drainware

User’s Manual v1.0

November 2013

0. INTRODUCTION

0.1. HOW TO READ THIS MANUAL

This manual is written either to be read sequentially the first time, or can be used as a reference guide. During this reading you can find notices in the following formats:

📝 Annotations: Concept clarifications

⚠ Important!: Important concepts to keep in mind

Tip: Tricks, shortcuts and other tips

0.2. ABOUT DRAINWARE

Drainware is a security platform that is like a service. It has several modules to protect the information and/or the computers that contain this information.

We offer Freemium license which means you can start using it for free with some restrictions in its features.

1. REQUIREMENTS

1.1. OPERATING SYSTEM

Drainware can be deployed on computers with Microsoft Windows OS installed. The currently supported versions are the following:

OS	Architecture
Windows XP	x86
Windows 7	x86/x64
Windows 8	x86/x64

⚠ Important!

Windows XP is supported only with Service Pack 3 or later. We also have support for Windows XP SP2, but you have to install the following components:

Windows Search 4.0 for Windows XP (KB940157)

Wireless LAN API (KB918997)

1.2. **MINIMUM** HARDWARE

CPU: Intel Pentium III 1 GHz or faster

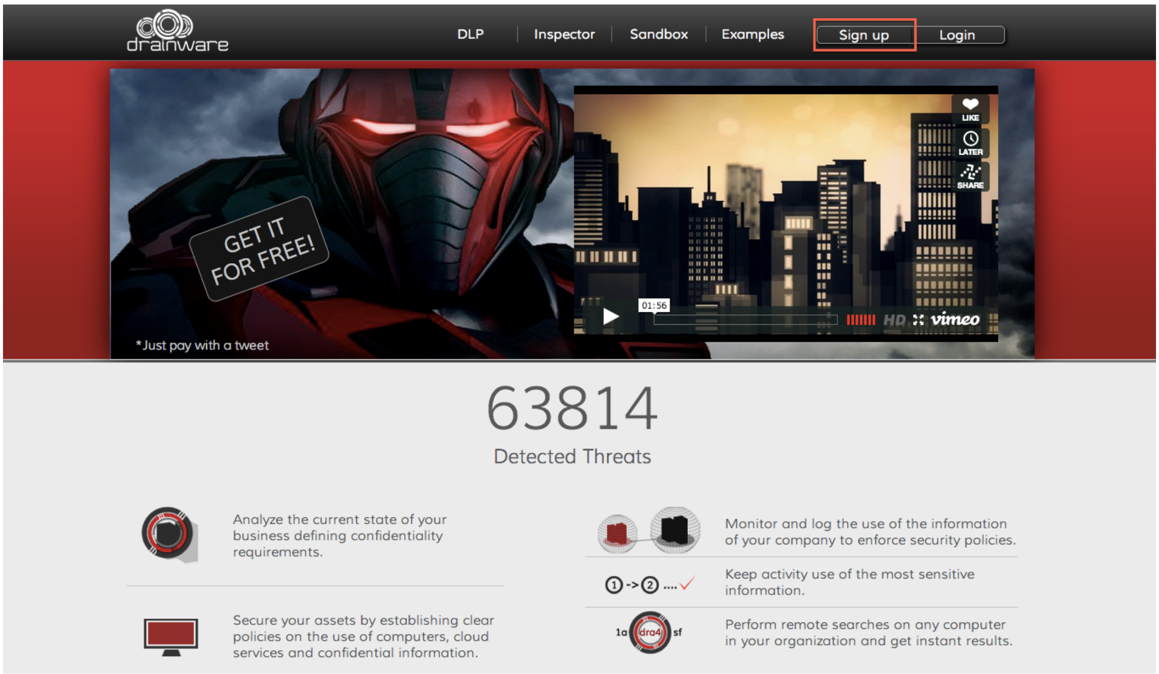
RAM: 1 GB (2GB recommended)

HDD: 200 MB

2. INSTALLATION

2.1. SIGNING UP IN THE SYSTEM

Before installing Drainware, it's necessary to have an account in the platform. To sign up in the system you'll have to go to the official Drainware website at https://www.drainware.com and click on the *sign up* button in the top right menu.



63814

Detected Threats

Analyze the current state of your business defining confidentiality requirements.

Secure your assets by establishing clear policies on the use of computers, cloud services and confidential information.

Monitor and log the use of the information of your company to enforce security policies.

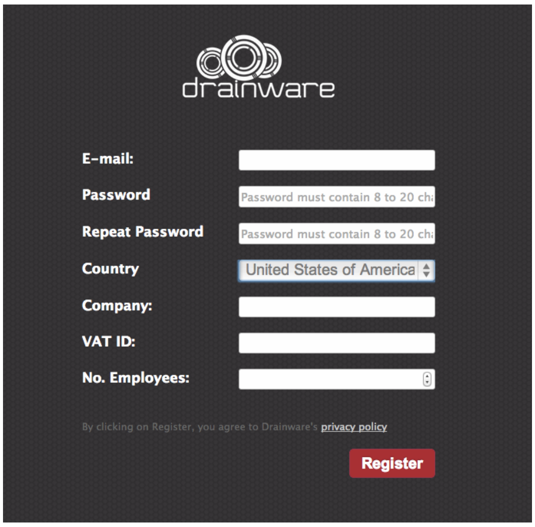
Keep activity use of the most sensitive information.

Perform remote searches on any computer in your organization and get instant results.

This will show us a form where we must input the information requested: registry data, company name, VAT ID, and number of employees.

The e-mail will be associated with you account and it won't be able to be changed in the future.

For the number of employees field, we only have to consider the ones that normally work with a computer.



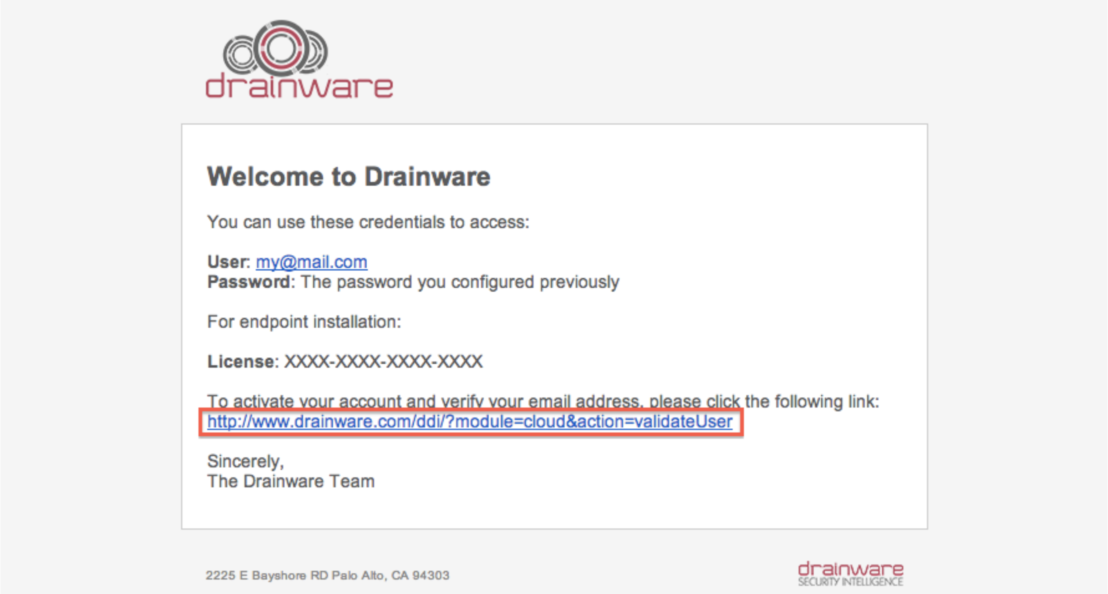
drainware

E-mail:	
Password	Password must contain 8 to 20 ch
Repeat Password	Password must contain 8 to 20 ch
Country	United States of America
Company:	
VAT ID:	
No. Employees:	

By clicking on Register, you agree to Drainware's privacy policy

⚠ Important!: The password must have at least 8 characters.

Afterwards, you will receive an e-mail that will allow you to validate your new account.



drainware

Welcome to Drainware

You can use these credentials to access:

User: my@mail.com
Password: The password you configured previously

For endpoint installation:

License: XXXX-XXXX-XXXX-XXXX

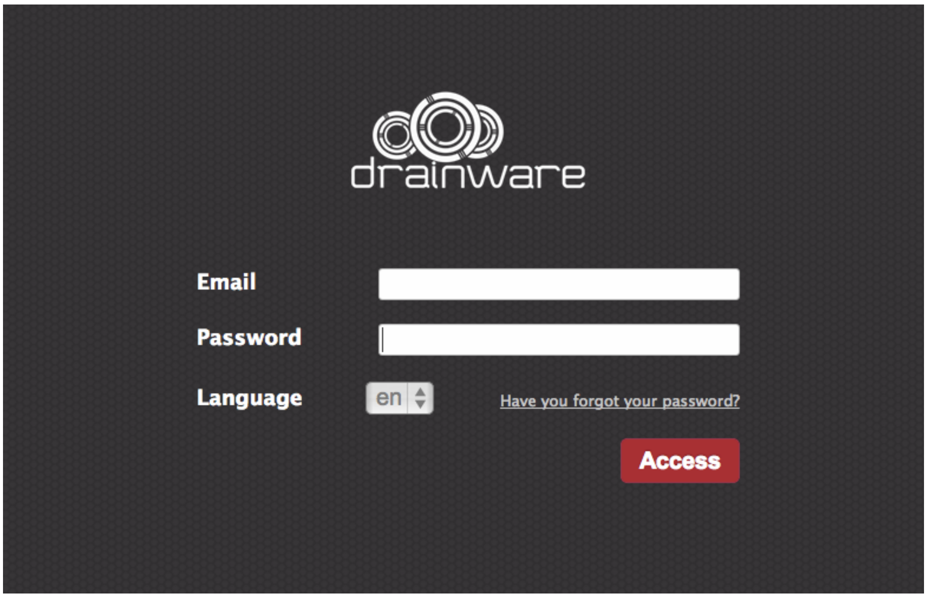
To activate your account and verify your email address, please click the following link:
http://www.drainware.com/ddi/?module=cloud&action=validateUser

Sincerely,
The Drainware Team

2225 E Bayshore RD Palo Alto, CA 94303

drainware SECURITY INTELLIGENCE

When the license has been validated, it will redirect us to the sign in page where we will have to input the e-mail and the password that we have entered in before.



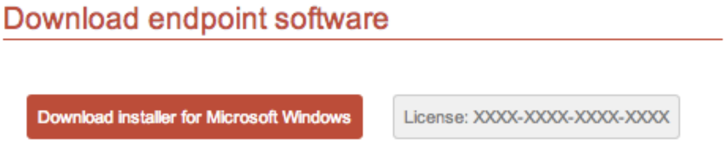
Email

Password

Language en

2.2. SOFTWARE ENDPOINT INSTALLATION

Once we have the license validated and entered our credentials, we are correctly signed in and able to download the software. After sign in, we have the possibility to download the installer. To the right of the download link, we have the license number that is a 16 digit code that we will need during the installation.



Download endpoint software

License: XXXX-XXXX-XXXX-XXXX

This installer will install the 32 or 64-bit version, depending on the operative system used.

2.3. ADVANCED INSTALLATION

It is possible to deploy the endpoint in an unattended manner. This is very useful if you have a lot of users and you want to deploy it on a mass scale.

