COMODO

Creating Trust Online®

Comodo
MyDLP

Software Version 2.0

Administration Guide

Guide Version 2.0.010215

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, 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. These two components work together to protect your sensitive information in your organization.

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 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
  - Changing your Password
  - Changing user information
- The Dashboard
- Data Transfer Control and Data Discovery
  - The Rules
  - The Objects
  - User Defined Objects
- Enforcing the Data Transfer Policy
  - Adding Policy Rules
  - Enabling or Disabling a Rule
  - Editing a Rule
  - Removing a Rule
- Configuring Data Discovery
  - Managing Discovery Rules
  - Viewing Discovery Scan Reports
- Deploying the Policy
- The Objects Tab
  - Managing Data Formats
  - Managing Keyword Groups
  - Managing Document Databases
  - Integrating Active Directory Domains

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**.

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:

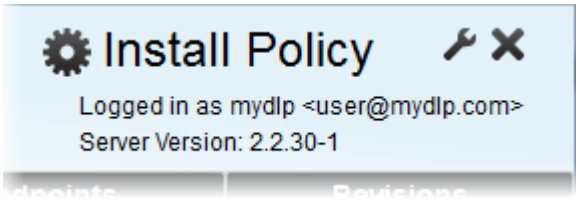
- You need to have a Flash enabled web browser to connect to the management console.
- The flash plug-in can be downloaded from: **http://get.adobe.com/flashplayer/**
- You can connect to the management console at the following URL: https://servername
  - "servername" = the hostname or IP address on 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

Click the  icon at the upper right of the Management Console to log out.

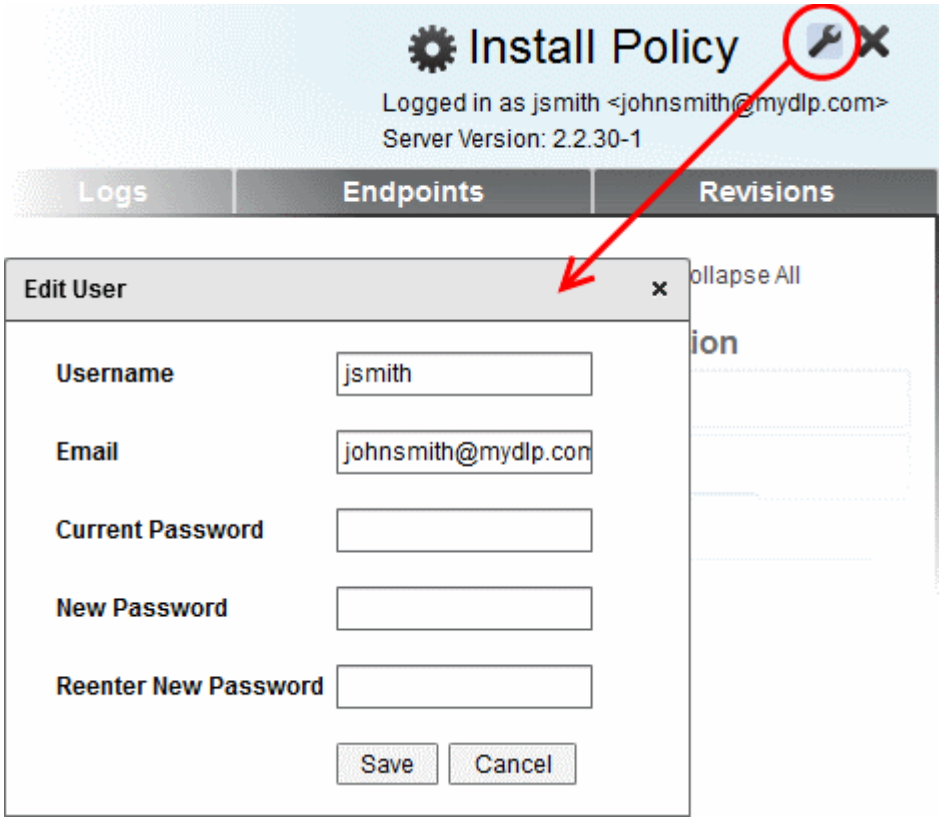
2.4. Checking Server Version

You can view the currently logged on user and server version at the top right of the Management Console. Providing the server version number will help accelerate issue resolution times should you need to contact support.



2.5. Changing your Password

1. Click on the wrench icon in the management console.
2. In the 'Edit User' dialog, enter your current password. Reminder - after initial setup, the default password is "mydlp" (without the quotes).



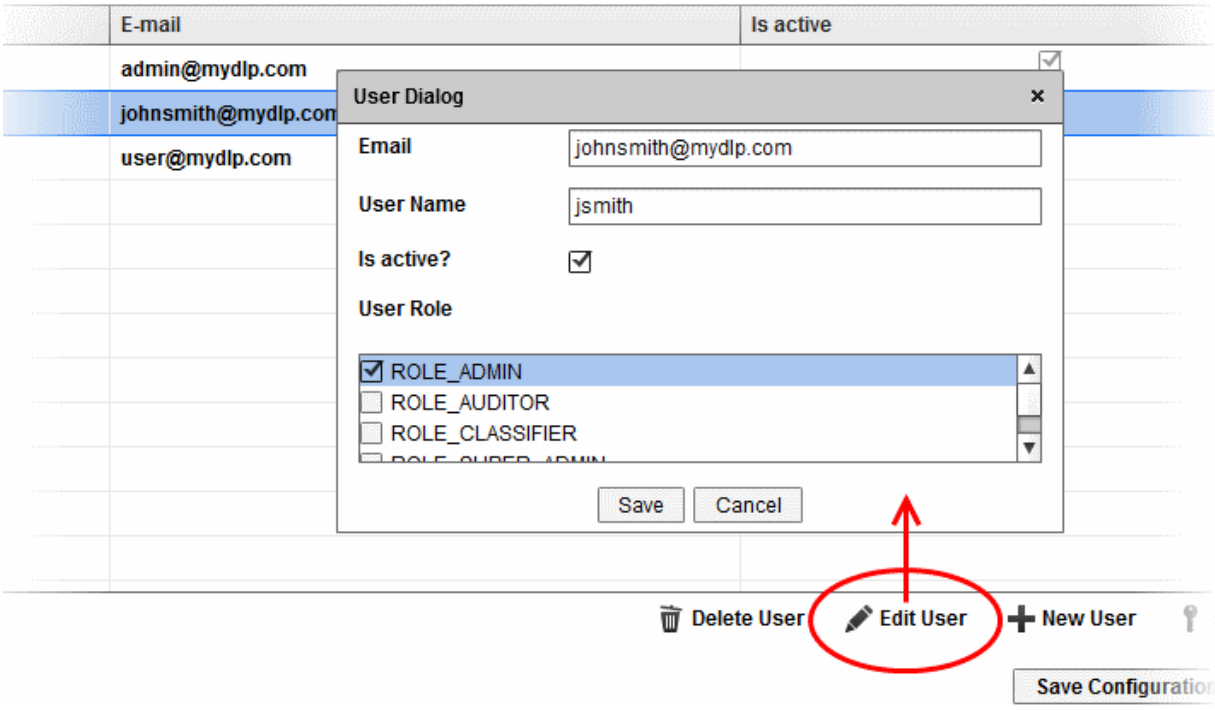
3. Enter and confirm your new password. Passwords must be at least 6 characters long and contain at least one uppercase and one lower case alphabets and one number.
4. Click 'Save' button.

2.6. Changing User Information

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

1. Click the 'Settings' tab.
2. Click 'Users'.
3. Select the user you wish to modify.

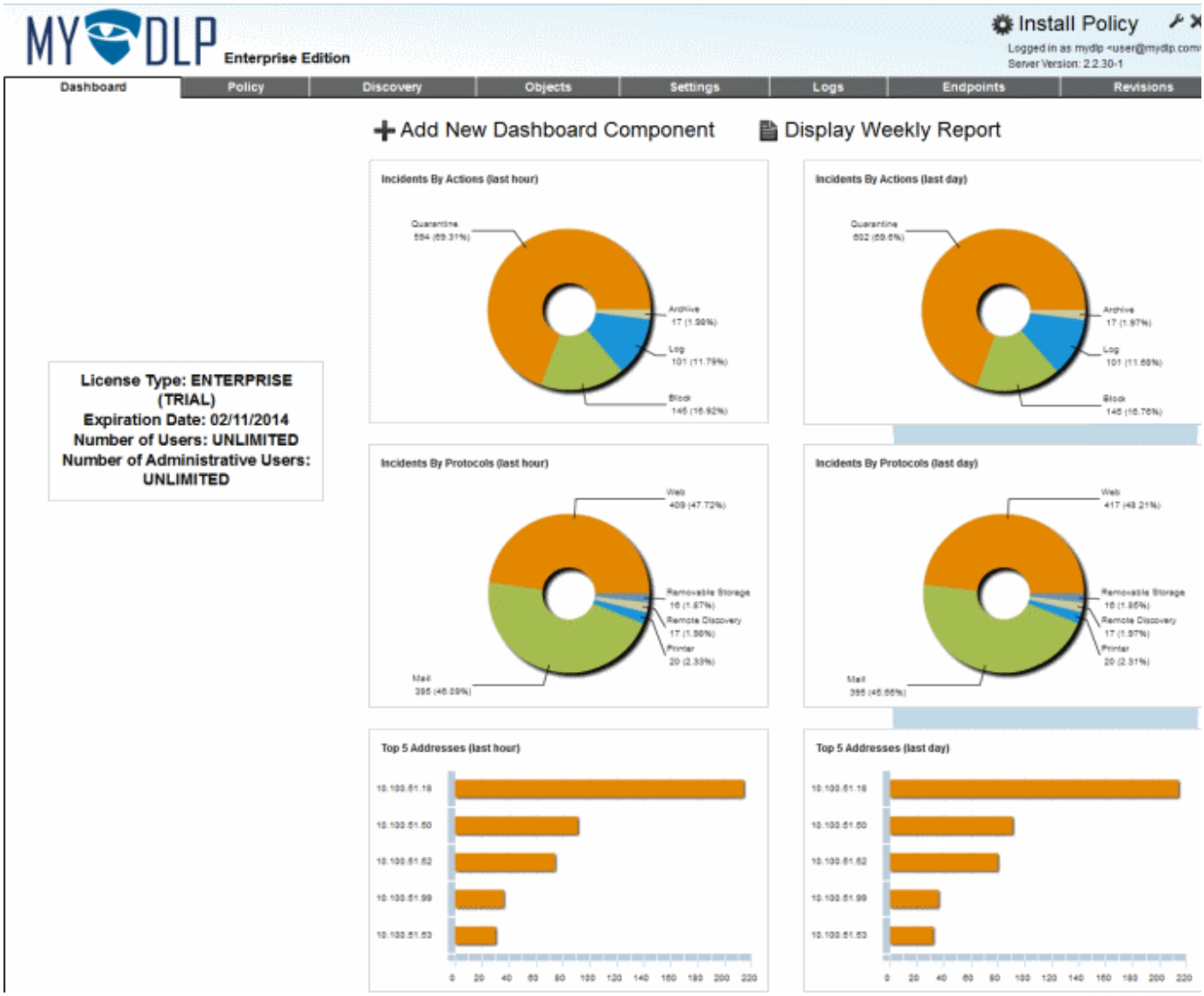
4. Click the 'Edit User' button.



5. Modify email and user name details as required.
6. 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 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)	The chart shows the incidents occurred within the last one hour / day and their proportion based on the rules, as a pie-diagram.
Incidents by Protocols (last day)	
Incidents by Actions (last hour)	The chart shows the incidents occurred within the last one hour / day and their proportion based on the actions executed on the intercepted data, as a pie-diagram.
Incidents by Actions (last day)	
Top 5 Addresses (last hour)	The bar graph shows the endpoints (represented by their IP

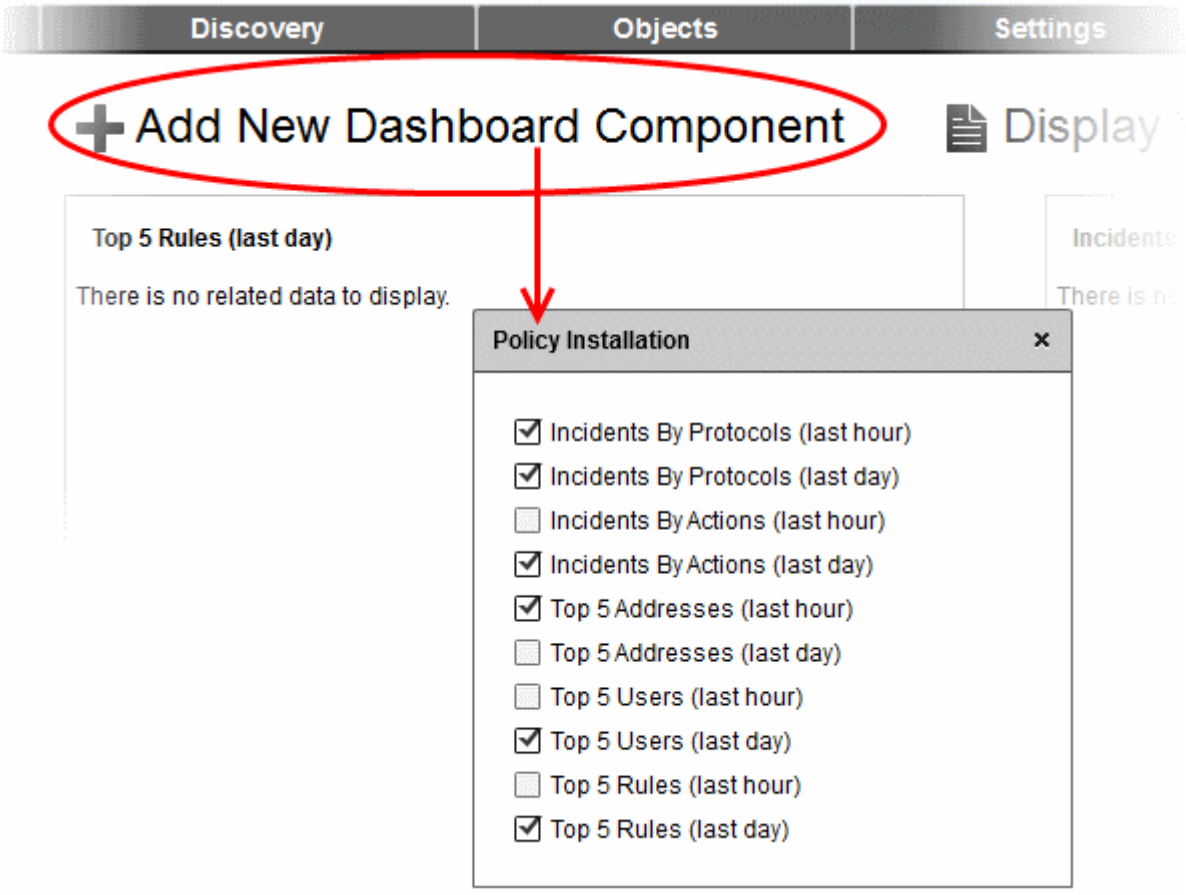
Top 5 Addresses (last day)	addresses) at the top 5 positions based on amount of data intercepted or discovered from them during the past one hour or the day verses the amount of data intercepted or discovered.
Top 5 Users (last hour)	The bar graph shows the users at the top 5 positions based on amount of data intercepted or discovered from them during the past one hour or the day verses the amount of data intercepted or discovered.
Top 5 Users (last day)	
Top 5 Rules (last hour)	The bar graph shows the rules at the top 5 positions based which data is intercepted or discovered during the past one hour or the day verses the amount of data intercepted or discovered.
Top 5 Rules (last day)	

Configuring the Dashboard

By default, the dashboard shows six important charts. The administrator can add or remove charts as per their requirements.

To add 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 add a new tile, select the tile
- To remove an existing tile, deselect the tile

Tip: Alternatively, you can remove a tile from the Dashboard itself, by clicking the 'X' at the top right of the tile.

- Close the dialog.

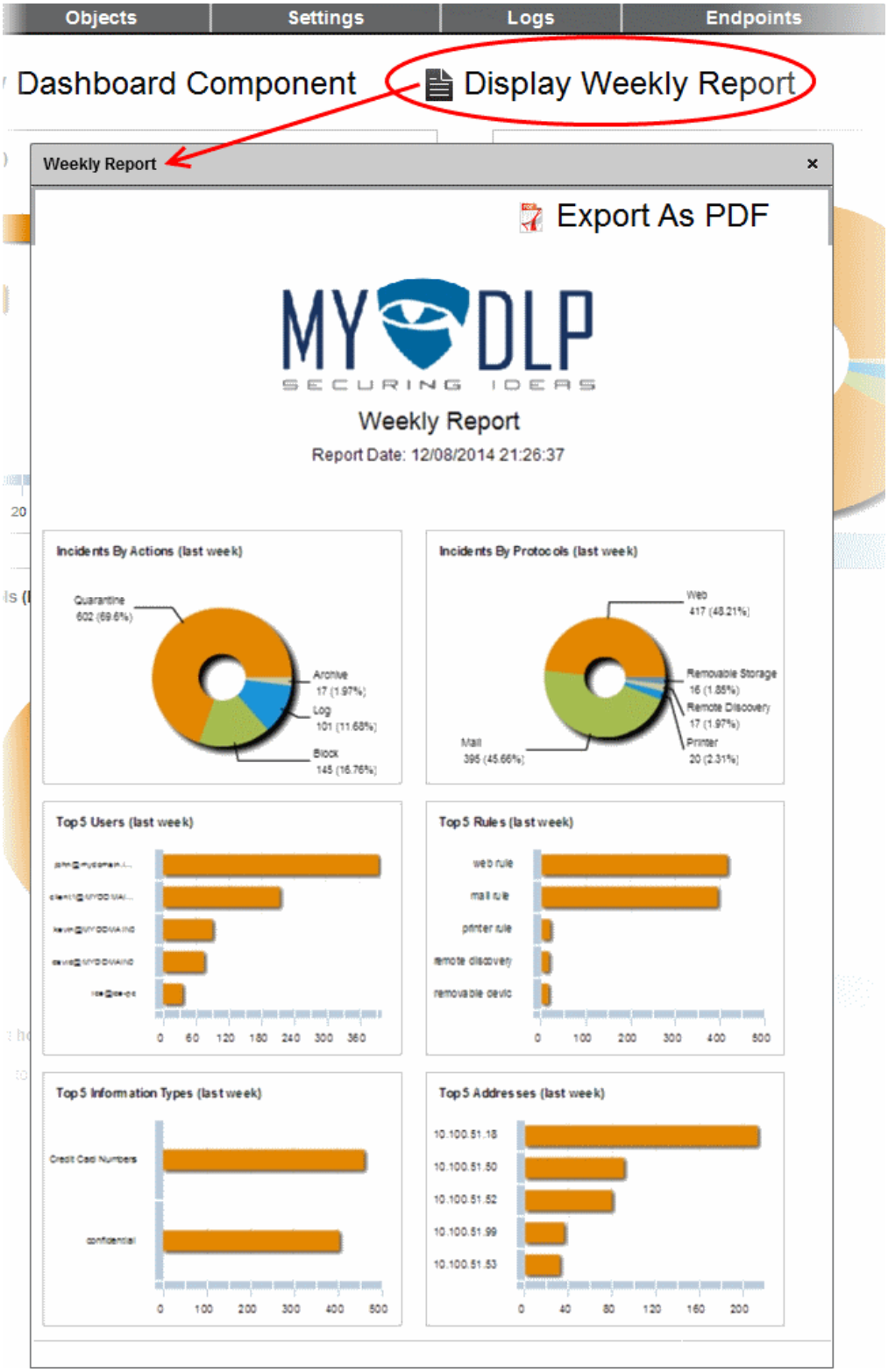
The new tile(s) will be added to the dashboard.

Viewing and Downloading Weekly Report

The Weekly Report provides the statistical summary of the logs of incidents and the top ranking users/endpoints from which large amount of data are intercepted/discovered for the past seven days.

To view the weekly report

- Click 'Display Weekly Report'. The weekly report will appear and display the statistics as explained above.



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

4. Data Transfer Control and Data Discovery

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.

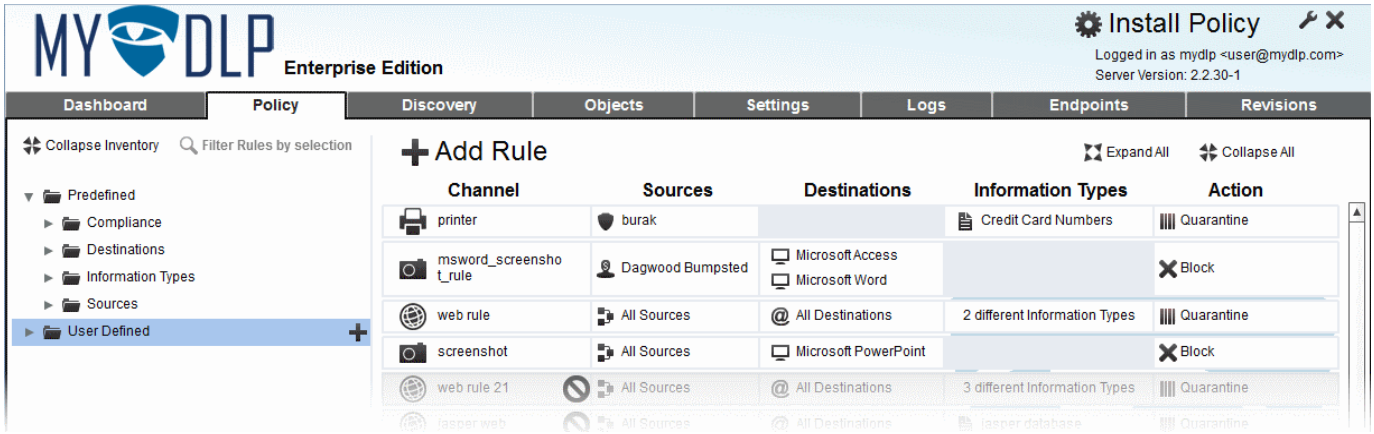
Data Transfer Policy ('Policy' tab)

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 **Enforcing Data Transfer Policy** for more Details.

Data Discovery ('Discovery' tab)

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 **Configuring Data Discovery** for more information.

Data transfer and data discovery rules are both constructed by dragging and dropping 'objects' into a rule - 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' and the 'Discovery' interfaces. These can be dragged into the rule creation interface which is shown on the right. You can create your own custom objects and new rules can be created by clicking the '+ Add rule' button.



The following sections contain more details on rules and objects:

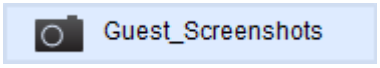
- **Rules**
  - **Rule Types**
  - **Rule Actions**
  - **Email Notifications and Messages**
- **Objects**
  - **Object Types**
  - **Information Types - An Overview**
    - **Predefined Matcher Types**
    - **Pre-Defined Information Types**
  - **User-Defined Objects**

4.1. The Rules

All rules that have been created for data transfer policy or data discovery are listed in the 'Policy' and 'Discovery' tabs respectively.

Both rule types have five common components, 'Channel', 'Sources', 'Destinations', 'Information Types' and 'Actions', while discovery rules also have a sixth component, 'Schedule'.

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 + rule name. You select the rule 'channel' then choose a rule name as the first steps when creating a new rule. Example data transfer 'channels' include 'Web Rule', 'Removable Storage Rule' and 'Screenshot Rule'. Discovery channels include 'Endpoint Discovery Rule' and 'Remote Storage Rule'. Once selected, the rule 'channel' is easily identified by the icon to the left of your rule name. 
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. 'Sources' can be dragged into the rule from the left hand tree.
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. 'Destinations' can be dragged into the rule from the left hand tree.
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. 'Information Types' can be dragged into the rule from the left hand tree.
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.

4.1.1. Rule Channels

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 the data 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 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

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

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

Discovery Rule Channels

Endpoint Discovery rules are used to inspect local storages and hard disk drives in the selected endpoints for files containing sensitive data of specified type(s) and control them. 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** action allows information to pass through the data channel freely without generation of any log entries. This action is available for all rule types.
- **LOG** action allows information to pass through data channel but generates event log. This action is not available for screenshot rules.
- **ARCHIVE** action 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.
- **BLOCK** action prevents information to pass through data channel and generates event log. This action is not available for removable storage inbound rules.
- **QUARANTINE** action prevents information to pass, generates event log and archives a copy of information. This action is not available for removable storage inbound rules and screenshot rules.
    - When this action applied with 'Endpoint discovery rule,all the 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. The Administrator 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 'Delete' action in an 'Endpoint discovery rule', with the difference that a copy of the matching files will be saved in the server.

- **ENCRYPT** action is only available for Removable Storage Encryption Rule. When applied, MyDLP detects any new USB storage device connected to the endpoints specified as Sources 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.
- **DELETE** action is only available for Discovery rules. It deletes matched discovered files. It is advised to use this action very carefully.

In addition to the default actions, the administrator can create custom actions for execution on files identified by Endpoint Discovery and Remote Storage Discovery rules based on Information Rights Management (IRM) by integrating Seclore FileSecure IRM solution to Comodo MyDLP. Refer to the following sections for more details:

- **Integrating Seclore FileSecure**
- **Creating new Custom Actions for MyDLP for use in Discovery Rules**

4.1.3. Email Notifications and Messages for a Rule

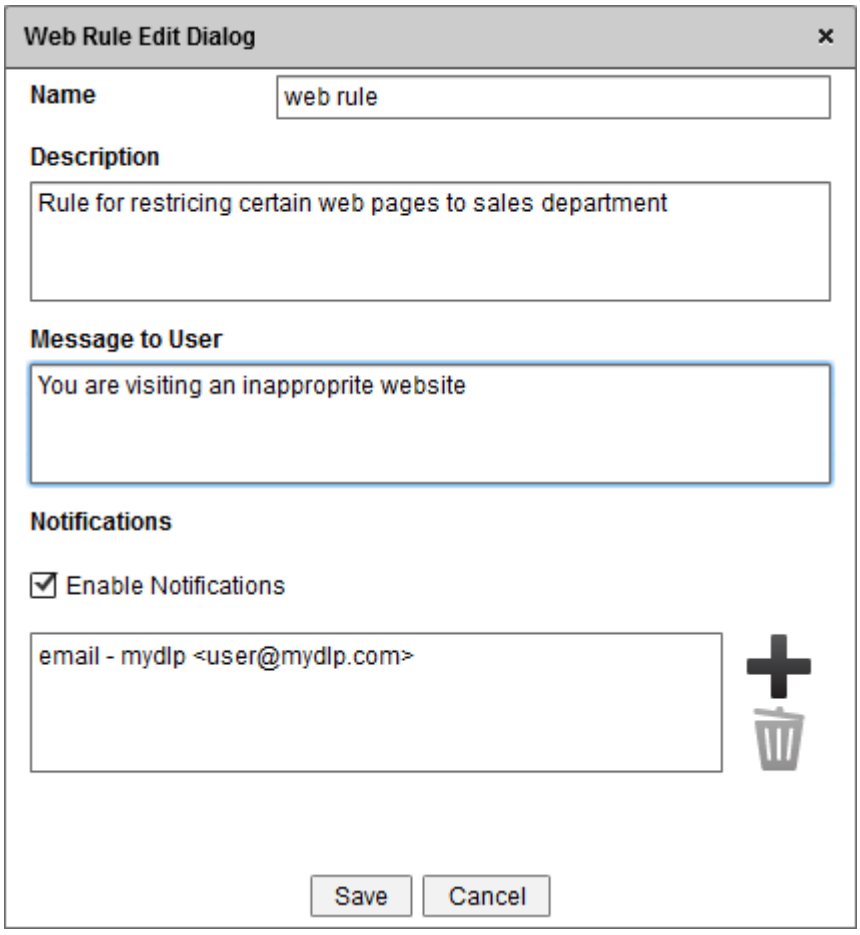
The administrator can configure MyDLP to send an email alert when an event occurs to self or other administrators for the following types of rules.

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

The notifications will be sent only to the administrative users in the list below 'Notifications'.

- The administrative users to be notified an be added to the list by clicking the plus button beside the text box, after enabling Notifications.
- These notifications can be customized from **'Settings' > 'Enterprise > Email Notification'** tab.

The administrator can also specify messages to be displayed to the user when MyDLP blocks or quarantines the data traffic from the user computer based on a Web Rule or Mail Rule. The message will be displayed only if the action set for the rule is to BLOCK or QUARANTINE.



4.1.4. Web Rule

Web Rule covers 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**.

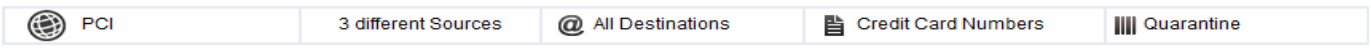
Web Sources - You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects or domain objects as Source for this rule. See the chapter **Objects Tab** for more details on creating user defined sources.

Web Destinations - You can use Domain objects as Destination for this rule type. Domains are Fully Qualified Domain Name (FQDN) accessed by users in web requests. See the chapter **Objects Tab** 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 sales department to all websites that contains credit card information. This rule is named as PCI because it is a part of PCI compliance policy.



4.1.5. Mail Rule

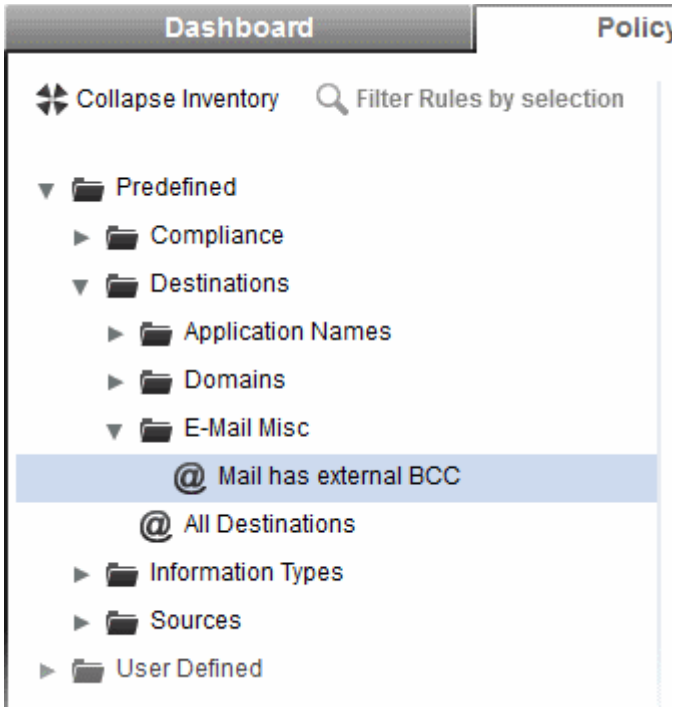
Mail Rule covers the mail channel and can be used to enforce policies for SMTP protocol. The emails that are sent through the

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) as Source for this rule.

Mail Destination - You can use Domain objects as Destination for this rule.

You can also configure additional miscellaneous destination properties for emails, from the 'E-Mail Misc' menu under Policy Objects tree in the left hand side, by navigating through 'Predefined' > 'Destinations' > E-Mail Misc. The option available is 'Mail has External BCC item' to filter those mails that have a BCC field.



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.

PCI	3 different Sources	All Destinations	Credit Card Numbers	Quarantine

4.1.6. Removable Storage Rule

The Removable Storage Rule can be used to govern the data moved to 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 or Endpoint Objects as Source for this rule.

Removable Storage Destination - Since it is not possible to specify destination for removable storage, the Destination field is not required for this rule.

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 to removable storage devices, such as USB sticks connected to their workstations or laptops. This rule is named as PCI because it is a part of PCI compliance policy.

Channel	Sources	Destinations	Information Types	Action
PCI	3 different Sources		Credit Card Numbers	Quarantine

4.1.7. 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 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	Sources	Destinations	Information Types	Action
Storage Logging	3 different Sources			Log

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.

4.1.8. 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 specified as Sources 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 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	Sources	Destinations	Information Types	Action
All Encr	All Sources			Encrypt

4.1.9. 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 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	Sources	Destinations	Information Types	Action
PCI	3 different Sources		Credit Card Numbers	Quarantine

4.1.10. 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 or Endpoint Objects as Source for this rule.

ScreenShot Destination - You can specify Application objects that refer to specific application or application group, 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	Sources	Destinations	Information Types	Action
Screenshot Restriction	sales1 sales2 sales3	Microsoft Access Microsoft Excel Microsoft OneNote-1 Microsoft OneNote-2 Microsoft Outlook Microsoft PowerPoint Microsoft Publisher Microsoft Word Notepad		Block

4.1.11. 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 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	Sources	Destinations	Information Types	Action
PCI CRM Int	10.0.0.0/24		Credit Card Numbers	Block

4.1.12. 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.

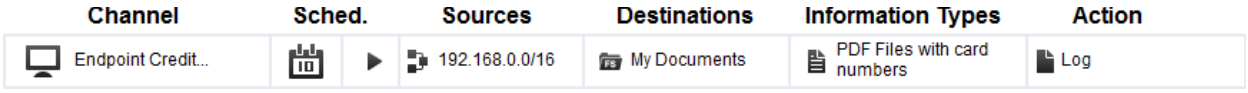
Discovery Source: - You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects, Computer Name objects or Endpoint Objects as Source for this rule.

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 pdf files containing credit card numbers, from the My Documents folder in the endpoints of 10.0.0.0/24 network.



4.1.13. 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.

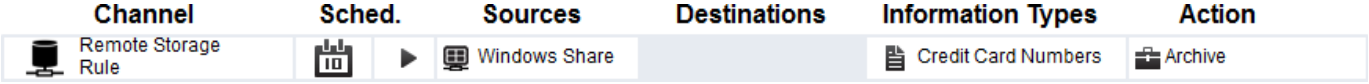
Discovery Source: - You can specify a Remote Storage object as Source for this rule. The Remote Storage objects pointing to remote storage locations can be created only from the 'Discovery' interface. Refer to the section **Adding a User Defined Remote Storage** for more details.

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

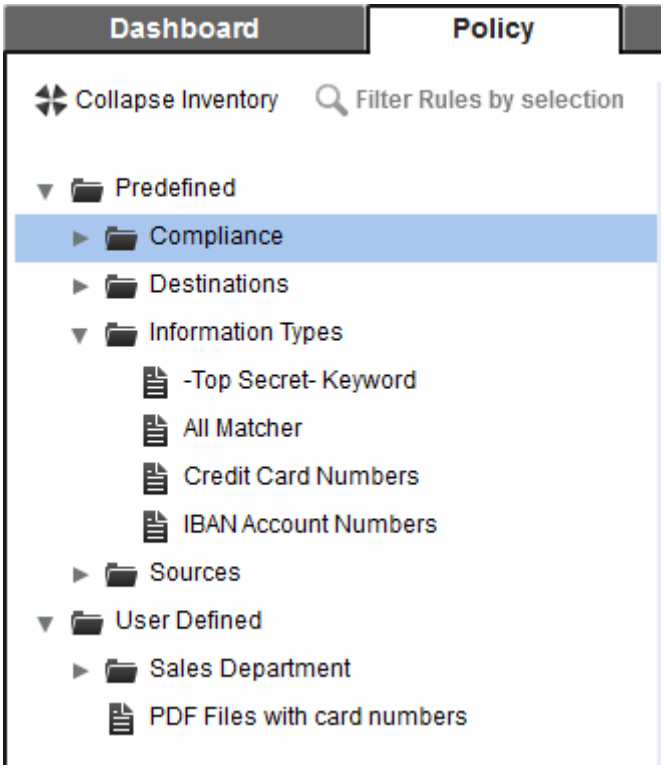
An example of Network Storage Discovery Rule is shown below. The rule is for archiving Office document files containing Permanent Account Number (PAN) from the Remote Storage.



4.2. The Objects

The Objects that can be used to construct rules are displayed as a tree structure in both the Policy and Discovery interfaces. These objects can be directly dragged to source, destination and information type fields while configuring the rules.

An example of objects tree is shown at 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 **Creating User Defined Objects** for more details.

4.2.1. 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
Category	The 'Category' is a container for several types of objects. Each category can be expanded by clicking the right arrow beside it from the left hand side pane to view the sub categories and individual objects contained in as a tree structure. The category or the sub category can be: • expanded and the individual objects can be applied to suitable components of rules. • dragged as a whole to required component of a rule so that the all the objects that are suitable for the rule component will be automatically applied to the component.	Depending on the individual objects contained in the 'Category'. The applications of the individual objects are explained in the following rows.
Network	The 'Network' object is used to define a network or a sub network by their IP address/Network Mask	As 'Source' in: • All types of Data Transfer Policy rules except Mail Rule • Endpoint Discovery rule
Computer Name	The Computer Name 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	As 'Source' in: • All types of Data Transfer Policy rules except Mail Rule • Endpoint Discovery rule

Object Type	Description	Application
	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.	
Endpoint	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.	As 'Source' in: • All types of both Data Transfer Policy rules except Mail Rule • Endpoint Discovery rule
Information Type	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 • Endpoint Discovery Rule • Remote Storage Rule
Information Type Group	The 'Information Type Group' object is a collection of Information Types	As 'Information Type' in: • Web Rule • Mail Rule • Removable Storage Rule • Printer Rule • API Rule • Endpoint Discovery Rule • Remote Storage Rule
Domain	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 or a discovery rule.	As 'Source' and 'Destination' in all types of Data Transfer Policy rules.
Application Name	The 'Application Name' object is used to specify a software application or executable.	As 'Destination' in Screenshot rule
User Object	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.	As 'Source' all types of Data Transfer Policy rules.

Object Type	Description	Application
	The rule in which the User Object is used will be effective only if the user is specified as displayed in the Endpoints interface.	
File System Directory	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 Storage	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

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 **Creating User Defined Objects** for more details.

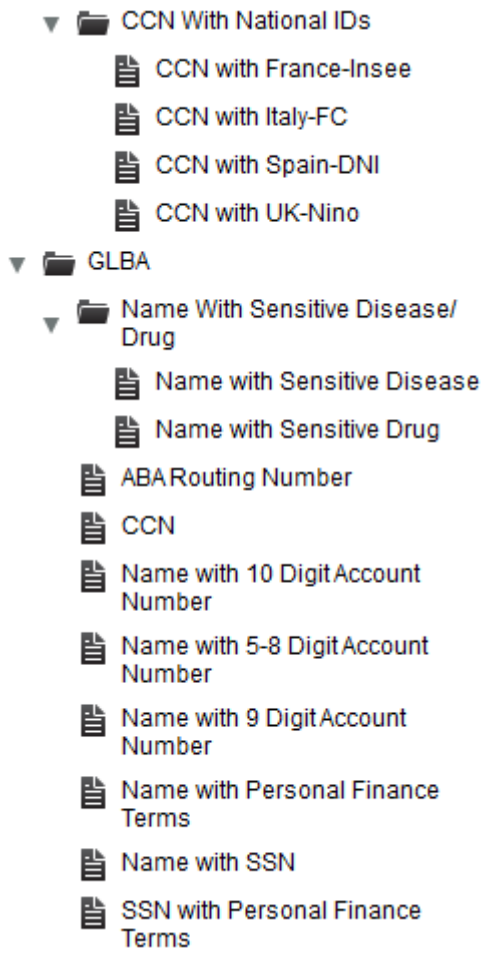
4.2.2. Information Types - An Overview

Data Loss Prevention depends on identifying data of specific type, included in the files that are transferred or the files that are residing on users' computers. The 'kind' of data to be identified is defined in each rule so that the data transfer or data storage containing the specific type is allowed, blocked, quarantined, or logged as mentioned in the rule. The kind of data is specified as 'Information Type' object in the rules.

MyDLP is shipped with a number of predefined information types and is constantly updated. In addition, the administrator can create custom information types as required by the organization.

Refer to the section **Adding a User Defined Information Type** for more details.

Picture at the right show some of these information types.



Each Information type is constituted by three components:

- Name - A Name to identify the information type
- **Data Format(s)** - The file format(s) included in the information type. The files of the specified format will be inspected for the occurrence of data with properties/string formats specified in the Information Features.
- **Information Features** - The properties of content data in the files of formats specified under Data Formats. The features include:
  - **Matcher** - The 'Matcher' parameter specifies data patterns or string formats - like birth-date, keywords, credit card number, account number and so on and a threshold for occurrence. 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** - The minimum extent of data size within which the data matching the matchers are to be identified for number of times specified as threshold to conclude a file as one falling within the Information Type.

If a file 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 the Objects interface. Refer to the section **Managing Data Formats** 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**

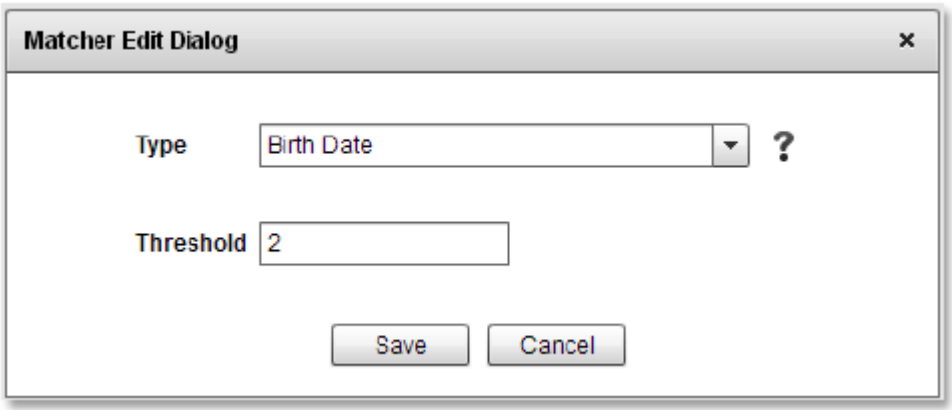
Matcher

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 contains two components:

- 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

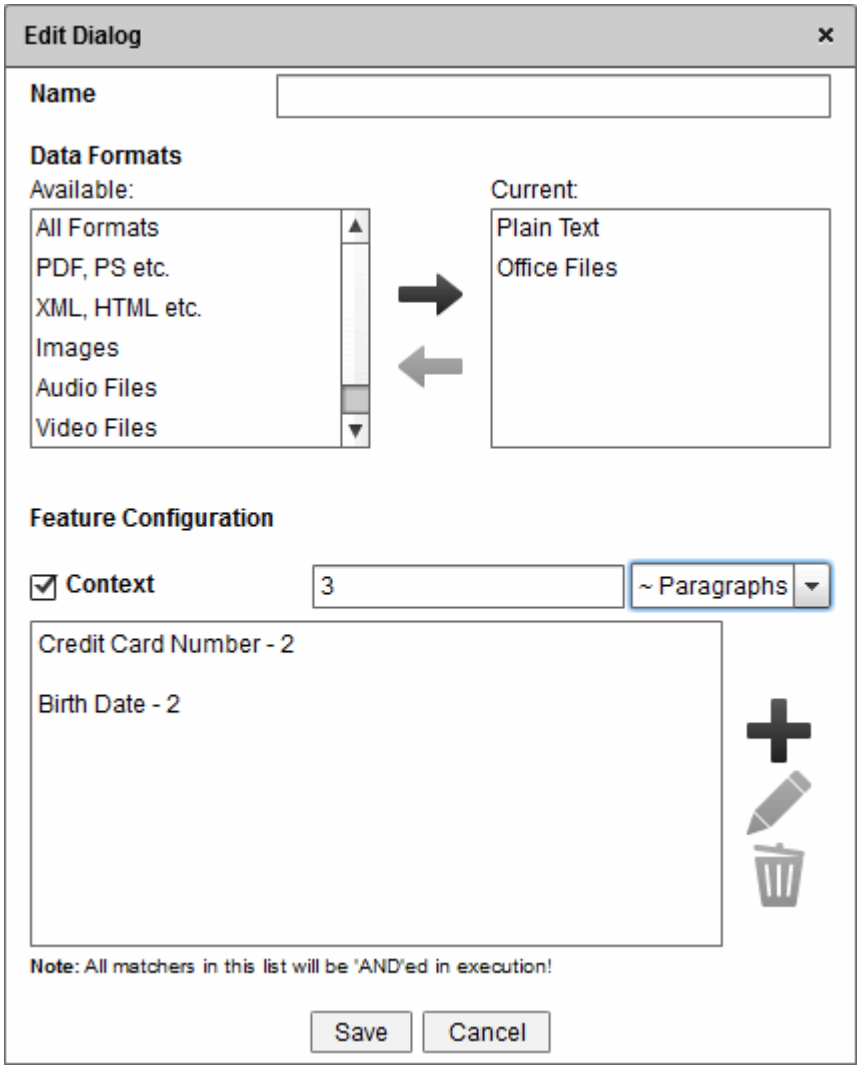
The 'Context' is an optional parameter used to specify the minimum extent of data size within which the data matching the 'Matchers' should occur, to consider a file as 'Information Type' object. DLP analysis will return positive only if all the defined Information Features are found within a portion 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 plain text and office document files 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 plain text and office document files 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.

4.2.2.1. 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.
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 Objects interface. Refer to the section **The Objects Interface** for more details.
MAC	Identifies the occurrence of MAC address included in the data stream or file
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.
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.

4.2.2.2. 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	

Information Type	Description	Matchers & Threshold Values		Context
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				
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	Credit Card Number	1	3 Sentences

Information Type	Description	Matchers & Threshold Values		Context
	and Italy Fiscal Code Number	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	
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

Information Type	Description	Matchers & Threshold Values		Context
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
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

Information Type	Description	Matchers & Threshold Values		Context
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	

Information Type	Description	Matchers & Threshold Values		Context
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	
		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	Keyword - "Restricted"	6	3 Pages

Information Type	Description	Matchers & Threshold Values		Context
	containing the term "Restricted"			
Sensitive - Keyword	Identifies documents containing the term "Sensitive"	Keyword - "Sensitive"	6	3 Pages
Top Secret - Keyword	Identifies documents containing the term "top secret"	Keyword - "top secret"	6	3 Pages
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

4.3. 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 **Rules Table** and the **Objects Tree**. This section explains on how to create 'User Defined Objects'. Refer to the following sections for more information.

- **Adding a User Defined Category**
- **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 Information Type Group**
- **Adding a User Defined Domain Name**
- **Adding a User Defined Application Name**
- **Adding a User Defined User Object**

- Adding a User Defined File System Directory
- Adding a User Defined Remote Storage

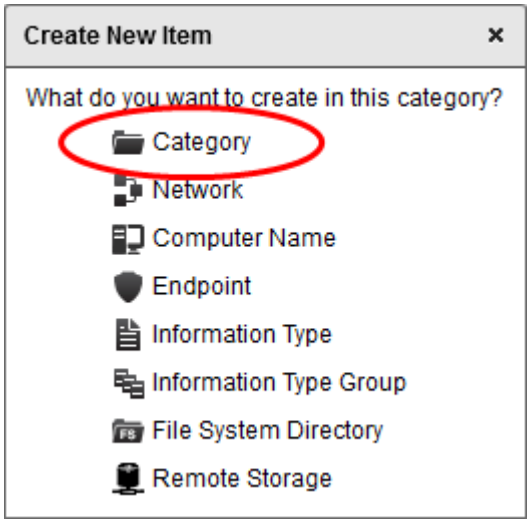
4.3.1. Adding a User Defined Category

A 'Category' is a collection of different user defined objects. The administrator can create any number of Categories and 'Sub-categories' within them. Each category or sub category can be added with several kinds of individual objects.

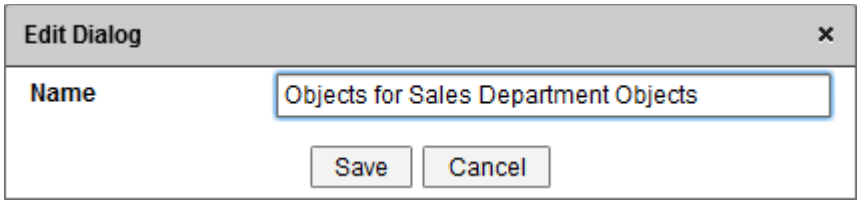
For example, the administrator can create a category for each department of the organization and add the source, destination and information type objects that are specific for the respective department. While creating data transfer policy and discovery rules for a department, the administrator can drag the objects from the respective category for inclusion in the rules.

To create a new category

1. Select the 'User Defined' folder from the left hand side pane in 'Policy' or 'Discovery' tab
2. Click the plus icon that appears on 'User Defined' stripe. The Create New Item dialog will appear.

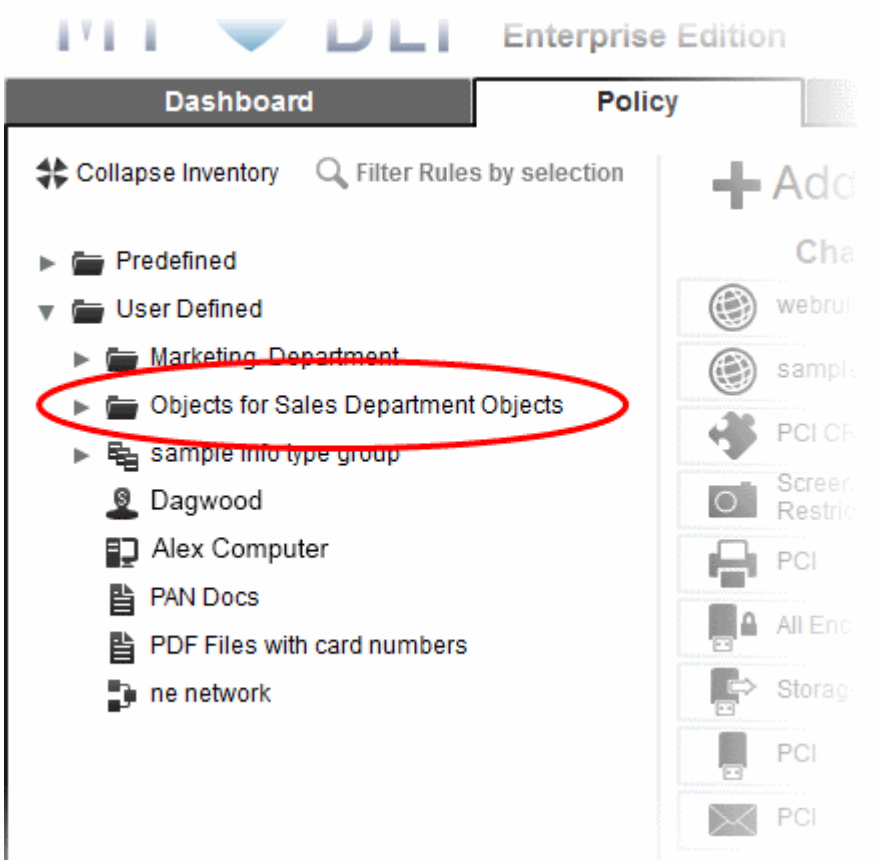


3. Select 'Category'. The Edit Dialog will appear.
4. Enter a name, briefly describing the category being created.



5. Click 'Save'.

The category will be added to the Objects tree in the left hand side pane.



6. To create a sub category, select the category from the LHS pane, click the icon and follow the same procedure as above.

You can add any number of individual objects in the created category. To deploy an object contained within a category, click the right arrow beside the category to expand it.

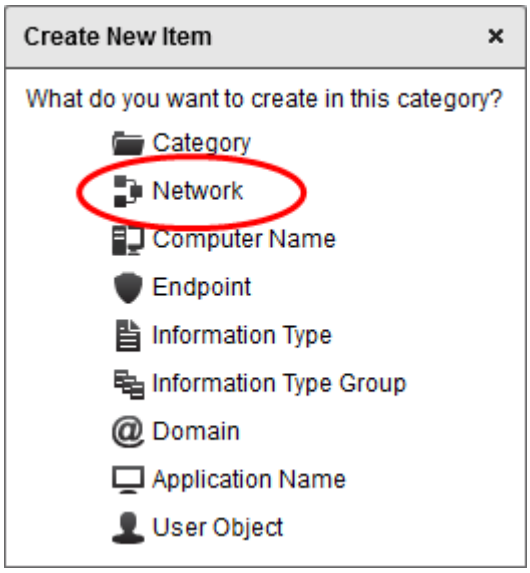
4.3.2. Adding a User Defined Network Object

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 except the mail rules.

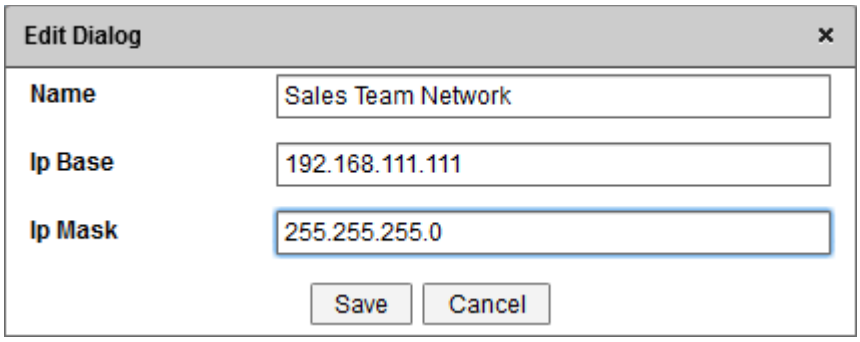
To create a new network object

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the 'Network' object, from the left hand side pane of 'Policy' or the 'Discovery' interface

2. Click the plus icon that appears on the selected folder stripe. The 'Create New Item' dialog will appear.

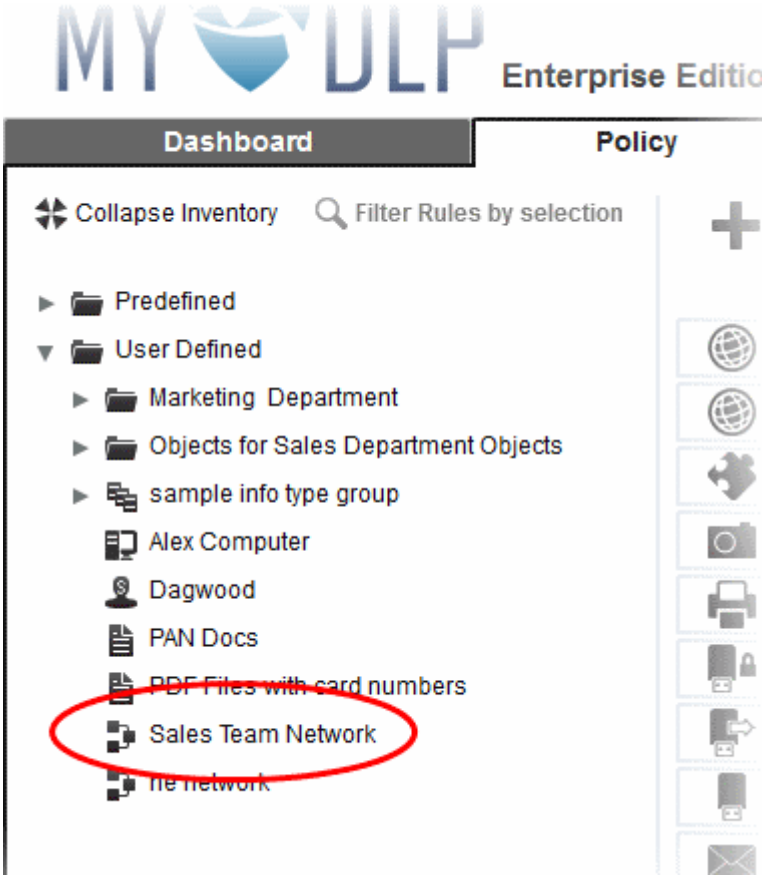


3. Select 'Network'. The 'Edit Dialog' will appear.



4. Enter the parameters:
   - Name - Enter a name shortly describing the network object
   - IP Base - 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
5. Click 'Save'.

The new user defined network object will be listed under 'User Defined'/Category folder in the LHS pane of the 'Policy' and 'Discovery' interfaces.



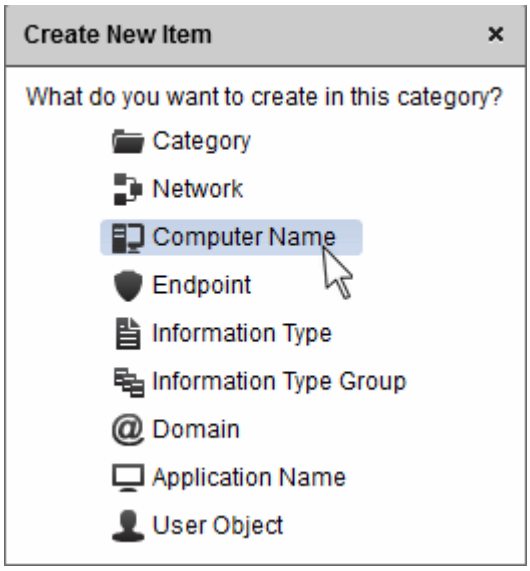
4.3.3. Adding a User Defined Computer Name Object

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

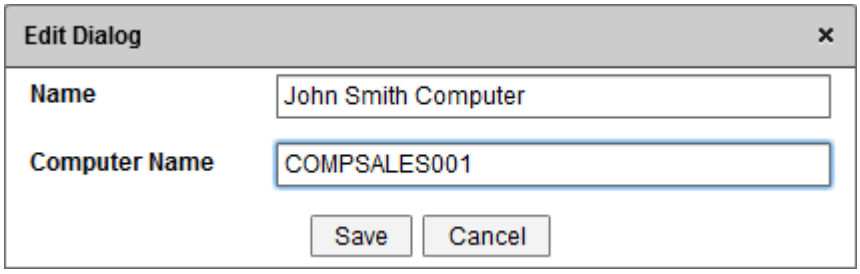
Prerequisite: The endpoints are to be installed with the MyDLP Endpoint Agent before adding them as Computer Name Objects. The endpoints installed with the agent are listed with their Endpoint IDs, Logged-in Usernames and Computer Names under the **Endpoints** tab. Refer to the **MyDLP Endpoint Installation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

To create a Computer Name object

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the new object, from the left hand side pane of 'Policy' or the 'Discovery' interface.
2. Click the plus icon  that appears on the selected folder stripe. The 'Create New Item' dialog will appear.

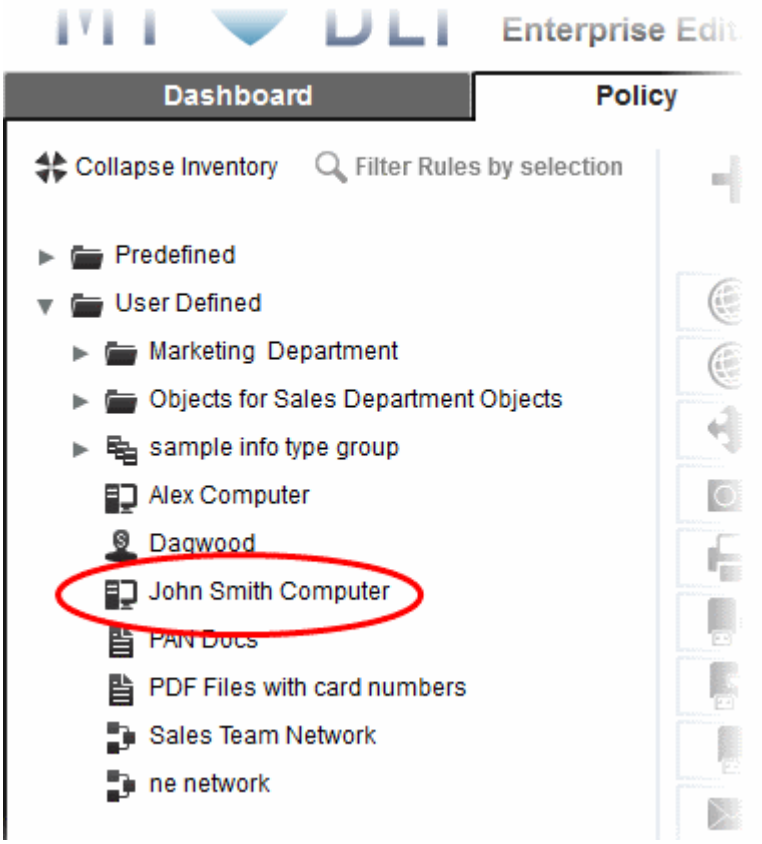


3. Select 'Computer Name'. The 'Edit Dialog' will appear.



4. 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.
5. Click 'Save'.

The new user defined computer name object will be listed under 'User Defined'/Category folder in the LHS pane of the 'Policy' and 'Discovery' interfaces.



4.3.4. 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 with 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.

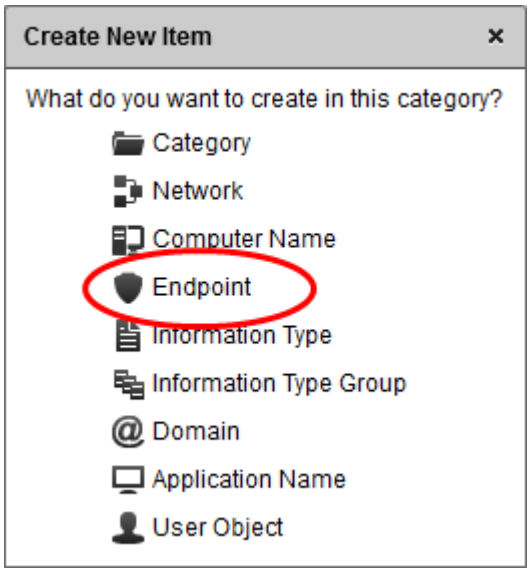
The administrator can create Endpoint Object by specifying the ID number for use in source component or the destination component in a rule. To apply the rule, MyDLP wil use the persistent ID number of the computer to identify it instead of the IP address, Computer name, Logged on username and so on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

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

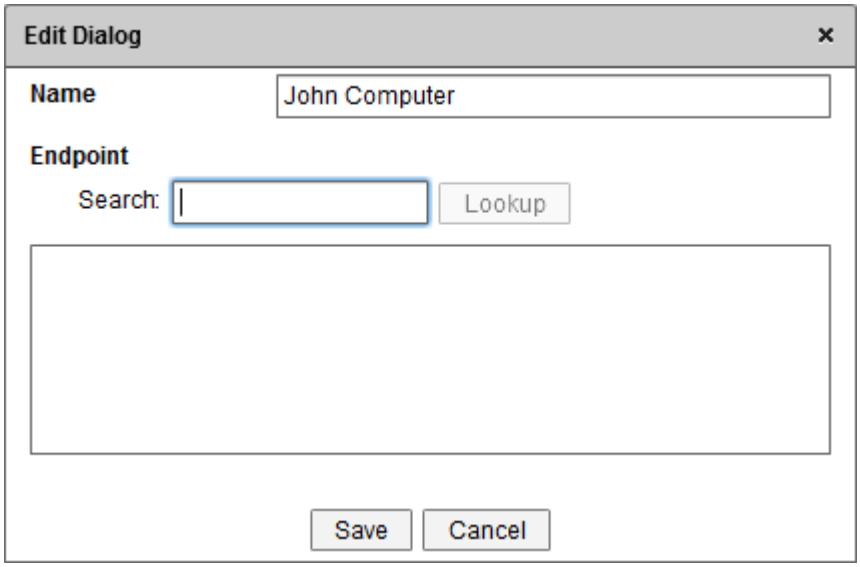
To add an endpoint object

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the 'Endpoint' object, from the left hand side pane of 'Policy' or the 'Discovery' interface

2. Click the plus icon  that appears on the selected folder stripe. The 'Create New Item' dialog will appear.

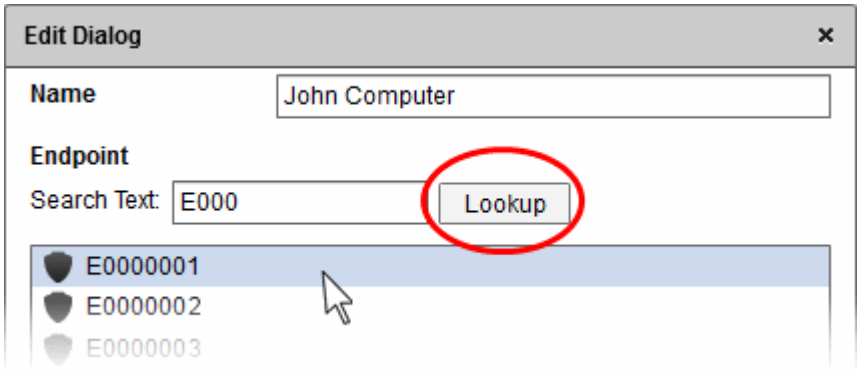


3. Select 'Endpoint'. The 'Edit Dialog' will appear.



4. Enter the parameters:

- Name - Enter a name shortly describing the computer
- Search - To specify an 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 in the text box.



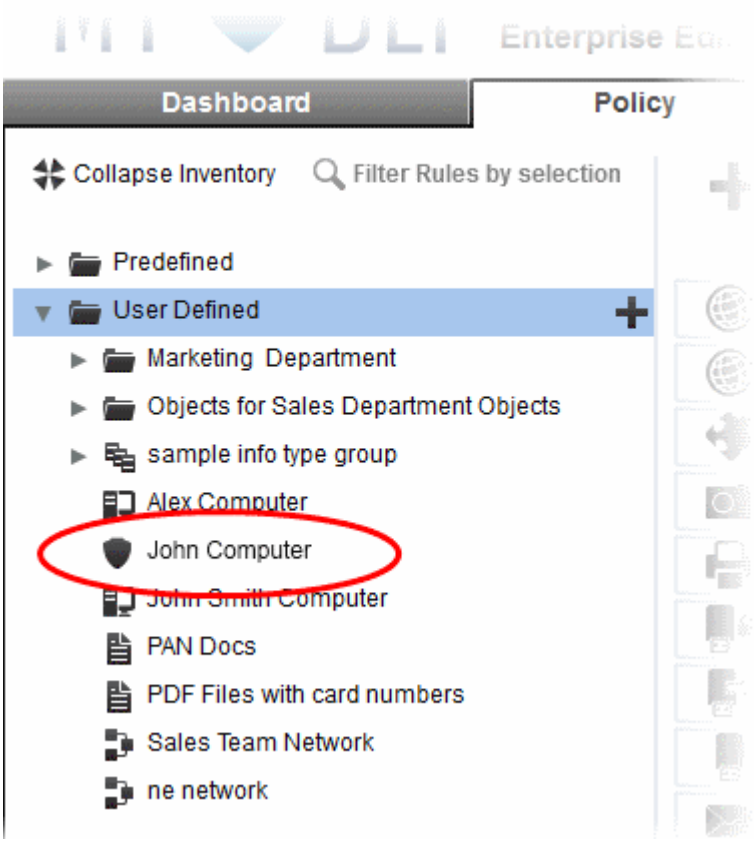
- Select the ID of the endpoint to be specified in the endpoint object

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**.

5. Click 'Save'.

The new user defined endpoint object will be listed under 'User Defined'/Category folder in the LHS pane of the 'Policy' and 'Discovery' interfaces.



