

SecurIdentity DLP

Installation & Administrator Guide

v1.08_2022

Intellectual property rights

This document is the property of SecurEnvoy No part of this document shall be reproduced, stored in a retrieval system, translated, transcribed, or transmitted by any means without permission from SecurEnvoy.

Information contained within this document is confidential and proprietary to SecurEnvoy and should not be disclosed to anyone other than the recipients and reviewers of this document.

However, in the event of award to SecurEnvoy, this information may be disclosed to and will be used on behalf of and according to the interests of the client to whom it is addressed.

Confidentiality Statement

The descriptive materials and related information in this document contain information that is confidential and proprietary to SecurEnvoy. This information is submitted with the express understanding that it will be held in strict confidence and will not be disclosed, duplicated, or used, in whole or in part, for any purpose other than evaluation of this document.

Copyright © SecurEnvoy, Inc 2022

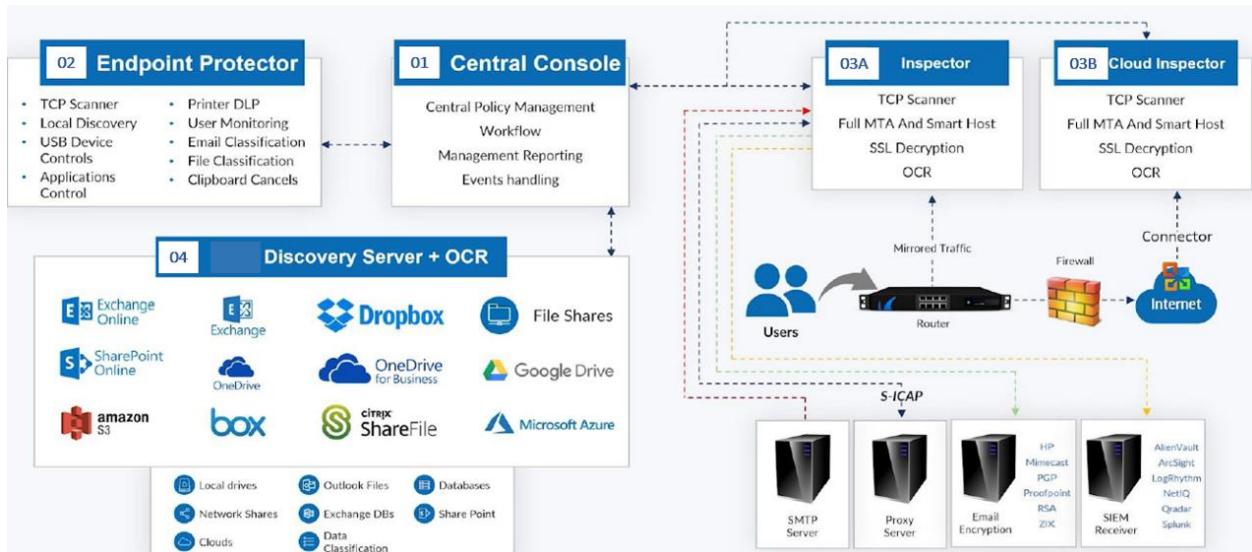
Revision	Author	Reviewer	Date
V1.00_2021	B Norcutt		05/2021
V1.01_2021	B Norcutt		07/2021
V1.02_2021	B Norcutt		08/2021
V1.03_2021	B Norcutt		09/2021
V1.04_2022	B Norcutt		01/2022
V1.05_2022	B Norcutt		01/2022
V1.06_2022	B Norcutt		01/2022 (2)
V1.07_2022	B Norcutt		04/2022
V1.08_2022	S Hanford		09/2022

Contents

Architecture Overview.....	5
Hardware Requirements.....	6
Central Console	6
Network OCR Server	6
Network Inspector	6
Discovery Server	7
Central Console Installation	8
Installation Source	8
Basic Installation.....	8
Central Console Basic Configuration	12
User Role Descriptions.....	13
Backup and Restore	13
Agent Installation	15
Windows Agent Installation	15
Mac Agent Installation	16
Security Manager	17
Installation.....	17
Configuration.....	21
Fingerprinting Files	22
Fingerprinting Databases	26
Adding fingerprints to a rule	26
Policy Management.....	27
Regular Expressions	28
Dictionaries	29
Policy Editor.....	30
Categories	31
Endpoint Protector Controls	34
Network DLP.....	34
Application Controls	37

Copy Controls	39
Other	39
Device Controls.....	40
Files Classification	43
Watermarking.....	45
Off Premise DLP.....	47
Local PC Discovery	47
Email Classification	50
File Share DLP	51
Printing DLP.....	52
MS Outlook Discovery.....	52
Screen Controls	53
Classification Setup.....	54
Classification Schema.....	54
Email Mapping.....	55
DLP Policy Mapping	56
Discovery Targets	58
File Shares	58
MS Exchange	58
MS SharePoint	58
Databases	58
Discovery – Cloud Platforms	58
Amazon S3.....	58
Citrix Sharefile	58
Miscellaneous.....	59
Upgrading the Central Console	59
Ports.....	60
OCR	60
Endpoint Comparison	61
Configure Windows Agent for New Console IP Address.....	62
Collect Agent Log Files	63
Uninstall the Windows Agent.....	63

Architecture Overview



Hardware Requirements

Central Console

The central console is supplied as a pre-packaged CentOS 7 hardened Linux installer

For 100,000 endpoints
Hard Disk Space: 1TB
RAM: 64GB
Number of CPU Cores: 32
NIC: 1

For 10,000 endpoints
Hard Disk Space: 500GB
RAM: 32GB
Number of CPU Cores: 16
NIC: 1

For 1,000 endpoints
Hard Disk Space: 250GB
RAM: 16GB
Number of CPU Cores: 4
NIC: 1

Network OCR Server

AVX2 instructions set available, to verify use Coreinfo
NIC: 1 minimum 2 required for bridge mode

[Coreinfo - Windows Sysinternals | Microsoft Docs](#)

Network Inspector

The Network Inspector is supplied as a pre-packaged CentOS 7 hardened Linux installer

Hard Disk Space: 60GB minimum
RAM: 2GB minimum
Number of CPU Cores: 2 minimum
NIC: 1 minimum more required dependent on deployment

Discovery Server

Hard Disk Space: 60GB minimum

RAM: 2GB minimum per core

Number of CPU Cores: 2 minimum

The Discovery Server scans 1 file per CPU core at a time. The more cores provided, the faster the scanning speed.

Central Console Installation

The SecureIdentity DLP Central Console ISO image contains a hardened and performance tuned 64bit operating system based on CentOS 7 Linux distribution. We guarantee that the system could be installed without any issues on many hardware servers. However, we cannot guarantee 100% compatibility with all brands and models of server platforms.

This guide will cover a generic install on an ESXi server and assumes you know the basics of mounting the iso and configuring the server to meet the minimum requirements.

Installation Source

[Secureenvoy.com/DLP binaries/](https://secureenvoy.com/DLP_binaries/)

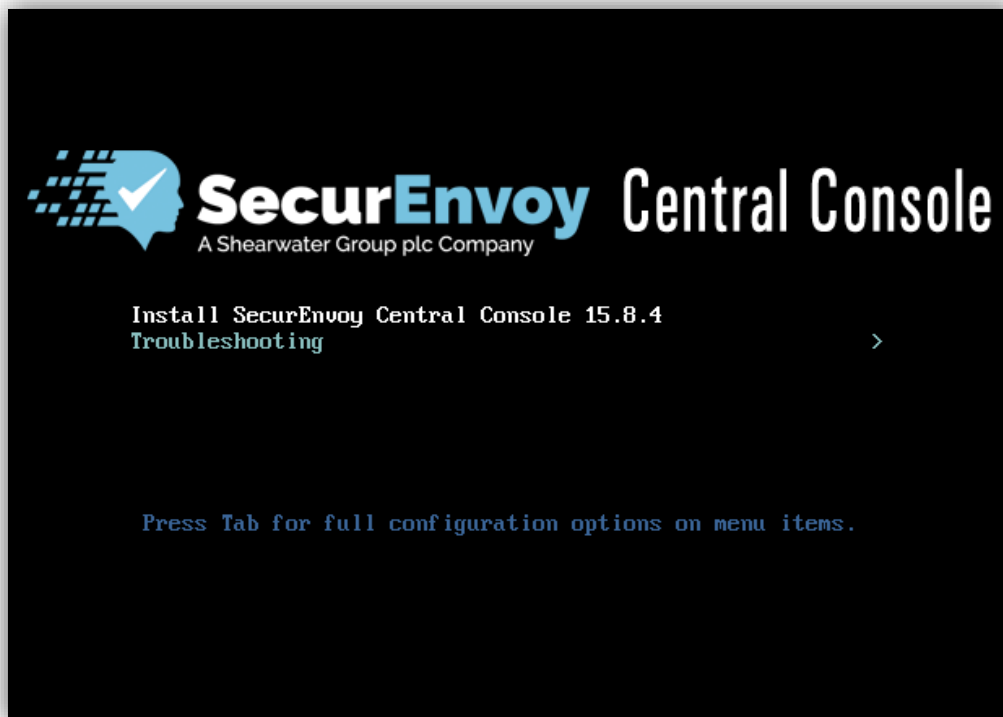
Download the ISO.

Optionally, also download the RPM file. This is typically the latest build update.

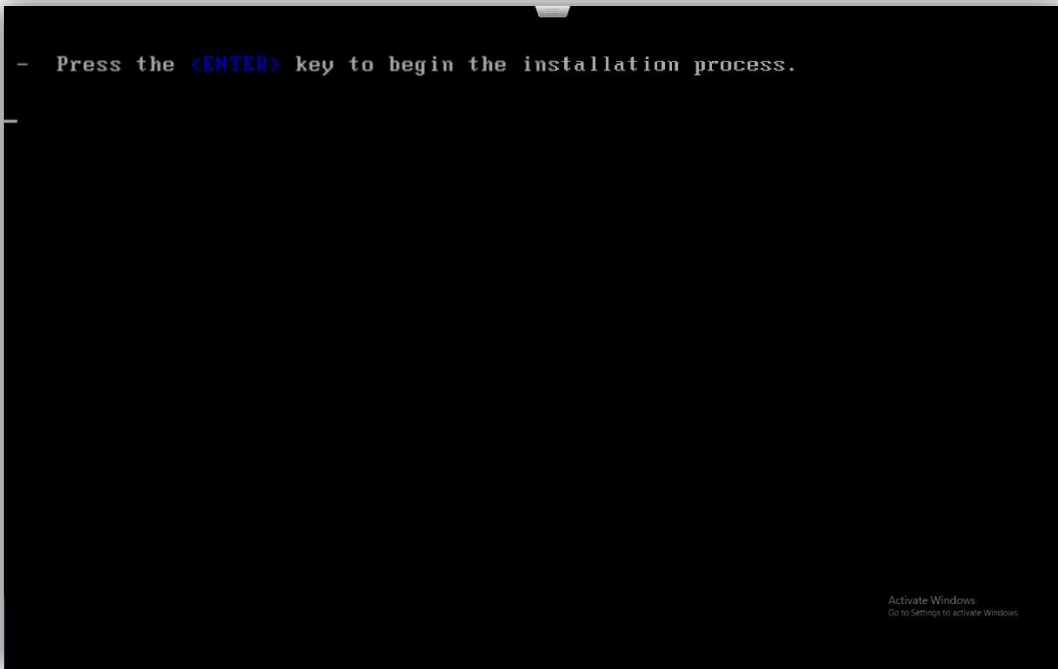
See the 'Upgrading the Central Console' section of this document, or the full upgrade guide can be found here <https://secureenvoy.com/support/>

Basic Installation

Start the server and look at the console output; it should be a boot screen as shown.



Press **Enter** to select the installation option. You should see the following screen.



Press **Enter** to start the installation.

Wait until all packages are installed and confirm the reboot when requested as shown below.



The installation takes about 15-20 minutes to complete and requires several reboots.

Note: Please do not interrupt the process.

Network Configuration

After basic installation, you need to assign an IP address to the SecureIdentity DLP Central Console appliance. Wait until all restarts are done and the system shows the login prompt.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.27.2.el7.x86_64 on an x86_64

securevoycc login:
```

Perform the following steps:

1. At the console login prompt, login as **wizard**, all characters of the username should be lower case.
2. At the password prompt, enter the password **password!**
3. Follow the wizard's instructions to configure the Central Console network connection.

An example of the configured network is shown below.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.27.2.el7.x86_64 on an x86_64

securevoycc login: wizard
Password:
Last login: Fri Sep 27 05:14:59 on tty1

#####
# Welcome to the Configuration Wizard #
#####

Current appliance configuration:
-----
Boot Protocol           : none
Management IP Address  : 192.168.100.20
Network mask           : 255.255.255.0
Default gateway        : 192.168.100.1
Machine Hostname       : securevoycc
Change the appliance settings (Press Ctrl+C to cancel):
-----

To change the IP address of the Management interface [192.168.100.20],
type the new IP, or press Enter to skip:
```

Licensing

At this stage, you should have access to the web-based UI of the SecureIdentity DLP Central Console.

1. Bring up a web browser and login to the Central Console using https://Central_Console_IP link (check the cable attached to the Central Console **eth0** management port, Central Console network configuration, firewall, and web-browser proxy if the connection fails). After entering the Username **Administrator** and the Password **password**.

Make sure that network configuration of the Central Console is correct and ports 80 and 443 are not being blocked by Corporate firewall.

2. Go to the **Maintenance > License** tab and press **Generate system info file** button to save the system information file on your local hard drive. Send this file to licensing@securenvoy.com, and we will process the request and provide you with an evaluation license as soon as practicable.
3. Go to the **Maintenance > Licenses** tab after you get the license file. Browse to the license file and press **Upload**. Make sure that the license was applied.

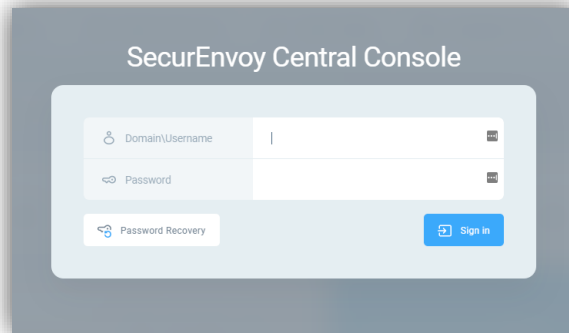
Note that Central Console license becomes invalid in case if hardware changes.

