DLP GUIDE

www.safetica.com

safetica®

Content

Introduction to context 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
- 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 only 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) Choose the mode – *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

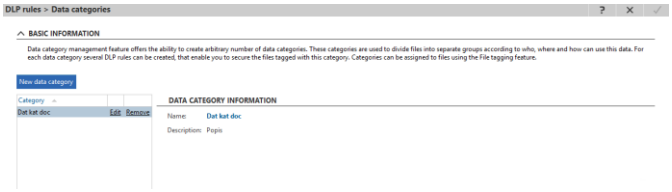
Prior to securing data, it is crucial to scan the computers and find the existing data you want to protect.

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



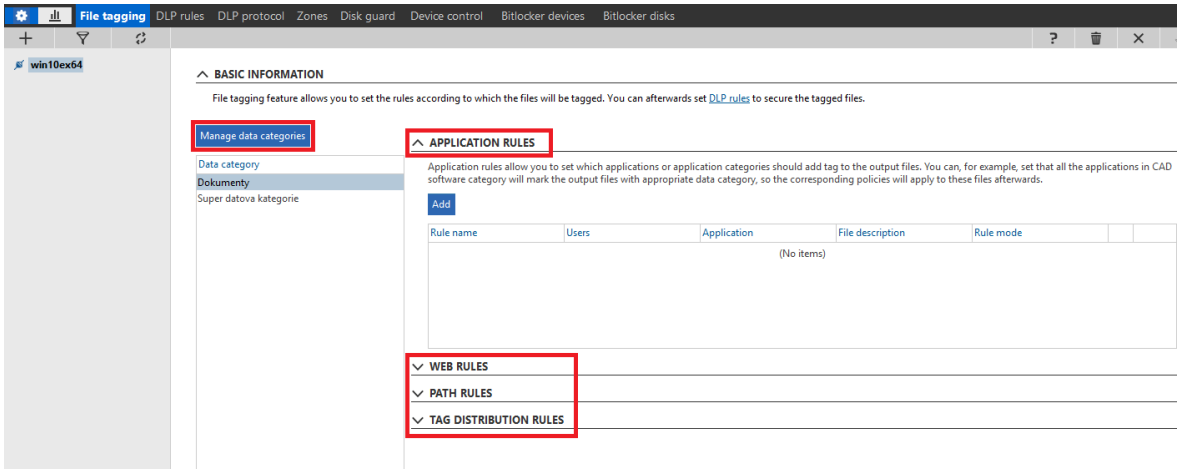
The left section of the view shows the list of data categories. After selecting the categories on the list, the name and description of the data category will be displayed on the right.

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 tagging task

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



1) Open *Safetica* - **DLP** – **File tagging**.
2) In Basic information select existing or create new *Data category (data category is create in a 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

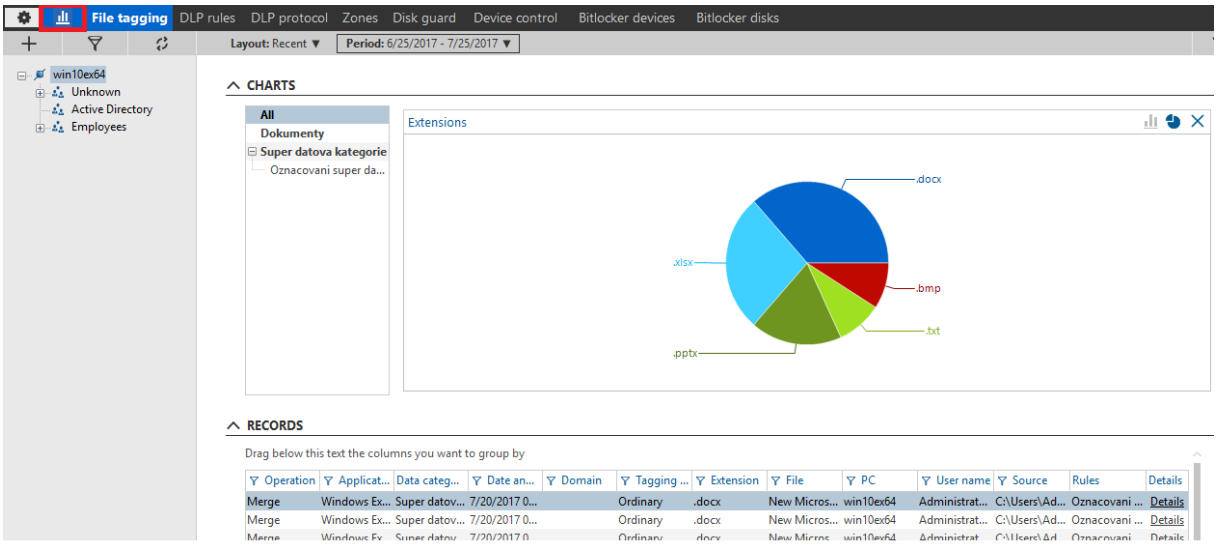
5) In the section *Creating filtering rule – Rule settings*
   a. Click to **Add application** and select *application Categories*
   b. Click to **Add extension** and *Select File type categories*