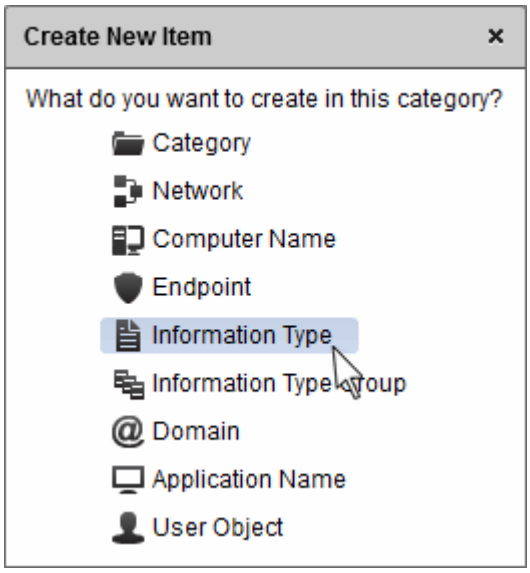
4.3.5. Adding a User Defined Information Type

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;

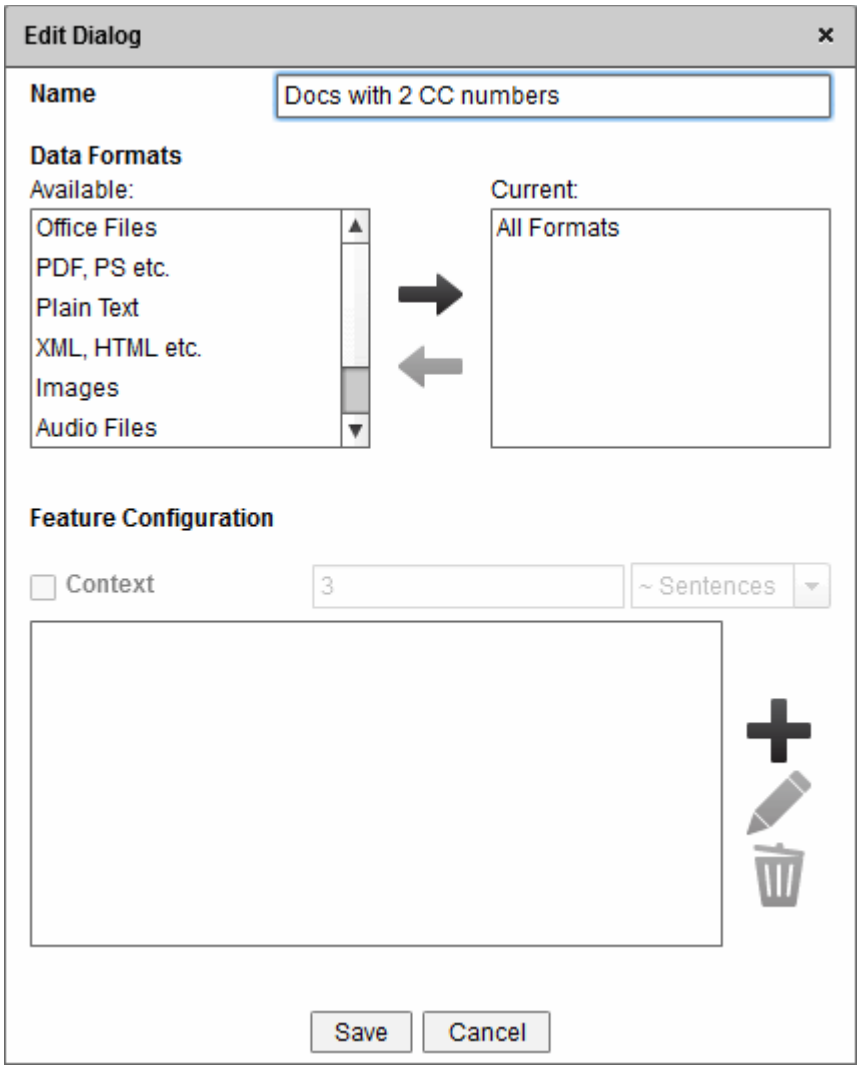
- Web Rule
- Mail Rule
- Removable Storage Rule
- Printer Rule
- API Rule
- Endpoint Discovery Rule
- Remote Storage Discovery Rule

To define a custom information type

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the new object, from the left hand side pane of 'Policy' or the 'Discovery' interface.
2. Click the plus icon  that appears on the selected folder stripe. The 'Create New Item' dialog will appear.



3. Select 'Information Type'. The 'Edit Dialog' will appear.



4. Enter a name shortly describing the information type, in the Name field.

5. Select the file formats to be included in the information type object under '**Data Formats**'. All the available formats are listed in the left hand side pane and the file formats included in the information type are listed in the right hand side pane. To include a file format to the information type, select it from the LHS pane and move to the RHS pane by

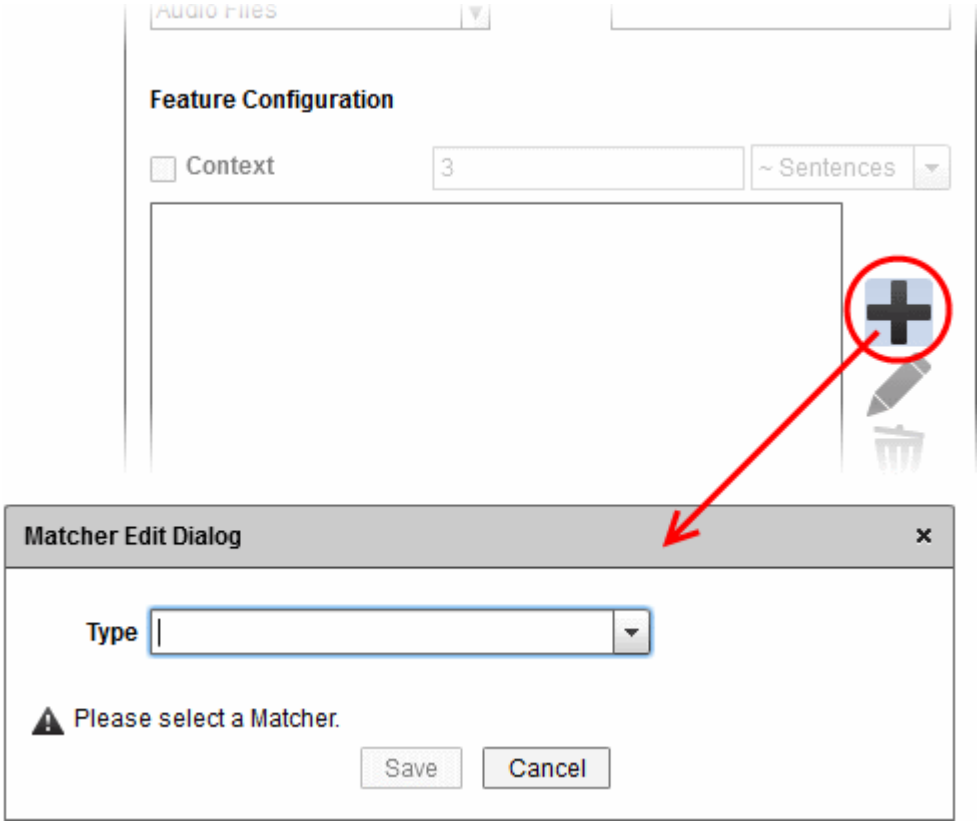
clicking the right arrow . To remove a file format from the information type, select it from the RHS pane and move to the LHS pane by clicking the left arrow . Refer to the explanation of **Data Formats** under the section **Information Types - An Overview** for more details.

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 'Objects' interface. Refer to the section **The Objects Interface** for more details.

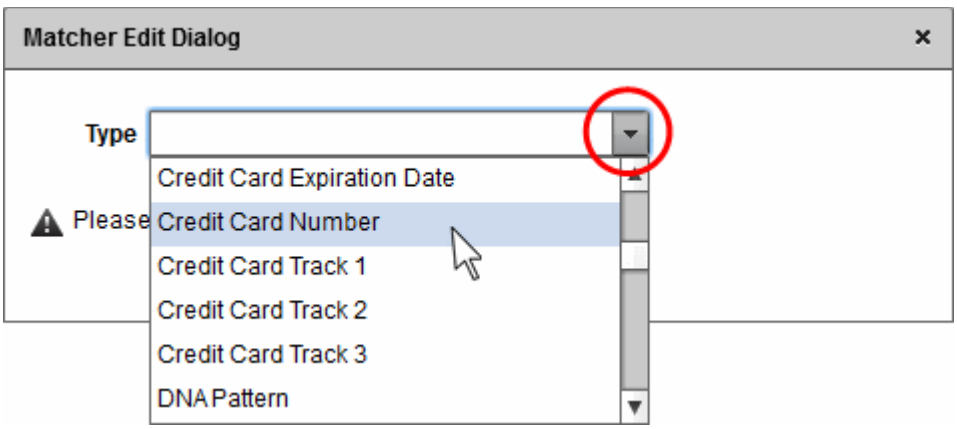
6. Configure the Information Features to be added to the Information Type under the '**Feature Configuration**'. Refer to the explanation of **Information Features** under the section **Information Types - An Overview** for more details on the components of the Information Feature.

Step 1 - Enter the matchers for the information feature

- Click the plus icon beside the text box



- Select the matcher type from the Type drop-down. 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.

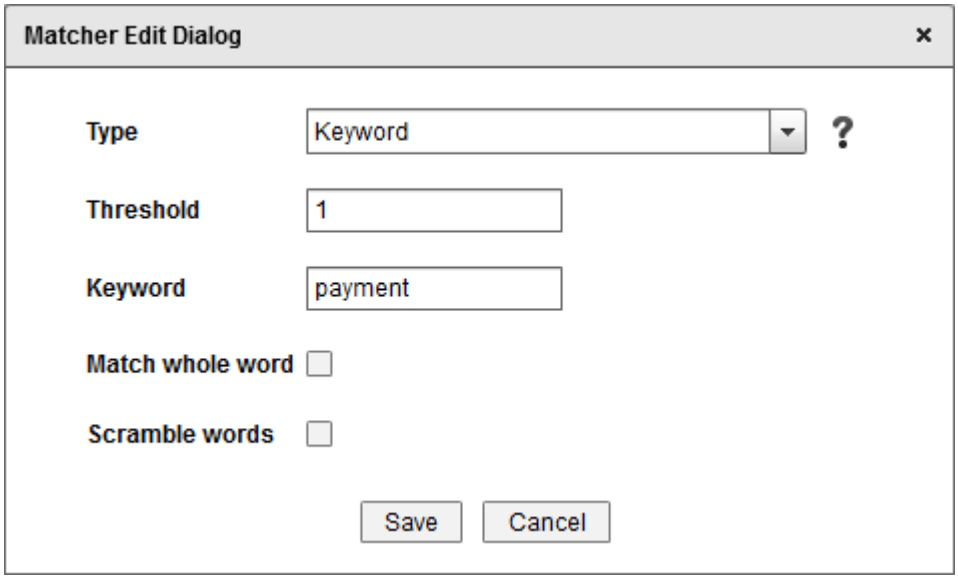
To edit a matcher

- Select the information type from the left hand side pane and click the Edit icon. The Edit dialog for the information type will appear.
- Select the matcher from the list and click the Edit icon at the right. The Matcher Edit dialog will appear as shown above and allow you to edit its parameters.
- Click Save for your changes to take effect

To remove a matcher

- Select the information type from the left hand side pane and click the Edit icon. The Edit dialog for the information type will appear.
- Select the matcher from the list and click the Trash can icon at the right. The matcher will be removed.

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.

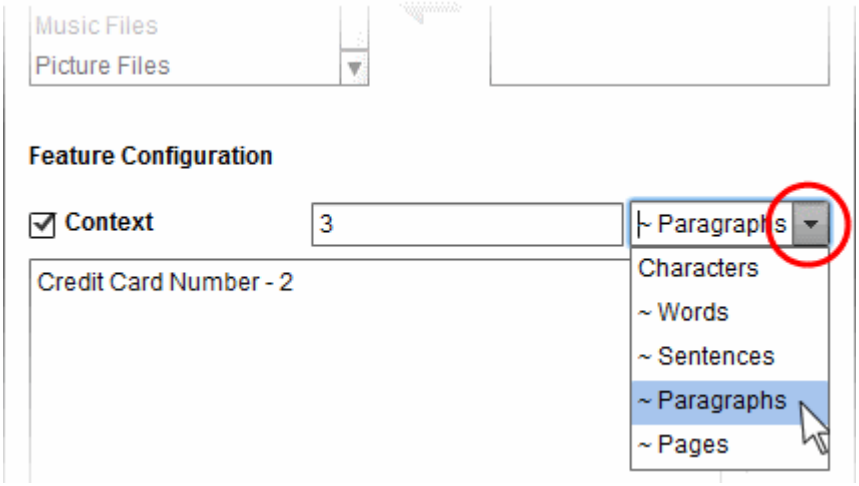


- Keyword - Enter the keyword to be included as the matcher
- Match whole word - Selecting this option will count only the occurrences of the keyword as full word. Else partial occurrences will also be counted
- Scramble words - Selecting this option will count the occurrences of the keyword even if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

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 are 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.

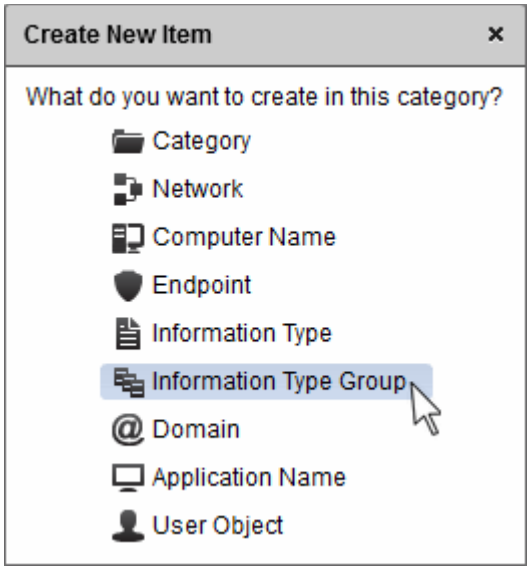
7. Click 'Save' to save the Information Type.

4.3.6. Adding a User Defined Information Type Group

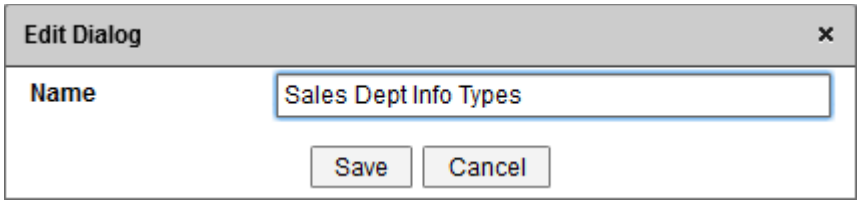
The administrator can create a collection of several individual Information type objects as a user defined Information Type Group and apply it for 'Information Type' component while creating a rule.

To create an Information Type Group

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the new object, from the left hand side pane of 'Policy' or the 'Discovery' interface.
2. Click the plus icon that appears on the selected folder stripe. The 'Create New Item' dialog will appear.



3. Select 'Information Type Group'. The 'Edit Dialog' will appear.



4. Enter a name shortly describing the information type group in the Name field.
5. Click Save to save the group.

The Information Type Group will be added as a sub-category under User Defined folder. You can add new Information Types under the Information Type Group.

1. Expand the 'Objects' tree in the left hand side pane and select the information type group
2. Click the plus icon that appears on the selected folder stripe. The 'Edit Dialog' for creating a new information type will appear.
3. Follow the procedure as explained in the previous section **Adding a User Defined Information Type**.
4. Repeat the process to add more number of information types to the group.

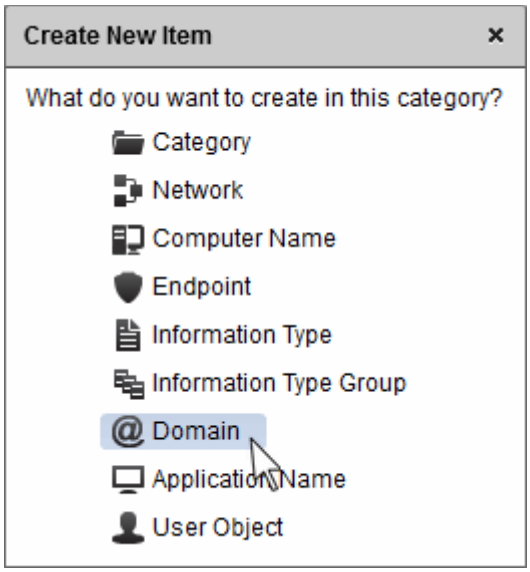
4.3.7. Adding a User Defined Domain Name

Comodo MyDLP ships with a number of per-defined domain objects including commonly used email domains, under Predefined > Destinations > 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.

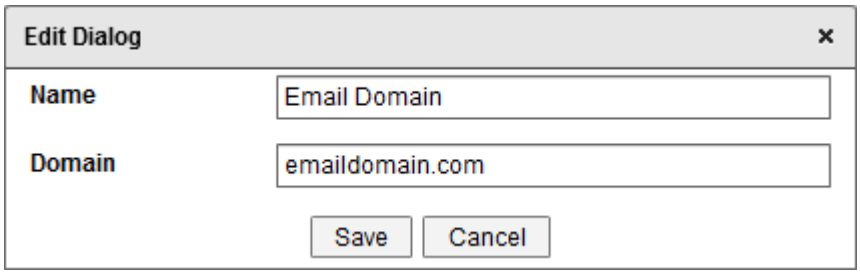
Note: The Domain objects can be used only as destination in the data transfer policy rules, like web rules and email rules, they can be created and viewed only from the 'Policy' interface.

To add a new domain name

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the new domain, from the left hand side pane of 'Policy' interface.
2. Click the plus icon that appears on the selected folder stripe. The 'Create New Item' dialog will appear.

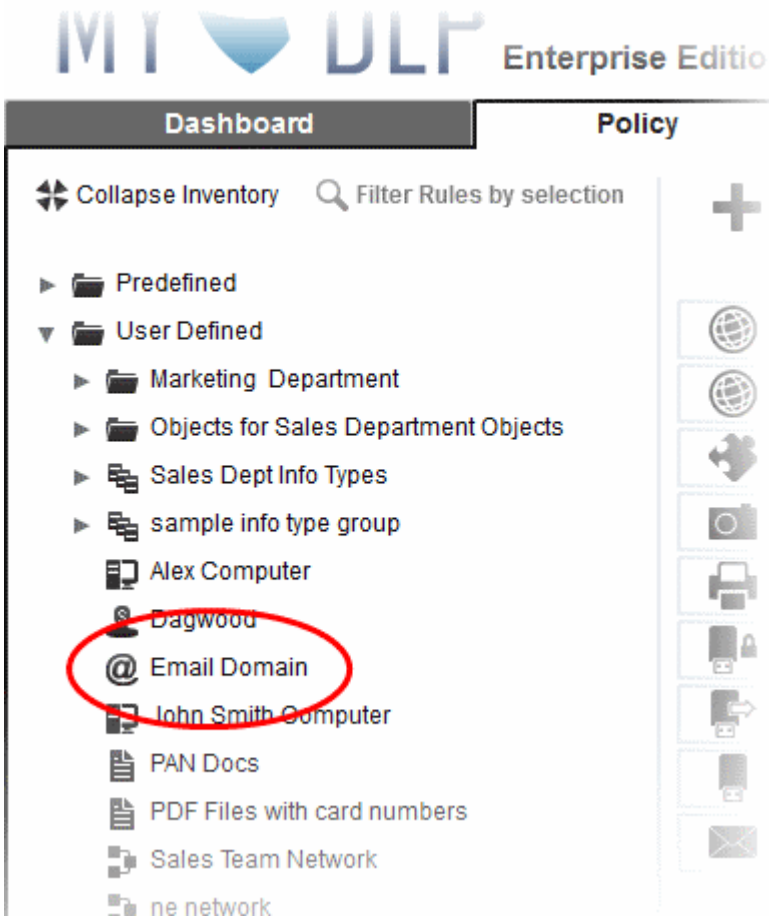


3. Select 'Domain'. The 'Edit Dialog' will appear.



4. Enter the parameters:
    - Name - Enter a descriptive name for the domain object
    - Domain - Enter the domain name or the full URL to be added
5. Click 'Save'.

The new user defined domain object will be listed under 'User Defined'/Category folder in the LHS pane of the 'Policy' interface, and can be dragged to be added as destination for web rules and email rules.



4.3.8. Adding a User Defined Application Name

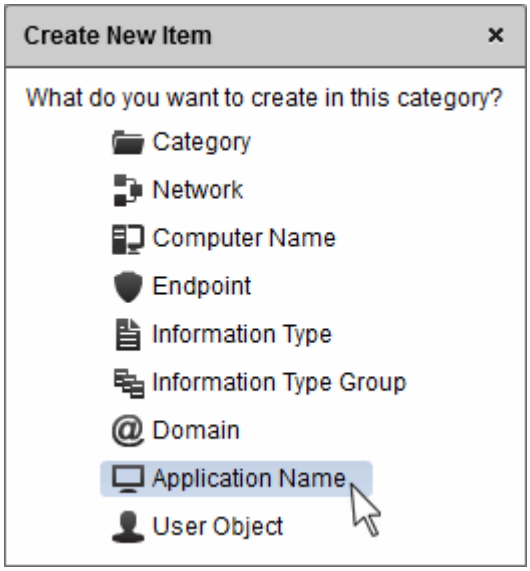
Comodo MyDLP ships with a number of pre-defined Application Name objects including commonly used Internet browsers, Design applications, Microsoft Office applications, and PDF viewers under Predefined > Destinations > Application Names. These applications can be specified for destination component for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

Note: The 'Application Name' objects can be used only as destination in the Screenshot rule, which is a data transfer policy rule, hence they can be created and viewed only from the 'Policy' interface.

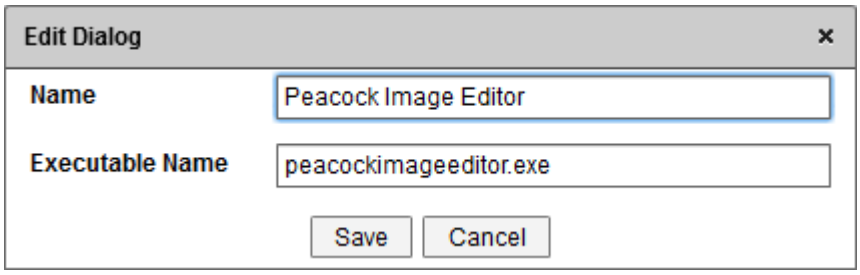
To add a new Application Name object

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the new application name, from the left hand side pane of 'Policy' interface.

2. Click the plus icon  that appears on the selected folder stripe. The 'Create New Item' dialog will appear.

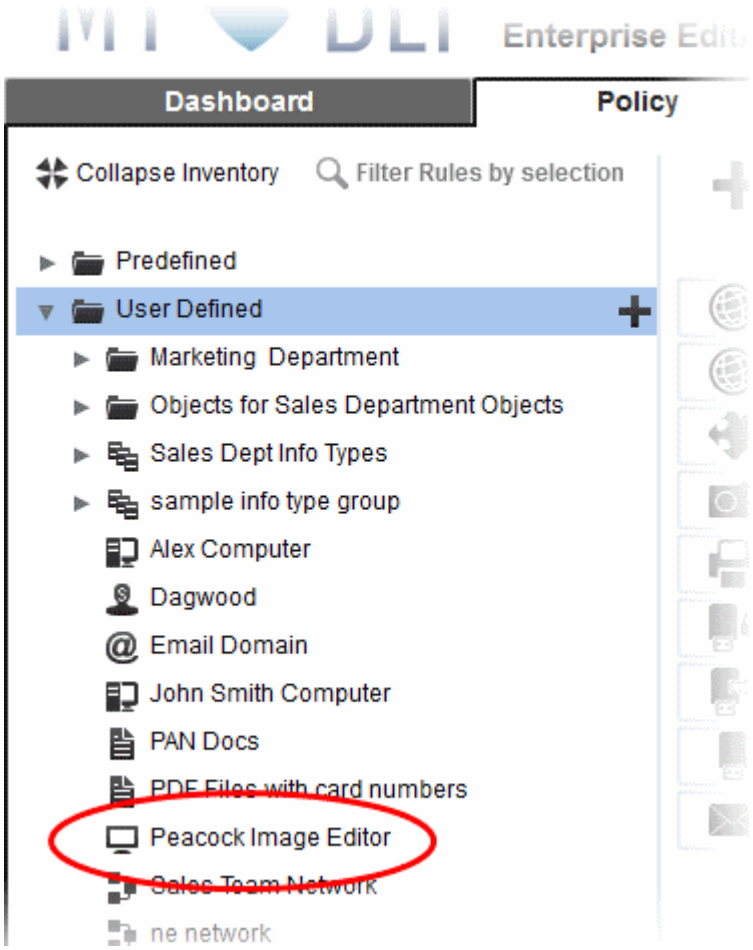


3. Select 'Application Name'. The 'Edit Dialog' will appear.



4. 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.
5. Click 'Save'.

The new user defined application will be listed under 'User Defined'/Category folder in the LHS pane of the 'Policy' interface, and can be dragged to be added as destination for Screenshot rule.



4.3.9. 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. 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.

The users can be added in two ways:

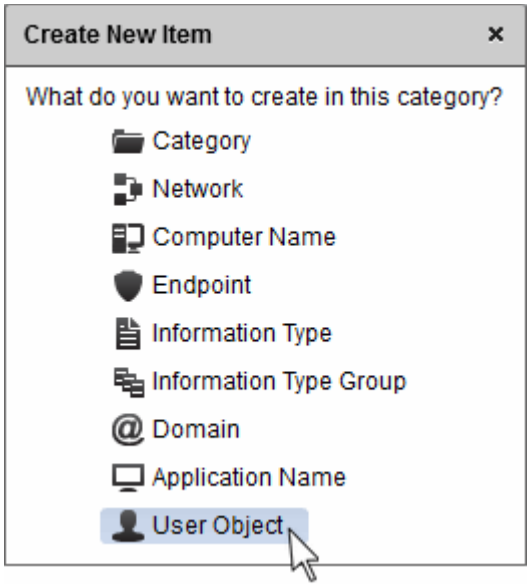
- Single users can be manually added by specifying the network login username of the user
- Multiple users can be added at once by importing from Active Directory (AD). The AD domain is to be integrated to the MyDLP server prior to importing from the AD. Refer to the section **Integration with Active Directory Domain** for more details.

Note: The 'User' objects can be used only as 'Source' in the data transfer policy rules, hence they can be created and viewed only from the 'Policy' interface.

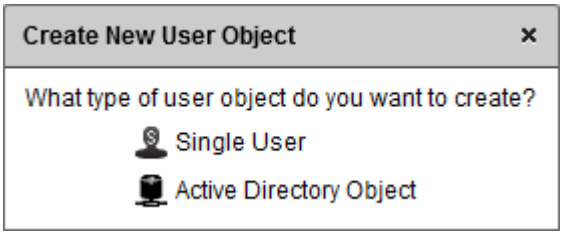
To add a new user

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the new user/users, from the left hand side pane of 'Policy' interface.

2. Click the plus icon  that appears on the selected folder stripe. The 'Create New Item' dialog will appear.



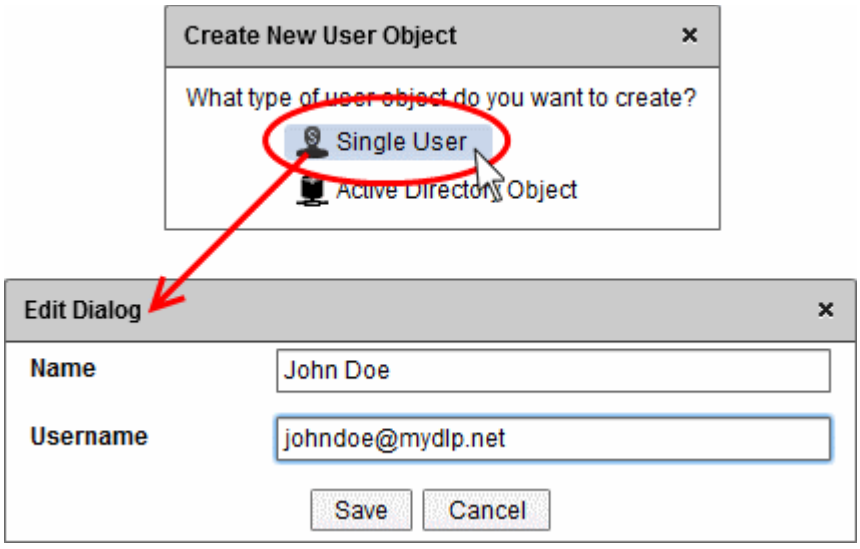
3. Select 'User Object'. The 'Create New User Object' will appear.



4. Select whether you wish to add a single user or import users from an AD domain. The following sections explain the processes in detail.
    - **Adding a Single User**
    - **Importing a user from the AD domain**

Adding a Single User

5. Select Single User from the Create New User Object. The Edit Dialog will appear.



6. Enter the parameters:
    - Name - Enter the name to identify the user
    - Username - Enter the username of the user. The user name can be entered in to 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.

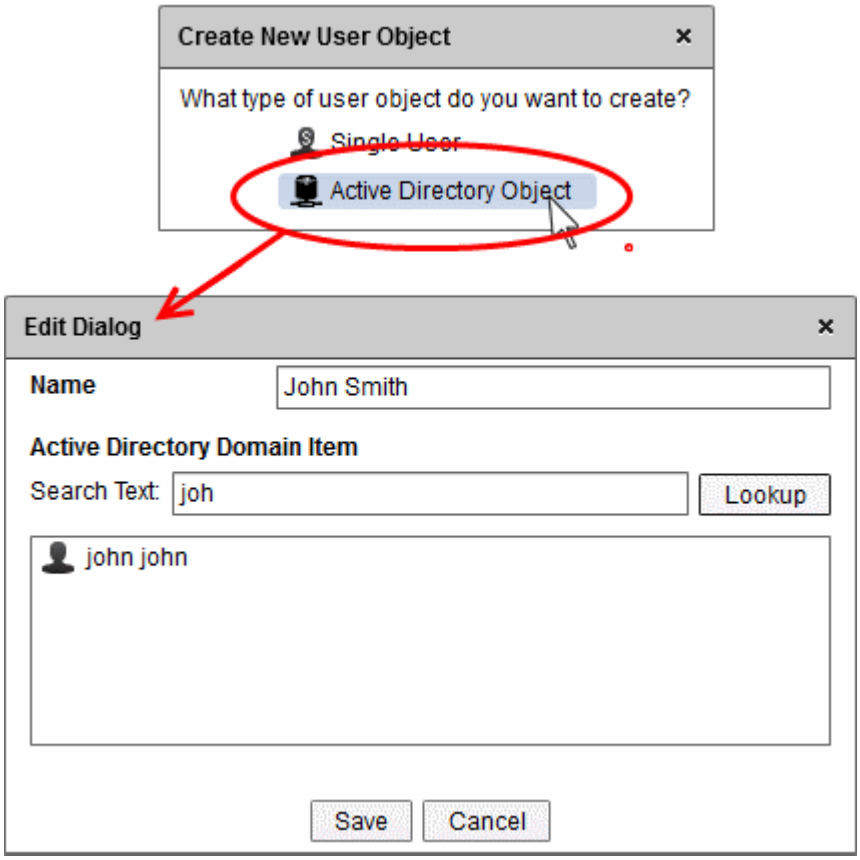
Tip: The user is currently logged-in, the username can be obtained from the 'Endpoints' interface. Refer to the section **The Endpoints Tab** for more details.

7. Click 'Save'.

The new user will be listed under 'User Defined'/Category folder in the LHS pane of the 'Policy' interface, and can be dragged to be added as source for various data transfer policy rules.

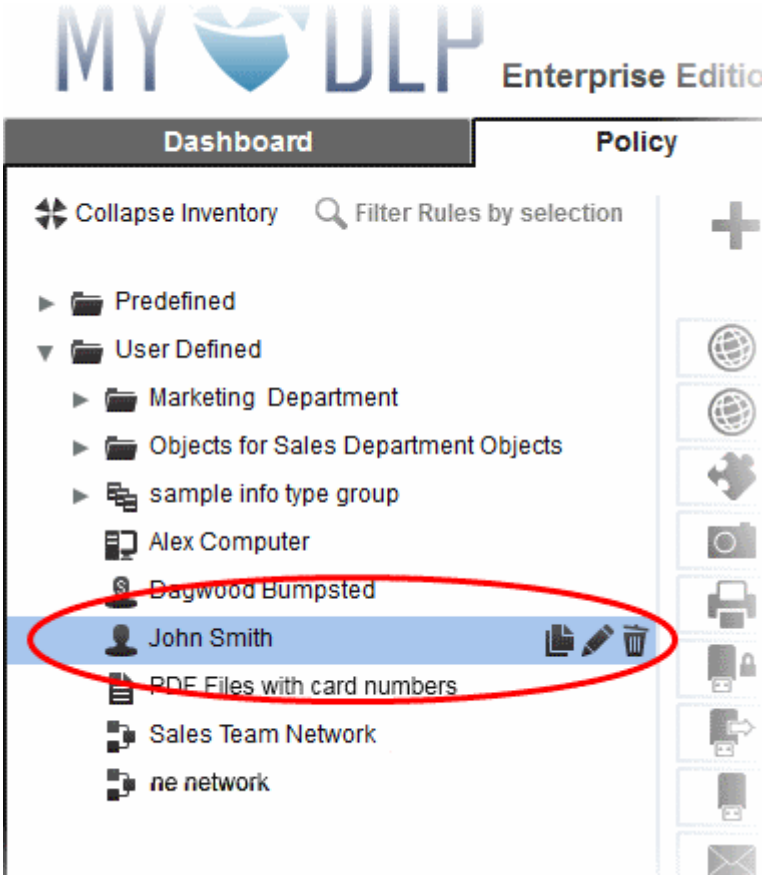
Importing User from AD domain

5. Select 'Active Directory Object' from the 'Create New User Object' dialog. The Edit Dialog will appear.



6. Enter the name to identify the user in the 'Name' field.
7. To search for the specific user from the pre-integrated AD Server, type the first three 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.
8. Choose the user to be added.
9. Click 'Save'.

The new user will be listed under 'User Defined'/Category folder in the LHS pane of the 'Policy' interface, and can be dragged to be added as source for various data transfer policy rules.



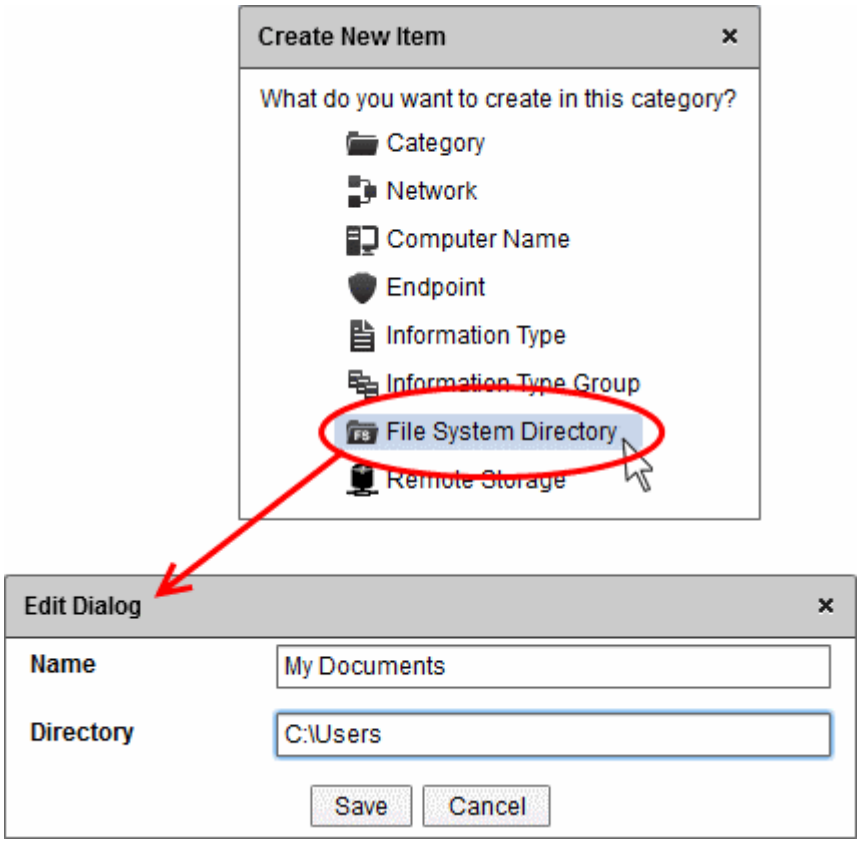
4.3.10. Adding a User Defined File System Directory

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**.

Note: The 'File System Directory' objects can be used only as 'Destination' in the Endpoint Discovery rules, hence they can be created and viewed only from the 'Discovery' interface.

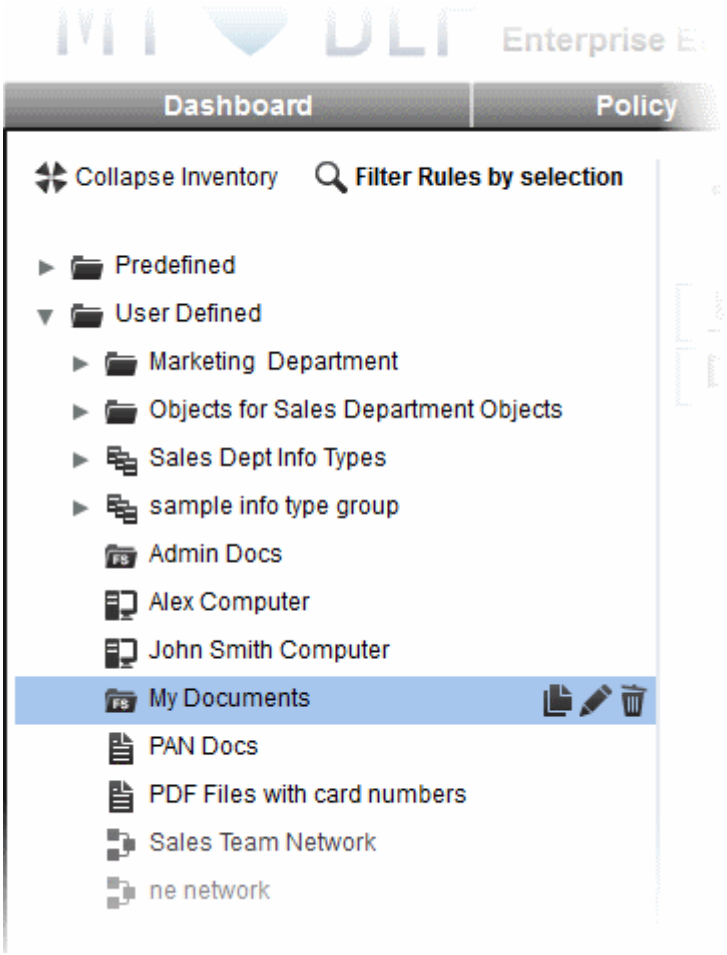
To add a custom file system directory

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the new user/users, from the left hand side pane of 'Discovery' interface.
2. Click the plus icon that appears on the selected folder stripe. The 'Create New Item' dialog will appear.
3. Select 'File System Directory'. The 'Edit Dialog' will appear.



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

The new user defined file system directory object will be listed under 'User Defined'/Category folder in the LHS pane of the 'Discovery' interface, and can be dragged to be added as destination for Endpoint Discovery rule.



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.

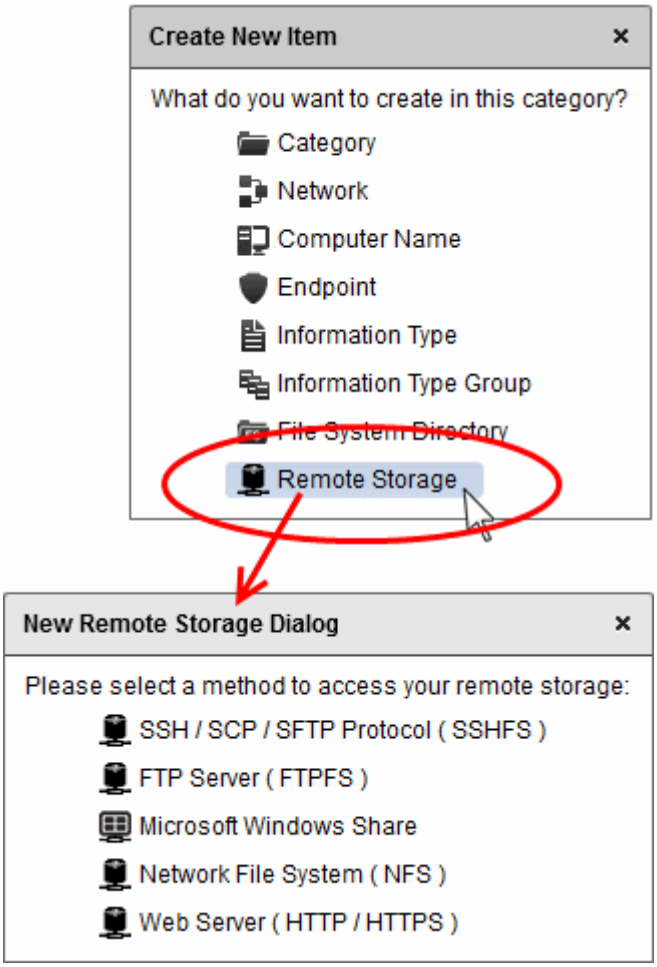
4.3.11. Adding a User Defined Remote Storage

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**.

Note: The 'Remote Storage' objects can be used only as 'Sources' in the Remote Storage rules, hence they can be created and viewed only from the 'Discovery' interface.

To add a new Remote Storage object

1. Select the 'User Defined' folder or the category/sub-category within which you wish to add the new remote storage object, from the left hand side pane of 'Discovery' interface.
2. Click the plus icon that appears on the selected folder stripe. The 'Create New Item' dialog will appear.
3. Select 'Remote Storage'. The 'New Remote Storage Dialog will appear.

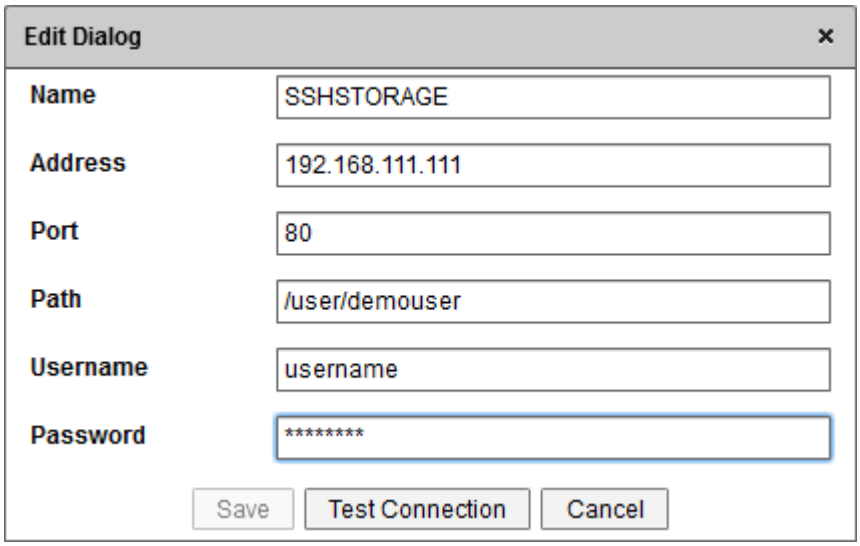


4. Choose the type of the remote storage you wish to specify for the object The following sections explain the processes in detail.
    - **SSH / SCP / SFTP Protocol**
    - **FTP Server**
    - **Microsoft Windows Share**
    - **Network File System**
    - **Web Server**

Adding a Remote Storage connected through SSH / SCP / SFTP Protocol

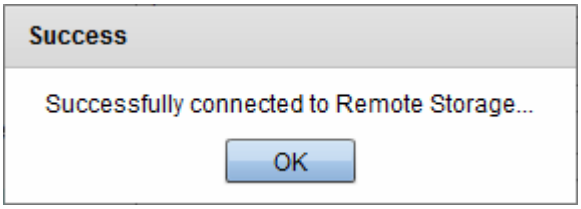
You can add a remote storage accessed through Secure Shell (SSH) connection, using Secure Copy (SCP) or Secure File Transfer Protocol (SFTP) protocol for file transfer as a remote storage object by selecting SSH / SCP / SFTP Protocol.

5. Choose SSH / SCP / SFTP Protocol from the New Remote Storage dialog



6. Enter the parameters:
    - Name - Enter a name shortly describing the remote storage
    - Address - Enter the IP address or hostname of the server/host, hosting the remote storage
    - Port - Enter the connection port for SSH connection to the server/host
    - 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

7. Click 'Test Connection'. MyDLP willl check whether the remote storage location is reachable. On successful connection, the 'Save' button will be enabled.



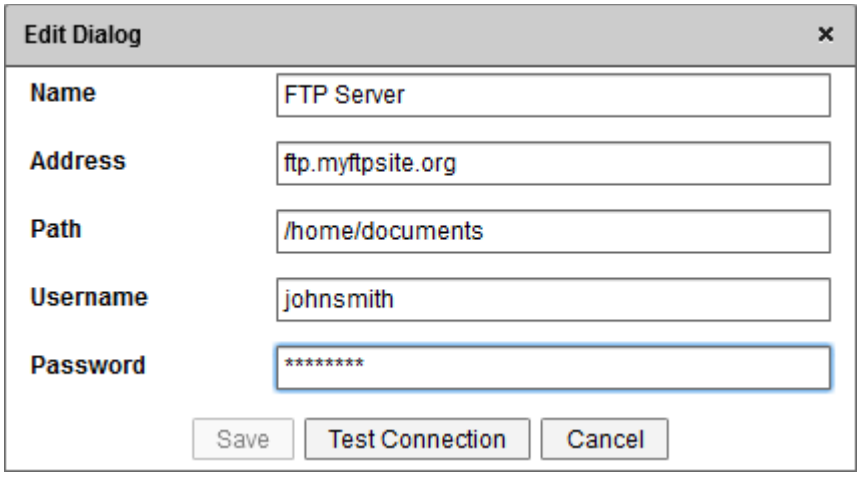
8. Click 'Save'.

The SSH / SCP / SFTP remote storage object will added to the 'User Defined'/Category folder in the LHS pane of the 'Discovery' interface, and can be dragged to be added as source for Remote Storage Discovery rule.

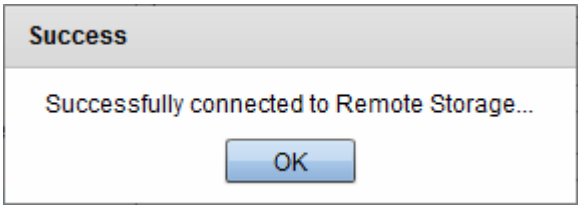
Adding a FTP Server

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

5. Choose 'FTP Server (FTPFS)' from the 'New Remote Storage dialog'. The 'Edit Dialog' will appear.



6. 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
7. Click 'Test Connection'. MyDLP will check whether the remote storage location is reachable. On successful connection, the 'Save' button will be enabled.



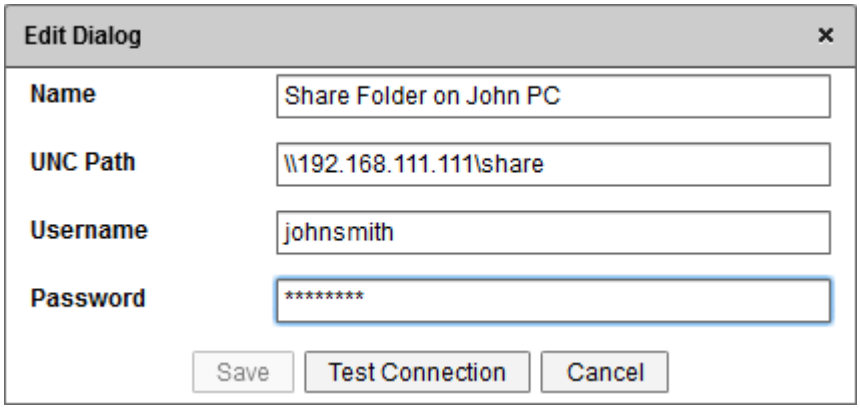
8. Click 'Save'.

The FTP server will be added as Remote Storage object to the 'User Defined'/Category folder in the LHS pane of the 'Discovery' interface, and can be dragged to be added as source for Remote Storage Discovery rule.

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.

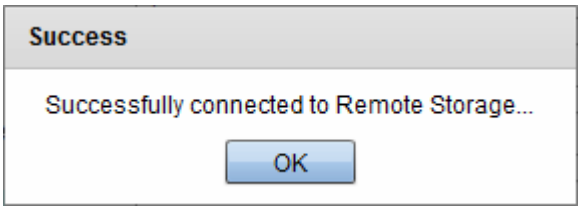
5. Choose 'Microsoft Windows Share' from the 'New Remote Storage dialog'. The 'Edit Dialog' will appear.



6. 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

7. Click 'Test Connection'. MyDLP willl check whether the remote storage location is reachable. On successful connection, the 'Save' button will be enabled.



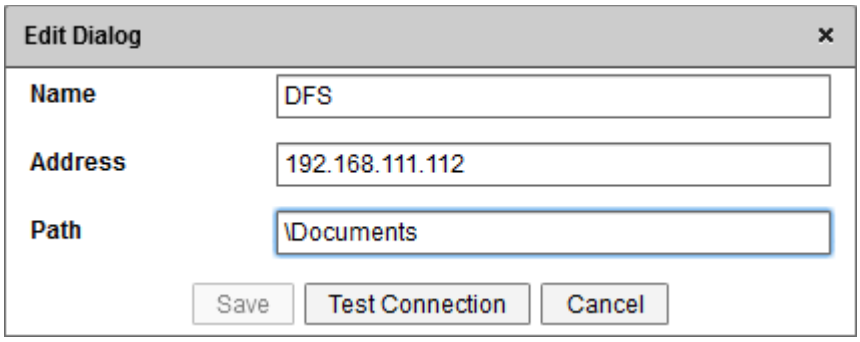
8. Click 'Save'.

The shared drive/folder will be added as a remote storage object to the 'User Defined'/Category folder in the LHS pane of the 'Discovery' interface, and can be dragged to be added 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.

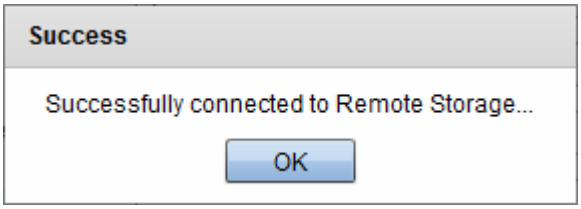
5. Choose 'Network File System (NFS)' from the 'New Remote Storage dialog'. The 'Edit Dialog' will appear.



6. 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

7. Click 'Test Connection'. MyDLP willl check whether the remote storage location is reachable. On successful connection, the 'Save' button will be enabled.



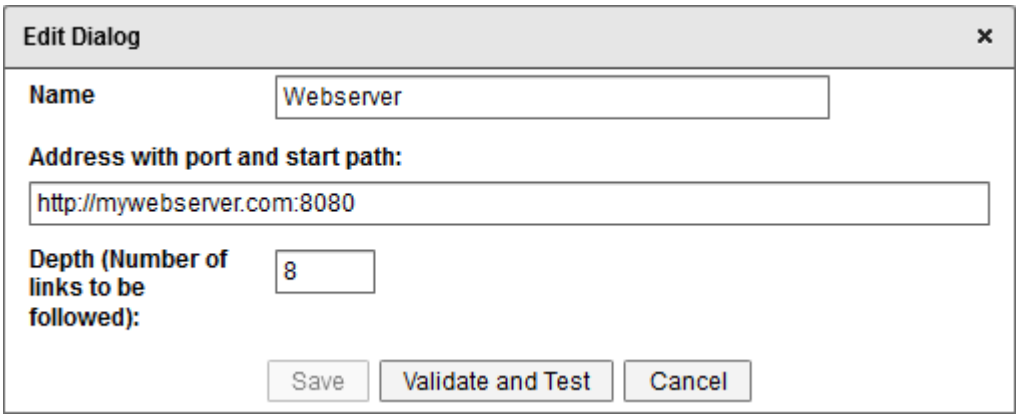
8. Click 'Save'.

The NFS will be added as a remote storage object to the 'User Defined'/Category folder in the LHS pane of the 'Discovery' interface, and can be dragged to be added 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.

5. Choose 'Web Server (HTTP / HTTPS)' from the 'New Remote Storage dialog'. The 'Edit Dialog' will appear.



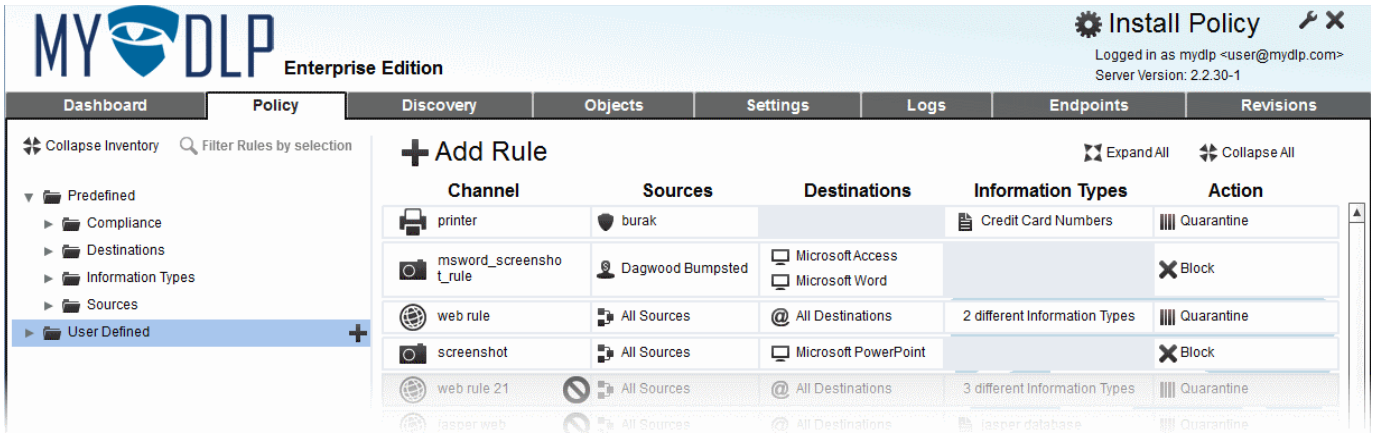
6. Enter the parameters:
    - Name - Enter a name shortly describing the Web server
    - Address with port and start path - Enter the URL or IP Address of the web server with its HTTP or HTTPS connection port and root path in the format <domain name or IP address>:<port>/<index page>
    - Depth (Number of links to be followed) - Enter the number of level of sub folders from the root to check in the web server
7. Click 'Validate and Test'. MyDLP will check whether the web server is reachable. On successful connection, the 'Save' button will be enabled.
8. Click 'Save'.

The web server will be added as Remote Storage object to the 'User Defined'/Category folder in the LHS pane of the 'Discovery' interface, and can be dragged to be added as source for Remote Storage Discovery rule.

5. Enforcing the Data Transfer Policy

MyDLP applies the data transfer control schemes for endpoints in your network as a policy. 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, 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, forbidding screenshots for specified application(s), to prohibit printing of documents containing sensitive data.

The 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**.

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

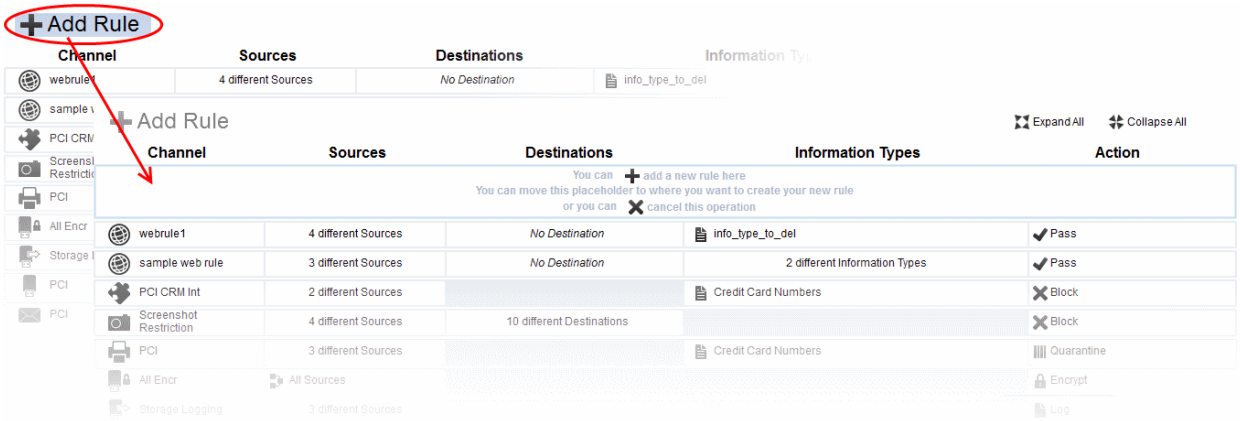
5.1. Adding Policy Rules

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

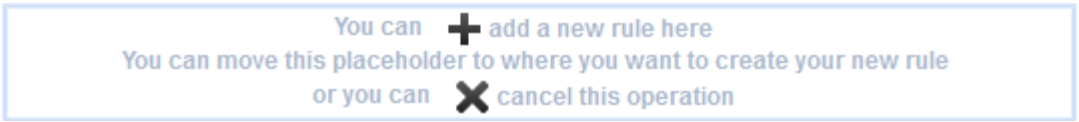
- **Step 1 - Create a place holder for the new rule and drag it to the required position in the list**
- **Step 2 - Add the new rule and select the type of the rule**
- **Step 3 - Enter a name for the rule and configure messages to be shown to the enduser and email notification sent to the administrator when the rule intercepts the data traffic**
- **Step 4 - Specify the sources for the rule**
- **Step 5 - Specify the Destinations for the rule**
- **Step 6 - Specify the 'Information Types' to be identified and intercepted in the data traffic**
- **Step 7 - Specify the action to be taken on the data if the rule is met**

Step 1 - Create a Place Holder

- Click the 'Add New Rule'. If you newly installed MyDLP and haven't added any rules, the 'Add Rule' control will appear at the center of the interface.



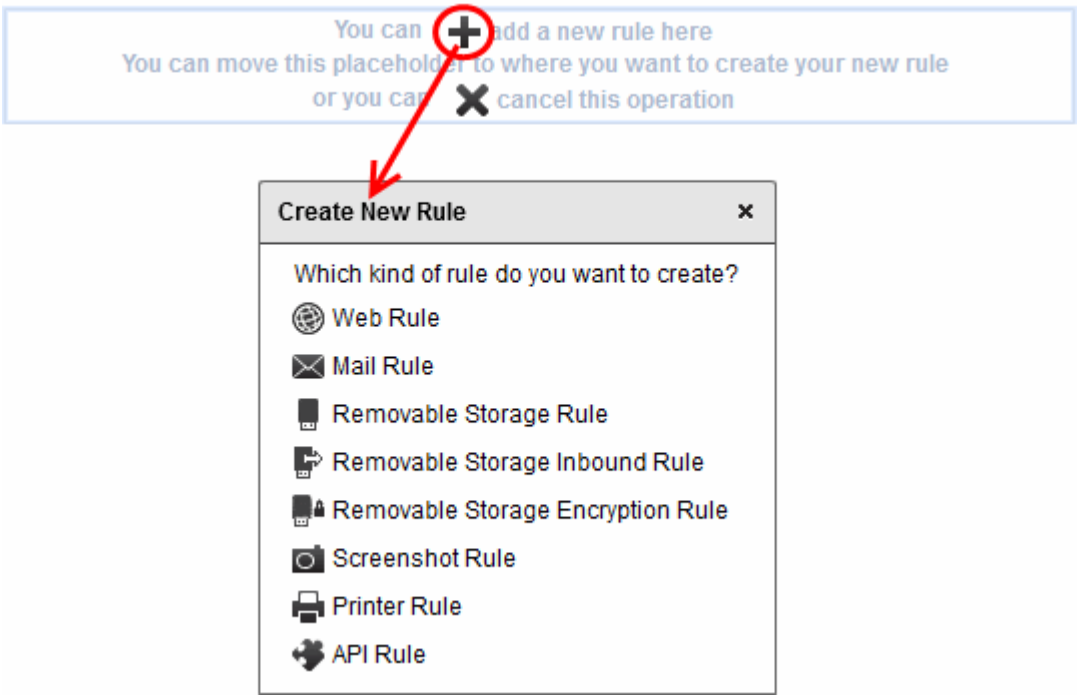
A new place holder box for the new rule will appear.



- Drag the box to the desired position in the list, depending on the nature of the rule. The rules at the top of the list 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.

Step 2 - Add the new rule and select the type of the rule

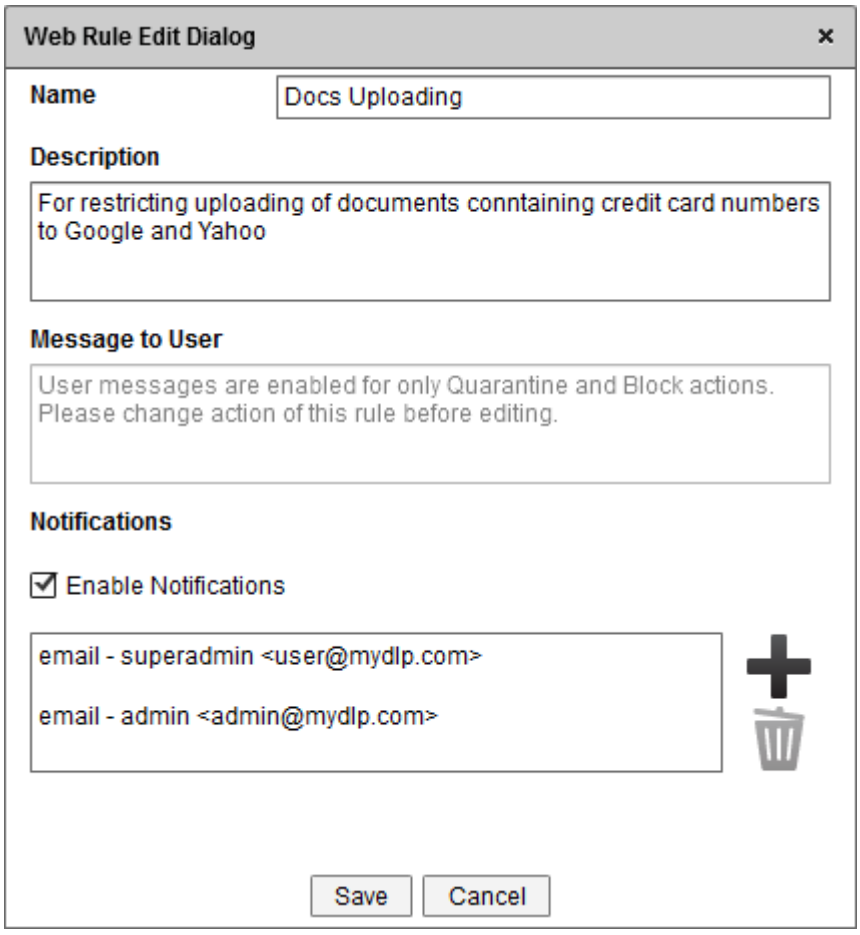
- Click the plus button in the box to add the new rule. The 'Create New Rule' dialog will appear.



- Select the type of the rule to be created. For more details on Rule Types, refer to the section **Rule Types**.

Step 3 - Enter Name for the rule and configure Messages and Notifications

On selecting the rule type from the Create New Rule dialog, the Rule Edit Dialog will appear. The 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

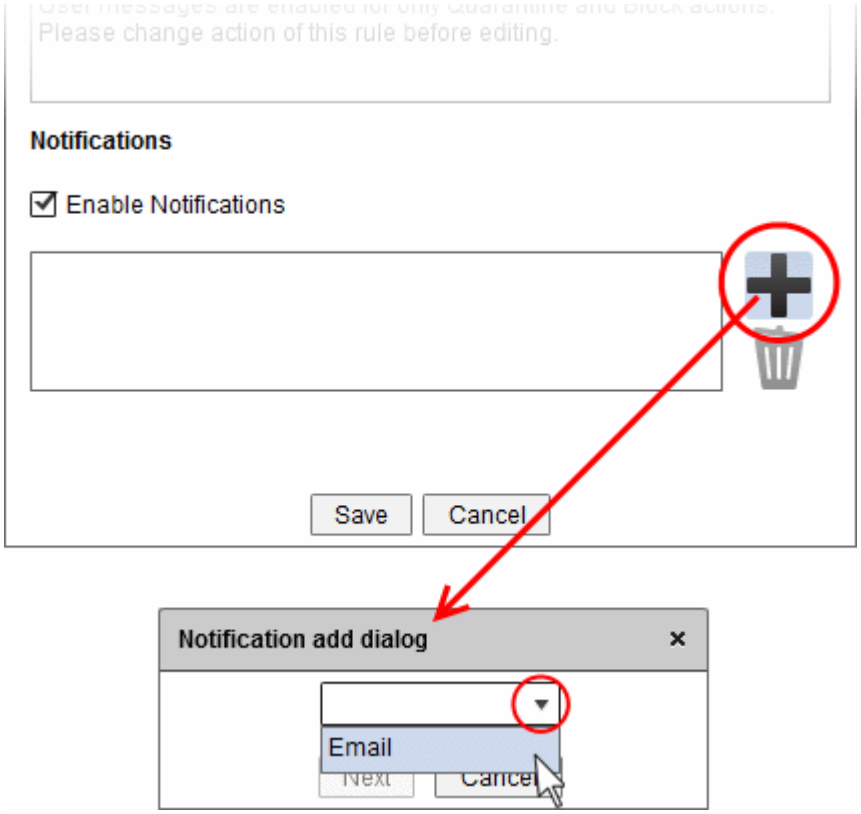
  The message will be displayed only if the action set for the rule is to block or quarantine the intercepted file. Hence this field will be enabled only after setting the action for the rule as BLOCK or QUARANTINE. You can leave this field blank at this time and add the message later time by editing the rule, after setting the action.

  - For more details on setting the action, refer to the description under 'Step 7 - 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 enduser, 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 **Enterprise Tab** for more details.

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

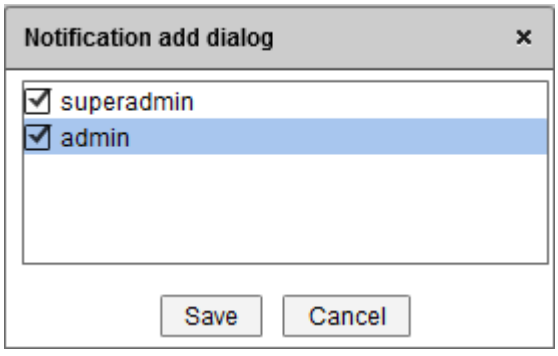
  - Web Rule
  - Mail Rule
  - Removable storage rule
  - Printer rule
  - API rule

- For MyDLP to send automated notification messages, select the 'Enable Notifications checkbox'
- To add a notification type and recipients, click the plus button beside the text box.

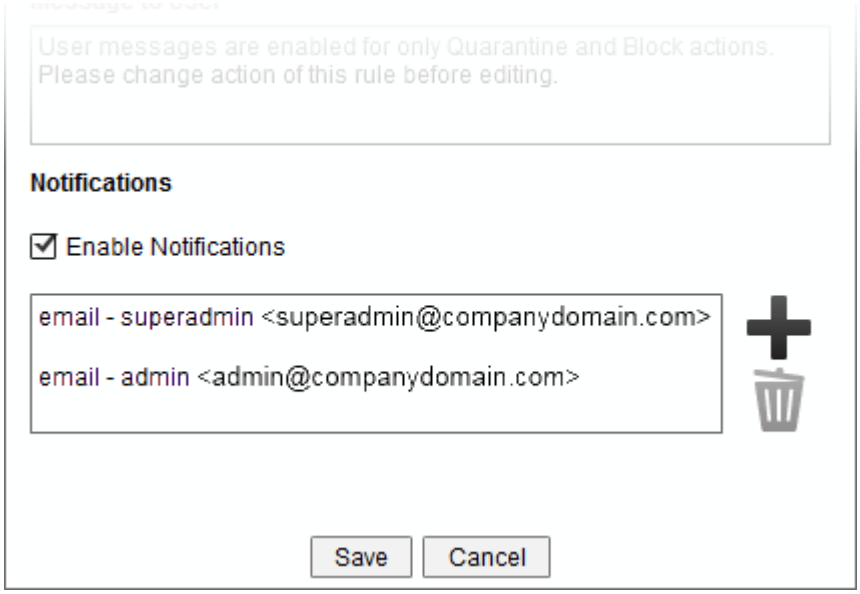


The 'Notification add dialog' will appear.

- Choose the notification type from the drop-down. Currently only 'Email' notification is available. More notification type will be added in the future versions.
- Click 'Next'.



