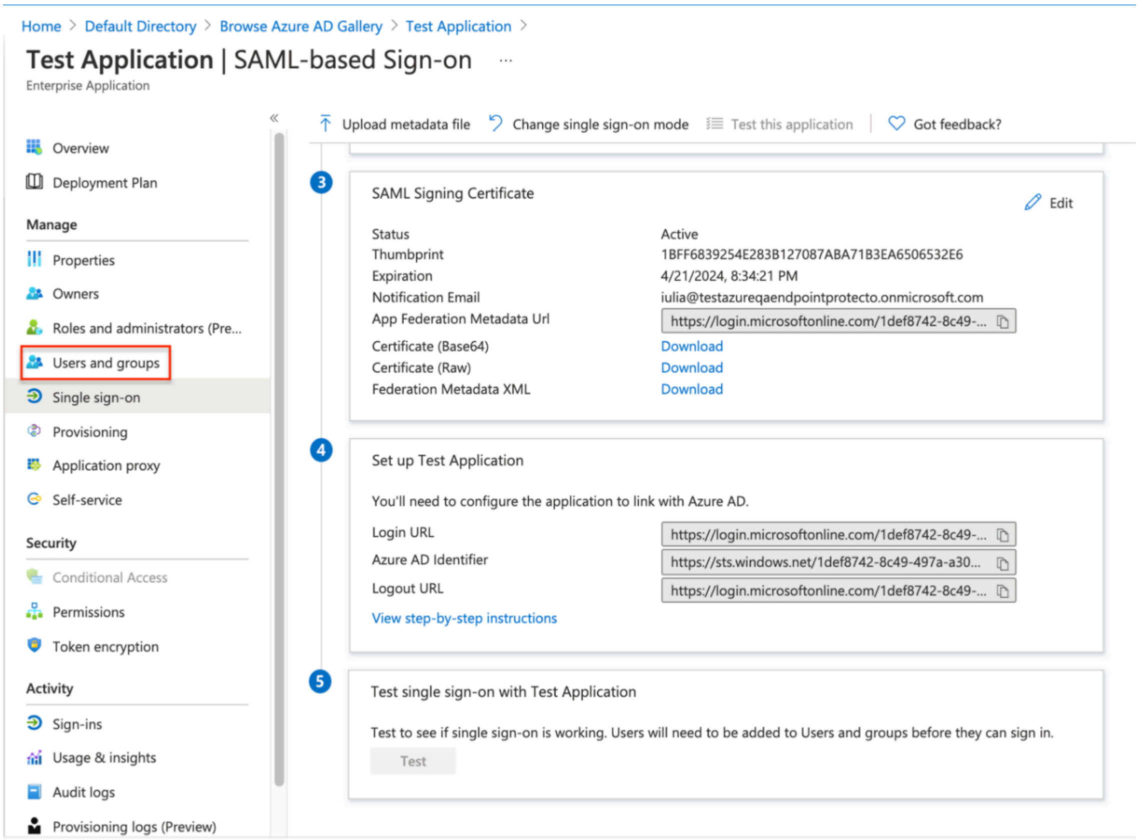
Security Certificate: ✓

```
R4uRbiQK0Uu+mGdRIduJwF6Fdcrv1ZaxFTLqahOF
xMkrRgu/j7pv9f/yq1VOjmfA3cyk/jkue7/M
JeLCWMHcjaVKAiwrU4oVrbjGb10QTrMnMQVzZYUU
yYXusXZTLBJEp4BiOhgSzDaZ+/YQgZqOD4t8
B7w9/SRmBitQUWqAnxoyD66nBx2EdPI9Uu/u7fXfB
MRWT2xLJ5hapbvbJ0zu48SWFv+pjVGgnLtW
88VTCsvfy6HCnClQbr+U44rpAQv6ROqoGOB6lq/HK
y360OSnr8aopJOO83GniAUWTtEfM7LBscbO
```

Logout URL: https://login.microsoftonline.com/1def8742-8c49-497 ✓

24. Save the settings on the Single Sign On page from Endpoint Protector Server.

25. Switch to Azure, Select Users and groups from the left menu.



Home > Default Directory > Browse Azure AD Gallery > Test Application >

Test Application | SAML-based Sign-on ...

Enterprise Application

3 SAML Signing Certificate

Edit

Status	Active
Thumbprint	1BFF6839254E283B127087ABA71B3EA6506532E6
Expiration	4/21/2024, 8:34:21 PM
Notification Email	iulia@testazureqaendpointprotecto.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/1def8742-8c49-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Test Application

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/1def8742-8c49-...
Azure AD Identifier	https://sts.windows.net/1def8742-8c49-497a-a30...
Logout URL	https://login.microsoftonline.com/1def8742-8c49-...

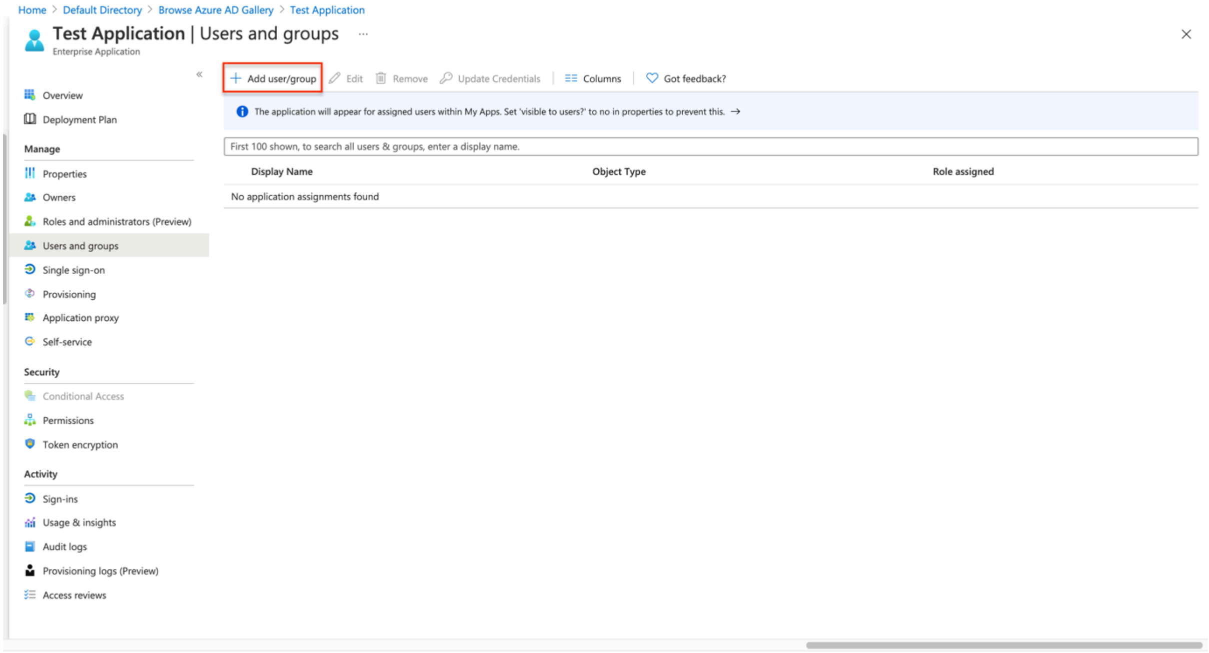
View step-by-step instructions

5 Test single sign-on with Test Application

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Test

26. Go to Add user/group, none Selected, search for the Azure User, Select, Assign.



Home > Default Directory > Browse Azure AD Gallery > Test Application

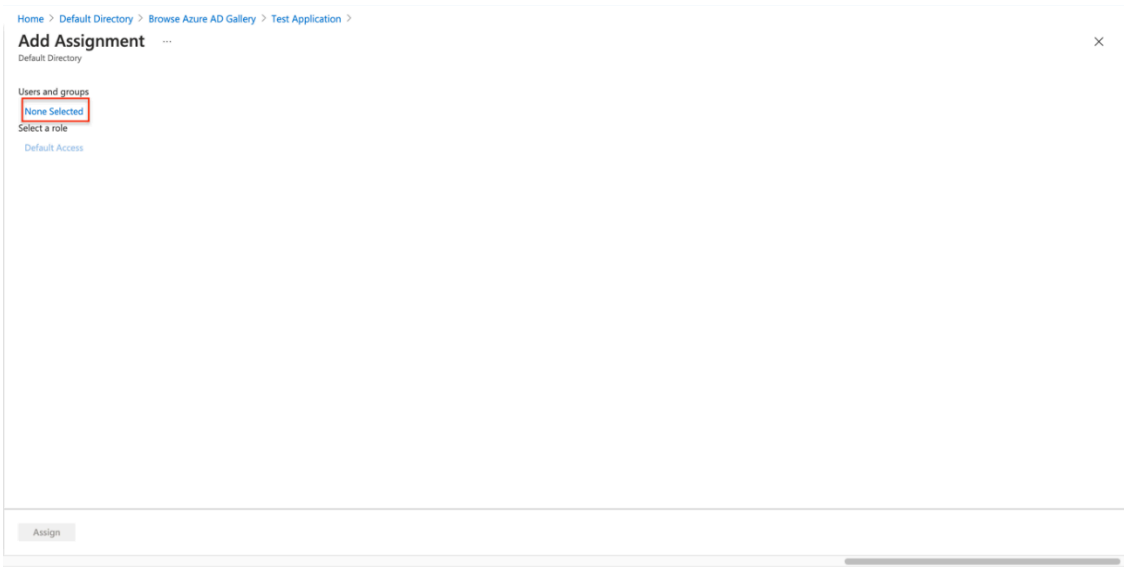
Test Application | Users and groups ...

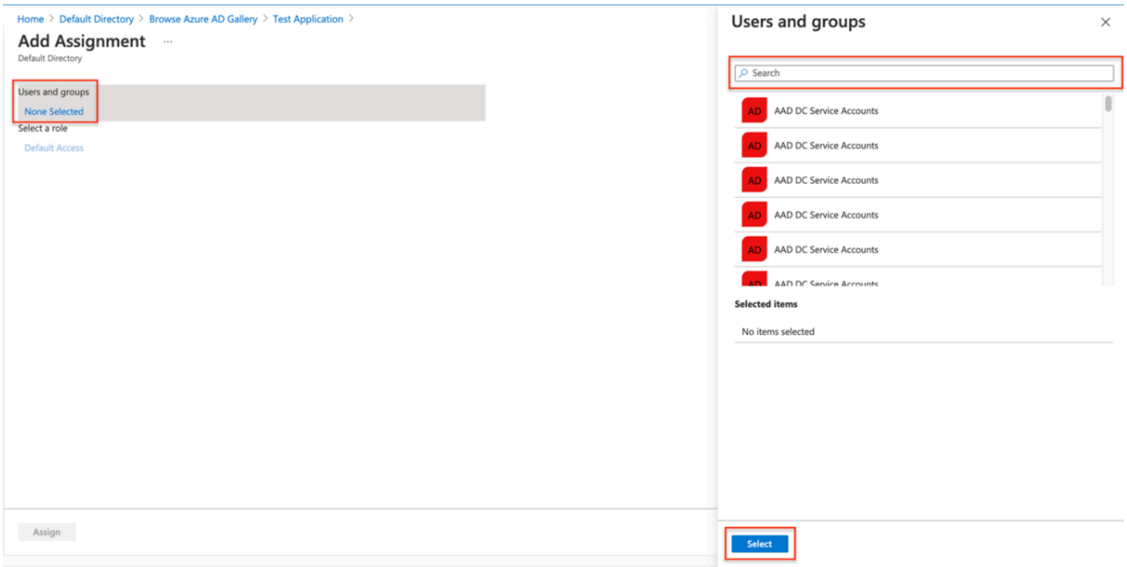
Enterprise Application

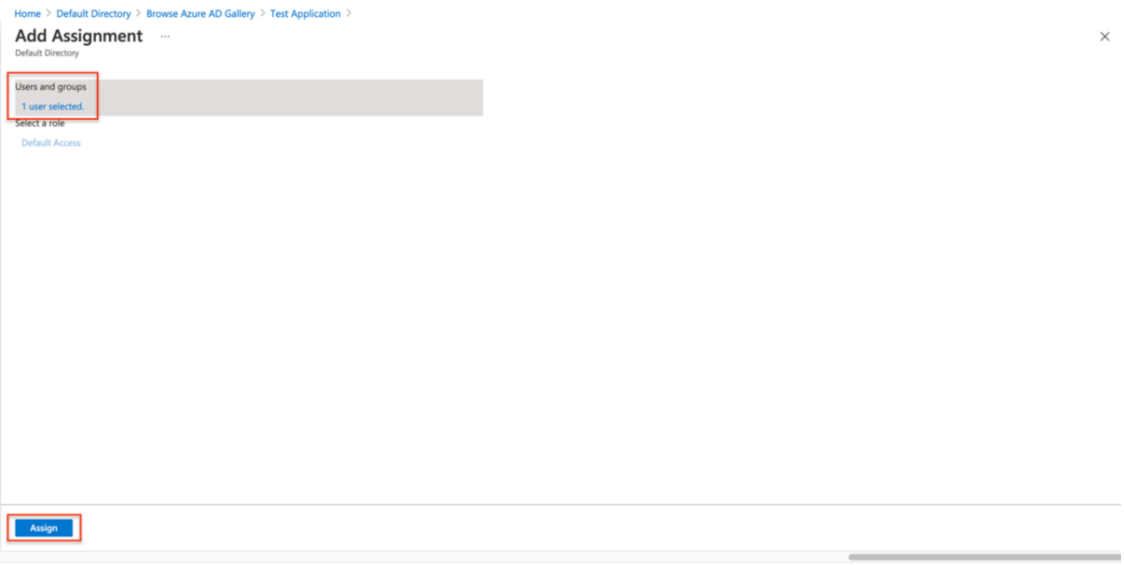
The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
No application assignments found		


Home > Default Directory > Browse Azure AD Gallery > Test Application >
Add Assignment ...
Default Directory
Users and groups
None Selected
Select a role
Default Access
Assign


Home > Default Directory > Browse Azure AD Gallery > Test Application >
Add Assignment ...
Default Directory
Users and groups
None Selected
Select a role
Default Access
Assign
Users and groups
Search
AD AAD DC Service Accounts
AD AAD DC Service Accounts
AD AAD DC Service Accounts
AD AAD DC Service Accounts
AD AAD DC Service Accounts
AD AAD DC Service Accounts
Selected items
No items selected
Select


Home > Default Directory > Browse Azure AD Gallery > Test Application >
Add Assignment ...
Default Directory
Users and groups
1 user selected.
Select a role
Default Access
Assign

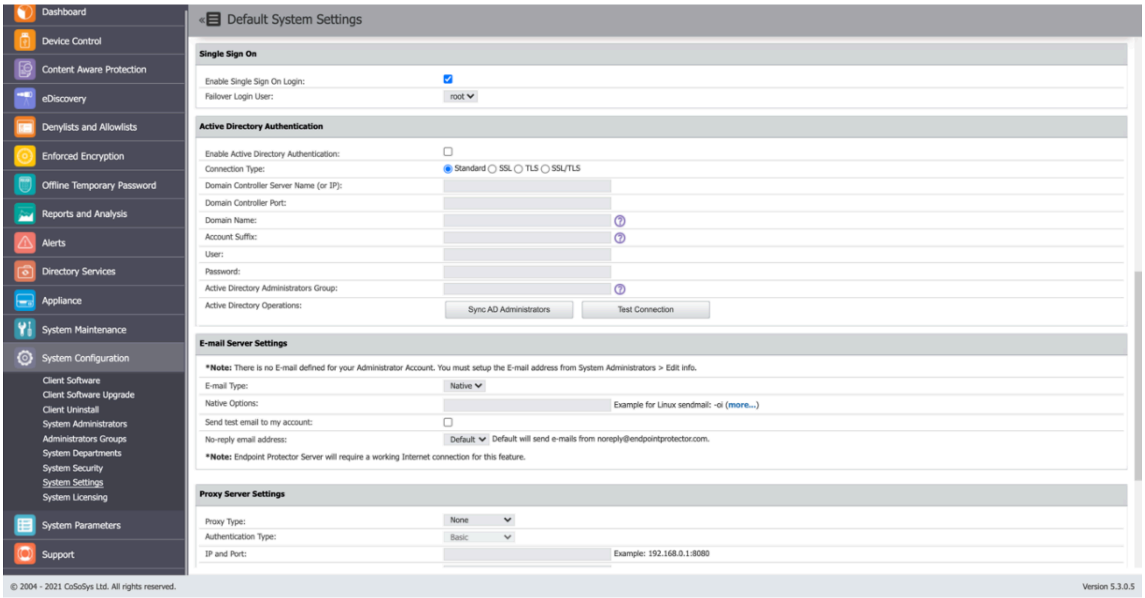
27. The User is assigned to the application and login in Endpoint Protector with Azure is now possible.

28. Logout from the Endpoint Protector Server and access it again. The Administrator should be redirected to http://login.microsoftonline.com/ for the Azure login process.

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

Single Sign On

Enable Single Sign On Login: ☑
Failover Login User: root

Active Directory Authentication

Enable Active Directory Authentication: □
Connection Type: ● Standard ○ SSL ○ TLS ○ SSL/TLS
Domain Controller Server Name (or IP):
Domain Controller Port:
Domain Name:
Account Suffix:
User:
Password:
Active Directory Administrators Group:
Active Directory Operations: Sync AD Administrators | Test Connection

E-mail Server Settings

***Note:** There is no E-mail defined for your Administrator Account. You must setup the E-mail address from System Administrators > Edit info.

E-mail Type: Native
Native Options: Example for Linux sendmail: -oi (more...)
Send test email to my account: □
No-reply email address: Default Default will send e-mails from noreply@endpointprotector.com.

***Note:** Endpoint Protector Server will require a working Internet connection for this feature.

Proxy Server Settings

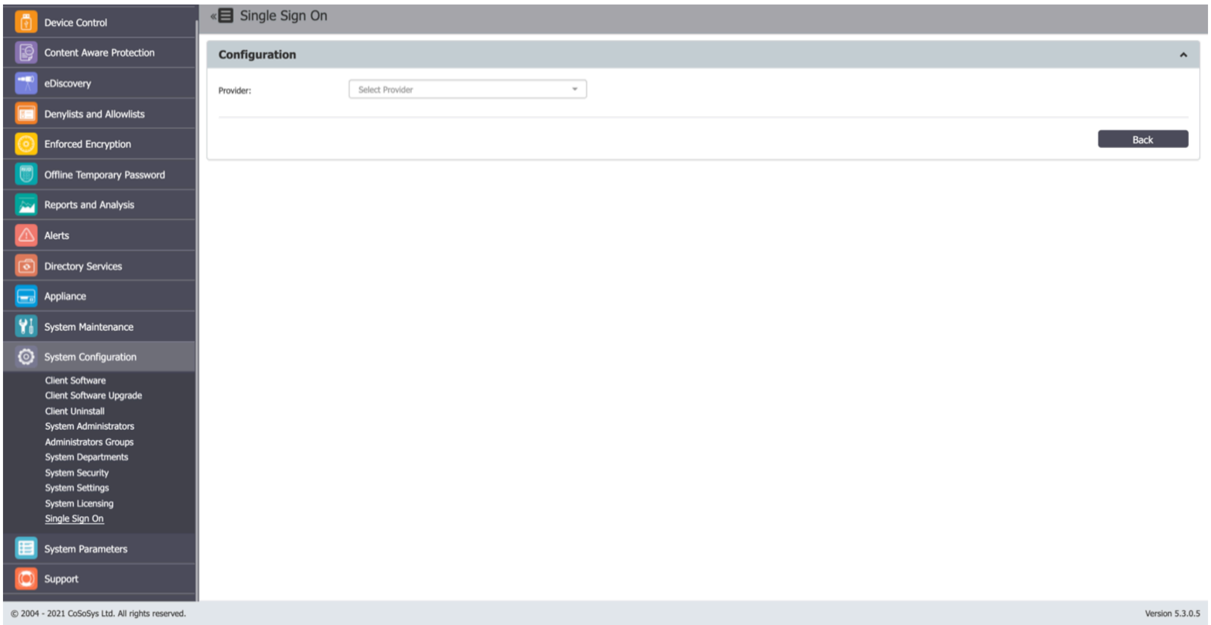
Proxy Type: None
Authentication Type: Basic
IP and Port: Example: 192.168.0.1:8080

© 2004 - 2021 CoSoSys Ltd. All rights reserved.

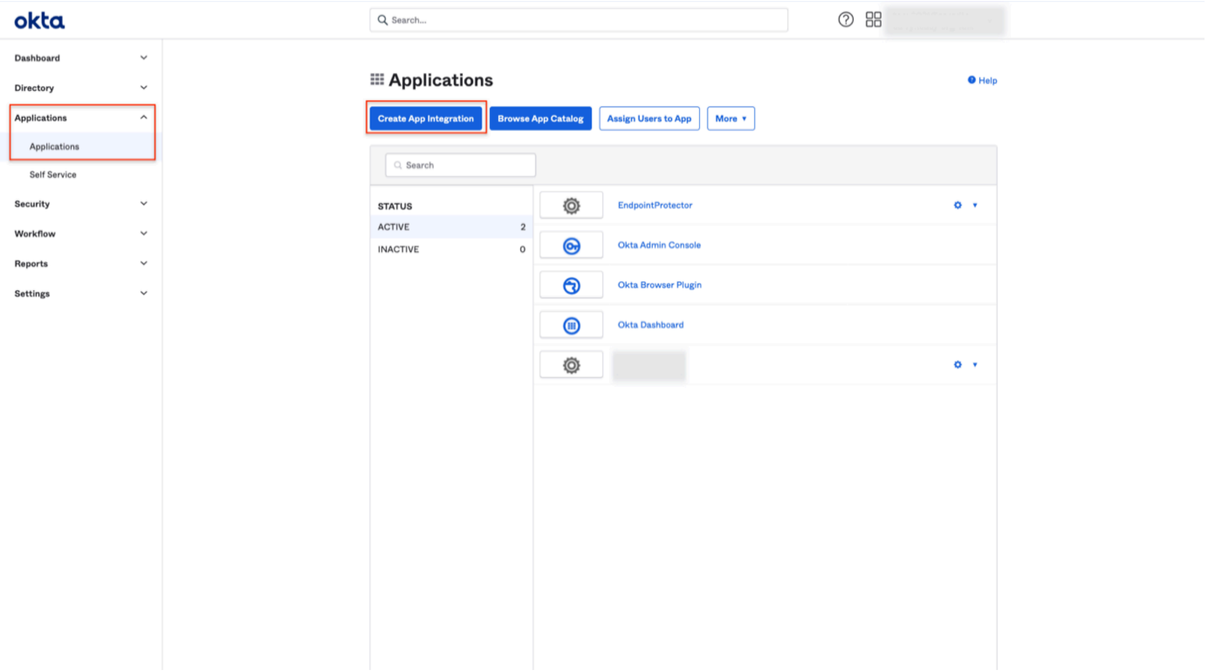
Version 5.3.0.5

After the above steps have been completed, a Single Sign On subsection is displayed in the System Configuration section.