To do that, you can find the .msi installers available in the following URL

http://update.drainware.com/

The procedure to install it through the command line is below (where you must replace the red text by your license number):

```
msiexec /i file.msi  /quiet /noreboot  DDI_LIC=XXXX-XXXX-XXXX-XXXX
```

If you prefer you can use this logon script:

Name: drainware_logon.vbs

```
Function GetWindowsArchitecture(strComputerName)

        Set objWMI = GetObject("winmgmts://" & strComputerName & "/root/cimv2")

        Set colItems = objWMI.ExecQuery("Select * from Win32_OperatingSystem", , 48)


        For Each objItem In colItems

                GetWindowsArchitecture = "32-bit"

                If left(objItem.Version,3) >= 6.0 Then

                        GetWindowsArchitecture = objItem.OSArchitecture

                End If

        Next

End Function



Function GetProgramsFolder()

        Set wshShell = WScript.CreateObject("WScript.Shell")

        GetProgramsFolder = wshShell.ExpandEnvironmentStrings("%programfiles%")

End Function



Function ExistDrainwareSecurityDir()

        Set objFSO = CreateObject("Scripting.FileSystemObject")

        ExistDrainwareSecurityDir = objFSO.FileExists(GetProgramsFolder() &
"\Drainware\Drainware Security Endpoint\DrainwareSecurityAgent.exe")

End Function


Function DownloadDSE(strRemoteDSE, strLocalDir)
```

```
        Set objFSO = CreateObject("Scripting.FileSystemObject")
        objFSO.CopyFile strRemoteDSE, strLocalDir & "\"
End Function



Function InstallDSE(strLicense, strRepository)
        If  Not ExistDrainwareSecurityDir() Then
                Set wshShell = WScript.CreateObject("WScript.Shell")
                Select Case GetWindowsArchitecture(".")
                        Case "64-bit"
                                Rem Msgbox  "Installing Endpoint 64-bit " &
strLicense
                                strRemoteDSE = strRepository & "\SetupCloud.msi"
                                strLocalDSE =
wshShell.ExpandEnvironmentStrings("%temp%") & "\SetupCloud.msi"
                        Case "32-bit"
                                Rem Msgbox  "Installing Endpoint 32-bit " &
strLicense
                                strRemoteDSE = strRepository & "\SetupCloud32.msi"
                                strLocalDSE =
wshShell.ExpandEnvironmentStrings("%temp%") & "\SetupCloud32.msi"
                End Select
                DownloadDSE strRemoteDSE,
wshShell.ExpandEnvironmentStrings("%temp%")
                Rem Msgbox "msiexec /qn /i " & strLocalDSE & " ddi_lic=" &
strLicense
                Rem WshShell.Run "msiexec /qn /i " & strLocalDSE & " ddi_lic=" &
strLicense
                Msgbox "Your computer will restart after a few seconds"
        End If
End Function


Dim strLicense
Dim strRepository

strLicense = WScript.Arguments(0)
strRepository = WScript.Arguments(1)
InstallDSE strLicense, strRepository
```

Usage:

drainware_logon.vbs LICENSE LOCATION

example: drainware_logon.vbs XXXX-XXXX-XXXX-XXXX \\mynas\resources\dlp\

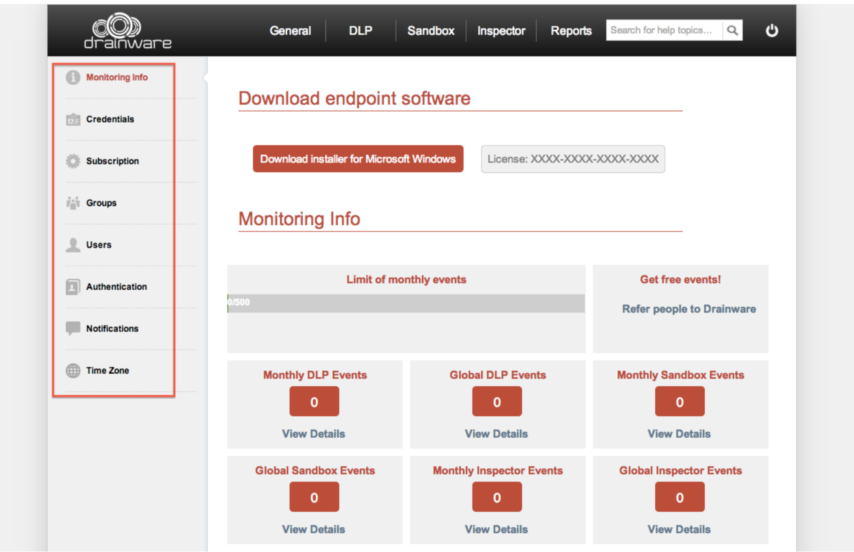
The location must contains both msi files (for x86 and x64)

Useful links

Create a GPO (Windows 2008)

3. INITIAL CONFIGURATION

In this section, we will go through the initial configuration of Drainware. These are the available options in the left menu (red area) of Drainware once you sign in.



Download endpoint software

License: XXXX-XXXX-XXXX-XXXX

Monitoring Info

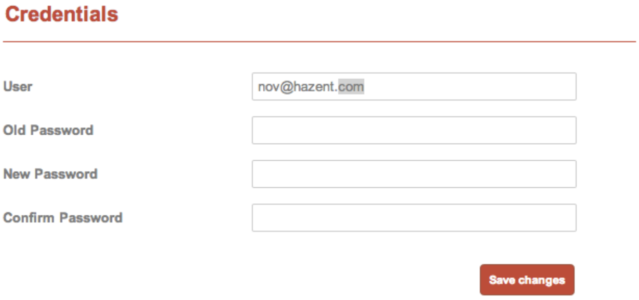
Limit of monthly events: 0/500

Get free events! Refer people to Drainware

Monthly DLP Events 0 View Details	Global DLP Events 0 View Details	Monthly Sandbox Events 0 View Details
Global Sandbox Events 0 View Details	Monthly Inspector Events 0 View Details	Global Inspector Events 0 View Details

3.1. CREDENTIALS

In this section we can update our password. If we want to change it, we also have to fill in the current password.



Credentials

User	nov@hazent.com
Old Password	
New Password	
Confirm Password	

3.2. SUBSCRIPTION

Drainware has two different subscription types. One is the Freemium option, which offers a monthly service with a limit of 500 security events; after 500 events, the organization will be unprotected until the first day of the next month.

On the other hand, we offer a Premium subscription that is based on the number of users you wish to protect. The Premium subscription includes unlimited events (as long as use remains reasonable).

In this section, it is possible to check the validity of the subscription and upgrade in the case of using a Freemium subscription.

If you have questions about this section, please write an e-mail to sales@drainware.com and our sales team will be happy to assist you.

3.3. GROUPS

It is possible that in your organization you would like to apply different policies depending on groups of users. We can organize the groups by areas or departments, depending on the requirements of the organization.

In this section we can create the groups inside our platform and then apply policies directly over them.

It is possible to integrate the groups in the organization directly with Drainware, and this topic is explained in more detail in section 4.5.

3.4. USERS

Every time that user logs into a computer protected with Drainware, the server is notified, and it will register it in the system. From that moment, we can associate that user to one or more groups.

3.5. AUTHENTICATION

To integrate Drainware with your organization, we offer an authentication module. We have 2 different options to configure the authentication module: local authentication or LDAP.

By default, Drainware works in the local authentication mode, in such a way that the group information is already in our platform.

With the LDAP option, it's possible to integrate an LDAP server or Active Directory Domain to be able to use the users and groups of the organization.

If you want to integrate LDAP, it's necessary to open the LDAP port to the Internet. We recommend opening it with SSL exclusively.

If you want to integrate it with Active Directory, you should use the following information:

Field	Value
Type	LDAP
SSL	Depending on your configuration
Version	2.0
Host	IP or Computer Name

Port	389 or 636 if it’s SSL
DN	DOMAIN\user
Password	User Password
Base	DC=DOMAIN, DC=LOCAL
User Attr	sAMAccountName
Recursive Groups	Optional

We also have the “Recursive Groups” option. This option allows users in nested groups to resolve the groups to which they don’t directly belong.

Annotation: If an LDAP user doesn’t belong to any of the imported groups, it will belong to the default group automatically.

Important!:

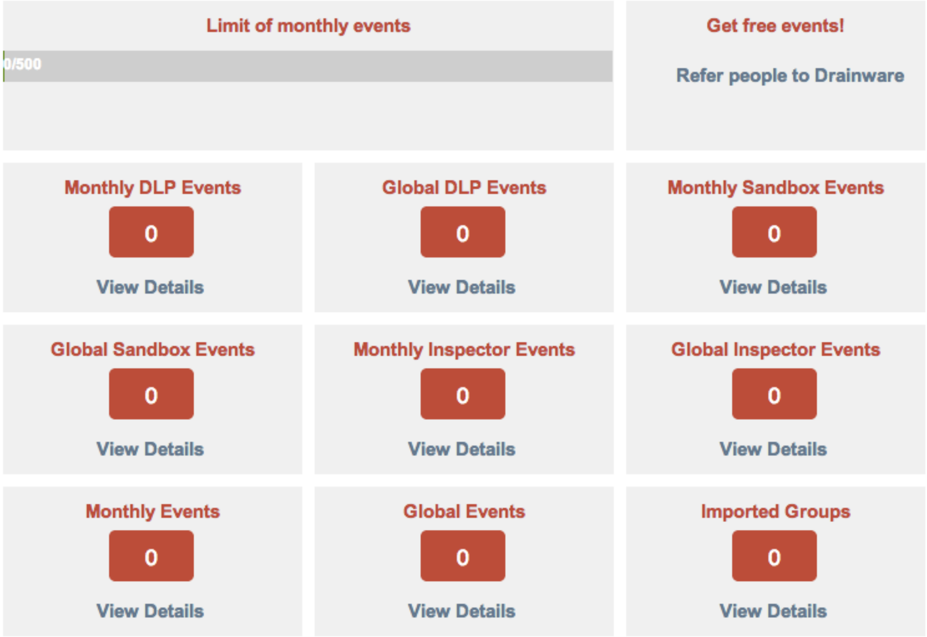
When the LDAP is integrated, all users will be available in the platform however same doesn’t happen with the groups. The groups must be imported one by one from the groups section, which will also be integrated with LDAP.

3.6. TIME ZONE

It’s possible that the employees of an organization work or travel around the world. Therefore, in Drainware, we work with the UTC time zone. In order to translate the time between different time zones, we offer the possibility to select the time zone where the administrator wishes to see the events.

4. DASHBOARD

The main window of Drainware shows an overview of the security events that happened since the installation of Drainware. It also shows the details of the events that happened since the beginning of every month.



Limit of monthly events

0/500

Get free events!

Refer people to Drainware

Monthly DLP Events
0
View Details

Global DLP Events
0
View Details

Monthly Sandbox Events
0
View Details

Global Sandbox Events
0
View Details

Monthly Inspector Events
0
View Details

Global Inspector Events
0
View Details

Monthly Events
0
View Details

Global Events
0
View Details

Imported Groups
0
View Details

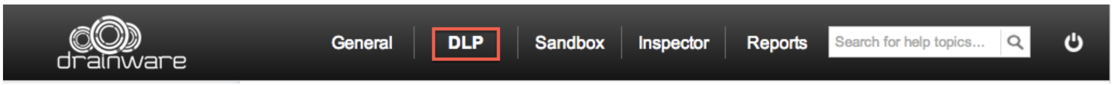
For Freemium users, it shows a status bar that shows the monthly events. When the number of events reaches 500, Drainware will stop working until the beginning of the next month. The administrator will then receive an e-mail notification that the organization is not protected with Drainware anymore.

Tip:

To the right of the monthly events bar you can find a link to get more free events per month in the Freemium version. To receive more free events, you only have to share a link with the reference code. For every verified installation referred to this code, Drainware will give you 100 extra free events per month.

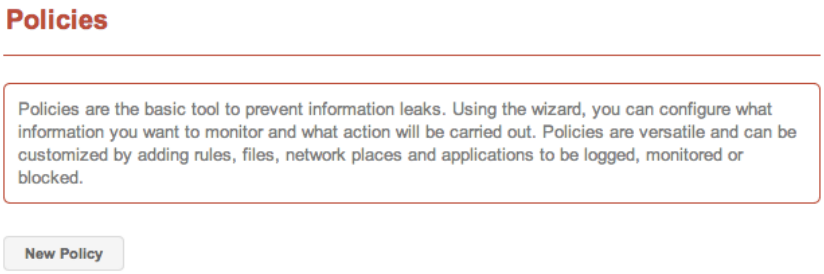
5. DLP

In the DLP module (Data Leak Prevention), we can control the confidential information inside the organization to prevent data leaks.