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



- Repeat the process to add more types of notification types or administrative users
- Click 'Save'.

The rule will be added to the list, at the position of the place holder box.

Step 4 - Specify the sources for the rule

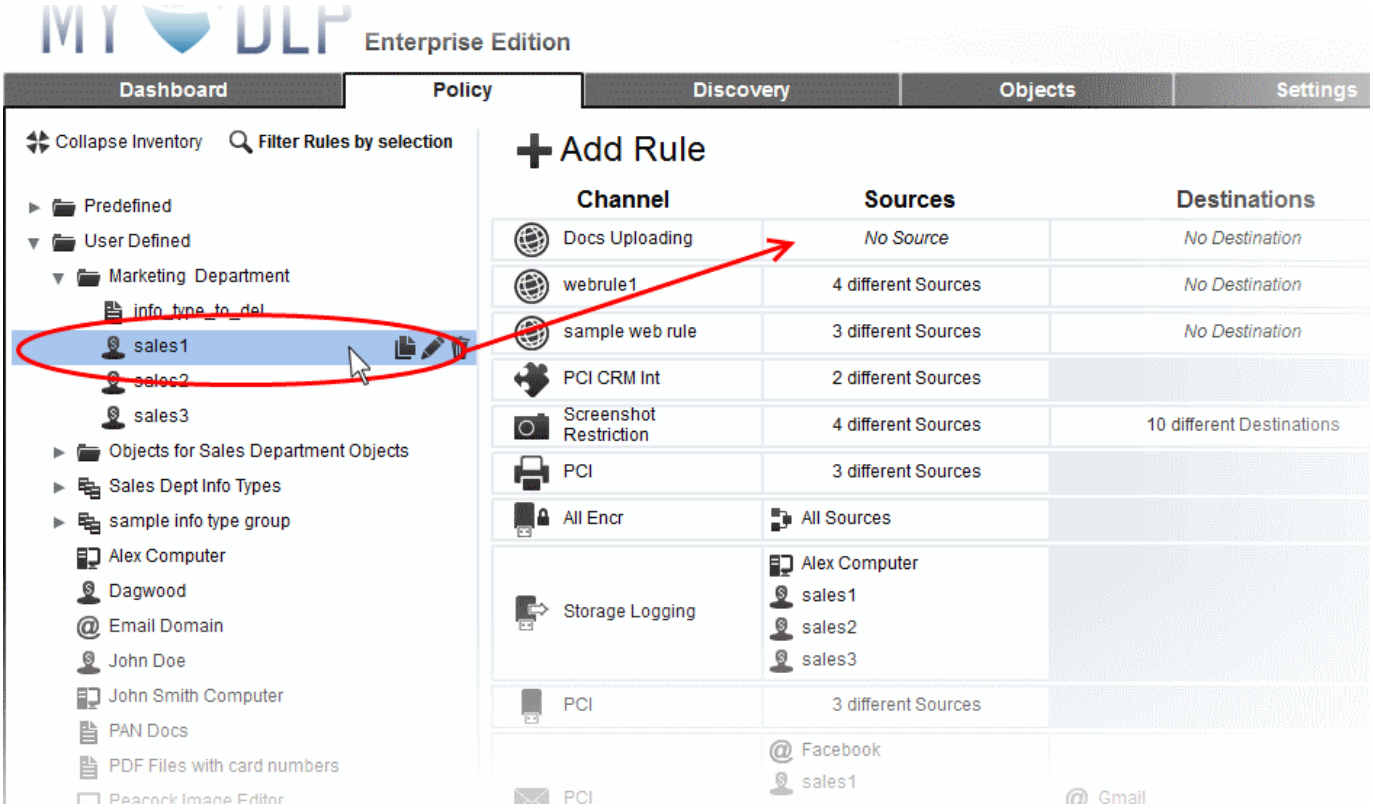
The origin of the data transfer can be added as the 'Source' component of the rule, by dragging a pre-defined or user-defined objects from the left hand side pane. The following table shows the object types that can be used for defining Sources and applicable rule types.

Object	Applicable Rule Types
Network	• Web Rule • Removable Storage Rule • Removable Storage Inbound Rule • Removable Storage Encryption Rule • Printer Rule • Screenshot Rule • API Rule
Computer Name	• Web Rule • Removable Storage Rule • Removable Storage Inbound Rule • Removable Storage Encryption Rule • Printer Rule • Screenshot Rule

Object	Applicable Rule Types
	• API Rule
Endpoint	• Web Rule • Removable Storage Rule • Removable Storage Inbound Rule • Removable Storage Encryption Rule • Printer Rule • Screenshot Rule • API Rule
Domain	• Web Rule • 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

To add a source object

- Expand the predefined, user defined or category folder containing the source you wish to add from the Objects tree in the LHS pane
- Drag the object and drop in the 'Sources' column of the newly added rule
- Repeat the process for adding more sources



You can drag and drop a category folder containing a number of source objects along with other objects so that all the objects that are applicable for sources for the rule, will be added to the rule.

You can add more source objects created after adding the rule, at a later time, by just dragging the object to the 'Sources' column of the rule.

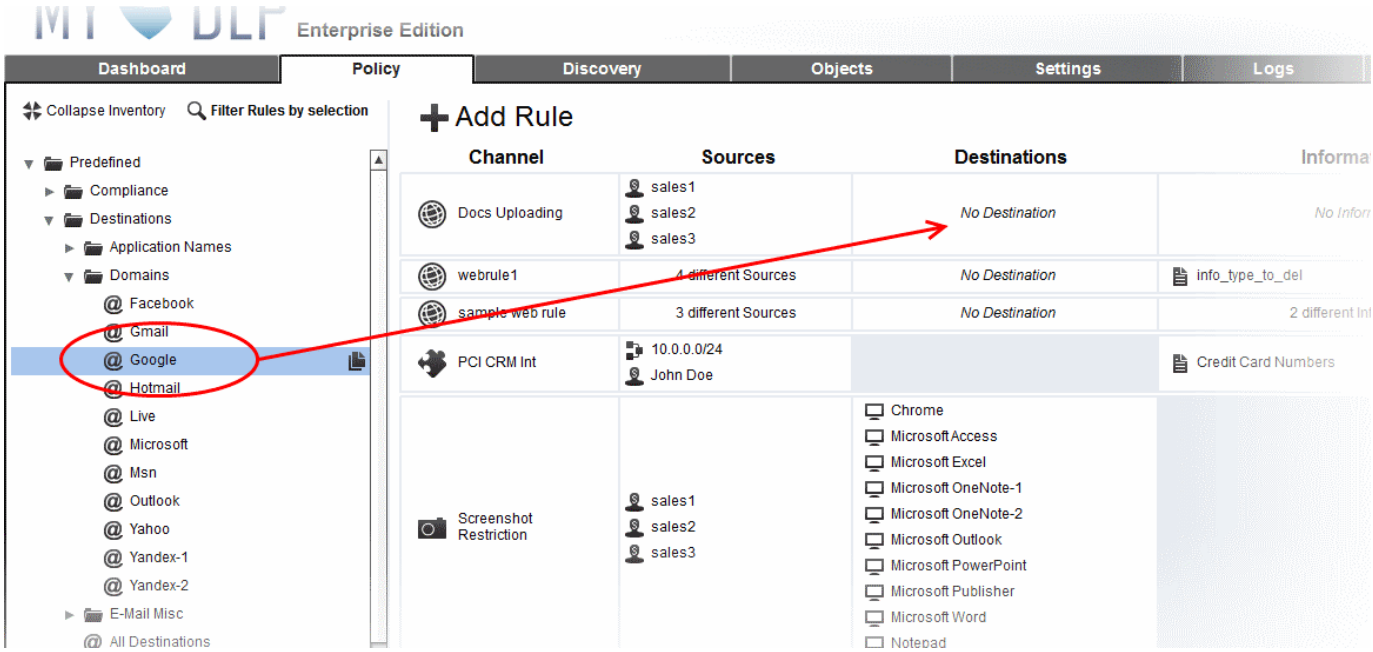
Step 5 - Specify the Destinations for the rule

The target of the data transfer can be added as the 'Destination' component of the rule, by dragging a pre-defined or user-defined destination objects from the left hand side pane. 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

To add a destination object

- Expand the predefined, user defined or category folder containing the destination object you wish to add from the Objects tree in the LHS pane
- Drag the object and drop into the 'Destinations' column of the newly added rule
- Repeat the process for adding more destinations



You can drag and drop a category folder containing a number of destination objects along with other objects so that all the objects that are applicable for destinations for the rule, will be added to the rule.

You can add more destination objects created after adding the rule, at a later time, by just dragging the object to the 'Destinations' column of the rule.

Step 6 - 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 'Objects' tree. In addition, the administrator can add more number of custom information typed under 'User-defined' category.

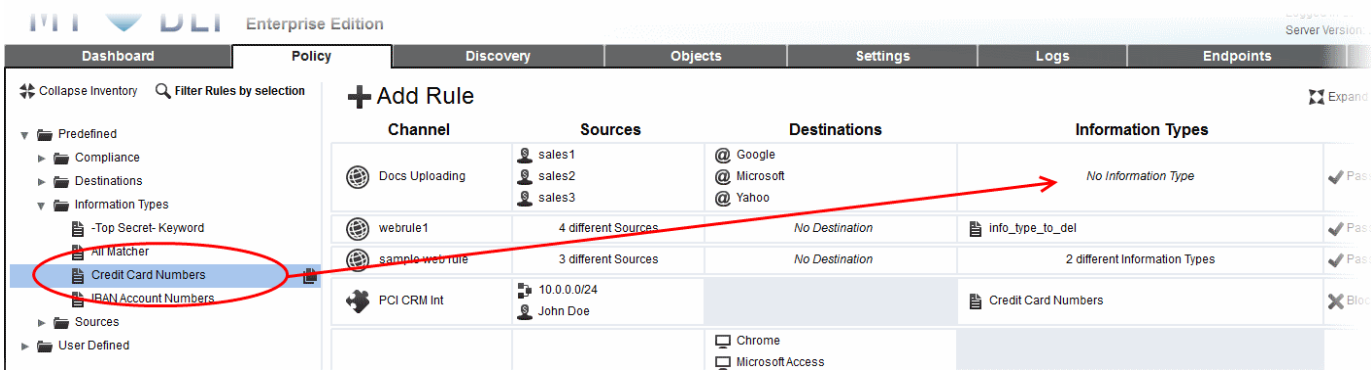
For MyDLP to intercept files containing sensitive data of specific type, the respective information type object is to be added to the rule. The following table shows the object types that can be used for defining Information Types and applicable rule types.

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

To add an Information Type object

- Expand the predefined, user defined or category folder containing the Information Type object you wish to add from the Objects tree in the LHS pane

- Drag the object and drop into the 'Information Types' column of the newly added rule
- Repeat the process for adding more Information Types

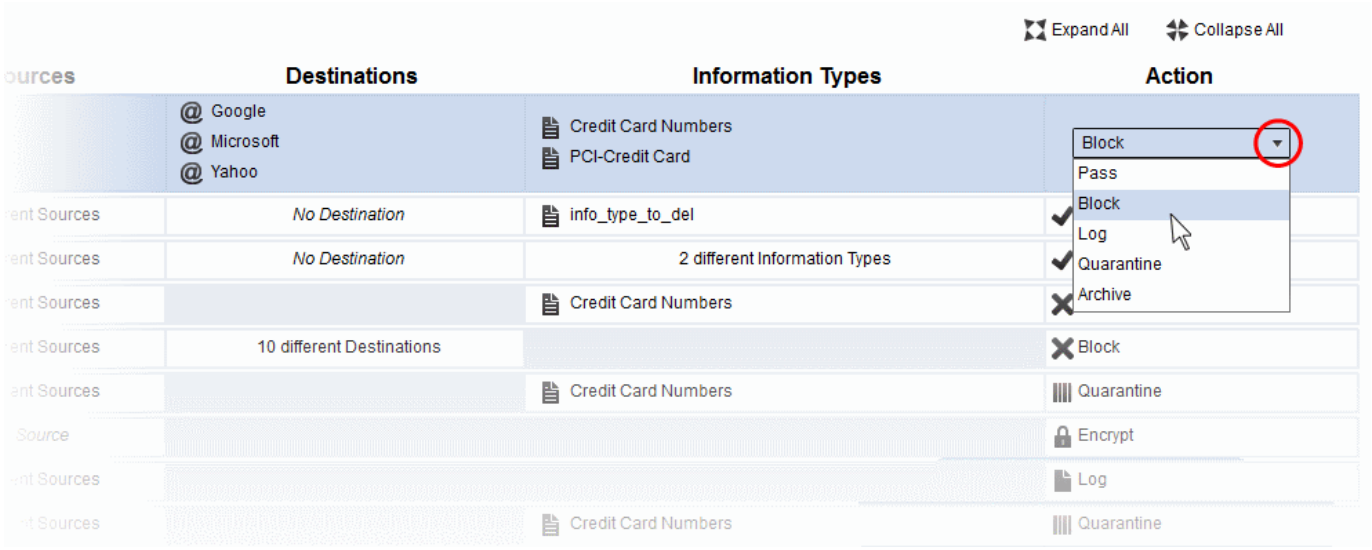


You can drag and drop a category folder containing a number of Information Types so that all the objects that are applicable for the rule, will be added to the rule.

You can add more Information Type objects created after adding the rule, at a later time, by just dragging the object to the 'Information Types' column of the rule.

Step 7 - 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 the drop-down in the 'Action' column. 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.
  - **LOG** - Allows information to pass through data channel but generates event log. This action is not available for screenshot rules.
  - **ARCHIVE** - Allows information to pass through data channel, generates event log and archives a copy of information. This action is not available for screenshot rule. The Administrator can download the file from the Logs interface. Refer to the section **Downloading the Files Archived by MyDLP** for more details.
  - **BLOCK** - Prevents information to pass through data channel and generates event log. This action is not available for removable storage inbound rules.
  - **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 rules and screenshot rules.

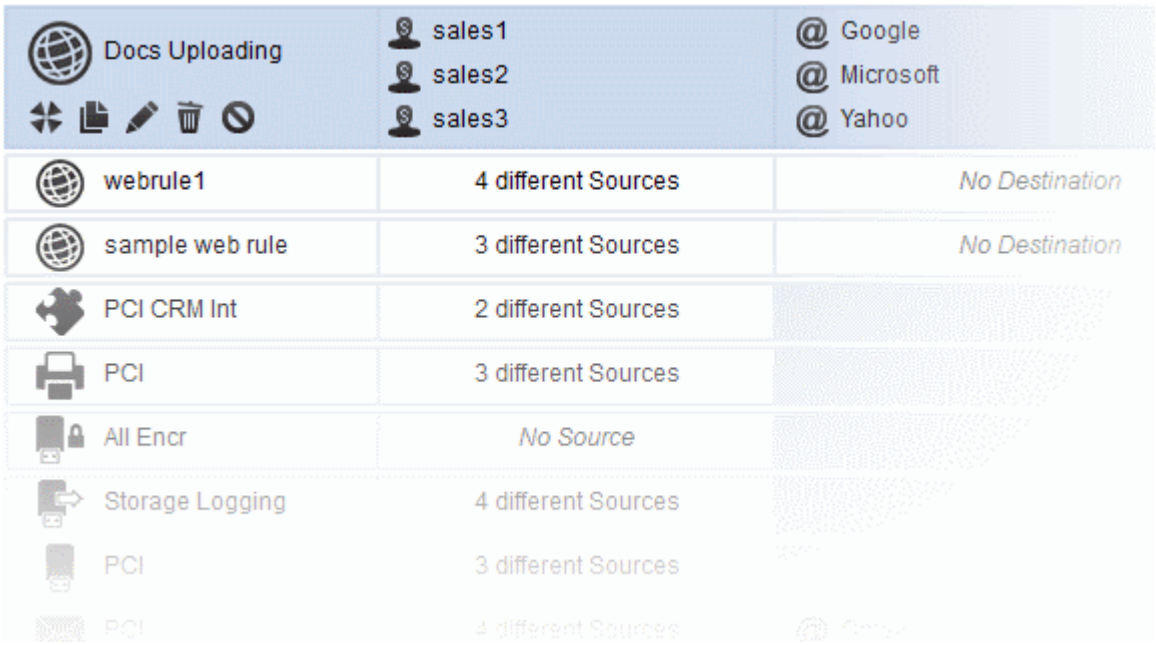
- **ENCRYPT** - Enforces encryption of connected removable devices. This action is only available for Removable Storage Encryption Rule.

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, copy delete, disable/enable it at any time.

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



Control	Description
/	Expands/Collapses the Rule stripe. In Expanded view, all the source, destination and information type components are listed in their respective columns.
	Clones the rule to create a new rule with minor changes in the components
	Enables the administrator to edit the name, message and notification settings of the rule. Refer to the section **Editing a Rule** for more details,
	Removes the rule from the policy. Refer to the section **Removing a Rule** for more details
	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.

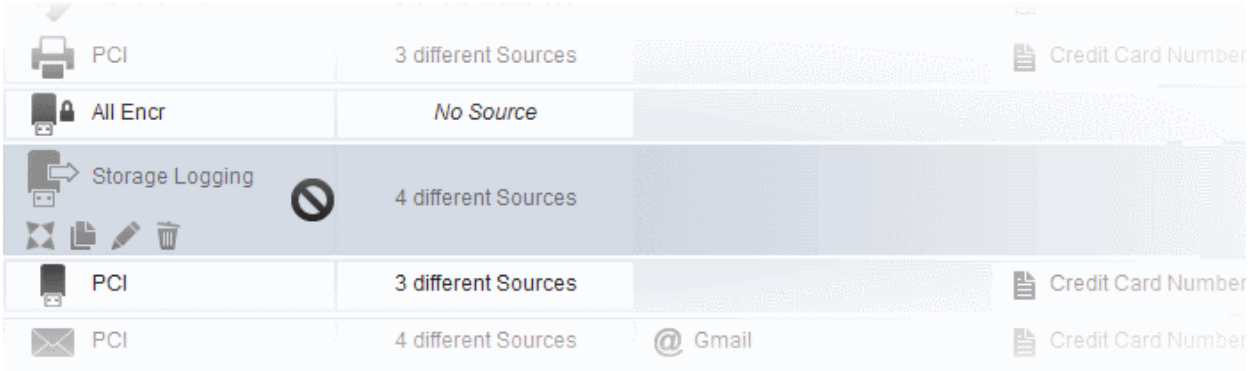
5.2. Enabling or Disabling a Rule

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.

To 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.



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

5.3. 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. The following sections provide more information on:

- **Editing the name and Notification Settings**
- **Removing an object from a rule**
- **Adding an object to the rule**

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.

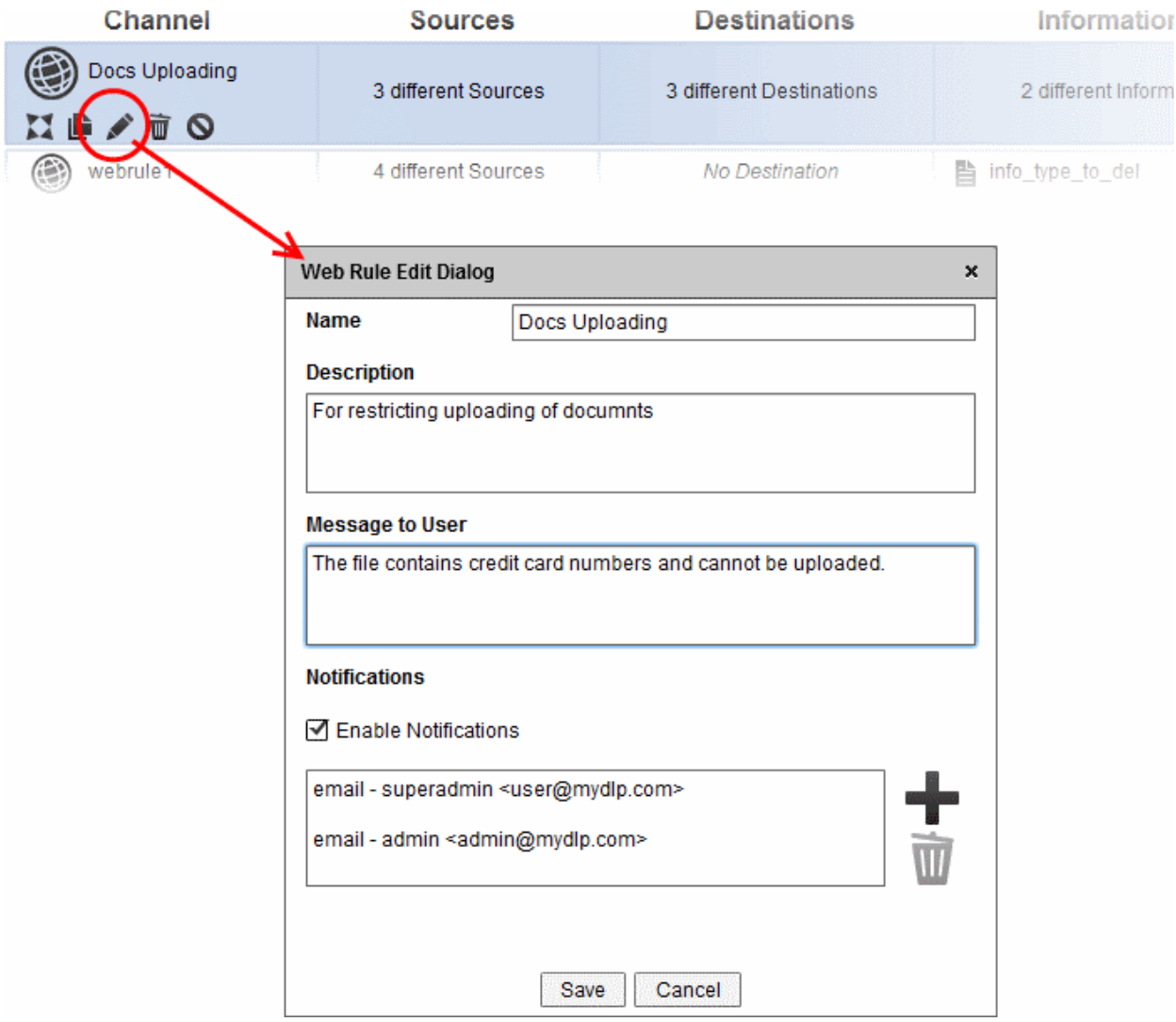
Editing the name and Notification Settings

The administrator can change the name of a rule, description and the notification settings from the 'Edit Dialog'.

The Message to be displayed to the end-user, when the MyDLP blocks or quarantines a file in the data transfer from the user based on the rule, can be added through the 'Edit Dialog'.

To edit a rule

- Click on the rule for the options to be displayed in the 'Channels' column.
- Click the pencil icon . The 'Edit Dialog' will open.



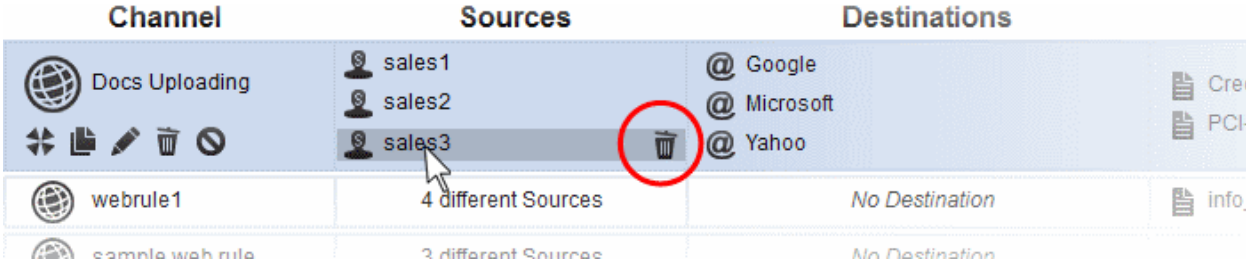
You can edit the 'Name', 'Description', 'Message to User' and Notification settings. The interface is same as the 'Edit Dialog' that appear while creating the rule. Refer to the description under **Step 3 - Enter a name for the rule and configure messages to be shown to the enduser and email notification sent to the administrator when the rule intercepts the data traffic** in the section **Adding Policy Rules** for more details.

Removing an object from a rule

The administrator can remove source, destination and information type objects that are not required for the rule, at any time.

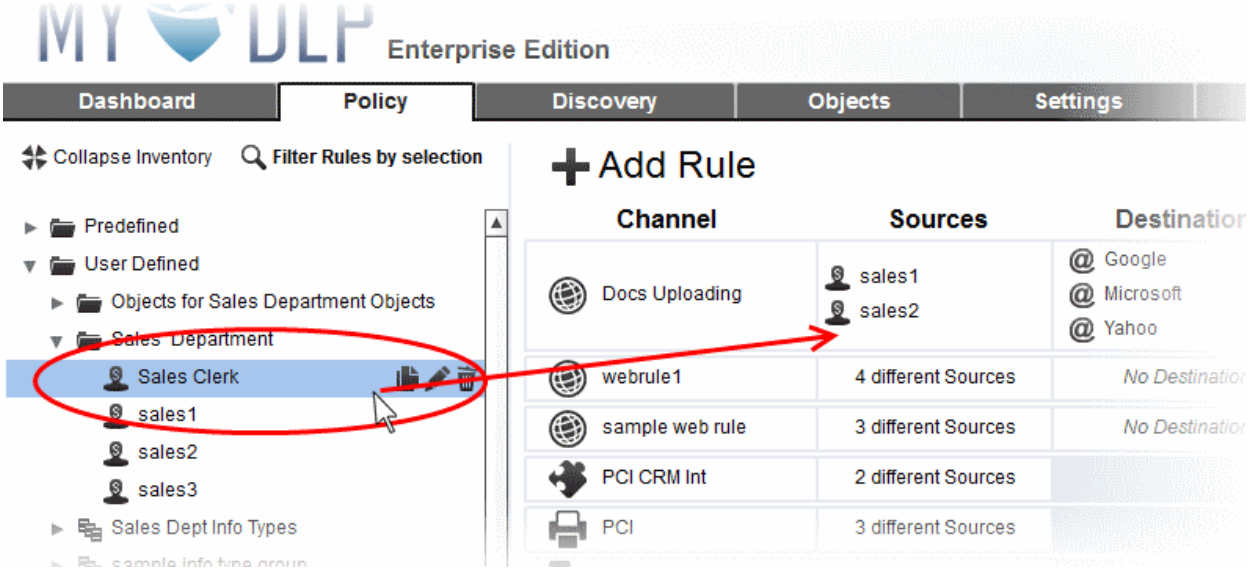
To remove an object

- Click on the rule for the options to be displayed in the 'Channels' column.
- Click the expand icon . All the objects added to the rule will be displayed under respective columns.
- Select the object to be removed. The 'Trash can' icon will be displayed.
- Click on the 'Trash can' icon to remove the object.



Adding an object to the rule

The administrator can add new source, destination and information type objects to a rule at any time, just by dragging the object from the left hand side pane and dropping to the respective column of the rule.



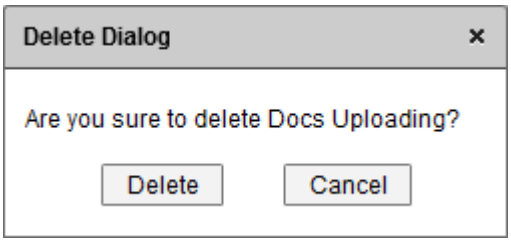
5.4. Removing a Rule

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

To remove a rule

- Click on the rule for the options to be displayed in the 'Channels' column
- Click the trash can icon .

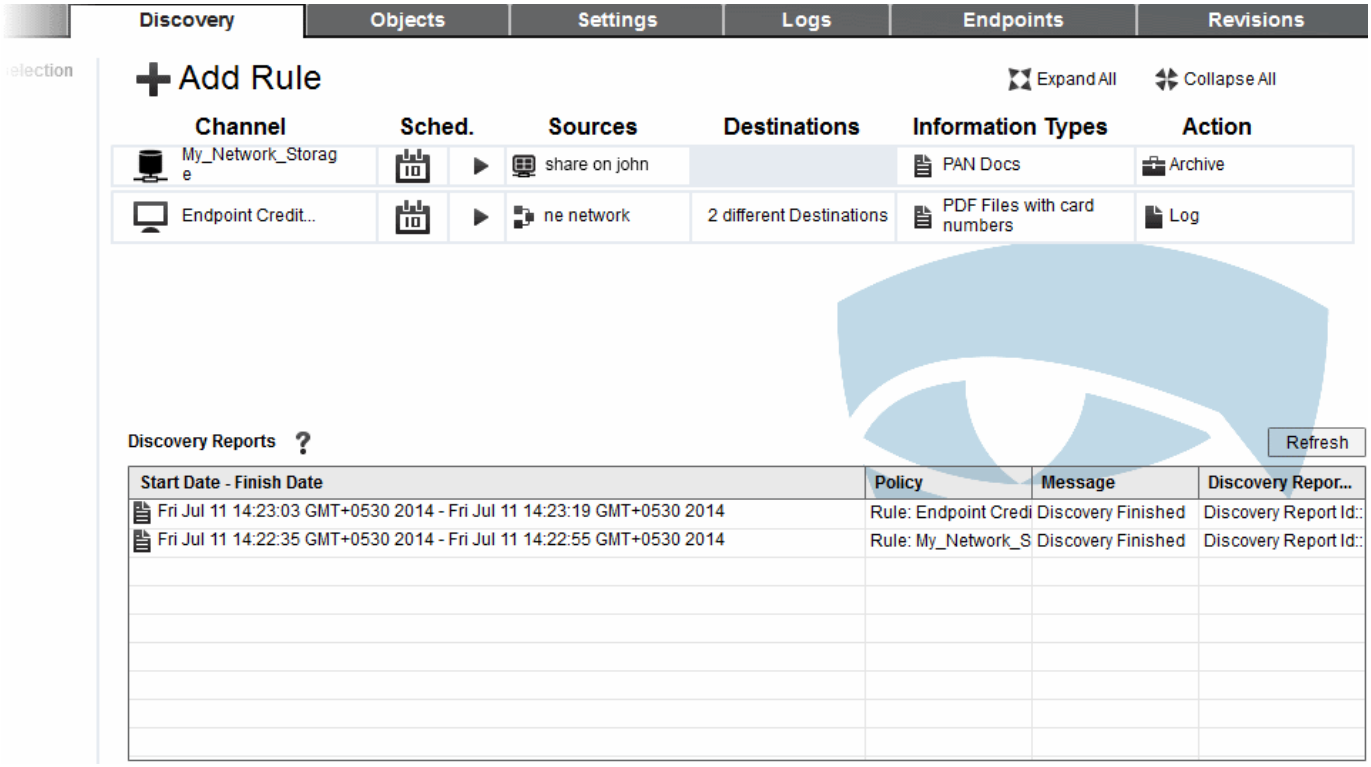
A confirmation dialog will be displayed.



- Click Delete to remove the rule

6. Configuring Data Discovery

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 main area of the interface displays all previously created rules. Collectively, these rules are known as the 'Discovery Policy' New rules can be created by clicking 'Add rule' and constructed by dragging objects from the left hand menu. Simply click on any rule to reveal controls which allow you to edit, clone, delete or disable a rule or rule component. The administrator can also run on-demand scans from this area. A list of reports from previous scans is available underneath the list of rules.

For more details on rule types and components, refer to **The Rules**.

The following sections provide more information on:

- **Managing Discovery Rules**
- **Viewing Discovery Scan Reports**

6.1. Managing Discovery Rules

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

The following sections provide more information on:

- **Adding Discovery Rules**
- **Running On-Demand Scans**

Once added, the rules can be enabled/disabled and edited in the same manner as the Data Transfer Control Policy rules. For more details, refer to the following sections in the previous chapter, **Enforcing the Data Transfer Policy**:

- Enabling or Disabling a Rule
- Editing a Rule
- Removing a Rule
- Deploying the Policy

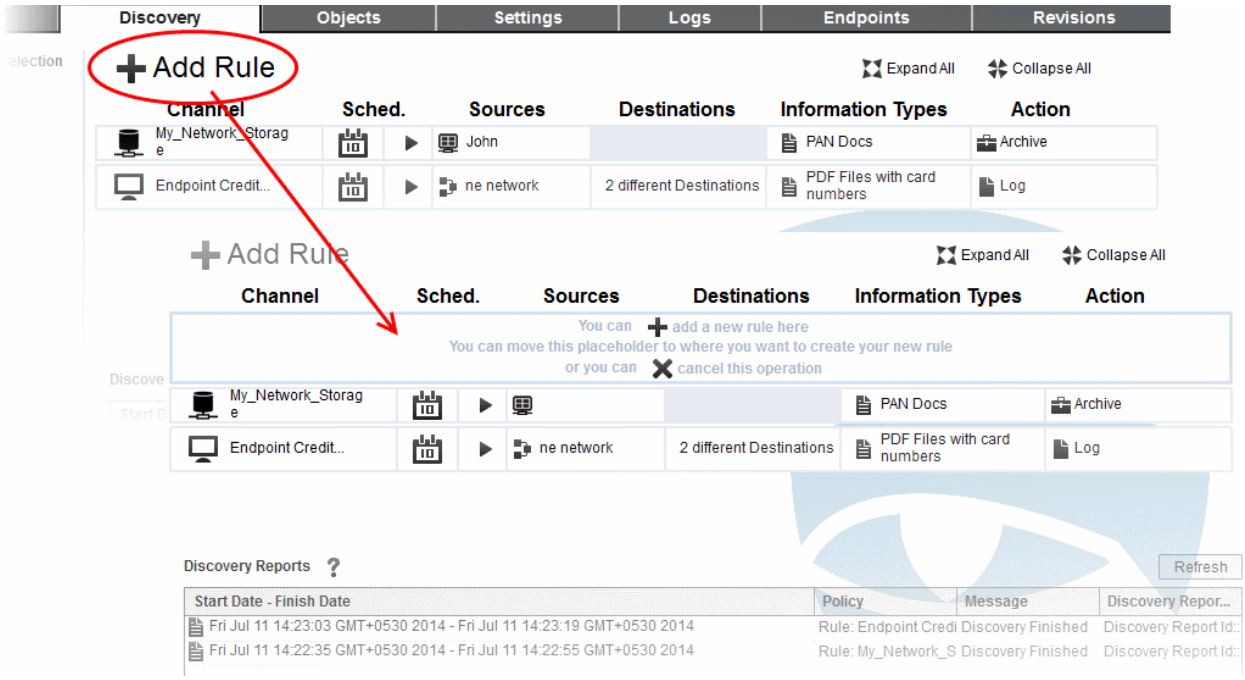
6.1.1. Adding Discovery Rules

Rules can be created and added to the Discovery Policy by the following steps. Each step is explained in detail after the brief descriptions:

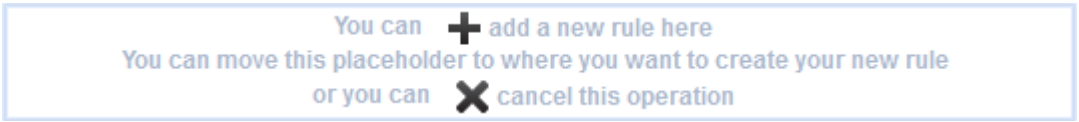
- Step 1 - Create a place holder for the new rule and drag it to the required position in the list
- Step 2 - Add the new rule and select the rule channel
- Step 3 - Enter a name for the rule and configure email notifications
- Step 4 - Specify the sources for the rule
- Step 5 - Specify the Destinations for the rule
- Step 6 - Specify the 'Information Types' to be identified
- Step 7 - Specify the action to be taken on the data if the rule is met
- Step 8 - Create a Schedule for running scans as per the rule

Step 1 - Create a Place Holder

- Click 'Add New Rule'. If you have not added any rules yet, the 'Add Rule' control will appear at the center of the interface.



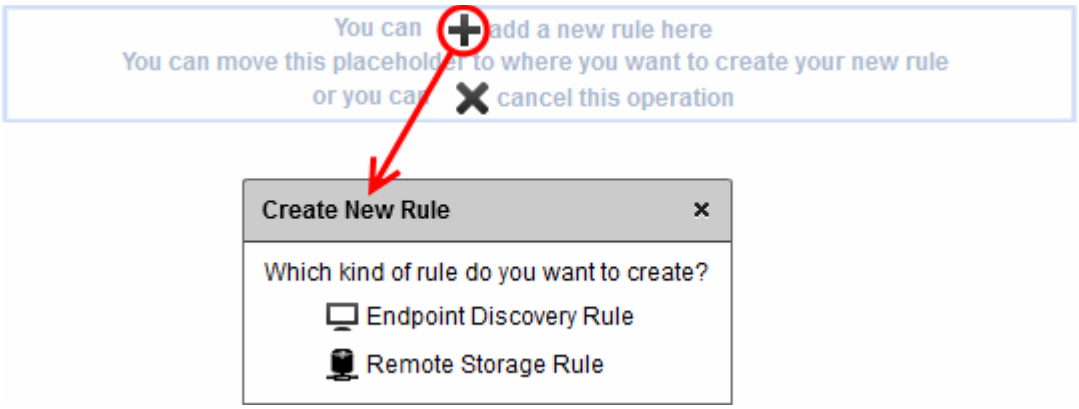
A new place holder box for the new rule will appear.



- Drag the box to the desired position in the list. The rules at the top of the list 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.

Step 2 - Add the new rule and select the rule channel

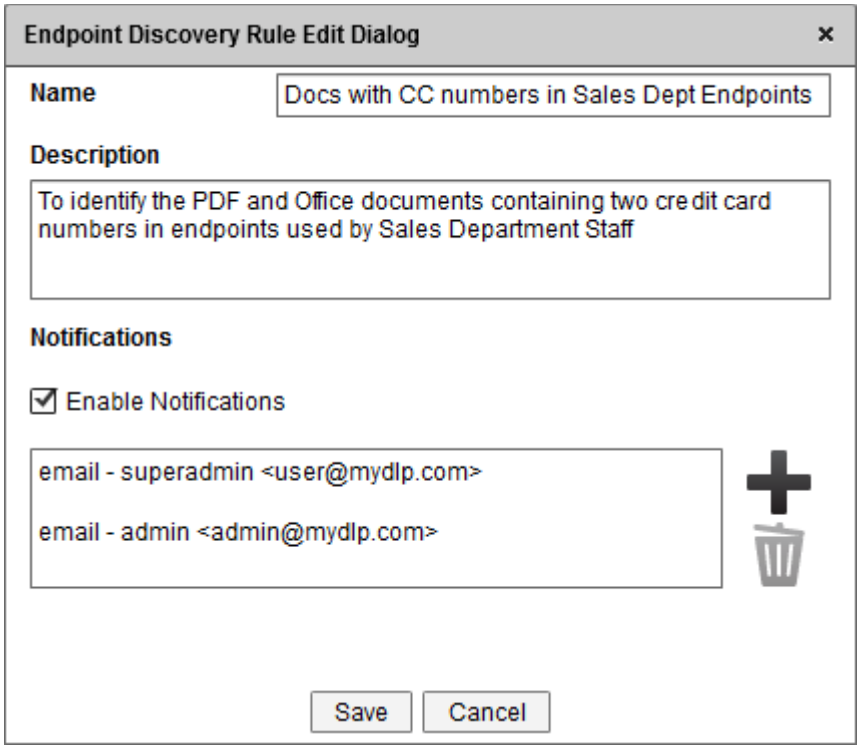
- Click the plus button in the box to add the new rule. The 'Create New Rule' dialog will appear.



- Select the type of the rule to be created. For more details on Rule Types, refer to the section **Rule Channels**.

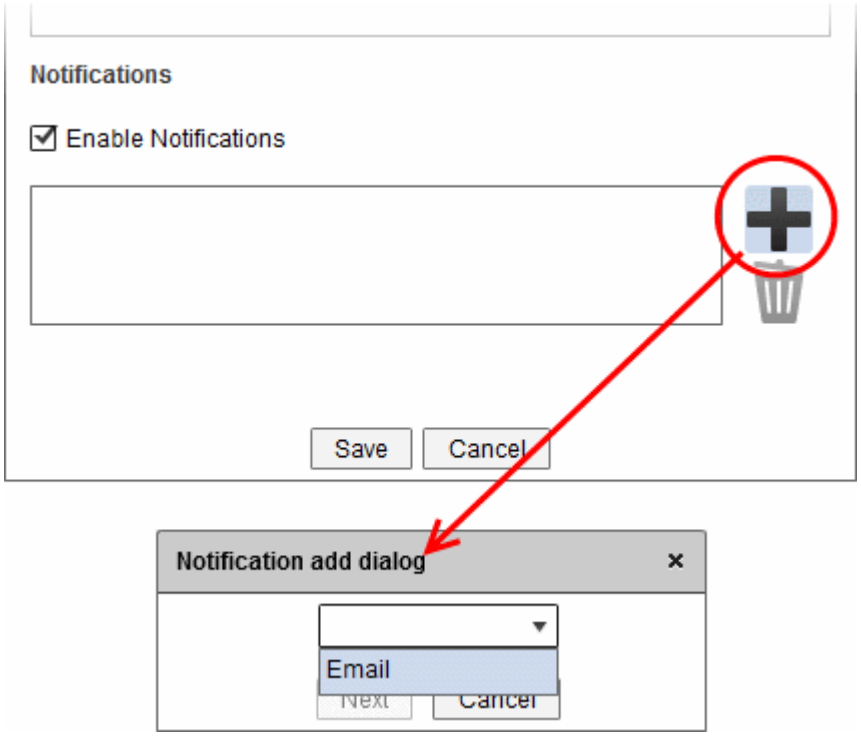
Step 3 - Enter a Name for the rule and configure Email Notifications

On selecting the rule type from the 'Create New Rule' dialog, the 'Rule Edit' Dialog will appear. The 'Rule Edit' dialog allows you to configure the general properties of the rule like the name, descriptions and notifications.



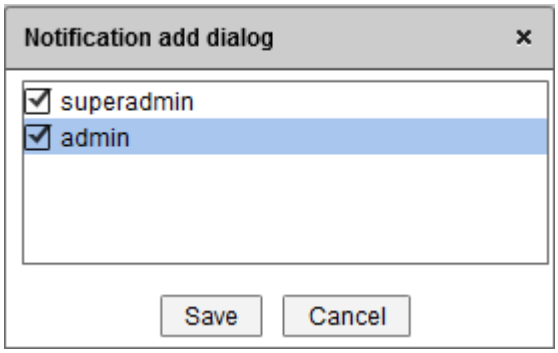
Enter the following information:

- **Name** - Enter a name, shortly describing the new rule
- **Description** - Enter a description for the rule
- **Notifications** - Configure the automated notifications to be sent to the administrators and other users when MyDLP identifies information in based on the rule during scheduled and on-demand scans. This step allows you to choose the notification type and the intended recipients. To view or edit the content of the notification messages, click 'Settings > Enterprise. Refer to the section **Enterprise Tab** for more details.
    - For MyDLP to send automated notification messages, select the 'Enable Notifications' checkbox
    - To add a notification type and recipients, click the plus button beside the text box.

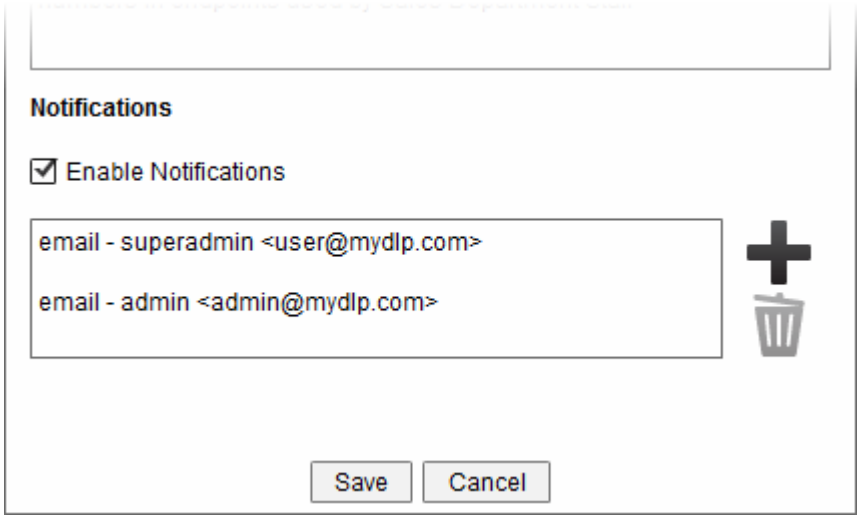


The 'Notification add dialog' will appear.

- Choose the notification type from the drop-down. Currently only 'Email' notification is available. More notification types will be added in future versions.
- Click 'Next'.

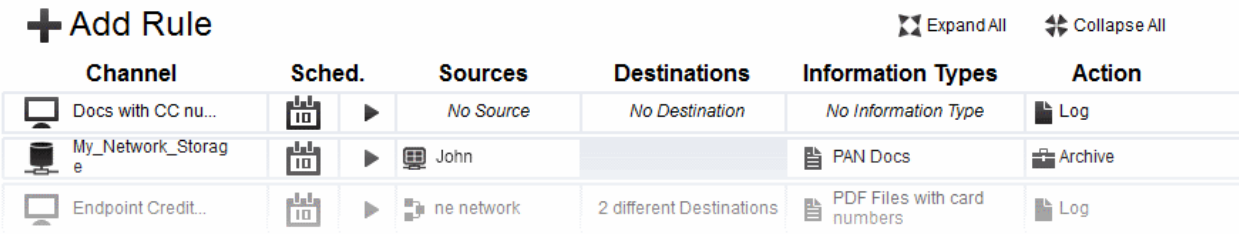


- Select the administrators and other users to whom the notifications are to be sent



- Repeat the process to add more notification types or recipients
- Click 'Save'.

The rule will be added to the list, at the position of the place holder box.



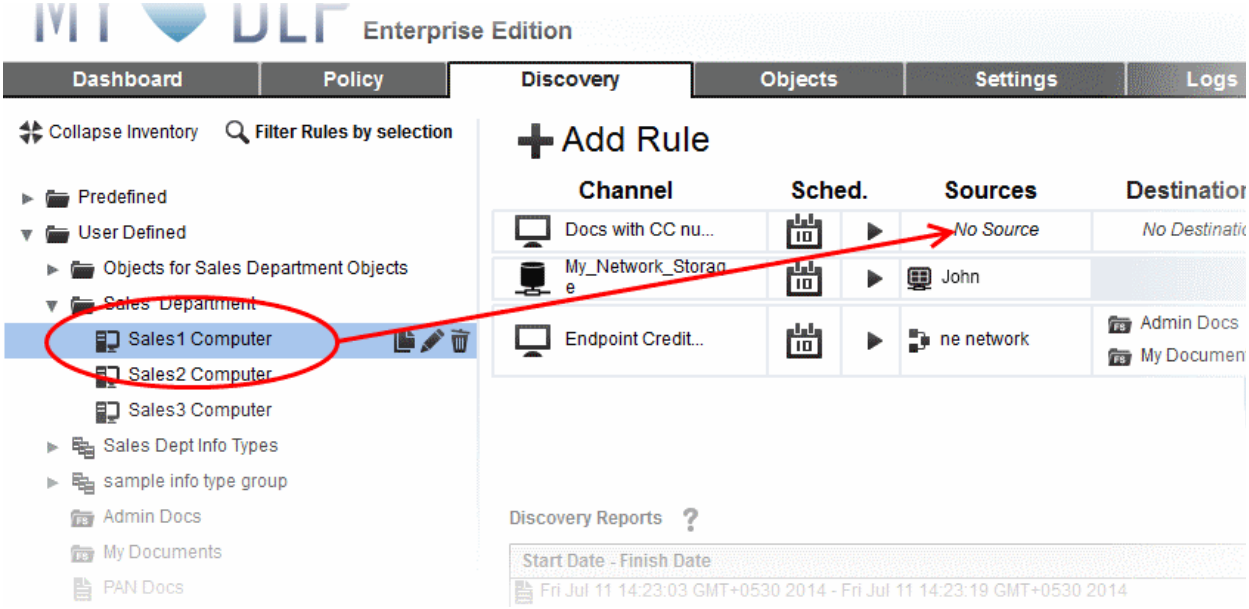
Step 4 - Specify the sources for the rule

The 'Source' component of a rule is where you specify the location to be scanned, like selected endpoints or remote storage. You add sources by dragging a pre-defined or user-defined object from the left hand side. 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

- Expand the predefined, user defined or category folder containing the source you wish to add from the Objects tree in the LHS pane
- Drag the object and drop in the 'Sources' column of the newly added rule



- Repeat the process for adding more sources

You can drag and drop a category folder containing a number of source objects along with other objects so that all the objects that are applicable for sources for the rule, will be added to the rule.

You can add more source objects created after adding the rule, at a later time, by just dragging the object to the 'Sources'

column of the rule.

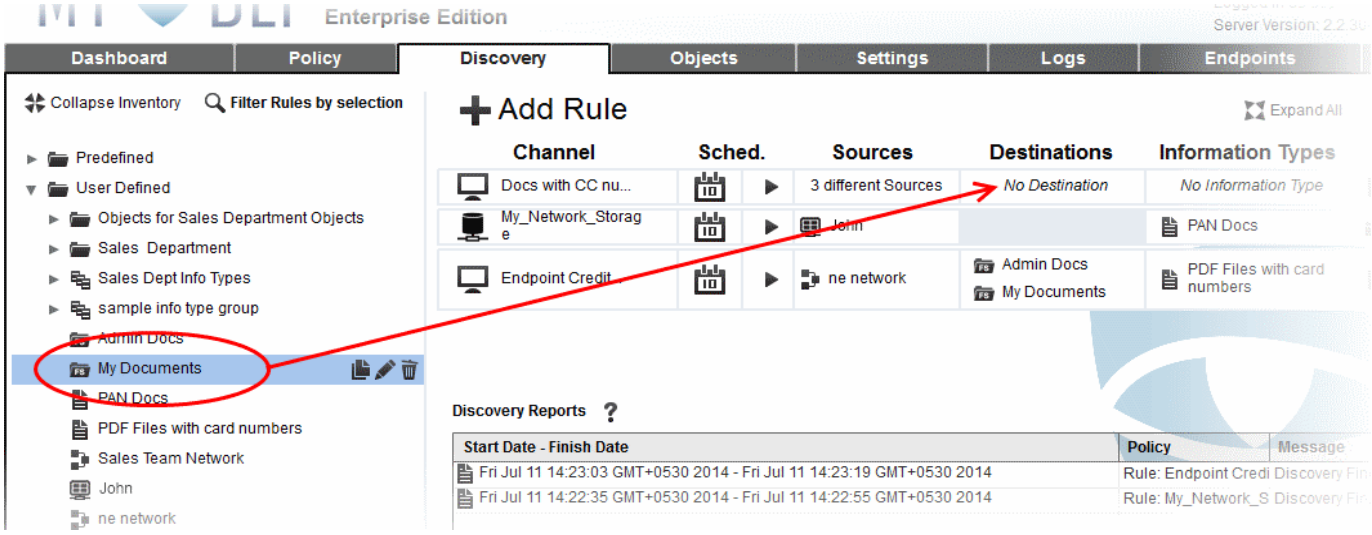
Step 5 - Specify the Destinations for the Rule

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 add destinations by dragging a pre-defined or user-defined 'File System Directory' object from the left hand side.

To add a destination object

- Expand the predefined, user defined or category folder containing the File System Directory object you wish to add from the Objects tree in the LHS pane
- Drag the object and drop into the 'Destinations' column of the newly added rule
- Repeat the process for adding more destinations



You can drag and drop a category folder containing a number of File System Directory objects along with other objects so that all the objects that are applicable for destinations for the rule, will be added to the rule.

You can add more destination objects created after adding the rule, at a later time, by just dragging the object to the 'Destinations' column of the rule.

Step 6 - 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**.

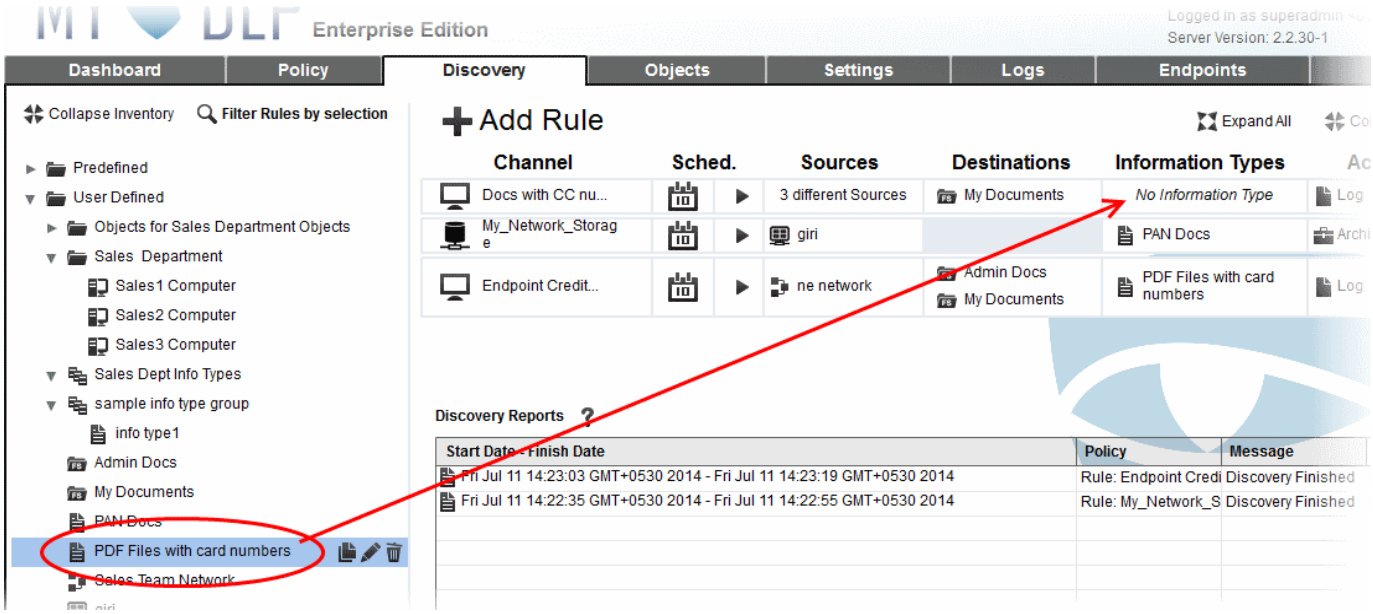
MyDLP is shipped with a number of commonly and frequently used Information Types. These information types are available under the 'Pre-defined' category in the 'Objects' tree. In addition, the administrator can add more number of custom information typed under 'User-defined' category.

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
Information Type Group	• Endpoint Discovery Rule • Remote Storage Rule

To add an Information Type object

- Expand the predefined, user defined or category folder containing the Information Type object you wish to add from the Objects tree in the LHS pane
- Drag the object and drop into the 'Information Types' column of the newly added rule
- Repeat the process for adding more Information Types

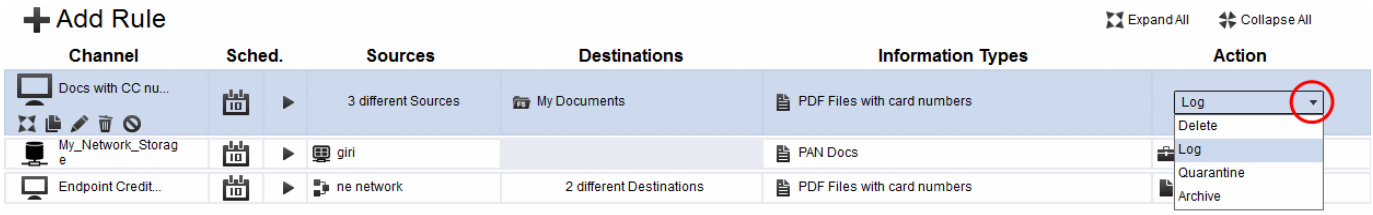


You can drag and drop a category folder containing a number of Information Types so that all the objects that are applicable for the rule, will be added to the rule.

You can add more Information Type objects created after adding the rule, at a later time, by just dragging the object to the 'Information Types' column of the rule.

Step 7 - Specify the Action to be Taken on the File Identified as per the Rule

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



- Choose the action from the drop-down in the 'Action' column. 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.

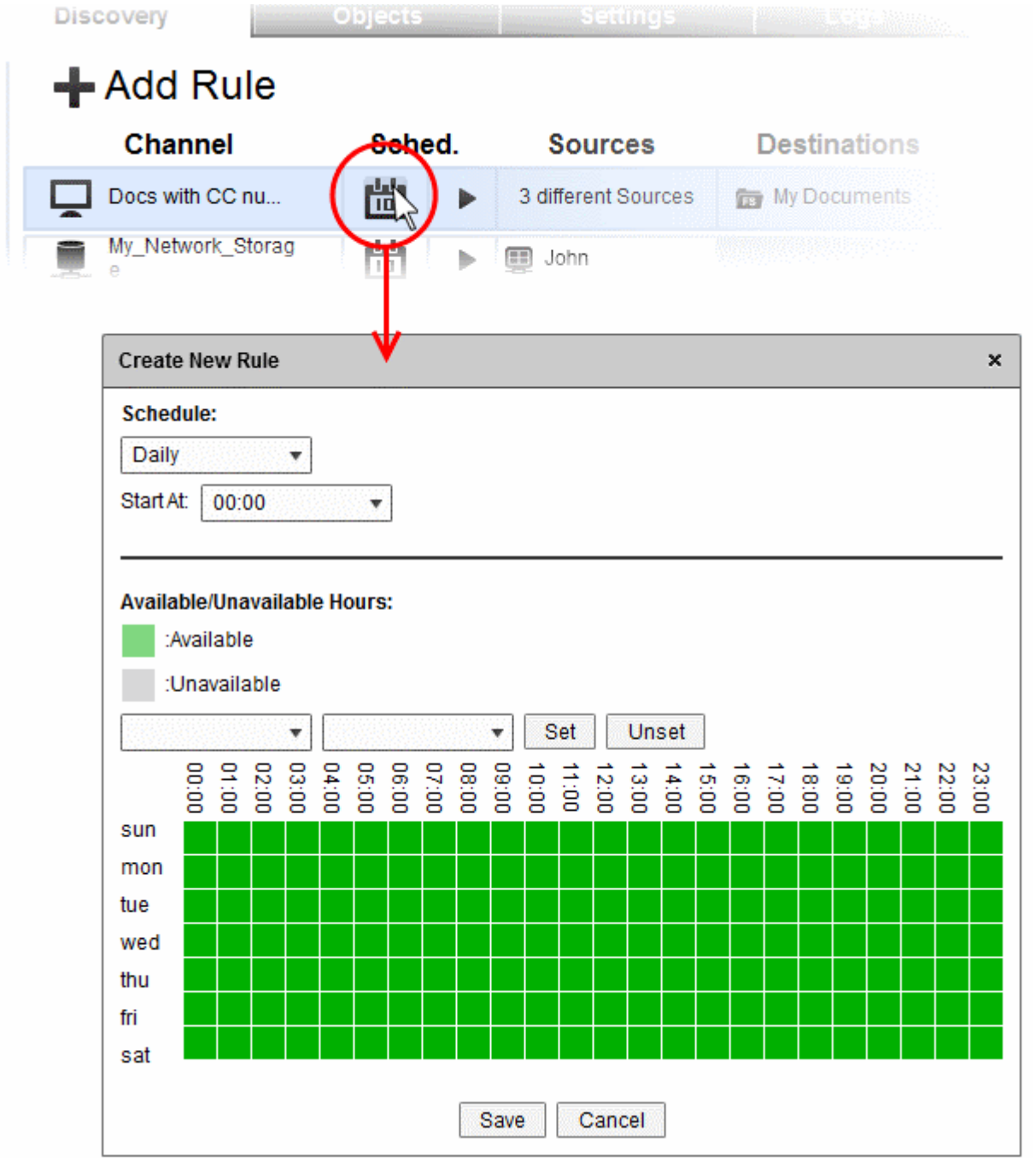
The rule will be saved. You can create as many rules as required. If you are creating a new rule with minor changes from an existing rule, you can clone the rule and edit it to change the required parameters.

Step 8 - 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

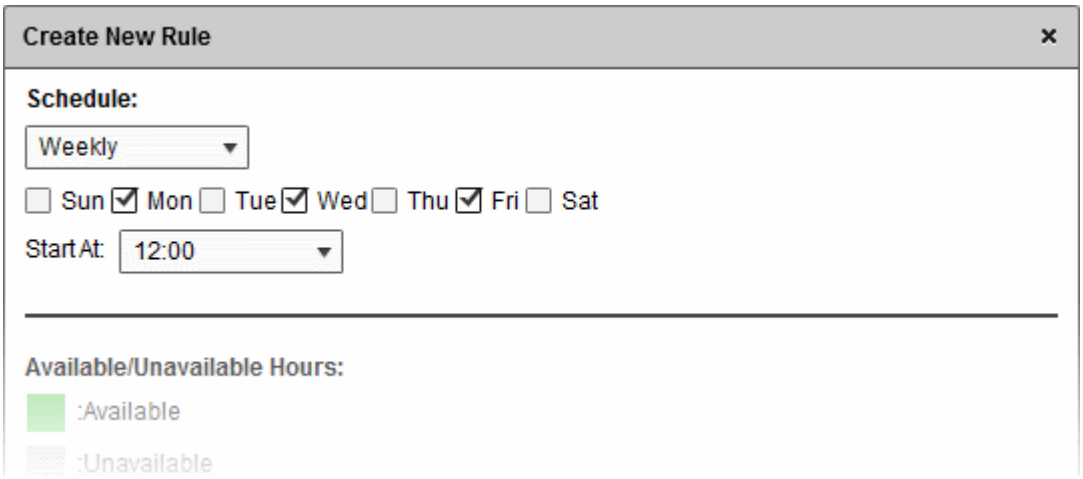
- Click the Calendar button under the Schedule column



The Create New Rule 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:

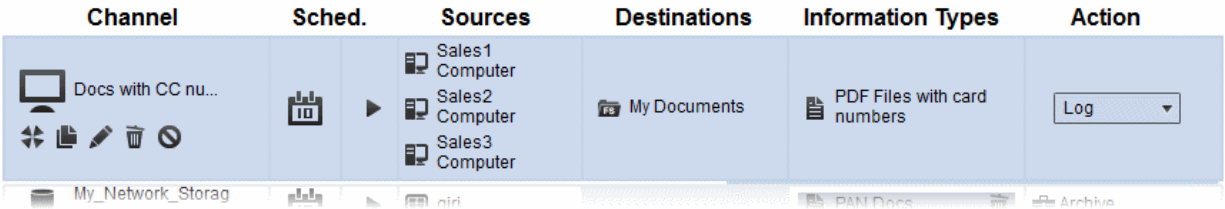
- Green blocks indicate that the endpoints/repositories are available for scanning
- Gray blocks indicate that the endpoints/repositories are not available for scanning

- 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 the 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



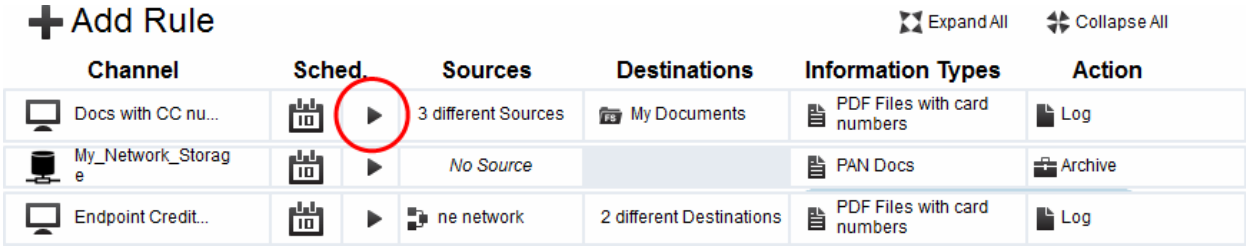
Control	Description
/	Expands/Collapses the Rule stripe. In Expanded view, all the source, destination and information type components are listed in their respective columns.
	Clones the rule to create a new rule with minor changes in the components

	Enables the administrator to edit the name, message and notification settings of the rule. Refer to the section **Editing a Rule** for more details,
	Removes the rule from the policy. Refer to the section **Removing a Rule** for more details
	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.

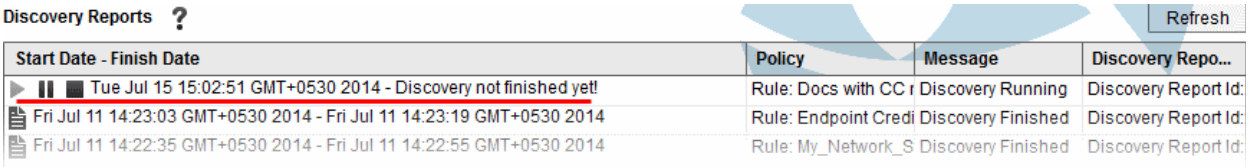
6.1.2. Running On-Demand Scans

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 the Policy** for more details.

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



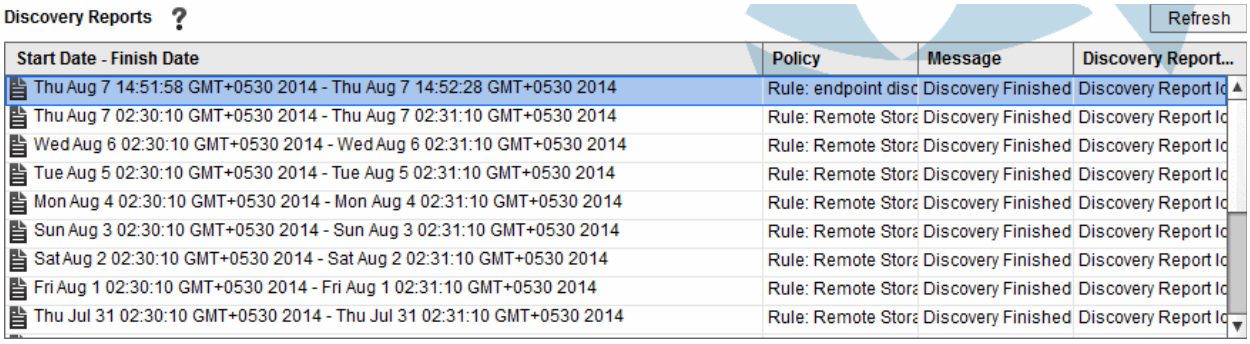
You can pause/resume or stop the scan by clicking the respective buttons.

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

6.2. 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.

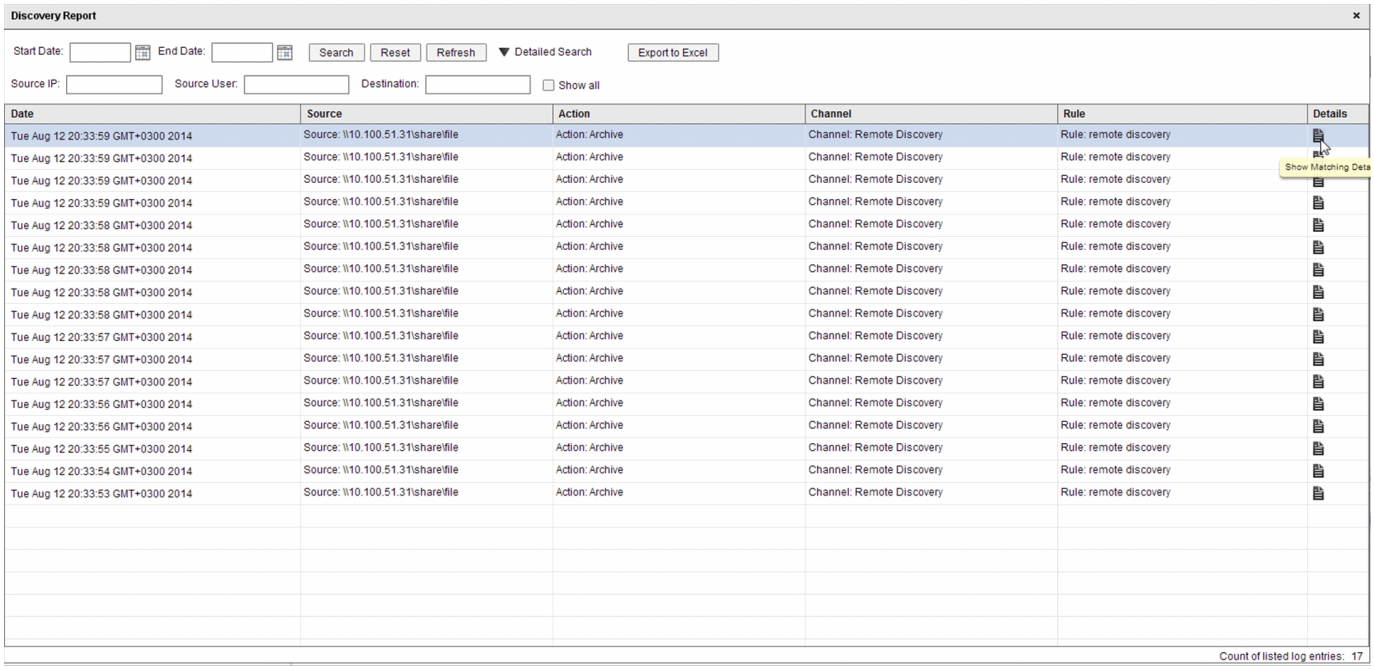
The lower pane of the Discovery interface displays a list of discovery reports with their details.



