



# Comodo Dome Data Protection

Software Version 3.13

## Administrator Guide

Guide Version 3.13.082918

## Table of Contents

<b>1. Introduction to Comodo Dome Data Protection.....</b>	<b>5</b>
<b>2. Get Started with CDDP.....</b>	<b>6</b>
2.1. Installation.....	6
2.2. Log in to the Management Console.....	6
2.3. Log Out.....	7
2.4. Check Server Version and License Information.....	8
2.5. Change your Password.....	8
2.6. Change User Information.....	9
<b>3. The Dashboard.....</b>	<b>11</b>
<b>4. Data Control and Data Transfer Policies.....</b>	<b>13</b>
4.1. The Rules Interface .....	15
4.1.1. Rule Channels / Types.....	17
4.1.2. Rule Actions .....	18
4.1.3. Email Notifications and Messages for a Rule.....	18
4.1.4. Add a Data Transfer Rule.....	19
4.1.5. Add a Data Discovery Rule.....	35
4.1.6. Deploy a Policy.....	56
<b>5. Rule Types, Objects and Matchers.....</b>	<b>56</b>
5.1. Rule Types.....	57
5.1.1. Web Rule .....	58
5.1.2. Mail Rule .....	59
5.1.3. Removable Storage Rule .....	59
5.1.4. Network Share Rule.....	61
5.1.5. Removable Storage Inbound Rule .....	61
5.1.6. Removable Storage Encryption Rule .....	62
5.1.7. Printer Rule .....	62
5.1.8. ScreenShot Rule .....	63
5.1.9. API Rule .....	64
5.1.10. USB Device Access Rule.....	65
5.1.11. CD-DVD Rule .....	66
5.1.12. Floppy Rule .....	66
5.1.13. Clipboard Rule.....	66
5.1.14. Endpoint Discovery Rule.....	67
5.1.15. Remote Storage Rule.....	67
5.1.16. Database Discovery Rule.....	68
5.2. Objects.....	69
5.2.1. Object Types.....	70
5.2.2. Information Types - An Overview.....	72
5.2.2.1. Predefined Matcher Types .....	76
5.2.2.2. Predefined Information Types.....	79
5.2.2.3. Predefined Information Type Groups.....	86

5.2.3.User Defined Objects .....	89
5.2.3.1.Add a User Defined Network Object.....	90
5.2.3.2.Add a User Defined Computer Object .....	92
5.2.3.3.Add a User Defined Information Type .....	94
5.2.3.4.Add a User Defined Information Type Group.....	104
5.2.3.5.Add a User Defined Domain Object .....	105
5.2.3.6.Add a User Defined Application Object .....	107
5.2.3.7.Add a User Defined USB Device Object.....	109
5.2.3.8.Add a User Defined User Object .....	114
5.2.3.9.Add a User Defined Active Directory Users Object.....	115
5.2.3.10.Add a User Defined File System Directory.....	117
5.2.3.11.Add a User Defined Remote Storage Object.....	118
5.2.3.12.Add a Database Discovery Object.....	126
5.3.Matchers.....	127
5.3.1.Manage Document Databases.....	128
5.3.1.1.Add a Document Database.....	128
5.3.1.2.Edit a Document Database.....	137
5.3.2.Manage File Extensions .....	138
5.3.2.1.Add a New File Extension .....	139
5.3.2.2.Edit a File Extension .....	140
5.3.3.Manage Keyword Databases.....	142
5.3.3.1.Add a User Defined Keyword Database.....	142
5.3.3.2.Edit a User Defined Keyword Database.....	154
5.3.4.Manage Data Formats.....	156
5.3.4.1.Add a New User Defined Data Format Entry.....	156
5.3.4.2.Edit a Data Format.....	159
5.4.Integrate Active Directory Domains.....	161
5.4.1.Add a New AD Domain.....	162
5.4.2.Edit Existing AD Domains.....	165
5.5.Integrate RDBMS Systems.....	166
5.5.1.Add a New RDBMS Object.....	167
5.5.2.Edit an RDBMS Object.....	169
<b>6. Configure Comodo Dome Data Protection Settings.....</b>	<b>170</b>
6.1.Configure Protocol Settings.....	170
6.2.Manage Administrators.....	172
6.2.1.Add New Administrative Users.....	173
6.2.2.Set and Reset Password for Administrative Users.....	175
6.2.3.Edit and Remove Admin Users .....	177
6.3.Configure Endpoint Settings.....	178
6.4.Configure Advanced Settings.....	181
6.5.Configure Enterprise Settings.....	184
<b>7. The Logs Tab .....</b>	<b>187</b>
7.1.View Hidden Archive Logs.....	190

7.2.View Details of a Log Entry.....	190
7.3.Download the Files Archived by CDDP.....	217
7.4.Resend Mails Intercepted by Mail Rules.....	218
7.5.Export the Logs to a Spreadsheet File.....	219
<b>8. The Endpoints Tab .....</b>	<b>220</b>
<b>9. The Revisions Tab .....</b>	<b>221</b>
<b>10. Configure License and CDDP Server settings.....</b>	<b>227</b>
10.1.Network Configuration.....	228
10.2.DNS Configuration.....	229
10.3.Shutting Down or Restarting the Server .....	231
10.4.Email Server Configuration.....	231
10.5.Manually Update the CDDP Server.....	233
10.6.Download and Configure Certificate Settings for CDDP.....	233
<b>About Comodo Security Solutions.....</b>	<b>235</b>

# 1. Introduction to Comodo Dome Data Protection

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

The two main components of the product are the Comodo Dome Data Protection Network Server and the Comodo Dome Data Protection Endpoint Agent.

## Protection and Administration with CDDP Network Server

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

## Endpoint Protection and Discovery with CDDP Endpoint

CDDP Endpoint can detect when confidential data is moved from endpoints to removable devices such as USB sticks or portable hard disks. You can also enforce full disk encryption on removable devices. Endpoint protection also covers any document printed using network and local printers and taking screenshots of sensitive documents. Endpoint data discovery lets you detect and enforce policy on stored data.

## Guide Structure:

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

- **Introduction to Comodo CDDP**
- **Get started with CDDP**
  - **Installation**
  - **Log in to the Management Console**
  - **Log out**
  - **Check Server Version and License Information**
  - **Change your Password**
  - **Change User Information**
- **The Dashboard**
- **Data Control and Data Transfer Policies**
  - **The Rules Interface**
- **Rule Types, Objects and Matchers**
  - **Rule Types**
  - **Objects**
  - **Matchers**
  - **Integrate Active Directory Domains**
  - **Integrate RDMBS Connections**
- **Configure CDDP Settings**
  - **Configure Protocol Settings**
  - **Manage Administrators**

- [Configure Endpoint Settings](#)
- [Configure Advanced Settings](#)
- [Configure Enterprise Settings](#)
- [The Logs tab](#)
  - [View Hidden Archive Logs](#)
  - [View Details of a Log Entry](#)
  - [Download the Files Archived by CDDP](#)
  - [Resend Mails Intercepted by Mail Rules](#)
  - [Export the Logs to a Spreadsheet File](#)
- [The Endpoints Tab](#)
- [The Revisions Tab](#)
- [Configure License and CDDP server settings](#)

## 2. Get Started with CDDP

Comodo offers Dome Data Protection application in two variations. You can install the application on a server located on your premises or use the SaaS version. This section describes how to install CDDP on your premises. For SaaS instructions, please see DDP Cloud Version guide.

**CDDP on-premise application** - After purchase, you can download the application images from the URL mentioned in the confirmation email. See the next section, '[Installation](#)', for details about installing and configuring CDDP application on your network server.

### 2.1. Installation

- For CDDP Network Server installation, please see [CDDP Installation Guide](#).
- For CDDP Endpoint deployment, please see [CDDP Endpoint Installation Guide](#).

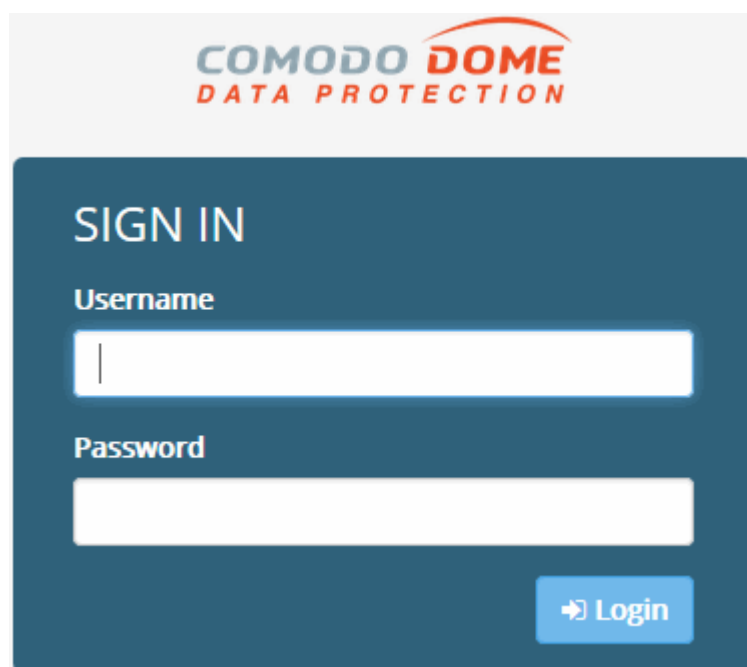
**Tip:** Comodo Dome Data Protection Windows Endpoint Agent setup file can be downloaded from the 'License' > 'Downloads' interface of the Comodo Dome Data Protection server administrative console. See [Configure Protocol Settings](#) for more details.

### 2.2. Log in to the Management Console

Comodo Dome Data Protection 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 CDDP Network Server was configured during installation. For more details, see 'CDDP Network Server Initial Configuration' in the CDDP Installation Guide.

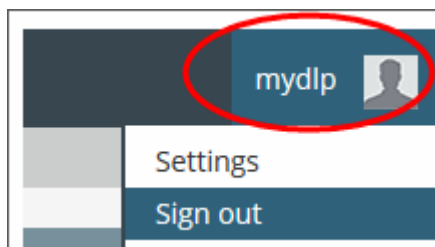


The image shows the 'SIGN IN' form for Comodo Dome Data Protection. At the top, the logo 'COMODO DOME DATA PROTECTION' is displayed. Below it, the text 'SIGN IN' is centered. There are two input fields: 'Username' and 'Password'. The 'Username' field has a cursor in it. Below the 'Password' field is a blue 'Login' button with a right-pointing arrow icon.

- 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 Change your Password](#).

## 2.3. Log Out

- Click your username top-right corner and choose 'Sign out' from the options:



## 2.4. Check Server Version and License Information

You can view the currently installed version of CDDP Server and the validity term of your license from the 'License' tab. Providing the server version number will help resolve issues faster should you need to contact support.

The screenshot shows the 'License' tab selected in the top navigation bar. A red circle highlights the 'License' tab, and a red arrow points from it to a red box in the main content area that says '19 days remaining to the expiration date'. On the left, the 'SERVER CONFIGURATION' sidebar lists: License, Network Configuration, DNS Configuration, Email Configuration, Firmware Configuration, Shutdown/Reboot, and Downloads. The main content area displays the following information:

- Server Version:** 3.13.0-01
- License Type:** Enterprise
- Subscription ID:** 439d46a772
- Expiration Date:** 16/9/2018
- Number of Allocated Seats:** 2
- Max Number of Seats:** 354
- Enter License Key:** [Text input field]
- Enter License Key** [Button]

You can also enter your new license key for renewals and configure your server settings. Please see [Configure License and CDDP server settings](#) for more details.