5.1. POLICIES

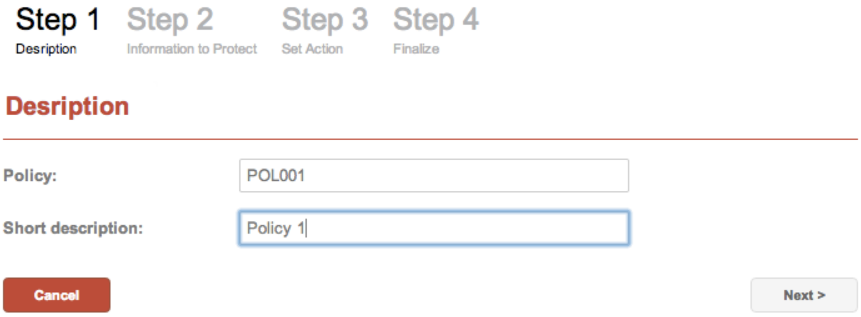
The policies define what information you want to monitor and what action will be carried out. In the policies creation section, we provide a wizard that makes the whole process easier. We're going to create a policy with the name POL001 and the description of "*Policy 1*".



Policies

Policies are the basic tool to prevent information leaks. Using the wizard, you can configure what information you want to monitor and what action will be carried out. Policies are versatile and can be customized by adding rules, files, network places and applications to be logged, monitored or blocked.

In the first step we have to provide a name and a short description for the policy:



Desription

Policy: POL001

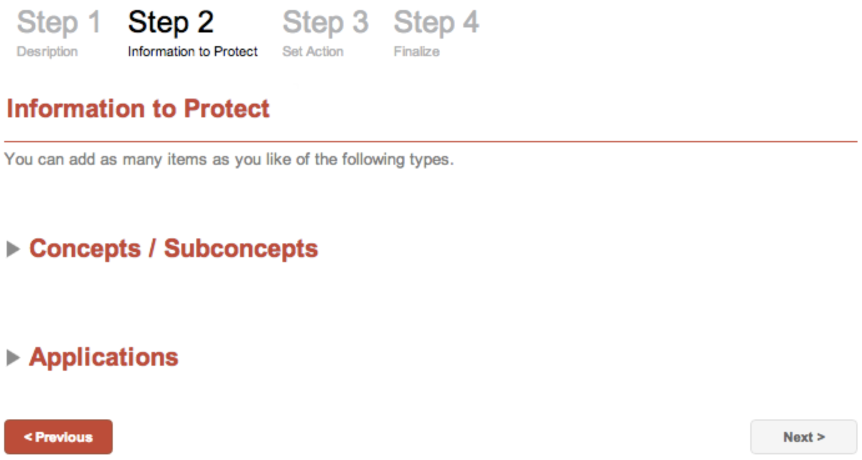
Short description: Policy 1

In the next step we have to define the information that we want to protect.

We can see the next menu:

- Concepts / Subconcepts: patterns predefined by Drainware to identify the information.
- Applications: applications that we'll deny any access to confidential information.

As we continue configuring Drainware, this section will contain other elements such as rules, files, and network sites; which will see in the next sections.



Step 1 Desription | Step 2 Information to Protect | Step 3 Set Action | Step 4 Finalize

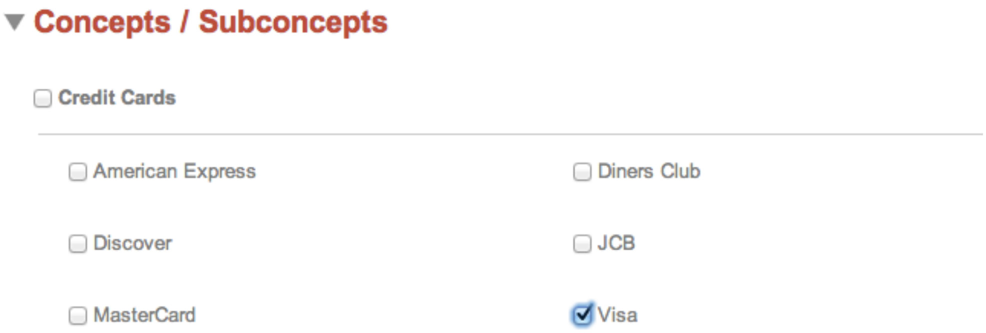
Information to Protect

You can add as many items as you like of the following types.

▶ Concepts / Subconcepts

▶ Applications

If we expand the Concepts/Subconcepts we will see a big list of categories. We can include a sub concept in our policy like Visa or the credit cards concept that would include all credit card types.

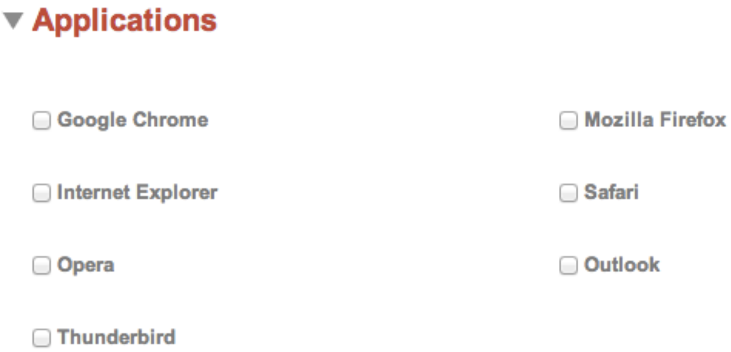


▼ Concepts / Subconcepts

□ Credit Cards

□ American Express
□ Diners Club
□ Discover
□ JCB
□ MasterCard
☑ Visa

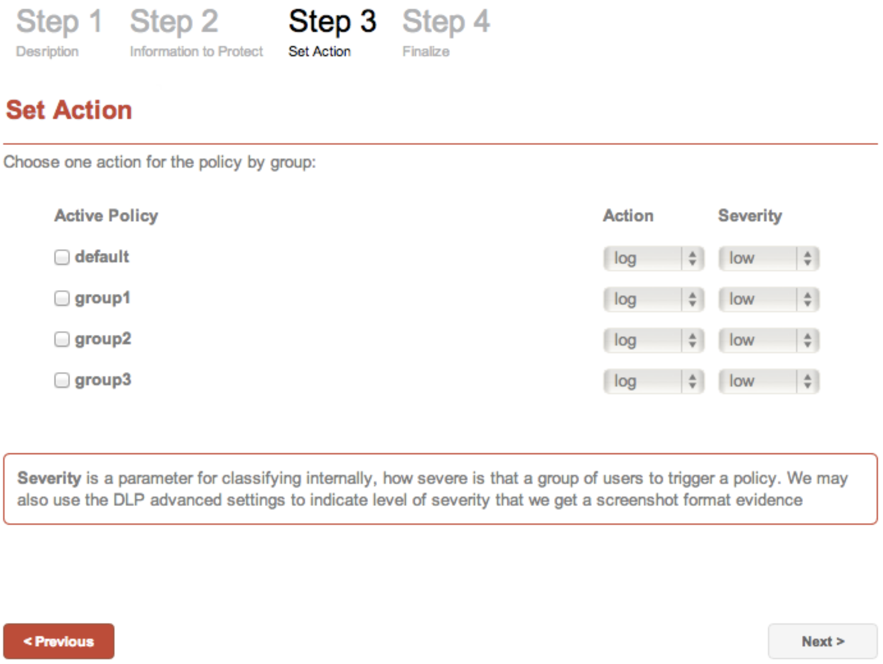
In the applications section, we can see a list (that can be extended by the user) that allows the blocking of several programs.



▼ Applications

□ Google Chrome
□ Mozilla Firefox
□ Internet Explorer
□ Safari
□ Opera
□ Outlook
□ Thunderbird

In the Step 3 we can see a list of the groups that we have already imported, the action that will be carried out, and the severity (how severe is the group of users that triggered the policy).



Set Action

Choose one action for the policy by group:

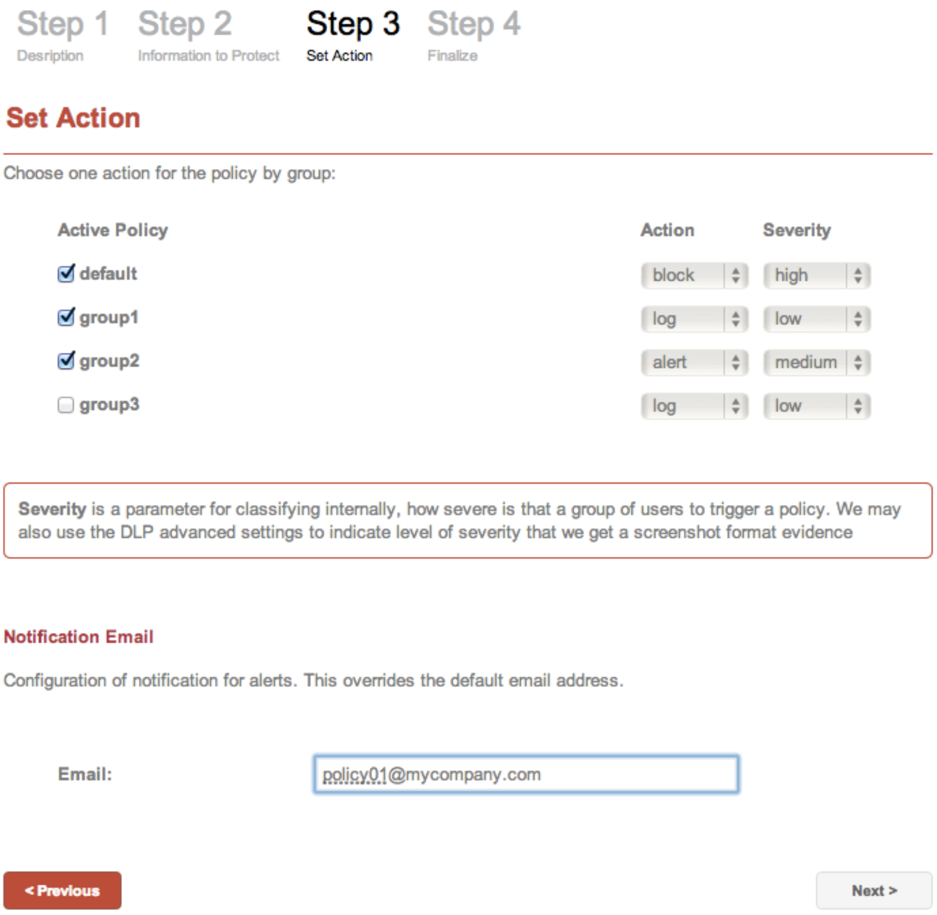
Active Policy	Action	Severity
□ default	log	low
□ group1	log	low
□ group2	log	low
□ group3	log	low

Severity is a parameter for classifying internally, how severe is that a group of users to trigger a policy. We may also use the DLP advanced settings to indicate level of severity that we get a screenshot format evidence

We only have to select the groups that we want to be affected by the policy. When defining the action, it can be:

- Log: logs the event in the Drainware database for audit purposes.
- Alert: an e-mail is sent by default to the e-mail address used for sign up in Drainware, but it can be overridden by another address specified only for this policy.
- Block: prevents filtering of information.

In all cases, the employee that executes the policy will see a notification.



Set Action

Choose one action for the policy by group:

Active Policy	Action	Severity
☑ default	block	high
☑ group1	log	low
☑ group2	alert	medium
□ group3	log	low

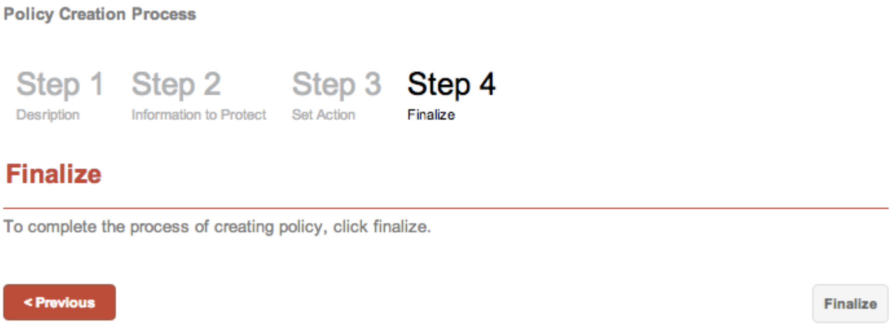
Severity is a parameter for classifying internally, how severe is that a group of users to trigger a policy. We may also use the DLP advanced settings to indicate level of severity that we get a screenshot format evidence

Notification Email

Configuration of notification for alerts. This overrides the default email address.