Discovery Reports Table - Description of Columns	
Column	**Description**
Start Date - Finish Date	The precise dates and time at which the scanning was started and completed. Clicking the icon in the column opens the respective discovery report. Refer to the following section **The Discovery Report** for more details.
Policy	The Discovery rule based on which the scan was executed.
Message	Indicates the status of the scan
Discovery Report Id	The Identity Number of the discovery report.

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.
Channel	The rule channel that indicates the type of the discovery rule based on which the files are discovered. Refer to the section **Rule Channels** for a list of rue types.
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 parameters**

To filter the logs for a specific time period

- Enter the start and end dates of the period by click the calendar icons beside Start Date and End Date fields and click 'Search'.

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

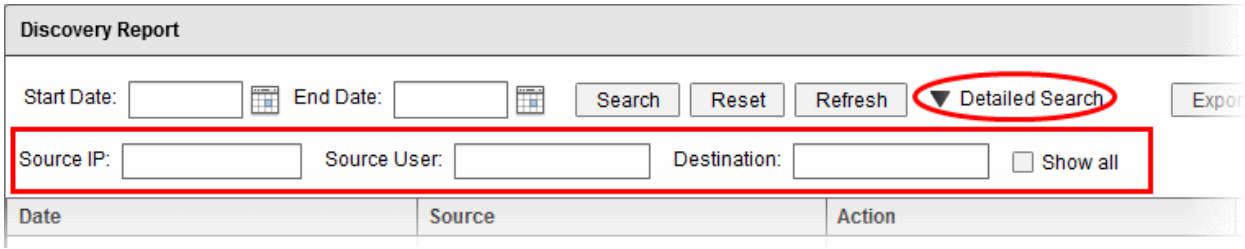
- To clear the filters, click 'Reset'.

Searching Logs based on Rule Parameters

The administrator can search for logs of incidents involving specific endpoint, end-user and destination to narrow down the search.

To search the logs based on rule parameters

- Click 'Detailed Search' to expand the search panel.

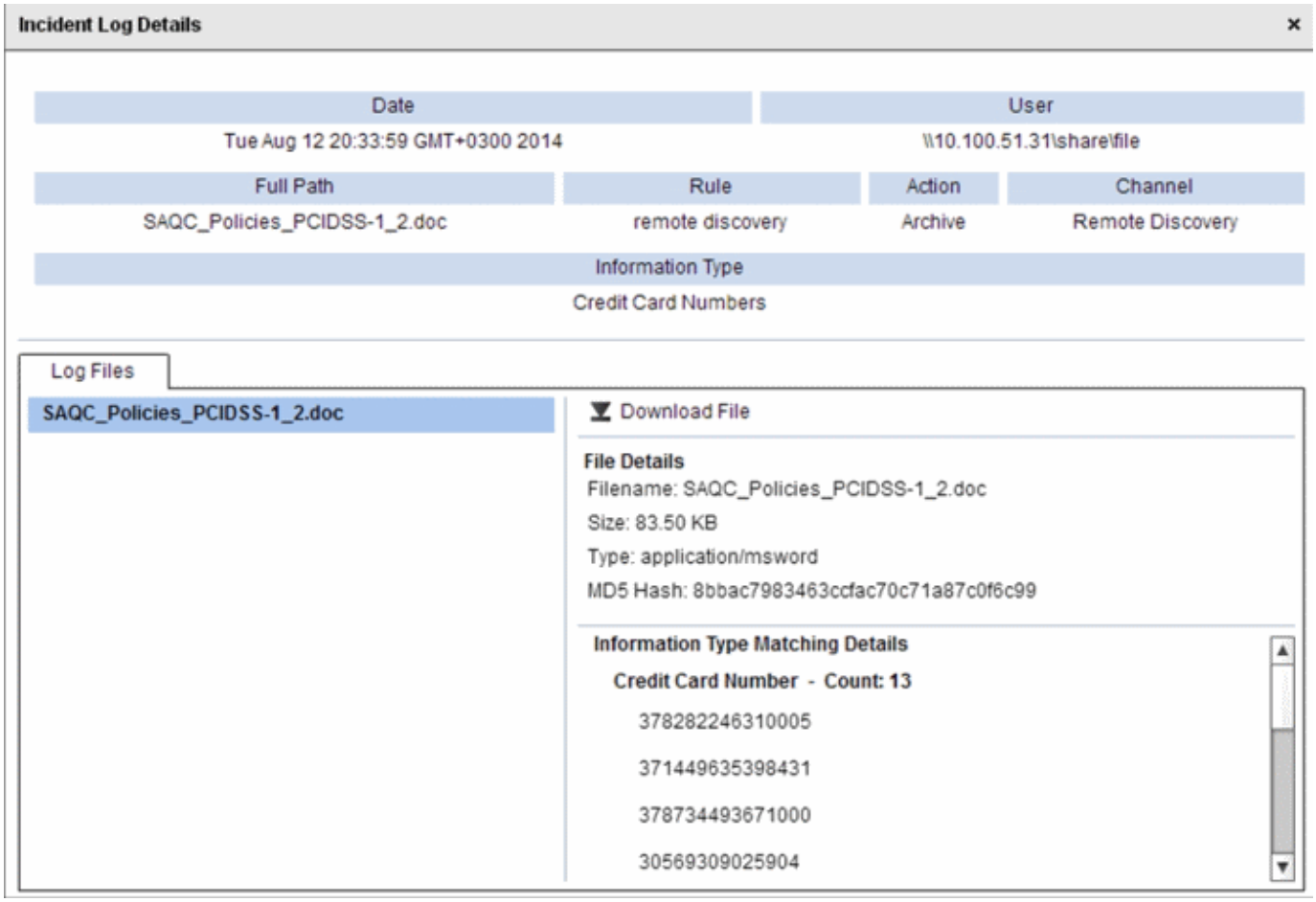


  - To search the logs of incidents involving a specific endpoint, enter the IP address of it in the Source IP field
  - To search the logs involving a specific end-user, enter the end-user name and the hostname of the endpoint name in the format <username>@<hostname> in the Source User field
  - To search the logs of incidents involving a specific destination, enter the destination object in the Destination 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.
User	The IP address of the source end-point or the network storage at which the file(s) is/are discovered.
Full Path	The file path from which the the files were discovered.
Rule	The name of the rule based on which the files were discovered.
Action	The action executed on the discovered file(s).
Channel	Indicates the type of the discovery rule based on which the files are discovered.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Log 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 in the right hand side pane.
Download File	Enables the administrator to download the selected file. Refer to the section **Downloading the Archived Files** for more details.
File Details	Displays the file name, size, file type and MD5 HASH digest of the selected file
Information Type Matching Details	Displays the data contained in the file, that matched with the Information Type specified in the rule.

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 Incident Log Details interface.

To download an archived file

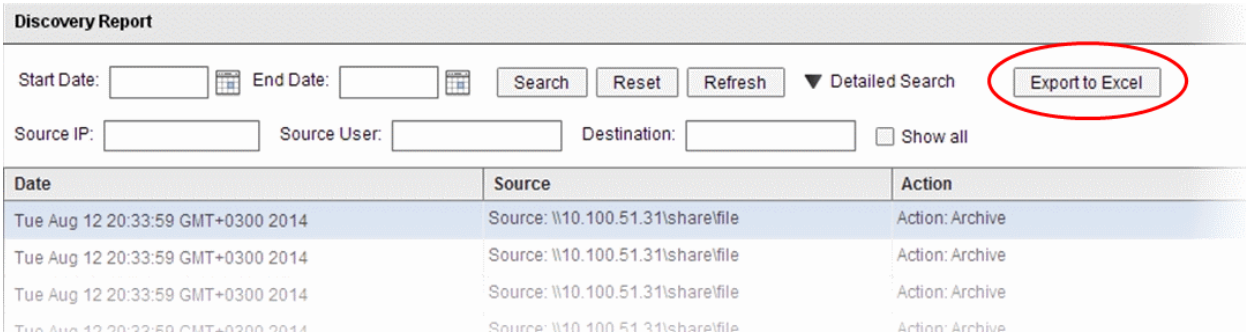
- Click the icon for the log entry under the Details column. The Incident Log Details pane will open.
- Select the file to be downloaded, under 'Log Files'
- Click the 'Download File' link.

You can save the file in your local storage.

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.

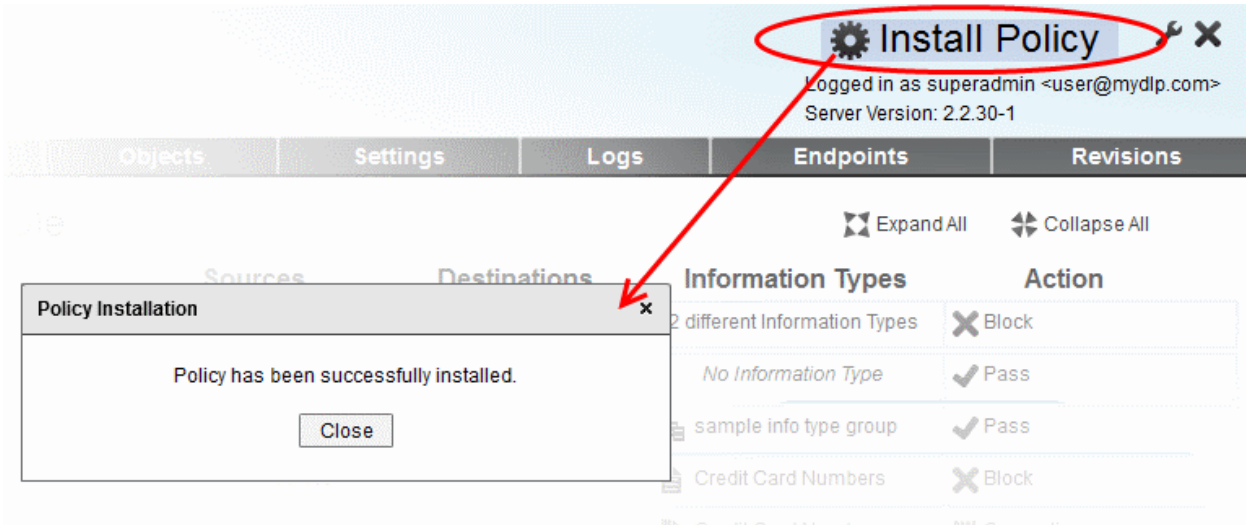
- To export the logs into an Excel file click 'Export to Excel' button at the top and save the file in your local drive.



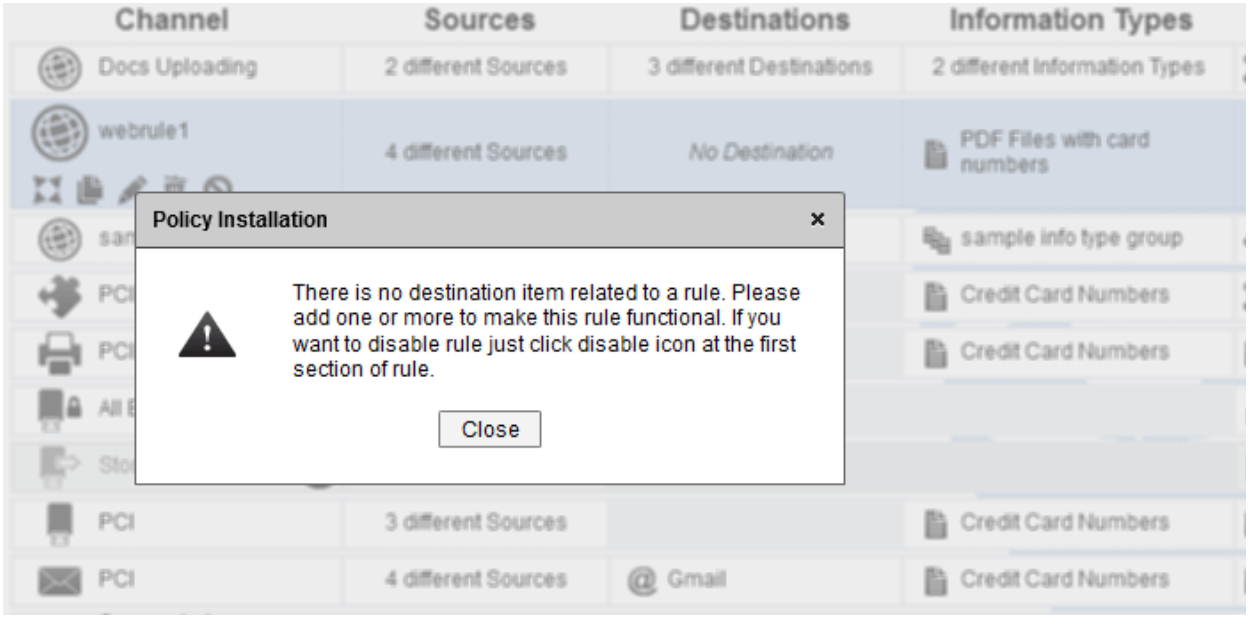
7.Deploying the Policy

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



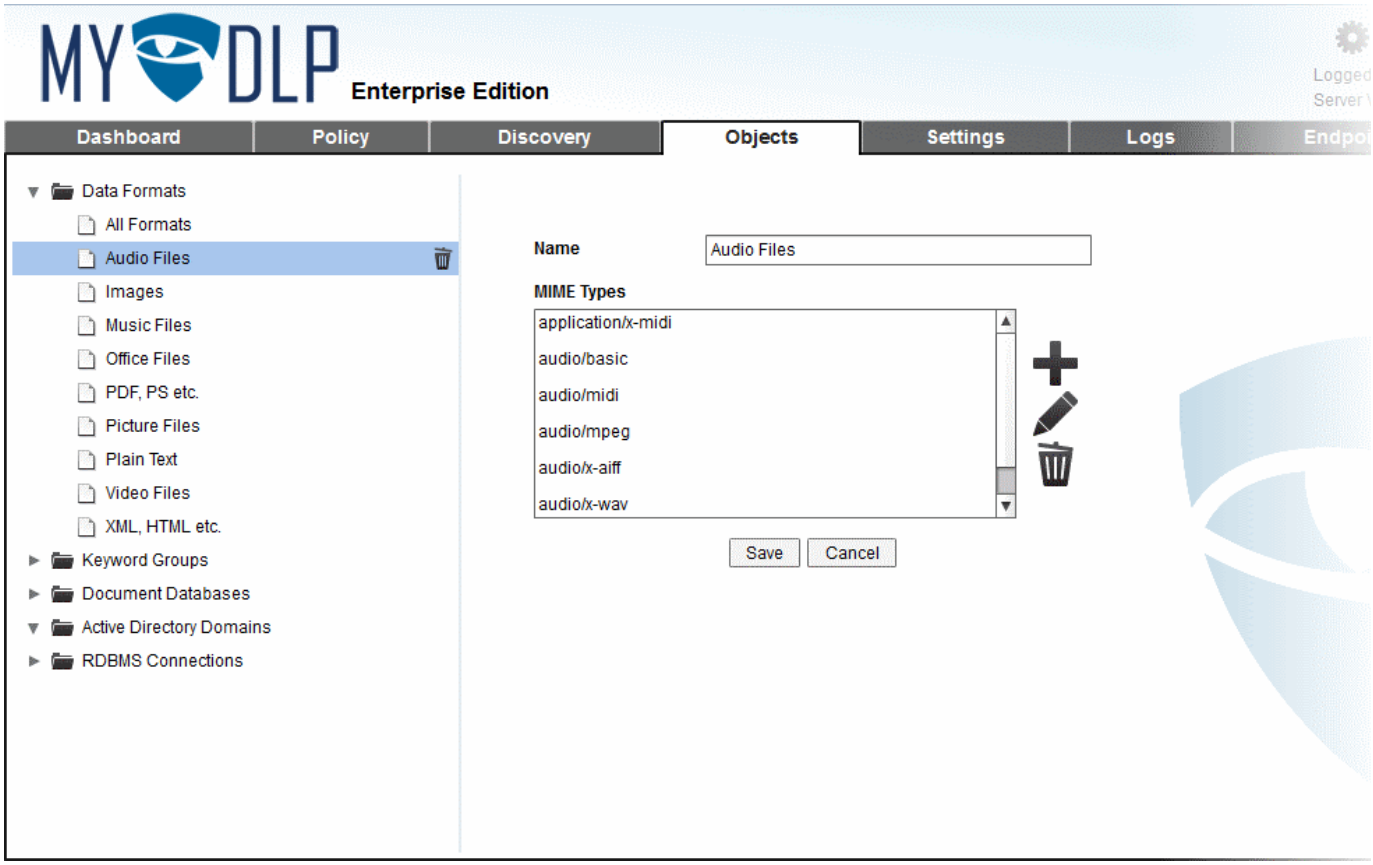
- If all enabled rules are correctly specified correctly then the policy will be compiled and installed instantly.
- If one or more of the enabled rules are not complete, the incomplete rule will be highlighted and a dialog will be displayed with advice to complete or disable the rule.



8. The Objects Tab

Objects are predefined pieces of information which can be dragged and dropped into rules - a flexible system that allows you to quickly create granular yet easily modifiable rule-sets. MyDLP comes with a series of pre-defined objects which are displayed on the left of the 'Policy' and the 'Discovery' interfaces.

The 'Objects' tab allows administrators to view, manage and create selected components of Information Type and User objects. The components that are created from this interface will be available for selection while creating the respective objects from the 'Policy' and the 'Discovery' interfaces.



- **Data Formats** - The 'Data Format' is used in 'Information Type' object, to specify the file format(s) to be inspected for the occurrence of sensitive data. Refer to the explanation of **Data Formats** in the section **Information Types - An Overview** for more details.
- **Keyword Groups** - The 'Keyword Group' is used as a 'Matcher' component in the construction of Information Type object to specify the keywords to be searched in every intercepted file to identify the files containing sensitive information. Refer to the explanation of **Keyword Groups** in the section **Predefined Matcher Types** for more details.
- **Document Databases** - The 'Document Database' is used as a 'Matcher' component in the construction of 'Information Type' object to specify the document databases to be searched using Hash comparison and Partial Data Matching (PDM) techniques for the occurrence of sensitive data. Refer to the explanation of **Document Databases** in the section **Predefined Matcher Types** for more details.
- **Active Directory Domain** - The 'Active Directory' object is used in construction of 'User Object', to specify an pre-integrated AD domain for the MyDLP to import the users from. Refer to the explanation of **importing users from AD domain** in the section **Adding a User Defined User Object** for more details.
- **RDBMS Connections** - The administrator can configure access to an RDBMS for MyDLP to import the keywords to be added to groups and Documents to be added to Document Databases.

Background Note:

The 'Information Type' component plays a key role in a policy rule as it is the factor used for identifying files containing specified types of sensitive data from a data traffic or from a storage. The information type component is constituted by adding pre-defined or user-defined 'Information Type' objects available from the left hand side pane in the Policy and Discovery interfaces.

The Information Type objects, in-turn are composed using two important components:

- **Data Format(s)** - Specify the file format(s) to be inspected for the occurrence of data with properties/string formats specified in the Information Features.
- **Matchers** - The 'Matcher' parameter specifies data patterns or string formats - like birth-date, keywords, keyword groups, credit card number, account number and so on and a threshold for occurrence.

For detailed explanations on the Information Type objects and their components, refer to the sections **Information Types - An Overview**.

The User object is used to specify users and user groups as source component in data transfer policy rules, so as to intercept the files matching the Information type specified in the rule, from the data transferred from the users' computers.

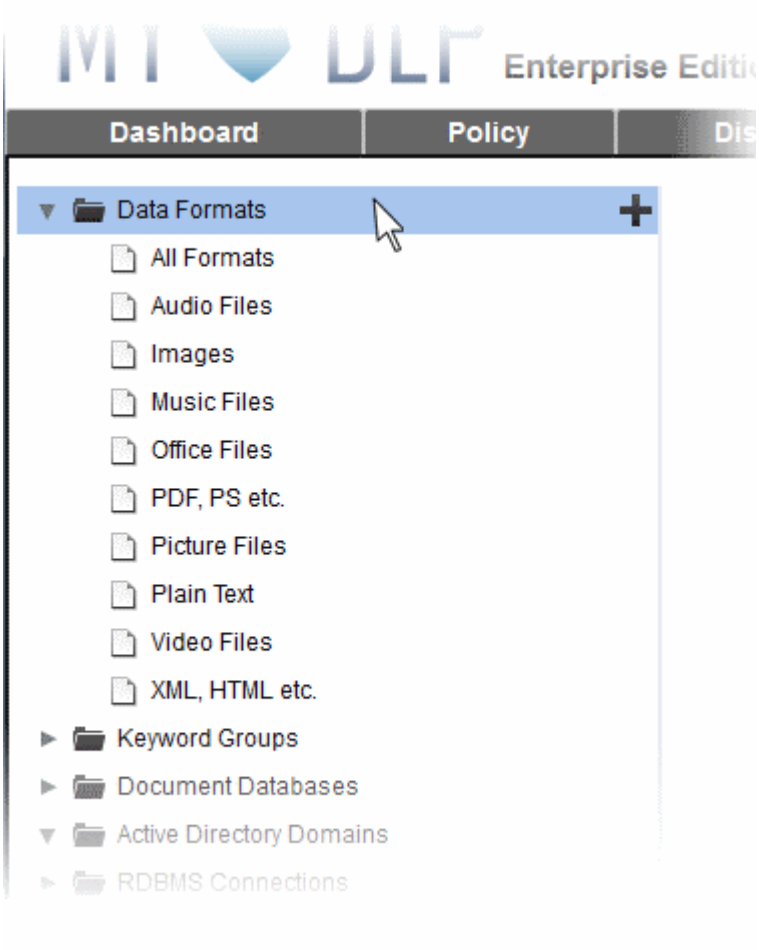
The following sections provide more explanations on:

- **Managing Data Formats**
- **Managing Keyword Groups**
- **Managing Document Databases**
- **Integrating Active Directory Domains**
- **Integrating RDBMS Systems**

8.1. Managing Data Formats

The Data Formats folder in the left hand side pane of the Objects interface allows the administrator to view and edit the predefined and existing user-defined data formats and create new data format types. The newly created data format types will be available for selecting while adding a new or editing an existing Information Type object.

To view the pre-defined and existing user-defined data formats, expand the 'Data Formats' category by clicking on it.



Refer to the following sections on managing the data formats:

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

8.1.1. Editing a Data Format

Each Data Format is defined with a set of file types belonging to a genre. For example, the pre-defined data format 'Images' contains the following formats, that can be opened in any image viewer or editor applications.

.bmp

.gif

.jpeg

.png

.svg + .xml

.tiff

Adobe Photoshop files

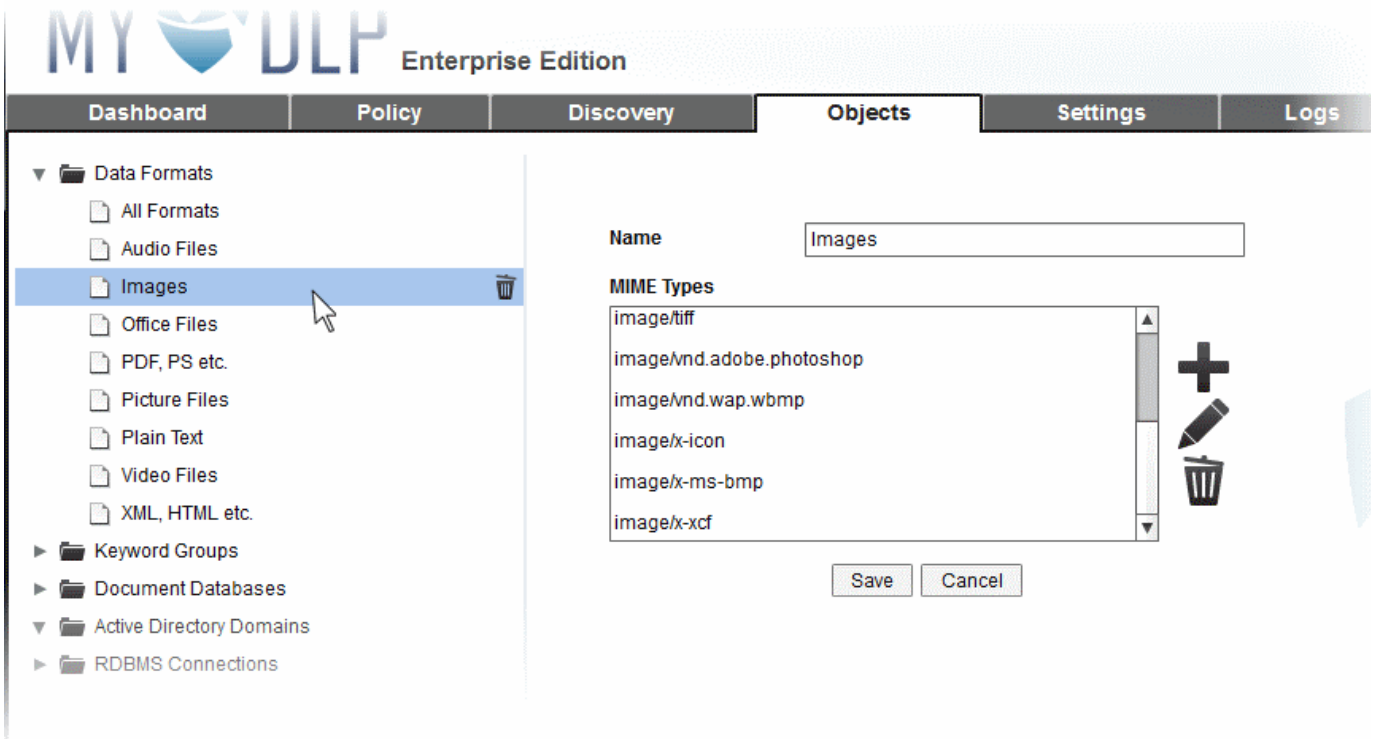
icon files

… and so on.

The administrator can add more or remove existing file types by editing the Data Format

To edit a data format

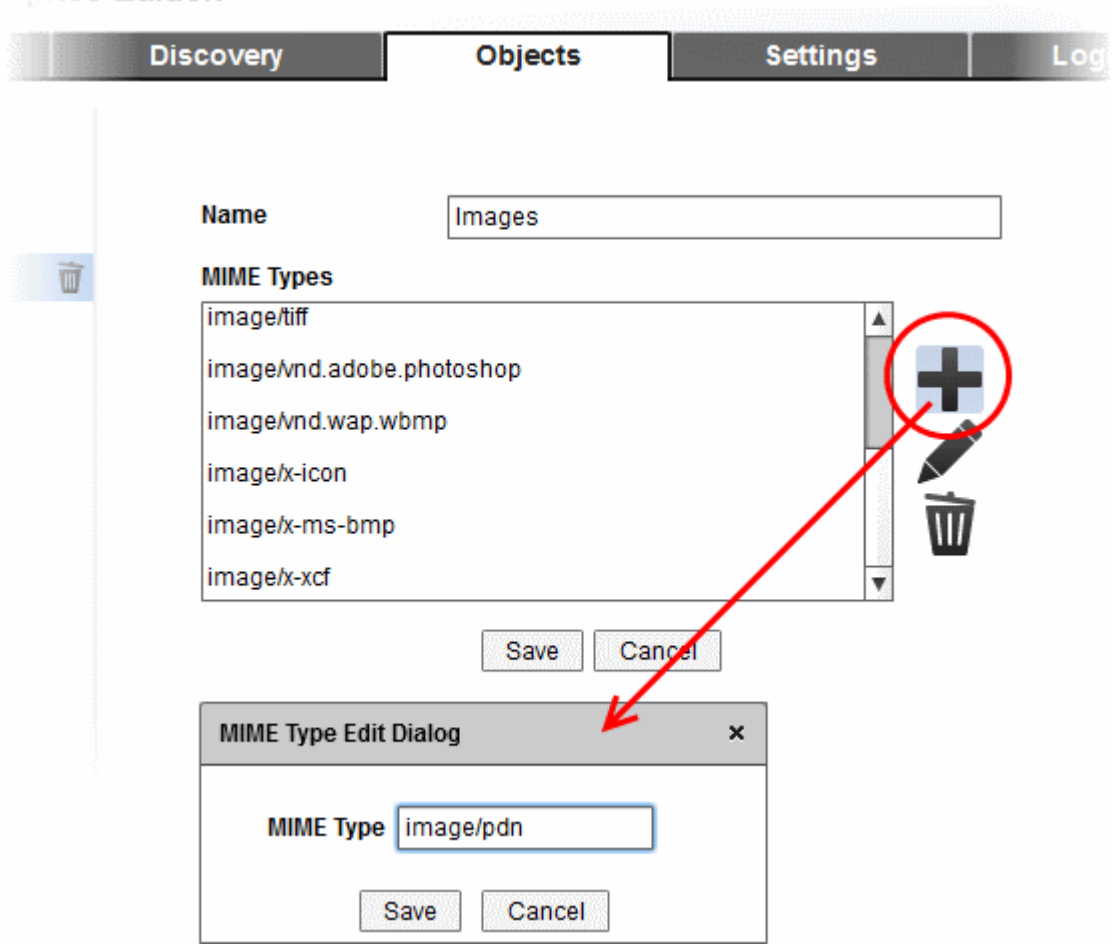
- Expand the Data Formats category and select the Data Format to be edited. The edit screen will open in the right hand side pane, displaying the name and the component file types in MIME format.



- To change the name of the Data Format, directly edit the name in the 'Name' text field.

To add a new file type

- Click the plus icon beside the list of file types



The MIME Type Edit Dialog will appear.

- Enter the new file type to be added to the data format collection in MIME type format .

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.

- Click 'Save' to add the MIME type to the Data Format
- To edit an MIME Type, select the MIME type from the list and click the pencil icon . The MIME Type Edit Dialog will appear. Edit the MIME type as explained earlier and click 'Save'.
- To remove an MIME Type from the list, select the MIME Type and click the trash can icon . You can only delete MIME types only from user-defined Data Formats.
- Click 'Save' in the right hand side pane to save the changes to the Data Format

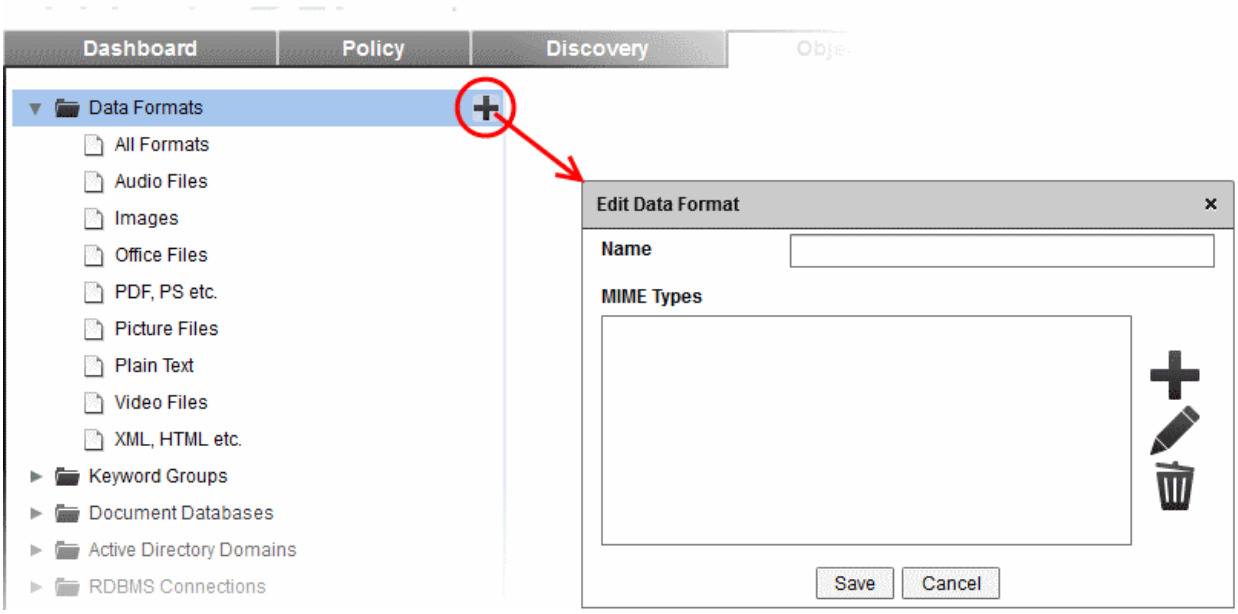
For the changes to propagate through the rules in which the data format being edited is applied, the policy needs to be re-deployed. Refer to the section **Deploying the Policy** for more details.

8.1.2. 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.

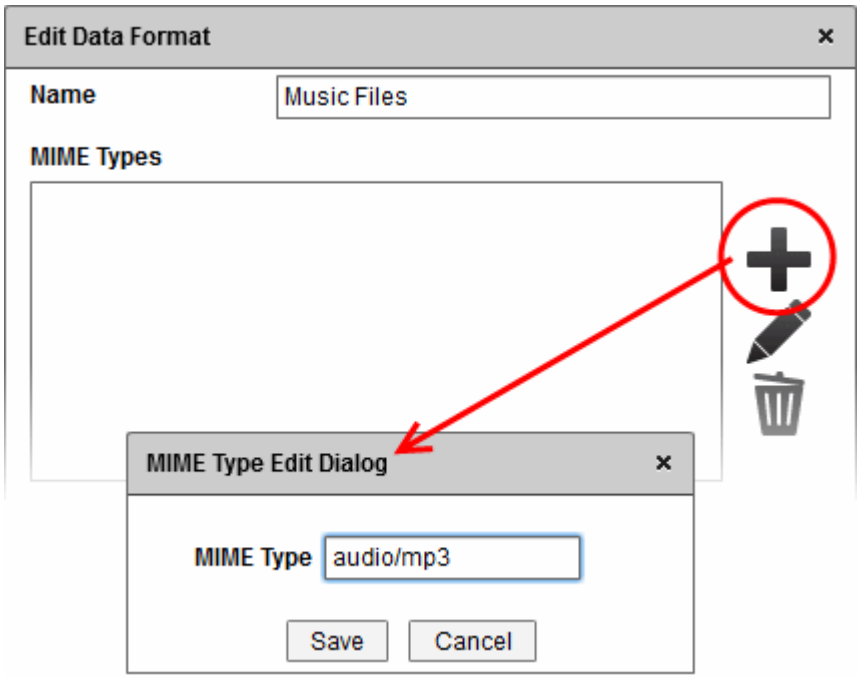
To add a new data format

- Select the Data Formats folder from the left hand side pane and click the plus icon



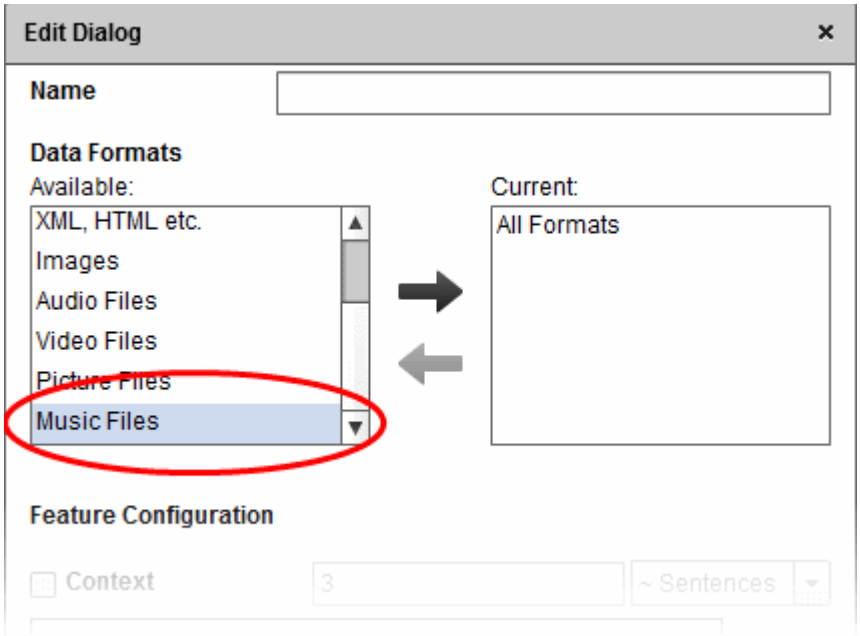
The 'Edit Data Format' dialog will appear.

- Enter a name for the Data Format in the Name field
- Add the MIME Types to be included in the Data Format collection by clicking the Plus icon and entering the file type in MIME Type format in the 'MIME Type Edit dialog'.



- Click 'Save' to add the MIME type to the Data Format
- Repeat the process for adding more MIME types
- Click 'Save' in the right hand side pane to save the changes to the Data Format

The newly added Data Format will be available for selecting while creating a new or editing an existing Information Type object.

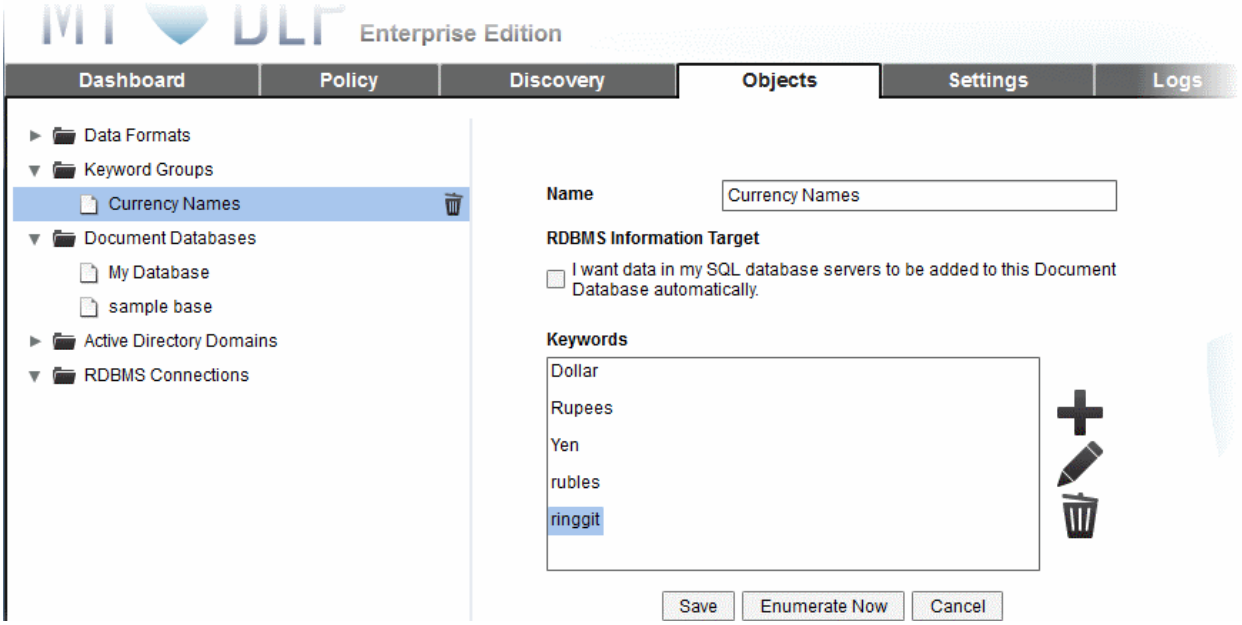


8.2. Managing Keyword Groups

Each Keyword Group is a collection of keywords pertaining to a specific field like business, medicine, finance, banking and so on. The Keyword Groups 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 is shipped with a number of pre-defined, uneditable keyword groups that are available for selection while creating an Information Type object.

The 'Objects' interface allows the administrator to create and add custom, user-defined keyword groups to MyDLP, which inturn, can be used in Information Type objects.



Refer to the following sections on managing the Keyword Groups:

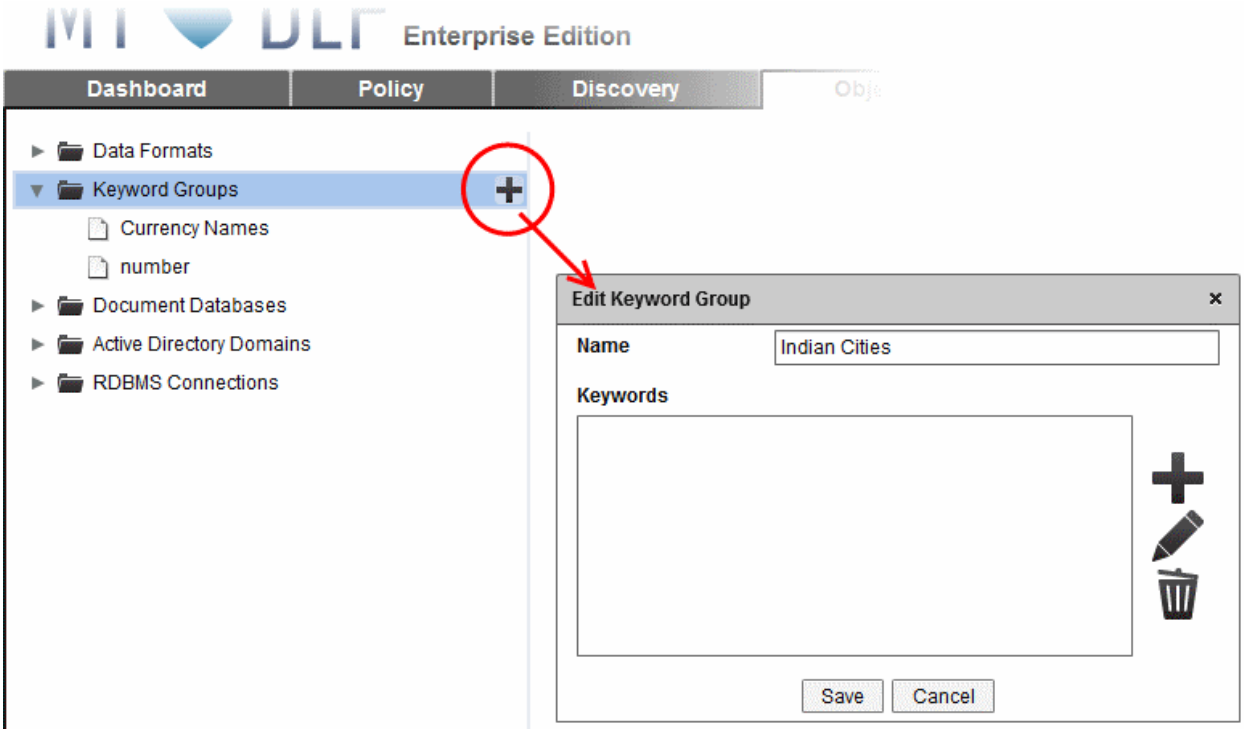
- **Adding a user defined Keyword Group**
- **Editing a user defined Keyword Group**

8.2.1. Adding a User Defined Keyword Group

The administrator can add new keyword groups by manually adding keywords, importing from a file or importing from a MySQL database.

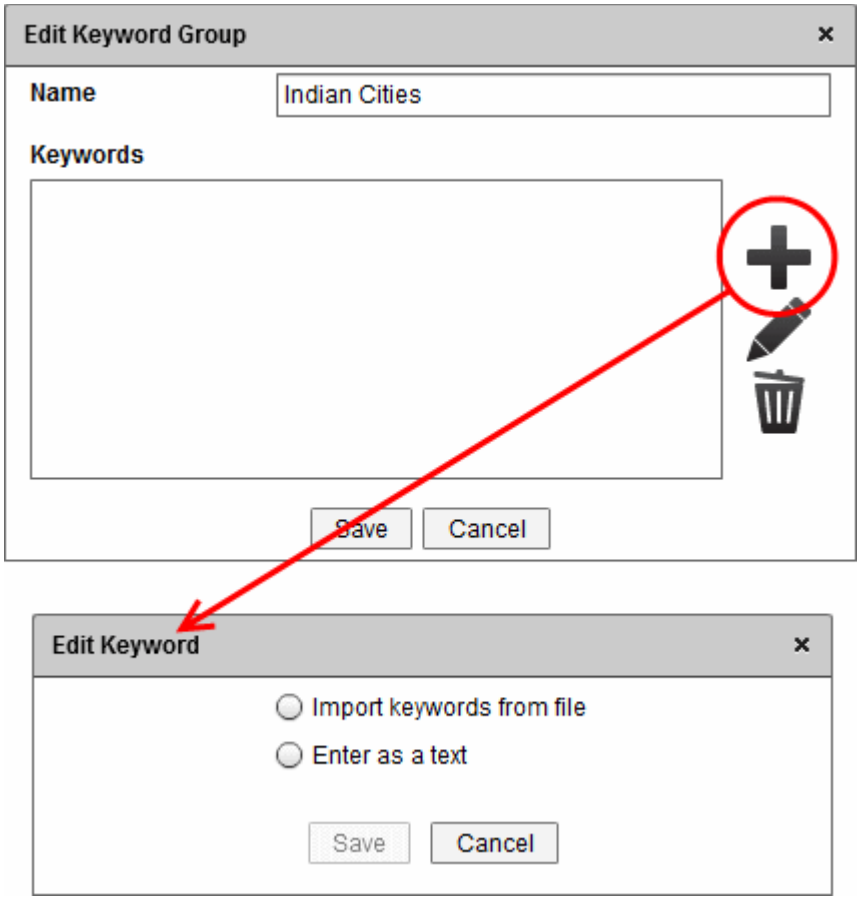
To add a new Keyword Group

- Select the Keyword Group folder from the left hand side of the Objects interface and click the plus icon.



The 'Edit Keyword Group' dialog will appear.

- Enter a name for the Keyword group in the Name field, shortly describing the group.
- To add the keywords to the group, click the Plus icon. The 'Edit Keyword' dialog will appear.

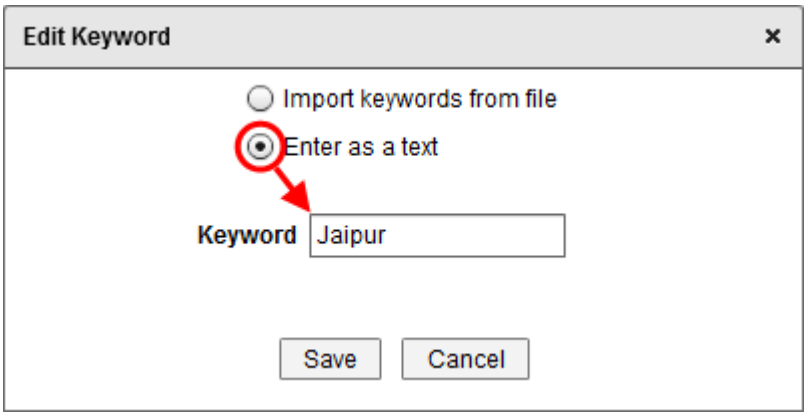


You can add the keywords in two ways:

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

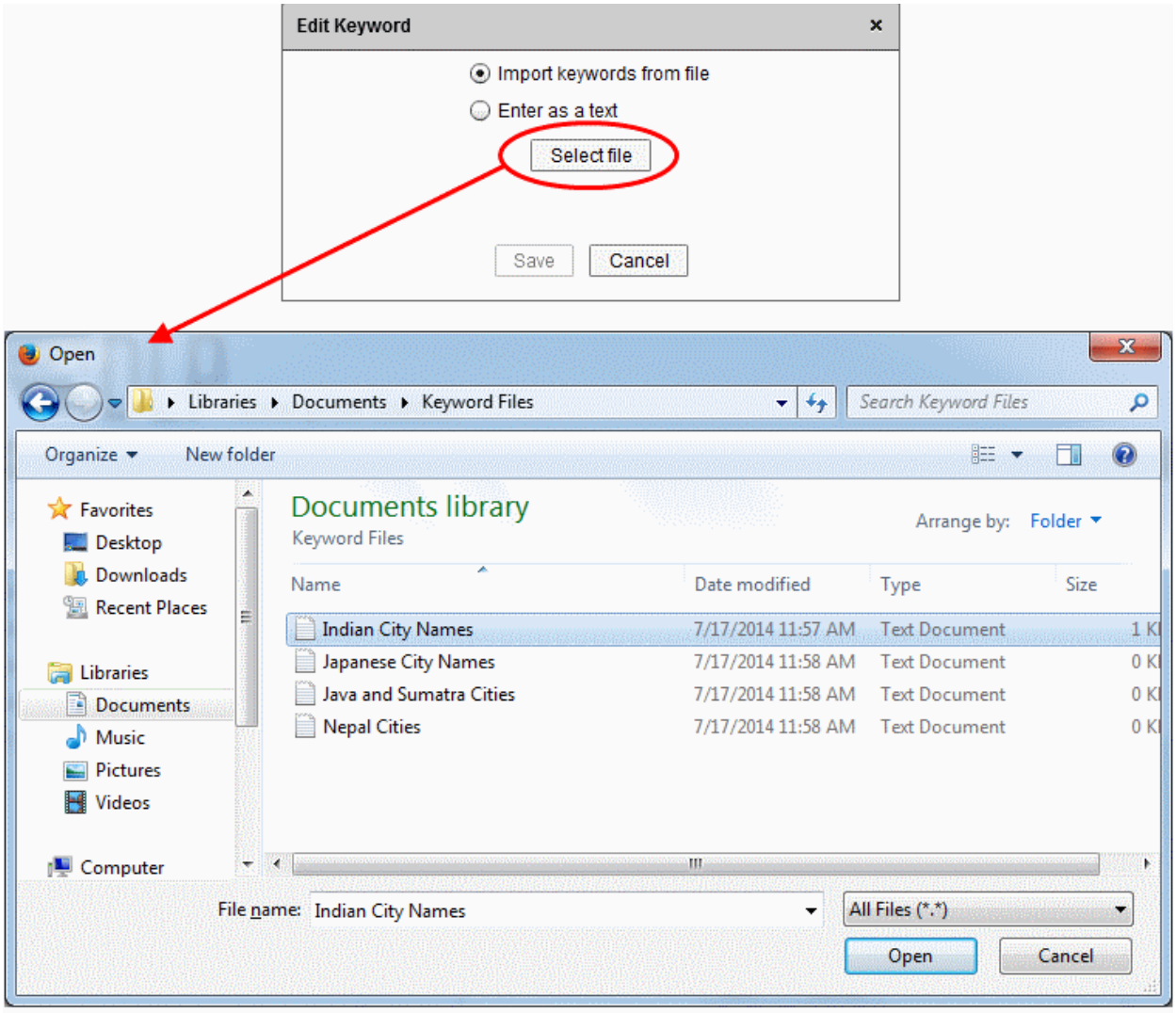
Tip: You can import keywords from a MySQL database servers too, through RDBMS connection. Refer to the section **Adding Keywords from MySQL Database Servers** for more details.

- To manually enter the keywords, choose 'Enter as a text' radio button. The Keyword field will appear in the same dialog

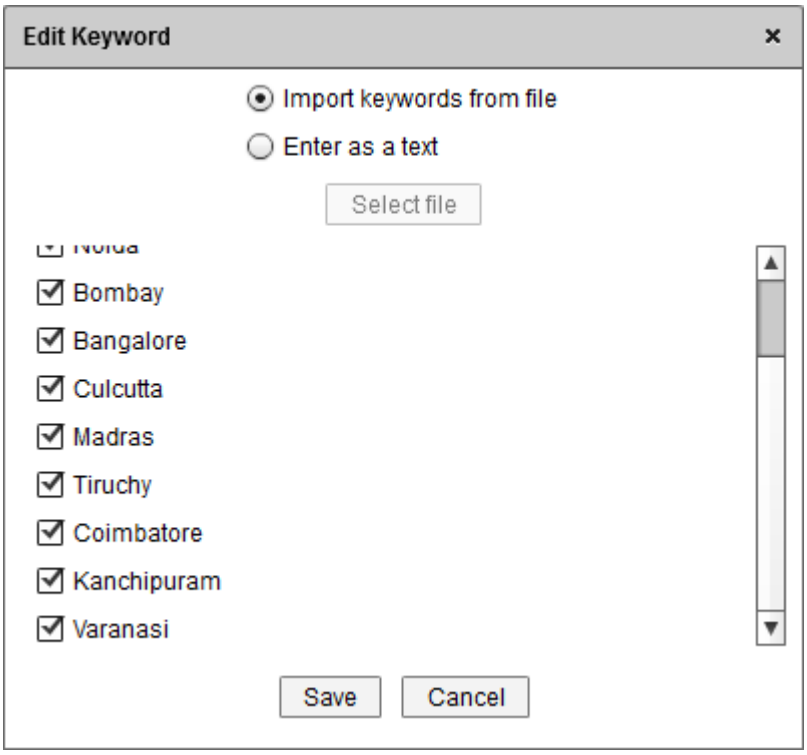


  - Enter the keyword and click 'Save'
  - Repeat the process to add more keywords
- To import keywords from a text file containing the keywords, choose 'Import keywords from file' radio button. The 'Select File' button will appear.

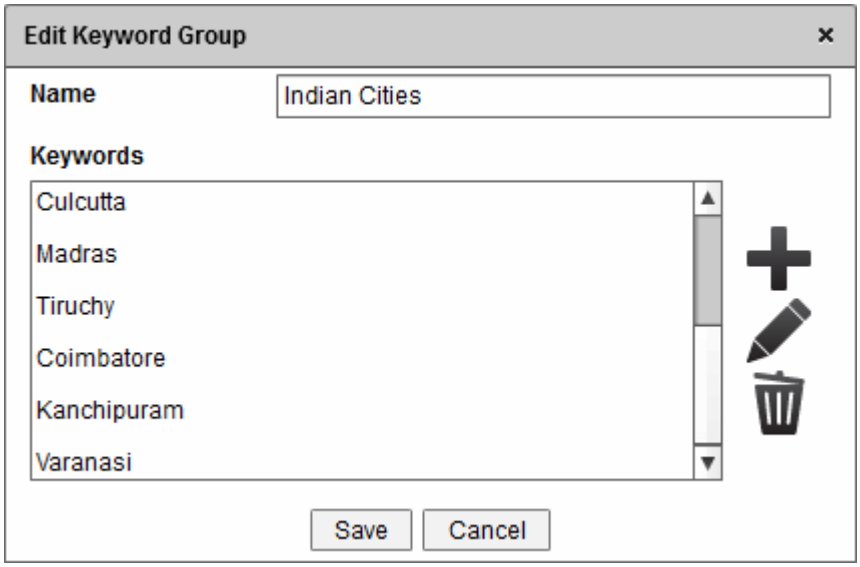
  - Click 'Select File' and navigate to the text file



- Click 'Open'. The keywords in the file will be listed in the 'Edit Keyword' dialog allowing you to select those to be included in the group.
- By default, all the imported keywords are selected. Deselect the words that are not to be included in the group and click 'Save'.

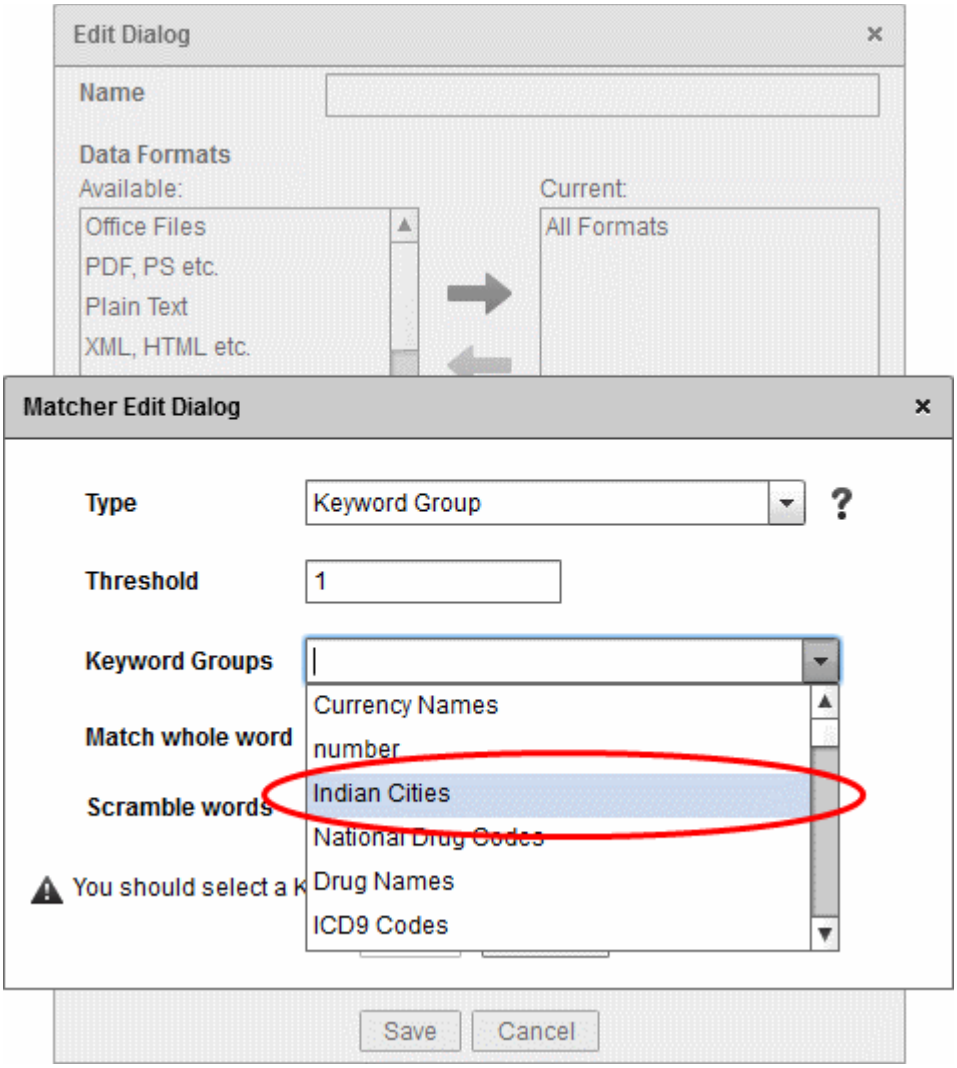


The keywords will be added to the group.



- Repeat the process for adding more keywords from different files.
- Click 'Save' in the 'Edit Keyword Group' dialog to save the group.

The newly added Keyword Group will be available for selection as a Matcher, while **creating a new** or editing an existing Information Type object.

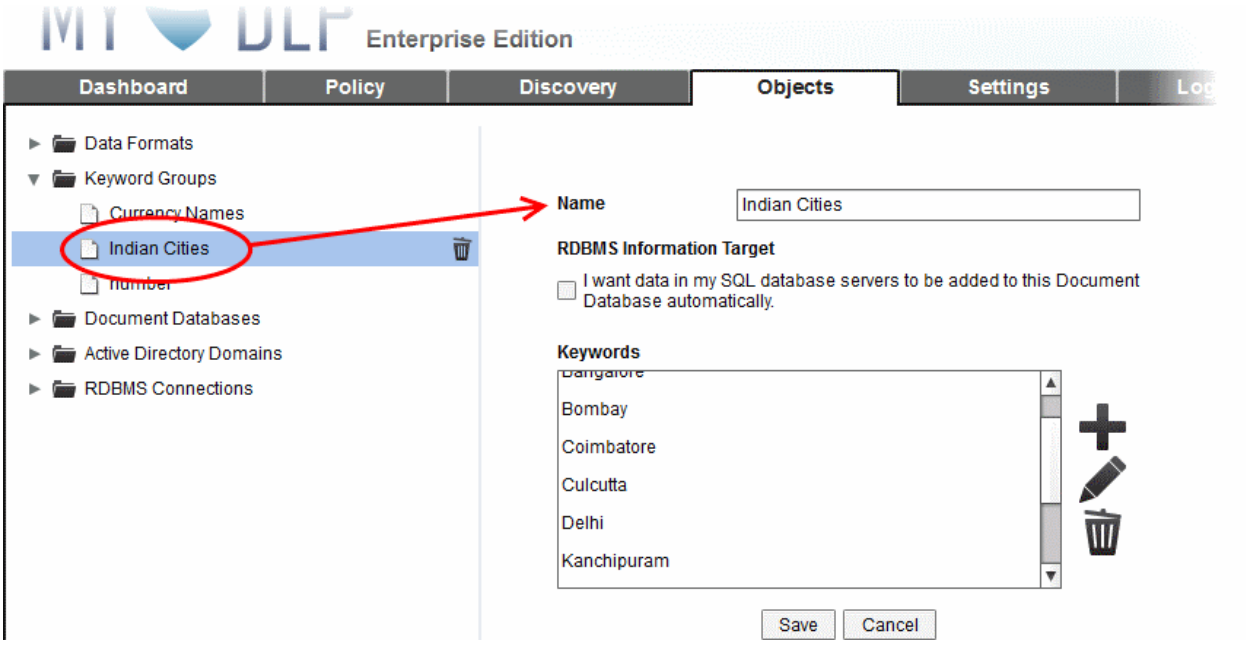


8.2.2. Editing a user defined Keyword Group

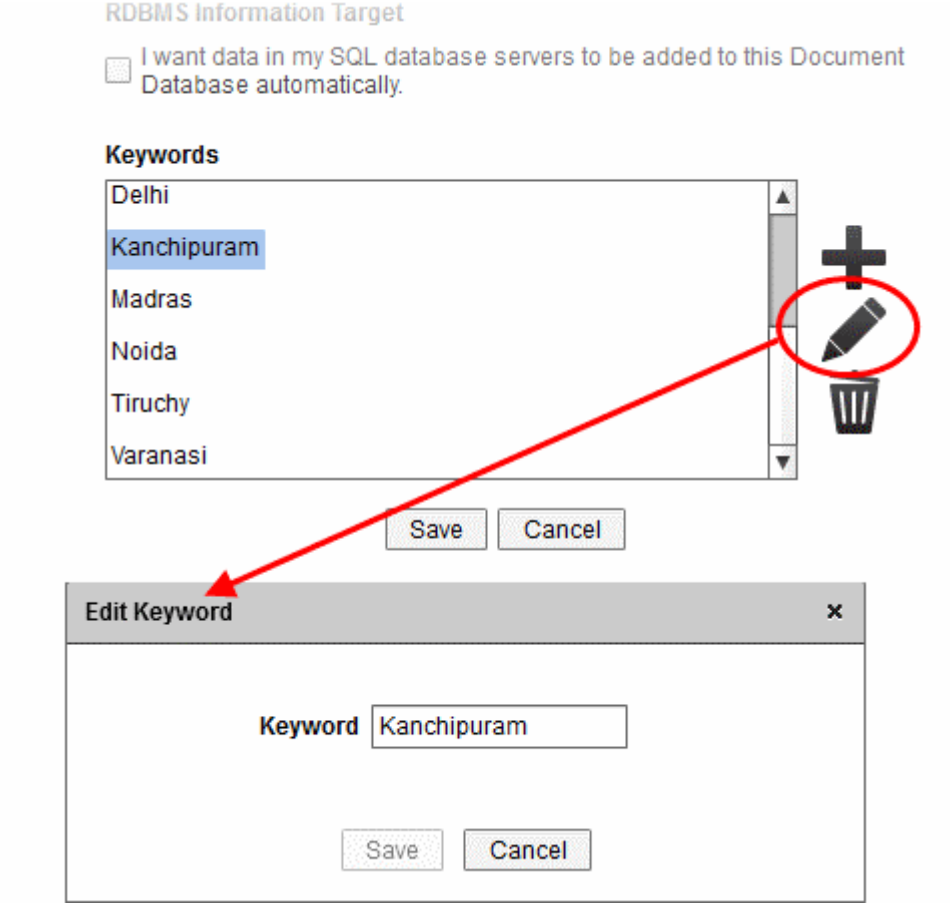
The administrator can edit a Keyword Group at anytime to add new keywords or to remove existing keywords from the group. Also, the administrator can import keywords from a MySQL database, by editing a keyword group. If a keyword group is altered , the policy has to be re-deployed to the network for the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

To edit a keyword group

- Expand the Keyword Groups category and select the group. The edit screen will open in the right hand side pane, displaying the name and the component keywords.



- To change the name of the group, directly edit the name in the 'Name' text field.
- To add new keyword(s) click the plus icon and follow the **same procedure** as explained in the section **Adding a User Defined Keyword Group**.
- To remove a keyword, select the keyword and click the trash can icon .
- To edit a keyword, select the keyword and click the pencil icon .



  - Edit the keyword and click 'Save' from the 'Edit Keyword' dialog.
- For the changes in the keyword group 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.

Importing keywords from MySQL Database Server

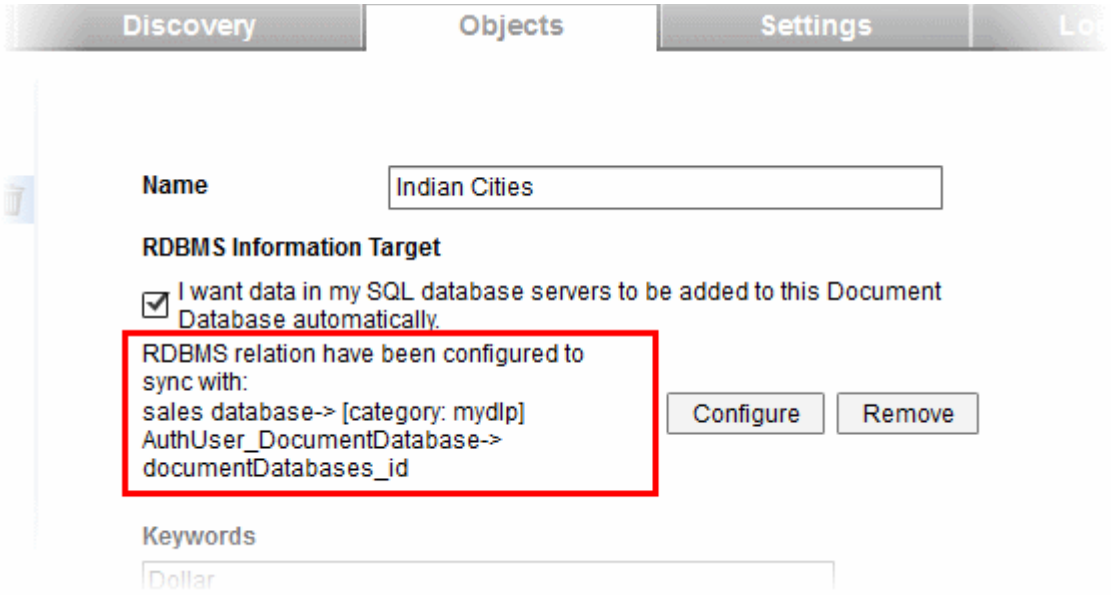
The Edit interface also allows the administrator to import keywords from a MySQL database server through RDBMS connection.

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.

