I DLP GUIDE



Content

Introduction to DLP – protecting data with Safetica
How does Safetica protect data?
Exercise: Use-cases for most common scenarios
Protecting data from a specific application4
Preventing data loss via external devices 4
DLP Guide: Analyzing and tagging of existing files
Create data categories
Creating a standard tagging task
Creating a File content rule tagging task7
Analyze tagging task
DLP Guide: Configuring DLP policies
Types of DLP policies
Create security policy
Configure the DLP rules
DLP protocol
DLP Tips: Configuring the environment 11
User groups
Web and application categories12
DLP Zones
Sensitive content
Regular expression
Advanced DLP: Secure channels
Restrict external devices
Enable device control
Device Control Settings 15
Restrict disk access
Enable Disk guard16
Logging settings
Paths17

Introduction to DLP - protecting data with Safetica

This DLP guide will give you an overview of how you can protect your data with Safetica.

The guide is split into three parts: Exercises, DLP guide and Advanced DLP.

Exercises will let you see how Safetica protects the files without having to understand individual settings. Just follow the steps in each exercise to configure Safetica for the given scenario. **DLP guide** explains the workflow of setting up DLP and goes through the main options for each option. Finally, **Advanced DLP** expands on the previous section with additional settings, giving you all the tools you need to configure Safetica for virtually any environment and workflow. But first...

How does Safetica protect data?

In order to be able to protect confidential data and set the rules how to work with them, Safetica tags the files that need to be protected. You have multiple options how to choose which files will be tagged as sensitive, based on:

- Application Rules
- Web Rules
- Path Rules
- Tag distribution Rules
- File content Rules
- Tag removal Rules
- Process Rules

Once you have the files tagged, you can apply the following restrictions to them:

Area access:

- Local drives and folders (where can you save the file?)
- External devices (what devices can you copy the file to?)
- Printers (can you print it?)
- Network (can you upload it?)
- Email (can you mail it?)
- Encrypted drives (can you copy the file to an encrypted device?)
- Cloud drives (can you upload it to a cloud drive?)
- Remote transfer (can you transfer it via RDP?)

Operations:

- Screenshots
- Clipboard
- Burning
- Virtual printing

The combination of a tagging rule and a restriction put together a DLP rule that effectively defines the way you can and cannot work with specific files, based on their location, origin and other attributes.

Exercise: Use-cases for most common scenarios

Protecting data from a specific application

Scenario: A company needs to protect their know-how and business data created in MS Office applications and they need to have control over these documents. Therefore, copying to external devices is denied, with the exception of specific flash drives approved by the company.

Follow these steps to configure this scenario:

- 1) Open Safetica DLP DLP rules Security policies.
- 2) Choose New Security Policy
- 3) Choose *Policy type* **Application policy**.
- 4) Fill in the name of the policy (e.g. Sensitive files), add description, and then click **Next**.
- 5) Choose the following settings:
 - a. Set External devices to Zone
 - b. Create new zone or choose existing one, which will contain the company's flash drives
 - c. Set this zone to Allow.
 - d. Set all other options to Denied.
 - e. Click Finish.
- 6) In Security policies, click **Finish**.
- 7) In **DLP** -> **DLP** rules, click New rule.
- 8) Choose application category from the list on the left Office suite; click Next.
- 9) Click Select Security policy ("Sensitive files" in our case).
- 10) <u>Choose the mode –</u> *Testing, Informative* or *Restrictive*.
- 11) Click Save.

More details about each of these steps and settings is available in the following chapters.

Preventing data loss via external devices

A Company has experienced a data leak. They now want to deny all external devices (USB flash drives ...) except several devices that are encrypted. CD/DVD burning shall be denied, but employees must be able to read CDs. Employees can charge their phones, but copying files to a phone is not allowed either.