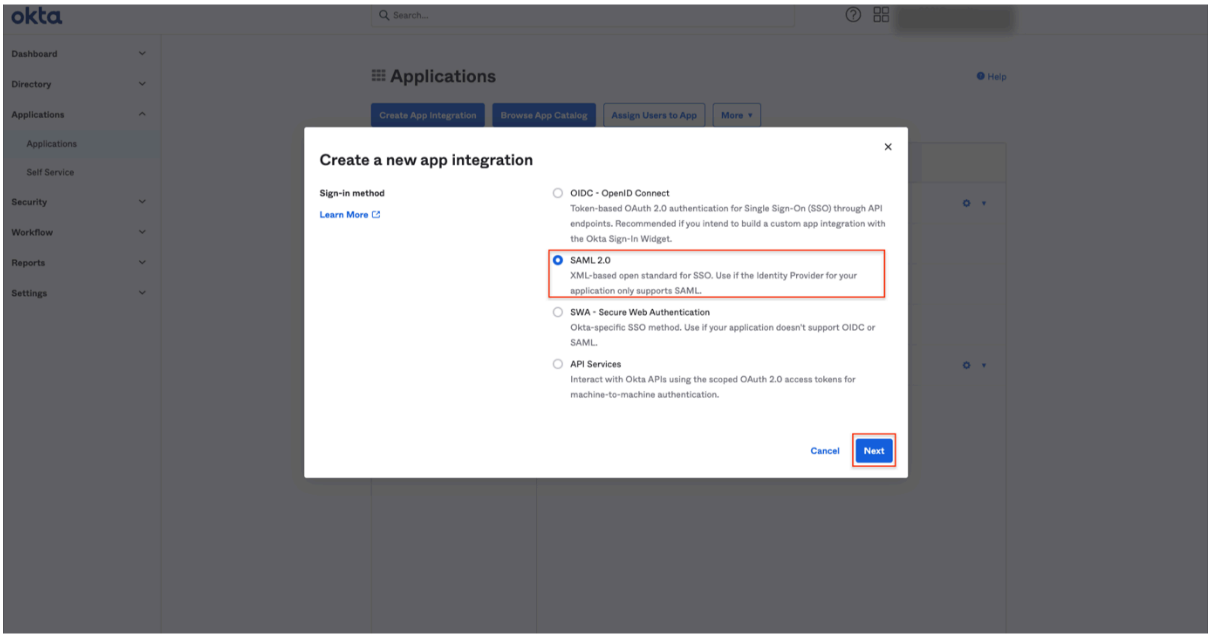
2. Select the Provider in order for Single Sign On subsection to be displayed.



3. Go to **yourcompany.okta.com**, **Applications**- and then **Create App Integration**.



4. On the following screen, select **SAML 2.0** and click **Next**.



Create a new app integration

Sign-in method

Learn More

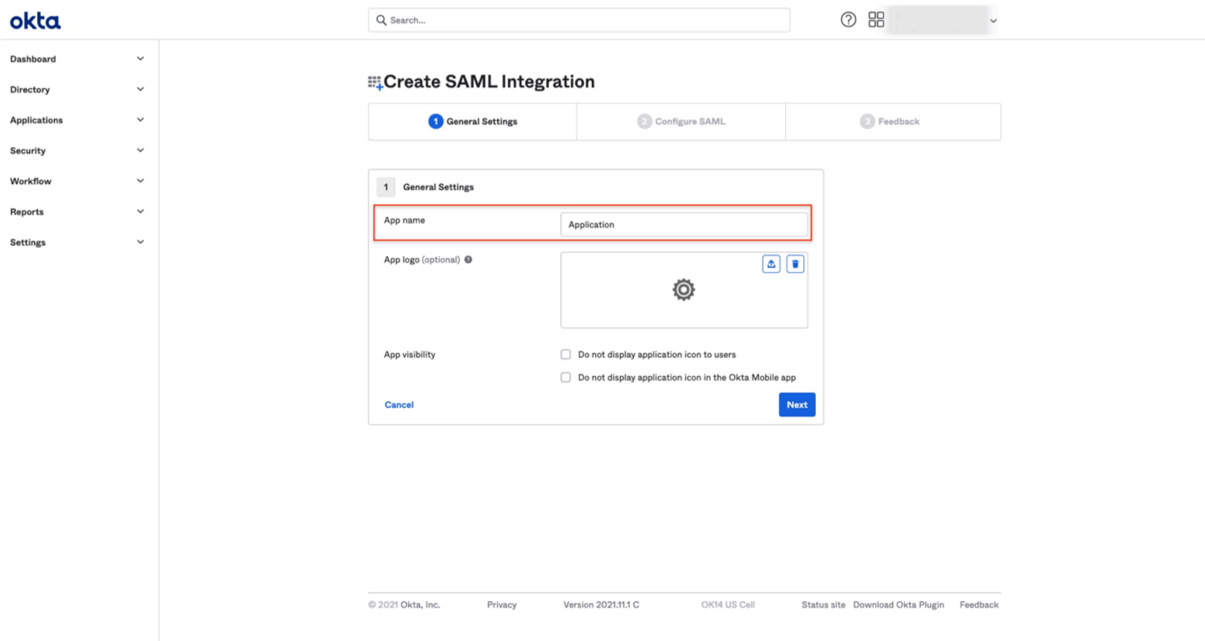
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

5. Set a **Name** for the Application and click **Next**.



Create SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

1 General Settings

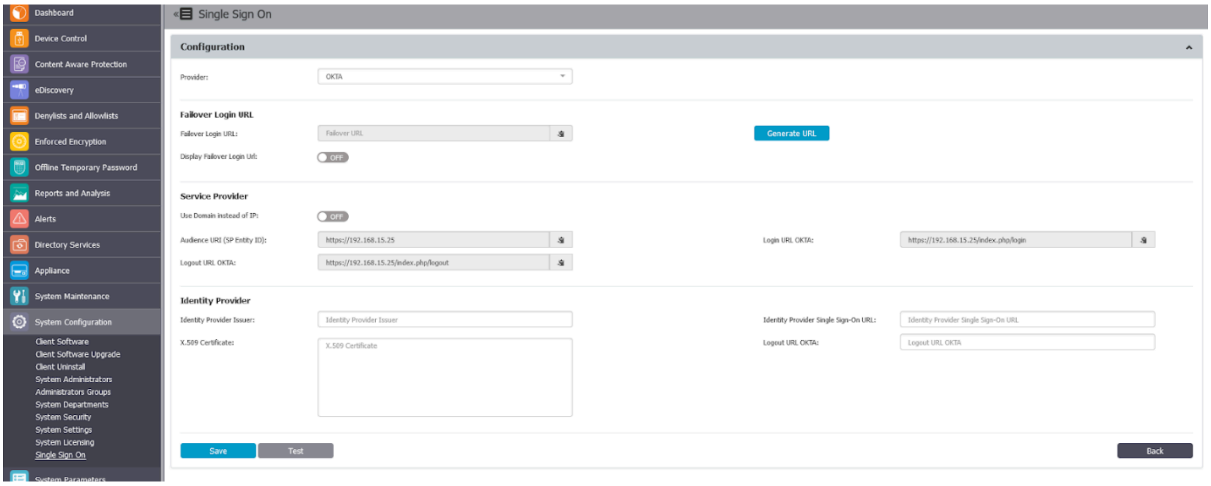
App name: Application

App logo (optional)

App visibility
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile app

6. Open the **Configure SAML** tab.

7. Go to your Endpoint Protector Server, System Configuration, Single Sign On.



Single Sign On

Configuration

Provider: OKTA

Failover Login URL

Failover Login URL: Failover URL

Display Failover Login Url: OFF

Service Provider

Use Domain instead of IP: OFF

Audience URI (SP Entity ID): https://192.168.15.25

Login URL OKTA: https://192.168.15.25/index.php/login

Logout URL OKTA: https://192.168.15.25/index.php/logout

Identity Provider

Identity Provider Issuer: Identity Provider Issuer

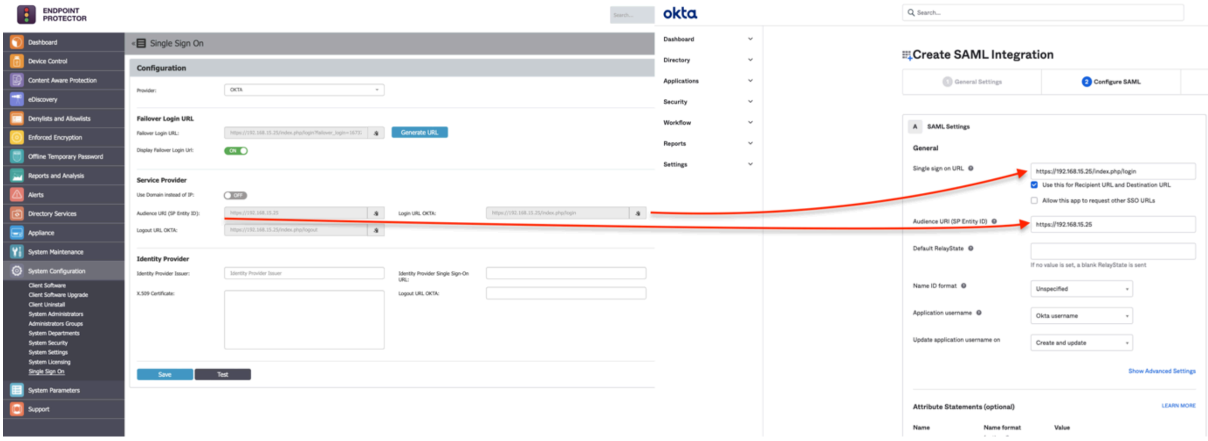
Identity Provider Single Sign-On URL: Identity Provider Single Sign-On URL

X.509 Certificate: X.509 Certificate

Logout URL OKTA: Logout URL OKTA

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**.



Single Sign On

Configuration

Provider: OKTA

Failover Login URL

Failover Login URL: https://192.168.15.25/index.php/login?failover_login=1673

Display Failover Login Url: ON

Service Provider

Use Domain instead of IP: OFF

Audience URI (SP Entity ID): https://192.168.15.25

Login URL OKTA: https://192.168.15.25/index.php/login

Logout URL OKTA: https://192.168.15.25/index.php/logout

Identity Provider

Identity Provider Issuer: Identity Provider Issuer

Identity Provider Single Sign-On URL:

X.509 Certificate:

Logout URL OKTA:

Create SAML Integration

A SAML Settings

General

Single sign on URL: https://192.168.15.25/index.php/login

☑ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://192.168.15.25

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

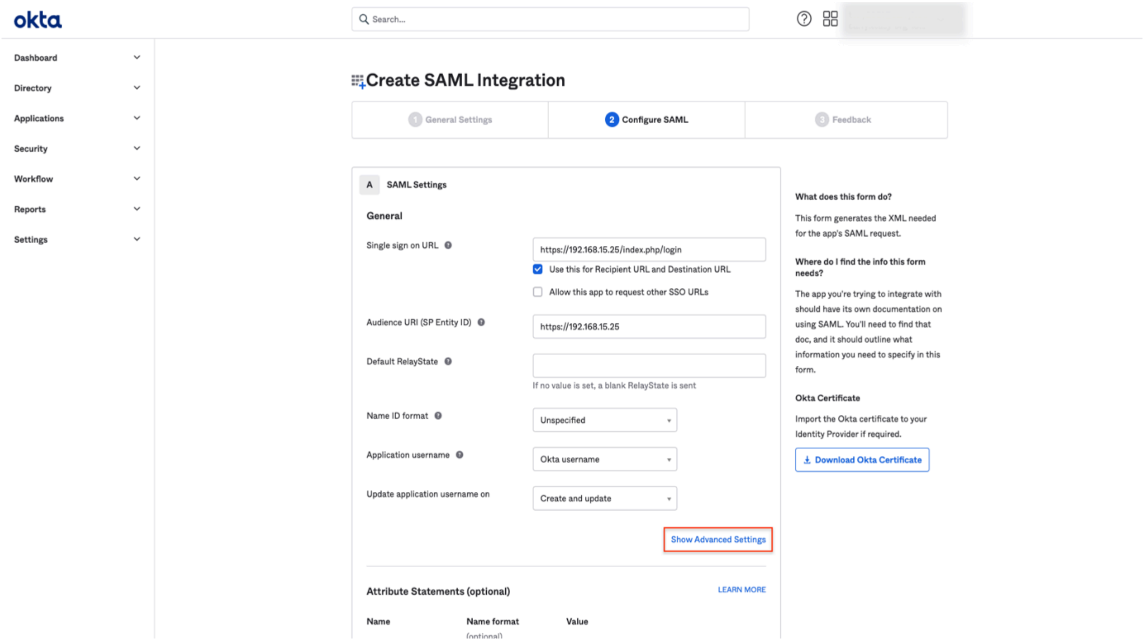
Application username: Okta username

Update application username on: Create and update

Attribute Statements (optional)

Name	Name format	Value

9. On the OKTA page, click **Show Advanced Settings**.



Create SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

A SAML Settings

General

Single sign on URL: https://192.168.15.25/index.php/login

☑ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://192.168.15.25

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

Update application username on: Create and update

Show Advanced Settings

Attribute Statements (optional) LEARN MORE

Name | Name format (optional) | Value

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

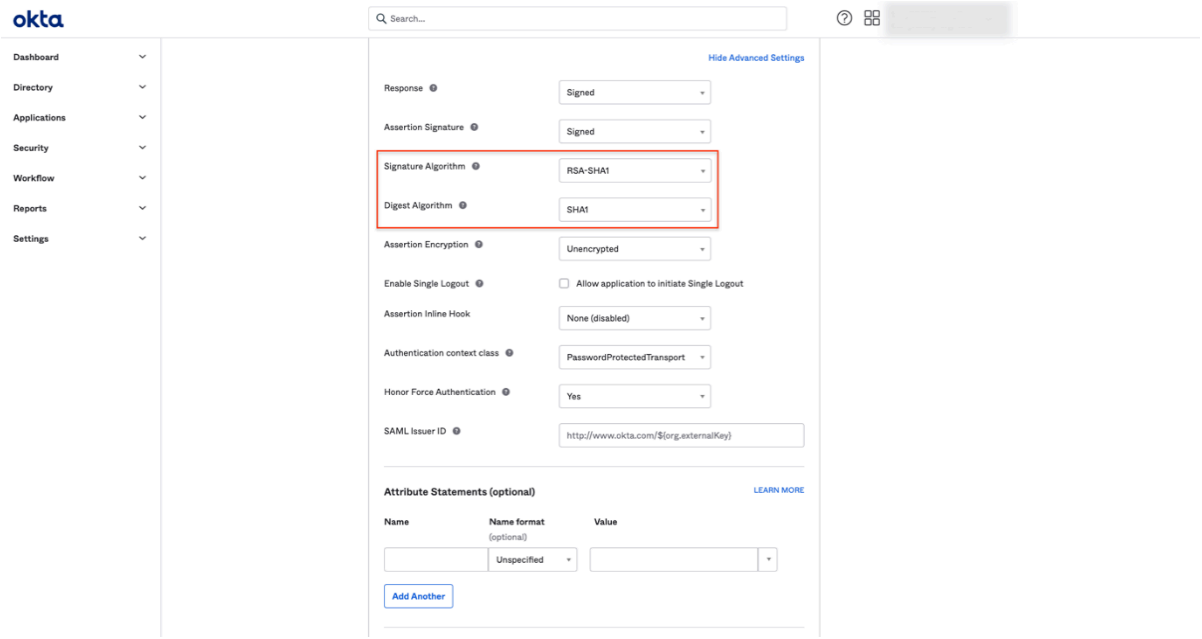
Okta Certificate

Import the Okta certificate to your Identity Provider if required.

Download Okta Certificate

10. Edit the following fields:

    - **Signature Algorithm**, select **RSA-SHA1**
    - **Digest Algorithm**, select **SHA1**



Hide Advanced Settings

Response: Signed

Assertion Signature: Signed

Signature Algorithm: RSA-SHA1

Digest Algorithm: SHA1

Assertion Encryption: Unencrypted

Enable Single Logout: ☐ Allow application to initiate Single Logout

Assertion Inline Hook: None (disabled)

Authentication context class: PasswordProtectedTransport

Honor Force Authentication: Yes

SAML Issuer ID: http://www.okta.com/${org.externalKey}

Attribute Statements (optional) LEARN MORE

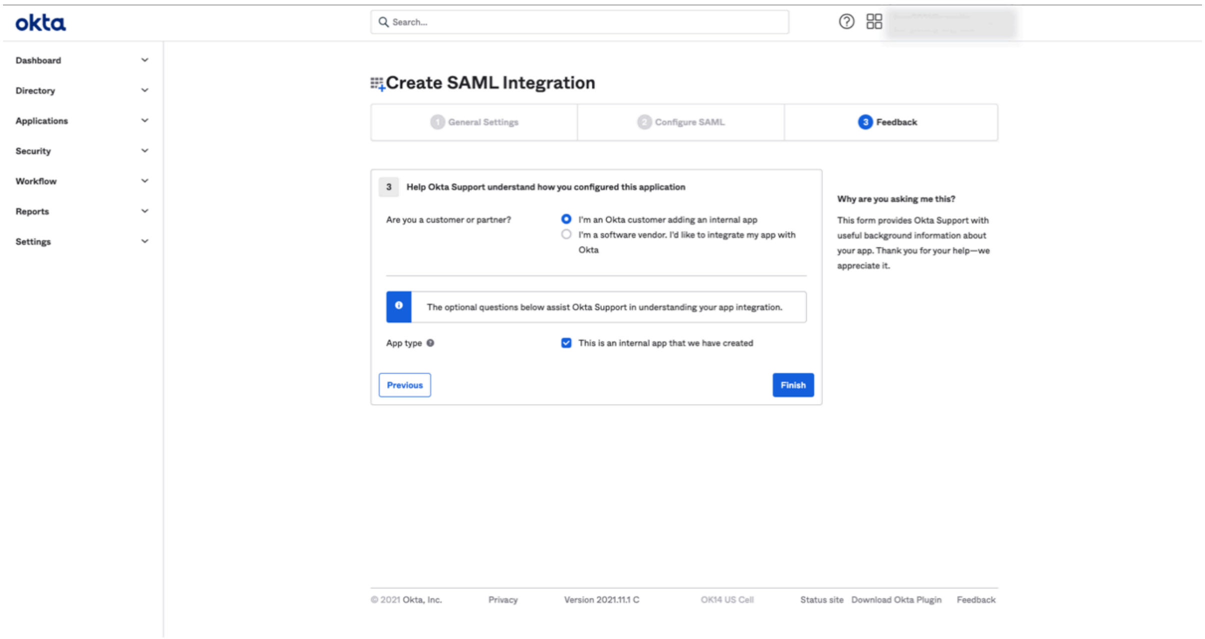
Name | Name format (optional) | Value

Unspecified

Add Another

11. Hide **Advanced Settings** and click **Next**.

12. At step 3, select an answer for each question and click **Finish**.



3 Help Okta Support understand how you configured this application

Are you a customer or partner?

● I'm an Okta customer adding an internal app

○ I'm a software vendor. I'd like to integrate my app with Okta

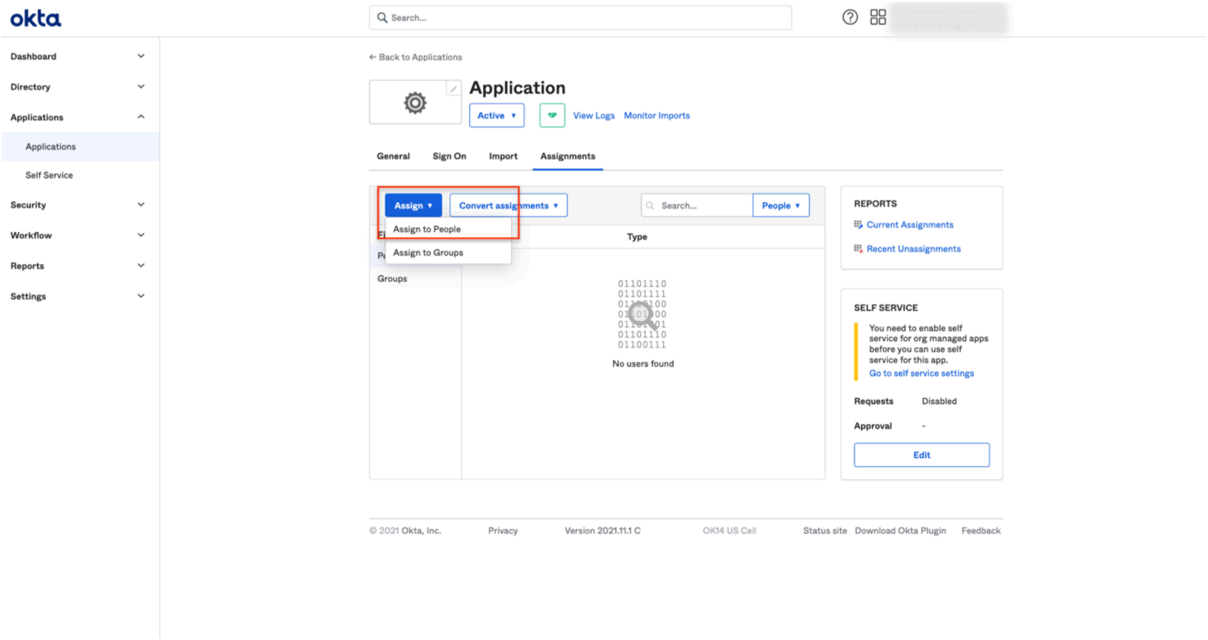
The optional questions below assist Okta Support in understanding your app integration.