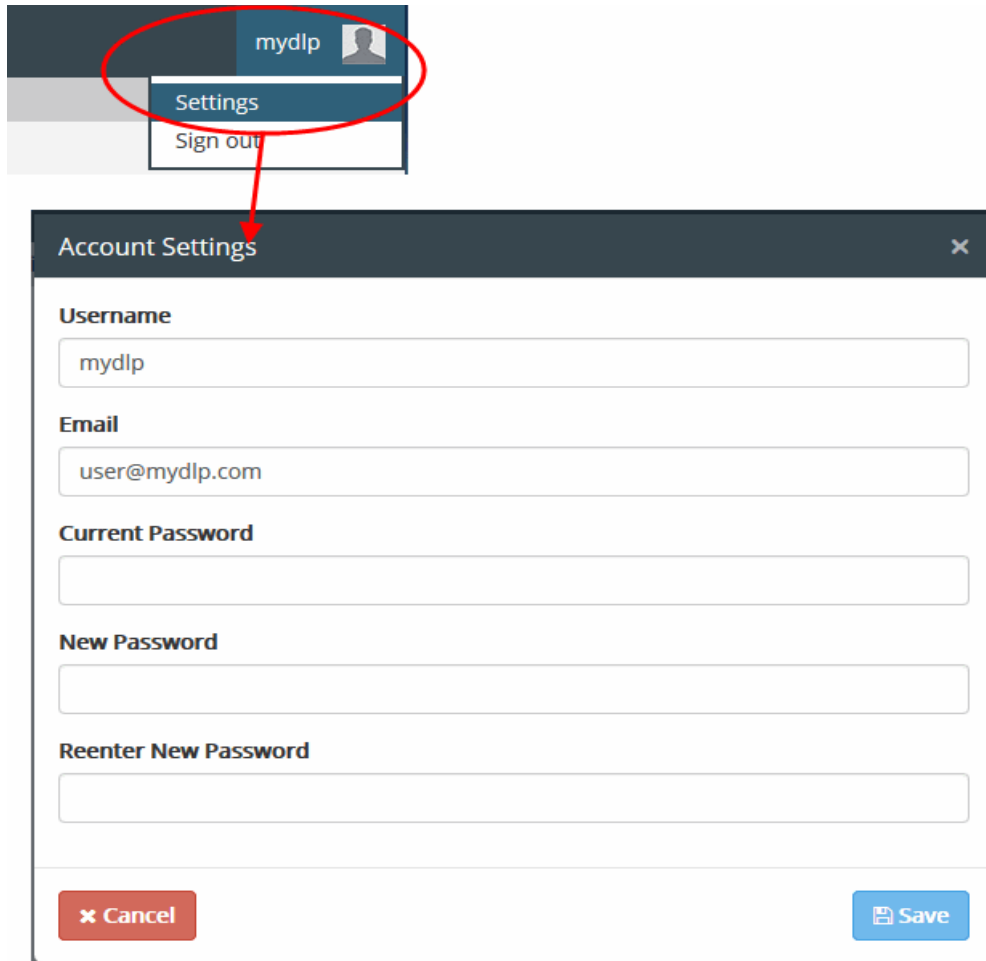
## 2.5. Change your Password

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

### To change the password

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





The image shows a user interface for 'mydlp'. A red circle highlights the 'Settings' menu item in the top navigation bar. A red arrow points from this menu item to the 'Account Settings' dialog box. The dialog box contains the following fields:

- Username:** mydlp
- Email:** user@mydlp.com
- Current Password:** (empty field)
- New Password:** (empty field)
- Reenter New Password:** (empty field)

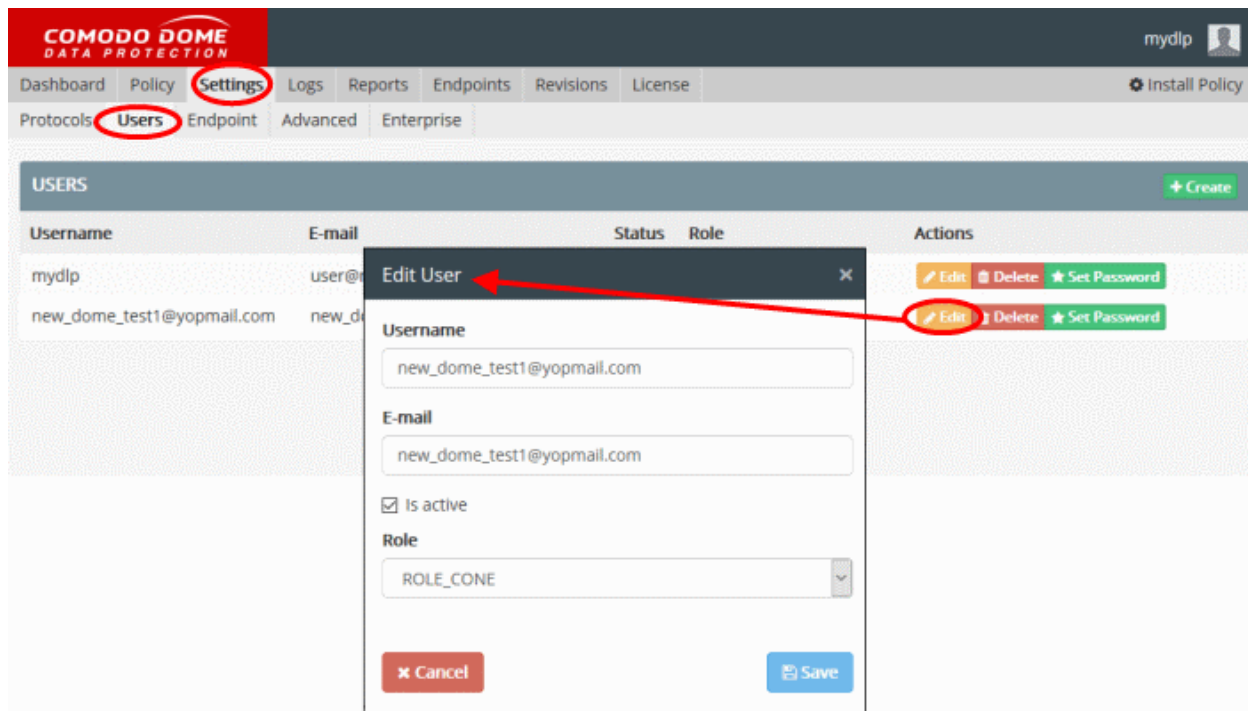
At the bottom of the dialog box, there are two buttons: 'Cancel' (red) and 'Save' (blue).

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

## 2.6. Change User Information

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

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



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

## 3. The Dashboard

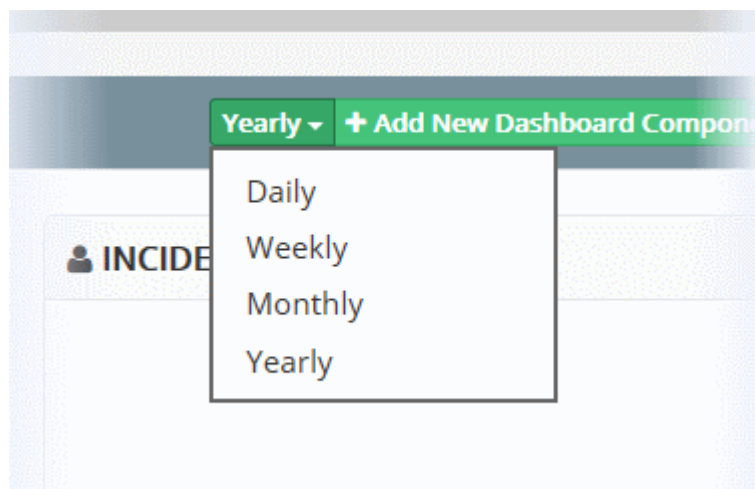
- The dashboard contains statistics which form a consolidated, 'at-a-glance' summary of all major CDDP activities for specific time intervals. Each tile is updated when one of your policy rules is triggered.
- Dashboard tiles include incidents by policy type, incidents by user, incidents by address and incidents by protocol.
- Click the '+ Add New Dashboard Component' button to change which tiles are shown on the dashboard.



- The dashboard is displayed by default after login. Click the 'Dashboard' tab at top-left to switch to the dashboard from a different screen.

**To chose time intervals**

- Click the interval selection button as shown in the screenshot below.
- Select your desired time period:



Statistics for the chosen interval will be displayed.

The dashboard can display the following types of tiles:

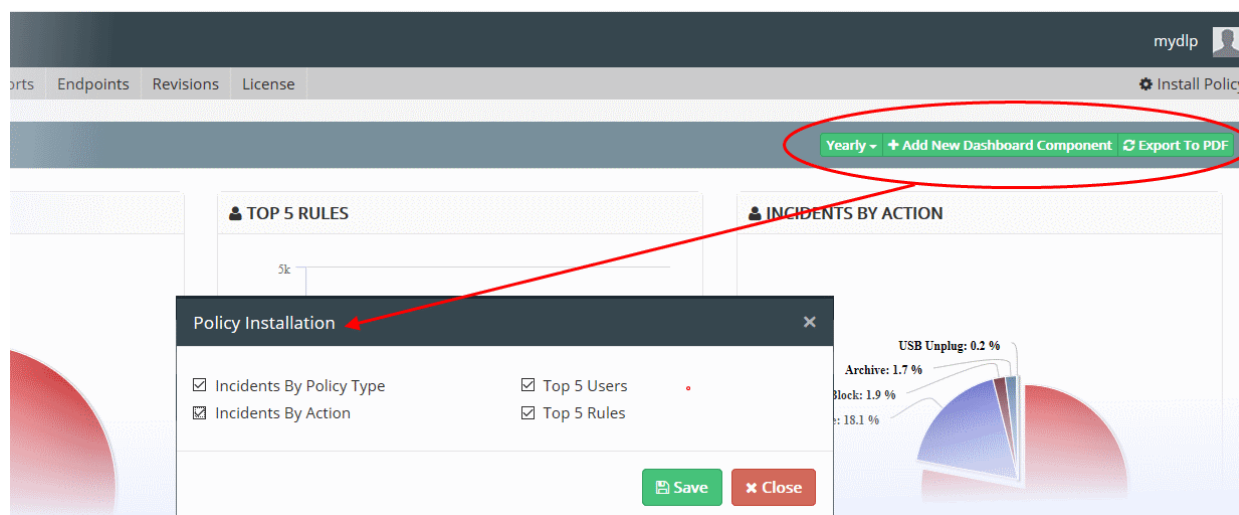
Tile	Description
Incidents by Policy Type	Shows the quantity of events triggered by various policy types.
Top 5 Rules	Shows the top 5 rules responsible for intercepting or discovering the most data during the last day / week / month / year.
Incidents by Actions	Shows incidents according to the type of action that generated the event.
Top 5 Users	Shows the 5 users from whom most data was intercepted or discovered, versus the total amount of data intercepted or discovered by all users.

**Configure the Dashboard**

By default, the dashboard shows all charts. Administrators can add or remove charts as per their requirements.

**To add or remove a tile**

- Click 'Add New Dashboard Component'



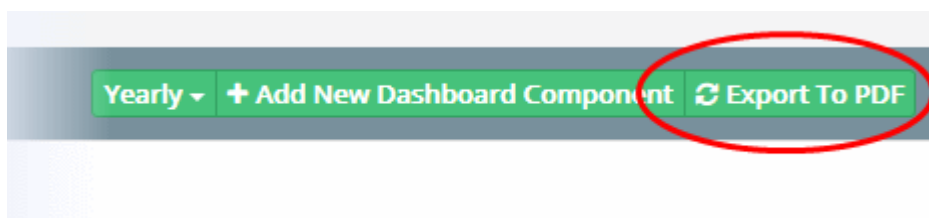
The Policy Installation dialog will appear, with the list of available tiles. The tiles existing on the dashboard are pre-selected.

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

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

#### Download the dashboard as a PDF

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



The report will be saved to your default download location.

## 4. Data Control and Data Transfer Policies

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

#### Data Transfer Policy ('General Policy')

- CDDP applies a 'Policy' to define the data control scheme for endpoints in your network.
- A policy is constructed from a series of rules. These govern restrictions on data traveling over the web, over email, and to/from removable storage.
- You can also set rules to prevent screenshots being taken when certain applications are running, and rules to prevent specific documents from being printed. See '[Add a Data Transfer Rule](#)' for more details.