Central Console Basic Configuration

Proceed to configure the SecureIdentity DLP Central Console

1. Bring up an Internet browser and log into the Central Console using https://Central_Console_IP link.

Default login credentials are user: Administrator and password: password



2. Go to the **DLP Setup > System > Network** and enter the corporate DNS server IP addresses in the **DNS Server IP** field. Configure the system proxy settings in the **Internet connection through proxy** section if the Central Console has no direct connection to the Internet. Press **Save** button.
3. Go to the **DLP Setup > LDAP**, configure the connection to your corporate LDAP server (Active Directory) and press **Save**. Make sure that your credentials are valid pressing **Test Connection**. The username should be entered as either DOMAIN\username (use the pre-windows 2000 domain name shown in AD users&computers) or distinguished name format CN=administrator,DC=foo,DC=bar
4. Go to the **DLP Setup > Emails and alerts** and enter your corporate SMTP server credentials. Press **Save** button. These settings are used to send of alerts to the Central Console users. Make sure that your credentials are valid pressing the **Send Test Email** button.
5. Go to the **DLP Setup > Company** and enter up your Company name.
6. Go to the **DLP Setup > Date & Time** and enter your Time Zone.
7. Go to the **Accounts Manager** tab and add a new Central Console user. You can press **Create User Account** to create local user or press **Create Domain User or Group** if you want to add a user from your Corporate Domain.

User Role Descriptions

One of three user Roles are available to configure:

-- **Administrator** is a short form for the Security Administrator, a responsible user who can modify the Central Console system settings and DLP rules without any limitations. Administrator has full permissions for all settings and pages.

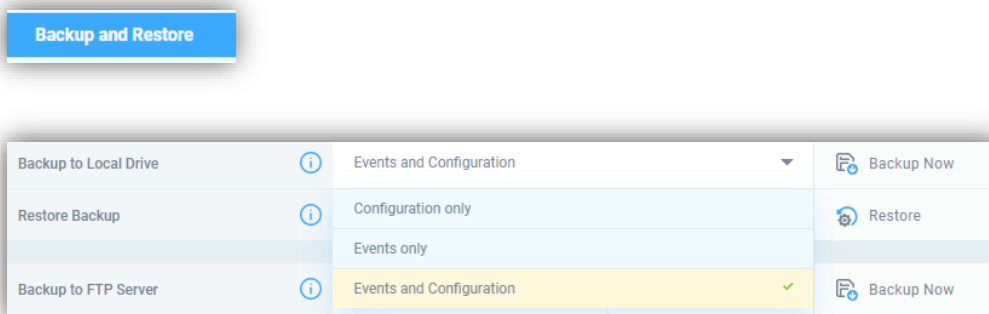
-- **Security Respondent** respondents who handle breach events and can reassign events to Event Handlers. Has no access to DLP settings and User Management. Security Respondent role is designed for a security officer who is responsible for role assignment of security events. Security Respondent does not have access to system and scan settings. Also has permission to tabs related only to events and reports.

-- **Event Handler** is a respondent who handles breach specific events. Event Handler has access to same sections as Security Respondent, but can only see and work with events that are assigned to him/her.

Backup and Restore

The first task after an installation is to create a backup of your fresh server

Navigate to Backup and Restore from the left-hand menu



Ensure that “Events and Configuration” is selected from the dropdown options and then click on “Backup Now” this will take a few seconds to complete and the backup file will download to your local machine.

Keep this file somewhere safe it is best practice to take a backup before any upgrades are installed.

You can also schedule a regular backup to an FTP server.

To restore a backup file, click on the folder icon and select your backup file and then click on Restore

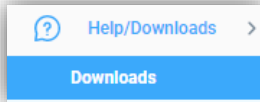


Inspector Installation

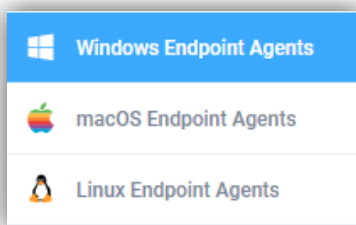
Coming soon.

Agent Installation

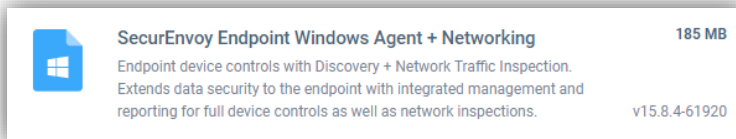
Download the relevant agent installer from the Help/Downloads menu in the central console



Windows Agent Installation



For example, the windows agent



The agents are pre-configured to communicate with the central console and just required deployment using your normal software deployment tool.

On each page there is a link to the list of AV exceptions that must be in place to ensure correct operation of the endpoint agent



The agents are pre-configured to communicate with the central console and just required deployment using your normal software deployment tool, however if the IP address of the central console has been changed or you wish for some agents to communicate to a child manager see the [Configure Windows Agent for New Console IP Address](#) section

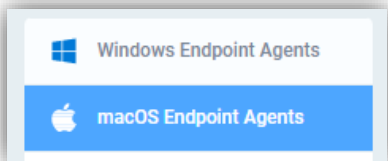
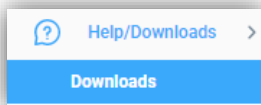
Silent installation of the msi can be achieved with the following command line

```
msiexec.exe /quiet /i agent_file_name_goes_here.msi
```

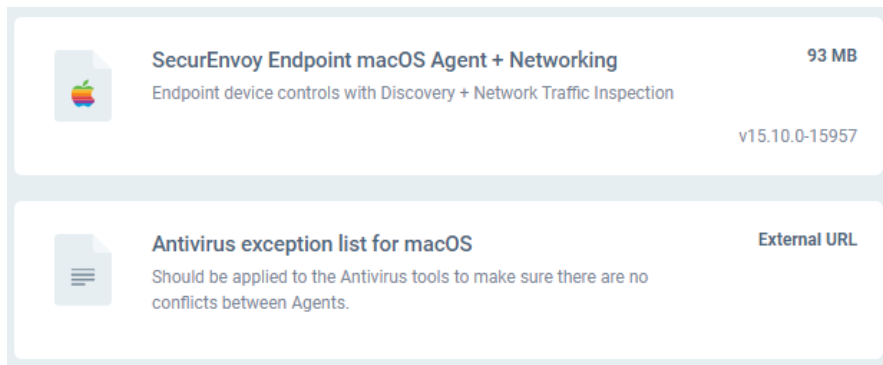
The agent can be uninstalled using this command

```
msiexec /X agent_name.msi REMOVE_SCANNER=1
```

Mac Agent Installation



Download the macOS package and the zip file containing a text list of AV exceptions required



Once you have deployed the installation package using your normal method you need to configure the agent to talk to the central console, this is achieved with a post install shell script

```
/Library/SecurEnvoy/support.sh -a ip_address_of_central_console
```

The macOS agent also requires full disk access to be granted to it.

Security Manager

Installation

SecureIdentity DLP allows you to fingerprint Files and Databases, fingerprinting content allows these unique identifiers to be used as part of your DLP policy and reduce false positives.

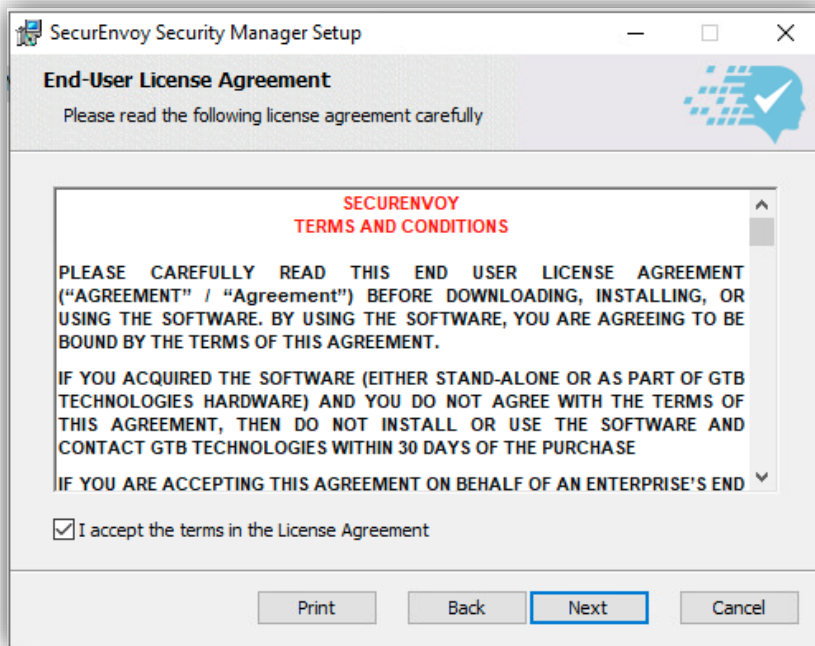
Security Manager is the Windows only application used to Fingerprint files and databases, you can download it from the help/downloads on the central console.



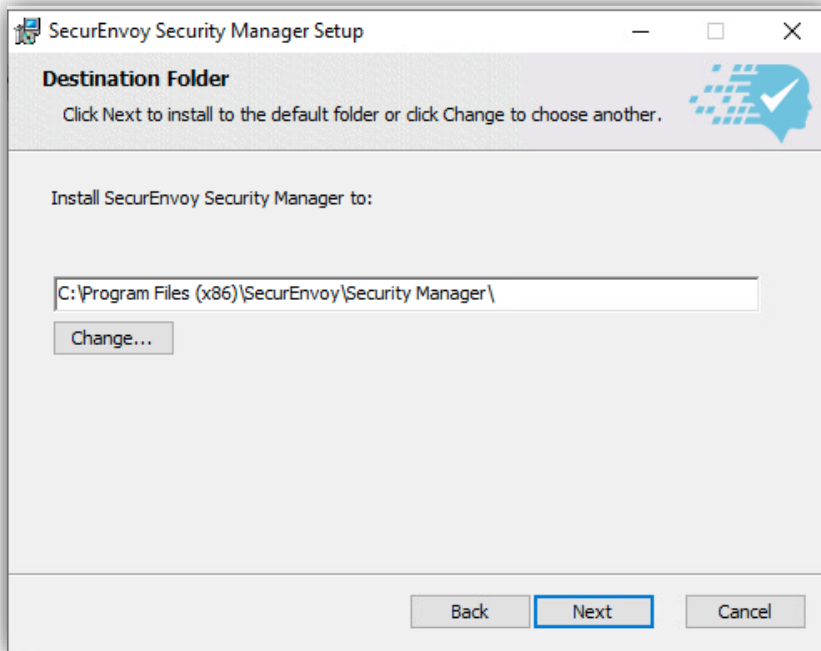
Download it from the central console Downloads section and once you extract the zip file run the installer.



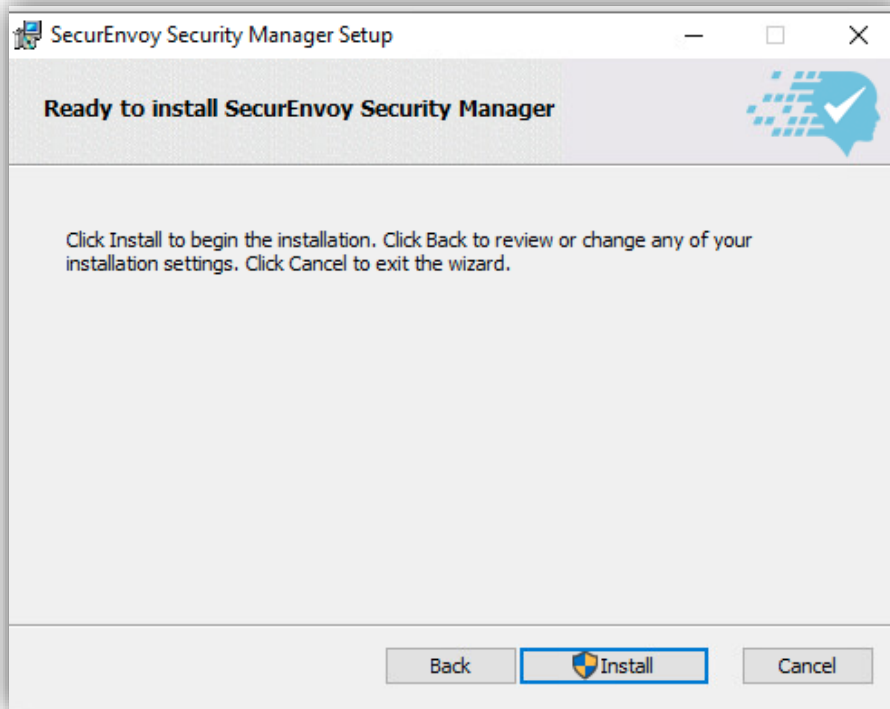
Accept the EULA and click “next”



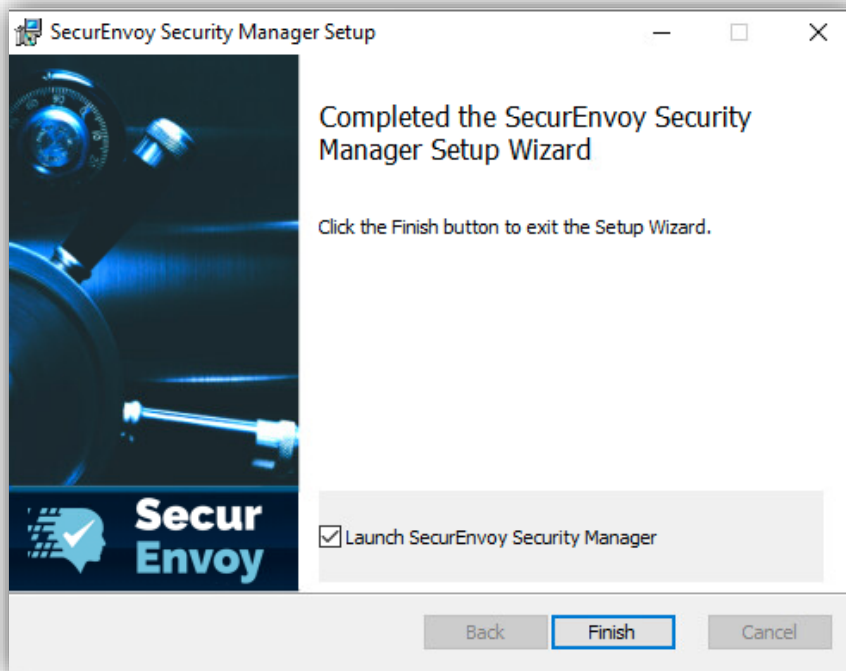
If you’re happy with the default installation path click “next”