6) Click **Finish**

One Data category can have more combination rules.

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.



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

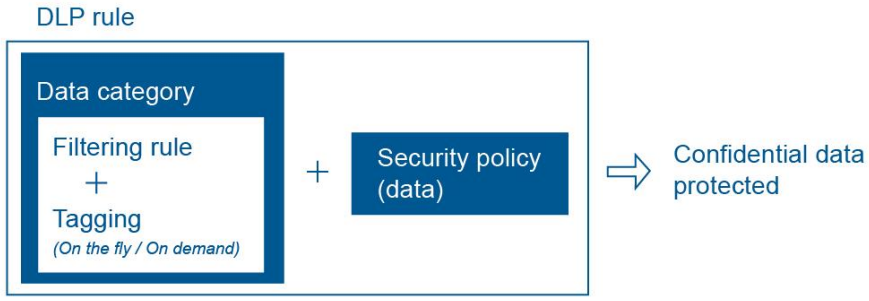
DLP Guide: Configuring DLP policies

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.



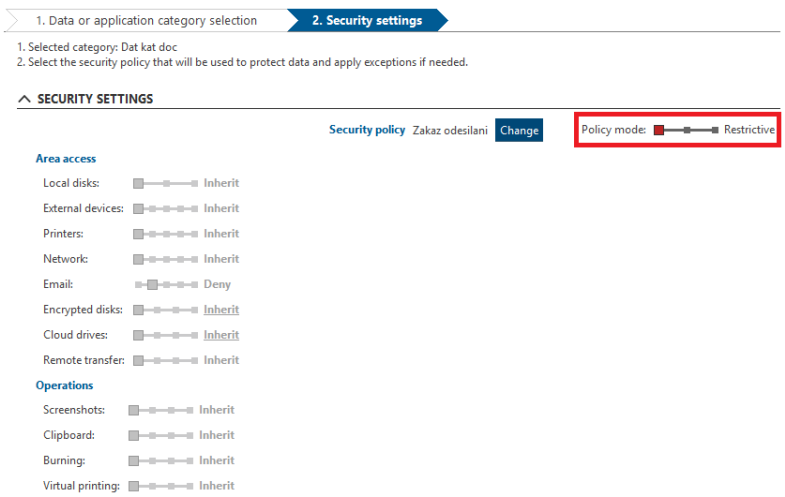
Types of DLP policies

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.