App type ☑ This is an internal app that we have created

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

13. Go to **Applications**, the Endpoint Protector application, **Assignments** and assign **People** to this application.

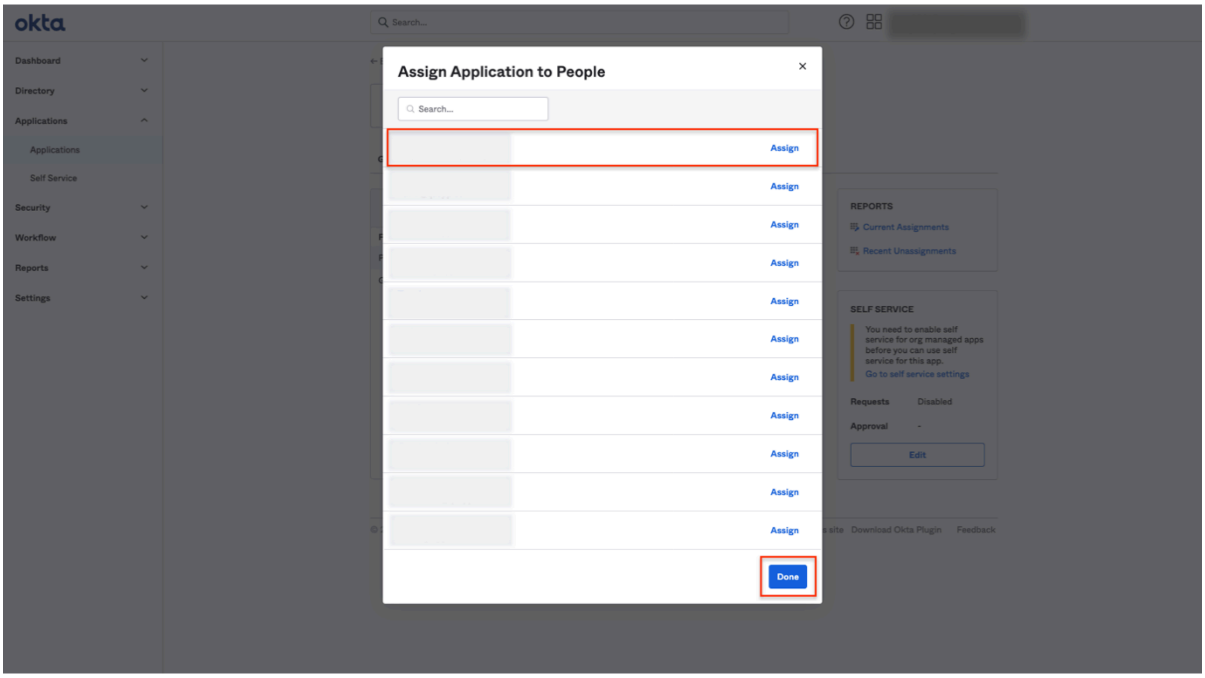


You need to enable self service for org managed apps before you can use self service for this app.

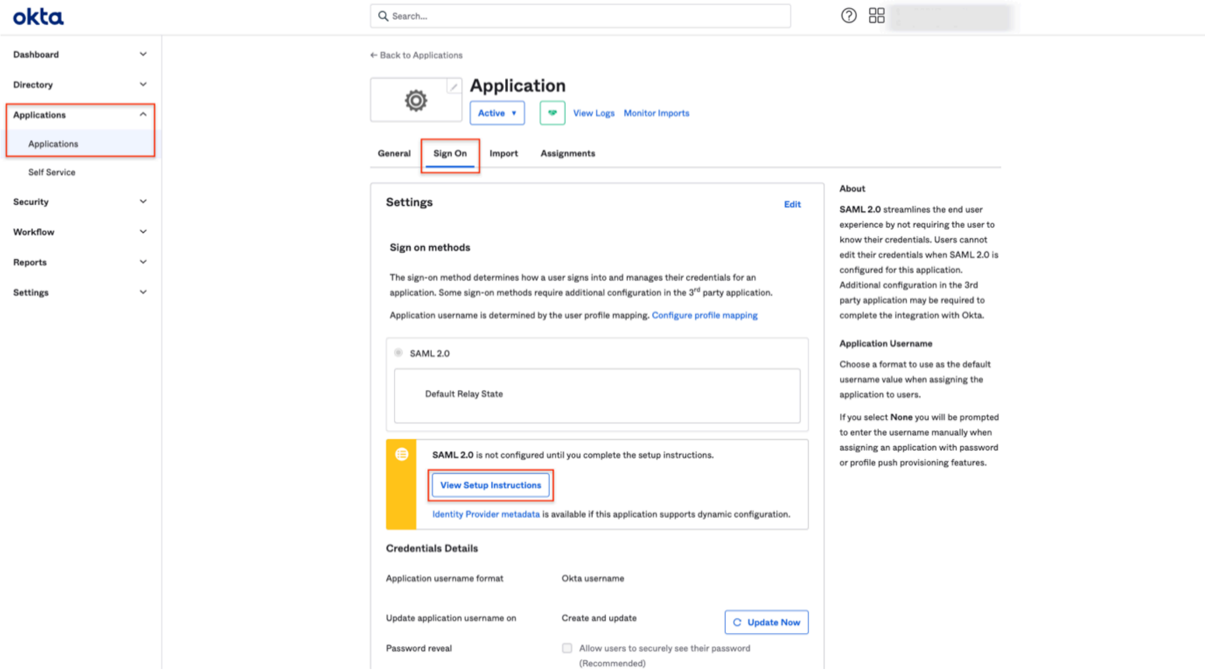
Requests Disabled

Approval -

14. After assigning the accounts, click **Done**.



15. Go to **Applications**, open the created app and click **Sign On**, **View Setup Instructions**.



The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

Application username format: Okta username

Update application username on: Create and update

Password reveal: □ Allow users to securely see their password (Recommended)

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

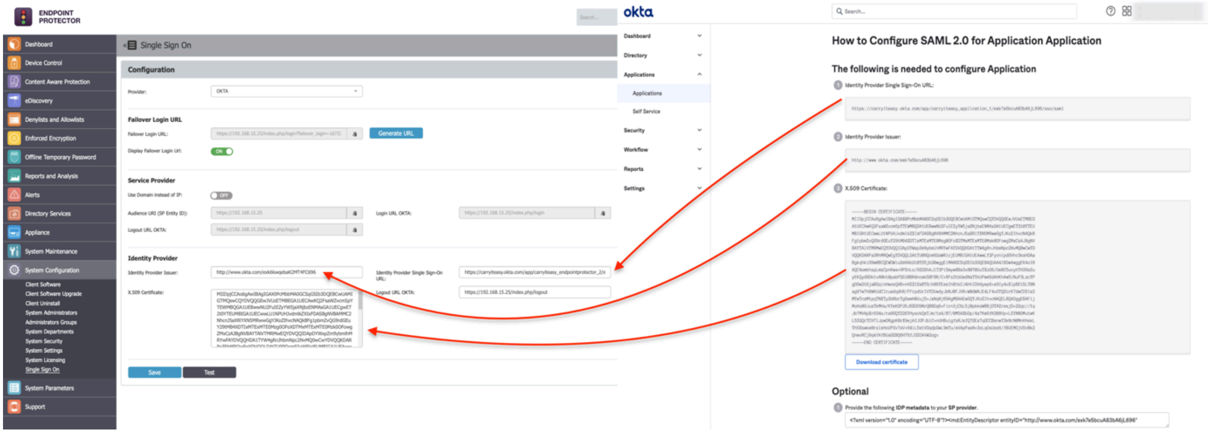
Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

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
- X.509 Certificate to Endpoint Protector Server, System configuration, Single Sign On, X.509 Certificate



Configuration

Provider: OKTA

Failover Login URL

Failover Login URL: https://192.168.15.25/index.php/login?failover_login=1673

Display Failover Login Url: ON

Service Provider

Use Domain instead of IP: OFF

Audience URI (SP Entity ID): https://192.168.15.25

Login URL OKTA: https://192.168.15.25/index.php/login

Logout URL OKTA: https://192.168.15.25/index.php/logout

Identity Provider

Identity Provider Issuer: http://www.okta.com/exk6kwqebaK2MT4FC696

Identity Provider Single Sign-On URL: https://carryiteasy.okta.com/app/carryiteasy_endpointprotector_2/e

X.509 Certificate: MIIDpjCCAo6gAwIBAgIGAX0PcMbbMA0GCSqGSIb3DQEBCwUAMI [illegible]

Logout URL OKTA: https://192.168.15.25/index.php/logout

How to Configure SAML 2.0 for Application Application

The following is needed to configure Application

1. Identity Provider Single Sign-On URL:
   https://carryiteasy.okta.com/app/carryiteasy_application_1/exk7e5bcuA83bA6jL696/sso/saml
2. Identity Provider Issuer:
   http://www.okta.com/exk7e5bcuA83bA6jL696
3. X.509 Certificate:
   -----BEGIN CERTIFICATE----- [illegible] -----END CERTIFICATE-----

Optional

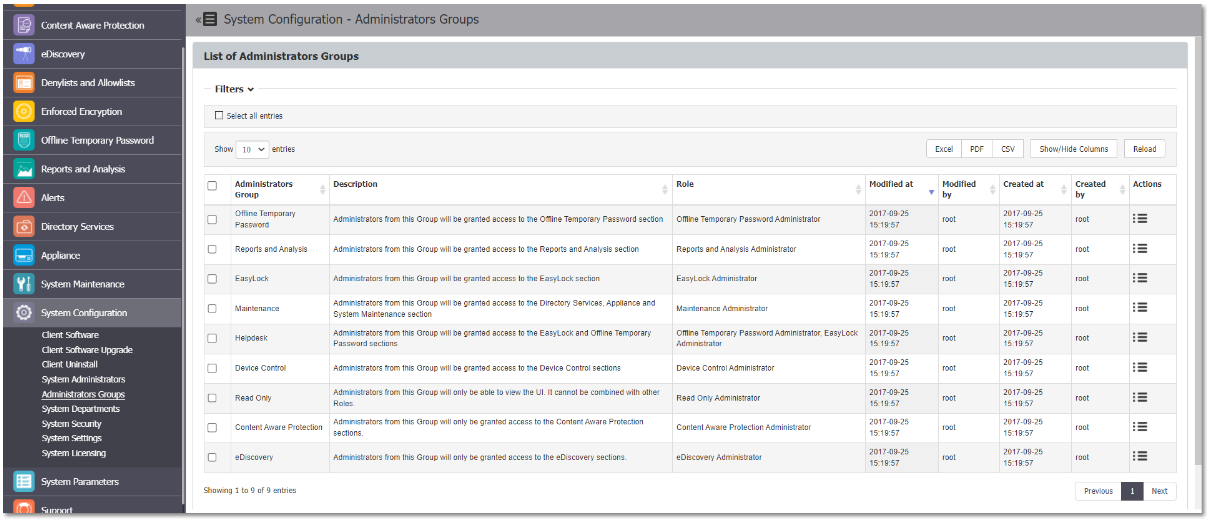
1. Provide the following IDP metadata to your SP provider.
   <?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor entityID="http://www.okta.com/exk7e5bcuA83bA6jL696"

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.



List of Administrators Groups

□ Select all entries

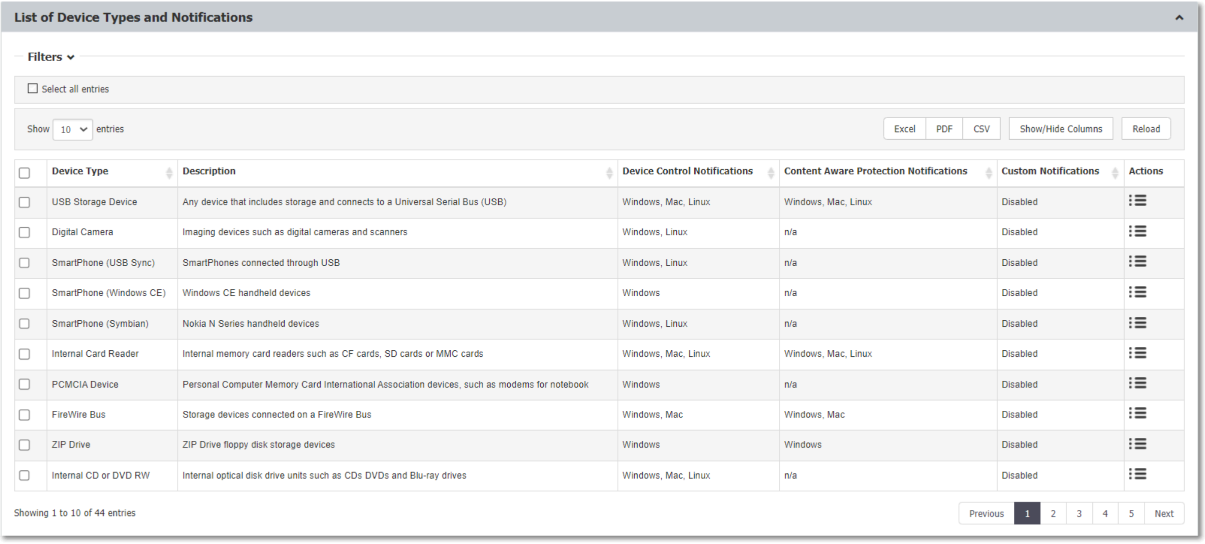
□	Administrators Group	Description	Role	Modified at	Modified by	Created at	Created by	Actions
□	Offline Temporary Password	Administrators from this Group will be granted access to the Offline Temporary Password section	Offline Temporary Password Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Reports and Analysis	Administrators from this Group will be granted access to the Reports and Analysis section	Reports and Analysis Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	EasyLock	Administrators from this Group will be granted access to the EasyLock section	EasyLock Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Maintenance	Administrators from this Group will be granted access to the Directory Services, Appliance and System Maintenance section	Maintenance Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Helpdesk	Administrators from this Group will be granted access to the EasyLock and Offline Temporary Password sections	Offline Temporary Password Administrator, EasyLock Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Device Control	Administrators from this Group will be granted access to the Device Control sections	Device Control Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Read Only	Administrators from this Group will only be able to view the UI. It cannot be combined with other Roles.	Read Only Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Content Aware Protection	Administrators from this Group will only be granted access to the Content Aware Protection sections.	Content Aware Protection Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	eDiscovery	Administrators from this Group will only be granted access to the eDiscovery sections.	eDiscovery Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰

Showing 1 to 9 of 9 entries

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.



List of Device Types and Notifications

Filters

☐ Select all entries

Show 10 entries

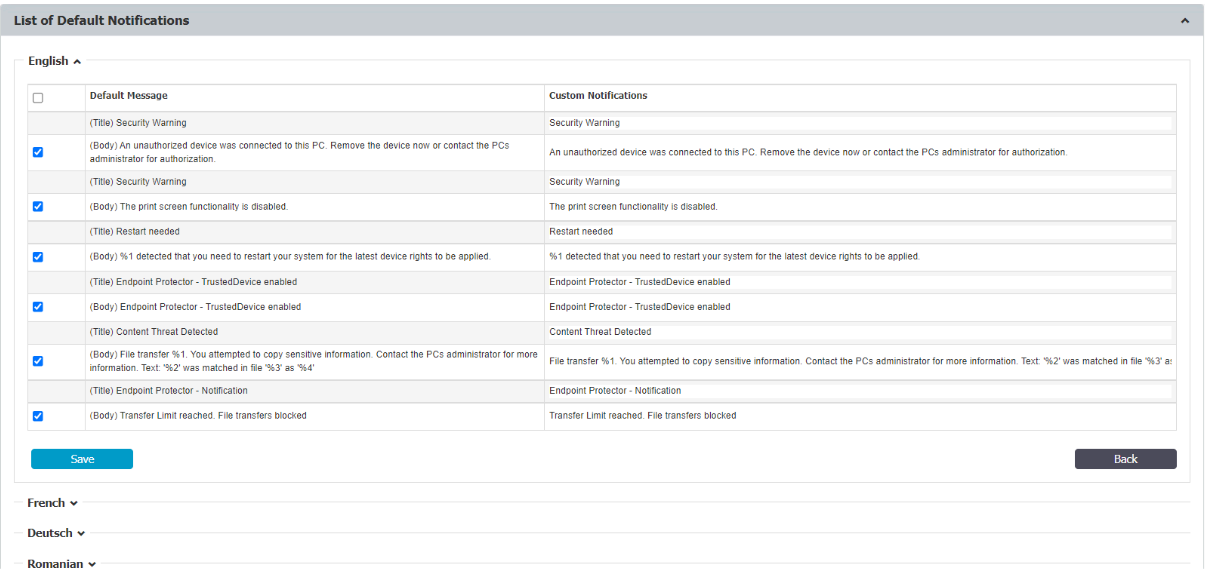
☐	Device Type	Description	Device Control Notifications	Content Aware Protection Notifications	Custom Notifications	Actions
☐	USB Storage Device	Any device that includes storage and connects to a Universal Serial Bus (USB)	Windows, Mac, Linux	Windows, Mac, Linux	Disabled	☰
☐	Digital Camera	Imaging devices such as digital cameras and scanners	Windows, Linux	n/a	Disabled	☰
☐	SmartPhone (USB Sync)	SmartPhones connected through USB	Windows, Linux	n/a	Disabled	☰
☐	SmartPhone (Windows CE)	Windows CE handheld devices	Windows	n/a	Disabled	☰
☐	SmartPhone (Symbian)	Nokia N Series handheld devices	Windows, Linux	n/a	Disabled	☰
☐	Internal Card Reader	Internal memory card readers such as CF cards, SD cards or MMC cards	Windows, Mac, Linux	Windows, Mac, Linux	Disabled	☰
☐	PCMCIA Device	Personal Computer Memory Card International Association devices, such as modems for notebook	Windows	n/a	Disabled	☰
☐	FireWire Bus	Storage devices connected on a FireWire Bus	Windows, Mac	Windows, Mac	Disabled	☰
☐	ZIP Drive	ZIP Drive floppy disk storage devices	Windows	Windows	Disabled	☰
☐	Internal CD or DVD RW	Internal optical disk drive units such as CDs DVDs and Blu-ray drives	Windows, Mac, Linux	n/a	Disabled	☰

Showing 1 to 10 of 44 entries

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.



List of Default Notifications

English

☐	Default Message	Custom Notifications
	(Title) Security Warning	Security Warning
☑	(Body) An unauthorized device was connected to this PC. Remove the device now or contact the PCs administrator for authorization.	An unauthorized device was connected to this PC. Remove the device now or contact the PCs administrator for authorization.
	(Title) Security Warning	Security Warning
☑	(Body) The print screen functionality is disabled.	The print screen functionality is disabled.
	(Title) Restart needed	Restart needed
☑	(Body) %1 detected that you need to restart your system for the latest device rights to be applied.	%1 detected that you need to restart your system for the latest device rights to be applied.
	(Title) Endpoint Protector - TrustedDevice enabled	Endpoint Protector - TrustedDevice enabled
☑	(Body) Endpoint Protector - TrustedDevice enabled	Endpoint Protector - TrustedDevice enabled
	(Title) Content Threat Detected	Content Threat Detected
☑	(Body) File transfer %1. You attempted to copy sensitive information. Contact the PCs administrator for more information. Text: '%2' was matched in file '%3' as '%4'	File transfer %1. You attempted to copy sensitive information. Contact the PCs administrator for more information. Text: '%2' was matched in file '%3' a:
	(Title) Endpoint Protector - Notification	Endpoint Protector - Notification
☑	(Body) Transfer Limit reached. File transfers blocked	Transfer Limit reached. File transfers blocked

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.