You can now click “install” to install the application



Once complete click “Finish” and the application will be launched

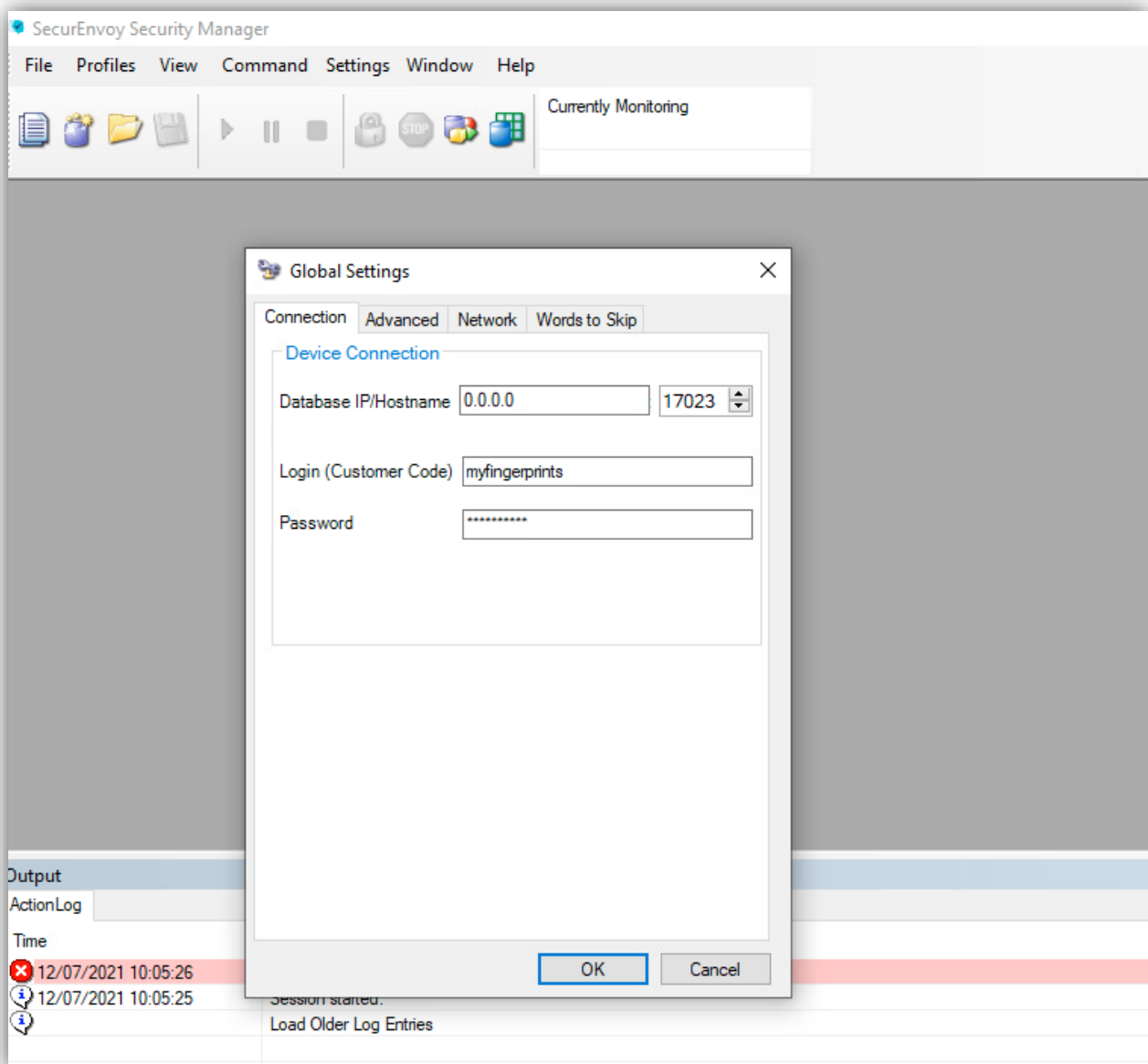


Configuration

Change the IP address to that of your inspector if you have one installed or your central console if you do not

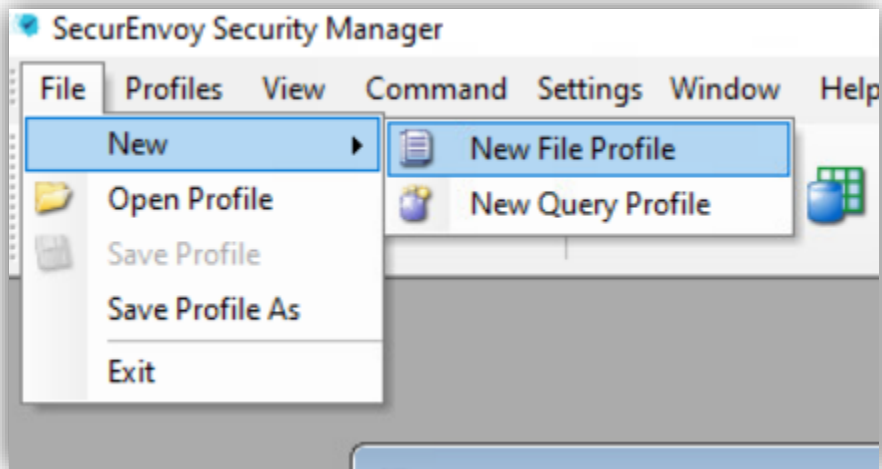
leave the login and password as the default.

Once the IP address is set click “OK”

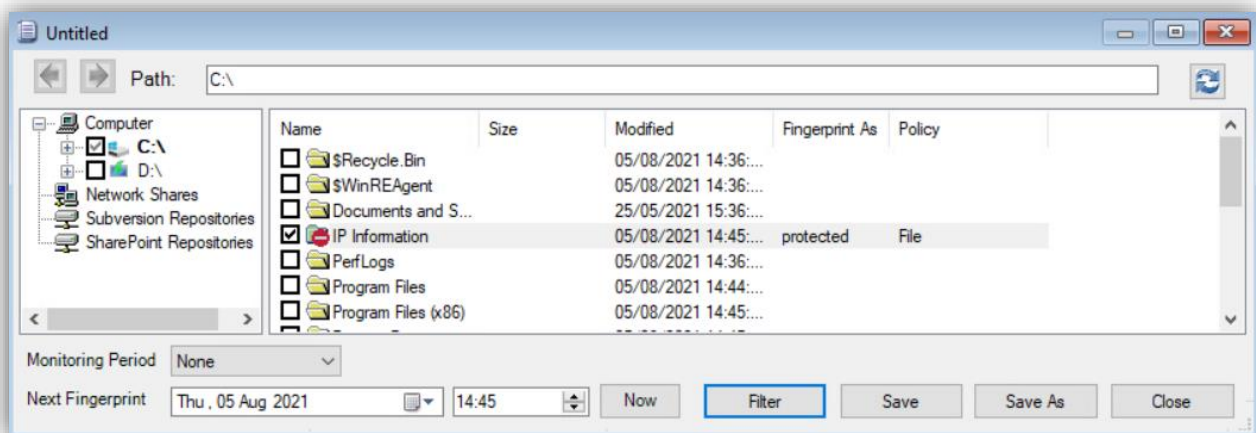


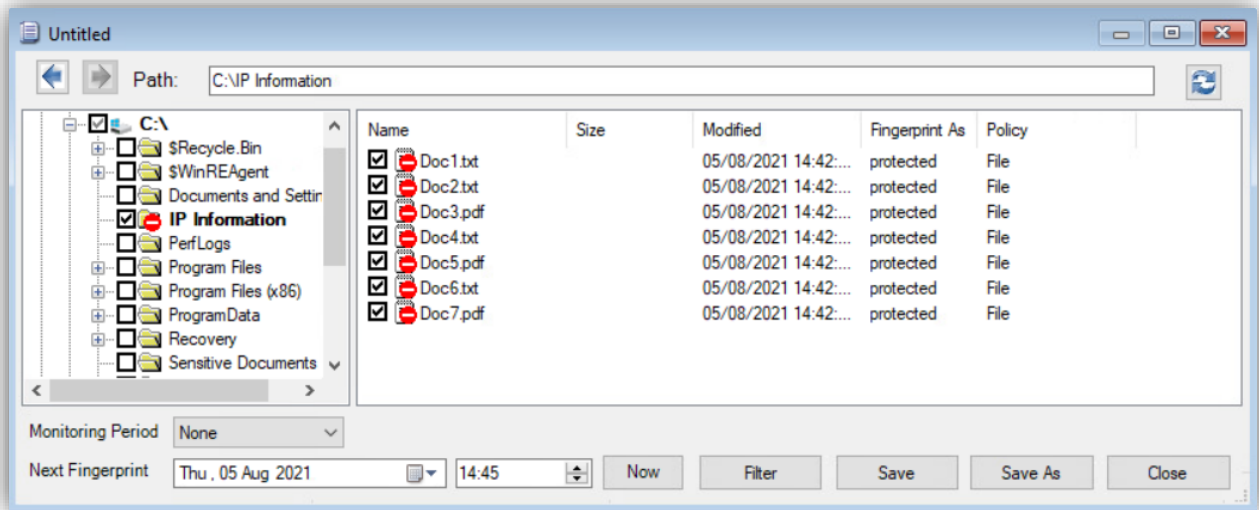
Fingerprinting Files

Select “New File Profile” from the File > New menu

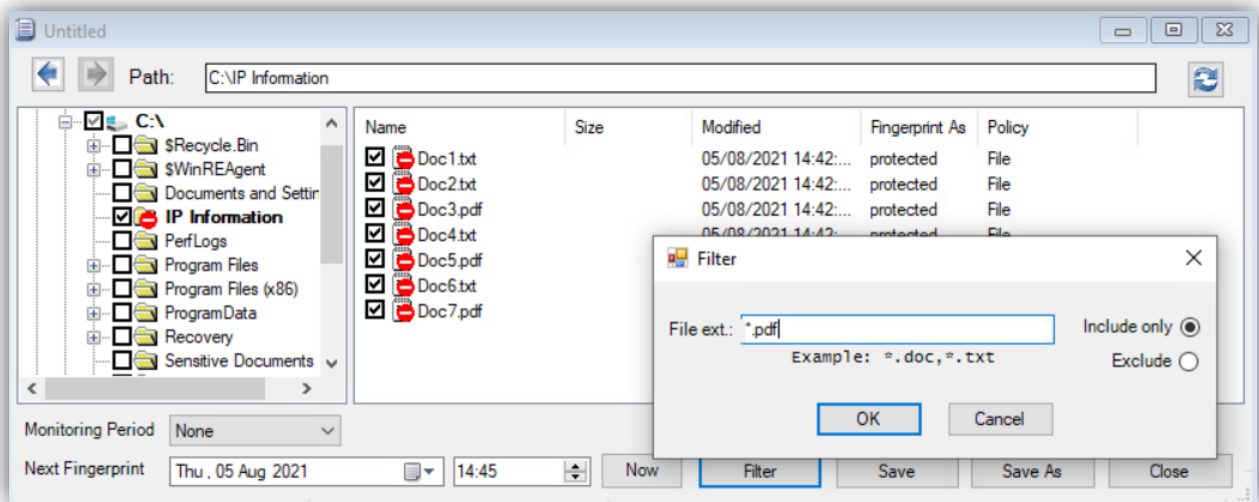


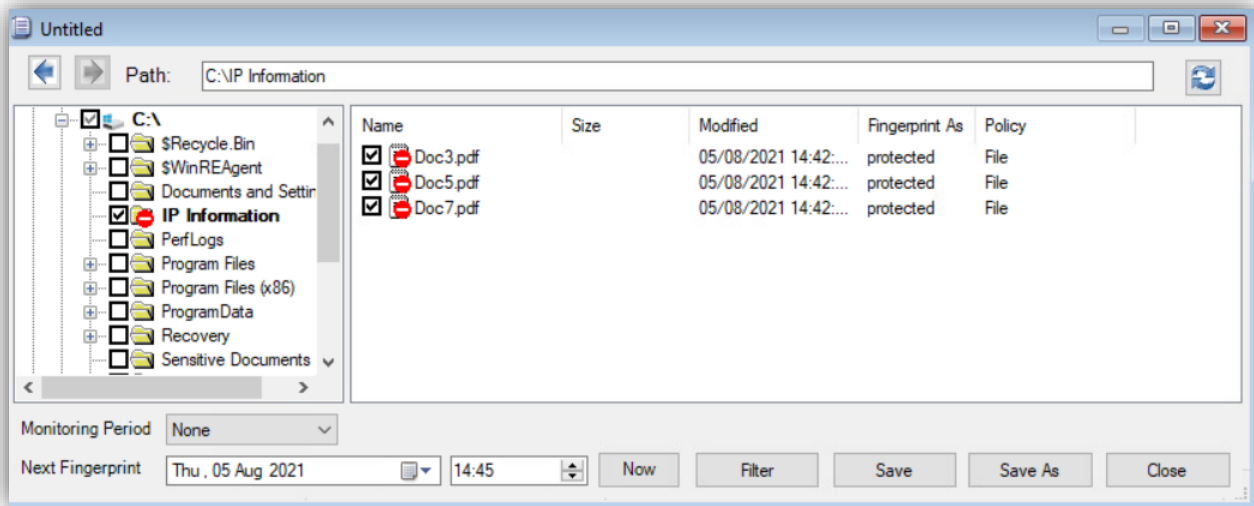
Select the folders or individual files you wish to protect