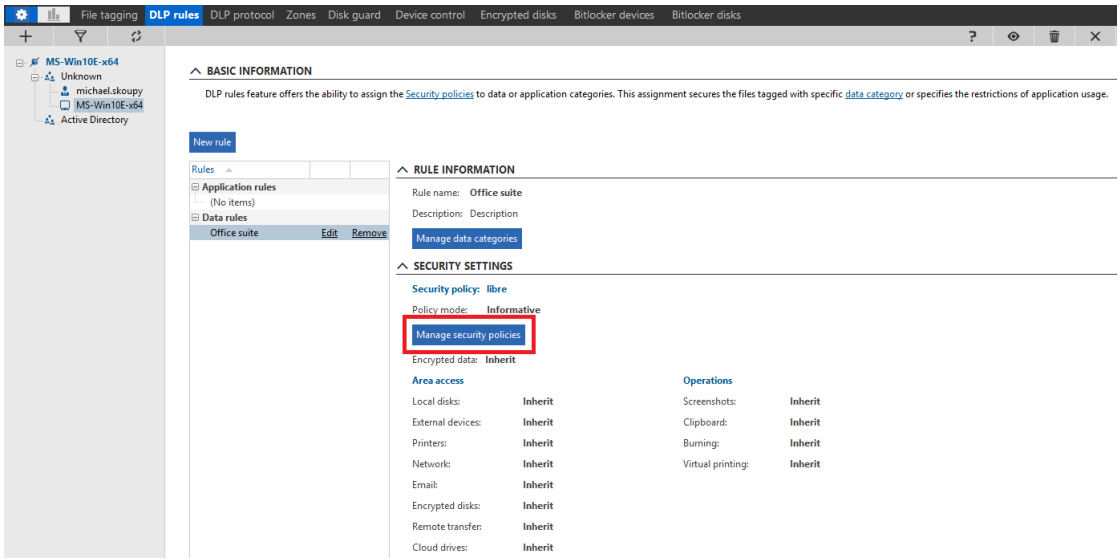


1. Create security policy

Security policies are available via Safetica -> DLP -> DLP rules -> Security policies

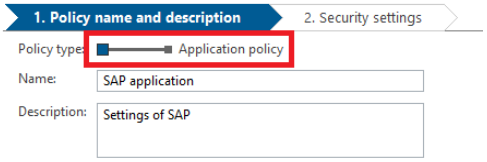
Security policies are rules through which data is protected. You can apply a policy either to data (tagged files), or to an application.

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

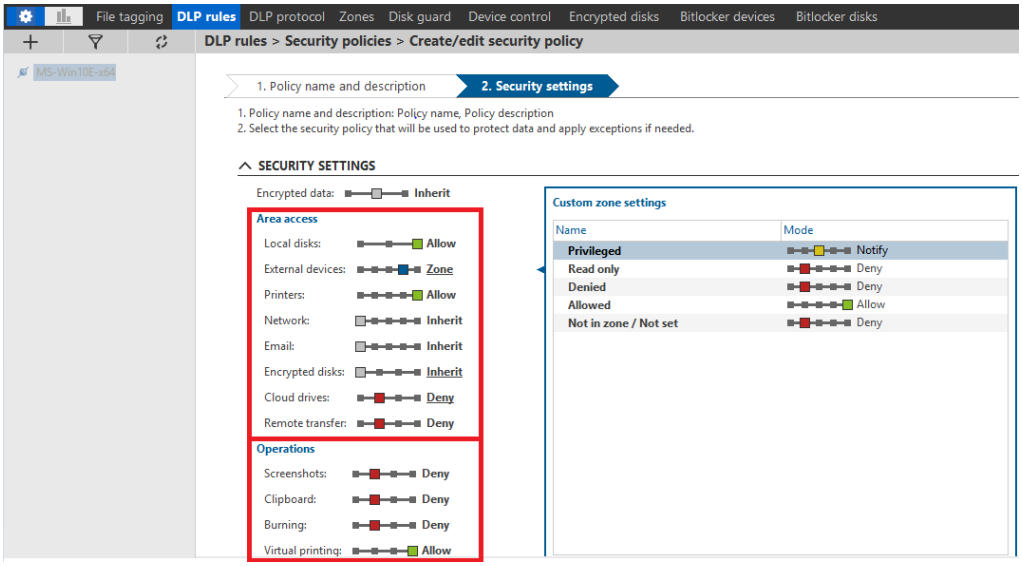


To create a Security policy:

1) 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.



2) Write Name and Description of the policy
3) Click Next.
4) Configure the Security settings for the policy.



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.

2. Configure the DLP rules

The Security policies that you have created can be assigned to Data or Application categories. New rules can be set in DLP -> DLP rules.