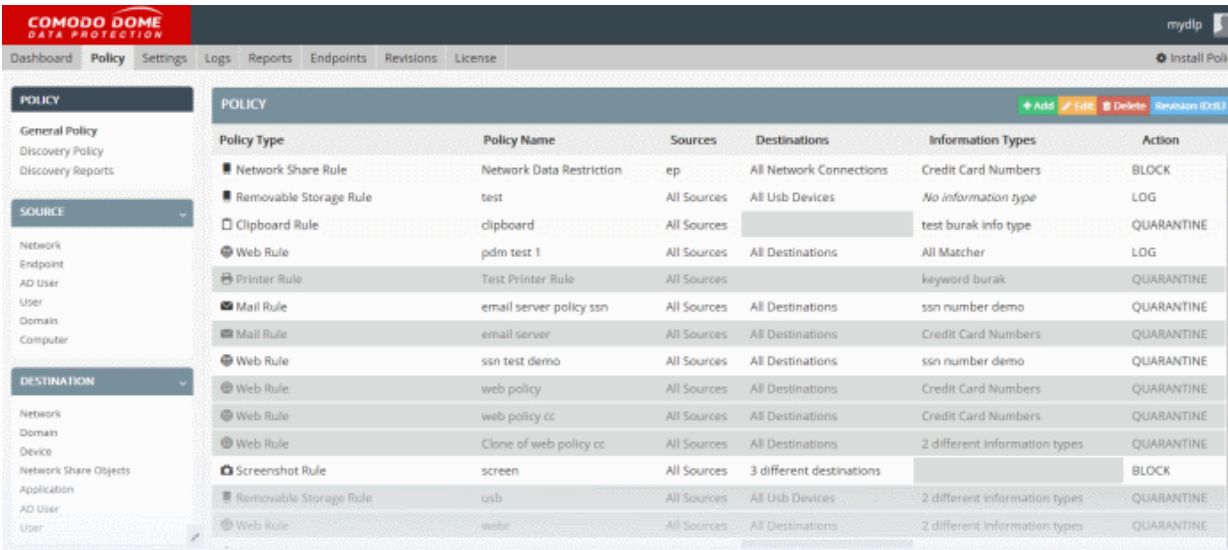
#### Data Discovery ('Discovery Policy')

- CDDP can run scheduled scans on endpoints, remote servers and databases to locate files containing sensitive information.

- 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 which contain sensitive information.
- Discovery reports can be viewed from the 'Discovery' interface. See '[Add a Data Discovery Rule](#)' for more information.

**Tip:** You can click on  collapse button to reveal or hide the left hand pane of the policy interface.

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



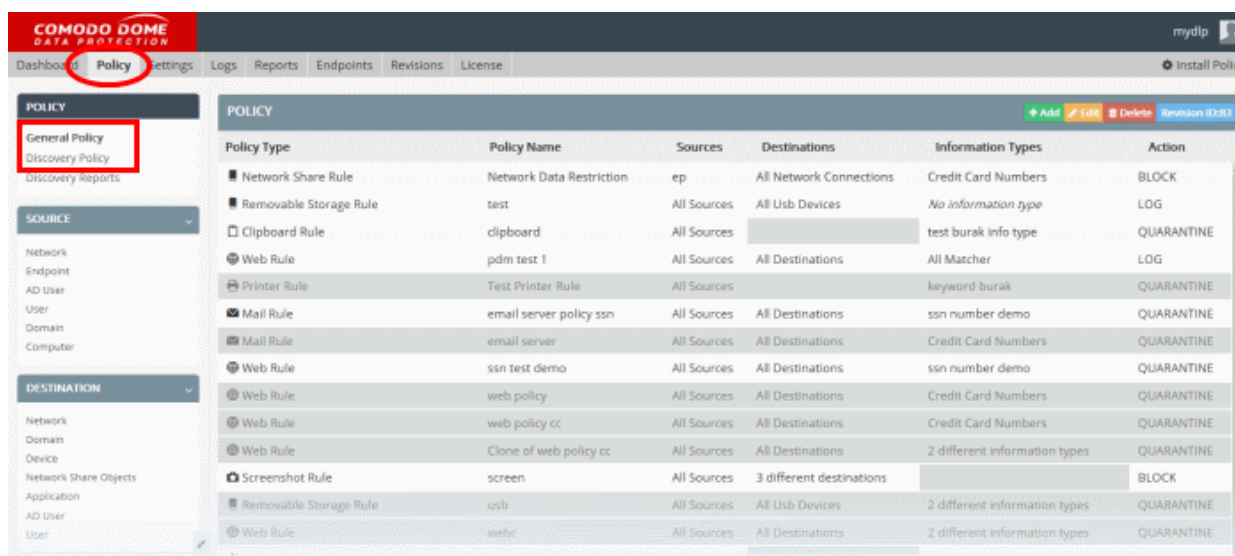
Policy Type	Policy Name	Sources	Destinations	Information Types	Action
Network Share Rule	Network Data Restriction	ep	All Network Connections	Credit Card Numbers	BLOCK
Removable Storage Rule	test	All Sources	All Usb Devices	No information type	LOG
Clipboard Rule	clipboard	All Sources		test burak info type	QUARANTINE
Web Rule	pdm test 1	All Sources	All Destinations	All Matcher	LOG
Printer Rule	Test Printer Rule	All Sources		keyword burak	QUARANTINE
Mail Rule	email server policy ssn	All Sources	All Destinations	ssn number demo	QUARANTINE
Mail Rule	email server	All Sources	All Destinations	Credit Card Numbers	QUARANTINE
Web Rule	ssn test demo	All Sources	All Destinations	ssn number demo	QUARANTINE
Web Rule	web policy	All Sources	All Destinations	Credit Card Numbers	QUARANTINE
Web Rule	web policy cc	All Sources	All Destinations	Credit Card Numbers	QUARANTINE
Web Rule	Clone of web policy cc	All Sources	All Destinations	2 different information types	QUARANTINE
Screenshot Rule	screen	All Sources	3 different destinations		BLOCK
Removable Storage Rule	usb	All Sources	All Usb Devices	2 different information types	QUARANTINE
Web Rule	webr	All Sources	All Destinations	2 different information types	QUARANTINE

The following sections contain more details on rules:



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

## 4.1. The Rules Interface

- 'Data transfer' rules are listed under 'Policy' > 'General Policy'
- 'Data discovery' rules are listed under 'Policy' > 'Discovery Policy'



- Both rule types have four common components - 'Sources', 'Destinations', 'Information Types' and 'Actions'.
  - Data transfer rules also have a 'Channel' rule component
  - Discovery rules have additional 'Discovery Type' and 'Schedule' components.
- Rules at the top of the table have a higher priority than those at the bottom. In the event of a conflict, CDDP will apply the setting in the rule nearer the top of the table.

Rules Table - Description of Columns	
Rule Component	Description
Channel	<p>Type of rule. You select the rule 'type' then choose a rule name as the first steps when creating a new rule. Example data transfer 'channels' include 'Web Rule', 'Removable Storage Rule', 'Screenshot Rule' and 'CD-DVD rule'. The rule 'channel' is easily identified by the icon to the left of your rule name in the table.</p> <div>  Web Rule         </div>
Discovery Type	<p>(Discovery rules only). Discovery types include 'Endpoint Discovery Rule', 'Remote Storage Rule' and 'Database Discovery Rule'. The rule type is easily identified by the icon to the left of rule name in the table.</p> <div>  Endpoint Discovery         </div>
Name / Policy Name	The name of the rule that was provided in the rule wizard.
Schedule	<p>(Discovery rules only). Allows administrators to set and view the schedule of the rule.</p> <p>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.</p>



Source	<p>Determines what user, user groups or locations should be covered by the rule.</p> <ul style="list-style-type: none"> <li>User / user group sources can be an IP address, network, computer, active directory element or email address (depending on the rule type).</li> <li>Location sources can be a network, computer or remote storage. Location sources are for discovery rules.</li> </ul>
Destinations	<p>'Destination' can be a domain, directory or application, depending on the rule type.</p> <p>Destination is not required for the following rule types: removable storage, removable storage inbound, printer, API, remote storage.</p>
Information Types	<p>The type of data that needs to be discovered or monitored.</p> <p>DDP provides many preset information types which you can slot into your rules. You can also define your own custom information types.</p> <p>The 'Information type' column is not required for <b>removable storage inbound</b> and <b>screenshot</b> rules.</p>
Action	<p>The response that DDP should take when all rule conditions are met. Available actions are:</p> <ul style="list-style-type: none"> <li>Pass</li> <li>Block</li> <li>Log</li> <li>Quarantine</li> <li>Archive</li> <li>Delete</li> </ul> <p><b>Note:</b> The 'Delete' action is available only for discovery rules. When 'delete' or 'quarantine' is chosen as the action in an endpoint discovery policy, matched items will be removed from the computer.</p>

The following sections contain more details on rules:

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



### 4.1.1. Rule Channels / Types

- CDDP has different categories of rules which are known as 'Rule Types'.
- Rule types are classified according to data inspection channel. Example channels include web, mail, and removable storage.
- Each rule type is only effective on data traversing through, or residing in, the named channel.
- Rule types form 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 **Web rules** for more details.



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



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



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



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



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



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



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



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



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



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



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



**Network Share Rules** are used to control data traffic in all network connections defined in the rule. See **Network Share Rules** to find out more.

### Discovery Rule Type



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



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



**Database Discovery rules** are used to locate files containing specific data types in network databases. For example, credit card numbers, social security numbers or other sensitive information.

### 4.1.2. Rule Actions

- **Pass** - Allows information to travel through the data channel freely without generating log entries. This action is available for all rule types.
- **Log** - Creates a log entry when data passes through the data channel. This action is not available for the screenshot and floppy rules.
- **Archive** - Allows information to pass through the data channel, generates an event log and archives a copy of the information. Administrators can download the file from the 'Logs' interface. See **Download the Files Archived by CDDP** for more details. This action is not available for the screenshot, USB Device Access, CD-DVD and Floppy rules.
- **Block** - Prevents information from passing through the data channel and generates an event log. This action is not available for the removable storage inbound rules.
- **Quarantine** - Prevents information from passing through, generates an event log and archives a copy of the information. This action is not available for the removable storage inbound, screenshot, USB Device Access rule, CD-DVD rule and Floppy rules.
  - When this action is applied with an 'Endpoint discovery' rule, all files that match the information type specified in the rule will be deleted from the endpoint - but a copy of the files will be archived in the Comodo Dome Data Protection server. Administrators can download the file from the 'Logs' interface. See **Download the Files Archived by CDDP** for more details. The action is similar to applying the 'Delete' action on an 'Endpoint discovery rule', with the difference that a copy of the matching files will be saved.
- **Encrypt** (only available for 'Removable Storage Encryption Rule'). Detects any new USB storage device connected to source endpoints, formats the device and encrypts it. After encryption, any data stored on the device can only be read if it is connected to your network and not by any other network. This prevents, for example, any guest or hostile from plugging in a USB drive, downloading data and taking it out of the network.
- **Delete** (only available for 'Discovery' rules). Deletes discovered files which match your criteria. It is advised to use this action very carefully.

### 4.1.3. Email Notifications and Messages for a Rule

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

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

- Notifications can be customized from **Settings > Enterprise > Email Notification Message**

General Rule Edit

Name

Block Credit Card Numbers

Type

Web Rule

Description

To block uploading documents containing credit card numbers to websites

Message to User

You cannot upload sensitive documents

☒ Enable Notifications

User Name	E-mail
✓ mydlp	user@mydlp.com
dlp_ent@yopmail.com	dlp_ent@yopmail.com
✓ johnsmith	

✕ Cancel

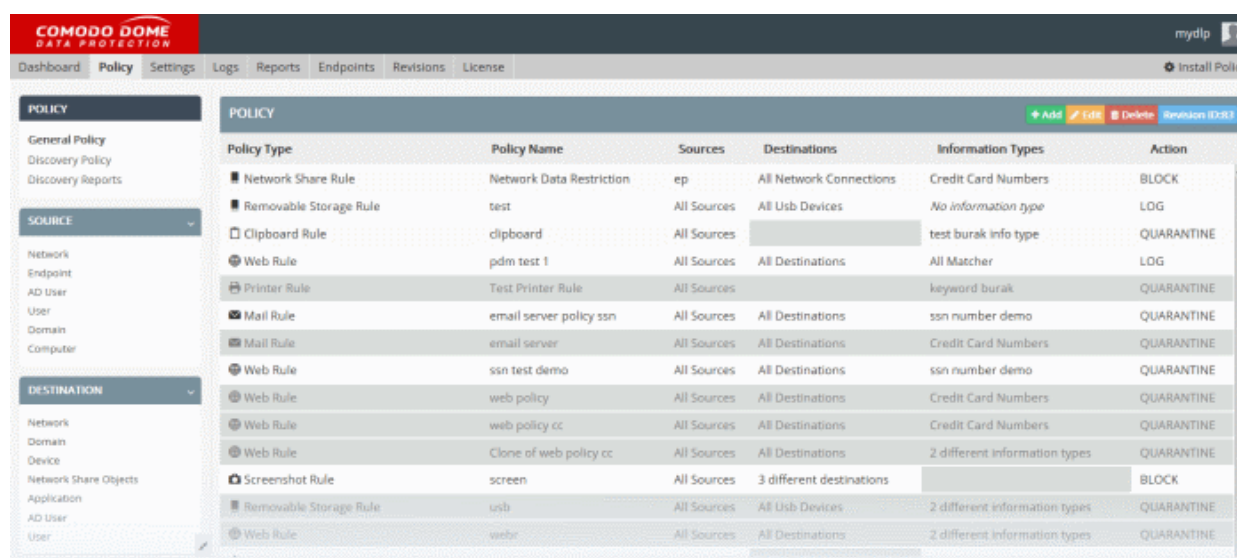
← Back

Next →

#### 4.1.4. Add a Data Transfer Rule

- Data transfer policies allow you to enforce traffic control schemes for endpoints in your network.
- You can create several rules in a policy. Each rule is designed to monitor a specific type of data traveling between a source and destination of your choice.
- You can assign actions to be taken if a rule is triggered. Actions include allow, block, quarantine, log, and encrypt. You can also block the use of USB storage devices with specific endpoints, forbid screenshots for specific applications, and prohibit printing of sensitive documents.