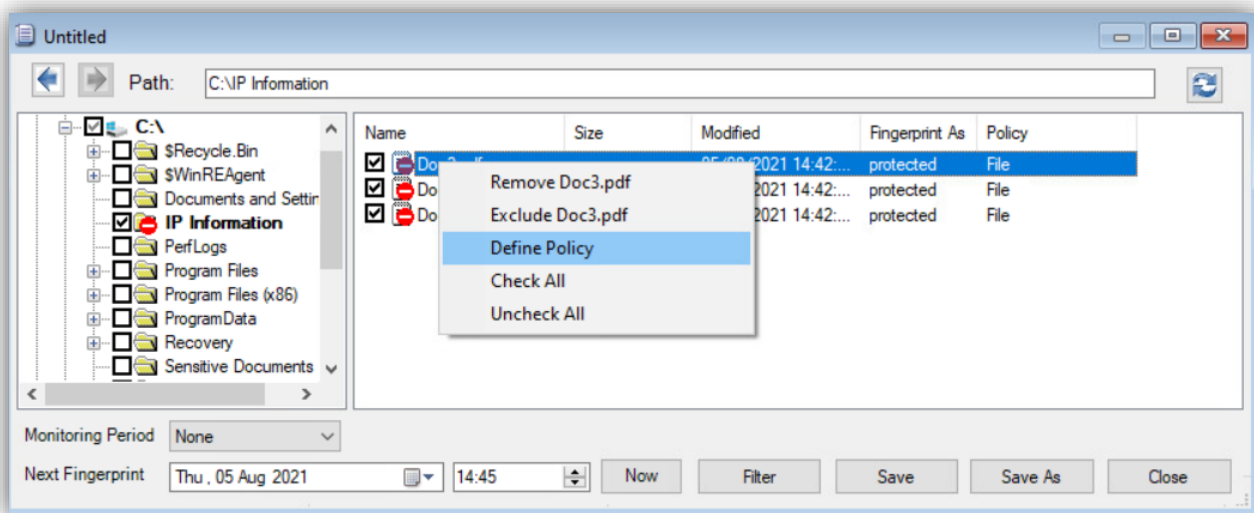
You can filter the files to be included by clicking the Filter button

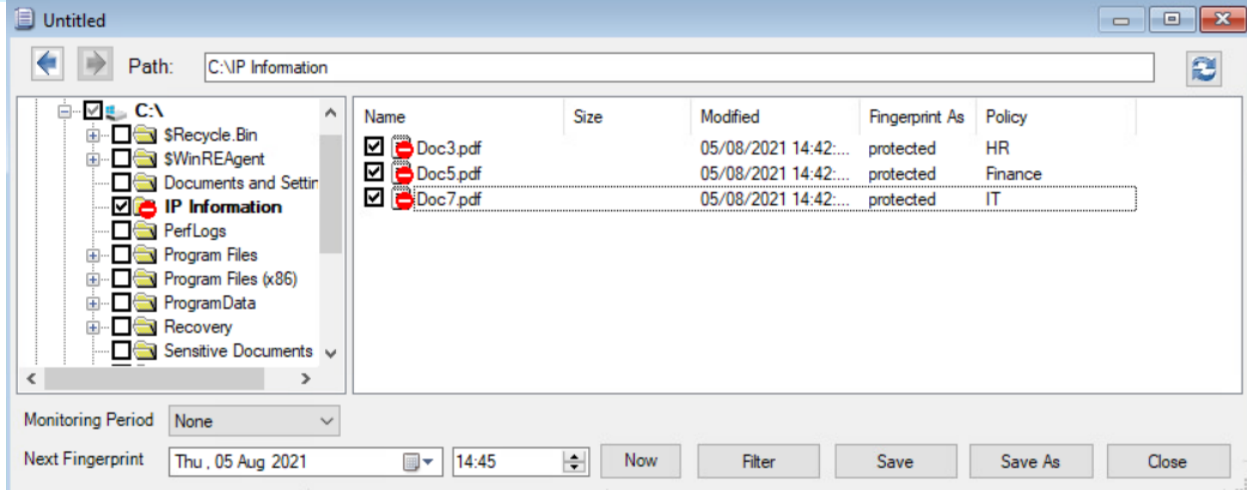




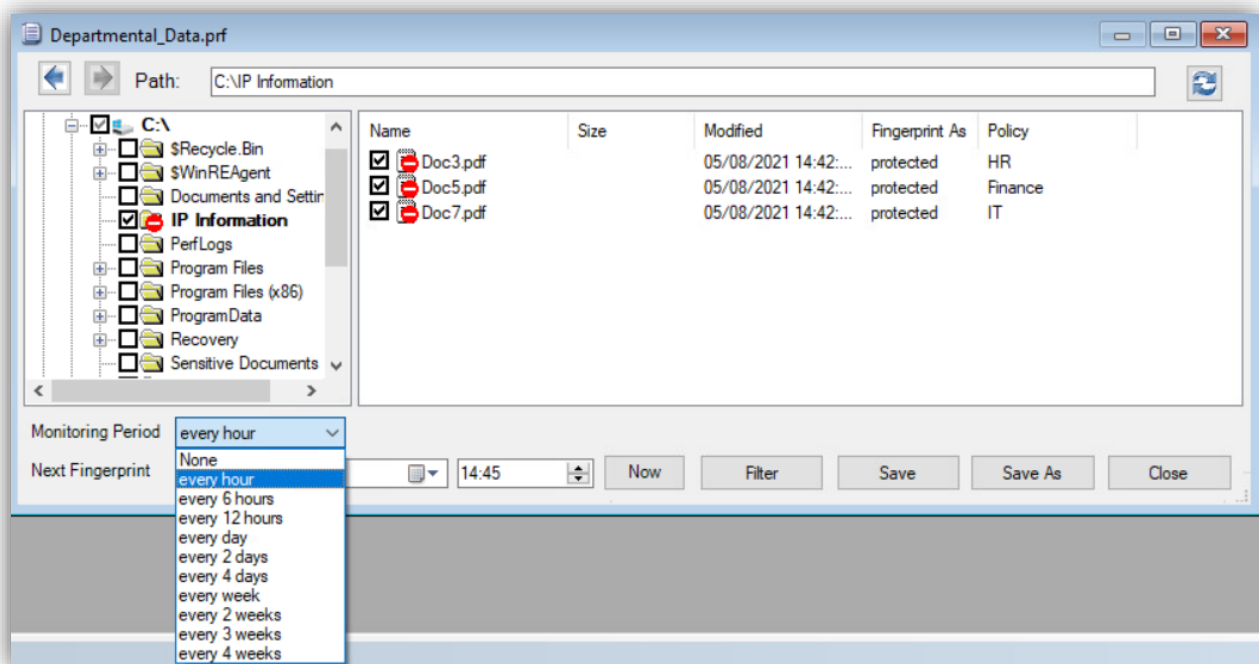
By default all protected files will be under the Policy “File” however you can assign a different Policy to them such as HR, Finance etc..

Right click on the folder to change it for all files in that folder or right click on a specific file to change the policy for that file





You can choose how often the files are checked using the “Monitoring Period” dropdown



Once you have selected all the sensitive files you wish to protect and assigned them to the relevant policy click on “Save or Save As” and give the prf file a name

Now you're ready to start monitoring and protecting your data, click on the play button



Fingerprinting Databases

Coming soon

Adding fingerprints to a rule

Add a new ACL rule, fingerprinted file policies are GREEN

Add ACL Rule ✕

Name	Detect Fingerprints				
Protocol	All Protocols ▼				
Destination	Any ▼				
File Type	Inspect files and data streams ▼				
Comment					

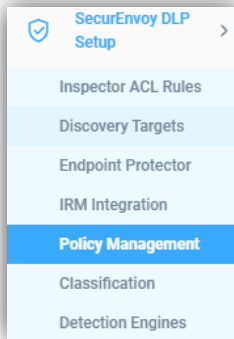
Remedial Action + Add Remedial Action

DLP POLICY/CATEGORY	REMEDIAL ACTION	NOTIFICATION	ORDER	
IP_DOCS ✕ Top_Secret ✕ File ✕	✕ ▼	🚫 Block ▼	🔔 <input checked="" type="checkbox"/>	▼ ^ 🗑️

Save
Cancel

Policy Management

Policy management is found under SecurEnvoy DLP Setup > Policy Management



When defining DLP rules we can use these as triggers:

- Policies - a collection of Regex, Dictionaries and Fingerprints
- Categories - a collection of policies
- Classifications – a classification label

Regular Expressions

Regular Expressions

Click “Regular Expressions” from the policy management menu

Add

Click “Add”

Edit Regular Expression

Matches customer numbers

Regular Expression	cust\d+
Description	Matches the word cust followed by any set of numbers
Examples	cust1234

Save Cancel

Once complete click on “Save”

This regex will match on the word cust + any number e.g., cust0001, cust0002, cust0067

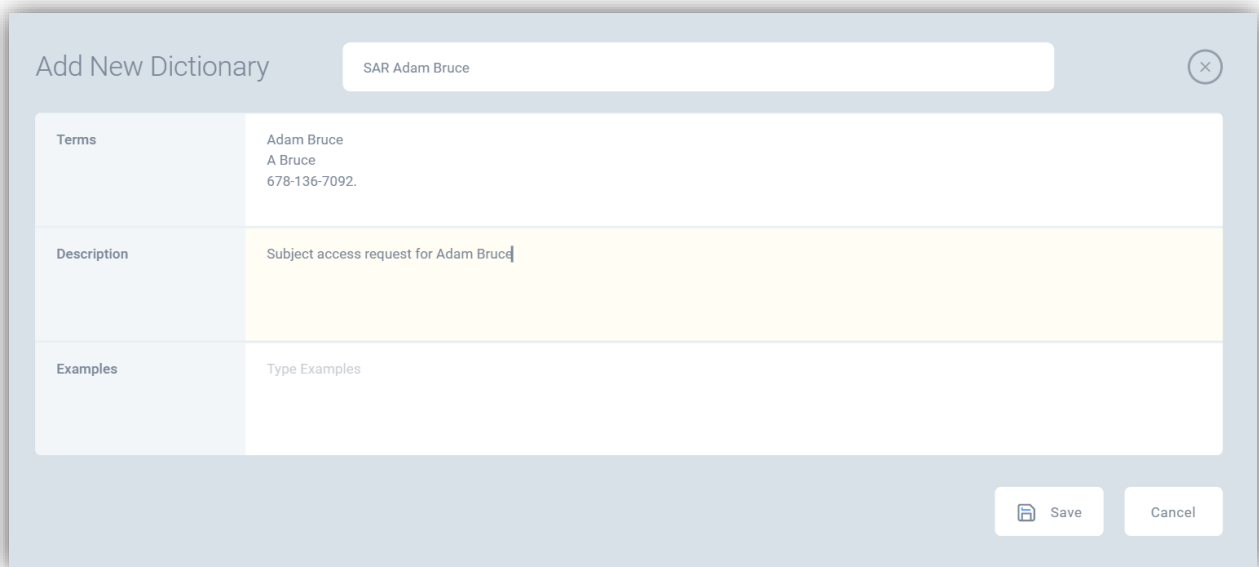
Dictionaries

 A blue button with a white 'A' icon and the text "Dictionaries".

Click "Dictionaries" from the policy management menu

 A white button with a green plus icon and the text "Add".

Click "Add"



The "Add New Dictionary" dialog box is shown. It has a title bar with "Add New Dictionary" on the left and a close button on the right. Below the title bar is a search input field containing "SAR Adam Bruce". The main area is a table with three rows:

Terms	Adam Bruce A Bruce 678-136-7092.
Description	Subject access request for Adam Bruce
Examples	Type Examples

At the bottom right of the dialog are "Save" and "Cancel" buttons.

This dictionary can be used as a subject access request.

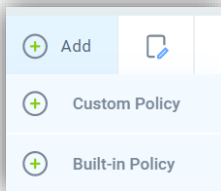
Policy Editor



Click “Policy Editor” from the policy management menu



Hover over “Add” then select one of the options



Adding a new “Custom Policy”

Edit Policy

UK Passport Information

✕

Description

Type Description

Proximity

600

characters

+ Add Regex
+ Add Dictionary
+ Add Structured Fingerprint

🗑 Delete
ℹ

<input type="checkbox"/>	#	OBJECT	TYPE	THRESHOLD / WEIGHT
<input type="checkbox"/>	1	<input checked="" type="radio"/> UK Passport Number	Custom Expression	1
<input type="checkbox"/>	2	<input checked="" type="radio"/> UK Passport Nationality Regex	Custom Expression	1
<input type="checkbox"/>	3	<input checked="" type="radio"/> UK Passport Authority Regex	Custom Expression	1
<input type="checkbox"/>	4	<input checked="" type="radio"/> UK Passport Country Code Regex	Custom Expression	1

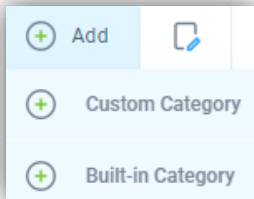
💾 Save
Cancel

Here we added 4 custom defined regex's and set the threshold to 1
 A combination of all sets of terms is required to trigger this policy

