COMODO

Creating Trust Online®

Comodo
MyDLP

Software Version 3.0

Administration Guide

Guide Version 3.0.053016

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1.Introduction to Comodo MyDLP

MyDLP is a fully fledged data loss prevention solution that allows you to discover, monitor and control the movement of confidential data in your organization's network. You can use policy actions to pass, log, archive and quarantine moving data, restrict use of removable storage devices, encrypt removable devices and even delete files discovered in storage.

The two main components of the product are the MyDLP Network Server and the MyDLP Endpoint Agent.

Protection and Administration with MyDLP Network Server

Network protection enables you to detect and prevent confidential data from leaving your network. The MyDLP Network Server also functions as the administration center.

Protection and Discovery with MyDLP Endpoint

MyDLP Endpoint protection allows you to detect when confidential data is moved from endpoints to removable devices such as USB sticks, CD/DVDs, portable hard disk drives or smart phones from protected workstations or laptops in your organization. You can also enforce full disk encryption on removable devices. Endpoint protection also covers any document printed using network and local printers connected to computers and grabbing screenshots of sensitive documents. Endpoint data discovery enables you to detect and enforce policy on stored data which is discovered on computers in your network.

Guide Structure:

This guide is intended to take you through the step-by-step process of Installation, Configuration and use of Comodo MyDLP and is broken down into the following main sections.

- Introduction to Comodo MyDLP
- Getting started with MyDLP
  - Installation
  - Logging on to the Management Console
  - Logging out
  - Checking Server Version and License Information
  - Changing your Password
  - Changing user information
- The Dashboard
- Data Control and Data Transfer Policies
  - The Rules Interface
- Rule Types, Objects and Matchers
  - Rule Types
  - Objects
  - Matchers
  - Integrating Active Directory Domains
  - Integrating RDMBS Connections
- Configuring Comodo MyDLP Settings
  - Configuring Protocol Settings
  - Managing Administrators
  - Configuring Endpoint Settings
  - Configuring Advanced Settings
  - Configuring Enterprise Settings

2. Getting started with MyDLP

2.1. Installation

- For MyDLP Network Server installation, please refer to the **MyDLP Installation Guide**.
- For MyDLP Endpoint deployment, please refer to the **MyDLP Endpoint Installation Guide**.

Tip: MyDLP Windows Endpoint Agent setup file can be downloaded from the 'Settings' > 'Protocols' interface of the MyDLP server administrative console. Refer to the section **Configuring Protocol Settings** for more details.

2.2. Logging on to the Management Console

MyDLP uses a web-based management console that allows administrator to build policies, review incident history and monitor user activity.

Preliminaries:

- You need to have a Flash enabled web browser to connect to the management console.
- The flash plug-in can be downloaded from: **http://get.adobe.com/flashplayer/**
- You can connect to the management console at the following URL: https://servername
  - "servername" = the hostname or IP address on which MyDLP Network Server was configured during installation. For more details, see 'MyDLP Network Server Initial Configuration' in the MyDLP Installation Guide.

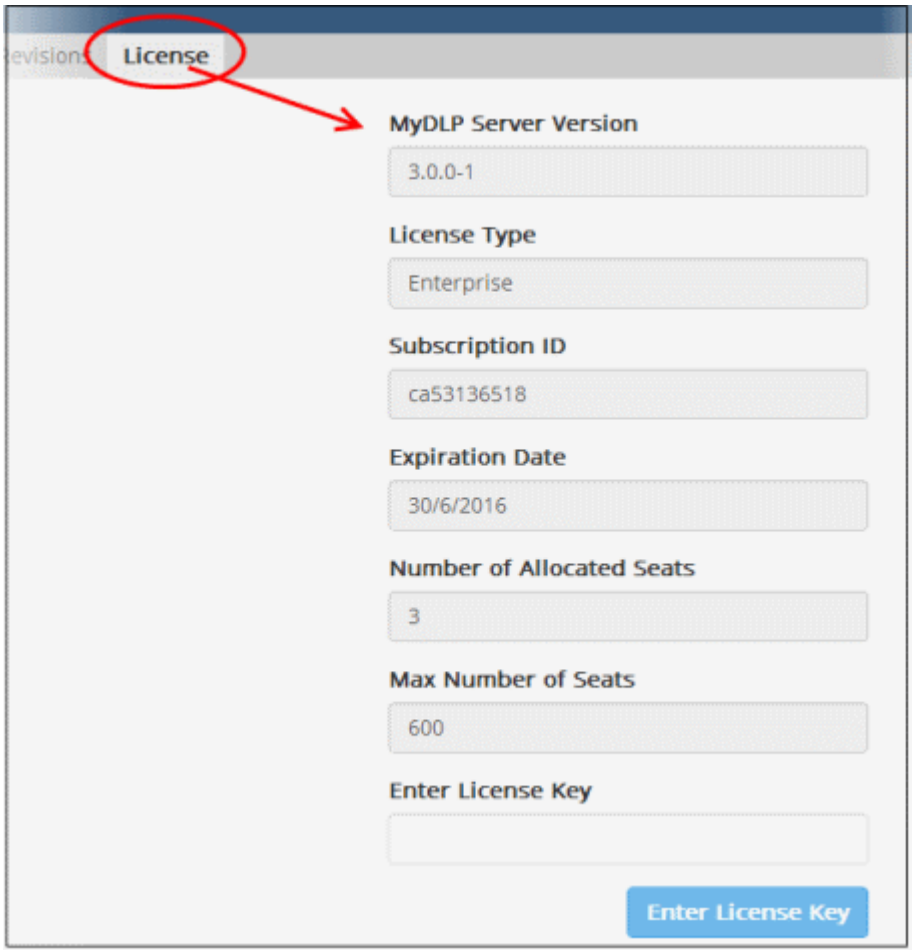
- Default username is "mydlp" and default password is "mydlp" (without the quotes). Please change these to a unique username and password immediately after logging in. For more details, see **2.5 Changing your Password**.

2.3. Logging Out

- To signout from the MyDLP management console, click your username displayed at the top right and choose 'Sign out" from the drop-down.

2.4. Checking Server Version and License Information

You can view the currently installed version of MyDLP Server and the validity term of your of license from the 'License' tab. Providing the server version number will help accelerate issue resolution times should you need to contact support.



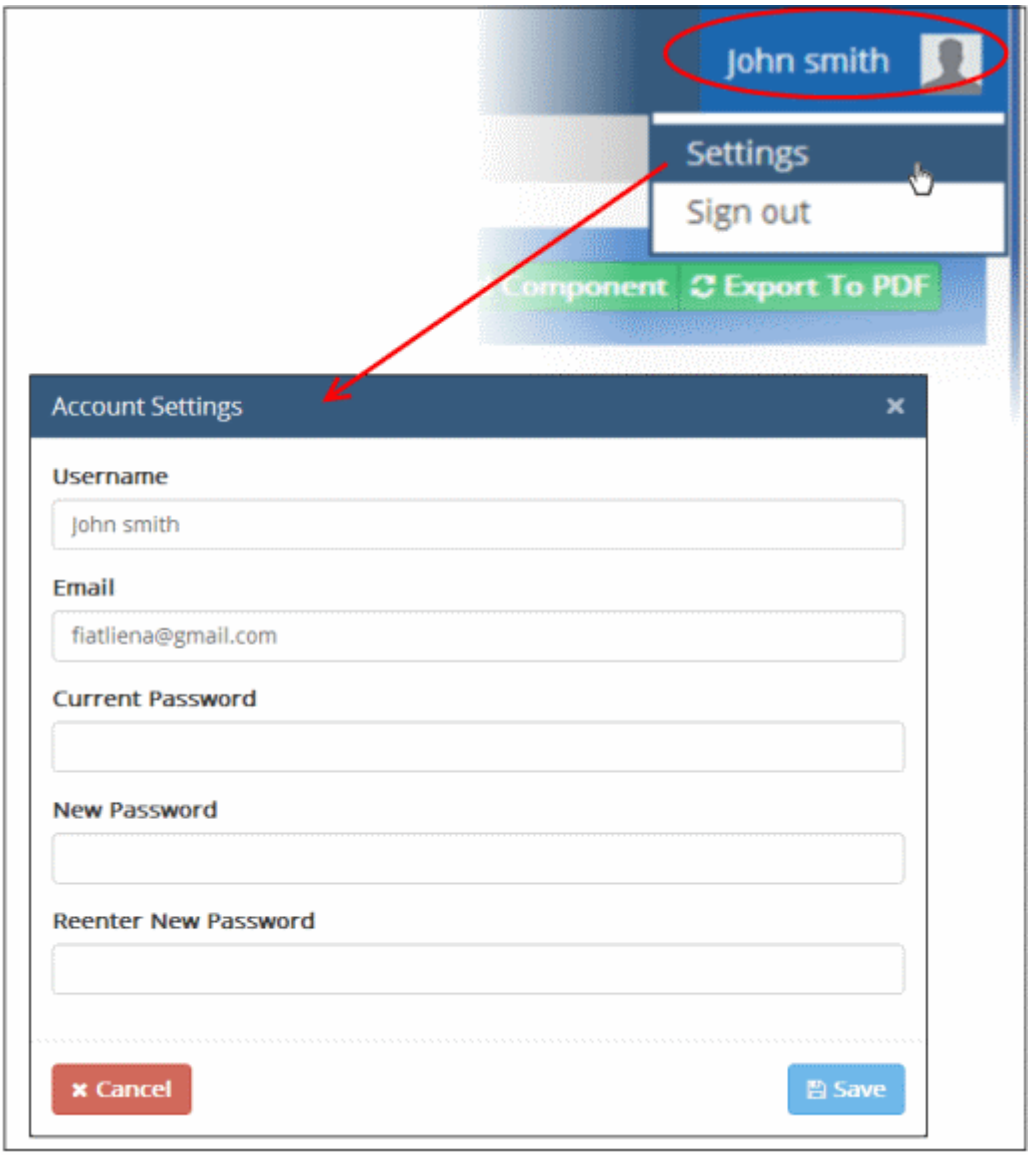
The interface also allows you to enter your new license key for renewals. Please refer to the section **The License Tab** for more details.

2.5. Changing Your Password

You can change your login password for MyDLP management console at any time.

To change the password

1. Click your username displayed at the top right of the interface and choose 'Settings' from the drop-down.
2. In the 'Account Settings' dialog, enter your current password. Reminder - after initial setup, the default password is "mydlp" (without the quotes).

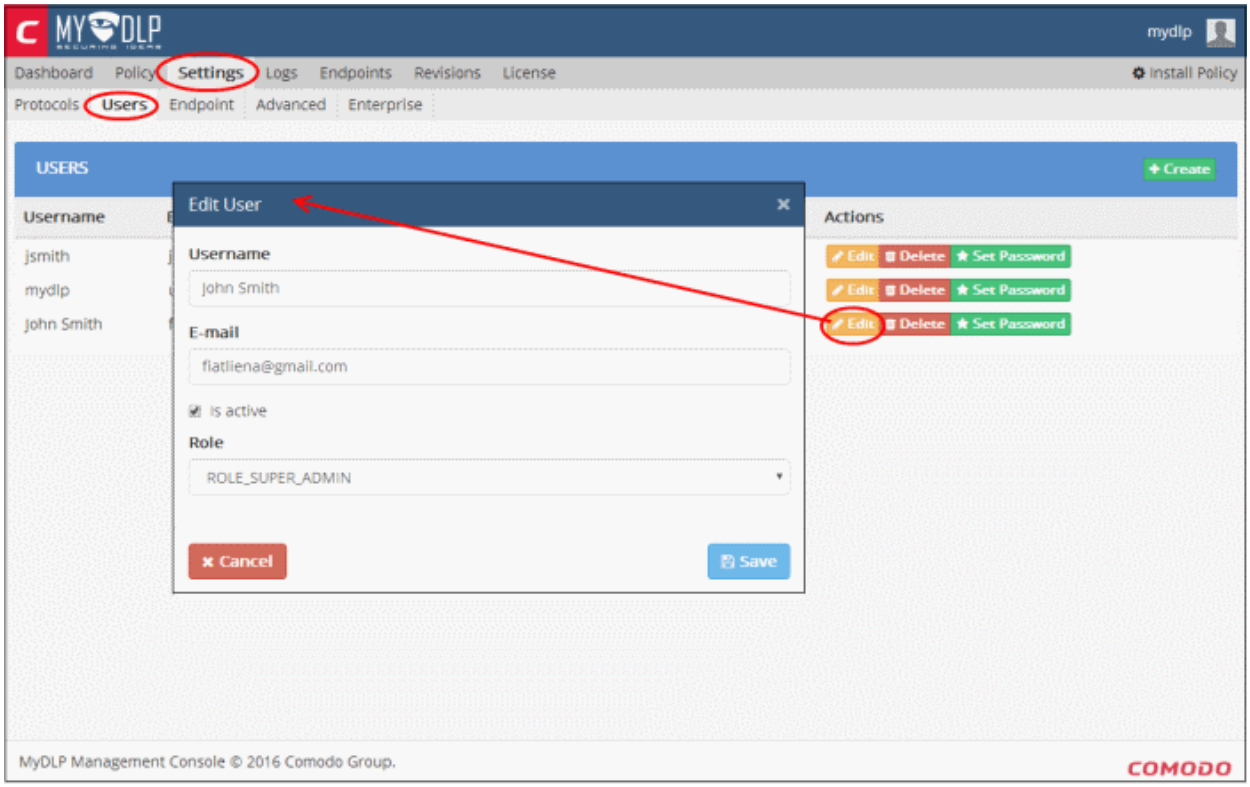


3. Enter and confirm your new password. Passwords must be at least 6 characters long and contain at least one uppercase letter, one lower case letter and one number.
4. Click 'Save'.

2.6. Changing User Information

You can change the user name, email address, AD objects and document database objects of self or other administrative users by following these steps:

1. Click the 'Settings' tab.
2. Click 'Users'.
3. Click the 'Edit' button beside the user you wish to modify.



4. Modify the details as required.
5. Click 'Save'.

3. The Dashboard

The Comodo MyDLP Dashboard contains statistics and tiles which form a consolidated, 'at-a-glance' summary of all major MyDLP activities. This includes incident logs, statistics about users and endpoints from which large amounts of data were intercepted/discovered, rules applied for the day and the ability for administrators instantly to view and download weekly reports. Administrators can customize the dashboard as required by adding or removing tiles.

The Dashboard is displayed by default whenever the administrator logs in to the administrative interface. To switch to the dashboard from a different screen, click the 'Dashboard' tab.

The Dashboard can display the following types of tiles:

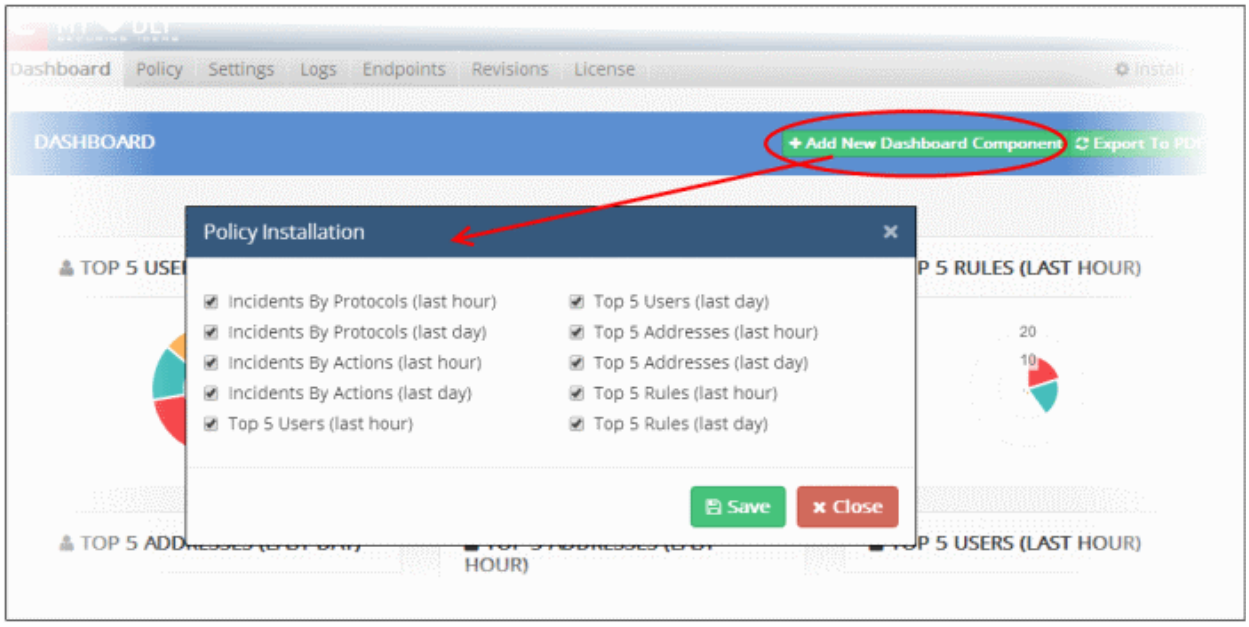
Tile	Description
Incidents by Protocols (last hour)	Shows incidents which occurred within the last hour / day according to the protocol used during the event.
Incidents by Protocols (last day)	
Incidents by Actions (last hour)	Shows incidents which occurred within the last hour/day according to the type of action which generated the event.
Incidents by Actions (last day)	
Top 5 Addresses (last hour)	Shows the 5 IP addresses from which the most data was intercepted or discovered during the past hour / day, versus the total amount of data intercepted or discovered.
Top 5 Addresses (last day)	
Top 5 Users (last hour)	Shows the 5 users from whom the most data was intercepted or discovered during the past hour / day, versus the total amount of data intercepted or discovered by all users.
Top 5 Users (last day)	
Top 5 Rules (last hour)	Shows the 5 rules from which the most data was intercepted or discovered during the past hour / day, versus the total amount of data intercepted or discovered by all rules.
Top 5 Rules (last day)	

Configuring the Dashboard

By default, the dashboard shows all the charts. The administrator can remove charts as per their requirements and add later on when required.

To add or remove a tile

- Click 'Add New Dashboard Component'



The Policy Installation dialog will appear, with the list of available tiles. The tiles existing on the dashboard are pre-selected.

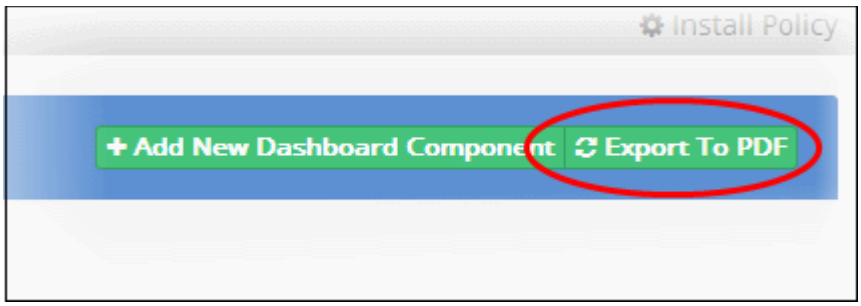
- To remove an existing tile, deselect the tile

- To add a new tile, select the tile
- Click 'Save'

The new tile(s) will be added to or removed from the dashboard.

Downloading the dashboard to PDF

- To download the report as a pdf file, click 'Export to PDF' and save the generated pdf file.



The report will be saved to your default download location.

4. Data Control and Data Transfer Policies

Data transfer policies allow you to monitor files containing sensitive data and restrict their outbound movement from endpoints and network storage. Data discovery allows you to scan your network to locate files which contain this sensitive data.

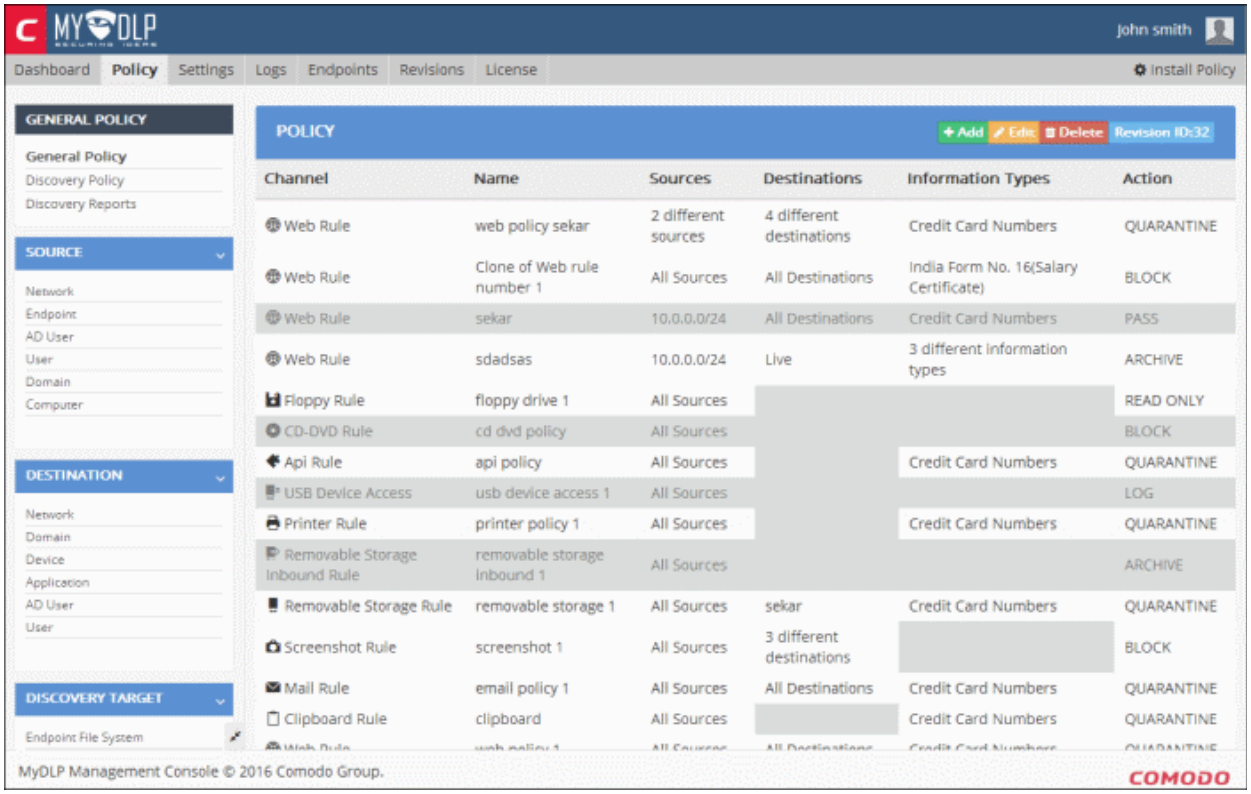
Data Transfer Policy ('General Policy')

MyDLP applies a 'Policy' to define the data control scheme for endpoints in your network. The policy is constructed from a series of rules which govern restrictions on data traveling over the web, over email, and to or from removable storage. You can also set rules which enforce automatic encryption if data is transferred to a removable device, rules to prevent screenshots being taken when certain applications are running and rules to prevent certain documents from being printed. Refer to '**Adding a Data Transfer Rule**' for more details.

Data Discovery ('Discovery Policy')

MyDLP can run scheduled scans on your network to discover files containing sensitive information stored on local and network drives. You can define multiple rules to scan different targets for files containing information types that you define. You can also specify the action to be taken on files discovered to contain sensitive information. Discovery reports can be viewed from the 'Discovery' interface. Refer to the section '**Adding a Data Discovery Rule**' for more information.

Data transfer and data discovery rules are both constructed by adding 'objects' into a rule using the rule wizard - a flexible system that allows you to create highly granular yet easily modifiable rule-sets. MyDLP comes with a series of pre-defined objects which are displayed on the left of the 'Policy' interface. You can create your own custom objects and new rules can be created by clicking the '+ Add' button.

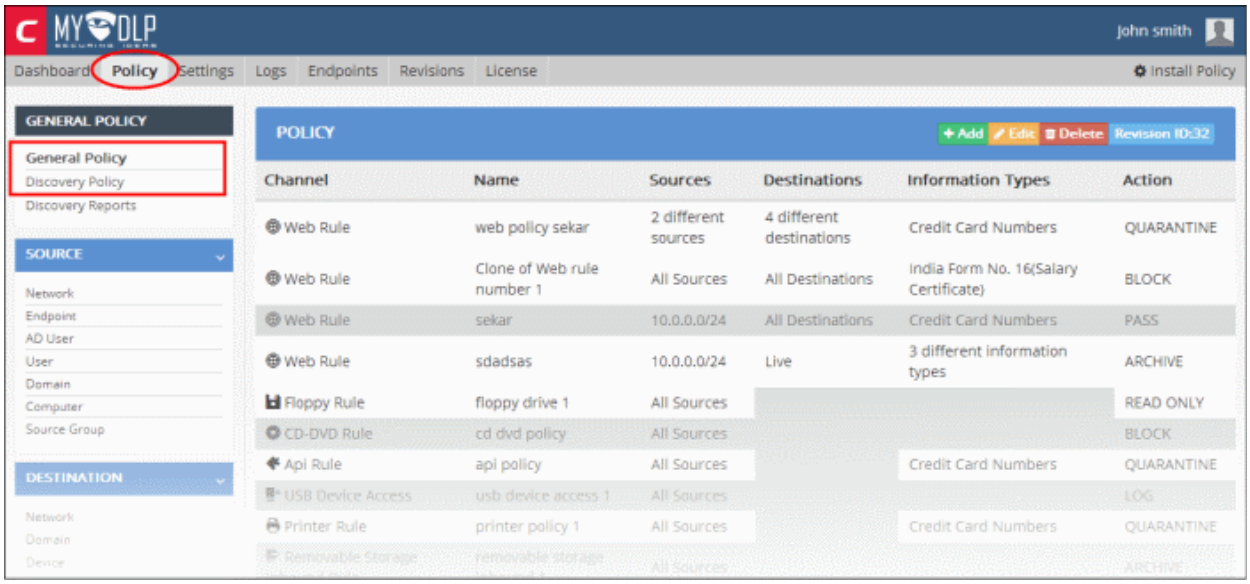


The following sections contain more details on rules:

- **The Rules Interface**
  - **Rule Channels / Types**
  - **Rule Actions**
  - **Email Notifications and Messages**
  - **Adding a Data Transfer Rule**
  - **Adding a Data Discovery Rule**
  - **Deploying a Policy**

4.1. The Rules Interface

All rules that have been created for data transfer policy and data discovery are listed under 'Policy' > 'General Policy' and 'Discovery Policy' respectively.



Both rule types have four common components, 'Sources', 'Destinations', 'Information Types' and 'Actions'. The Data transfer policy rule has a 'Channel' rule component, while discovery rules have 'Discovery Type' and 'Schedule' components.

Rules at the top of the table have a higher priority than those at the bottom and are applied first. In the event of a conflict between rules, the setting in the rule nearer to the top of the table will be applied.

Rules Table - Description of Columns	
Rule Component	**Description**
Channel	Type of rule. You select the rule 'type' then choose a rule name as the first steps when creating a new rule. Example data transfer 'channels' include 'Web Rule', 'Removable Storage Rule' , 'Screenshot Rule' and 'CD-DVD rule'. The rule 'channel' is easily identified by the icon to the left of your rule name in the table. 
Discovery Type	(Discovery rules only). Type of discovery rule. Discovery types include 'Endpoint Discovery Rule' and 'Remote Storage Rule'. The rule type is easily identified by the icon to the left of rule name in the table. 
Name / Policy Name	The name of the rule that was provided in the rule wizard.
Schedule	(Discovery rules only). Allows administrators to set and view the schedule of the rule. The administrator can also run on-demand discovery scans as per the rule at anytime. Clicking the arrow to the right will commence the scan immediately.
Source	Determines what user, user groups or locations should be covered by the rule. Users and user group sources can be defined by an IP address, network, Computer name, Endpoint ID, Active Directory element or an email address depending on the rule type. Location sources are for discovery rules and can be a network, computer name, endpoint or remote storage.
Destinations	The 'Destination' can be domain, directories or application names, depending on the rule type.

	Destination column is not required for removable storage, removable storage inbound, printer, API and Remote Storage rules.
Information Types	The particular type of information to be searched for or monitored. There are many pre-defined information types and the administrator can define custom information types too. Information type column is not required for **removable storage inbound** and **screenshot** rules.
Action	Action to be taken when all conditions of the rule are met. Available actions are: • **PASS** • **BLOCK** • **LOG** • **QUARANTINE** • **ARCHIVE** • **DELETE** **Note**: The DELETE action is available only for discovery rules.

The following sections contain more details on rules:

- **Rule Channels / Types**
- **Rule Actions**
- **Email Notifications and Messages**
- **Adding a Data Transfer Rule**
- **Adding a Data Discovery Rule**
- **Deploying a Policy**

4.1.1. Rule Channels / Types

MyDLP has different categories of rules which are known as 'Rule Types'. Rule types are classified according to data inspection channel and each type is effective only on data traversing through, or residing in, the named channel. Each rule type forms a starting point from which very specific rules can be created by adding or removing rule objects.

Data Transfer Policy Channels

Web rules are used to monitor and control all traffic that passes to and from your network over HTTP and HTTPS. This includes data exchanged with any external network like the Internet. See the section **Web rules** for more details.

Mail rules are used to monitor and control data passed over email and other SMTP traffic from specified sources. See the section **Mail rule** for more details.

Removable Storage rules control data transferred to external devices such as USB memory sticks, removable hard drives and smart phones. See the section **Removable Storage rule** for more details.

Removable Storage Inbound rules are used to archive data copied from removable memory devices on to the computer. See the section **Removable Storage Inbound rule** for more details.

Removable Storage Encryption rules allow you to encrypt removable devices connected to endpoints on your network. After encryption, any data on the drive can only be read if it is connected to your network

and not by any other network. If you enable this rule for all sources then any new devices will be immediately encrypted as soon as they are connected. This would prevent, for example, any guest or hostile from plugging in a USB drive, downloading data and taking it out of your network. See the section **Removable Storage Encryption rule** for more details.

Screenshot rules prevent print screen function while a sensitive application is running. See the section **Screenshot rule** for more details.

Printer rules allow you to prevent documents matching specific criteria from being printed. See the section **Printer rule** for more details.

API rules are a unique feature which allow you to integrate custom applications with MyDLP. See the section **API rule** for more details.

USB Device Access rules are used to monitor or block use of USB memory devices on the selected computers covered by the source object defined in the rule. See the section **USB Device Access Rule**for more details.

CD-DVD rules are used to control the use of optical disks like CD and DVD on selected computers covered by the source object. You can choose to monitor or block use of disks or set them to 'Read-Only' mode. See the section **CD-DVD Rule** for more details.

Floppy rules are used to control the use of Floppy disks on selected computers covered by the source object. You can choose to allow or block use of disks or set Floppy disks to Read-Only mode to allow reading of data from the disks and blocking writing of data on to them. See the section **Floppy Rule** for more details.

Clipboard rules are used to control the copy and paste function on selected computers covered by the source object. You can choose actions such as pass, block and more for this rule. See the section **Clipboard Rule** for more details.

Discovery Rule Type

Endpoint Discovery rules are used to discover and control sensitive data on local storage and hard disks. See the section **Endpoint Discovery rules** for more details

Remote Storage rules are used to discover files containing sensitive data of specified type(s) from remote servers and network file systems. See the section **Remote Storage rule** for more details

4.1.2. Rule Actions

- **PASS** - Allows information to travel through the data channel freely without generating log entries. This action is available for all rule types.
- **LOG** - Creates a log entry when data passes through the data channel. This action is not available for screenshot rule and Floppy rule.
- **ARCHIVE** - Allows information to pass through the data channel, generates an event log and archives a copy of the information. Administrators can download the file from the 'Logs' interface. Refer to the section **Downloading the Files Archived by MyDLP** for more details. This action is not available for the screenshot, USB Device Access, CD-DVD and Floppy rules.
- **BLOCK** - Prevents information from passing through the data channel and generates an event log. This action is not available for the removable storage inbound rules.
- **QUARANTINE** - Prevents information from passing through, generates an event log and archives a copy of the information. This action is not available for the removable storage inbound, screenshot , USB Device Access rule, CD-DVD rule and Floppy rules.
    - When this action is applied with an 'Endpoint discovery' rule, all files that match the information type specified in the rule will be deleted from the endpoint - but a copy of the files will be archived

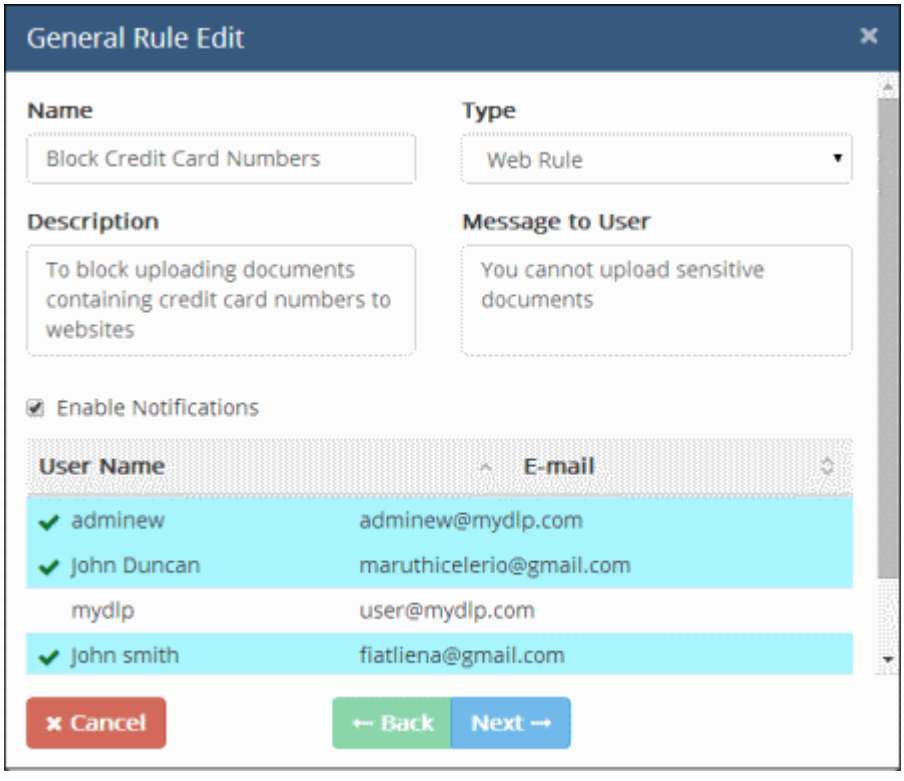
in the MyDLP server. Administrators can download the file from the 'Logs' interface. Refer to the section **Downloading the Files Archived by MyDLP** for more details. The action is similar to applying the 'Delete' action on an 'Endpoint discovery rule', with the difference that a copy of the matching files will be saved.

- **ENCRYPT** (only available for 'Removable Storage Encryption Rule'). Detects any new USB storage device connected to source endpoints, formats the device and encrypts it. After encryption, any data stored on the device can only be read if it is connected to your network and not by any other network. This prevents, for example, any guest or hostile from plugging in a USB drive, downloading data and taking it out of the network.
- **DELETE** (only available for 'Discovery' rules). Deletes discovered files which match your criteria. It is advised to use this action very carefully.
- **READ-ONLY** (only available for CD-DVD and Floppy rules). Allows reading and copying of files from DVD and floppy disks but does not allow data to be copied from endpoints to the disks.

4.1.3. Email Notifications and Messages for a Rule

Administrators can configure MyDLP to send email alerts to themselves or other administrators for events concerning the following types of rules:

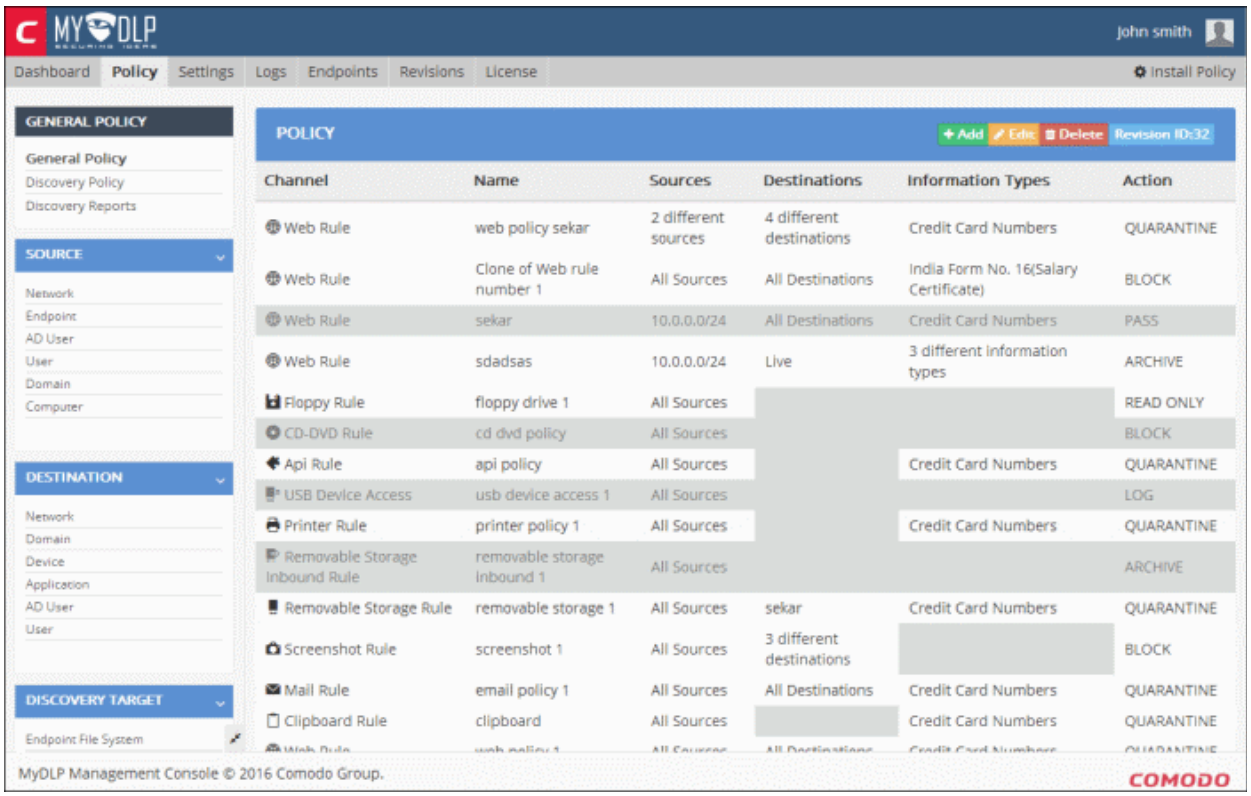
- Web
- Mail
- Select 'Enable Notifications' to enable this feature:
- All eligible admin users added to your account will be listed. Select the ones to which you want to send notifications.
- Recipients can be added by selecting them from the list
- Notifications can be customized from **Settings** > **Enterprise** > Email Notification Message



4.1.4. Adding a Data Transfer Rule

Data transfer policies allow you to enforce traffic control schemes for endpoints in your network. The policy is made up of several rules. Each rule is constructed for intercepting the data traveling over the web, over email and to or from removable storage, or copied to removable storage devices, CDs, DVDs, Floppy disks from specified source user(s), endpoint(s) and to implement the action like allow, block, quarantine or log the data. Rules can also be configured for automatic encryption in a removable device, prohibit use of USB storage devices with specified endpoints, forbidding screenshots for specified application(s) and to prohibit printing of documents containing sensitive data.

The General Policy interface displays the list of rules that are added to the data transfer policy.



The right side of the Policy interface displays the rules with their components as a table and allows the administrator to add new rules, edit existing rules and remove unwanted rules. For more details on the types of the rules and the components of the rules, refer to the section **The Rules Interface**.

The following sections explain on constructing the rules for the policy and implementing them on to the network:

- **Adding a Data Transfer Rule**
- **Enabling or Disabling a Rule**
- **Editing a Rule**
- **Removing a Rule**

Adding a Data Transfer Rule

The rules can be created using the wizard and added to the Policy. Each step is explained in detail after the brief descriptions:

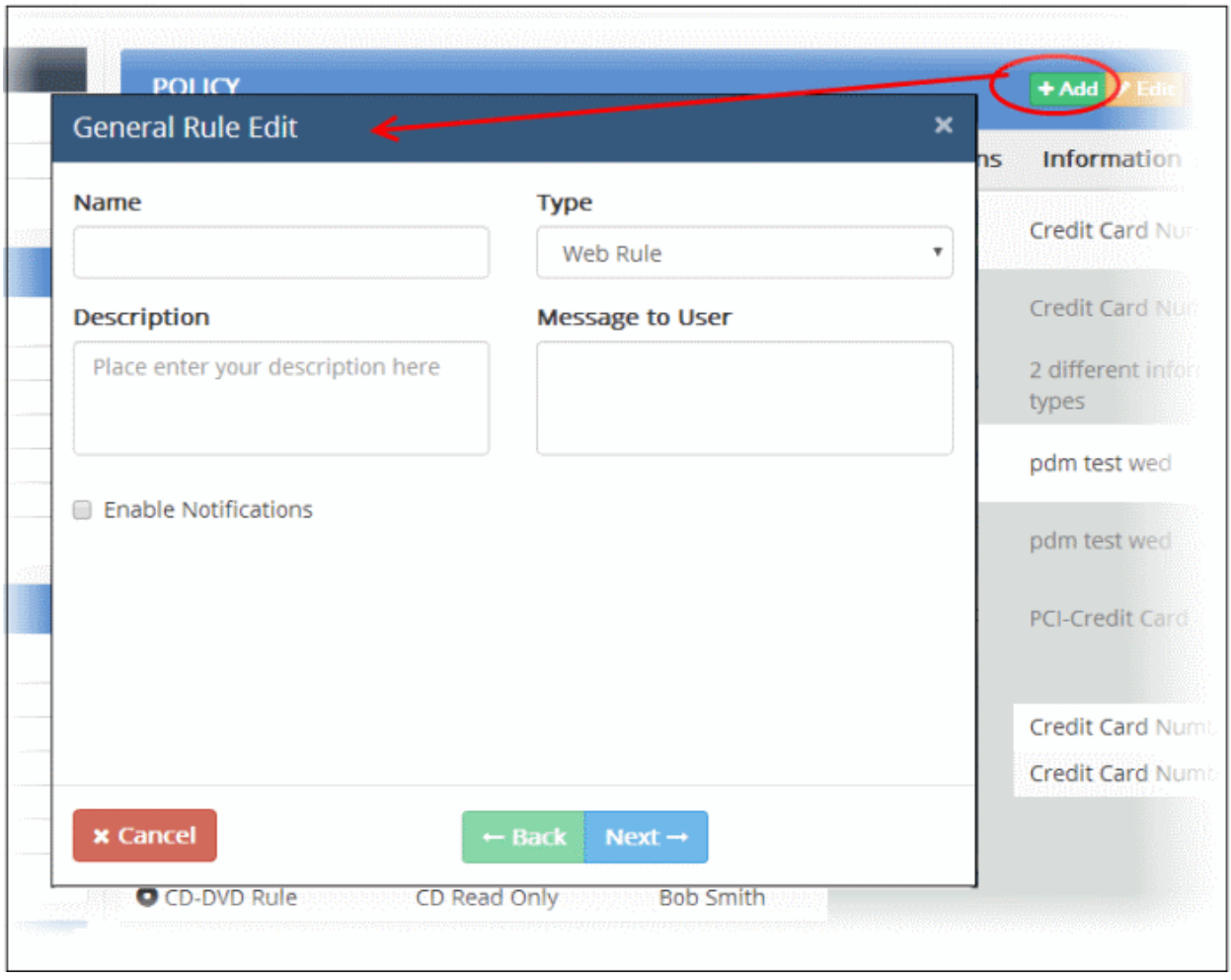
- **Step 1 - Add new rule and select the rule type**
- **Step 2 - Enter a name for the rule and configure messages to be shown to the enduser and email notification sent to the administrator when the rule intercepts the data traffic**

- **Step 3 - Specify the sources for the rule**
- **Step 4 - Specify the Destinations for the rule**
- **Step 5 - Specify the 'Information Types' to be identified and intercepted in the data traffic**
- **Step 6 - Specify the action to be taken on the data if the rule is met**

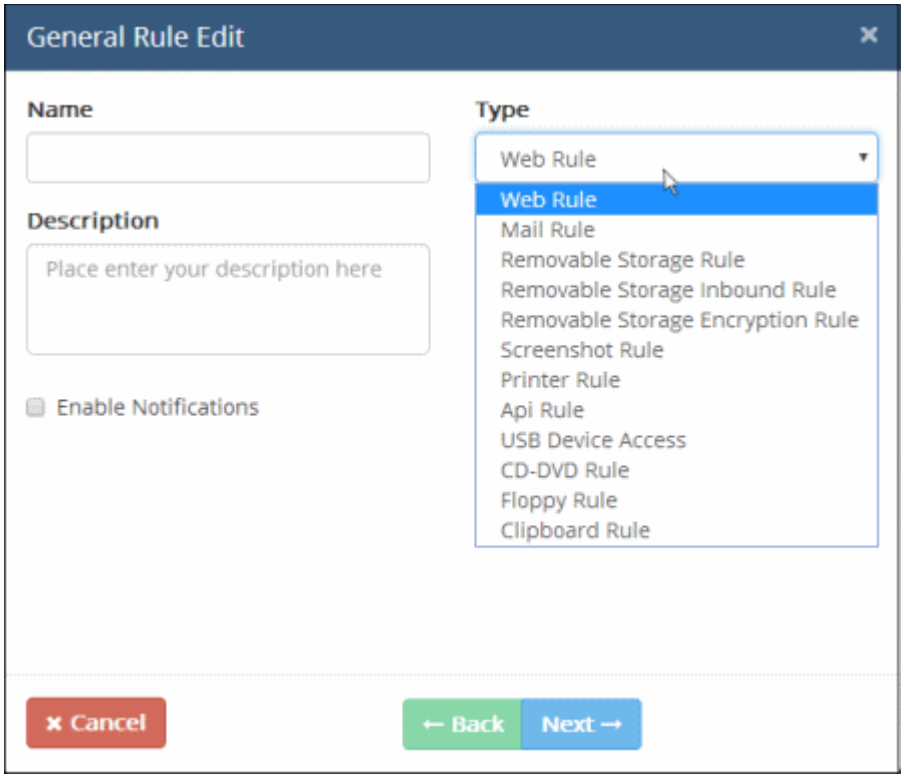
Step 1 – Add a new rule and select the rule type

- To add a new data transfer policy rule, click 'Policy' tab at the top, then 'General Policy' under 'Policy' menu on the left

- Click the 'Add' button from the Policy interface to add a new rule. The 'General Rule Edit' dialog will appear.

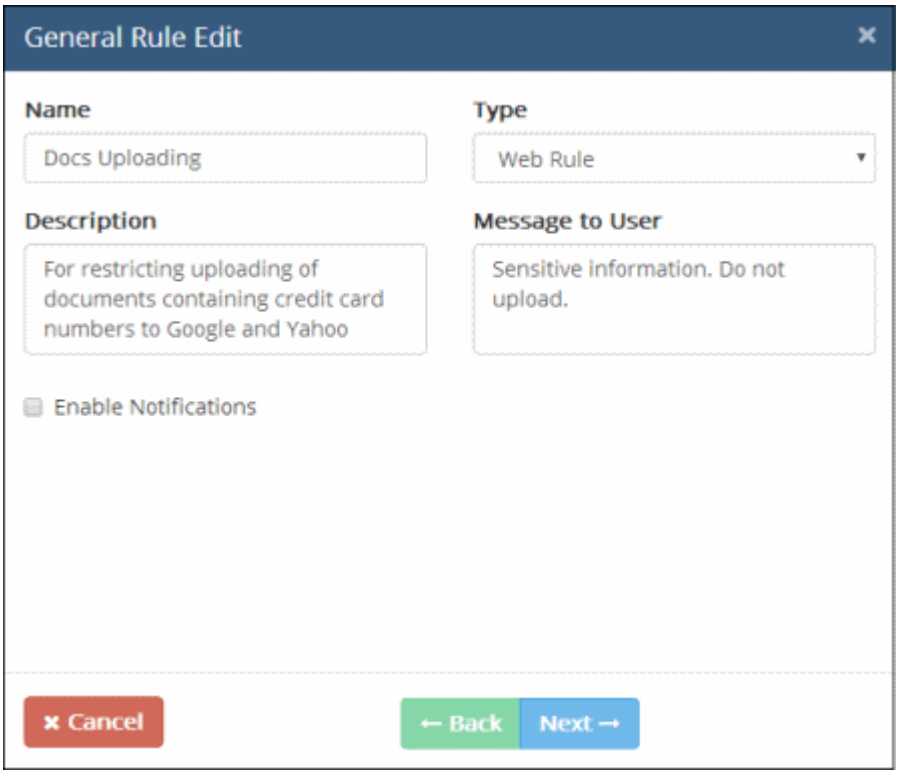


- Select the type of the rule to be created from the 'Type' drop-down. For more details on Rule Types, refer to the section **Rule Channels / Types**.



Step 2 - Enter Name for the rule and configure Messages and Notifications

The 'General Rule Edit' dialog allows to configure the general properties of the rule like the name, descriptions and notifications.



Enter the following information:

- **Name** - Enter a name, shortly describing the new rule
- **Description** - Enter a description for the rule
- **Message to User** - The message to be displayed to the end user when MyDLP blocks or quarantines the data traffic from the user computer based on this new rule.

  MyDLP displays the message for the following rule types:

  - Web Rule
  - Mail Rule

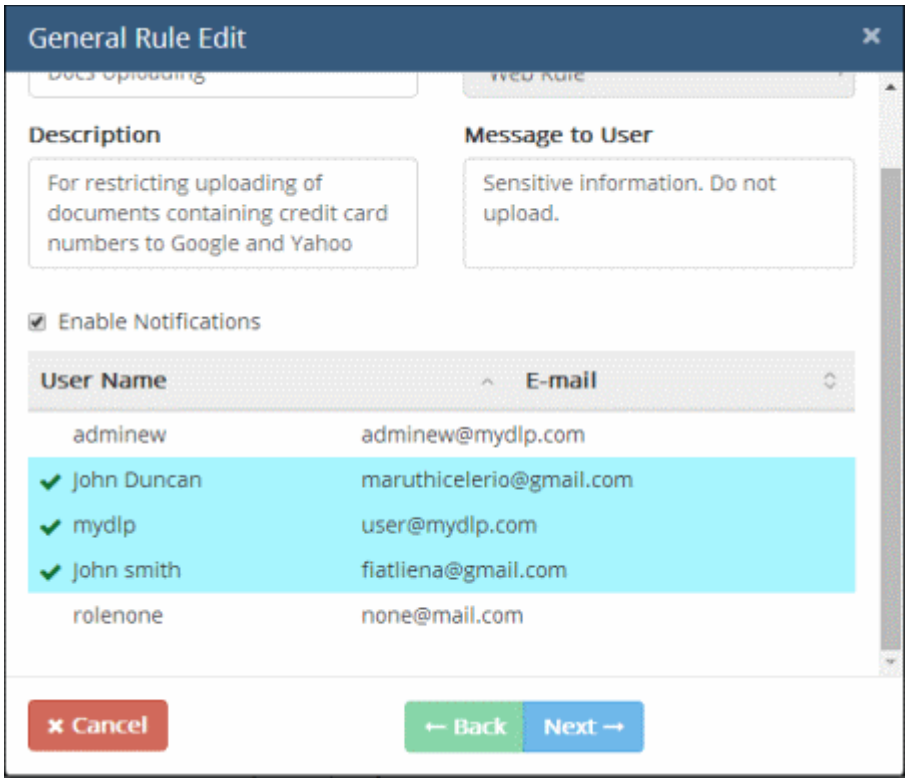
  The message will be displayed only if the action set for the rule is to block or quarantine the intercepted file.

  - For more details on setting the action, refer to the description under '**Step 6 - Specify the action to be taken on the data if the rule is met**'
  - For more details on editing the rule, refer to the section **Editing a Rule**.
- **Notifications** - Configure the automated notifications to be sent to the administrators and other users when MyDLP intercepts the data traffic from any end-user, based on the new rule. This step allows you to choose the notification type and the intended recipients. The notification messages sent to the recipients can be edited under 'Settings' > 'Enterprise' tab. Refer to the section **Configuring Enterprise Settings** for more details.

  MyDLP can send automated notifications only for the following rule types:

  - Web Rule
  - Mail Rule
  - For MyDLP to send automated notification messages, select the 'Enable Notifications checkbox'

The administrators and users lists will be displayed below:



- Select the administrators and other users that have access to the MyDLP interface, to whom the notifications are to be sent
- Click 'Next'.

Step 3- Specify the sources for the rule

The origin of the data transfer can be added as the 'Source' component of the rule, by selecting the source object type from the 'Type' drop-down. The following table shows the object types that can be used for defining Sources and applicable rule types.

Object	Applicable Rule Types
Network	• Web Rule • Mail Rule • Removable Storage Rule • Removable Storage Inbound Rule • Removable Storage Encryption Rule • Printer Rule • Screenshot Rule • API Rule • USB Device Access Rule • CD-DVD Rule • Floppy Rule • Clipboard Rule
Computer Name	• Web Rule • Removable Storage Rule • Removable Storage Inbound Rule • Removable Storage Encryption Rule • Printer Rule • Screenshot Rule • API Rule • USB Device Access Rule • CD-DVD Rule • Floppy Rule • Clipboard Rule
Endpoint	• Web Rule • Removable Storage Rule • Removable Storage Inbound Rule • Removable Storage Encryption Rule • Printer Rule • Screenshot Rule • API Rule • USB Device Access Rule • CD-DVD Rule • Floppy Rule

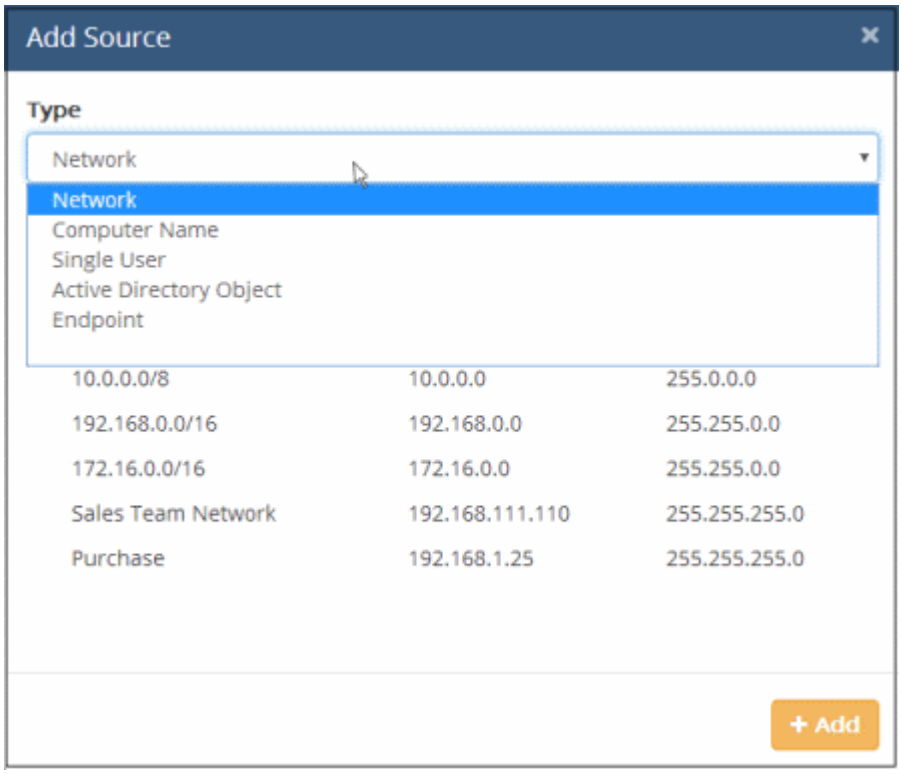
Object	Applicable Rule Types
	• Clipboard Rule
Domain	• Mail Rule
User Object	• Web Rule • Mail Rule • Removable Storage Rule • Removable Storage Inbound Rule • Removable Storage Encryption Rule • Printer Rule • Screenshot Rule • API Rule • USB Device Access Rule • CD-DVD Rule • Floppy Rule • Clipboard Rule
AD User Object	• Web Rule • Mail Rule • Removable Storage Rule • Removable Storage Inbound Rule • Removable Storage Encryption Rule • Screenshot Rule • Printer Rule • API Rule • USB Device Access Rule • CD-DVD Rule • Floppy Rule • Clipboard Rule

To add a source object

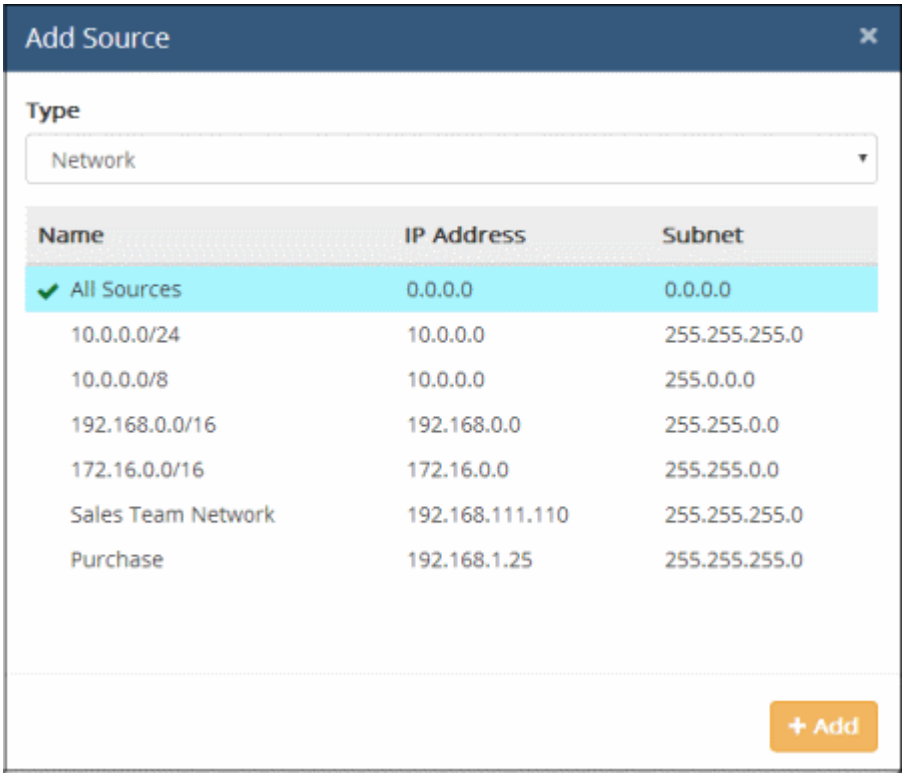
- Click the 'Next' button after selecting the rule type and completing other parameters as explained in Step 2.

The 'Sources' dialog will be displayed:

- Click the 'Edit' button and select the type of source object from the drop-down

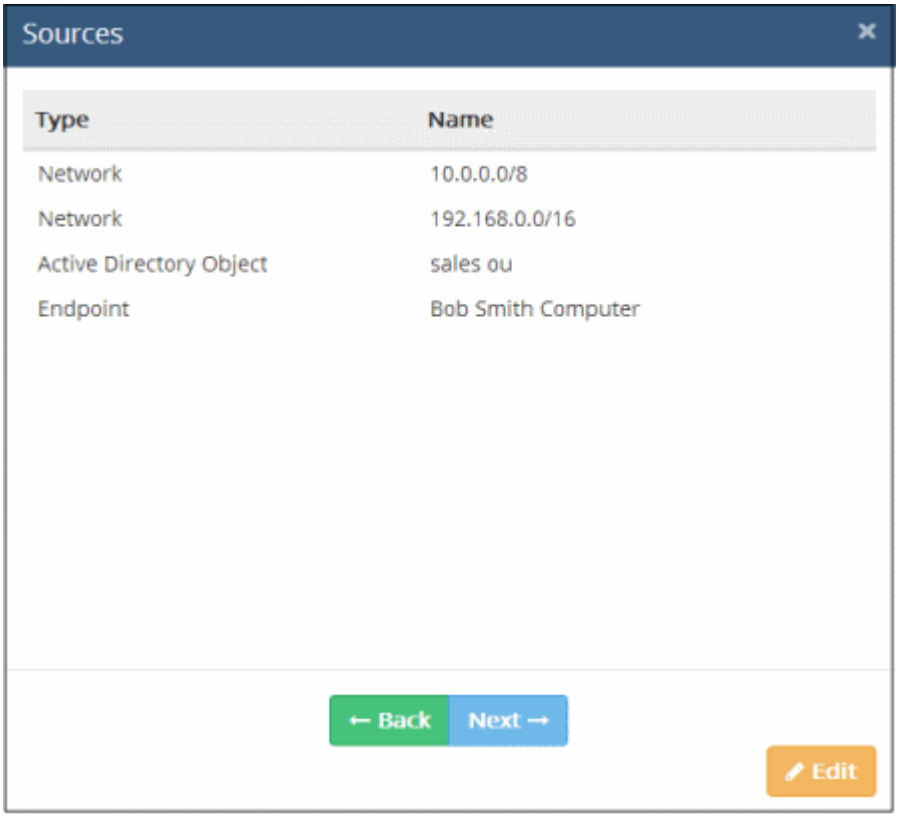


The objects listed for the selected object type depends on the predefined and user defined objects defined for it. Refer to the section **User Defined Objects** for more details. For example, if you choose 'Network', the predefined and user defined network objects will be displayed.



- Select the object(s) from the list
- To add more sources for other object types, select another object type from the 'Type' drop-down again and follow the same procedure explained above.

All the sources added for different object types will be listed.



- Click 'Edit' to add more objects or click 'Next' to proceed to add destinations

Step 4 - Specify the Destinations for the rule

The target of the data transfer can be added as the 'Destination' component of the rule, by selecting the destination object type from the 'Type' drop-down. The following table shows the object types that can be used for defining Destinations and applicable rule types.

Object	Applicable Rule Types
Domain	• Web Rule • Mail Rule
Application Name	• Screenshot Rule
USB Devices with IDs	• Removable Storage Rule
User Object	• Mail Rule
AD User Object	• Mail Rule

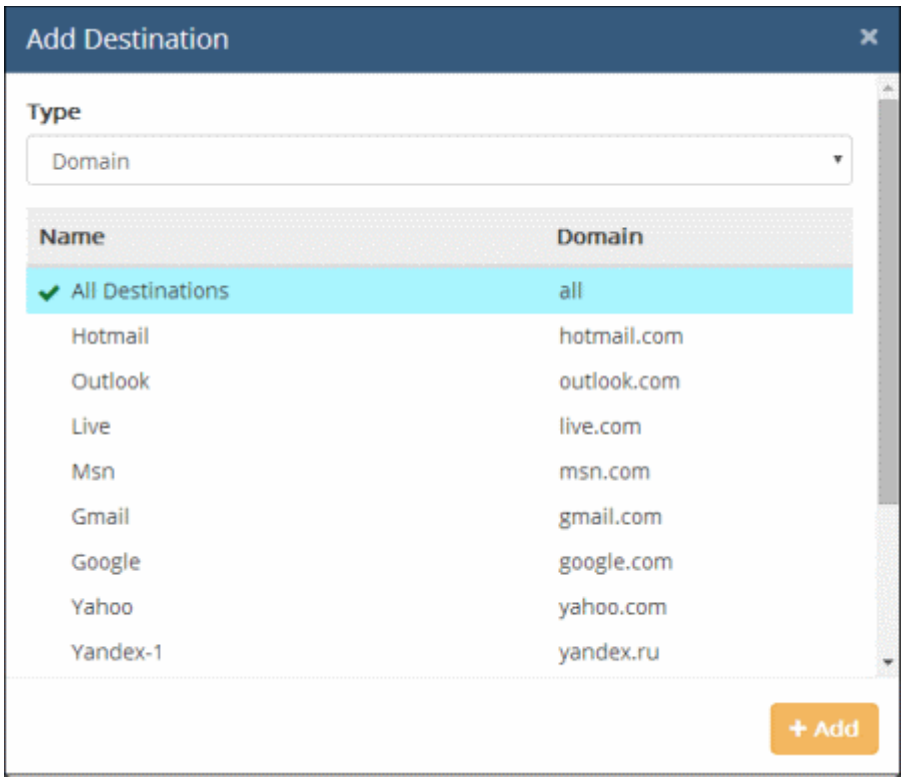
To add a destination object

- Click the 'Next' button after selecting the source and completing other parameters as explained in Step 3

The 'Destinations' dialog will be displayed:

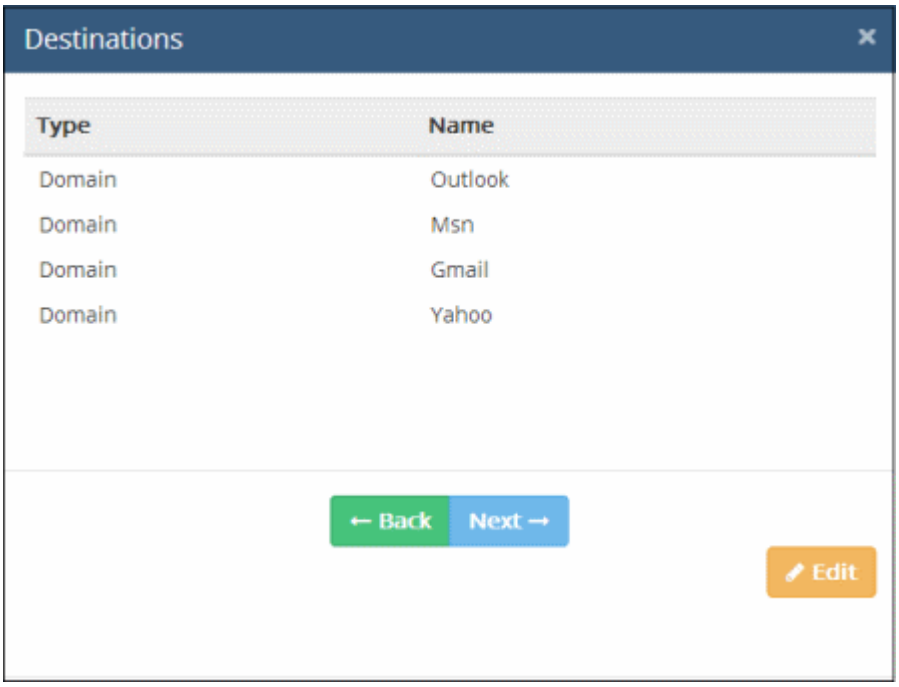
- Click the 'Edit' button and select the type of destination object from the drop-down

The objects listed for the selected object type depends on the predefined and user defined objects defined for it. Refer to the section **User Defined Objects** for more details. For example, if you choose 'Domains', the predefined and user defined domain objects will be displayed.



- Select the object(s) from the list
- To add more destinations for other object types, select another object type from the 'Type' drop-down again and follow the same procedure explained above.

All the destinations added for different object types will be listed.



- Click 'Edit' to add more objects or click 'Next' to proceed add information types

Step 5 - Specify the 'Information Types' to be identified and intercepted in the data traffic

The files to be identified as containing sensitive data in a data traffic, are specified as Information Type in a rule. Each information type is defined with a set of 'Information Features'. For more details on Information Types, refer to the section **Information Types - An Overview**.

MyDLP is shipped with a number of commonly and frequently used Information Types. These information types are available under the 'Pre-defined' category in the 'Information Type' tree. In addition, the administrator can add more number of custom information types.

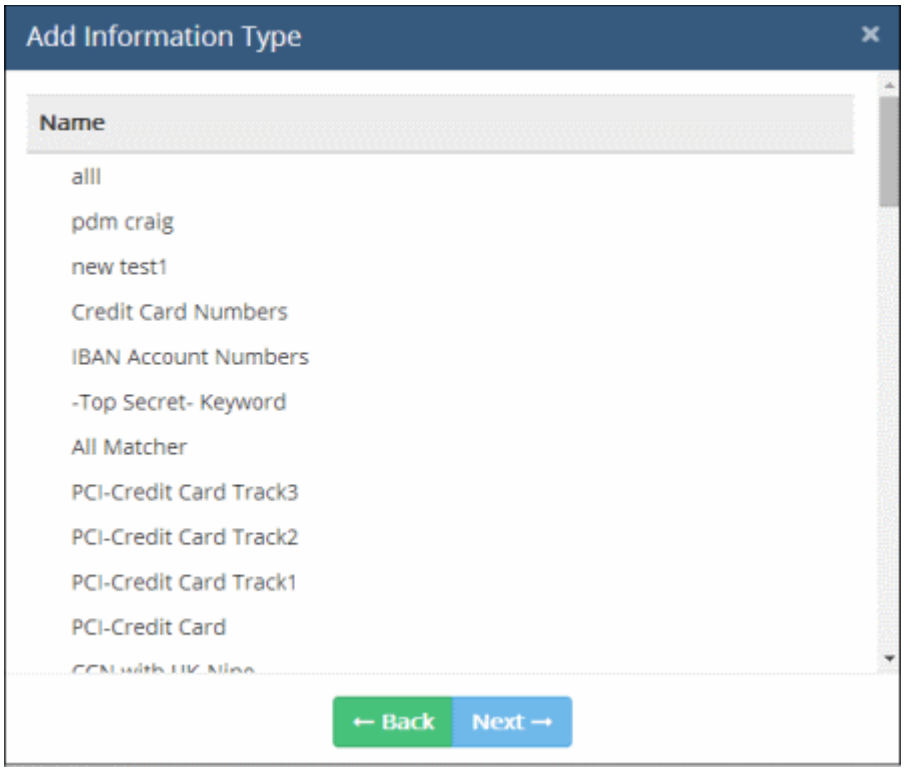
For MyDLP to intercept files containing sensitive data of specific type, the respective information type object is to be added to the rule. The following table shows the object types that can be used for defining Information Types and applicable rule types.

Object	Applicable Rule Types
Information Type	• Web Rule • Mail Rule • Removable Storage Rule • Printer Rule • API Rule • Clipboard Rule

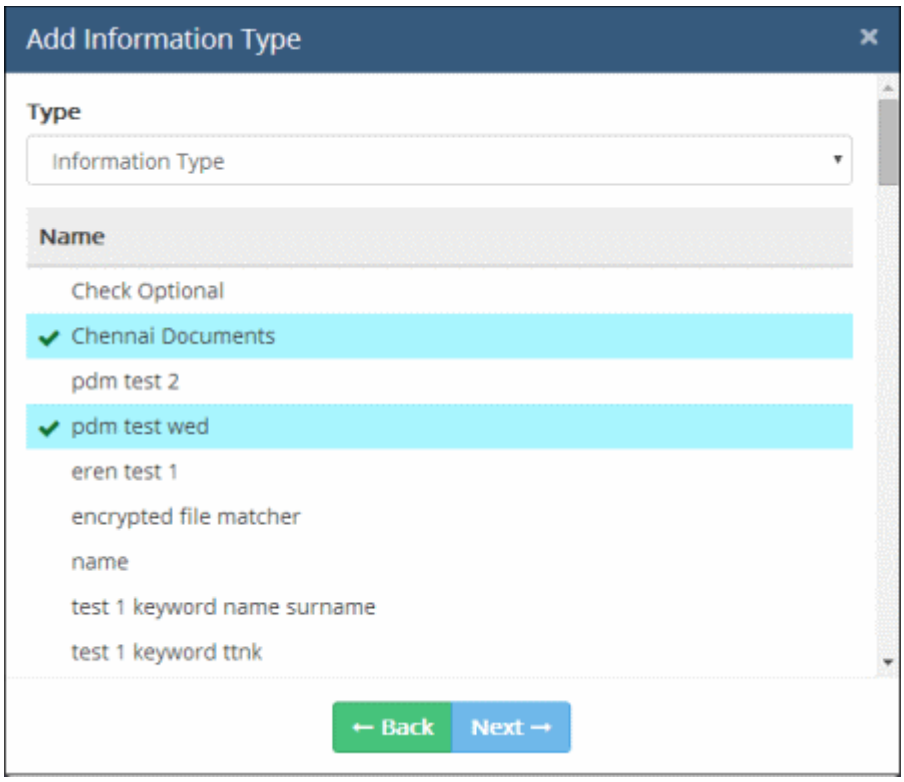
To add an Information Type object

- Click the 'Next' button after selecting the destination type and completing other parameters as explained in Step 4

The 'Add Information' dialog will be displayed:



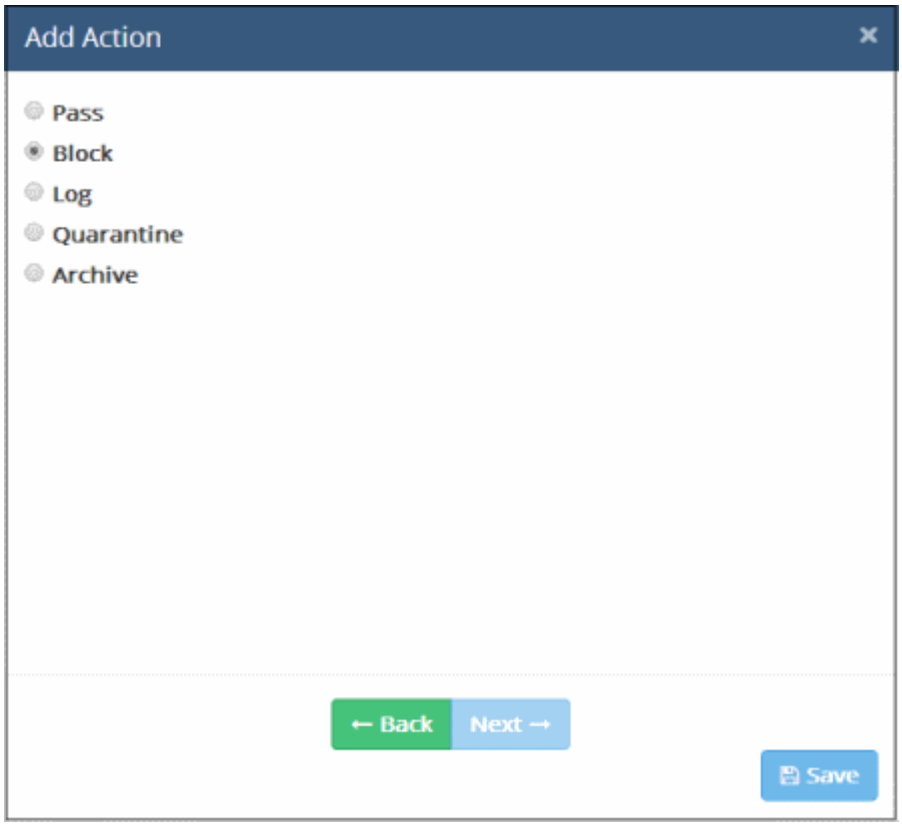
The objects listed for the selected object type depends on the predefined and user defined objects defined for it. Refer to the sections '**Information Types – An Overview**', '**Predefined Information Types**' and '**Adding a User Defined Information Type**' for more details.



- Select the information type(s) from the list
- To add more objects from 'Information Type', select it from the 'Type' drop-down again and follow the same procedure explained above.
- Click 'Next' to proceed to specify the action for the rule

Step 6 - Specify the action to be taken on the data if the rule is met

The final step is to specify the action to be taken on the file as specified in the information type, in the data traffic between the source and the destination.