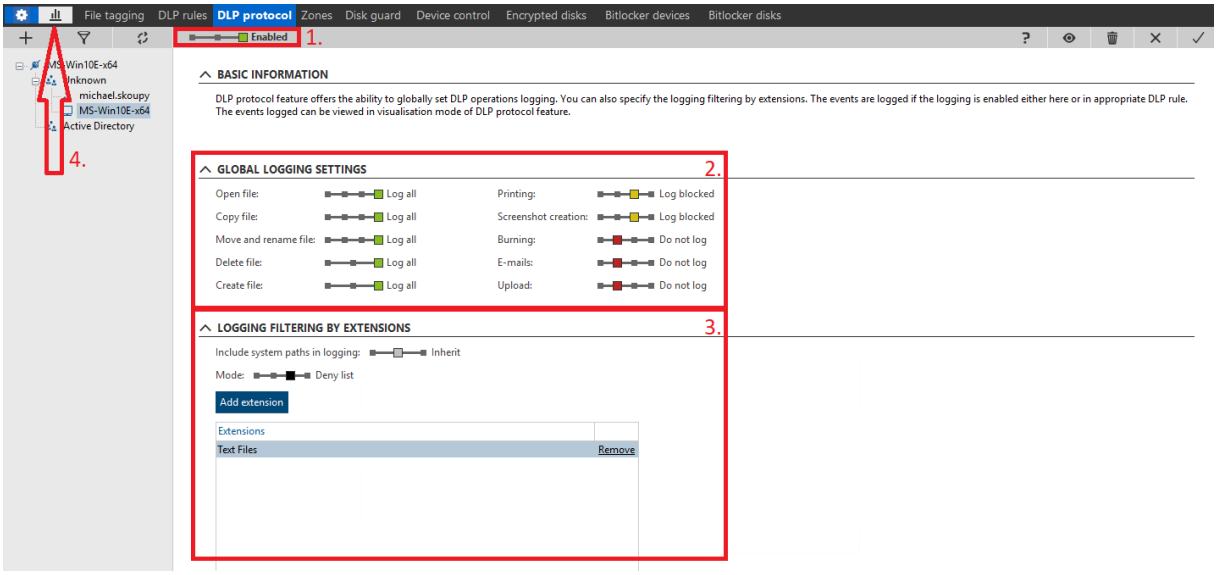
Click *New rule* and follow these steps:

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

3. Configure the DLP protocol

DLP protocol (DLP -> DLP protocol) contains configuration of which file operations and rules should be logged. This configuration applies only to files with a Safetica tag (tagged files).

1) At the top of the page is slider to Enable DLP protocol.
2) In the next part of the main settings you can specify which operations should be recorded. See **Help -> Console -> DLP -> DLP protocol** for detailed description of each operation.
   Every operation has several recording modes:
   - *Inherit* – settings are inherited from the parent group.
   - *Do not log* – the respective operation is not recorded.
   - *Log blocked* – only respective Safetica-blocked operations are recorded.
   - *Log all* – all files are monitored
3) Logging filtering by extension - you can use the Deny list or Allow list to specify which files shall be monitored.
   - *Disabled* – logging by extensions is disabled
   - *Inherit* – settings is same as in parent tree
   - *Deny list* - operations will be monitored on all files in the system except for those whose extensions are on the list
   - *Allow list* - only operations on files with extensions on the list will be monitored
4) Visualization
   All recorded data, you will see in the Visualization mode (top left corner). In the top half of the view is for charts, in the bottom half you can see detailed record. Detailed description of every all possible filter categories, you can find in **Help -> Console -> DLP -> DLP protocol**.



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*.

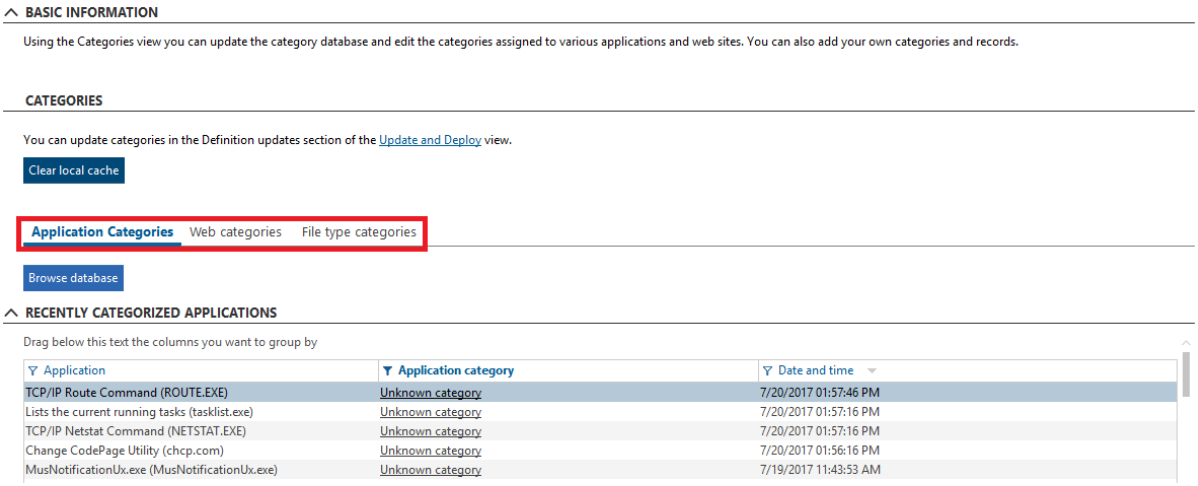
Unknown - once a new client is connected, the newly connected users and computers are allocated into this group. You can copy and paste/move these users and computers from the Unknown group to the groups you have created by yourself. If you delete a user or computer from your own groups, they will move 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 tree. 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 nor 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.