The 'General Policy' interface shows all rules that have been added to the data transfer policy:



Use this interface to add new rules, edit existing rules and remove unwanted rules. See [The Rules Interface](#) for more help with this area.

The following sections explain how to construct rules for a policy and deploy them to a network:

- [Add a Data Transfer Rule](#)
- [Enable or Disable a Rule](#)
- [Edit a Rule](#)
- [Remove a Rule](#)

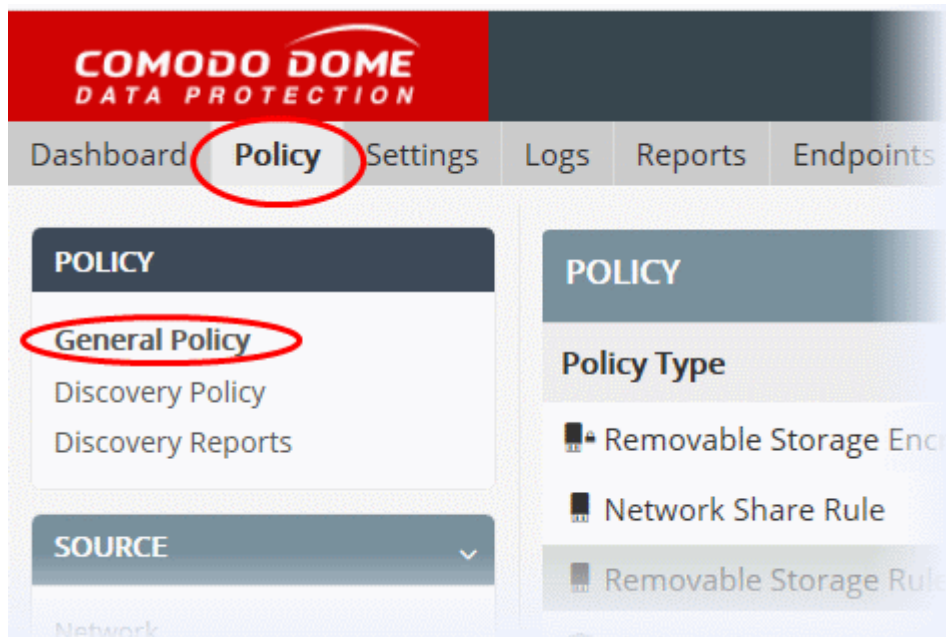
### Add a Data Transfer Rule

Rules can be created using the wizard and added to a policy:

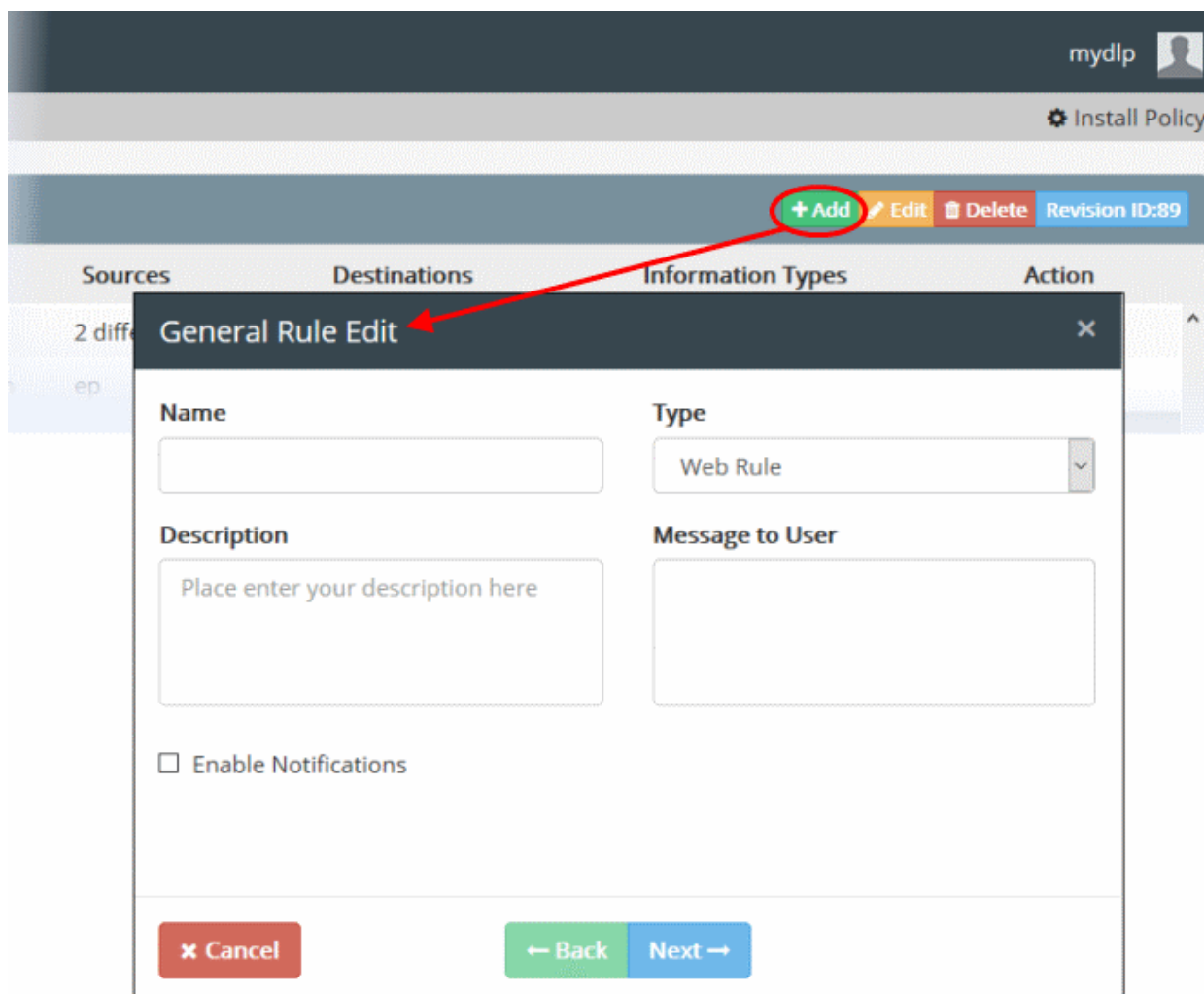
- [Step 1 - Add new rule and select the rule type](#)
- [Step 2 - Create a name for the rule / Configure messages and notifications](#)
- [Step 3 - Specify the sources for the rule](#)
- [Step 4 - Specify the destinations for the rule](#)
- [Step 5 - Specify the types of information you want to capture in the rule](#)
- [Step 6 - Specify the action that is taken if the rule conditions are met](#)

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

- Click the 'Policy' tab > 'Policy' > 'General Policy'



- Click the 'Add' button from to create a new rule:



The screenshot shows the Comodo Dome Data Protection Administrator interface. At the top right, there is a user profile icon labeled 'mydlp' and an 'Install Policy' button. Below this, a navigation bar contains buttons for '+ Add', 'Edit', 'Delete', and 'Revision ID:89'. The main interface has tabs for 'Sources', 'Destinations', 'Information Types', and 'Action'. A 'General Rule Edit' dialog box is open, featuring a title bar with a close button. The dialog box contains the following fields:

- Name:** A text input field.
- Type:** A dropdown menu currently set to 'Web Rule'.
- Description:** A text area with the placeholder text 'Place enter your description here'.
- Message to User:** A text area.
- Enable Notifications:** A checkbox.

At the bottom of the dialog box, there are three buttons: 'Cancel', 'Back', and 'Next'.

- **Type:** Choose the type of rule you want to create. All full explanation each rule type can be found in [Rule Channels / Types](#).

General Rule Edit

Name

Description

Place enter your description here

Type

Web Rule

Web Rule

Mail Rule

Removable Storage Rule

Network Share Rule

Removable Storage Inbound Rule

Removable Storage Encryption Rule

Screenshot Rule

Printer Rule

Api Rule

USB Device Access

CD-DVD Rule

Floppy Rule

Clipboard Rule

**Step 2 – Create a name for the rule and configure messages and notifications**

General Rule Edit

Name

Docs Uploading

Type

Web Rule

Description

documents containing confidential information like credit card numbers, to selected websites

Message to User

The document you are attempting to upload contains sensitive information. The operation is blocked.

☐ Enable Notifications

Cancel

Back

Next



Enter the following information:

- **Name** - Create a label for the rule that will help you easily identify its purpose.
- **Description** – Provide a short description if required.
- **Message to User** – This is shown on endpoints when CDDP blocks or quarantines traffic based on this rule.

CDDP displays messages for the following rule types:

- Web Rule
- Mail Rule
- Network Share Rule

The message is only shown if the rule action is 'block' or 'quarantine'.

- **Notifications** – Alerts which are sent to admins and other users when the rule intercepts target data.
  - The content of the notification can be edited in 'Settings' > 'Enterprise'. See **Configure Enterprise Settings** for more details.
  - Notifications are only available for the following rule types:
    - Web Rule
    - Mail Rule
  - Select 'Enable Notifications' if you want to receive these alerts
  - Select the alert recipients and click 'Next'

User Name	E-mail
✓ mydlp	user@mydlp.com
dlp_ent@yopmail.com	dlp_ent@yopmail.com
✓ johnsmith	johnsmith@yopmail.com

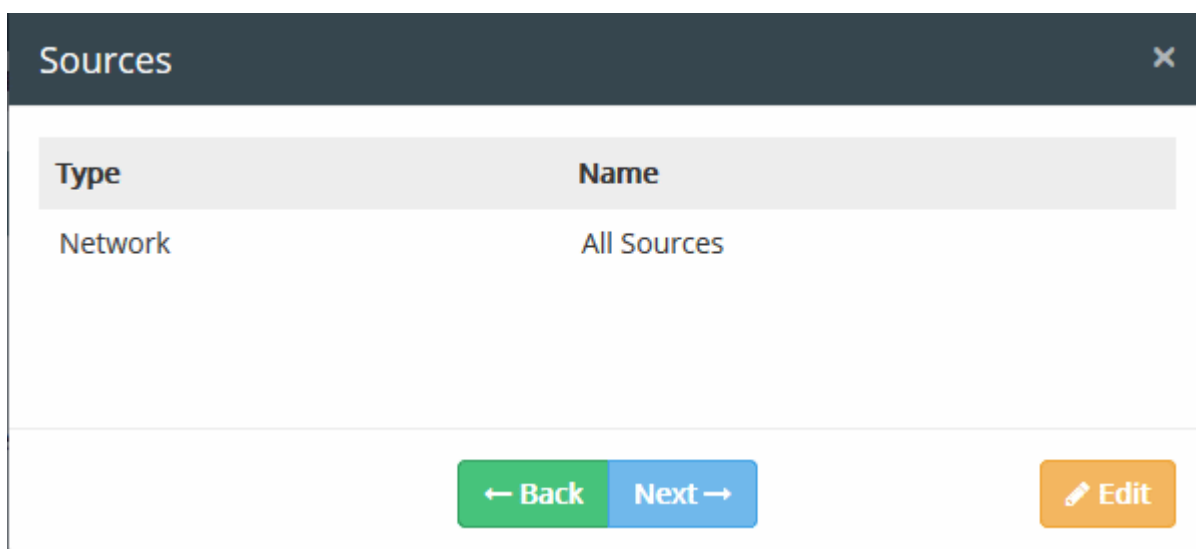
### Step 3- Specify the sources for the rule

- A source is the origin of the data you want to inspect.
- Example source types include 'endpoint', 'network', 'active directory' and 'user'.
- You can then pick specific objects within the source type.
  - The default type is 'Network' and default source object is 'All Sources'.
- You can change the source type and objects by clicking the 'Edit' button at lower right.