- 1) Open Safetica DLP Device control.
- 2) At the top of the page, move the slider to *Enabled*.
- 3) In the section *Advanced settings,* where you will see the port settings. Set them as follows:
 - a. USB Deny (we will set specific flash drives later)
 - b. Windows Portable Devices Read only (phones, cameras, ...) Charging is possible, but no data can be copied
 - c. CD/DVD Read only (no burning)
 - d. Other ports Deny
- 4) In the section *Devices settings* click the button Add devices or edit zones.
 - a. Choose tab Unassigned items.
 - b. Select devices which should be allowed in the Company and drag&drop them to the zone *Allowed* (or create a new one).
 - c. Finish editing zones with the **Finish** button.
- 5) For the zone *Allowed*, set the slider to *Allow*.
- *6)* Set other zones to *Deny*.

Only devices added to the zone *Allowed* will be able to connect to computers. Any new device (in the zone *Not in zone/Not set*) will behave based on the port settings.

Detailed settings of Device control are described in chapter Device control settings.

DLP Guide: Analyzing and tagging of existing files

Prior to securing data, it is crucial to scan the computers and find the existing data you want to protect.

Create data categories

In the Data categories view you can create any number of data categories. Data categories are practically a label used for the tagged files. DLP rules and restrictions are then assigned to the categories. This helps to keep your DLP rules organized.

You can access the management of categories from two basic locations, where you use the filtering rules:

- DLP -> File tagging -> Manage data categories
- DLP -> DLP rules -> data category

P rules > Data cat	tegories				?	×
A BASIC INFORMA	TION					
Data category man	agement feature	offers the abilit	to create	e arbitrary number of data categories. These categories are used to divide files into separate groups according to who, where and how ca	n use thi	s data. Fo
each data category	several DLP rule	s can be created	hat enal	ble you to secure the files tagged with this category. Categories can be assigned to files using the File tagging feature.		
New data category						
Category A		D	TA CAT	regory information		
Dat kat doc	Edit B	Remove No	16	Dat kat doc		
		De	ription	Popis		

The left section of the view shows the list of data categories. After selecting the categories on the list, the name and description of the data category will be displayed on the right.

If you wish to create a new data category, click **New data category**. Enter a name and description and by clicking **OK** the category will be added to the list shown on the left.

You can edit the name and description of an existing data category by clicking the **Edit** button in the list with each data category.

Creating a standard tagging task

Tagging the files makes it possible for Safetica to protect them.

🚯 📶 File tagging DL	Prules DLP protocol Zones Disk guard	d Device control En	crypted disks Bitlocke	devices Bitlocker disk	s Sensitive content						
+ 🛛 🖇						?	ŵ	×			
,⊯ MS-Win10E-x64	A BASIC INFORMATION File tagging feature allows you to set the	rules according to which th	e files will be tagged. You ca	n afterwards set <u>DLP rules</u> to	secure the tagged files.						
	Manage data categories		ULES								
	Data category		Application rules allow you to set which applications or application categories should add tag								
	Documents to the output files. You can, for example, set that all the applications in CAD software category will mark the output files with appropriate data category, so the corresponding policies will										
	Sensitive data	apply to these files		category, so the corresponding	ig policies will						
		Add									
		Rule name	Users	Application	File description	Rule mode					
				(No i	tems)						
		V WEB RULES									
		V PATH RULES									
		V TAG DISTRIBUTI	ON RULES								
		V FILE CONTENT F	RULES								

- 1) Open *Safetica* **DLP File tagging** Settings mode
- 2) In Basic information select existing or create new *Data category (create data category is possible in the Manage data categories)*
- 3) In the section Application Rules (etc. another rules) click to add button
- 4) In the section *Creating filtering rule Basic information*
 - a. Fill rule name and description
 - b. Select object for the rule
 - c. Choose rule mode Tagging or Testing (Testing files will not get the tag, but the logs for analyze are created)

- d. Click to Next button
- 5) In the section Creating filtering rule Rule settings
 - a. Click to Add application and select application Categories
 - b. Click to Add extension and Select File type categories
- 6) Click Finish

One Data category can have more combination rules.