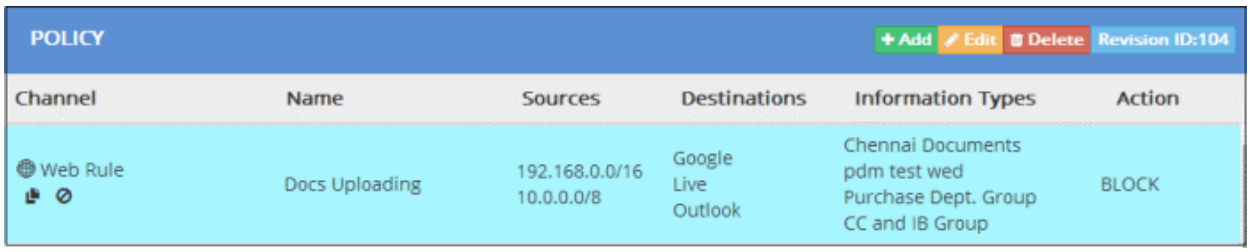
- Choose the action from options. The available actions are:
  - **PASS** - Allows information to pass through the data channel freely without generation of any log entries. This action is is the default action and available for all rule types.
  - **BLOCK** - Prevents information to pass through data channel and generates event log. This action is not available for removable storage inbound rules.
  - **LOG** - Creates a log entry when data passes through the data channel. This action is not available for screenshot rule and Floppy rule.
  - **QUARANTINE** - Prevents information to pass, generates event log and archives a copy of information in the MyDLP Server. The Administrator can download the file from the Logs interface. Refer to the section **Downloading the Files Archived by MyDLP** for more details. This action is not available for removable storage inbound rule, screenshot rule, USB Device Access rule, CD-DVD rule and Floppy rule.
  - **ARCHIVE** - Allows information to pass through data channel, generates event log and archives a copy of information. The Administrator can download the file from the Logs interface. Refer to the section **Downloading the Files Archived by MyDLP** for more details. This action is not available for screenshot rule, USB Device Access rule, CD-DVD rule and Floppy rule.
  - **ENCRYPT** - Enforces encryption of connected removable devices. This action is only available for Removable Storage Encryption Rule.
  - **READ-ONLY** action is available only for CD-DVD rule and Floppy rule. It allows reading and copying of files from optical and magnetic storage disks like CD, DVD and Floppy disks but does not allow copying of data from the endpoints to the disks. This action is available for CD-DVD Rule and Floppy Rule.
- At any time during the rule creation, click 'Back' to review your configuration for the rule
- Click 'Save'

The rule will be saved. You can create as many rules as required. If you are creating a new rule with minor changes from an existing rule, you can clone the rule and edit it to change the required parameters.

The rules take effect only on applying/reapplying the policy to the network. Refer to the section **Deploying the Policy** for more details.

Once a rule is added you can edit, clone, delete, disable/enable it at any time.

- Click on the rule to view the control buttons displayed in the Channel column



The expanded rule is displayed in cyan color and provides full component details available for the rule under Sources, Destination and Information Types columns.

Control	Description
+ Add	Allows administrators to add a new rule
Edit	Enables the administrator to edit the name, message and notification settings of the rule. Refer to the section **Editing a Rule** for more details,
Delete	Removes the rule from the policy. Refer to the section **Removing a Rule** for more details
	Available in an expanded rule. Clones the rule to allow administrators to create a new rule with minor changes in the components
	Available in an expanded rule. Enables the administrator to disable or enable the rule. Refer to the section **Enabling or Disabling a rule** for more details.

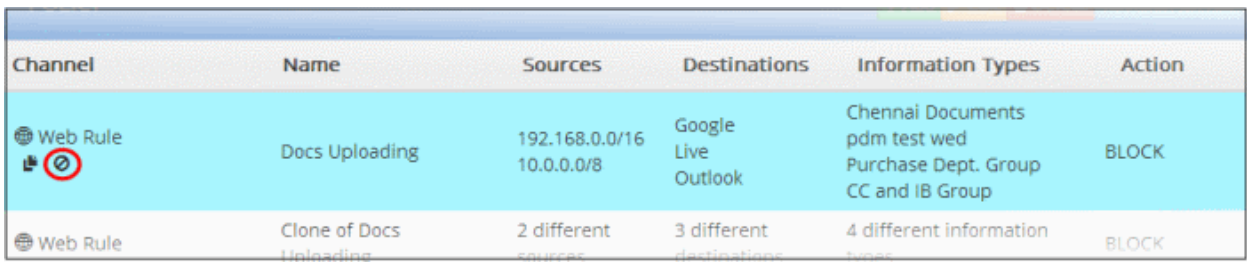
Rules at the top of the table have a higher priority than those at the bottom and are applied first. In the event of a conflict between rules, the setting in the rule nearer the top of the table will be applied. The administrator can change the order of the rules at any time by dragging any rule to the desired position.

Enabling or Disabling a Rule

The rules added to the policy are automatically enabled by default. The administrator can disable a rule if it is found unnecessary and deemed to be of use at a later time. The disabled rules are gray in color in the table.

To disable / disable a rule

- Click on the rule for the options to be displayed in the 'Channels' column
- Click the Disable icon



The rule will be disabled and the background color will change to gray.

- To re-enable the rule, click the 'Enable' icon.

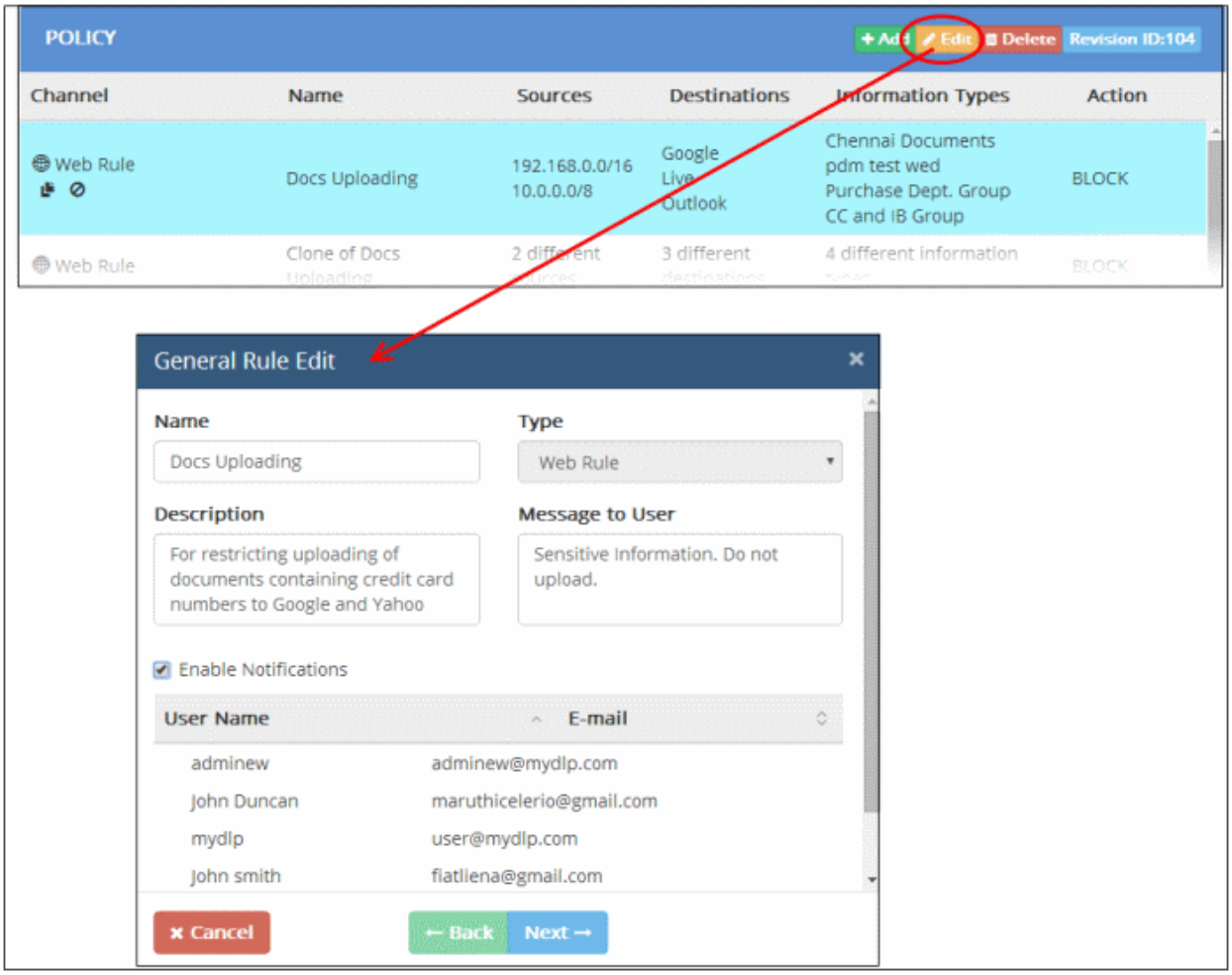
Editing a Rule

A rule can be edited at anytime for the changes in the source, destination, information type components, the action to be taken, the name of the rule and the notification settings. Please note that only rules that are enabled can be edited.

Any change you make in a rule will take effect only on re-deployment of the policy. Refer to the section **Deploying the Policy** for more details on implementing the policy.

To edit a rule

- Select the rule and click the 'Edit' button at the top



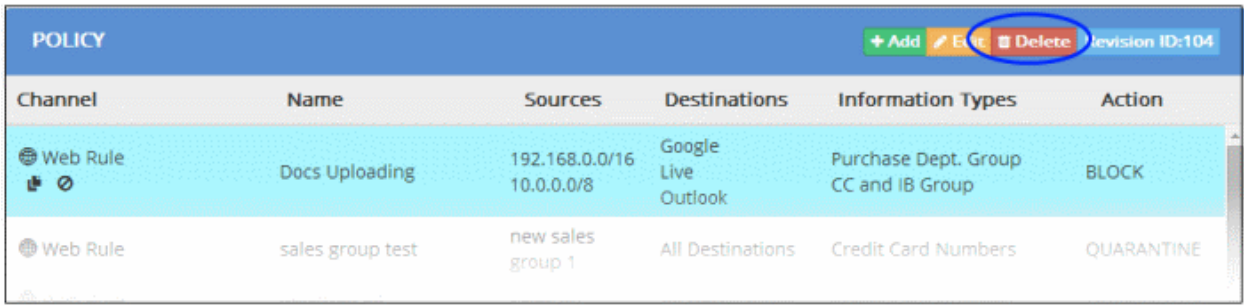
You can edit the 'Name', 'Description', 'Message to User', 'Notification', settings, add new source, destination and information types. Please note you can not edit the rule type. The interface is same as the 'Edit Dialog' that appear while creating the rule. Refer to the rule creation wizard from **Step 2** onward till the final step for more details.

Removing a Rule

The administrator can remove unwanted rules from the policy at any time.

To remove a rule

- Select the rule and click the 'Delete' button at the top

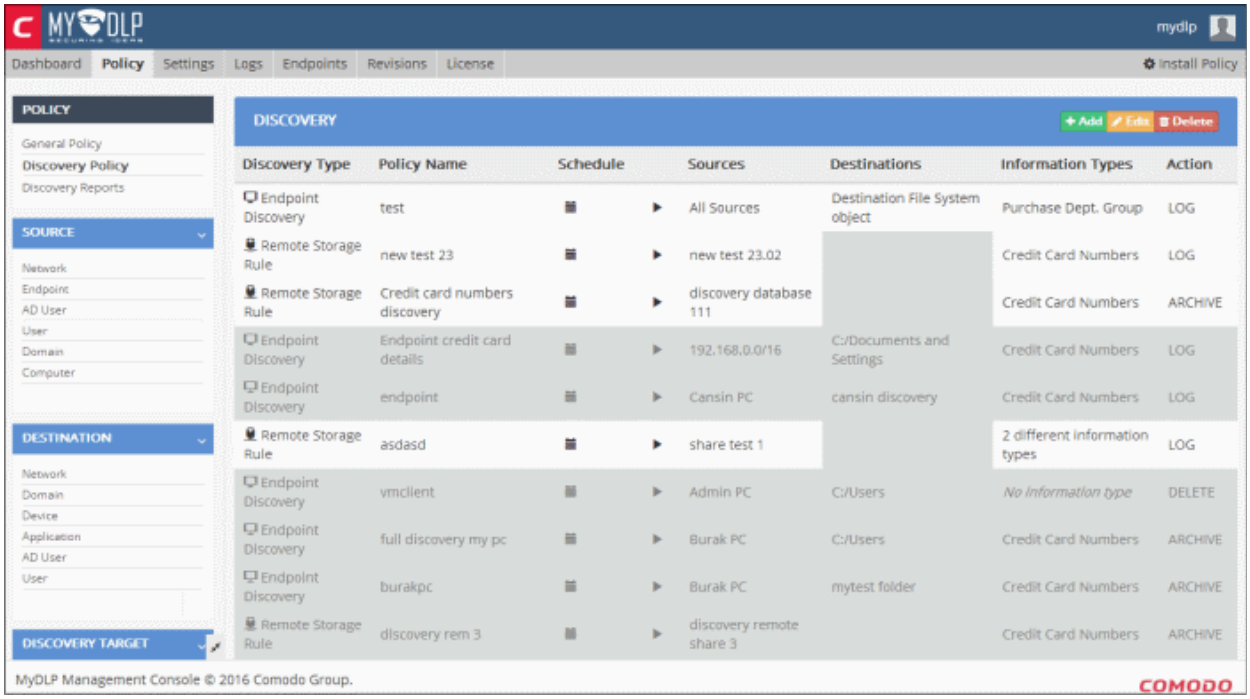


A confirmation dialog will be displayed.

- Click 'Yes' to remove the rule.

4.1.5. Adding a Data Discovery Rule

Comodo MyDLP can run scheduled scans on network endpoints and storage locations to identify files containing sensitive information. The targets, schedule, information searched for, and the action to be taken is specified in a Discovery Rule.



The right side of the interface displays all previously created discovery rules. Collectively, these rules are known as the 'Discovery Policy' and administrators can add new rules, edit existing rules and remove unwanted rules. The administrator can also run on-demand scans from this area. A list of reports from previous scans is available under 'Discovery Reports' section. For more details on rule types and components, refer to **The Rules Interface**.

The following sections explain more about rule construction and implementation:

- **Adding a Data Discovery Rule**
- **Enabling or Disabling a Rule**
- **Editing a Rule**

- **Removing a Rule**
- **Running On-Demand Scans**
- **Viewing Discovery Scan Reports**

Adding a data discovery rule

Discovery rules are intended to identify data residing on selected endpoints and on remote storage locations like FTP servers, shared folders, network file systems and web servers.

- A Discovery rule is constructed from a channel, a source, a schedule, a destination, an information type and an action to be taken if the rule is triggered.
- Administrators can create an unlimited number of rules to search specific targets for specific information types.
- Rules can be run 'on-demand' by clicking the ▶ icon next to 'Schedule'.

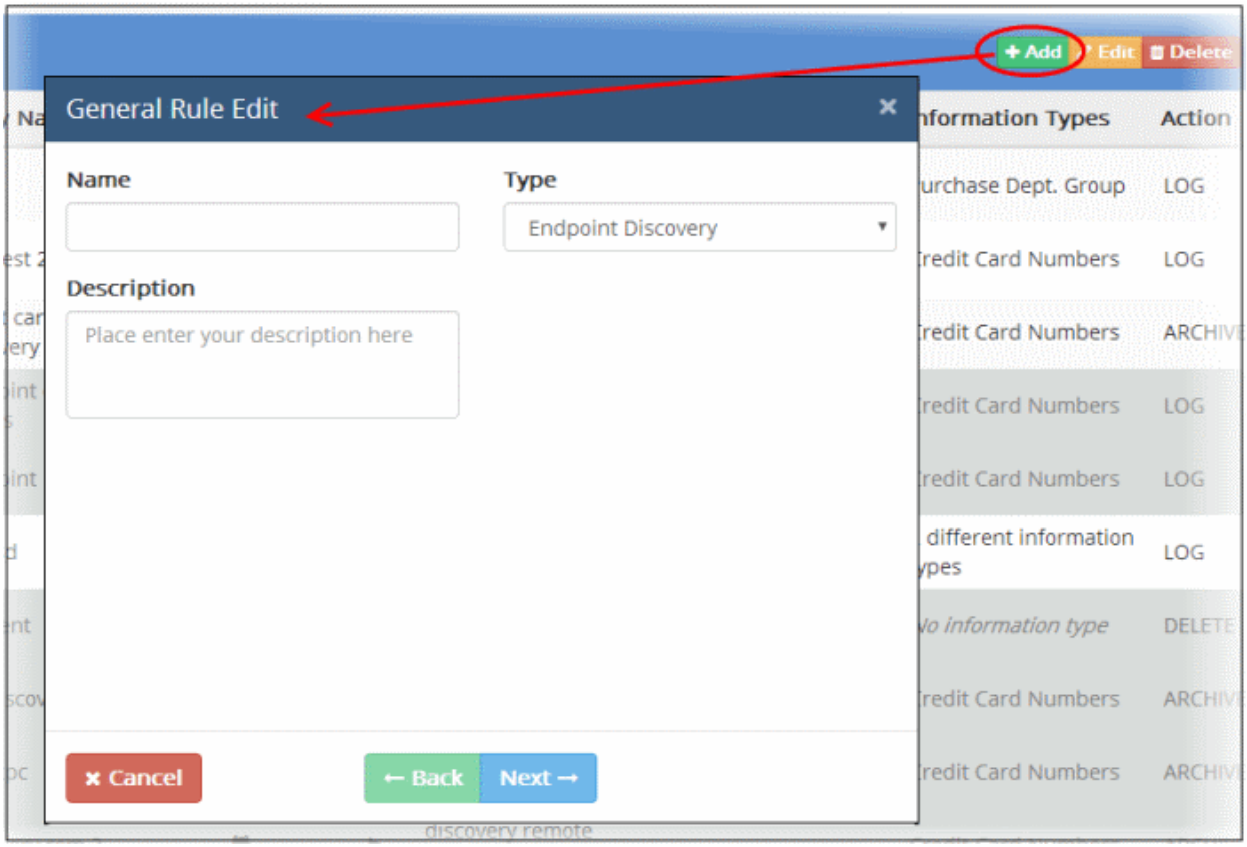
Rules can be created using the wizard and added to the Policy. Each step is explained in detail after the brief descriptions:

- **Step 1 - Add new rule and select the rule type**
- **Step 2 - Enter a name and description for the rule**
- **Step 3 - Specify the sources for the rule**
- **Step 4 - Specify the destinations for the rule**
- **Step 5 - Specify the 'Information Types' to be identified**
- **Step 6 - Specify the action to be taken on the data if the rule is met**
- **Step 7 – Create a schedule for running scans as per the rule**

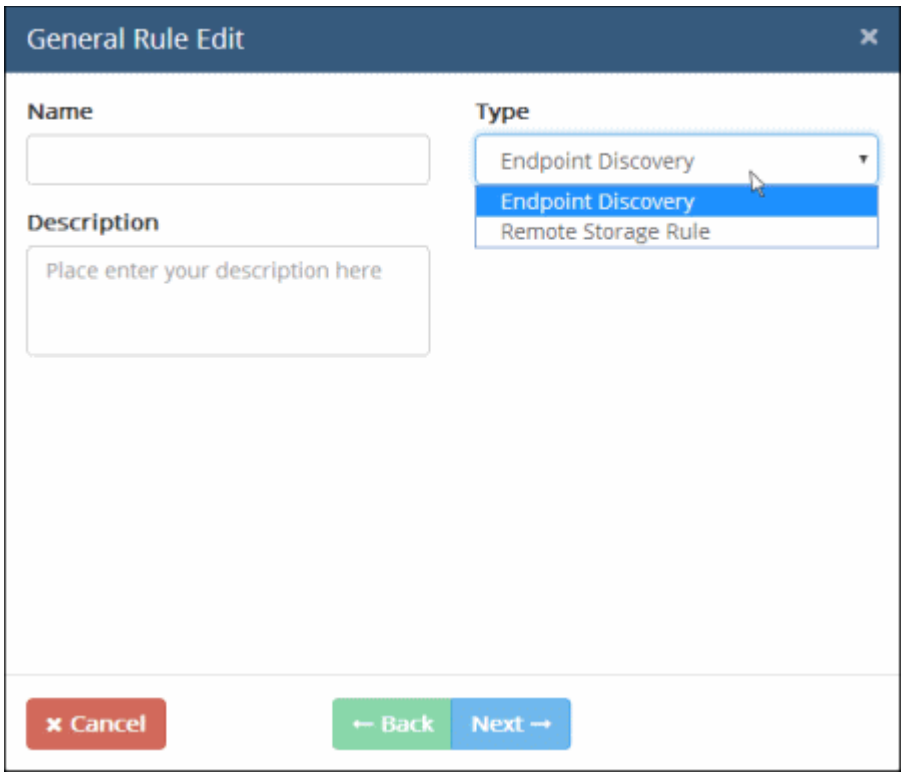
Step 1 – Add new rule and select the rule type

- To add a new data discovery policy rule, click the 'Policy' tab at the top, then 'Discovery Policy' under 'Policy' menu on the left

- Click the 'Add' button from the Policy interface to add a new rule. The 'General Rule Edit' dialog will appear.

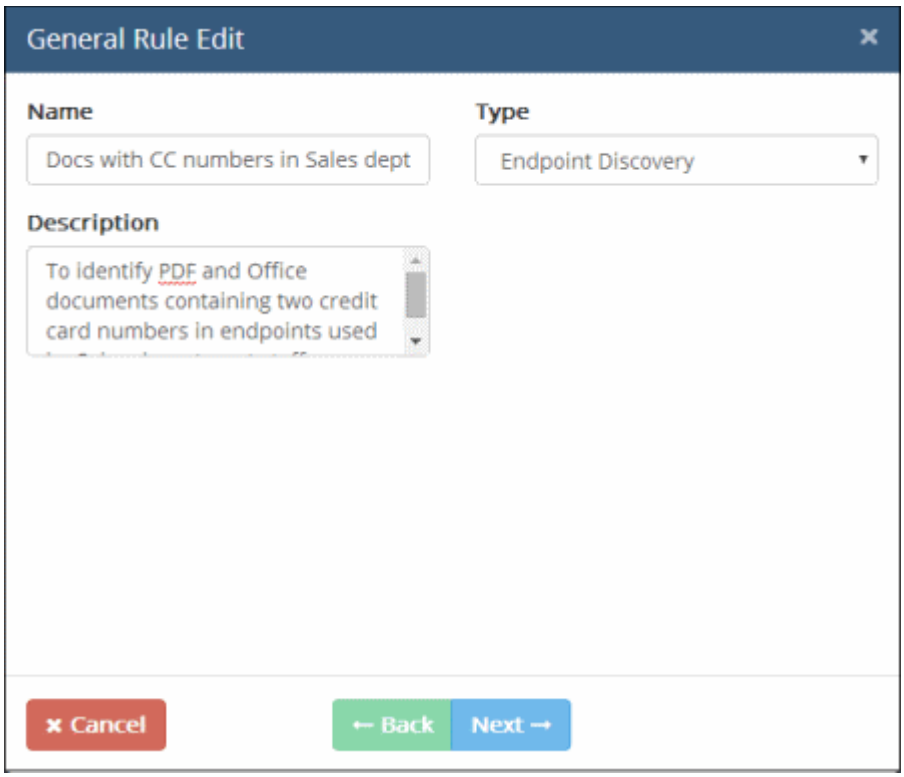


- Select the type of the rule, Endpoint Discovery' or 'Remote Storage Rule' to be created from the 'Type' drop-down. For more details about these rule types, refer to the section **Rule Channels / Types**.



Step 2 – Enter a name and description for the rule

After selecting the type of discovery rule, enter a name and description for the rule.



- Click 'Next'.

Step 3 – Specify the sources for the rule

The 'Source' component of a rule is where you specify the location to be scanned, like selected endpoints or remote storage. The following table shows the object types that can be used for defining Sources and applicable rule types:

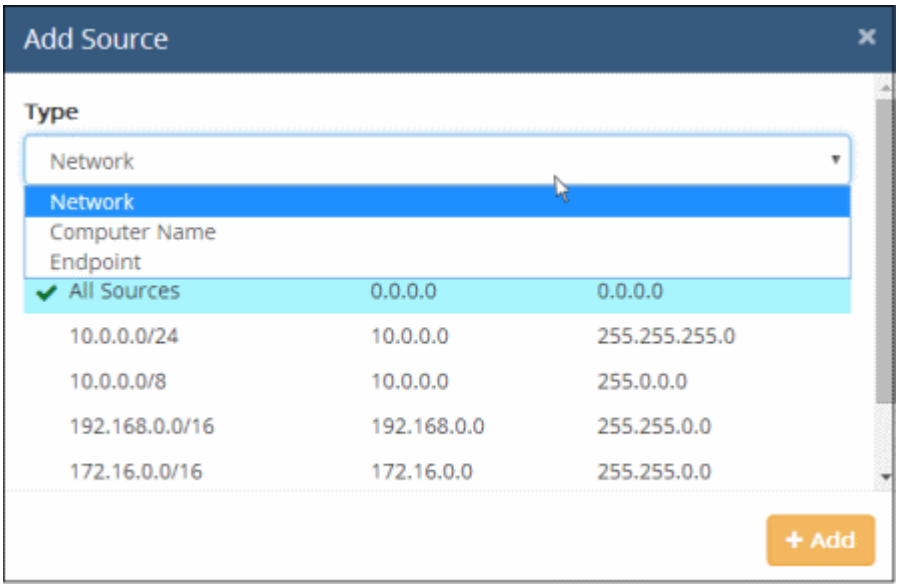
Object	Applicable Rule Types
Network	• Endpoint Discovery rule
Computer Name	• Endpoint Discovery rule
Endpoint	• Endpoint Discovery rule
Remote Storage	• Remote Storage rule

To add a source object

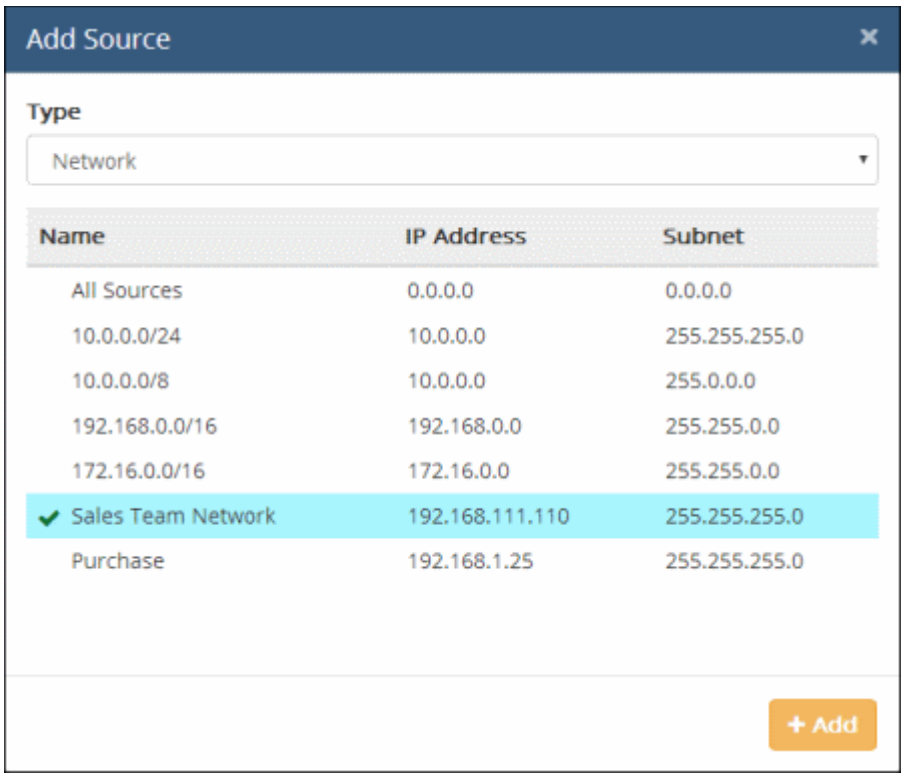
- Click the 'Next' button after selecting the rule type and completing other parameters as explained in Step 2

The 'Sources' dialog will be displayed:

- Click the 'Edit' button and select the type of source object from the drop-down

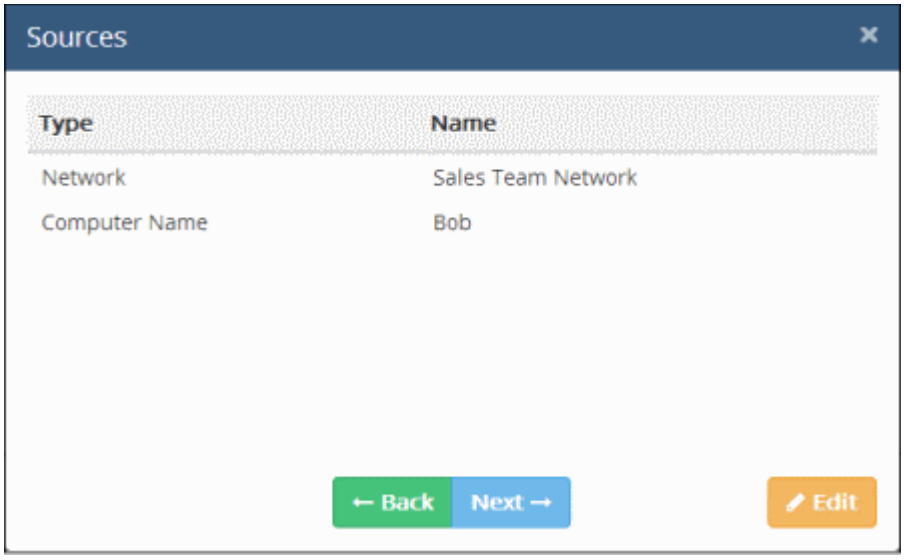


The objects listed for the selected type depend on the objects defined for it (both predefined and user defined objects). Refer to the section **User Defined Objects** for more details. For example, if you choose 'Network', the predefined and user defined network objects will be displayed.



- Select an object(s) from the list
- To add more sources for other object types, select another object type from the 'Type' drop-down again and follow the same procedure explained above.

All the sources added for different object types will be listed.



- Click 'Edit' to add more objects or click 'Next' to proceed to add destinations

Step 4 – Specify the destinations for the rule

The 'Destination' component of a discovery rule is where you specify the target folder to be scanned in the selected endpoints. The destination can be specified only for Endpoint Discovery rule. For the Remote Storage rule, MyDLP scans the full storage for the information type specified in the rule, hence, you need not specify the destination component.

You can add destinations by selecting a pre-defined or user-defined 'File System Directory' object from the 'Type'

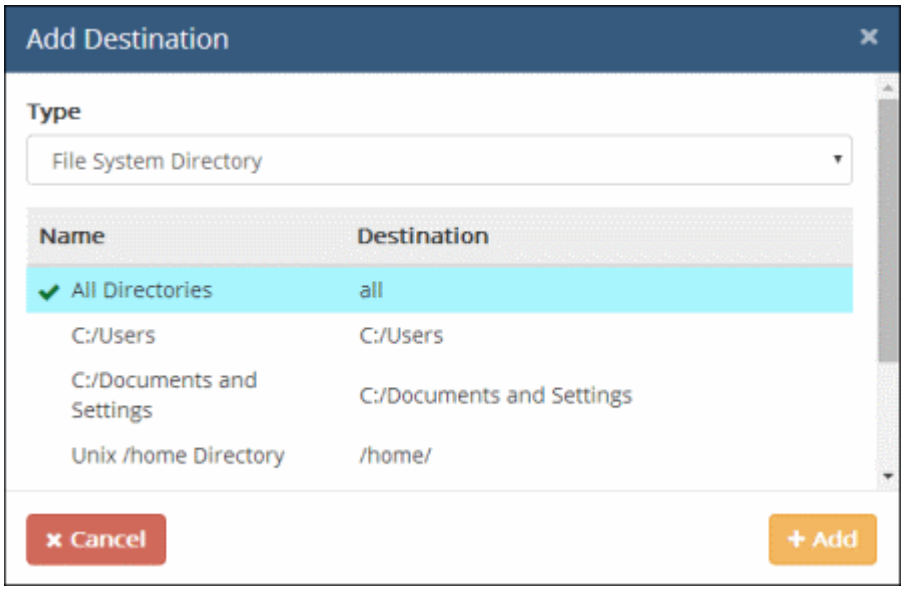
drop-down.

To add a destination object

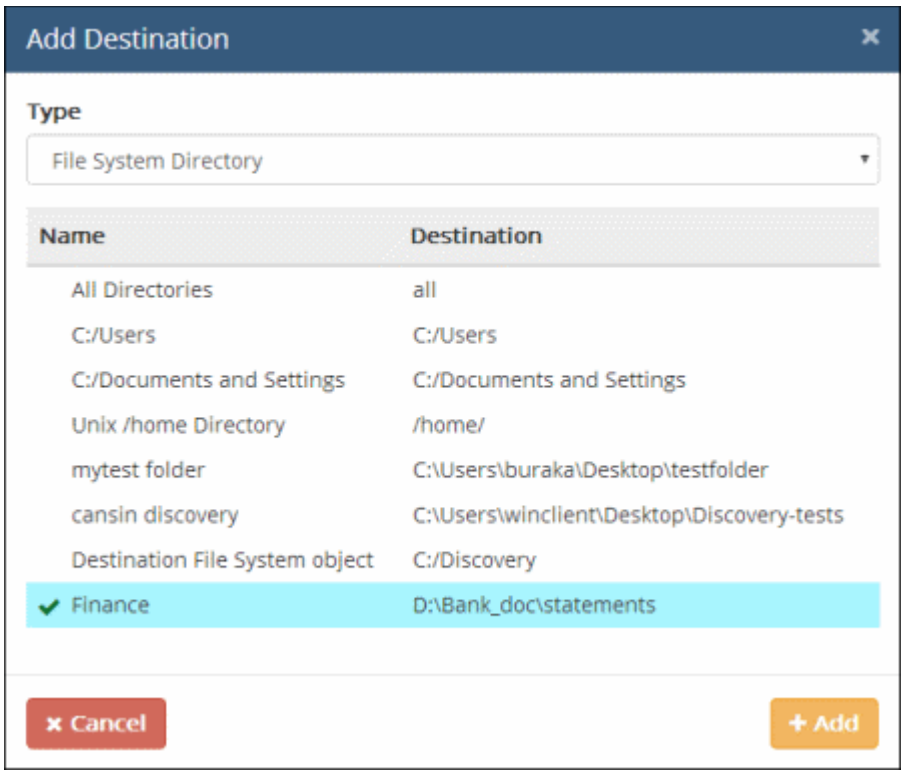
- Click the 'Next' button after selecting the source and completing other parameters as explained in Step 3

The 'Destinations' dialog will be displayed:

- Click the 'Edit' button and select the type of destination object from the drop-down

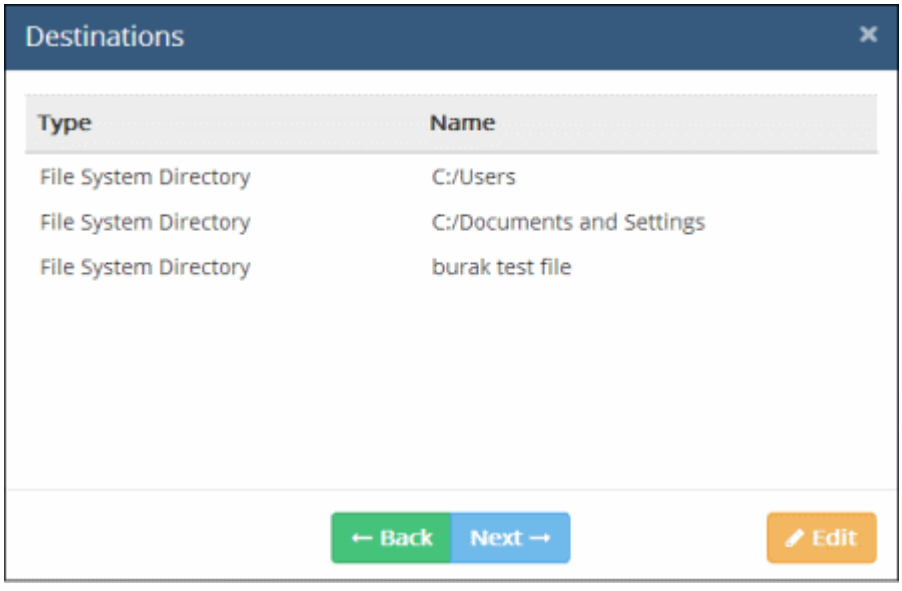


The objects listed for the selected object type depends on the predefined and user defined objects defined for it. Refer to the section **User Defined Objects** for more details. For example, if you choose 'File System Directory', the predefined and user defined file system objects will be displayed.



- Select an object(s) from the list
- To add more destinations for other object types, select another object type from the 'Type' drop-down again and follow the same procedure explained above and click 'Add'

All the destinations added will be listed.



- Click 'Edit' to add more objects or click 'Next' to proceed to add information types

Step 5 – Specify the 'Information Types' to be identified

The files to be identified as containing sensitive data in a data storage, are specified as Information Type in a rule. Each information type is defined with a set of 'Information Features'. For more details on Information Types, refer to the section **Information Types - An Overview**.

MyDLP is shipped with a number of commonly and frequently used Information Types. These information types are

available under the 'Pre-defined' category in the 'Objects' tree. In addition, the administrator can add more number of custom information typed under 'User-defined' category.

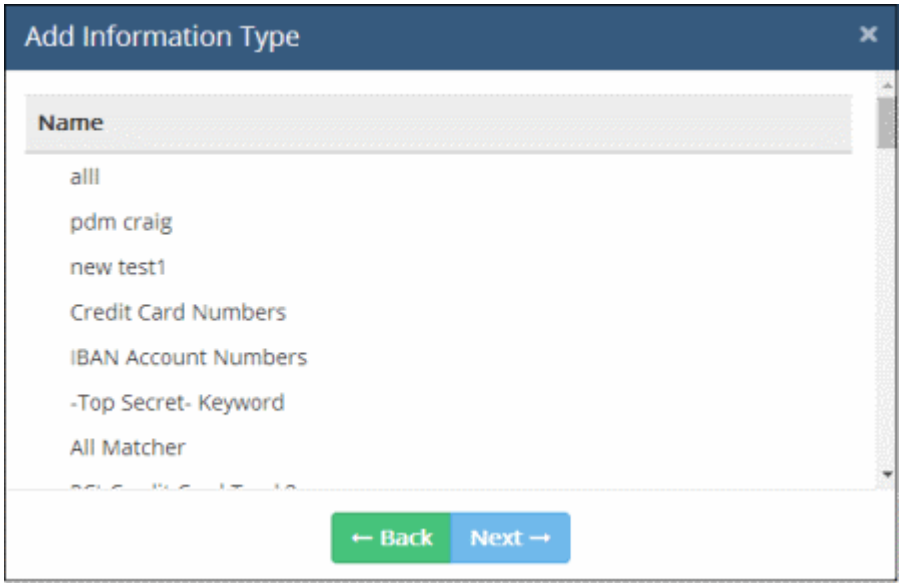
For MyDLP to identify files containing sensitive data of specific type, the respective information type object is to be added to the rule. The following table shows the object types that can be used for defining Information Types and applicable rule types.

Object	Applicable Rule Types
Information Type	• Endpoint Discovery Rule • Remote Storage Rule

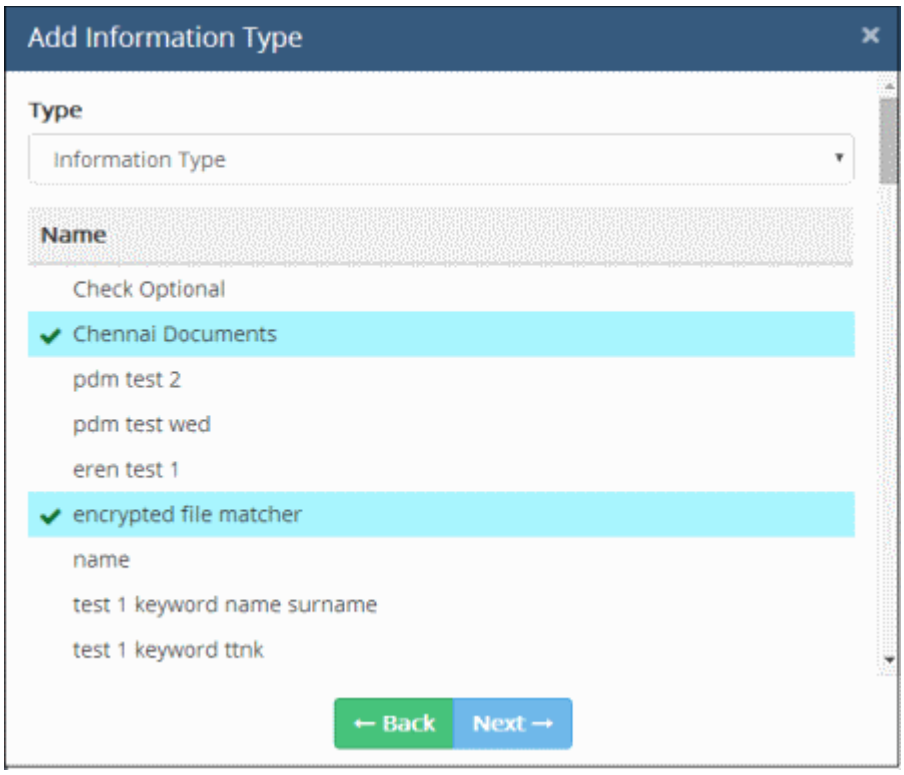
To add an Information Type object

- Click the 'Next' button after selecting the destination type and completing other parameters as explained in Step 4

The 'Add Information' dialog will be displayed:



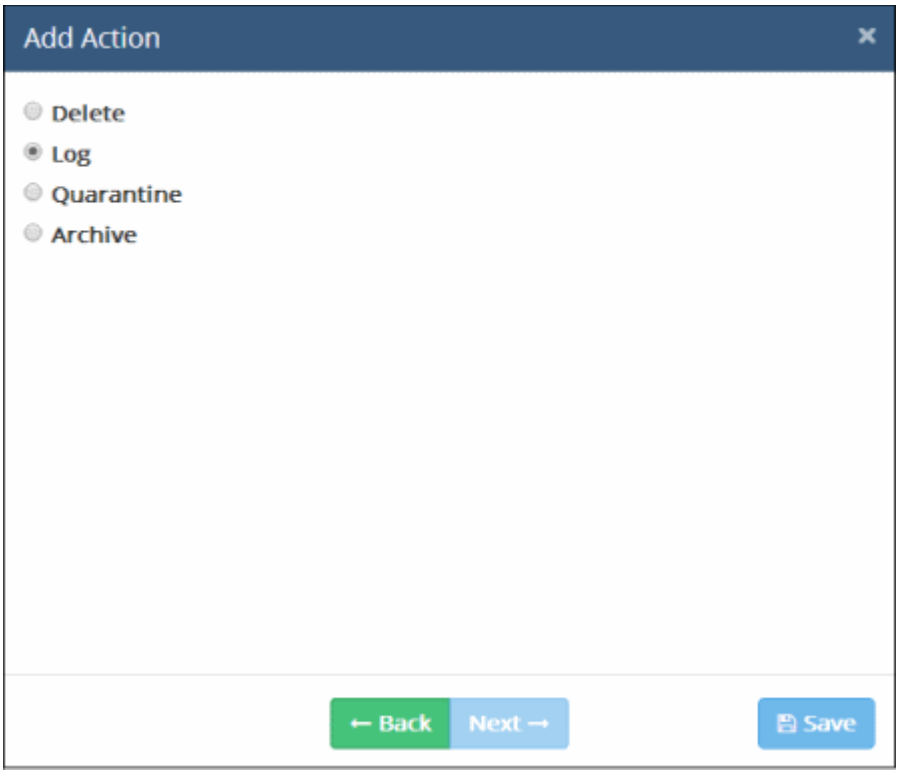
The objects listed for the selected object type depends on the predefined and user defined objects defined for it. Refer to the sections '**Information Types – An Overview**', '**Predefined Information Types**' and '**Adding a User Defined Information Type**' for more details. For example, if you choose 'Information Type', the predefined and user defined information objects will be displayed.



- Select the information type(s) from the list
- To add more objects from 'Information Type' select it from the 'Type' drop-down again and follow the same procedure explained above.
- Click 'Next' to proceed to specify the action for the rule

Step 6 – Specify the action to be taken on the data if the rule is met

The next step is to specify the action to be taken on the file identified from the storage.



- Choose the action from the options. The available actions are:
    - **DELETE** - Deletes matched discovered files. It is advised to use this action very carefully. This action is available only for Endpoint Discovery Rules.
    - **LOG** - Generates event log.
    - **QUARANTINE** - Removes the identified file from the endpoint and saves an archive copy in the MyDLP server. The Administrator can download the file from the Logs interface. Refer to the section **Downloading the Files Archived by MyDLP** for more details.
    - **ARCHIVE** - Generates event log and archives a copy of information. The Administrator can download the file from the Logs interface. Refer to the section **Downloading the Files Archived by MyDLP** for more details.

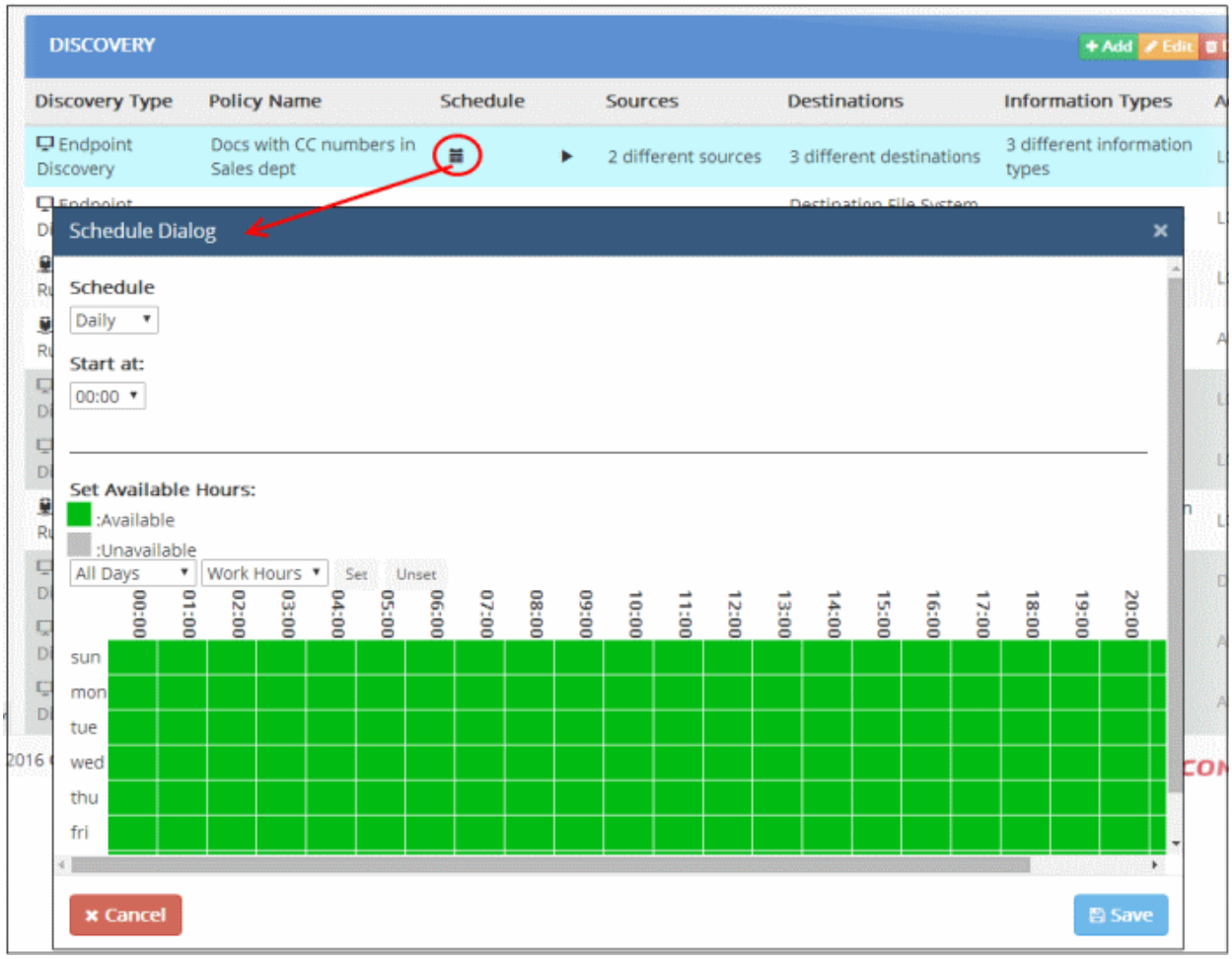
The rule will be saved. You can create as many rules as required. If you are creating a new rule with minor changes from an existing rule, you can clone the rule and edit it to change the required parameters.

Step 7 – Create a schedule for running scans as per the rule

The final step is to set a schedule for MyDLP to periodically scan the endpoints and storage locations.

To set a scan schedule in a rule

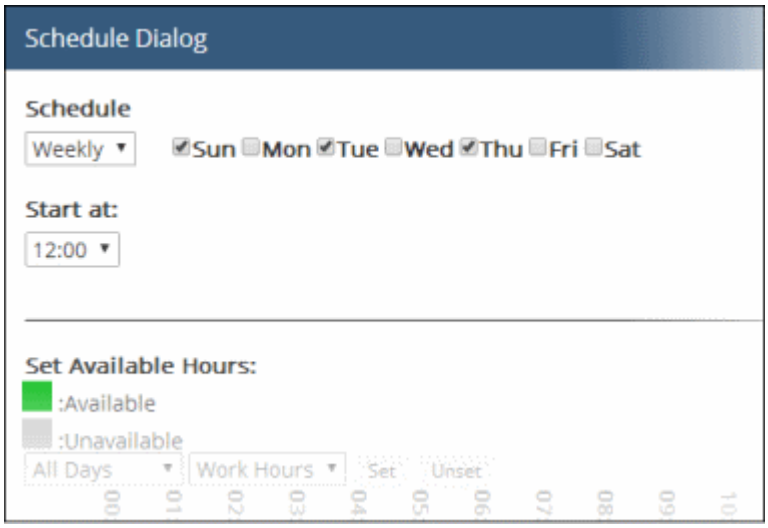
- Click the Calendar button under the Schedule column.



The 'Schedule' dialog will appear, enabling you to set a schedule.

Schedule

- Select whether you wish the scans to be run on daily or weekly basis from the drop-down. If you are choosing Weekly, then select the days at which the schedule needs to be run.



- Start at - Select the time at which the scan should commence.

Available/Unavailable Hours

You can also specify when the endpoints and the network repositories will be available for MyDLP scans, so that the scans scheduled at the periods at which the endpoints and the repositories are not available, will be skipped.

The table below 'Available/Unavailable Hours' indicate the time periods at which the endpoints/repositories will be available/unavailable:

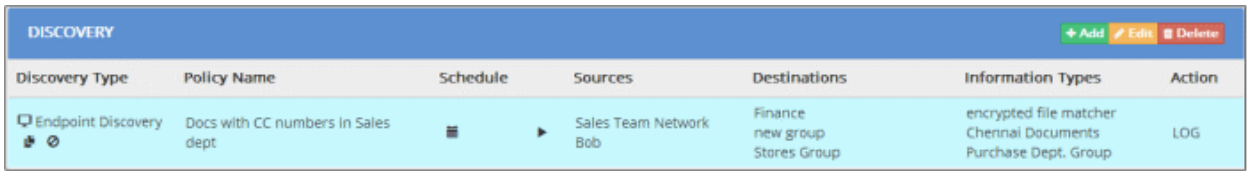
- Green blocks indicate that the endpoints/repositories are available for scanning
- Gray blocks indicate that the endpoints/repositories are not available for scanning

- To manually switch specific hours of days at which the endpoints/repositories will be unavailable, click the respective blocks.
- To automatically set specific time periods as unavailable hours,
  - Choose the day(s) of the week from the first drop-down.
  - Choose the hours from the second drop-down
  - Click 'Unset'
- To automatically set specific time periods as available hours,
  - Choose the day(s) of the week from the first drop-down.
  - Choose the hours from the second drop-down
  - Click 'Set'
- Click 'Save' to save the schedule

The rules take effect only on applying/reapplying the Discovery policy to the network. Refer to the section **Deploying a Policy** for more details.

Once a rule is added you can edit, copy delete, disable/enable it at any time.

- Click on the rule to view the control buttons displayed in the Channel column



Control	Description
+ Add	Allows administrators to add a new rule
Edit	Enables the administrator to edit the name, source, destination, information type and action settings of the rule. Refer to the section **Editing a Rule** for more details,
Delete	Removes the rule from the policy. Refer to the section **Removing a Rule** for more details.
	Available in an expanded rule. Clones the rule to allow administrators to create a new rule with minor changes in the components
	Available in an expanded rule. Enables the administrator to disable or enable the rule. Refer to the section **Enabling or Disabling a rule** for more details.

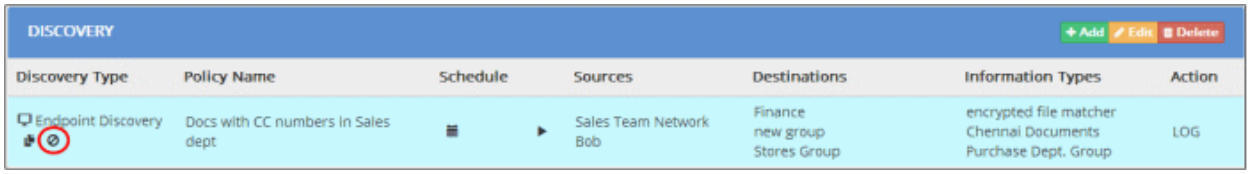
Rules at the top of the table have a higher priority than those at the bottom and are applied first. In the event of a conflict between rules, the setting in the rule nearer the top of the table will be applied. The administrator can change the order of the rules at any time by dragging any rule to the desired position.

Enabling or disabling a rule

The rules added to the policy are automatically enabled by default. The administrator can disable a rule if it is found unnecessary and deemed to be of use at a later time. The disabled rules are gray in color in the table.

To disable / disable a rule

- Click on the rule for the options to be displayed in the 'Channels' column
- Click the Disable icon



The rule will be disabled and the background color will change to gray.

- To re-enable the rule, click the 'Enable' icon.

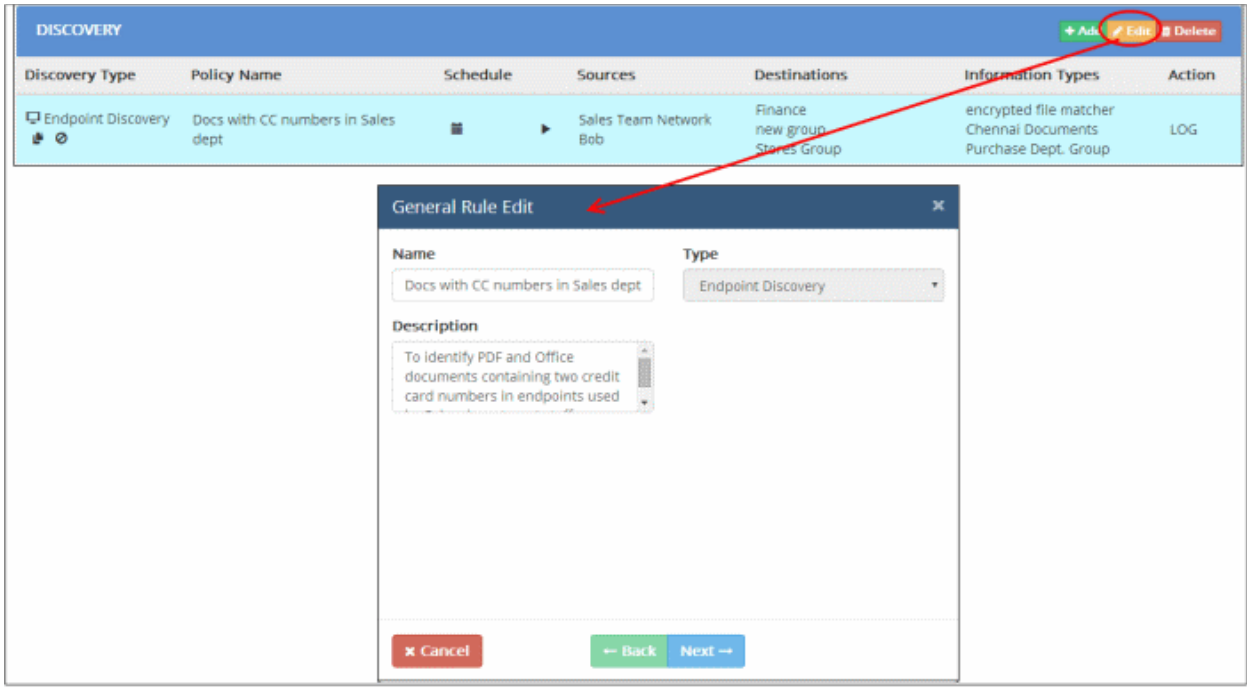
Editing a rule

A rule can be edited at anytime for the changes in the source, destination, information type components, the action to be taken, and the name of the rule. Please note that only rules that are enabled can be edited.

Any change you make in a rule will take effect only on re-deployment of the policy. Refer to the section **Deploying the Policy** for more details on implementing the policy.

To edit a rule

- Select the rule and click the 'Edit' button at the top



You can edit the 'Name', 'Description', add new source, destination, information types and action. Please note you cannot edit the rule type. The interface is same as the 'Edit Dialog' that appear while creating the rule. Refer to the rule creation wizard from **Step 2** onward till the final step for more details.

Removing a rule

The administrator can remove unwanted rules from the policy at any time.

To remove a rule

- Select the rule and click the 'Delete' button at the top

A confirmation dialog will be displayed.

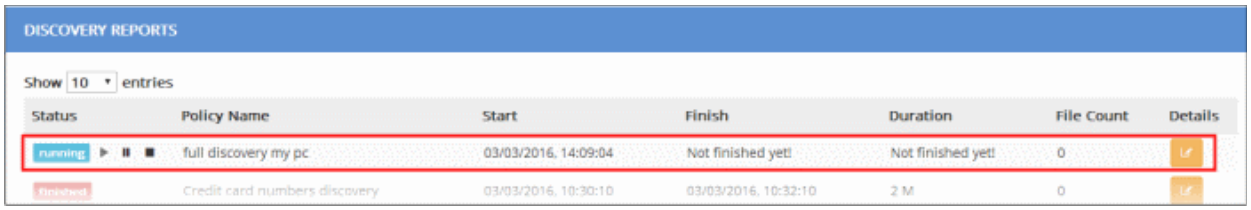
- Click 'Yes' to remove the rule.

Running On-Demand Scans

The administrator can run an instant scan for any rule at any time by clicking the ▶ button in the schedule column.

Note: You need to deploy the policy before running scans based on any new or changed rules. Refer to the section **Deploying a Policy** for more details.

The scan will start immediately and indicated in the list of reports under the 'Discovery Reports'.



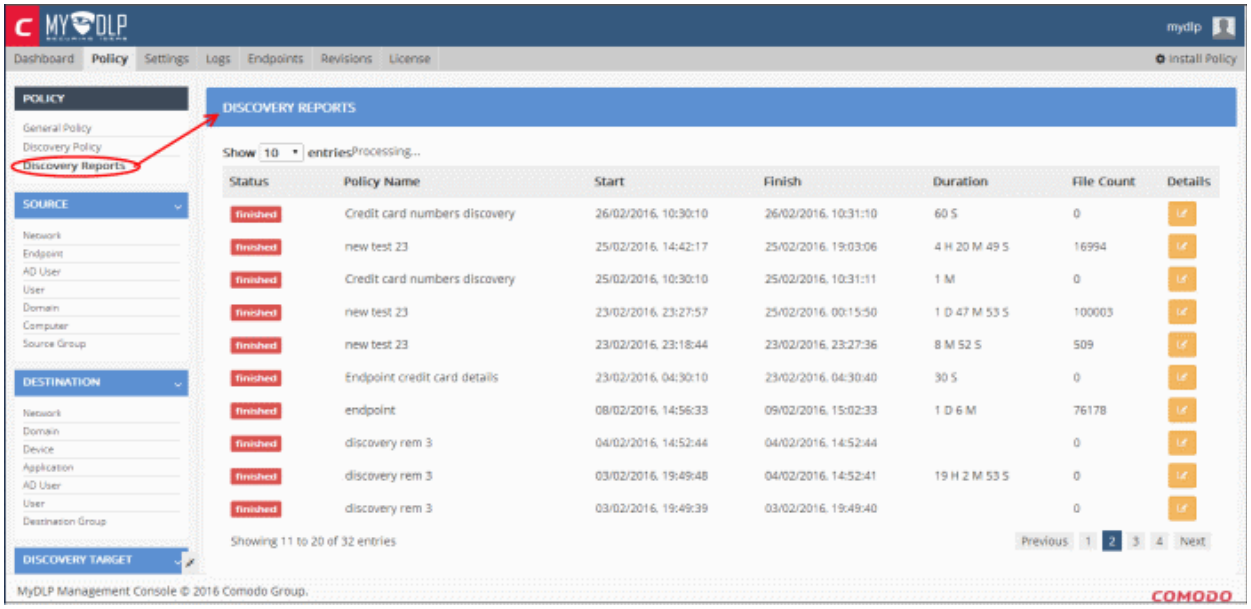
You can pause/resume or stop the scan by clicking the respective buttons.

At the end of the scan, the scan report will be added to the list of reports.

Viewing discovery scan reports

The Discovery interface enables the administrator to quickly access the discovery reports generated at the end of each of scheduled and on-demand scans. The report provides a list of files identified as containing sensitive information, based on the rule for which the scan was run and allows the administrator to save it as a spreadsheet file for future analysis.

To view discovery reports, click 'Discovery Reports' on left under 'Policy'.

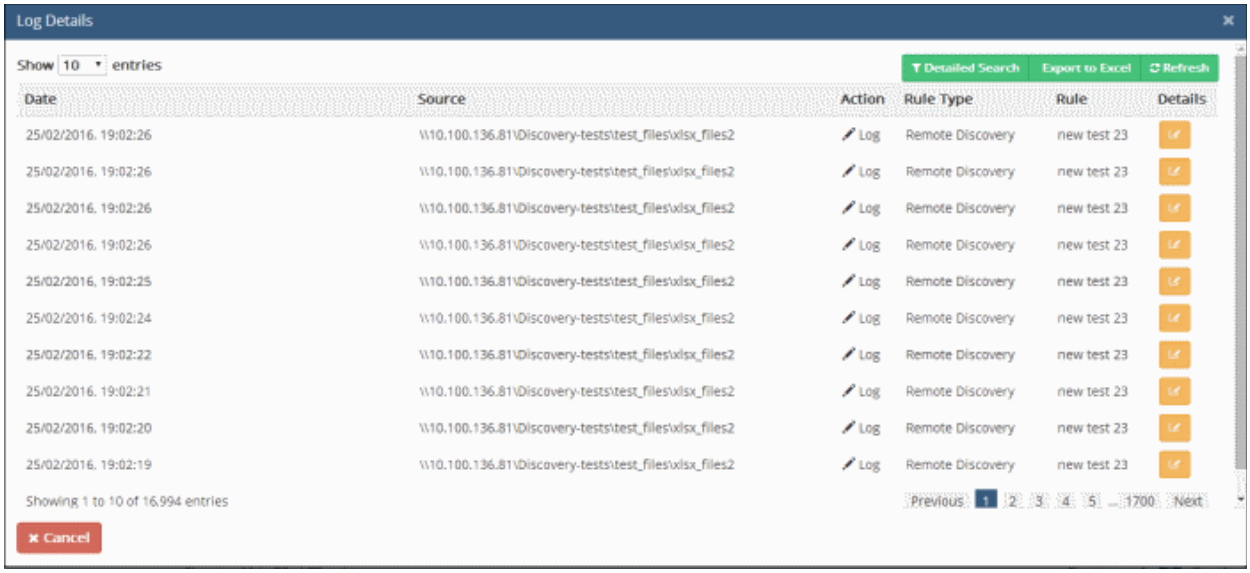


Discovery Reports Table - Description of Columns	
Column	**Description**
Status	Indicates whether the on-demand or scheduled scan is under process or completed.
Policy Name	The Discovery rule based on which the scan was executed.
Start	The precise dates and time at which the scanning was started.
Finish	The date and time the scan was completed.

Duration	Indicates the time taken to complete the scan.
File Count	The number of items discovered at the endpoints covered by the Source object of the rule, containing the data specified in the Information type, in the directory specified as destination.
Details	Clicking the icon in the column opens the respective discovery report. Refer to the following section **The Discovery Report** for more details.

The Discovery Report

- To open a discovery report, click the icon in the respective row. The 'Discovery Report' displays a log of files discovered during the scan.



The Discovery Report - Description of Columns	
Column	**Description**
Date	The precise date and time at which the scan was completed.
Source	The IP address of the source end-point and the file path at which the file was discovered.
Action	The action executed on the file(s) discovered as per the Endpoint Discovery/Remote Storage Discovery rule. Refer to the section **Rule Actions** for a list of actions.
Rule Type	Indicates the type of the discovery rule (Endpoint Discovery or Remote Storage Discovery) based on which the files are discovered.
Rule	The name of the discovery rule based on which the files are discovered.
Details	Enables the administrator to view the complete details of the incident and download the copies of the files discovered. Refer to the section **Viewing Details of a Discovery Log Entry** for more details.

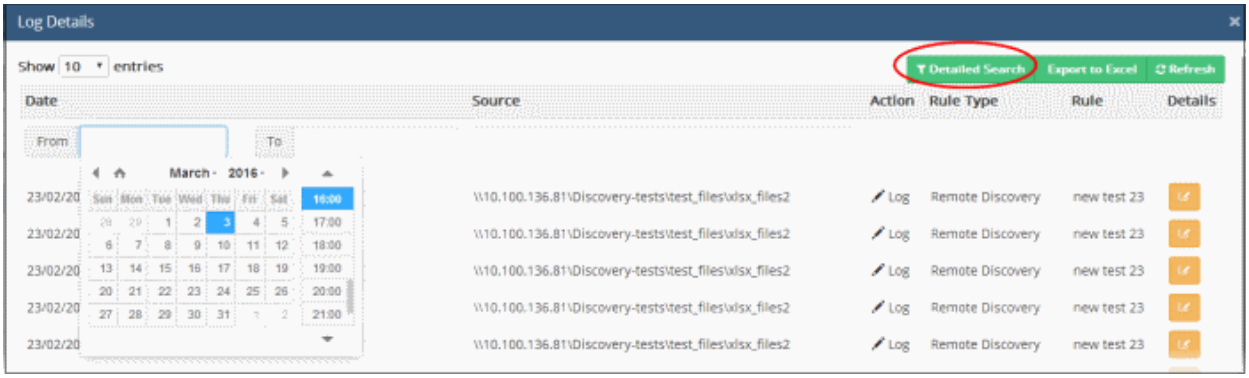
Filtering and Search Options

The logs can be filtered to view the files discovered within a specified period by specifying the start date and end date and further filtered based on the sources, destinations, actions taken and the rule channels.

- **Filtering the Logs for a specific time period**
- **Searching Logs based on rule source parameter**

To filter the logs for a specific time period

- Click 'Detailed Search' at the top



- Click on the 'From' and 'To' fields, select the dates from the calendar

Only the discovery logs for the specified time period will be displayed.

- To show all the entries again, clear the date fields

Searching Logs based on Rule Source Parameters

The administrator can search for logs of incidents involving specific source to narrow down the search.

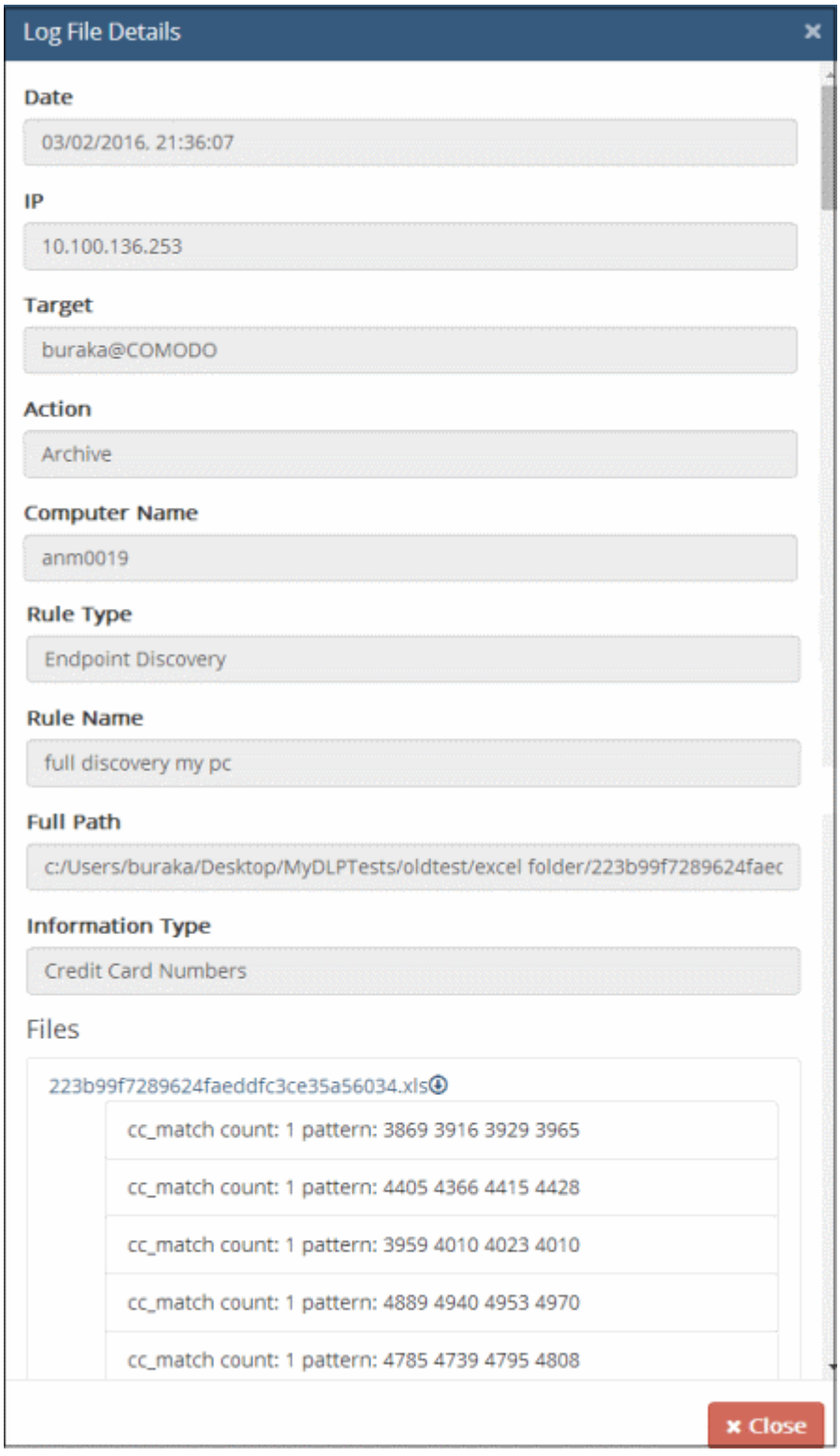
To search the logs based on rule source parameter

- Click 'Detailed Search' to expand the search panel.
  - To search the logs of incidents involving a specific source, enter the IP address of it in the Source field
- Click 'Refresh' to view the logs filtered as per the criteria specified in the search fields.

Viewing Details of a Discovery Log Entry

The administrator can view the granular details of any discovery log entry from the Discovery Report, including the source endpoint, user, destination, files discovered, the rule, information type of sensitive data contained in the files and so on for investigation and auditing purposes. The administrator can open and view the 'Incident Log details' pane for the required log entry that displays the complete details of the incident. The pane also allows the administrator to download a copy of the quarantined/archived file that was identified as containing the sensitive information based on the discovery rule.

- To open the Incident Log Details pane for a log entry, click the  icon for the log entry under the Details column.



Incident Log Details - Table of Parameters	
Field	**Description**
Date	Precise date and time at which the file(s) were discovered.
IP	The IP address of the endpoint at which the file(s) were discovered.
Target	Endpoint Discovery rule - target indicates the computer / user where the discovery was performed

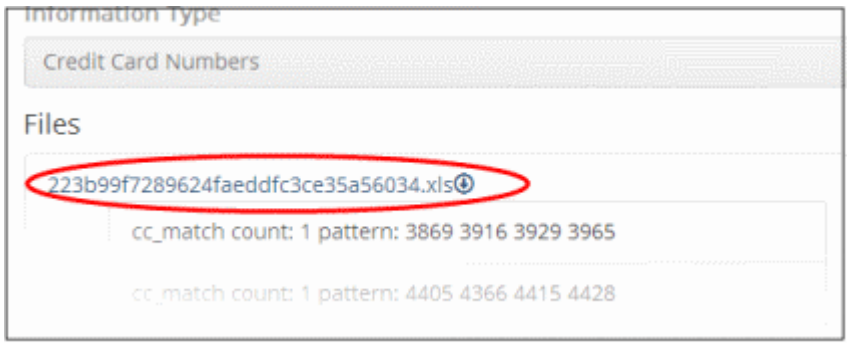
	Remote Storage rule – target indicates the address of the remote remote serer where discovered
Action	The action executed on the discovered file(s).
Computer Name	The host name of the endpoint computer at which the file(s) were discovered.
Rule Type	Indicates the type of the discovery rule (Endpoint Discovery or Remote Storage Discovery) based on which the files are discovered.
Rule Name	The name of the Discovery Rule based on which the file(s) were discovered.
Full Path	The file path from which the files were discovered.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Files	The Log Files displays a list of files that were identified as containing sensitive data matching the Information type specified in the Discovery rule. The details of the selected file will be displayed below the file name. You can download the discovered files by clicking on the file number. Refer to the section **Downloading the Archived Files** for more details.

Downloading the Archived Files

The administrator can download a copy of archived or quarantined files, that were identified as containing sensitive information and discovered based on the discovery rules, for investigation purposes, from the Log File Details interface.

To download an archived file

- Click the  icon for the log entry under the Details column. The Log File Details pane will open.
- Click on the file name, under 'Files'

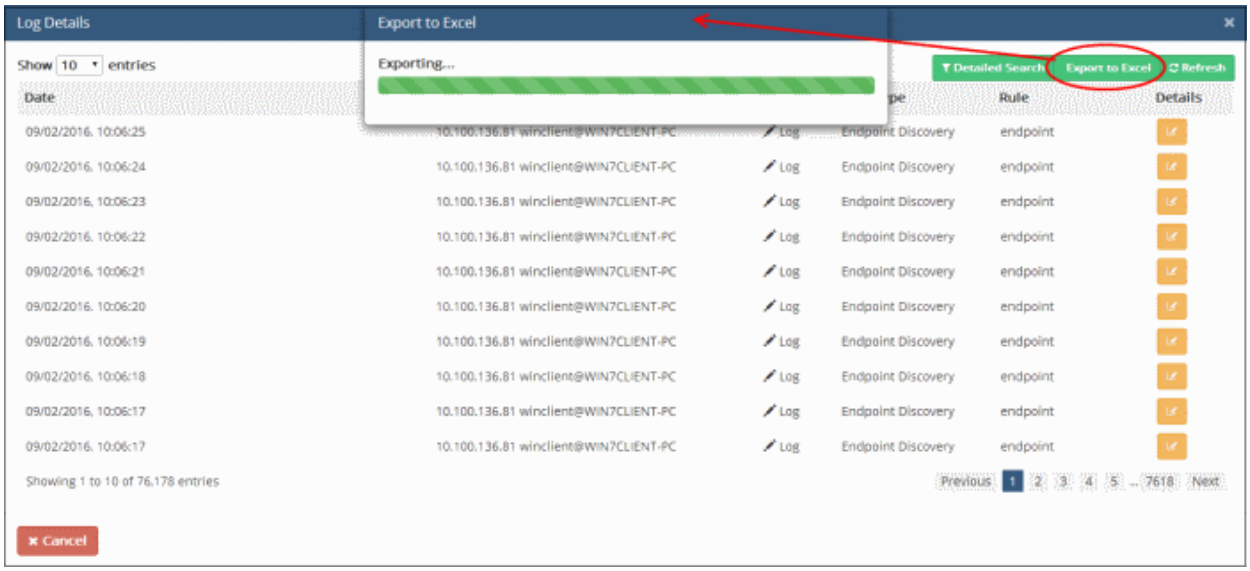


The file will be saved to your default download location.