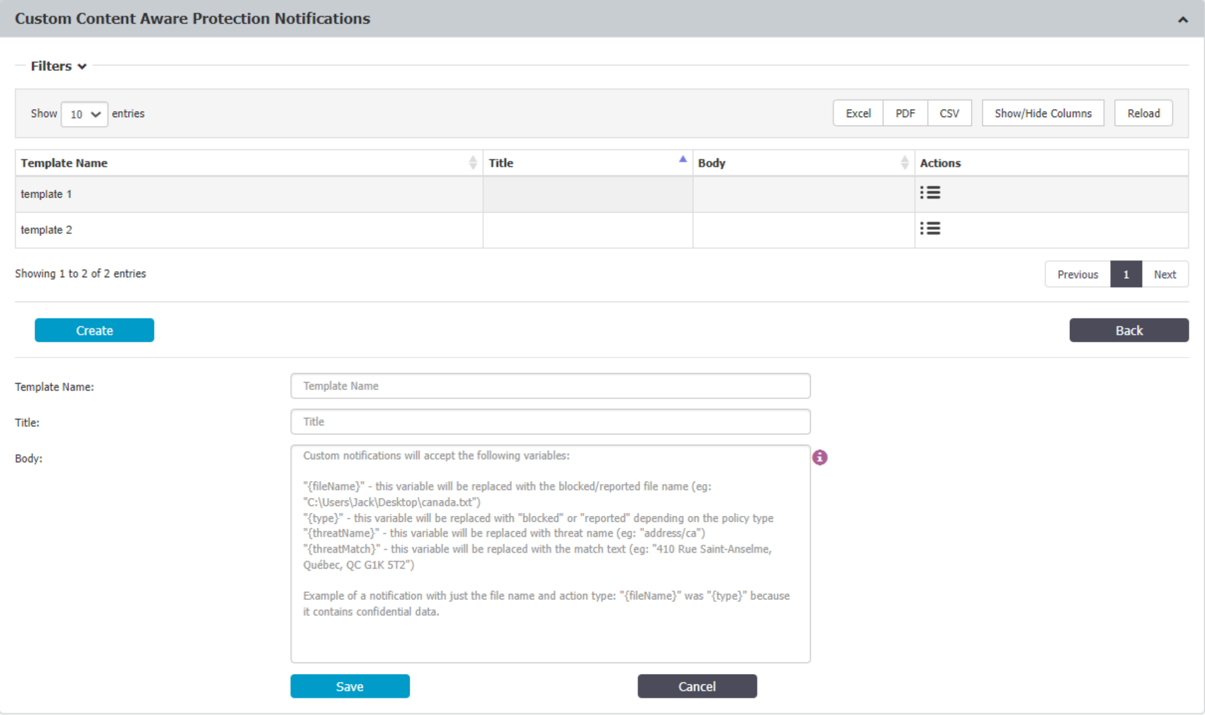
Use these parameters to create your custom message:

- **{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.



Custom Content Aware Protection Notifications

Template Name	Title	Body	Actions
template 1			☰
template 2			☰

Showing 1 to 2 of 2 entries

Template Name:	Template Name
Title:	Title
Body:	Custom notifications will accept the following variables: "{fileName}" - this variable will be replaced with the blocked/reported file name (eg: "C:\Users\Jack\Desktop\canada.txt") "{type}" - this variable will be replaced with "blocked" or "reported" depending on the policy type "{threatName}" - this variable will be replaced with threat name (eg: "address/ca") "{threatMatch}" - this variable will be replaced with the match text (eg: "410 Rue Saint-Anselme, Québec, QC G1K 5T2") Example of a notification with just the file name and action type: "{fileName}" was "{type}" because it contains confidential data.

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:

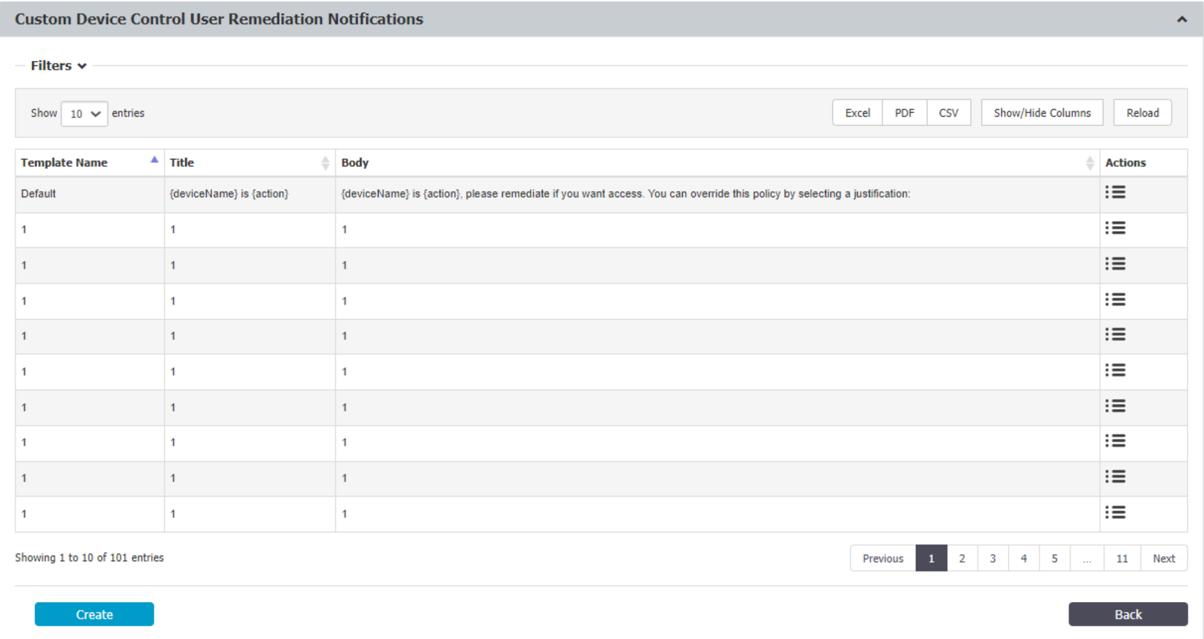
1. Click **Create**
2. Use these parameters to create your custom message:

- **{deviceName}**
- **{action}**

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**.



Custom Device Control User Remediation Notifications

Template Name	Title	Body	Actions
Default	{deviceName} is {action}	{deviceName} is {action}, please remediate if you want access. You can override this policy by selecting a justification:	☰
1	1	1	☰
1	1	1	☰
1	1	1	☰
1	1	1	☰
1	1	1	☰
1	1	1	☰
1	1	1	☰
1	1	1	☰
1	1	1	☰

Showing 1 to 10 of 101 entries

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).

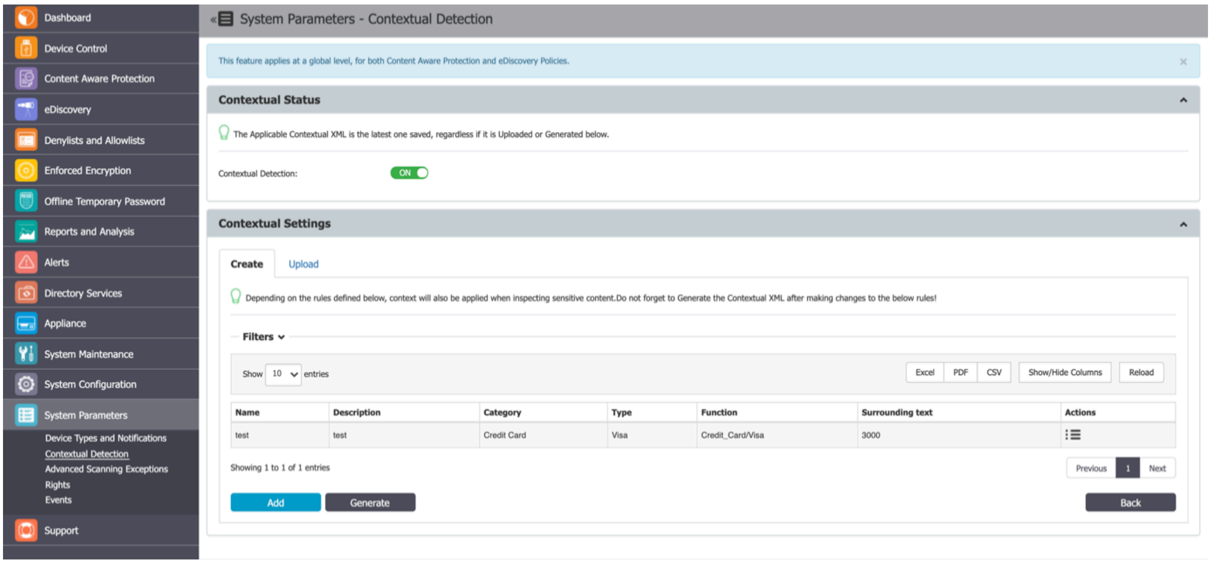
There are two options to create the Contextual rules:

- creating it directly from the Endpoint Protector Server
- manually editing the Contextual XML and then uploading it to the Endpoint Protector Server

Important: To address conflicts between Global and per-policy Contextual Rules, EPP clients no longer receive Global Contextual Rules if at least one policy has its individual Contextual Rule set. This marks the deprecation of Global Contextual Rules, emphasizing the prioritization of individual policy configurations.

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.



System Parameters - Contextual Detection

This feature applies at a global level, for both Content Aware Protection and eDiscovery Policies.

Contextual Status

The Applicable Contextual XML is the latest one saved, regardless if it is Uploaded or Generated below.

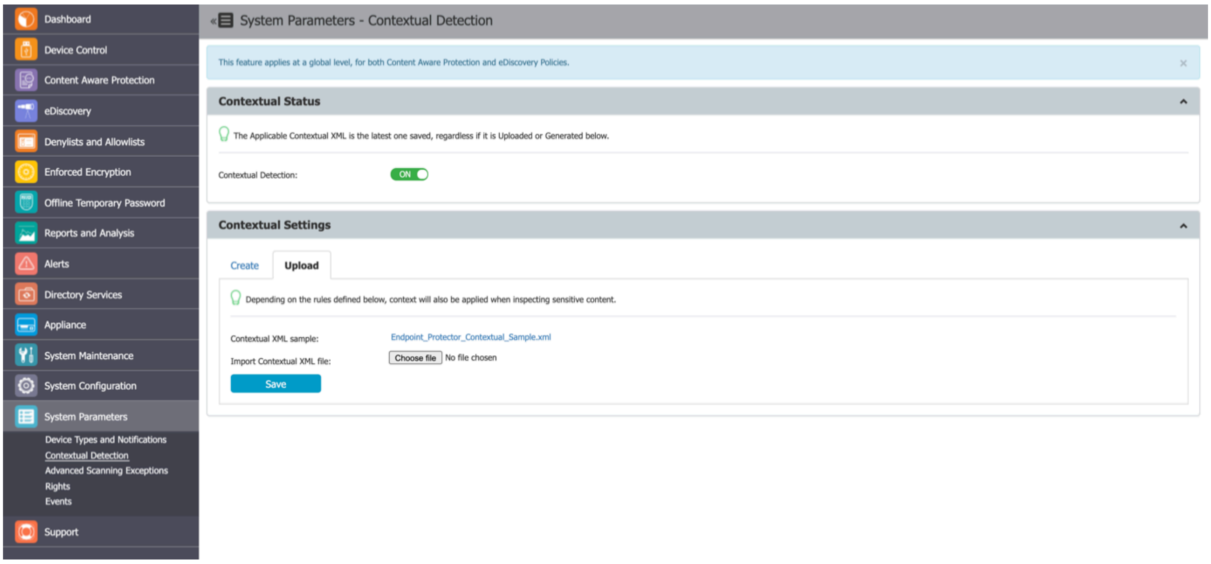
Contextual Detection: ON

Contextual Settings

Depending on the rules defined below, context will also be applied when inspecting sensitive content.Do not forget to Generate the Contextual XML after making changes to the below rules!

Name	Description	Category	Type	Function	Surrounding text	Actions
test	test	Credit Card	Visa	Credit_Card/Visa	3000	☰

Showing 1 to 1 of 1 entries



System Parameters - Contextual Detection

This feature applies at a global level, for both Content Aware Protection and eDiscovery Policies.

Contextual Status

The Applicable Contextual XML is the latest one saved, regardless if it is Uploaded or Generated below.

Contextual Detection: ON

Contextual Settings

Depending on the rules defined below, context will also be applied when inspecting sensitive content.

Contextual XML sample: Endpoint_Protector_Contextual_Sample.xml

Import Contextual XML file: No file chosen

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.
- **Unelated 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

```
 <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

```
 <Keyword id="keywords_Canada_SSN_1">
     <Group matchStyle="word">
            <Term>sin</Term>
                        <Term>social insurance</Term>
```

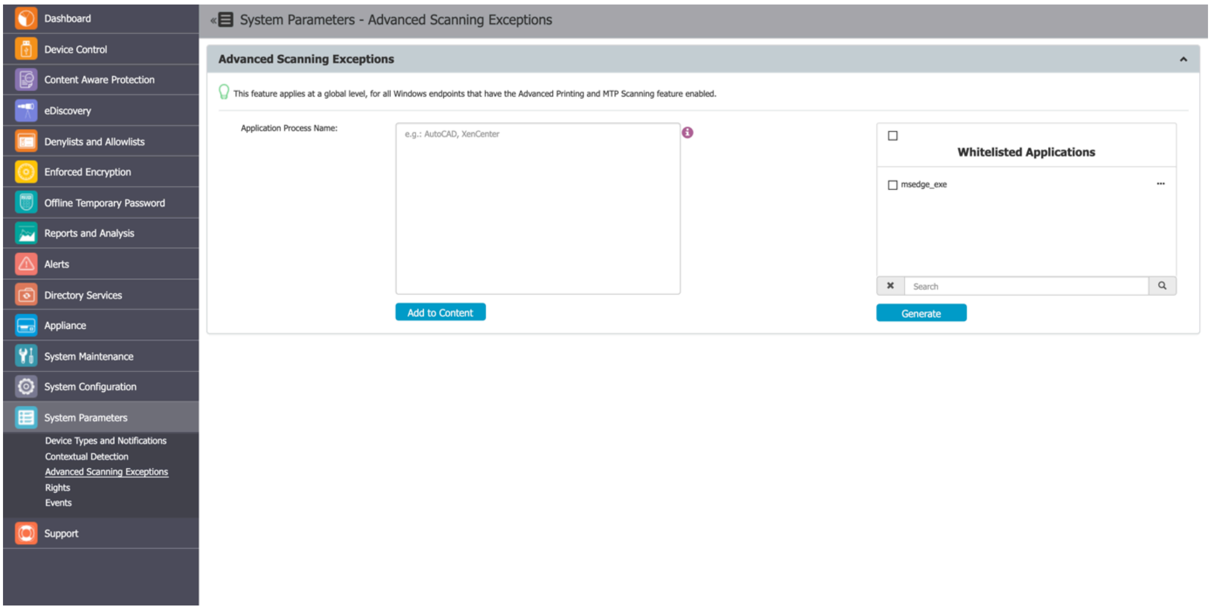
```
             <Term>numero d'assurance sociale</Term>
             <Term>sins</Term>
             <Term>ssn</Term>
             <Term>ssns</Term>
             <Term>social security</Term>
             <Term>numero d'assurance sociale</Term>
             <Term>national identification number</Term>
             <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>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.

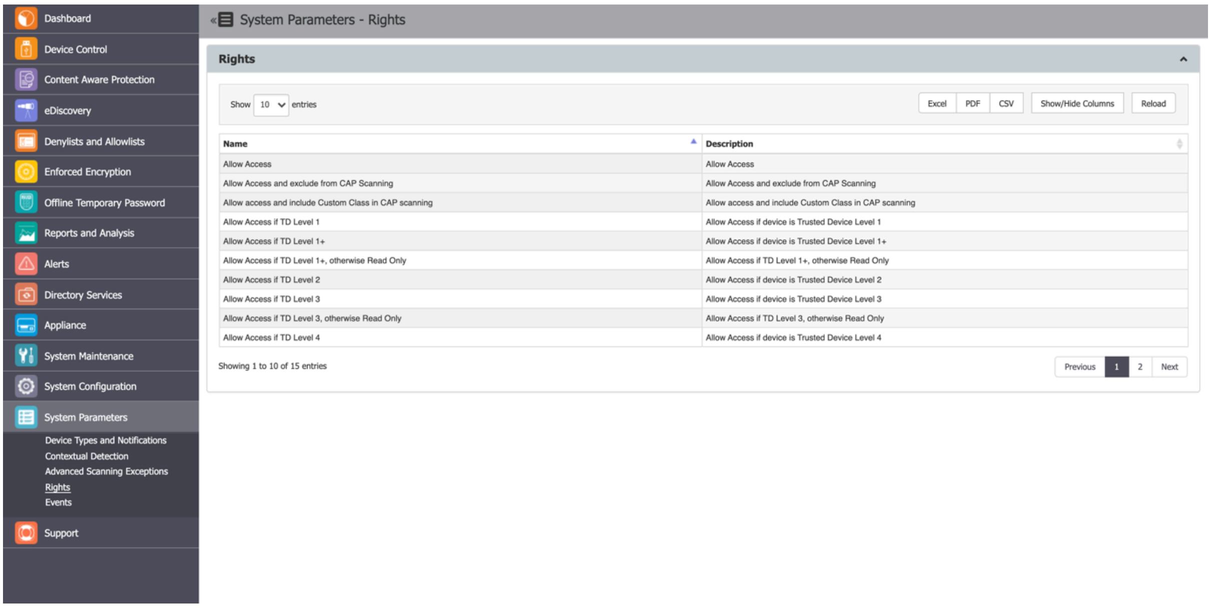


This feature applies at a global level, for all Windows endpoints that have the Advanced Printing and MTP Scanning feature enabled.

Application Process Name: e.g.: AutoCAD, XenCenter

17.4. Rights

This subsection displays a list with all access rights that can be assigned to devices.



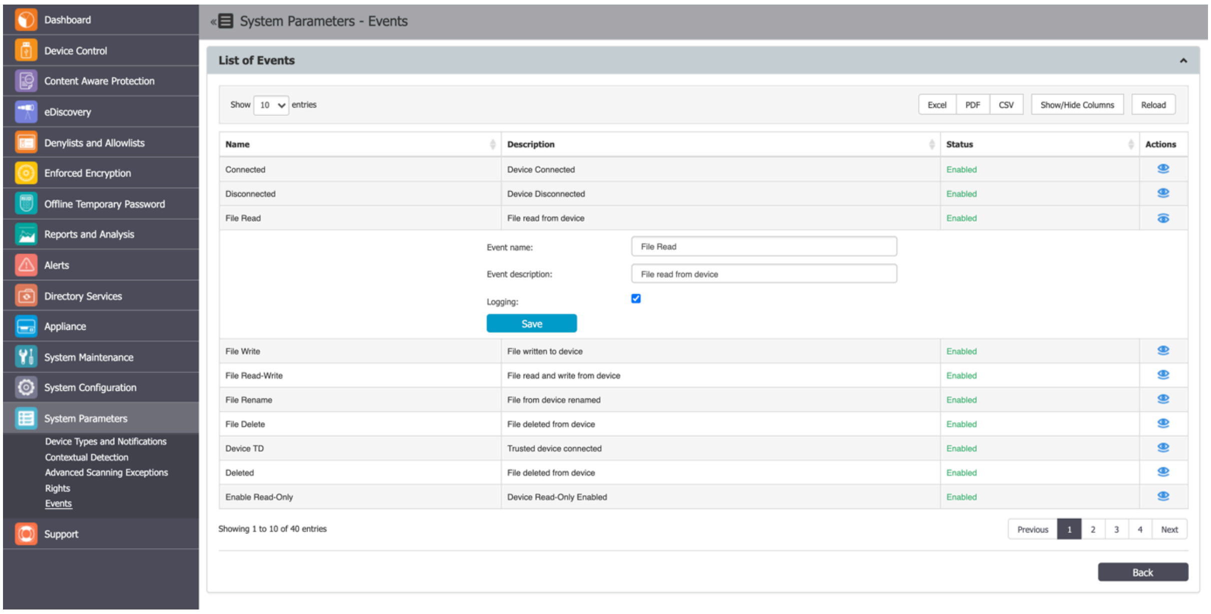
Name	Description
Allow Access	Allow Access
Allow Access and exclude from CAP Scanning	Allow Access and exclude from CAP Scanning
Allow access and include Custom Class in CAP scanning	Allow access and include Custom Class in CAP scanning
Allow Access if TD Level 1	Allow Access if device is Trusted Device Level 1
Allow Access if TD Level 1+	Allow Access if device is Trusted Device Level 1+
Allow Access if TD Level 1+, otherwise Read Only	Allow Access if TD Level 1+, otherwise Read Only
Allow Access if TD Level 2	Allow Access if device is Trusted Device Level 2
Allow Access if TD Level 3	Allow Access if device is Trusted Device Level 3
Allow Access if TD Level 3, otherwise Read Only	Allow Access if TD Level 3, otherwise Read Only
Allow Access if TD Level 4	Allow Access if device is Trusted Device Level 4

Showing 1 to 10 of 15 entries

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.



Name	Description	Status	Actions
Connected	Device Connected	Enabled	👁
Disconnected	Device Disconnected	Enabled	👁
File Read	File read from device	Enabled	👁

Event name: File Read

Event description: File read from device

Logging: ☑

Name	Description	Status	Actions
File Write	File written to device	Enabled	👁
File Read-Write	File read and write from device	Enabled	👁
File Rename	File from device renamed	Enabled	👁
File Delete	File deleted from device	Enabled	👁
Device TD	Trusted device connected	Enabled	👁
Deleted	File deleted from device	Enabled	👁
Enable Read-Only	Device Read-Only Enabled	Enabled	👁

Showing 1 to 10 of 40 entries

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.