Creating a File content rule tagging task

File content tagging task specifies a rule which tags files based on its content. This tagging task scans files and looks for predefined dictionaries or a custom keyword.

- 1) Follow 4 steps as for Creating a standard tagging task
- 2) In the section *Creating filtering rule Rule settings*
 - a. Click Add paths and select folder or network path
 - b. Click Add extension and Select File type categories
 - c. Choose a dictionary, which you want to use for tagging, or a specific *Keyword* which you want to search within files. You can have specific *Keywords* or <u>Regular</u> <u>expression</u>.
- 3) Click Finish



Analyze tagging task

Once the task is launched, you can see the results in the Visualization mode. You can select specific tagging task and see the results only from this task.

*	Ш	File tagging	DLP r	ules DLP protoc	ol Zones	Disk guard	Device control	Bitlocker	devices	Bitlocker dis						
+		7 3		Layout: Recent	Period:	6/25/2017 - 7/2	5/2017 🔻									
	win10e	₹ () ex64		Layout: Recent 1 CHARTS All Dokument Super date	y Period:	6/25/2017 - 7/2 Extensions	5/2017 🔻	Bitlocker	devices .dsx .ppt		ks		.docx .bmp —.bt			
				∧ RECORDS	is tout the cel	umns you want	te ereue hu									
				-		-			- ·		-	- 00		-		.
				Y Operation Merge		Data categ Super datov	Y Date an Y E 7/20/2017 0				Y File New Micros	Y PC	♥ User name		Rules Oznacovani	Details
				Merge		Super datov Super datov					New Micros				Oznacovani	
				Merce	Windows Fy	Super datoy	7/20/2017 0	On	dinanz	docx	New Micros	win10ev64	∆dministrat	C\Ulcerc\∆d	Oznacovani	Details

See more details in Help -> Console -> DLP -> File tagging.

DLP Guide: Configuring DLP policies

Safetica uses DLP policies to protect tagged files (see previous chapter on how to tag your sensitive files), and also to secure any new files created by some application, downloaded from an internal system, etc.

There are two types of DLP Policies – Application and Data policy:

 Application policy protects files created in the application – e.g. all files created in Excel or Autocad.



• Data policy protects files on your hard drive – e.g. existing DWX and XLS files.



Types of DLP policies

There are three levels of DLP policies mode which can be configured to match the expected behavior:

Restrictive - the security policy will be applied exactly according to its settings. The user will be able to access only allowed areas and any deny operations will be blocked.

Informative - the security policy will not be applied, but a warning dialogue will be shown. This mode is used for testing and user education.

Testing – all blocked or restricted operations are logged, but there is no notification for the user and the operations are not blocked. This is used for data flow analysis and for initial testing of restrictive DLP rules.