Email: policy01@mycompany.com

We only have to click the "Finalize" button and the policy will be created.



Policy Creation Process

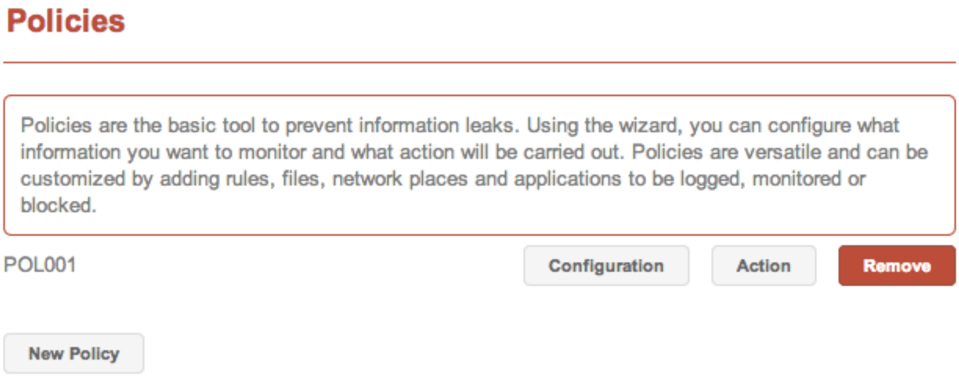
Finalize

To complete the process of creating policy, click finalize.

Every time we create a policy, it will appear in the policies list. In this list, we have 3 buttons:

- Configuration: we can configure the information to protect, like we configured in step 2.
- Action: we can re-define actions for the different groups, like we configured in step 3.
- Remove: removes the policy.

Once the policy is created, it can't be renamed.



Policies

Policies are the basic tool to prevent information leaks. Using the wizard, you can configure what information you want to monitor and what action will be carried out. Policies are versatile and can be customized by adding rules, files, network places and applications to be logged, monitored or blocked.

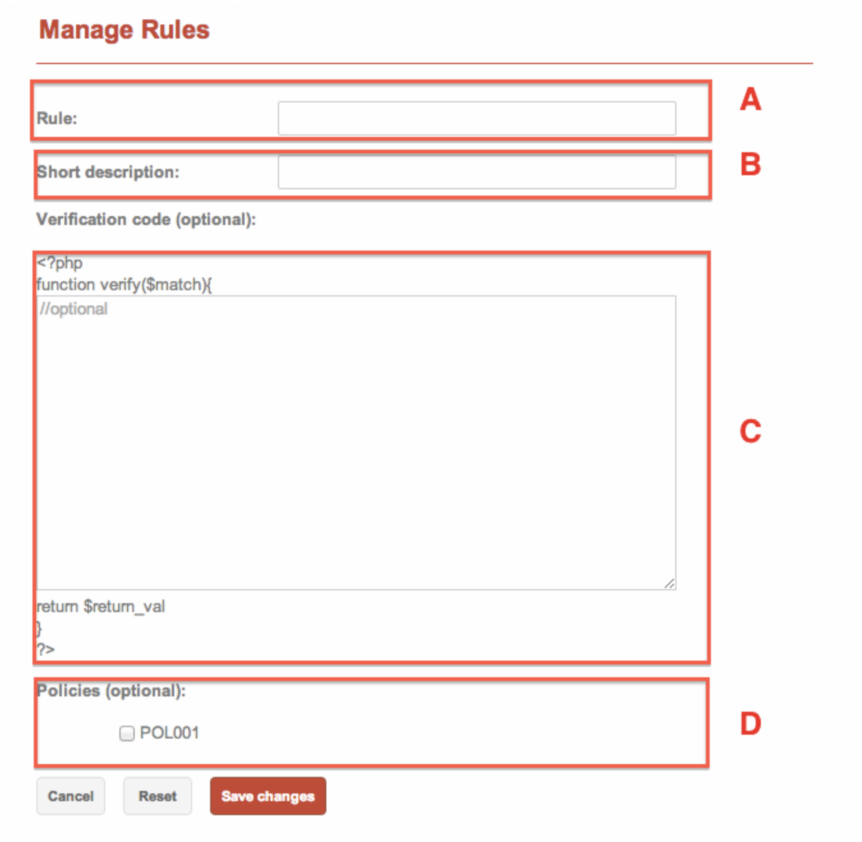
5.2. RULES

With "Rules", we can define our own information patterns to protect inside the policies. We can include, for example, confidential footers that we usually introduce in documents with confidential information. We can also add regular expressions that describe any confidential documents that we want to protect.

To create a rule, we have to introduce a name without spaces and special characters (A), a description (B), optionally, we can include a verification function in PHP (C) and we can define which policies we want to associate with this rule (D). Like policies, rules can't be renamed either.

Tip:

If we want to use a verification function in PHP, it will receive the variable "$match" that contains the resulting match after the regular expression is applied. It will be necessary that after analyzing $match, it will assign TRUE (accept match) or FALSE (deny match) to the "$return_val" variable.



Manage Rules

Rule:

Short description:

Verification code (optional):

```
<?php
function verify($match){
//optional
return $return_val
}
?>
```

Policies (optional):

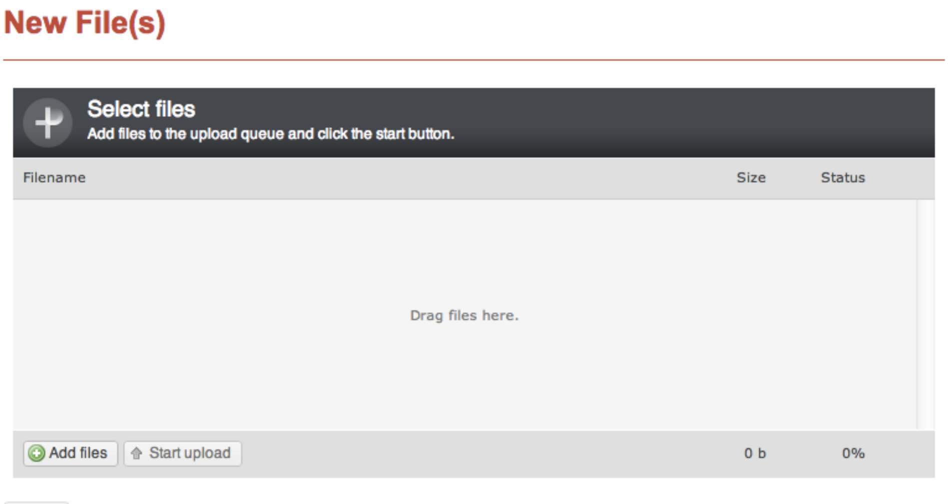
□ POL001

5.3. FILES

For very exceptional cases, it’s possible that a rule can’t cover all our requirements and we’d want to sign up a file. In these cases we can upload a file to help Drainware to identify when someone is trying to filter information.

The procedure is very simple. We can upload one or more files and they will be automatically available to associate to our policies. We only have to go to the policy configuration and select the filename.

Every time we upload a file, this will be available in the new policies wizard.



New File(s)

Select files

Add files to the upload queue and click the start button.

⚠ Important!:

Before uploading a file, we suggest to use a unique filename or even put the current date to distinguish it from another with the same name.

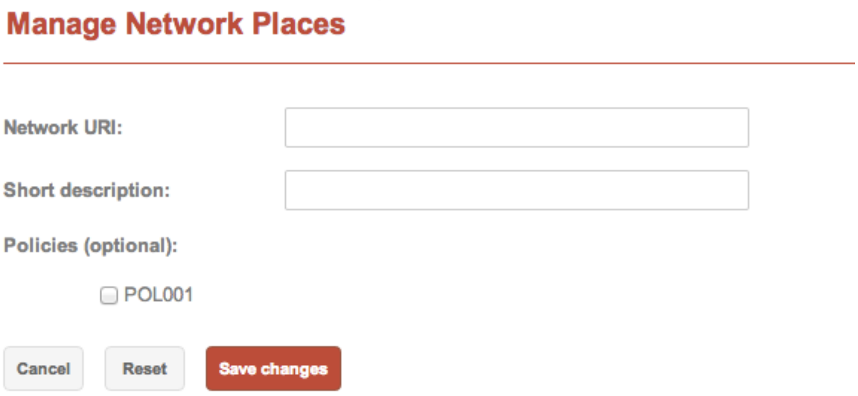
5.4. NETWORK SITES

In the network sites section, we can add Windows shared folders with the format \\server\resource.

This functionality is one of the most interesting ones. The endpoint software is ready to identify all the files copied in a computer from the shared folder added in Drainware. Once the file is copied, Drainware will check every file or every copy of them throughout the computer’s file system, allowing you to work with it, but denying its filtration.

For Network URI, we have to input the shared folder location., We must also introduce a short description, and then select the different policies to apply.

It will be available in the new policies wizard.



Manage Network Places

Network URI:

Short description:

Policies (optional):

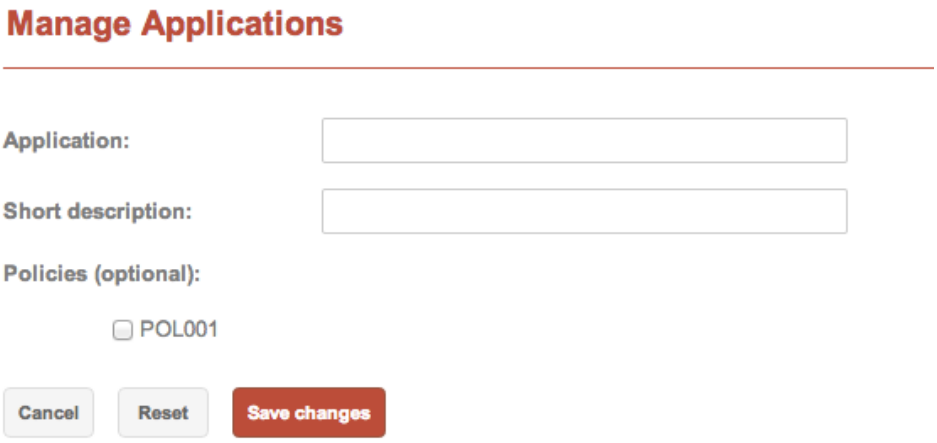
□ POL001

> ⚠ Important!:
>
> Only files that have been copied after add the shared folder will be monitored.

5.5. APPLICATIONS

To add more applications and include them in our policies, we can add them in the “Manage Applications” section.

To add a new application, we will need its name, for example iexplorer.exe, or skype.exe. Similarly to the other sections, we have to put a short description and select the policies to associate with it. It will be available in the new policies wizard.



Manage Applications

Application:

Short description:

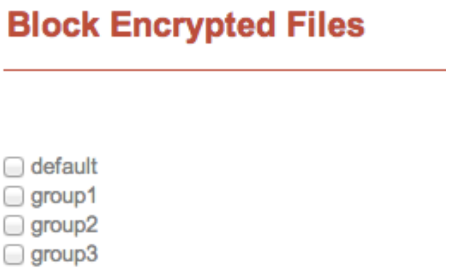
Policies (optional):

□ POL001

5.6. ADVANCED

In the Advanced section of Drainware, we can configure the behavior of the DLP. We have 3 sections to configure its behavior.

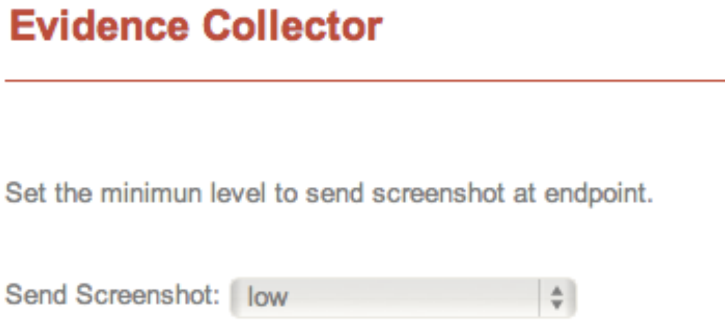
The first section will allow us to block the access to encrypted information within particular groups. The behavior will be the same as a file affected with blocked policy.