Exporting the Logs to a Spreadsheet File

The administrator can save the logs as a spreadsheet file in 'Microsoft Excel' file format for later analysis by exporting the logs. The spreadsheet file will contain the first 1000 entries in the log. If needed, the administrator can apply filters and search options to export the log pertaining to a specific time period or to export logs pertaining to specified filtering criteria. Refer to the explanation under '**Filtering and Search Options**' above.

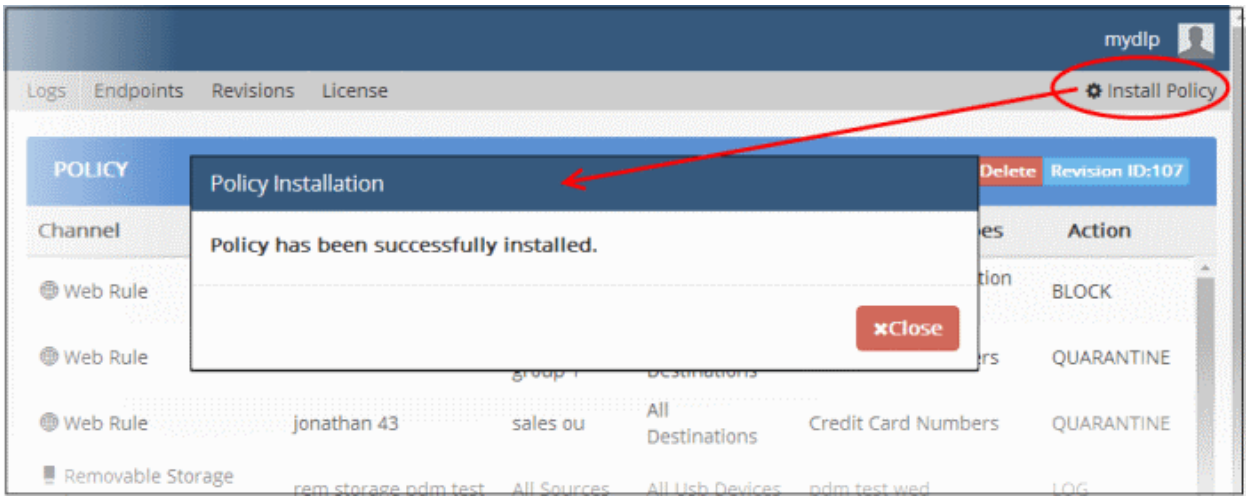
- To export the logs into an Excel file click 'Export to Excel' button at the top and save the file in your local drive.



4.1.6. Deploying a Policy

The rules comprising your Data transfer control policy and Discovery policy will only take effect once you install the policy. If you make modifications to a rule or add a new rule, then you must re-install the policy.

- Click 'Install Policy' at the top right to deploy your policy



- If all enabled rules are correctly specified correctly then the policy will be compiled and installed instantly.
- If one or more of the enabled rules are not complete, the incomplete rule will be highlighted and a dialog will be displayed with advice to complete or disable the rule.

After the policy is deployed, MyDLP assigns a revision ID no. for the policy in order to track which policy is enforced at endpoints. Refer to the section '**The Revisions Tab**' for more details.

5.Rule Types, Objects and Matchers

MyDLP has different categories of rules which are known as 'Rule Types'. Rule types are classified according to data inspection channel and each type is effective only on data traversing through, or residing in, the named channel. Each rule type forms a starting point from which very specific rules can be created by adding or removing rule objects. Refer to the section 'Rule Types' for more details.

The Objects that can be used to construct rules are displayed on the left side of Policy interface under Source, Destination, Discovery Target, Information Type and Matcher sections. These objects can be added to source, destination and information type fields while configuring the rules. Refer to the section 'Objects' for more details.

Data Loss Prevention depends on identifying specific types of information in data at rest and in transit. To do this, an 'information type' is added to a rule to in order to discover and apply actions to data matching the information type. Once matching information is found, it can be allowed, blocked, quarantined, or logged as per the rule. MyDLP ships with predefined information types and you can also create new information types. The information types can be constructed using various components such as document databases, file extensions, keyword database and data formats. These information type building blocks are available under the 'Matcher' section. Refer to the section 'Matcher' for more details.

Click on the following links for more information:

- **Rule Types**
- **Objects**
- **Matchers**

5.1. Rule Types

There are two types of rules that can be configured in MyDLP, one type is for data transfer control and the other is for data discovery. The data control rules are displayed in the 'General Policy' interface and the data discovery rules are displayed in the 'Discovery Policy' screen.

Data control rules

- **Web rules** are used to monitor and control all traffic that passes to and from your network over HTTP and HTTPS. This includes data exchanged with any external network like the Internet. See the section **Web rules** for more details.
- **Mail rules** are used to monitor and control data passed over email and other SMTP traffic from specified sources. See the section **Mail rule** for more details.
- **Removable Storage rules** control data transferred to external devices such as USB memory sticks, removable hard drives and smart phones. See the section **Removable Storage rule** for more details.
- **Removable Storage Inbound rules** are used to archive data copied from removable memory devices on to the computer. See the section **Removable Storage Inbound rule** for more details.
- **Removable Storage Encryption rules** allow you to encrypt removable devices connected to endpoints on your network. After encryption, any data on the drive can only be read if it is connected to your network and not by any other network. If you enable this rule for all sources then any new devices will be immediately encrypted as soon as they are connected. This would prevent, for example, any guest or hostile from plugging in a USB drive, downloading data and taking it out of your network. See the section **Removable Storage Encryption rule** for more details.
- **Screenshot rules** prevent print screen function while a sensitive application is running. See the section **Screenshot rule** for more details.
- **Printer rules** allow you to prevent documents matching specific criteria from being printed. See the section **Printer rule** for more details.
- **API rules** are a unique feature which allow you to integrate custom applications with MyDLP. See the section **API rule** for more details.
- **USB Device Access rules** are used to monitor or block use of USB memory devices on the selected computers covered by the source object defined in the rule. See the section **USB Device Access Rule**for more details.
- **CD-DVD rules** are used to control the use of optical disks like CD and DVD on selected computers covered by the source object. You can choose to monitor or block use of disks or set them to 'Read-Only' mode. See the section **CD-DVD Rule** for more details.

- **Floppy rules** are used to control the use of Floppy disks on selected computers covered by the source object. You can choose to allow or block use of disks or set Floppy disks to Read-Only mode to allow reading of data from the disks and blocking writing of data on to them. See the section **Floppy Rule** for more details.
- **Clipboard rules** are used to control the copy and paste function on selected computers covered by the source object. You can choose actions such as pass, block and more for this rule. See the section **Clipboard Rule** for more details.

Data discovery rules

- **Endpoint Discovery rules** are used to discover and control sensitive data on local storage and hard disks. See the section **Endpoint Discovery rules** for more details
- **Remote Storage rules** are used to discover files containing sensitive data of specified type(s) from remote servers and network file systems. See the section **Remote Storage rule** for more details

5.1.1. Web Rule

Web Rules cover the whole Web channel and can be used to enforce policies for protocols like HTTP, HTTPS, FTP. Restrictions for Social networking sites, Web mail services, blogs, wikis, forums, almost everything that can be accessed through a web browser can be implemented by this rule type. To use Web Rules you need to configure your web traffic to pass over MyDLP Network Server. Please see **MyDLP Installation Guide**.

Web Sources	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, computer name objects,endpoints as Source for this rule. See the chapter **The Objects** for more details on creating user defined sources.
Web Destinations	-	You can specify domain objects as Destination for this rule type. Domains are Fully Qualified Domain Name (FQDN) accessed by users in web requests. See the chapter **The Objects** for more details on creating domain objects.
Web Information Types	-	You can specify any 'Information Type' in Web rules.

Example Web Rule

An example of web rule is shown below. The rule is for quarantining all web requests by users from all sources to all websites that contains credit card information. This rule is named as PCI because it is a part of PCI compliance policy.

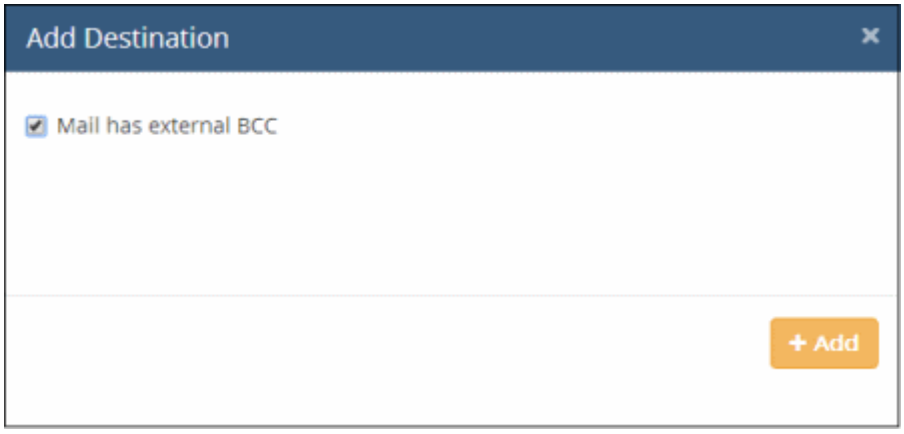
Channel	Name	Sources	Destinations	Information Types	Action
Web Rule	PCI	All Sources	All Destinations	PCI-Credit Card	QUARANTINE

5.1.2. Mail Rule

Mail Rule covers the mail channel and can be used to enforce policies for SMTP protocol. The emails that are sent through the local mail servers will be analyzed using the configured mail rules. Please see **MyDLP Installation Guide** for details in integration of your email server with My DLP.

Mail Source	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects or domain objects as Source for this rule.
Mail Destination	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units) and / or domain objects as Destination for this rule.

You can also configure 'Mail has External BCC item' to filter those mails that have a BCC field from the Destination screen.



Mail Information Types - You can specify any 'Information Type' in Mail rules.

Example Mail Rule

An example of mail rule is shown below. The rule is for quarantining all mails sent by users from sales department to all mail domains that contains credit card information. This rule is named as PCI because it is a part of PCI compliance policy.

Channel	Name	Sources	Destinations	Information Types	Action
Mail Rule	PCI Mail	9 different sources	All Destinations	Credit Card Numbers	QUARANTINE

5.1.3. Removable Storage Rule

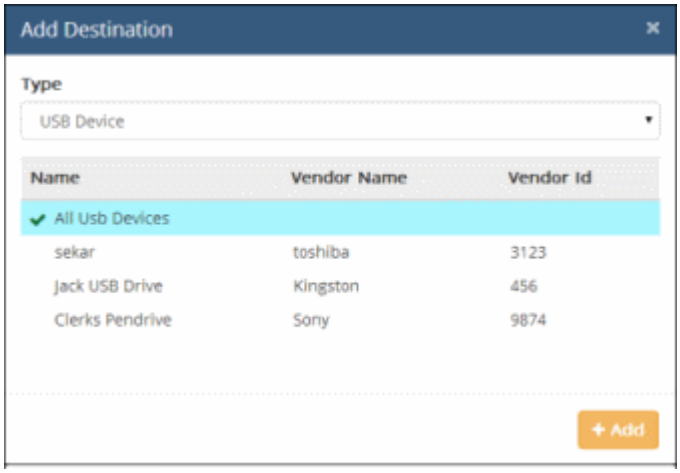
The Removable Storage Rule can be used to govern the data moved to selected removable devices at the endpoints through any operation.

For the Removable Storage Rule to be enforced, the MyDLP Endpoint Agent should be deployed at each endpoint. Please refer to **MyDLP Endpoint Agent Installation Guide**.

Removable Storage Source - You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and / or Endpoint Objects as Source for this rule.

Removable Storage Destination - You can specify USB Device objects as Destination for this rule. For individual USB devices, create them as USB Device Objects and add them as destination.

To restrict copying files to all USB devices, choose All USB Devices from the Destination screen



Removable Storage Information Types - You can specify any 'Information Type' in Removable Storage rules.

Example Removable Storage Rule

An example of Removable Storage Rule is shown below. The rule is for quarantining all the files that contains credit card information, copied by users from sales department and a single user to all USB storage devices connected to their workstations or laptops. This rule is named as PCI because it is a part of PCI compliance policy.

Channel	Name	Sources	Destinations	Information Types	Action
Removable Storage Rule	PCI	2 different sources	All Usb Devices	Credit Card Numbers	QUARANTINE

Note: The Removable Storage Rule can restrict only the files copied to specific removable devices covered by destination objects defined in the rule. If you want to restrict access to USB devices altogether for selected endpoints, you can create USB Device Access rule for them. Refer to the section **USB Device Access Rule** for more details.

5.1.4. Removable Storage Inbound Rule

The Removable Storage Rule can be used to govern file copy or read operations from removable devices to endpoint at endpoints. This rule cannot make any kind of DLP analysis, but can be configured to simply Pass, Log or Archive the transferred data. Any operation that transfers information to computer from a removable storage device is intercepted by this rule.

For the Removable Storage Inbound Rule to be enforced, the MyDLP Endpoint Agent should be deployed at each endpoint. Please refer to **MyDLP Endpoint Agent Installation Guide**.

Removable Storage Inbound Source - You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and / or Endpoint Objects as Source for this rule.

Removable Storage Inbound Destination and Information Type - Since Destination is always the endpoint itself and Information Type is not checked in this rule type, these objects are not required and cannot be defined for this rule type.

Example Removable Storage Inbound Rule

An example of Removable Storage Inbound Rule is shown below. The rule is for logging all the files copied by users from sales department from removable storage devices to their workstations or laptops. This rule is named as

storage logging and can be used to audit memory stick usage behavior of the users.

Channel	Name	Sources	Destinations	Information Types	Action
Removable Storage Inbound Rule	Storage logging	3 different sources			ARCHIVE

Note: The Removable Storage Inbound Rule can restrict only the files that are smaller than the Maximum Object Size configured under **Settings > Advanced** tab. Refer to the explanation under **Maximum Object Size** in the section **Configuring Advanced Settings** for more details. If you have specified 'Archive' action, depending on your users' behavior you may need significant storage to store archived files.

The Logs pertaining to Removable Storage Inbound Rule will be displayed under the 'Logs' tab only if 'Show All' is selected under 'Detailed Search'. Refer to the section **Detailed Log Search** for more details.

5.1.5. Removable Storage Encryption Rule

The Removable Storage Encryption Rule can be configured for the encryption of removable devices connected to the endpoints on the network. This rule cannot make any kind of DLP analysis, but can be configured to simply Pass (Do not encrypt) or Encrypt the removable storage devices.

If the rule action is selected as 'Encrypt' MyDLP detects any new USB storage device connected to the endpoints covered by Source objects of the rule, formats the device and encrypts it, making it usable by the users for storing data from their endpoints. After encryption, any data stored on the device can only be read if it is connected to your network and not by any other network. This would prevent, for example, any guest or hostile from plugging in a USB drive, downloading data and taking it out of the network.

Warning: The rule will first format any new USB device plugged-in for the first time to a source endpoint before it is encrypted. It is advised to backup the data stored in the device before plugging-in to the source endpoint.

For the Removable Storage Encryption Rule to be enforced, the MyDLP Endpoint Agent should be deployed at each endpoint. Please refer to **MyDLP Endpoint Agent Installation Guide**.

Removable Storage Encryption Source - You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and / or Endpoint Objects as Source for this rule.

Removable Storage Encryption Destination and Information Type - Since Destination is always the endpoint itself and Information Type is not checked in this rule type, these objects are not required and cannot be defined for this rule type.

Example Removable Storage Encryption Rule

An example of Removable Storage Encryption Rule is shown below. The rule is for encrypting all the removable storage devices connected to workstations or laptops in the company network. This rule is named as 'all encryption' and can be used to ensure no data leak will occur through removable storage devices from company network to other networks. This the most common usage scenario for this rule.

Channel	Name	Sources	Destinations	Information Types	Action
Removable Storage Encryption Rule	All Encrypted	All Sources			ENCRYPT

5.1.6. Printer Rule

The Printer rule can be configured to control printing of data from the endpoints at any type of printer like network printers, USB printers, shared printers and much more. The rule can enforce policies to printers connected to the endpoints to inspect each and every printing operation.

On application of a printer rule, virtual printers will be created by MyDLP for each physical printer connected to the network. The virtual printers will be displayed with the name of the respective physical printer with a prefix in their name and available for selection while printing the documents from the endpoints added as sources to the printer rule.

For MyDLP to monitor the data/document passed to the printer as per the rule, the physical printers will be displayed with the status 'Unavailable' and the end-users are forced to use the virtual printers. If the data/document does not contain any sensitive data as defined by the rule, MyDLP forwards the documents to the respective physical printer.

The prefix added to the virtual printer name can be configured through Settings > Endpoint Interface. Refer to the description under **Secure Printer Prefix** in the section **Configuring Endpoint Settings** for more details.

For the Printer Rule to be enforced, the MyDLP Endpoint Agent should be deployed at each endpoint. Please refer to **MyDLP Endpoint Agent Installation Guide**.

Printer Source:	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and / or Endpoint Objects as Source for this rule.
Printer Destination	-	The Destination need not be defined for the printer rule.
Printer Information Types	-	You can specify any 'Information Types' in printer rules.

Example Printer Rule

An example of Printer Rule is shown below. The rule is for quarantining all the print jobs that contain credit card information, sent by users from sales department from their workstations or laptops. Print job will be blocked and content of the document to be printed is saved as a XPS document on MyDLP. This rule is named as PCI because it is a part of PCI compliance policy.

Channel	Name	Sources	Destinations	Information Types	Action
Printer Rule	PCI	2 different sources		Credit Card Numbers	QUARANTINE

5.1.7. ScreenShot Rule

The Screenshot Rule can be used to prevent screenshot captures when certain sensitive applications are running or certain sensitive documents are opened at the endpoints. This rule does not send any log to management server but simply blocks the screenshot actions for the selected Applications.

ScreenShot Source	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and / or Endpoint Objects as Source for this rule.
ScreenShot Destination	-	You can specify Application objects that refer to specific application(s) as 'Destination' for this rule.

Example ScreenShot Rule

An example of Screenshot Rule is shown below. The rule is for preventing print screen function when Microsoft Office applications are running. This is one of a common usage scenario.

Channel	Name	Sources	Destinations	Information Types	Action
Screenshot Rule	Screenshot Restriction	Sales Team Network	Microsoft Excel Microsoft Access Notepad Microsoft Word PDF Quick View Microsoft Outlook Microsoft Publisher		BLOCK

5.1.8. API Rule

The API rules can be configured to manage behavior of MyDLP API. MyDLP API that help you to integrate MyDLP with other applications.

API Sources	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and / or Endpoint Objects as Source for this rule.
API Information Types	-	You can specify any 'Information Types' in API rules.

Example API Rule

An example of API Rule is shown below. The rule is for blocking response to web requests from applications on 10.0.0.0/24 network if the request body contains credit card number.

Channel	Name	Sources	Destinations	Information Types	Action
Api Rule	PCI CRM Int	10.0.0.0/24		Credit Card Numbers	BLOCK

5.1.9. USB Device Access Rule

The USB Device Access rule can be created to control and monitor plug-in and plug-out of USB memory devices like pen-drives at the endpoints. This rule cannot make any kind of DLP analysis, but can be configured to simply Pass, Log or Block the use of USB devices on the endpoints covered by the source object defined in the rule.

For the USB Device Access Rule to be enforced, the MyDLP Endpoint Agent should be deployed at each endpoint. Please refer to **MyDLP Endpoint Agent Installation Guide**.

USB Device Access Rule Source:	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and/or Endpoint Objects as Source for this rule.
USB Device Access Rule Destination and Information Type	-	Since Destination is always the endpoint itself and Information Type is not checked in this rule type, these objects are not required and cannot be defined for this rule type.

Example USB Device Access Rule

An example of USB Device Access Rule is shown below. The rule is for blocking use of USB devices with workstations or laptops used by sales department staff.

Channel	Name	Sources	Destinations	Information Types	Action
USB Device Access	Block USB devices	Sales Team Network			BLOCK

5.1.10. CD-DVD Rule

The CD-DVD rule can be added to control and monitor the use of optical disks like Compact Disk (CD), Digital Versatile Disk (DVD) at the endpoints covered by the source object defined in the rule. This rule cannot make any kind of DLP analysis, but can be configured to simply Pass, Log or Block the use of disks or set them to 'Read-Only' mode.

For the CD-DVD Rule to be enforced, the MyDLP Endpoint Agent should be deployed at each endpoint. Please refer to **MyDLP Endpoint Agent Installation Guide**.

CD-DVD Rule Source:	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and/or Endpoint Objects as Source for this rule.
CD-DVD Rule and Information Type	-	Since Destination is always the endpoint itself and Information Type is not checked in this rule type, these objects are not required and cannot be defined for this rule type.

Example CD-DVD Rule

An example of CD-DVD Rule is shown below. The rule is for setting the use of CD-DVD to Read-Only mode at a specified endpoint.

Channel	Name	Sources	Destinations	Information Types	Action
CD-DVD Rule	CD Read Only	Bob Smith			READ ONLY

5.1.11. Floppy Rule

The Floppy rule can be added to control and monitor the use of Floppy disks at the endpoints covered by the source object defined in the rule. This rule cannot make any kind of DLP analysis, but can be configured to simply Pass or Block the use of disks or set them to 'Read-Only' mode.

For the Floppy Rule to be enforced, the MyDLP Endpoint Agent should be deployed at each endpoint. Please refer to **MyDLP Endpoint Agent Installation Guide**.

Floppy Rule Source:	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and/or Endpoint objects as Source for this rule.
Floppy Rule and Information Type	-	Since Destination is always the endpoint itself and Information Type is not checked in this rule type, these objects are not required and cannot be defined for this rule type.

Example Floppy Rule

An example of Floppy Rule is shown below. The rule is for blocking the use of Floppy disks at the work stations or laptops used by Sales Department staff, integrated as a Source.

Channel	Name	Sources	Destinations	Information Types	Action
Floppy Rule	Block Floppy Disks	Sales Team Network			BLOCK

5.1.12. Clipboard Rule

The Clipboard Rule can be used to prevent copying certain sensitive information from documents at the endpoints. The rule will disable users from copying configured information type such as credit card numbers to clipboard.

For the Clipboard Rule to be enforced, the MyDLP Endpoint Agent should be deployed at each endpoint. Please refer to **MyDLP Endpoint Agent Installation Guide**.

Clipboard Source	-	You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and / or Endpoint Objects as Source for this rule.
Clipboard Destination	-	Since Destination is always the endpoint itself, this object cannot be defined for this rule type.
Clipboard Information Types	-	You can specify any 'Information Types' in Clipboard rules.

Example Clipboard Rule

An example of Clipboard Rule is shown below. The rule is to block copying of credit card numbers from any document. This is one of a common usage scenario.

Channel	Name	Sources	Destinations	Information Types	Action
Clipboard Rule	Block copy function	All Sources		Credit Card Numbers	BLOCK

5.1.13. Endpoint Discovery Rule

The Endpoint Discovery rule can be configured scan local disks/file paths of specific endpoints to discover files containing sensitive information. The administrator is notified in advance, on the information leakage risk before any incident happened by this rule.

Discovery Source: - You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects and / or Endpoint Objects as Source for this rule.

Discovery Destination - You can specify File System Directory objects as Destination for this rule. The folders specified as Destinations on endpoints will be scanned by Discovery Rule to find whether they match the specified Information Type.

Discovery Information Types - You can specify any 'Information Types' in Discovery rules.

Example Endpoint Discovery Rule

An example of Endpoint Discovery Rule is shown below. The rule is for logging the files containing credit card numbers, from the Documents and Settings folder in the endpoints of 192.168.0.0/16 network.

Discovery Type	Policy Name	Schedule	Sources	Destinations	Information Types	Action
Endpoint Discovery	Endpoint credit card details		192.168.0.0/16	C:/Documents and Settings	Credit Card Numbers	LOG

5.1.14. Remote Storage Rule

The Remote Storage rule can be configured scan remote servers like FTP servers, Web servers, file share locations, network file systems and so on to discover files containing sensitive information. The administrator can choose to Log or Archive if files containing sensitive information are identified from the remote storage locations as per the rule.

Discovery Source: - You can specify a Remote Storage object as Source for this rule. The Remote Storage objects pointing to remote storage locations can be created only from the 'Discovery' interface. Refer to the section **Adding a User Defined Remote Storage** for more details.

Discovery Destination: - Since it is not possible to specify destination for a remote storage, the Destination field is not required for this rule.

Discovery Information Types: - You can specify any 'Information Types' in Discovery rules

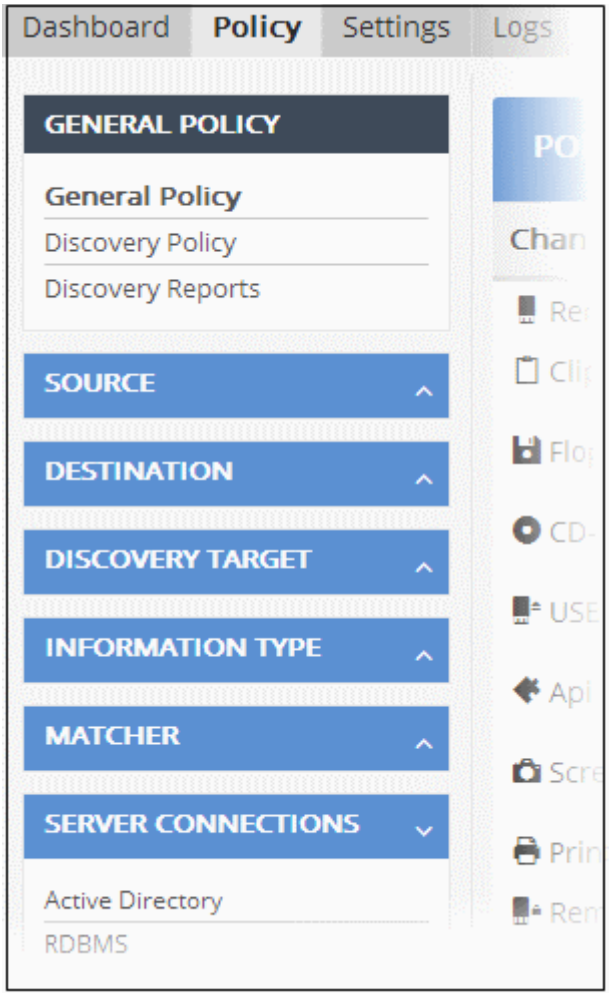
Example Remote Storage Discovery Rule

An example of Network Storage Discovery Rule is shown below. The rule is for archiving Office document files containing credit card numbers from the Remote Storage.

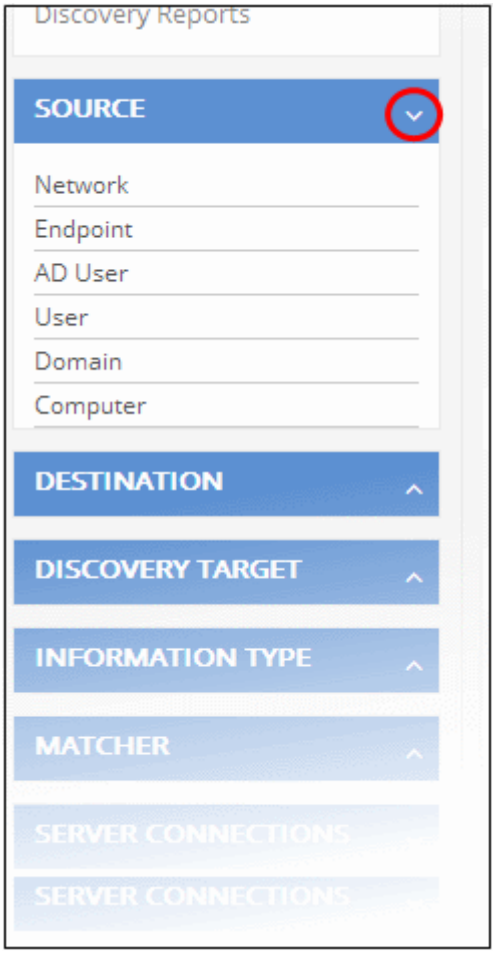
Discovery Type	Policy Name	Schedule	Sources	Destinations	Information Types	Action
Remote Storage Rule	Credit card numbers discovery		discovery database 111		Credit Card Numbers	ARCHIVE

5.2. Objects

The Objects that can be used to construct rules are displayed on the left side of Policy interface under Source, Destination, Discovery Target, Information Type and Matcher sections. These objects can be added to source, destination and information type fields while configuring the rules.



You can expand/collapse a section by clicking the drop-down button on the right.



MyDLP ships with a set of pre-defined objects that are commonly and frequently used.

- Predefined sources represent common network addresses.
- Predefined information types are common information types such as credit card numbers, IBAN, SSN. It also includes all matcher which is used to match all traffic.
- Compliance is an information type that includes predefined policies such as PCI DSS, HIPAA, SOX, and GLBA etc.
- Pre-defined Destinations are items that can be used in Destination component of a rule.

Administrator can create different types of user defined objects and object groups with the parameters as required by the organization and can use them in their rules. Refer to the section **User Defined Objects** for more details.

5.2.1. Object Types

'Objects' are the building blocks for defining each component of the 'Rules'. MyDLP uses different types of objects that can be suitably used for source, destination and information type components of the rule.

Object Type	Description	Application
Network	Available under 'Source' and 'Destination' sections. The 'Network' object is used to define a network or a sub network by their IP address/Network Mask	As 'Source' and 'Destination' in: • All types of Data Transfer Policy rules • Endpoint Discovery rule
Endpoint	Available under 'Source' section.	As 'Source' in:

Object Type	Description	Application
	The Endpoint is used to define a single endpoint computer by specifying its unique Endpoint ID number. Upon successful installation of the MyDLP Endpoint Agent on to the Endpoints, each endpoint is assigned with an unique 'Endpoint ID' and displayed in the **Endpoints** interface. The Administrator can use the 'Endpoint ID's from this interface to specify the endpoints while creating the 'Endpoint' objects. The rule in which the Endpoint Object is used will be effective only if the Endpoint ID is specified as displayed in the Endpoints interface.	• All types of both Data Transfer Policy rules except Mail Rule • Endpoint Discovery rule
AD User	Available under 'Source' and 'Destination' sections. The 'AD User' Object is used to specify a single user or a group of users.	As 'Source' in all types of Data Transfer Policy rules.
User	Available under 'Source' and 'Destination' sections. The 'User' Object is used to specify a single user or a group of users. Upon successful installation of the MyDLP Endpoint Agent on to the Endpoints, the logged-on user at each endpoint is displayed in the **Endpoints** interface. The Administrator can use the User Names from this interface to specify the users while creating the 'User' objects. The rule in which the User Object is used will be effective only if the user is specified as displayed in the Endpoints interface.	As 'Source' in all types of Data Transfer Policy rules.
Domain	Available under 'Source' and 'Destination' sections. The 'Domain' object is used to specify a domain name, which can be specified as source or destination of data traffic when configuring a data transfer control policy.	As 'Source' and 'Destination' in all types of Data Transfer Policy rules.
Computer	Available under 'Source' section. The 'Computer' object is used to define a single endpoint computer by specifying its host name. Upon successful installation of the MyDLP Endpoint Agent on to the Endpoints, the 'Computer Names' for the Endpoints are displayed in the **Endpoints** interface. The Administrator can use the Computer name from this interface to specify the computer name while creating the 'Computer Name' objects. The rule in which the 'Computer Name' Object is used will be effective only if the computer name is specified as displayed in the Endpoints interface.	As 'Source' in: • All types of Data Transfer Policy rules except Mail Rule • Endpoint Discovery rule
Devices	Available under 'Destination' section. The 'Devices' object is used to specify USB devices with their name, vendor name and vendor ID. These	As 'Destination' in Removable Storage rule

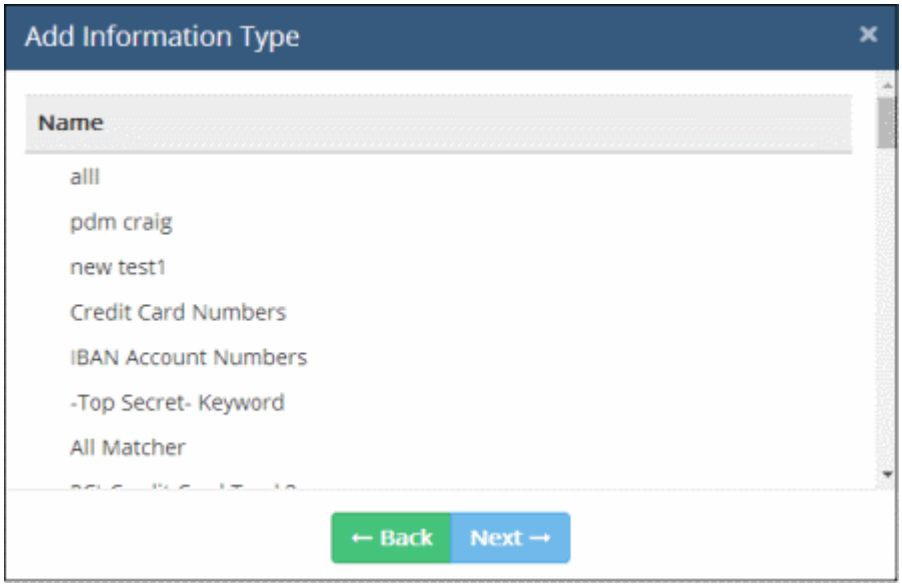
Object Type	Description	Application
	objects can be specified as destinations in the Removable Storage rules to monitor and control data transferred to them from the endpoints. You must first add USB devices to MyDLP by specifying their Vendor and Product ID under 'Devices' in the 'Destination' section. Refer to the section **Adding a User Defined USB Device Object** for more information on adding USB devices to MyDLP.	
Application	Available under 'Destination' section. The 'Application Name' object is used to specify a software application or executable.	As 'Destination' in Screenshot rule
Endpoint File System	Available under 'Discovery Target' section. The 'File System Directory' object is used to specify a file path like C:/Users/ for checking existence of files with sensitive information in the specified file path or folder in the specified endpoints added as sources for a discovery rule.	As 'Destination' in Endpoint Discovery Rule
Remote Connections	Available under 'Discovery Target' section. The 'Remote Storage' object is used to specify a remote server, for checking existence of files with sensitive information in it.	As 'Source' in Remote Storage Rule
Information Type	Available under 'Information Type' section. The 'Information Type' object is used to define the type of data to be checked for imposing the rule action to the file containing the data. More details on Information are available in the next section **Information Types - An Overview**.	As 'Information Type' in: • Web Rule • Mail Rule • Removable Storage Rule • Printer Rule • API Rule • Clipboard Rule • Endpoint Discovery Rule • Remote Storage Rule

Comodo MyDLP is shipped with a number of pre-defined Object types that are commonly and frequently used. The administrator can create different types of user defined objects and object groups with the parameters as required by the organization and can use them in their rules. Refer to the section **User Defined Objects** for more details.

5.2.2. Information Types - An Overview

Data Loss Prevention depends on identifying specific types of information in data at rest and in transit. To do this, an 'information type' is added to a rule to in order to discover and apply actions to data matching the information type. Once matching information is found, it can be allowed, blocked, quarantined, or logged as per the rule.

The 'Add Information Type' interface allows administrators to define granular data types which MyDLP should search for. MyDLP also ships with a number of predefined information types that can be used in rules.



Each Information type consists of the following components:

- Name - A Name to identify the information type
- **Data Format(s)** - The file format(s) included in the information type. Files matching the specified data format will be inspected for the occurrence of data with properties/string formats specified in Information Features. Examples of data formats are 'Office Files', 'Plain Text', 'Images', 'Audio Files' and so on.
- **Extensions** – The file extensions included in the information type. Files with the specified extension will be inspected for the occurrence of data with properties/string formats specified in Information Features. Examples of file extensions are .asp, .psd, .avi, .exe and so on.
- **Information Features** – Specific content types in the file types specified in Data Formats and File Extensions. The features include:
    - **Matcher** - Data patterns or string formats such as birth-date, keywords, credit card number, account number and so on. You can also specify an occurrence threshold. MyDLP identifies the data matching the pattern/format as candidate data and checks whether they occur for number of times specified as the threshold.
    - **Context** – Allows you to further refine the matcher thresholds by specifying the extent of data within which the information must be found. For example, your matchers might be 'Credit Card Numbers' set to 2 occurrences. If you set a context of '3 Paragraphs', then 2 credit card numbers must be found within 3 paragraphs.

If a file with the specified extension contains data that matches the string format/keyword for the number of times as specified as threshold, within an extent as specified in the context parameter, then the file falls into the defined information type. If such file is found in the data transfer from the source to the destination of a rule, the file will be passed, quarantined, logged or blocked as specified in the action component of the rule.

Data Formats

The 'Data Formats' parameter is used to define the file format(s) to identify the candidate files for the Information Type. The files of specified file format in the data traffic or the resident files in the users' computers will be analyzed and checked whether they contain data with properties specified under Information Features. If they contain such data, then the files will be classified as the Information Type. Examples:

- If you select 'All Formats', every single file will be inspected for the data with the information features to identify the files that fall under the 'Information Type'
- If you select 'PDF, PS, etc', only the files in Portable Document Format and PostScript formats will be inspected to identify the files that fall under the 'Information Type'

Comodo MyDLP is shipped with a set of pre-defined Data Formats that are commonly and frequently used. The

administrator can add more custom data formats from Matcher > Data Formats interface. Refer to the section **Managing Data Formats** for more details.

Extensions

The 'Extensions' parameter is used to define the file extension to identify the target files for the Information Type. The files of specified extension in the data traffic or the resident files in the users' computers will be analyzed and checked whether they contain data with properties specified under Information Features. If they contain such data, then the files will be classified as the Information Type. For example:

- If you select '.BAT', only the files with .bat extension will be inspected to identify the files that fall under the 'Information Type'

Comodo MyDLP is shipped with a set of pre-defined file extensions that are commonly and frequently used. The administrator can add more custom file extensions from Matcher > File Extension interface. Refer to the section **Managing File Extensions** for more details.

Information Features

The 'Information Features' can be used to define the criteria to identify specific data content in the candidate files. There are two broad types of criteria that can be defined:

- **Matcher**
- **Context**

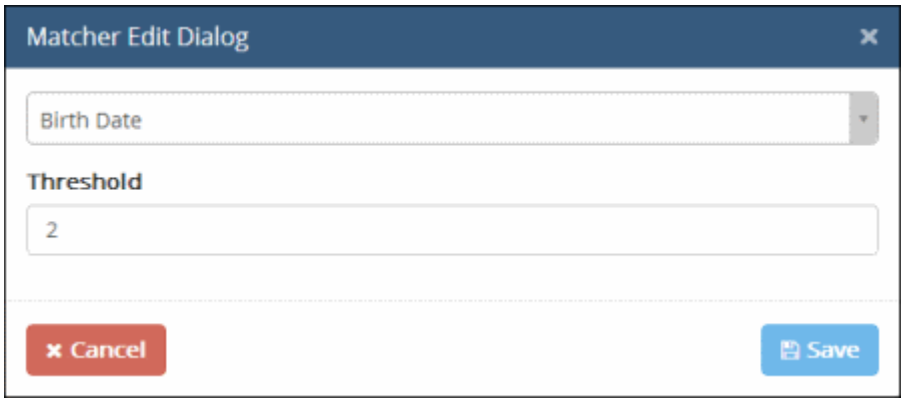
Matcher

The 'Matcher' is a specific data string format, pattern or keyword defined as a criteria for the information type. An information feature can be configured with any number of matchers so that a document file will be shortlisted based on the information type, only if it contains data matching all the matchers.

Each Matcher generally contains two components, Type and Threshold. Some of the matchers such as Keyword, Regular Expression, Keyword Groups, Document Database (PDM) and Document Database (Hash) contain additional fields allowing you to add customized parameters.

- Type - The 'Type' parameter specifies the pattern or data string format for the data or information to be identified. Examples: credit card number, date, account number, names and so on.
- Threshold - The minimum number of times the data or information matching the 'Type' should occur in the document file or data.

If any file shortlisted based on the 'Data Format' contains any content data satisfying the above criteria, then the file falls as the Information Type object and the action specified under the rule is applied to it. In the example given below, the data string format is specified as birth date and the Threshold is set as two. All the document files containing at least two birth dates will be considered as the information type object.



Refer to the following section **Predefined Matcher Types** for a full list of available matcher types.

Context

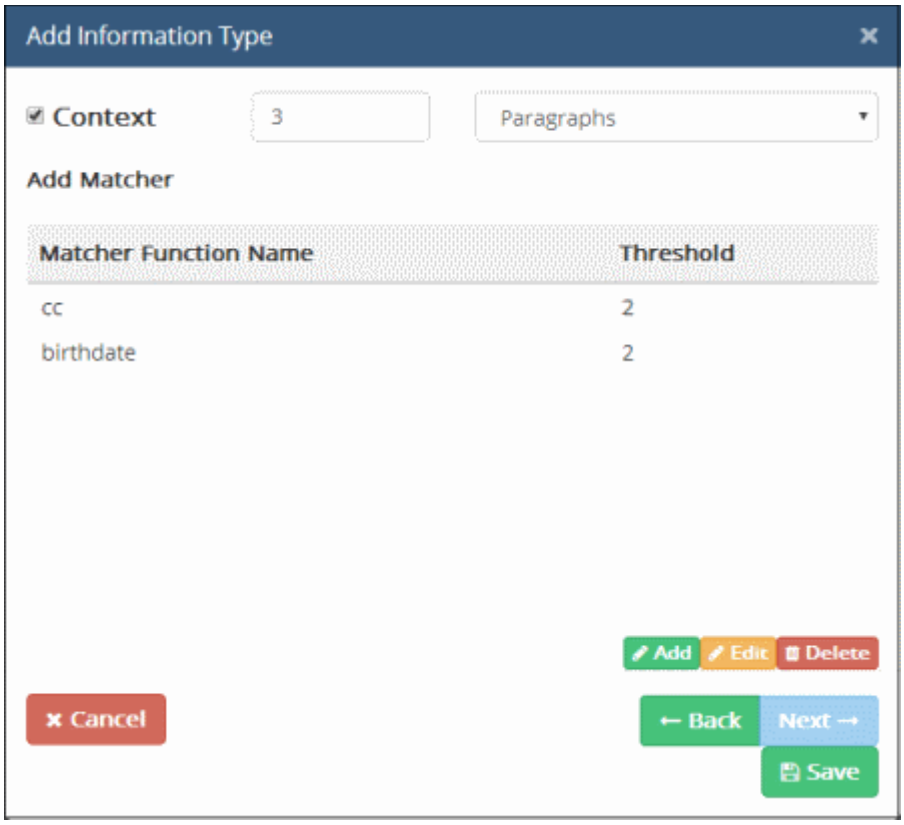
The 'Context' is an optional parameter used to specify the minimum extent of data size within which the data matching the 'Matchers' should occur, to consider a file as 'Information Type' object. DLP analysis will return positive

only if all the defined Information Features are found within a portion of specified extent in the document. This feature lets you make DLP analysis in a context and drastically decrease false positives in big files. The extent can be specified in terms of number of words, sentences, paragraphs and pages.

If the 'Context' parameter is not enabled, then the document will be identified as the 'Information Type' and the action will be applied as per the rule, if the information matching the matchers occur for minimum number or times specified as the threshold within the whole document.

The example shown below describes the identification of a file as briefly. In this example, there are two matchers:

- Credit Card Number with threshold 2; and
- Birth Date with threshold value 2;
- The Context parameter is enabled and set as three paragraphs.



Data Transfer Policy Rule

If the above said example information type is applied in a data transfer policy rule, then, all the specified files with configured extensions in the data transfer between the sources and destinations will be checked and any of the document that contains two birth-dates and two credit card numbers only within any three consecutive paragraphs then the file will be allowed to pass, blocked, quarantined or logged specified as the action.

If the 'Context' is not enabled, any document that contains two birth-dates and two credit card numbers in the whole, then the file will be applied with the action.

Discovery Rule

If the above said example information type is applied in a discovery rule, then, all the specified files with configured extensions in the local storages of sources will be checked and any of the document that contains two birth-dates and two credit card numbers only within any three consecutive paragraphs then the file will be allowed applied with the action.

If the 'Context' is not enabled, any of the document that contains two birth-dates and two credit card numbers in the whole, then the file will be applied with the action.

5.2.2.1. Predefined Matcher Types

This section provides a list of predefined Information Features available in MyDLP.

Feature	Description
10 Digit Account Number 5-8 Digit Account Number 9 Digit Account Number ABA Routing Number	Identifies occurrences of bank account numbers.
All Matcher	Can be used in rules for certain data formats such as for preventing any outgoing office file.
Birth Date	Identifies occurrences of birth dates specified in the files
Brazil Natural Persons Register (CPF)	Identifies occurrence of Brazilian citizen identification number in a data stream or file.
Canada Social Insurance Number	Identifies matches Canada Social Secure Security Number in a data stream or file.
China Identity Card Number	Identifies occurrence of Chinese citizen identification card number in a data stream or file.
Chinese Name	Identifies occurrence of Chinese names in a data stream or file.
Credit Card Expiration Date	Identifies occurrences of data containing expiry date of credit card in data stream or file.
Credit Card Number	Identifies occurrences of credit card number in data stream or file. If you use credit card number with threshold 5 it will match any document with 5 or more credit card numbers in it.
Credit Card Track 1	Identifies occurrences of credit card data as it is contained in Track 1 of the magnetic stripe of the credit card (data encoded in the format established by IATA (International Air Transport Association)).
Credit Card Track 2	Identifies occurrences of credit card data as it is contained in Track 2 of the magnetic stripe of the credit card (data encoded in the format established by ABA (American Bankers Association)).
Credit Card Track 3	Identifies occurrences of credit card data as it is contained in Track 3 of the magnetic stripe of the credit card (THRIFT information).
DNA Pattern	Identifies occurrences of DNA pattern representations in the data stream or file.
Document Database (Hash)	Identifies any document in data stream whose file hash exactly matches with that of any of the documents in document database.

Feature	Description
Document Database (PDM)	Partial document matching (PDM) feature identifies any chunk of document in data stream where it significantly resembles a part of a document in document database.
Encrypted Archive Matcher	Identifies encrypted archive files such as zip, rar etc.
Encrypted Document Matcher	Identifies encrypted documents that are password protected or encrypted.
France INSEE Number	Identifies France INSEE number in a data stream or file.
General Date	Identifies occurrences of any date in the data stream or file.
IBAN Account Number	IBAN is the International Bank Account Number. This feature identifies bank account number in IBAN format in data stream or file of the specified file format.
ICD-10 Code	Identifies occurrences of codes of International Statistical Classification of Diseases - 10 format, in the data stream or file.
India Permanent Account Number	Permanent Account Number (PAN) is unique alpha numeric 10 character identifier assigned to income tax payers in India. This feature identifies PAN numbers in data stream or file of the specified file format.
India Tax Deduction Account Number	Tax Deduction Account Number (TAN) is unique alpha numeric identifier assigned to companies or individuals who are required to deduct tax on payments made by them to their employees under the Indian Income Tax Act, 1961 This feature identifies TAN numbers in data stream or file of the specified file format.
IP	Identifies the IP address included in the data stream or file
Italy Fiscal Code Number	Italy Fiscal Code Number is unique 16 character identifier given to Italian citizens. This feature identifies Italy Fiscal Code Numbers in data stream or file of the specified file format.
Keyword	Identifies occurrence of the keyword entered during creation of information type, in a data stream or file. The administrator can specify any number of keywords as individual information feature matchers.
Keyword Group	Identifies occurrence of the group of keywords pertaining to predefined groups like Personal Finance Terms, drug names, common names and so on. Administrators can add custom keyword groups from the Information Type interface.
MAC	Identifies the occurrence of MAC address included in the data stream or file

Feature	Description
Regular Expression	Identifies the occurrence of regular expressions included in the data stream or file
Social Security Number	National Social Security Number (NSSN) is the United States social security number. This feature identifies NSSN in a data stream or file of the specified file format.
Source Code (Ada)	Identifies Ada programming language expressions in a data stream or file.
Source Code (C/C++/C#/Java)	Identifies expressions in C, C++, C# and Java programming languages in a data stream or file.
South African ID Number	Identifies occurrence of South Africa citizen ID number in a data stream or file.
Spain DNI Number	Identifies occurrence of Spanish ID number in a data stream or file.
Taiwan National ID Number	Identifies occurrence of Taiwanese ID number in a data stream or file.
Texas Driver License	Identifies occurrence of Texas Driver License number in a data stream or file.
Turkey National ID Number	Turkey National ID Number or T.C. Kimlik No. is the citizen number in Turkey. This feature identifies occurrences of this number in a data stream or file.
UK National Insurance Number	Identifies United Kingdom insurance number in a data stream or file.
Uruguay SSN	Identifies matches Uruguay Social Secure Security Number in a data stream or file.

5.2.2.2. Predefined Information Types

Comodo MyDLP ships with a series of pre-defined 'Information Types' for use in myDLP rules. Information types are optimized to identify the specific type of data contained in the files transferred and hence cannot be edited. This section provides a list of predefined Information Types available in My DLP version 2.2. under two categories:

- **Compliance**
- **Information Types**

Compliance

MyDLP contains several predefined Information Types that can be used for creating rules to prevent loss of documents and other types of files containing sensitive data in compliance with the Government law and business policies. The 'Compliance' category contains five subcategories of predefined information types:

- **Federal Regulations**
- **Finance**
- **Network Security Information**
- **Personal Information**

- Sensitive Documents

Federal Regulations

The Information Types in the 'Federal Regulations' category are created to meet requirements of HIPAA (Health Insurance Portability and Accountability Act). The purpose of Act is to protect billing and the confidential medical records of patients. MyDLP allows the institution to protect customer's confidential information and meet the requirements of HIPAA with following matchers.

Information Type	Description	Matchers & Threshold Values		Context
CCN with Common Disease Names	Consists of Credit Card Number and Keyword Group-Common Disease Names	Credit Card Number	1	3 Sentences
		Keyword Group - Common Disease Names	1	
DNA	Consists of DNA Pattern matcher	DNA Pattern	1	Not Specified
Date of Birth with Names	Consists of Birth Date and Keyword Group-Names	Birth Date	1	3 Sentences
		Keyword Group-Names	1	
Names with Common Disease	Consists of Keyword Group-Common Disease Names and Keyword Group - Names	Keyword Group-Common Disease Names	1	Not Specified
		Keyword Group - Names	1	
National Drug Codes	Consists of National Drug Codes	Keyword Group - National Drug Codes	1	Not Specified
SSN with Common Disease Names	Consists of Social Security Number and Keyword Group- Common Disease Names	Social Security Number	1	3 Sentences
		Keyword Group- Common Disease Names	1	
Sub-Category: CCN with Sensitive Diseases/Drugs				
CCN with Sensitive Disease Names	Consists of Credit Card Number and Keyword Group-Sensitive Disease Names	Credit Card Number	1	3 Sentences
		Keyword Group-Sensitive Disease Names	1	
CCN with Sensitive Drug Names	Consists of Credit Card Number and Keyword Group- Sensitive Drug Names	Credit Card Number	1	3 Sentences
		Keyword Group-Sensitive Drug Names	1	
Sub-Category: Name with Sensitive Diseases/Drugs				
Name with Sensitive Disease	Consists of Keyword Group-Names and Keyword Group-Sensitive Disease Names	Keyword Group - Names	1	3 Sentences
		Keyword Group-Sensitive Disease Names	1	
Name with Sensitive Drug	Consists of Keyword Group-Names and Keyword Group-Sensitive Drug Names	Keyword Group - Names	1	3 Sentences
		Keyword Group - Sensitive Drug Names	1	
Sub-Category: SSN with Sensitive Diseases/Drugs				

Information Type	Description	Matchers & Threshold Values		Context
Sensitive Disease Names	Consists of Social Security Number and Keyword Group- Sensitive Disease Names	Social Security Number	1	3 Sentences
		Keyword Group - Sensitive Disease Names	1	
SSN with Sensitive Drug Names	Consists of Social Security Number and Keyword Group- Sensitive Drug Names	Social Security Number	1	3 Sentences
		Keyword Group - Sensitive Drug Names	1	

Finance

The 'Finance' category contains predefined Information Types that are specific to Finance applications.

Information Type	Description	Matchers & Threshold Values		Context
Sub-Category: EU Finance > CCN with National IDs				
CCN with France-Insee	Consists of Credit card number and France INSEE (Institut National de la Statistique et des Études Économiques) Number	Credit Card Number	1	3 Sentences
		France INSEE Number	1	
CCN with Italy-FC	Consists of Credit card number and Italy Fiscal Code Number	Credit Card Number	1	3 Sentences
		Italy Fiscal Code Number	1	
CCN with Spain-DNI	Consists of Credit card number and Spanish DNI (Documento nacional de identidad) Number	Credit Card Number	1	3 Sentences
		Spain DNI Number	1	
CCN with UK-Nino	Consists of Credit card number and UK National Insurance Number	Credit Card Number	1	3 Sentences
		UK National Insurance Number	1	
Sub-Category: GLBA				
ABA Routing Number	Consists of American Bankers Association (ABA) routing number, the nine digit bank code, printed in negotiable instruments in the US.	ABA Routing Number	1	Not Specified
CCN	Consists of Credit card number	Credit Card Number	1	Not Specified
Name with 10 Digit Account Number	Consists of Keyword Group 'Names' and 10 digit bank account number	Keyword Group - Names	1	3 Sentences
		10 Digit Account Number	1	

Information Type	Description	Matchers & Threshold Values		Context
Name with 5-8 Digit Account Number	Consists of Keyword Group 'Names' and 5-8 digit bank account number	Keyword Group - Names	1	3 Sentences
		5-8 Digit Account Number	1	
Name with 9 Digit Account Number	Consists of Keyword Group 'Names' and 9 digit bank account number	Keyword Group - Names	1	3 Sentences
		9 Digit Account Number	1	
Name with Personal Finance Terms	Consists of Keyword Groups 'Names' and 'Personal Finance Terms'	Keyword Group - Names	1	3 Sentences
		Keyword Group - Personal Finance Terms	1	
Name with SSN	Consists of Social Security Number and Keyword Group 'Names'	Social Security Number	1	3 Sentences
		Keyword Group - Names	1	
SSN with Personal Finance Terms	Consists of Social Security Number and Keyword Group 'Personal Finance Terms'	Social Security Number	1	3 Sentences
		Keyword Group - Personal Finance Terms	1	
Sub-Category: GLBA > Name with Sensitive Disease/Drug				
Name with Sensitive Disease	Consists of Keyword Groups 'Names' and 'Sensitive Disease Names'	Keyword Group - Names	1	3 Sentences
		Keyword Group-Sensitive Disease Names	1	
Name with Sensitive Drug	Consists of Keyword Groups 'Names' and 'Sensitive Drug Names'	Keyword Group - Names	1	3 Sentences
		Keyword Group - Sensitive Drug Names	1	
Sub-Category: India Financial Documents				
India Form No. 16 (Salary Certificate)	Consists of Keyword Group 'India Form No. 16'	Keyword Group - India Form No. 16	10	1 Page
India Form No. 16A (TDS)	Consists of Keyword Group 'India Form No. 16A'	Keyword Group - India Form No. 16A	10	1 Page
Sub-Category: Investment Information				
Investment Related Documents	Consists of Keyword Group 'Investment informations'	Keyword Group - Investment informations	5	4 Paragraphs
Sub-Category: PCI				
PCI-Credit Card	Consists of Credit Card Numbers	Credit Card Number	1	Not Specified
Sub-Category: PCI > PCI Credit Card Tracks				
PCI-Credit Card Track1	Consists of Credit Card Track1 information	Credit Card Track1	1	Not Specified

Information Type	Description	Matchers & Threshold Values		Context
PCI-Credit Card Track2	Consists of Credit Card Track2 information	Credit Card Track2	1	Not Specified
PCI-Credit Card Track3	Consists of Credit Card Track3 information	Credit Card Track2	1	Not Specified
Sub-Category: Pricing				
Pricing Information	Consists of Keyword Group 'Pricing information'	Keyword Group - Pricing informations	5	4 Paragraphs
Sub-Category: SOX (Sarbanes-Oxley Act of 2002 (public company accounting reform))				
Sub-Category: SOX > 10K Forms				
10K Forms Cover Page	Consists of Keyword Group '10K Form Cover Page Keywords'	Keyword Group - 10K Form Cover Page Keywords	6	6 Paragraphs
10K Forms Financial Statements	Consists of Keyword Group '10K Form Financial Statement Keywords'	Keyword Group - 10K Form Financial Statement Keywords	3	6 Sentences
10K Forms Selected Financial Data	Consists of Keyword Group '10K Form Financial Data Keywords'	Keyword Group - 10K Form Financial Data Keywords	3	2 Paragraphs
10K Forms Stock Performance Graph	Consists of Keyword Group '10K Form Performance Graph Keywords'	Keyword Group - 10K Form Performance Graph Keywords	2	5 Sentences
10K Forms Table of Contents Page	Consists of Keyword Group '10K Form Table of Contents Keywords'	Keyword Group - 10K Form Table of Contents Keywords	12	2 Pages
Sub-Category: SOX > 10Q Forms				
10Q Forms Consolidated Balance Sheets	Consists of Keyword Group '10Q Form Consolidated Balance Sheets Keywords'	Keyword Group - 10Q Form Consolidated Balance Sheets Keywords	6	6 Paragraphs
10Q Forms Cover Page	Consists of Keyword Group '10Q Form Cover Page Keywords'	Keyword Group - 10Q Form Cover Page Keywords	5	6 Paragraphs
10Q Forms Other Information	Consists of Keyword Group '10Q Form Other Information Keywords'	Keyword Group - 10Q Form Other Information Keywords	4	8 Paragraphs
10Q Forms Table of Contents Page	Consists of Keyword Group '10Q Form Table of Contents Keywords'	Keyword Group - 10Q Form Table of Contents Keywords	5	2 Pages

Network Security Information

The 'Network Security Information' category contains predefined Information Types that can be used to identify files containing network related terms and data.

Information Type	Description	Matchers & Threshold Values		Context
IP with Network Patterns	Consists of IP Addresses and Keyword Group 'Network Patterns'	IP Address	2	5 Sentences
		Keyword Group - Network Patterns	2	
Mac Address	Consists of Mac Address	Mac Address	4	4 Sentences
Network Patterns	Consists of Keyword Group 'Network Patterns'	Keyword Group - Network Patterns	4	4 Sentences

Personal Information

The 'Personal Information' category contains predefined Information Types that can be used to identify files containing person names and addresses.

Information Type	Description	Matchers & Threshold Values		Context
Sub-Category: China / Hongkong				
China Address with Name	Consists of Chinese name and Keyword Groups of Chinese Common Names, Chinese Lastnames, Cities in China, Regions in China, Chinese Address Terms.	Chinese Name	1	3 Words
		Keyword Group - Chinese Common Names	1	
		Keyword Group - Chinese Lastnames	1	
		Keyword Group - Cities in China	1	
		Keyword Group - Regions in China	1	
		Keyword Group - Chinese Address Terms	1	
Chinese Name with Lastname	Consists of Chinese name and Keyword Groups of Chinese Common Names and Chinese Lastnames.	Chinese Name	1	1 Sentences
		Keyword Group - Chinese Common Names	1	
		Keyword Group - Chinese Lastnames	1	
Hong Kong Address with Name	Consists of Chinese name and Keyword Groups of Chinese Common Names, Chinese Lastnames, Cities in Hong Kong, Regions in Hong Kong, and Chinese Address Terms.	Chinese Name	1	3 Words
		Keyword Group - Chinese Common Names	1	
		Keyword Group - Chinese Lastnames	1	
		Keyword Group - Cities in Hong Kong	1	
		Keyword Group - Regions in Hong Kong	1	

Information Type	Description	Matchers & Threshold Values		Context
		Keyword Group - Chinese Address Terms	1	
Sub-Category: Taiwan				
Taiwan Address with Name	Consists of Chinese name and Keyword Groups containing Chinese Common Names, Taiwanese Lastnames, Cities in Taiwan, Regions in Taiwan, Chinese Address Terms.	Chinese Name	1	3 Words
		Keyword Group - Chinese Common Names	1	
		Keyword Group - Taiwanese Lastnames	1	
		Keyword Group - Cities in Taiwan	1	
		Keyword Group - Regions in Taiwan	1	
		Keyword Group - Chinese Address Terms	1	
Taiwanese Name with Lastname	Consists of Chinese name and Keyword Groups containing of Chinese Common Names and Taiwanese Lastnames.	Chinese Name	1	1 Word
		Keyword Group - Chinese Common Names	1	
		Keyword Group - Taiwanese Lastnames	1	

Sensitive Documents

The 'Sensitive Documents' category contains predefined Information Types that can be used to identify documents containing sensitive business and man power information and prevent them from being lost.

Information Type	Description	Matchers & Threshold Values		Context
Sub-Category: Resume For HR				
CV Policy	Consists of Keyword Group containing Curriculum Vitae Keywords	Keyword Group - Curriculum Vitae Keywords	8	8 Paragraphs
Sub-Category: Sensitive Keywords				
Confidential - Keyword	Identifies documents containing the term "Confidential"	Keyword - "Confidential"	6	3 Pages
Restricted - Keyword	Identifies documents containing the term "Restricted"	Keyword - "Restricted"	6	3 Pages
Sensitive - Keyword	Identifies documents containing the term "Sensitive"	Keyword - "Sensitive"	6	3 Pages
Top Secret - Keyword	Identifies documents	Keyword - "top secret"	6	3 Pages

Information Type	Description	Matchers & Threshold Values		Context
	containing the term "top secret"			
Sub-Category: Strategic Business Document				
Strategic Business Documents	Identifies documents containing keywords related to business strategies.	Keyword Group - Strategic Business Document Keywords	10	8 Paragraphs

Information Types

The 'Information Types' category contains predefined Information Types that can be used to identify documents containing sensitive information like credit card numbers, bank account numbers documents labeled 'Top Secret' and to block transfer of any data from specified source(s) to destination(s).

Information Type	Description	Matchers & Threshold Values		Context
Top Secret- Keyword	Identifies documents containing the term "top secret"	Keyword - "top secret"	1	Not Specified
All Matcher	Can be used to block data transfer of any file from specified source(s) to specified destination(s)	N/A		
Credit Card Numbers	Identifies documents containing at least one credit card number.	Credit Card Number	1	Not Specified
IBAN Account Numbers	Identifies documents containing at least one Bank Account number in IBAN format.	IBAN Account Number	1	Not Specified

5.2.3. User Defined Objects

Each rule is composed of five 'Objects' namely, the Channel or Name of the rule, Source, Destination, Information type and Action. Comodo MyDLP is shipped with several predefined objects and allows the administrators to create Objects as required for the Organization. The Rule types and the pre-defined objects are explained in the sections **Rule Types** and the **Objects Types**. This section explains on how to create 'User Defined Objects'. Refer to the following sections for more information.

- **Adding a User Defined Network object**
- **Adding a User Defined Computer Name Object**
- **Adding a User Defined Endpoint Object**
- **Adding a User Defined Information Type**
- **Adding a User Defined Domain Name**
- **Adding a User Defined Application Name**
- **Adding a User Defined User Object**
- **Adding a User Defined Active Directory Users Object**

- Adding USB Devices Object
- Adding a User Defined File System Directory
- Adding a User Defined Remote Storage

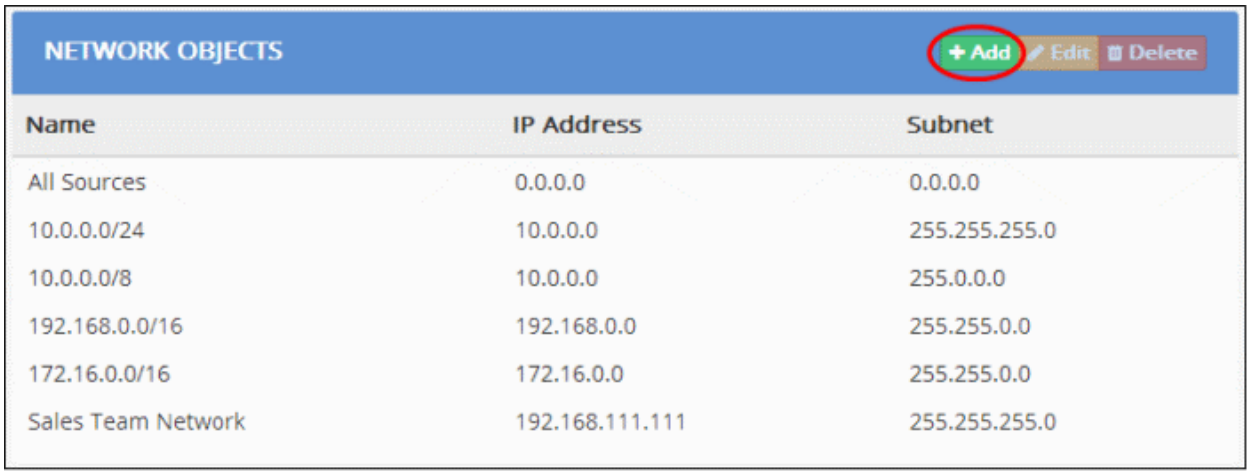
5.2.3.1. Adding a User Defined Network Object

The administrator can specify network addresses to be protected to create network objects. The networks objects can be used as 'Source' in endpoint discovery rule and all types of data transfer policy rules.

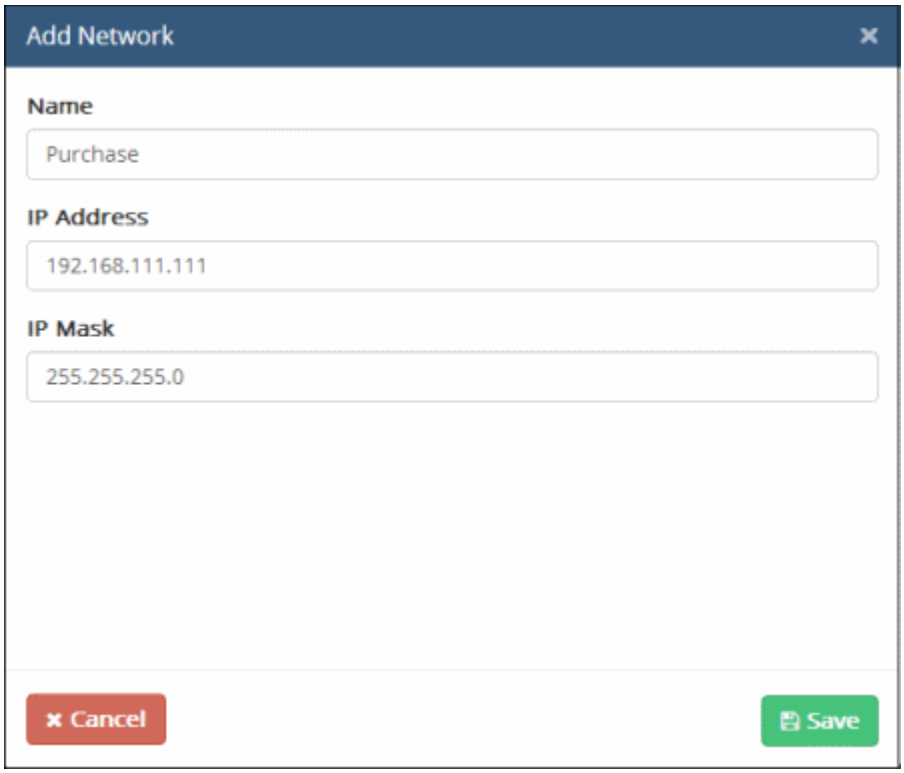
To create a new network object

1. Click the 'Policy' tab at the top and then 'Network' under 'Source' or 'Destination' sections

The 'Network Objects' screen will be displayed:

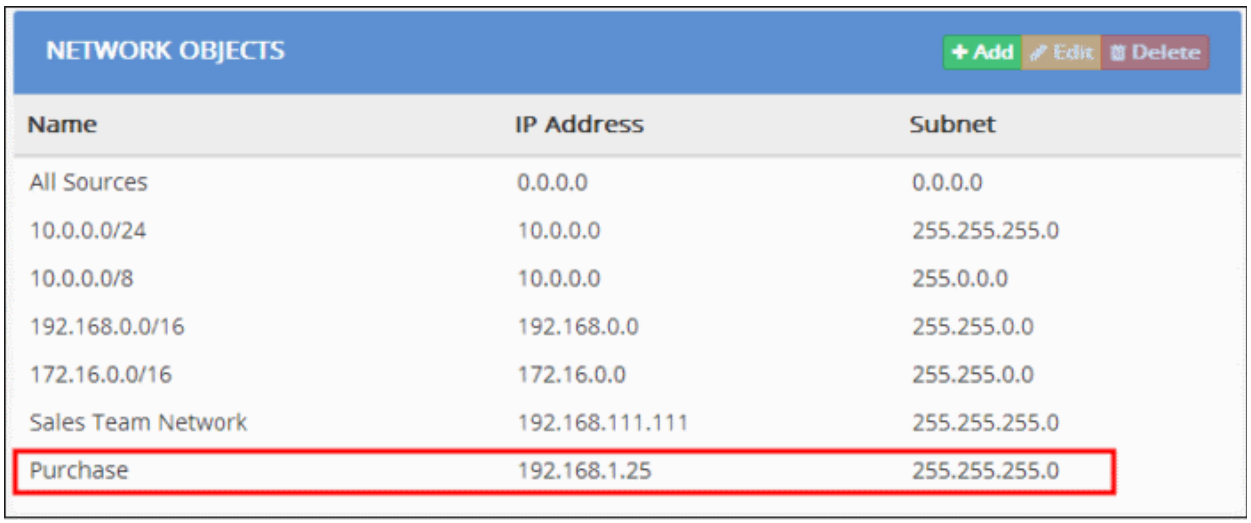


2. Click 'Add' at the top right. The 'Add Network' dialog will appear.



3. Enter the parameters:
    - Name - Enter a name shortly describing the network object
    - IP Address - Enter the start IP address of the network
      Example: 192.168.1.25
    - IP Mask - Enter the IP Net Mask
      Example : 255.255.255.0
4. Click 'Save'.

The new user defined network object will be listed in the 'Network Objects' screen.



- To edit the details of a network object, select it, click 'Edit' and modify the details as explained above.
- To remove a network object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

Please note you cannot edit or delete a predefined network object.

5.2.3.2. Adding a User Defined Computer Name Object

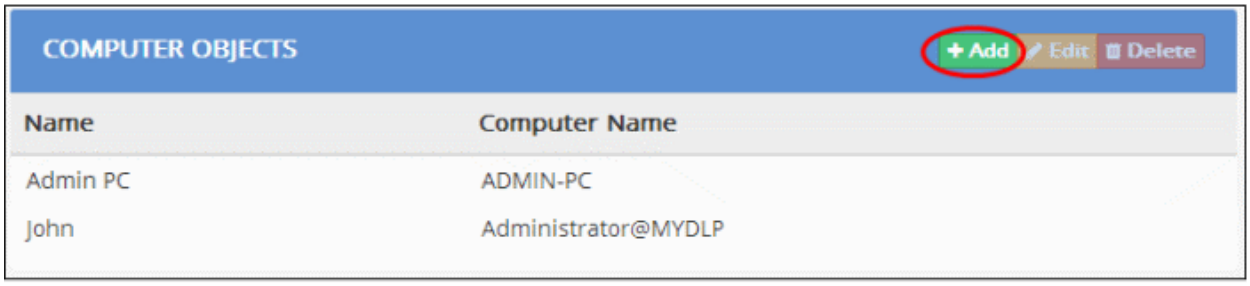
The administrator can specify a single endpoint to be protected, as Computer Name Object, by specifying its host name. The endpoint can be added as a source to endpoint discovery rule and all the data transfer policy rules except mail rule.

Prerequisite: The endpoints are to be installed with the MyDLP Endpoint Agent before adding them as Computer Name Objects. The endpoints installed with the agent are listed with their Endpoint IDs, Logged-in Usernames and Computer Names under the **Endpoints** tab. Refer to the **MyDLP Endpoint Installation Guide** for explanations on installing the agent.

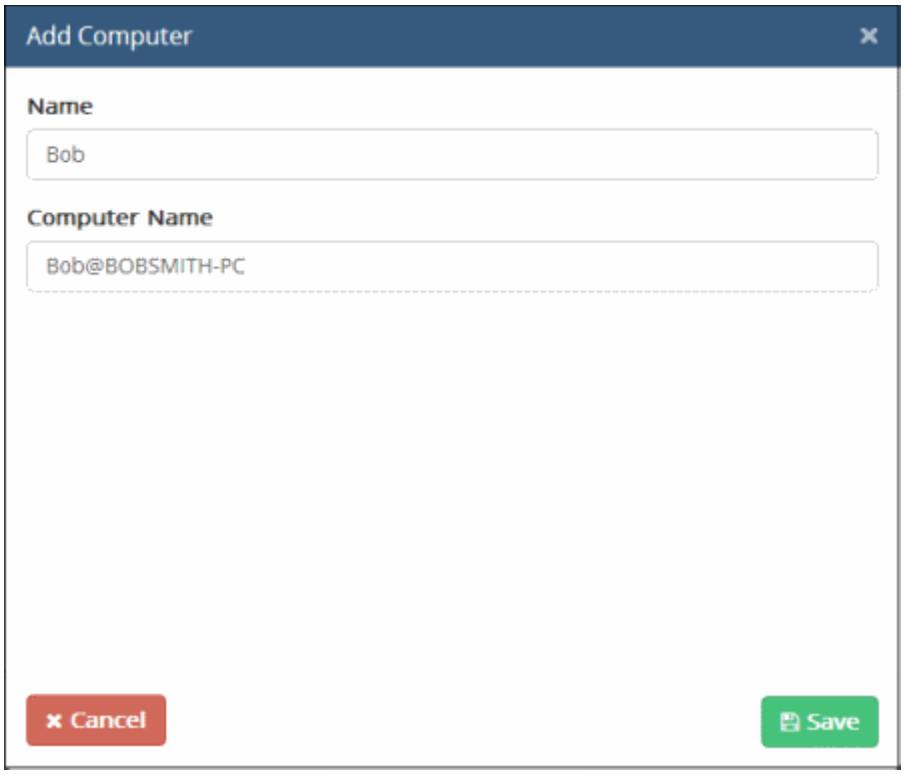
To create a Computer Name object

1. Click the 'Policy' tab at the top and then 'Network' under 'Source' section.

The 'Computer Objects' screen will be displayed:

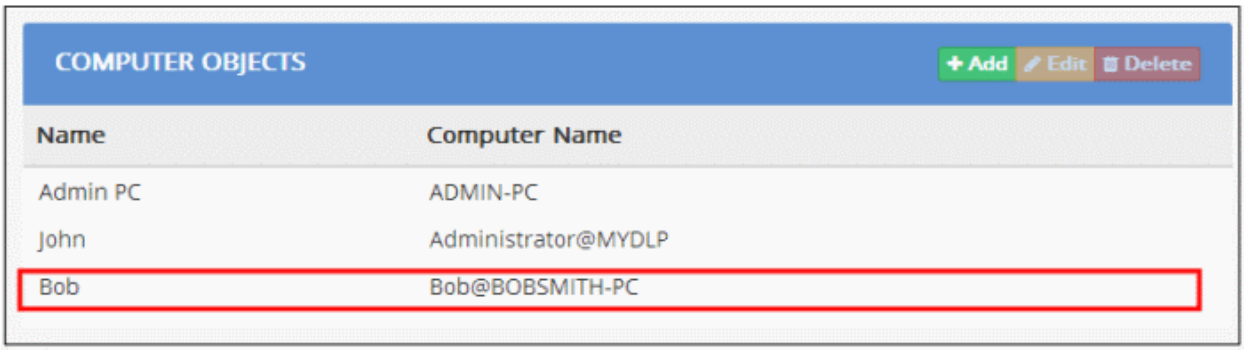


2. Click 'Add' at the top right. The 'Add Computer' dialog will appear.



3. Enter the parameters:
   - Name - Enter a name shortly describing the computer
   - Computer Name - Enter the host name of the computer. The host name or the 'Computer Name' should be specified as it is mentioned in the **Endpoints** tab. The Administrator should refer to the Endpoint tab and enter the computer name.
4. Click 'Save'.