elect the security policy that will be used to protect data and apply exceptions if needed. SECURITY SETTINES	elected category: [)at kat doc				
Area access Local disks Local			t data and apply exception	s if needed.		
Security policy Zakaz odesilani Change Policy mode: Test Restri Area access Local disks: Inherit Inherit External devices: Inherit Inherit Printers: Inherit Inherit Network: Inherit Inherit Email: Inherit Inherit Cloud drives: Inherit Inherit Operations Inherit Inherit						
Area access Local disks: Inherit External devices: Inherit Printers: Inherit Network: Inherit Email: Inherit Email: Inherit Cloud drives: Inherit Remote transfer: Inherit Coperations Screenshots: Inherit Cipboard: Inherit	SECURITY SETT	INGS			_	
Local disk: Local disk: External devices: Inherit Printers: Inherit Network: Inherit Ernalit: Inherit Cloud drives: Inherit Remote transfe: Inherit Screenshots: Inherit			Security policy	Zakaz odesilani Change	Policy mode:	Restrict
External devices: Printers: Inherit Network: Inherit Email: Cloud drives: Inherit Cloud drives: Inherit Prerations: Screenshots: Inherit	Area access					
Printers: Network: Inherit Email: Cloud drive:: Inherit Cloud drive:: Inherit Perations: Screenshots: Inherit Cipboard:	Local disks:	Inherit				
Network Email: Deny Encrypted disk: Inherit Cloud drives: Inherit Remote transfe: Inherit Coperations	External devices:	Inherit				
Email: Deny Encrypted disk: Inherit Cloud drives: Inherit Remote transfer: Inherit Operations Screenshots: Inherit Clipboari: Inherit	Printers:	Inherit				
Encrypted disks: I Inherit Cloud drives: Inherit Remote transfer: Inherit Operations Screenshots: Inherit Clipboard: Inherit	Network:	Inherit				
Cloud drives: Inherit Remote transfer: Inherit Operations Screenshots: Inherit Clipboard: Inherit	Email:	Deny				
Remote transfer: Inherit Operations Screenshots: Inherit Clipboard: Inherit	Encrypted disks:	Inherit				
Operations Screenshots: Interit Clipboard: Interit	Cloud drives:	Inherit				
Screenshots: Inherit Clipboard: Inherit	Remote transfer:	Inherit				
Clipboard: Inherit	Operations					
	Screenshots:	Inherit				
Burning: Inherit	Clipboard:	Inherit				
	Burning:	Inherit				

Create security policy

Security policies are rules through which data is protected. You can apply a policy either to data (tagged files), or to an application.

These Security policies are assigned to either Data category (Data policy) or Application category (Application policy).

🔅 🕼 File tagging DL	Prules DLP protocol Zon	es Disk	guard	Device control Encry	pted disks Bitla	ocker devices Bitlocker	disks						
+ 7 3			-							?	۲	Ŵ	×
		N											
MS-Win10E-x64	DLP rules feature offers	the ability f	o assigr	n the <u>Security policies</u> to data	or application categ	ories. This assignment secure	es the files tagge	d with specific <u>data c</u>	<u>ategory</u> or specifies t	he restri	ctions of a	applicatio	n usage.
	New rule												
	Rules 🔺				N								
	Application rules			Rule name: Office s	uite								
	(No items) Data rules			Description: Descript	ion								
	Office suite	Edit	Remove	Manage data categor	ies								
					is								
				Security policy: libre	•								
				Policy mode: Info									
				Manage security poli Encrypted data: Inhe									
				Area access		Operat	tions						
				Local disks:	Inherit	Screen		Inherit					
				External devices:	Inherit	Clipbo	ard:	Inherit					
				Printers:	Inherit	Burnin	g:	Inherit					
				Network:	Inherit	Virtual	printing:	Inherit					
				Email:	Inherit								
				Encrypted disks:	Inherit								
				Remote transfer:	Inherit								
				Cloud drives:	Inherit								

To create a Security policy:

- 1) Open Safetica DLP DLP rules Security policies New security policy
- 2) Select Data Policy or Application policy:
 - a. **Data Policy** using data policy, you can determine what can be done with the data (files). Where the data can be stored, where it can be moved and what applications will have access to the data.
 - b. Application Policy using the application policy, you can specify to which location applications will have access and how they can work with the data.
 1. Policy name and description 2. Security settings

		Er betanit) settings
Policy type:	Application policy	
Name:	SAP application	
Description:	Settings of SAP	

- 4) Click Next.
- 5) Configure the Security settings for the policy.