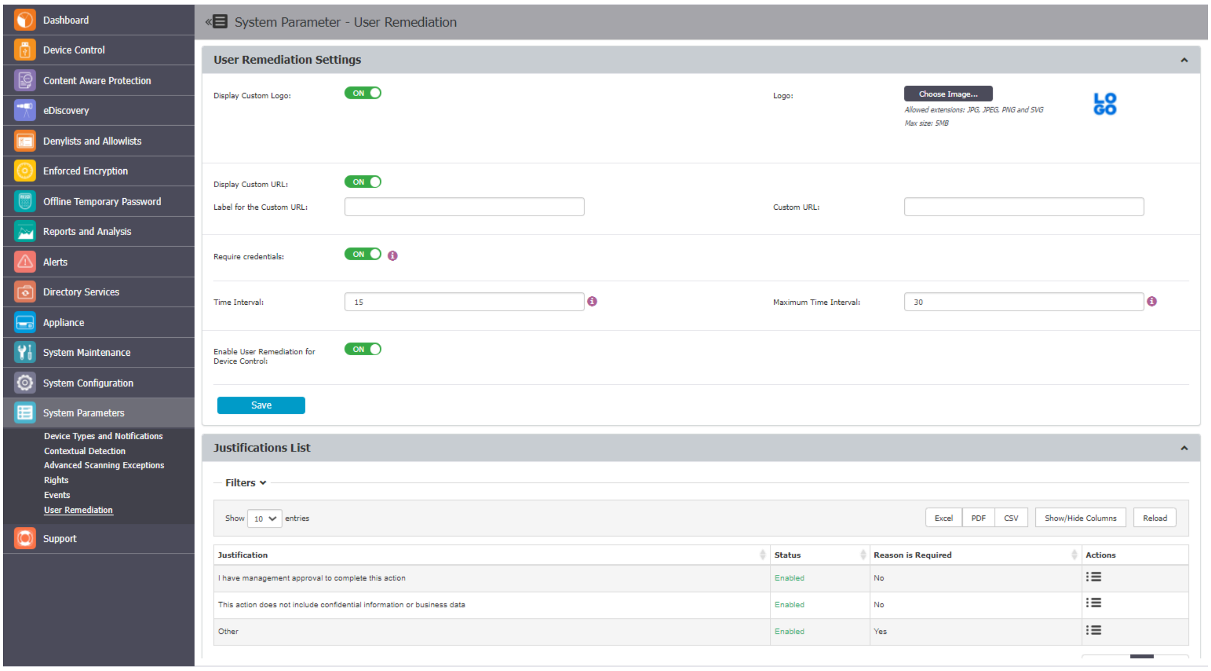
Events Types and Descriptions

Event Name	Description
Connected	Device Connected
Disconnected	Device Disconnected
File Read	File read from device
File Write	File written to device
File Read-Write	File read and write from device
File Rename	File from device renamed
File Delete	File deleted from device
Device TD	Trusted Device™ connected
Deleted	File deleted from device
Enable Read-Only	Device Read-Only Enabled
Enable if TD Level 1	Allows access when a Trusted Device™ is connected (e.g., a USB stick with EasyLock installed, which is automatically launched)
Enable if TD Level 2	Allows access when Trust Level 2 device is connected
Enable if TD Level 3	Allows access when Trust Level 3 device is connected
Enable if TD Level 4	Allows access when Trust Level 4 device is connected
AD Synchronization	AD Synchronization
Blocked	Device or port blocked
Unblocked	Device or port unblocked
Offline Temporary Password Used	Offline Temporary Password Used
User Login	User Login
File Encrypt	File encrypted using EasyLock
File Decrypt	File decrypted using EasyLock
File Encrypt (offline)	File encrypted using EasyLock when not communicating with the Endpoint Protector Server
File Decrypt (offline)	File decrypted using EasyLock when not communicating with the Endpoint Protector Server
Content Threat Detected	Content Aware Protection - Threat Detected
Content Threat Blocked	Content Aware Protection - Threat Blocked

File Copy	A file was copied to or from a removable device
Content Threat Discovered	eDiscovery - Threat Discovered
eDiscovery Client Action	eDiscovery - Action received successfully
User Logout	User Logout
Client Integrity OK	Endpoint Protector Client Integrity ok
Client Integrity Fail	Endpoint Protector Client Integrity failed
Policies Received	Endpoint Protector Client received policy successfully
Uninstall Attempt	Endpoint Protector Client uninstall attempt
EasyLock - successfully deployed	EasyLock - successfully deployed
EasyLock - deployment failed	EasyLock - deployment failed
File Printed	File sent to printer successfully
User Information Updated	User information updated successfully
Transfer Limit Reached	Transfer Limit Reached
External Repository Upload	File Shadow uploaded to Repository successfully
External Repository Upload Fail	File Shadow uploaded to Repository failed
Content Remediation Session Active	Content Aware Protection - Threat Remediated
Content Remediation Request Canceled by User	Content Aware Protection - User Remediation dialog was closed by the user
Forced Uninstall Attempt	Endpoint Protector Client forced uninstall attempt
Device Remediation Request Canceled by User	Device Control - User Remediation dialog was closed by the user
Device Remediation Session Canceled	Device Temporarily Unlock with User Remediation canceled
Device Remediation Session Active	Device Temporarily Unlocked with User Remediation
Device Remediation Session Ended	Device Temporarily Unlock with User Remediation ended
Certificate added to Keychain/store	Certificate added to Keychain/store successfully
Unplanned Client Termination	Unplanned Client Termination
Artifact Received	Artifact Received
DPI Bypassed Traffic	DPI Bypassed Traffic

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.



System Parameter - User Remediation

User Remediation Settings

Display Custom Logo: ON

Logo: Choose Image...
Allowed extensions: JPG, JPEG, PNG and SVG
Max size: 5MB

Display Custom URL: ON

Label for the Custom URL:

Custom URL:

Require credentials: ON

Time Interval: 15

Maximum Time Interval: 30

Enable User Remediation for Device Control: ON

Save

Justifications List

Filters

Show 10 entries

Excel PDF CSV Show/Hide Columns Reload

Justification	Status	Reason is Required	Actions
I have management approval to complete this action	Enabled	No	☰
This action does not include confidential information or business data	Enabled	No	☰
Other	Enabled	Yes	☰

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**)

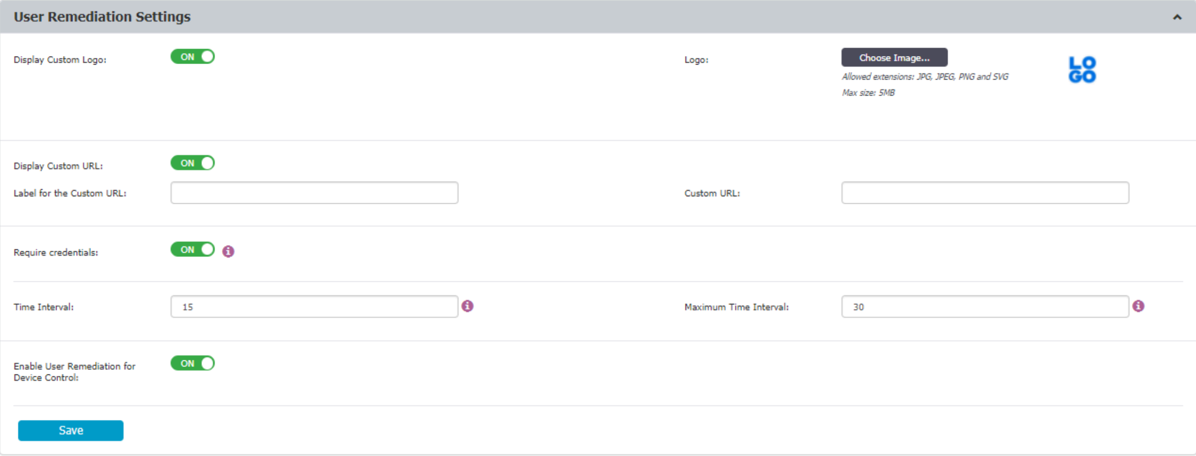
  - ip\username (**192.168.14.140\John**)

- **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.



User Remediation Settings

Display Custom Logo: ON

Logo: Choose Image...

Allowed extensions: JPG, JPEG, PNG and SVG

Max size: 5MB

Display Custom URL: ON

Label for the Custom URL:

Custom URL:

Require credentials: ON

Time Interval: 15

Maximum Time Interval: 30

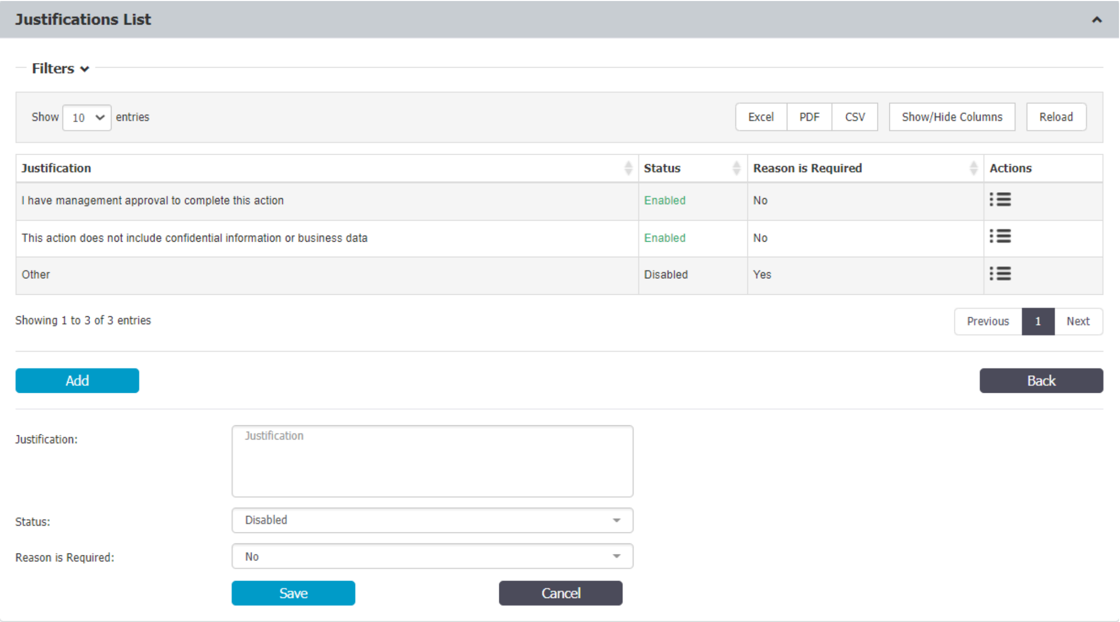
Enable User Remediation for Device Control: ON

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.



Justifications List

Filters

Show 10 entries

Justification	Status	Reason is Required	Actions
I have management approval to complete this action	Enabled	No	☰
This action does not include confidential information or business data	Enabled	No	☰
Other	Disabled	Yes	☰

Showing 1 to 3 of 3 entries

Justification: Justification

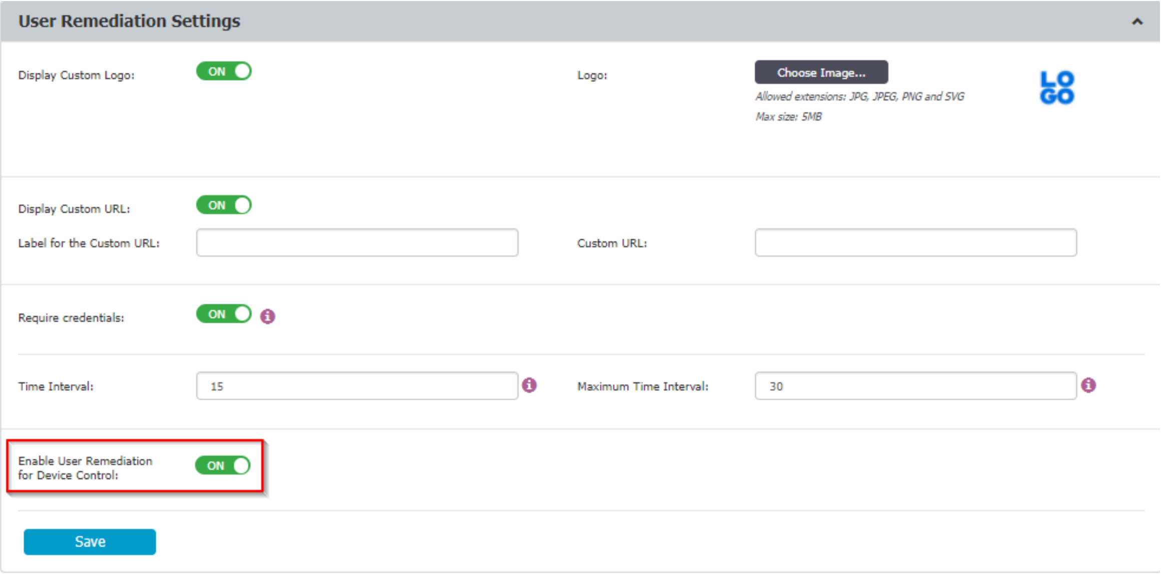
Status: Disabled

Reason is Required: No

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;



User Remediation Settings

Display Custom Logo: ON

Logo: Choose Image...

Allowed extensions: JPG, JPEG, PNG and SVG

Max size: 5MB

Display Custom URL: ON

Label for the Custom URL:

Custom URL:

Require credentials: ON

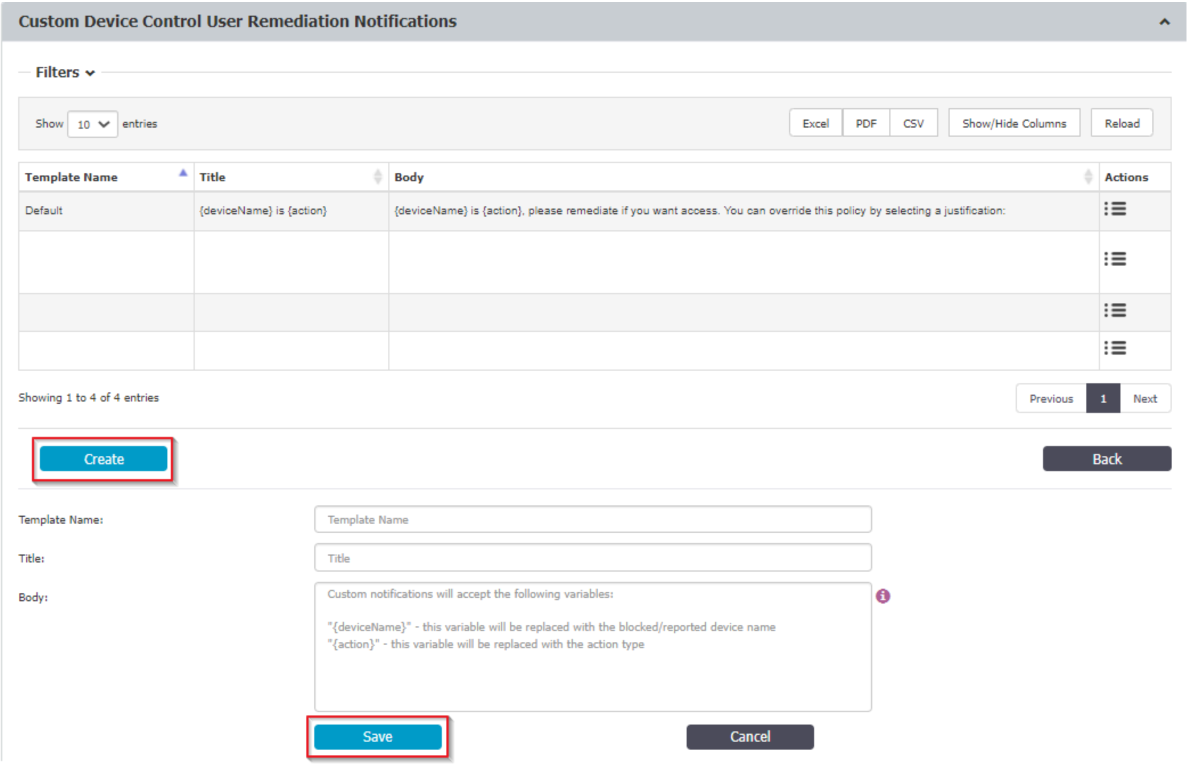
Time Interval: 15

Maximum Time Interval: 30

Enable User Remediation for Device Control: ON

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**;



Custom Device Control User Remediation Notifications

Template Name	Title	Body	Actions
Default	{deviceName} is {action}	{deviceName} is {action}, please remediate if you want access. You can override this policy by selecting a justification:	☰
			☰
			☰
			☰

Showing 1 to 4 of 4 entries

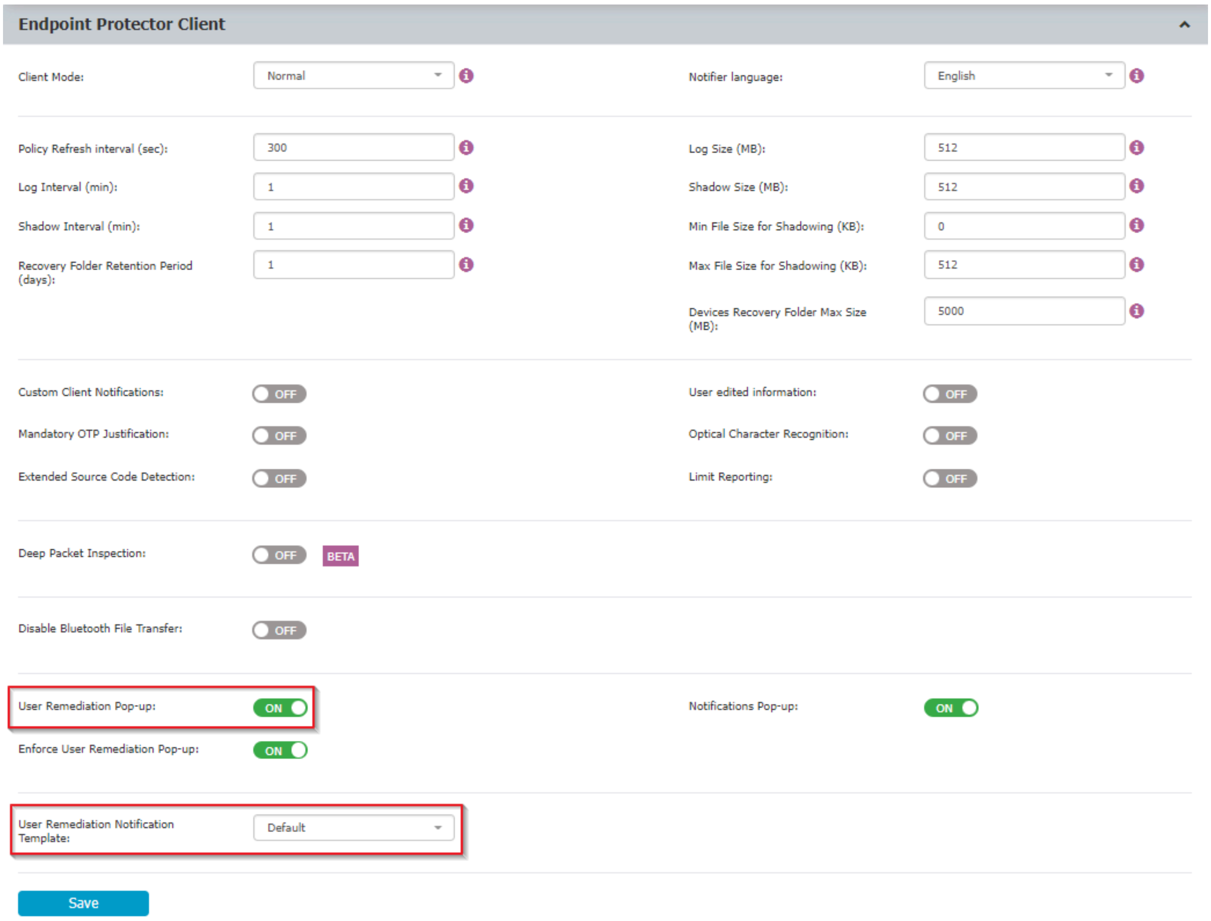
Template Name: Template Name

Title: Title

Body: Custom notifications will accept the following variables:

"{deviceName}" - this variable will be replaced with the blocked/reported device name
"{action}" - this variable will be replaced with the action type

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;

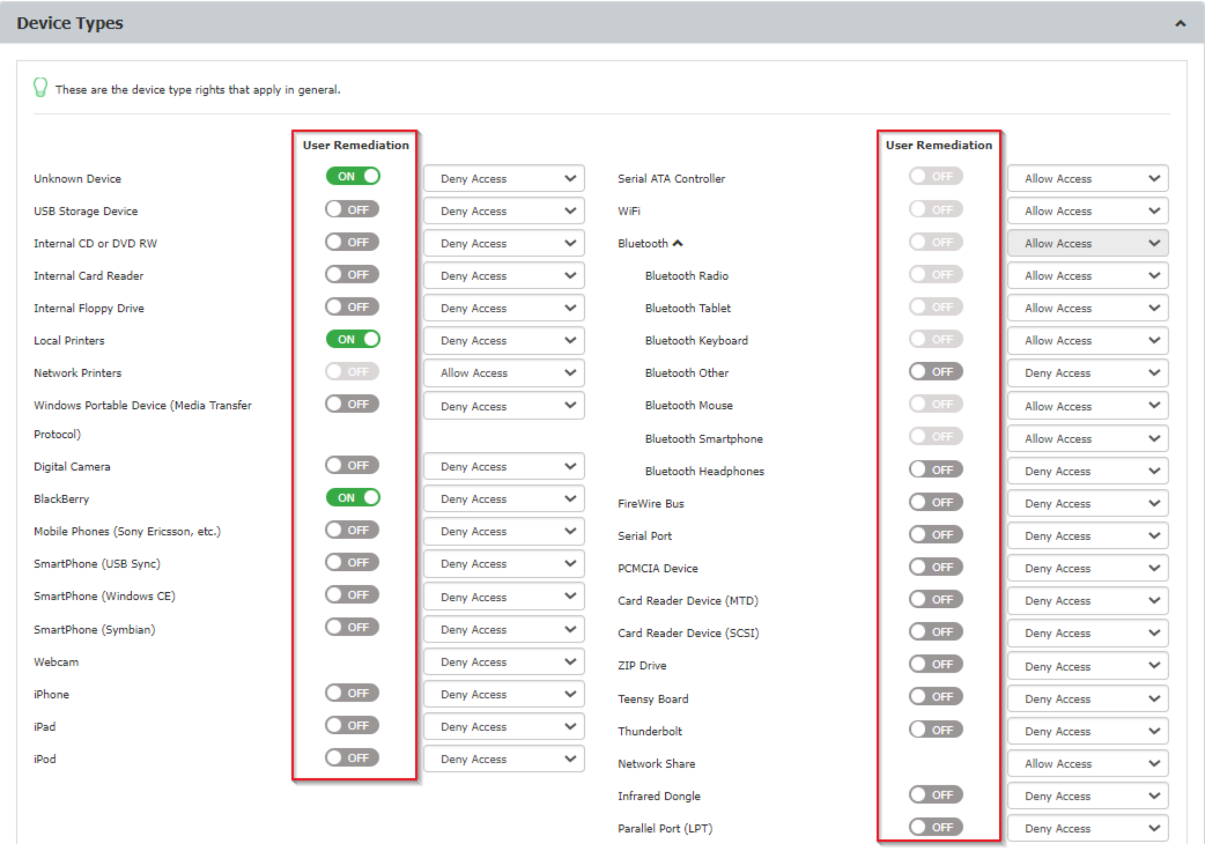


Endpoint Protector Client

Client Mode:	Normal	Notifier language:	English
Policy Refresh interval (sec):	300	Log Size (MB):	512
Log Interval (min):	1	Shadow Size (MB):	512
Shadow Interval (min):	1	Min File Size for Shadowing (KB):	0
Recovery Folder Retention Period (days):	1	Max File Size for Shadowing (KB):	512
		Devices Recovery Folder Max Size (MB):	5000
Custom Client Notifications:	OFF	User edited information:	OFF
Mandatory OTP Justification:	OFF	Optical Character Recognition:	OFF
Extended Source Code Detection:	OFF	Limit Reporting:	OFF
Deep Packet Inspection:	OFF BETA		
Disable Bluetooth File Transfer:	OFF		
User Remediation Pop-up:	ON	Notifications Pop-up:	ON
Enforce User Remediation Pop-up:	ON		
User Remediation Notification Template:	Default		

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.