Block Encrypted Files

☐ default
☐ group1
☐ group2
☐ group3

The second section will allow us to collect evidence every time an event is carried out. This configuration is directly related to an action defined in the policy, where we can define a criticality level for each group. In this configuration we can select ‘None’ if we don’t want to collect evidence or the minimum level from which we would want to make for the collection. If we select the low level, the collection will be available for the low, medium, and high levels. If we select the medium level, it will be available only for the medium and high levels. And if we select high, it will be available only for that level.



Evidence Collector

Set the minimun level to send screenshot at endpoint.

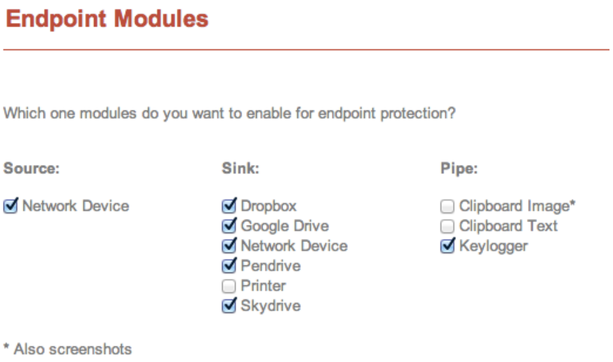
Send Screenshot: low

⚠ Important!:

The configuration of the evidence collector is only available for the Premium users. The Freemium users will receive the first 3 screenshots every month.

In the last section we can globally enable or disable modules that affect all policies. In Drainware we consider 3 types of elements:

- Source: information origin
- Sink: information destination
- Pipe: information channel



Endpoint Modules

Which one modules do you want to enable for endpoint protection?

Source:	Sink:	Pipe:
☑ Network Device	☑ Dropbox ☑ Google Drive ☑ Network Device ☑ Pendrive ☐ Printer ☑ Skydrive	☐ Clipboard Image* ☐ Clipboard Text ☑ Keylogger

* Also screenshots

In sources, we currently only have “Network device”. That allows us to recognize Windows shared folders. If we disable this origin, the “Network Sites” section will stop working and it won’t be visible in the menu anymore.

In Sinks we have several modules that monitor the application of the corresponding action (block, alert or log):

- Dropbox
- Skydrive
- Google Drive
- Network Device
- Pendrive
- Printer

Finally, in Pipes we can monitor:

- Clipboard Image
- Clipboard Text
- Keylogger

⚠ Important!:

The keylogger module doesn’t allow block the tipping, because until it isn’t written it can’t be analyzed.

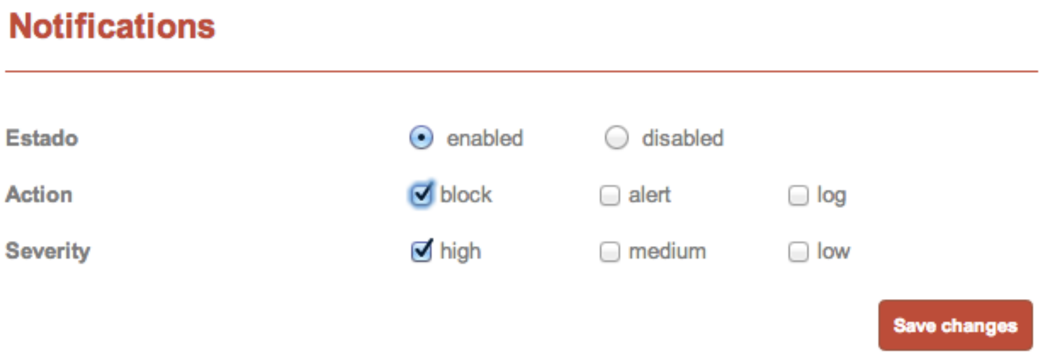
5.7. NOTIFICATIONS

Notifications can’t be configured in the DLP menu, they must be defined in the “General” section, but they are directly related with the DLP.

The notifications allow, as long as we have a browser opened and logged in, the receiving of notifications in real time when an event is carried out.

We don’t recommend enabling the notifications for all actions and events, because, if they are executed regularly, it can be annoying.

The notifications are HTML5 notifications and they are integrated with the desktop of the operating system, as long as the browser and the operating system support it.

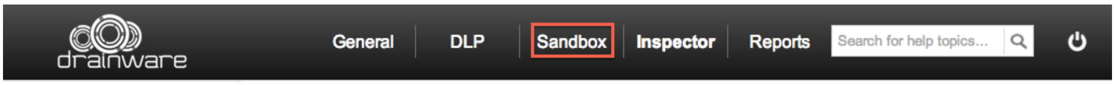


Notifications

Estado	● enabled	○ disabled	
Action	☑ block	□ alert	□ log
Severity	☑ high	□ medium	□ low

6. SANDBOX

The Sandbox feature allows us to protect applications against virus. It's not an antivirus replacement, but rather, a complement.

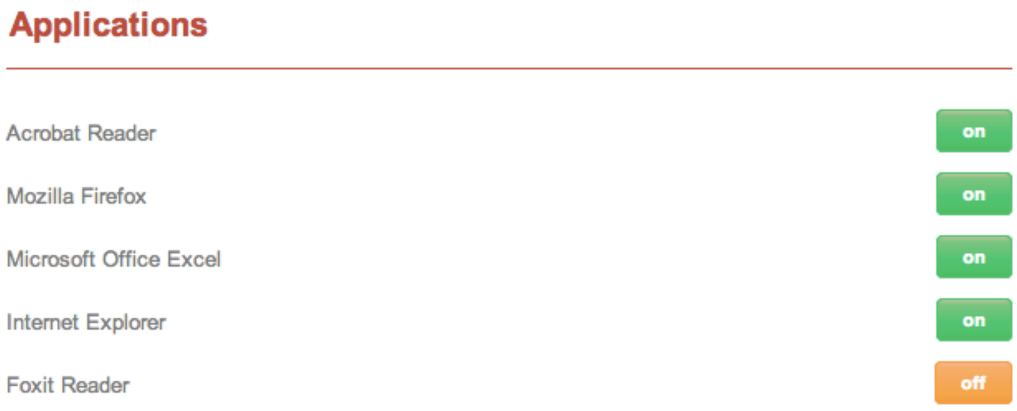


Previously, hackers took advantage of security problems in the server's software to gain access to the organization. But a security suite was developed to enable firewalls, IDS, IPS…

In the last few years, hackers have taken advantage of new vectors. Using tools like LinkedIn, they can discover who a financially responsible person is, and what contacts he has. From that moment they can make an attack based on spear-phishing that consists of sent e-mails assuming his identity with an attached PDF or an URL that steals data or opens a connection to the outside.

6.1. APPLICATIONS

In Drainware, we develop rules that allow us to block the affected applications before the system will be affected.

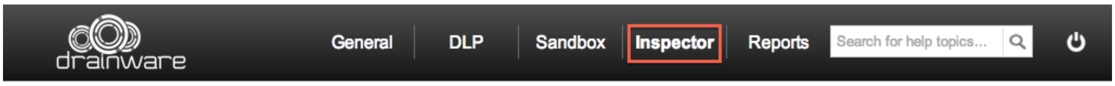


Applications

Acrobat Reader	on
Mozilla Firefox	on
Microsoft Office Excel	on
Internet Explorer	on
Foxit Reader	off

7. INSPECTOR

With the Inspector module, you can search in real-time over all the computers in the organization.

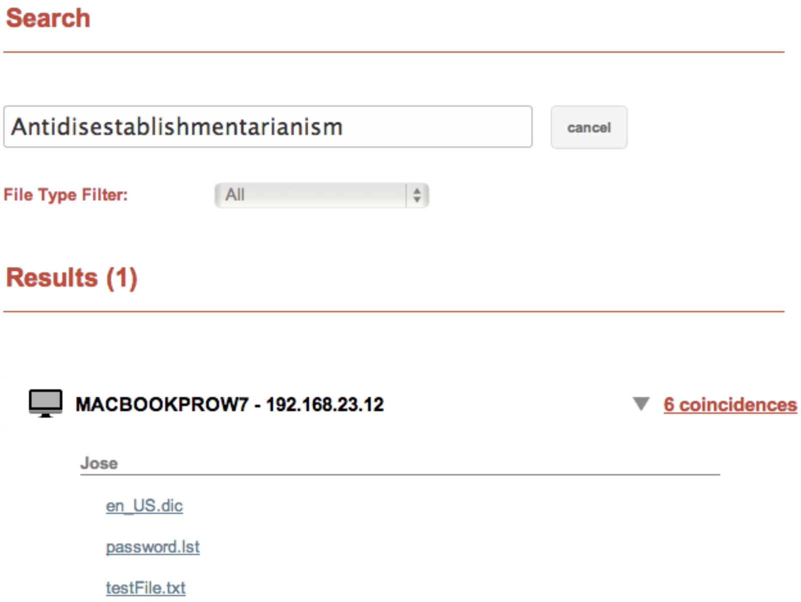


It's possible that in the organization we have a person or a group of people working with the kind of information to which they shouldn't have access. It could be done unconsciously or premeditated. Either way, we can find out with the Inspector tool.

Furthermore, once we have experienced a leak of information, it is often very difficult to check all the computers where the related document was. With Inspector, it is possible in seconds, to find very specific files, download them, and even browse through the file system of the computers affected.

7.1. REMOTE SEARCH

With the remote search we can start to obtain results.



Search

Antidisestablishmentarianism

File Type Filter: All

Results (1)

MACBOOKPROW7 - 192.168.23.12 ▼ 6 coincidences

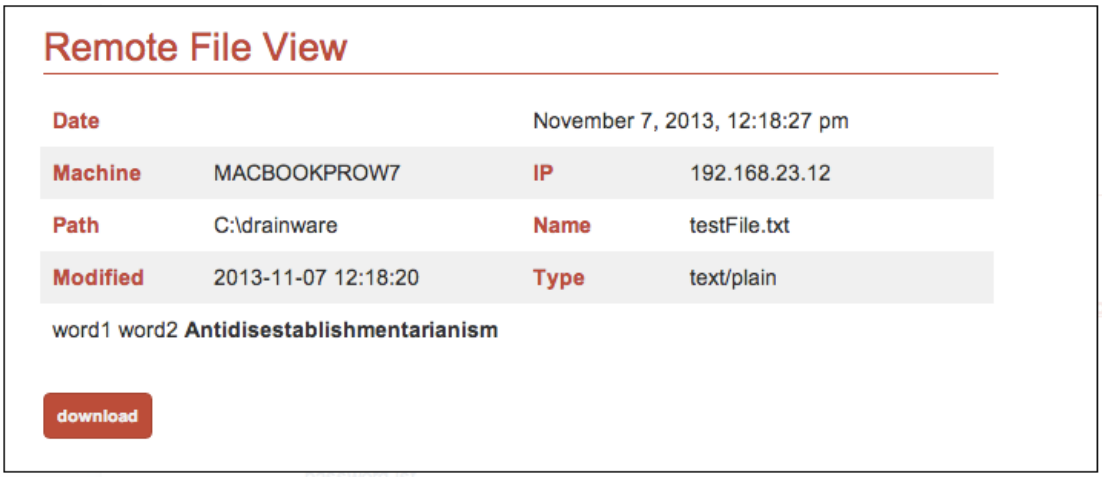
Jose

en_US.dic

password.lst

testFile.txt

The search can take several minutes. The results are shown grouped by the name of the computer where the file was found. Expanding the results by computer, it's possible to see the file details by clicking on it. We can see information about the modification date, file name, mime type, creation date, and short information about the file header. It's also possible to download it.



Remote File View

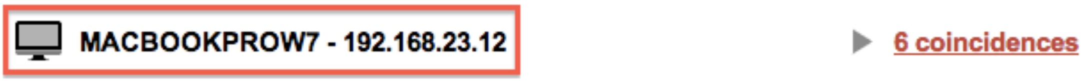
Date		November 7, 2013, 12:18:27 pm	
Machine	MACBOOKPROW7	IP	192.168.23.12
Path	C:\drainware	Name	testFile.txt
Modified	2013-11-07 12:18:20	Type	text/plain

word1 word2 **Antidisestablishmentarianism**

⚠ Important!:

You shouldn't search by very short terms or generic terms. The result can take too much time or it can be unmanageable.