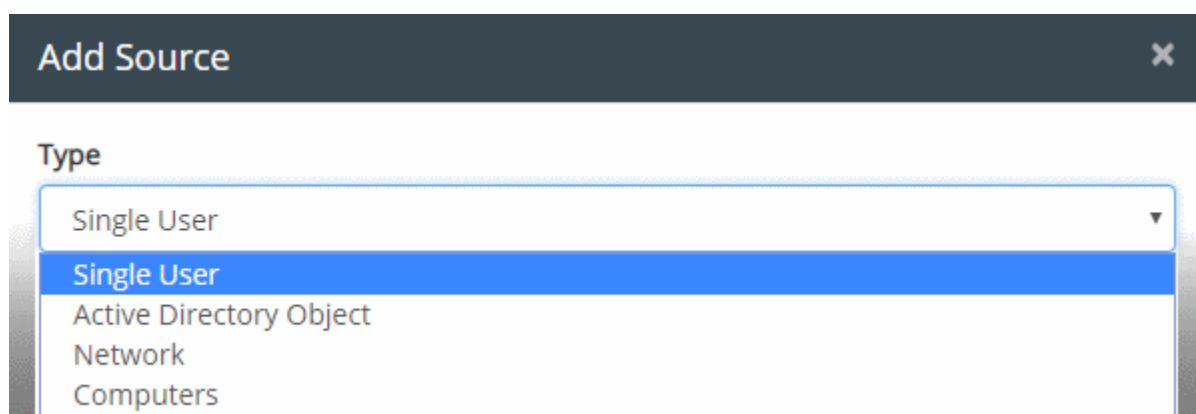
#### To add a source object

- Click the 'Next' button after completing step 2 to open the source configuration screen:





- Click the 'Edit' button
- Select the source type from the drop-down:



The objects you can select varies according to source type. See [User Defined Objects](#) for more details. For example, if you choose 'Network' you will see a list of IP addresses and sub-nets:

Add Source

Type

Network

Name	IP Address	Subnet
✓ All Sources	0.0.0.0	0.0.0.0
10.0.0.0/24	10.0.0.0	255.255.255.0
10.0.0.0/8	10.0.0.0	255.0.0.0
192.168.0.0/16	192.168.0.0	255.255.0.0
172.16.0.0/16	172.16.0.0	255.255.0.0

+ Add

- Select the objects you require from the list then click 'Add'.
- You can add multiple source types to each rule. Simply select another object type from the 'Type' drop-down and repeat the procedure explained above.

Sources

Type	Name
Network	172.16.0.0/16
Single User	Bob Smith

← Back
Next →
Edit

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

The following table shows which information types can be used in each type of rule:

Source Type	Applicable Rule Types
Network	<ul style="list-style-type: none"> <li>• Web Rule</li> </ul>

Source Type	Applicable Rule Types
	<ul style="list-style-type: none"> <li>• Mail Rule</li> <li>• Removable Storage Rule</li> <li>• Network Share Rule</li> <li>• Removable Storage Inbound Rule</li> <li>• Removable Storage Encryption Rule</li> <li>• Printer Rule</li> <li>• Screenshot Rule</li> <li>• API Rule</li> <li>• USB Device Access Rule</li> <li>• CD-DVD Rule</li> <li>• Floppy Rule</li> <li>• Clipboard Rule</li> </ul>
Computers	<ul style="list-style-type: none"> <li>• Web Rule</li> <li>• Removable Storage Rule</li> <li>• Network Share Rule</li> <li>• Removable Storage Inbound Rule</li> <li>• Removable Storage Encryption Rule</li> <li>• Printer Rule</li> <li>• Screenshot Rule</li> <li>• API Rule</li> <li>• USB Device Access Rule</li> <li>• CD-DVD Rule</li> <li>• Floppy Rule</li> <li>• Clipboard Rule</li> </ul>
Domain	<ul style="list-style-type: none"> <li>• Mail Rule</li> </ul>
User Object	<ul style="list-style-type: none"> <li>• Web Rule</li> <li>• Mail Rule</li> <li>• Removable Storage Rule</li> <li>• Network Share Rule</li> <li>• Removable Storage Inbound Rule</li> <li>• Removable Storage Encryption Rule</li> <li>• Printer Rule</li> <li>• Screenshot Rule</li> <li>• API Rule</li> <li>• USB Device Access Rule</li> </ul>

Source Type	Applicable Rule Types
	<ul style="list-style-type: none"> <li>• CD-DVD Rule</li> <li>• Floppy Rule</li> <li>• Clipboard Rule</li> </ul>
AD User Object	<ul style="list-style-type: none"> <li>• Web Rule</li> <li>• Mail Rule</li> <li>• Removable Storage Rule</li> <li>• Network Share Rule</li> <li>• Removable Storage Inbound Rule</li> <li>• Removable Storage Encryption Rule</li> <li>• Screenshot Rule</li> <li>• Printer Rule</li> <li>• API Rule</li> <li>• USB Device Access Rule</li> <li>• CD-DVD Rule</li> <li>• Floppy Rule</li> <li>• Clipboard Rule</li> </ul>
Device	<ul style="list-style-type: none"> <li>• Removable Storage Rule</li> </ul>
Endpoints File Systems	<ul style="list-style-type: none"> <li>• Endpoint discovery Rule</li> </ul>
Remote Connections	<ul style="list-style-type: none"> <li>• Remote Storage Rule</li> </ul>
Database Connection	<ul style="list-style-type: none"> <li>• Database Discovery Rule</li> </ul>

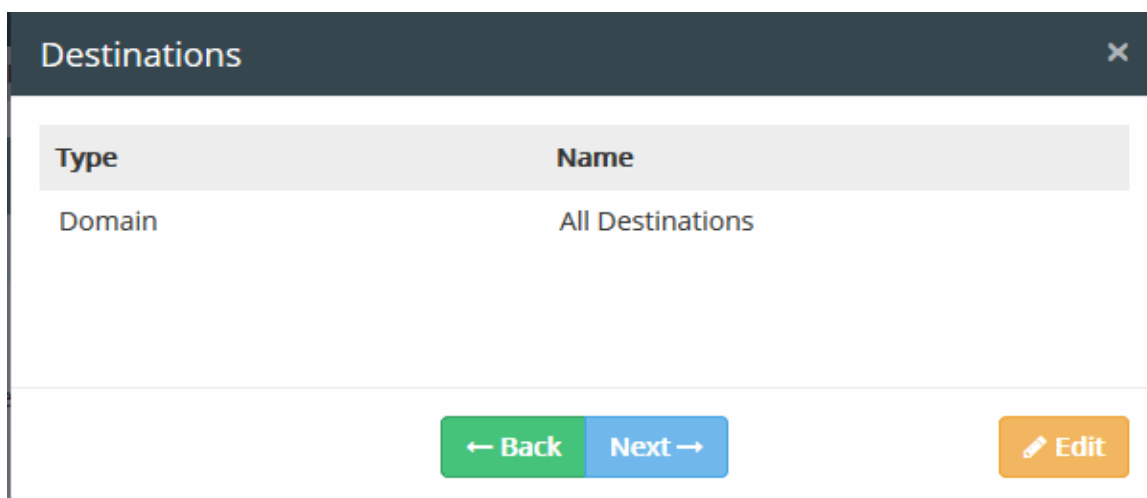
#### Step 4 - Specify the destinations for the rule

- A destination object is the target of the rule. Example destinations include applications, domains, devices and users.
- The following table shows which destination types can be used in which rules:

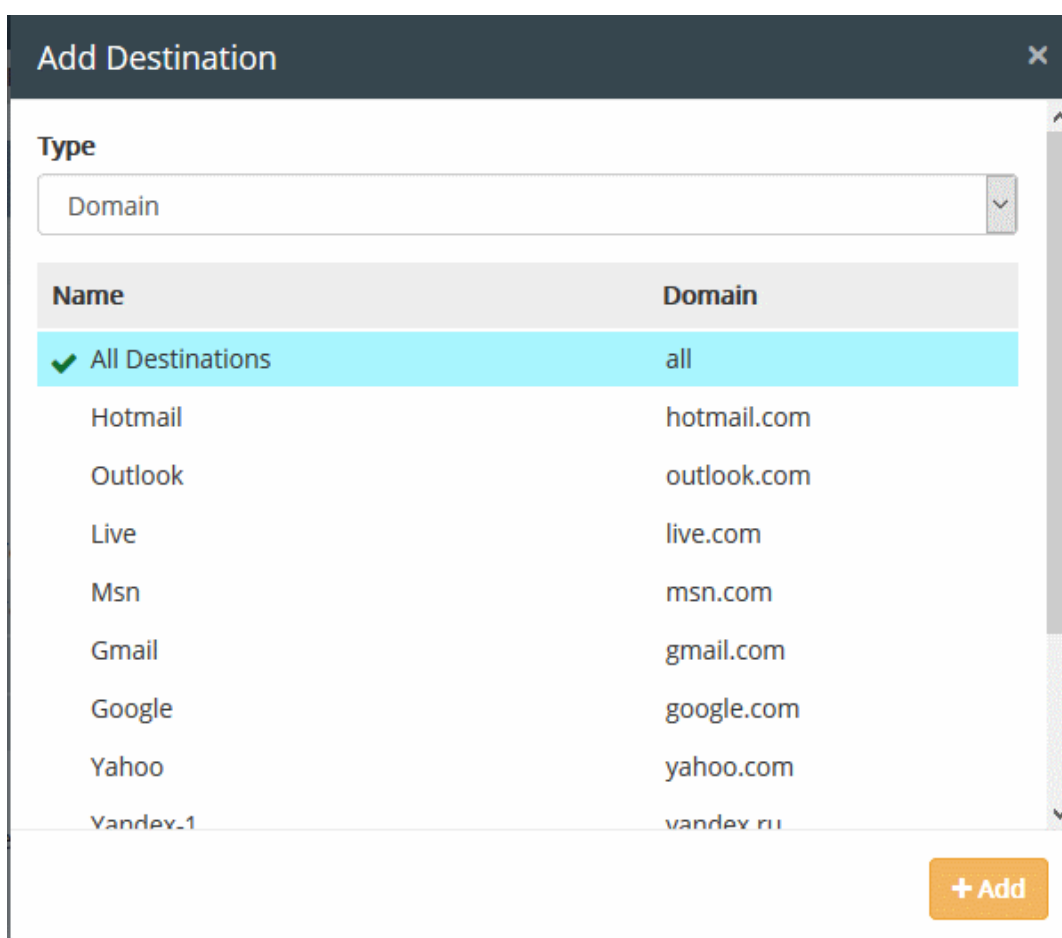
Destination Type	Applicable Rule Types
Domain	<ul style="list-style-type: none"> <li>• Web Rule</li> <li>• Mail Rule</li> </ul>
Application Name	<ul style="list-style-type: none"> <li>• Screenshot Rule</li> </ul>
Device	<ul style="list-style-type: none"> <li>• Removable Storage Rule</li> </ul>
User Object	<ul style="list-style-type: none"> <li>• Mail Rule</li> </ul>
AD User Object	<ul style="list-style-type: none"> <li>• Mail Rule</li> </ul>

#### To add a destination object

- Click the 'Next' button after choosing your source in the previous step.
- Click the 'Edit' button in the 'Destinations' dialog:



The objects you can select varies according to destination type. See [User Defined Objects](#) for more details. For example, if you choose 'Domains' you can select from a list of websites:



- Select the objects you require from the list then click 'Add'.
- You can add multiple destination types to each rule. Simply select another type from the drop-down and repeat the procedure explained above.

Destinations
×

Type	Name
Domain	Hotmail
Domain	Outlook
Domain	Live
Domain	Gmail
Domain	Google
Domain	Yahoo
Domain	Facebook

← Back
Next →
Edit

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

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

An 'Information Type' is the kind of data which you wish to search for in scanned locations. For example, credit card numbers, social security numbers and so on.