Device Types

These are the device type rights that apply in general.

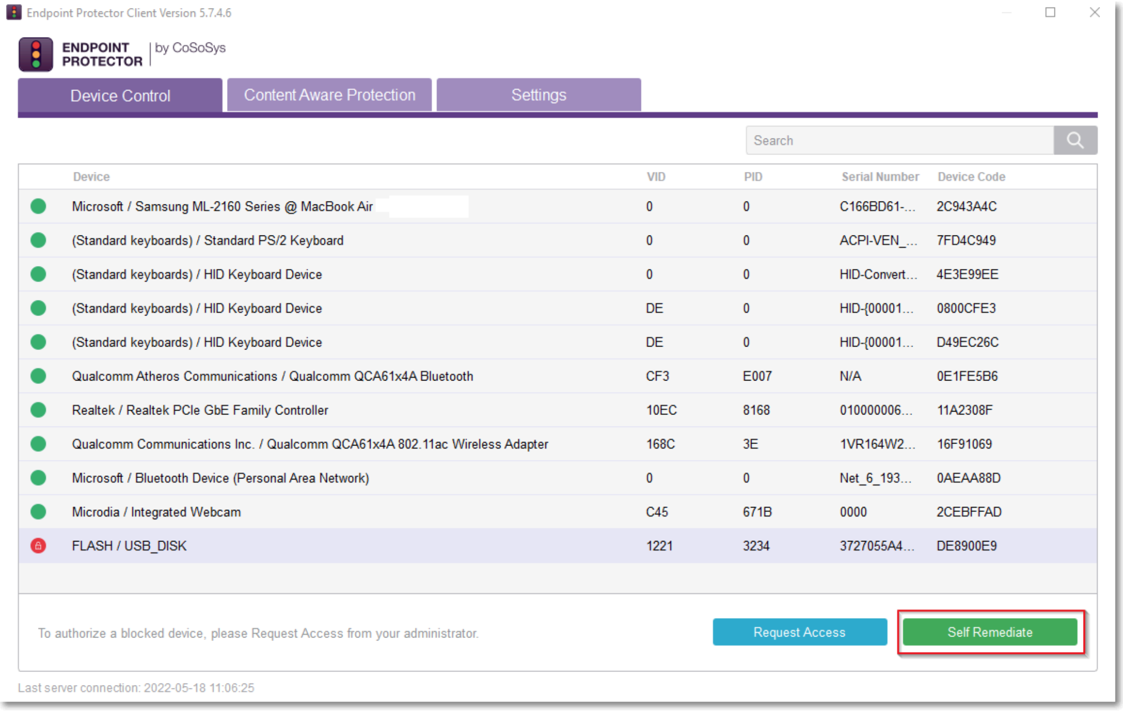
	User Remediation	
Unknown Device	ON	Deny Access
USB Storage Device	OFF	Deny Access
Internal CD or DVD RW	OFF	Deny Access
Internal Card Reader	OFF	Deny Access
Internal Floppy Drive	OFF	Deny Access
Local Printers	ON	Deny Access
Network Printers	OFF	Allow Access
Windows Portable Device (Media Transfer Protocol)	OFF	Deny Access
Digital Camera	OFF	Deny Access
BlackBerry	ON	Deny Access
Mobile Phones (Sony Ericsson, etc.)	OFF	Deny Access
SmartPhone (USB Sync)	OFF	Deny Access
SmartPhone (Windows CE)	OFF	Deny Access
SmartPhone (Symbian)	OFF	Deny Access
Webcam		Deny Access
iPhone	OFF	Deny Access
iPad	OFF	Deny Access
iPod	OFF	Deny Access

	User Remediation	
Serial ATA Controller	OFF	Allow Access
WiFi	OFF	Allow Access
Bluetooth	OFF	Allow Access
Bluetooth Radio	OFF	Allow Access
Bluetooth Tablet	OFF	Allow Access
Bluetooth Keyboard	OFF	Allow Access
Bluetooth Other	OFF	Deny Access
Bluetooth Mouse	OFF	Allow Access
Bluetooth Smartphone	OFF	Allow Access
Bluetooth Headphones	OFF	Deny Access
FireWire Bus	OFF	Deny Access
Serial Port	OFF	Deny Access
PCMCIA Device	OFF	Deny Access
Card Reader Device (MTD)	OFF	Deny Access
Card Reader Device (SCSI)	OFF	Deny Access
ZIP Drive	OFF	Deny Access
Teensy Board	OFF	Deny Access
Thunderbolt	OFF	Deny Access
Network Share		Allow Access
Infrared Dongle	OFF	Deny Access
Parallel Port (LPT)	OFF	Deny Access

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**;



Endpoint Protector Client Version 5.7.4.6

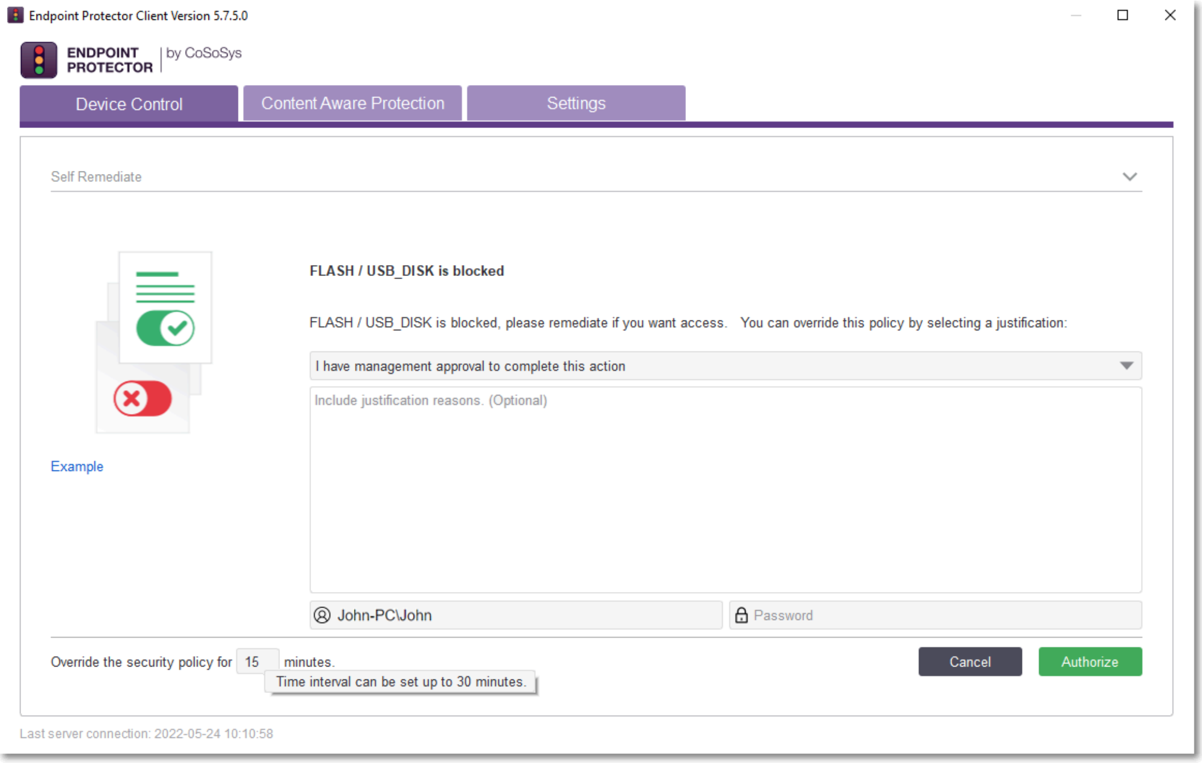
	Device	VID	PID	Serial Number	Device Code
●	Microsoft / Samsung ML-2160 Series @ MacBook Air	0	0	C166BD61-...	2C943A4C
●	(Standard keyboards) / Standard PS/2 Keyboard	0	0	ACPI-VEN_...	7FD4C949
●	(Standard keyboards) / HID Keyboard Device	0	0	HID-Convert...	4E3E99EE
●	(Standard keyboards) / HID Keyboard Device	DE	0	HID-{00001...	0800CFE3
●	(Standard keyboards) / HID Keyboard Device	DE	0	HID-{00001...	D49EC26C
●	Qualcomm Atheros Communications / Qualcomm QCA61x4A Bluetooth	CF3	E007	N/A	0E1FE5B6
●	Realtek / Realtek PCIe GbE Family Controller	10EC	8168	010000006...	11A2308F
●	Qualcomm Communications Inc. / Qualcomm QCA61x4A 802.11ac Wireless Adapter	168C	3E	1VR164W2...	16F91069
●	Microsoft / Bluetooth Device (Personal Area Network)	0	0	Net_6_193...	0AEAA88D
●	Microdia / Integrated Webcam	C45	671B	0000	2CEBFFAD
●	FLASH / USB_DISK	1221	3234	3727055A4...	DE8900E9

To authorize a blocked device, please Request Access from your administrator.

Last server connection: 2022-05-18 11:06:25

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.



FLASH / USB_DISK is blocked

FLASH / USB_DISK is blocked, please remediate if you want access.   You can override this policy by selecting a justification:

I have management approval to complete this action

Include justification reasons. (Optional)

John-PC\John

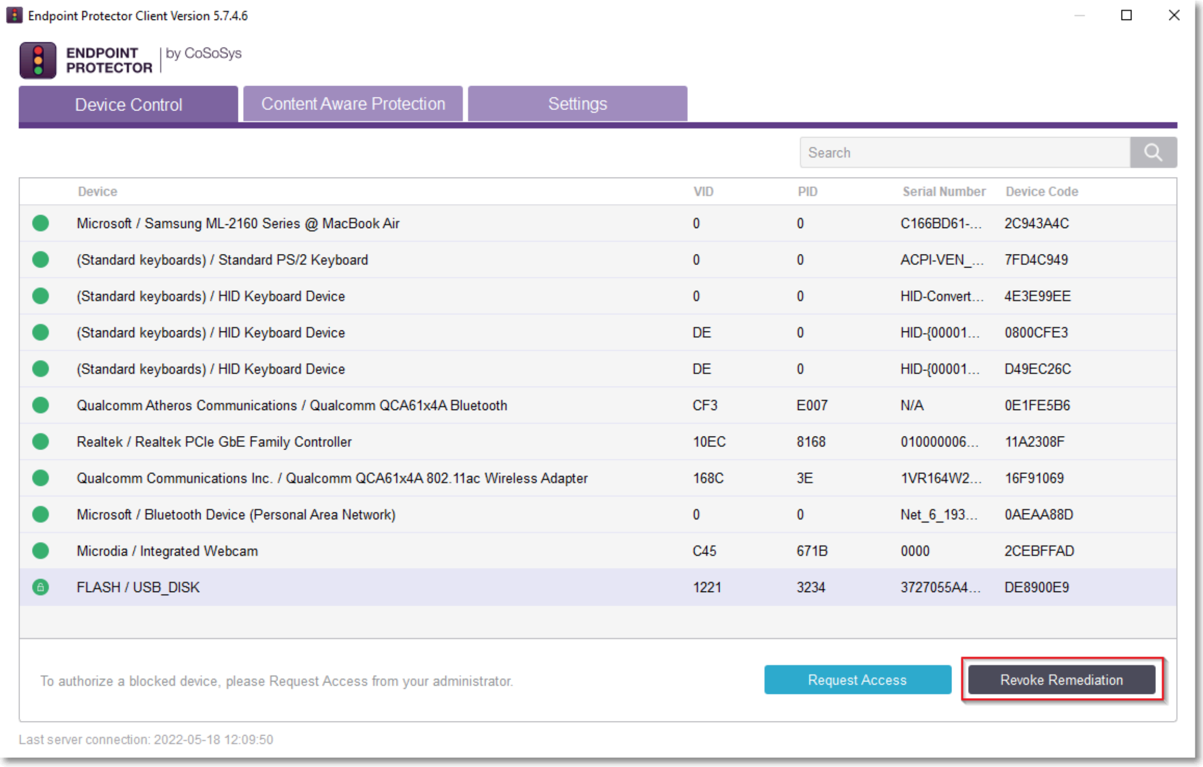
Password

Override the security policy for 15 minutes.

Time interval can be set up to 30 minutes.

Last server connection: 2022-05-24 10:10:58

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**.


Endpoint Protector Client Version 5.7.4.6
ENDPOINT PROTECTOR | by CoSoSys
Device Control
Content Aware Protection
Settings
Search

	Device	VID	PID	Serial Number	Device Code
●	Microsoft / Samsung ML-2160 Series @ MacBook Air	0	0	C166BD61-...	2C943A4C
●	(Standard keyboards) / Standard PS/2 Keyboard	0	0	ACPI-VEN_...	7FD4C949
●	(Standard keyboards) / HID Keyboard Device	0	0	HID-Convert...	4E3E99EE
●	(Standard keyboards) / HID Keyboard Device	DE	0	HID-{00001...	0800CFE3
●	(Standard keyboards) / HID Keyboard Device	DE	0	HID-{00001...	D49EC26C
●	Qualcomm Atheros Communications / Qualcomm QCA61x4A Bluetooth	CF3	E007	N/A	0E1FE5B6
●	Realtek / Realtek PCIe GbE Family Controller	10EC	8168	010000006...	11A2308F
●	Qualcomm Communications Inc. / Qualcomm QCA61x4A 802.11ac Wireless Adapter	168C	3E	1VR164W2...	16F91069
●	Microsoft / Bluetooth Device (Personal Area Network)	0	0	Net_6_193...	0AEAA88D
●	Microdia / Integrated Webcam	C45	671B	0000	2CEBFFAD
🔒	FLASH / USB_DISK	1221	3234	3727055A4...	DE8900E9

To authorize a blocked device, please Request Access from your administrator.

Last server connection: 2022-05-18 12:09:50

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

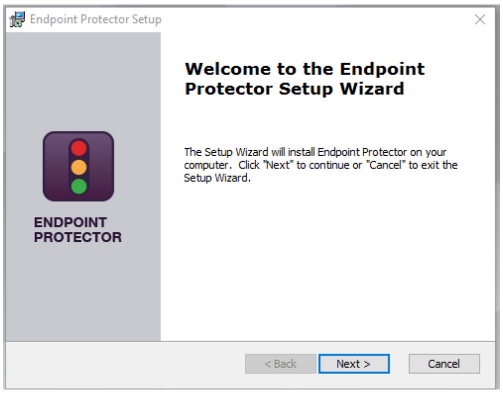
For **Windows** and **Mac**, your input in installing the Endpoint Protector Agent is minimal. The Installation folder and Server information are already preconfigured, and downloadable from the Endpoint Protector Server.

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.

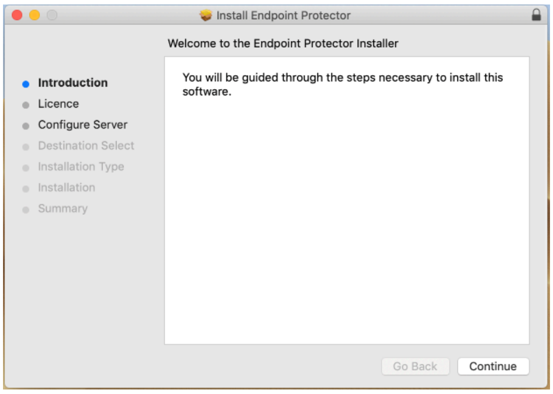
The following are several examples of supported distributions:

- **Ubuntu 14.04+**
- **Mint 18.X**
- **CentOS 7.x**
- **Fedora 29**
- **OpenSUSE 42.2 and 42.3**



Welcome to the Endpoint Protector Setup Wizard

The Setup Wizard will install Endpoint Protector on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

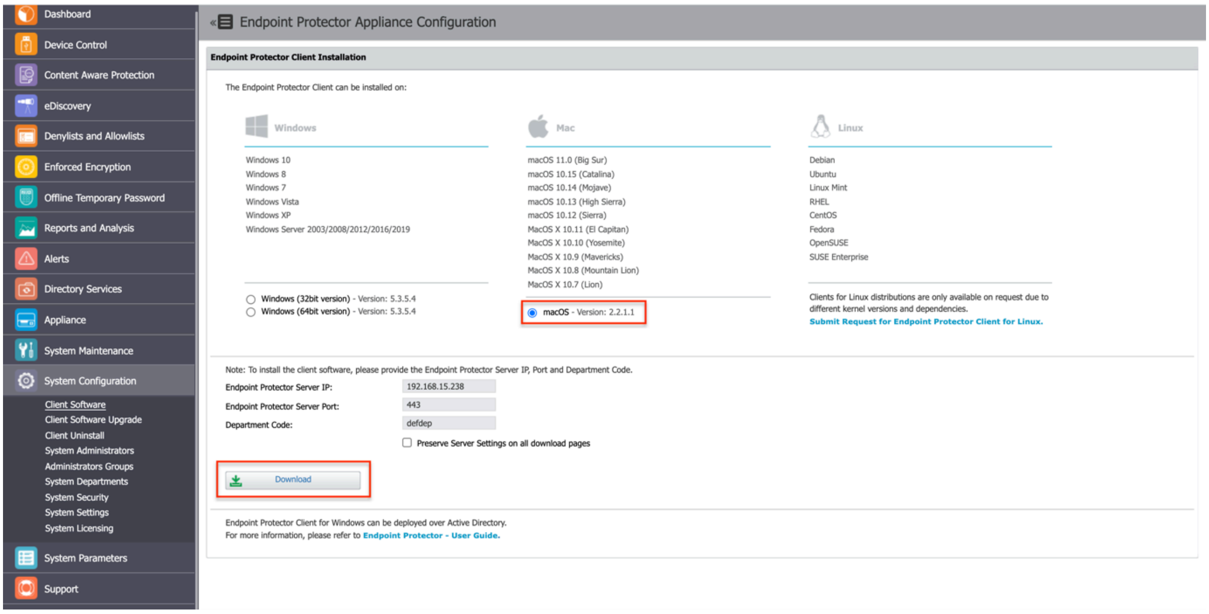


Welcome to the Endpoint Protector Installer

You will be guided through the steps necessary to install this software.

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.



Endpoint Protector Client Installation

The Endpoint Protector Client can be installed on:

Windows 10
Windows 8
Windows 7
Windows Vista
Windows XP
Windows Server 2003/2008/2012/2016/2019

○ Windows (32bit version) - Version: 5.3.5.4
○ Windows (64bit version) - Version: 5.3.5.4

macOS 11.0 (Big Sur)
macOS 10.15 (Catalina)
macOS 10.14 (Mojave)
macOS 10.13 (High Sierra)
macOS 10.12 (Sierra)
MacOS X 10.11 (El Capitan)
MacOS X 10.10 (Yosemite)
MacOS X 10.9 (Mavericks)
MacOS X 10.8 (Mountain Lion)
MacOS X 10.7 (Lion)

● macOS - Version: 2.2.1.1

Debian
Ubuntu
Linux Mint
RHEL
CentOS
Fedora
OpenSUSE
SUSE Enterprise

Clients for Linux distributions are only available on request due to different kernel versions and dependencies.
Submit Request for Endpoint Protector Client for Linux.

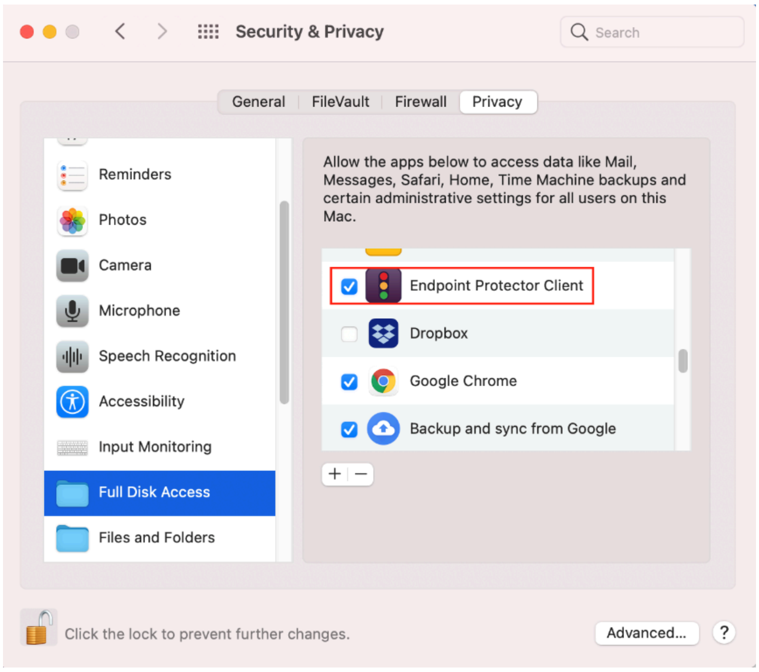
Note: To install the client software, please provide the Endpoint Protector Server IP, Port and Department Code.