To import keywords from MySQL database

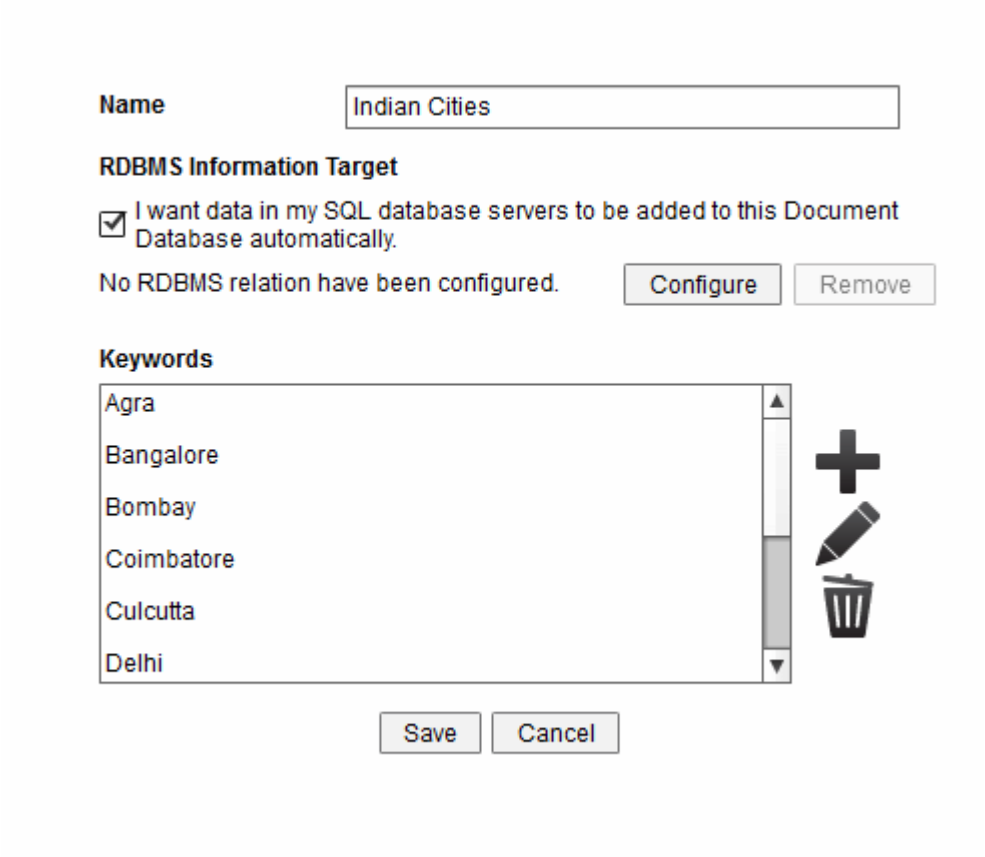
- Expand the Keyword Groups category and select the group. The edit screen will open in the right hand side pane, displaying the name and the component keywords.
- Select the checkbox below 'RDBMS Information Target'

If you have RDBMS Connections configured already, the list of the connections will be displayed.

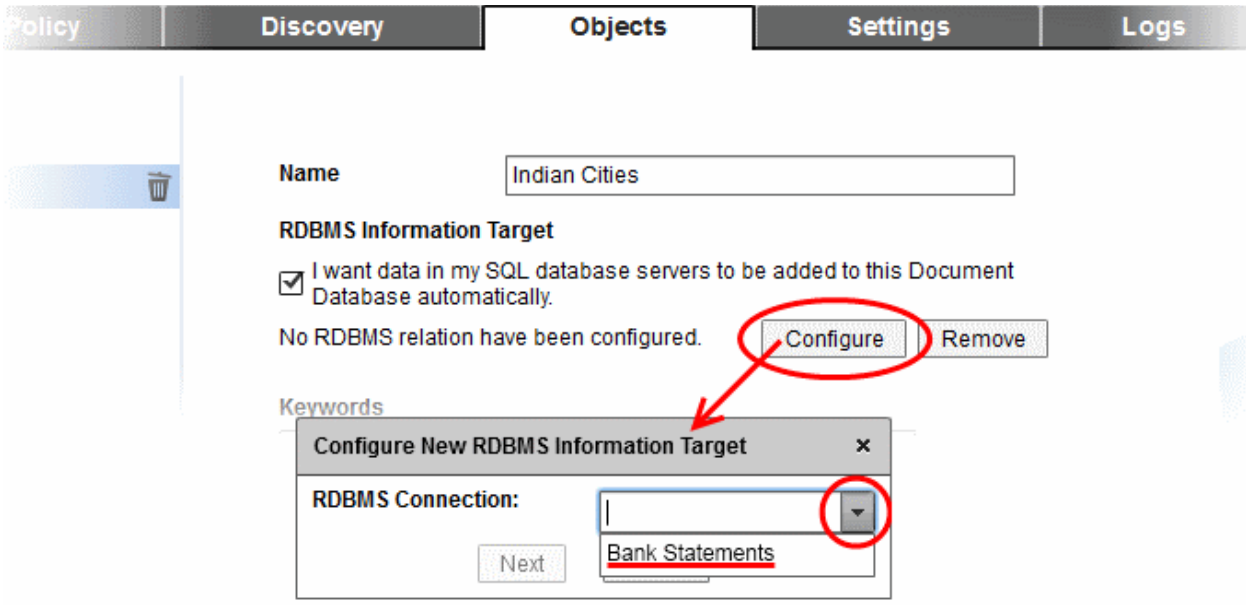


- You can re-configure an existing connection, by clicking 'Configure'.

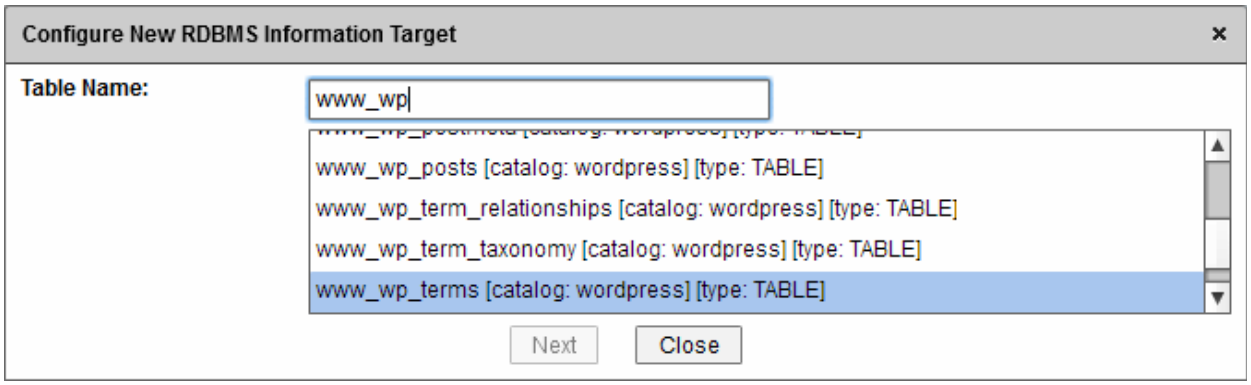
If you do not have have RDBMS connections configured, you can configure from this interface.



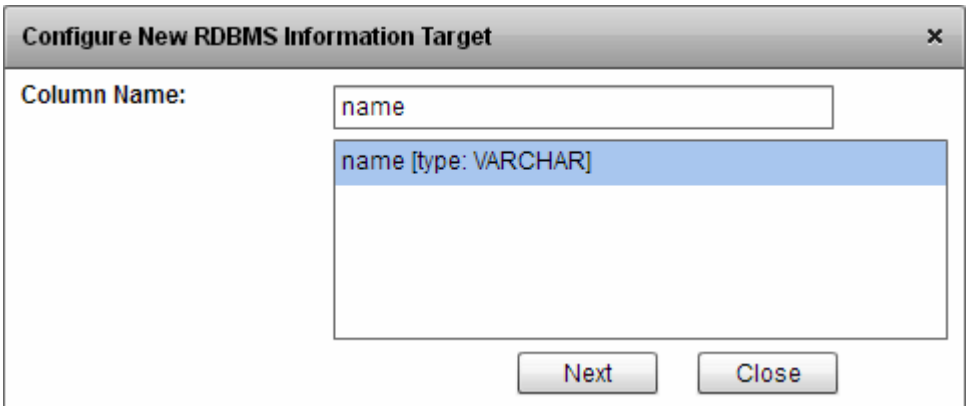
- Click 'Configure'. The Configure New RDBMS Information Target dialog will appear.



- Select the pre-added RDBMS connection from the drop-down.

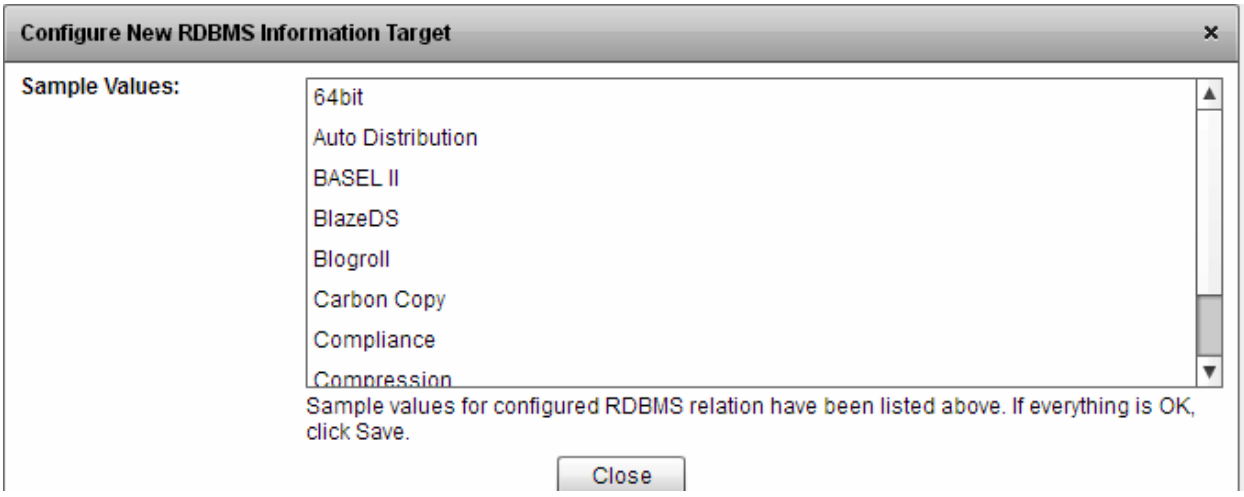


- Select the table from the MySQL database. Type the first few characters of the table name in the Table Name text box. All the tables with the matching names will be displayed in the list below. Select the table from the list and click 'Next'.



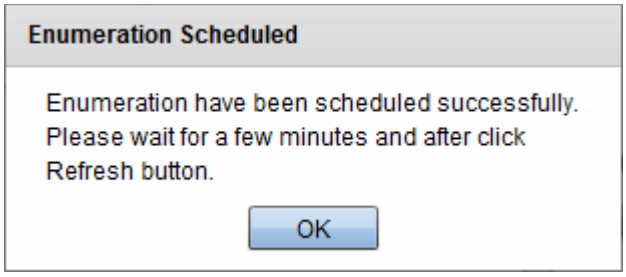
- Enter the column name from which the keywords are to be imported. Type the first few characters of the column header in the Column Name text box. All the column headers with the matching names will be displayed in the list below. Select the column header from the list and click 'Next'.

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 and click 'Close'.
- Click 'Save' from the right hand side pane of the 'Objects' interface.

The database will be checked periodically for updates and all the new entries added to the selected column will be updated to the keyword group. If you want to include all the keywords immediately, click 'Enumerate Now'

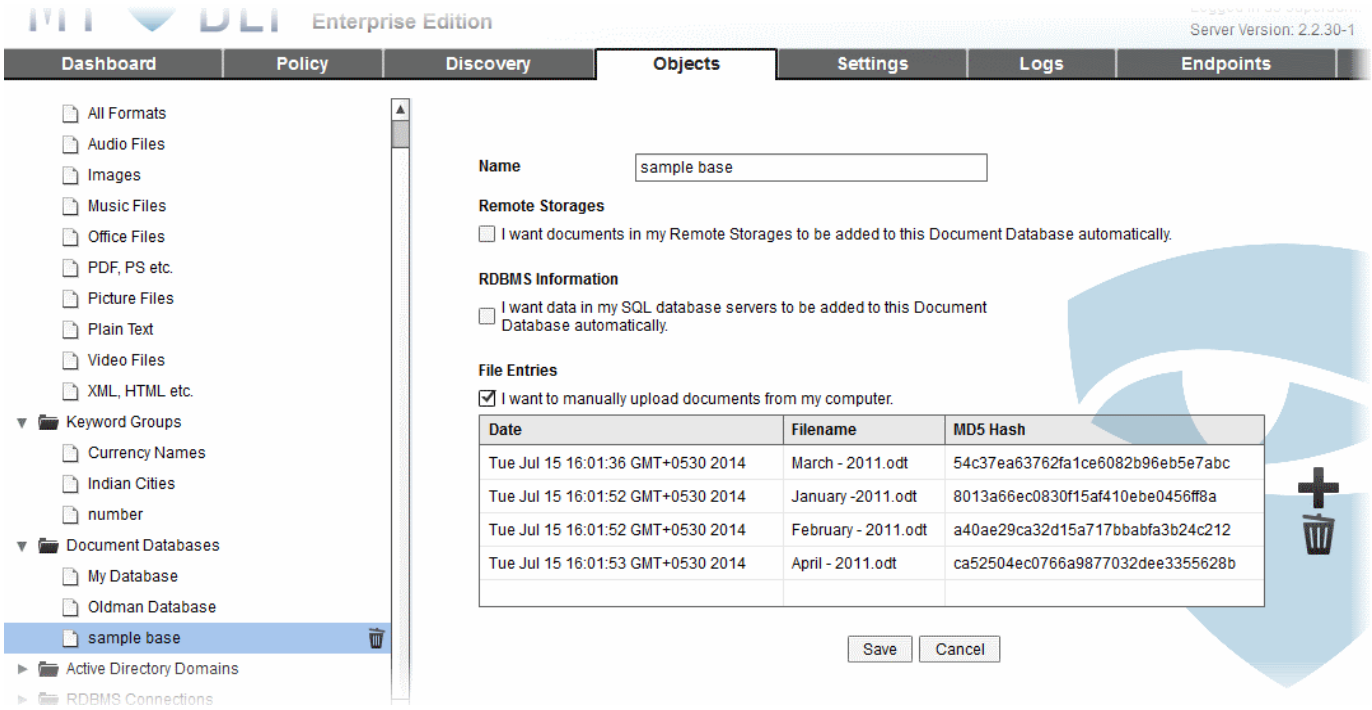


All the keywords from the selected column will be fetched and added to the group.

8.3. 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 'Objects' interface allows the 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.



Refer to the following sections on managing the Document Databases:

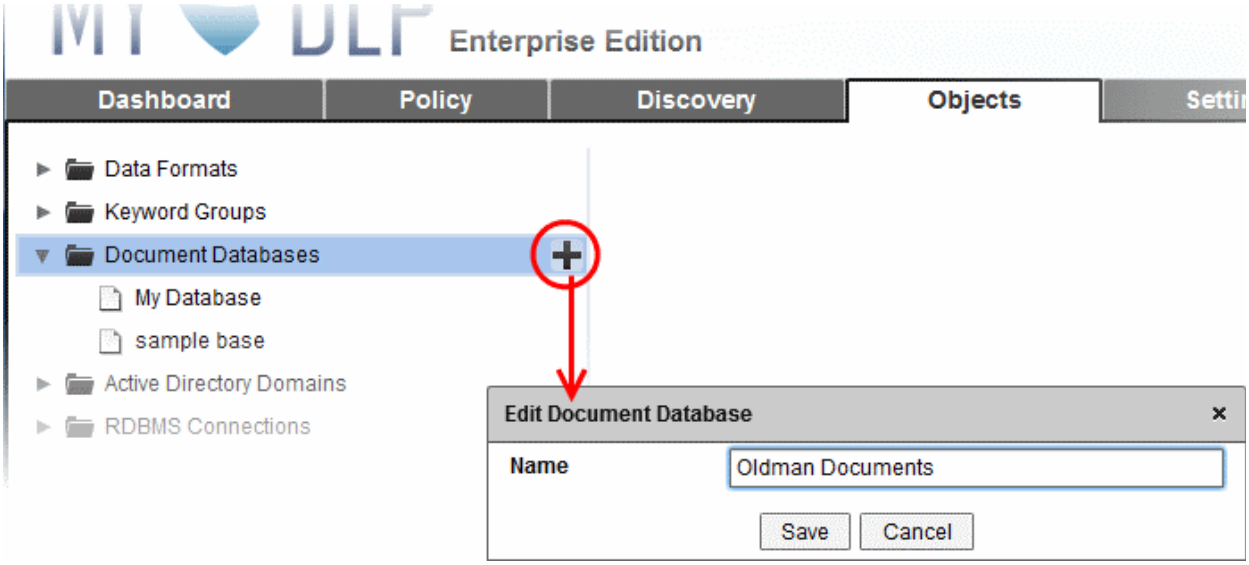
- **Adding a Document Database**
- **Editing a Document Database**

8.3.1. Adding a Document Database

The administrator can create a new document databases and add document files in two steps:

Step 1 - Create a Document Database

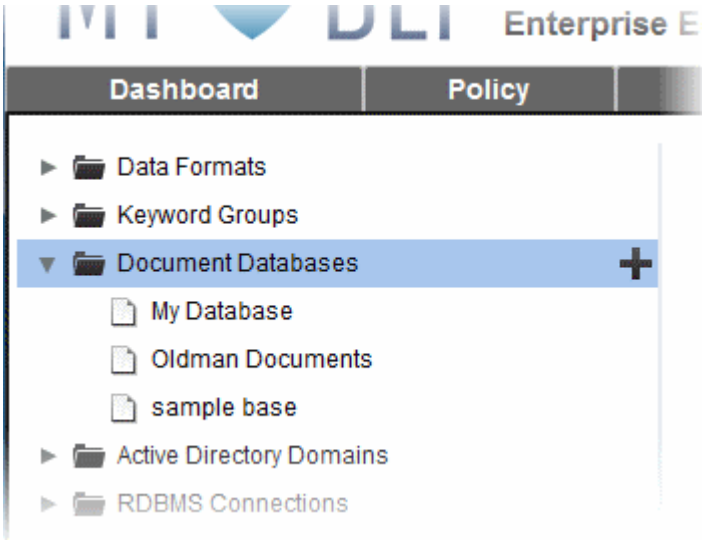
- Select the Document Databases folder from the left hand side pane of the 'Objects' interface and click the plus icon.



The Edit Document Database dialog will open.

- Enter a name for the database and click 'Save'.

The database entry will be saved and listed below the Document Databases category.



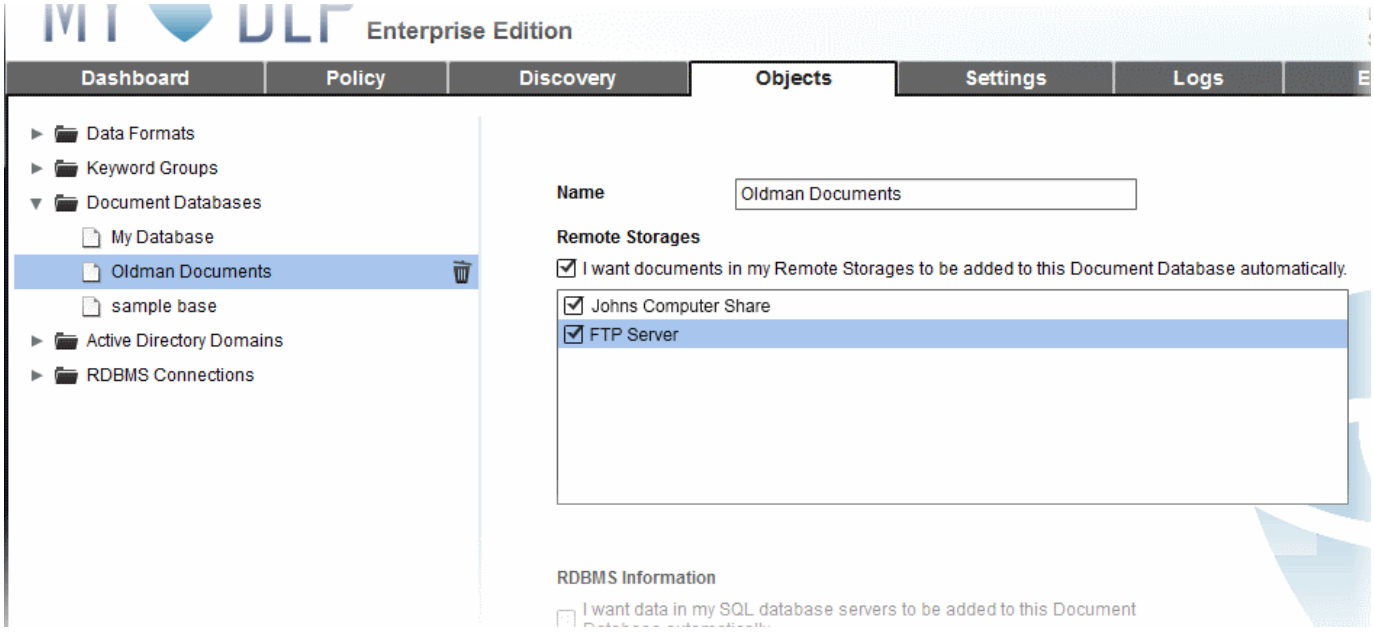
Step 2 - Adding document files to the database

The document files can be added to the database in three ways:

- **Integrating a remote storage location as a document database**
- **Integrating a MySQL database to document database**
- **Manually adding files to the database**

Integrating a remote storage location as a document database

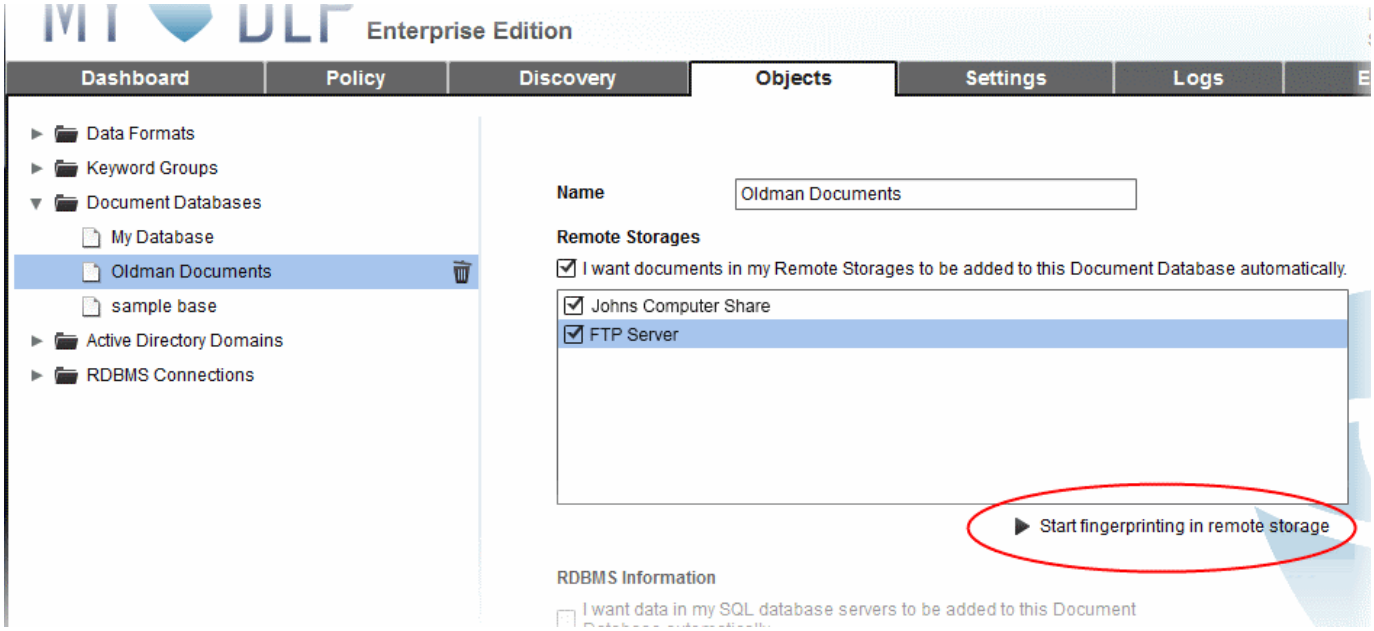
- Expand the Document Databases category and select the database. The edit screen will open in the right hand side pane, displaying the name and the options.
- Select the checkbox under 'Remote Storages'



The user defined Remote Storage objects pointing to the remote storage locations, added to MyDLP under the 'Discovery' tab > 'User Defined' category will be displayed as a list.

- Select the Remote Storages from which you want to import the documents to the Document Database
- Click Save in the Objects interface.

The Remote Storages will be added to the Document Database.



The document database will be available for selection to define the Matcher component while creating in the remote storage. 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, click the 'Start fingerprinting in remote storage' link that appears below the list of remote storages.

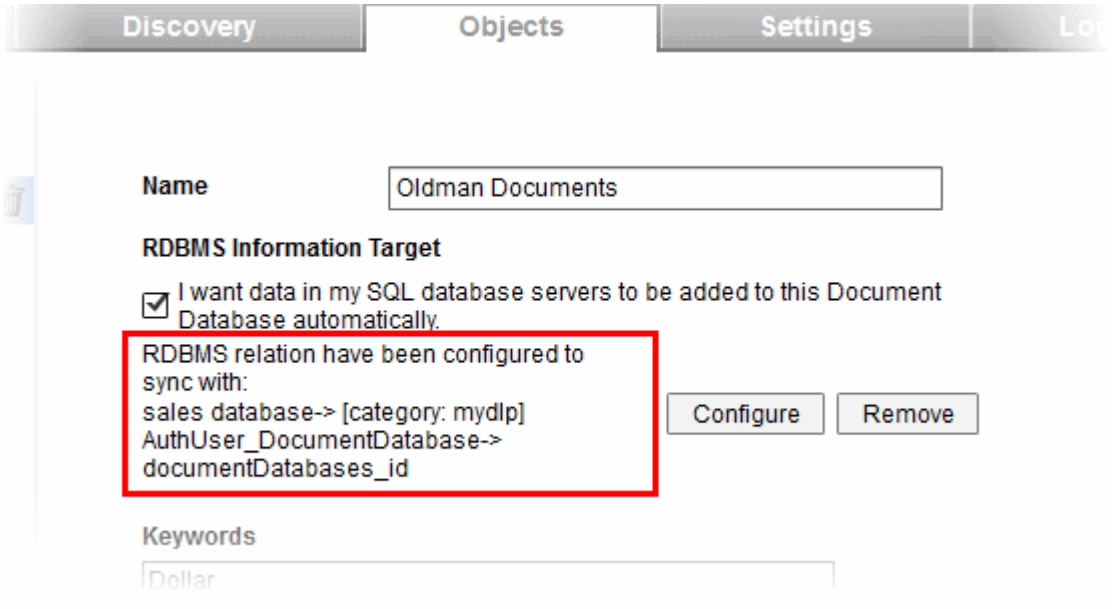
MyDLP will create MD5 Hash values and saves them.

- Click 'Save' in the Objects interface.

Integrating a MySQL Database to Document Database

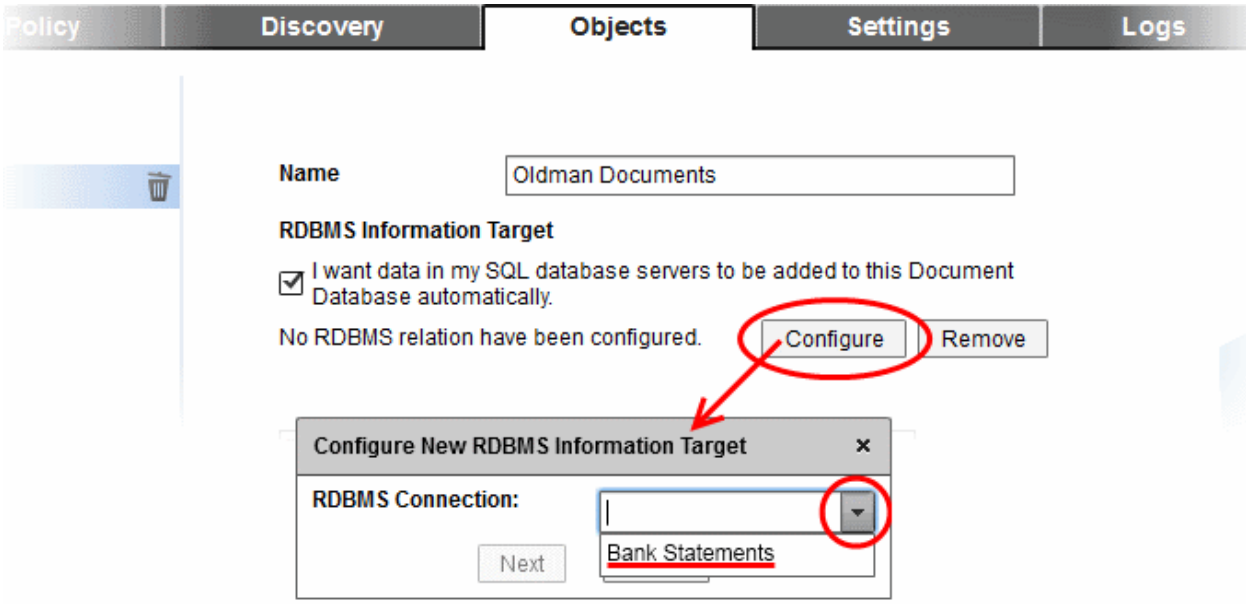
- Expand the Document Databases category and select the database. The edit screen will open in the right hand side pane, displaying the name and the options.
- Select the checkbox under 'RDBMS Information'

If you have RDBMS Connections configured already, the list of the connections will be displayed.

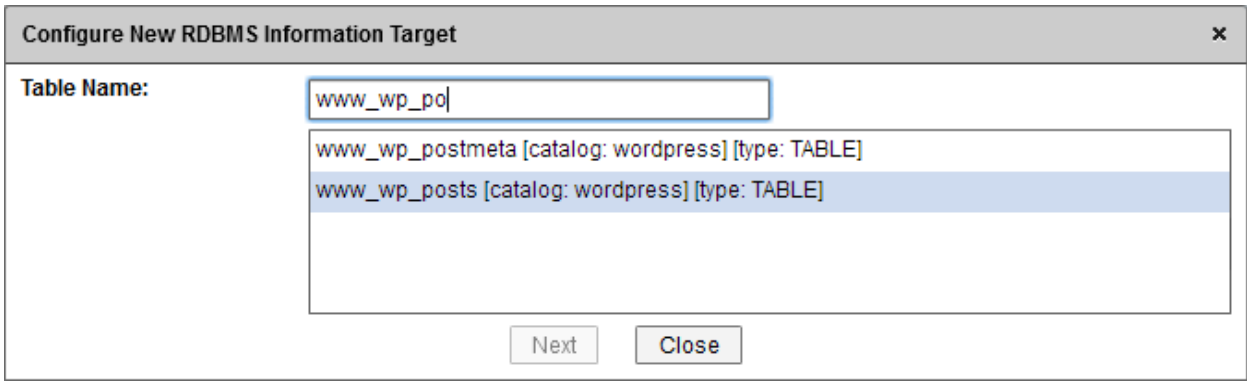


- You can reconfigure the connection by clicking 'Configure'.

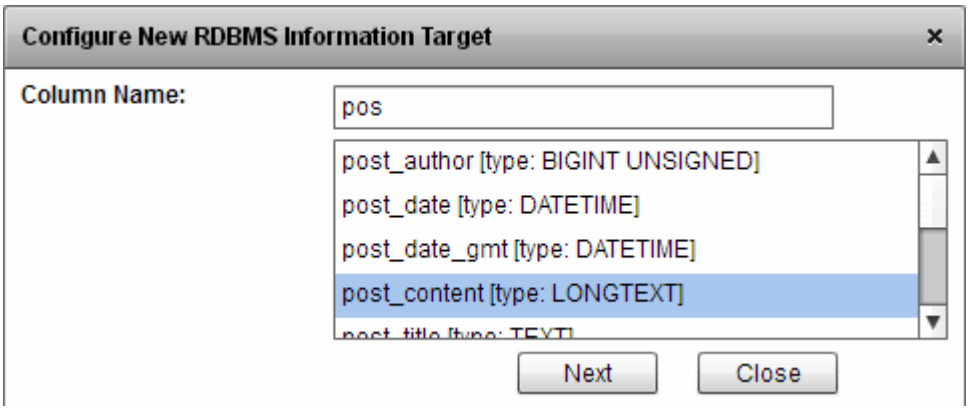
If you do not have have RDBMS connections configured, you can configure from this interface.



- Click 'Configure'. The Configure New RDBMS Information Target dialog will appear.
- Select the pre-added RDBMS connection from the drop-down.

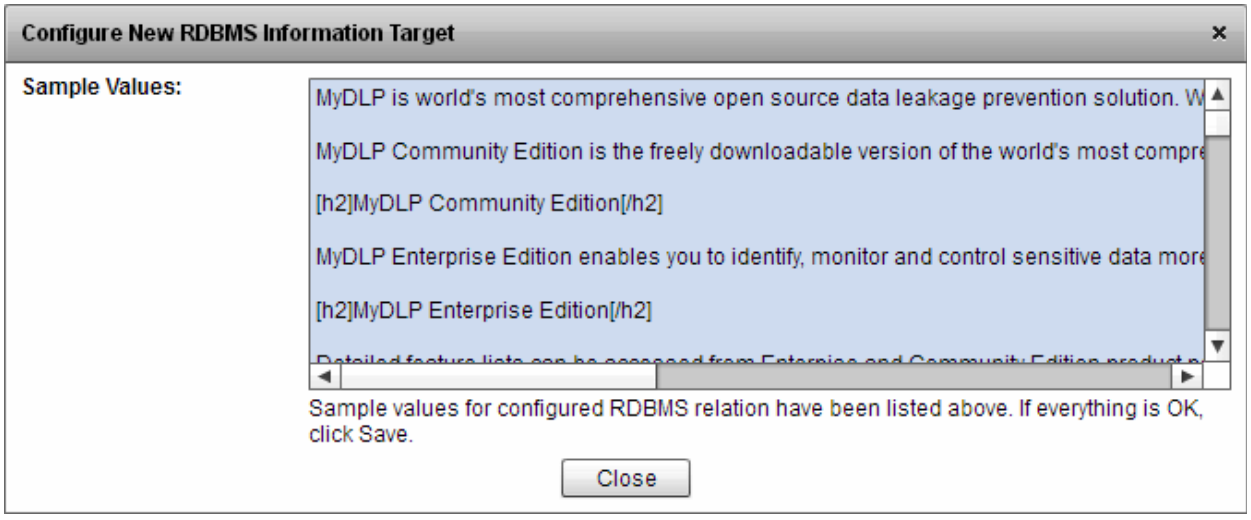


- Select the table from the MySQL database. Type the first few characters of the table name in the Table Name text box. All the tables with the matching names will be displayed in the list below. Select the table from the list and click 'Next'.



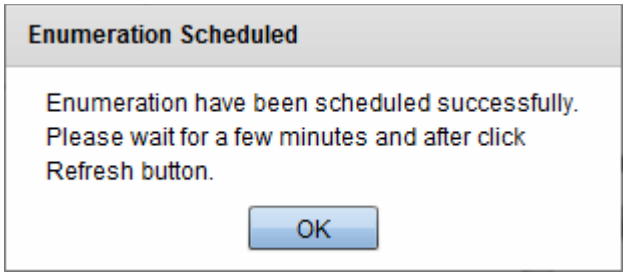
- Enter the column name from which the documents are to be imported. Type the first few characters of the column header in the Column Name text box. All the column headers with the matching names will be displayed in the list below. Select the column header from the list and click 'Next'.

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 document sample and click 'Close'.
- Click 'Save' from the right hand side pane of the 'Objects' interface.

The database will be checked periodically for updates and all the new entries added to the selected column will be updated to the document database. If you want to include all the documents immediately, click 'Enumerate Now'



All the documents from the selected column will be fetched and added to the document database.

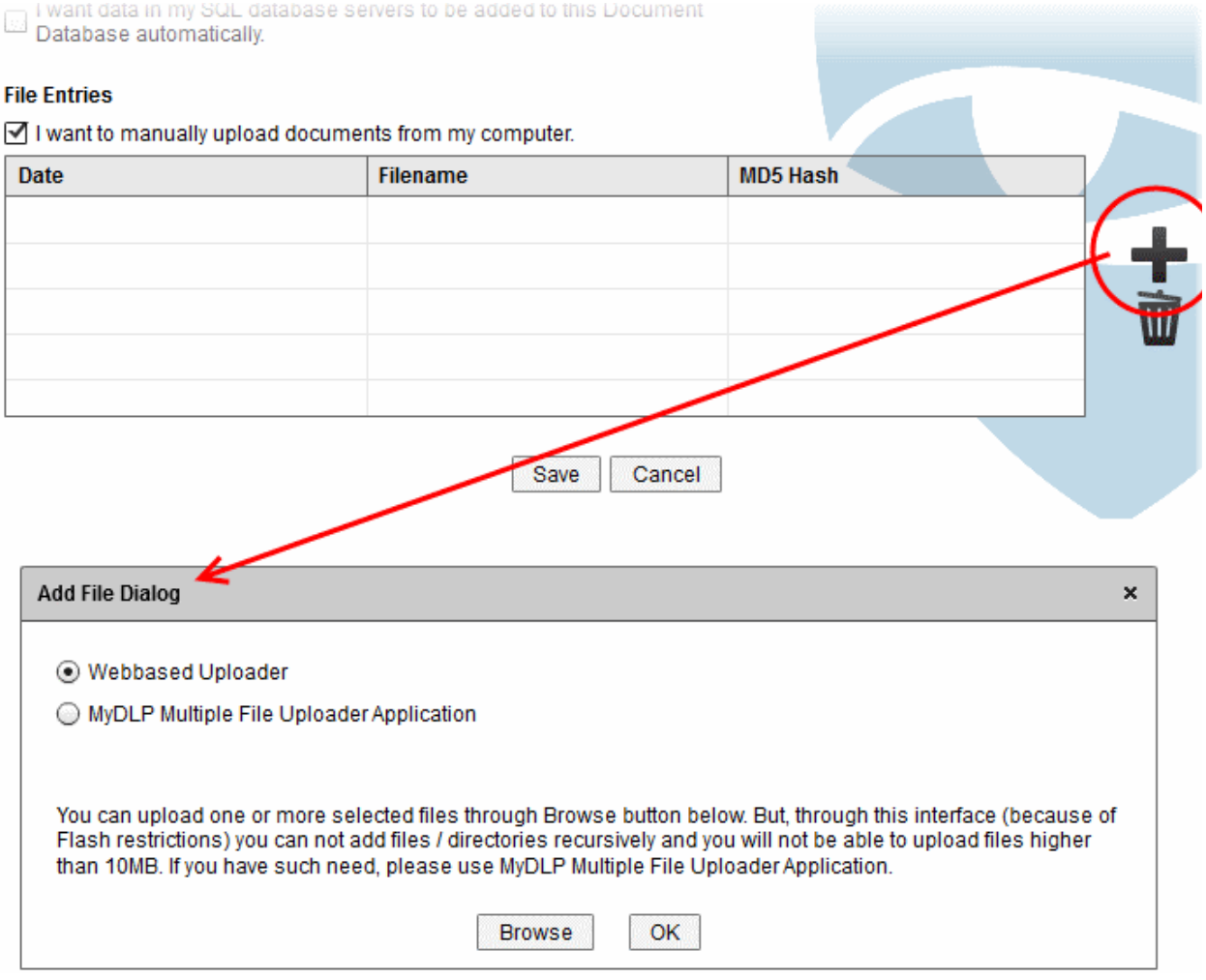
- For the changes in the document database to take effect in the 'Information Type' object in which it is used and in the Rules in which the Information Type object is applied, re-install the policy by clicking the Install Policy at the top right. Refer to the section **Deploying the Policy** for more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

Manually Adding Files to the Database

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

- Expand the Document Databases category and select the database. The edit screen will open in the right hand side pane, displaying the name and the options.
- Select the checkbox under 'File Entries'. A table showing a list of files added will be displayed.
- To add a new file, click the plus icon beside the list.



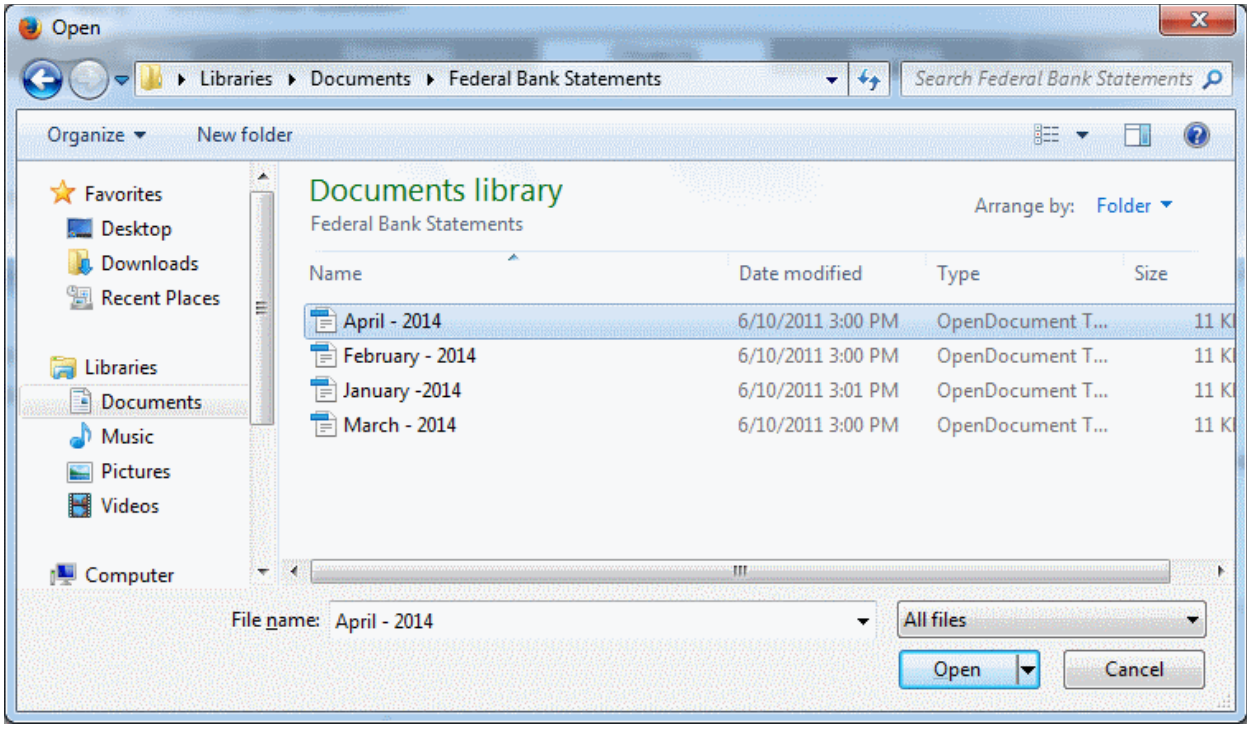
The 'Add File Dialog' will appear. The Files can be manually added to the data base in two ways:

- Uploading the files one-by-one using the Web based uploader
- Uploading the files in a folder at once using MyDLP Multiple File Uploader Application

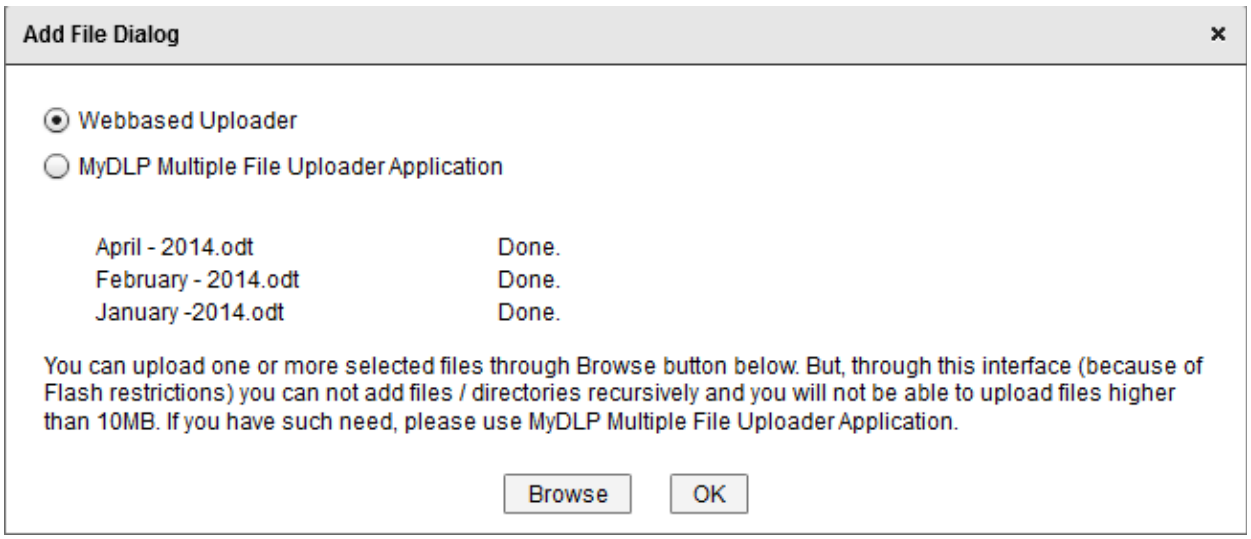
Uploading file one-by-one using the Web based uploader

The Webbased Uploader allows you to files of size less than 10MB from your local drives one-by-one.

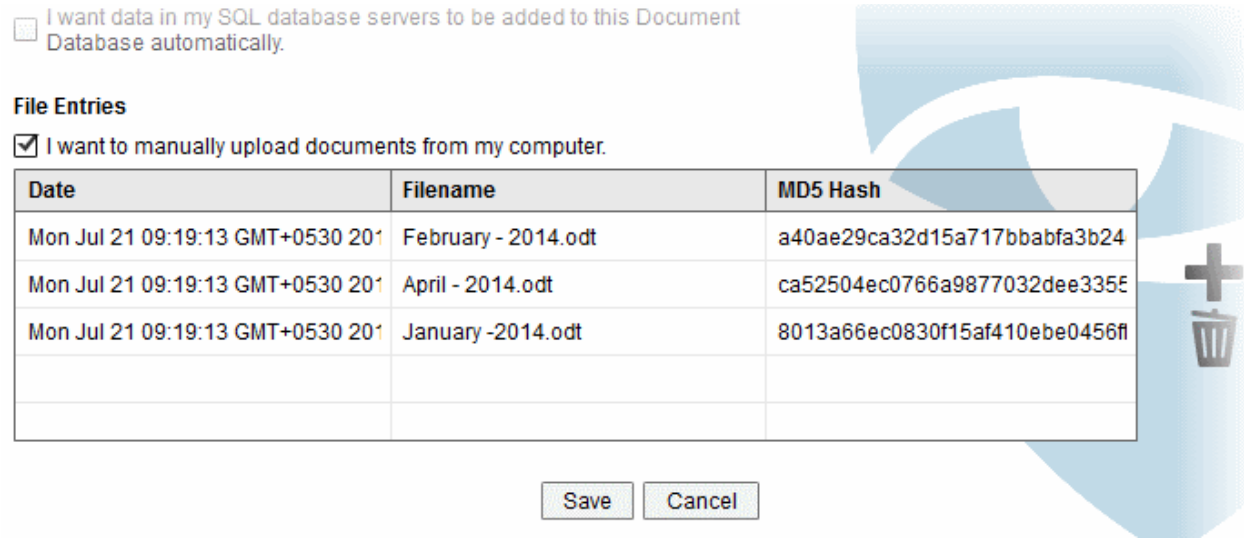
- Select 'Webbased Uploader' from the 'Add File Dialog' and click 'Browse'.
- Navigate to the location of the files and select the files.



- Click Open. The files will be added to the document database...



… and displayed in the list below 'File Entries' with their MD5 hash values.



- Repeat the process to add more files.
- Click 'Save' to save the document database.
- 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.

Uploading the Files in a Folder at once using MyDLP Multiple File Uploader Application

You can upload files and folders of larger sizes recursively by using the MyDLP Multiple File Uploader application. The application first needs to be installed on the computer from which you are uploading the files and folders.

Prerequisite: The MyDLP Multiple File Uploader needs Adobe AIR Package pre-installed on your system. If you do not have Adobe AIR, download the installation package from **http://get.adobe.com/air/** and install the package.

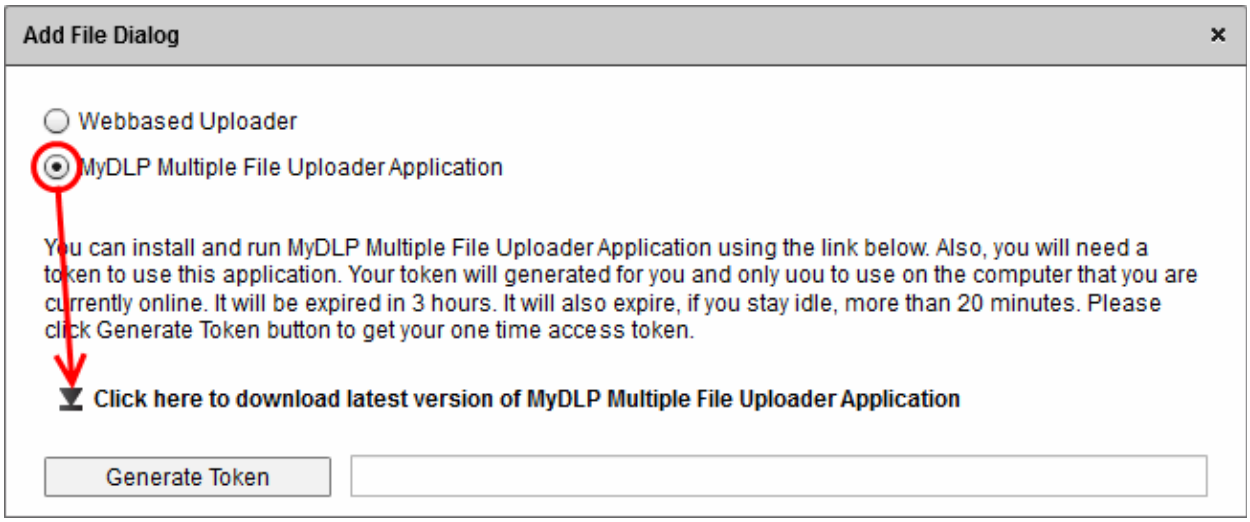
Refer to the following sections for more explanations on:

- **Installation of MyDLP Multiple File Uploader Application**
- **Uploading Files and Folders**

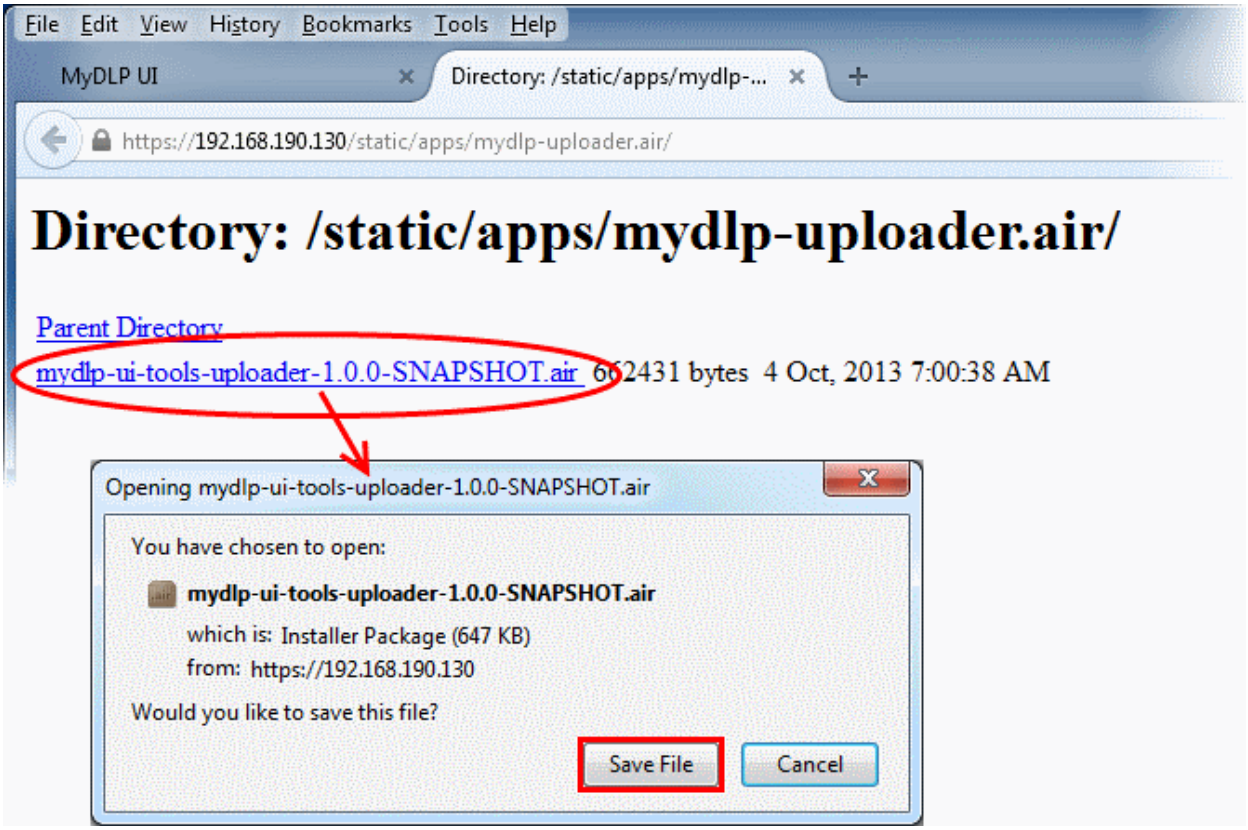
Installation of MyDLP Multiple File Uploader Application

You can download the Multiple File Uploader application from the Add File Dialog.

- Select 'MyDLP Multiple File Uploader' from the 'Add File Dialog'.

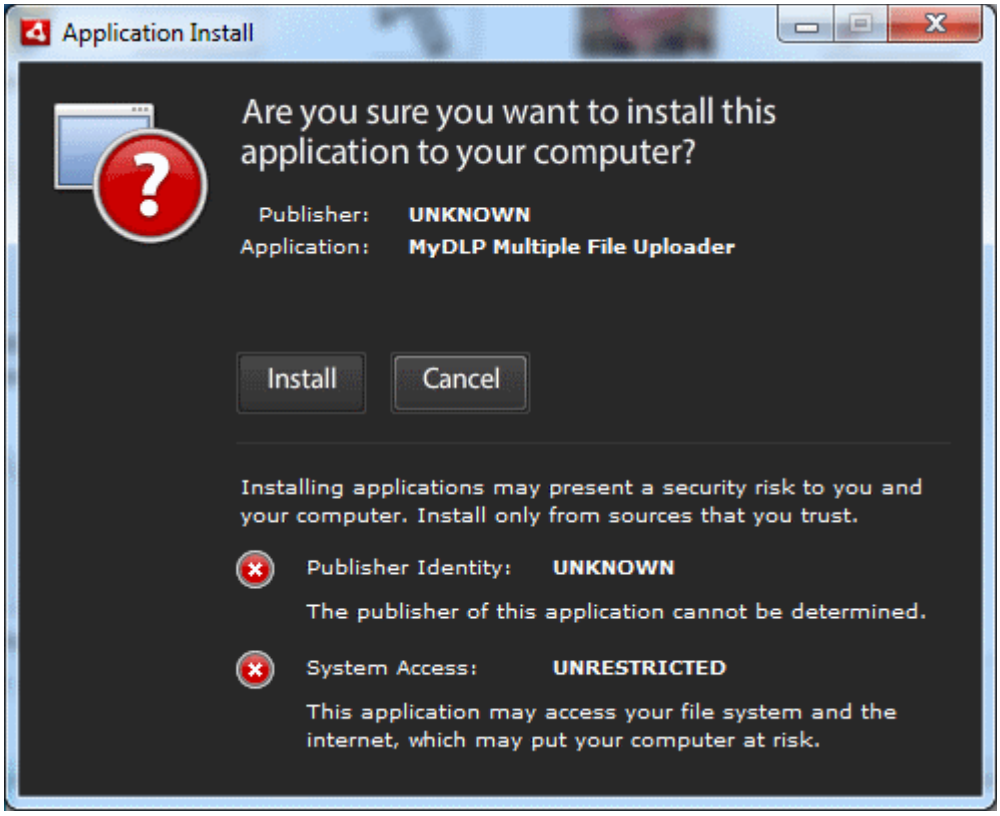


- Click the icon. You will be taken to the download page in a new browser tab.
- Click the 'mydlp-ui-tools-uploader-1.0.0-SNAPSHOT.air' link

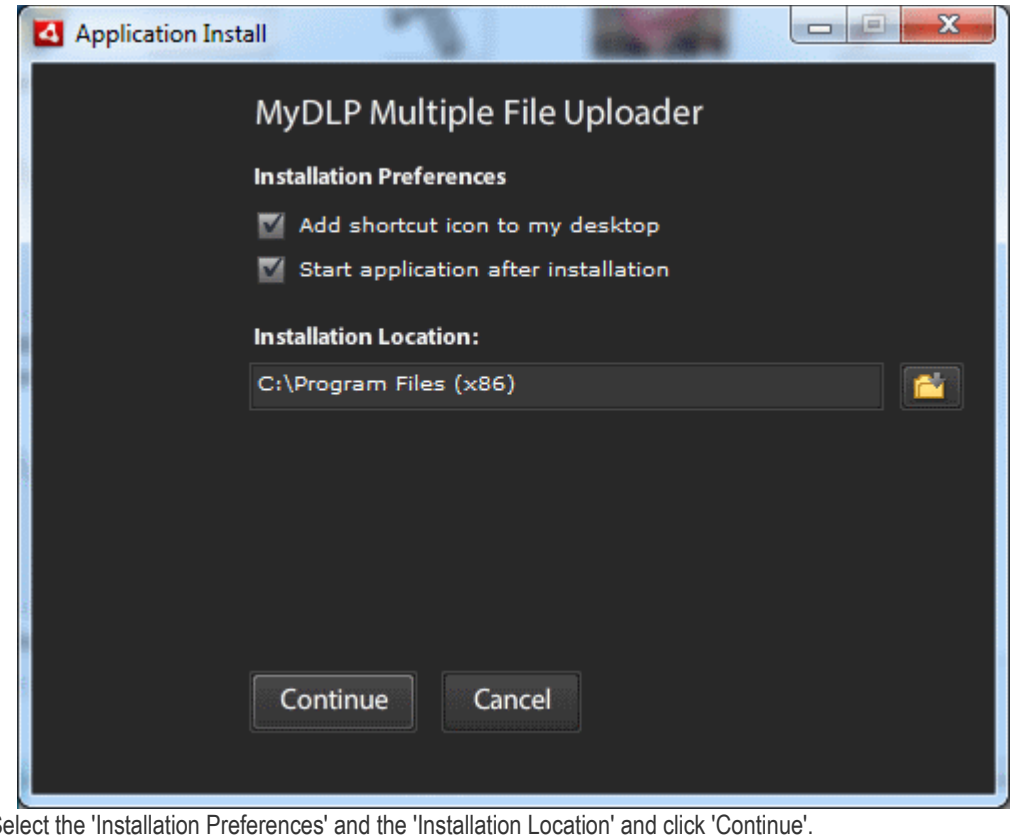


- Save the installation package.
- On completion of download, double click on the installation package file 

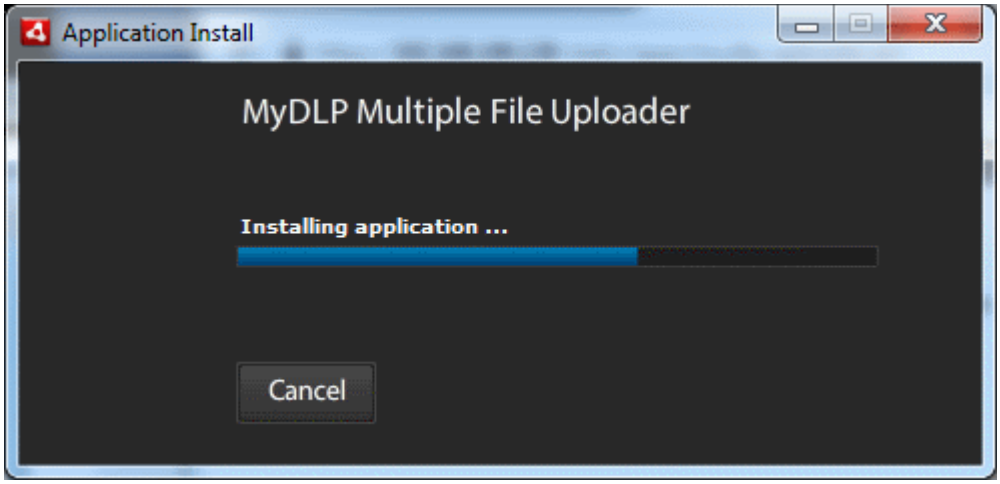
to start the installation. The installation wizard will start.



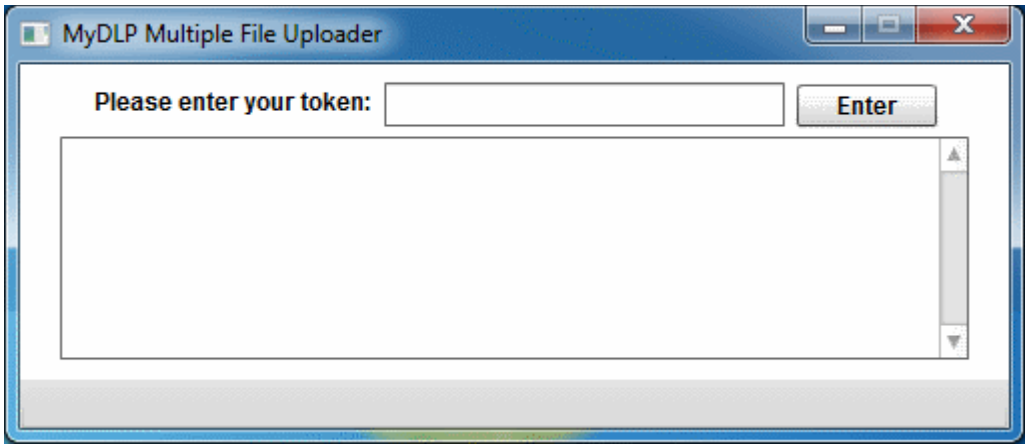
- Click 'Install'. The 'Installation Configuration' screen will appear.



- Select the 'Installation Preferences' and the 'Installation Location' and click 'Continue'.



The application will be installed and on completion, the uploader application interface will appear.

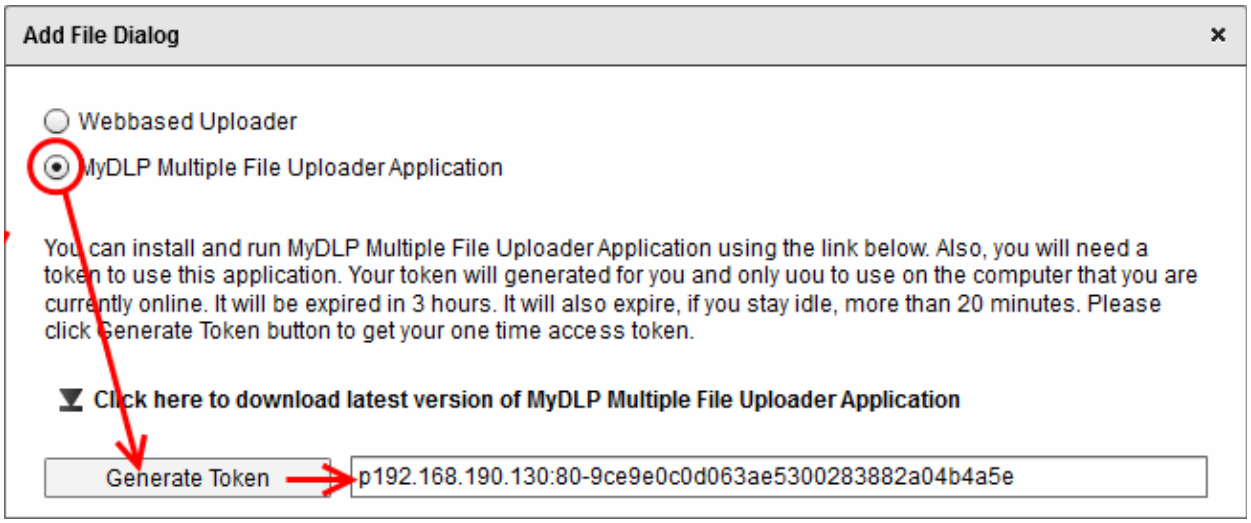


Uploading Files and Folders

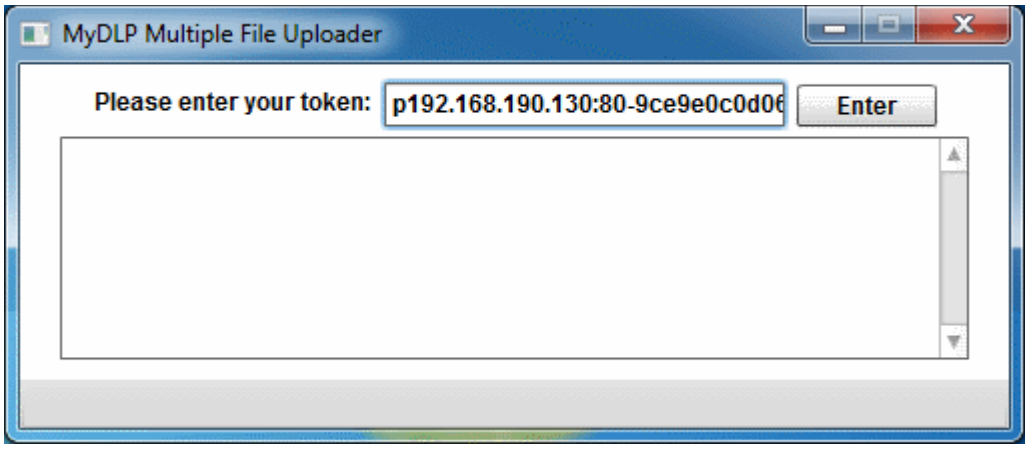
MyDLP generates an one time use tokens for each document file upload session. The token serves for creating a unique secure channel for file transfer between the endpoint computer from which the administrative console is accessed and the MyDLP server. The life time of the key is three hours and the idle tome out period is twenty minutes. You can generate a new key every time the previous key expires due to the life time or being continuously idle for twenty minutes.

To upload files/folders using the pre-installed multiple file uploader

- Select 'MyDLP Multiple File Uploader' from the 'Add File Dialog'.
- Click 'Generate Token'. The token string will be generated and displayed in the text box.

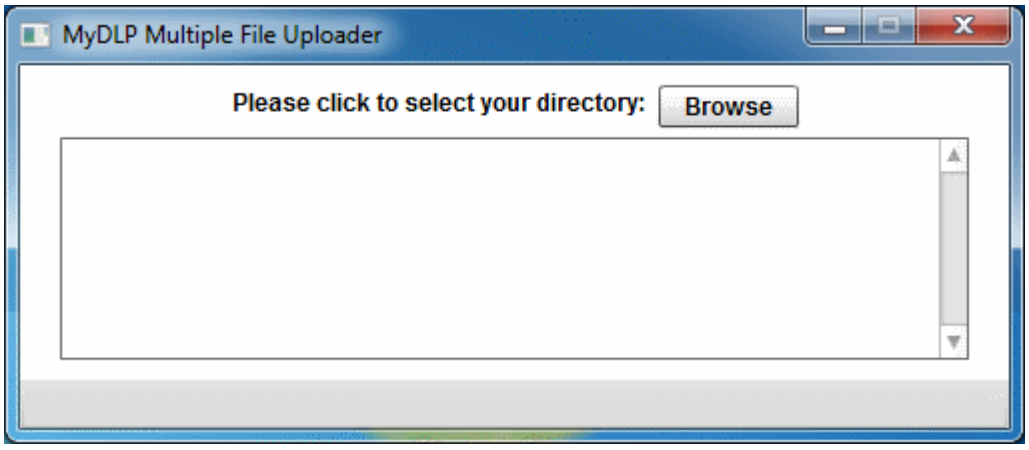


- Start the MyDLP Multiple File Uploader application from the Windows Start menu.