The new user defined computer name object will be listed in the Computer Objects screen.



- To edit the details of a computer object, select it, click 'Edit' and modify the details as explained above.

- To remove a computer object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

5.2.3.3. Adding a User Defined Endpoint Object

The computers in the local network can be added as endpoints to the MyDLP server by installing the MyDLP agent client onto them. Each network computer installed with the agent will be assigned a unique MyDLP Endpoint Identity (ID) number and listed under the Endpoints tab of the MyDLP interface. For more details on the Endpoints interface, refer to the section **Endpoints**.

Prerequisite: The endpoints are to be installed with the MyDLP Endpoint Agent before adding them as Computer Name Objects. The endpoints installed with the agent are listed with their Endpoint IDs, Logged-in Usernames and Computer Names under the **Endpoints tab**. Refer to the **MyDLP Endpoint Installation Guide** for explanations on installing the agent.

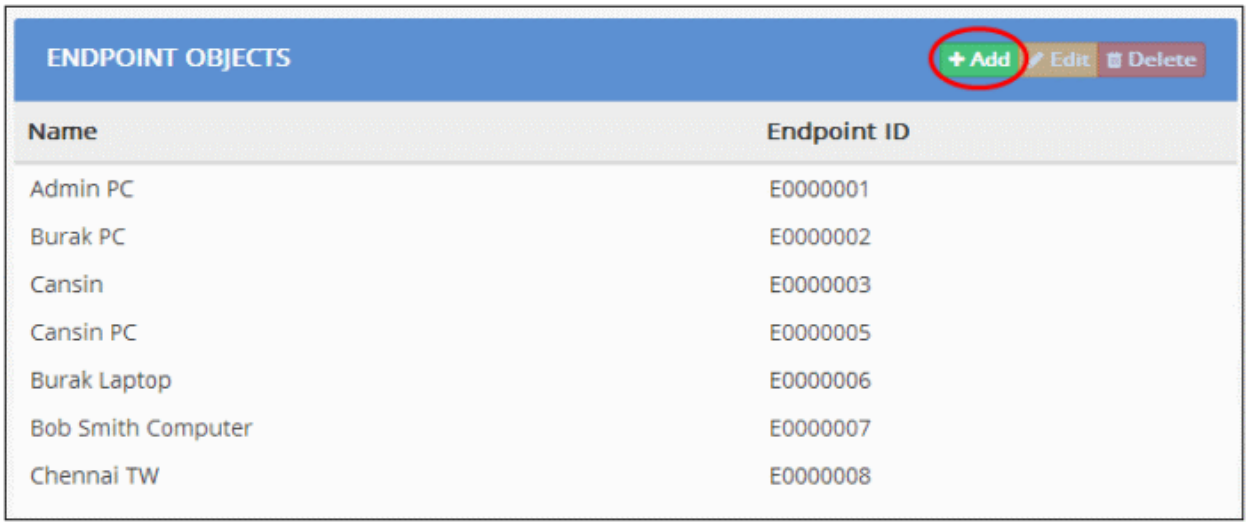
The administrator can create Endpoint Object by selecting the ID number for use in source component in a rule. To apply the rule, MyDLP wil use the persistent ID number of the computer to identify it instead of the IP address, Computer name, Logged on username and so on which are prone to change.

For more details on installing the MyDLP client onto endpoints refer to **MyDLP Endpoint Installation Guide**.

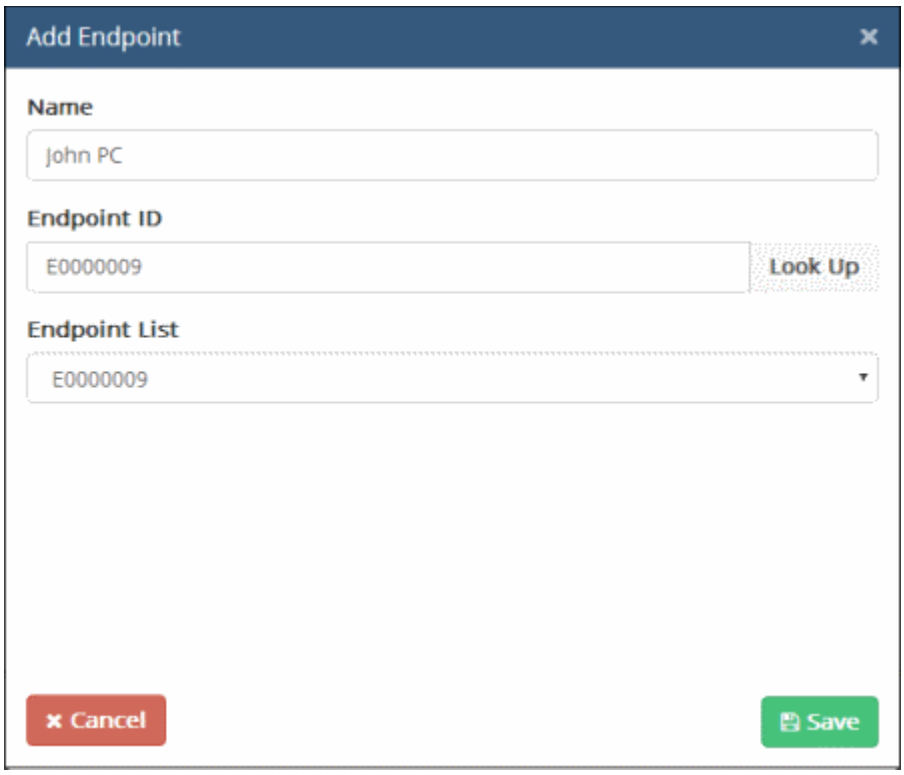
To add an endpoint object

1. Click the 'Policy' tab at the top and then 'Endpoint' under 'Source' section.

The 'Endpoint Objects' screen will be displayed:



2. Click 'Add' at the top right. The 'Add Endpoint' dialog will appear.

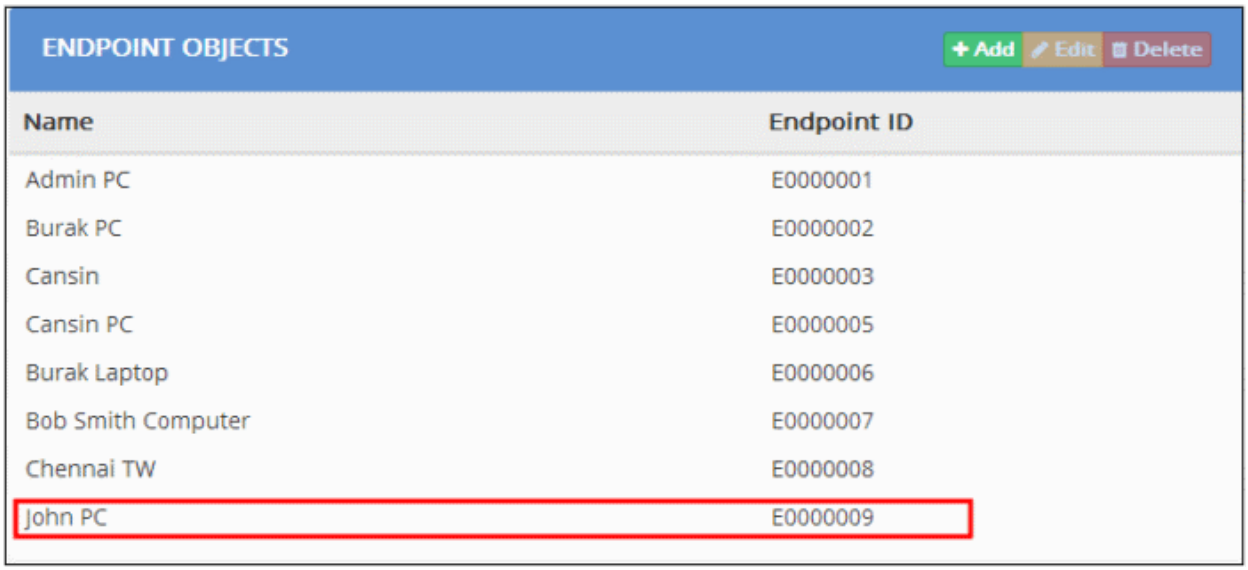


3. Enter the parameters:
    - Name - Enter a name shortly describing the computer
    - Endpoint ID – You can search for particular endpoint. Type the first few characters of the endpoint ID and click Look up. All the ID numbers matching the first few characters will be listed under Endpoint List.
    - Endpoint List – Displays all the endpoints or the endpoints that matches the search parameters entered in Endpoint ID field. To display the full list, clear the Endpoint ID field and click 'Look Up'.
        - Select the ID of the endpoint to be specified in the endpoint object

Tip: You can get the Endpoint ID of the computer to be added as endpoint object from the Endpoints Interface. Open the Endpoints interface by clicking the 'Endpoints' tab. The list of computers added to the MyDLP server is displayed with the Endpoint ID in the first column. For more details, refer to the chapter **The Endpoints**.

4. Click 'Save'.

The new user defined endpoint name object will be listed in the Endpoint Objects screen.



- To edit the details of an endpoint object, select it, click 'Edit' and modify the details as explained above.
- To remove an endpoint object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

5.2.3.4. Adding a User Defined Information Type

MyDLP is shipped with a number of pre-defined Information Types. If required, the administrator can also create custom Information Types. These types can be used in following types of rules;

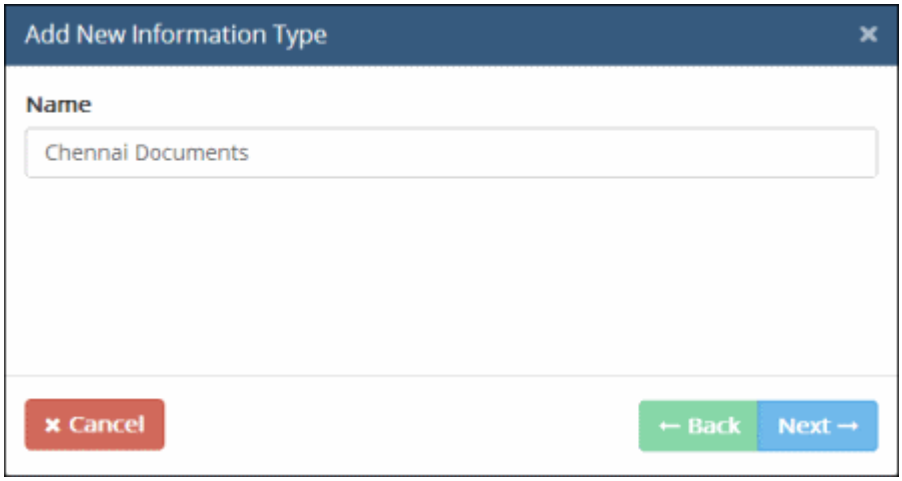
- Web Rule
- Mail Rule
- Removable Storage Rule
- Printer Rule
- API Rule
- Clipboard Rule
- Endpoint Discovery Rule
- Remote Storage Discovery Rule

To define a custom information type

1. Click the 'Policy' tab at the top and then 'Information Type' under 'Information Type' section.

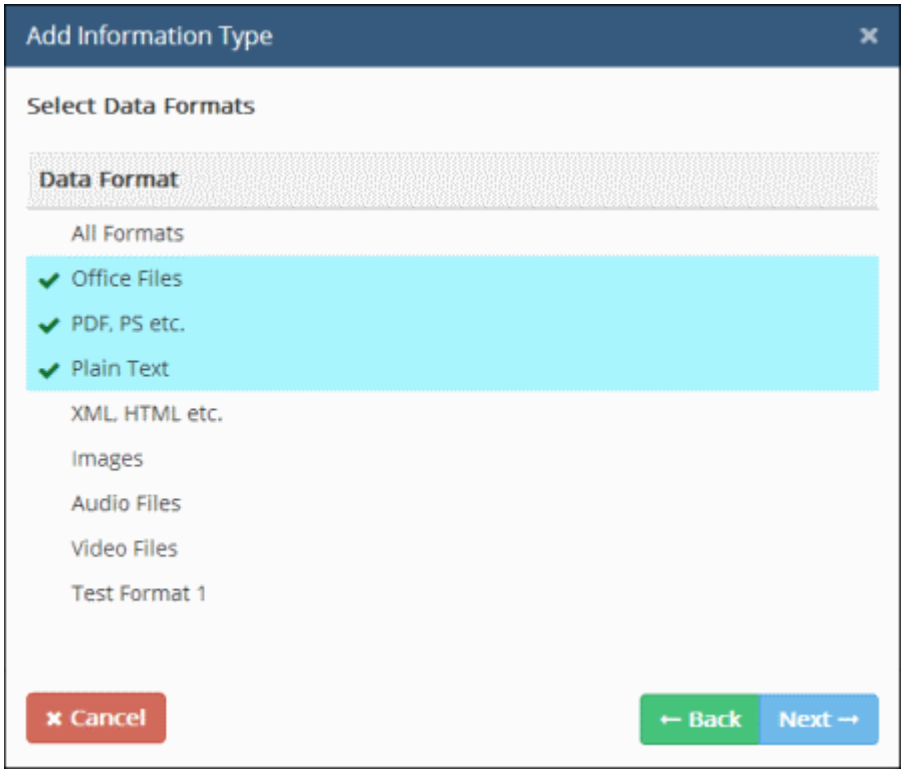
The 'Information Types' screen will be displayed:

2. Click 'Add' at the top right. The 'Add New Information Type' dialog will appear.



3. Enter a name shortly describing the information type, in the 'Name' field and click 'Next'.

The Select Data Formats dialog will be displayed:

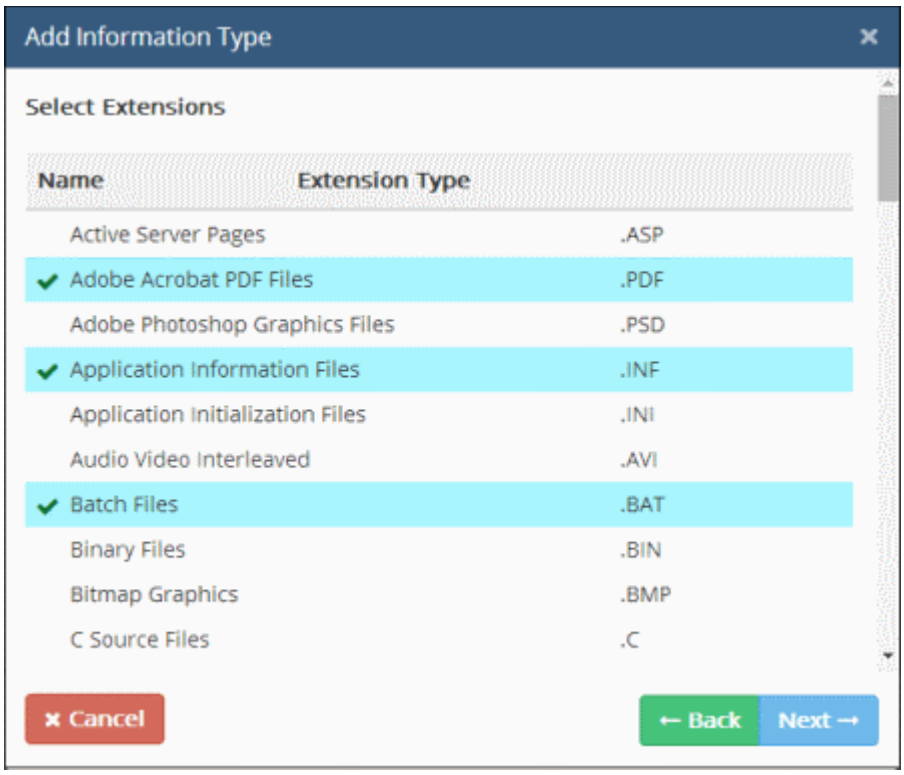


4. Select the file format(s) to be included in the information type object from the list. To remove a format, just deselect it. Refer to the explanation of **Data Formats** under the section **Information Types - An Overview** for more details about data formats.

Tip: In addition to the predefined file formats in the list of available file formats, the administrator can add custom file types as 'Data Formats' to the list from the 'Data Formats' interface. Refer to the section **Managing Data Formats** under **Matchers** for more details.

5. Click 'Next'

The Select Extensions dialog will be displayed:

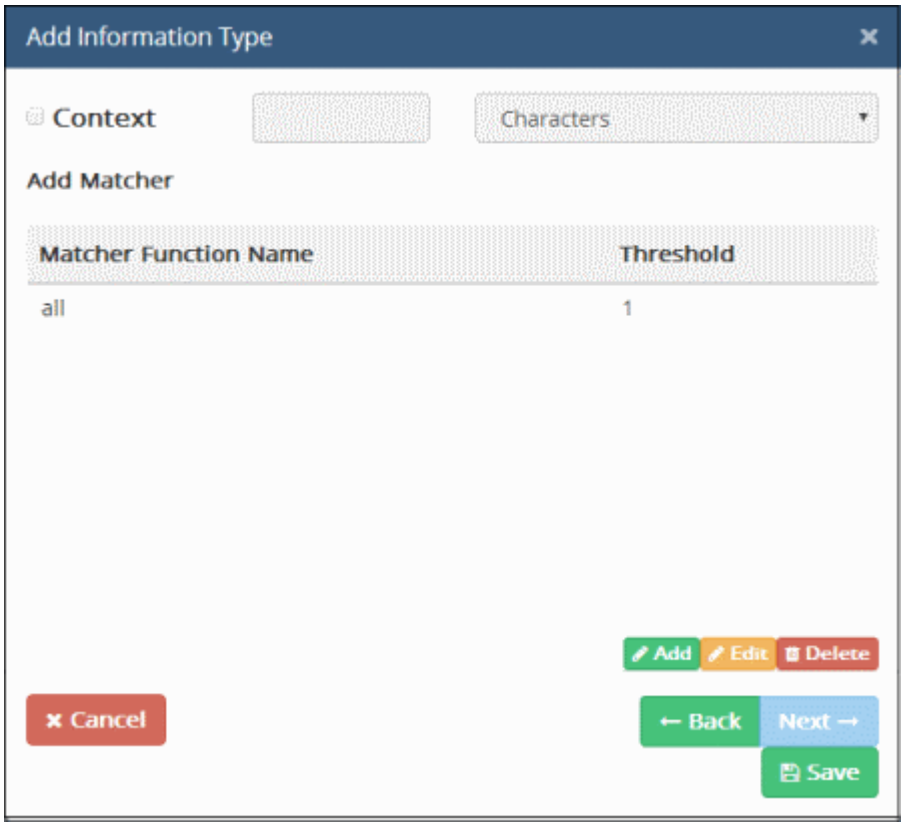


6. Select the extension type(s) to be included in the information type object from the list. To remove an extension, just deselect it.

Tip: In addition to the predefined file extensions in the list of available extensions, the administrator can add custom extension types as 'File Extensions' to the list from the 'File Extensions' interface. Refer to the section **Managing File Extensions** under **Matchers** for more details.

7. Click 'Next'

The 'Add Matcher' and 'Context' dialog will be displayed:

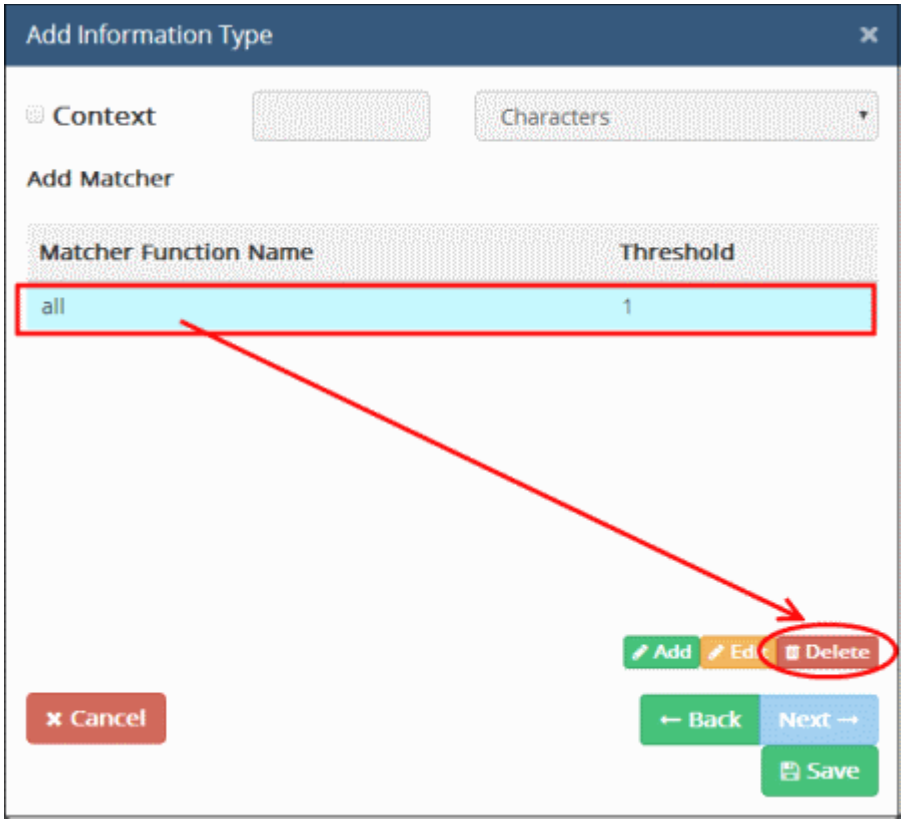


By default, 'All Matcher' will be selected. The full list of available matchers and their descriptions is available in the section **Pre-defined Matcher Types**.

8. Configuring the Matcher and Context parameters. Refer to the explanation of **Information Features** under the section **Information Types - An Overview** for more details on the components of the Information Feature.

Step 1 – Configuring the matcher

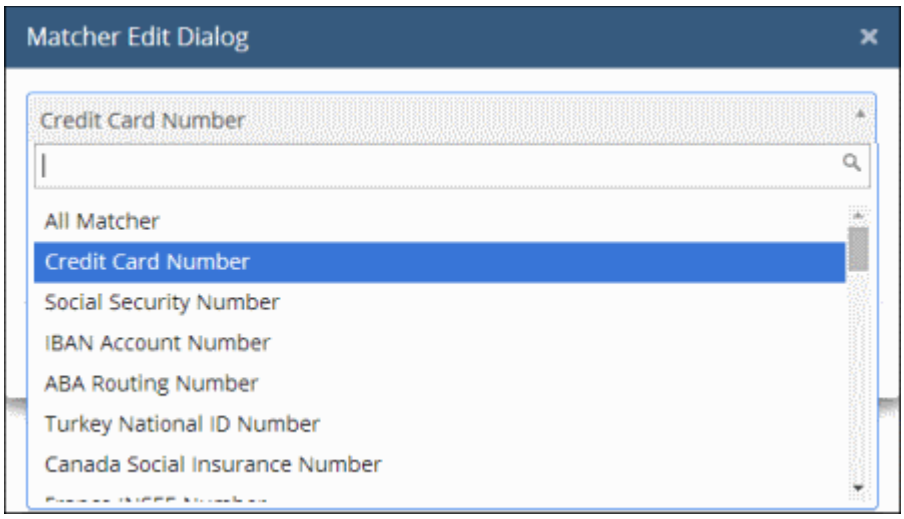
- For 'All Matcher', the 'Context' will be disabled.
- To add specific matcher(s), first select 'all' and click 'Delete'.



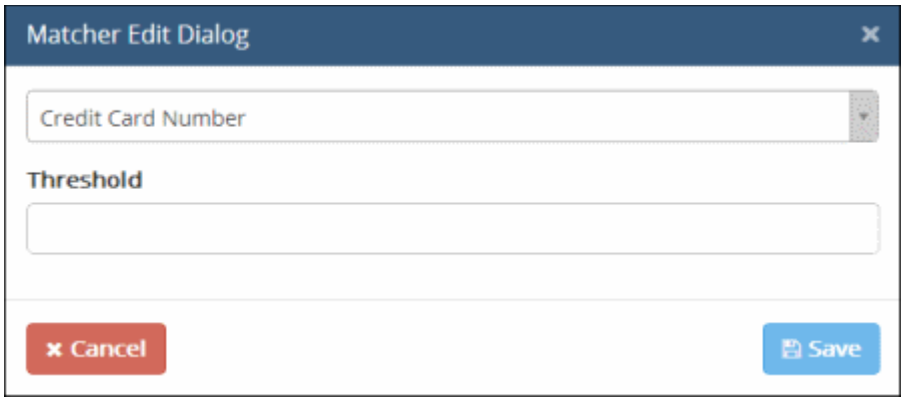
- Next, click the 'Add' button

The 'Matcher Edit Dialog' will be displayed:

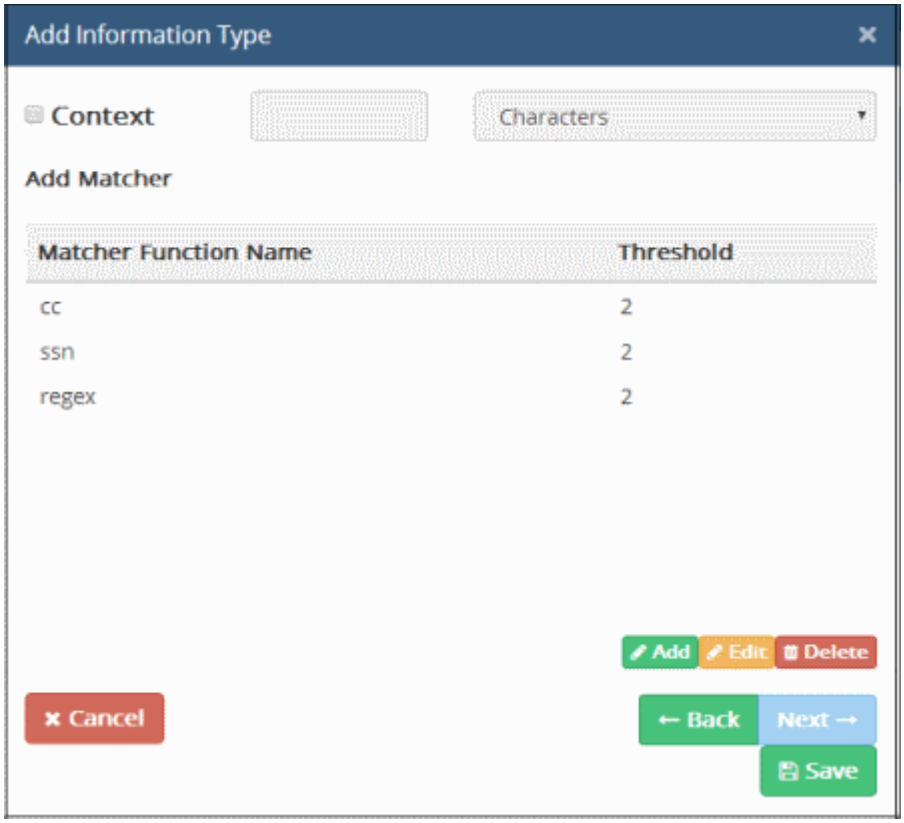
- Click on the drop-down and select the matcher from the list. The full list of available matchers and their descriptions is available in the section **Pre-defined Matcher Types**.



- Enter the minimum number of times the matcher terms to be identified in the document file for deciding it as the specified information type, in the 'Threshold' field.



- Click 'Save'. The matcher will be added to the list.
- Repeat the process to add more number of matchers.



You can edit or remove any matcher at any time.

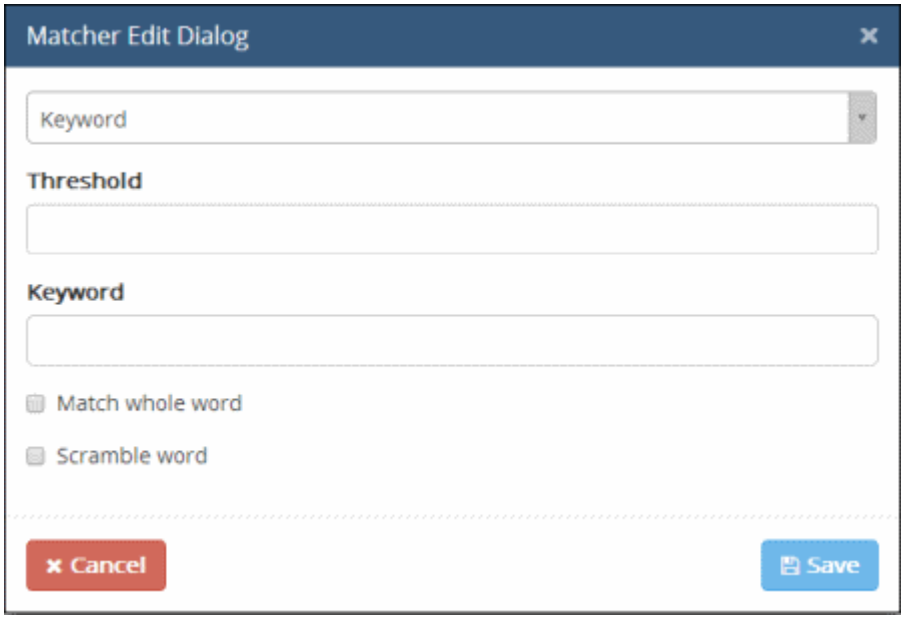
To edit a matcher

- Select the matcher from the list, click 'Edit' and modify the details from the 'Matcher Edit Dialog'
- Click Save for your changes to take effect

To remove a matcher

- Select the matcher from the list and click 'Delete'
- The matcher will be removed from the list

Note: If you are adding 'Keyword' as the matcher type, enter the keyword to be searched in the document files to identify the information and also configure the search options.



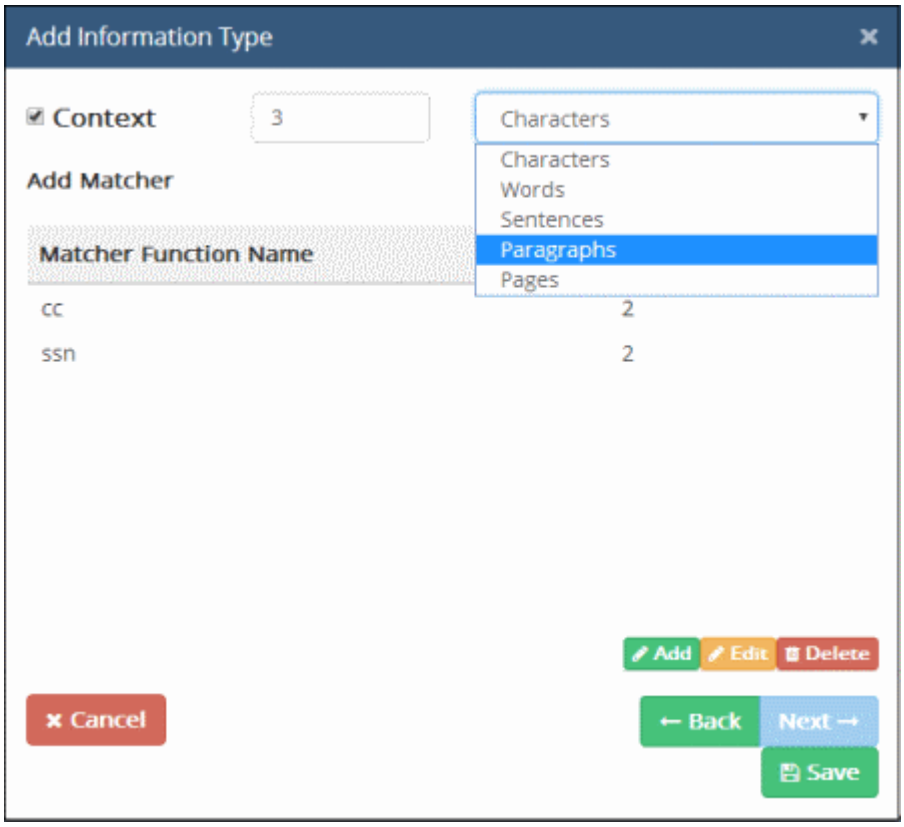
- Keyword - Enter the keyword to be included as the matcher
- Match whole word - Selecting this option will count only the occurrences of the keyword as full word. Else partial occurrences will also be counted
- Scramble words - Selecting this option will count the occurrences of the keyword even if it is scrambled

Please note the matchers, 'Document Database (PDM)', 'Document Database (Hash)' and 'Keyword Group', will allow you to add predefined / customized parameters fetched from the respective sections. Refer to the sections '**Managing Document Databases**' and '**Managing Keyword Groups**' for more details.

Step 2 - Specify the Context parameter (Optional)

If you wish to specify minimum extent of text within which the data or information matching the matchers occur for the file to be considered as the information type, enable the Context parameter and specify the text size.

- Enable 'Context' parameter by selecting the 'Context' checkbox



- Choose the text unit i.e. characters, words, sentences, paragraphs or pages from the drop-down and enter the number of such units within which the matching term should occur for number of times as specified in the threshold, in the text field beside the 'Context' checkbox.

9. Click 'Back' to review the configurations.
10. Click 'Save' to add the new Information Type.

The added 'Information Type' can now be used while constructing data transfer and data discovery rules.

- To edit the details of an information type object, select it, click 'Edit' and modify the details as explained above.
- To remove an information type object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

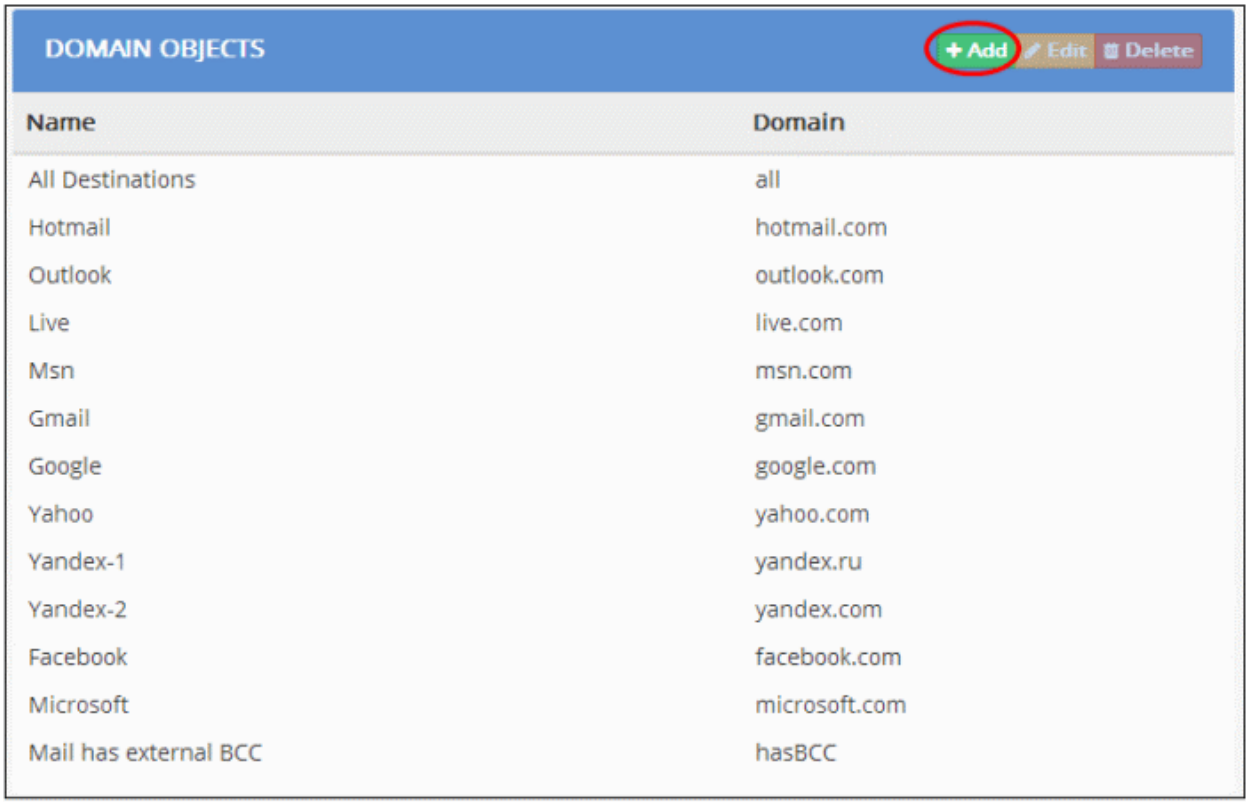
5.2.3.5. Adding a User Defined Domain Object

Comodo MyDLP ships with a number of pre-defined domain objects including commonly used email domains. These domains can be specified for destination component for **web rules** and **email rules**. In addition, administrator can add custom domains for use in web and email rules.

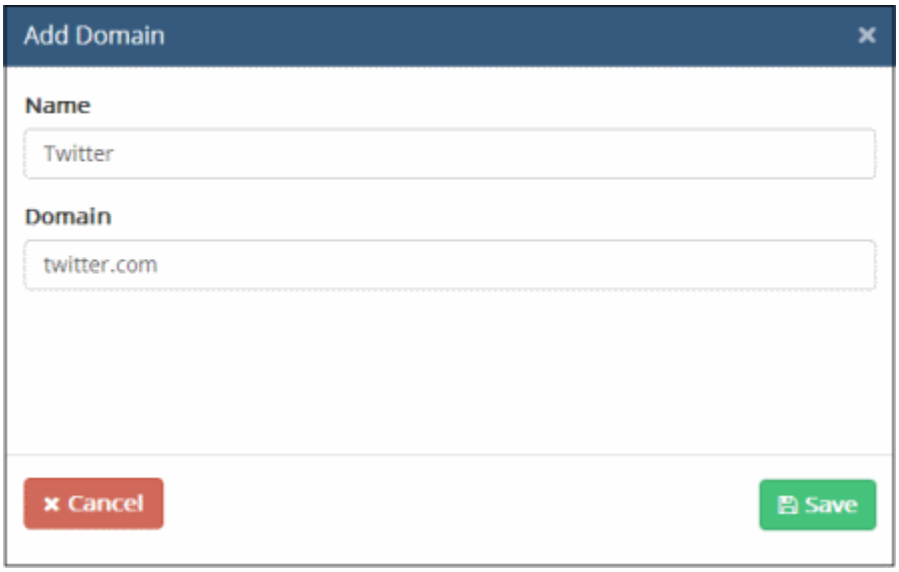
To add a new domain name

1. Click the 'Policy' tab at the top and then 'Domain' under 'Source' or 'Destination' sections

The 'Domain Objects' screen will be displayed:



2. Click 'Add' at the top right. The 'Add Network' dialog will appear.



3. Enter the parameters:

- Name - Enter a descriptive name for the domain object
- Domain - Enter the domain name or the full URL to be added

4. Click 'Save'.

The new user defined network object will be listed in the 'Network Objects' screen.

- To edit the details of a domain object, select it, click 'Edit' and modify the details as explained above.
- To remove a domain object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

Please note you cannot edit or delete a predefined domain object.

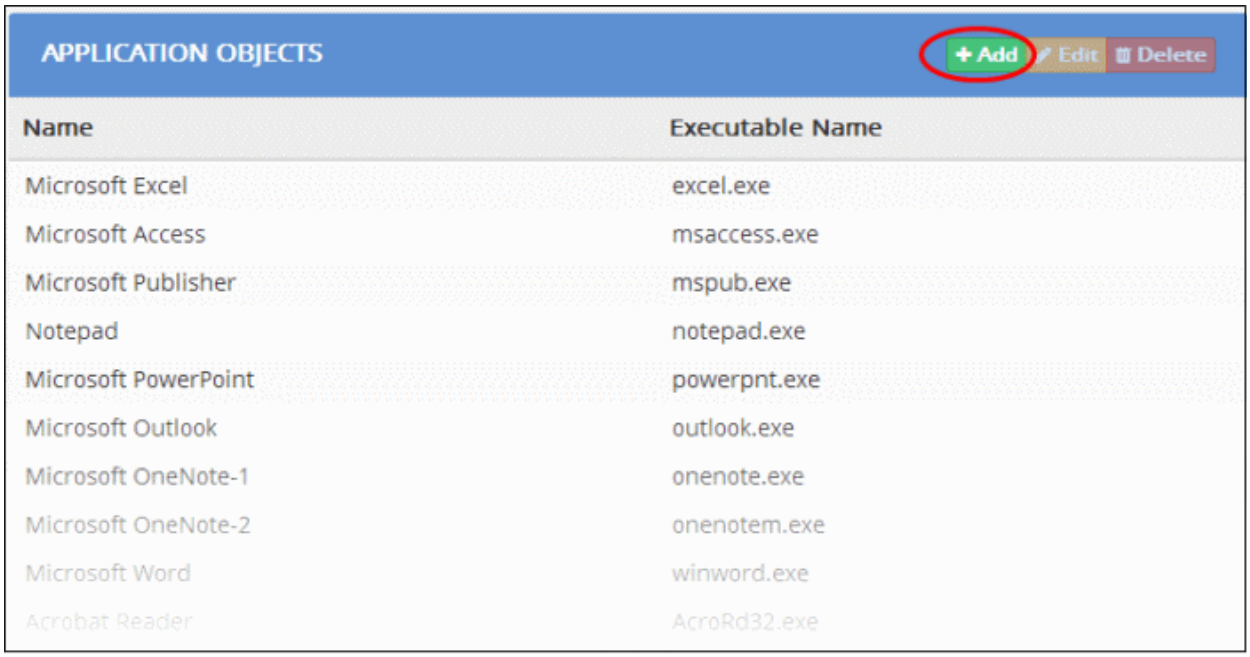
5.2.3.6. Adding a User Defined Application Object

Comodo MyDLP ships with a number of pre-defined Application objects including commonly used Internet browsers, Design applications, Microsoft Office applications, and PDF viewers under Source > Application interface. These applications can be specified for destination component for **Screenshot rules**. In addition, administrator can add custom application names for use in Screenshot rules.

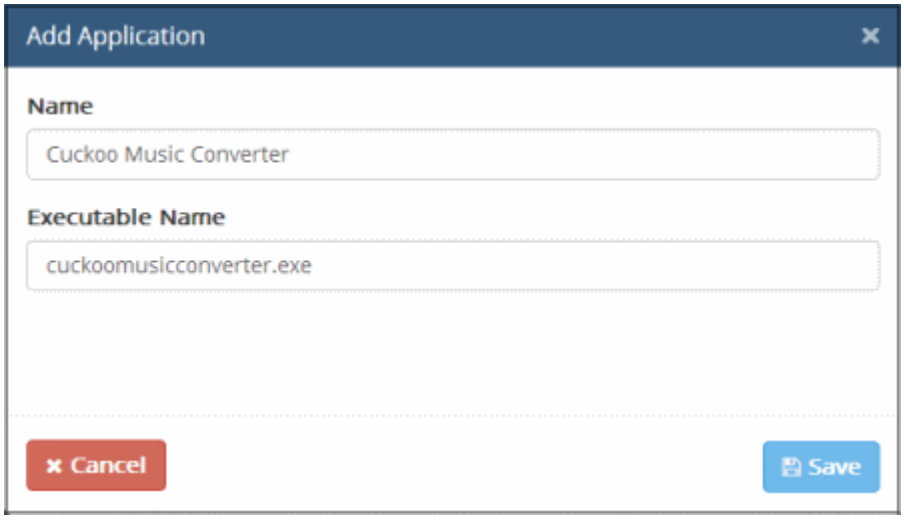
To add a new Application object

1. Click the 'Policy' tab at the top and then 'Application' under 'Destination' section

The 'Application Objects' screen will be displayed:

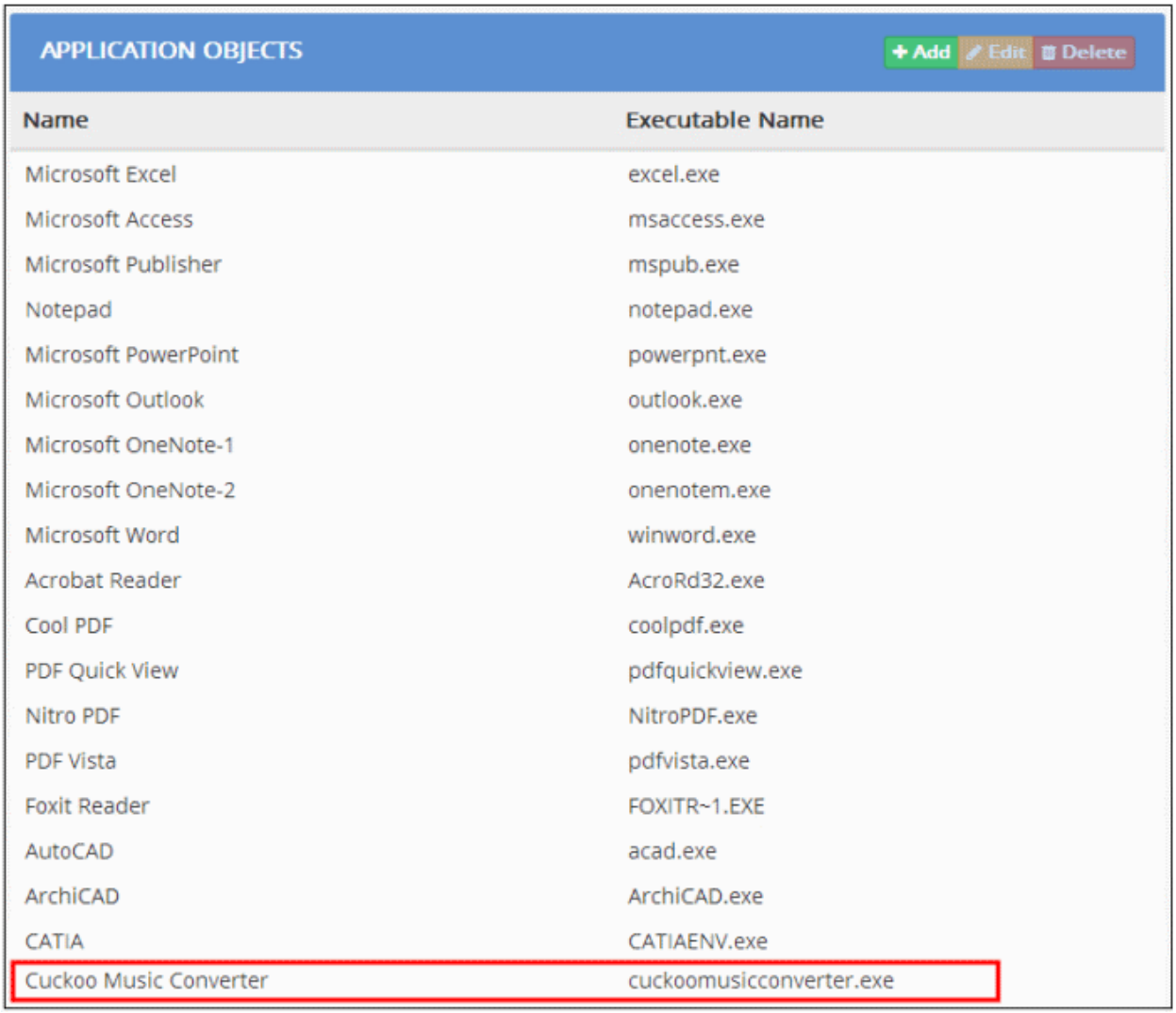


2. Click 'Add' at the top right. The 'Add Application' dialog will appear.



3. Enter the parameters:
   - Name - Enter a descriptive name for the Application
   - Executable Name - Enter the file name of the application executable of the program, with the file extension.
4. Click 'Save'.

The new user defined application object will be listed in the 'Application Objects' screen.



- To edit the details of an application object, select it, click 'Edit' and modify the details as explained above.
- To remove an application object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

Please note you cannot edit or delete a predefined application object.

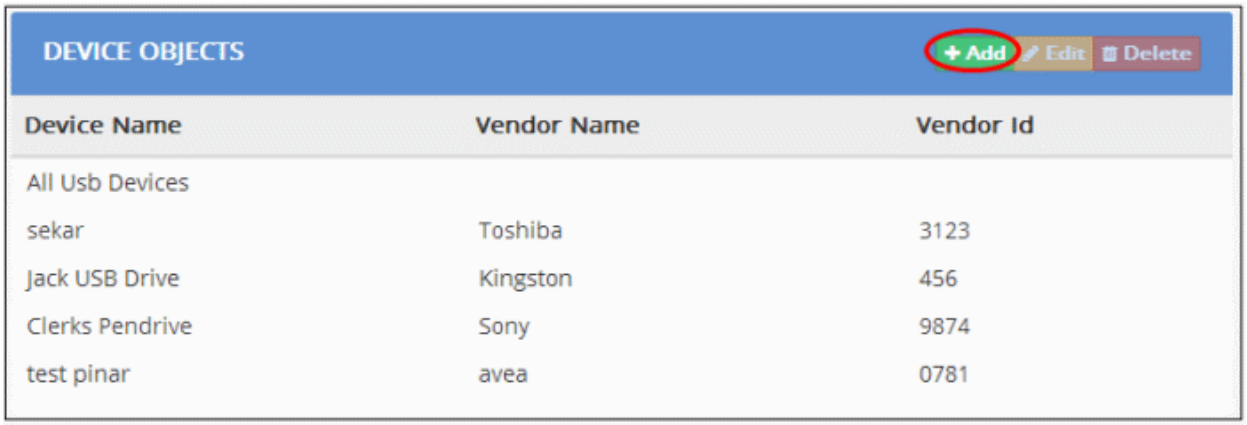
5.2.3.7. Adding a User Defined USB Device Object

USB devices to be specified as destinations in Removable Storage rules, to allow, monitor and control the transfer of data from the endpoints covered by the source object of the rule, are to be added to MyDLP. Only those USB devices pre-added to MyDLP by specifying their vendor ID (VID) and product ID (PID) will be available for selection while creating a rule.

To add a new USB Device object

1. Click the 'Policy' tab at the top and then 'Devices' under 'Destination' section

The 'Device Objects' screen will be displayed:



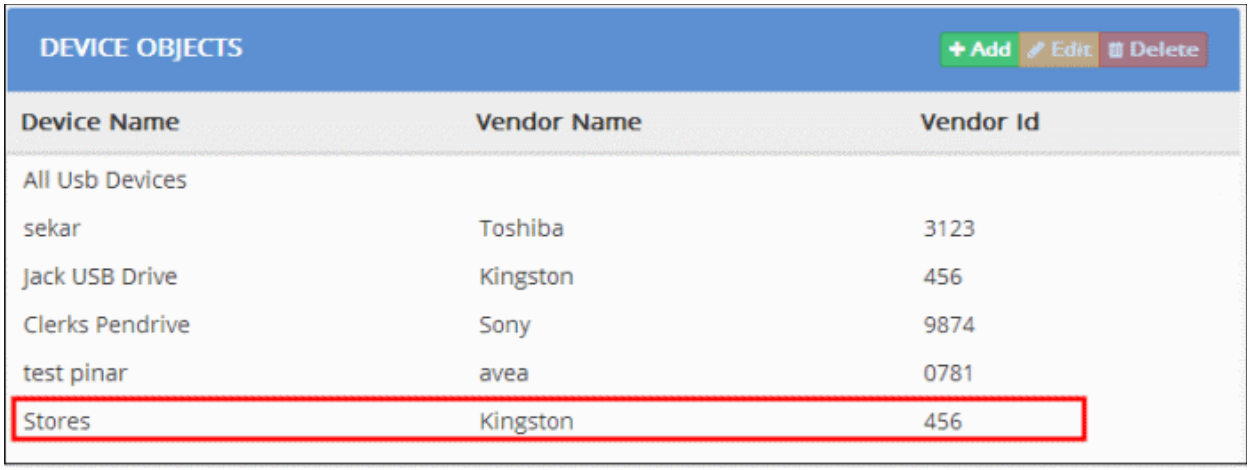
2. Click 'Add' at the top right. The 'Add Device' dialog will appear.

3. Enter the parameters:
   - Device Name - Enter a name shortly describing the device object
   - Vendor Name - Enter the name of the device vendor
   - Vendor ID – Enter the ID of the vendor

Refer to the section **Identifying Vendor ID** for explanation on finding the vendor ID of the device.

4. Click 'Save'.

The new user device object will be listed in the 'Device Objects' screen.



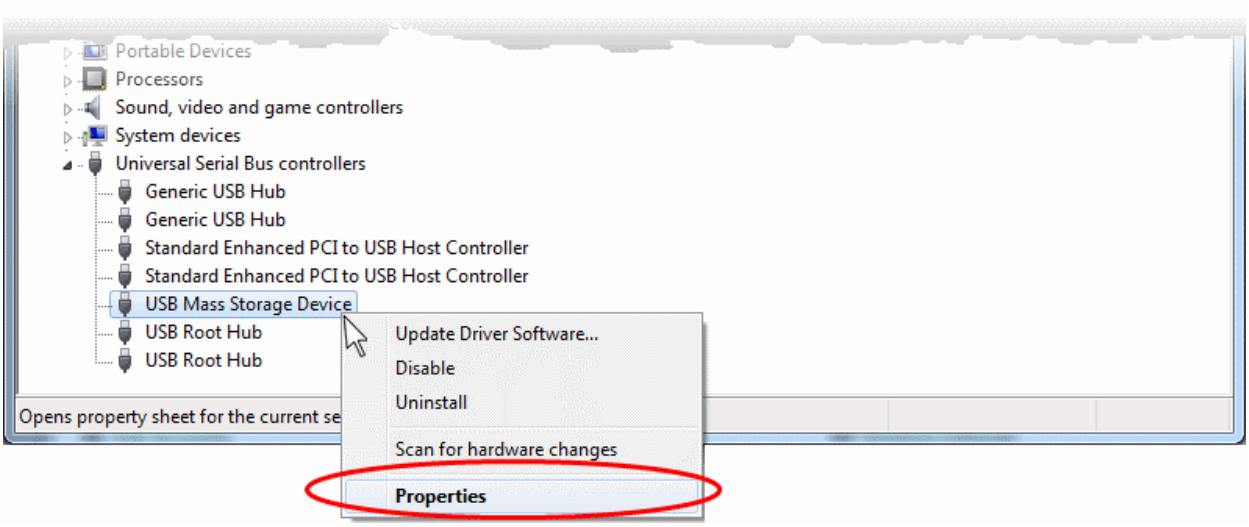
- To edit the details of a device object, select it, click 'Edit' and modify the details as explained above.
- To remove a device object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

Identifying Vendor ID and Product ID of a USB Device

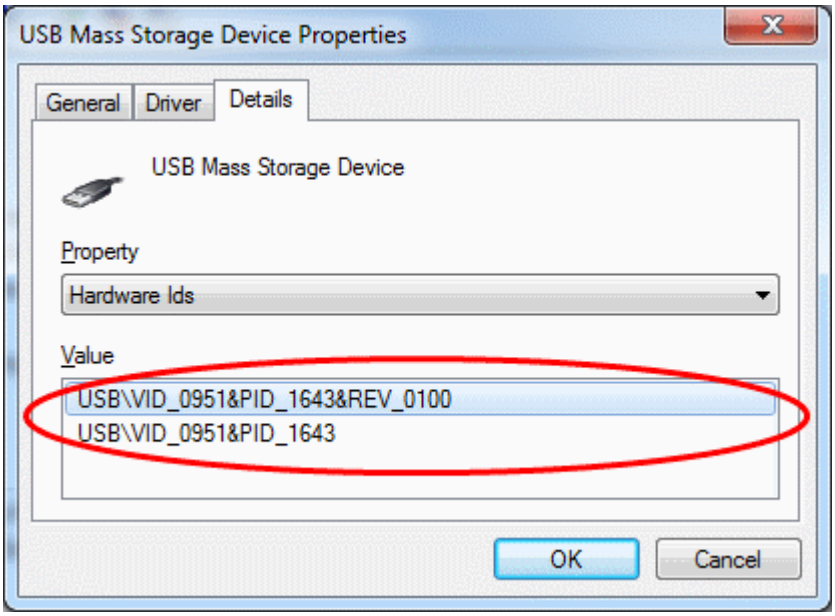
The VID and PID of a USB device can be identified by plugging-in it on a computer and viewing its properties.

To obtain the VID and PID of a USB Device

- Plug-in the device to a computer.
- Click 'Start' > 'Control Panel' > 'Device Manager'.
- Expand the 'Universal Serial Bus Controllers' category to view the list of USB ports.
- Right click on the port at which the device is connected and choose 'Properties'.



- In the 'Properties' interface, select 'Details' tab and choose 'Hardware Ids' from the 'Property' drop-down.



The 'Values' field displays the 'VID' and 'PID' of the device. In the example shown above, VID is 0951 and PID is 1643.

5.2.3.8. Adding a User Defined User Object

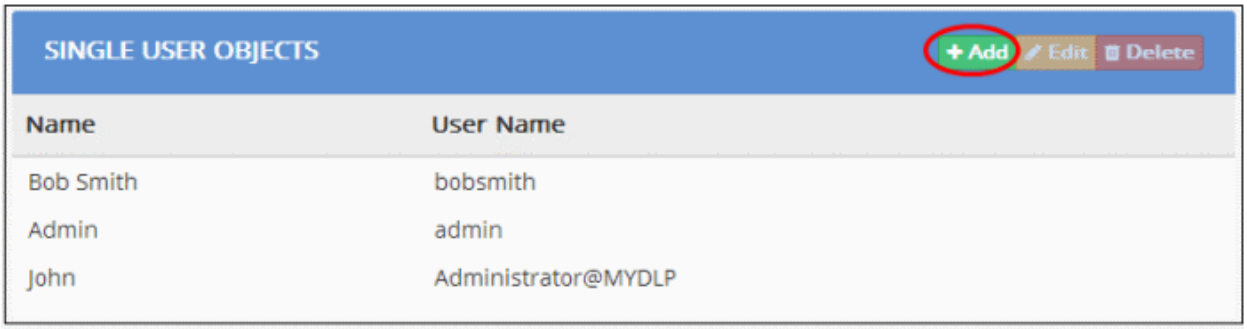
The administrator can add new end user objects to MyDLP to inspect the data traffic from the respective users logged-in from different computers in the network. Multiple users can also be added at once by importing from Active Directory (AD). The AD domain is to be integrated to the MyDLP server prior to importing from the AD. Refer to the section **Adding a User Defined Active Directory Users Object** for more details. This section explains how to add single user objects. The new users can be defined as source in data transfer policy rules.

Prerequisite: The endpoints are to be installed with the MyDLP Endpoint Agent before adding them as Computer Name Objects. The endpoints installed with the agent are listed with their Endpoint IDs, Logged-in Usernames and Computer Names under the **Endpoints** tab. Refer to the **MyDLP Endpoint Installation Guide** for explanations on installing the agent.

To add a new user object

1. Click the 'Policy' tab at the top and then 'User' under 'Source' or 'Destination' sections

The 'Single User Objects' screen will be displayed:



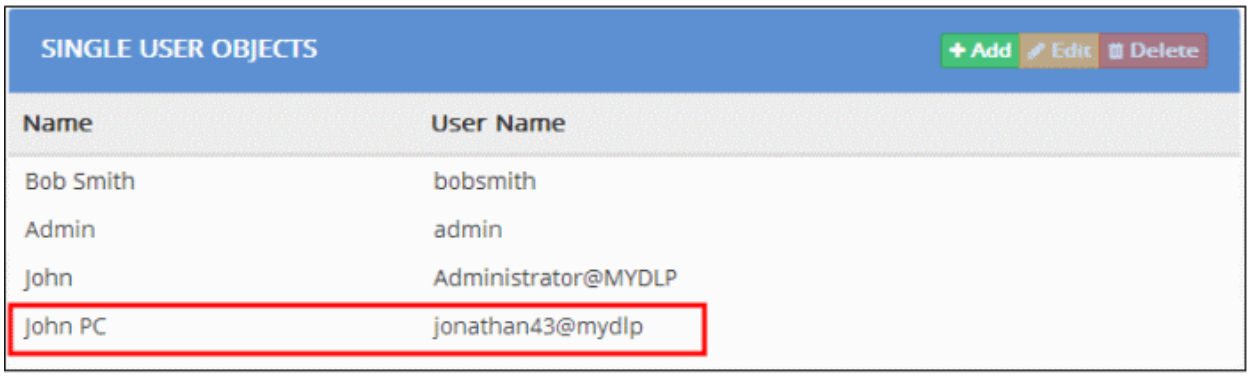
2. Click 'Add' at the top right. The 'Add Single User' dialog will appear.

3. Enter the parameters:
    - Name - Enter the name to identify the user
    - Username - Enter the username of the user. The user name can be obtained in two ways:
        - The username as per the Active Directory user account, e.g. user@domain.com.
        - The email address of the user, e.g. user@domain.com.

Tip: The user is currently logged-in, the username can be obtained from the 'Endpoints' interface. Refer to the section **The Endpoints Tab** for more details.

4. Click 'Save'.

The new user defined single user object will be listed in the 'Single User Objects' screen.



- To edit the details of a user object, select it, click 'Edit' and modify the details as explained above.
- To remove a single user object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

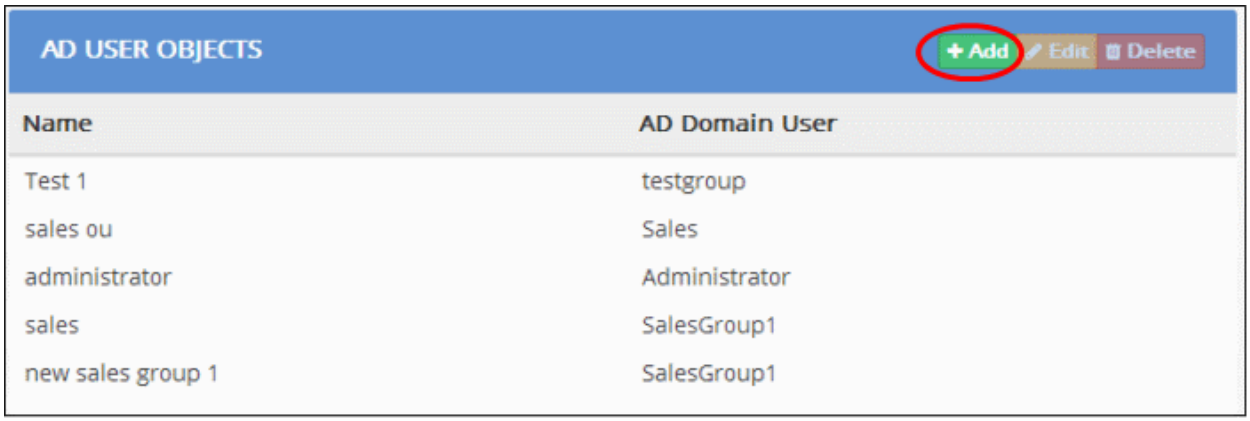
5.2.3.9. Adding a User Defined Active Directory Users Object

Administrators have the option to add multiple user objects from Active Directory in addition to adding single user object explained in the previous section **Adding a User Defined Users Object**. In order to add bulk users, you have to first integrate Active Directory domains into MyDLP. Refer to the section **Integration with Active Directory Domain** for more details.

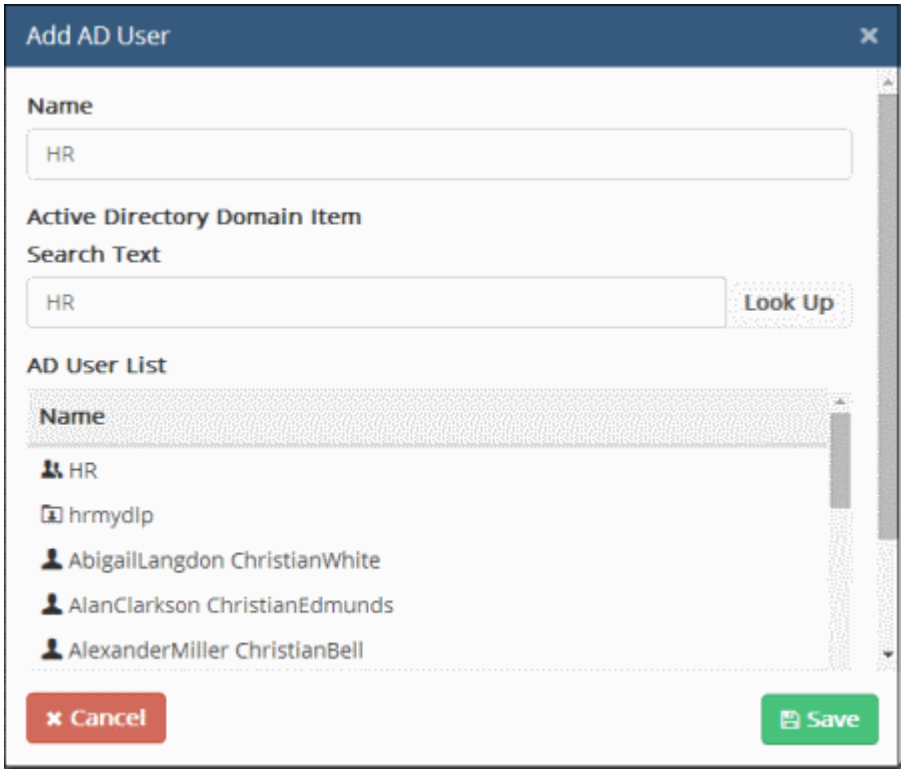
To import Users from AD domain

1. Click the 'Policy' tab at the top and then 'AD User' under 'Source' or 'Destination' sections

The 'AD User Objects' screen will be displayed:

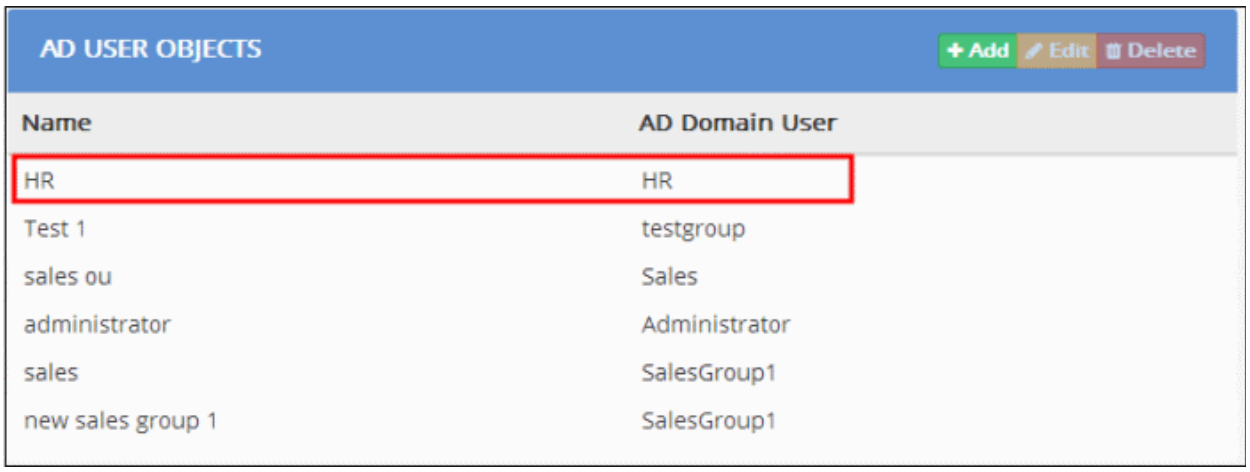


2. Click 'Add' at the top right. The 'Add AD User' dialog will appear.



3. Enter the name to identify the user in the 'Name' field.
4. To search for the specific user from the pre-integrated AD Server, type the first three two or letters of the user name as per the Active Directory user account in the 'Search Text' field and click 'Lookup'. The matching user names will be shown as a list in the text box.
5. Choose the user to be added.
6. Click 'Save'.

The new user defined AD user object will be listed in the 'AD User Objects' screen.



- To edit the details of an AD user object, select it, click 'Edit' and modify the details as explained above.
- To remove an AD user object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

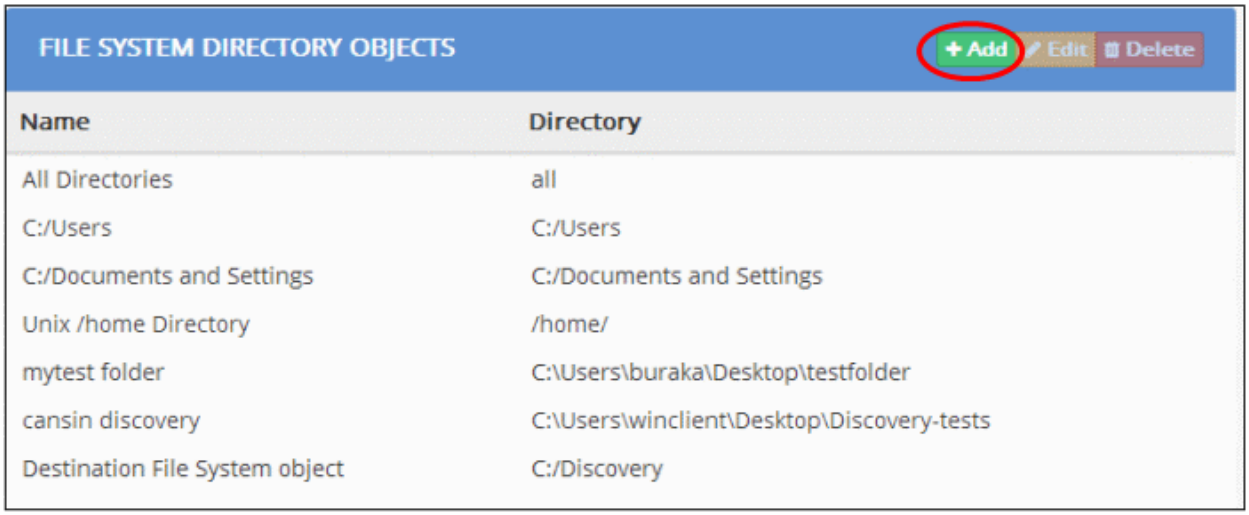
5.2.3.10. Adding a User Defined File System Directory

The administrator can define custom file paths in local drives of endpoint computers, for checking existence of files containing the sensitive information as defined in an Information Type object in a rule. The custom file path can be added as a File System Directory object and can be specified as 'Destination' in **Endpoint Discovery rules**.

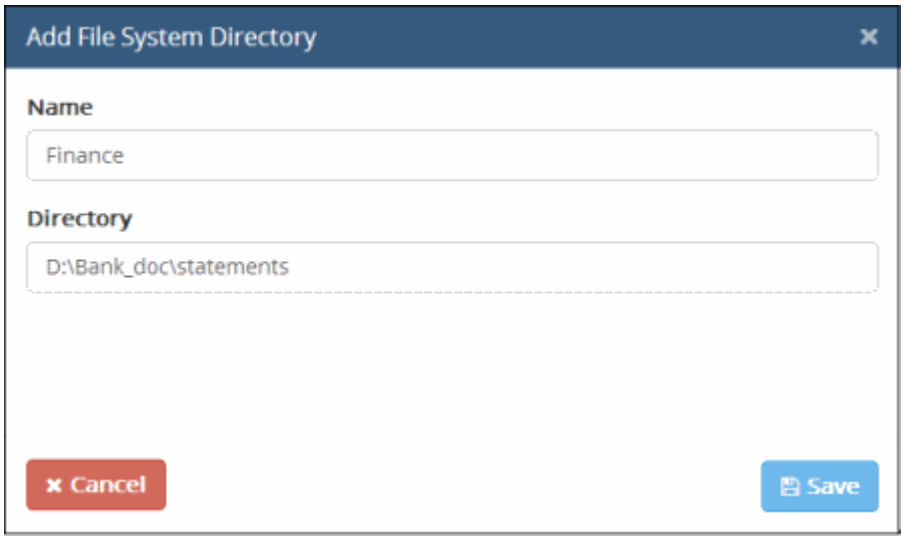
To add a custom file system directory

1. Click the 'Policy' tab at the top and then 'Endpoint File System' under 'Discovery Target' section

The 'File System Directory Objects' screen will be displayed:

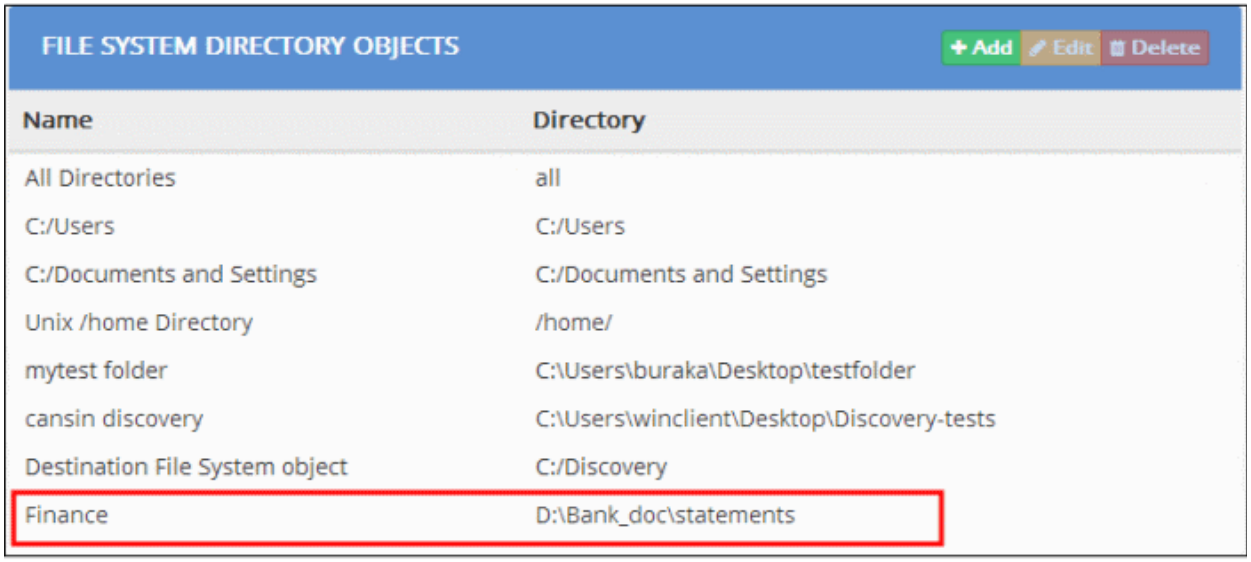


2. Click 'Add' at the top right. The 'Add File System Directory' dialog will appear.



3. Enter the parameters:
   - Name - Enter a name shortly describing the file path
   - Directory - Enter the file path to be checked.
4. Click 'Save'.