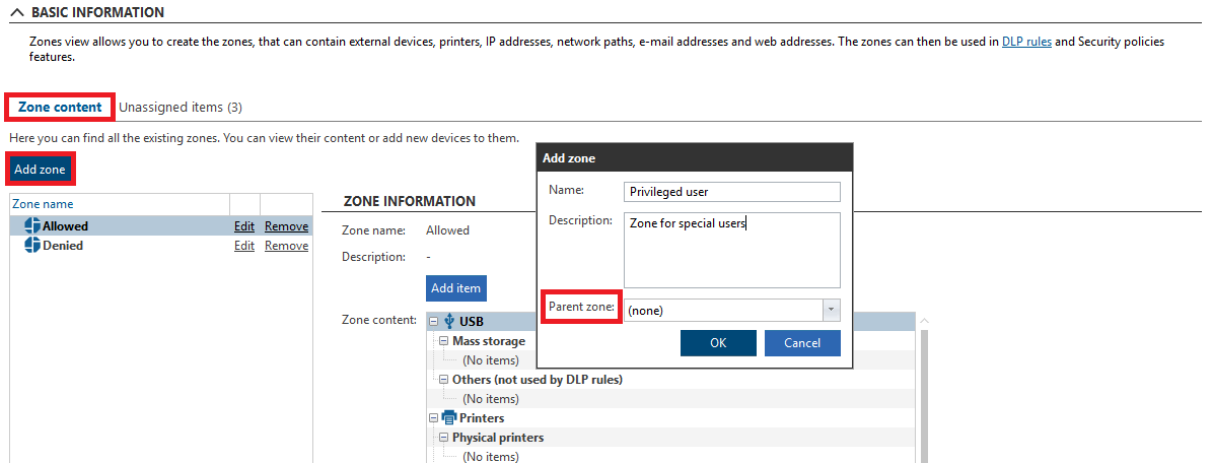


DLP Zones

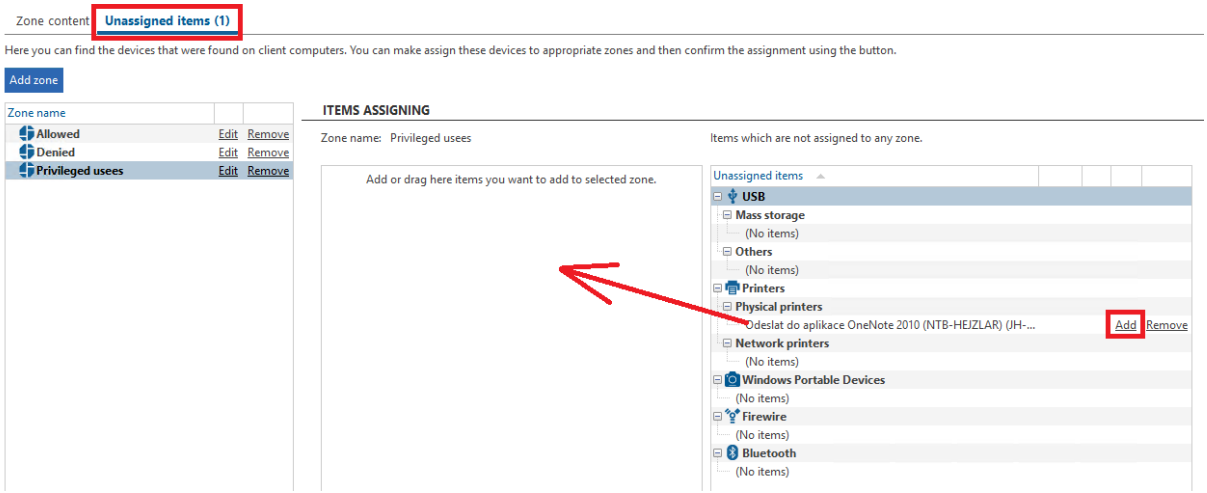
All settings regarding Zones is available in **DLP -> Zones**.