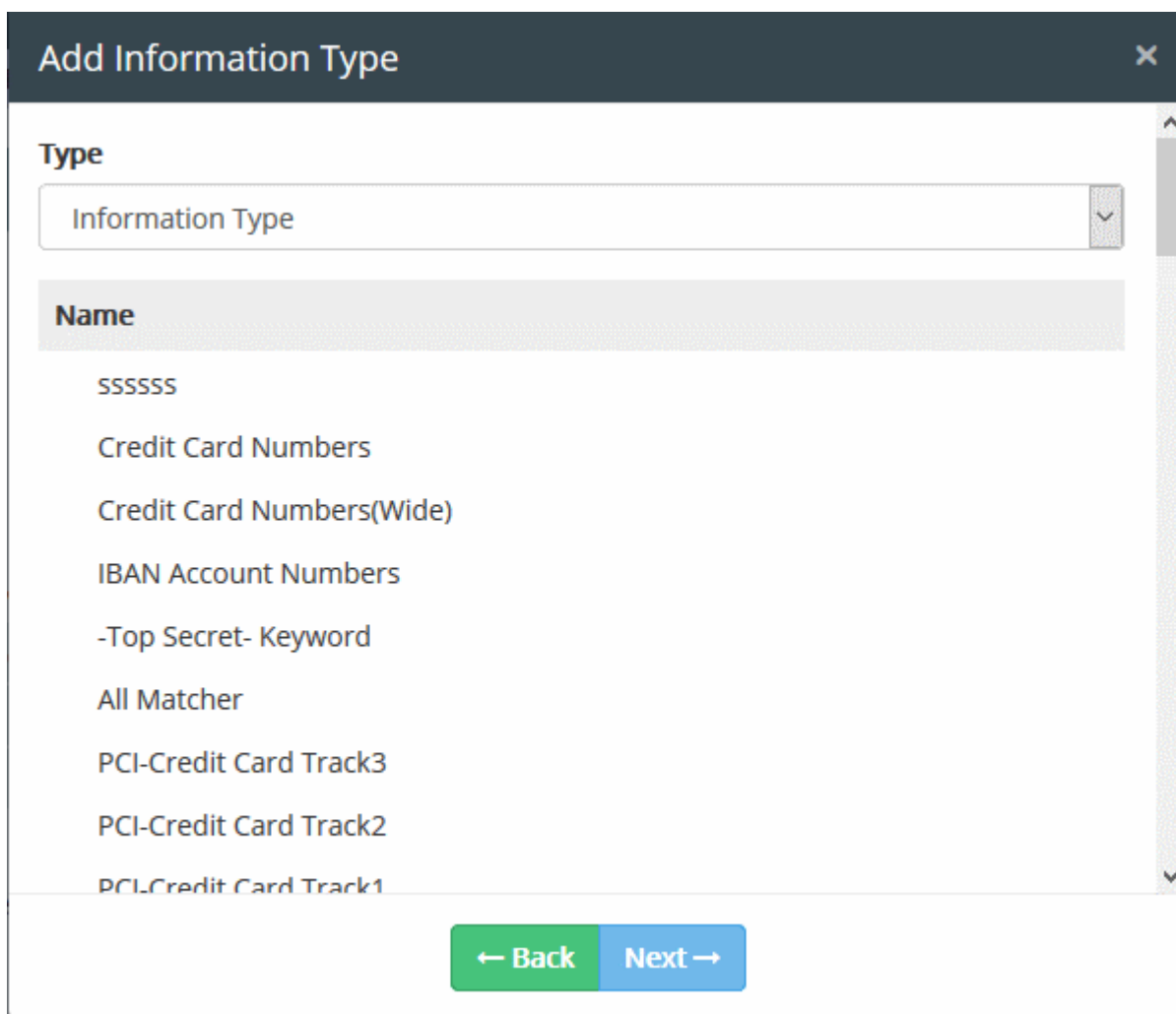
- For CDDP to intercept files containing data of a specific type, an 'Information Type' object needs to be added to the rule.
- CDDP ships with a number of commonly used 'Information Types' and 'Information Type Groups'.
- Each group contains a set of predefined information types that pertain to a category. Information types and groups are available under the 'Information Type' tree on the left.
- Administrators can also add custom information types and groups.

For more details on information types, refer to [Information Types - An Overview](#).

Object	Applicable Rule Types
Information Type	<ul style="list-style-type: none"> <li>Web Rule</li> <li>Mail Rule</li> <li>Removable Storage Rule</li> <li>Printer Rule</li> <li>API Rule</li> <li>Clipboard Rule</li> <li>Network Share Rule</li> </ul>

### To add an Information Type object

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



**Add Information Type**

Type

Information Type

**Name**

- SSSSSS
- Credit Card Numbers
- Credit Card Numbers(Wide)
- IBAN Account Numbers
- Top Secret- Keyword
- All Matcher
- PCI-Credit Card Track3
- PCI-Credit Card Track2
- PCI-Credit Card Track1

← Back   Next →

The 'Add Information Type' dialog will be displayed. Choose whether you want to add individual information types or information groups from the drop-down at the top:

- Choose whether you are adding Information Types or Information Type Groups from the drop-down at the top.



**Add Information Type**

Type

Information Type

Information Type

Information Type Group

← Back   Next →

- Select your information type(s) from the list.
- The types available depend on the predefined and user defined objects created for it. If you wish to define a custom type, see '[Add a User Defined Information Type](#)' and '[Add a User Defined Information Type Group](#)'.
- To add more objects choose 'Information Type' or 'Information Type Group' from the drop-down at the top

and repeat the procedure.

- Click 'Next' to specify the action for the rule

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

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

- Choose the action from options. The available actions are:
  - **PASS** - Allows information to move freely without generating a log entry. This action is the default action and available for all rule types.
  - **BLOCK** - Prevents the information from moving and generates an event log. This action is not available for removable storage inbound rules.
  - **LOG** - Creates a log entry when data moves. This action is not available for screenshot rule and Floppy rule.
  - **QUARANTINE** - Prevents information from moving, generates an event log and archives a copy of the information on the CDDP Server. Administrators can download the quarantined file from the 'Logs' interface. See [Download the Files Archived by CDDP](#) for more details. This action is not available for removable storage inbound rule, screenshot rule, USB Device Access rule, CD-DVD rule and Floppy rule.
  - **ARCHIVE** - Allows information to pass, generates event log and creates an archive copy. Administrators can download the archived file from the 'Logs' interface. See [Download the Files Archived by CDDP](#) for more details. This action is not available for screenshot rule, USB Device Access rule, CD-DVD rule and Floppy rule.
  - **ENCRYPT** - Enforces encryption of connected removable devices. This action is only available for Removable Storage Encryption Rule.
- At any time during the rule creation, click 'Back' to review your configuration for the rule
- Click 'Save'

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

The rules take effect only on applying/reapplying the policy to the network. See [Deploy the Policy](#) for more details.






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

- Click on the rule to view the control buttons:



POLICY					
<a href="#">+ Add</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Revision ID:89</a>					
Policy Type	Policy Name	Sources	Destinations	Information Types	Action
 	TEST policy	All Sources	All Destinations	Strategic Business Documents	QUARANTINE

Expanded details of the rule are displayed under the 'Source', 'Destination' and 'Information Type' columns.


Control	Description
	Create a new rule
	Edit the name, message and notification settings of the rule. Refer to the section <a href="#">Editing a Rule</a> for more details.
	Removes the rule from the policy. Refer to the section <a href="#">Removing a Rule</a> for more details
	Available in an expanded rule. Clones the rule to allow administrators to create a new rule with minor changes in the components
	Available in an expanded rule. Enables the administrator to disable or enable the rule. Refer to the section <a href="#">Enabling or Disabling a rule</a> for more details.

Rules at the top of the table have a higher priority than those at the bottom. In the event of a conflict between rules, the setting in the rule nearer the top of the table will be applied. Administrators can change the priority of the rules at any time by dragging a rule to a new position.

### Enabling or Disabling a Rule

Rules added to the policy are automatically enabled by default. Administrators can can disable a rule if required. Disabled rules are shown in gray in the table.

#### To disable / disable a rule

- Click on the rule for the options to be displayed in the 'Policy Type' column
- Click the disable icon 

POLICY					
<a href="#">+ Add</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Revision ID:89</a>					
Policy Type	Policy Name	Sources	Destinations	Information Types	Action
 	TEST policy	All Sources	All Destinations	Strategic Business Documents	QUARANTINE

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

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

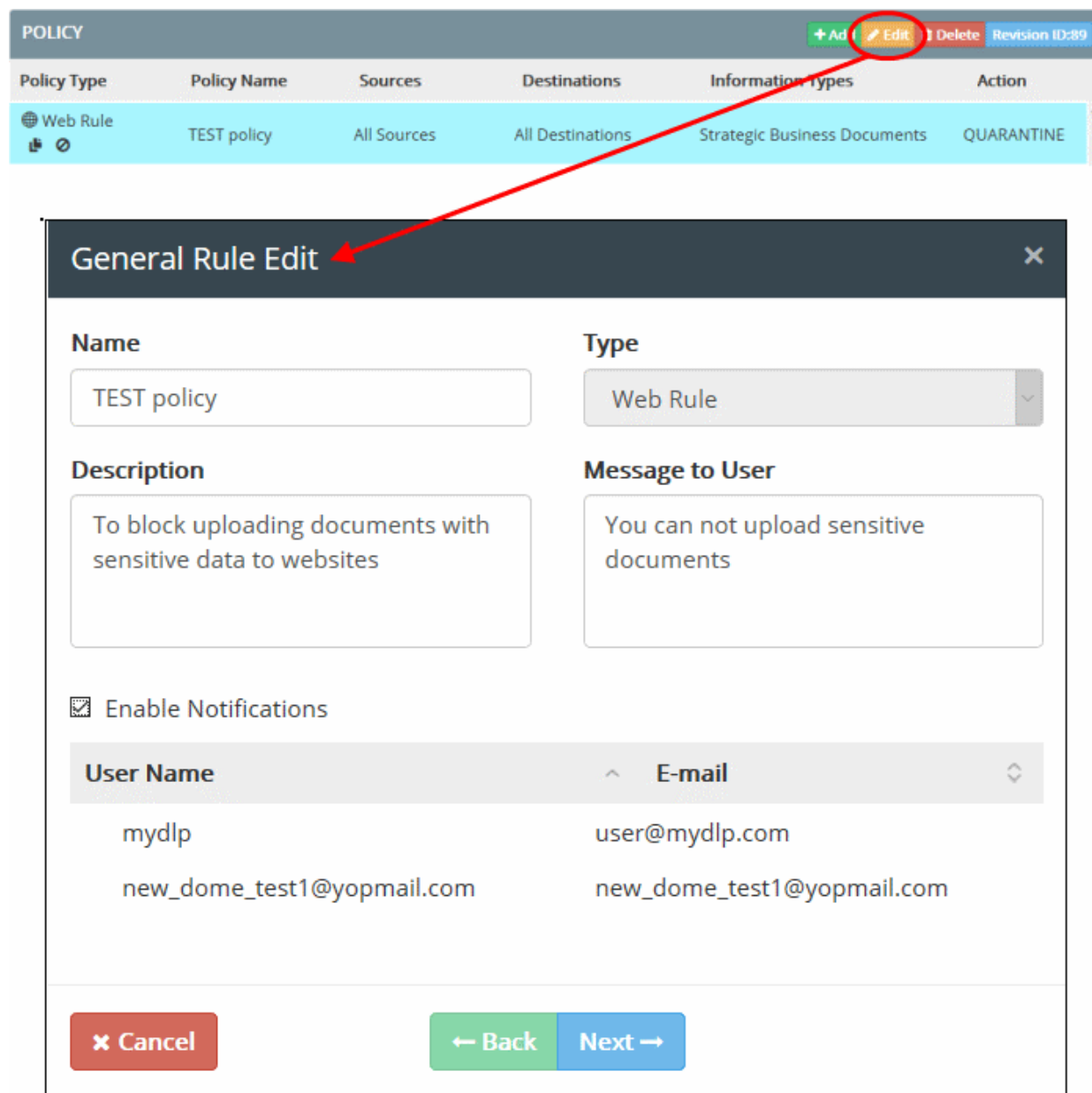
### Editing a Rule

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

Any change you make in a rule will take effect only on re-deployment of the policy. See [Deploy the Policy](#) for more details on implementing the policy.

### To edit a rule

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



The screenshot shows the 'POLICY' management interface. At the top, there are buttons for '+ Add', 'Edit' (circled in red), and 'Delete', along with 'Revision ID:89'. Below this is a table with columns: Policy Type, Policy Name, Sources, Destinations, Information Types, and Action. A row is highlighted with a light blue background, showing 'Web Rule' as the Policy Type, 'TEST policy' as the Policy Name, 'All Sources' as Sources, 'All Destinations' as Destinations, 'Strategic Business Documents' as Information Types, and 'QUARANTINE' as the Action.