The new user defined file system directory object will be listed in the 'File System Directory Objects' screen.



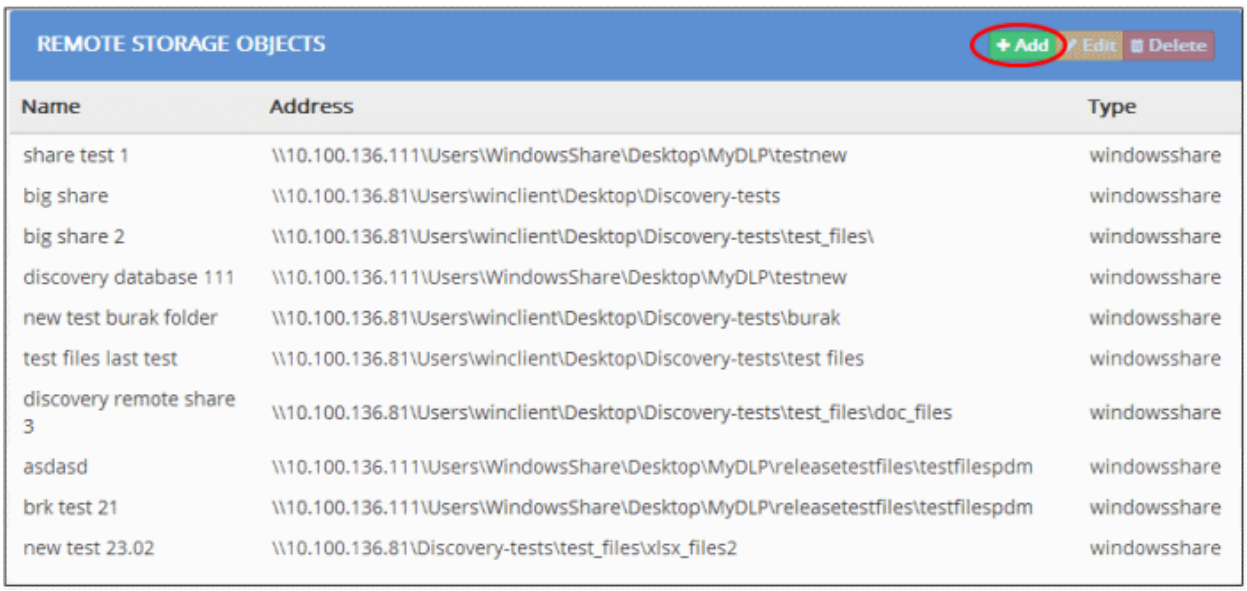
On application of the file system directory object as destination in the rule, MyDLP checks all the files in the specified path, in all the endpoints added as 'Sources' in the rule. If the file path is not present in any of the endpoint included as the sources, then those endpoints will be skipped.

5.2.3.11. Adding a User Defined Remote Storage Object

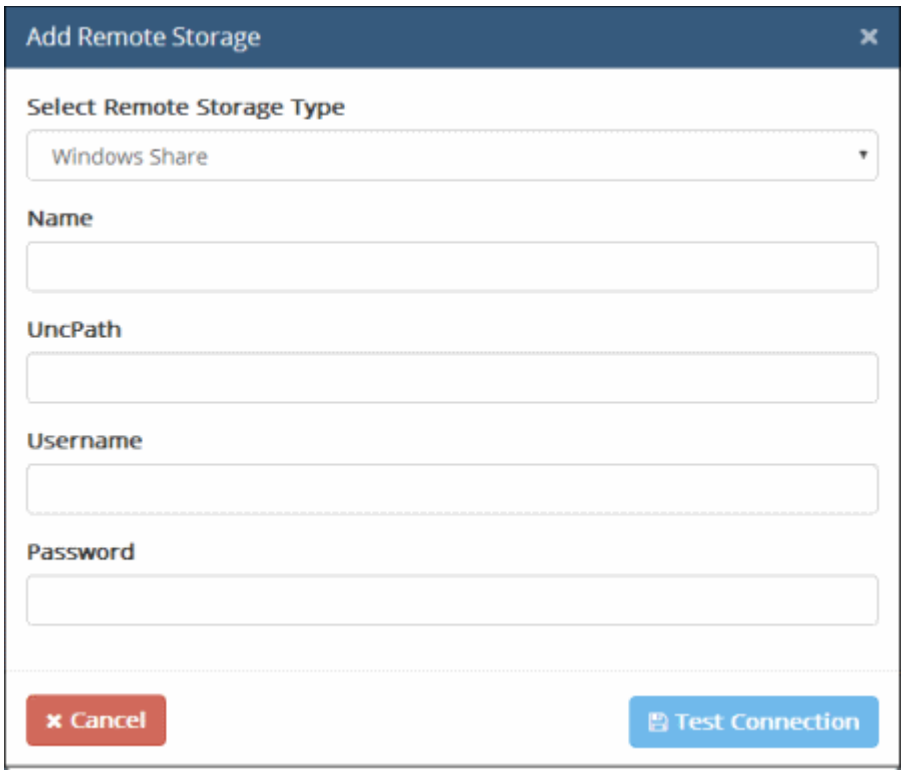
The administrator can create Remote Storage objects to specify network storage and external storage like FTP Server, Microsoft Windows Share folder in any of the endpoints, network file system and so on, for checking existence of files containing the sensitive information as defined in an Information Type object in a rule. The Remote Storage object can be added as 'Source' for a **Remote Storage Rule**.

To add a new Remote Storage object

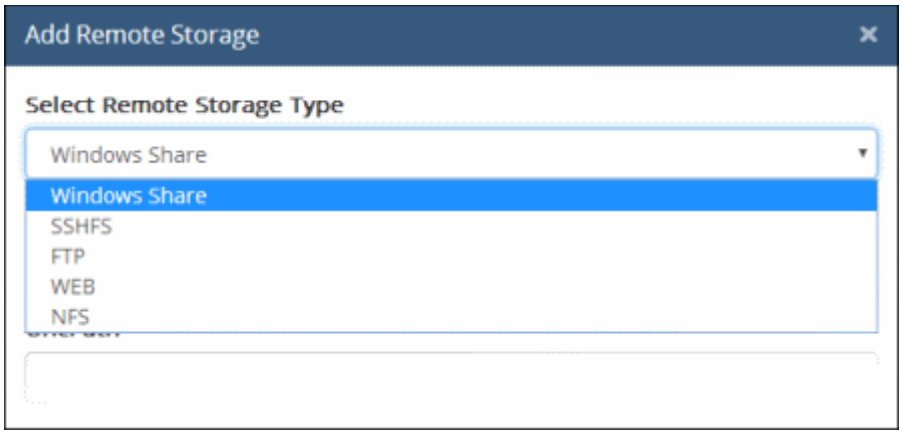
1. Click the 'Policy' tab at the top and then 'Remote Connections' under 'Discovery Target' section



2. Click 'Add' at the top right. The 'Add Remote Storage' dialog will appear.



3. Choose the type of the remote storage you wish to specify for the object from the drop-down.



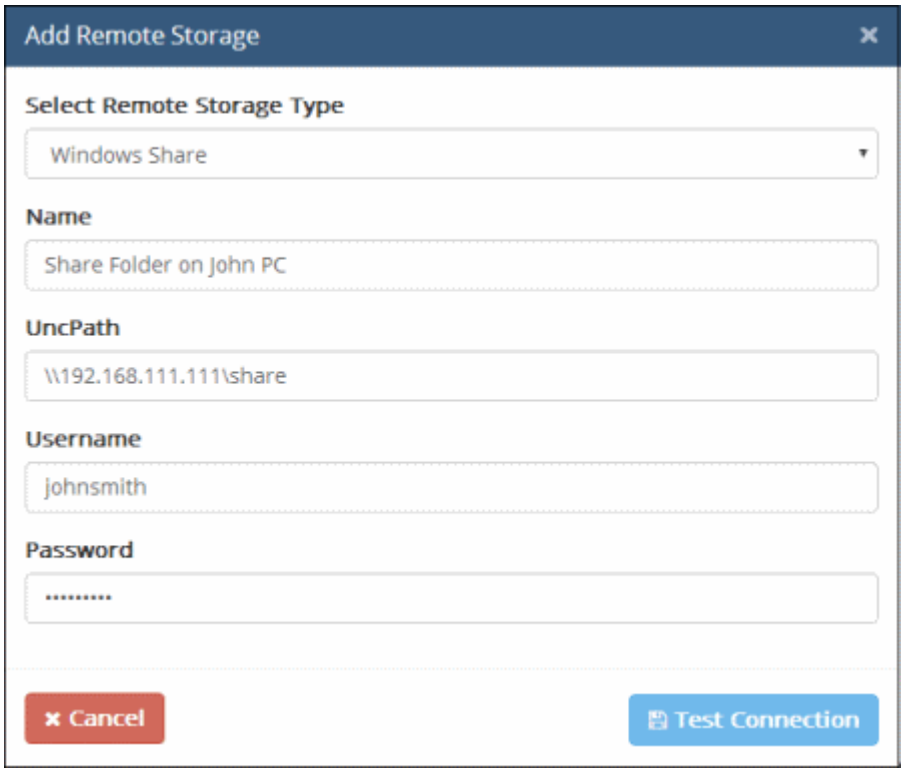
The following sections explain the processes in detail.

- **Windows Share**
- **SSHFS**
- **FTP**
- **WEB**
- **NFS**

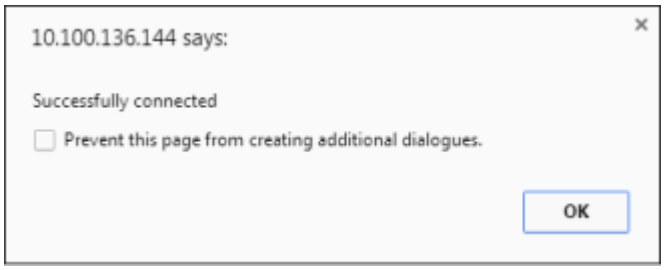
Adding a Shared Storage Location in a Remote Computer in the Network Storage

You can add a shared drive/folder on a computer within the network as a Remote Storage object, by specifying its Universal Naming Convention (UNC) path and login credentials for that computer.

4. Choose 'Windows Share' from the 'Add Remote Storage' dialog.



5. Enter the parameters:
   - Name - Enter a name shortly describing the shared folder or drive
   - UNC Path - Enter the shared file path in the format \\<hostname or IP address of the computer>\<shared folder name>
   - Username/Password - Enter the username and password of the user account that MyDLP can use to login to the server/host
6. Click 'Test Connection'. MyDLP willl check whether the remote storage location is reachable.



On successful connection, the 'Save' button will be enabled.

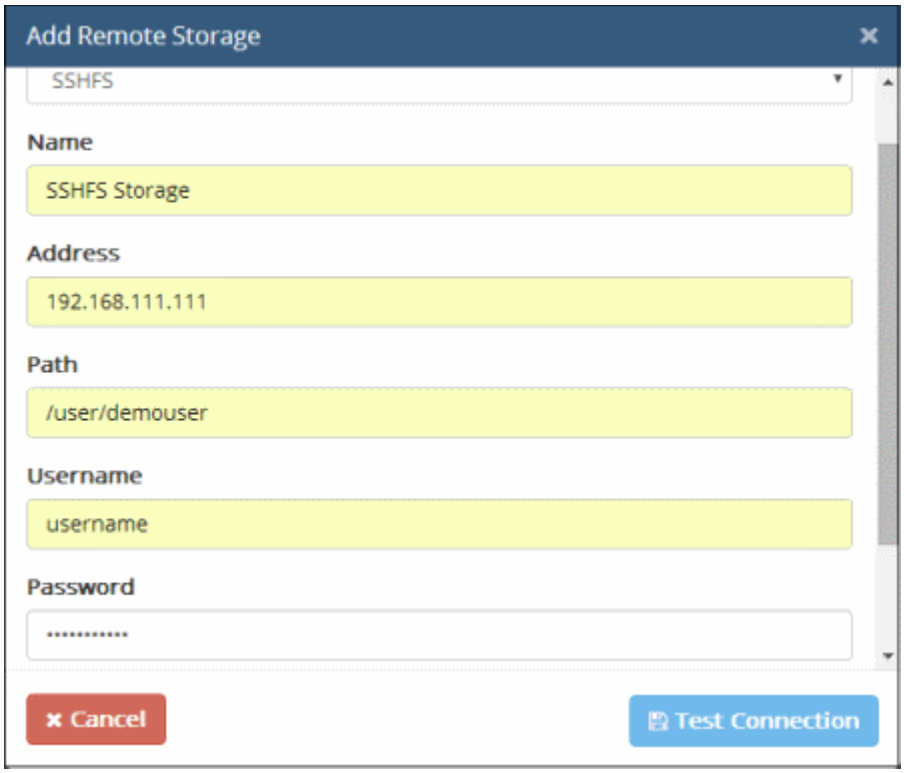
7. Click 'Save'.

The shared drive/folder will be added as a remote storage object and can be used as source for Remote Storage Discovery rule.

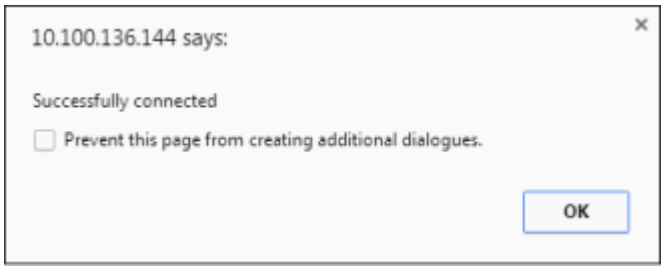
Adding a Remote Storage connected through SSH / SCP / SFTP Protocol (SSHFS)

You can add a remote storage accessed through Secure Shell (SSH) connection, using Secure Copy (SCP) or Secure File Transfer Protocol (SFTP) protocol for file transfer as a remote storage object by selecting SSH / SCP / SFTP Protocol.

4. Choose SSHFS from the ' Add Remote Storage' dialog



5. Enter the parameters:
   - Name - Enter a name shortly describing the SSHFS remote storage
   - Address - Enter the IP address or hostname of the server/host, hosting the remote storage
   - Path - Enter the file path to be checked in the remote storage
   - Username/Password - Enter the username and password of the user account that MyDLP can use to login to the server/host
   - Port - Enter the connection port for SSH connection to the server/host
6. Click 'Test Connection'. MyDLP willl check whether the remote storage location is reachable.



On successful connection, the 'Save' button will be enabled.

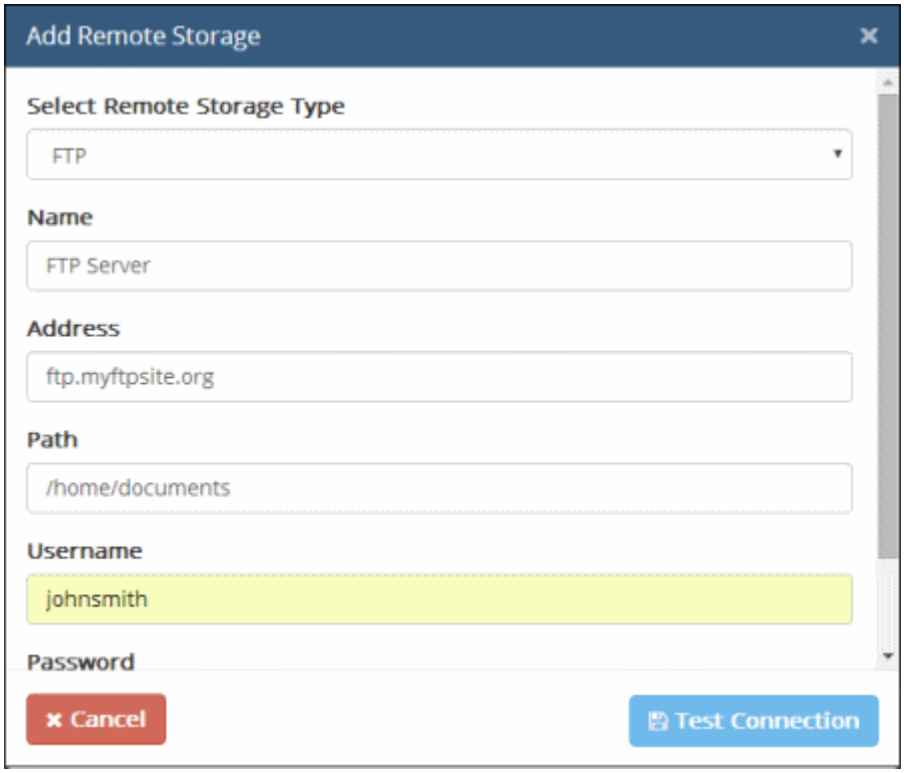
7. Click 'Save'.

The SSHFS will be added as a remote storage object and can be used as source for Remote Storage Discovery rule.

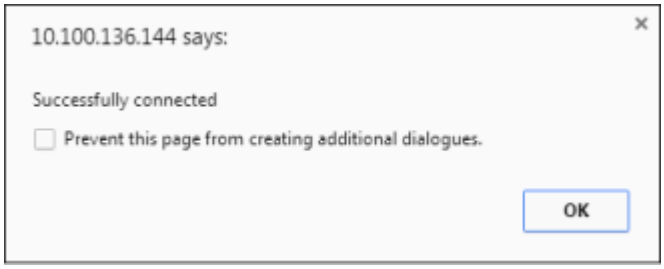
Adding a FTP Server

You can add a FTP server as a remote storage object by specifying its address and login credentials.

4. Choose FTP from the ' Add Remote Storage' dialog



5. Enter the parameters:
   - Name - Enter a name shortly describing the FTP server
   - Address - Enter the IP address or hostname of the FTP server
   - Path - Enter the file path to be checked in the FTP server
   - Username/Password - Enter the username and password of the user account that MyDLP can use to login to the FTP server
6. Click 'Test Connection'. MyDLP willl check whether the remote storage location is reachable.



On successful connection, the 'Save' button will be enabled.

7. Click 'Save'.

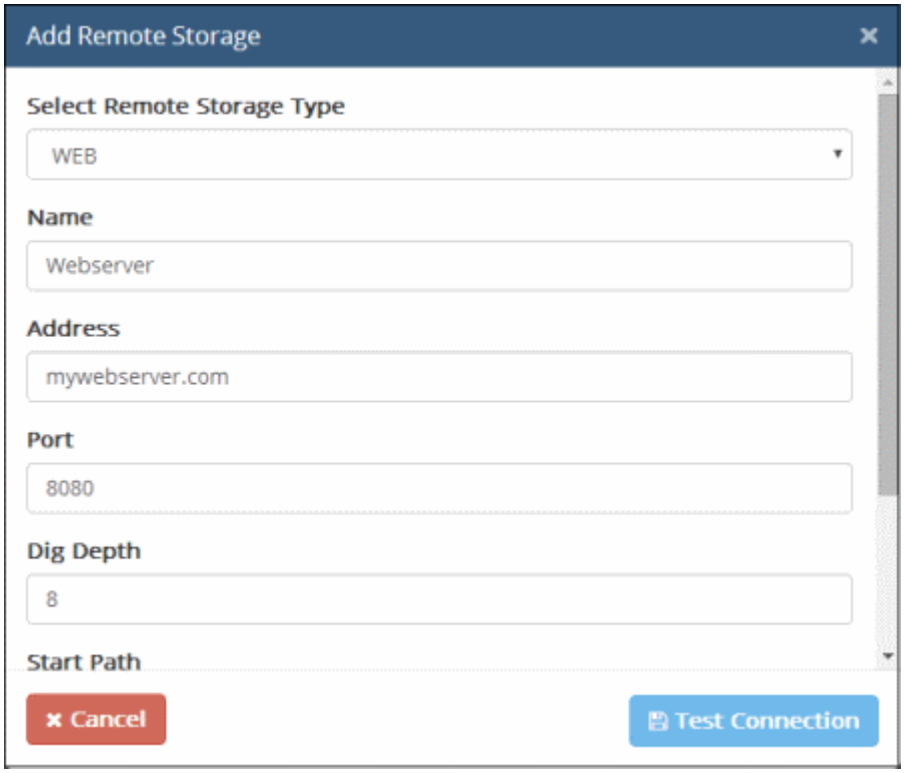
The FTP server will be added as a remote storage object and can be used as source for Remote Storage Discovery rule.

Adding a WEB Server

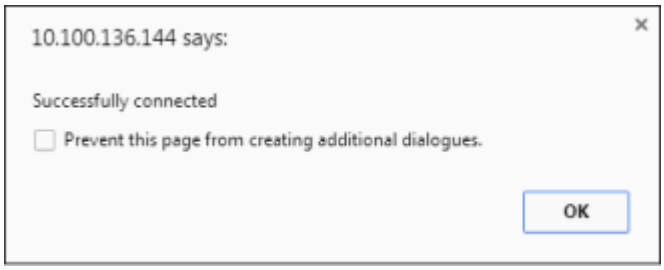
You can add a Web server that can be accessed through HTTP or HTTPS connection, as a remote storage object by

specifying its address.

4. Choose WEB from the ' Add Remote Storage' dialog



5. Enter the parameters:
   - Name - Enter a name shortly describing the Web server
   - Address - Enter the IP address or hostname of the Web server
   - Port – Enter the connection port
   - Dig Depth – Number of links to be followed. Enter the number of level of sub folders from the root to check in the web server.
   - Start Path – Enter the start path from which MyDLP should start the discovery process
6. Click 'Test Connection'. MyDLP willl check whether the remote storage location is reachable.



On successful connection, the 'Save' button will be enabled.

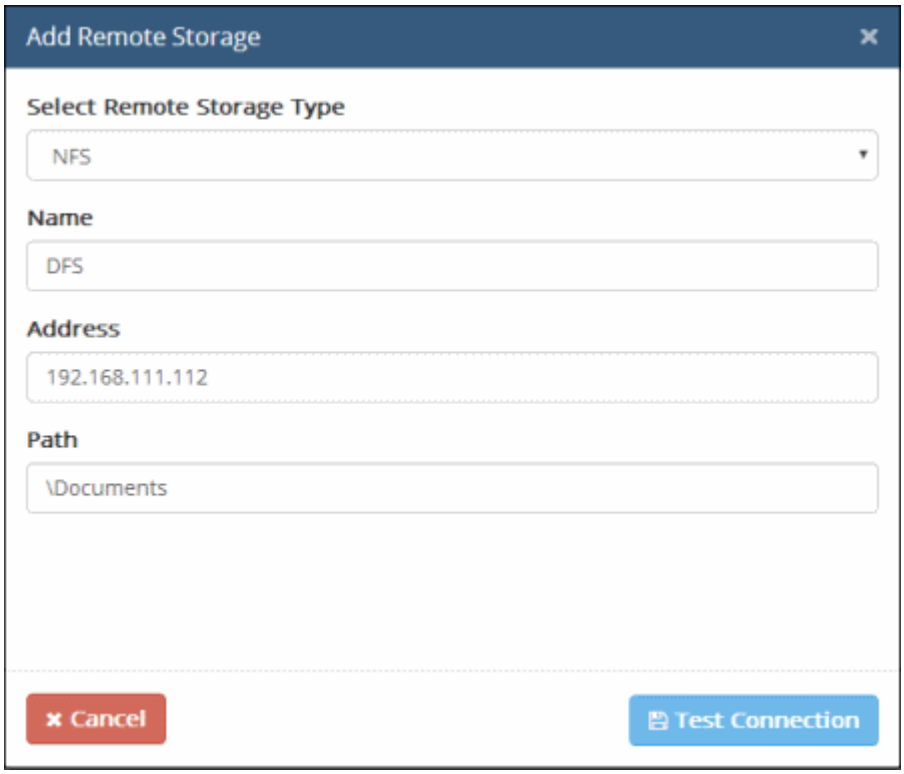
7. Click 'Save'.

The Web server will be added as a remote storage object and can be used as source for Remote Storage Discovery rule.

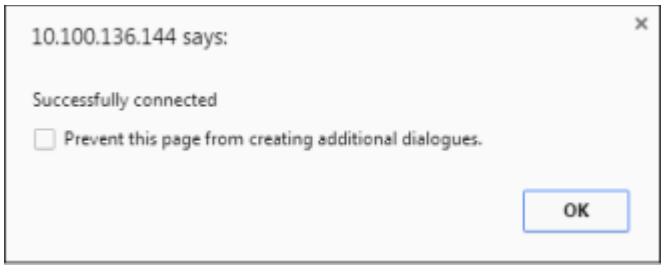
Adding a Network File System (NFS)

You can add a NFS or Distributed File System (DFS) in the network as a Remote Storage object, by specifying its address and file path to be checked.

4. Choose Network File System (NFS) from the ' Add Remote Storage' dialog



5. Enter the parameters:
   - Name - Enter a name shortly describing the NFS
   - Address - Enter the IP Address of the NFS
   - Path - Enter the file path/folder in the NFS to be checked
6. Click 'Test Connection'. MyDLP willl check whether the remote storage location is reachable.



On successful connection, the 'Save' button will be enabled.

7. Click 'Save'.

The NFS will be added as a remote storage object and can be used as source for Remote Storage Discovery rule.

5.3. Matchers

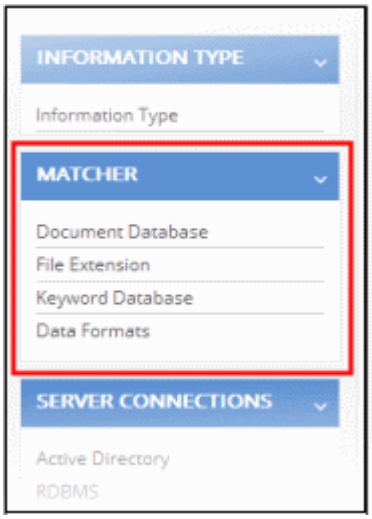
Used when creating a custom 'Information Type', a 'Matcher' is a very specific piece of data that can be used to fine-tune the information type. For example, if you create a new information type called 'Social Security Numbers', you

could narrow the scope of the type by adding specific matchers for 'Uruguay SSN', 'UK National Insurance Number', 'South African ID Number' and so forth. The information type can then be added to a data control or data discovery rule.

MyDLP ships with a set of predefined information types and administrators can also create custom types. Refer to the sections **Information Types – An Overview**, **Predefined Matcher Types** and **Predefined Information Types** for more details.

The 'Matchers' tab allows administrators to view, manage and create selected components of Information Type. The items in this interface will be available for selection as components when creating a new information type object. For example, the predefined and user-defined data format objects available under the 'Data Formats' interface can be selected as a 'Data Format' component for an 'Information Type' object.

To open the Matcher section, click the 'Policy' tab at the top and 'Matcher' on the left.



Refer to the following sections for more details:

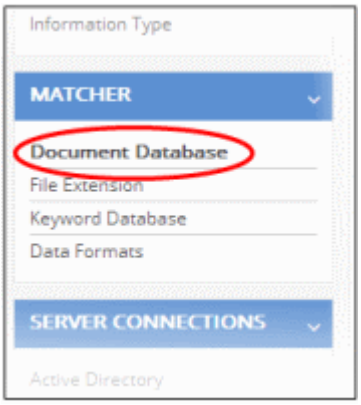
- **Managing Document Databases**
- **Managing File Extensions**
- **Managing Keyword Groups**
- **Managing Data Formats**

5.3.1. Managing Document Databases

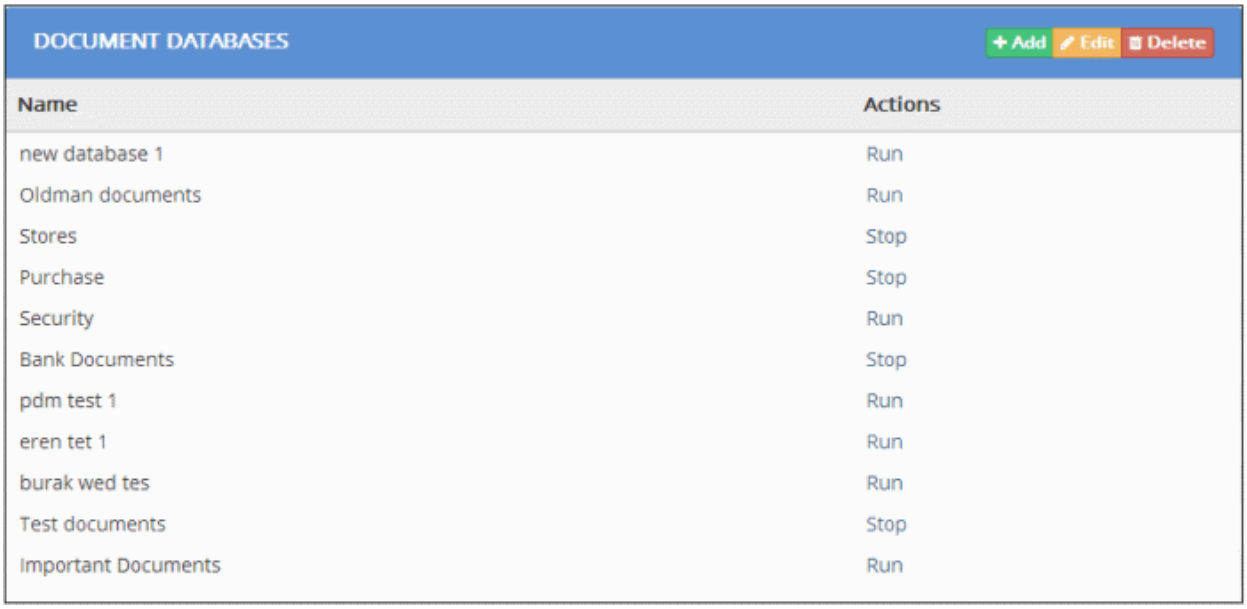
Document Databases are collections of document files stored in different locations in your network, that can be specified as a Document Database (HASH) and Document Database (PDM) Matcher types while creating an Information Type object.

The 'Document Databases' interface allows administrator to add custom document databases to MyDLP. Only the document databases added through this interface, will be available for selection while creating an information type object with Document Database type matcher.

To open the document databases screen, click 'Policy' at the top and then 'Document Database' under 'Matcher' menu



The 'Document Databases' screen will be displayed:



The 'Run' link under the 'Actions' column allows to generate hash values for the files in the databases. The document database will be available for selection to define the Matcher component while creating an Information Type object. But for specifying the document database for Document Database (Hash) matcher, the hash values of the files need to be created and stored, so that MyDLP will use the hash values to intercept the data traffic if it contains any of the files from the database. For more details, refer to the description of '**Document Database (Hash)**' in the section **Information Types - An Overview**.

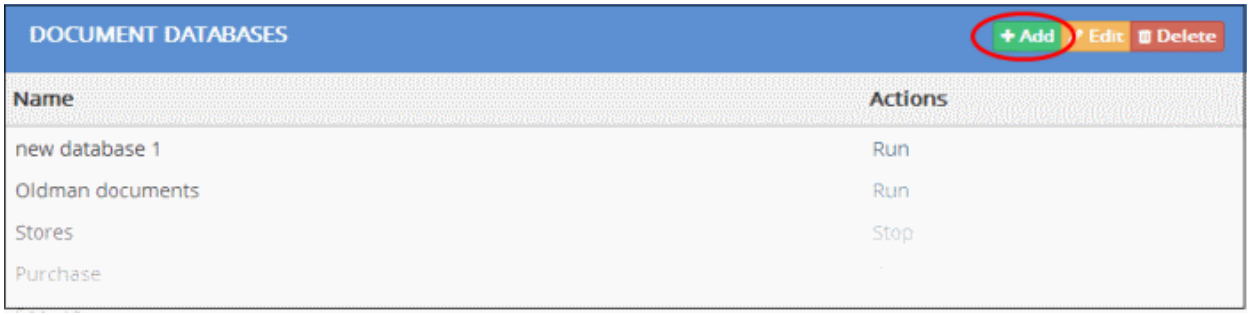
Refer to the following sections on managing the Document Databases:

- **Adding a Document Database**
- **Editing a Document Database**

5.3.1.1. Adding a Document Database

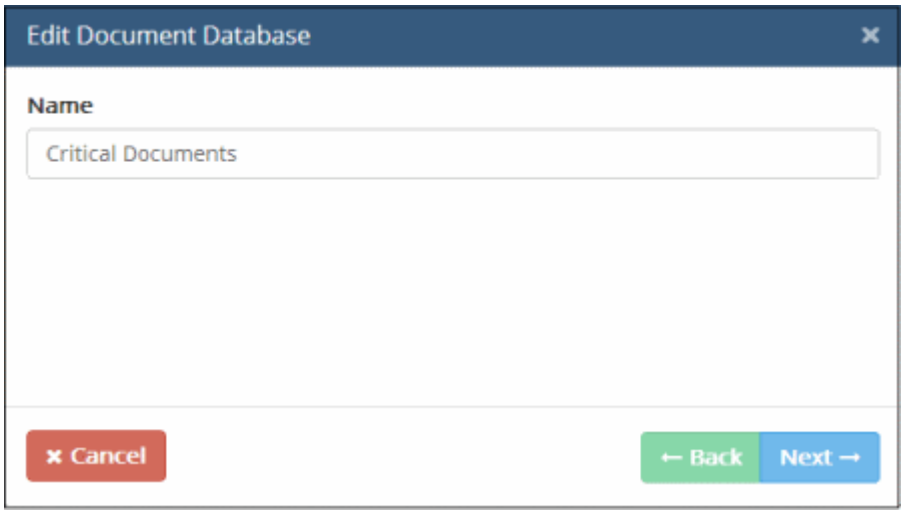
The administrator can create a new document database and add document files in three methods.

To add a document database, click 'Policy' tab at the top > 'Matcher' > 'Document Database > 'Add' button at the top



Step 1 – Enter a name

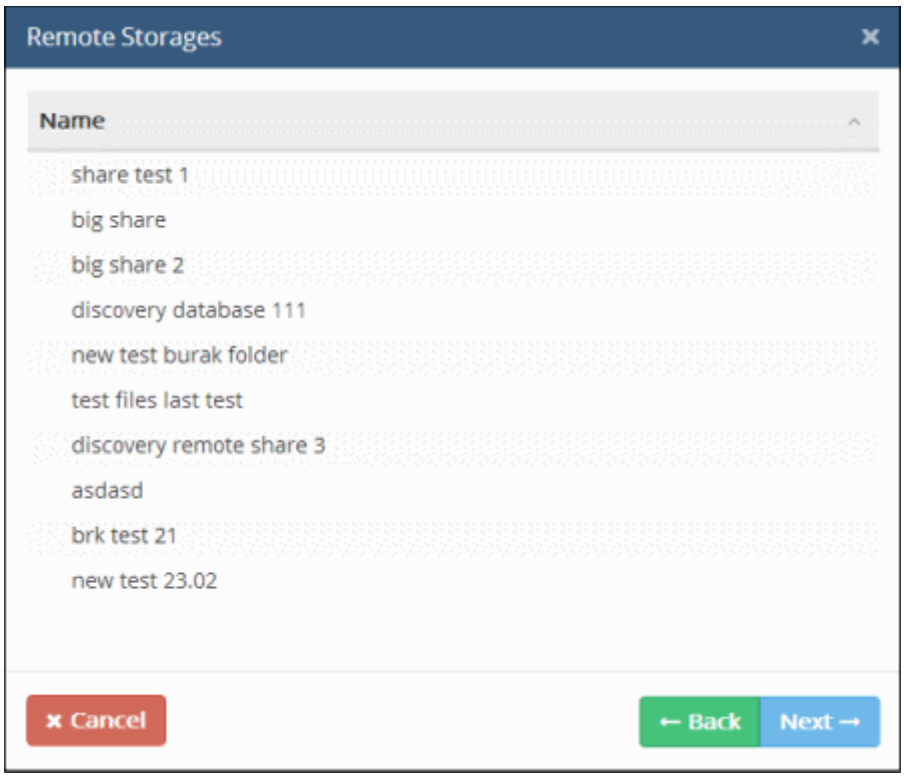
The 'Edit Document Database' dialog will be displayed.



- Enter a name for the document database and click 'Next'

Step 2 – Adding files from remote storage

The Remote Storages screen will be displayed:

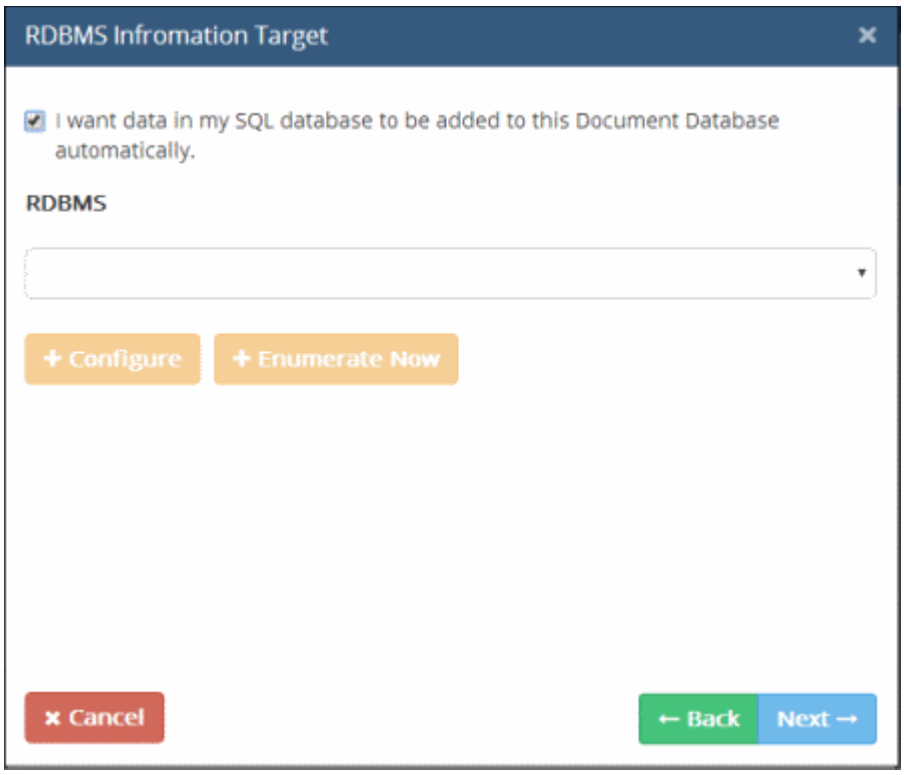


The files that are displayed here are fetched from Remote Connections under the 'Discovery Target' section. Refer to the section '**Adding a User Defined Remote Storage Object**' for more details about how to add a remote storage object.

- Select the files and click 'Next'

Step 3 – Integrating a MySQL Database to Document Database

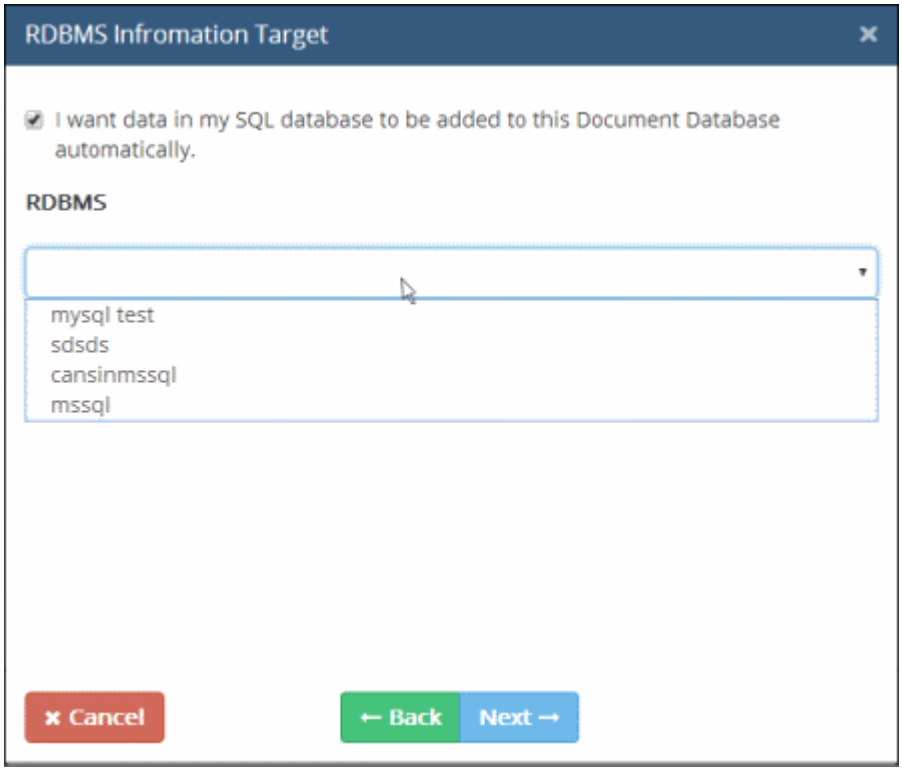
The 'RDBMS Information Target' will be displayed.



The administrator can import documents from a MySQL database server through RDBMS connection.

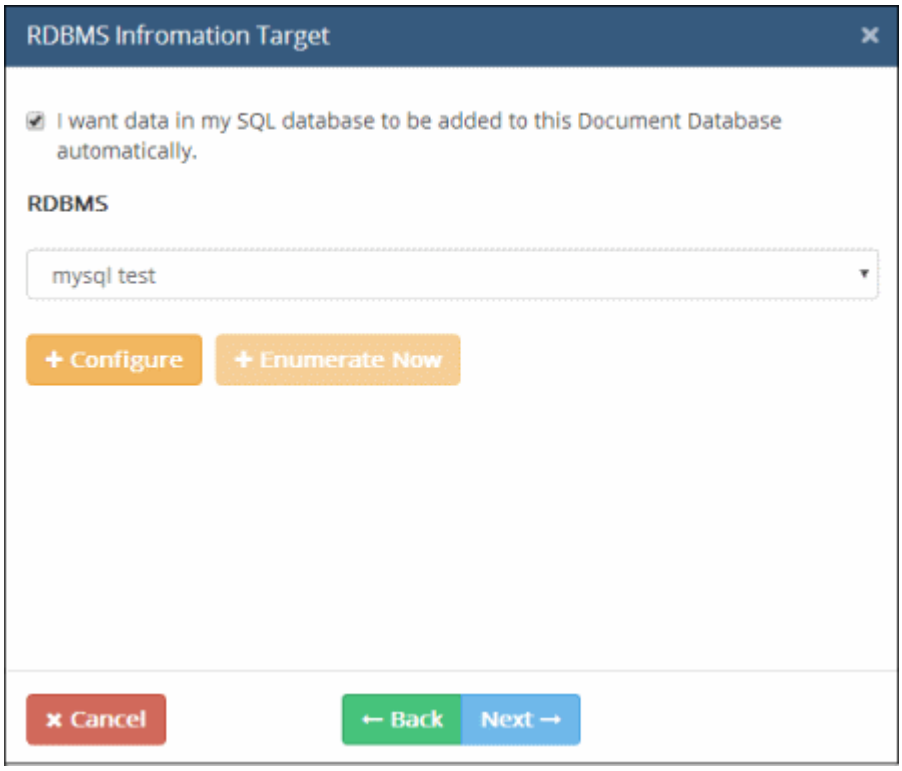
- Select the check box 'I want data in my SQL database to be added to this Document Database automatically'

If you have RDBMS Connections configured already, the list of the connections will be displayed. Refer to the section '**Integrating RDBMS Systems**' for more details.

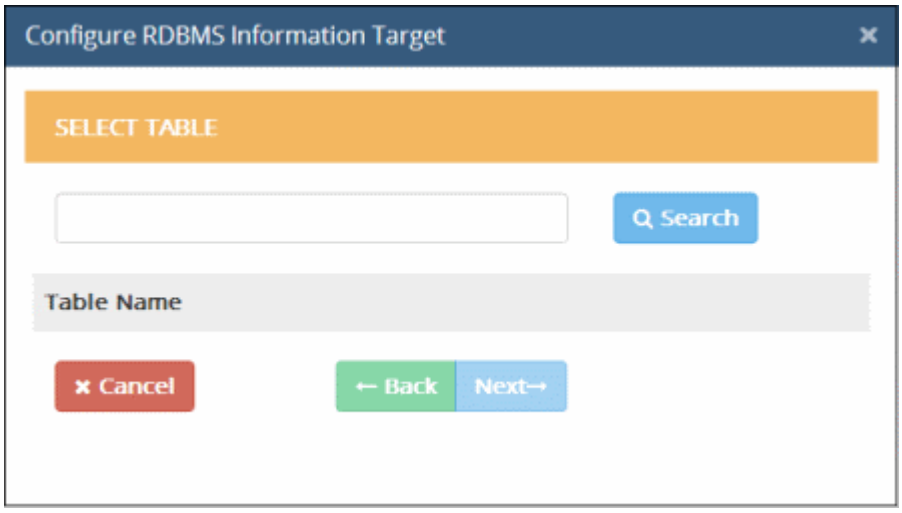


- If you have not configured RDBMS connections, you can configure from this interface by clicking 'Configure'.

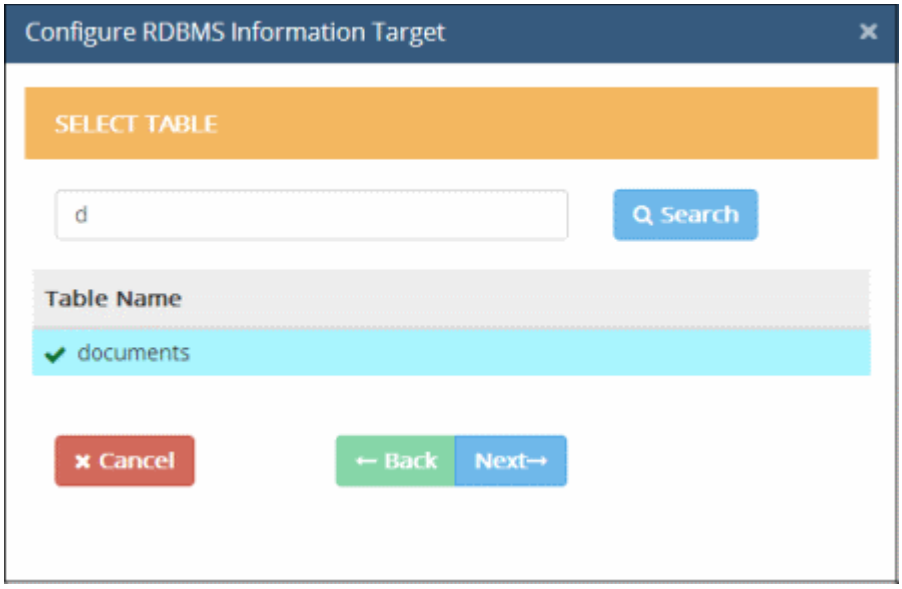
- If you have already configured the RDBMS connection, you can re-configure an existing connection if required.



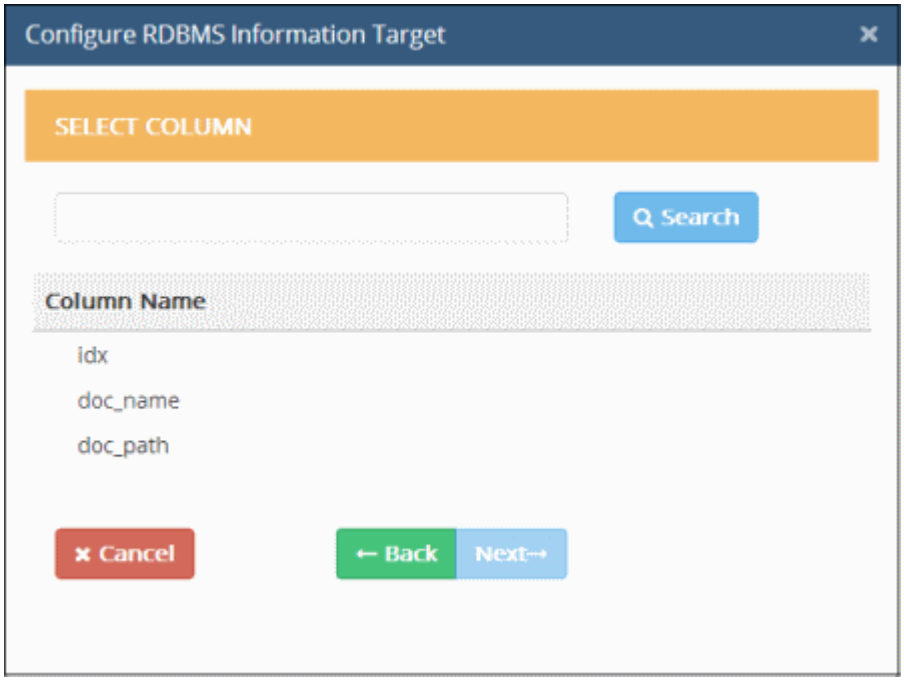
- Click 'Configure'. The 'Configure RDBMS Information Target' dialog will appear.



- Select the table from the MySQL database. Type the first few characters of the table name in the field below 'Table Name' and click the 'Search button. To view all the items, click 'Search' keeping the field blank. All the tables with the matching names will be displayed in the list below. To view all the items, click 'Search' keeping the field blank. Select the table from the list and click 'Next'

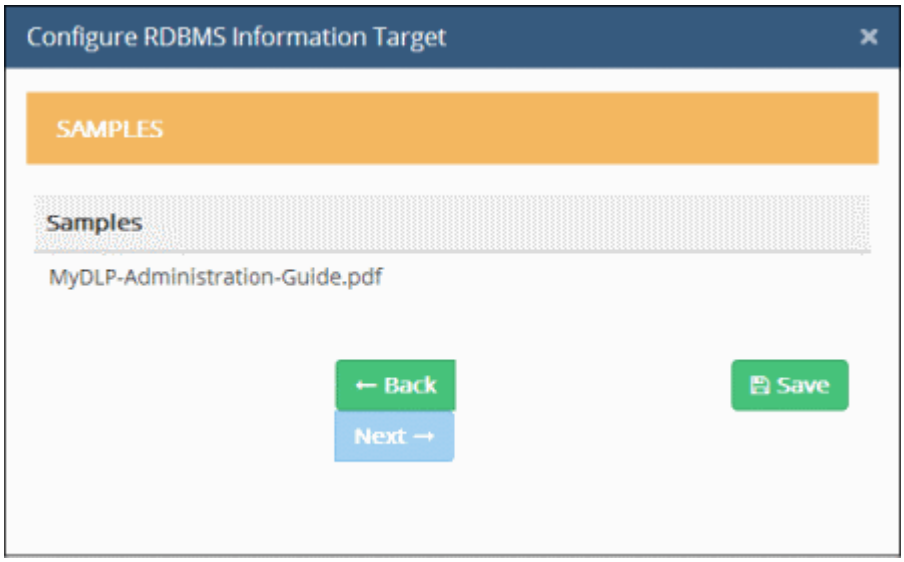


The 'Select Column' dialog will appear.



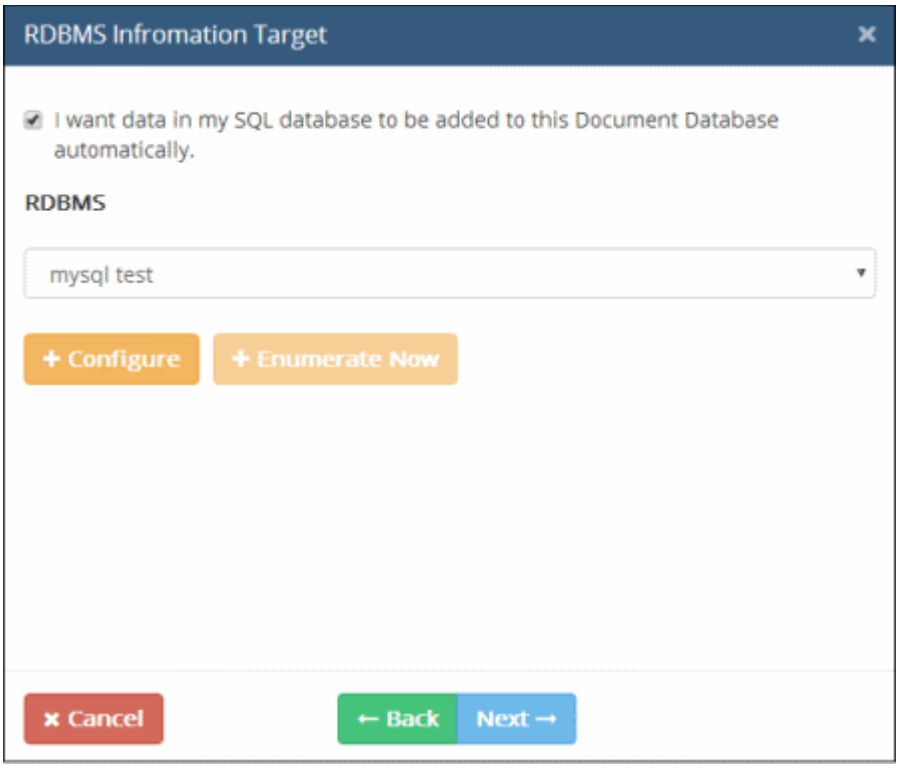
All the column names will be displayed. You can also search for particular column by entering the first few characters of the column header in the field below 'Select Column' and clicking 'Search'. All the column headers with the matching names will be displayed in the list below.

- Select the column header from the list and click 'Next'.



The sample items in the selected column will be displayed as a list.

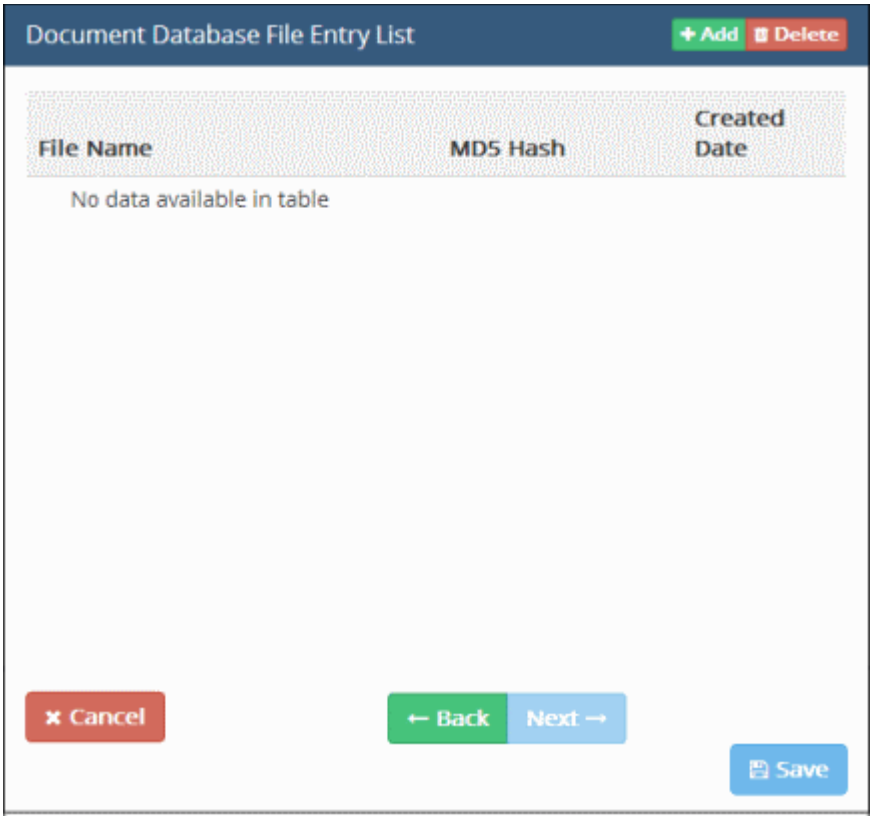
- Check whether the correct table and column are chosen from the displayed documents. Click 'Back' in any of the screens to review your parameters.
- Click 'Save'



- Click 'Enumerate Now' to include all the documents immediately,
- Click 'Next'

Step 4 – Manually Adding Files to the Database

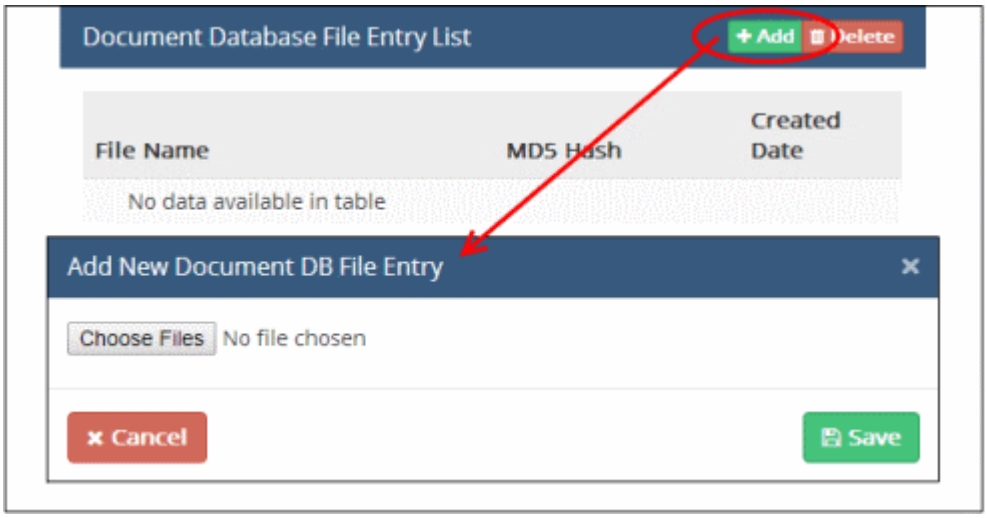
The 'Document Database File Entry List' dialog will be displayed.



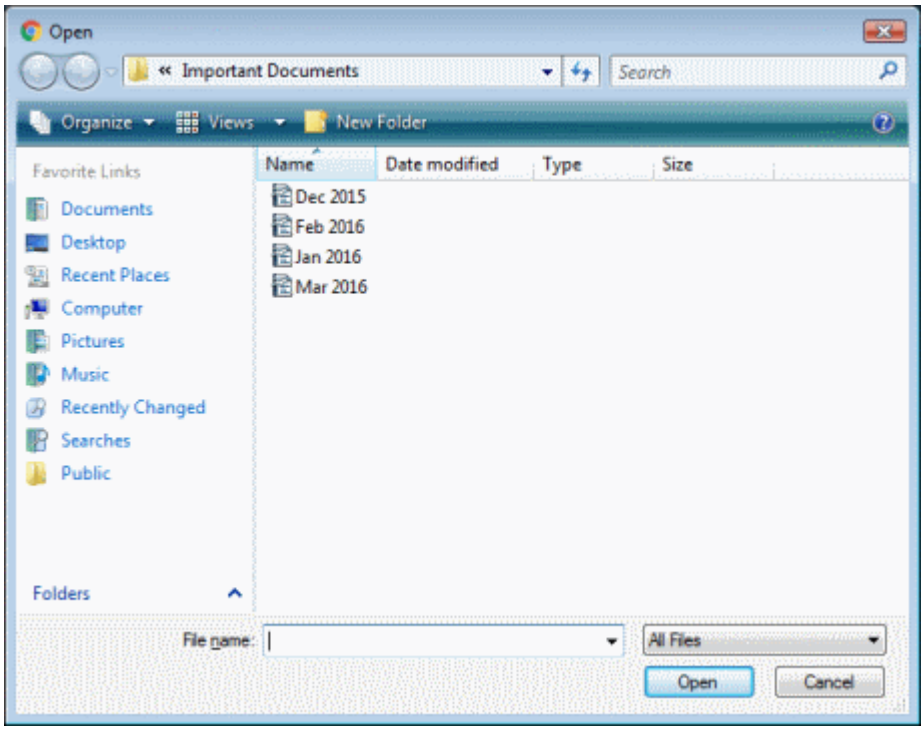
You can upload the files from the local drives of the computer from which you are accessing the MyDLP administrative interface to build the document database.

To upload the files

- To add a new file, click the 'Add' button at the top

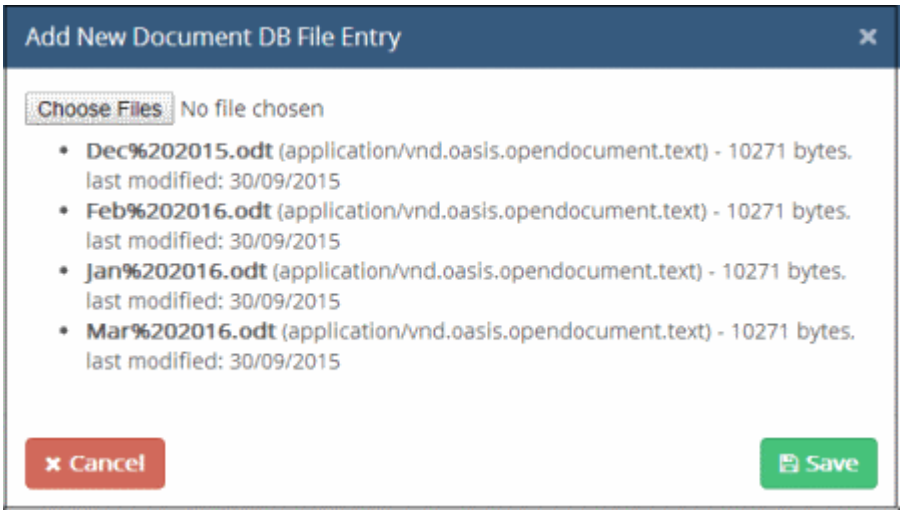


- Click 'Choose Files' and navigate to the location of the files



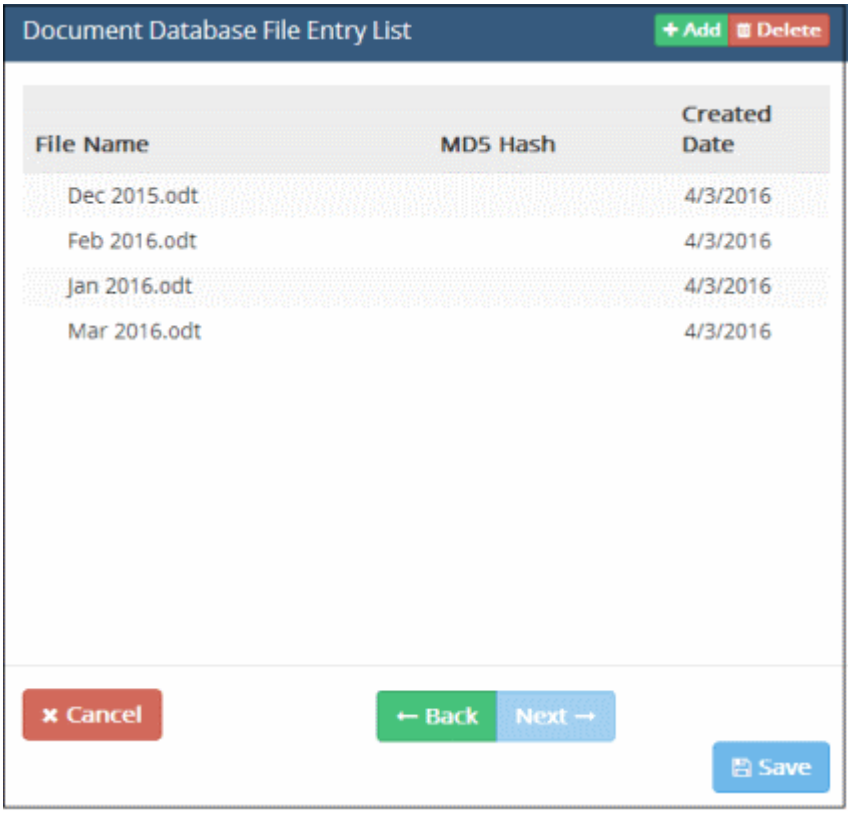
- Select the file(s) and click 'Open'

The selected file(s) will be added to the list



- Click 'Save'

The files will be saved in 'Document Database File Entry List' screen.



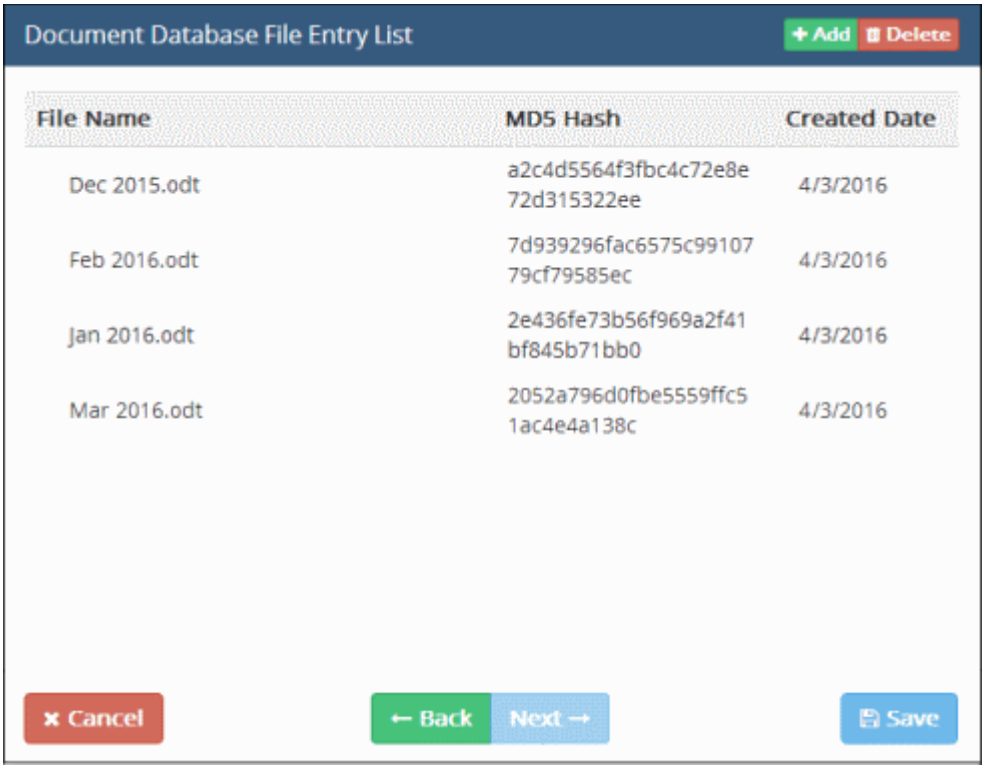
- Repeat the process to add more files
- To remove a file from the list, select it and click 'Delete' at the top
- Click 'Back' to review your selections
- Click 'Save' to save the document database.

The document database will be available for selection to define the Matcher component while creating an Information Type object. But for specifying the document database for Document Database (Hash) matcher, the hash values of the files need to be created and stored, so that MyDLP will use the hash values to intercept the data traffic if it contains any of the files from the database. For more details, refer to the description of '**Document**

Database (Hash)' in the section **Information Types - An Overview**.

- To create the hash values for the files that are added via Remote Storages, RDBMS and manually, click 'Run' beside the database that you want to create hash values.

MyDLP will create MD5 Hash values and saves them. You can view the generated hash values of the files by selecting the database and clicking 'Edit' at the top. Proceed to the 'Document Database File Entry List' screen to view the hash values.



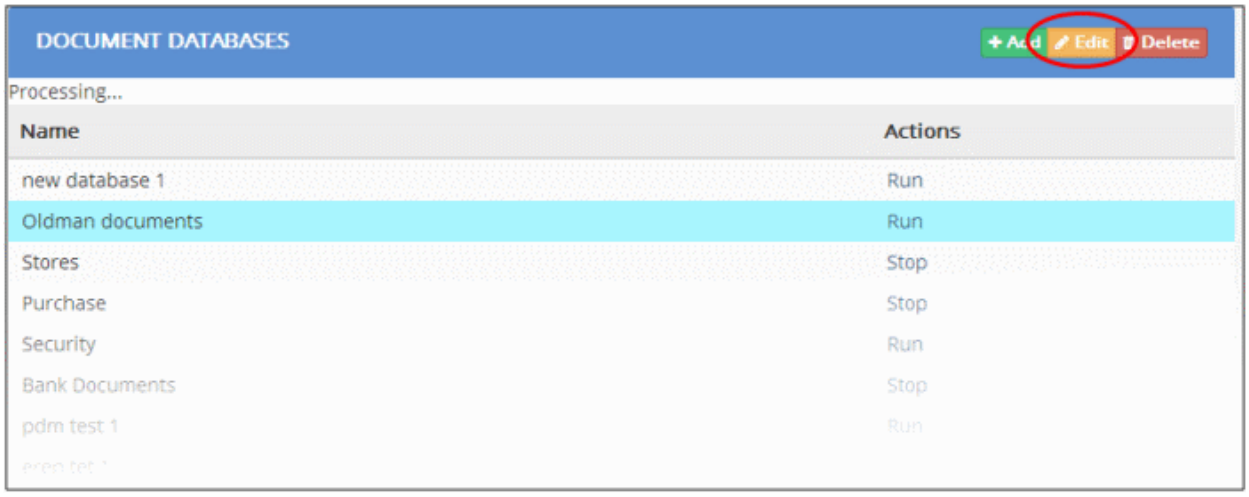
For the changes in the document database to take effect in the 'Information Type' object in which it is used and in the Rules in which the Information Type object is applied, re-install the policy by clicking the Install Policy at the top right. Refer to the section **Deploying the Policy** for more details.

5.3.1.2. Editing a Document Database

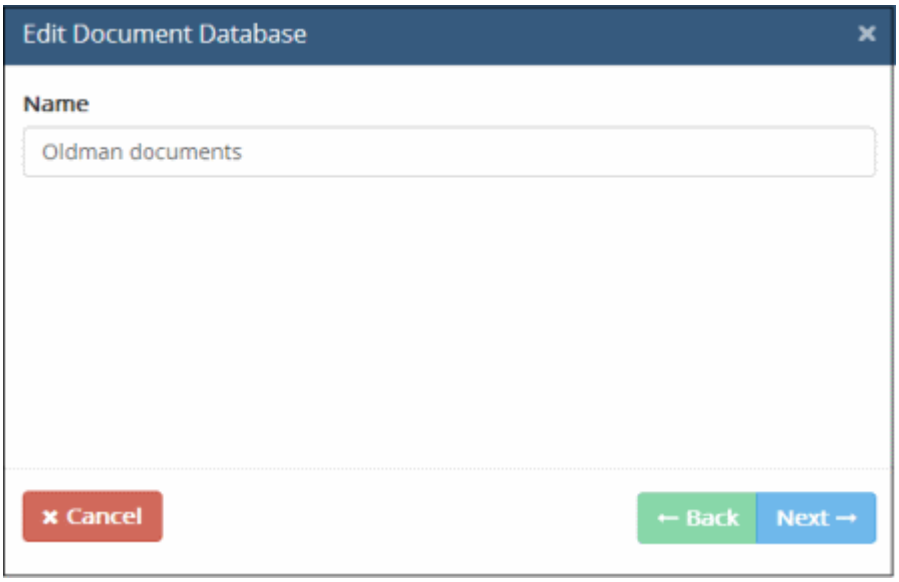
The administrator can add new documents, edit or remove unnecessary documents from any database from the 'Document Database' interface. The changes will take effect immediately on reapplying the policy to the network.

To edit a document database

- Click 'Policy' tab at the top > 'Matcher' > 'Document Database
- Select the document database and click the 'Edit'



The 'Edit Document Database' dialog will be displayed:



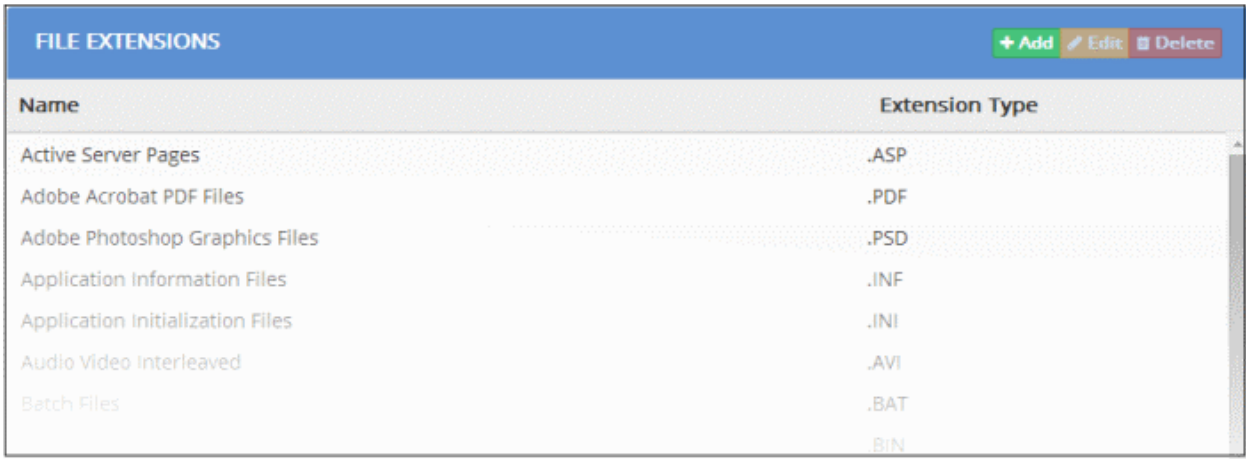
All the files included in the document database, imported from the remote storage or MySQL database or or by manually adding the files will be displayed in the respective screens. The process is same as adding a document database. Refer to the section '**Adding a Document Database**' for more details.

- To remove a document database, select it and click 'Delete'. Please note the database cannot be removed if it is in use in a rule.

For the changes in the document database to take effect in the 'Information Type' object in which it is used and in the Rules in which the Information Type object is applied, re-install the policy by clicking the Install Policy at the top right. Refer to the section **Deploying the Policy** for more details.

5.3.2. Managing File Extensions

'File extensions' are used to specify the type of extension in the 'Information Type' object, which is used as a component for a rule. Refer to the section '**Information Types – An Overview**' and '**Adding a User Defined Information Type**' for more details about information type object.



MyDLP ships with a set of predefined extensions that are commonly used. You can also add custom extensions from this interface. Refer to the following sections for more details.

- **Adding a New File Extension**
- **Editing Existing File Extension**

5.3.2.1. Adding a New File Extension

In addition to predefined file extensions that is shipped with MyDLP, administrators can also add user-defined extensions according to their requirements.

To add a new file extension

- Click 'Policy' tab at the top > 'Matcher' > 'File Extension'
- Click 'Add' from the 'File Extensions' screen

The 'Add Extension' dialog will be displayed.

- Enter the new extension type, for example, .swf, in the field
- Click 'Save'

The new extension type will be added and displayed in the list. Once added, the file extension will available for selection while creating a new information type. Refer to the section '**Adding a User Defined Information Type**' for more details.

5.3.2.2. Editing Existing File Extension

The 'File Extensions' interface allows administrator to edit existing extensions or remove unwanted items.

To edit an existing extension

- Click 'Policy' tab at the top > 'Matcher' > 'File Extension'
- Select the file extension from the list and click 'Edit' at the top right

The 'Edit Extension' for the selected extension will be displayed.

- Edit as required and click 'Save' for the changes to take effect.

For the changes in the file extension to take effect in the 'Information Type' object in which it is used and in the Rules

in which the Information Type object is applied, re-install the policy by clicking the Install Policy at the top right. Refer to the section **Deploying the Policy** for more details.