It's possible to browse through one of the computers listed in the results. To do this, you must click on the computer name or IP address (red area).



The file explorer feature is further detailed in section 7.3 of this manual.

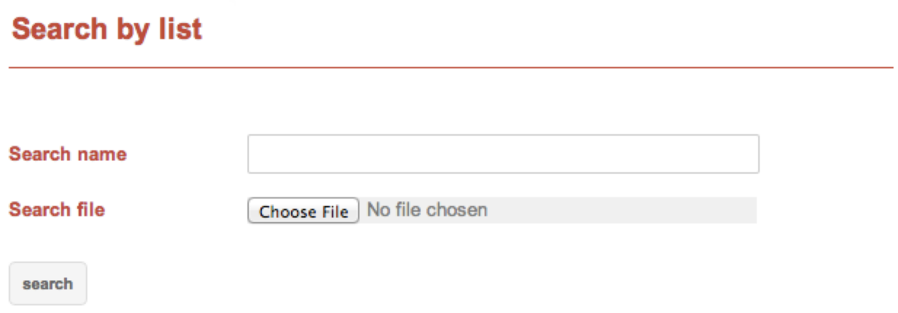
7.2. MULTIPLE REMOTE SEARCHES

If we want to search by a lot of terms, it's possible to use the Multiple Remote Searches function.

To use this feature, you have to create a file with all the search terms in one line, separated by commas. We can create different lines, each one with its own keywords.

```
keyWordGroupA-1, keyWordGroupA-2, keyWordGroupA-3
keyWordGroupB-1, keyWordGroupB-2
keyWordGroupC-1, keyWordGroupC-2, keyWordGroupC-3
```

The file extension must be TXT. In addition to uploading the file, we must input a name for this report.



Search by list

Search name

Search file

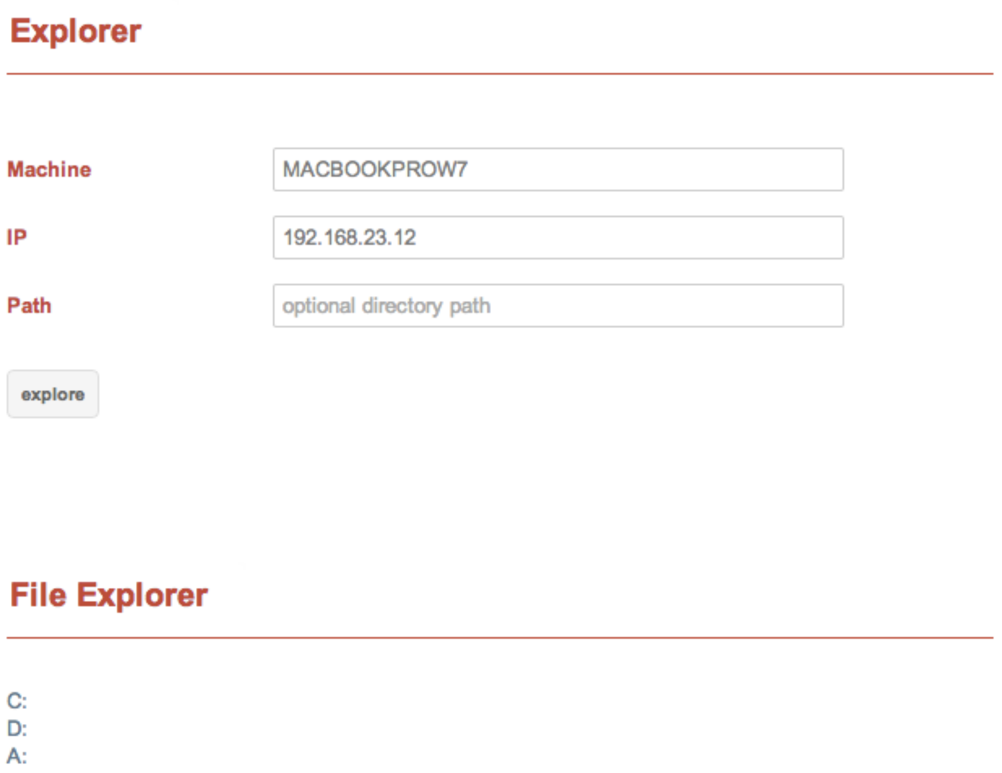
⚠ Important!:

You shouldn't search by very short terms or generic terms. The results can take too much time to obtain, or the results can be unmanageable.

7.3. REMOTE FILES EXPLORER

The Remote Files Explorer allows us to inspect any computer in the organization with Drainware installed.

We will have to provide some details about the computer: computer name, IP address, and optionally, the path. From this point we can browse through any device in the computer and even download files.



Explorer

Machine MACBOOKPROW7

IP 192.168.23.12

Path optional directory path

File Explorer

C:
D:
A:

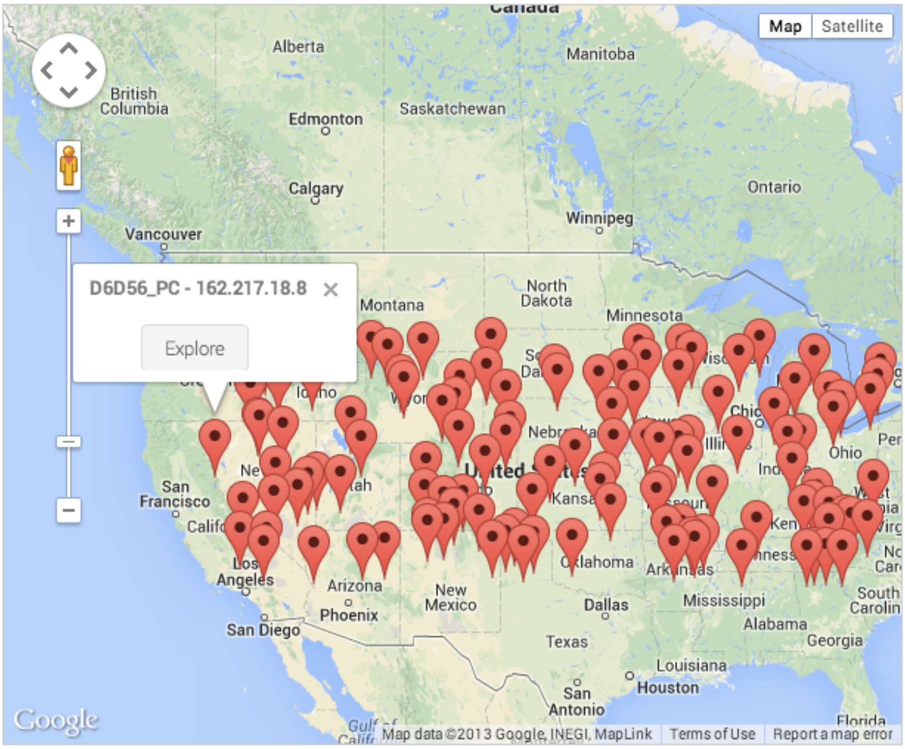
⚠ Important!:

Drainware is not developed to be an FTP server. Downloading a file with several MB in size can take several minutes until the download starts.

7.4. REMOTE DEVICES

With this feature, we can see the geographic position of all the devices that have Drainware installed.

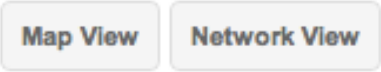
In most cases, the geolocation is performed through the IP address, but when the Wi-Fi is activated, it’s possible that the geolocation is performed through Wi-Fi triangulation.

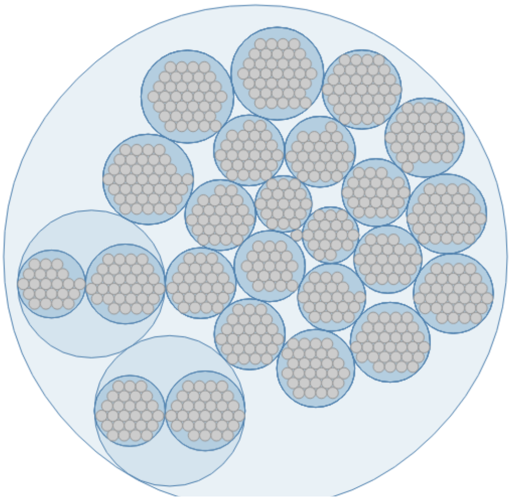


⚠ Important!:

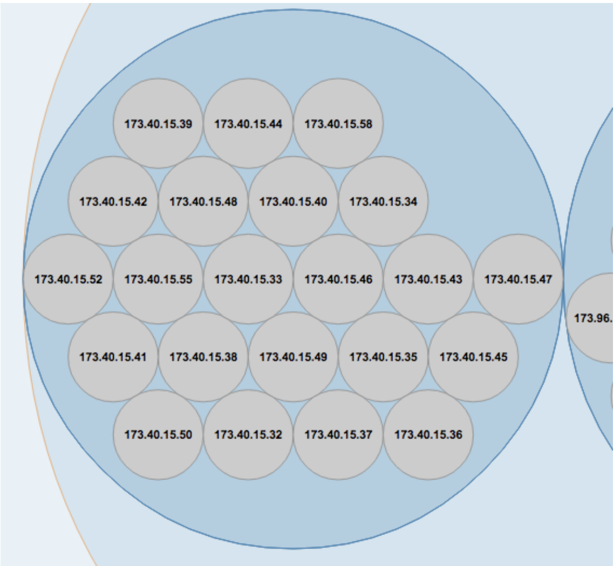
Make sure that you don't refresh the webpage until all the endpoints have responded, especially in networks with thousands of endpoints, as the webpage loading could take several minutes.

In addition to the geolocation of the devices, it's possible to get a network map encapsulating all the computers that belong to the same ranges. To that effect, we will click on the Network View tab.





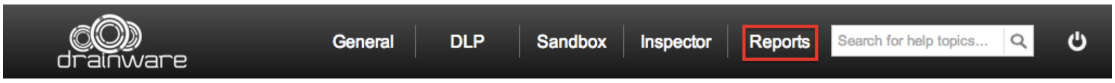
The results are shown in circles, where every circle represents a range or a group of ranges.



It’s possible to click on the segments that we want to inspect and see all the computers connected at that moment.

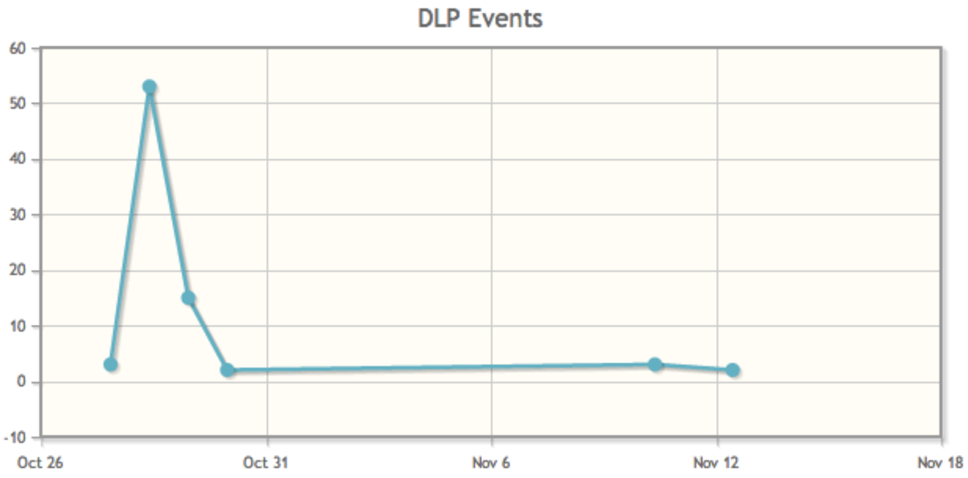
8. REPORTER

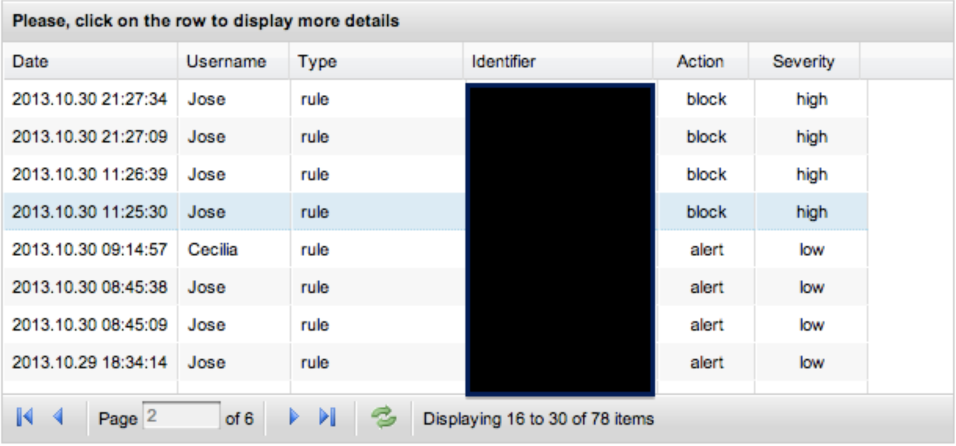
With the Reporter module, we can have access to the data recorded by Drainware. We can get details of every module or statistic from the global behavior of the DLP, Inspector, or Sandbox.