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.

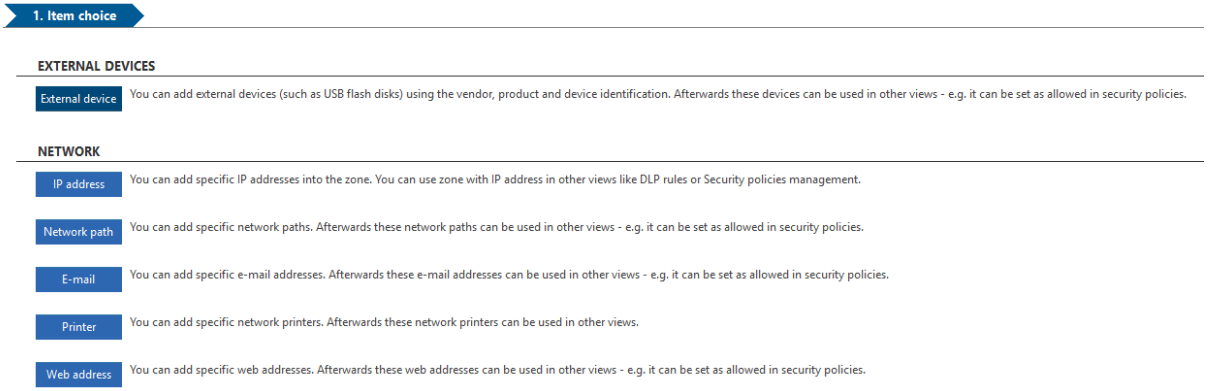
In the first tab *Zone content*, there are two basic categories – *Allowed* and *Denied*. You can create any other category based on your needs (departments, offices, groups of users, etc.) and structure it by setting a parent zone.



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 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.



You can add 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*.



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.

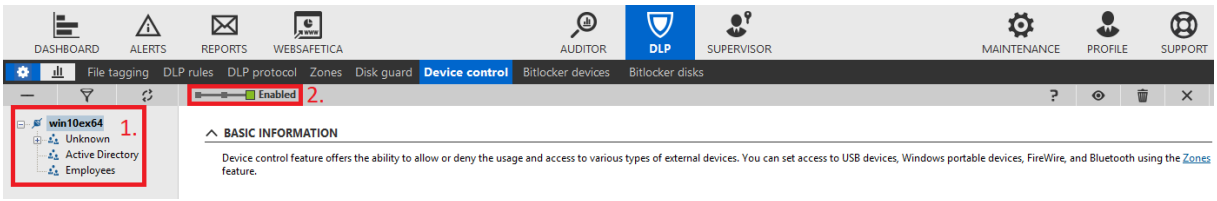
Restrict external devices

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.