Categories



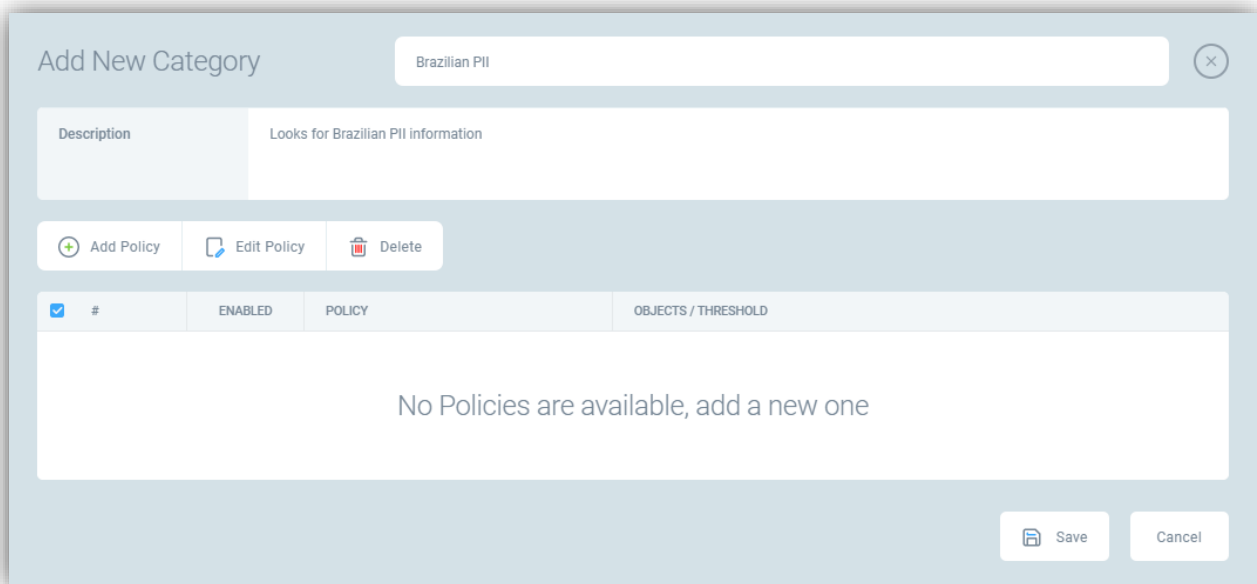
Click “Categories” from the policy management menu



Hover over “Add” then select one of the options

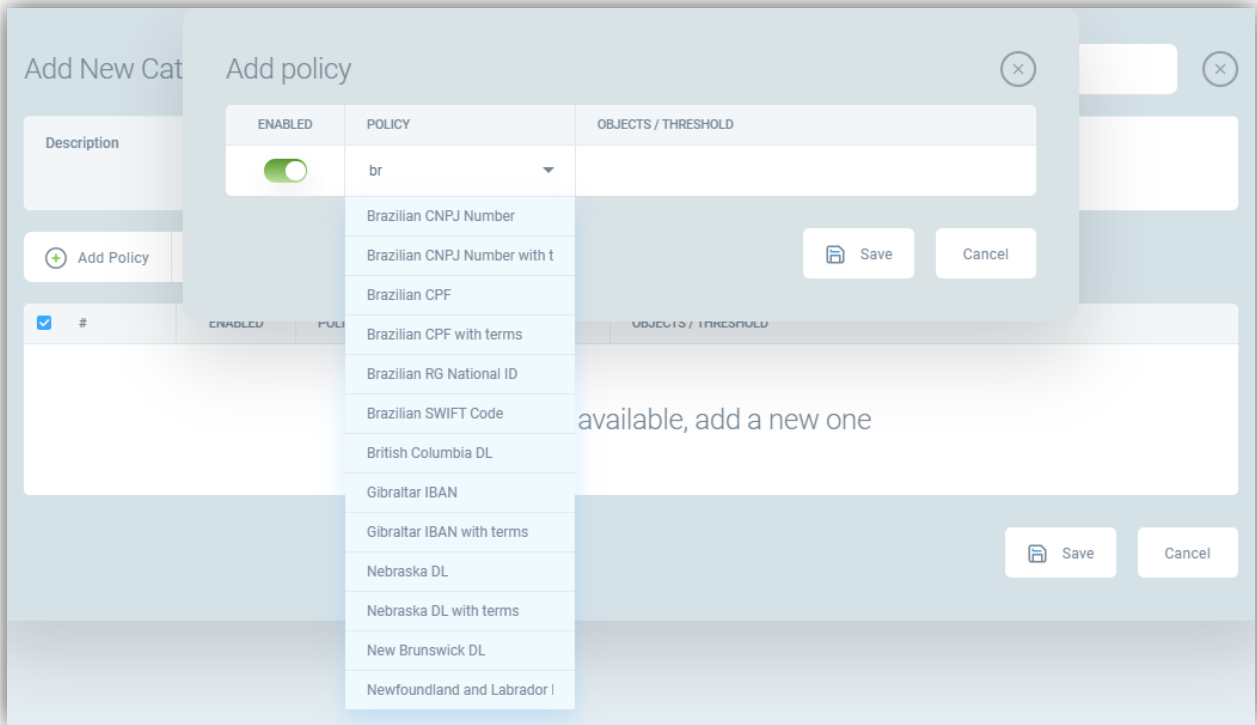
We’re going to add a “Custom Category”

Step 1: Give it a name and Description

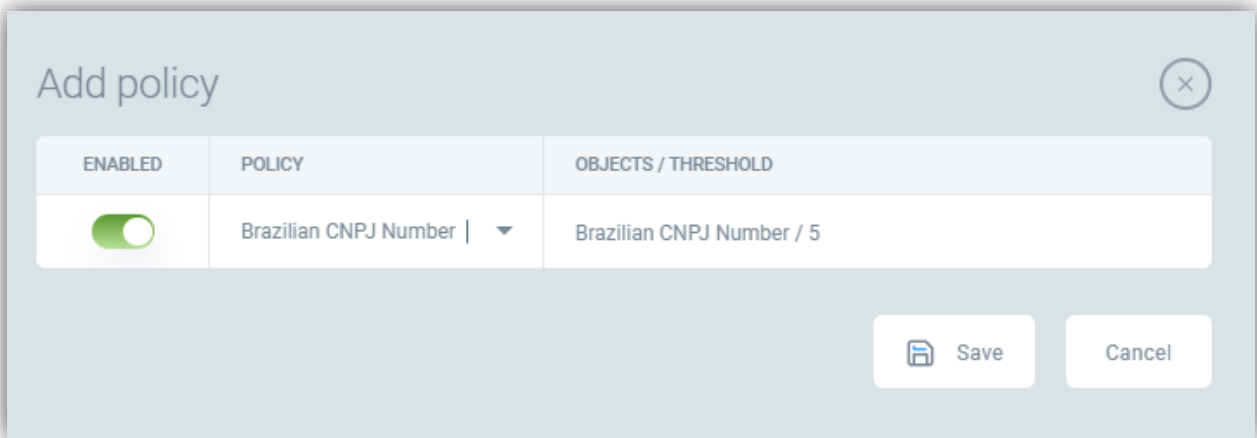


The "Add New Category" dialog box is shown. It has a title bar with "Add New Category" and a close button. Below the title bar is a text input field containing "Brazilian PII". Underneath is a "Description" field with the text "Looks for Brazilian PII information". Below the description field are three buttons: "Add Policy", "Edit Policy", and "Delete". Below these buttons is a table with the following columns: a checkbox (checked), "#", "ENABLED", "POLICY", and "OBJECTS / THRESHOLD". The table is currently empty, with the text "No Policies are available, add a new one" centered below it. At the bottom right of the dialog are "Save" and "Cancel" buttons.

Step 2: Search for matching policies



Step 3: Save the policies you wish you to add to the category



Step 4: Save the new Category

Add New Category

✕

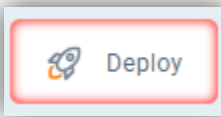
Description: Looks for Brazilian PII information

+ Add Policy ✎ Edit Policy 🗑 Delete

<input type="checkbox"/>	#	ENABLED	POLICY	OBJECTS / THRESHOLD
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Brazilian CPF	Brazilian CPF / 5
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Brazilian SWIFT Code	Brazilian SWIFT Code / 5
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Brazilian RG National ID	Brazilian RG National ID / 5
<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	Brazilian CNPJ Number	Brazilian CNPJ Number / 5

Save Cancel

Step 5: Deploy the new changes



Endpoint Protector Controls

Endpoint Protector

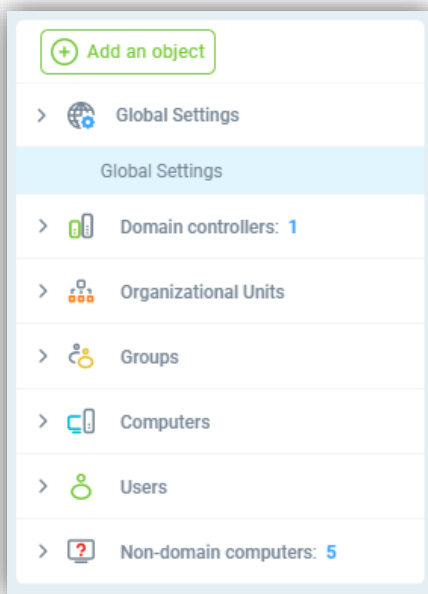
Network DLP

 Network DLP

Network DLP controls apply to data in motion on a protected endpoint

These controls can be granularly controlled

The least granular rules will be “Global Settings” and these will apply if there is no match further down the structure, a ruleset associated to a user or individual computer would override the global ruleset.



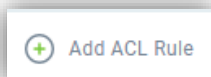
Each object starts with a default set of rules

#	RULE NAME	PROTOCOL	DESTINATION	FILES CONDITION	DLP POLICY/CATEGORY	REMEDIAL ACTION	NOTIFICATION		ORDER
1	Exclude Local Netw...	All Protocols	10.0.0.0...	Inspect files and data streams		Pass		<input checked="" type="checkbox"/>	^ v
2	Any	All Protocols	All	Inspect files and data streams	All Policies	Log		<input checked="" type="checkbox"/>	^ v

Each ACL rule consists of several parts

- **Name** Free text entry but must be unique
- **Protocol** Either “All Protocols” to apply the rule to all communications channels or an individual one such as HTTPS
- **Destination** Depending on the protocol selected this will be
 - “Any, IP Address, Email Address/Domain, HTTP(s) Domain”
- **File Type** This relates to the content you want to inspect
 - “Inspect files and data streams” – Attached files, Uploads and TCP data such as a post to a web page
 - “Inspect only files” – Attached files or Uploads
 - “Inspect only encrypted files” – Trigger if a file is encrypted
- **Comment** – Free text entry
- **DLP POLICY / CATEGORY** – Which policy(s) or Categories the rule is looking for
- **REMEDIAL ACTION** – What action to take when the rule is triggered
 - Log
 - Block
 - S-Block
 - User Justification
 - Pass
- **NOTIFICATION**
 - None
 - Flag User – A pop up will be displayed to the user, can be combined with Notify Manager
 - Notify Manager – An email will be sent to their manager, can be combined with Flag User
- **FILE CAPTURE** – Take a copy of the file that triggered the breach
- **ORDER** – The arrows can be used to re-order the rules

You can add a new rule, click on “Add ACL Rule”



Example for blocking PCI uploads to HTTPS websites

Add ACL Rule

Name	Block PCI Uploads
Protocol	HTTPS
Destination	Any
File Type	Inspect files and data streams
Comment	Blocks uploads of PCI data

Remedial Action [+ Add Remedial Action](#)

DLP POLICY/CATEGORY	REMEDIAL ACTION	NOTIFICATION		ORDER	
Category: PCI <input checked="" type="checkbox"/>	Block		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

[Save](#) [Cancel](#)

You can edit an existing rule by double clicking on the rule itself or ticking the checkbox next to it and clicking “Edit”



You can delete a rule by ticking the next box next to the rule(s) you wish to delete and the clicking “Delete”



You can import and export your current ruleset by clicking the relevant action



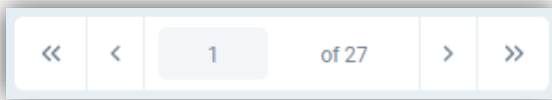
Rules are exported as JSON files

Application Controls

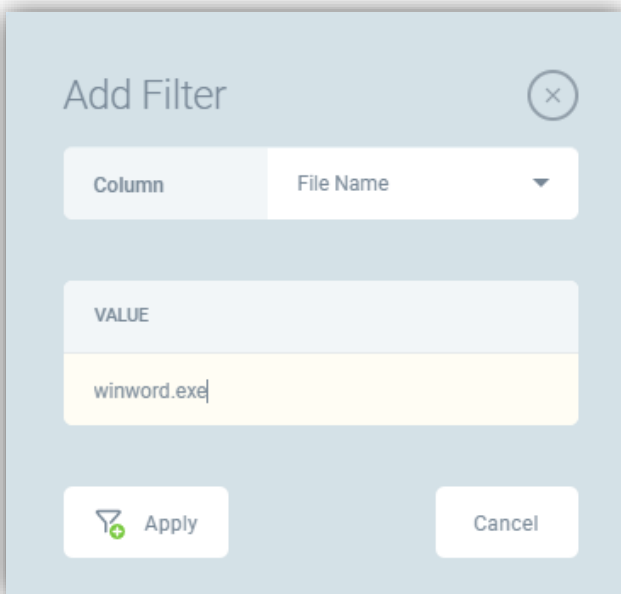
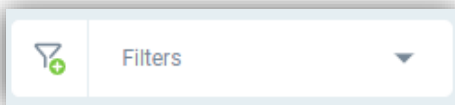


Application controls allows you to block or allow an application from running as well as inspect the data that is transferred via that application over TCP or to a USB device, please note that not all applications can be inspected due to their own security controls if in doubt please contact support.

Navigate through the pages of data



Adding a filter to target a specific application or device



Double clicking on a line gives more information about the application

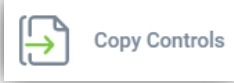
Application Details ✕

Process Name	Zoom.exe
MD5	3C36049D8A28C6BF3C8EAFBFAD226BA
SHA1	3b42ed143944aff5d9c1d06b694a8496e353431
SHA256	DD344DA7DD8CA15C927E3152C3D43FD7CC1C81F40D66BFA3CE0EB70...
Process Start Time	May 25, 2021 04:00:06 PM
Process ID (PID)	32052
Process Directory	C:\Users\bnorcutt\AppData\Roaming\Zoom\bin
Internal Name	Zoom.exe
Command Line Details	"C:\Users\bnorcutt\AppData\Roaming\Zoom\bin\Zoom.exe" --action=join ...
Creation Time	June 02, 2021 10:47:23 AM
Modification Time	May 06, 2021 01:00:51 PM
Company Name	Zoom Video Communications, Inc.
Product Name	Zoom Meetings
Product Version	5.6.5.823
File Description	Zoom Meetings
File Version	5,6,5,823
Legal Copyright	© Zoom Video Communications, Inc. All rights reserved.