3) Write Name and Description of the policy

٠	<u>Ih</u> I	ile tagging	DLP rules	DLP protocol		Disk guard	Device control	Encrypted disks	Bitlocker devices	Bitlocker disks
+	7	° 0	DLP I	rules > Securit	y polici	es > Create/	edit security po	olicy		
ST MS		164								
, 1 110				1. Policy name	and de	scription	2. Security se	ttings		
			-	1. Policy name and	descripti	on: Policy name	Policy description			
				2. Select the securit	y policy t	that will be used	to protect data and	apply exceptions if nee	aded.	
				∧ SECURITY SE						
				Encrypted data		Inherit	(ustom zone settings		
				Area access				Name		Mode
				Local disks:		Allow		Privileged		Notify
				External devic	es:	Zone		Read only		Deny
				Printers:		Allow		Denied		Deny
				Network:		Inheri	.	Allowed		Allow
								Not in zone / Not se	et	Deny
				Email:		Inheri	t			
				Encrypted dis	ks: 🔲 🛏	Inheri	t			
				Cloud drives:		Deny				
				Remote trans	fer: -	Deny				
				Operations	_		- 1			
				Screenshots:		Denv				
						· · · ·				
				Clipboard:		Deny				
				Burning:		- Deny				
				Virtual printin	q: 🛏	Allow				

Please, see the Help -> Console -> DLP -> DLP rules -> Security policies -> Security Settings – Data Policy for detailed information about all the options you can set here in this view.

Configure the DLP rules

The Security policies that you have created can be assigned to Data or Application categories.

Click New rule and follow these steps:

- 1) Open Safetica DLP DLP rules
- 2) Choose **Data** or **Application category** from the list that you want to restrict. If no category fits, create a new one (see <u>Create data category</u> section above). Click Next.
- 3) Select the Security policy that you want to apply for the chosen category. If no policy fits, create a new one (See <u>Create security policy</u> section above).
- 4) Select mode how the DLP policy should be applied (Restrictive Informative Testing).
- 5) Click Finish to add DLP rule to the list and click to save and apply DLP rule to selected groups, users or PCs.

DLP protocol

In the DLP protocol you can see record of all file operation with tagged file by Safetica.

Open Safetica – DLP – DLP Protocol – View mode. In the top half of the view is for charts, in the bottom half you can see detailed record.



DLP Tips: Configuring the environment

User groups

To create an effective DLP policy, it is needed to set the right structure of computers and users in your company network. Different settings (monitoring, restrictions ...) can be applied to different users (computers) or groups of users depending on their role or needs in the company.

There are two built-in groups that cannot be deleted: *Unknown* and *Active Directory*.

Unknown - once a new client is connected, the newly connected users and computers are allocated into this group. You can copy and paste/move these users and computers from the Unknown group to the groups you have created by yourself. If you delete a user or computer from your own groups, they will move back to the Unknown group. The same applies to the users and computers from a group which has been deleted in the user tree. Delete the users or computers from the Unknown group to erase them completely.

Active Directory – this is used for Active Directory synchronization to server. You can select the Active Directory tree in the Server settings and, after confirmation, users and computers will be loaded into the AD group. If the computers already exist in Unassigned category, they will move to AD group. If they already exist in different group, they will be in both – AD tree and original group. This group is read-only, so you cannot create new users and computers here not delete existing ones, but you can copy them into your custom groups. The AD group is only used as a connection between the Active Directory tree and the user tree in console.



More detailed description of User tree and its settings you can find in **Help -> Console -> Interface** description -> User tree

Web and application categories

Settings of Categories is available in Maintenance -> Categories. Safetica can monitor or restrict specific web sites, applications or file types. Therefore, there are three databases with the most known Application, Web and File type categories that you can use in DLP rules. Each category has its own tab. You can customize every category based on your company needs. Items which are not categorized yet are listed in the *Unknown category*. Another possibility to categorize Websites and Applications is in Auditor. On respective view – you will see uncategorized items, choose Web Categorization (Applications Categorization) layout, click on the Unknown category and choose the correct one.