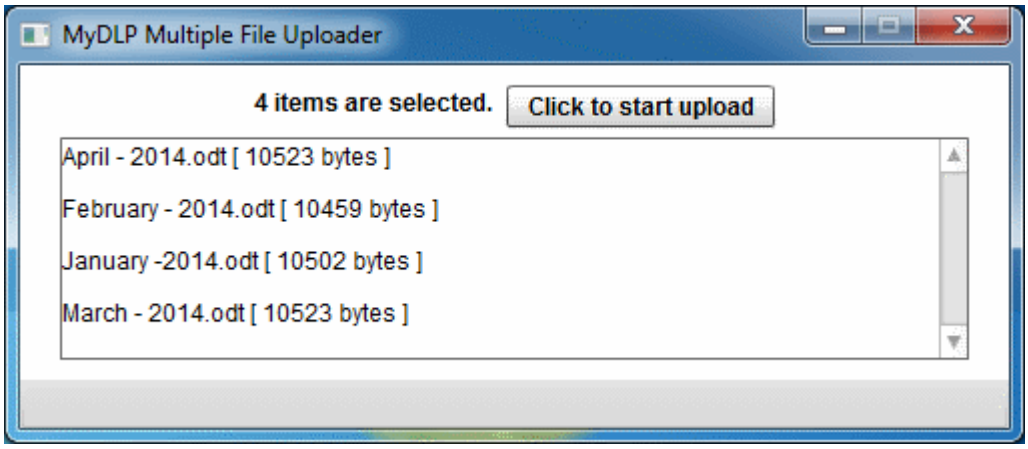


- Copy and paste the token into the textbox at the top and click 'Enter'.

Once the Token is accepted, a secure session channel will be created and the Browse button will appear.



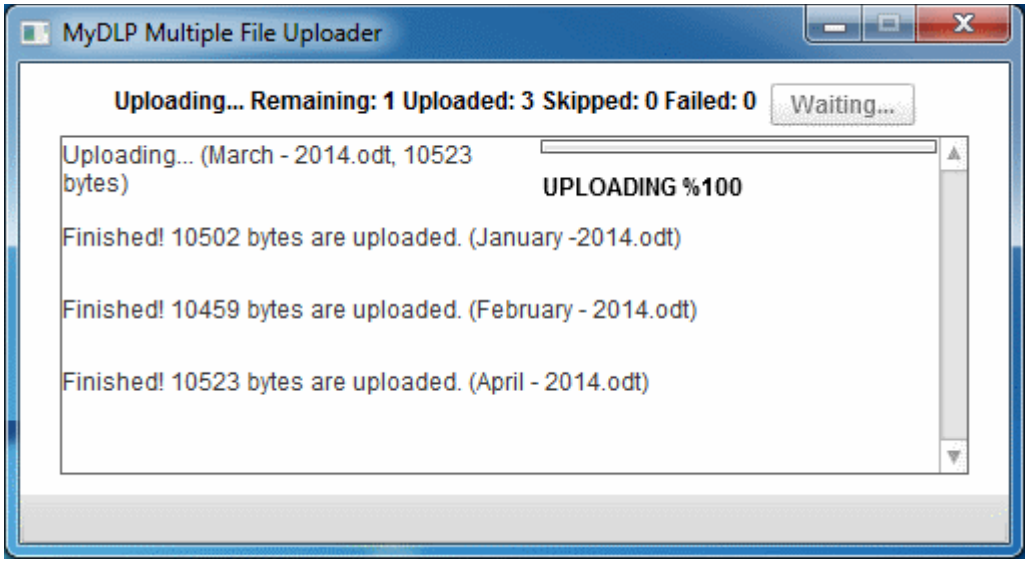
- Click 'Browse' and navigate to the folder containing the files to be added to the document database.



All the files in the folder will be included for uploading and displayed as a list.

- Confirm that you have chosen the correct directory and click 'Click to start upload'.

The files will be uploaded one-by-one.



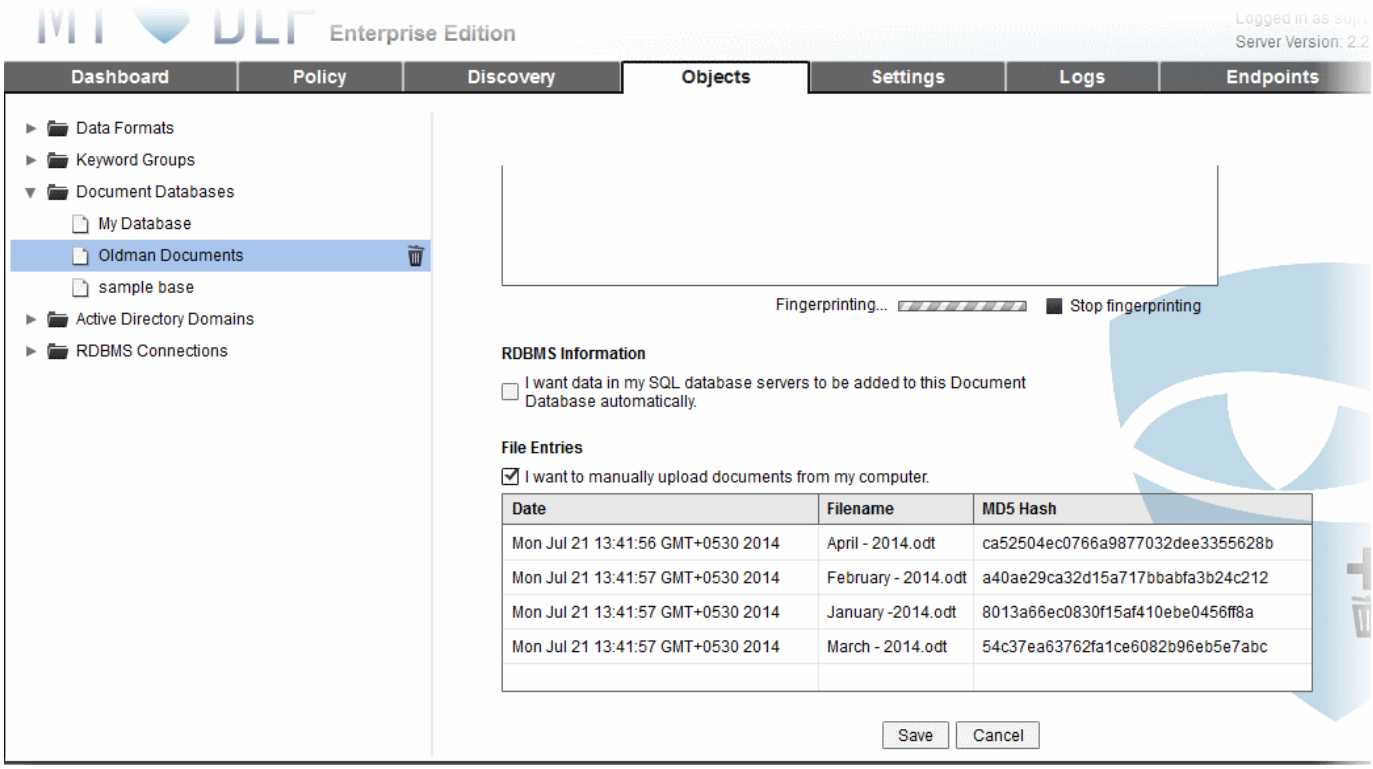
- On Completion click Close to terminate the session.
- Repeat the process for adding more files from different folders to the document database.
- Click 'Save' from the 'Objects' interface.
- For the changes in the document database to take effect in the 'Information Type' object in which it is used 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.

8.3.2. Editing a Document Database

The administrator can add new documents to or removing unnecessary documents from any database from the Objects interface. The changes will take effect immediately on reapplying the policy to the network.

To edit a document database

- Expand the Document Databases category and select the database. The edit screen will open in the right hand side pane.



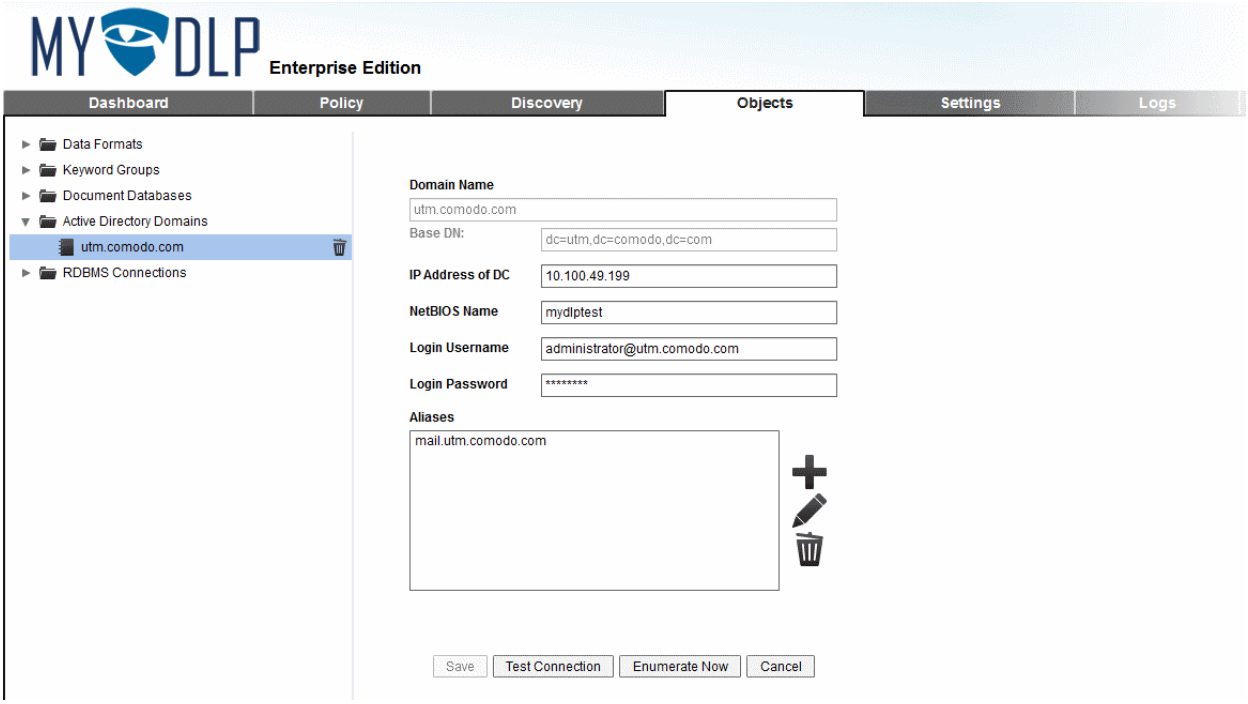
All the files included in the document database, imported from the remote storage or MySQL database or or by manually adding the files will be displayed as a list under 'File Entries' with their MD5 hash values.

- To remove a document file, select the file and click the Trash Can icon .
- To add a new remote storage fro importing the documents from it, select the checkbox under 'Remote Storages' and choose the remote storage object displayed in the text box. Refer to the section explaining '**Integrating a remote storage location as a document database**' in the previous section **Adding a Document Database**.
- To integrate a new MySQL database or import documnt files from a pre-added database, select the checkbox below 'RDBMS Information' and select the database tables and columns. Refer to the section explaining **Integrating a MySQL database to document database** in the previous section **Adding a Document Database**.
- To add files and folders from the local drives of the computer from which the administrative console is accessed, click the plus button beside 'File Entries' and use the 'Webbased uploader' or 'MyDLP Multiple File Uplaoder' application. Refer to the section explaining **Manually adding files to the database** in the previous section **Adding a Document Database**.
- 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.

8.4. 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 'Objects' interface allows the administrator to integrate AD domains which in-turn, can be used in User objects.



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

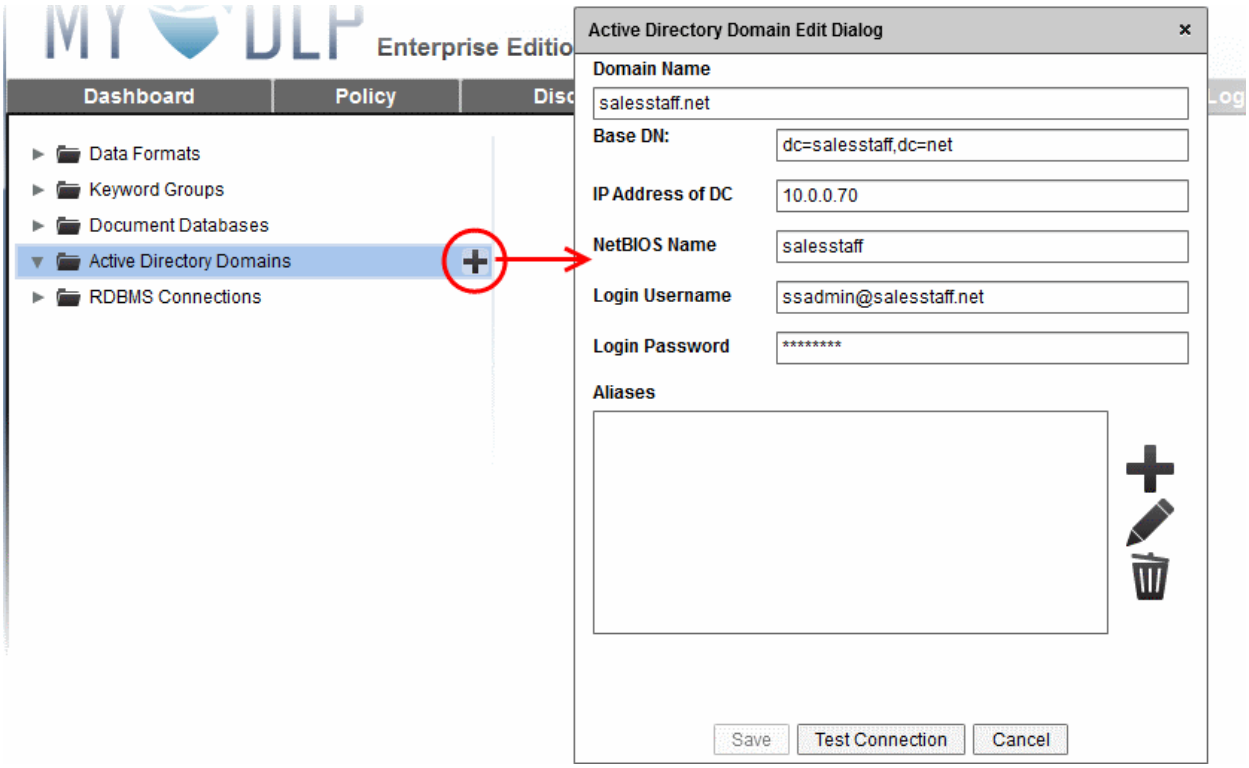
- **Adding new AD Domains**
- **Edit Existing Domains**

8.4.1. 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

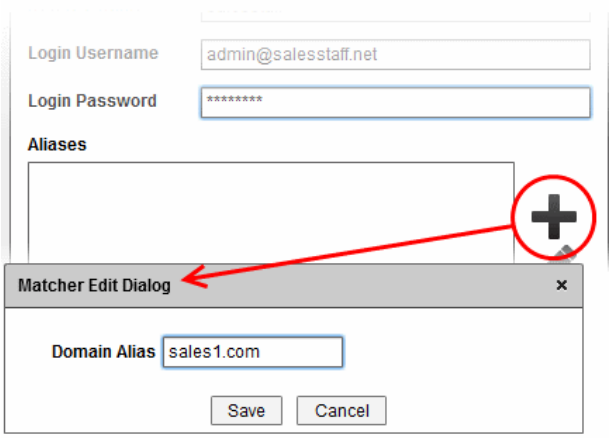
- Select the 'Active Directory Domains' folder from the left hand side of the Objects interface and click the plus icon.



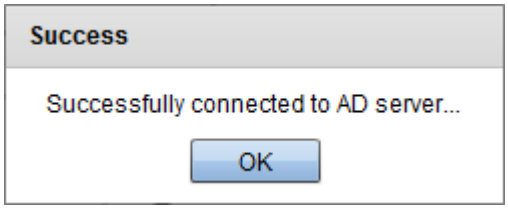
The 'Active Directory Domain Edit Dialog' will appear.

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

Field	Description

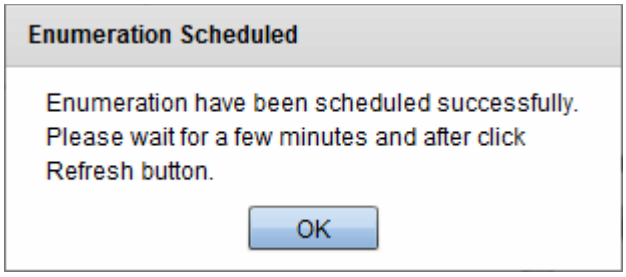
Domain Name	Enter the Fully Qualified Domain Name (FQDN) of your domain as defined in your Domain Controller (DC).
Base DN	The Base DN will be automatically populated based on your FQDN.
IP Address of DC	Enter the IP address or the DNS resolvable hostname of your Domain Controller. If you have more than 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..
Aliases	If you have domain aliases for email addresses of the users in your AD domain, enter the aliases one by one. To add the alias names • Click the plus button. The Matcher Edit Dialog will appear. • Enter the alias name for the name and click Save. The alais name will be added. • Repeat the process for adding more alias names. 

- Click 'Test Connection'. MyDLP will check whether the AD server is reachable. On successful connection, the 'Save' button will be enabled.

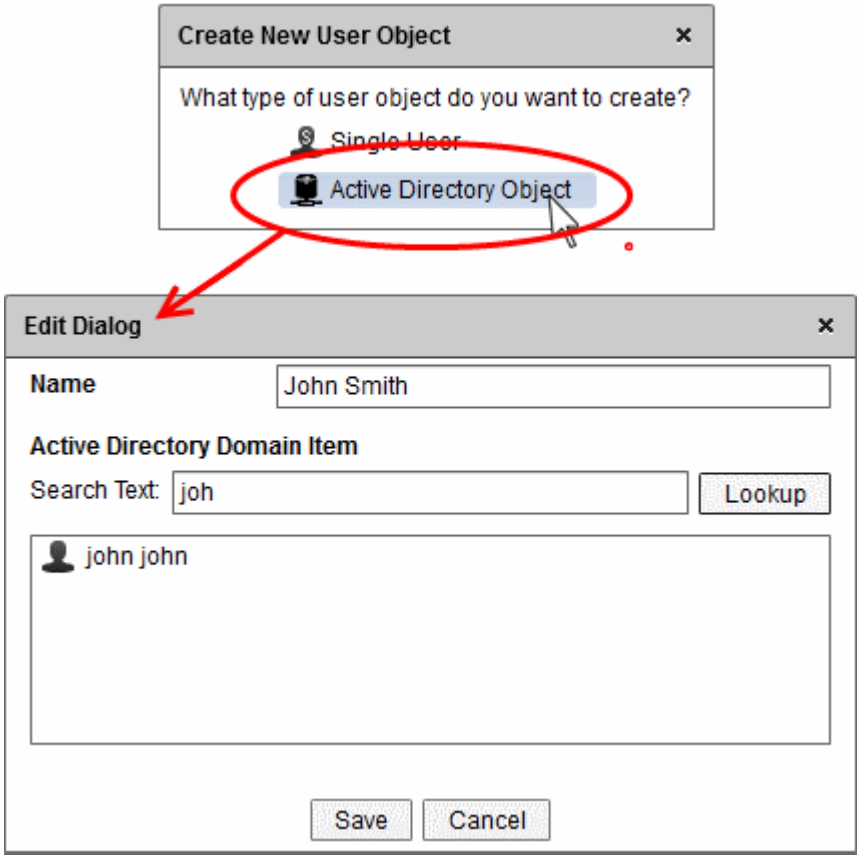


9. Click 'Save'.

The AD Server will be checked periodically for updates and all the entries will be imported. If you want all the users to be imported immediately, click 'Enumerate Now'



All the users will be imported and will be available for selection while creating User objects.

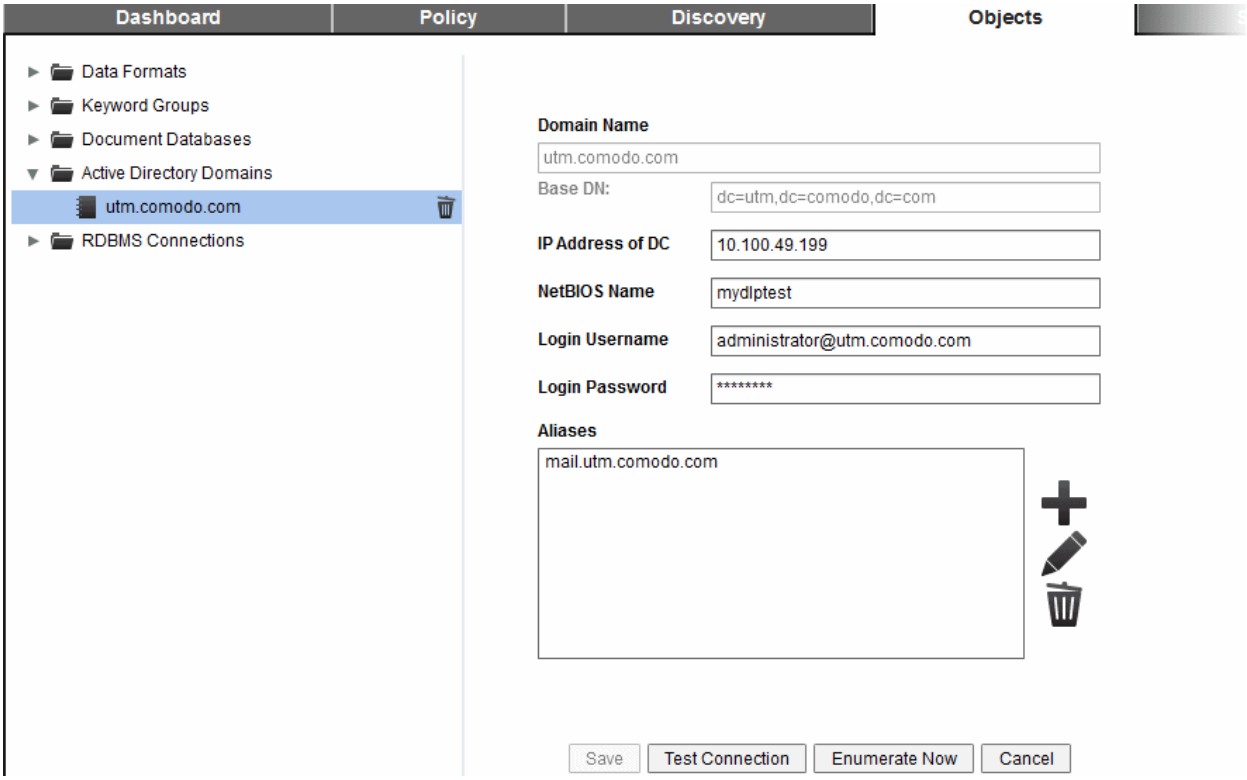


8.4.2. Editing Existing AD Domains

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

To edit an AD Domains

- Expand the Active Directory Domains category and select the AD Domain. The edit screen will open in the right hand side pane.



The Edit interface is similar to the 'Active Directory Domain Edit 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.

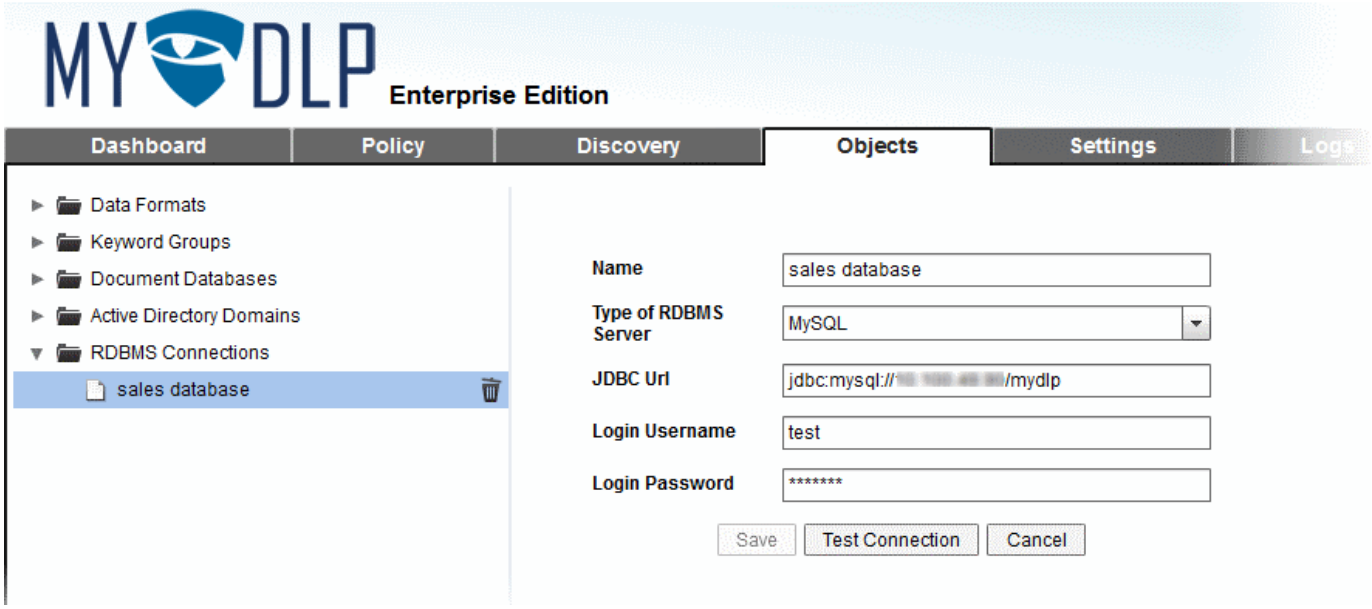
8.5. Integrating RDBMS Systems

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 Objects 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:

- **Importing keywords from MySQL Database Server**
- **Integrating a MySQL database to document database**

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



Refer to the following sections for more details on:

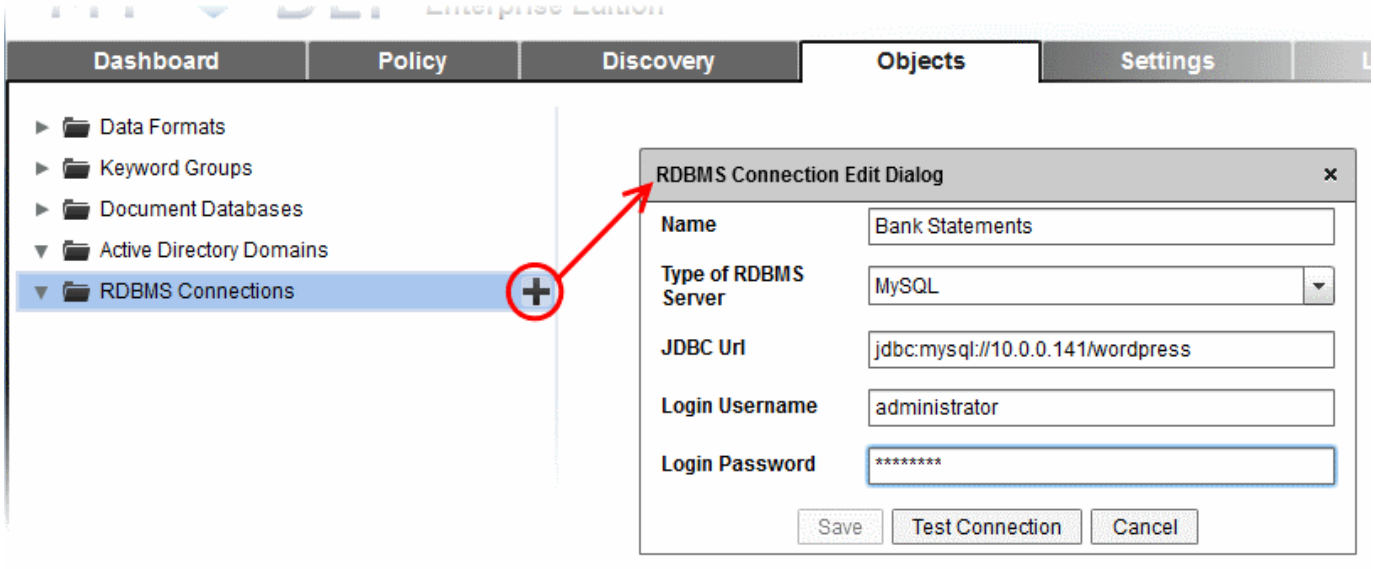
- **Adding a new RDBMS connection**
- **Editing an RDBMS Connections**

8.5.1. Adding a New RDBMS Connection

The administrator can add a new RDBMS connection to integrate MySQL 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 AD Domain

- Select the 'RDBMS Connections' folder from the left hand side of the Objects interface and click the plus icon.



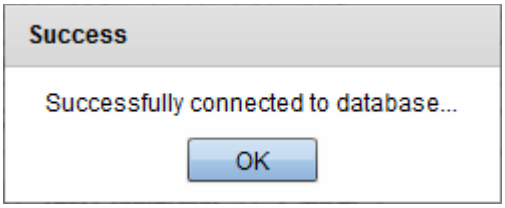
The 'RDBMS Connection Edit Dialog' will appear.

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

Field	Description
Name	Enter a name shortly describing the connection.
Type of RDBMS Server	Choose the type of server from the drop-down. Currently only 'MySQL' is available. More database server types will be added in the future versions.

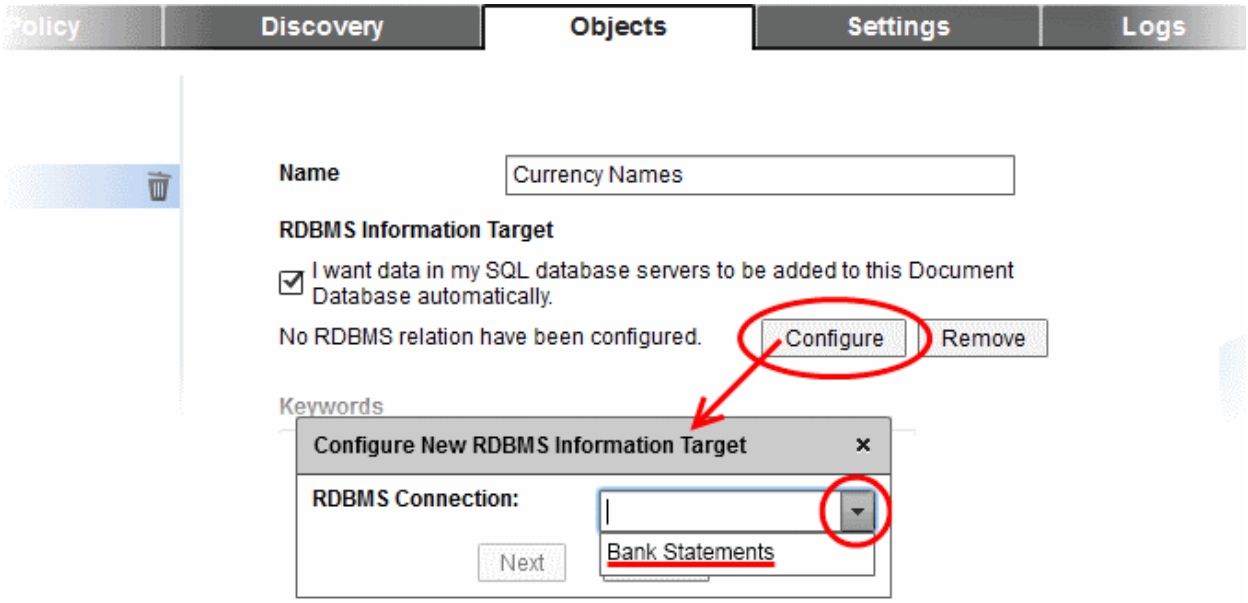
JDBC URL	Enter the Java Database Connectivity (JDBC) URL of the RDBMS server
Login username and Login password	Enter the username and password of a valid user account for MyDLP to login to the RDBMS server. For security reasons, it is advised to create a new account for Comodo MyDLP with only the required privileges to enumerate all users and groups in your AD domain..

- Click 'Test Connection'. MyDLP willl check whether the RDBMS server is reachable. On successful connection, the 'Save' button will be enabled.



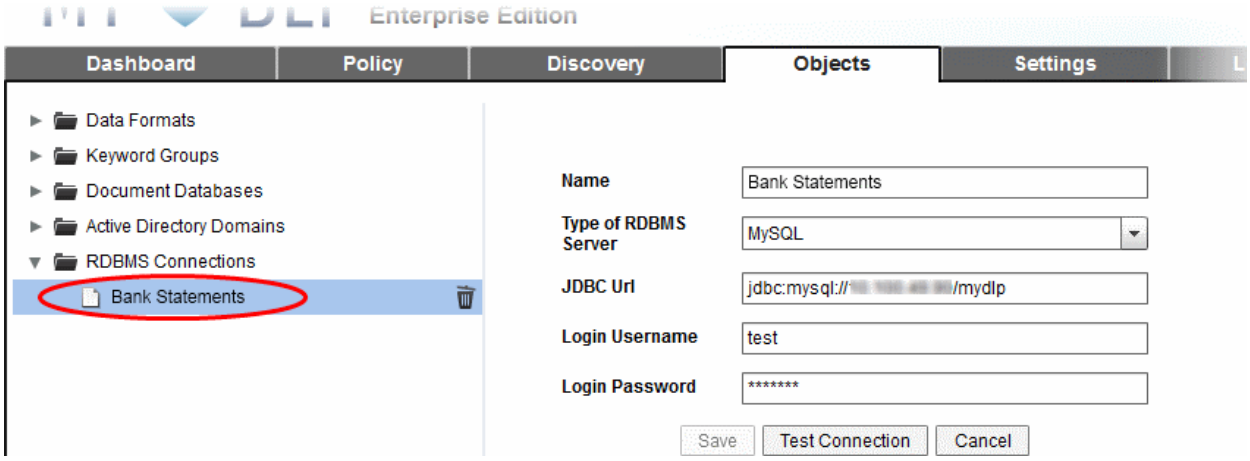
- Click 'Save'.

The RDBMS server will be connected to MyDLP and will be available for selection for importing keywords or documents when creating Keyword Groups and Document Databases under the Objects interface.



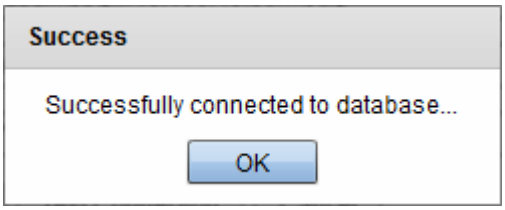
8.5.2. Editing an RDBMS Connections

The administrator can view the details of and edit an RDBMS connecton at any time by selecting the connection from the Objects > RDBMS interface.



To change the parameters, directly edit the parameters

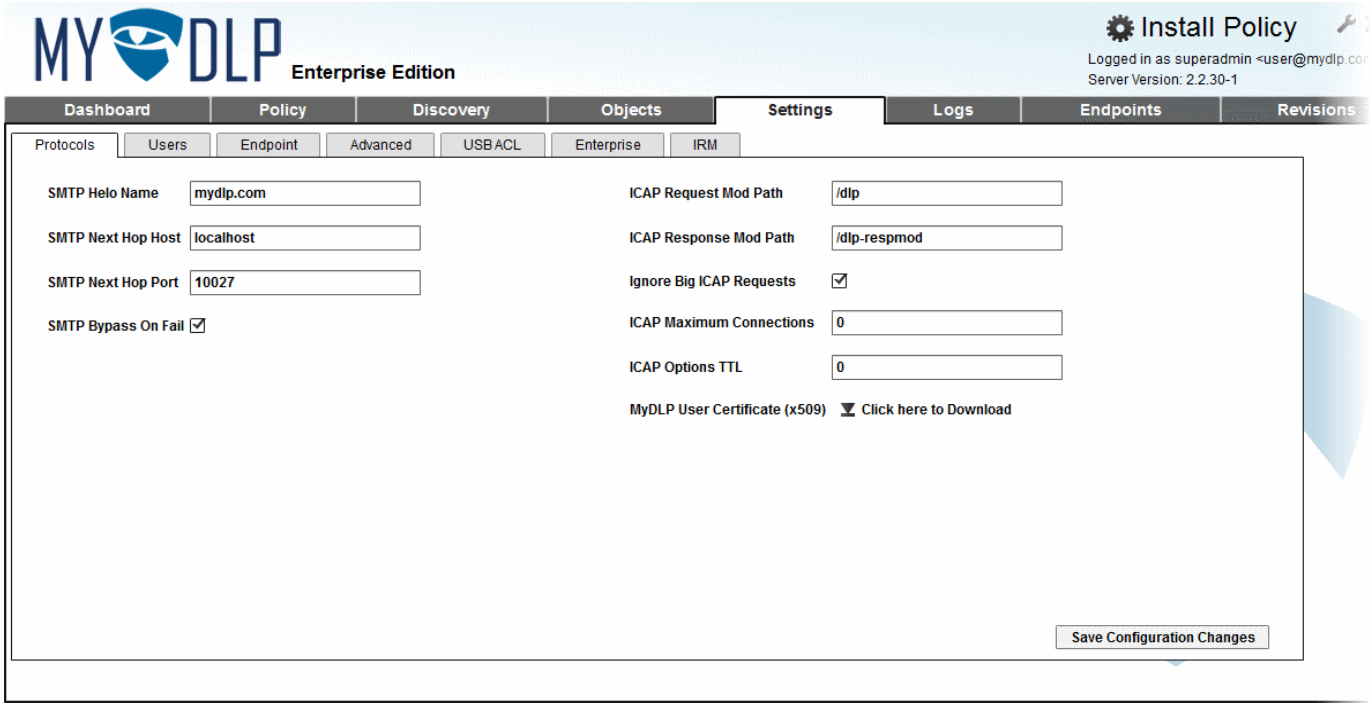
- Click 'Test Connection'. MyDLP willl check whether the RDBMS server is reachable. On successful connection, the 'Save' button will be enabled.



- Click 'Save'.
- To Remove a RDBMS connection, select the connection and click the Trash Can icon that appears in the blue stripe.

9.Configuring Comodo MyDLP Settings

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



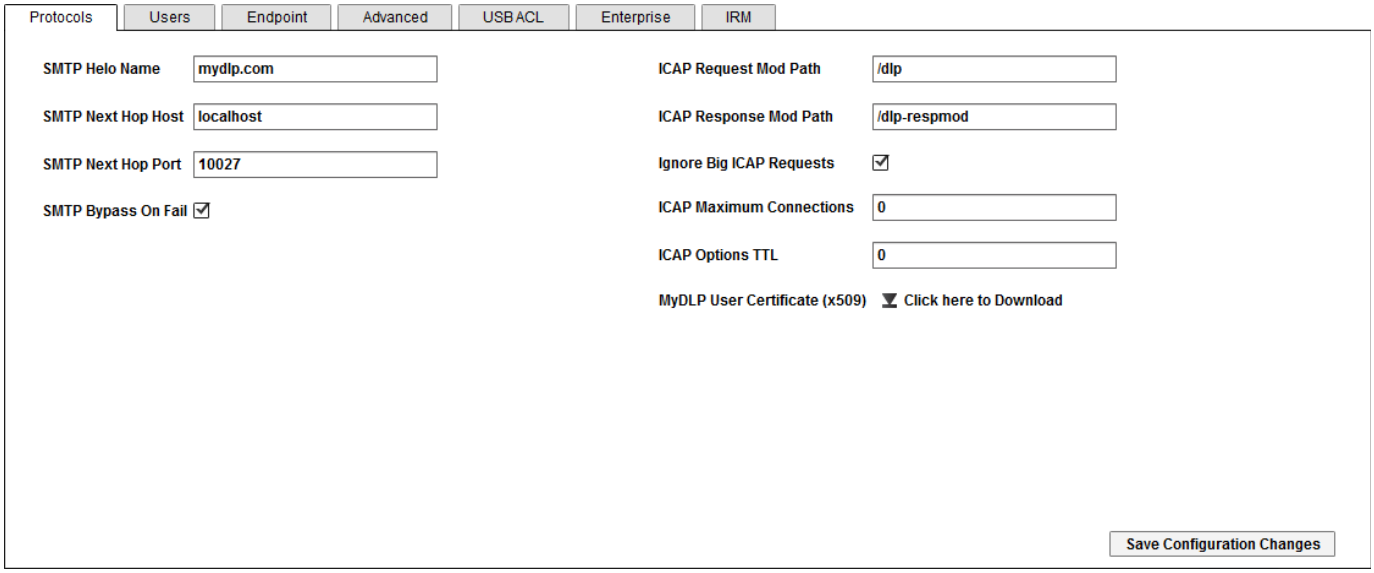
The interface contains seven tabs:

- **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.
- **USB ACL** - Enables the administrator to configure access restrictions to USB devices over the network. Refer to the section Configuring **Access Restrictions to USB Devices** 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.
- **IRM** - Enables the administrator to configure Information Rights Management (IRM) parameters. Refer to the section **Configuring IRM Settings** for more details.

9.1. 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 Configuration Changes' for your changes to take effect.

MyDLP User Certificate - 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.

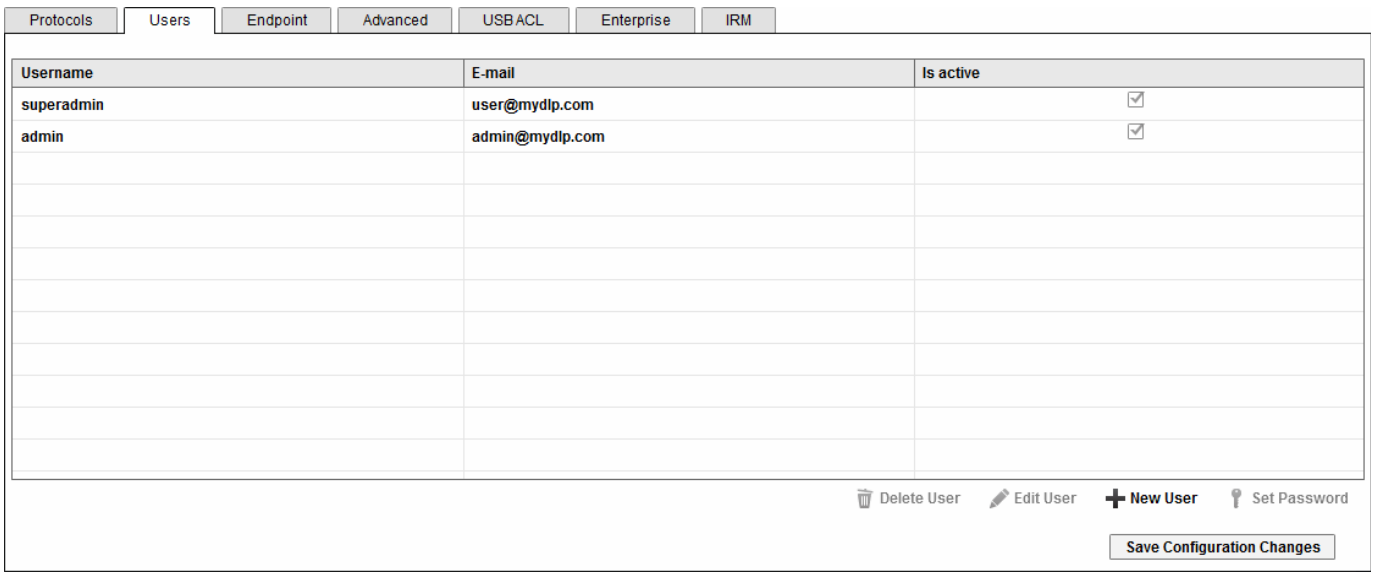
- To download the certificate in X509 format, click the 'Click here to Download' link.

9.2. 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:

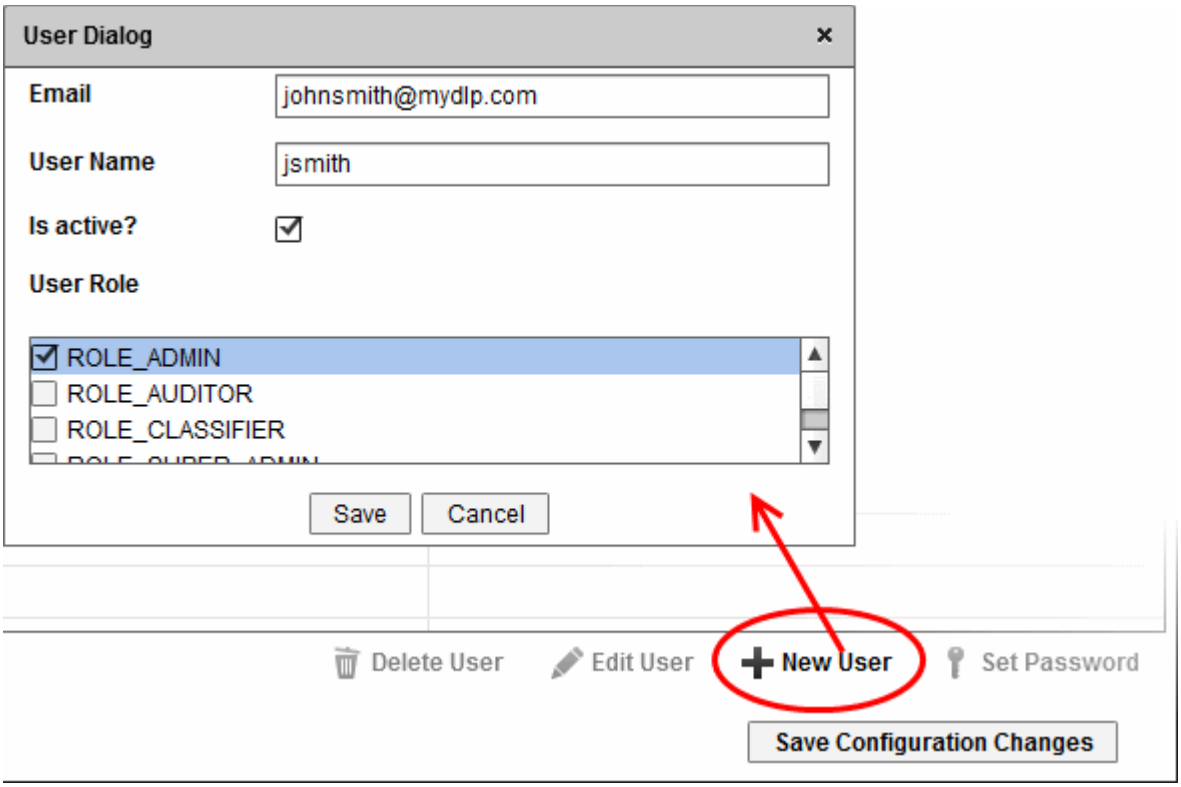
- **Add New Administrative Users**
- **Set/Reset Password for Administrative Users**
- **Edit and Remove Users**

9.2.1. 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 New User from the bottom right. The 'User Dialog' will appear.

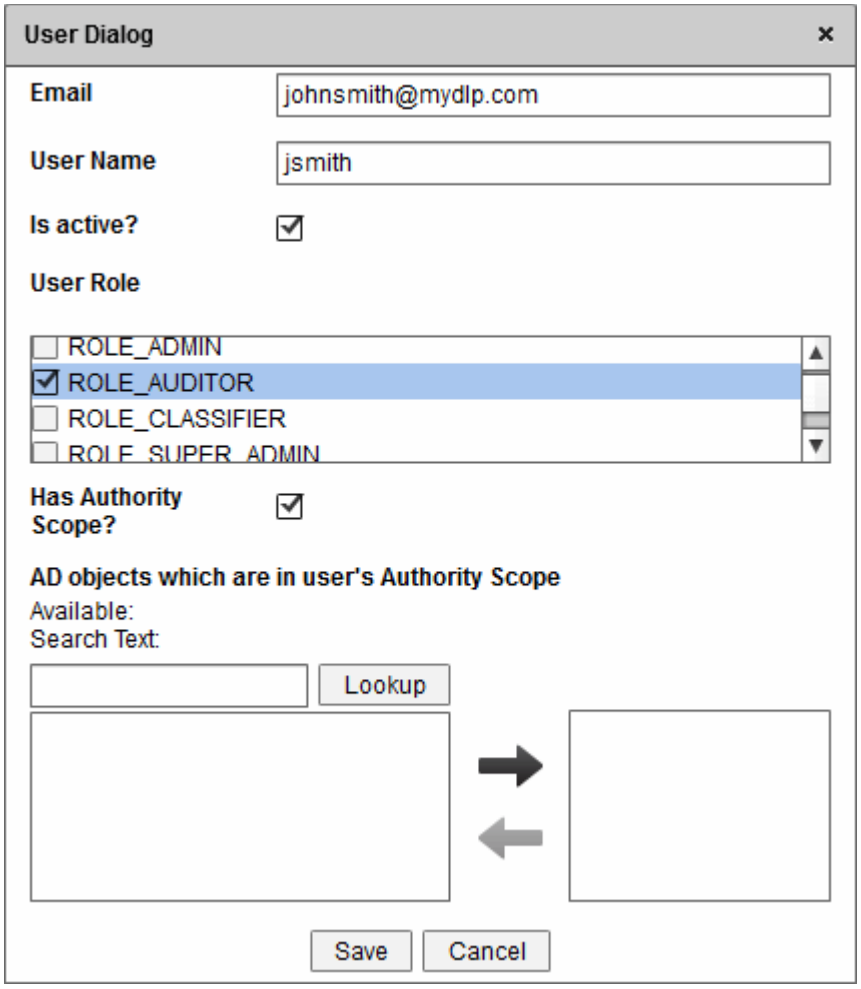


- Enter the details of the new user as shown below:
  - Email - Enter the email address of the new user
  - User Name - Enter the login username for the new user
- Select the 'Is Active' checkbox if the user should be enabled upon creation
- Select the User Role from the list box. For more details on the **Administrative Roles** refer to the table at the top of the section **9.2 Managing Administrators**.

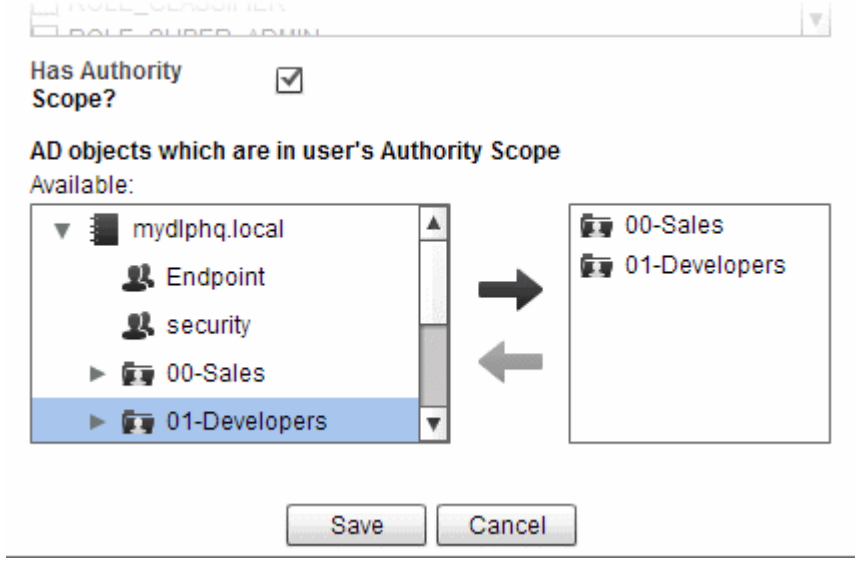
If you are adding an auditor or classifier, you need to specify additional parameters as shown below:

- **Auditor**
- **Classifier**

Auditor

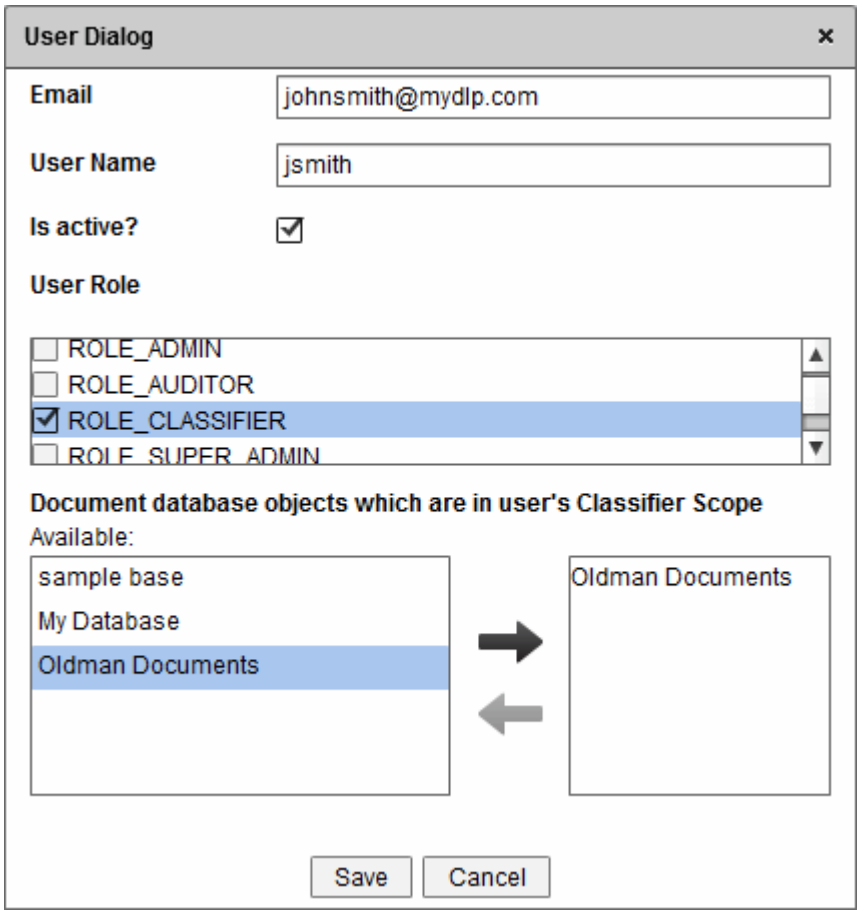


- If you want to restrict the ability of the auditor in viewing the logs, select 'Has Authority Scope' checkbox. This requires the MyDLP server integrated with your AD domains.
- Enter the first few characters of the AD object to be included within the auditor' scope in the search text textbox and click Lookup. The matching entries will be displayed as a list in the text box below it.



- Select the AD Objects or Users from the LHS box and move them to the RHS box by clicking the right arrow to add them to the auditors scope.

Classifier



On choosing the ROLE_CLASSIFIER, the document databases previously configured in the MYDLP are listed in the LHS box

- Select the databases to be included into the classifier's scope from the LHS box and move them to the RHS box by clicking the right arrow.

- Click 'Save' in the User Dialog. The new user will be added.

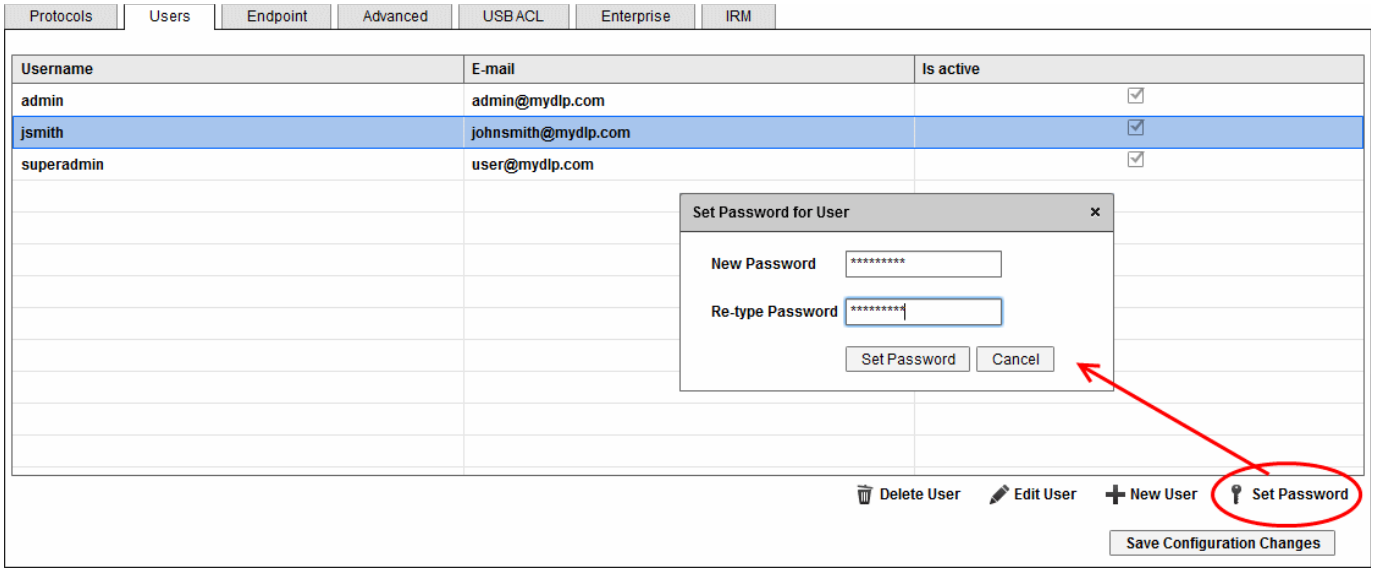
The next step is to set a password for the new administrative user to enable them to login. Refer to the next section **Setting and Resetting Password for Administrative Users** for explanation on setting password for the new user. Once logged-in the new administrator can change his/her login password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

9.2.2. 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

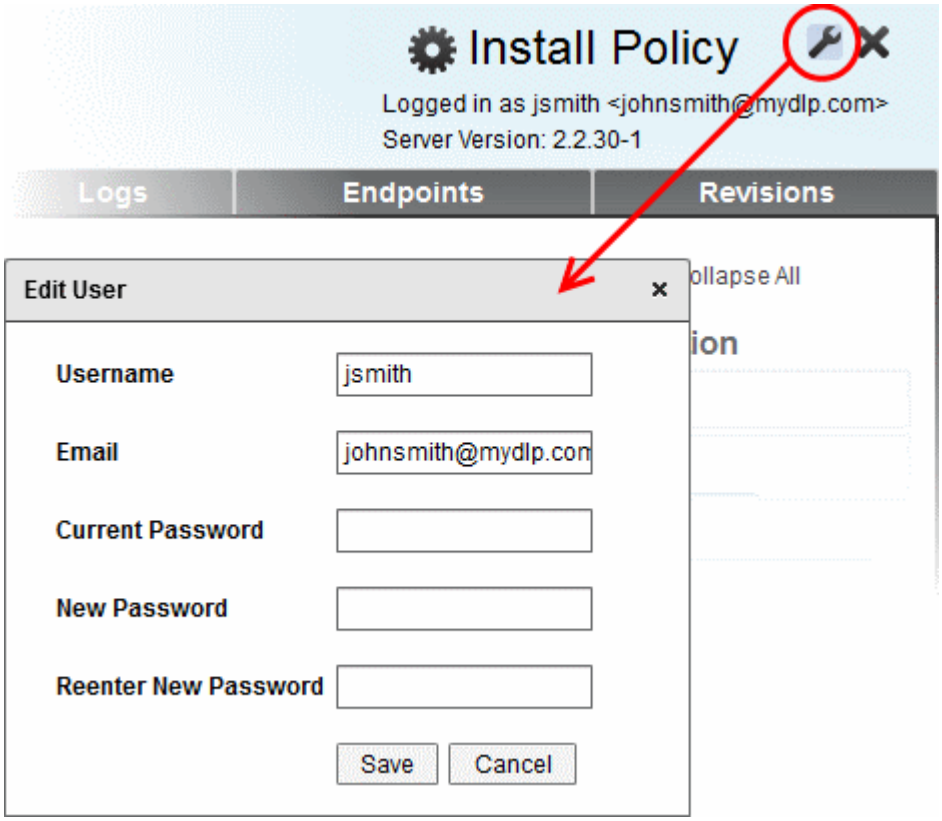
- Open Settings > Users interface
- Select the user and click 'Set Password'. The 'Set Password for User' Dialog will appear.



- 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 'Save Password'.
- Click 'Save Configuration' from the 'Users' interface.

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 the 'Wrench' icon at the top right of the interface and entering the new password in the 'Edit User' dialog.

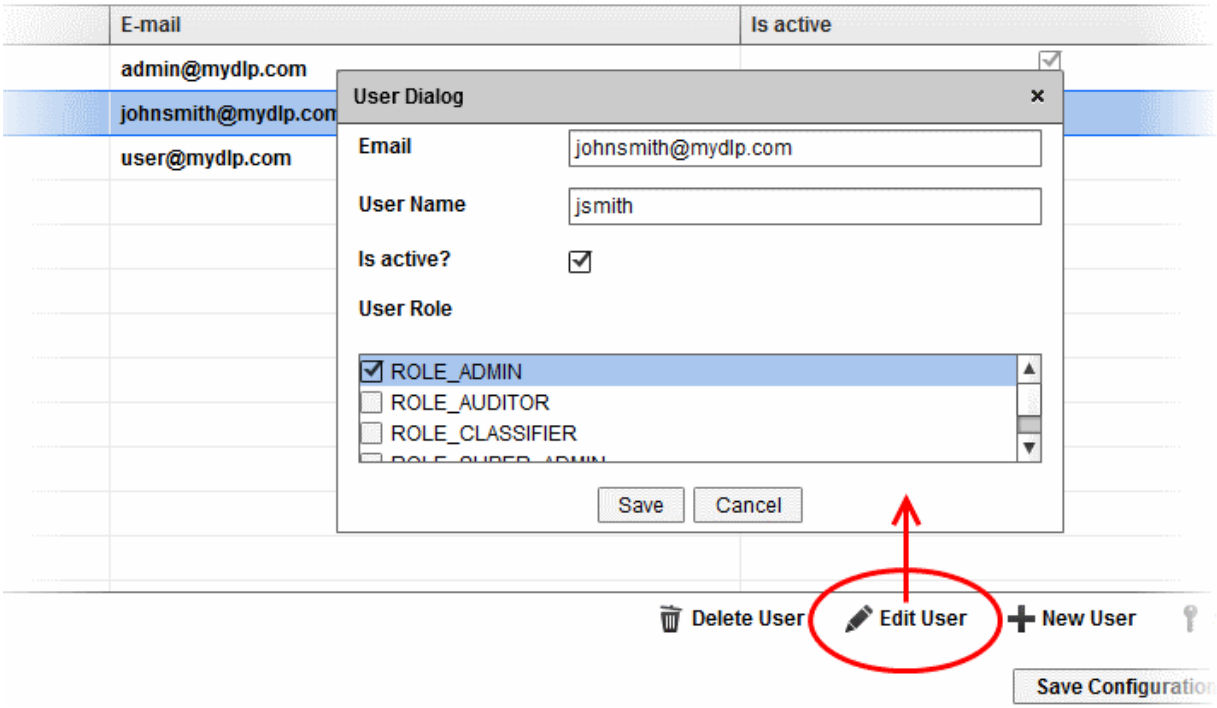


9.2.3. Editing and Removing Users

The administrative users can be edited by other administrators with appropriate privileges for enabling/disabling the user, change the login username and the administrative role.

To edit an user

- Open Settings > Users interface
- Select the user and click 'Edit User'. The 'User Dialog' will appear.



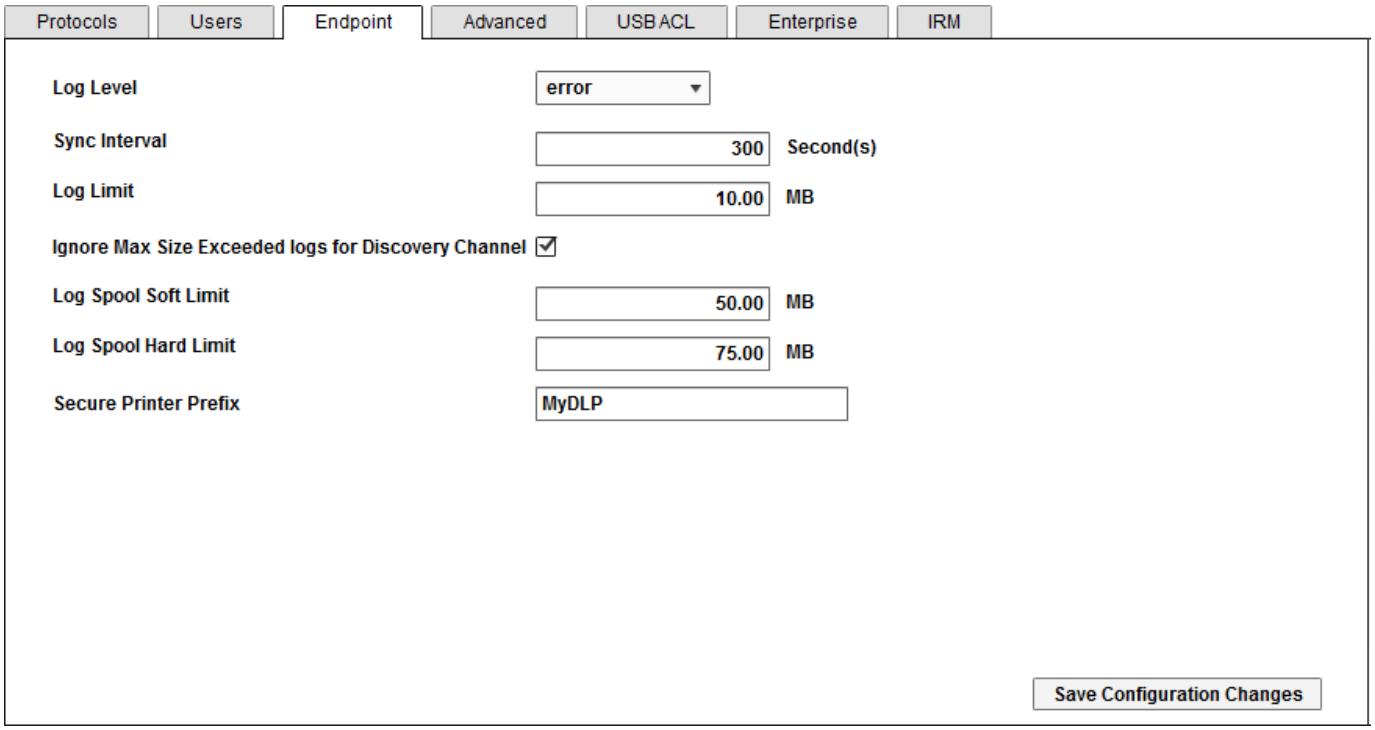
  - To change the email or username, directly edit the respective fields
  - To disable or enable a user, de-select/select the Is active checkbox
  - To change the administrative role of the user, select the new role from the 'User Role' list box
- Click 'Save' from the 'User Dialog'
- Click 'Save Configuration' for your changes to take effect.

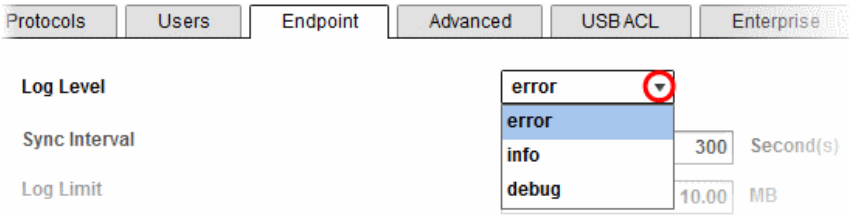
Tip: You can set/reset the login password for an user by selecting the user and clicking 'Set Password'. Refer to the section **Setting and Resetting Password for Administrative Users** for more details.