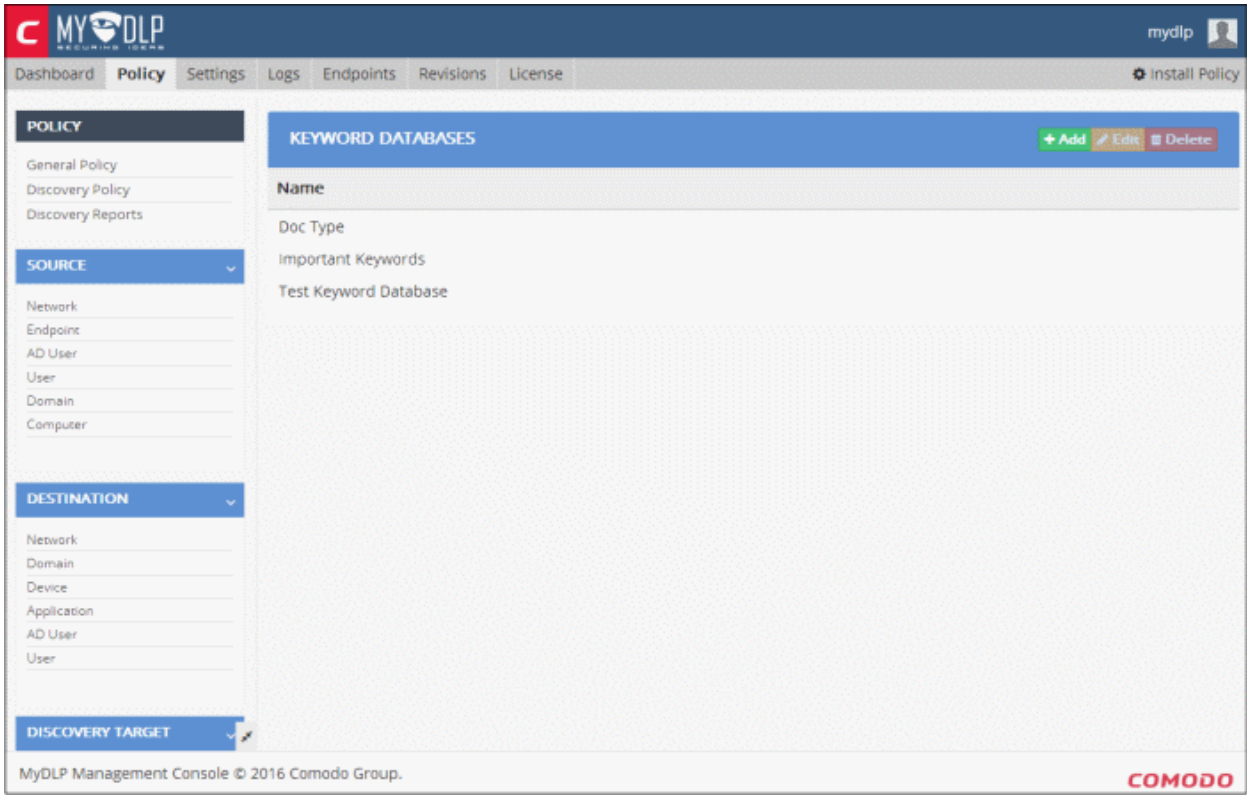
- To remove a file extension, select it and click 'Delete'. Please note a file extension cannot be removed if it is in use in a rule.

5.3.3. Managing Keyword Databases

Each Keyword Database is a collection of keywords pertaining to a specific field like business, medicine, finance, banking and so on. The Keyword Database can be specified as a Matcher while creating an Information Type object. Once added in a rule, the candidate files that are scanned as per the rule containing the 'Information Type', will be searched for the keywords contained in the group to identify files containing sensitive information.

Comodo DLP ships with a number of pre-defined, uneditable keyword groups that are available for selection while creating an Information Type object.

The 'Keyword Databases' interface allows the administrator to create and add custom, user-defined keyword databases to MyDLP, which in turn, can be used in Information Type objects. Keywords can be entered manually, imported from a text file or imported from a RDBMS server.



Refer to the following sections about managing the Keyword Databases:

- **Adding a user defined Keyword Database**
- **Editing a user defined Keyword Database**

5.3.3.1. Adding a User Defined Keyword Database

Administrators can add a new keyword database and keywords by manually entering them, importing from a file, or importing from a RDBMS database.

To add a new Keyword Database

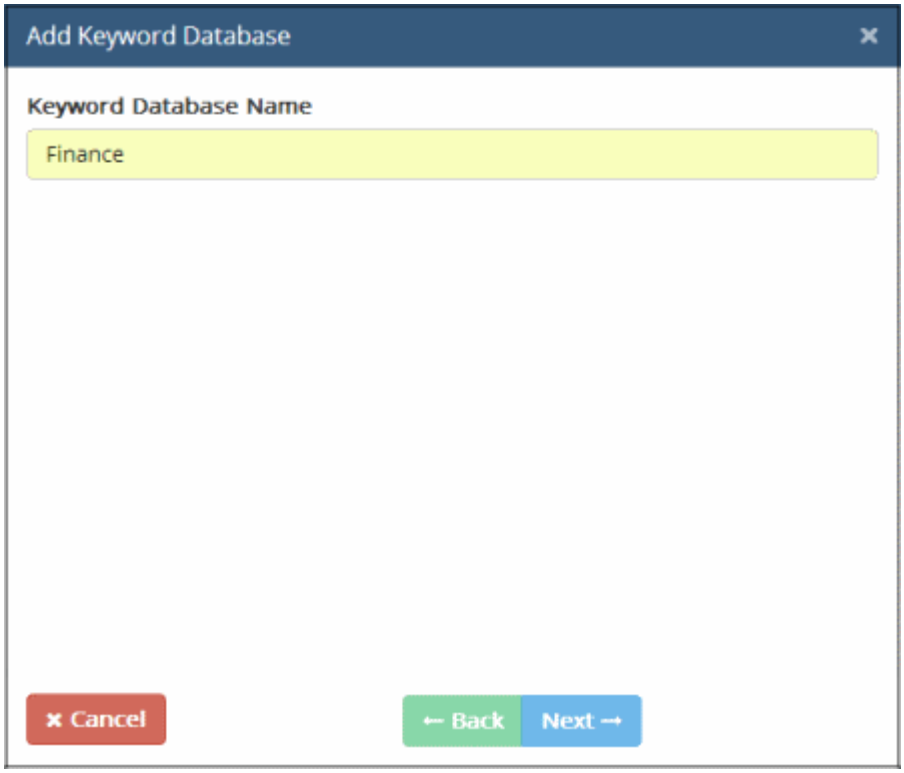
- Click the 'Policy' tab then 'Matcher' > 'Keyword Database'

- Click 'Add' from the 'Keyword Databases' screen

Step 1 – Enter a name

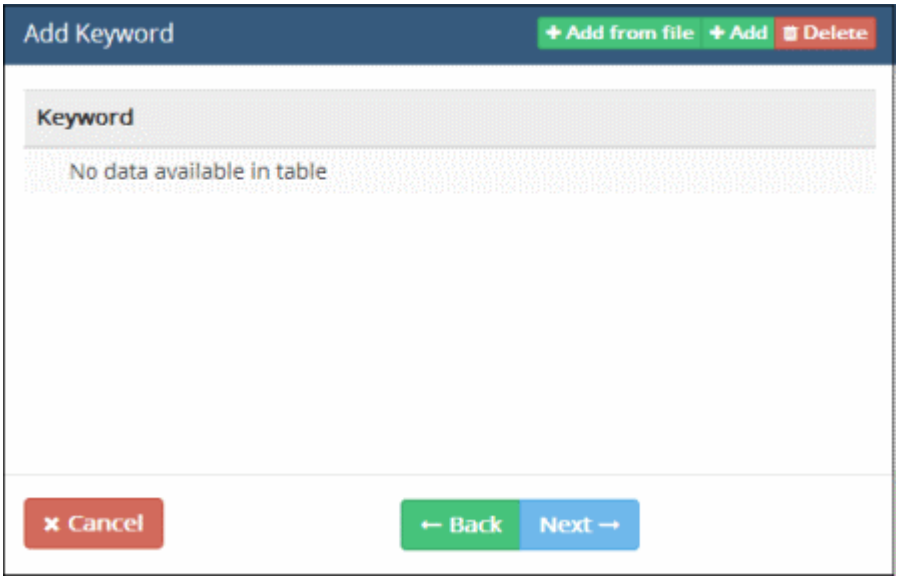
The 'Add Keyword Database' dialog will be displayed.

- Enter a name for the keyword database and click 'Next'



Step 2 – Add keywords to the database

The Add Keyword dialog will be displayed.



You can add the keywords in two ways:

- **Manually enter the keywords one-by-one**
- **Import keywords from a file**

Manually enter the keywords one-by-one

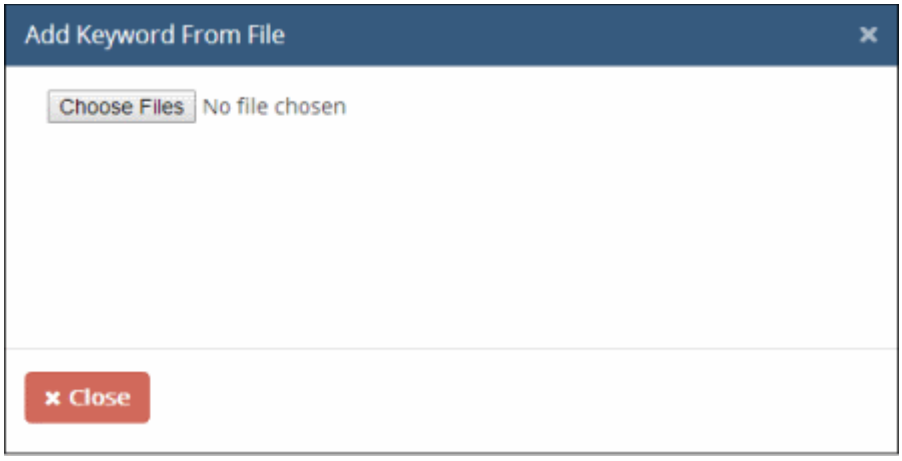
- To manually enter the keywords, click 'Add' at the top. The 'Keyword Add Dialog' will appear.

- Enter a single keyword and click 'Save'
- Repeat the process to add more keywords

Import keywords from a file

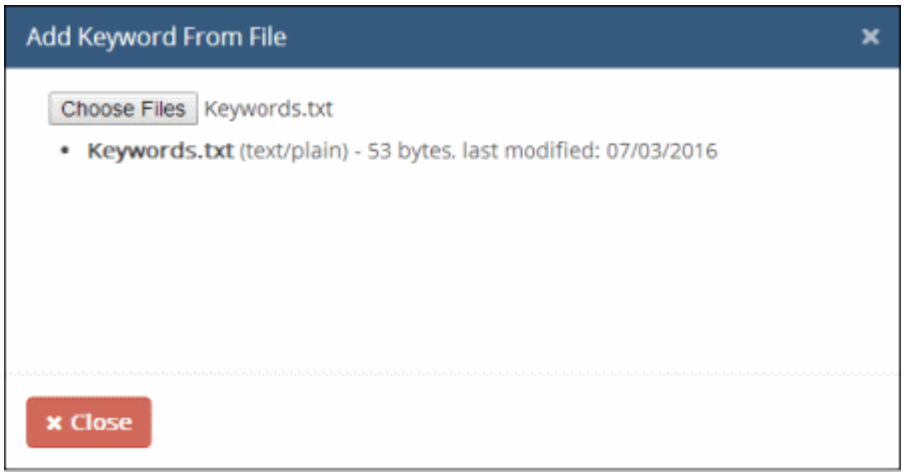
Please not the keywords should be saved in separate lines in the text file.

- To import keywords from a text file containing the keywords, click 'Add from file' at the top. The 'Add Keyword From File' dialog will appear.



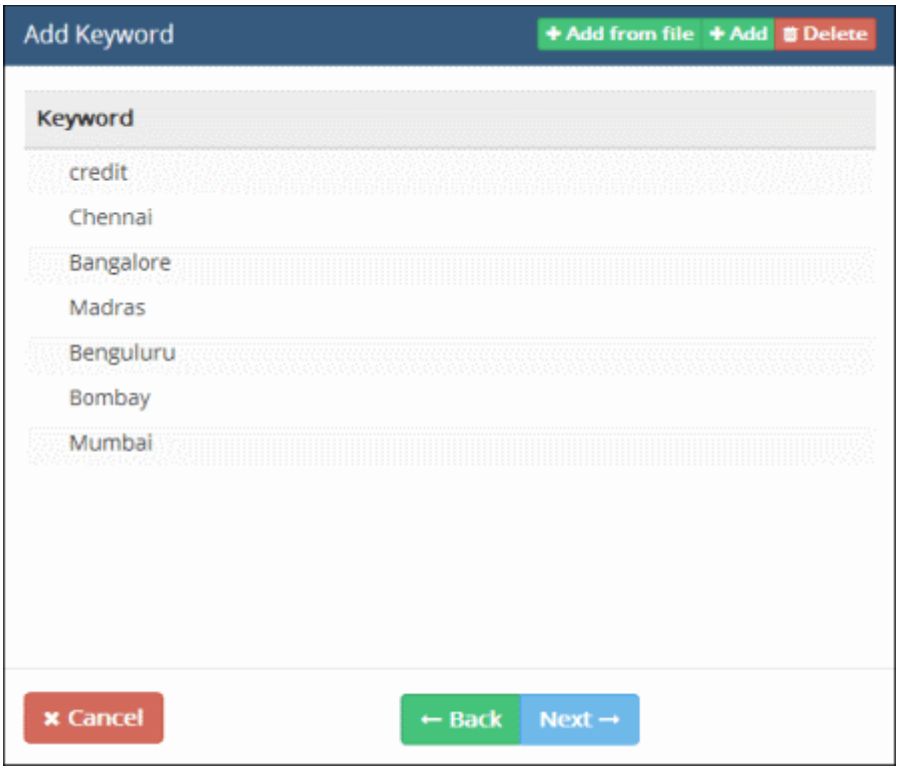
- Click 'Choose File' and navigate to the text file, select the text file and click 'Open'.

The selected file will be listed.



- Click 'Close'.

The list of added keywords will be displayed.

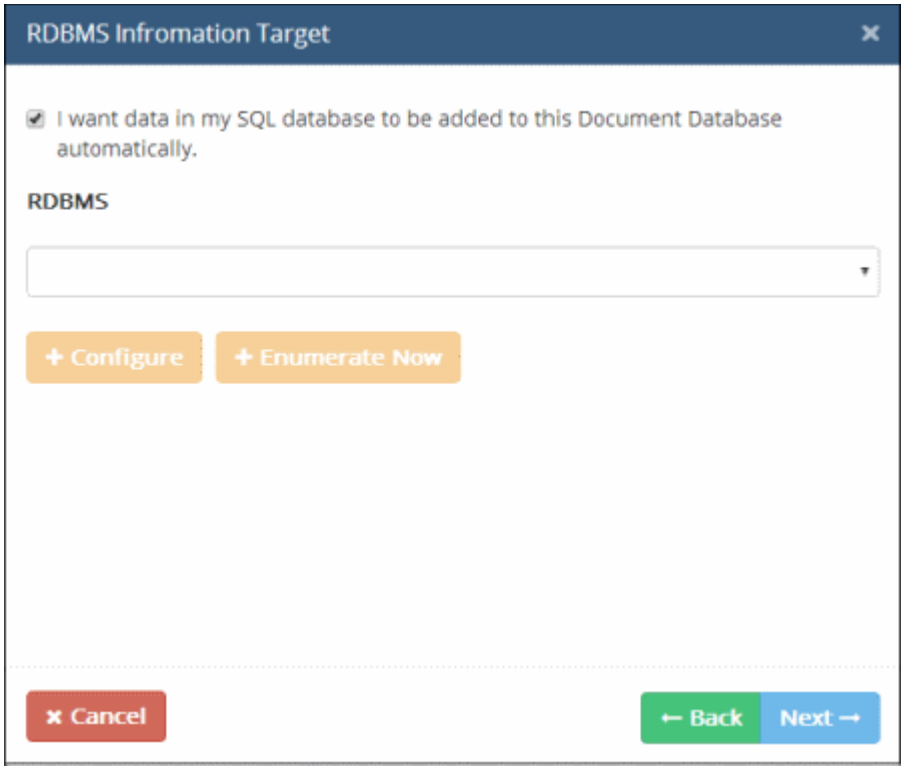


By default, all the imported keywords and added keywords are selected. To remove a keyword, select it and click 'Delete.

- Click 'Next'

Step 3 - Integrating a MySQL Database to Keyword Database

The RDMBS Information Target dialog will be displayed.

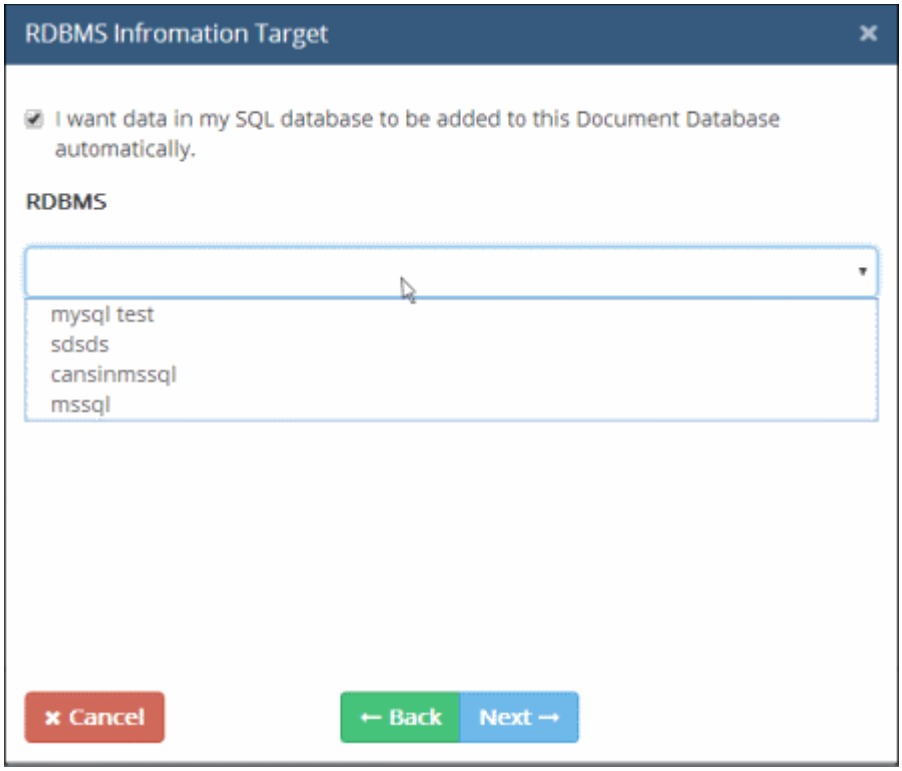


The administrator can import keywords from a MySQL database server through RDBMS connection.

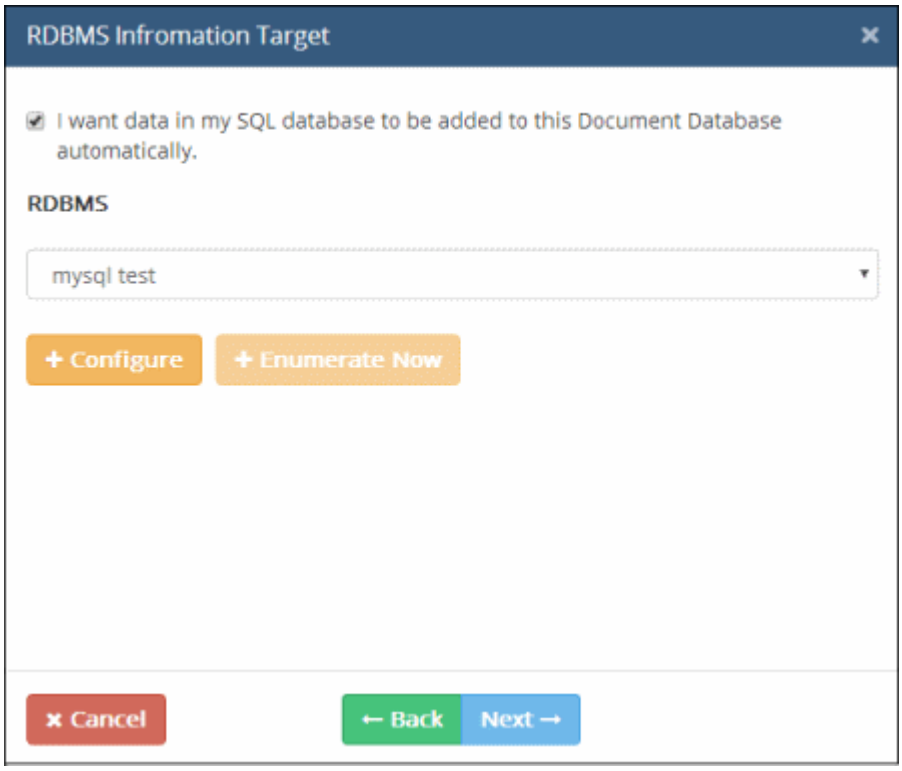
Tip: Comodo MyDLP can be added with several RDBMS connections through the 'RDBMS Connections' interface Refer to the section **Integrating RDBMS Systems** for more details.

- Select the check box 'I want data in my SQL database to be added to this Document Database automatically'

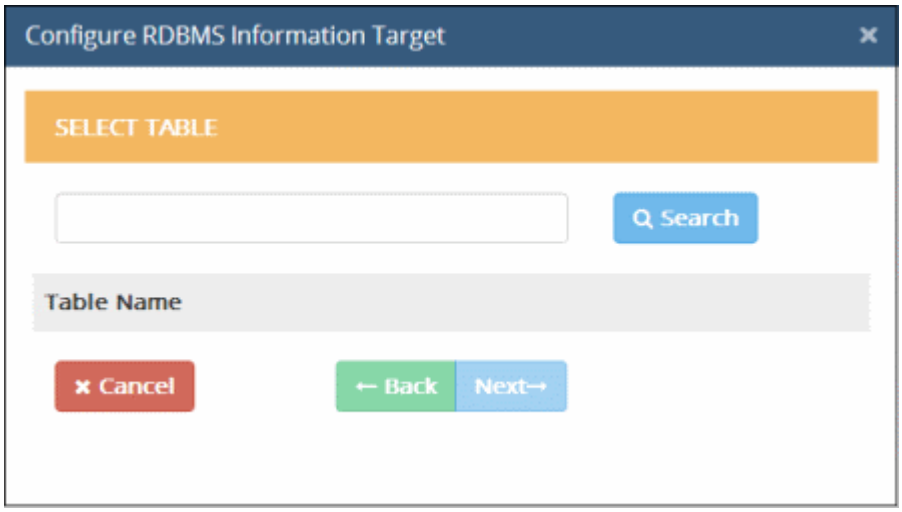
If you have RDBMS Connections configured already, the list of the connections will be displayed from the RDBMS drop-down. Refer to the section '**Integrating RDBMS Systems**' for more details.



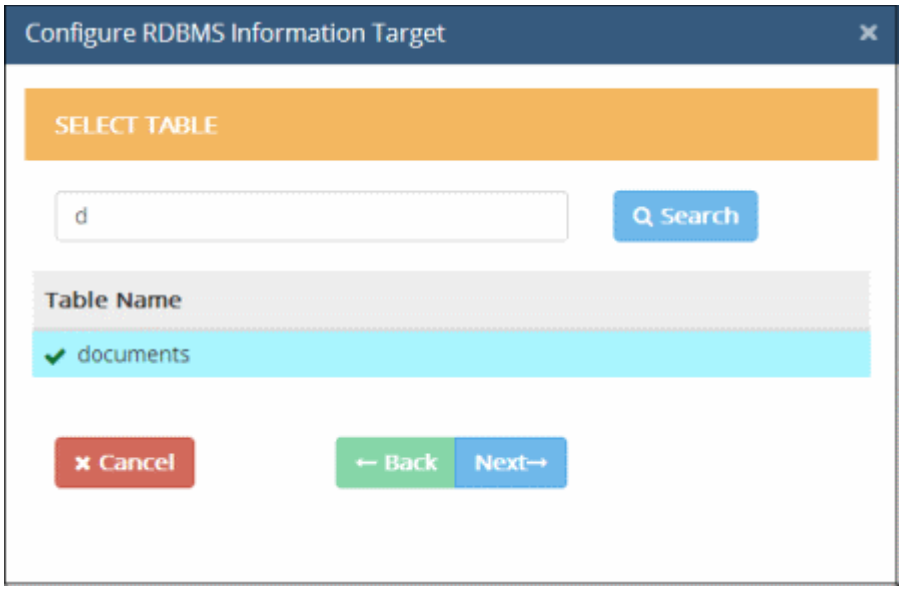
- If you have not configured RDBMS connections, you can configure from this interface by clicking 'Configure'.
- If you have already configured the RDBMS connection, you can re-configure an existing connection if required.



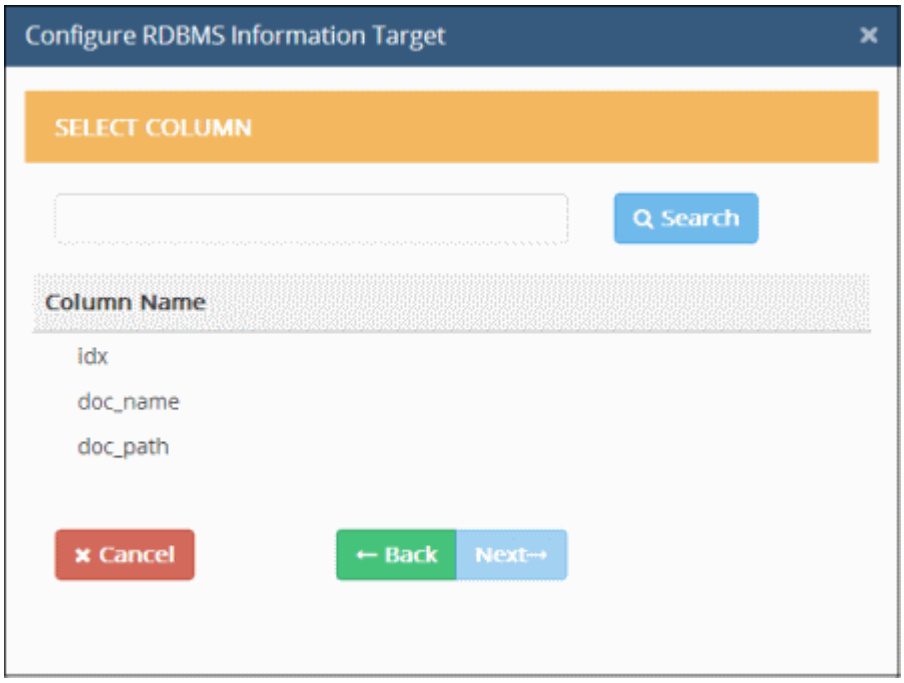
- Click 'Configure'. The 'Configure RDBMS Information Target' dialog will appear.



- Select the table from the MySQL database. Type the first few characters of the table name in the field below 'Table Name' and click the 'Search button. All the tables with the matching names will be displayed in the list below. Select the table from the list and click 'Next'

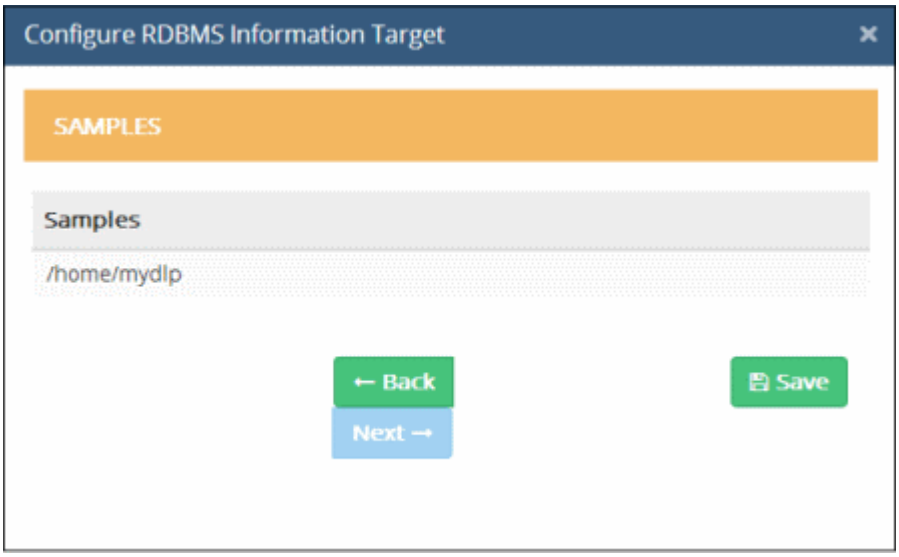


The 'Select Column' dialog will appear.



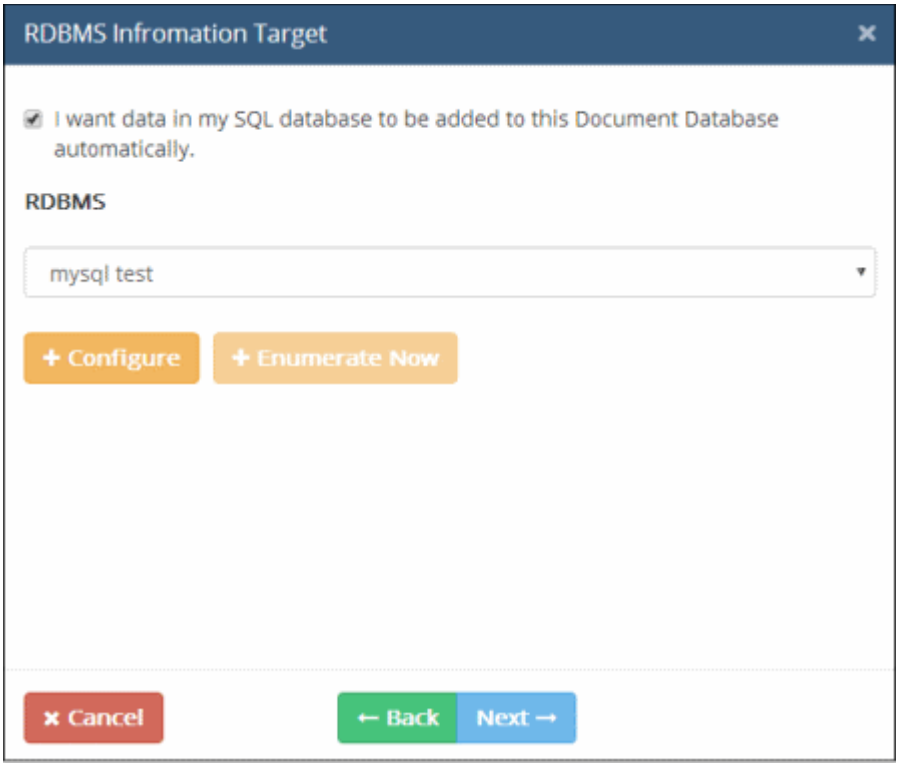
All the column names will be displayed. You can also search for particular column by entering the first few characters of the column header in the field below 'Select Column' and clicking 'Search'. All the column headers with the matching names will be displayed in the list below.

- Select the column header from the list and click 'Next'.



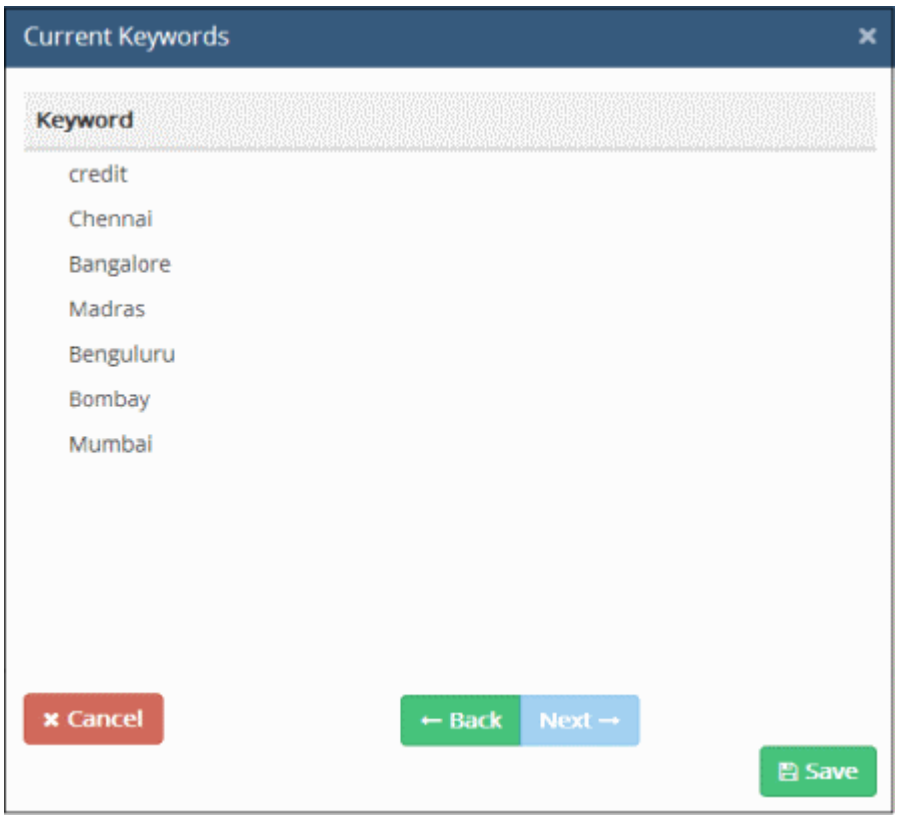
The sample keywords in the selected column will be displayed as a list.

- Check whether the correct table and column are chosen from the displayed keywords. Click 'Back' in any of the screens to review your parameters.
- Click 'Save'



- Click 'Enumerate Now' to include all the keywords immediately.
- Click 'Next'

The 'Current Keywords' screen will be displayed.



- Click 'Back' to review and make any changes
- Click 'Save'

The added keyword database will be listed.

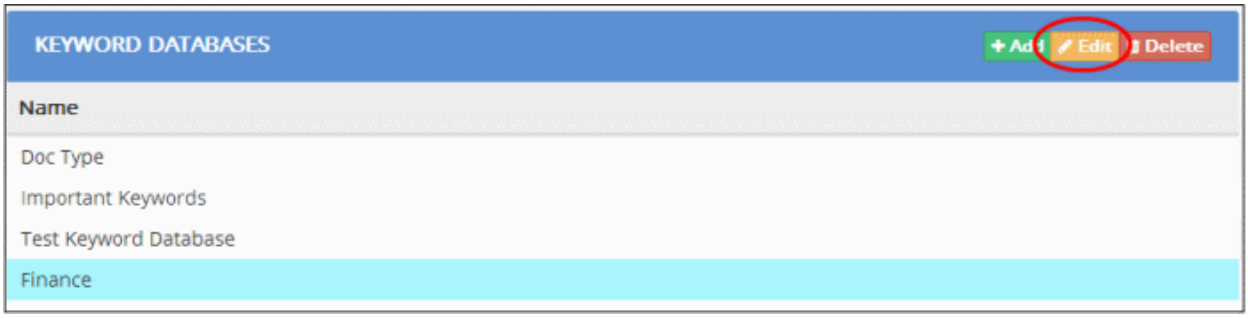
This will be available for selection in the Information Type object for specifying the Keyword Group component. Refer to the section '**Adding a User Defined Information Type**' for more details.

5.3.3.2. Editing a User Defined Keyword Database

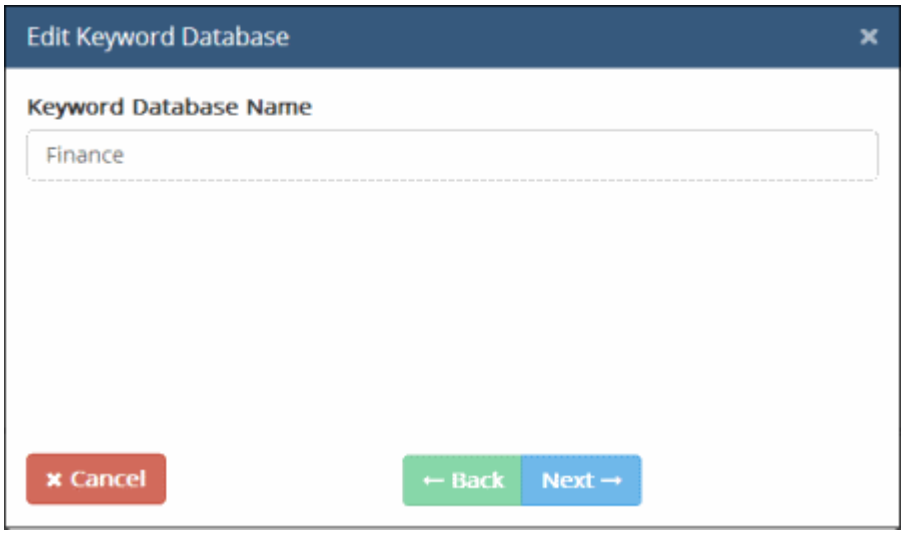
The administrator can edit a Keyword Database at anytime to add new keywords or to remove existing keywords from the group. If a keyword group is altered , the policy has to be re-deployed to the network for the changes to propagate to the rules in which the keyword group is used as matcher for the information type object.

To edit a keyword database

- Click 'Policy' tab at the top > 'Matcher' > 'Keyword Database'
- Select the keyword database and click 'Edit'



The 'Edit Keyword Database' dialog will be displayed:



All the keywords included in the keyword database, imported from MySQL database or or by manually adding the files will be displayed in the respective screens. The process is same as adding a keyword database. Refer to the section '**Adding a User Defined Keyword Database**' for more details.

- To remove a keyword database, select it and click 'Delete'. Please note the database cannot be removed if it is in use in a rule.

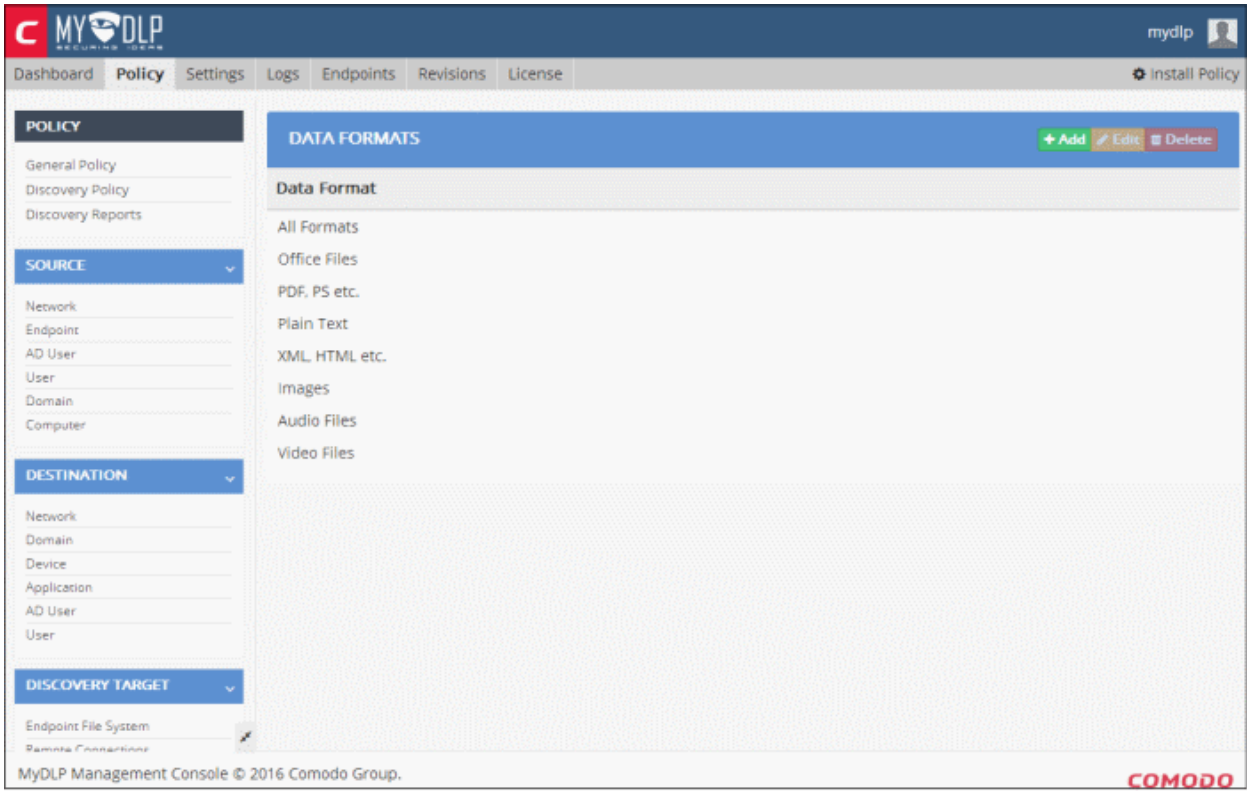
For the changes in the document database to take effect in the 'Information Type' object in which it is used and in the Rules in which the Information Type object is applied, re-install the policy by clicking the Install Policy at the top right. Refer to the section **Deploying the Policy** for more details.

5.3.4. Managing Data Formats

MyDLP is capable of protecting a wide range of data types and formats. Data Formats are organized into broad genres (such as 'Audio Files', 'Images' and so on) which in turn contain a list of specific types (like '.mp3', '.wav' or '.jpg', '.bmp'). MyDLP also allows administrators to add custom data formats and file types and to edit existing user defined data formats. These data formats will be available for selection when adding or editing an 'Information Type' object.

The administrator can view, edit and add file genres and file formats by selecting the 'Data Formats' under the 'Matcher' section. The file formats for each genre, can be defined as MIME Type or file extension.

To open the 'Data Formats' screen, click 'Matcher' on the left and then 'Data Formats'



Refer to the following sections for more details about managing the data formats:

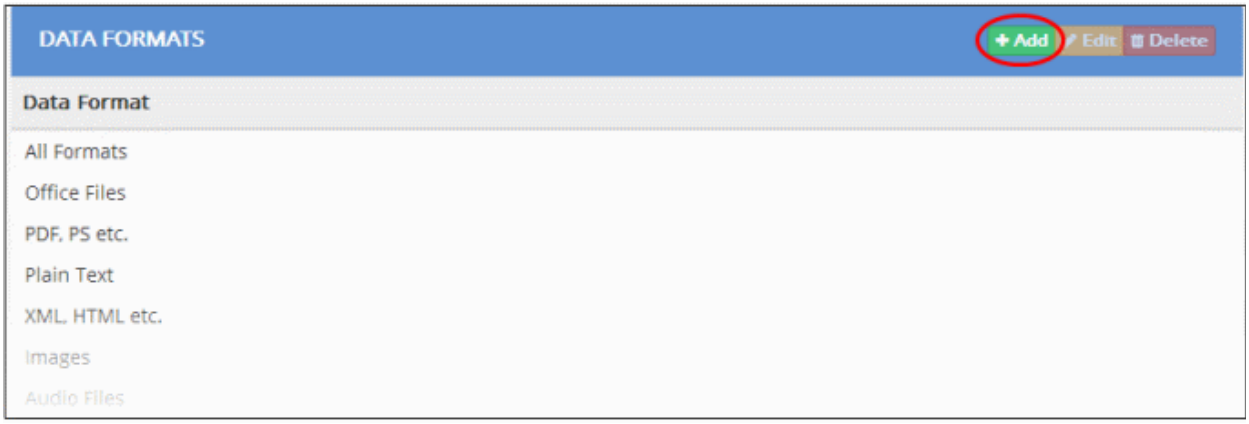
- **Adding a new Data Format**
- **Editing a Data Format**

5.3.4.1. Adding a New User Defined Data Format Entry

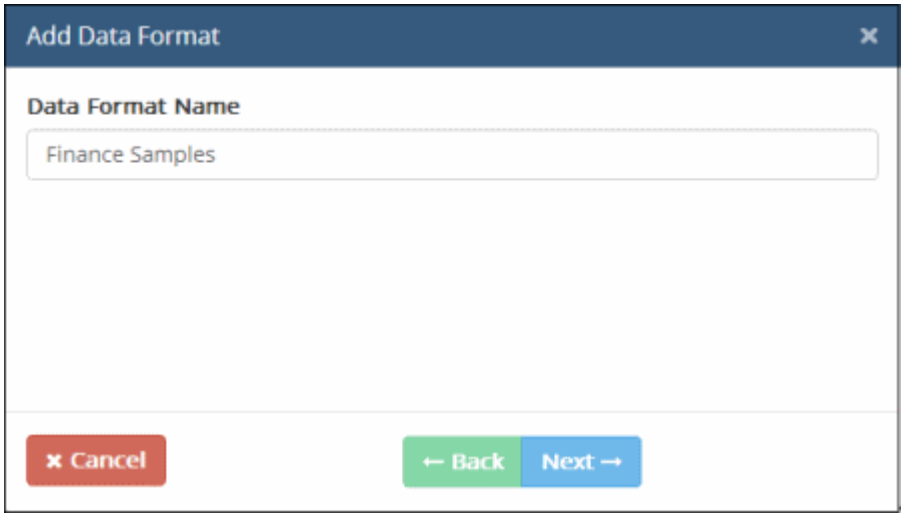
The administrator can add new user defined Data Format entries by specifying a name and the file types to be added to the Data Format collection.

To add a new data format

- Click 'Policy' tab at the top > 'Matcher' > 'Data Formats'
- Click 'Add' from the 'Data Formats" screen

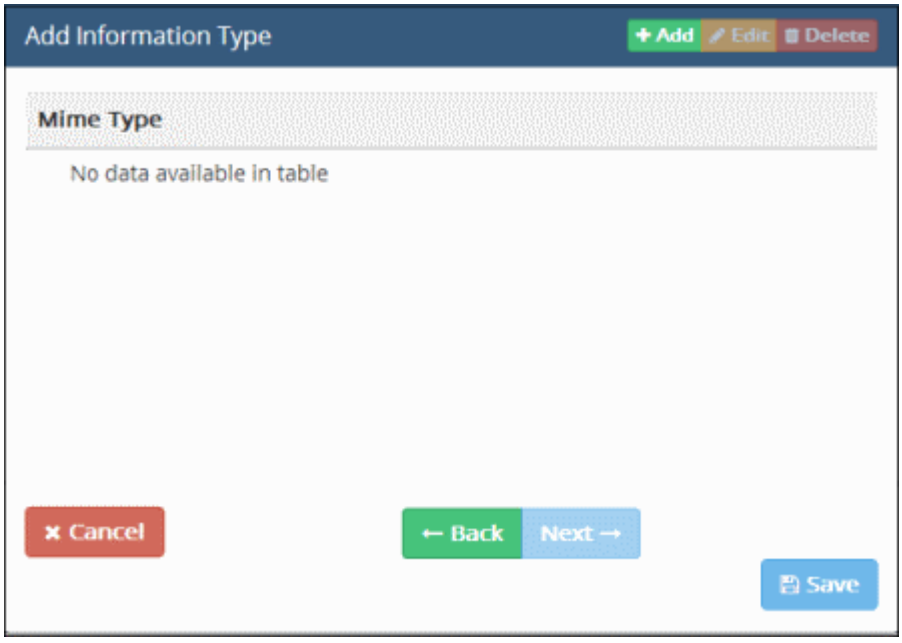


The 'Add Data Format' dialog will be displayed.



- Enter a name for the data format in the 'Data Format Name' field
- Click 'Next'

The 'MIME Type' dialog' will appear.

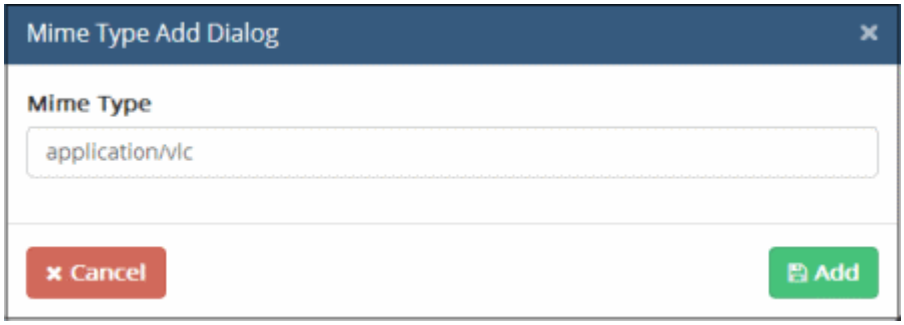


Background Note: The MIME type is a two part string identifier for a file type, containing the "type"/ "subtype". The "type" refers to a logical grouping of many MIME types that are closely related to each other. "subtypes" are specific to one file type within the "type".

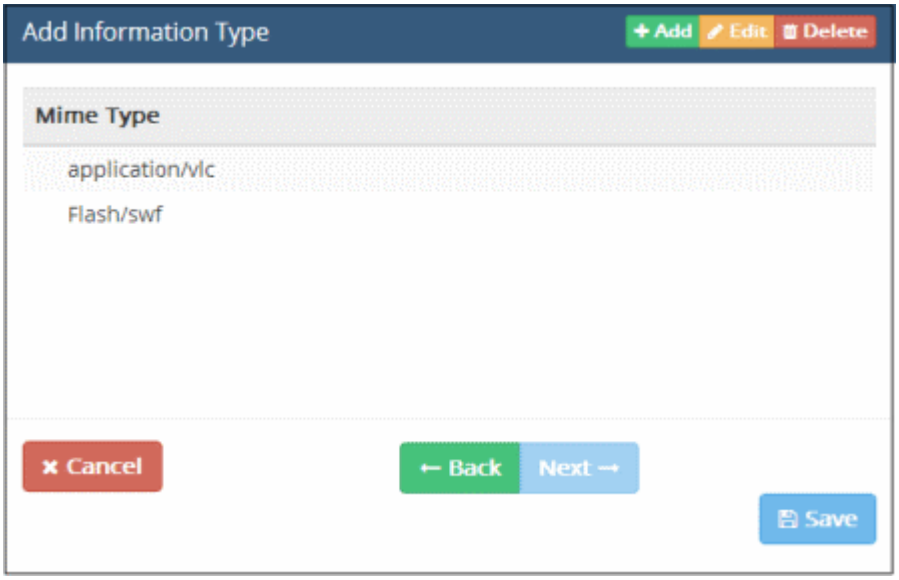
For example, the MIME value "images/jpg" is used for jpeg image files and specifies that the "jpg" subtype belongs to the "image" type.

- To add a file type by specifying in 'MIME Type', click the 'Add' button at the top

The 'MIME Type Add Dialog' will be displayed.



- Enter the new file type to be added to the data format collection in MIME type format
- Click 'Add'
- Repeat the process to add more file types.



- Click 'Back' to review and make any changes
- Click 'Save'

The Data Format will be saved and listed.

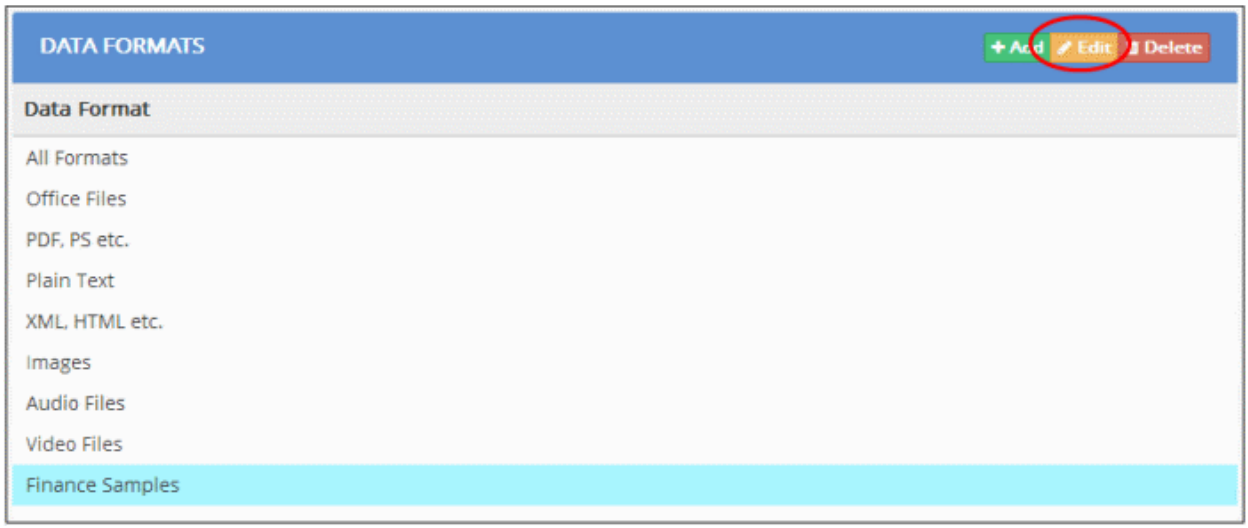
For the changes to propagate through the rules in which the data format being edited is applied, the policy needs to be re-deployed. Refer to the section **Deploying a Policy** for more details.

5.3.4.2. Editing a Data Format

The administrator can add more or remove existing file types by editing the Data Format. Each Data Format contains file types belonging to a genre. MyDLP allows the file types to be added as both MIME Type and file extension. Please note you can edit only the user defined data format type.

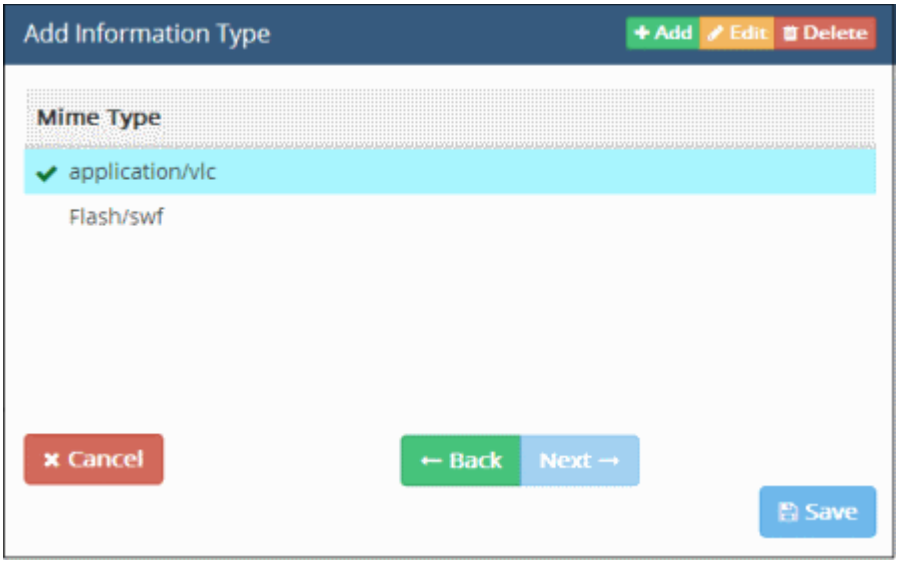
To edit a data format

- Click 'Policy' tab at the top > 'Matcher' > 'Data Formats'
- Select the data format and click 'Edit'



The 'Add Data Format' dialog will be displayed:

- Click 'Next'



- Select the MIME type and click 'Edit'. The process is similar to **adding a data format** as explained above.
- To remove a MIME type, select it and click 'Delete'
- Click 'Save' for your changes to take effect.

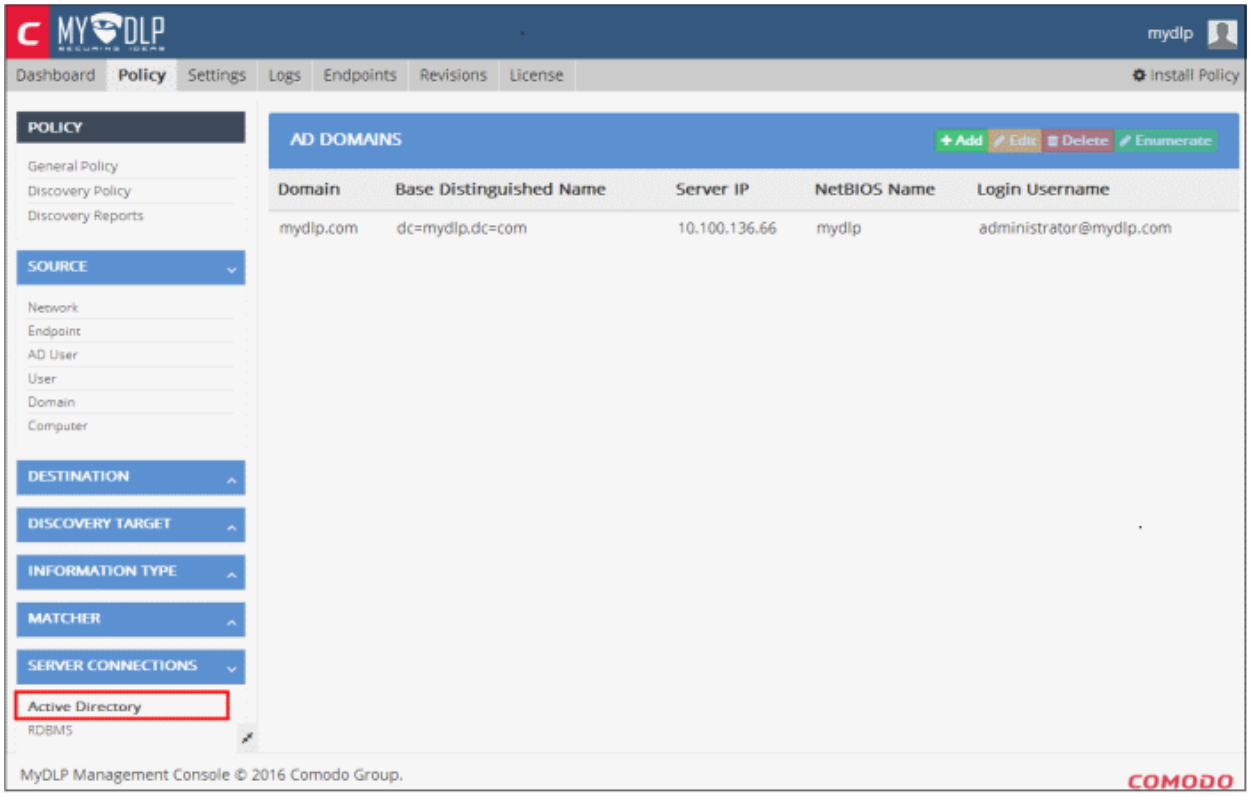
For the changes to propagate through the rules in which the data format being edited is applied, the policy needs to be re-deployed. Refer to the section **Deploying the Policy** for more details.

5.4. Integrating Active Directory Domains

MyDLP can import users from Active Directory (AD) Domains integrated to it. The AD domains integrated can be used to define user groups for creating the User Objects, which can be applied as Source Objects for all types of Data Transfer Policy rules.

The 'Server Connections' section allows the administrator to integrate AD domains which in-turn, can be used in User objects.

- Click 'Policy' tab at the top > 'Server Connections' > 'Active Directory' to open the interface



The Active Directory Domains interface displays a list of pre-integrated AD domains and allows the administrator to

- **Add new AD Domains**
- **Edit Existing Domains**

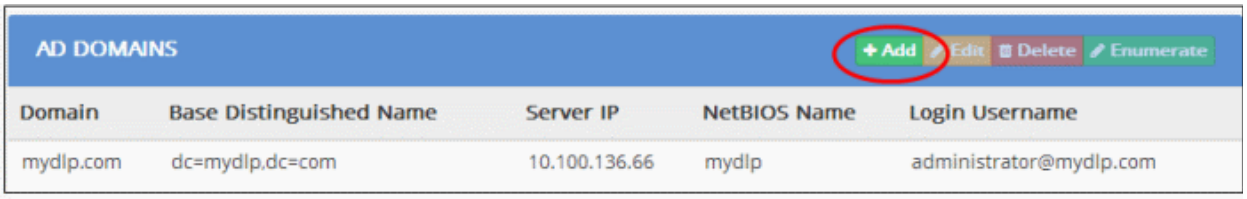
5.4.1. Adding a New AD Domain

The administrator can integrate new AD Domain specifying the domain name IP Address of the Domain Controller (DC) and the login credentials for MyDLP to access the AD server. If there are more than one domain with separate domain controllers, the administrator needs to integrate them one-by-one.

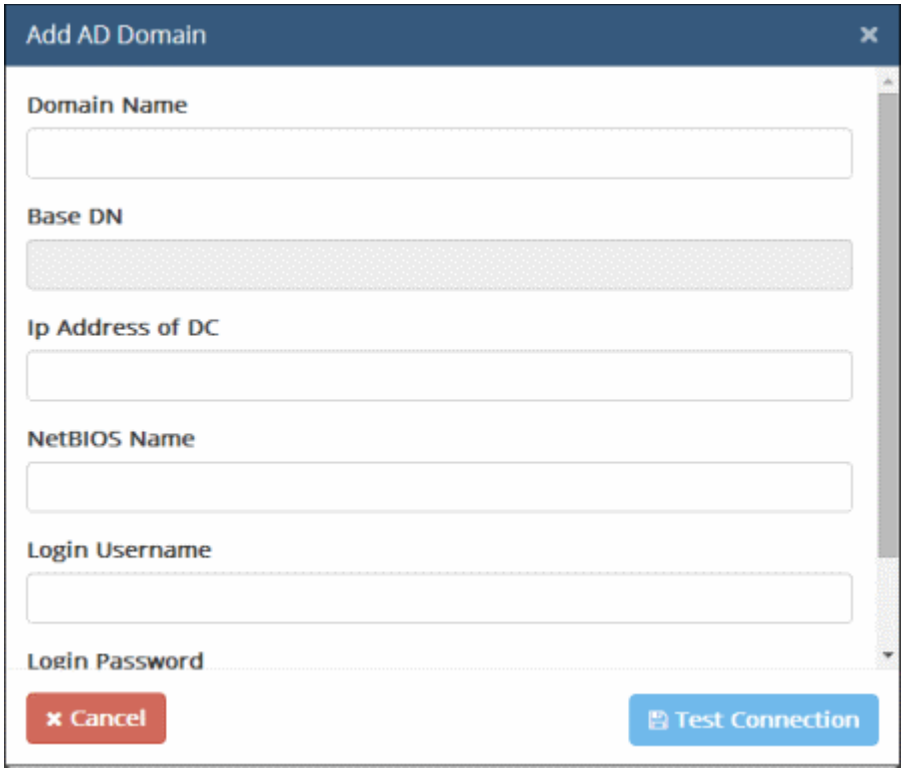
To integrate a new AD Domain

- Click 'Policy' tab then 'Server Connections' > 'Active Directory'

The AD Domains screen will be displayed.



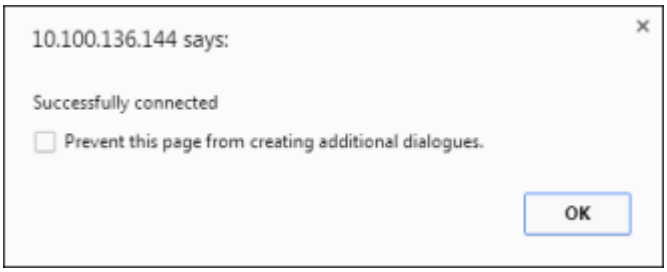
- Click the 'Add' button at the top



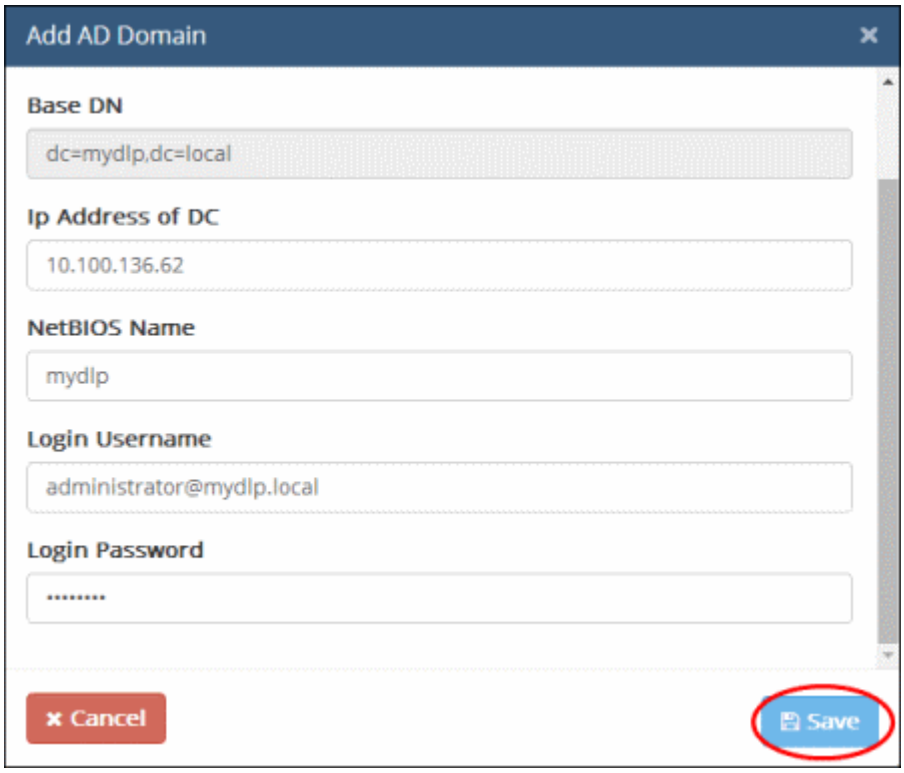
- Enter the details of the AD Domain as shown below:

Field	Description
Domain Name	Enter the Fully Qualified Domain Name (FQDN) of your domain as defined in your Domain Controller (DC).
Base DN	The Base DN will be automatically populated based on your FQDN.
IP Address of DC	Enter the IP address or the DNS resolvable hostname of your Domain Controller. If you have more than one DC in your domain enter the IP address or hostname of the primary DC.
NetBIOS Name	Enter the 16 character Network Basic Input/Output System (NetBIOS) name of your DC.
Login username and Login password	Enter the username and password of a valid user account for MyDLP to login to the AD server and import the users. For security reasons, it is advised to create a new account for Comodo MyDLP with only the required privileges to enumerate all users and groups in your AD domain..

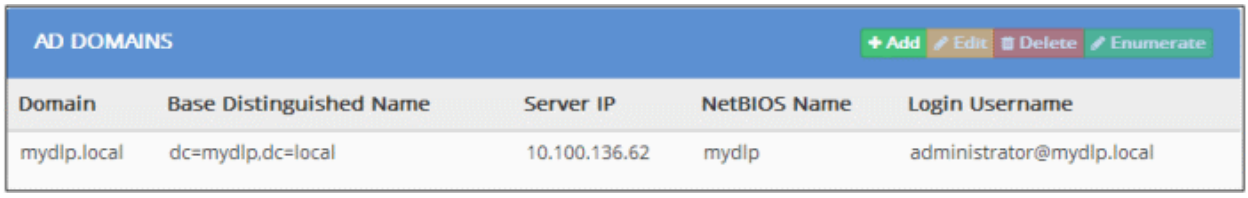
- Click 'Test Connection'. MyDLP will check whether the AD server is reachable. On successful connection, the AD domain will be added to the list.



After successful connection, Save button will appear in the 'Add AD Domain' dialog.

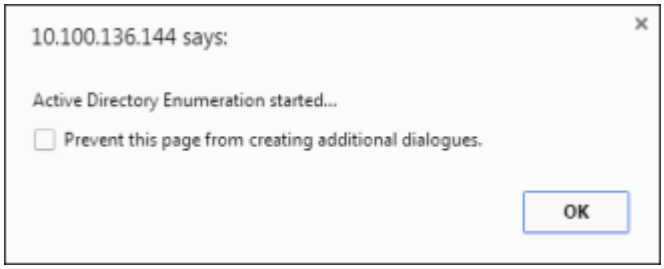


The AD Server will be added and the users can will be imported into MyDLP.



In order to import users from the AD server, select the AD Domain in the list and click 'Enumerate'.

The AD enumeration process will begin....



...and when completed, the success message will be displayed.

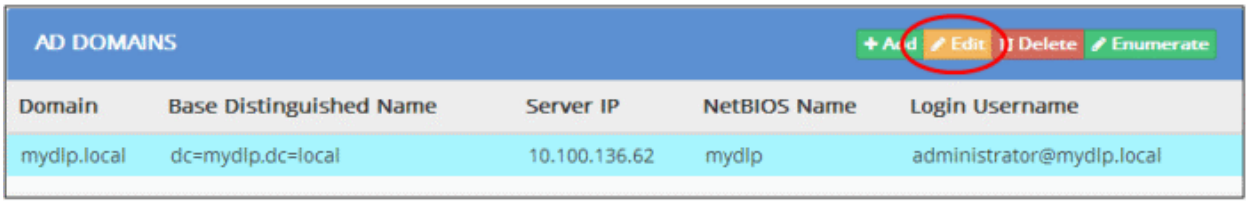
The AD users now can be added as user object. Refer to the section '**Adding a User Defined Active Directory Users Object**' for more details.

5.4.2. Editing Existing AD Domains

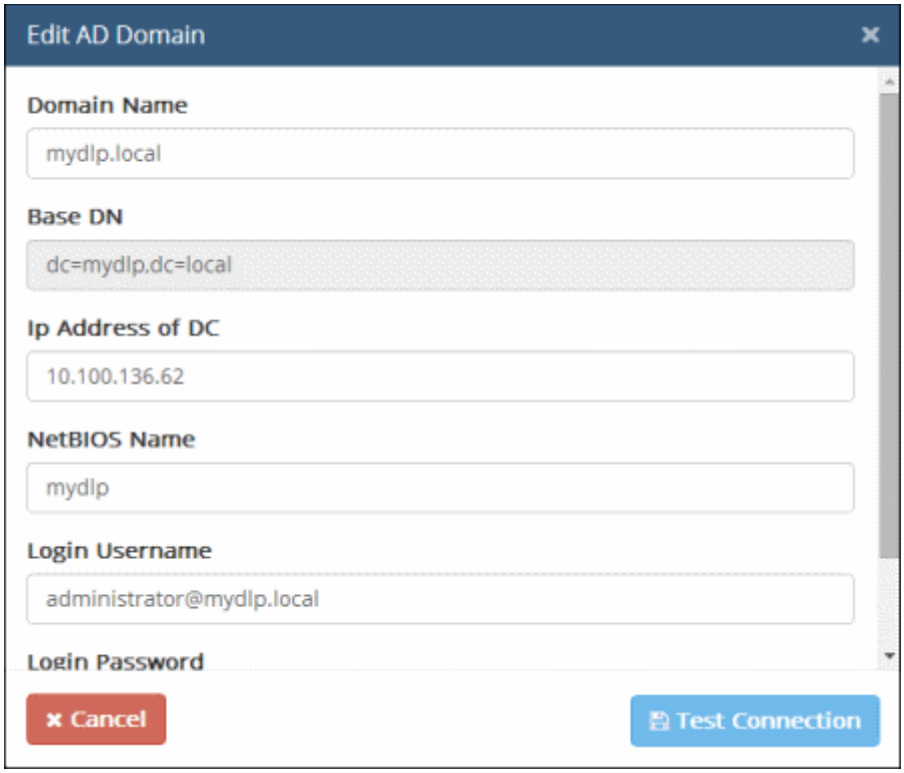
The administrator can edit the details of the pre-integrated AD Domain(s) at anytime from the 'Active Directory' interface. The changes will take effect immediately on reapplying the policy to the network.

To edit an 'AD Domain'

- Click 'Policy' tab then 'Server Connections' > 'Active Directory'
- Select the domain and click 'Edit' at the top



The 'Edit AD Domain' dialog will be displayed.



The Edit interface is similar to 'Add AD Domain' dialog. The administrator can directly edit the details, test the connections and save the changes. Refer to the section **Adding a New AD Domain** for more details on the parameters that can be configured through the interface.

- To remove an AD Domain, select it and click 'Delete'. Please note you cannot delete an AD Domain from which user objects are added. Refer to the section '**Adding a User Defined Active Directory Users Object**' for more details.

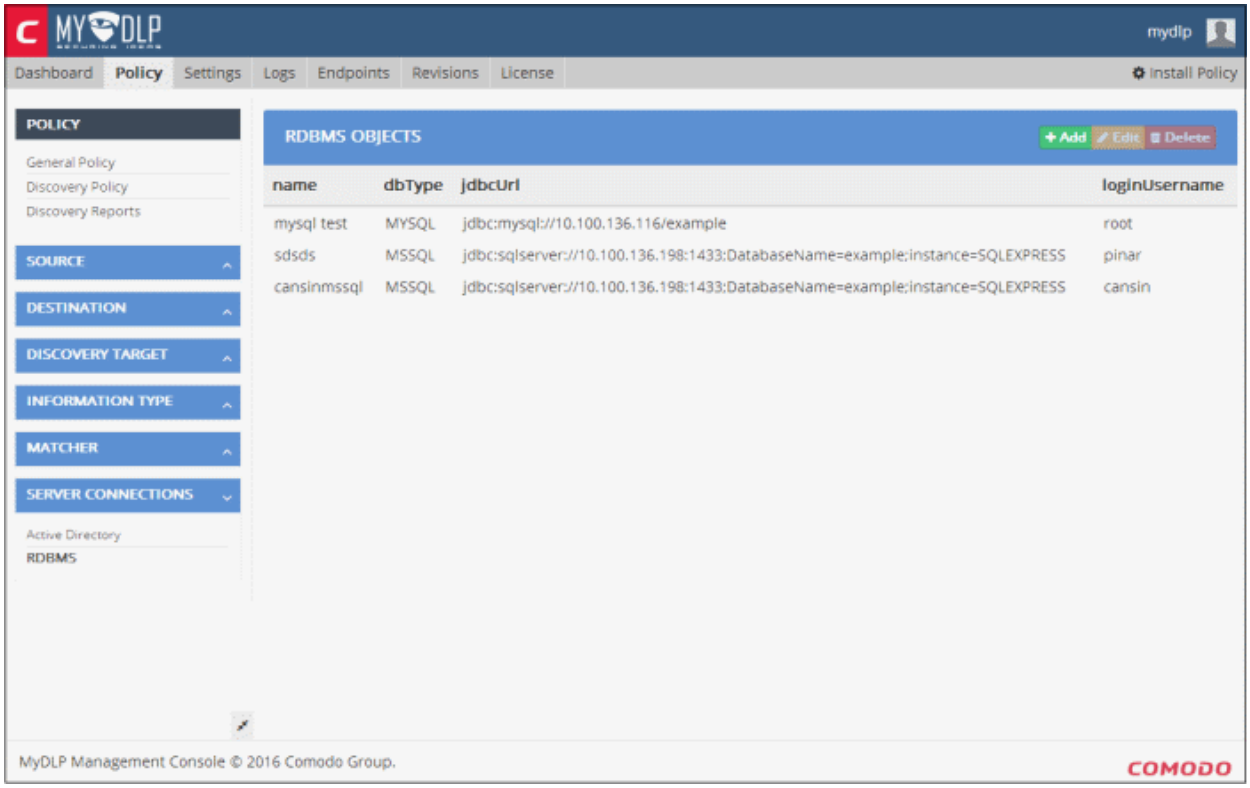
5.5. Integrating RDBMS Systems

The administrator can integrate MySQL database servers through RDBMS connections and configure MyDLP to import Keywords for use in 'Keyword Groups' and documents for use in 'Document Databases' matchers that are created from the Information Type interface. The database will be periodically checked for updates and the Keyword Groups and Document Databases will be synchronized with the respective databases.