Using the Categories view you can update the category d	latabase and edit the categories assigned to various applica	tions and web sites. You can also add your own categories and records.	
CATEGORIES			
You can update categories in the Definition updates secti	ion of the <u>Update and Deploy</u> view.		
Clear local cache			
Application Categories Web categories File	type categories		
Application Categories Web categories File	type categories		
	type categories		
Browse database	type categories		
Browse database RECENTLY CATEGORIZED APPLICATIONS	type categories		
Browse database RECENTLY CATEGORIZED APPLICATIONS Drag below this text the columns you want to group by	type categories	Y Date and time マ	
Browse database RECENTLY CATEGORIZED APPLICATIONS Orag below this text the columns you want to group by Y Application		▼ Date and time ▼ 7/20/2017 01:57:46 PM	
Browse database RECENTLY CATEGORIZED APPLICATIONS Drag below this text the columns you want to group by Y Application TCP/IP Route Command (ROUTE.EXE)	▼ Application category	• • • • • • • • • • • • • • • • • • • •	
Browse database RECENTLY CATEGORIZED APPLICATIONS Drag below this text the columns you want to group by Vapplication TCP/IP Route Command (ROUTEEXE) Lists the current running tasks (tasklist.exe)	▼ Application category Unknown category	7/20/2017 01:57:46 PM	
Application Categories Web categories File Browse database RECENTLY CATEGORIZED APPLICATIONS State of the second	▼ Application category Unknown category Unknown category	7/20/2017 01:57:46 PM 7/20/2017 01:57:16 PM	

DLP Zones

All settings regarding Zones is available in **DLP -> Zones**.

Zones can be used for creating named sets of external devices, printers, IP addresses, network paths and e-mail addresses which we can link to as separate entities. You can then use them in Security Policies, DLP rules and Device Control. Zones can be arranged in a tree structure.

In the first tab *Zone content*, there are two basic categories – *Allowed* and *Denied*. You can create any other category based on your needs (departments, offices, groups of users, etc.) and structure it by setting a parent zone.



Any new device that has been found on workstations with Safetica client will be shown in the second tab – *Unassigned items*. You can assign devices to prepared categories, or create a new category. Mark the field (zone) you want the device assign to and then add selected device by clicking on *Add*, or simply drag and drop the item to the middle field.

Zone content Unassigned	l items (1)		
Here you can find the devices that	at were found on client co	omputers. You can make assign these devices to appropriate zones and then	confirm the assignment using the button.
Add zone			
Zone name		ITEMS ASSIGNING	
Allowed	Edit Remove	Zone name: Privileged usees	Items which are not assigned to any zone.
Privileged usees	<u>Edit</u> <u>Remove</u>	Add or drag here items you want to add to selected zone.	Unassigned items
			- Mass storage (No items)
		\sim	(No items)
			Physical printers Odeslat do aplikace OneNote 2010 (NTB-HEJZLAR) (JH Add Remove Network printers
			(No items) Output (No items) (No items) (No items)
			□ ° Firewire (No items)
			Bluetooth (No items)

You can add (Add zone) two types of items – *External device* and *Network*. Details about each item and its settings can be found in Help. Here in Zones, you will set only the structure of Zones and items, which belong to each zone. Any device connected to computer with Safetica client will show up automatically and you can simply add them to the Zone of your choice. The rules that will apply to each zone can be set in *DLP Rules, Security policies* or *Device control*.

	1. Item choice	
	EXTERNAL DE	/ICES
_	External device	You can add external devices (such as USB flash disks) using the vendor, product and device identification. Afterwards these devices can be used in other views - e.g. it can be set as allowed in security policies.
	NETWORK	
	IP address	You can add specific IP addresses into the zone. You can use zone with IP address in other views like DLP rules or Security policies management.
	Network path	You can add specific network paths. Afterwards these network paths can be used in other views - e.g. it can be set as allowed in security policies.
	E-mail	You can add specific e-mail addresses. Afterwards these e-mail addresses can be used in other views - e.g. it can be set as allowed in security policies.
	Printer	You can add specific network printers. Afterwards these network printers can be used in other views.
	Web address	You can add specific web addresses. Afterwards these web addresses can be used in other views - e.g. it can be set as allowed in security policies.