Close

You can Block/Allow access to an application or multiple applications by clicking

Copy Controls



Copy controls allow you to control what types of data can be copied to the clipboard and copied to the endpoint.

You can also disallow clipboard or file copy use completely by toggling the switch to off.

Back
Deploy
?

Copy to Clipboard

ALLOW	REMEDIAL ACTIONS	DLP POLICY/CATEGORY	FLAG USER	NOTIFY MANAGER
<input checked="" type="checkbox"/>	Log	Customer Details ×	✗	✔
	Block	ACME CORP:Top Secret × ACME CORP:Internal ×	✗	✔

Copy Files

ALLOW	REMEDIAL ACTIONS	DLP POLICY/CATEGORY (MS OFFICE FILES ONLY)	FLAG USER	NOTIFY MANAGER
<input checked="" type="checkbox"/>	Log	Not File Owner ×	✗	○
	Block	ACME CORP:Top Secret × ACME CORP:Secret ×	✗	✔

Other

Back
Deploy
?

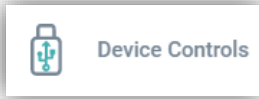
Printing DLP in Off-Premises Mode

ALLOW PRINTING	REMEDIAL ACTIONS	DLP POLICY/CATEGORY	FLAG USER	NOTIFY MANAGER	LOG OPERATIONS
<input checked="" type="checkbox"/>	Log	ACME CORP:Public ×	○	○	○
	Block	ACME CORP:Top Secret × ACME CORP:Secret × Customer Details ×	✗	✔	
	Justify	ACME CORP:Personal ×	✗	✔	

Other DLP Settings

1. Block Files in Off-Premises ⓘ
2. Block Wi-Fi in On-Premises ⓘ

Device Controls

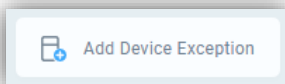


Back Deploy

ALLOW READ	ALLOW WRITE	ALLOW EXECUTE	LOG I/O OPERATIONS	ENCRYPT ALL FILES	SHADOW ALL FILES
				Disabled	Disabled

REMEDIAL ACTIONS	DLP POLICY/CATEGORY		FLAG USER	NOTIFY MANAGER
Log	Category: PCI			<input type="radio"/>
Block	ACME CORP:Top Secret ACME CORP:Secret			<input type="radio"/>
Justify	ACME CORP:Personal			<input type="radio"/>

You can add exception to the controls based on devices



The exceptions can be based on the device type, name, or volume

Add Device Exception

Device Type
 Device names
 Device volumes

#	DEVICE TYPE	ADDED
1	Floppy Disk Drives	<input type="radio"/>
2	DVD/CD-ROM Drives	<input type="radio"/>
3	USB Storage Devices	<input type="radio"/>
4	MTP Devices	<input type="radio"/>

Add Device Exception

Device Type
 Device names
 Device volumes

#	DEVICE NAME	DEVICE TYPE	ADDED
1	LG USB Drive USB Device	USB Storage Devices	<input type="radio"/>
2	Micron 1100 SATA 256GB	DVD/CD-ROM Drives	<input type="radio"/>
3	Microsoft Virtual Disk	DVD/CD-ROM Drives	<input type="radio"/>
4	NECVMWar VMware SATA CD00	DVD/CD-ROM Drives	<input type="radio"/>
5	NVMe PC611 NVMe SK hynix 1TB	DVD/CD-ROM Drives	<input type="radio"/>
6	Samsung Flash Drive	USB Storage Devices	<input type="radio"/>
7	SanDisk Cruzer Blade USB Device	USB Storage Devices	<input type="radio"/>
8	SanDisk Cruzer Edge USB Device	USB Storage Devices	<input type="radio"/>
9	SanDisk Ultra Fit USB Device	USB Storage Devices	<input type="radio"/>
10	SDHC Card	USB Storage Devices	<input type="radio"/>

Add Device Exception

Device Type
 Device names
 Device volumes

#	DEVICE VOLUME	DEVICE NAME	DEVICE TYPE	ADDED
1		NECVMWar VMware SATA ...	DVD/CD-ROM Drives	<input type="radio"/>
2	08E47727	Micron 1100 SATA 256GB	DVD/CD-ROM Drives	<input type="radio"/>
3	1C9351C1	VMware Virtual disk SCSI Di...	DVD/CD-ROM Drives	<input type="radio"/>
4	2AD7FEB6	VMware Virtual disk SCSI Di...	DVD/CD-ROM Drives	<input type="radio"/>
5	4E11DA2F	SanDisk Cruzer Blade USB ...	USB Storage Devices	<input type="radio"/>
6	4E946323	Microsoft Virtual Disk	DVD/CD-ROM Drives	<input type="radio"/>
7	527AA45A	VMware Virtual disk SCSI Di...	DVD/CD-ROM Drives	<input type="radio"/>
8	5A8A9420	VMware Virtual disk SCSI Di...	DVD/CD-ROM Drives	<input type="radio"/>
9	628A1806	TOSHIBA KSG602MV512G ...	DVD/CD-ROM Drives	<input type="radio"/>
10	8A238043	SanDisk Ultra Fit USB Device	USB Storage Devices	<input type="radio"/>

You can add exceptions based on file type of file group

Add Device Exception

File Type | File Group

#	FILE TYPE	ADDED
1	7zip Archive	<input type="radio"/>
2	ActiveX Control	<input type="radio"/>
3	Adobe PDF	<input type="radio"/>
4	Adobe Photoshop	<input type="radio"/>
5	Apple Disk Image	<input type="radio"/>
6	ARJ Archive	<input type="radio"/>
7	Batch file	<input type="radio"/>
8	Bitmap	<input type="radio"/>
9	CAB File	<input type="radio"/>
10	Command File	<input type="radio"/>

Add Cancel

Add Device Exception

File Type | File Group

#	FILE GROUP	ADDED
1	Audio/Video	<input type="radio"/>
2	Compressed Files	<input type="radio"/>
3	Disk Images	<input type="radio"/>
4	Images	<input type="radio"/>
5	Microsoft Office	<input type="radio"/>
6	Open Office	<input type="radio"/>

Add Cancel

You can add an exception based on filename

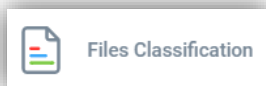
Add File Name Exceptions

Example: *.docx Add

#	FILE NAME EXCEPTION	OPTIONS
1	test.docx	

Add Cancel

Files Classification
















For windows you have several options to deal with classification

Adhoc classification – users can choose to classify document if they want to


All the options can be enabled/disabled using the switches, green means it is enabled and yellow disabled, you can control what information if any gets put into the header and footer of the document including the font, size, colour as well as what the content using placeholders

Adhoc Classification

ENABLE
 Font: Arial
 Size: 14px
 B I U A
             

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Header	%%CLASSIFICATION_LABEL%%
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Footer	%%USER_NAME%% %%TIMESTAMP%%

Add Placeholder
 Overlay icon: Enabled

 Add Placeholder

- Username
- Classification Label
- Classification Depen...
- Timestamp

Force user to classify – users will not be able to save a document until they classify it, it provides the same options as ad-hoc

Force User to Classify

ENABLE		Font: Arial	Size: 14px	B	I	U	A	≡	≡	≡	🔍	</>	Add Placeholder
<input checked="" type="checkbox"/>	✓ Header	%%COMPANY_NAME%%											
<input type="checkbox"/>	○ Footer												

Classify Based on Content – The file will be classified based on its contents referenced to the DLP Policy Mapping setup under classification, if the PCI category is mapped to a classification of financial then any document containing PCI data will be classified as Financial

Classify Based on Content

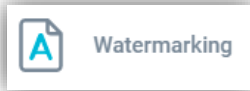
ENABLE		Font: Arial	Size: 14px	B	I	U	A	≡	≡	≡	🔍	</>	Add Placeholder
<input checked="" type="checkbox"/>	✓ Header	SecurEnvoy %%CLASSIFICATION_LABEL%%											
<input checked="" type="checkbox"/>	✓ Footer	SecurEnvoy %%CLASSIFICATION_LABEL%%											

Classification Override – controls whether a user can change the classification of a document once it is set and optionally if they have to provide a reason for the change in classification

Classification Override

1. Allow Classification Override	i	<input checked="" type="checkbox"/>
2. Force User to Justify	i	<input checked="" type="checkbox"/>

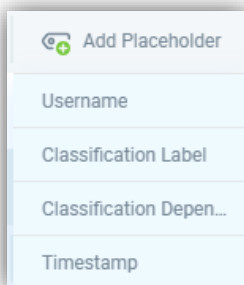
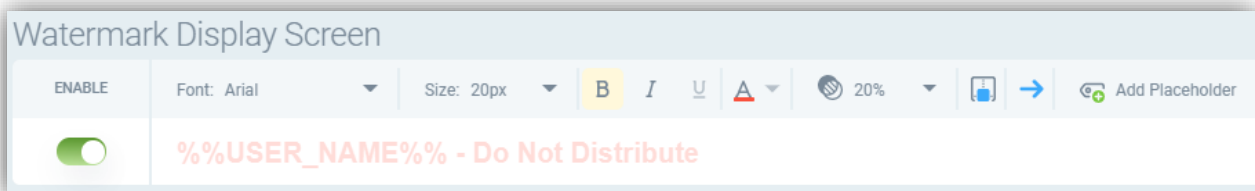
Watermarking



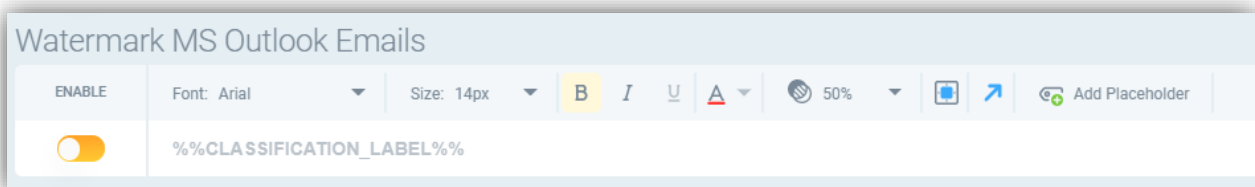
Watermarking allows you put a visual indicator relating to DLP in various locations, switch enables or disables them.

Watermark Display Screen – Adds a watermark to the users monitors in the location specified to discourage screenshots and snipping during screensharing.

The text size, colour, opacity and location can be configured and placeholders can be added to generate dynamic information.



Watermark MS Outlook Emails – Adds the selected text at the beginning of an email, the same options for text size etc. and placeholders are available



Watermark Printed Materials – Will add the selected watermark to a document when it is physically printed out.

Watermark Printed Materials	
ENABLE	Font: Arial Size: 14px B <i>I</i> <u>U</u> A 50% Add Placeholder
<input checked="" type="checkbox"/>	%%CLASSIFICATION_LABEL%% %%USER_NAME%% %%TIMESTAMP%%

Watermark MS Office and PDF Files – Adds selected watermark to these types of document

Watermark MS Office and PDF Files					
ENABLE	VISUALIZATION Size: 14px B <i>I</i> <u>U</u> A 60% Add Placeholder				
<input checked="" type="checkbox"/>	<table border="1"> <tr> <td><input checked="" type="radio"/> Text</td> <td>%%USER_NAME%% %%CLASSIFICATION_LABEL%% %%TIMESTAMP%%</td> </tr> <tr> <td><input type="radio"/> Image</td> <td> Upload new image with .png extension Height: 0 inch </td> </tr> </table>	<input checked="" type="radio"/> Text	%%USER_NAME%% %%CLASSIFICATION_LABEL%% %%TIMESTAMP%%	<input type="radio"/> Image	Upload new image with .png extension Height: 0 inch
<input checked="" type="radio"/> Text	%%USER_NAME%% %%CLASSIFICATION_LABEL%% %%TIMESTAMP%%				
<input type="radio"/> Image	Upload new image with .png extension Height: 0 inch				

Off Premise DLP



Off-Premises DLP

Off Premise DLP adds additional controls when a device is away from the corporate network, printing can be blocked completely by toggling the switch off or rules enforced based on Policy or Classification of documents

Printing DLP in Off-Premises Mode

ALLOW PRINTING	REMEDIAL ACTIONS	DLP POLICY/CATEGORY	FLAG USER	NOTIFY MANAGER	LOG OPERATIONS
<input checked="" type="checkbox"/>	Log	ACME CORP:Public X	X	<input type="checkbox"/>	<input type="checkbox"/>
	Block	Customer Details X ACME CORP:Top Secret X ACME CORP:Secret X	X	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Justify	ACME CORP:Personal X	X	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Local PC Discovery



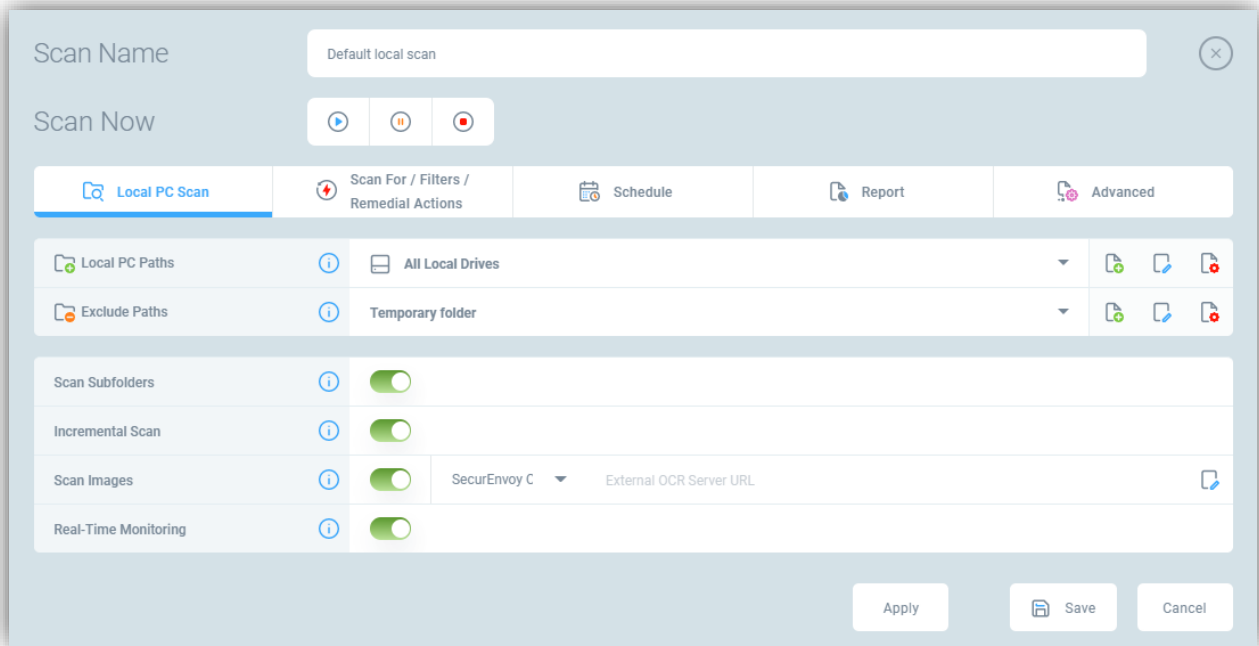
Local PC Discovery

You can run local discovery scans to search for an remediate sensitive data located on your endpoint.