Endpoint Protector Server IP:	192.168.15.238
Endpoint Protector Server Port:	443
Department Code:	defdep

□ Preserve Server Settings on all download pages

Endpoint Protector Client for Windows can be deployed over Active Directory.
For more information, please refer to **Endpoint Protector - User Guide.**

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.



Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups and certain administrative settings for all users on this Mac.

☑ Endpoint Protector Client

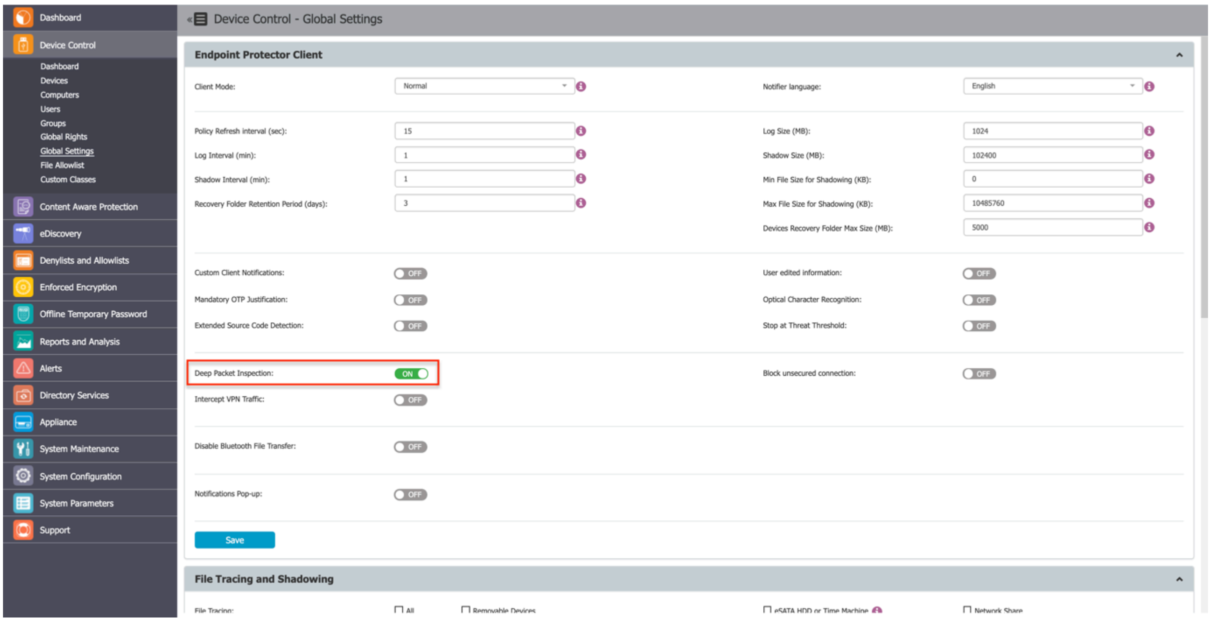
□ Dropbox

☑ Google Chrome

☑ Backup and sync from Google

Click the lock to prevent further changes.

6. Open the Endpoint Protector Server and activate **Deep Packet Inspection** from the Device Control subsection: **Users/Computer/Group/Global Settings**, **Manage Settings**, **Endpoint Protector Client**, **Deep Packet Inspection**.



Device Control - Global Settings

Endpoint Protector Client

Client Mode: Normal

Notifier language: English

Policy Refresh interval (sec): 15

Log Interval (min): 1

Shadow Interval (min): 1

Recovery Folder Retention Period (days): 3

Log Size (MB): 1024

Shadow Size (MB): 102400

Min File Size for Shadowing (KB): 0

Max File Size for Shadowing (KB): 10485760

Devices Recovery Folder Max Size (MB): 5000

Custom Client Notifications: OFF

Mandatory OTP Justification: OFF

Extended Source Code Detection: OFF

User edited information: OFF

Optical Character Recognition: OFF

Stop at Threat Threshold: OFF

Deep Packet Inspection: ON

Block unsecured connection: OFF

Intercept VPN Traffic: OFF

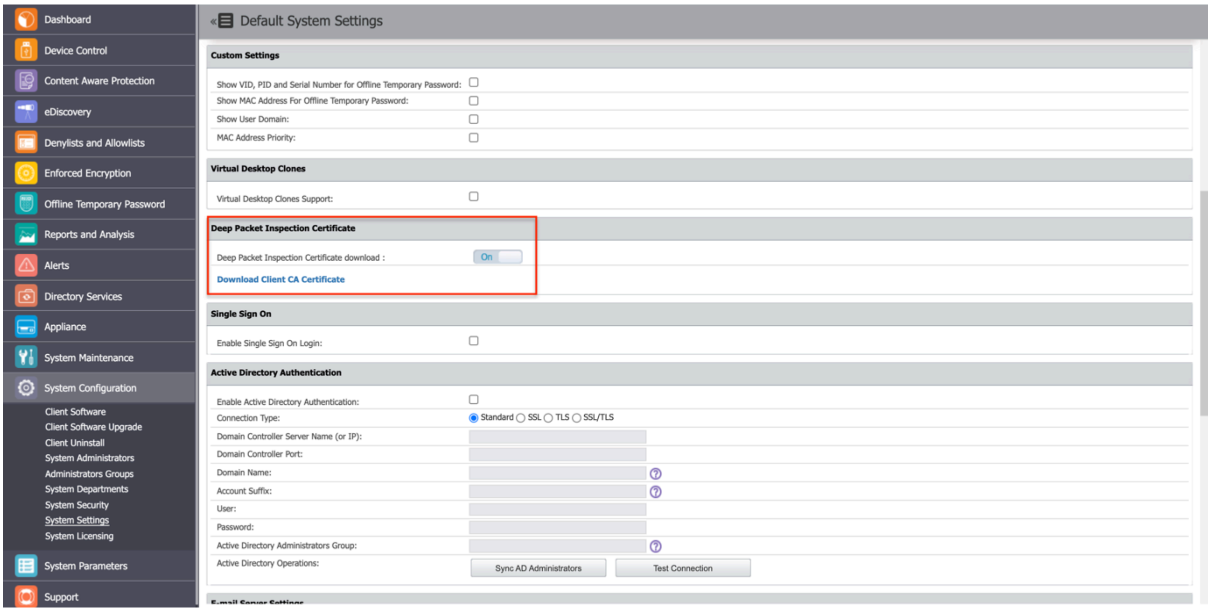
Disable Bluetooth File Transfer: OFF

Notifications Pop-up: OFF

File Tracing and Shadowing

File Tracing: □ All □ Removable Devices □ eSATA HDD or Time Machine □ Network Share

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



Default System Settings

Custom Settings

Show VID, PID and Serial Number for Offline Temporary Password: □
Show MAC Address For Offline Temporary Password: □
Show User Domain: □
MAC Address Priority: □

Virtual Desktop Clones

Virtual Desktop Clones Support: □

Deep Packet Inspection Certificate

Deep Packet Inspection Certificate download : On

Download Client CA Certificate

Single Sign On

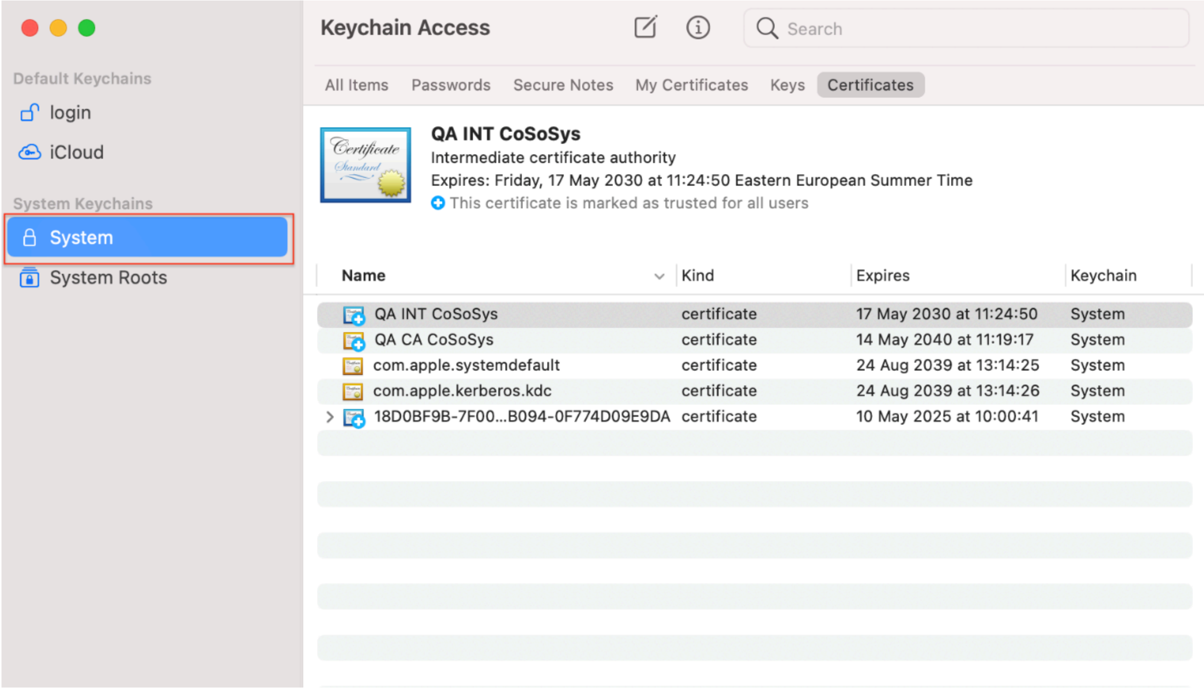
Enable Single Sign On Login: □

Active Directory Authentication

Enable Active Directory Authentication: □
Connection Type: ● Standard ○ SSL ○ TLS ○ SSL/TLS
Domain Controller Server Name (or IP):
Domain Controller Port:
Domain Name:
Account Suffix:
User:
Password:
Active Directory Administrators Group:
Active Directory Operations:

E-mail Server Settings

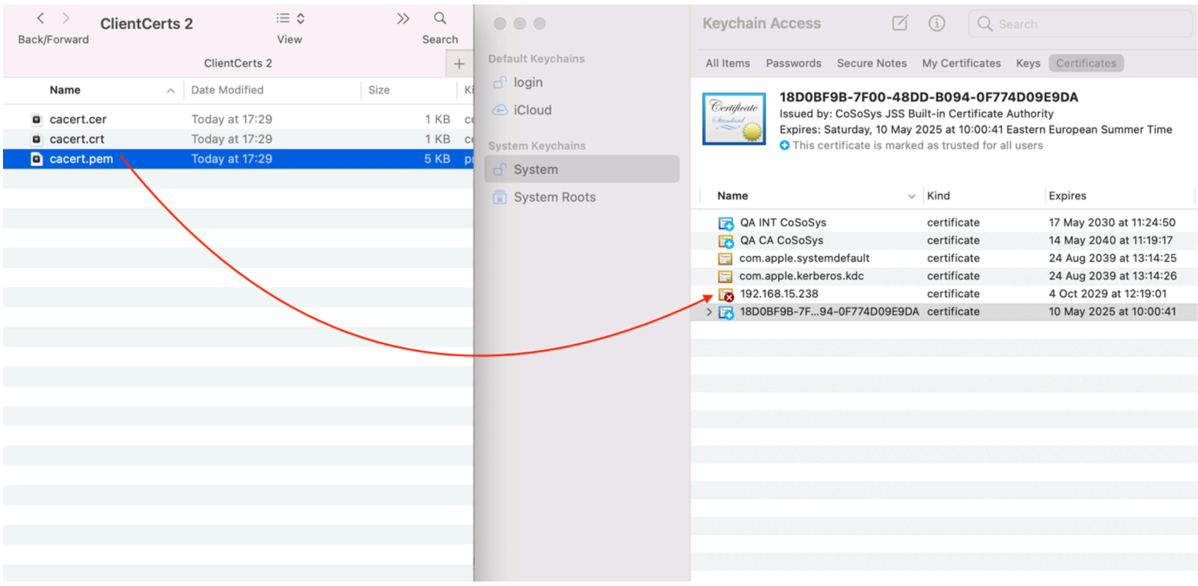
8. Open the **Keychain Access** application from your macOS and select **System**.



QA INT CoSoSys
Intermediate certificate authority
Expires: Friday, 17 May 2030 at 11:24:50 Eastern European Summer Time
This certificate is marked as trusted for all users

Name	Kind	Expires	Keychain
QA INT CoSoSys	certificate	17 May 2030 at 11:24:50	System
QA CA CoSoSys	certificate	14 May 2040 at 11:19:17	System
com.apple.systemdefault	certificate	24 Aug 2039 at 13:14:25	System
com.apple.kerberos.kdc	certificate	24 Aug 2039 at 13:14:26	System
18D0BF9B-7F00...B094-0F774D09E9DA	certificate	10 May 2025 at 10:00:41	System

9. Decompress the downloaded **ClientCerts** file.
10. Select **cacert.pem** file and drag and drop it on **Keychain Access**, **System**

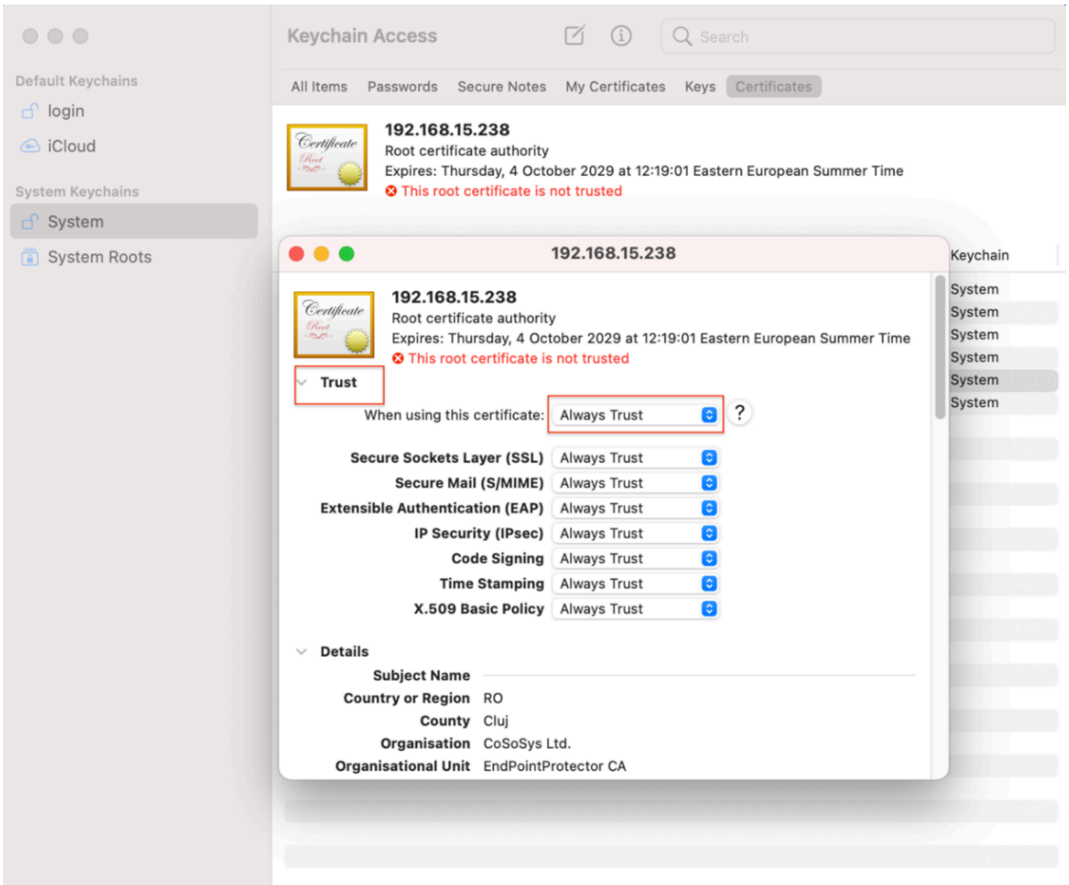


Name	Date Modified	Size
cacert.cer	Today at 17:29	1 KB
cacert.crt	Today at 17:29	1 KB
cacert.pem	Today at 17:29	5 KB

18D0BF9B-7F00-48DD-B094-0F774D09E9DA
Issued by: CoSoSys JSS Built-in Certificate Authority
Expires: Saturday, 10 May 2025 at 10:00:41 Eastern European Summer Time
This certificate is marked as trusted for all users

Name	Kind	Expires
QA INT CoSoSys	certificate	17 May 2030 at 11:24:50
QA CA CoSoSys	certificate	14 May 2040 at 11:19:17
com.apple.systemdefault	certificate	24 Aug 2039 at 13:14:25
com.apple.kerberos.kdc	certificate	24 Aug 2039 at 13:14:26
192.168.15.238	certificate	4 Oct 2029 at 12:19:01
18D0BF9B-7F...94-0F774D09E9DA	certificate	10 May 2025 at 10:00:41

11. Double-click the **x** on the newly added certificate and on the **Trust** section, select **Always Trust**.



192.168.15.238
Root certificate authority
Expires: Thursday, 4 October 2029 at 12:19:01 Eastern European Summer Time
This root certificate is not trusted

192.168.15.238
Root certificate authority
Expires: Thursday, 4 October 2029 at 12:19:01 Eastern European Summer Time
This root certificate is not trusted

Trust

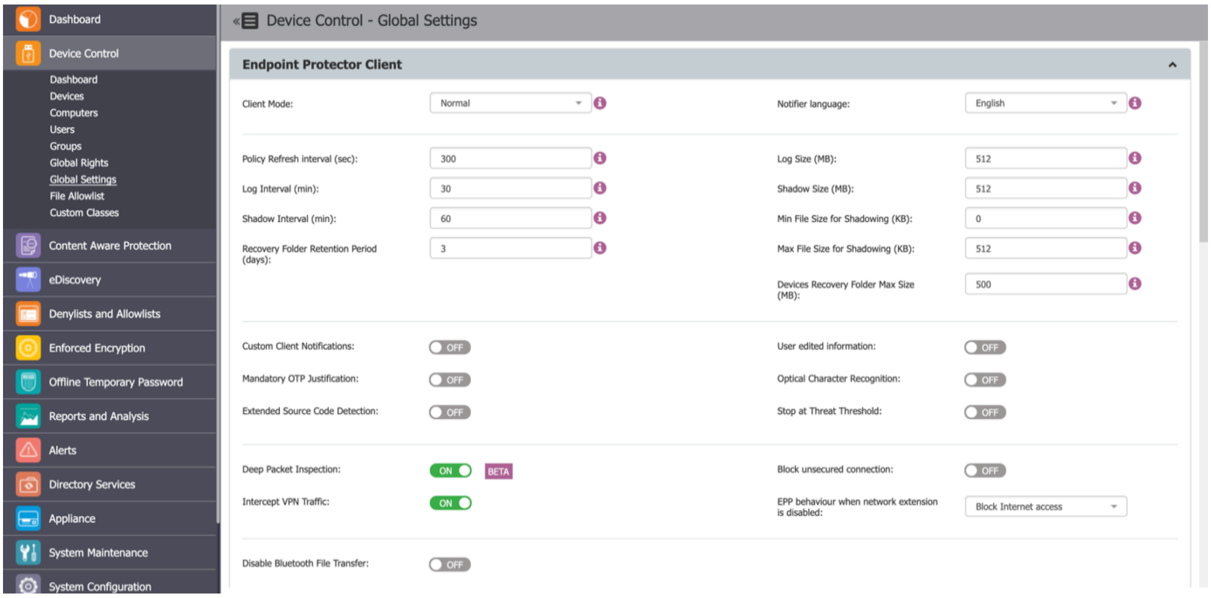
When using this certificate:	Always Trust
Secure Sockets Layer (SSL)	Always Trust
Secure Mail (S/MIME)	Always Trust
Extensible Authentication (EAP)	Always Trust
IP Security (IPsec)	Always Trust
Code Signing	Always Trust
Time Stamping	Always Trust
X.509 Basic Policy	Always Trust

Details

Subject Name	
Country or Region	RO
County	Cluj
Organisation	CoSoSys Ltd.
Organisational Unit	EndPointProtector CA

12. Save the changes.
13. Activate **Intercept VPN Traffic**.
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.



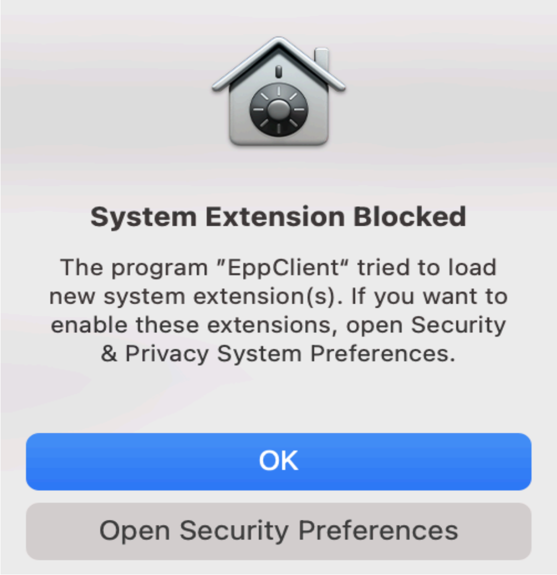
Device Control - Global Settings

Endpoint Protector Client

Client Mode:	Normal	Notifier language:	English
Policy Refresh interval (sec):	300	Log Size (MB):	512
Log Interval (min):	30	Shadow Size (MB):	512
Shadow Interval (min):	60	Min File Size for Shadowing (KB):	0
Recovery Folder Retention Period (days):	3	Max File Size for Shadowing (KB):	512
		Devices Recovery Folder Max Size (MB):	500
Custom Client Notifications:	OFF	User edited information:	OFF
Mandatory OTP Justification:	OFF	Optical Character Recognition:	OFF
Extended Source Code Detection:	OFF	Stop at Threat Threshold:	OFF
Deep Packet Inspection:	ON BETA	Block unsecured connection:	OFF
Intercept VPN Traffic:	ON	EPP behaviour when network extension is disabled:	Block Internet access
Disable Bluetooth File Transfer:	OFF		