8.1. DLP EVENTS

Once we open the DLP events information, we can see a graph with all the events related to the data leak. Under the graph we can see a table with a list of related events, ordered from the most recent to the oldest. The table has some controls at the bottom where we can refresh it or browse through.





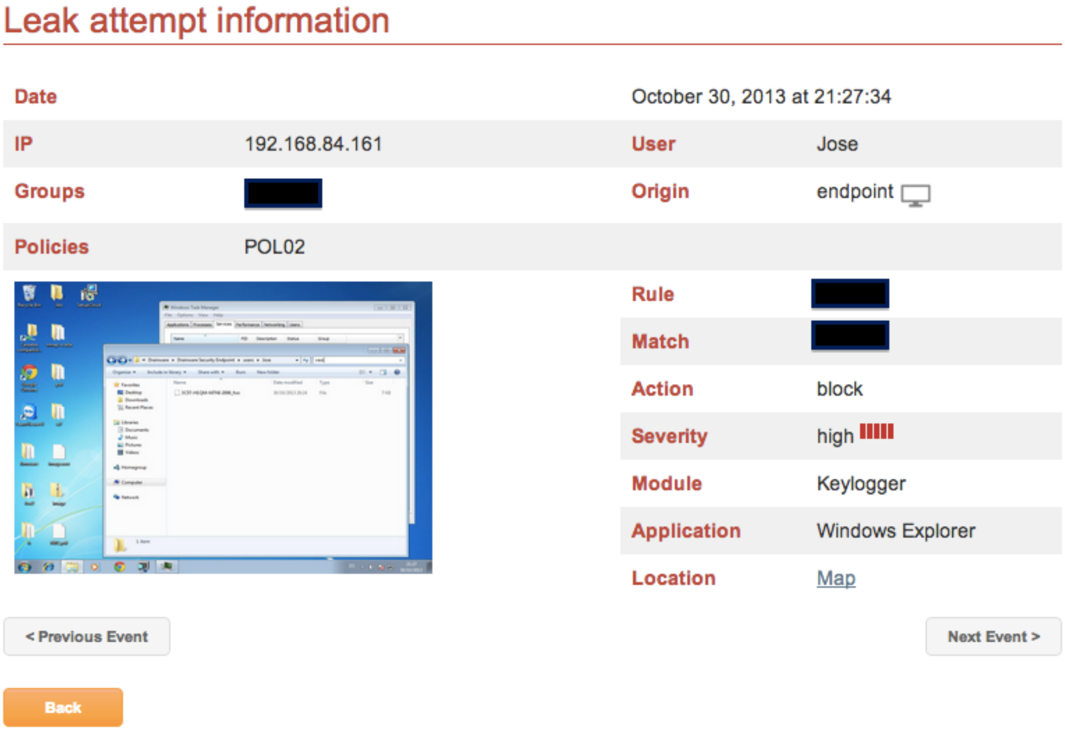
Please, click on the row to display more details

Date	Username	Type	Identifier	Action	Severity
2013.10.30 21:27:34	Jose	rule	[redacted]	block	high
2013.10.30 21:27:09	Jose	rule	[redacted]	block	high
2013.10.30 11:26:39	Jose	rule	[redacted]	block	high
2013.10.30 11:25:30	Jose	rule	[redacted]	block	high
2013.10.30 09:14:57	Cecilia	rule	[redacted]	alert	low
2013.10.30 08:45:38	Jose	rule	[redacted]	alert	low
2013.10.30 08:45:09	Jose	rule	[redacted]	alert	low
2013.10.29 18:34:14	Jose	rule	[redacted]	alert	low

Page 2 of 6 Displaying 16 to 30 of 78 items

The list only shows a preview of the event. If we want to see detailed information, we must click on it.

The details of each event are shown in a table that provides all the information related to the event. Depending on the configuration, it's also possible to see a screenshot done in the same moment that the event was carried out.

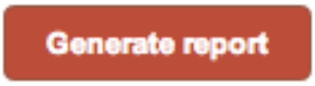


Leak attempt information

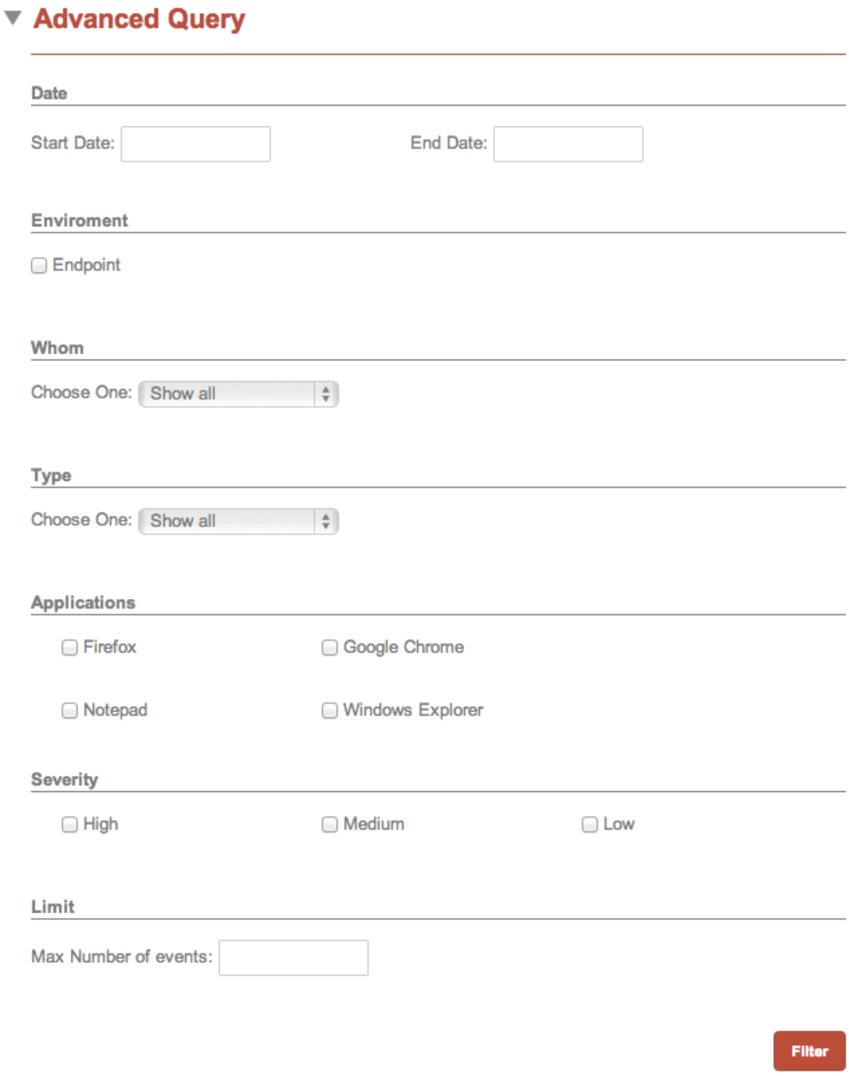
Date		October 30, 2013 at 21:27:34	
IP	192.168.84.161	User	Jose
Groups	[redacted]	Origin	endpoint 🖥
Policies	POL02		
		Rule	[redacted]
		Match	[redacted]
		Action	block
		Severity	high ▮▮▮▮▮
		Module	Keylogger
		Application	Windows Explorer
		Location	Map

Annotations: Freemium users can only see the first 3 screenshots every month.

Under the table, there is a button which generates a report with the latest security events.



If we want to find events by range of dates, event type, policy, severity, rule, etc., we can use the "Advanced Query" system. As we can have a result with too many events, it's possible to fill in the maximum number of events we want to show in the result.



▼ Advanced Query

Date

Start Date:

End Date:

Enviroment

□ Endpoint

Whom

Choose One: Show all

Type

Choose One: Show all

Applications

□ Firefox

□ Google Chrome

□ Notepad

□ Windows Explorer

Severity

□ High

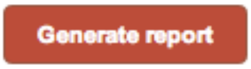
□ Medium

□ Low

Limit

Max Number of events:

Every time a query is generated, it's possible to export the results in CSV format. In order to do this, you have to click on the Generate Report button at the end of the page:

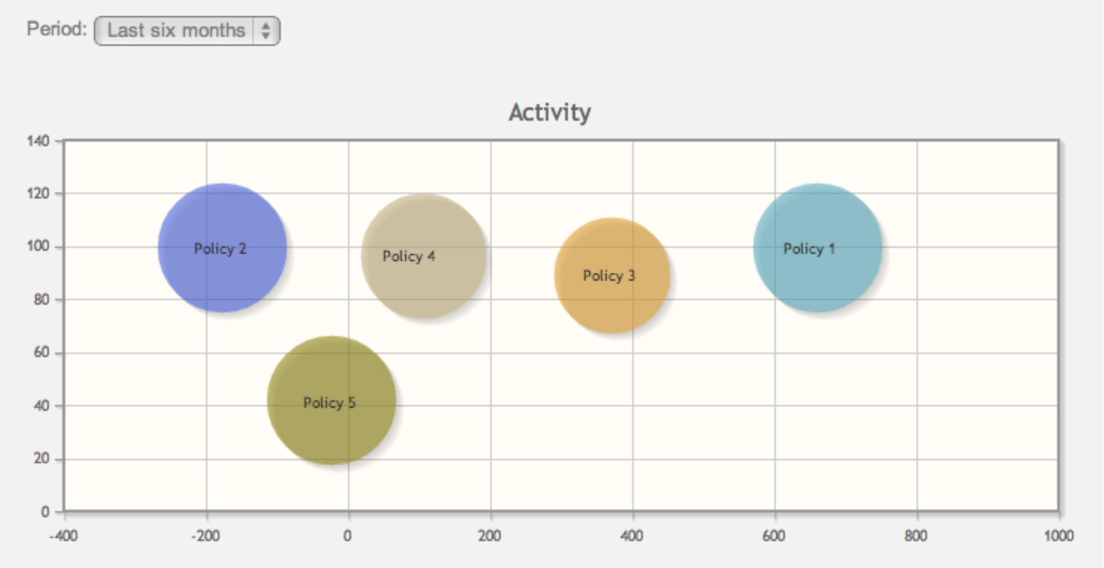


8.2. DLP STATS

The events and detail of events information is interesting, but in many cases, it's necessary to have view at a higher level of what is happening with confidential information or to know how the policies that we have configured are working. To do so, we will create the data analysis and statistics.