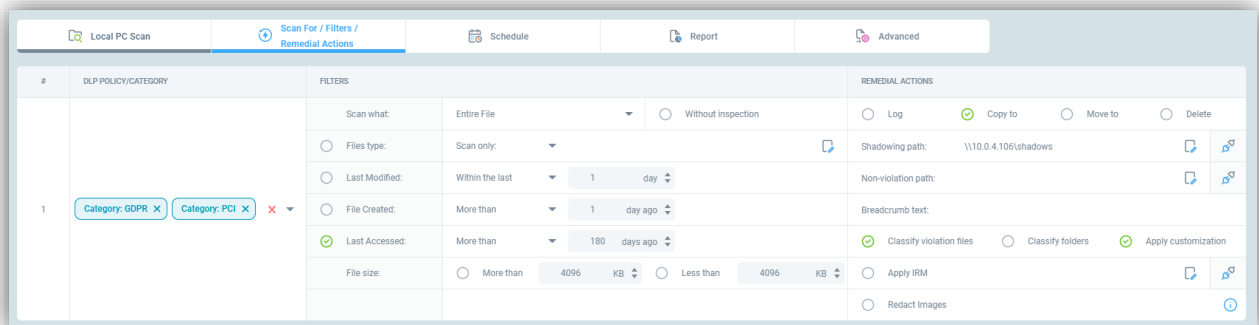
SCAN NAME			TOTAL FILES	SCANNED FILES	SCANNED, MB	REMEDIATION	MATCHES	DURATION	STATUS
Default local scan	--	--	--	--	--	--	--	--	--
	6	6	3121	3022	25,156.42		17	670h 31m	Calculated, 83%

Double clicking on the scan allows you to modify it.

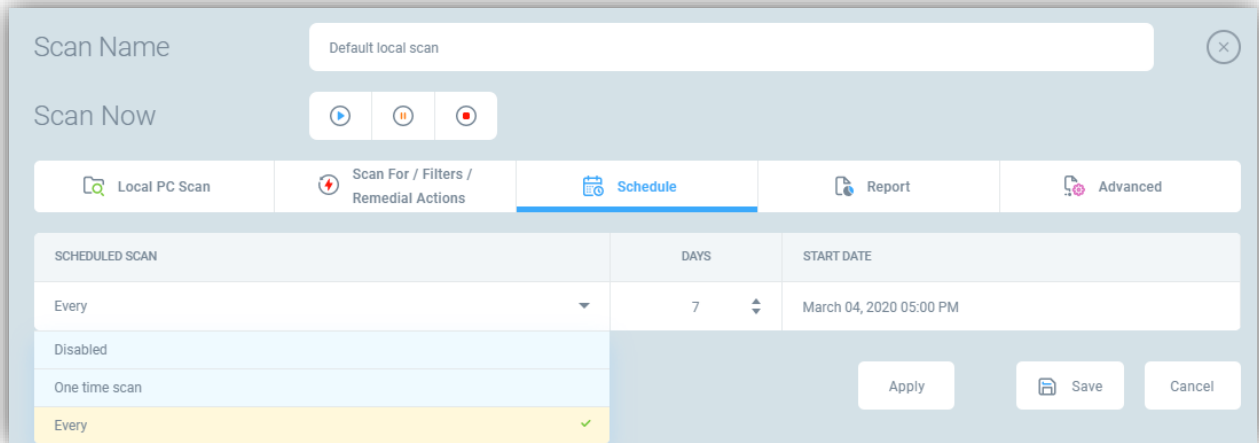
Choose what specific folders to scan and exclude, scan subfolders, configure incremental scans after the first run, scan images using the built in OCR capability or an external OCR server and monitor additional files and folders as they are created in realtime.



Configure the DLP policies you are looking for, filters on data creation and the remedial action to take when data is found



Choose how often you wish to run the scan.



Scan Name: Default local scan

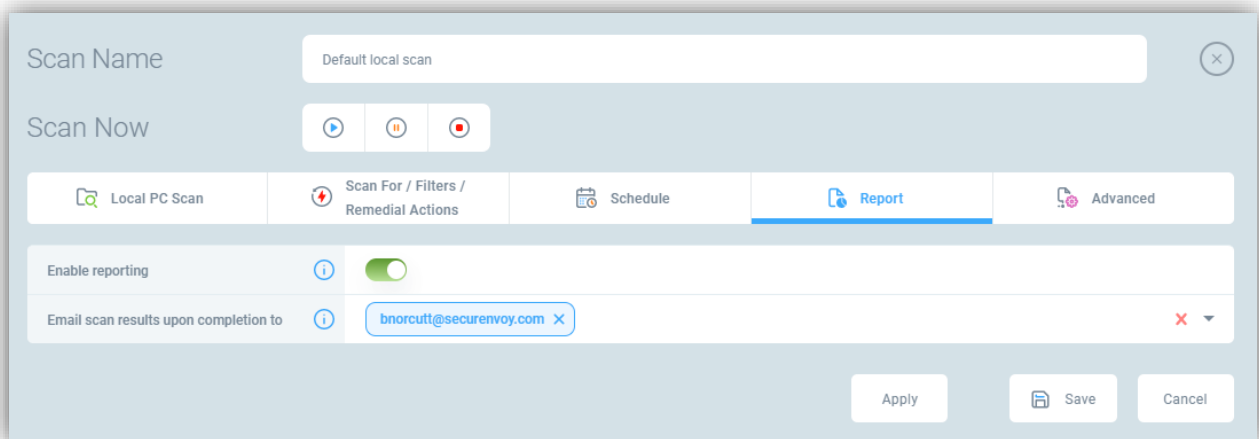
Scan Now: [Play] [Pause] [Stop]

Local PC Scan | Scan For / Filters / Remedial Actions | **Schedule** | Report | Advanced

SCHEDULED SCAN	DAYS	START DATE
Every	7	March 04, 2020 05:00 PM
Disabled		
One time scan		
Every		

Apply Save Cancel

Configure an email containing the scan results



Scan Name: Default local scan

Scan Now: [Play] [Pause] [Stop]

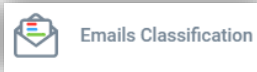
Local PC Scan | Scan For / Filters / Remedial Actions | Schedule | **Report** | Advanced

Enable reporting:

Email scan results upon completion to: bnorcutt@securenvoy.com

Apply Save Cancel

Email Classification



Adhoc classification – users can choose to classify the email if they want to

All the options can be enabled/disabled using the switches, green means it is enabled and yellow disabled, you can control what information if any gets put into the header and footer of the document including the font, size, colour as well as what the content using placeholders

Adhoc Classification		
ENABLE	INSERT	Font: Arial
<input type="checkbox"/>	<input type="radio"/> Header	Size: 14px
<input type="checkbox"/>	<input type="radio"/> Footer	B I U A

Force user to classify – users will not be able to send an email until they classify it, it provides the same options as ad-hoc

Force User to Classify		
ENABLE	INSERT	Font: Arial
<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Header	Size: 10px
<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Footer	B I U A

Classification: %%CLASSIFICATION_LABEL%%
 This email was classified by the sender. Please handle with care.

Classify Based on Content – The email will be classified based on its contents referenced to the DLP Policy Mapping setup under classification, if the PCI category is mapped to a classification of financial then any email containing PCI data will be classified as Financial

Classify Based on Content		
ENABLE	INSERT	Font: Arial
<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Header	Size: 10px
<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Footer	B I U A

Classification: %%CLASSIFICATION_LABEL%%
 This email contains **sensitive** data. Please handle with care.

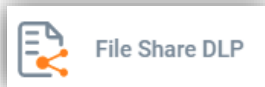
Classify Based on Emails Mapping – The email will be classified based the mappings set under *Classification > Emails Mapping*

Classify Based on Emails Mapping

ENABLE
INSERT
Font: Arial
Size: 8px
B
I
U
A
≡
≡
≡
</>
Add Placeholder

<input checked="" type="checkbox"/>	<input type="checkbox"/> Header	
<input type="checkbox"/>	<input type="checkbox"/> Footer	

File Share DLP

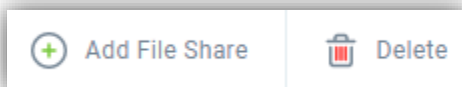


File share DLP allows you to monitor the configured file share for activities performed by users and apply controls on the types of data that is allowed to be interacted with on that particular file share.

#	DISPLAY NAME	ALLOW READ	ALLOW WRITE	MONITOR READ	MONITOR WRITE	MONITOR DELETE	MONITOR COPY	MONITOR ATTACH
1	All File Shares	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
REMEDIAL ACTIONS		DLP POLICY/CATEGORY			SHADOW FILES	FLAG USER	NOTIFY MANAGER	
Log	Not File Owner			x	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Block	Encrypted file	ACME CORP:Top Secret		x	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Justify	ACME CORP:Financial	ACME CORP:HR		x	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Add Exception
Edit
Delete

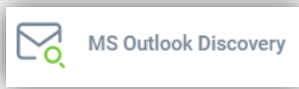
You can add and delete entries using the result selector



Printing DLP



MS Outlook Discovery



Outlook discovery scans local PST/OST outlook file stores for matching sensitive data, double click on the scan to modify the settings.

Choose what specific Mailboxes to scan, scan images using the built in OCR capability or an external OCR server and monitor additional emails as they are created in real time.

Scan Name

✕

Scan Now

▶
⏹

🔍 Outlook Scan

⚠ Scan For / Filters / Remedial Actions

📅 Schedule

📄 Report

⚙️ Advanced

Target Location	📁 Local Outlook files
Mailboxes	<div style="display: flex; align-items: center;"> i <div style="border: 1px solid #ccc; border-radius: 4px; padding: 2px 5px; margin-left: 5px;">All Outlook files</div> ✕ ✕ ▼ </div>
Autoupdate accounts list	<div style="display: flex; align-items: center;"> i <div style="margin-left: 5px;"> <input checked="" type="checkbox"/> </div> </div>
Scan Images	<div style="display: flex; align-items: center;"> i <div style="margin-left: 5px;"> <input checked="" type="checkbox"/> </div> <div style="margin-left: 10px;"> SecurEnvoy C ▼ External OCR Server URL </div> </div>
Real-Time Monitoring	<div style="display: flex; align-items: center;"> i <div style="margin-left: 5px;"> <input checked="" type="checkbox"/> </div> </div>

Apply

📄 Save

Cancel

Configure the DLP policies you are looking for, filters on email creation and the remedial action to take when data is found

#	DLP POLICY/CATEGORY	FILTERS	REMEDIAL ACTIONS
1	Category: PCI ✕	Scan what: Entire Email Email sent on: More than 1 day ago	Remedial action to Local PST/OST: <input type="radio"/> Log <input checked="" type="radio"/> Copy to <input type="radio"/> Move to <input type="radio"/> Delete MS Outlook folder: Remedial action to File Share: <input type="radio"/> Log <input checked="" type="radio"/> Copy to Shadowing path: \\10.0.4.106\shadows

Screen Controls



You can control if print screen is allowed and block it for certain Policies or Document classifications

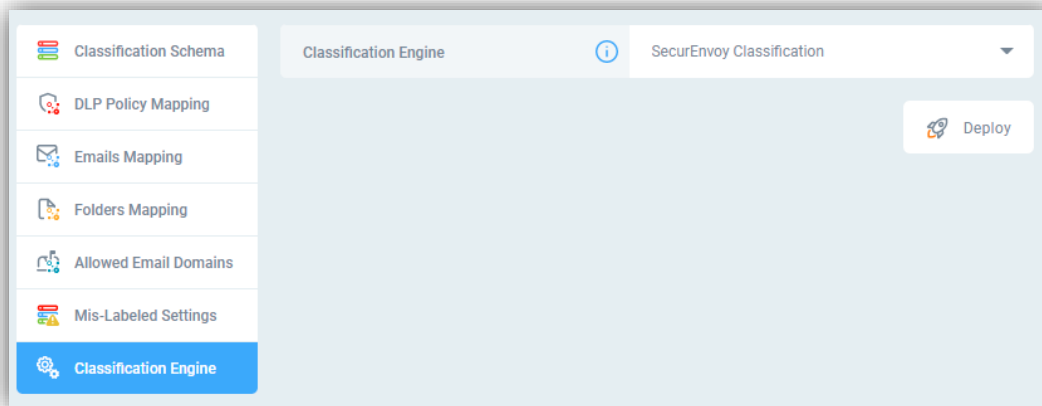
ALLOW PRINT SCREEN	REMEDIAL ACTIONS	CLASSIFICATION LABEL
<input checked="" type="checkbox"/>	<input type="checkbox"/> Log <input checked="" type="checkbox"/> Block	ACME CORP:HR ✕

Classification Setup

Classification setup is found under **SecurEnvoy DLP Setup > Classification**

 Classification Engine

To use the built-in classification engine, select “SecurEnvoy Classification” from the Classification Engine dropdown menu. Or, you can use 3rd party integration with Microsoft MIP labels, or Titus Labs (now part of HelpSystems).