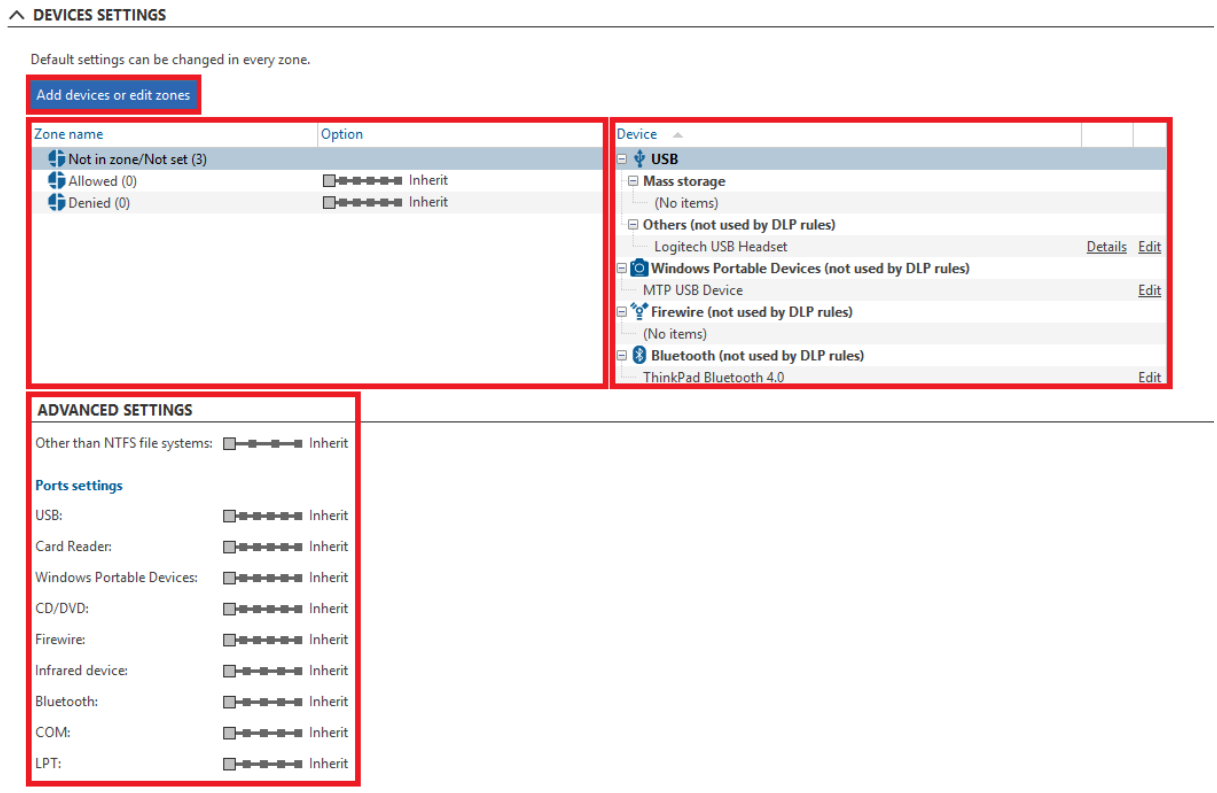
1) From User tree, choose the group you want apply the settings on
2) Choose Enable, *Disable* or *Inherit* on selected group/user. If you choose inherit, the settings will be same as for parent group.



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



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 *DLP Zones* 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**

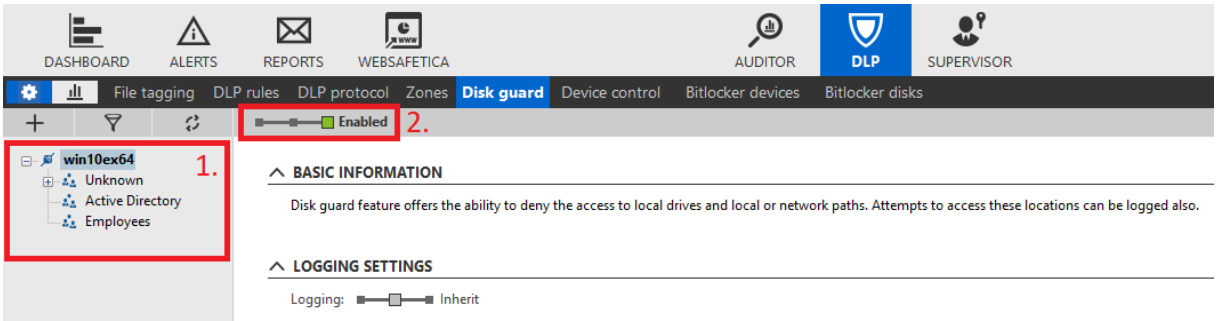
Restrict disk access

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

Enable Disk guard

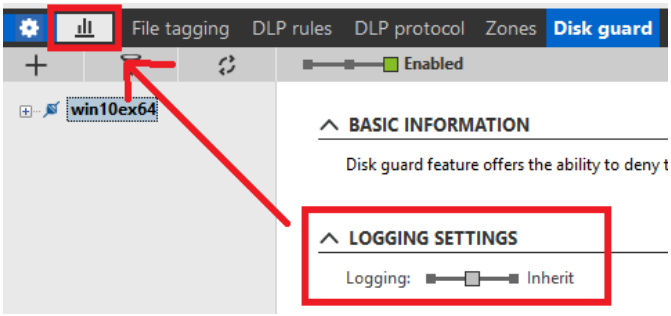
To enable the device control, there are two important steps.

1) 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 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**.