Sensitive content

Sensitive content is a feature for scanning emails and file attachments based on the Dictionary and *Keywords*, defined in Sensitive content. When user wants to send an email which contains certain content, user will be informed and then must agree whether to send the sensitive content or not. This activity is logged in DLP protocol.

- 1) Open Safetica DLP Sensitive content
- 2) Choose Enable.
- 3) Choose dictionary or specific *Keywords* which you want to search for. You can have specific *Keywords* or <u>Regular expression</u>.
- 4) Save the settings.

DLP rules	DLP protocol	Zones	Disk guard	Device control	Encrypted disks	Bitlocker devices	Bitlocker disks	Sensi	itive co	ntent
-	Enabled						?	0	ŵ	×
^	BASIC INFORM	ATION								
		notified ar				searched for in e-mails ant to tag the local files				
<u>~</u>		ow the use	er to choose wh	at types of content v	will be searched for in (e-mails.				
	Social security nu	mbers (US	A):	Inherit	1					
	National identifica	ation num	bers (CZE):	Inherit						
	National insuranc	e number	s (UK):	Inherit						
	Credit card numb	ers:		Inherit						
	Social security nu	mbers (US	A) + HIPAA:	Inherit						
li	Searched keyword	ds: Add I	keyword		j					

Regular expression

Regular expressions are a sequence of characters that defines a search pattern which is compared with individual words. Words are delimited by specific characters (space, -, , , /, $\{\}$, [], ())

For example:

If you want to tag all documents containing the word "Invoice4343" you can easily create regular expression like this (Invoice4343). However, if you want to tag all invoices, not only with number 4343, you can use the expression: (Invoice[0-9]{4}). This will tag all invoices (Invoice0000 - Invoice9999). We can also ignore upper and lower case. Words "INVOICE4343" and "invoice4343" can be described in regex as: [Ii][Nn][Vv][Oo][Ii][Cc][Ee][0-9]{4}

Advanced DLP: Secure channels

Using Safetica DLP you can restrict the input and output channels by specifying the restrictions in File guard and external devices restriction in Device control.

Restrict external devices

Device control feature offers the ability to allow or deny the usage and access to various types of external devices. You can set access to USB devices, Windows portable devices, FireWire and etc. using the Zones feature.

Enable device control

To enable the device control, there are two important steps.

- 1) From User tree, choose the group you want apply the settings on
- 2) Choose Enable, *Disable* or *Inherit* on selected group/user. If you choose inherit, the settings will be same as for parent group.



Device Control Settings

Settings consist from two sections.

- 1) General settings of all ports (section *Advanced settings*), which will be applied to all new and unknown devices
- 2) Settings in zones
 - a. List of devices connected to workstations with client
 - b. Zones created for customized settings

∧ DEVICES SETTINGS

Default settings can be chang	jed in every zone.							
Add devices or edit zones								
Zone name	one name Option		Device 🔺					
Not in zone/Not set (3)			E 🔹 USB	∃ 🖞 USB				
Allowed (0)		Inherit	- Mass storage	🕀 Mass storage				
Denied (0)		Inherit	(No items)					
			Others (not used by DLP rules)					
			Logitech USB Headset	Details	Edit			
			Windows Portable Devices (not used by DLP rules)					
			MTP USB Device		Edit			
			[•]					
			(No items)					
			Bluetooth (not used by DLP rules)					
			ThinkPad Bluetooth 4.0		Edit			
Other than NTFS file systems	s: 🔲 💶 💶 Inherit							
Ports settings								
USB:	Inherit							
Card Reader:	🔲 = = = = Inherit							
Windows Portable Devices:	🔲 🖛 🚥 🚥 🖬 Inherit							
CD/DVD:	🔲 🖛 🖛 🖛 🖬 Inherit							
Firewire:	🔲 🖛 🖛 🖛 🖬 Inherit							
Infrared device:	🔲 🖛 🖛 🖬 Inherit							
Bluetooth:	Inherit							
COM:	Inherit							
LPT:	Inherit							