A red arrow points from the 'Edit' button to the 'General Rule Edit' dialog box. The dialog box has a title bar with 'General Rule Edit' and a close button. It contains the following fields:

- Name:** A text input field containing 'TEST policy'.
- Type:** A dropdown menu showing 'Web Rule'.
- Description:** A text area containing 'To block uploading documents with sensitive data to websites'.
- Message to User:** A text area containing 'You can not upload sensitive documents'.
- ☒ **Enable Notifications**
- User Name:** A list containing 'mydlp' and 'new\_dome\_test1@yopmail.com'.
- E-mail:** A list containing 'user@mydlp.com' and 'new\_dome\_test1@yopmail.com'.

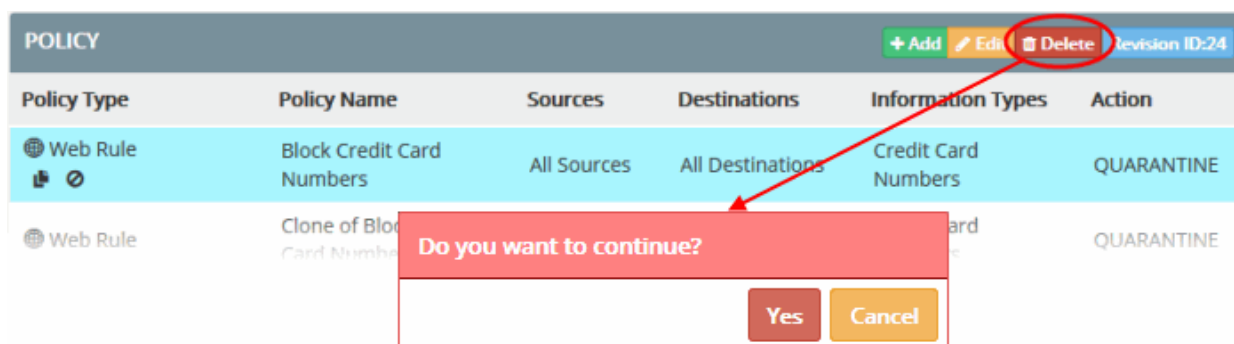
At the bottom of the dialog box are three buttons: 'Cancel' (red), 'Back' (green), and 'Next' (blue).

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

### Remove a Rule

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

A confirmation dialog will be displayed.



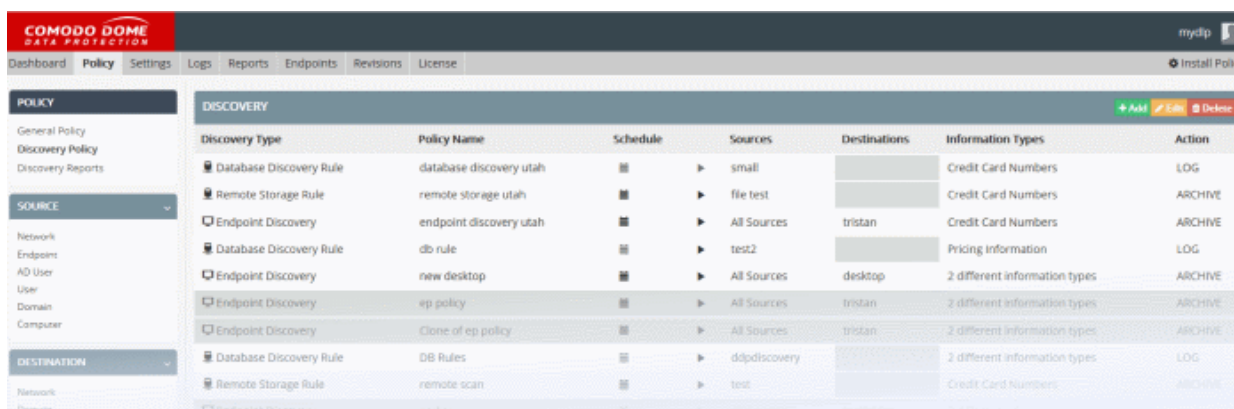
- Click 'Yes' to remove the rule.

#### 4.1.5. Add a Data Discovery Rule

- CDDP can run scheduled scans on endpoints and remote storage to discover files containing sensitive information.
- Discovery rules let you specify the targets, schedule, type of information and the actions to be taken

There are three types of discovery rules:

- **Endpoint Discovery Rule** – CDDP scans the local disks and file paths of specific Windows endpoints. The DDP agent needs to be installed.
- **Remote Storage Rule** – CDDP scans remote servers, including FTP servers, web servers and file shares. You can log or archive files which contain sensitive information.
- **Database Discovery Rule** – CDDP scans databases to find out sensitive information stored on them.



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

The following sections explain more about rule construction and implementation:

- **Adding a Data Discovery Rule**
- **Enabling or Disabling a Rule**
- **Editing a Rule**
- **Removing a Rule**
- **Running On-Demand Scans**
- **Viewing Discovery Scan Reports**

## Adding a data discovery rule

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

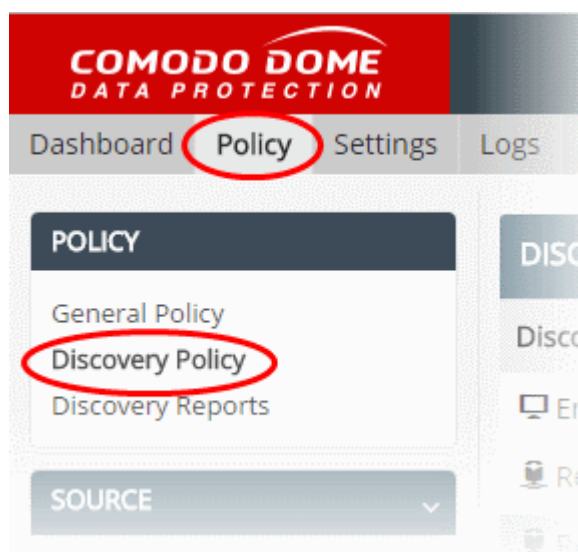
- A discovery rule is constructed from a channel, source, schedule, destination, information type and an action to be taken if the rule is triggered.
- Administrators can create unlimited rules to search targets for specific information types.
- Rules can be run 'on-demand' by clicking the ► icon next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

Rules can be created using the wizard and added to a policy. Follow these steps to add a new data discovery rule:

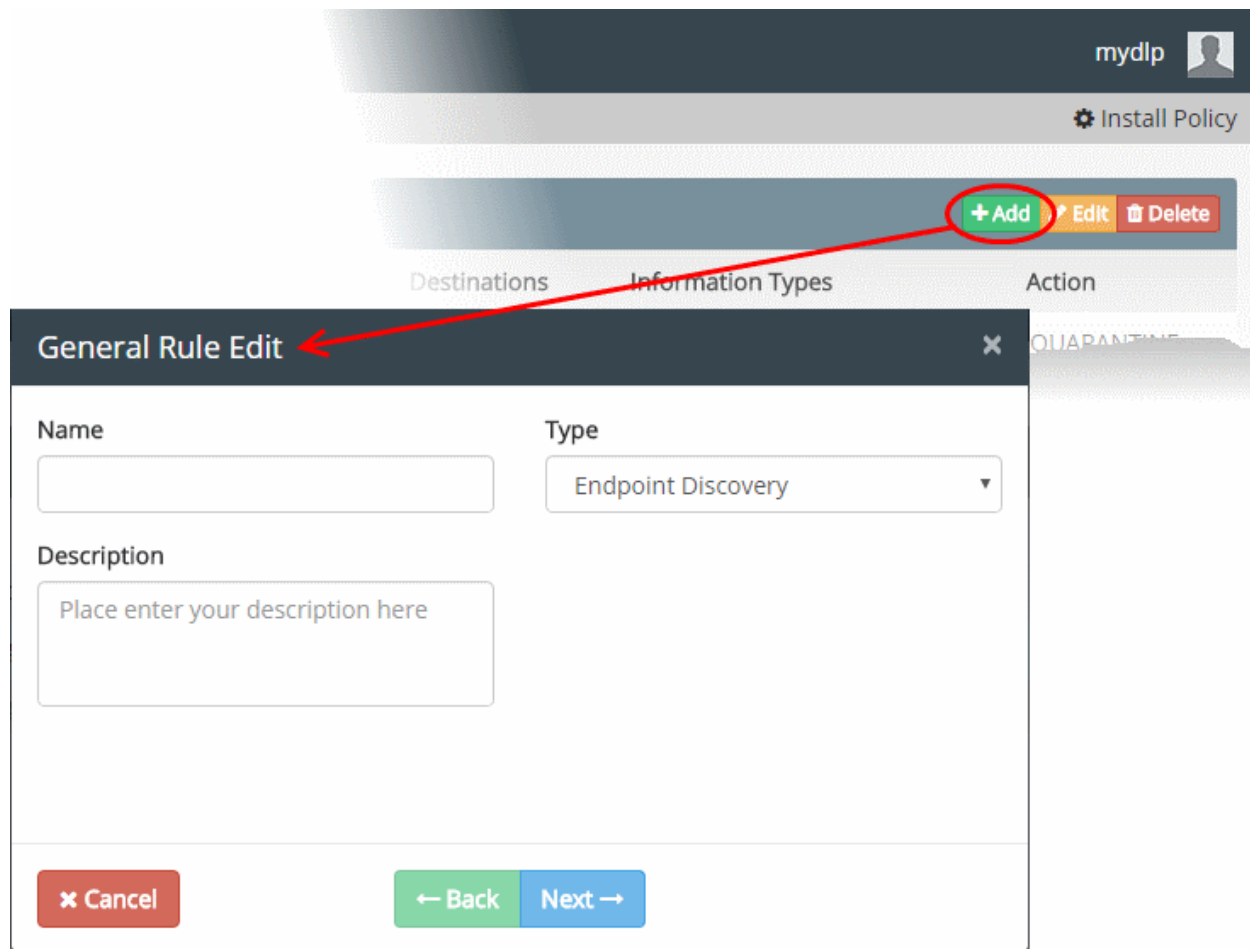
- **Step 1 - Add new rule and select the rule type**
- **Step 2 - Enter a name and description for the rule**
- **Step 3 - Specify the sources for the rule**
- **Step 4 - Specify the destinations for the rule**
- **Step 5 - Specify the 'Information Types' to be identified**
- **Step 6 - Specify the action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

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

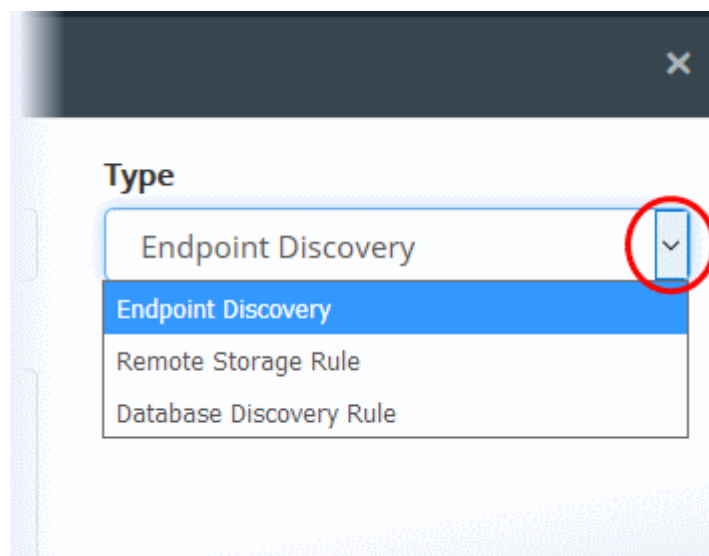
- To add a new data discovery policy rule, click the 'Policy' tab, then 'Discovery Policy' under 'Policy' on the left



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

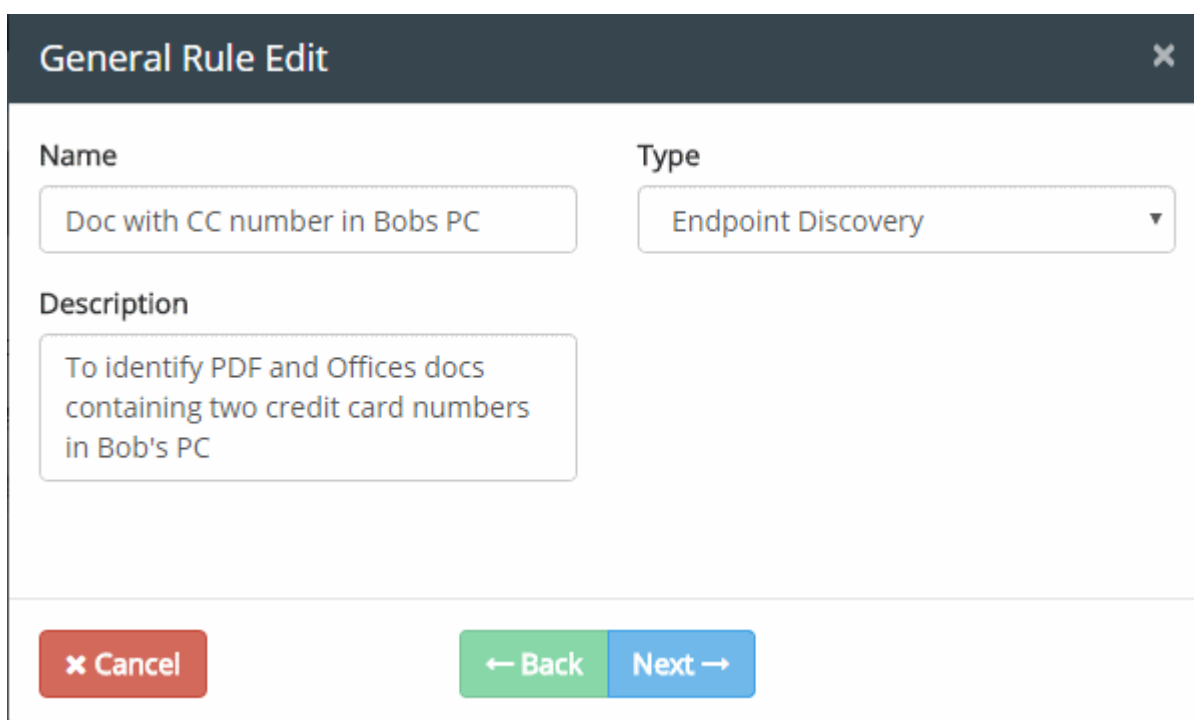


- Select the type of rule you want to create from the 'Type' drop-down ('Endpoint Discovery' or 'Remote Storage' or Database Discovery). For more details about these rule types, see [Rule Channels / Types](#).