Refer to the following sections for more information on importing data from the MySQL Servers:

- **Integrating a MySQL Database to Keyword Database**
- **Integrating a MySQL database to document database**

The RDBMS objects interface allows the administrator to add MySQL database servers. The RDBMS objects added to this interface will be available for selection for importing keywords and documents.



Refer to the following sections for more details on:

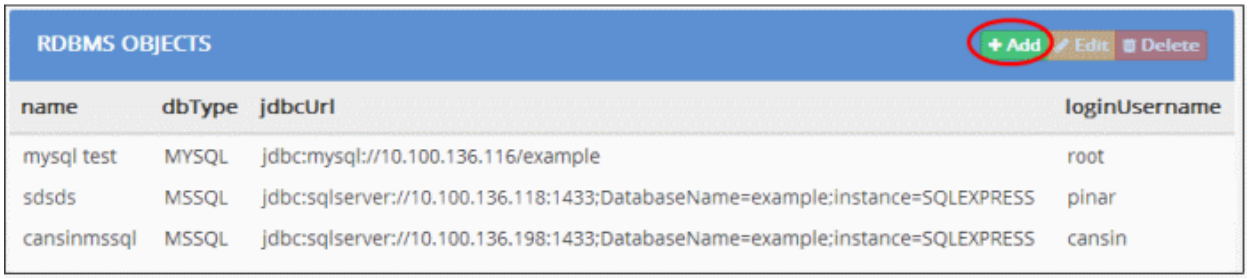
- **Adding a new RDBMS Object**
- **Editing an RDBMS Object**

5.5.1. Adding a New RDBMS Object

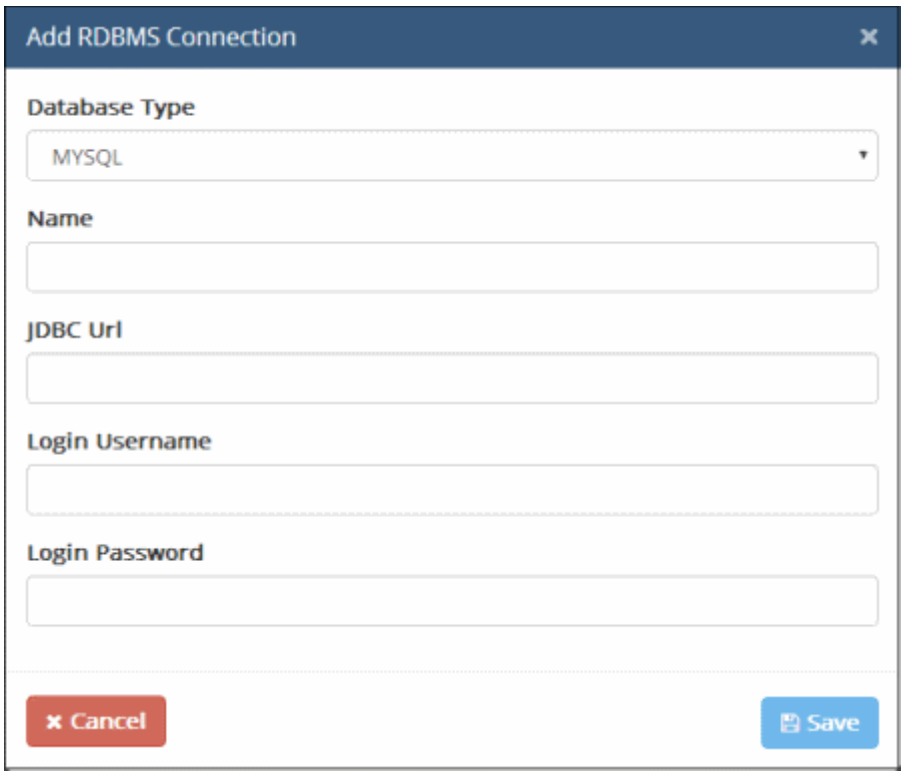
The administrator can add a new RDBMS object to integrate MySQL, MsSQL or Oracle database server by specifying the URL and login credentials of the RDBMS server. If there are more than one database server, the administrator needs to add them one-by-one.

To add a new RDBMS object

- Click the 'Policy' tab then 'Server Connections' > 'RDBMS'
- Click 'Add' from the 'RDBMS Objects' screen



The 'Add RDBMS Connection' dialog will be displayed.



- Enter the details of the RDBMS server as shown below:

Field	Description
Database Type	Choose the type of database from the drop-down. The available options are: • MySQL • MsSQL • Oracle
Name	Enter a name shortly describing the connection.
JDBC URL	Enter the Java Database Connectivity (JDBC) URL of the RDBMS server
Login username and Login password	Enter the username and password of a valid user account for MyDLP to login to the RDBMS server. For security reasons, it is advised to create a new account in the server for Comodo MyDLP with only the

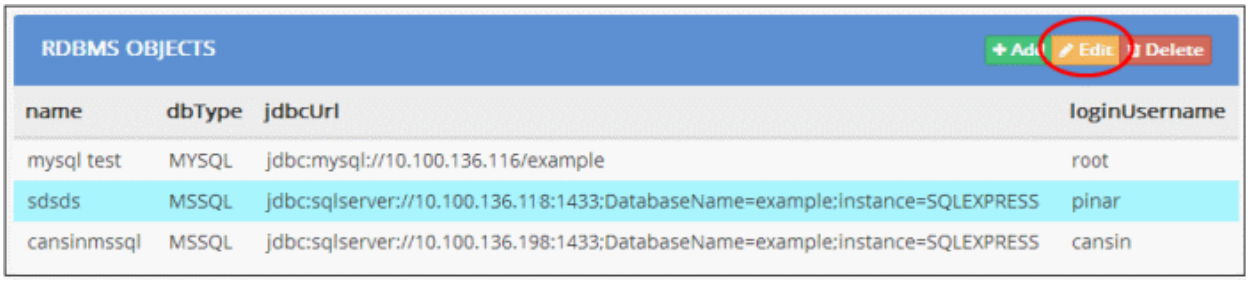
	required privileges to enumerate required entries from the server.

- Click 'Save'

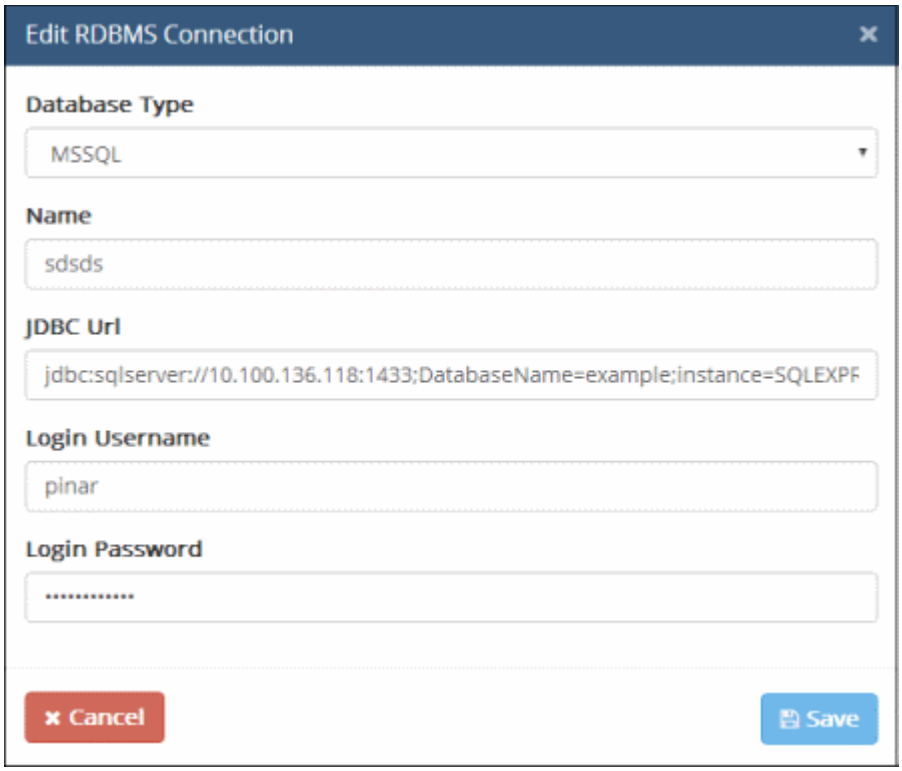
MyDLP will connect to the server and if the credentials are successful, the RDBMS server will be connected to MyDLP. The database server will be available for selection for importing keywords or documents when creating **Keyword Database** and **Document Database** under the Matcher section.

5.5.2. Editing an RDBMS Object

The administrator can view the details of and edit an RDBMS object at any time by selecting the connection from the 'Server Connections' > 'RDBMS' interface.



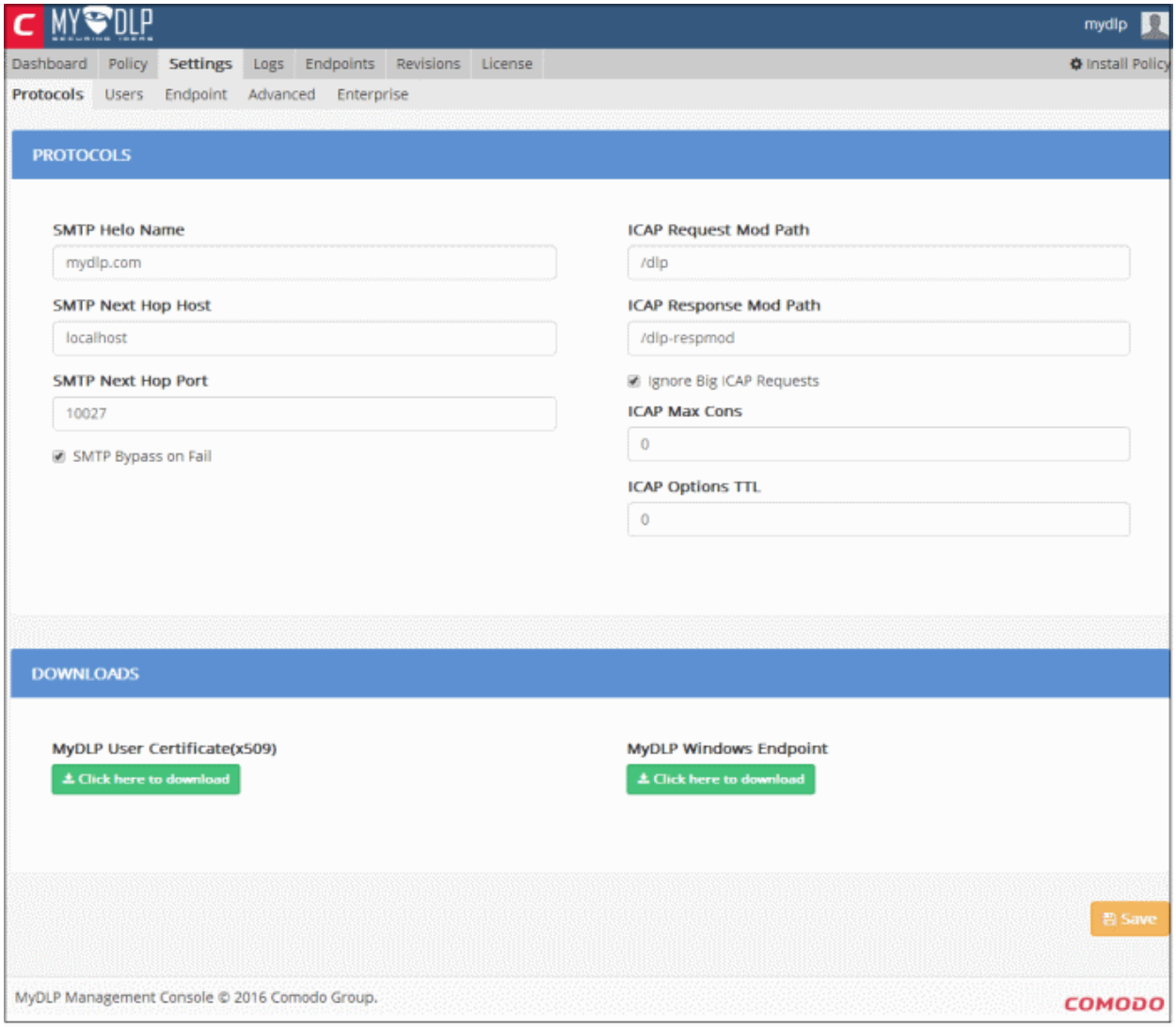
The 'Edit RDMBS Connection' dialog will be displayed.



- To change the parameters, directly edit the parameters
- Click 'Save'. MyDLP willl check whether the RDBMS server is reachable and on successful connection, the database will be available for selection.
- To remove a RDBMS object, select it from the list and click the 'Delete' button. Please note you cannot delete an RDBMS object from which keyword and document databases are added. Refer to the sections '**Keyword Database**' and '**Document Database**' for more details.

6.Configuring Comodo MyDLP Settings

The Settings interface allows the administrator to configure various parameters of Comodo MyDLP.



The interface contains five tabs:

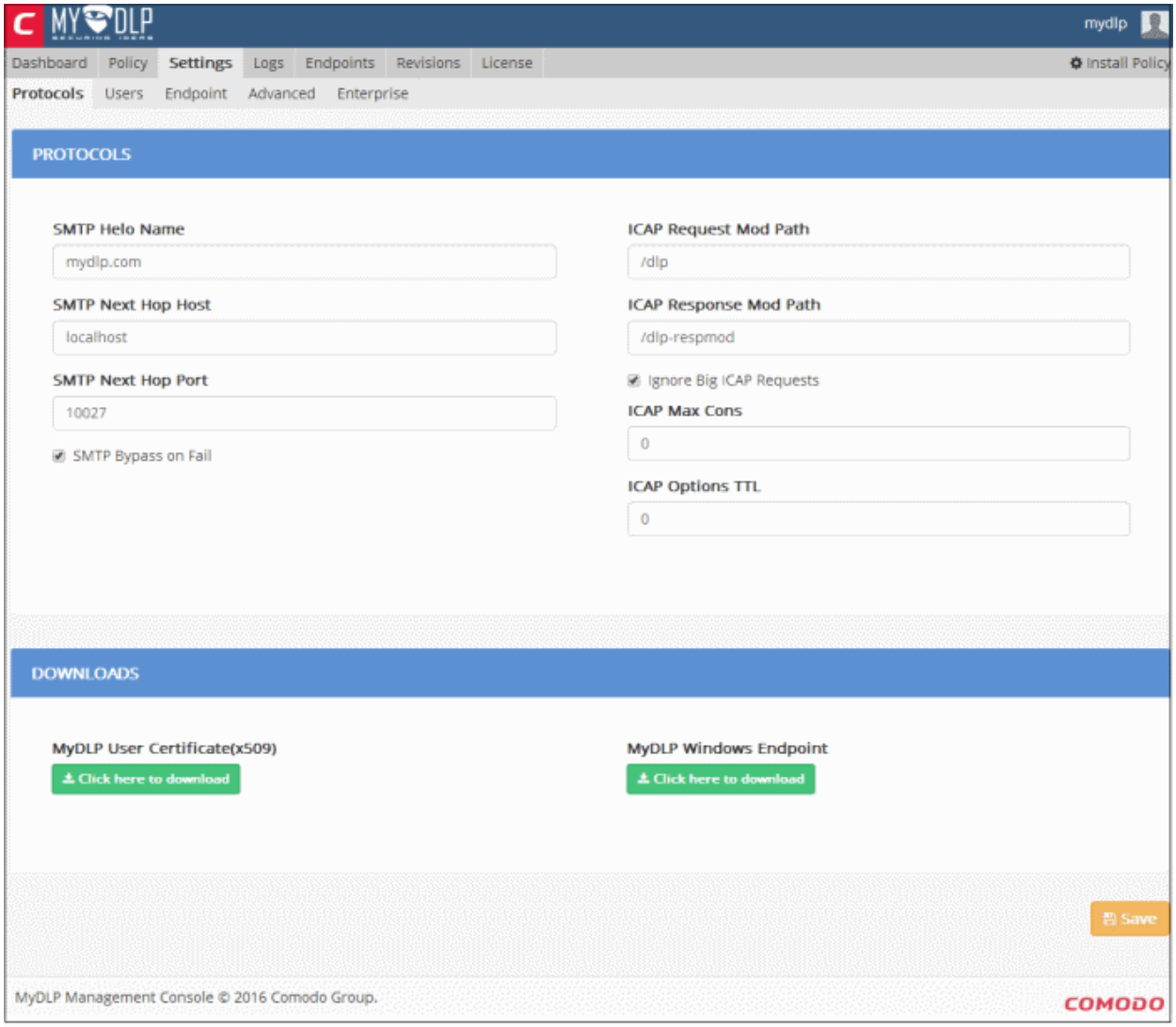
- **Protocols** - Enables the administrator to view and configure connection protocols used by the DLP server to the endpoints and the web proxy server. Refer to the section **Configuring Protocol Settings** for more details.
- **Users** - Enables the administrator to add and manage peer administrative users. Refer to the section **Managing Administrators** for more details.
- **Endpoint** - Enables the administrator to configure the connection parameters for the MyDLP server to connect to the endpoints. Refer to the section **Configuring Endpoint Settings** for more details.
- **Advanced** - Enables the administrator to configure the advanced application settings of MyDLP. Refer to the section **Configuring Advanced Settings** for more details.
- **Enterprise** - Enables the administrator to configure miscellaneous settings as per the enterprise policy and email notifications. Refer to the section **Configuring Enterprise Settings** for more details.

6.1.Configuring Protocol Settings

The 'Protocol' tab allows the administrator to configure the Simple Mail Transfer Protocol (SMTP) parameters used

for sending mails from the MyDLP server and the Internet Content Adaptation Protocol (ICAP) parameters for connection to the web proxy for Internet connection. The administrator can also download the user authentication certificate from the interface and install at the endpoints for connection authentication to the MyDLP server.

The Protocol interface is displayed by default whenever the Settings interface is opened. To return to the Protocol interface from other interfaces, click the 'Protocol' tab.



Field	Description
SMTP Helo Name	The mail domain name used for HELO greeting command in SMTP protocol by the MyDLP server. Default = mydlp.com. You can change it to your mail domain name.
SMTP Next Hop Host	The host used for the next SMTP hop during outgoing mail delivery from MyDLP server. Default = localhost. You can change it if you want to use a different host
SMTP Next Hop Port	The TCP port number of the host used for the next SMTP hop during outgoing mail delivery from MyDLP server. Default = 10027.
SMTP Bypass on Fail	Determines the behavior of email engine of MyDLP in case of any error. If this option is selected, MyDLP will pass mails on error case for availability. If this option is not selected, MyDLP will block mails on error for security. Default =

	Selected.
ICAP Request Mod Path	The ICAP request module path used by the MyDLP Server for integration with ICAP enabled web proxy. Default = /dlp
ICAP Response Mod Path	The ICAP response module path used by the MyDLP Server for integration with ICAP enabled web proxy. Default = /dlp-respmod
Ignore Big ICAP Requests	Instructs MyDLP to ignore ICMP requests if their data volume is larger than a specified value. Default = Selected.
ICAP Maximum Connections	The maximum number of ICAP connections that can be allowed to run simultaneously. Default = 0 - Denotes unlimited number of connections
ICAP Options TTL	The Time To Live (TTL) parameter for the ICAP connections. Default = 0 - Denoted unlimited

- Click 'Save' for your changes to take effect.

MyDLP User Certificate (x509) - MyDLP intercepts even SSL enabled webpages and relays them to the endpoints for monitoring the webbased traffic as per the Web rules. In such cases, a certificate mismatch error will be displayed to the user. To avoid this, the administrator can download the MyDLP Server certificate and install it on to the endpoints or the AD server.

- To download the certificate in X509 format, click the 'Click here to Download' link.

MyDLP Windows Endpoint - The MyDLP admin console requires MyDLP agents installed on all the endpoints to be monitored in the network. The agent is responsible for deploying the data transfer policy at the endpoint in order to monitor the data traffic through various channels and to allow, log, quarantine, block the data as per the rules. The agent also scans the endpoint to identify the data that match the discovery rules and to log, allow, quarantine or delete them as per the rules. The endpoint agent installation is password protected and cannot be uninstalled from the endpoint without entering the password set in the Settings Endpoint interface. Refer to the section **Configuring Endpoint Settings** for more details.

The administrator can download the agent set-up file for installation on to endpoints from the 'Protocols' interface.

- To download the certificate in X509 format, click the 'Click here to Download' link.

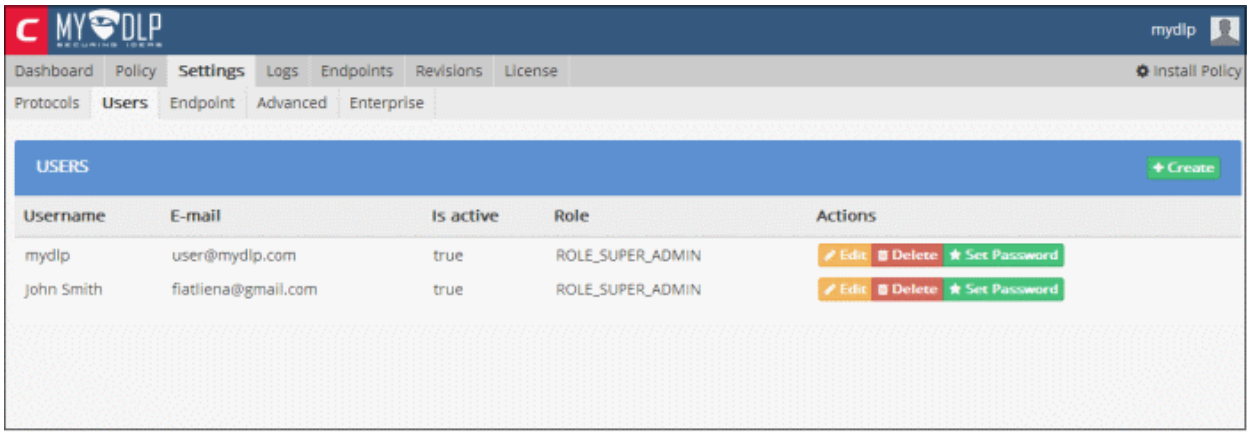
For more details on MyDLP Endpoint deployment, please refer to the **MyDLP Endpoint Installation Guide**.

6.2. Managing Administrators

The 'Users' tab displays the list of administrative users that can receive automated notification emails from MyDLP and access the MyDLP administrative console and allows the administrator add and manage the users. There are five administrative roles in MyDLP with different privilege levels.

Administrative Role	Description and Privilege Levels
Super Administrator	Super Administrator role has the ultimate authority in a MyDLP system. The Super Administrator can set up and configure MyDLP during deployment. Super Administrator has all the privileges as shown below: • Create and manage administrative users of any administrative role. • See DLP event logs and content data attached to event logs. • Edit DLP policy and objects • Install policy

	• Edit all settings under Settings Tab.
Administrator	Administrator has restricted technical management access. Administrator can manage day-to-day operations, manage policy and edit almost all settings. Administrators are added from employees of the IT department and do not need to have the privilege to see confidential file contents captured during Archive or Quarantine actions. Administrator will not able to see the content data in DLP incident logs and cannot download archived files. Administrator has the following privileges: • Create and manage administrative users with roles of peer Administrator and Classifier and None. • See DLP event logs but cannot access files attached to logs. • Edit DLP policy and objects. • Install policy. • Edit all settings under Settings Tab, has restricted access to Users Tab.
Auditor	Auditor has restricted access to Logs Tab. The Auditor does not have the ability to change any settings or DLP policy. The Auditor can be an executive from legal department, will be able to see DLP event logs and can access content data attached to these logs. Authority Scope is a restriction which can be defined when MyDLP is integrated with Microsoft Active Directory to limit the events that can be seen by the Auditor for one or more specified organization units. Auditor has the following privileges: • See all DLP logs and content data attached to logs (If Authority Scope is not specified) • See DLP logs related to specified Authority Scope(If Authority Scope Specified)
Document Classifier	Classifier has restricted access to the Objects Tab. Classifier can upload documents to previously specified Document Databases. Classifier has the following privileges: • Upload documents to predefined Document Databases
None	The administrator with the role 'None' will be able to receive the automated notifications sent by MyDLP on occurrences of various incidents intercepted by the data transfer policy and discovery rules configured in MyDLP. The administrator does not have any rights to create or modify the rules and cannot access MyDLP administrative interface.



The 'Settings' > 'Users' interface allows the administrator with appropriate privileges for the following:

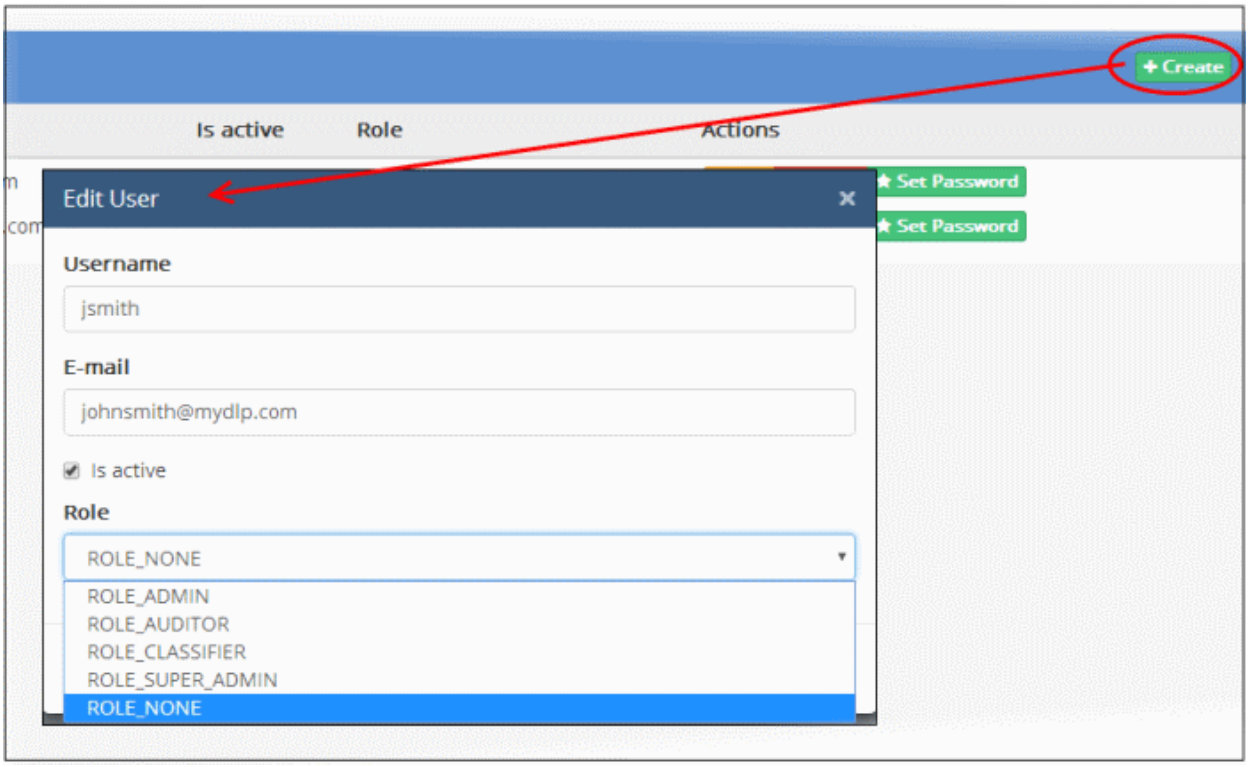
- **Add New Administrative Users**
- **Set/Reset Password for Administrative Users**
- **Edit and Remove Users**

6.2.1. Adding new Administrative Users

The super administrator can add peer super administrators and other administrators of any role and administrators can create peer administrators and classifiers from the Users interface.

To add a new administrative user

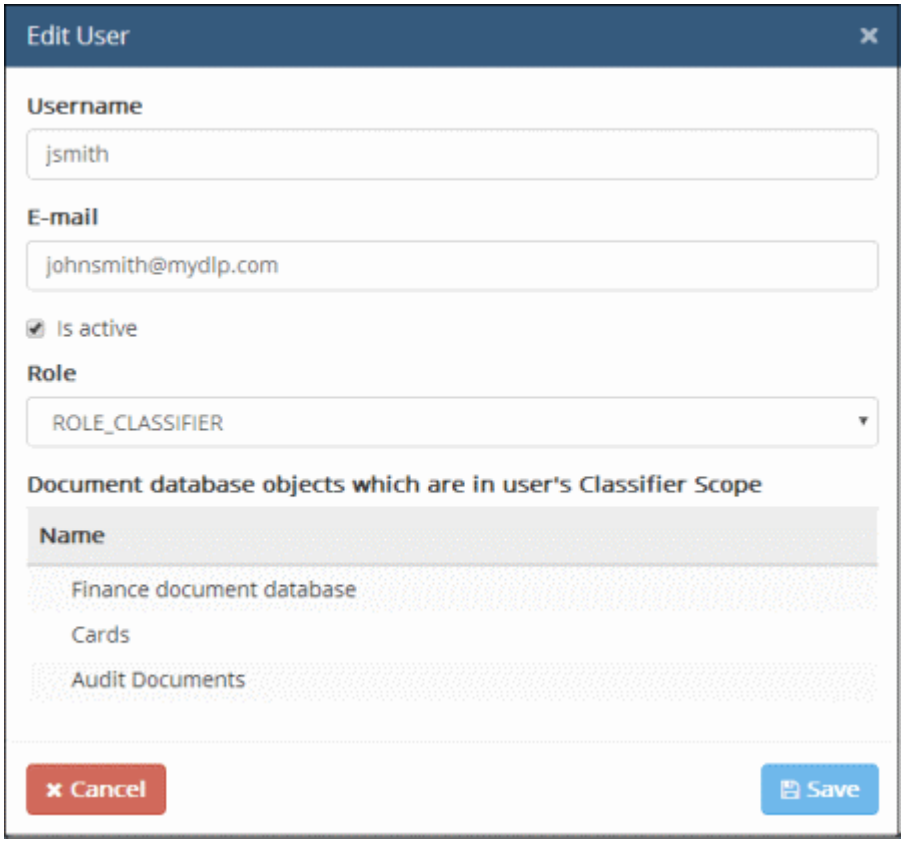
- Open Settings > Users interface and click Create at the top right. The 'User Dialog' will appear.



- Enter the details of the new user as shown below:
  - User Name - Enter the login username for the new user
  - Email - Enter the email address of the new user
- Select the 'Is Active' checkbox if the user should be enabled upon creation

- Select the User Role from the list box. For more details on the **Administrative Roles** refer to the table at the top of the section **Managing Administrators**.

If you are adding an admin with classifier role, you need to specify additional parameters as shown below:



On choosing the ROLE_CLASSIFIER, the document databases previously configured in '**Document Database**' under 'Matcher' section are listed below 'Name'.

- Select the databases to be included into the classifier's scope from the list and click 'Save'.

The new user will be added.

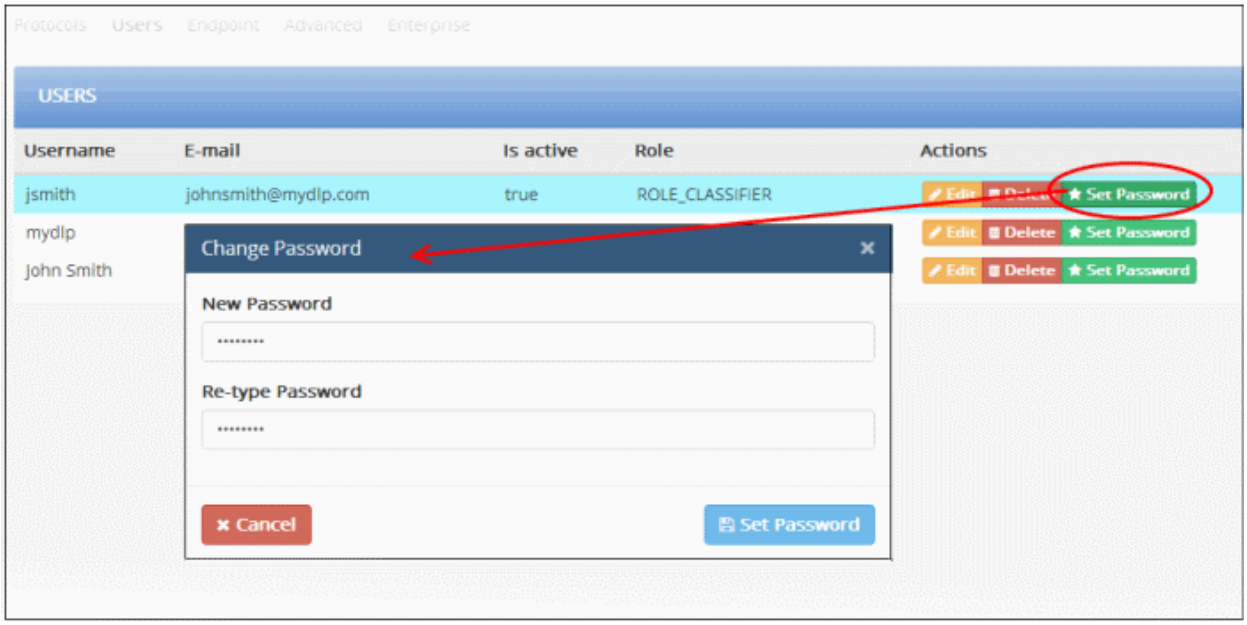
The next step is to set a password for the new administrative user to enable them to login. Refer to the next section **Setting and Resetting Password for Administrative Users** for explanation on setting password for the new user. Once logged-in the new administrator can change his/her login password by clicking their username displayed at the top right of the interface.

6.2.2. Setting and Resetting Password for Administrative Users

The super administrator can set new password or reset password for peer super administrators and the other administrators of any role. The Administrators can set new password and reset password for peer administrators and classifier.

To set or Reset password for an administrative user

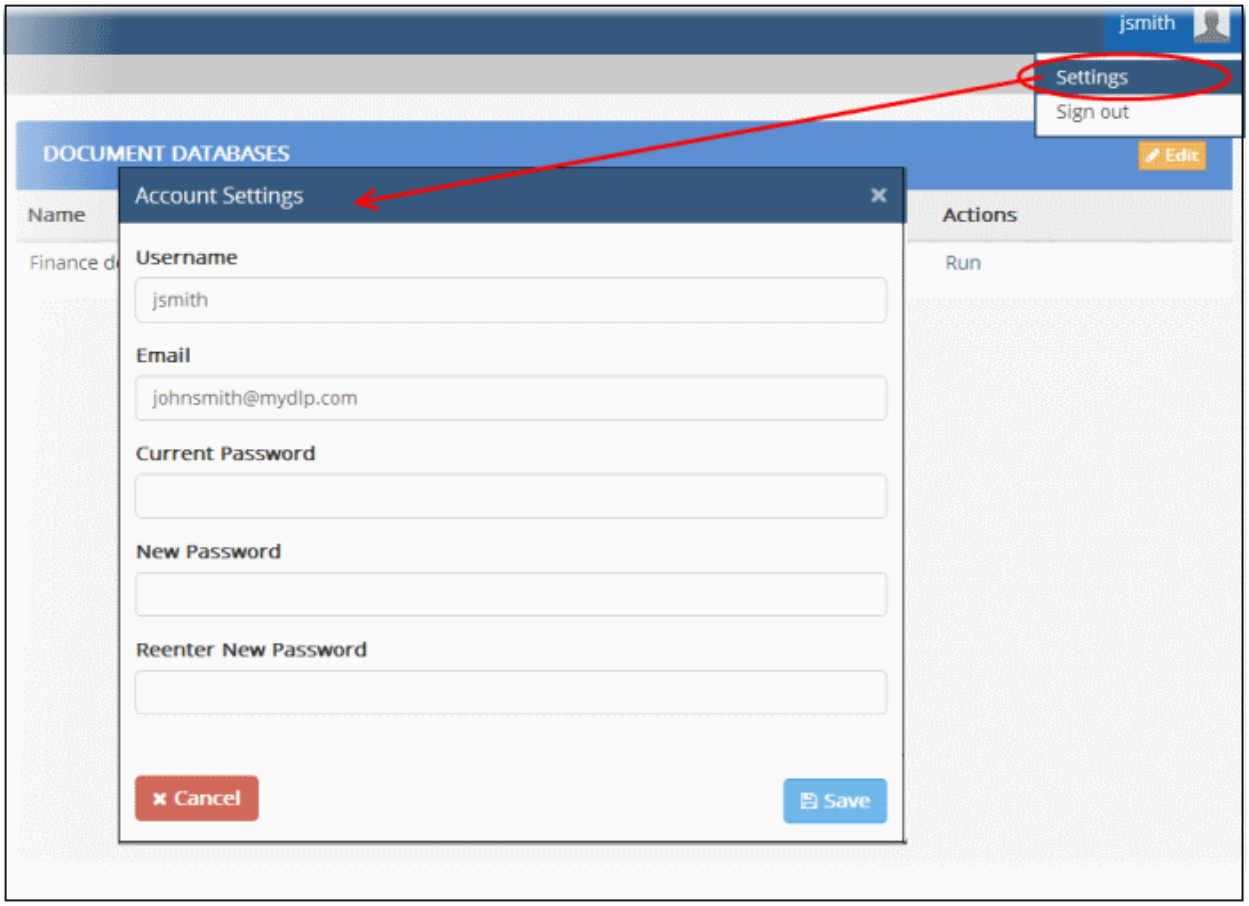
- Open 'Settings' > 'Users' interface
- Click 'Set Password' beside the user that you want to set password. The 'Change Password' dialog will appear.



- Enter a new password for the user in the New Password text field. The password should contain at least one upper case character, one lowercase character and a numeral and should be of minimum six characters. Select the password as a combination of upper/lower case alphabets, numerals and special characters so that it could not be easily guessed.
- Reenter the password for confirmation in the 'Re-type Password' field and click 'Set Password'.

The user will now be able to login to the administrative console using the username created while adding the user and the password set in this dialog.

Upon their login, the user can change his/her password by clicking their username displayed at the top right of the interface, choosing 'Settings' from the drop-down and entering the new password in the 'Account Settings' dialog.

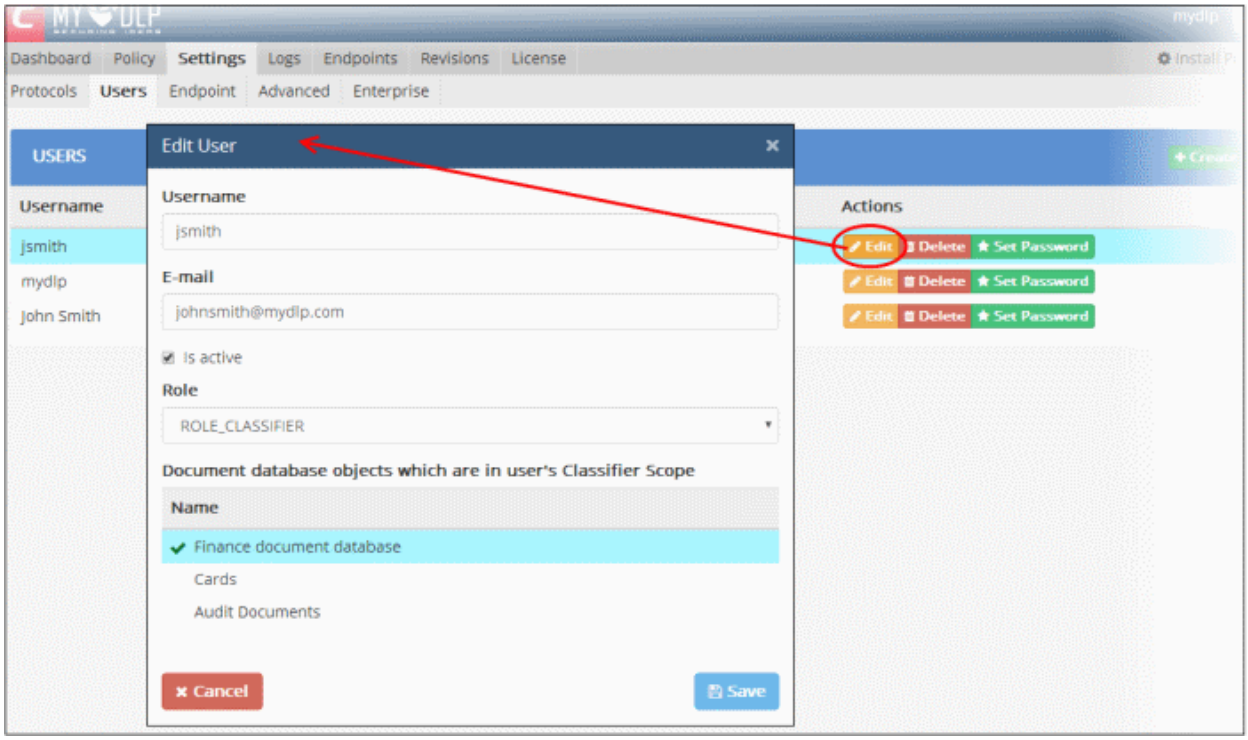


6.2.3. Editing and Removing Admin Users

Admin users can be edited by other administrators who have the appropriate privileges.

To edit an admin user

- Open Settings > Users interface
- Click 'Edit' beside the user whose details you wish to view or modify. The 'Edit User' dialog will appear:



The dialog allows you to:

- Change username and email address
- Enable or disable the user via the 'Is Active?' check-box
- Change their role and modify role privileges

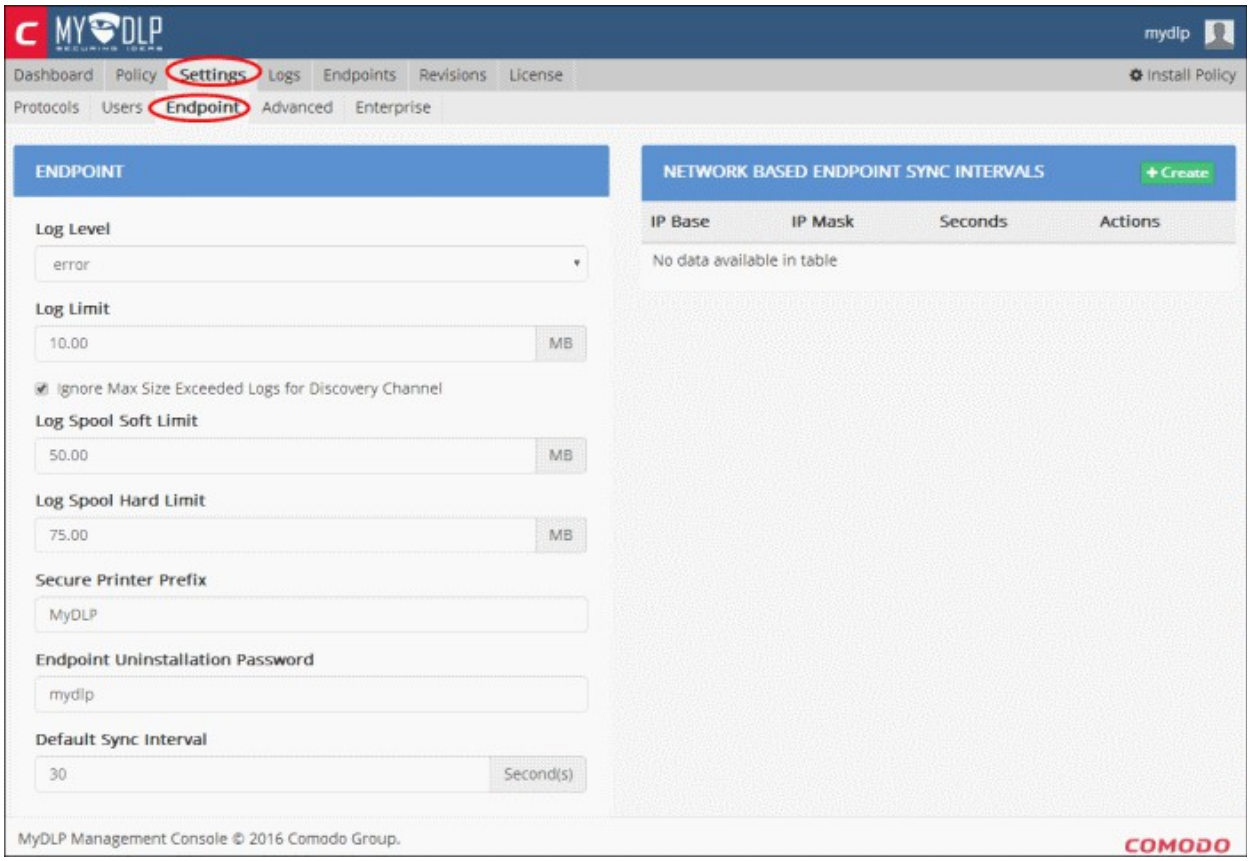
Click 'Save' for your changes to take effect.

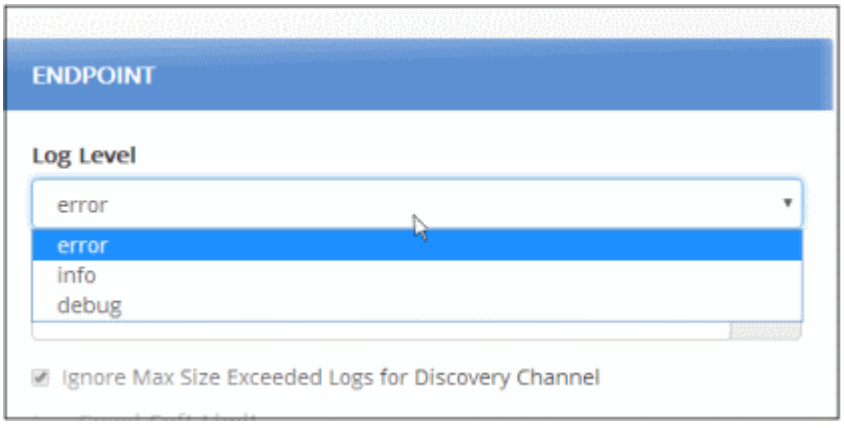
Tip: You can update passwords by selecting a user and clicking the green 'Set Password' button on the right.

6.3. Configuring Endpoint Settings

The 'Endpoint' tab in the 'Settings' interface allows administrators to configure log parameters and various other endpoint settings. The settings configured here apply to all endpoints connected to the MyDLP Server.

To access the Endpoint tab, click 'Settings' > 'Endpoint':



Field	Description
Log Level	Indicates the level of log details generated by endpoint agent that an administrator wants view.  • Info – Displays only the captured data based on policy • Error – Displays error log at endpoint in addition to notification (Default value) • Debug – Displays more details logs about system, error and incident logs. Helps system support engineers to get more detailed logs in case of having any problem at endpoint agent. Default = Error
Log Limit	The maximum size (in MB) of the overall log file that can be stored in an endpoint.

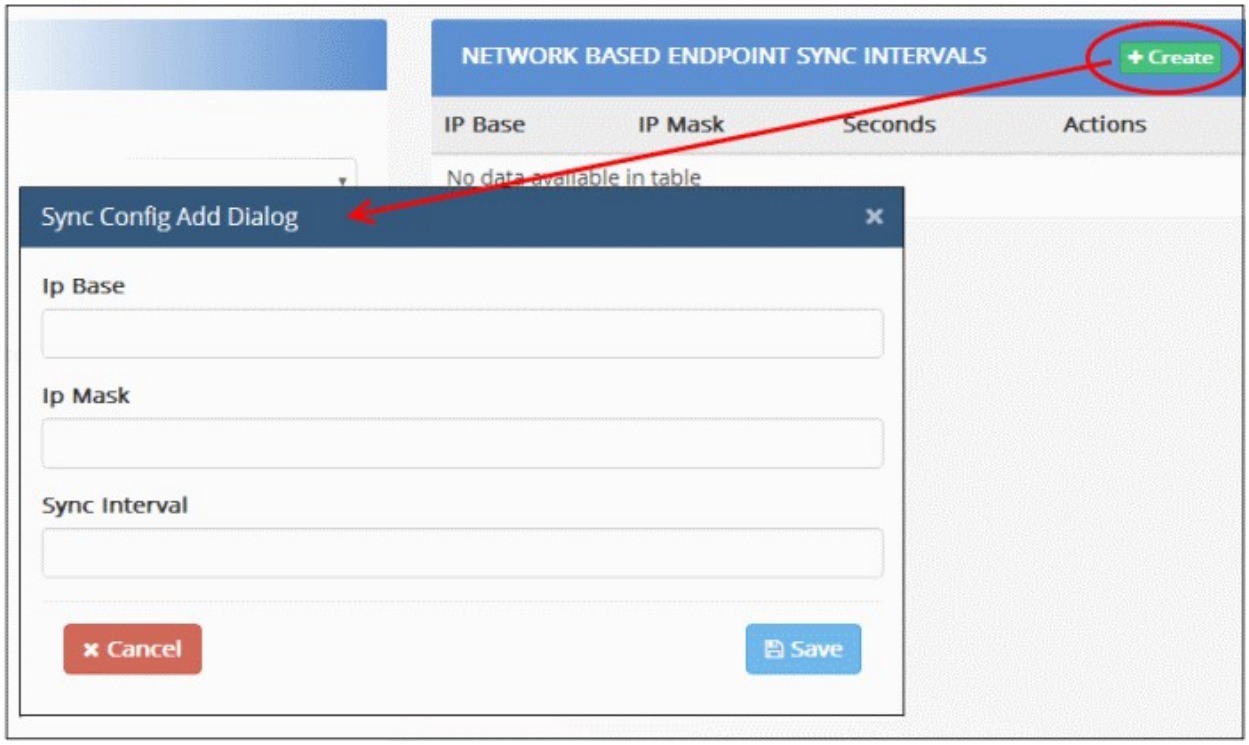
	Default = 10 MB
Ignore Max Size Exceeded logs for Discovery Channel	Instructs MyDLP to discard redundant logs that appear on identifying large number of files during discovery scans. Ignoring redundant logs conserves the disk apace at the endpoints. Default = Selected
Log Spool Soft Limit	The upper limit of log and content data stored by the MyDLP server at the endpoints. If this limit is exceeded only the content data will be discarded from the subsequent log entries. Default = 50 MB
Log Spool Hard Limit	The upper limit of log and content data stored by the MyDLP server at the endpoints. If this limit is exceeded, both the log and the content data will be discarded from the subsequent log entries. Default = 75 MB
Secure Printer Prefix	Administrators can specify a prefix for MyDLP Virtual Printers that are created upon adding a Printer Rule. Virtual printers are listed in the MyDLP interface with their physical name and the prefix defined in this field. Default = MyDLP. You can change the prefix as required. **Background Note**: MyDLP creates a virtual printer for each network printer and makes it available for printing documents from endpoints added as sources to a printer rule. End-users are forced to use the virtual printers for MyDLP to monitor the data/document passed to the printer as per the rule. If the data/document does not contain any sensitive data as defined by the rule, MyDLP forwards the documents to the physical printer.
Endpoint Uninstallation Password	Administrators can specify that a password is required to uninstall the MyDLP agent from an endpoint. Password protection prevents inadvertent uninstallation and ensures that the endpoint complies to the MyDLP policy.
Default Sync Interval	The time interval (in seconds) at which MyDLP Endpoints should synchronize with the MyDLP Server. Default = 30 seconds Administrators can set custom sync intervals for endpoints in different network zones through the 'Network based Endpoint Sync Intervals' setting explained below. The default sync interval will be applied to all other endpoints for which the custom interval is not set.

Network based Endpoint Sync Intervals - Administrators can set custom sync intervals for specific endpoint(s) by defining their network IP addresses and mask.

To set custom sync intervals for a network

- Click 'Create' beside 'Network based Endpoint Sync Intervals'

The 'Sync Config Add Dialog' will appear.



- Enter the IP address and the network mask for the endpoints to be covered
- Enter the custom sync interval for the endpoints (in seconds) in the Sync Interval field.
- Click 'Save'
- Repeat the process to add more custom sync interval settings

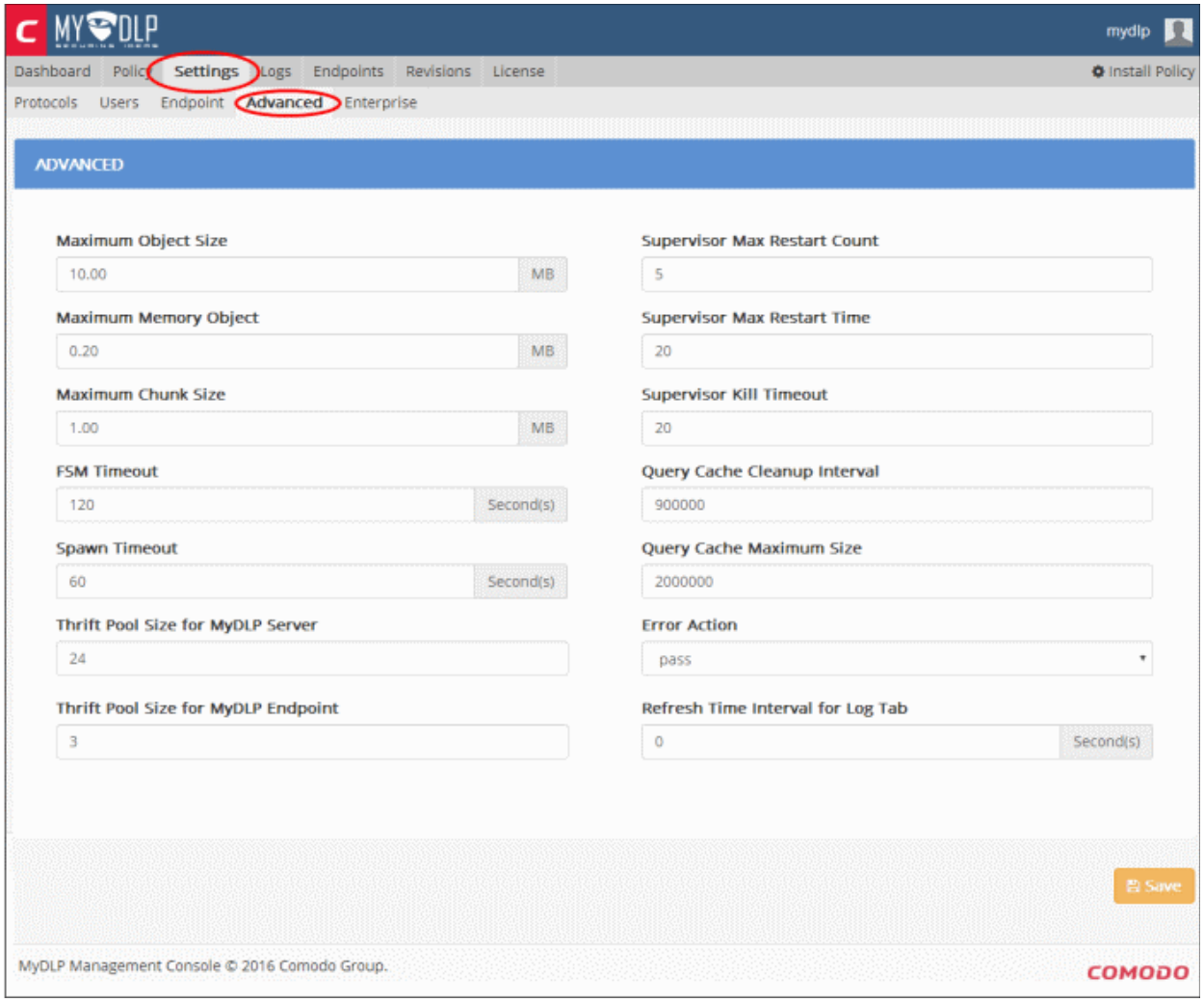
Click 'Edit' beside a sync interval to modify its details or click 'Delete' to remove it from the list.

- Click 'Save' at the bottom of the 'Endpoint' setting screen for your changes to take effect.

6.4. Configuring Advanced Settings

The 'Advanced' tab of the 'Settings' interface allows administrators to configure advanced parameters such as time-out periods and maximum sizes of memory objects, chunks and files. MyDLP ships with optimal default values for these parameters but, in certain circumstances, administrators may wish to modify these settings for special deployment and clustering scenarios.

To open the Advanced Settings interface, click 'Settings' > 'Advanced' tab.



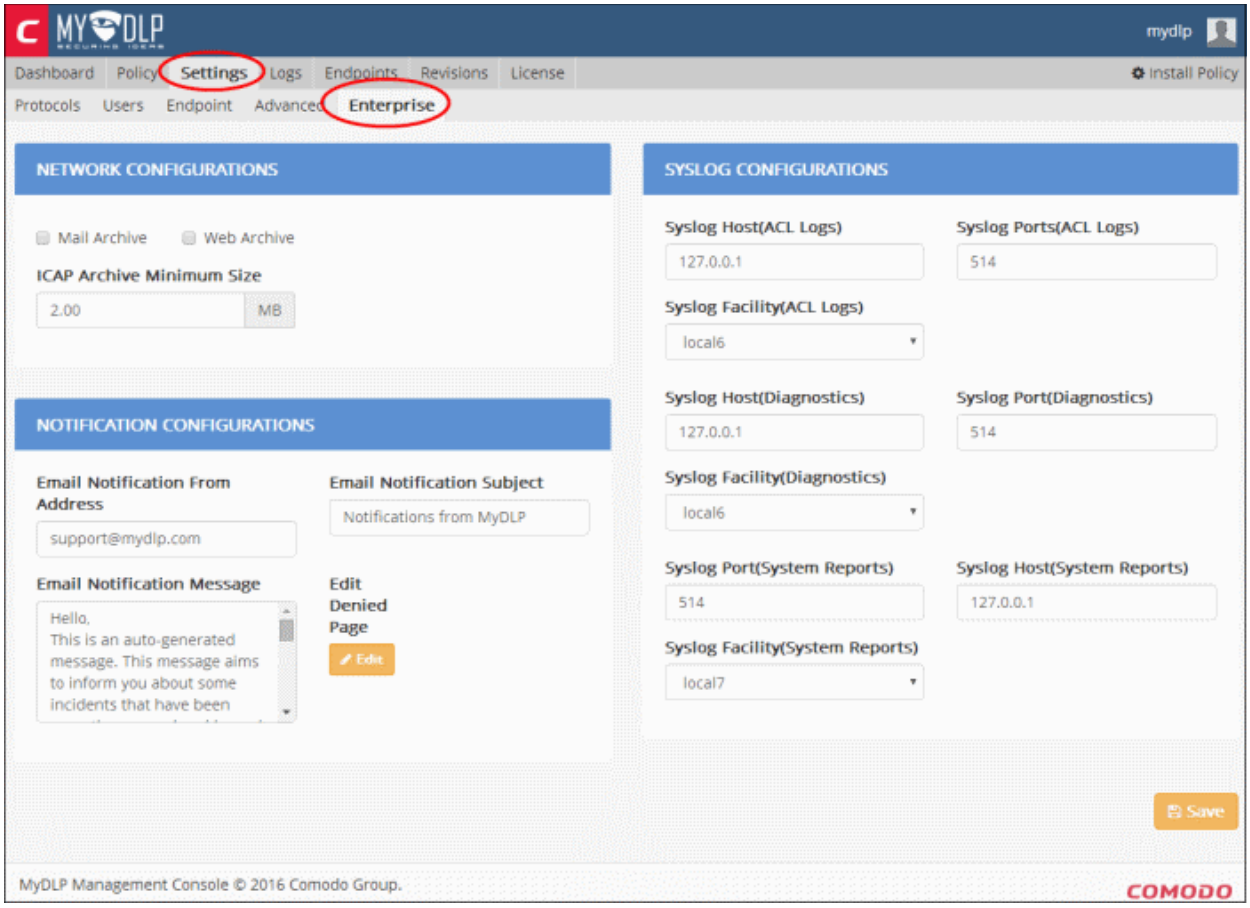
Field	Description
Maximum Object Size	The maximum chunk size of object which is processed in MyDLP in MB. Default = 10 MB You can increase this value to analyze larger files. Although MyDLP is efficient, analyzing very large files can decrease performance and archiving or quarantining large files may require substantial storage space. If you try to copy or move a file of size larger than this value, the incident will be logged. The Incident Log Details pane of the respective log entry will show a message "Max file size exceed". Refer to the explanation under '**Removable Storage Inbound rule**' in the section **Viewing Details of a Log Entry** for more details.
Maximum Memory Object	The maximum size of the objects (in MB) that can be loaded to memory in the work flow. Default = 0.20 MB
Maximum Chunk Size	The maximum size (in MB) of chunk for getting MIME type and hash in MyDLP incident logging process. Default = 1 MB
FSM Timeout	The time-out interval for each state in Finite State Machines (FSM) in MyDLP server which are used for processing ICAP, SMTP connections and communication between MyDLP server and MyDLP endpoints. Default = 120 Seconds
Spawn Timeout	The time-out of each spawned process in MyDLP work flow. Default = 60 Seconds

Thrift Pool Size for MyDLP Server	Active number of connections to the MyDLP backend service which is used for converting files to the meaningful data in MyDLP Server. Default = 24
Thrift Pool Size for MyDLP Endpoint	Active number of connections to the MyDLP backend service which is used for converting files to the meaningful data in MyDLP Endpoint. Default = 3
Supervisor Max Restart Count	The maximum number of retry count for restarting worker processes controlled by a supervisor process. Default = 5
Supervisor Max Restart Time	The maximum waiting time (in milliseconds) for restarting workers controlled by the supervisor process. Default = 20 Milliseconds
Supervisor Kill Timeout	Upon termination of child/worker processes, the supervisor process sends 'Terminate' command and makes the child/worker process wait for an exit signal. If no exit signal is received within the specified time the child processes are unconditionally terminated. The 'Supervisor Kill Timeout' specifies the maximum waiting time (in milliseconds) for the 'Exit' signal. Default = 20 Milliseconds
Query Cache Cleanup Interval	The cache containing the queries generated by several channels (Web, Mail, Api, removable storage, etc.) is cleared periodically to maintain the efficiency. The 'Query Cache Cleanup Interval' specifies the time interval at which the cache is cleared. Default = 900000 Milliseconds.
Query Cache Maximum Size	The upper limit of size (in Bytes) of queries to be cached, for speeding up future queries coming from inspecting channels. Default = 2000000 Bytes
Error Action	The action executed on data intercepted or discovered by MyDLP if any error occurs in MyDLP Server. Default = Pass. You can choose between 'Pass' and 'Block' as required from the drop-down. 
Refresh Time Interval for Log Tab	The interval at which the log of events is updated and displayed under the 'Logs' tab of the MyDLP console. Refer to the section **The Logs Tab** for more details.

6.5. Configuring Enterprise Settings

The 'Enterprise' tab of the 'Settings' interface allows administrators to configure archive settings depending on corporate policies, customize email notifications and messages displayed to end-users when MyDLP blocks their requests while sending mails or uploading documents to web pages and log storage settings.

To open the Endpoint tab, click 'Settings' > 'Enterprise'.



Archive Configurations

MyDLP can archive all the web traffic and the mail traffic to and from the network irrespective of their content. These archives can be later used by the administrators for audits on data uploaded to or downloaded from the webpages visited by end-users and emails sent and received by the end-users for investigation purposes. All the archived web pages and the mails are logged, enabling the administrator to download the archived files from the Logs interface. Refer to the section **The Logs tab** for more details.

Note: Archiving the web and/or mail traffic by MyDLP requires substantial disk space in the MyDLP server. Ensure you have sufficient space in the server before enabling these features.

- **Mail Archive** - Enables the Mail Archive feature. MyDLP stores all the mail traffic to and from the server irrespective of their content
- **Web Archive** - Enables the Web Archive feature. MyDLP stores all the web traffic to and from the server irrespective of their content
- **ICAP Archive Minimum Size** - Specify the minimum size (in MB) of web traffic data to be archived. Only those Web transactions of size equal to or larger than the size specified here will be archived.

Notification Configurations

MyDLP sends notification mails to the administrators configured as intended recipients, whenever it blocks or quarantines data transfer as per the following types of rules:

- Web
- Mail
- Removable Storage

- Printer
- API
- Endpoint Discovery
- Remote Discovery

MyDLP displays a message to the end-user when it blocks or quarantines the data traffic from the user computer based on the following types of the rules:

- Web Rule
- Mail Rule

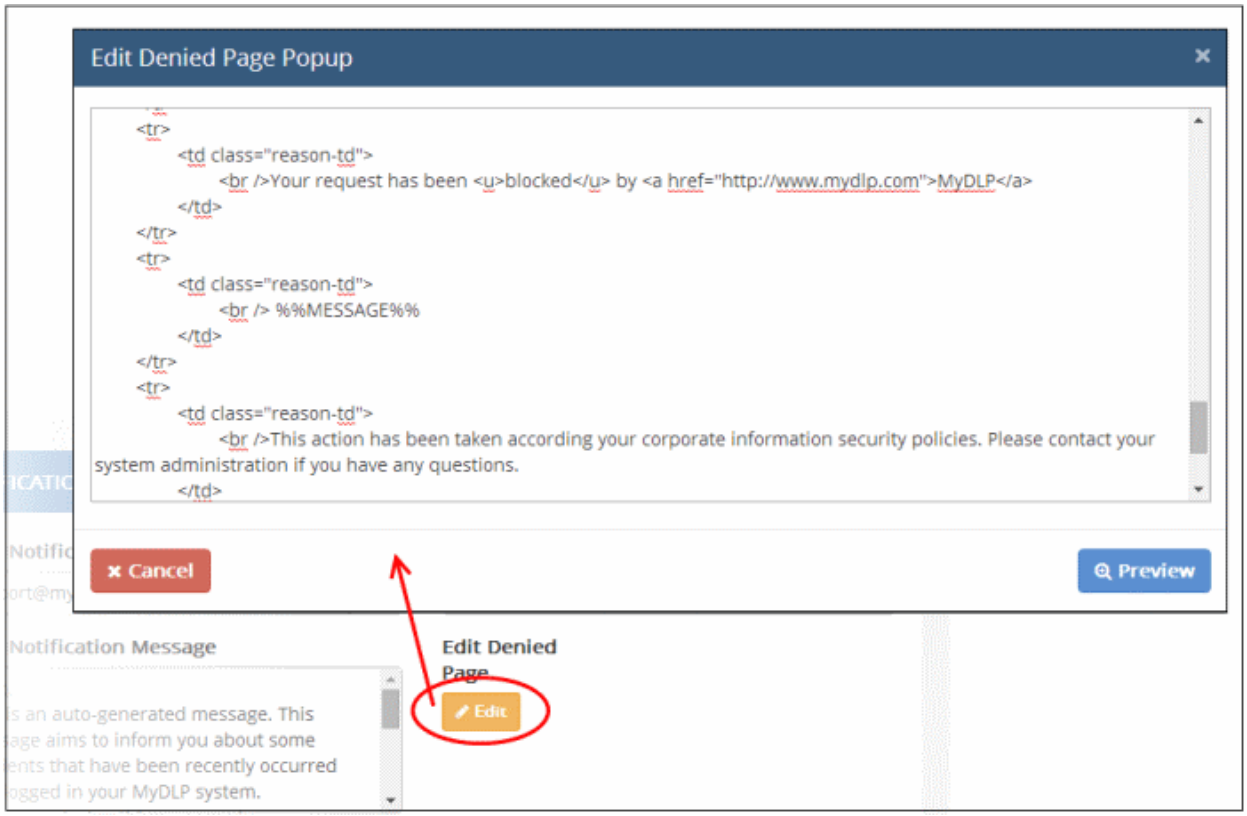
The 'Enterprise' tab in the 'Settings' interface allows the administrator to customize the content in the email notification and the message pop-up displayed to the end-user.

Edit Denied Page - Allows the administrator to edit the content in the message pop-up window that is displayed to end-user, when MyDLP blocks or quarantines the data traffic. An Example is shown below:

The customized messages for the web rules and the mail rules are displayed to the end-user as specified during creation of the respective rules in the pop-up window with a common template. The administrator can edit the common template as per the requirements of the organization, through the 'Edit Denied Page' option.

To edit the common template

- Click the 'Edit' Button beside the 'Edit Denied Page'.



The HTML page of the pop-up will open in a HTML Editor window. Within the content %%MESSAGE%% is defined as the variable to be replaced by the message specified by the administrator during creation of the rule. Refer to the description under **Step 2 - Enter Name for the rule and configure Messages and Notifications** in the section **Adding a Data Transfer Rule** for more details on message entered by the administrator while adding the rule.

- Edit the format and content of the template directly in the editor.
- To preview the edited page, click 'Preview'.
- To save the changes, click 'Save'.

Email Notification From Address - The email address from which the automated notification mails are to be sent by MyDLP. The administrator can edit the address as required.

Email Notification Subject - The subject line of the notification mails. The administrator can customize the subject line as required.

Email Notification Message - The message content in the notification mail. The administrator can directly edit the content as per the corporate requirements.

Syslog Configurations

Comodo MyDLP has the ability to forward logs to a remote Syslog server Common Event Format (CEF) and User Datagram Protocol (UDP). The administrator can integrate MyDLP with a remote Syslog server used by the organization and configure MyDLP to redirect the logs to it, for easy analysis of the logs and conserving disk space in the MyDLP server.

Background Note: MyDLP can transfer the logs in both UDP an CEF formats. Though UDP is faster, it is not secure. In order to protect the log data from the sniffing and spoofing attacks, it is recommended to use CEF format. For more details on CEF, refer to the CEF white paper available from **http://mita-tac.wikispaces.com/file/view/CEF+White+Paper+071709.pdf**

Three types of logs can be diverted to the Syslog server:

- **ACL Logs** - The logs of the MyDLP incidents, pertaining data transfer policy and discovery rules
- **Diagnostics** - The logs pertaining to operation errors and system health of the MyDLP server
- **System Reports** - The audit logs which have detail about every action taken on MyDLP server

For each type of the log the administrator can specify the following details of the external Syslog server in the respective fields:

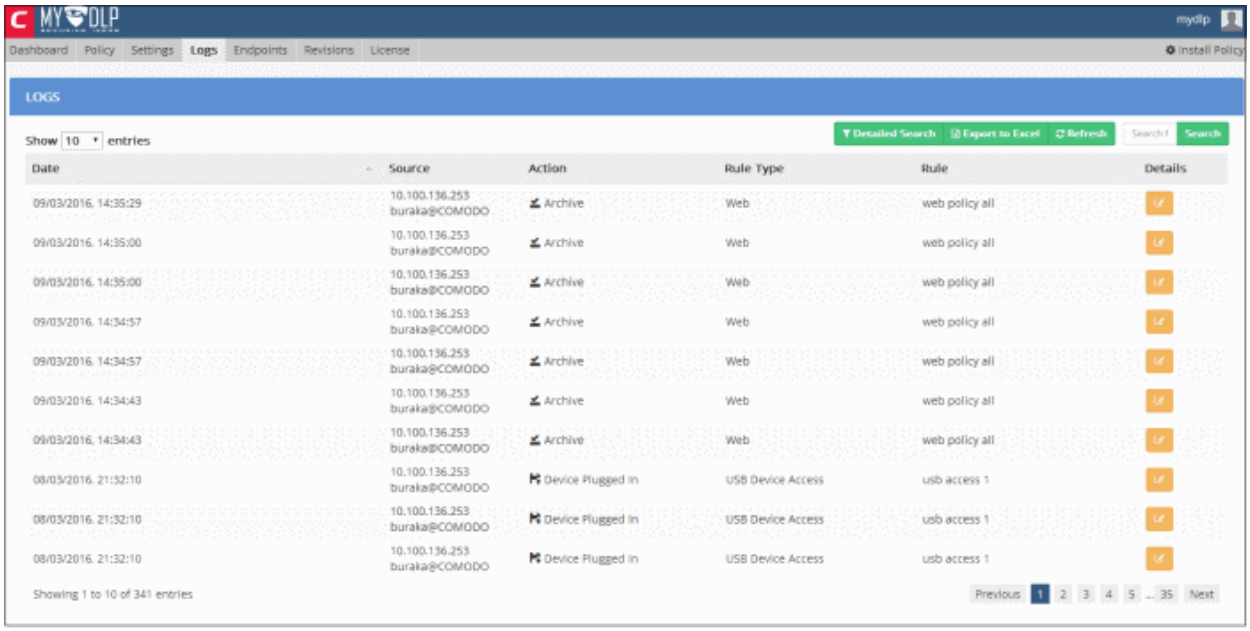
- **Syslog Host** - The administrator can specify the IP address or hostname of the external Syslog server
- **Syslog Port** - The administrator can specify the UDP listening port through which the server receives the logs. Default is 514.
- **Syslog Facility** - The administrator can choose the type of program that is sending the logs from the drop-down. The default for MyDLP is 'local6'

Click 'Save' at the bottom of the 'Enterprise' setting screen for your changes to take effect.

7.The Logs tab

The 'Logs' interface lists all events where a MyDLP rule was triggered. It displays the rule name and type, the date the event occurred, the affected endpoint and the action that took place.

Depending on the rule type, administrators can download the files that triggered the rule, resend legitimate mails that were intercepted, and other actions. The logs interface is automatically updated at the interval set under **'Settings' > 'Advanced'** interface.



Logs Table - Description of Columns	
Column Header	**Description**
Date	Date and time of the incident.
Source	The IP address of the source end-point and the user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted or discovered as per the rule. Refer to the section

	Rule Actions for a list of actions.
Rule Type	Indicates the type of the rule based on which files are intercepted or discovered. Refer to the section **Rule Channels / Types** for a list of rule types.
Rule	The name of the rule that created the event.
Details	Enables administrators to view complete details of the incident and download copies of the files intercepted or discovered. Refer to the section **Viewing Details of a Log Entry** for more details.

Filtering and Search Options

Logs can be filtered to show incidents that occurred within a specific period of time, and by source, action and rule type.