9.3. Configuring Endpoint Settings

The 'Endpoint' tab in the 'Settings' interface allows the administrator to configure the parameters related to the log entries and content data stored by MyDLP server on the endpoints. The settings configured in this interface is applicable for all the endpoints connected to the MyDLP Server.

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



Field	Description
Log Level	The administrator can choose the global operational log level depending on level of activities of MyDLP is to be monitored and logged.  Default = Error.
Sync Interval	The time interval (in seconds) at which the MyDLP Endpoints are to be synchronized with the MyDLP Server. Default = 30 seconds
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 y the content data will be discarded from the subsequent log entries.

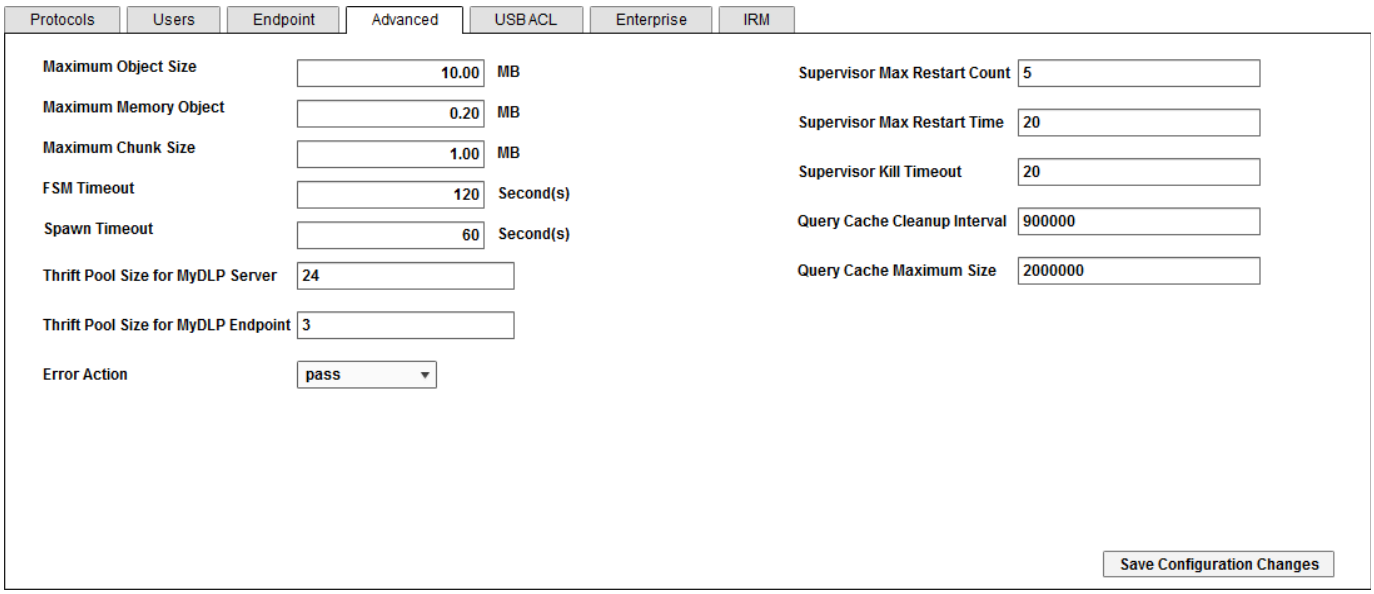
	Default = 75 MB
Secure Printer Prefix	The administrator can specify a prefix to be displayed with the MyDLP Virtual Printers that are created upon adding a Printer Rule. Default = MyDLP. You can change the prefix as required, for example set the name of your organization as printer prefix. **Background Note**: MyDLP creates a virtual printer for each network printer and makes it available for selection printing the documents from the endpoints added as sources to the printer rule. The 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 respective physical printer. The virtual printers are displayed with the name of the physical printer with a prefix defined in this field. The administrator can set the prefix as required.

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

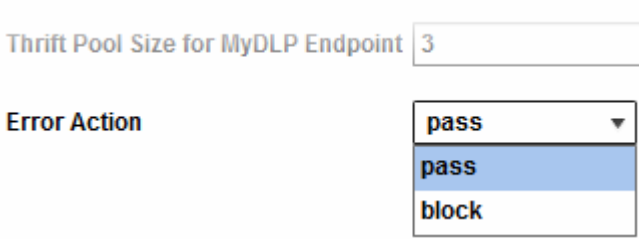
9.4. Configuring Advanced Settings

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 access 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
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. 
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

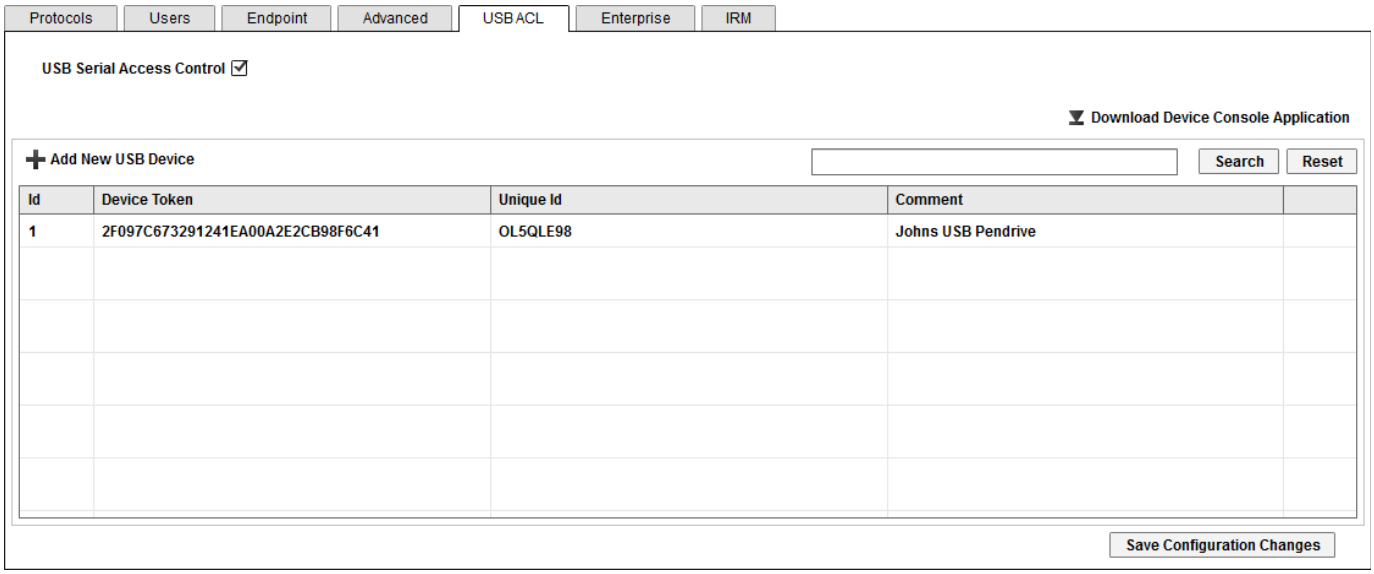
9.5. Configuring Access Restrictions to USB Devices

MyDLP has the ability to block using unknown USB devices on the endpoints on which the MyDLP Endpoint Agent is installed in order to prevent unauthorized copying of files even from the endpoints that are not covered as sources in Removable Storage Rules. The administrator can add the legitimate and allowable USB devices in the whitelist under the USB Access Control List (ACL) tab.

In order to add a USB to the white list, the administrator needs to specify the Device Token and Unique Identifier of the USB device. For identifying the Device Token and Unique Identifier, the administrator can use a tiny Device Console executable that can be downloaded from the USB ACL interface itself.

The USB ACL interface displays the list of USB devices added to the white list and allows the administrator to add new and manage existing devices.

To access the USB ACL Settings interface, click 'Settings' > 'USB ACL' tab.



USB ACL Table - Description of Columns		
Rule Component		**Description**
Id		The identifier assigned to the device by MyDLP
Device Token		The unique 'Device Token' of the USB Device. The Device Token can be obtained by using the Device Console utility. Refer to the section **Obtaining Device Token and Unique ID of a USB Device** for more details.
Unique ID		The 'Unique Identifier' of the USB Device. The Unique Identifier can be obtained by using the Device Console utility. Refer to the section **Obtaining Device Token and Unique ID of a USB Device** for more details.
Comment		A short description of the USB device, entered during device creation.
Controls	Edit	Enables the administrator to edit the details of the USB device.
	Remove	Enables the administrator to remove the USB device from the whitelist.

You can search for a specific device in the list by entering its name fully or partially in the text box above the table and clicking 'Search'.

- To block the usage of unauthorized USB devices by the en-users, select the 'USB Serial Access Control' check box and add the authorized USB devices to the whitelist by clicking 'Add New USB Device'.

Refer to the following sections for more information on:

- **Obtaining the Device Token and Unique ID of a USB Device**
- **Adding a USB Device to Whitelist**

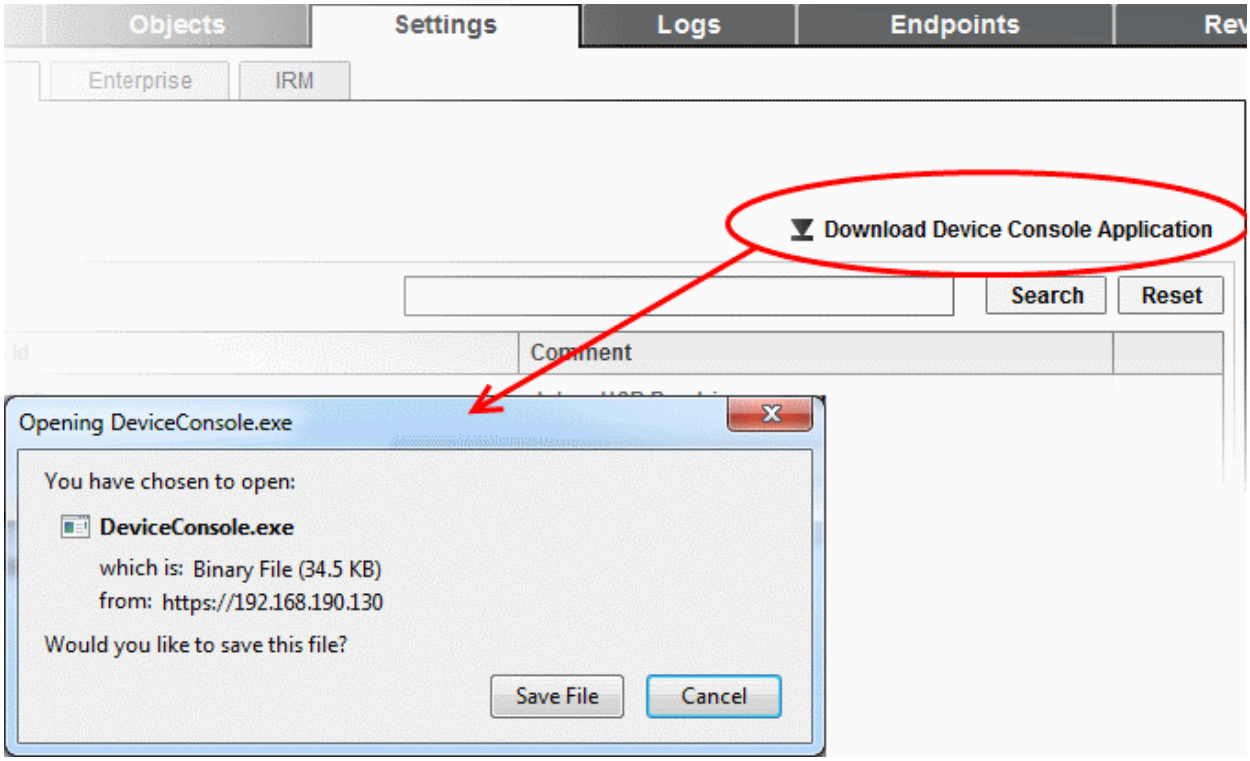
9.5.1. Obtaining the Device Token and Unique ID of a USB Device

Comodo MyDLP Device Console Application is a tiny executable that can be downloaded from the USB ACL interface. The application does not require installation and can be run as a portable executable. On execution, the application detects the USB devices plugged-in to the computer and displays the device parameters such as the Device Token, Unique ID, size and product name/model of the device.

To download the application

- Click 'Settings' > 'USB ACL' tab.

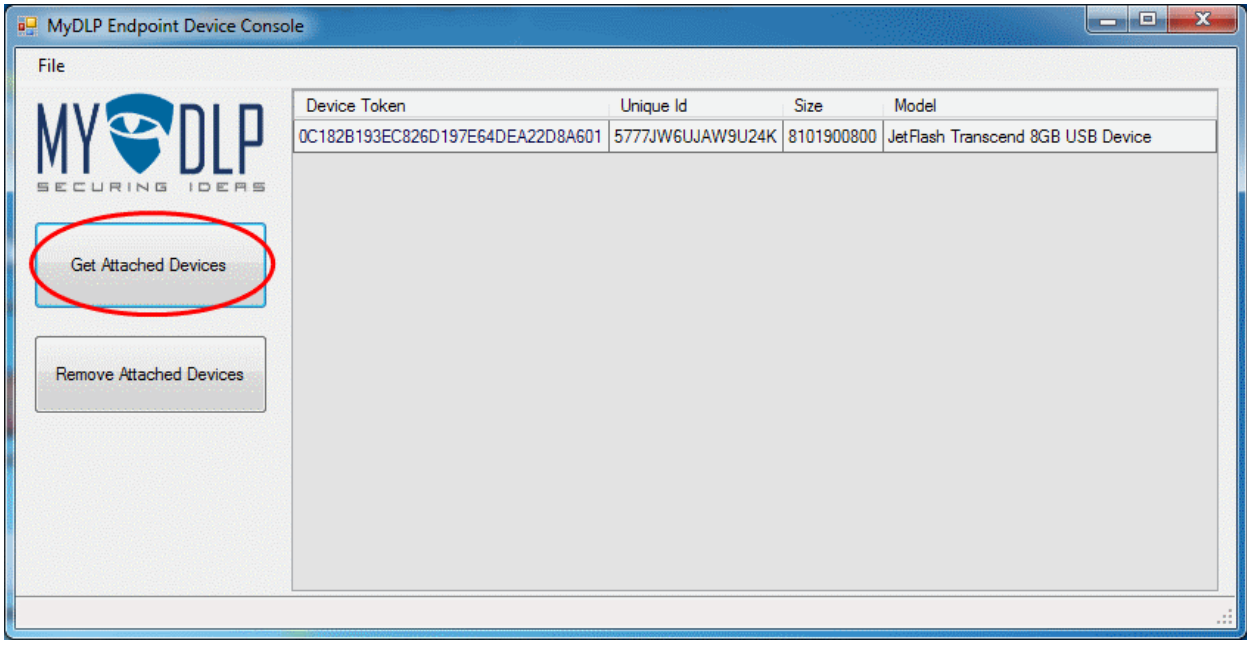
- Click the 'Download Device Console Application' link at the top right and save the application on the computer from which you are accessing the administrative console.



To get the Device Token and Unique ID

- Plug-in the USB device(s) to the computer in which the application is saved.
- Run the application by navigating to the location where the application was saved and double clicking the application icon 

.
- Click 'Get Attached Devices'.



The Device Token, Unique ID, Size and the Model of the currently plugged-in USB devices are displayed as a table. You can

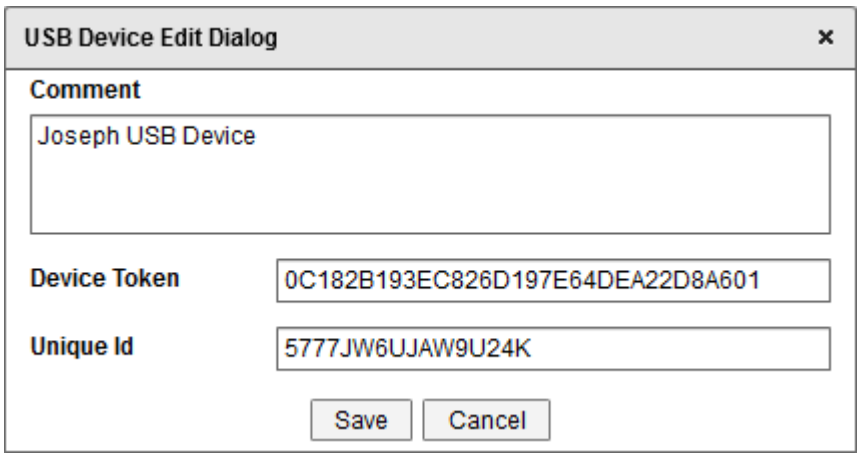
copy the values and paste in the administrative interface for whiltelisting the devices. Refer to the next section **Adding a USB Device to Whitelist** for more details.

9.5.2. Adding a USB Device to Whitelist

The USB storage devices that are allowed to be used by the end-users in the network can be added to the whitelist, by specifying their device token and Unique ID number.

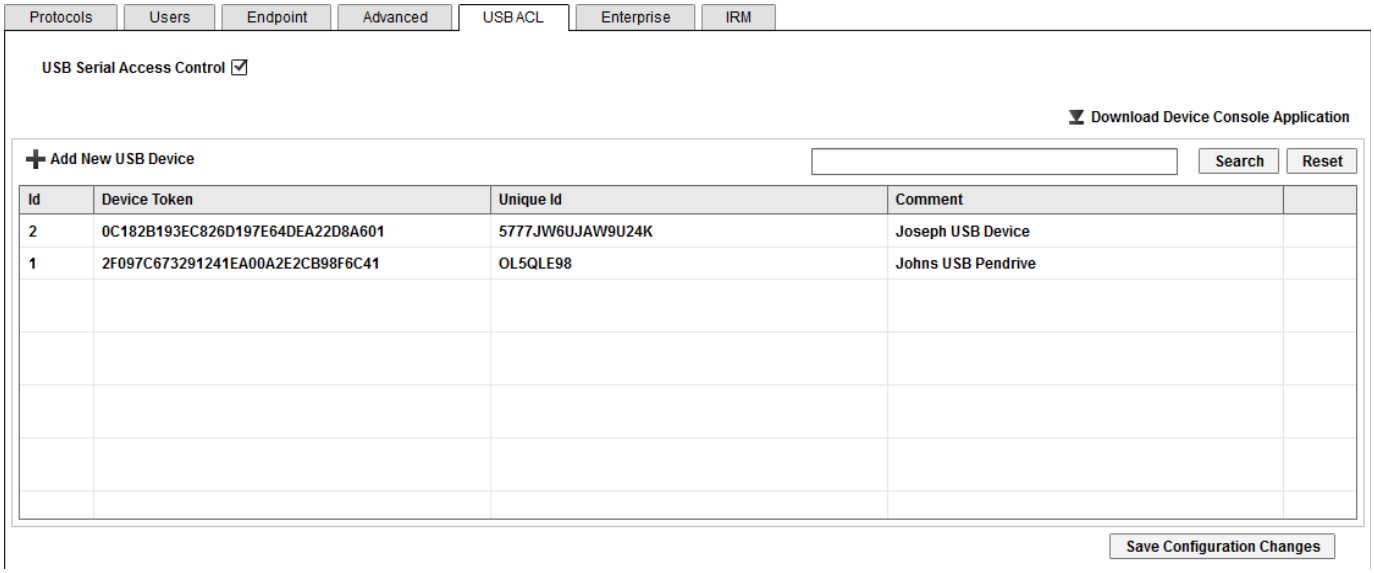
To add a new device to the whitelist

- Click 'Settings' > 'USB ACL' tab.
- Click the 'Add New USB Device' link at the top left of the table. The 'USB Device Edit Dialog' will appear.

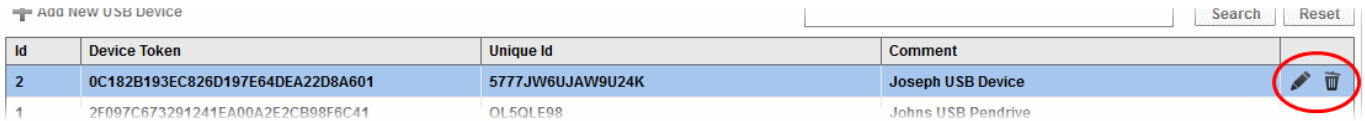


- Enter a name describing the device in the Comment field.
- Enter or paste the Device Token as obtained from the Device Console Application.
- Enter or paste the Unique ID as obtained from the Device Console Application.
- Click Save in the 'USB Device Edit Dialog'.

The USB device will be added to the list.



You can edit the details or remove a device at any time by selecting it and clicking the respective control buttons that appear in the last column.

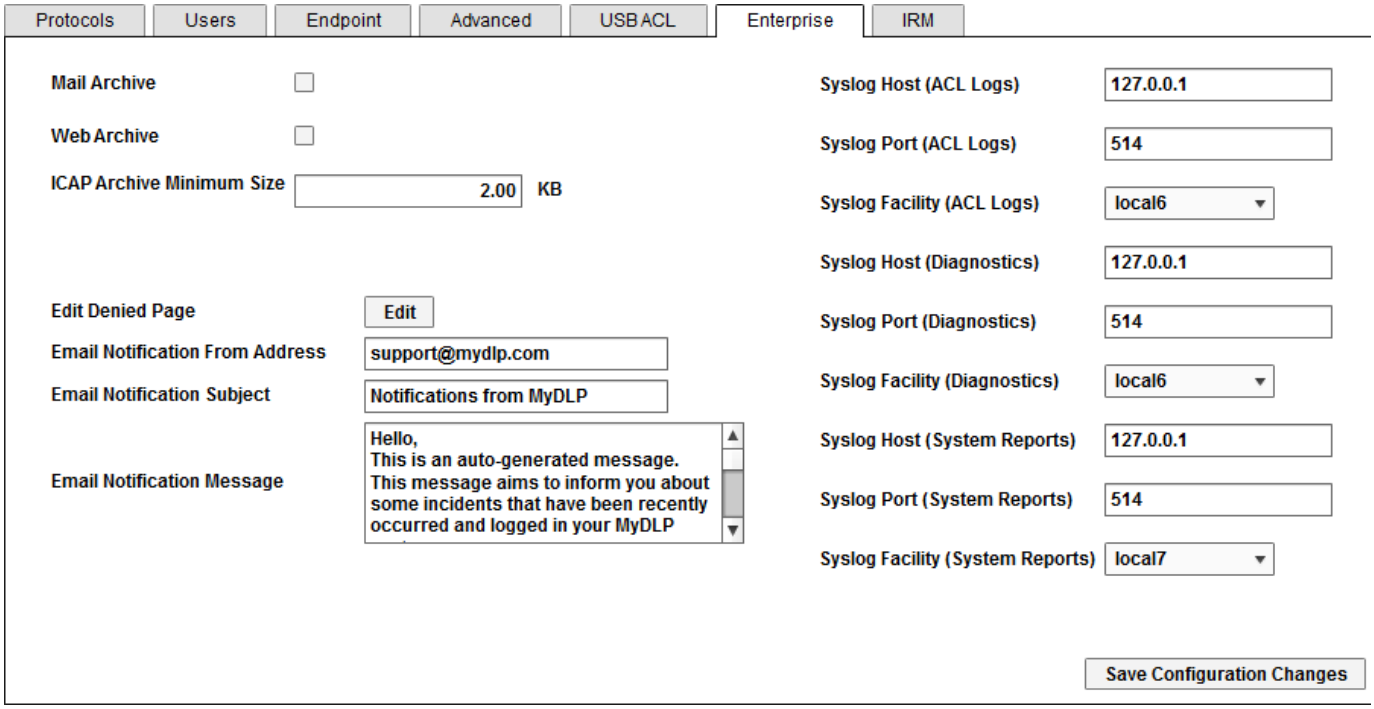


- Click 'Save Configuration Changes' for your changes to take effect.

9.6. 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 access the Endpoint tab, click 'Settings' > 'Enterprise'.



Archive Settings

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 KB) 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 Settings

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

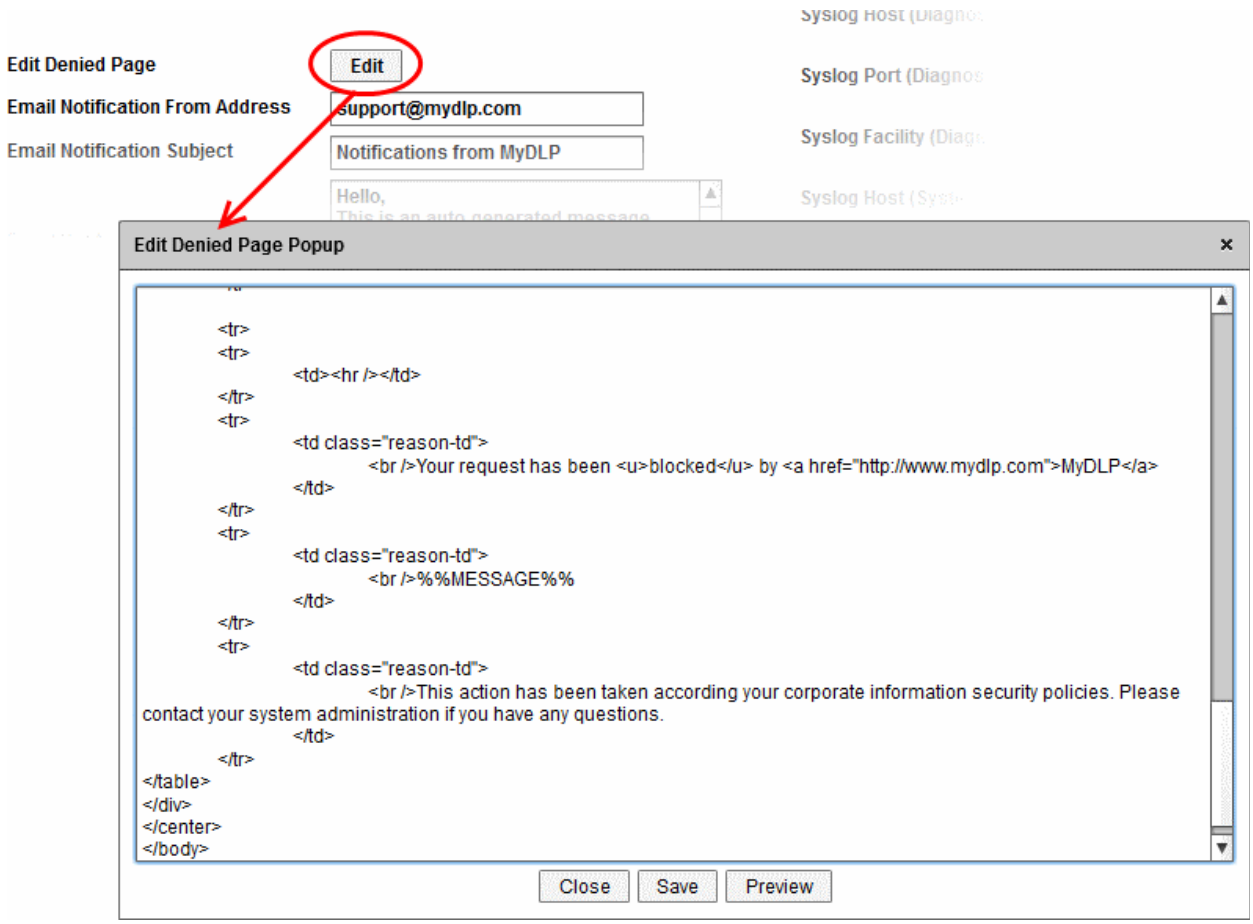
The 'Enterprise' tab in the 'Settings' interface allows the administrator to customize the content in the email notification and the message pop-up displayed to the end-user.

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 3 - Enter Name for the rule and configure Messages and Notifications** in the section **Adding Policy Rules** 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 Settings

Comodo MyDLP has the ability to forward the logs to a remote Syslog server Common Event Format (CEF) and User Datagram Protocol (UDP). The administrator can integrate MyDLP with the 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'

Currently MyDLP supports integration with two third-party log management servers:

- **HP ArcSight Logger** - Refer to the section **Integrating MyDLP with HP Arc Sight Logger** for more details.
- **Alien Vault OSSIM** - Refer to the section **Integrating MyDLP with Alien Vault OSSIM** for more details.

More Syslog servers will be added in the future versions.

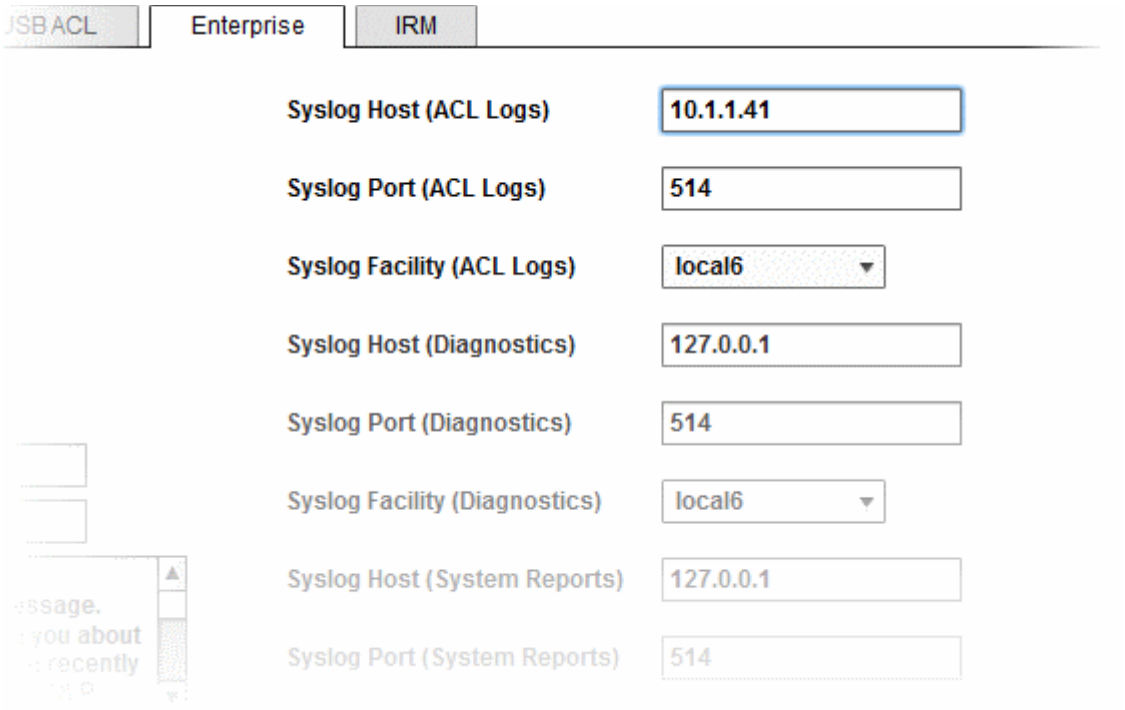
9.6.1. Integrating MyDLP with HP Arc Sight Logger

Administrators can configure HP ArcSight Logger as the default destination of MyDLP ACL logs in the 'Settings > Enterprise' area.

Prerequisite: The administrator should have configured the HP ArcSight Logger and it should be reachable from the MyDLP server.

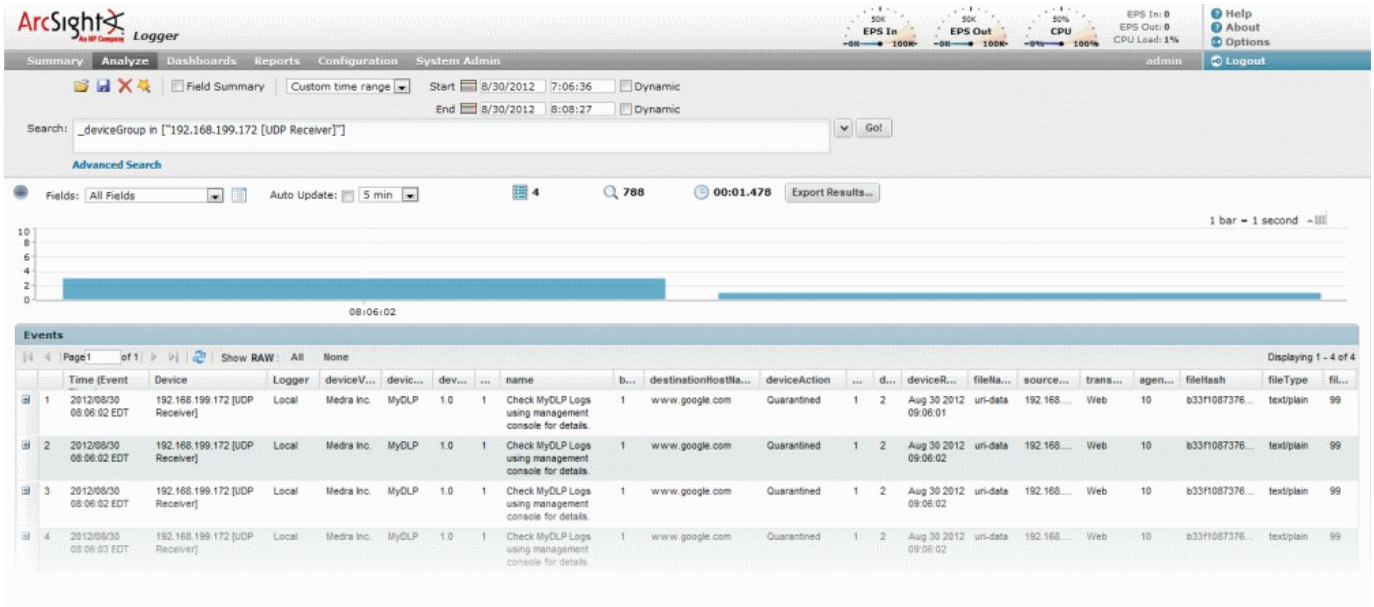
To integrate HP ArcSight Logger

- Click 'Settings' > 'Enterprise' tab.
- Enter IP Address of the HP ArcSight Logger in the Syslog Host (ACL Logs) field



- Enter UDP Listener port of the HP ArcSight Logger in the Syslog Port (ACL Logs) field (Default = 514)
- Click 'Save Configuration Changes'
- Reinstall the policy for your changes to take effect.

You can see the events related to the data loss incidents are logged in the HP ArcSight Logger.



9.6.2. Integrating MyDLP with Alien Vault OSSIM

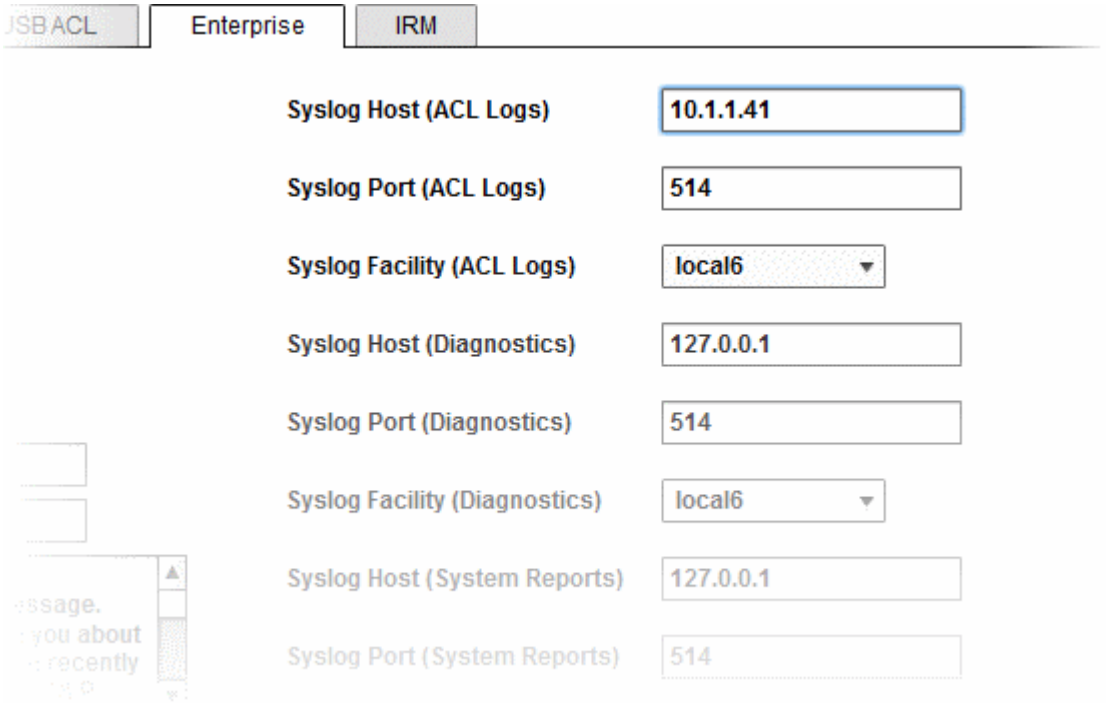
Administrators can configure Alien Vault OSSIM as the default destination of MyDLP ACL logs in the 'Settings > Enterprise' area.

Prerequisite: Alien Vault OSSIM server is to be installed with the MyDLP plug-in in order to view the logs of incidents from it. To install the plug-in:

- Connect to the Alien Vault OSSIM server through SSH connection and login as Root
- Create a new folder for temporary installation files and navigate into it
- Download auto configuration script from the path 'src/sysconf/ossim/configure-ossim.sh' in **mydlp@github.com**
- Run the script with administrative privileges

To integrate Alien Vault OSSIM

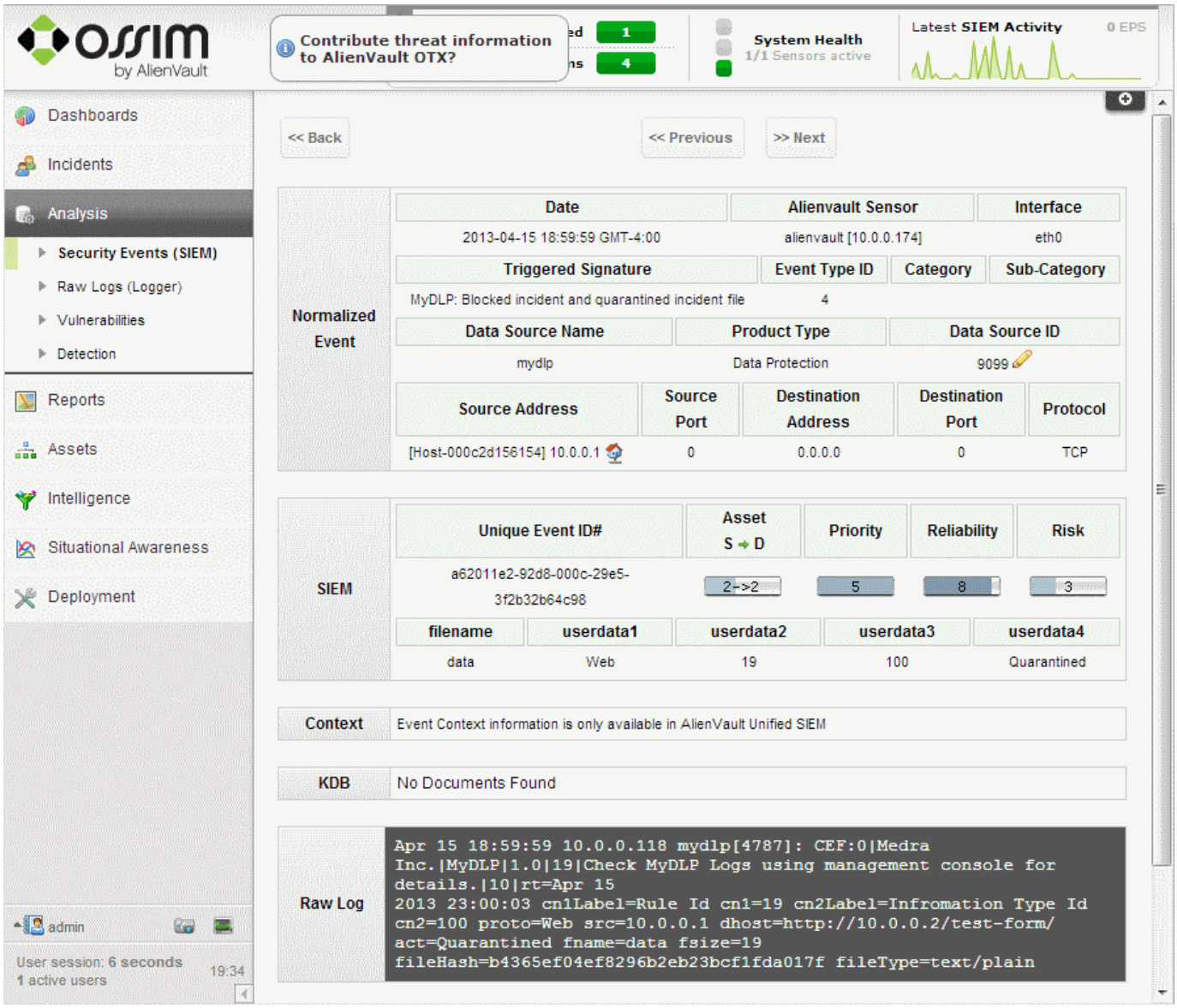
- Click 'Settings' > 'Enterprise' tab.
- Enter IP Address of the Alien Vault OSSIM server in the Syslog Host (ACL Logs) field



- Enter UDP Listener port of the Alien Vault OSSIM server in the Syslog Port (ACL Logs) field (Default = 514)

- Click 'Save Configuration Changes'
- Reinstall the policy for your changes to take effect.

You can see the events related to the data loss incidents are logged in the Alien Vault OSSIM



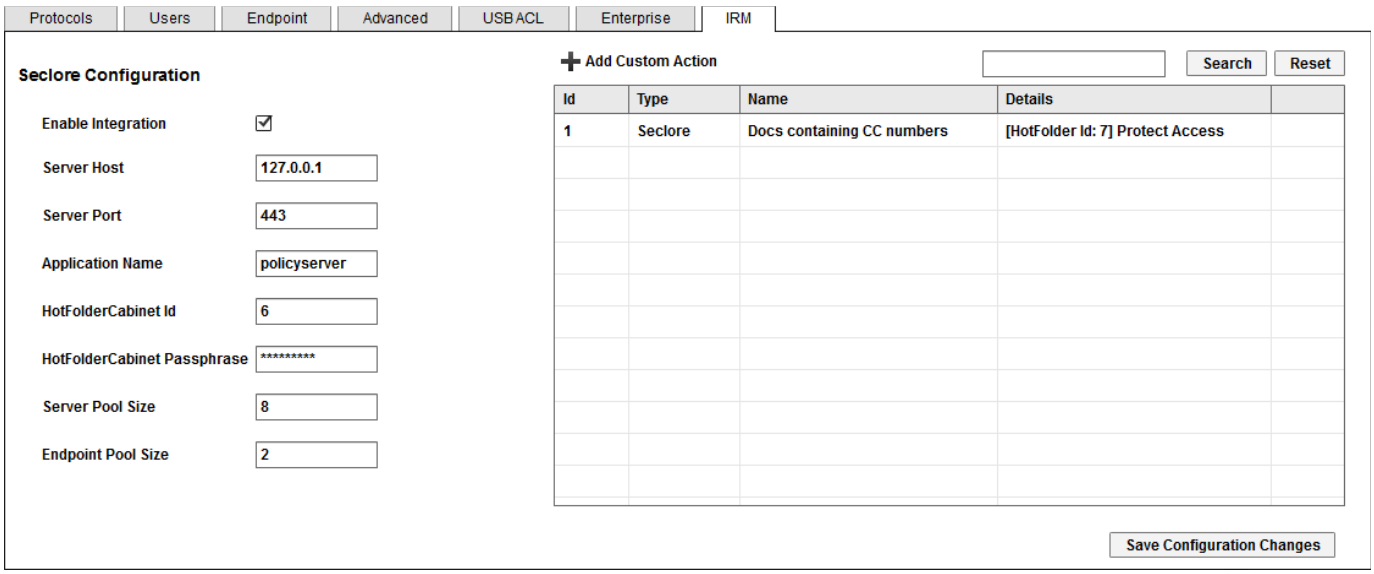
9.7. Configuring IRM Settings

Comodo MyDLP's integration with Seclore FileSecure allows that product's custom actions to be applied to files discovered by MyDLP discovery rules. Discovered files will then be protected by Seclore and user access to the file will be governed by the rights assigned in Seclore.

For more details on Seclore FileSecure, please visit **http://www.seclore.com/**.

Together, Comodo MyDLP and Seclore provide an effective solution to achieve automated data protection combining benefits of DLP and IRM.

The 'IRM' tab in the 'Settings' interface allows the administrator to enable the integration, configure the Seclore server and add custom action for discovery rules.



Refer to the following sections for more details

- **Integrating Seclore FileSecure**
- **Creating new Custom Actions for MyDLP to use in Discovery Rules**

9.7.1. Integrating Seclore FileSecure

In order to integrate Seclore FileSecure server installed in the network, the administrator needs to configure the Seclore FileSecure server for creating Hot Folder cabinet for MyDLP and Hot Folders for use with rules with different information types. The administrator can then integrate the Seclore FileSecure server to MyDLP by specifying the Hot Folder Cabinet ID. The custom actions can then be created for discovery rules defined with different information types and sources by specifying the ID numbers of Hot Folders created inside the cabinet.

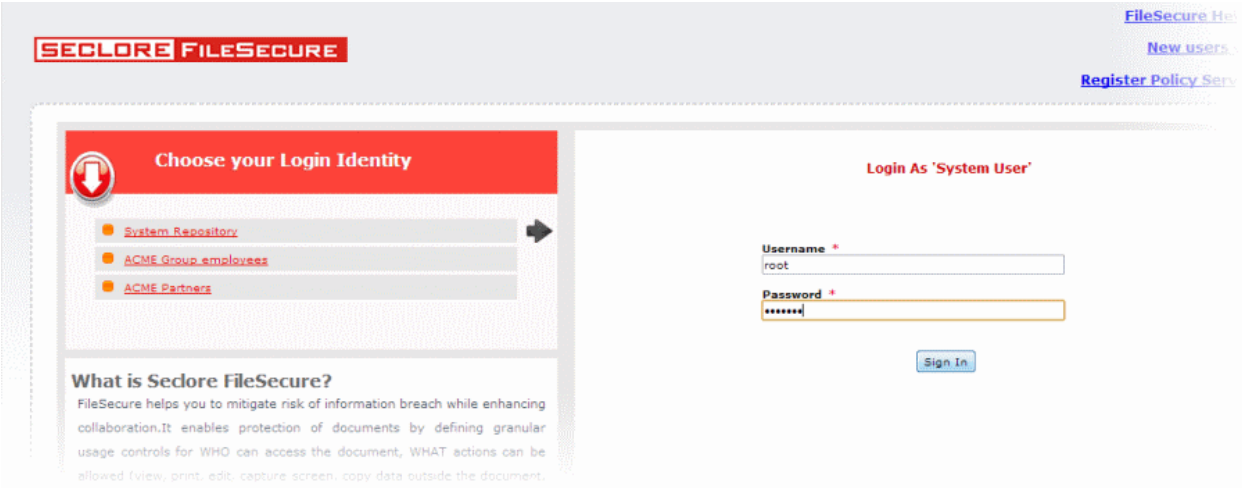
Integrating MyDLP with Seclore FileSecure is a two step process.

- **Step 1 - Create a new Seclore HotFolder Cabinet for MyDLP**
- **Step 2 - Configure MyDLP to use Seclore FileSecure as IRM**

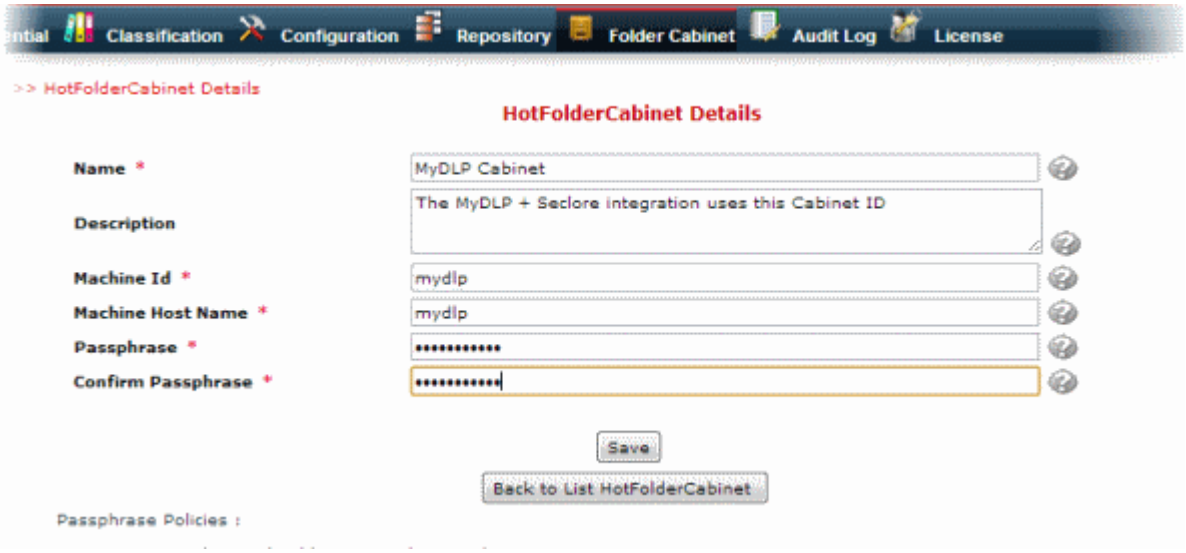
Prerequistie: The Seclore FileSecure IRM has been installed in the network and reachable by the MyDLP server by specifying the host name of the Seclore FileSecure server. A proper DNS configuration is necessary for the domain name of the Seclore FileSecure , so that it could be resolved by all the endpoints. If necessary the administrator can add host entries for the Seclore FileSecure in the hosts files (C:\Windows\System32\drivers\etc\hosts or /etc/hosts) of the endpoints.

Step 1 - Defining a new Seclore HotFolder Cabinet for MyDLP

- Login to the web console of the Seclore policy server with root username and password.



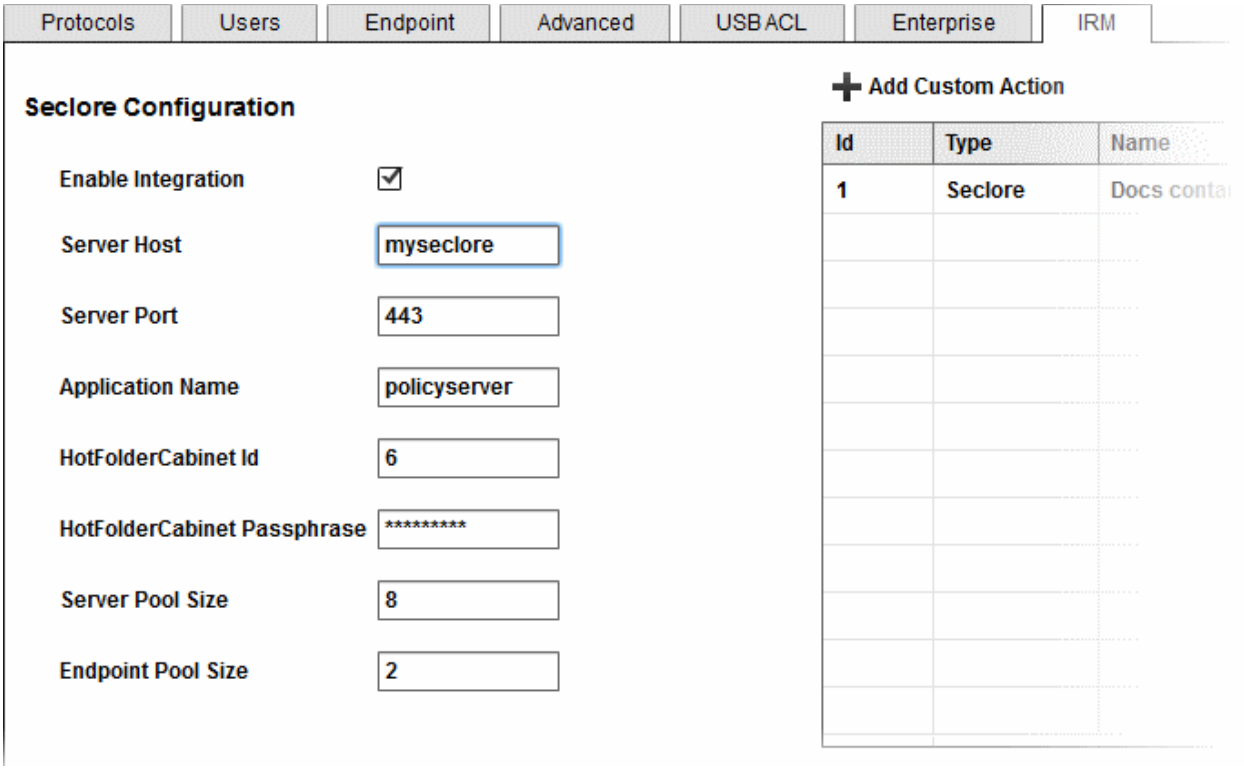
- Open the 'Folder Cabinet' tab and click Add 'HotFolder Cabinet' to create a new cabinet for integration with MyDLP
- In the HotFolder Cabinet Details form. enter the name, description and other fields. Enter 'mydlp' in the Machine Id field and 'Machine Host Name' field. Remember the passphrase specified for the cabinet. You need to enter this passphrase while configuring MyDLP to use this cabinet.



- Click Save to create the cabinet
- Click 'Back to List HotFolder Cabinet to view the list of cabinet with the newly created cabinet in the list.
- Note the HotFolderCabinet Id of newly created HotFolder Cabinet. You need to enter this ID while configuring MyDLP to use this cabinet.
- Click the HotFolder icon to view the list of hotfolders inside the cabinet and create new folders for use with different discovery rules. Note the HotFolder ID numbers of the newly created HotFolders. You need to enter this ID while configuring the custom IRM protection actions according to this HotFolder profile.

Step 2 - Configuring MyDLP to use Seclore FileSecure as an IRM

- Login to MyDLP administrative interface and click 'Settings' > 'IRM' tab.
- Select the 'Enable Integration' checkbox and enter the configuration parameters to connect to your Seclore FileSecure server.



Field	Description
Server Host	Enter the hostname of the Seclore FileSecure server. The hostname should be resolvable by the DLP server. If required, add a host entry for the Seclore FileSecure server in the hosts file of the MyDLP Server. Entering IP address of the Seclore FileSecure server is not recommended.
Server Port	Enter the port number through which the Seclore FileSecure server listens to the requests from MyDLP.
Application Name	Enter the Application Name of your Seclore PolicyServer. This is folder part of the url (https://seclore/policyserver)
HotFolderCabinet ID and HotFolderCabinet Passphrase	Enter the ID number of the HotFolder Cabinet you created for MyDLP in the Seclore server and the passphrase to access the cabinet.
Server Pool Size	Enter the number of active connections for sending files from MyDLP server to the IRM backend service. Default = 8.
Endpoint Pool Size	Enter the number of active connections for sending files from MyDLP service in endpoints to the IRM backend service. Default = 2.

- Click 'Save Configuration Changes'. MyDLP will connect to the Seclore Server and you will be able to create new custom actions for the Discovery rules, using the IRM policies.

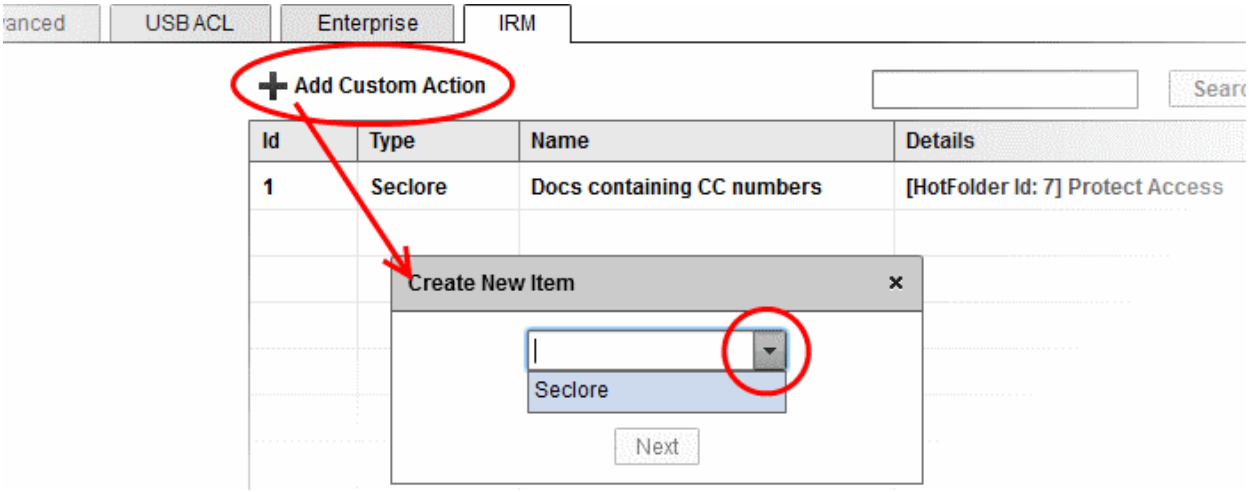
9.7.2. Creating new Custom Actions for MyDLP for use in Discovery Rules

Integration with Seclore FileSecure enables the administrator to create custom actions to be executed on discovered files. The action can be applied in Endpoint Discovery rules and Remote Storage rules so that the files found during discovery scans and identified as containing sensitive information as per the rules will be allowed/denied access to the end-users based on the access rights assigned to the user.

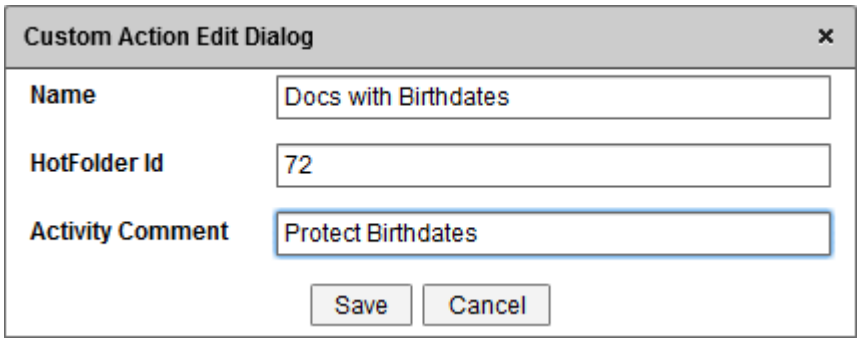
Prerequistie: The Seclore FileSecure IRM has been integrated to MyDLP by specifying the HotFolder Cabinet created in Seclore FileSecure for MyDLP. One or more HotFolders are created inside the HotFolder Cabinet for different rules and their identity numbers are noted.

To create a custom action

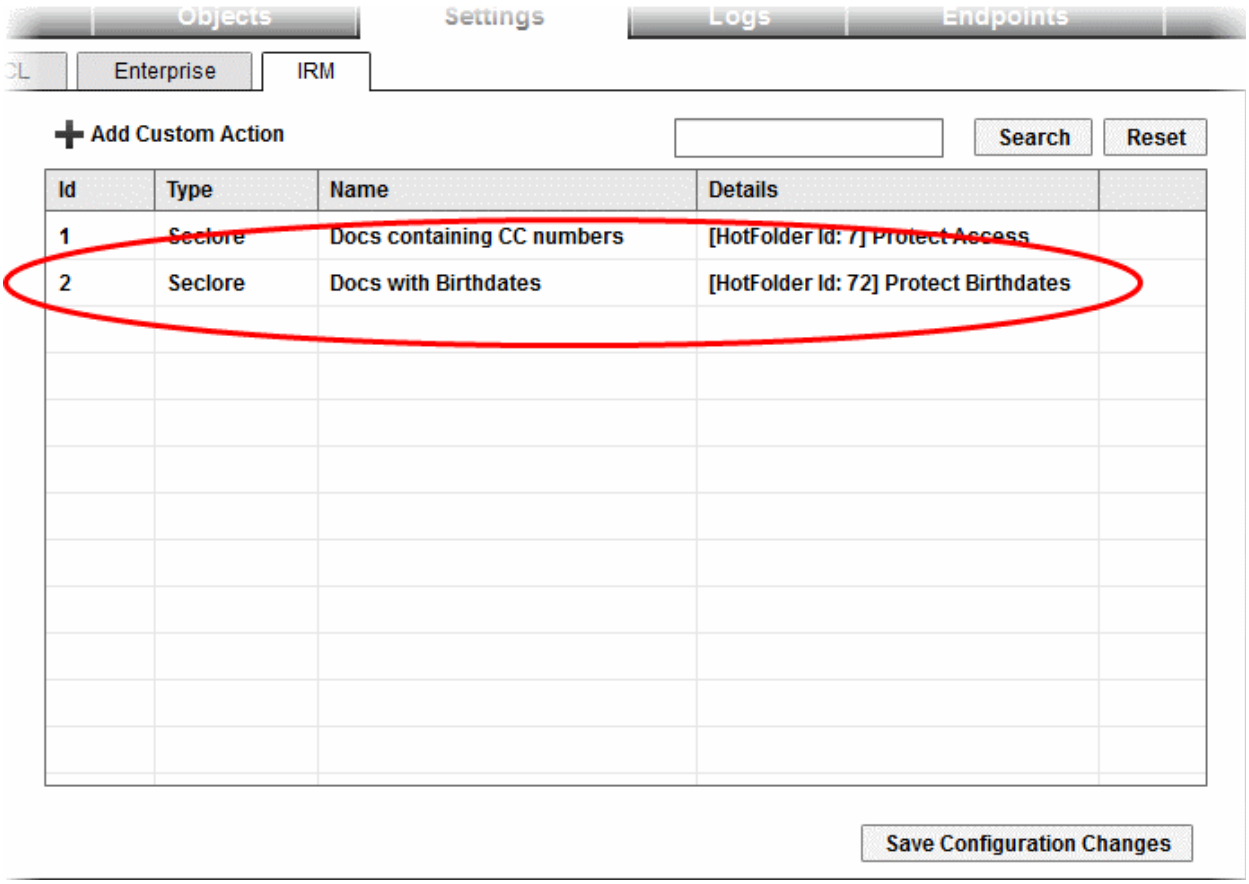
- Login to MyDLP administrative interface and click 'Settings' > 'IRM' tab.
- Click Add Custom Action. The 'Create New Item' dialog will appear for adding the new action.



- From the dop-down, choose 'Seclore' and click 'Next'. The 'Custom Action Edit Dialog' will appear.

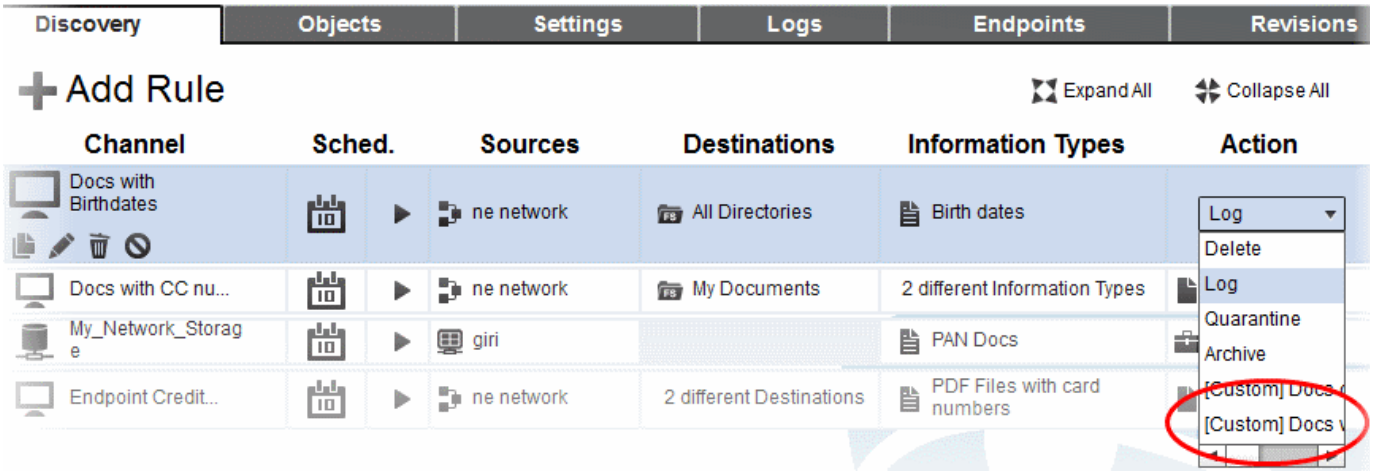


- Enter the parameters for the new action
  - Name - Enter a name for shortly describing the action or its purpose
  - HotFolder Id - Enter the ID number of the HotFolder created for the action inside the Seclore FileSecure HotFolder Cabinet. Refer to the description under '**Step 1 - Defining a new Seclore HotFolder Cabinet for MyDLP**' for more details on creating HotFolder Cabinet and the HotFolders.
  - Activity Comment - Enter the name for the action as it should be displayed in the 'Action' drop-down in the Discovery interface.
- Click 'Save'. The action will be added to the list of custom actions in the IRM interface.



- Click 'Save Configuration Changes'.

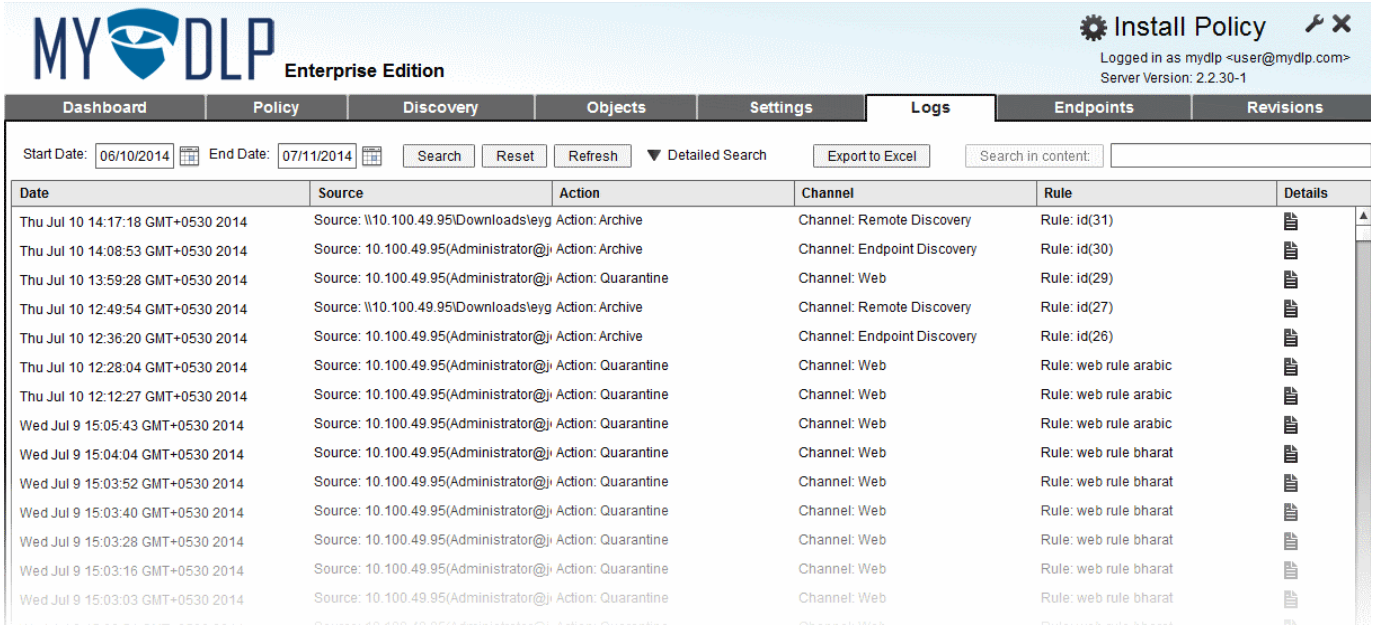
The new action will be available for selection for any discovery rule in the Discovery interface.