15. Save the changes.

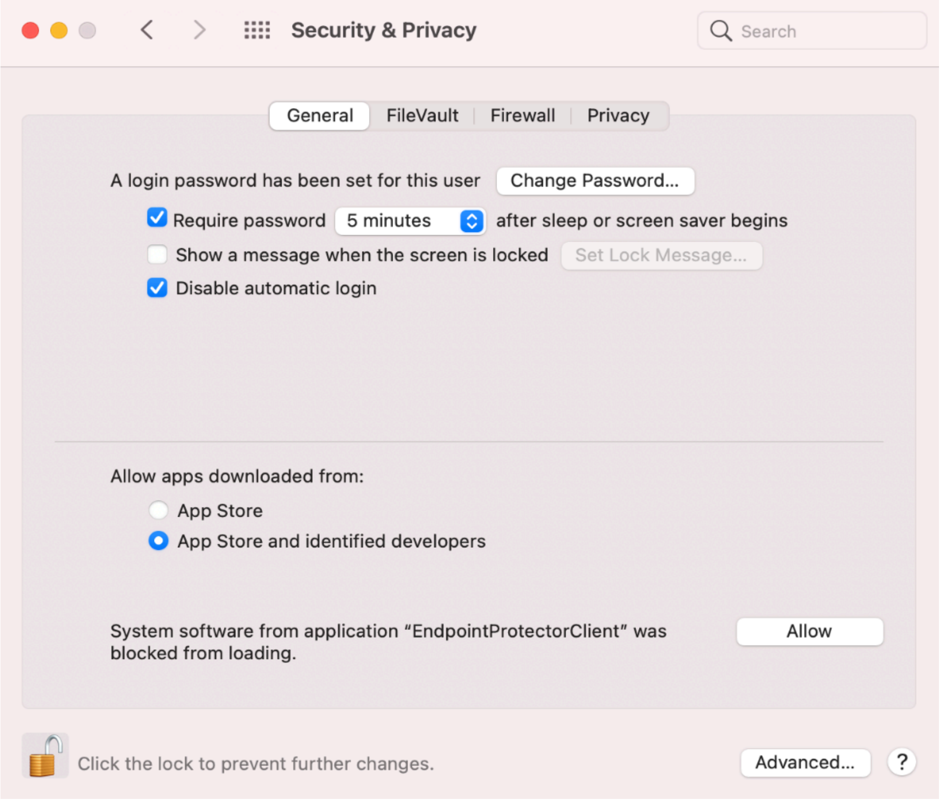
16. The following pop-up will be displayed informing the end-user that a System Extension is blocked and needs to be allowed.



System Extension Blocked

The program "EppClient“ tried to load new system extension(s). If you want to enable these extensions, open Security & Privacy System Preferences.

17. Go to **System Preferences**, **Security and Privacy**, select the **General** tab and allow the Endpoint Protector Client Extension.



Security & Privacy

General | FileVault | Firewall | Privacy

A login password has been set for this user [Change Password...]

☑ Require password [5 minutes] after sleep or screen saver begins

□ Show a message when the screen is locked [Set Lock Message...]

☑ Disable automatic login

Allow apps downloaded from:

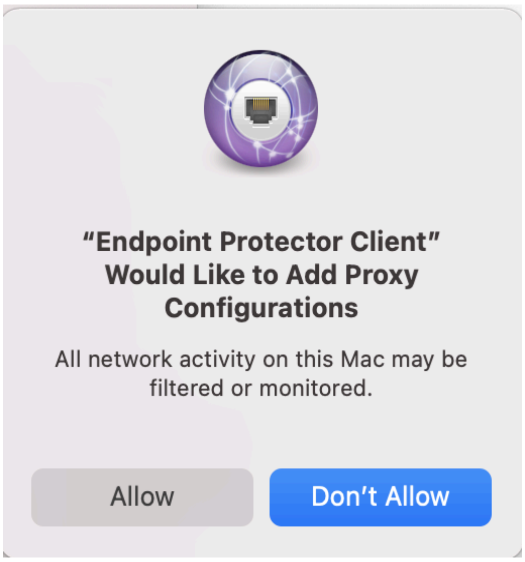
○ App Store

● App Store and identified developers

System software from application “EndpointProtectorClient” was blocked from loading. [Allow]

Click the lock to prevent further changes. [Advanced...] [?]

18. Allow the Endpoint Protector Proxy Configuration from the pop-up window.



“Endpoint Protector Client” Would Like to Add Proxy Configurations

All network activity on this Mac may be filtered or monitored.

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.

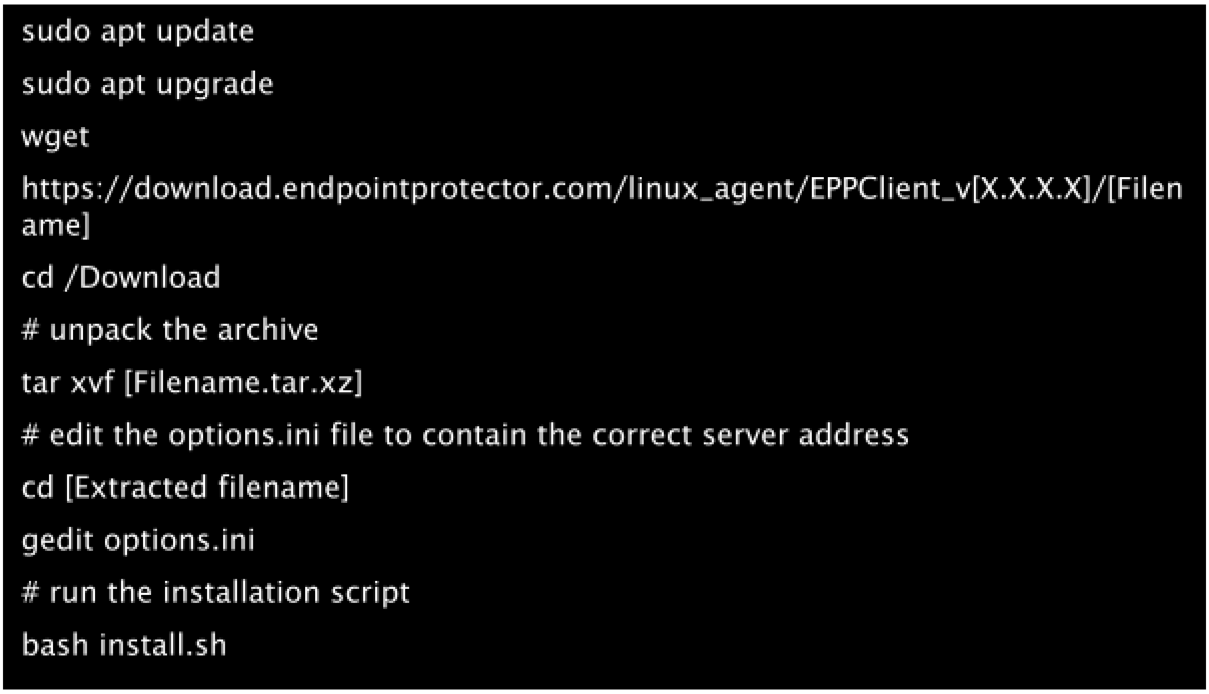
In situations where the EPP client is installed and then uninstalled on macOS, you may still see EPPNotifier in the Notification settings. To remove it from the list, simply right-click and select "Reset notifications."

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**



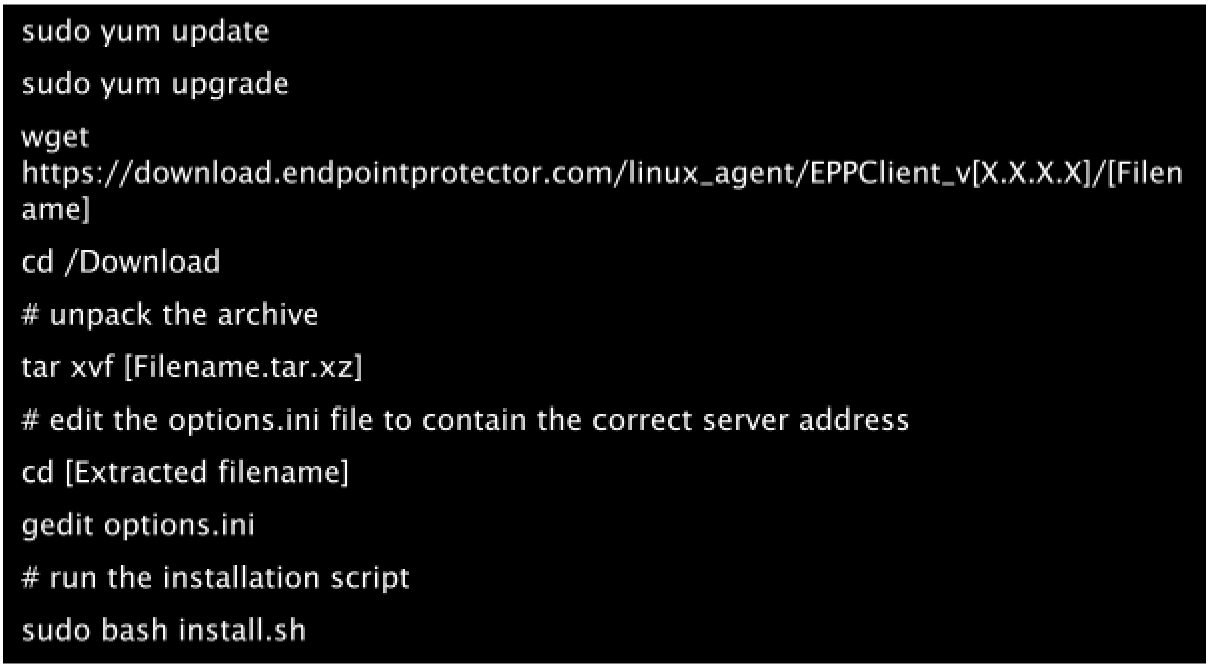
```
sudo apt update
sudo apt upgrade
wget
https://download.endpointprotector.com/linux_agent/EPPClient_v[X.X.X.X]/[Filename]
cd /Download
# unpack the archive
tar xvf [Filename.tar.xz]
# edit the options.ini file to contain the correct server address
cd [Extracted filename]
gedit options.ini
# run the 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.

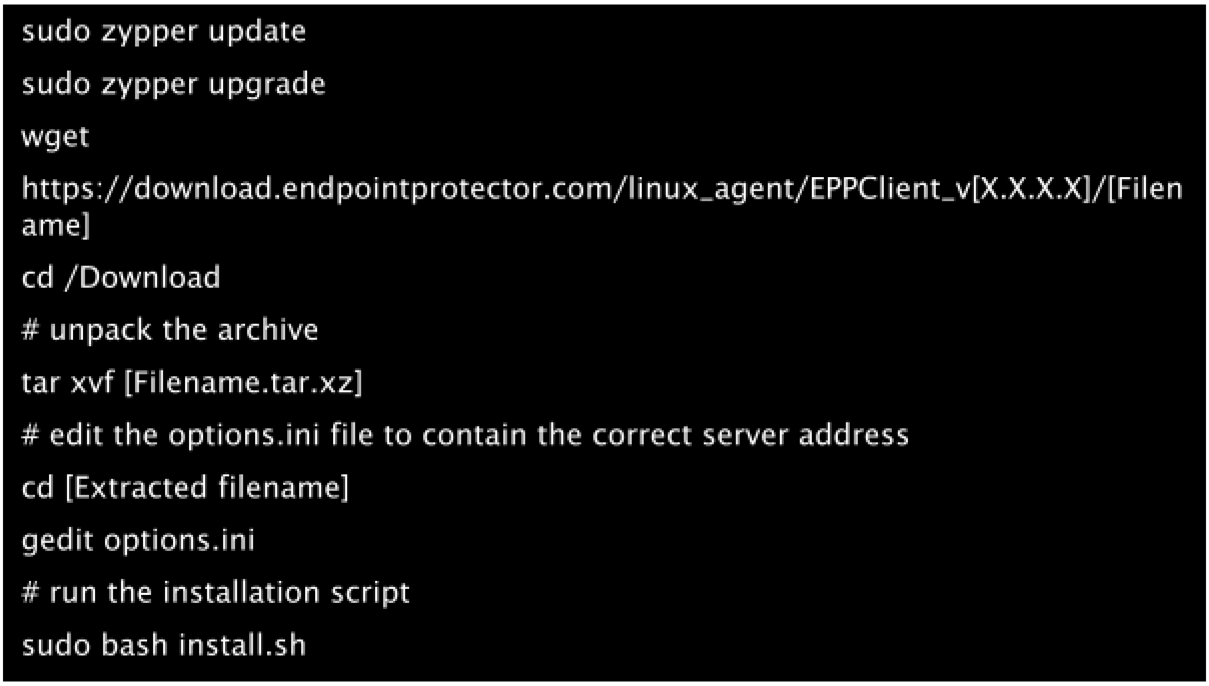
The following are several examples of supported distributions:

- **CentOS 7.x**
- **RedHat 8.x**
- **Fedora 32, 33, 34, 35**
- **AWS Linux 2**



```
sudo yum update
sudo yum upgrade
wget
https://download.endpointprotector.com/linux_agent/EPPClient_v[X.X.X.X]/[Filen
ame]
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**

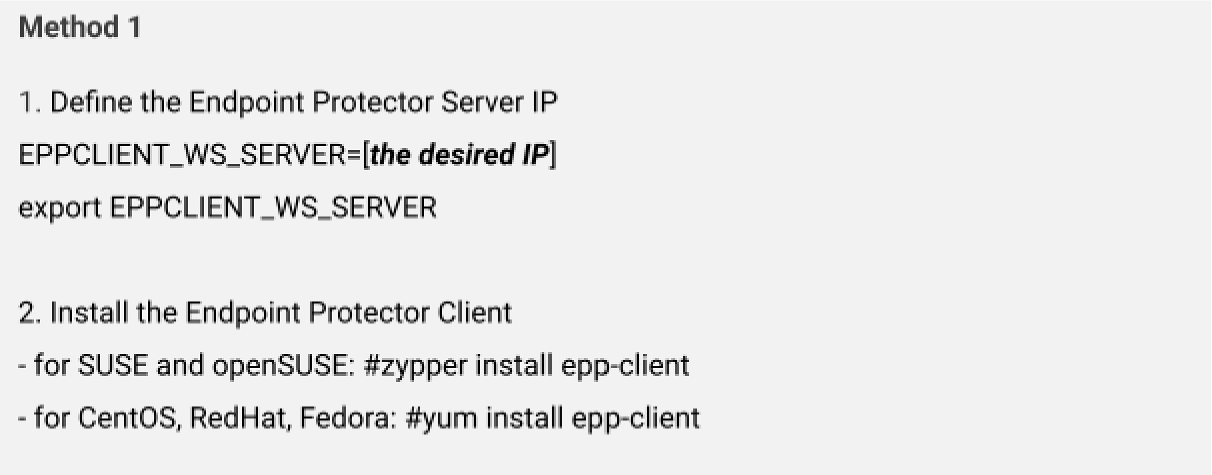


```
sudo zypper update
sudo zypper upgrade
wget
https://download.endpointprotector.com/linux_agent/EPPClient_v[X.X.X.X]/[Filen
ame]
cd /Download
# unpack the archive
tar xvf [Filename.tar.xz]
# edit the options.ini file to contain the correct server address
cd [Extracted filename]
gedit options.ini
# run the installation script
sudo bash install.sh
```

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

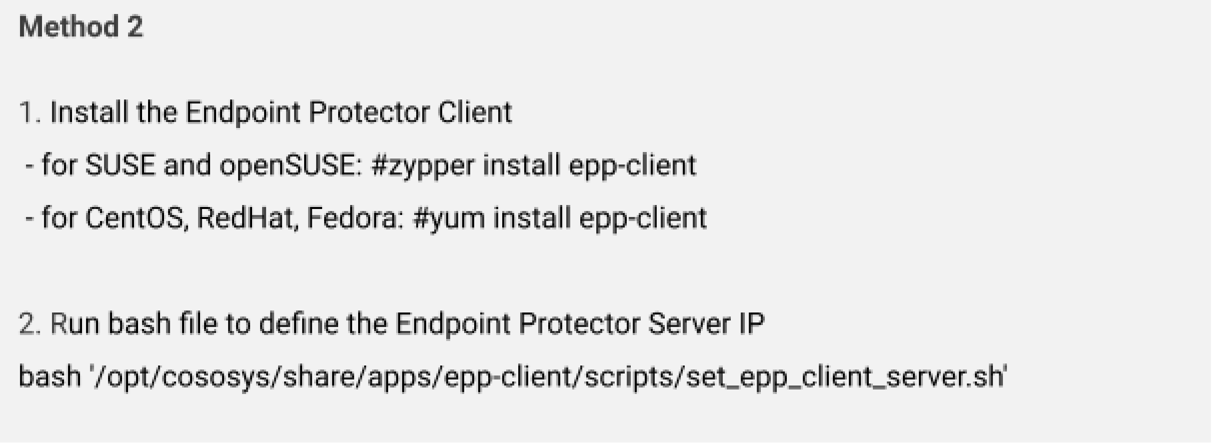
EPPCLIENT_WS_SERVER=[***the desired IP***]

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'
```

19. Endpoint Protector Server – Client communication

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

TLS 1.3 Compatibility			
OS	**Older version**	**Newer version**	**Endpoint Protector Client Particularities**
Windows	❌ Windows 7, XP, and versions older than Windows 10	✓ Windows 10, version 1903 and higher	Uses Windows' built-in TLS encryption engine (Schannel).
macOS	✓	✓	Uses a custom bundled OpenSSL package shipped with the Endpoint Protector Client.
Linux	❌	✓	Uses Linux's built-in OpenSSL engine.

19.2.Endpoint Protector Server

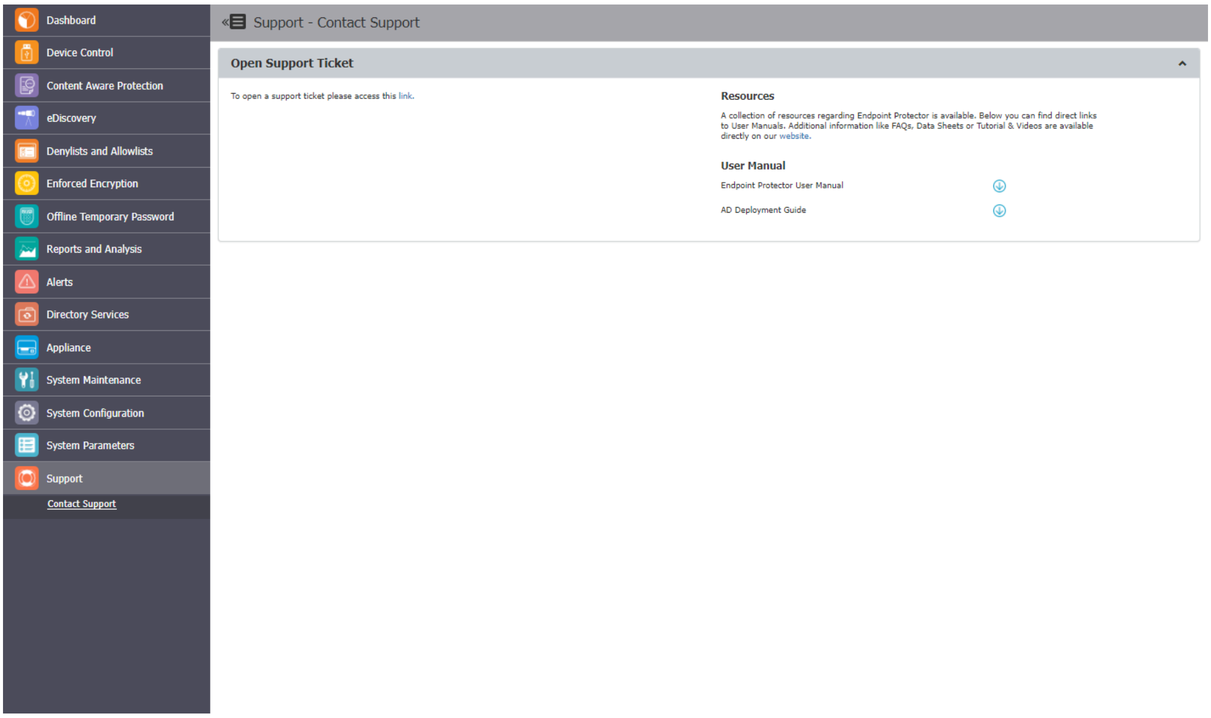
TLS 1.3 Compatibility

Older than 5.7.0.0	
Version 5.7.0.0 or higher	For **in-place upgrades via Live Update**, the Linux OS libraries must be upgraded by Customer Support

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.



To open a support ticket please access this link.

Resources

A collection of resources regarding Endpoint Protector is available. Below you can find direct links to User Manuals. Additional information like FAQs, Data Sheets or Tutorial & Videos are available directly on our website.

User Manual

Endpoint Protector User Manual

AD Deployment Guide

21. Disclaimer

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.

EndpointProtector.com