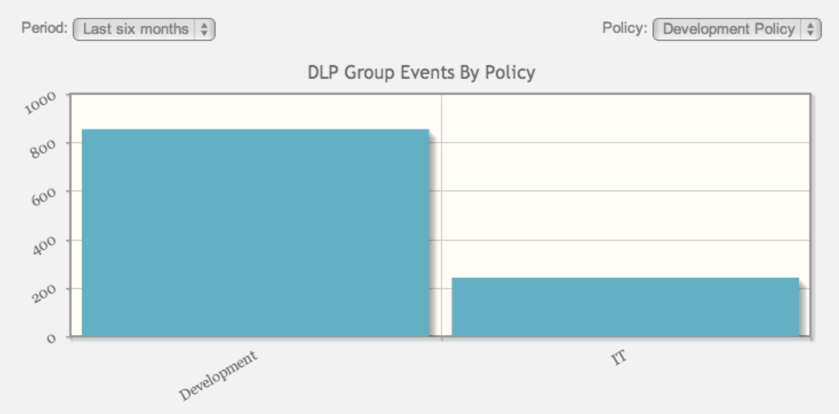
Activity

In the same graph, it represents the average between severity, action, and number of events. The policies with more events are located to the right, with the vertical axis representing the average of the actions carried out, where the block is the highest part. The average of the severity is shown in the size of the circle. In the top left combo box you can select the period of time.


Period: Last six months

Groups by policy

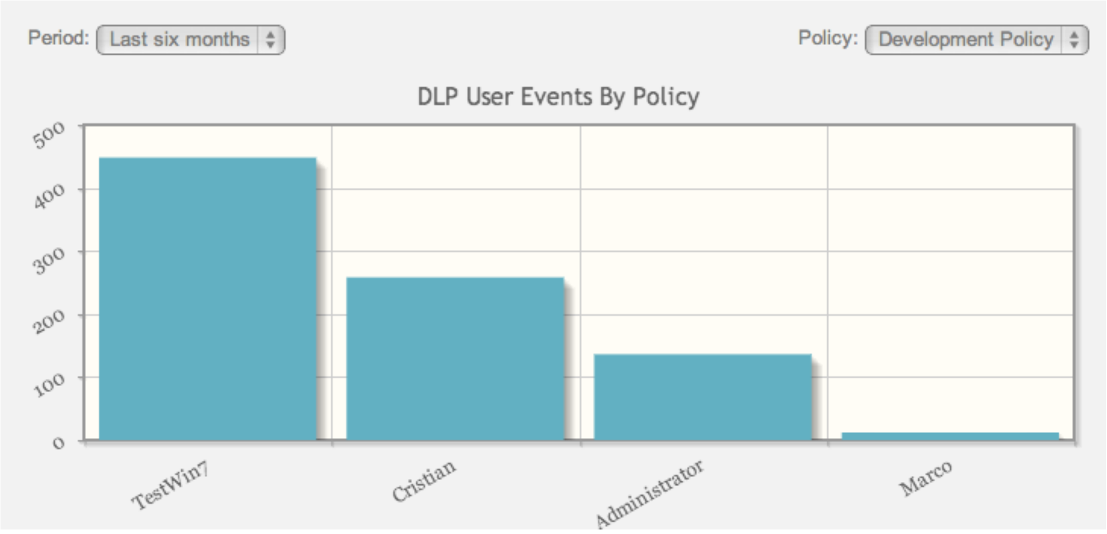
In this graph we can see the groups that carried out more events of one policy. In the top left combo box you can select the period of time. In the top right combo box you can select the policy.


Period: Last six months

Policy: Development Policy

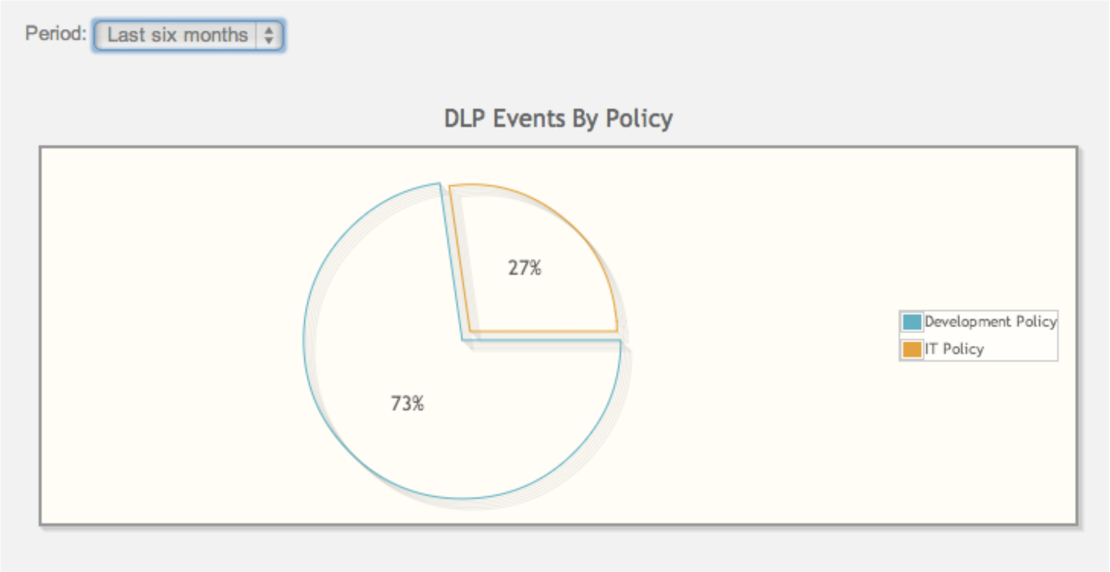
Users by policy

In this graph, we can see the users that carried out more events of one policy. In the top left combo box you can select the period of time. In the top right combo box you can select the policy.



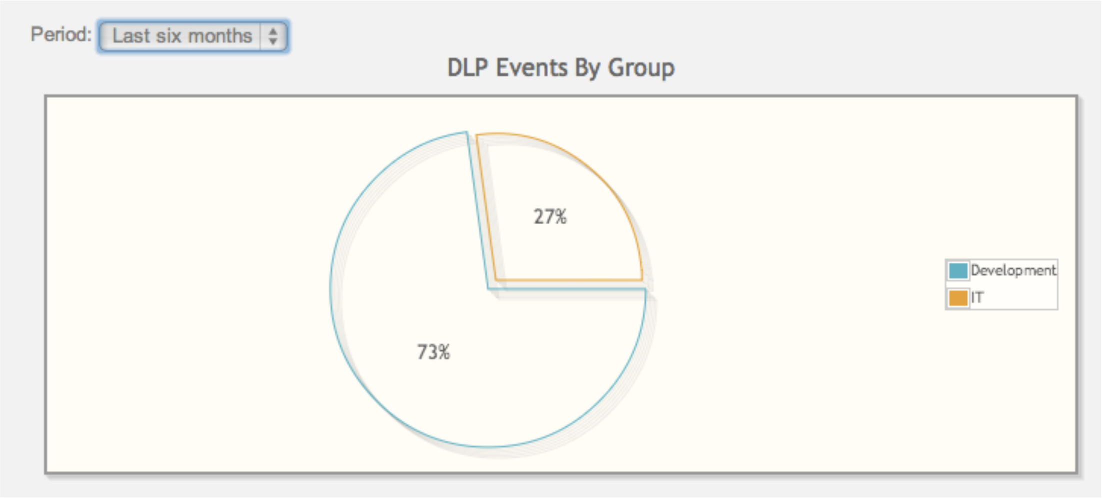
Policy

With the policy graph, we can analyze the policies with more activity. In the top left combo box you can select the period of time.



Groups

With the policy graph we can analyze the groups with more activity. In the top left combo box you can select the period of time.



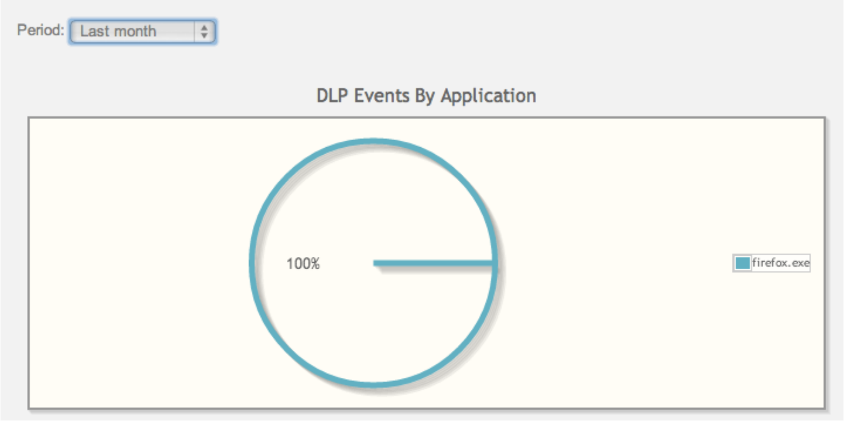
8.3. SANDBOX EVENTS

We can see a graph with related events with attempts to abuse applications. Under the graph we can see a table with the list of events, ordered from the most recent to the oldest. The table has some controls in the bottom where we can refresh it or browse through.

8.4. SANDBOX STATS

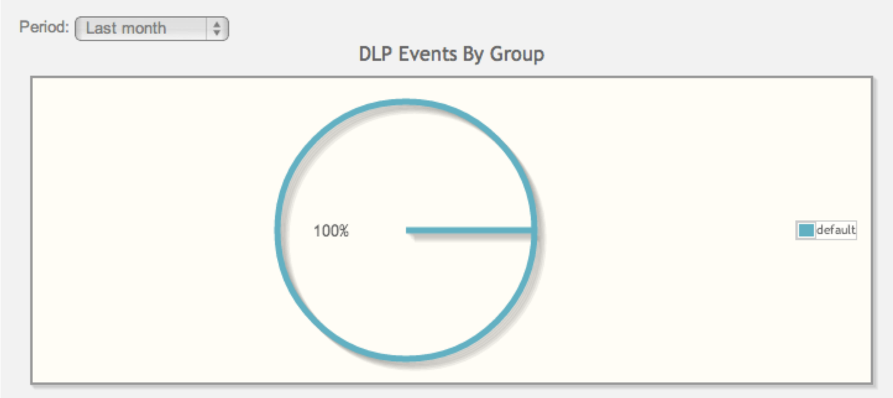
Applications

With the applications graph, we can analyze the policies with more activity. In the top left combo box you can select the period of time.



Groups

With the policy graph, we can analyze the groups with more activity. In the top left combo box you can select the period of time.

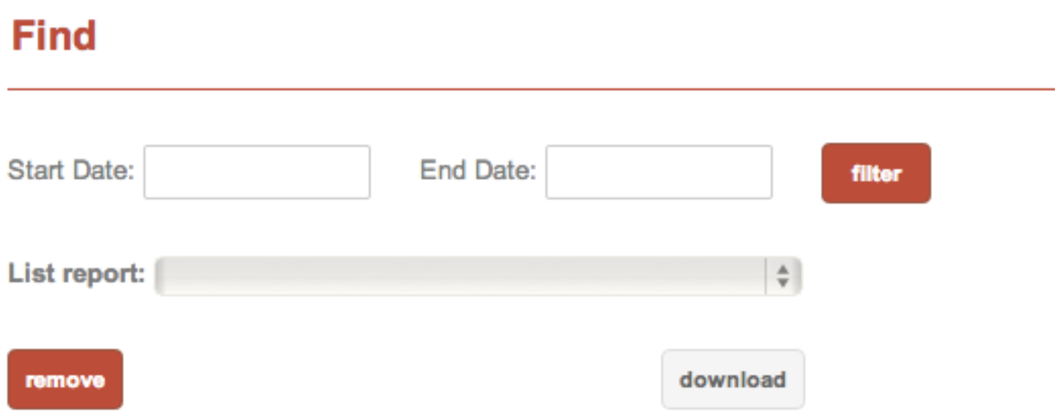


Period: Last month

DLP Events By Group

8.5. INSPECTOR SEARCH REPORTS

When we make multiple remote searches from the Inspector section, the results are generated in this section. We can find the report by range of dates to download in Microsoft Excel format.



Find

Start Date:

End Date:

List report:

9. TROUBLESHOOTING

9.1. CORPORATE PROXY

Drainware supports connection though a proxy, either configured in the system, or auto-configured. However, if the proxy uses authentication, it’s necessary to enable “*.drainware.com” in the accessible domains without authentication.

If you are using SQUID, the configuration would be the next one:

```
acl drainware dstdomain .drainware.com
acl CONNECT method CONNECT
acl dwCONNECT dstdomain .drainware.com
http_access allow CONNECT dwCONNECT localnet
http_access allow drainware localnet
```