- Click 'Detailed Search' at the top

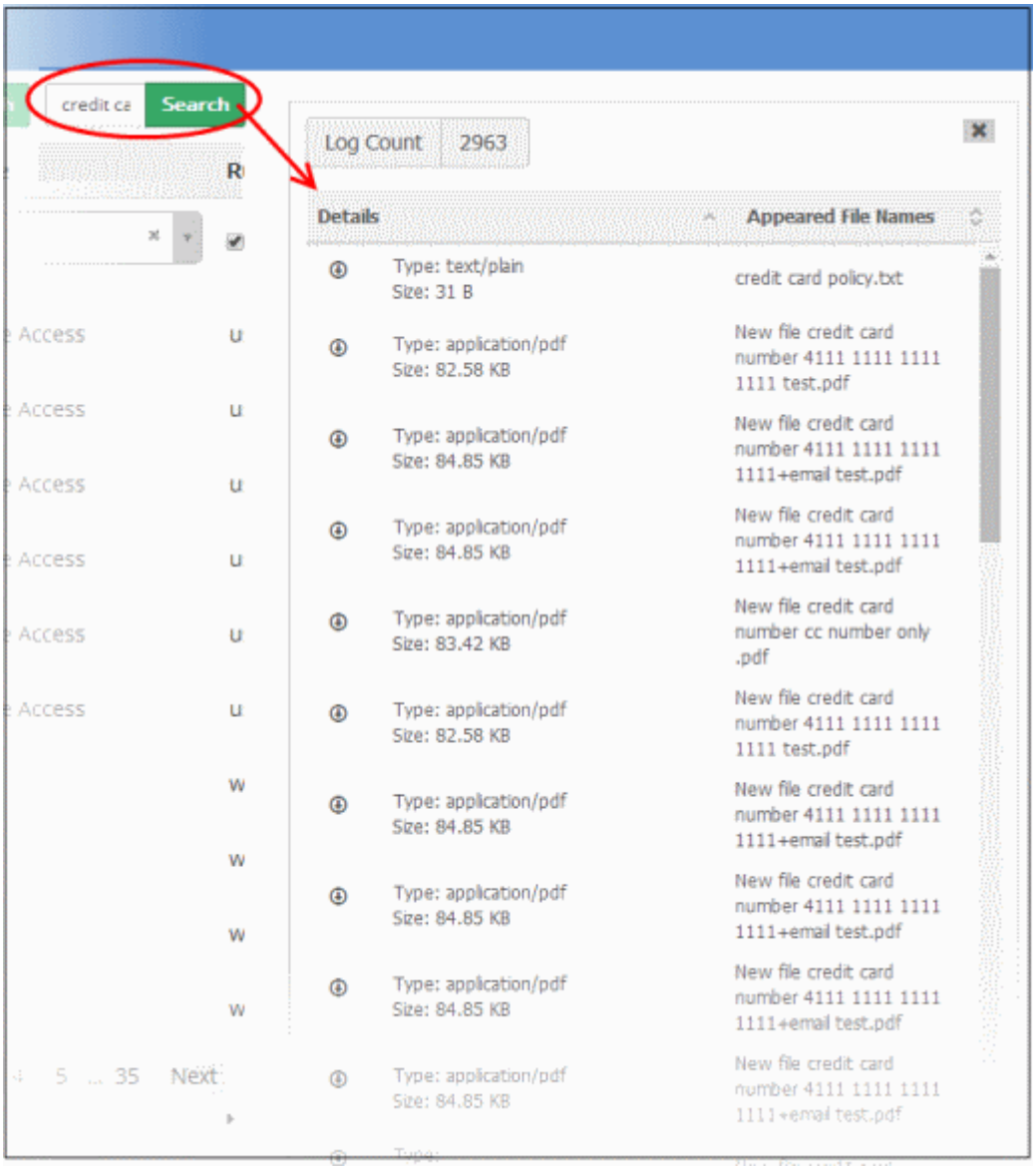
You can search for logs based on 'From' and 'To' dates, 'Source', 'Action', and 'Rule Type'. You can also combine these search parameters to narrow down your search.

- From and To dates - Only the logs of incidents occurred within the specified time period will be displayed. Enter the dates or select from the calendar to specify the period.
- Source - Displays logs from the specified source. You can enter IP addresses, user email addresses and discovery locations.
- Action – Filter incidents based on a specific action executed on the intercepted/discovered files. Choose the action from the 'Action' drop-down.
- Rule Type – Filter incidents based by rule type. Choose the type from the 'Rule Type' drop-down.
- Click the 'Refresh' button to apply your filters.

To search the logs of archived files containing specified keywords

- Enter a keyword in the search box on the upper-right and click 'Search'.

Files containing the keyword will be listed in a separate panel on the right:



Administrators can download any file by clicking the download icon.

The following sections provide detailed explanations about:

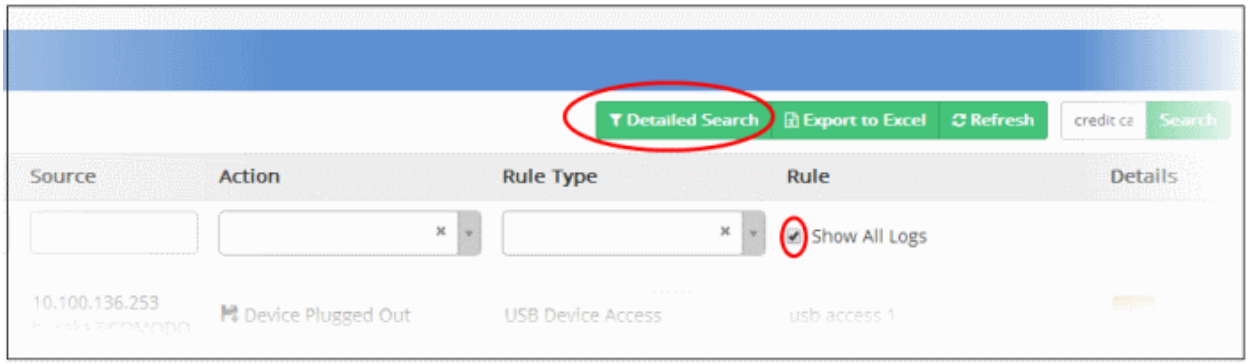
- **Viewing Hidden Archive Logs**
- **Viewing Details of a Log Entry**
- **Downloading the files archived by MyDLP**
- **Resending mails intercepted by mail rules**
- **Exporting the Logs to a Spreadsheet file**

7.1. Viewing Hidden Archive Logs

By default, logs pertaining to the Removable Storage Archive Inbound rule, Web rules with Archive action and Email rules with Archive action are not displayed in the logs interface.

To view the hidden logs

- Click 'Detailed Search' to expand the search panel.
- Enable the 'Show All Logs' check-box.



7.2. Viewing Details of a Log Entry

The incident log details pane enable administrators to view granular details of any logged incident, including the source endpoint, user, destination, files intercepted/discovered, information type, serial number and so on.

- To open the incident details pane for a particular log, click the details icon at the end of any row

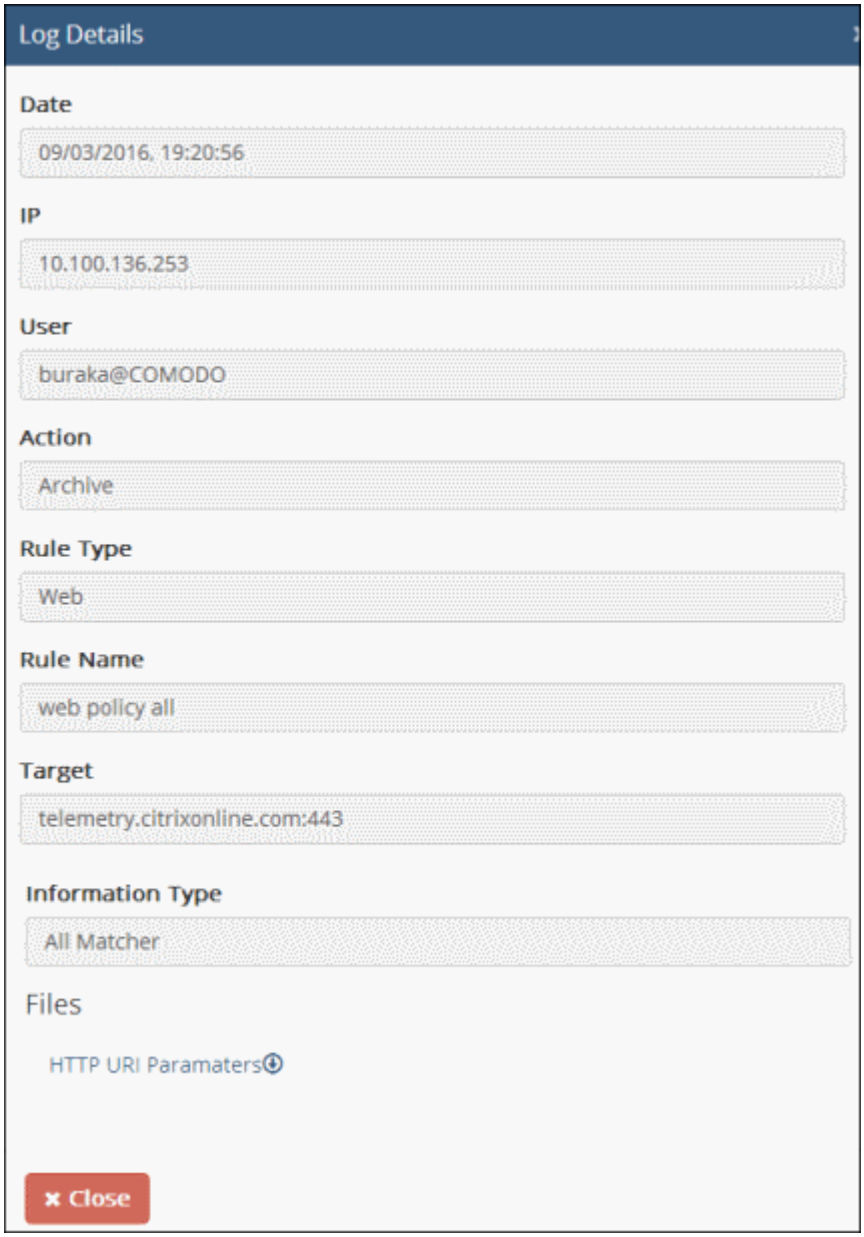
The pane also allows the administrator to download a copy of the quarantined/archived file that was identified as containing the sensitive information based on the data transfer policy rule or the discovery rule.

The pane differs slightly depending on the rule channel.

The following sections explain the Incident Log Details of different Rule Channels:

- **Web Rule**
- **Mail Rule**
- **Removable Storage Rule**
- **Removable Storage Inbound Rule**
- **Printer Rule**
- **API Rule**
- **USB Device Access Rule**
- **CD-DVD Rule**
- **Floppy Rule**
- **Clipboard Rule**
- **Screenshot Rule**
- **Endpoint Discovery Rule**
- **Remote Storage Discovery Rule**

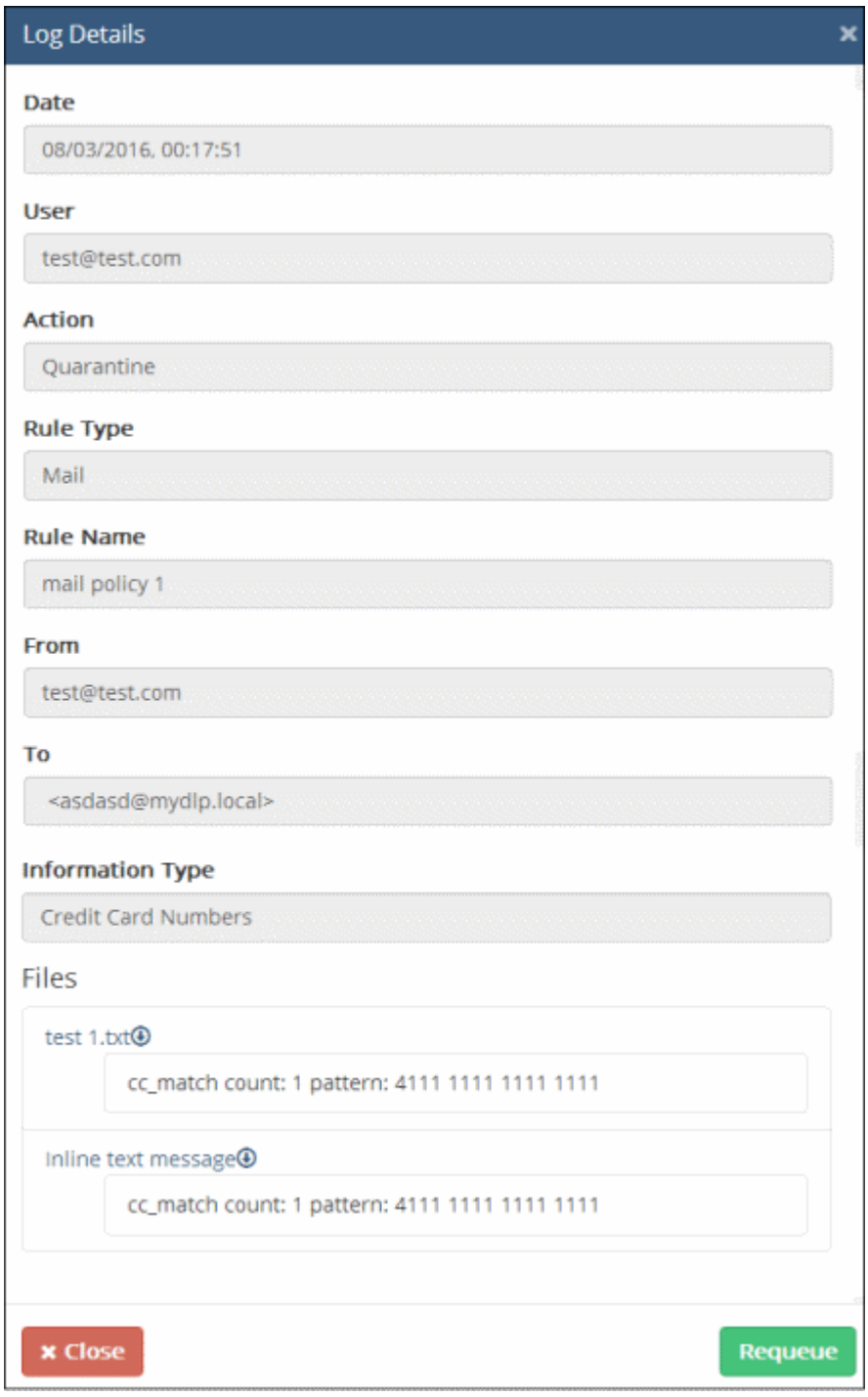
Web rule



Incident Log Details - Web Rule	
Field	**Description**
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the file(s) is/are uploaded.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted. Refer to the section **Rule Actions** for a list of actions.
Rule Type	Indicates the type of the rule based on which the files are intercepted.

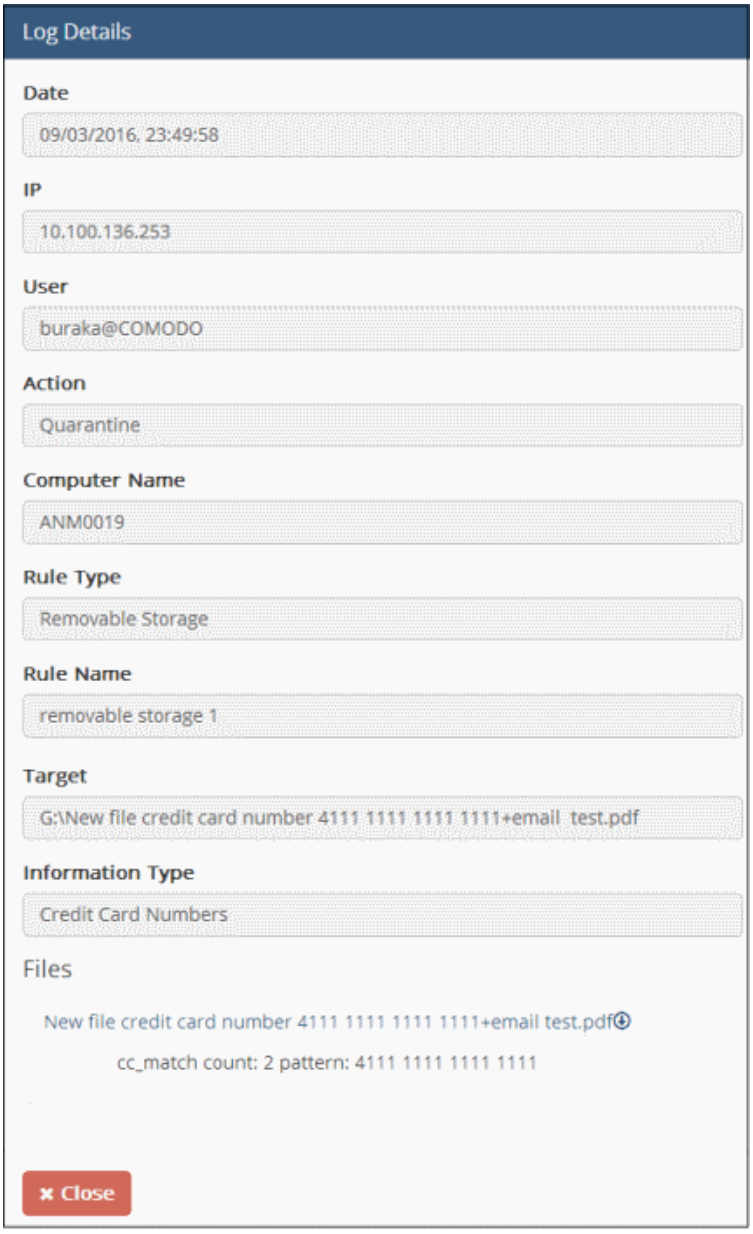
Rule Name	The name of the rule based on which the files are intercepted.
Target	The destination webpage to which the file(s) is/are uploaded.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the web rule. You can download the files by clicking on its name. Refer to the section **Downloading the Files Archived by MyDLP** for more details.

Mail rule



Incident Log Details - Mail Rule	
Field	**Description**
Date	Precise date and time of the incident.
User	The user logged-in at the end-point during time of incident.
Action	The action executed on the file(s) intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
From	The email account from which the mail was sent
To	The email address to which the email was sent
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the mail rule. You can download the files by clicking on its name. Refer to the section **Downloading the Files Archived by MyDLP** for more details.
Requeue	Allows the administrator to resend the mail if found legitimate. Refer to the section '**Resending Mails Intercepted by Mail Rules**' for more details.

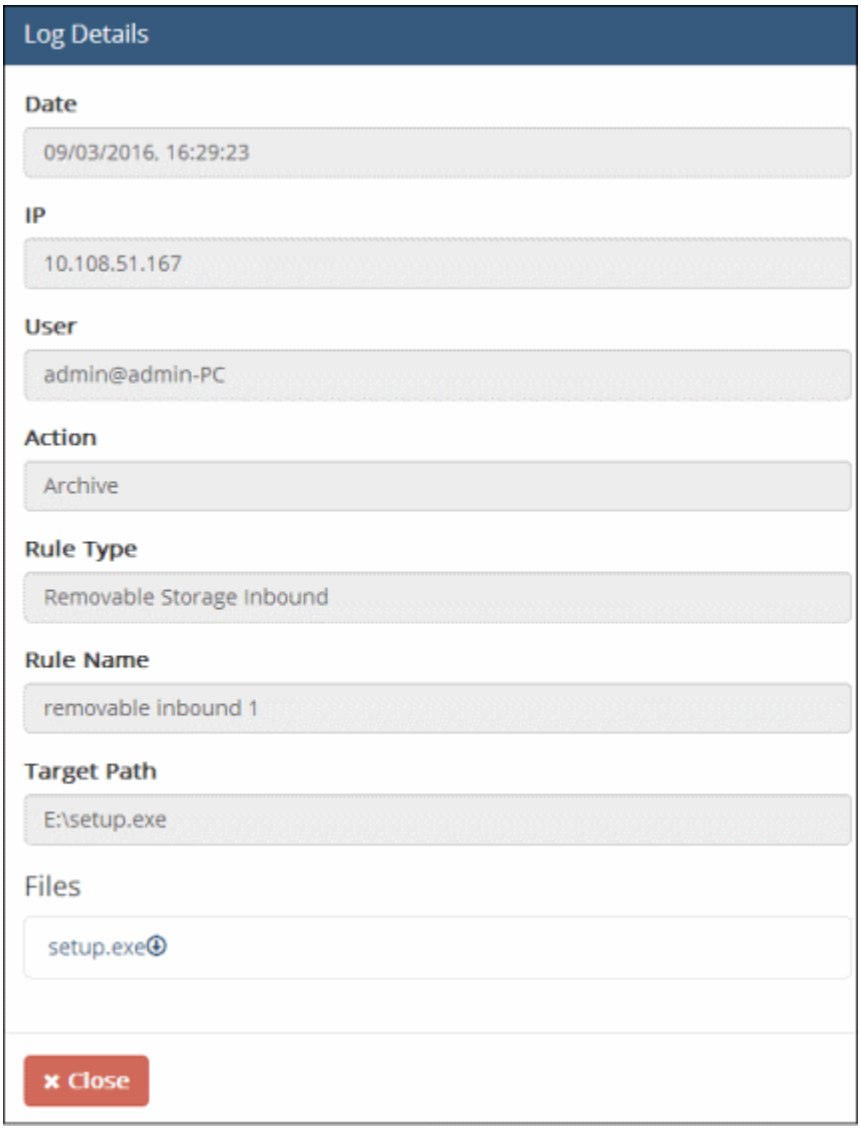
Removable Storage rule



Incident Log Details - Removable Storage Rule	
Field	**Description**
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the file(s) is copied/moved to removable storage.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted.
Computer Name	Indicates the host name of the endpoint from which the files are intercepted.

Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
Target	The location in the local drive of the endpoint computer or the network storage from which the file was copied/moved.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the Removable Storage rule. You can download the files by clicking on its name. Refer to the section **Downloading the Files Archived by MyDLP** for more details.

Removable Storage Inbound rule

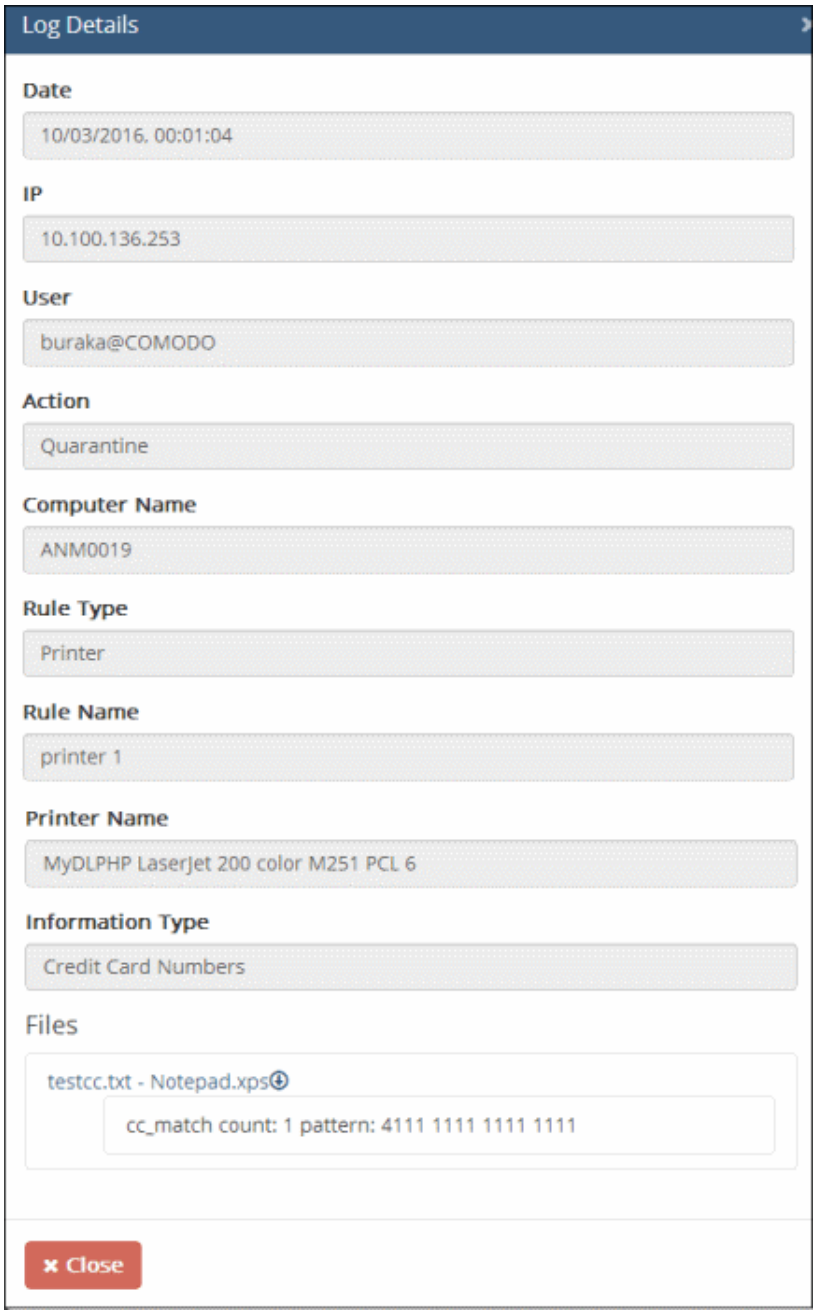


Incident Log Details - Removable Storage Inbound Rule	
Field	**Description**
Date	Precise date and time of the incident.

IP	The IP address of the source end-point at which the file(s) is read/copied from a removable storage.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
Target Path	The location in the removable storage from which the file was read/copied.
Files	Displays a list of files that were identified as per the Removable Storage Inbound rule. You can download the files by clicking on its name. Refer to the section **Downloading the Files Archived by MyDLP** for more details.

The Removable Storage Inbound Rule also blocks reading or copying files which exceed the 'Maximum Object Size' specified in the **Settings > Advanced** interface and logs the incident. For those incidents, the Rule name will be displayed as 'Default rule'.

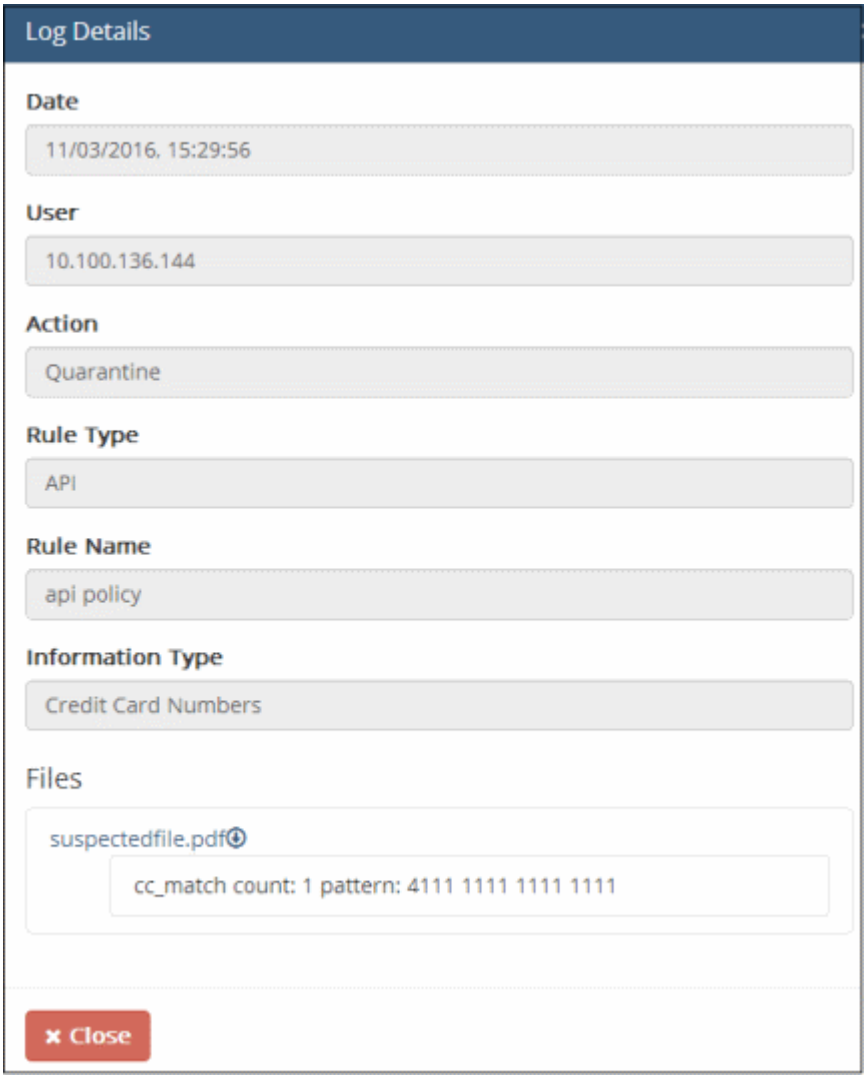
Printer rule



Incident Log Details - Printer Rule	
Field	**Description**
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the file(s) is transferred for printing.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted.
Computer Name	Indicates the host name of the endpoint from which the files are intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.

Rule Name	The name of the rule based on which the files are intercepted.
Printer Name	The printer chosen for printing the file.
Information Type	The information type specified in the printer rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the Printer rule. You can download the files by clicking on its name. Refer to the section **Downloading the Files Archived by MyDLP** for more details.

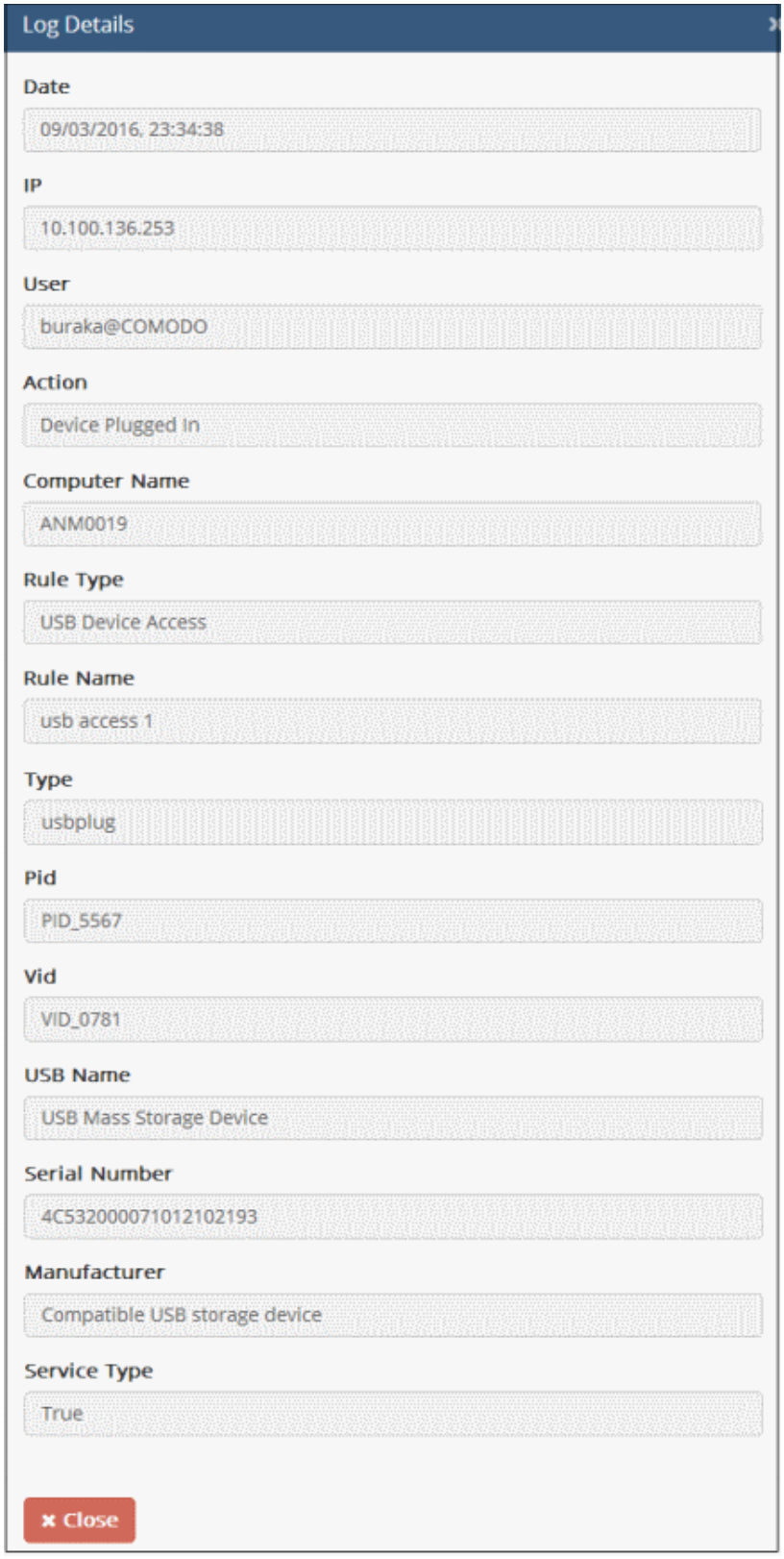
API rule



Incident Log Details - API Rule	
Field	**Description**
Date	Precise date and time of the incident.
User	The IP address of the source end-point from which the file(s) is transferred through an API
Action	The action executed on the file(s) intercepted.

Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
Information Type	The information type specified in the API rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the API rule. You can download the files by clicking on its name. Refer to the section **Downloading the Files Archived by MyDLP** for more details.

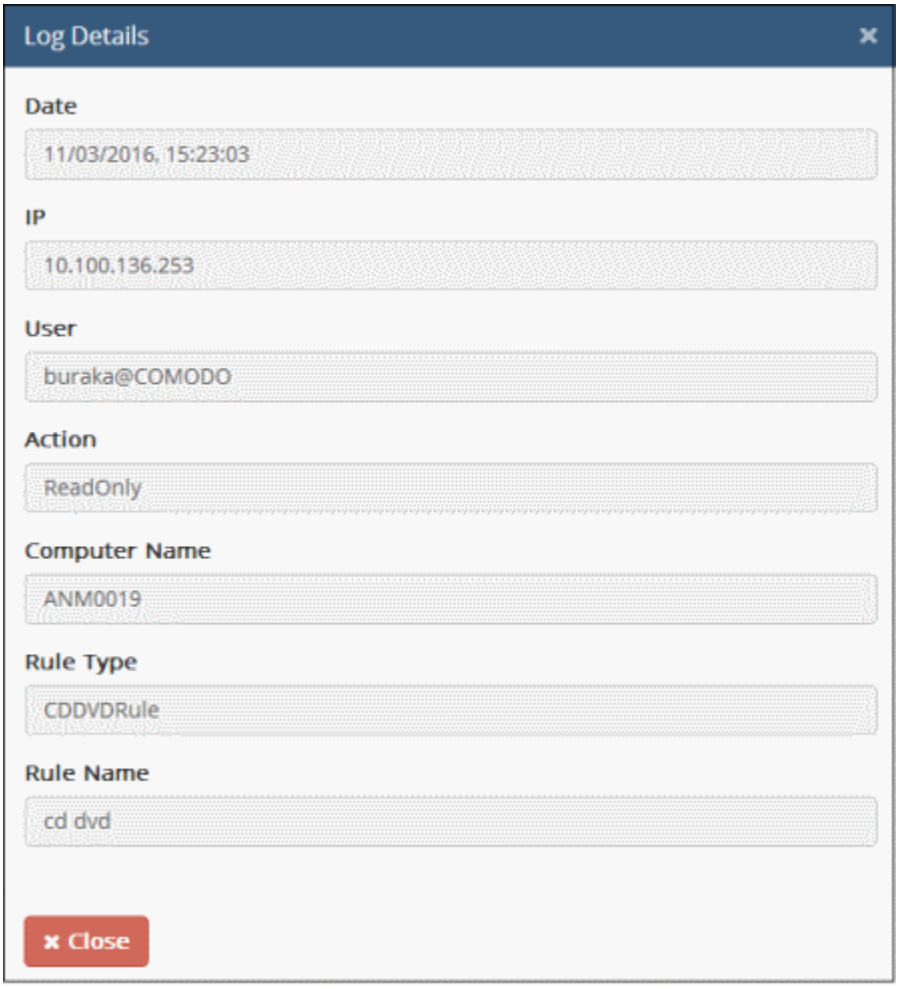
USB Device Access Rule



Incident Log Details - USB Device Access Rule	
Field	**Description**
Date	Precise date and time of the incident.
IP	The IP address of the endpoint at which the incident occurred.

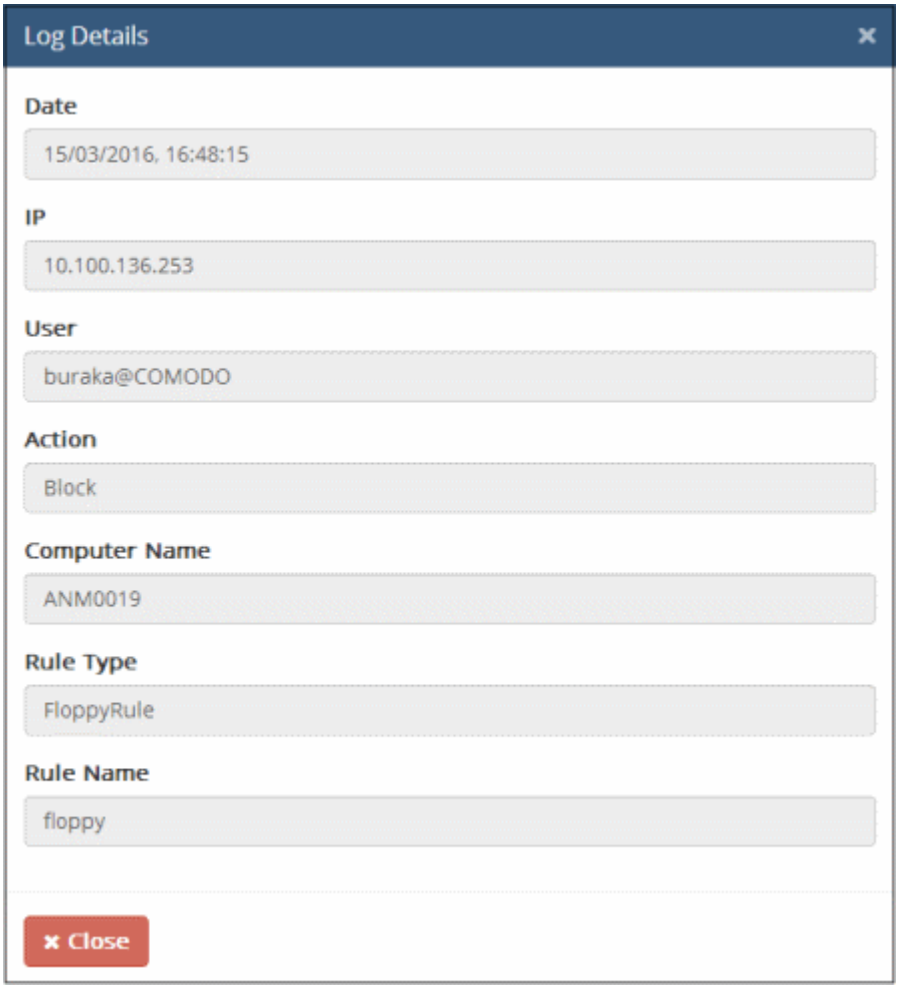
User	The user logged-in at the time of incident.
Action	The action executed on the incident.
Computer Name	Indicates the host name of the endpoint at which the incident occurred
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the incident was identified.
Type	Indicates the activity of the USB device at the endpoint, such as plug-in, plug-out or block.
PID	Indicates the Product ID (PID) of the USB device that was used with the endpoint
VID	Indicates the Vendor ID (VID) of the USB device that was used with the endpoint
USB Name	The device name of the USB device responsible for the incident
Serial Number	Indicates the device serial number of the USB device
Manufacturer	Indicates the manufacturer of the USB device

CD-DVD Rule



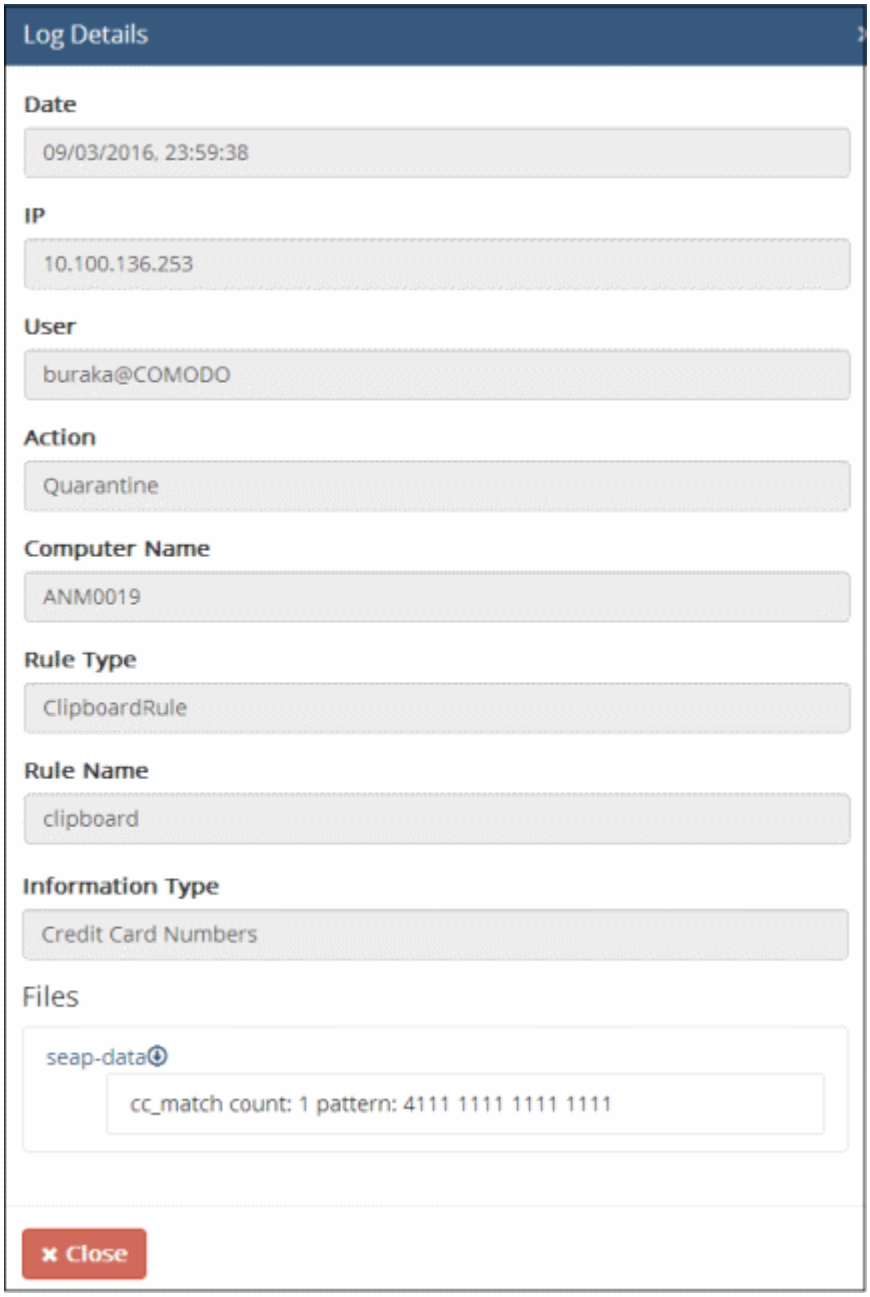
Incident Log Details - CD-DVD Rule	
Field	**Description**
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the file(s) is copied/moved to CD or DVD.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted.
Computer Name	Indicates the host name of the endpoint from which the files are intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.

Floppy Rule



Incident Log Details - Floppy Rule	
Field	**Description**
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the file(s) is copied/moved to CD or DVD.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted.
Computer Name	Indicates the host name of the endpoint from which the files are intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.

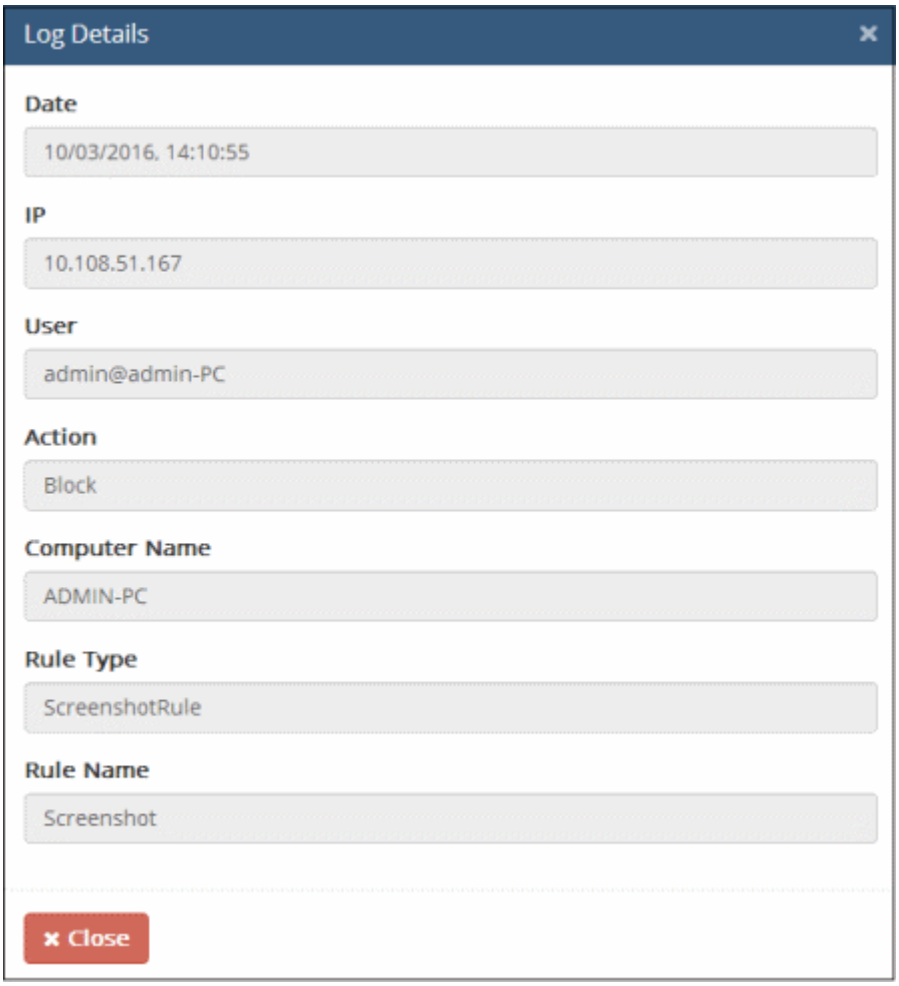
Clipboard Rule



Incident Log Details - Clipboard Rule	
Field	**Description**
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the file(s) is copied.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted.
Computer Name	Indicates the host name of the endpoint from which the files are intercepted.

Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
Information Type	The information type specified in the Clipboard rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the Clipboard rule. You can download the files by clicking on its name. Refer to the section **Downloading the Files Archived by MyDLP** for more details.

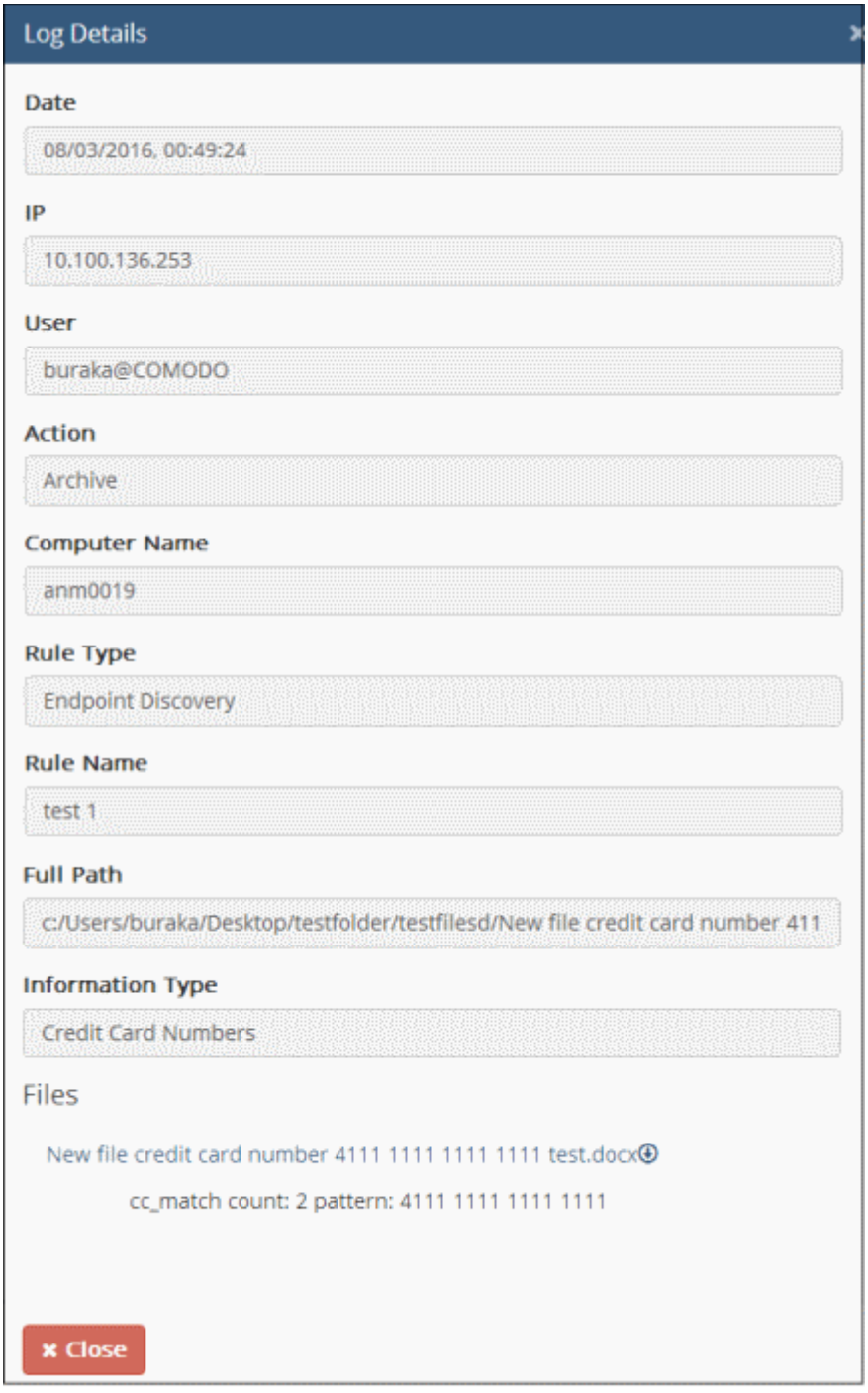
Screenshot Rule



Incident Log Details - Screenshot Rule	
Field	**Description**
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the screenshot was taken.
User	The user logged-in at the time of incident.

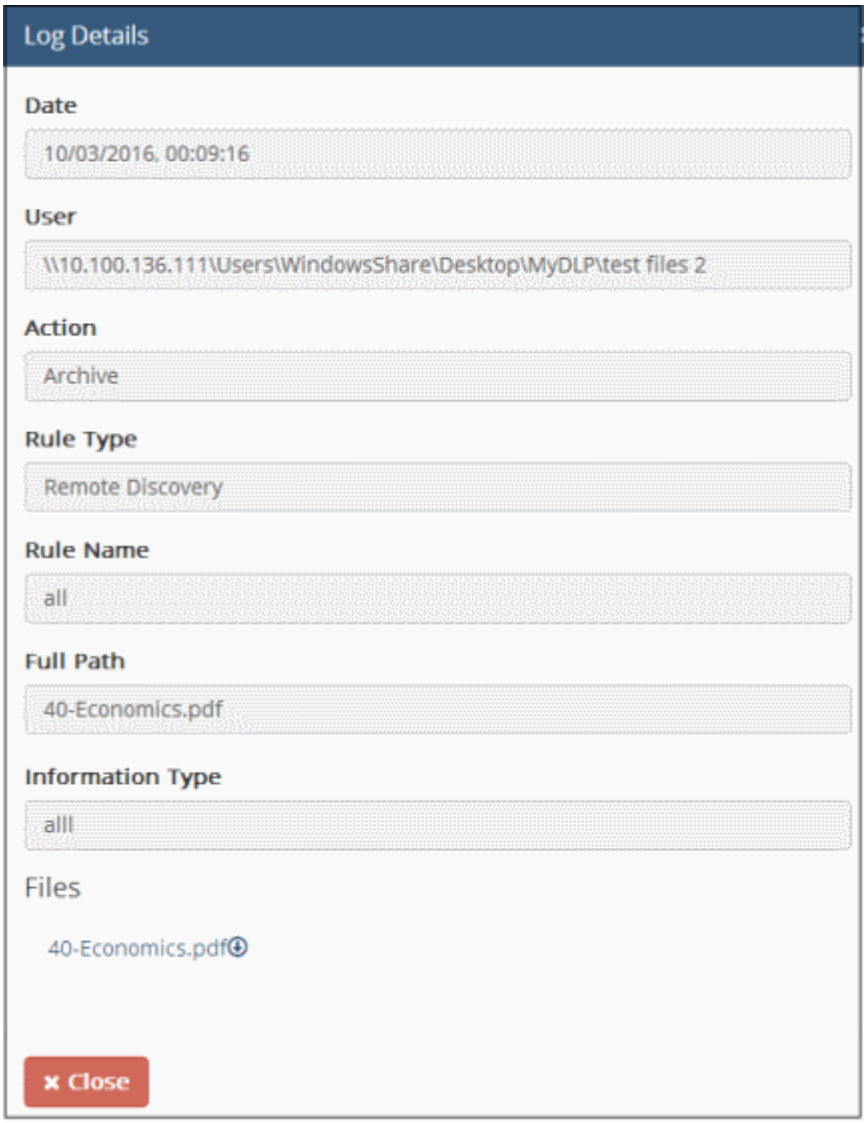
Action	The action executed on the file(s) intercepted.
Computer Name	Indicates the host name of the endpoint from which the files are intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.

Endpoint Discovery Rule



Incident Log Details - Endpoint Discovery Rule	
Field	**Description**
Date	Precise date and time at which the file(s) were discovered.
IP	The IP address of the source end-point at which the file(s) is discovered.
User	The user logged-in at the time of incident.
Action	The action executed on the discovered file(s).
Computer Name	Indicates the host name of the endpoint on which the files were discovered.
Rule Type	Indicates the type of the rule based on which the files were discovered.
Rule Name	The name of the rule based on which the files were discovered.
Full Path	The file paths of locations in the local drive of the end-point, from which the the files were discovered.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the Endpoint Discovery rule. You can download the files by clicking on its name. Refer to the section **Downloading the Files Archived by MyDLP** for more details.

Remote Storage Discovery Rule



Incident Log Details - Remote Storage Discovery Rule	
Field	**Description**
Date	Precise date and time at which the file(s) were discovered.
User	The network storage location like FTP Server, Microsoft Windows Share, Network File System (NFS) or Web server.
Action	The action executed on the discovered file(s).
Rule Type	Indicates the type of the rule based on which the files are discovered.
Rule Name	The name of the rule based on which the files were discovered.
Full Path	The file paths of locations in the remote storage from which the the files were discovered.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the Remote Discovery rule. You can download the files by clicking on its name.

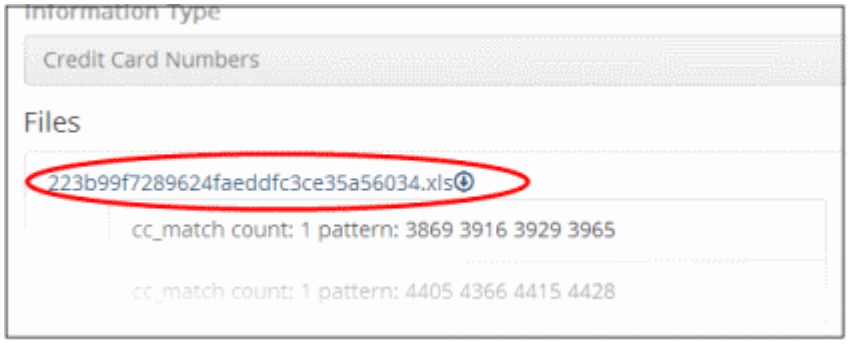
	Refer to the section **Downloading the Files Archived by MyDLP** for more details.

7.3. Downloading the Files Archived by MyDLP

The administrator can download a copy of archived or quarantined files, that were identified as containing sensitive information and intercepted/discovered based on data transfer policy rules or discovery rules, for investigation purposes, from the Logs interface.

To download an archived file

- Open the Logs interface by clicking the Logs tab
- Search for the log entry of the required incident using the search options. Refer to the explanation under '**Filtering and Search Options**' in the section '**The Logs tab**' for more details.
- Click the icon for the log entry under the Details column. The Log Details pane will open.
- Click on the file name, under 'Files'



The file will be saved to your default download location.

7.4. Resending Mails Intercepted by Mail Rules

MyDLP can pass, log, archive, block and quarantine emails which have confidential information according to the action specified in the mail rules. The emails that are passed, logged or archived will reach their recipients. Blocked emails are discarded and prevented from reaching the intended recipients. Quarantined emails are prevented from reaching their recipients and a copy of then are saved in the MyDLP archives. The administrator or auditor can examine these emails by downloading the archived copies of them from the 'Log Details' pane. If these emails are found legitimate, they can be forwarded to the indented recipients from the 'Log Details' pane.

To resend the archived emails

- Open the Logs interface by clicking the Logs tab
- Search for the log entry pertaining to the quarantined email using the search options. Refer to the explanation under '**Filtering and Search Options**' in the section '**The Logs tab**' for more details.
- Click the icon for the log entry under the Details column. The Log Details pane will open.
- Click on the file name, under 'Files'

- If the email is found legitimate, click 'Requeue' at the bottom.

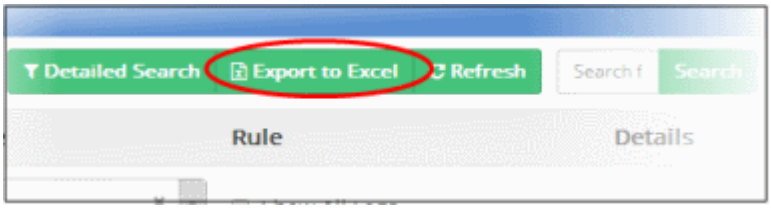
The mail will be added to the delivery queue and the status will change to 'Requeue in Progress'.

- Click 'Refresh' from the Logs interface. The mail will be sent.

7.5. Exporting the Logs to a Spreadsheet File

The administrator can save the logs as a spreadsheet file in 'Microsoft Excel' file format for later analysis by exporting the logs. The spreadsheet file will contain the first 1000 entries in the log. If needed, the administrator can apply filters and search options to export the log pertaining to a specific time period or to export logs pertaining to specified filtering criteria. Refer to the explanation under '**Filtering and Search Options**' in the section '**The Logs tab**' for more details.

To export the logs into an Excel file click 'Export to Excel' button at the top.



The file will be saved to your default download location.

8. The Endpoints Tab

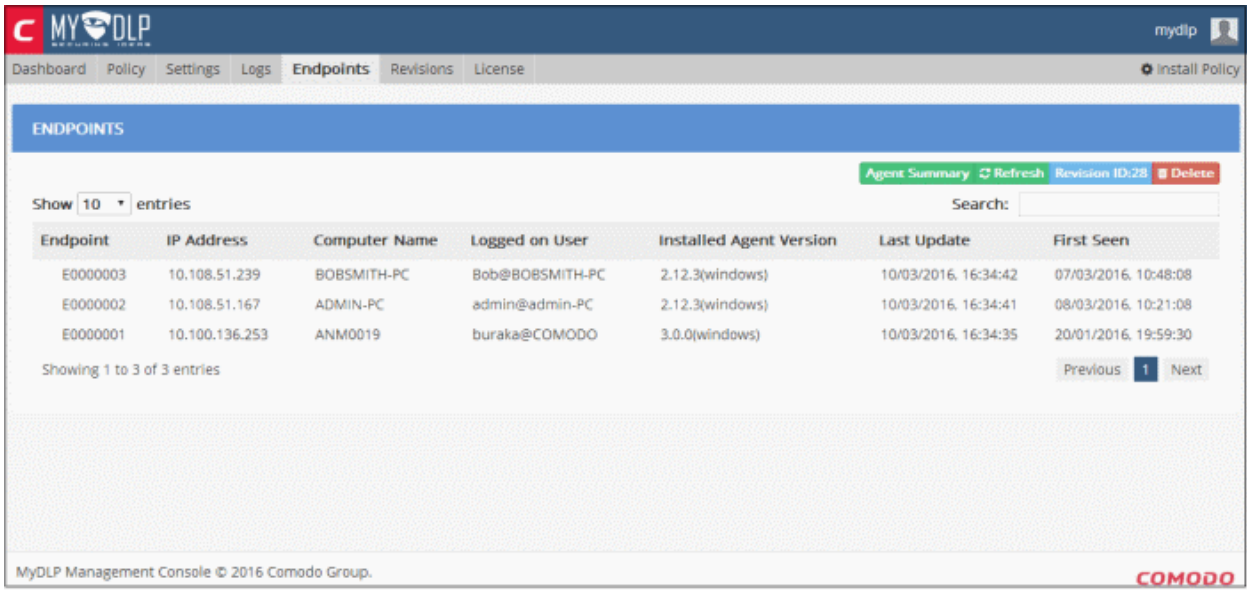
Comodo MyDLP monitors and controls data passing to and from endpoints and can also run discovery scans to identify confidential data in existing files. In order for MyDLP to monitor and scan endpoints, the MyDLP Agent needs to be installed on each endpoint.

The endpoint agent can be installed on the network computers in different ways. For more details on installing the endpoint agent, refer to the MyDLP Endpoint Agent Installation Guide available from **http://www.mydlp.com/wp-content/uploads/MyDLP-Endpoint-Installation-Guide.pdf**.

The Endpoints interface displays a list of endpoint computers on which the agent is installed and in communication with the server. Administrators can search for specific endpoint(s) by entering their hostname, IP address, ID, or version of agent installed. You can search by typing either a partial or full entry in the search box above the table.

- Click 'Refresh' to add any new endpoints and remove endpoints from which the agent has been uninstalled.
- Click 'Agent Summary' to the latest agent version number, the number of endpoints that are currently online and offline, the total number of endpoints on which the agent is installed, and the number of endpoints

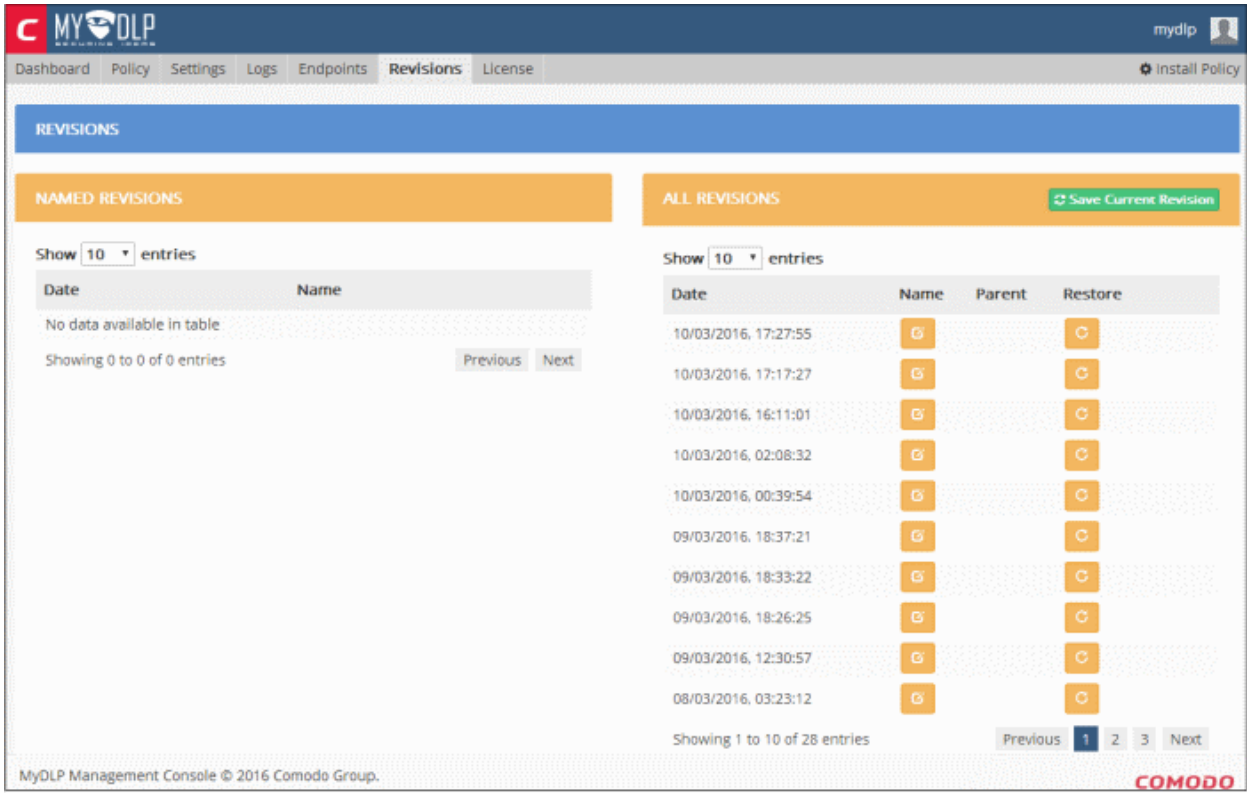
running outdated agents.



Endpoints Table - Column Descriptions	
Column	**Description**
Endpoint	The Unique Identification (ID) number assigned to the endpoint after the agent first contacted the server. The ID remains unchanged even if the host name and/or the IP address of the endpoint is changed. The unique ID number is used when specifying an endpoint while **creating a user defined Endpoint object**.
IP Address	The current IP address of the endpoint.
Computer Name	The host name of the endpoint.
Logged on user	The username of the currently logged-in user.
Installed Agent Version	The version number of the MyDLP Endpoint Agent installed on the endpoint.
Last Update	Indicates the date and time at which the agent was last updated.
First Seen	Indicates the date and time at which the agent first polled the MyDLP server.

9. The Revisions Tab

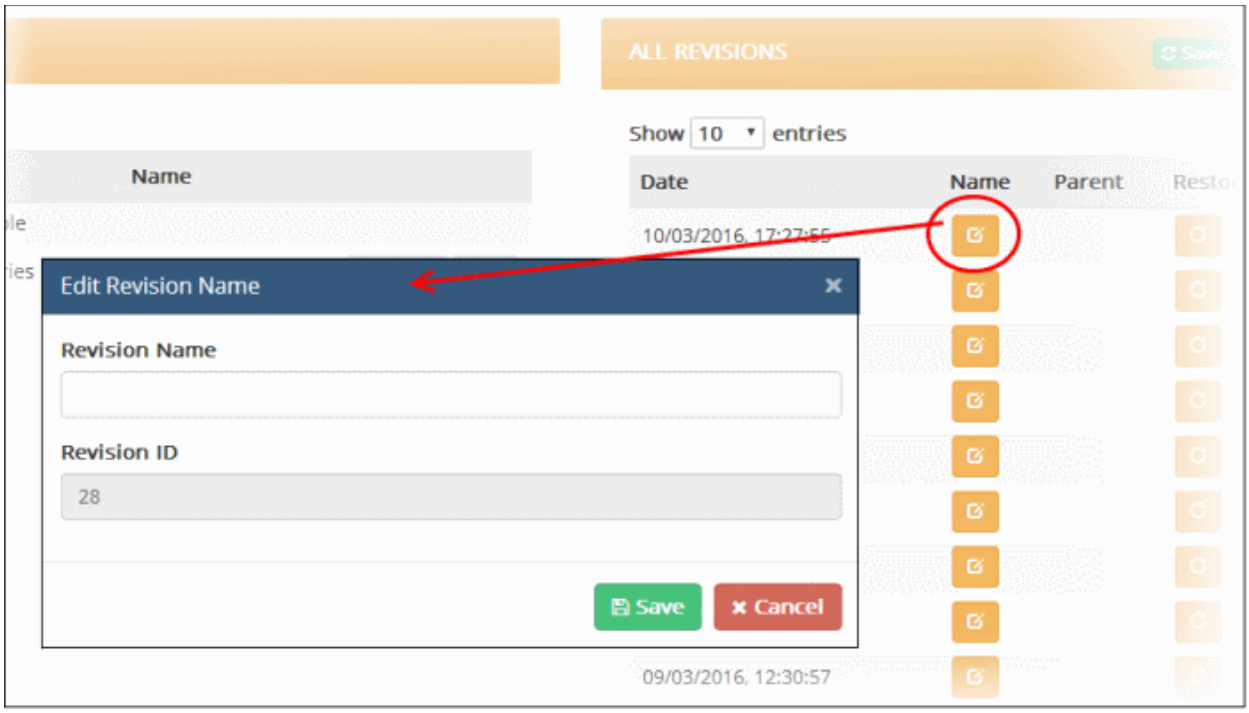
Comodo MyDLP saves the policies with the set of rules, every time a new policy is applied to the network. The 'Revisions' interface displays a list of MyDLP Policies that were applied whenever an administrator creates/edits rules in chronological order. The administrator can bookmark the policies by specifying a name shortly describing the change done. The administrator can also revert MyDLP to an earlier time point and apply the policy to the network with the set of rules that was in action at that time by restoring MyDLP to the selected Policy Revision.



The right hand side of the interface displays the list of all the policy revisions automatically created by MyDLP, every time the policy is updated with new/edited rules and installed on the network. The left hand side pane displays the list of policies that are bookmarked by the administrator.

To bookmark a policy

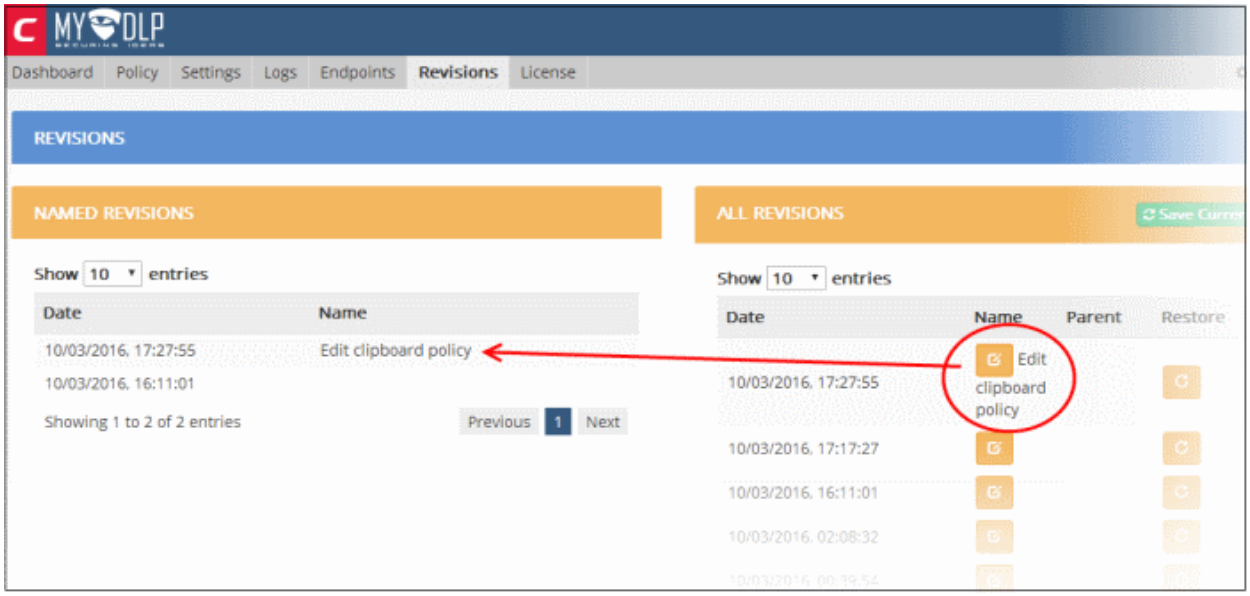
- Click the edit button  beside the policy revision that you want to save with a revision name.



The 'Edit Revision Name' dialog will appear.

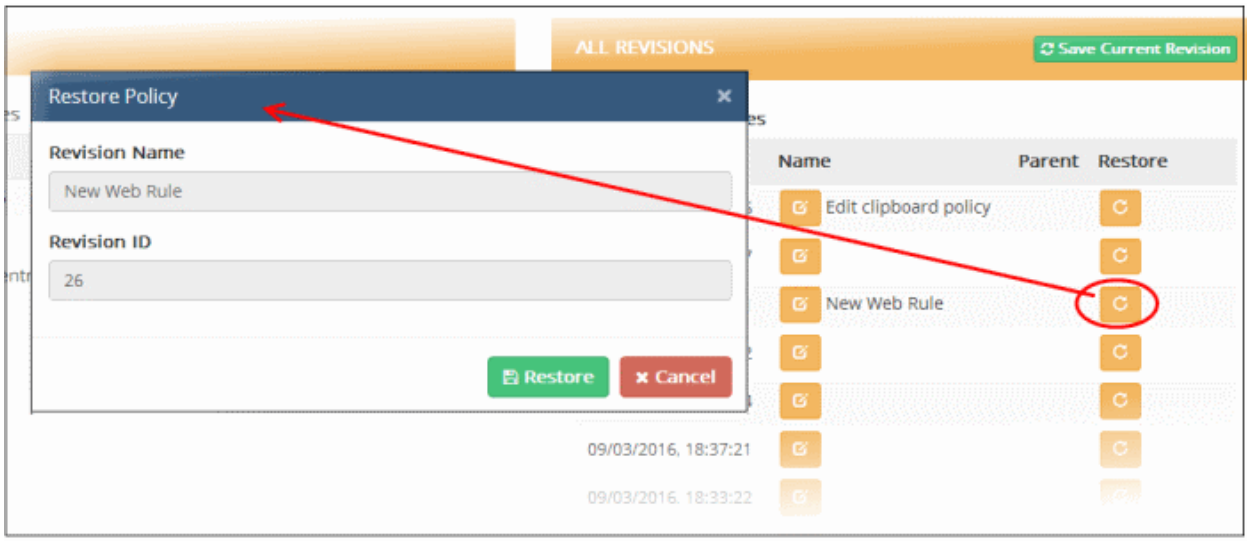
- Enter a name shortly describing the revision and click 'Save'.

The revision will be saved as a bookmark and added to the list on the left hand side.



To re-apply a policy from the revisions

- Click the icon  beside the policy revision that you want to restore. The 'Restore Policy' dialog will appear.

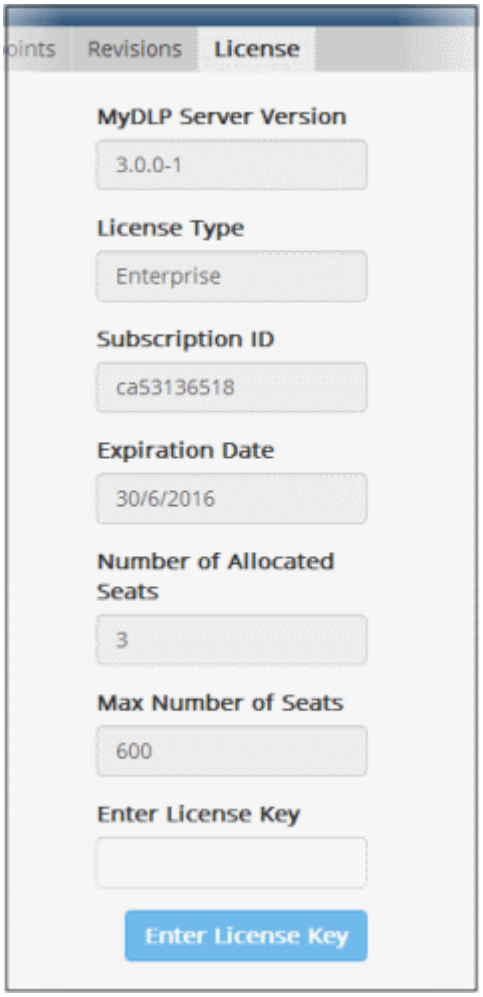


- Click 'Restore'
- Click 'Install Policy' at the top right side to apply the restored policy. Refer to the section '**Deploying a Policy**' for more details.

MyDLP will apply the policy to the network with the rules that were in action at that point of time.

10. The License Tab

The license tab allows you to view existing license information, including subscription ID and expiry date, and to activate new licenses.



Renew or Upgrade your License

You can purchase licenses for MyDLP by logging-in to **https://accounts.comodo.com/mydlp/management/signup**. After sign-up, you will receive your license key through email.

- Enter the license key in the 'Enter License Key' text box and click 'Submit License'

Once verified, your license will take effect immediately.

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **http://www.comodo.com**.