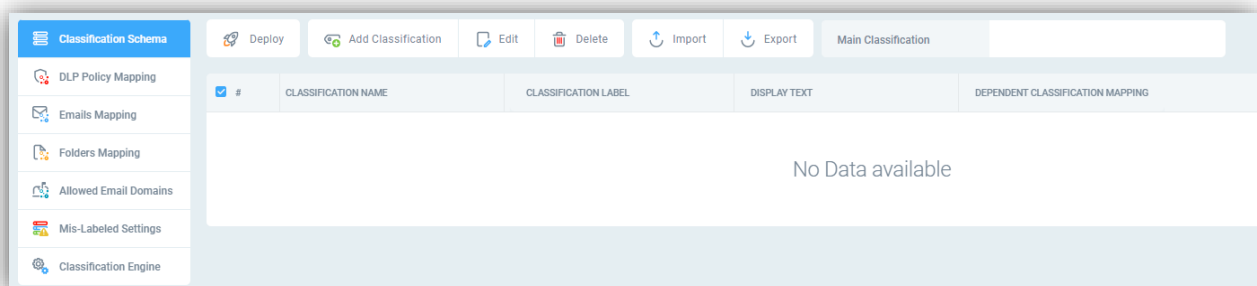


Once it is set click on “Deploy” to push these settings out

Classification Schema

 Classification Schema

Now you need to configure the mapping of classifications



Click on “Add Classification”

Add a description for the Classification Schema, here we have used “ACME CORP”

Click on “Add allowed Classification” for each new classification label you wish to add.

Add Classification Label ACME CORP DEFAULT CLASSIFICATION ✕

➕ Add allowed Classification
🗑️ Delete

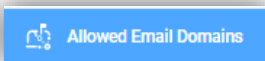
<input type="checkbox"/>	ORDER	CLASSIFICATION	DISPLAY TEXT	DEPENDENT CLASSIFICATION MAPPING	
<input type="checkbox"/>	1	Top Secret	Top Secret		⌵ ⌶
<input type="checkbox"/>	2	Secret	Secret		⌵ ⌶
<input type="checkbox"/>	3	Restricted	Restricted		⌵ ⌶
<input type="checkbox"/>	4	Confidential	Confidential		⌵ ⌶
<input type="checkbox"/>	5	Medical	Medical		⌵ ⌶
<input type="checkbox"/>	6	Financial	Financial		⌵ ⌶
<input type="checkbox"/>	7	HR	HR		⌵ ⌶
<input type="checkbox"/>	8	Public	Public		⌵ ⌶
<input type="checkbox"/>	9	Personal	Personal		⌵ ⌶
<input type="checkbox"/>	10	Internal	Internal Only - Do not distribute		⌵ ⌶

💾 Save 🚫 Cancel

Click on “Save”

Click on “Deploy”

Email Mapping



It’s a good idea to configure your “allowed” internal email domains when using classification labels. Open the Allowed Email Domains section

☰ Classification Schema
🚀 Deploy
➕ Add Mapping
✎ Edit
🗑️ Delete
📶 Import
📄 Export
🔄 Refresh Fingerprints

- 🔗 DLP Policy Mapping
- ✉️ Emails Mapping
- 📁 Folders Mapping
- 📧 Allowed Email Domains
- 🚫 Mis-Labeled Settings
- ⚙️ Classification Engine

<input type="checkbox"/>	#	CLASSIFICATION NAME	CLASSIFICATION LABEL	DEPENDENT CLASSIFICATION LABEL	ALLOWED EMAIL DOMAINS/ADDRESSES
<input type="checkbox"/>	1	ACME CORP	Internal		+securenvoy.com +securenvoy/lab.co.uk

Click Add Mapping, select the ‘Internal’ name from the dropdown list and enter the required internal domain(s) in the following format... “.+DomainName.com”

Edit Allowed Domains Mapping ✕

Classification Name	i	ACME CORP	
Classification Label	i	Internal	▼
Dependent Classification Label			
Email Domains/Addresses	i	<input type="text" value="+secureenvoy.com"/> ✕ <input type="text" value="+secureenvoylab.co.uk"/> ✕	✕ ▼

Click on “Save”

Click on “Deploy”

DLP Policy Mapping



Map DLP Policies to the appropriate mapping of classification label. Open the DLP Policy Mapping section.

#	CLASSIFICATION NAME	CLASSIFICATION LABEL	DEPENDENT CLASSIFICATION LABEL	DLP POLICIES
<input type="checkbox"/>	ACME CORP	Internal		<input type="button" value="UK PHI"/> <input type="button" value="UK Passport Information"/> <input type="button" value="CCN"/>
<input type="checkbox"/>	ACME CORP	Finance		<input type="button" value="Brazilian SWIFT Code 1"/>
<input type="checkbox"/>	ACME CORP	HR		<input type="button" value="SSN"/>
<input type="checkbox"/>	ACME CORP	Restricted		<input type="button" value="Encrypted file"/>

For example, set specific DLP Policies for ‘Internal’ classification label (e.g. regex, dictionary, file type, fingerprint). Open the entry and add the required DLP Policy(s).

Edit DLP Policy Mapping ✕

Classification Name	ACME CORP
Classification Label	Internal ▼
Dependent Classification Label	
DLP Policies	UK PHI ✕ UK Passport Information ✕ CCN ✕ ✕ ▼

Save Cancel

Click on “Save”

Click on “Deploy”

Discovery Targets

File Shares

MS Exchange

MS SharePoint

Databases

Discovery – Cloud Platforms

Amazon S3

Citrix Sharefile

Miscellaneous

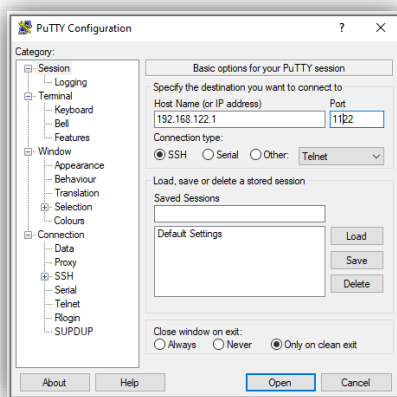
Upgrading the Central Console

IMPORTANT – Take a backup of the Configuration settings including the Event logs. Also, it is best practice to take a complete server backup (or snapshot) of the current server state BEFORE performing the upgrade.

- 1) Log in to the Console CLI using PuTTY and root credentials on port 1122

Username: root

Password: pass8397@



- 2) Once logged in you need to obtain the latest upgrade patch, this actual filename can be obtained by contacting your partner or SecurEnvoy, in this example we are upgrading to 15.13.x **make a note of the exact file name you've been given for the command below**

- 3) Type the following command at the prompt:

```
rpm -Uvh https://downloads.securenvoy.com/dlp/SecurEnvoy-cc-15.13.1-22505.NG.SecurEnvoy.el7.x86_64.rpm
```

- 4) Once this has installed type the following command

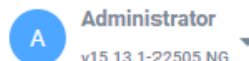
```
yum update
```

Note: "yum update" updates all the presently installed packages to their latest versions that are available in the repositories.

- 5) Answer "Y" to any prompts and wait for "Complete!". Then type "exit" to close the PuTTY session.

- 6) **Open the Central Console URL from a browser.** You will note the "System restart required..." message. Click the 'Restart' button and wait for the system to restart...

System restart required to apply OS updates



Ports

FROM	TO													
	Inspector						Central Console			SMTP	DNS	LDAP	File Share	OCR Server
	25	443	1122	1344	2222 (udp)	17023	443	1122	17023	25	53	389		443
Central Console			●			●				●	●	●	●	●
Inspector						●	●	●	●	●	●	●	●	
Endpoint Agent					●	●	●		●				●	●
Security Manager						●			●				●	
Admin PC		●	●		●	●	●	●	●				●	●
Proxy Server				●										
SMTP Server	●													

Additional ports:

Port 17023 TCP from Endpoint to Endpoint to share fingerprints

Port 443 TCP from Endpoint to IRM server if IRM is being used

Port 3128 TCP from Endpoint to the inspector if internal SSL Proxy is used

OCR

The following filetypes are supported by the OCR engine

BMP, GIF, PNG, TIF, JPEG, AI, JFIF, PNM, JPS, JPF

The following languages are supported by the OCR engine

English language only

Endpoint Comparison

DLP Agent Functionality Matrix

Function	Windows	Mac	Linux
Network DLP	●	●	●
Application Controls	●	●	●
Copy Controls	●	●	●
Other (e.g. block tethering, Bluetooth, notify on USB, write limit notifications)	●	●	●
Device Controls	●	●	●
File Classification (Office)	●	●	●
Watermarking	●	●	●
Local Discovery	●	●	●
Email Classification (Outlook)	●	●	●
File Share Audit	●	●	●
Printing DLP	●	●	●
MS Outlook Discovery	●	●	●
Screen Controls	●	●	●

● = Feature available

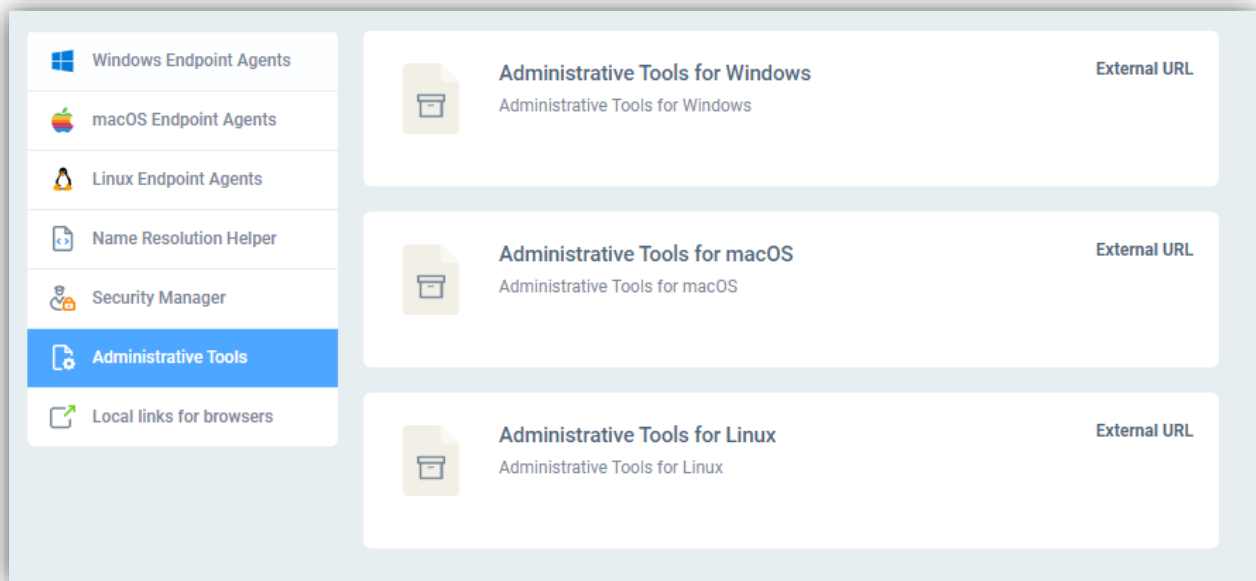
● = Feature being developed

● = Feature not available

Configure Windows Agent for New Console IP Address

If the IP address of the central console has changed or you wish to point agents at a child console for their policy there are 2 approaches to achieve this

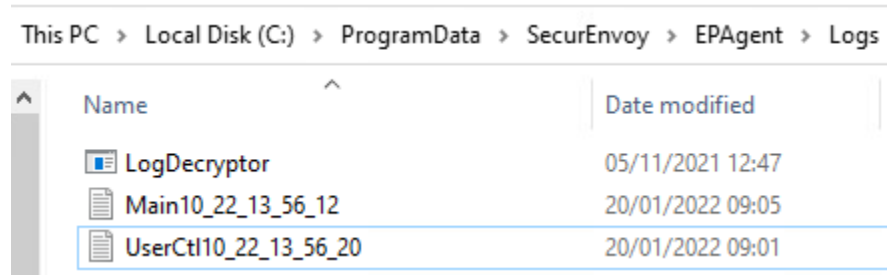
1. Change IP using commandline
 - a. `msiexec.exe /quiet /i path_to_agent.msi CONSOLE_ADDRESS=10.0.0.1 DISCOVERY=0`
2. Patch msi package with new IP
 - a. Download the administrative tools from the central console



- b. Extract the zip file to a folder and copy the agent msi executable to the EPAgent subfolder, SecurEnvoyAdministrativeTools-windows\SecurEnvoyAdministrativeTools-windows\EPAgent Configure
- c. Open a cmd or PowerShell prompt
- d. Run `configure.bat` and follow the prompts, choose 0 for the priority
- e. The agent is now patched with the IP address and can be deployed as normal

Collect Agent Log Files

Windows Agent log files are located in: C:\programdata\SecurEnvoy\EPAgent\Logs



Name	Date modified
LogDecryptor	05/11/2021 12:47
Main10_22_13_56_12	20/01/2022 09:05
UserCtl10_22_13_56_20	20/01/2022 09:01

The log files are obfuscated (hidden) by default. The 'LogDecryptor' tool is used to convert them to plain text, this tool will not exist in the folder by default but is available from the Administrative Tools zip package available on the Central Console

- EPAgent Configure
- EPAgent Log Decryptor
- EPAgent Remove
- EPAgent Service Unlocker
- EPAgent UserInfo

Uninstall the Windows Agent

The Windows uninstall process is designed to keep the "SecurEnvoy Network Scanner" service (and also if Agent uninstall command is used *without* a special key).

To uninstall Agent completely you can use one of the following ways:

1) Run CMD as Administrator and browse to the folder with the MSI (it should be exactly the same version of the MSI, which is installed)

Type: `msiexec /x AGENT_NAME.MSI REMOVE_SCANNER=1`

2) Download the Administrative tools from the Central Console "-> Help -> Downloads -> Administrative Tools -> For Windows"

- Extract the archive.
- Run CMD as Administrator and browse to the folder "EPAgent Remove".
- Run the "Remove.bat" file.