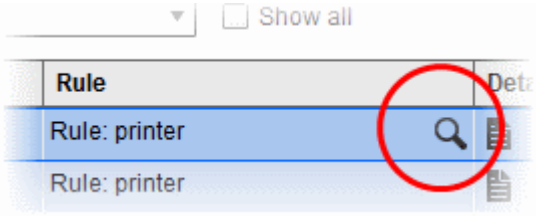


For more details on creating a Discovery Rules and specifying action to it, refer to the section **Adding Discovery Rules**.

10. The Logs tab

The 'Logs' interface displays the list of log of data loss incidents with details on source of the files, rule based on which the files are intercepted, action taken MyDLP. It also allows the administrator to download a copy of archived files that were intercepted based on various rules and resend legitimate mails that were intercepted by mail rules.



Logs Table - Description of Columns	
Column Header	**Description**
Date	Precise 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.
Channel	The rule channel that indicates the type of the rule based on which the files are intercepted or discovered. Refer to the section **Rule Channels** for a list of rue types.
Rule	The name of the rule based on which the files are intercepted or discovered. The Rule column also allows the administrator to view the rule from the Policy or Discovery interface by clicking the magnifier icon that appears beside the rule name on selecting the log entry. 
Details	Enables the administrator to view the complete details of the incident and download the copies of the files intercepted or discovered. Refer to the section **Viewing Details of a Log Entry** for more details.

Filtering and Search Options

The logs can be filtered to view the incidents that occurred within a specified period of time 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 parameters**

To filter the logs for a specific time period

- Enter the start and end dates of the period by click the calendar icons beside Start Date and End Date fields and

click 'Search'.

Only the logs of incidents occurred within the specified time period will be displayed.

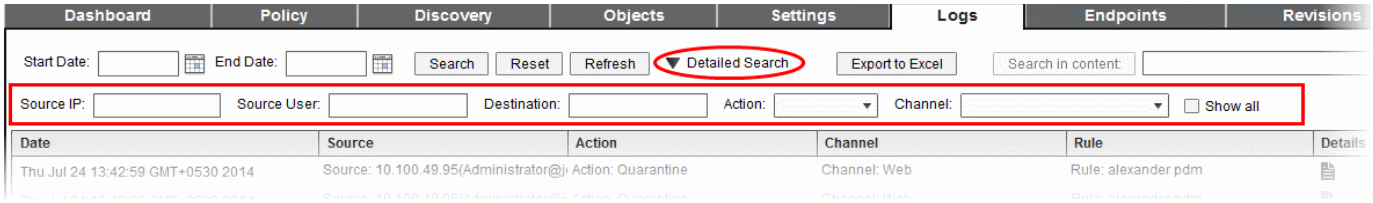
- To clear the filters, click 'Reset'.

Searching Logs based on Rule Parameters

The administrator can search for logs of incidents involving specific endpoint, end-user, destination, action and / or the rule channel. You can specify a combination of these parameters to narrow down the search. The administrator can also search the logs based on keywords contained in the quarantined/archived files from this interface.

To search the logs based on rule parameters

- Click 'Detailed Search' to expand the search panel.

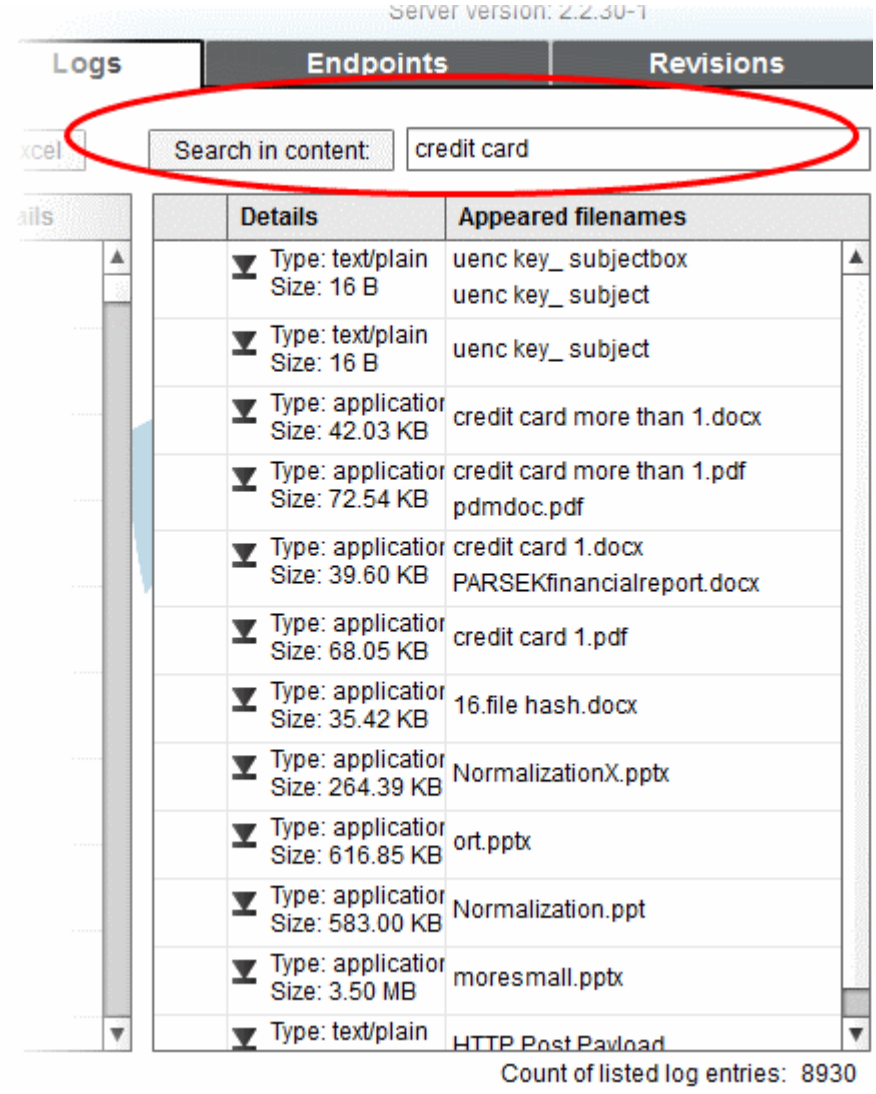


  - To search the logs of incidents involving a specific endpoint, enter the IP address of it in the Source IP field
  - To search the logs involving a specific end-user, enter the end-user name and the hostname of the endpoint name in the format <username>@<hostname> in the Source User field
  - To search the logs of incidents involving a specific destination, enter the destination object in the Destination Field
  - To search the log of incidents based on a specific action executed on the intercepted or discovered files, choose the action from the 'Action' drop-down
  - To search the log of incidents triggered by specific rule channel, choose the rule channel from the 'Channel' drop-down
- Click 'Refresh' to view the logs filtered as per the criteria specified in the search fields.

To search the logs of the archived files containing specified keywords

- Enter the keyword in the text field beside the 'Search in Content' button and click the button

Only the logs pertaining to the files containing the entered keyword and the respective file names will be displayed as a separate list at the right of the interface.



The administrator can download any file by clicking the download icon.

The following sections provide detailed explanations on:

- **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**

10.1. Viewing Hidden Archive Logs

By default, the logs pertaining to 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.
- Select the 'Show all' checkbox.

10.2. Viewing Details of a Log Entry

Comodo MyDLP enables the administrator to view the granular details of any logged incident, including the source endpoint,

user, destination, files intercepted/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 data transfer policy rule or the discovery rule.

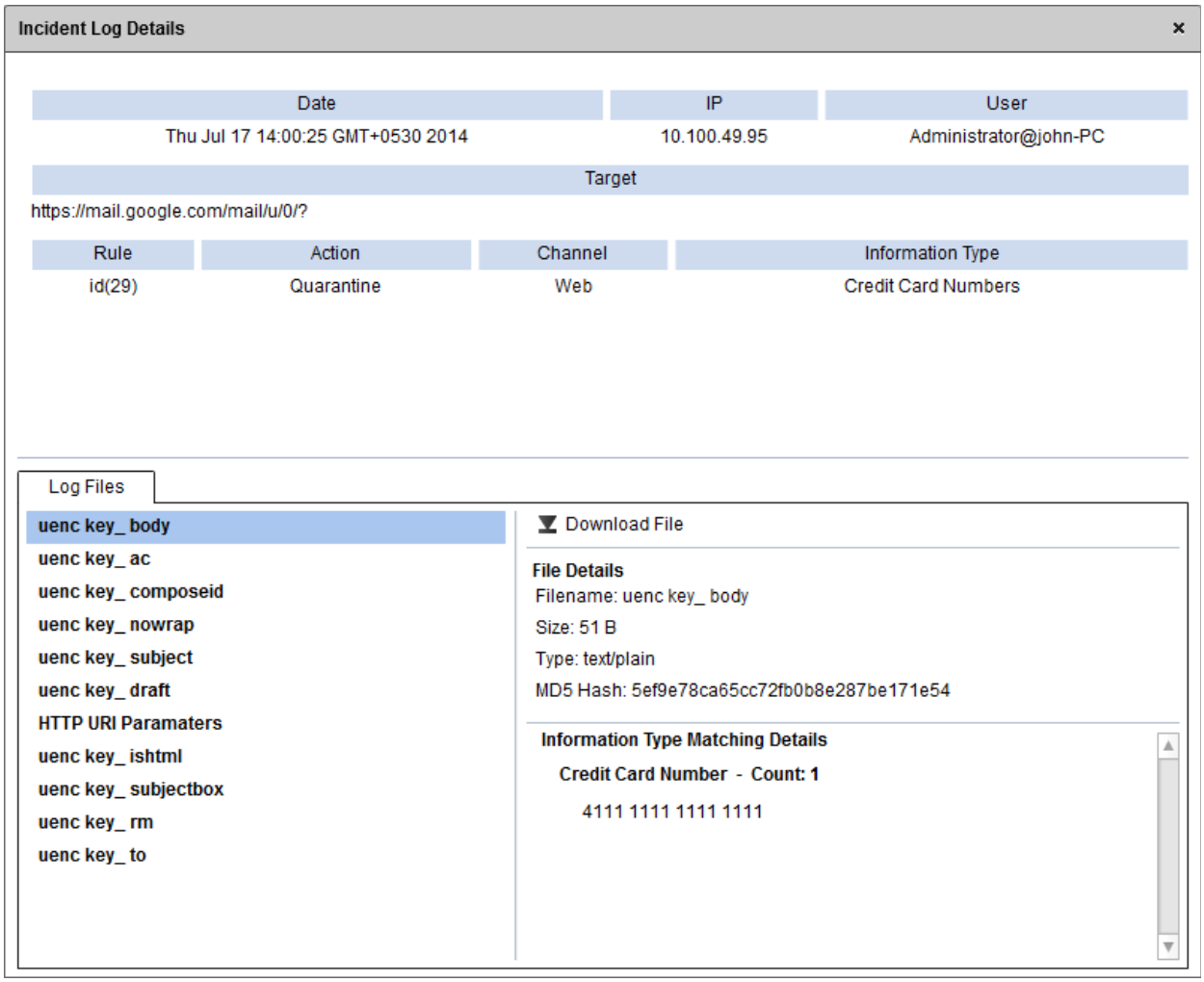
- To open the Incident Log Details pane for a log entry, click the icon for the log entry under the Details column.

The pane is slightly different for the incidents depending on the Rule Channels, to show the details that pertain to the respective 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**
- **Endpoint Discovery Rule**
- **Remote Storage Discovery Rule**

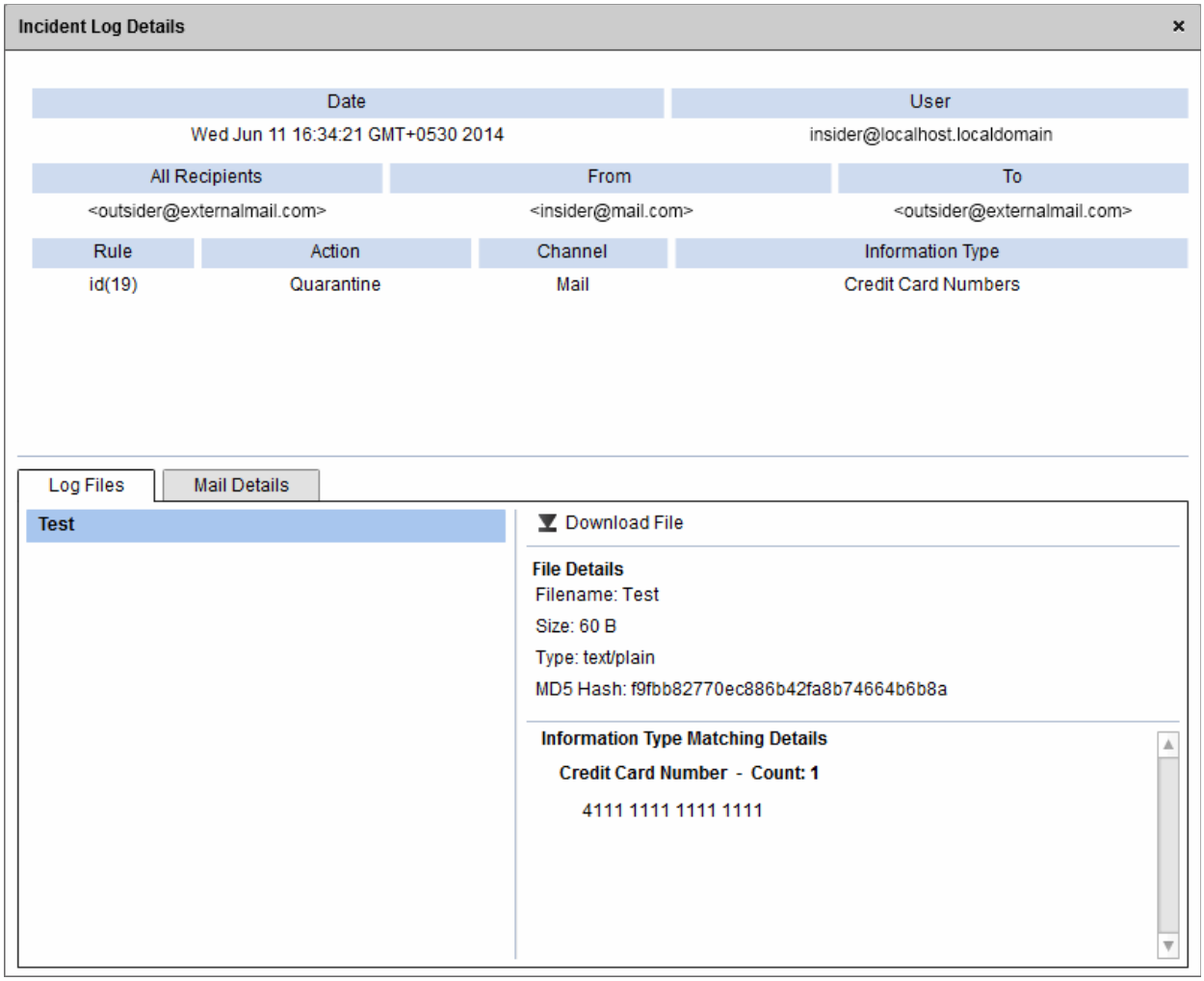
Web rule



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.
Target	The destination webpage to which the file(s) is/are uploaded.
Rule	The name of the rule based on which the files are intercepted.
Action	The action executed on the file(s) intercepted. Refer to the section **Rule Actions** for a list of actions.
Channel	Indicates the type of the rule based on which the files are intercepted.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Log Files	The Log Files displays a list of files that were identified as containing sensitive data matching the Information type specified in the web rule. The details of the select file will be displayed at the right hand side pane.
Download File	Enables the administrator to download the selected file. Refer to the section **Downloading the Files Archived by MyDLP** for more details.
File Details	Displays the file name, size, file type and MD5 HASH digest of the selected file
Information Type Matching Details	Displays the data contained in the file, that matched with the Information Type specified in the web rule.

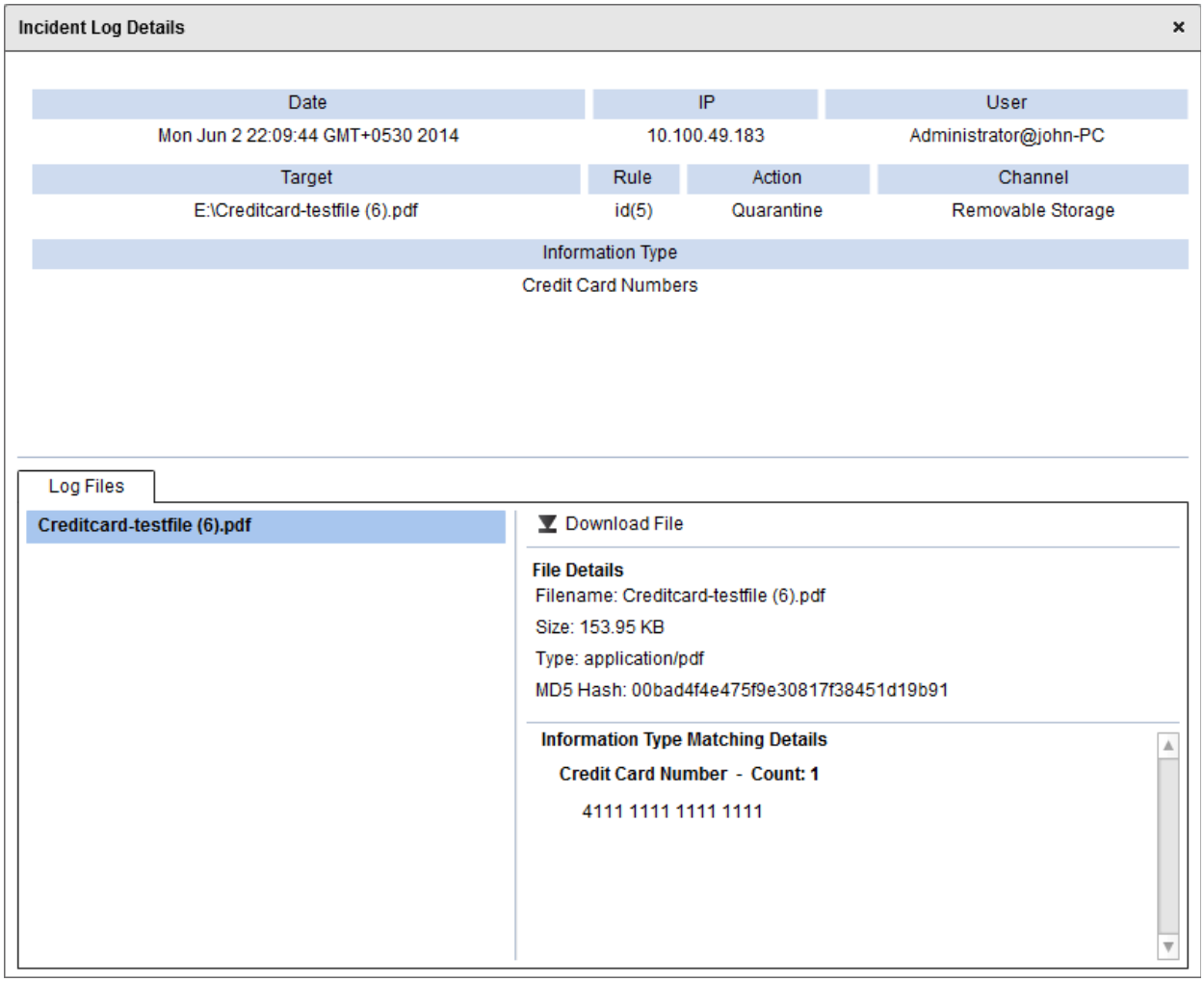
Mail rule



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.	
All Recipients	Displays the email addresses of all the mail recipients, that were added to the To:. CC:, and BCC: fields	
From	The email account from which the mail was sent	
To	The email address to which the email was sent	
Rule	The name of the rule based on which the files are intercepted.	
Action	The action executed on the file(s) intercepted.	
Channel	Indicates the type of the rule based on which the files are intercepted.	
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)	
Log Files tab	The Log Files displays a list of files that were identified as containing sensitive data matching the Information type specified in the mail rule. The details of the selected file will be displayed in the right hand side pane.	
	Download File	Enables the administrator to download the selected file. Refer to the section

		Downloading the Files Archived by MyDLP for more details.
	File Details	Displays the file name, size, file type and MD5 HASH digest of the selected file
	Information Type Matching Details	Displays the data contained in the file, that matched with the Information Type specified in the rule.
Mail Details tab	Displays the Email addresses of the sender, recipient(s) add to the To: field, recipient(s) add to the CC: field, recipient(s) add to the BCC: field separately and allows the administrator to resend the mail if found legitimate. Refer to the section '**Resending Mails Intercepted by Mail Rules**' for more details.	

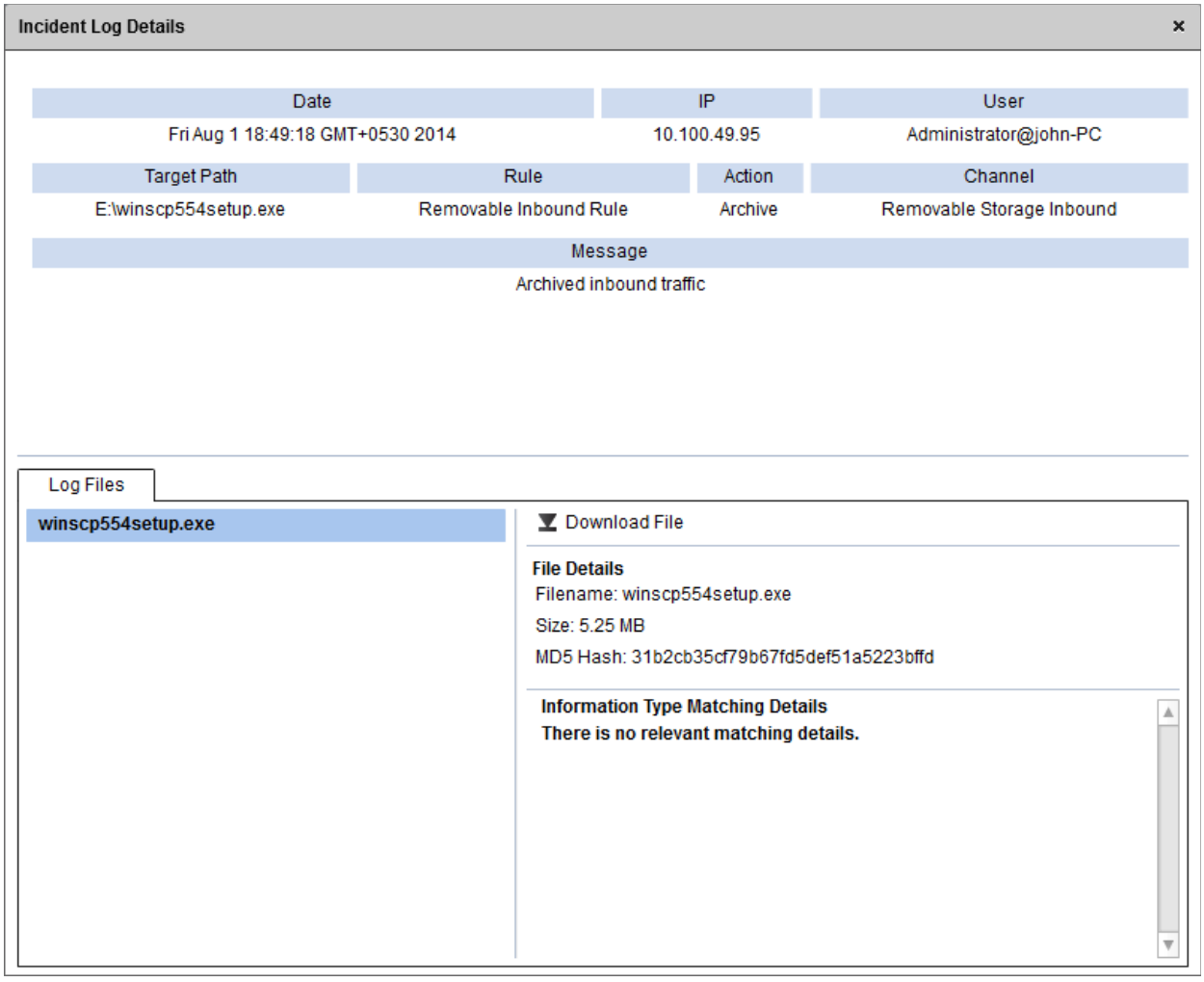
Removable Storage rule



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.
Target	The location in the local drive of the endpoint computer or the network storage from which the file was copied/moved.
Rule	The name of the rule based on which the files are intercepted.

Action	The action executed on the file(s) intercepted.
Channel	Indicates the type of the rule based on which the files are intercepted.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Log Files	The Log Files displays a list of files that were identified as containing sensitive data matching the Information type specified in the Removable Storage rule. The details of the selected file will be displayed in the right hand side pane.
Download File	Enables the administrator to download the selected file. Refer to the section **Downloading the Files Archived by MyDLP** for more details.
File Details	Displays the file name, size, file type and MD5 HASH digest of the selected file
Information Type Matching Details	Displays the data contained in the file, that matched with the Information Type specified in the rule.

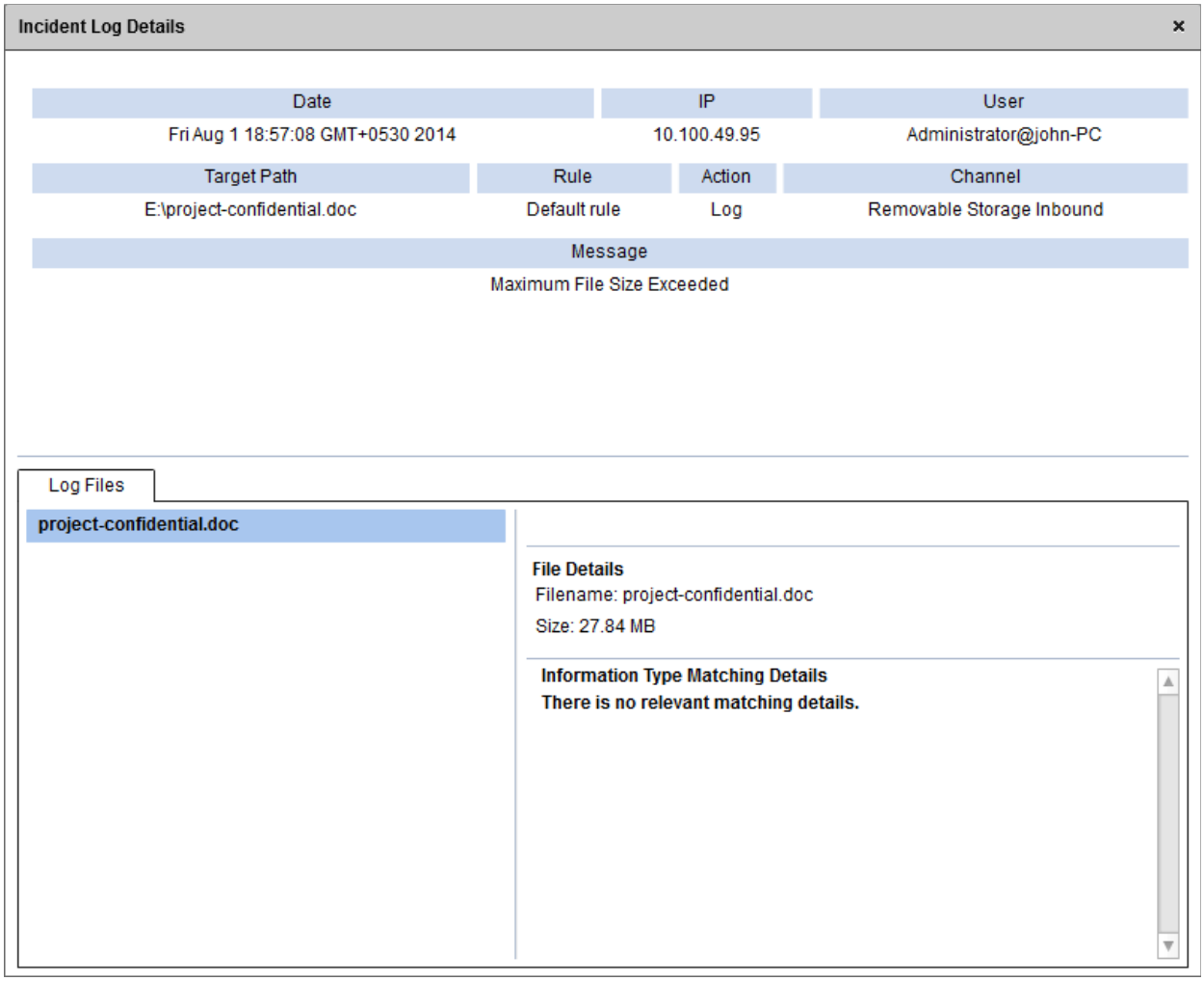
Removable Storage Inbound rule



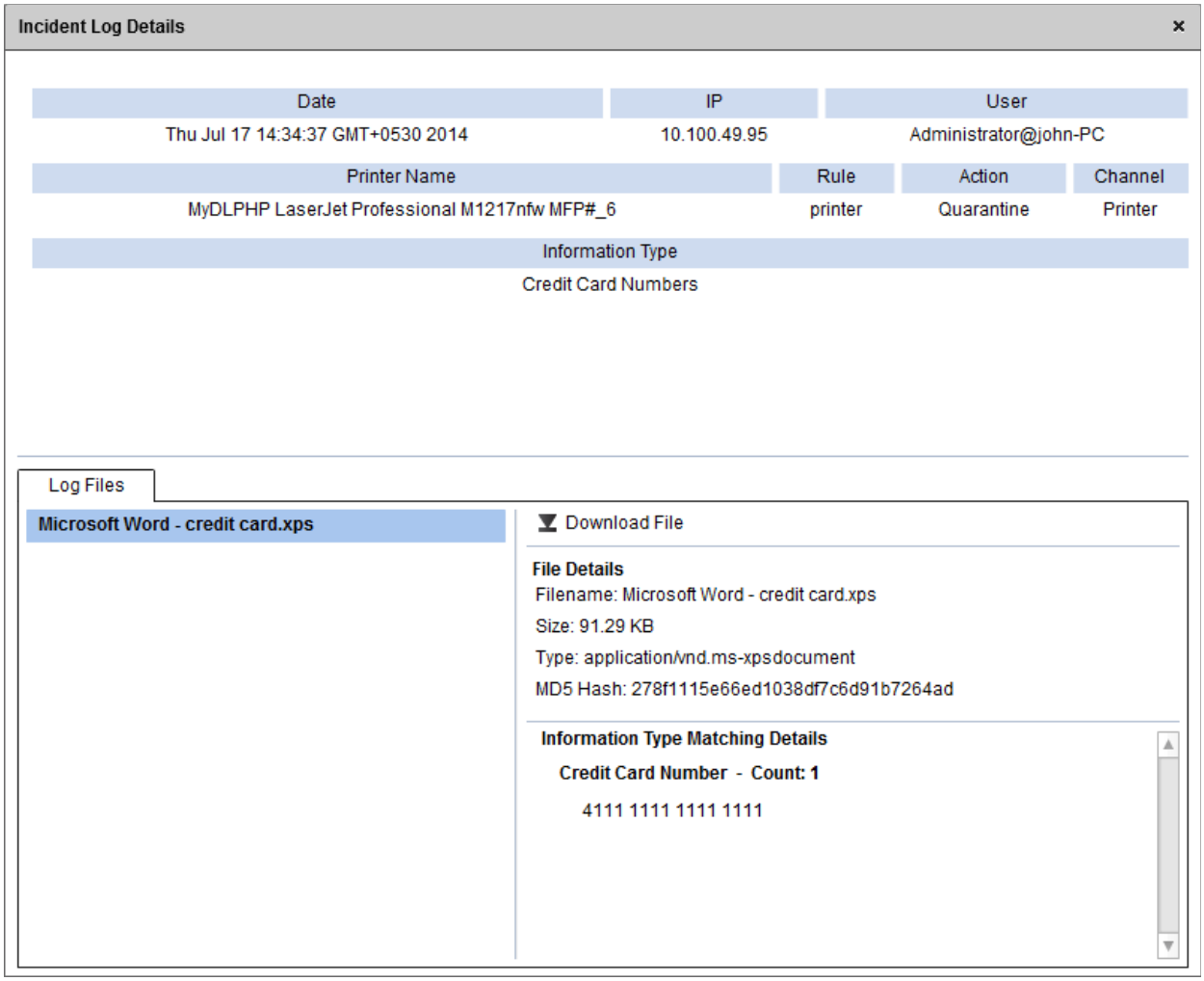
Incident Log Details - Removable Storage Rule	
Field	**Description**
Date	Precise date and time of the incident.

IP	The IP address of the source end-point at which the file(s) is read/copied from a removable storage.
User	The user logged-in at the time of incident.
Target Path	The location in the removable storage from which the file was read/copied.
Rule	The name of the rule based on which the files are intercepted.
Action	The action executed on the file(s) intercepted.
Channel	Indicates the type of the rule based on which the files are intercepted.
Message	A short description of the incident.
Log Files	The Log Files displays a list of files that were identified as per the Removable Storage Inbound rule. The details of the selected file will be displayed in the right hand side pane.
Download File	Enables the administrator to download the selected file. Refer to the section **Downloading the Files Archived by MyDLP** for more details.
File Details	Displays the file name, size, file type and MD5 HASH digest of the selected file
Information Type Matching Details	Displays the data contained in the file, that matched with the Information Type specified in the rule.

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' as shown below.



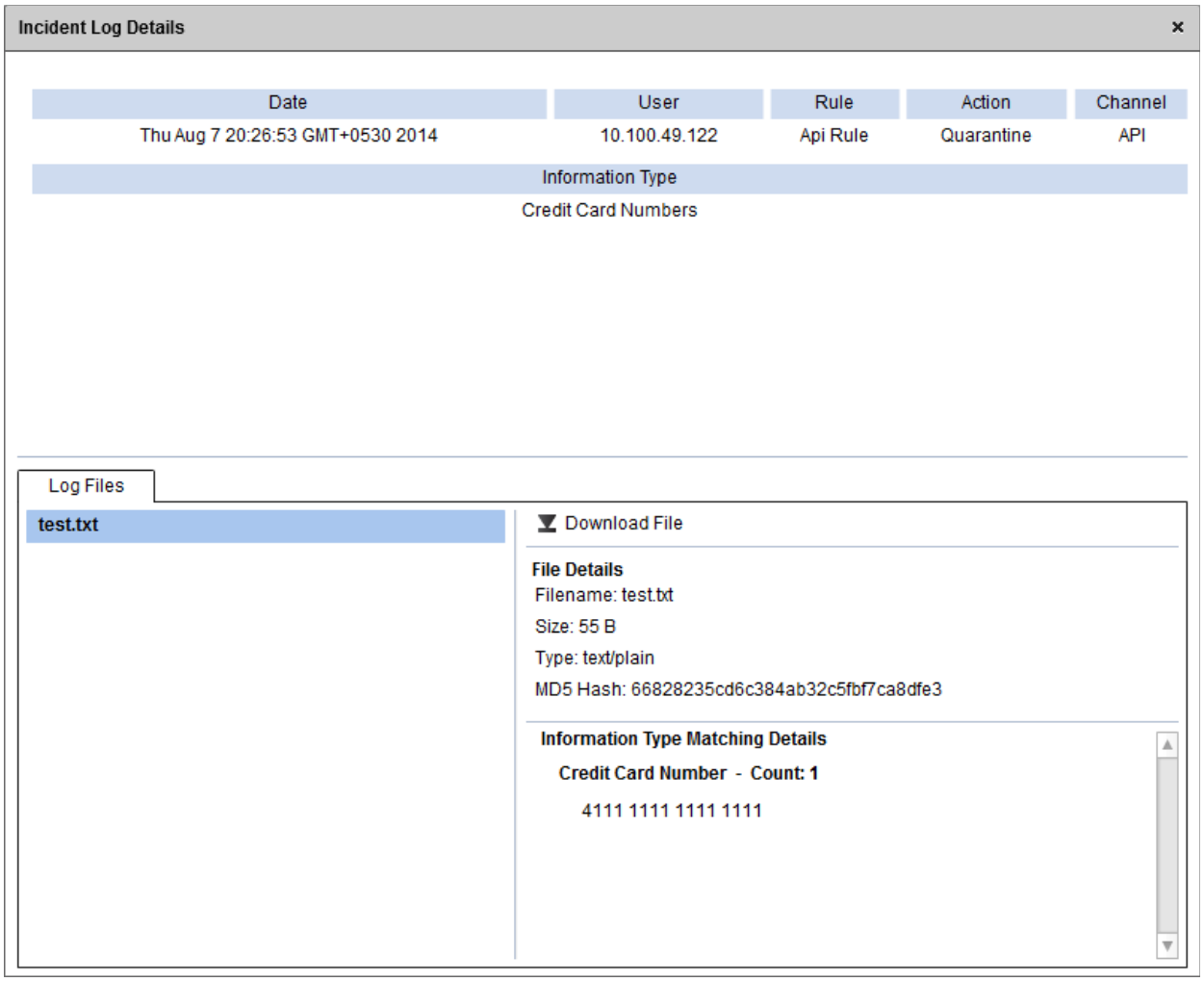
Printer rule



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.
Printer	The printer chosen for printing the file.
Rule	The name of the rule based on which the files are intercepted.
Action	The action executed on the file(s) intercepted.
Channel	Indicates the type of the rule based on which the files are intercepted.
Information Type	The information type specified in the printer rule, matching which, the sensitive data were contained in the file(s)
Log Files	The Log Files displays a list of files that were identified as containing sensitive data matching the Information type specified in the Printer rule. The details of the selected file will be displayed in the right hand side pane.
Download File	Enables the administrator to download the selected file. Refer to the section **Downloading the Files**

	Archived by MyDLP for more details.
File Details	Displays the file name, size, file type and MD5 HASH digest of the selected file
Information Type Matching Details	Displays the data contained in the file, that matched with the Information Type specified in the rule.

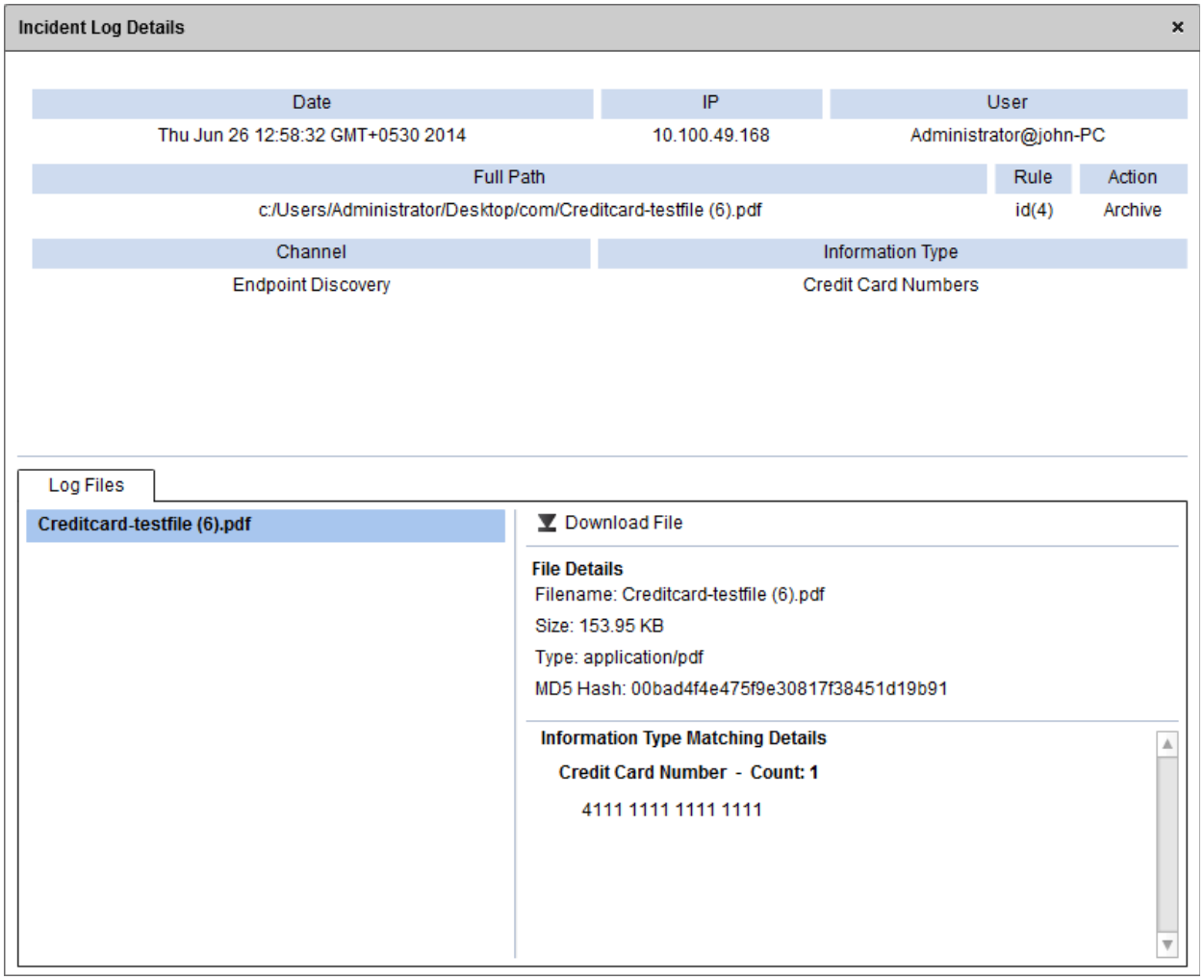
API rule



Incident Log Details - Printer 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
Rule	The name of the rule based on which the files are intercepted.
Action	The action executed on the file(s) intercepted.
Channel	Indicates the type 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)

Log Files	The Log Files displays a list of files that were identified as containing sensitive data matching the Information type specified in the Printer rule. The details of the selected file will be displayed in the right hand side pane.
Download File	Enables the administrator to download the selected file. Refer to the section **Downloading the Files Archived by MyDLP** for more details.
File Details	Displays the file name, size, file type and MD5 HASH digest of the selected file
Information Type Matching Details	Displays the data contained in the file, that matched with the Information Type specified in the rule.

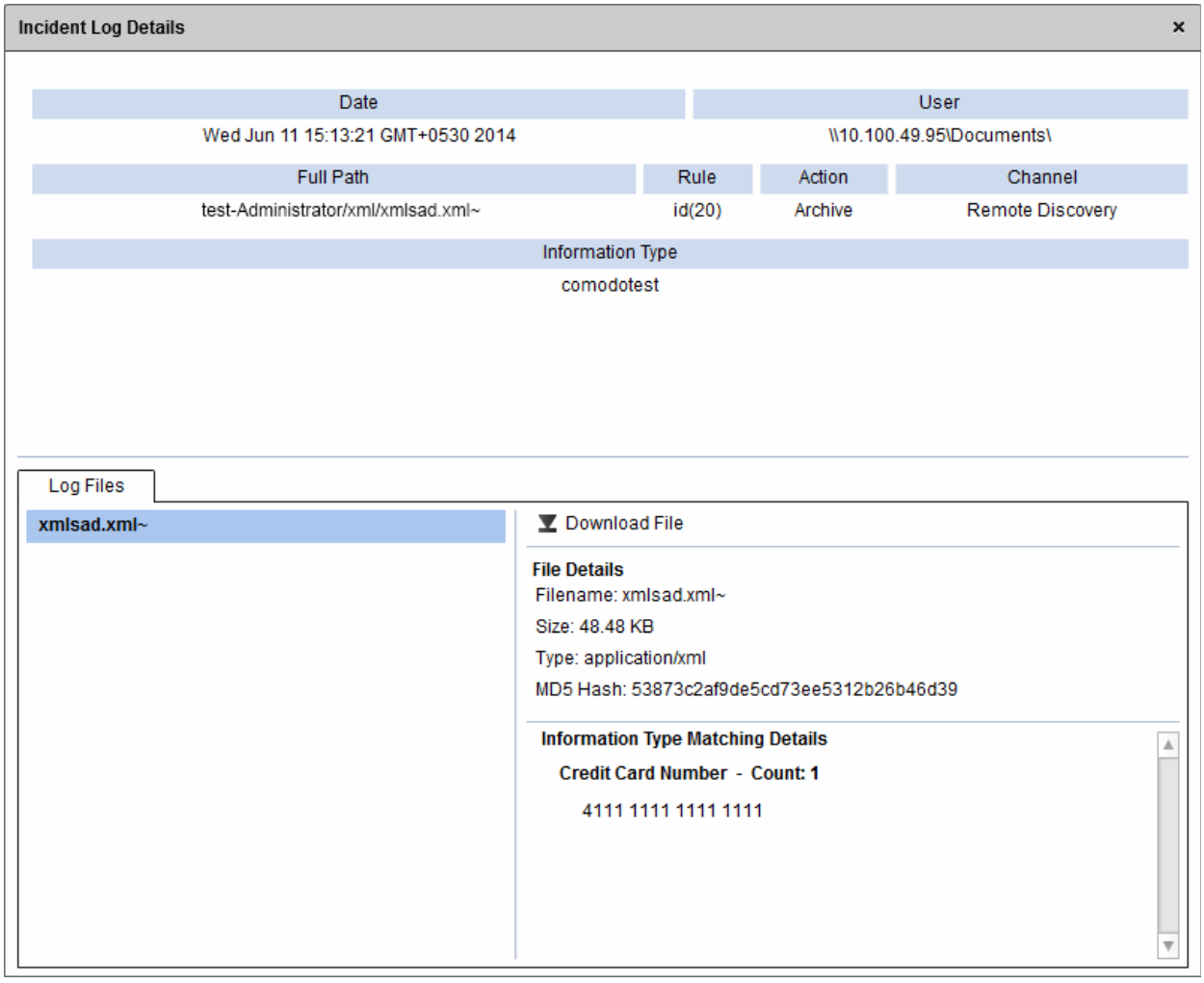
Endpoint Discovery Rule



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.
Full Path	The file paths of locations in the local drive of the end-point, from which the the files were discovered.
Rule	The name of the rule based on which the files were discovered.

Action	The action executed on the discovered file(s).
Channel	Indicates the type of the rule based on which the files are discovered.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Log Files	The Log Files displays a list of files that were identified as containing sensitive data matching the Information type specified in the Endpoint Discovery rule. The details of the selected file will be displayed in the right hand side pane.
Download File	Enables the administrator to download the selected file. Refer to the section **Downloading the Files Archived by MyDLP** for more details.
File Details	Displays the file name, size, file type and MD5 HASH digest of the selected file
Information Type Matching Details	Displays the data contained in the file, that matched with the Information Type specified in the rule.

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.
Full Path	The file paths of locations in the remote storage from which the the files were discovered.
Rule	The name of the rule based on which the files were discovered.
Action	The action executed on the discovered file(s).
Channel	Indicates the type of the rule based on which the files are discovered.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Log Files	The Log Files displays a list of files that were identified as containing sensitive data matching the Information type specified in the Network Storage Discovery rule. The details of the selected file will be displayed in the right hand side pane.
Download File	Enables the administrator to download the selected file. Refer to the section **Downloading the Files Archived by MyDLP** for more details.
File Details	Displays the file name, size, file type and MD5 HASH digest of the selected file
Information Type Matching Details	Displays the data contained in the file, that matched with the Information Type specified in the rule.

10.3. 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 Incident Log Details pane will open.
- Select the file to be downloaded, under 'Log Files'
- Click the 'Download File' link.

You can save the file in your local storage.

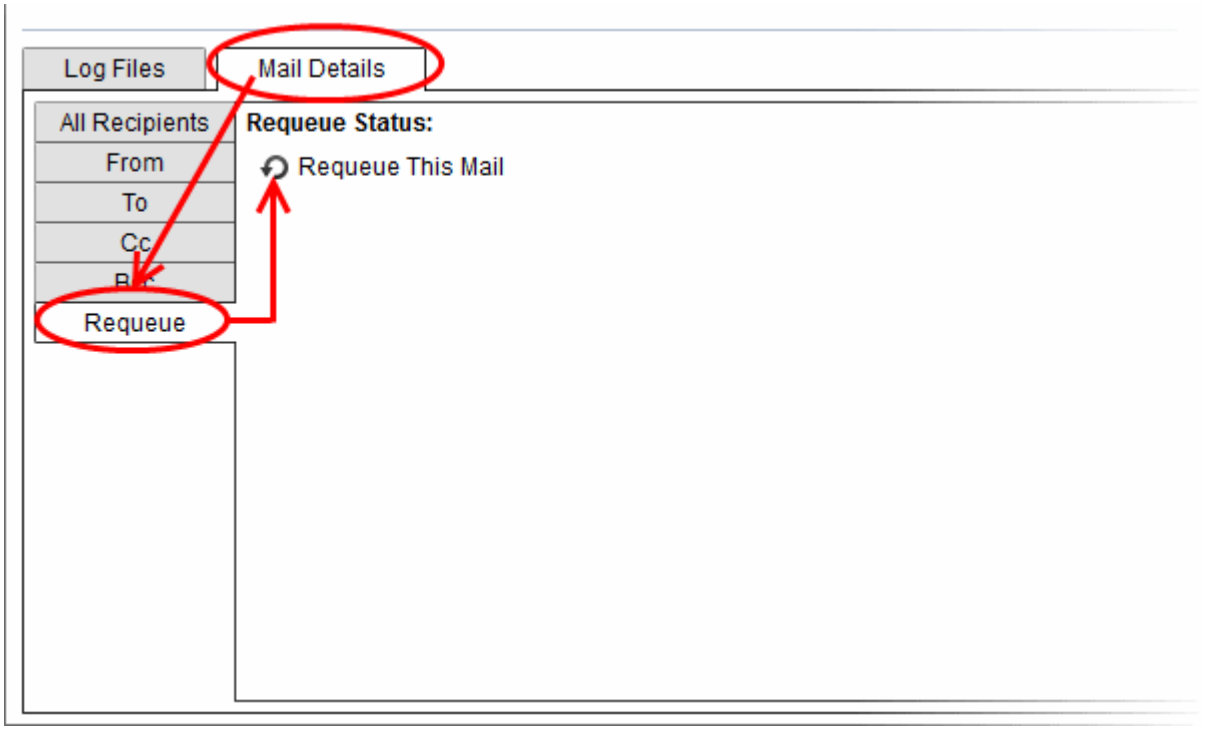
10.4. Resending Mails Intercepted by Mail Rules

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

To resend the archived emails

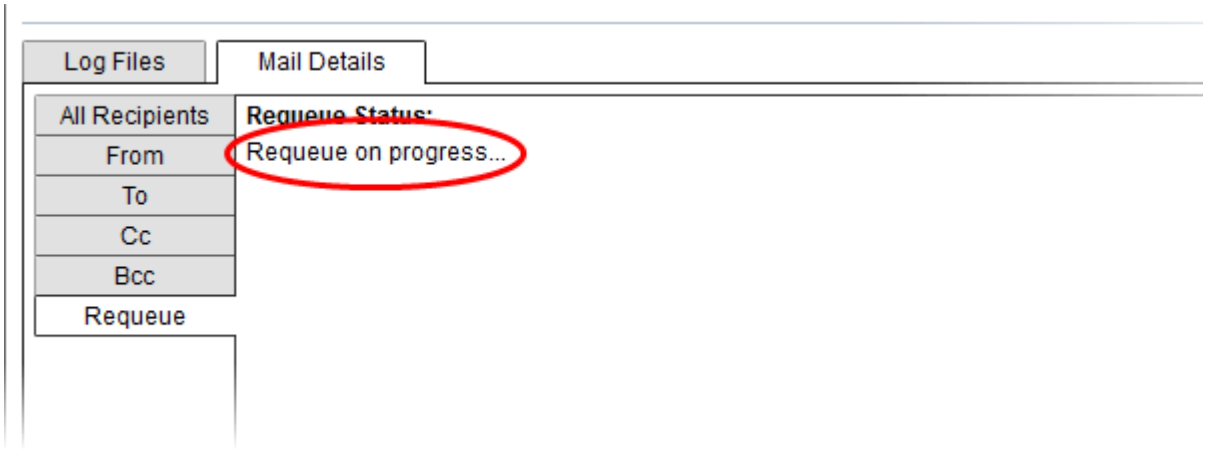
- Open the Logs interface by clicking the Logs tab
- Search for the log entry pertaining to the quarantined email using the search options. Refer to the explanation under '**Filtering and Search Options**' in the section '**The Logs tab**' for more details.
- Click the icon for the log entry under the Details column. The Incident Log Details pane will open.
- Select the file to be downloaded, under 'Log Files'
- Click the 'Download File' link, save the file in your local storage and examine them.

- If the email is found legitimate, click the Mail Details from the lower pane and select 'Requeue'



- Click the 'Requeue This Mail' link from the RHS pane.

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

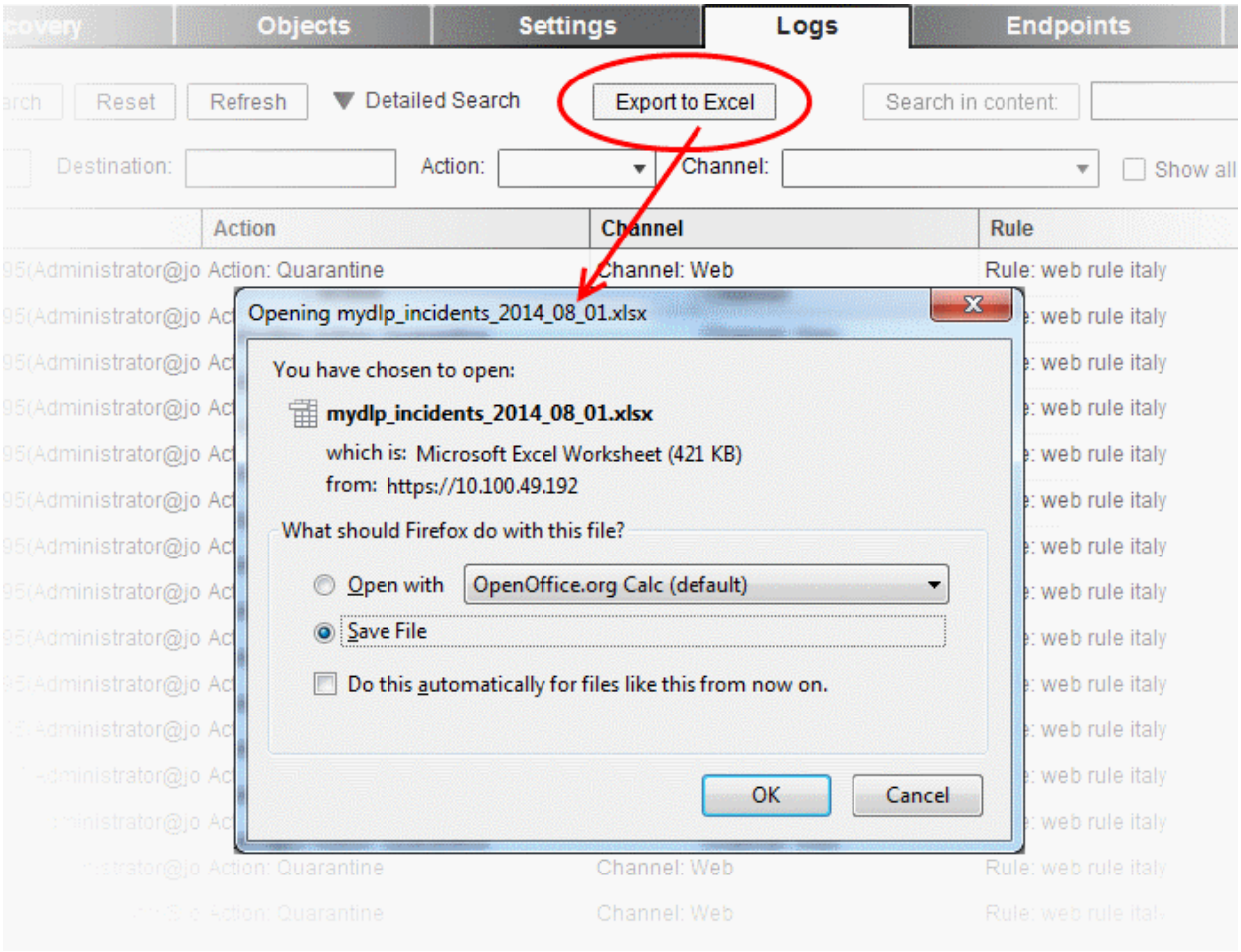


- Click 'Refresh' from the Logs interface. The mail will be sent.

10.5. 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 and save the file in your local drive.



11. The Endpoints Tab

Comodo MyDLP monitors and controls the data transfer to and from the endpoints and performs discovery scans on the endpoints based on the Data Transfer Policy rules and Endpoint Discovery rules in which they are specified as sources. In order for MyDLP server to monitor the traffic and scan the endpoints, the MyDLP Endpoint Agent needs to be installed in each of the endpoint. Once installed, the agent will poll the MyDLP server periodically and receive the commands from the MyDLP server and form a secure communication channel between the endpoint and the server.

The endpoint agent can be installed on the network computers in many 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 communicate with the server.

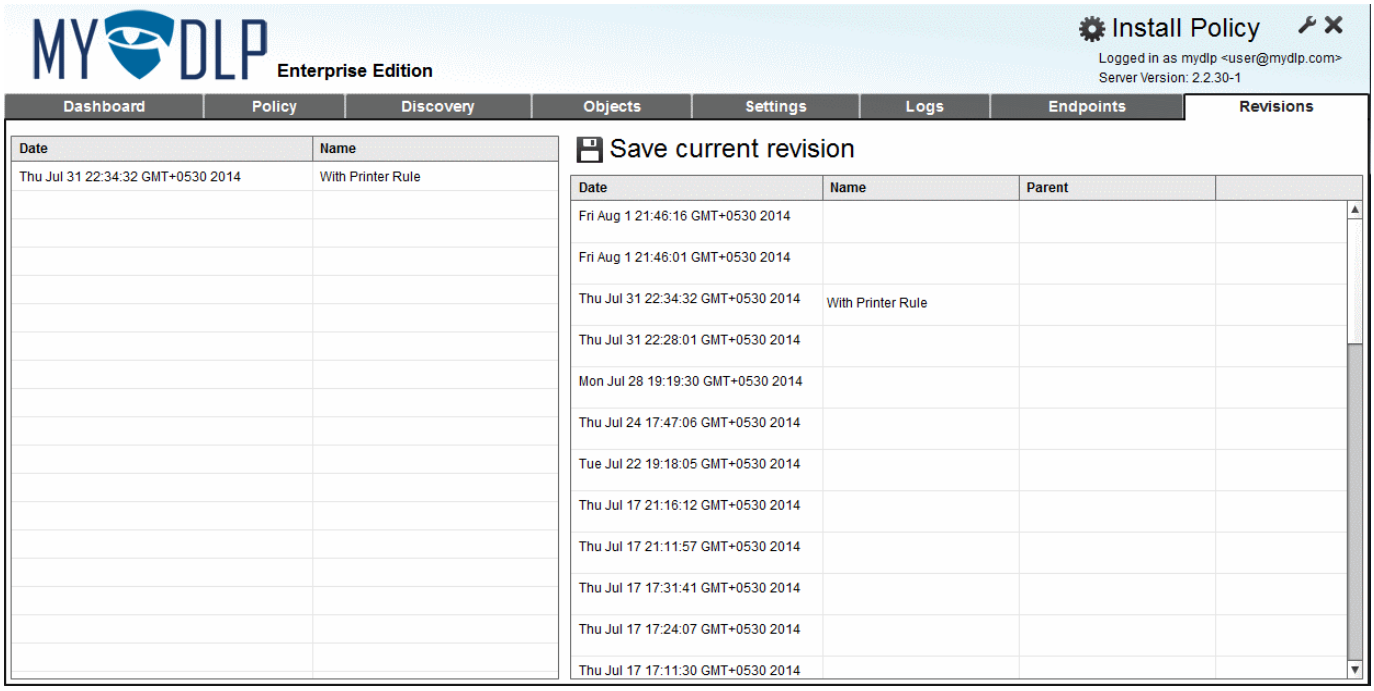
Endpoints Table - Column Descriptions	
Column	**Description**
Endpoint	The Unique Identification (ID) number assigned to the endpoint by MyDLP, upon installation of the agent and the first time when the agent polls the server, via a secure protocol. The ID remains unchanged even if the host name and/or 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.

The interface displays a snapshot summary of status of the endpoints and the agent versions. The administrator can search for specific endpoint(s) by entering their hostname, IP address, ID, and version of the installed agent either partially of fully in the text box at the top of the table and clicking 'Search'.

- Clicking 'Refresh' adds the newly added endpoints and removes the endpoints from which the agent is removed.
- Clicking 'Truncate' clears the full list and creates a new list of endpoints that are currently connected to the server.

12. The Revisions Tab

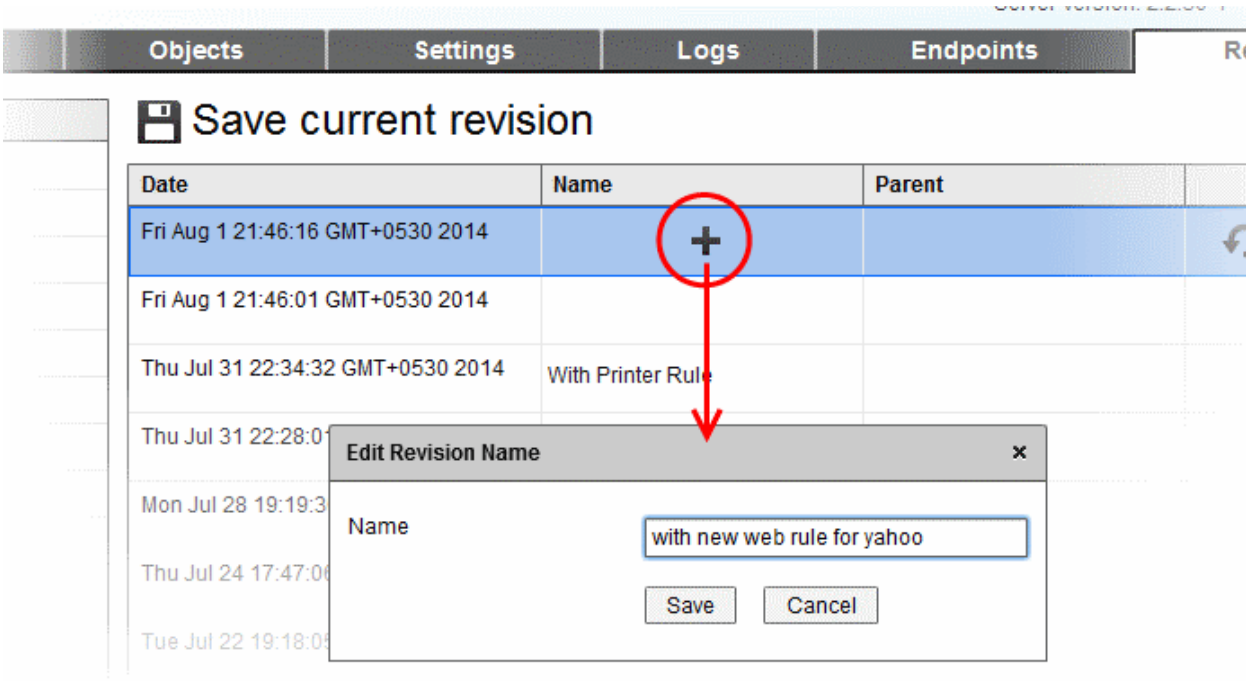
Comodo MyDLP saves the policies with the set of rules, every time a new policy is applied to the network. The 'Revisions' interface displays a list of MyDLP Policies that were applied whenever an administrator creates/edits rules in chronological order. The administrator can bookmark the policies by 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

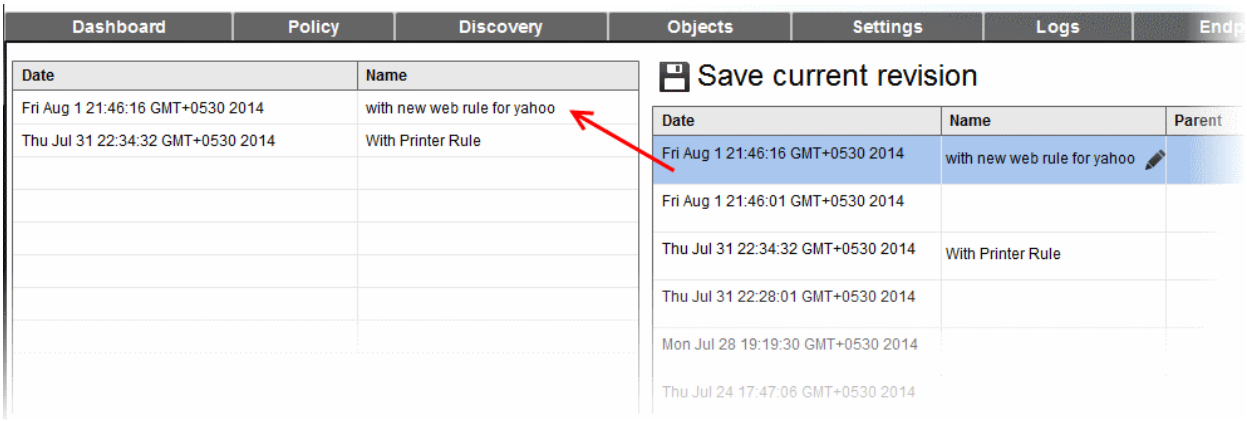
- Select the policy revision and select the  icon that appears in the Name column.



The 'Edit Revision Name' dialog will appear.

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

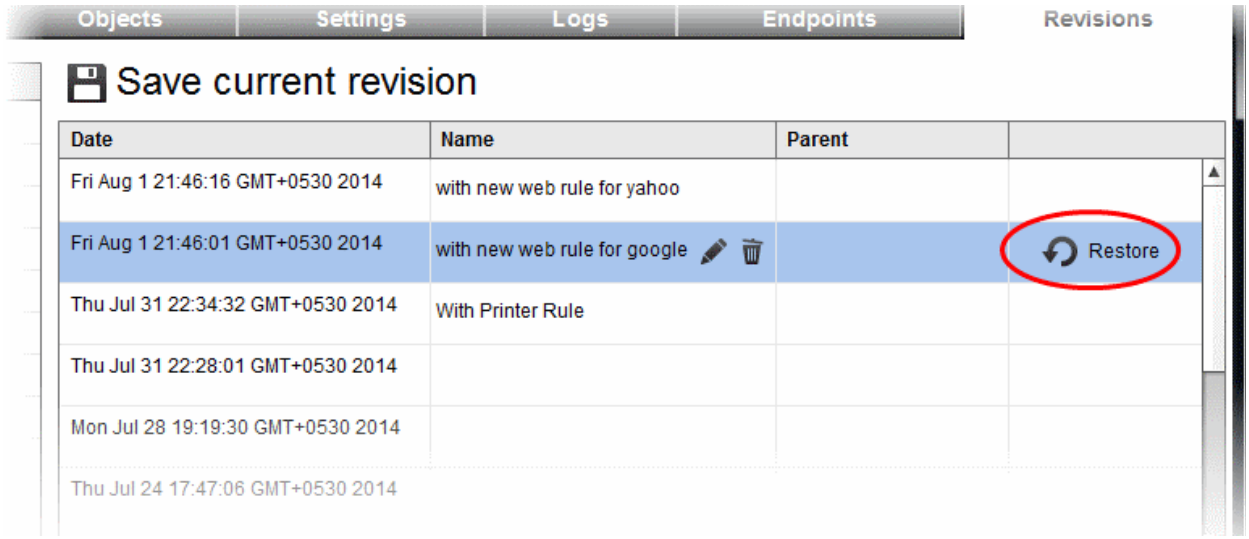
The revision will be saved as a bookmark and added to the list at the left hand side.



To re-apply a policy from the revisions

- Select the policy revision
- Click the Restore icon that appears in the Controls column at the right end.

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



About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

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**.