General settings are made on each port separately. It defines the default behavior when an unknown device is connected. When you know a device, you can add it to a certain zone and set a different rule. If you want to add new device to Zone or edit Zone, click on *Add devices* or *edit zones* (see chapter <u>DLP Zones</u> on how to edit them). Zone settings have always higher priority than port settings. For example, if USB ports are disabled in the port settings but enabled for a certain zone, the use of USB ports will be enabled in that particular zone.

All settings here – either in zones or in ports – have six options to choose from.

- Inherit settings are inherited from the parent group.
- Deny reading and writing on the external devices is disabled.
- *Read only* the external device can only be read from, but not written to.
- *Notify* when using an external device, the user will see a notification in the dialog box and a corresponding record will be created.
- *Test mode* similar behavior as the previous option *Notify*, but the end user is not informed in any way. A record is made only. This mode is intended for testing the behavior of the setting.
- Allow reading and writing on the external devices is enabled.

More detailed info you will in Help -> DLP -> Device control

Restrict disk access

Disk guard feature offers the ability to deny the access to local or cloud drivers and local or network paths. Attempts to access these locations can be logged also.

Enable Disk guard

To enable the device control, there are two important steps.

- 1) Open Safetica DLP Disk guard
- 2) From User tree, choose the group you want apply the settings on
- 3) Choose Enable, *Disable* or *Inherit* on selected group/user. If you choose inherit, the settings will be same as for parental group.



Logging settings

At the top of the settings page is **logging settings** with 3 easy options: Disabled – Inherit – Enabled. You can find the log in the Visualization mode in the top menu.



Paths

There are four categories, which you can apply the settings on. At any location, the settings are always *Inherit – Deny – Read only – Allow*.

- Local path path to folders on an end station (e.g. D:\Folder\name).
- *Network path* path to folders shared over the network. You must enter the path in the network format (e.g. \\Shared\Folder)
- *Drives* there is a list of letters which identifies drives. You can set access rights for each drive there.
- Cloud drives here you can specify access settings for local folders that are used by certain cloud services. The supported cloud services are OneDrive (Personal, Business), SharePoint, Google Drive, Dropbox and Box Sync. You can set up access rights for all of the supported cloud services or for each of them individually. This works only for cloud applications, not for accessing to cloud via browser.

Always keep in mind that all the settings you do here is only valid for group of users/computers that you have selected in Users tree on the left side. Read more details in **Help -> DLP -> Disk guard**.

🔅 <u>III</u> File tagging DL	.P rules DLP protocol Zones Disk	guard Device control	Bitlocker devices Bitlocker disks					
+ 🕈 🖇	Enabled							
	BASIC INFORMATION Disk guard feature offers the ability to deny the access to local drives and local or network paths. Attempts to access these locations can be logged also. A LOGGING SETTINGS							
	Logging: Inherit	Logging: Inherit						
	PATHS							
	Λ Disabling of system disk may cause malfunction of important programs. Those settings will be ignored on the endpoint station.							
	Add local path Add network path							
	Path	Access						
	Local paths							
	(No items)							
	Network paths	Inherit						
	(No items)							
	B Drives							
	Cloud drives							
	OneDrive Personal	Inherit	<u>1 endpoints</u>					
	OneDrive Bussiness	Inherit	<u>1 endpoints</u>					
	SharePoint	Inherit	<u>1 endpoints</u>					
	Google Drive	Inherit	<u>0 endpoints</u>					
	Dropbox	Inherit	<u>0 endpoints</u>					
	Box Sync	Inherit	<u>0 endpoints</u>					