## Step 2 – Enter a name and description for the rule

- After specifying the rule type, enter a name and description for the rule.



- Click 'Next'.

### Step 3 – Specify the sources for the rule

The 'Source' component of a rule is where you specify the location to be scanned, like selected endpoints or remote storage. For remote storage rules you can specify locations which should be skipped during scanning.

The following table shows object types that can be used as sources and the corresponding rule type:

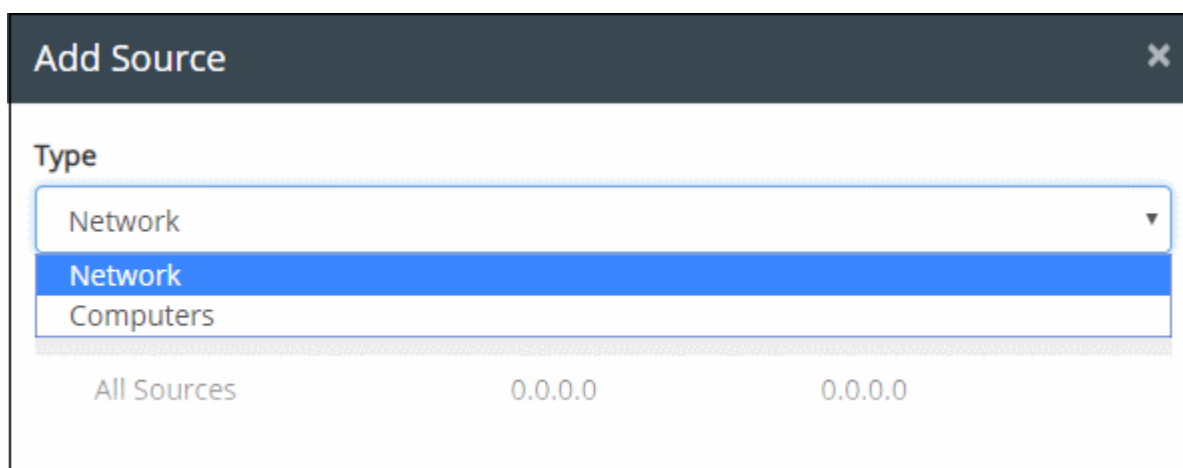
Object	Applicable Rule Types
Network	Endpoint Discovery rule
Computers	Endpoint Discovery rule
Remote Storage	Remote Storage rule
Database Connections	Database Discovery Rule

The following sections explain more about:

- **Add sources for Endpoint Discovery Rule**
- **Add sources for Remote Storage Rule**
- **Add sources for Database Discovery Rule**

#### To add a source object for an Endpoint Discovery Rule

- Click the 'Edit' button in the 'Sources' dialog
- Select the type of source object from the 'Type' drop-down



**Add Source** [X]

Type

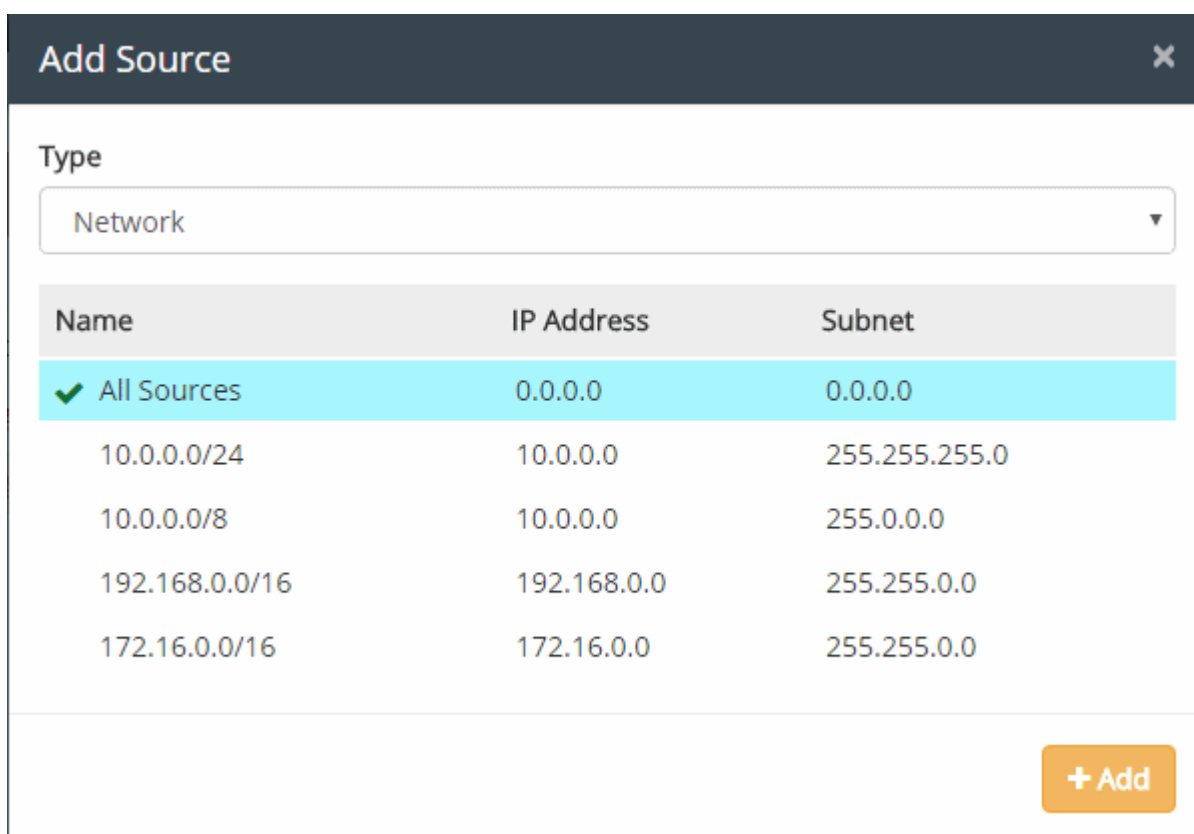
Network ▼

Network

Computers

All Sources      0.0.0.0      0.0.0.0

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



**Add Source** [X]

Type

Network ▼

Name	IP Address	Subnet
✓ All Sources	0.0.0.0	0.0.0.0
10.0.0.0/24	10.0.0.0	255.255.255.0
10.0.0.0/8	10.0.0.0	255.0.0.0
192.168.0.0/16	192.168.0.0	255.255.0.0
172.16.0.0/16	172.16.0.0	255.255.0.0

+ Add

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

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



Type	Name
Computers	Bobs PC

← Back   Next →   Edit

- Click 'Edit' to add more objects or click 'Next' to proceed to **Step 4 - Specify the destinations for the rule.**

#### To add a source object for a Remote Storage Rule

- Click the 'Edit' button in the 'Sources' dialog

The 'Remote Storage' object type will be auto-selected from the 'Type' drop-down. A list of remote storage objects available in CDDP will be displayed. If you have not yet added any remote storage objects, see **Adding a User Defined Remote Storage Object**.

Name	Address	Type
windows 81	192.168.1.36.81\Discovery-test-burak	wir
✓ Sales Team Share	192.168.1.36.81\Discovery-test-burak	wir

+ Add

- Select the remote storage object(s) to be added to the rule and click 'Add'.

The storage objects will be added.

- If you want to specify locations in the remote storage location(s) to be excluded from the CDDP scan, enter the path in the text box under 'Discovery Exception Path' and click the '+' button.



The location will be added to the list under 'Discovery Exception Path'.

- To remove an exclusion path, select it and click the '-' button.
- Click 'Edit' to add more objects or click 'Next' to proceed to **Step 4 - Specify the destinations for the rule**.

#### To add a source object for a Database Discovery Rule

- Click the 'Edit' button in the 'Sources' dialog

A list of 'Database Connections' objects available in CDDP will be displayed. If you have not yet added any database connection objects, see **Add a Database Discovery Object**.

**Add Source** [X]

Type

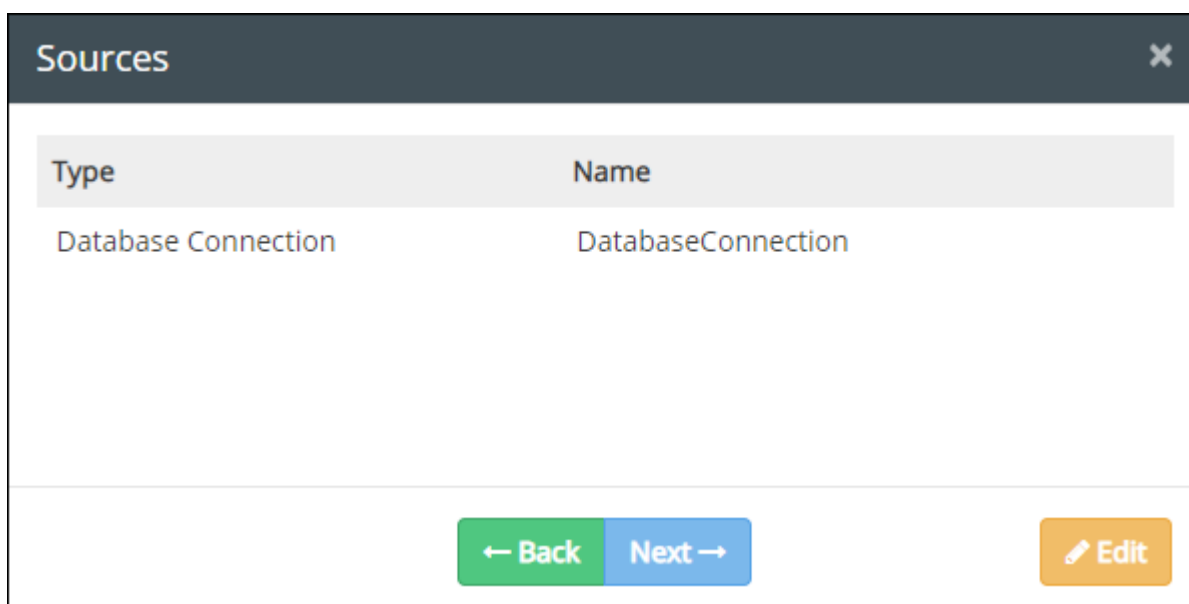
Database Connection

Name	Type	DB Url	Username
✓ DatabaseConnection	MYSQL	jdbc:mysql://10.100.136.236/mydlp_test_small	

+ Add

- Select the database connection object(s) to be added to the rule and click 'Add'.

The database connection object will be added.



Type	Name
Database Connection	DatabaseConnection

← Back   Next →   Edit

- Click 'Next' to proceed to **Step 5 – Specify the 'Information Types'**. Note – The source and destination for this rule is same, so the destination step will be skipped.

#### Step 4 – Specify the destinations for the rule

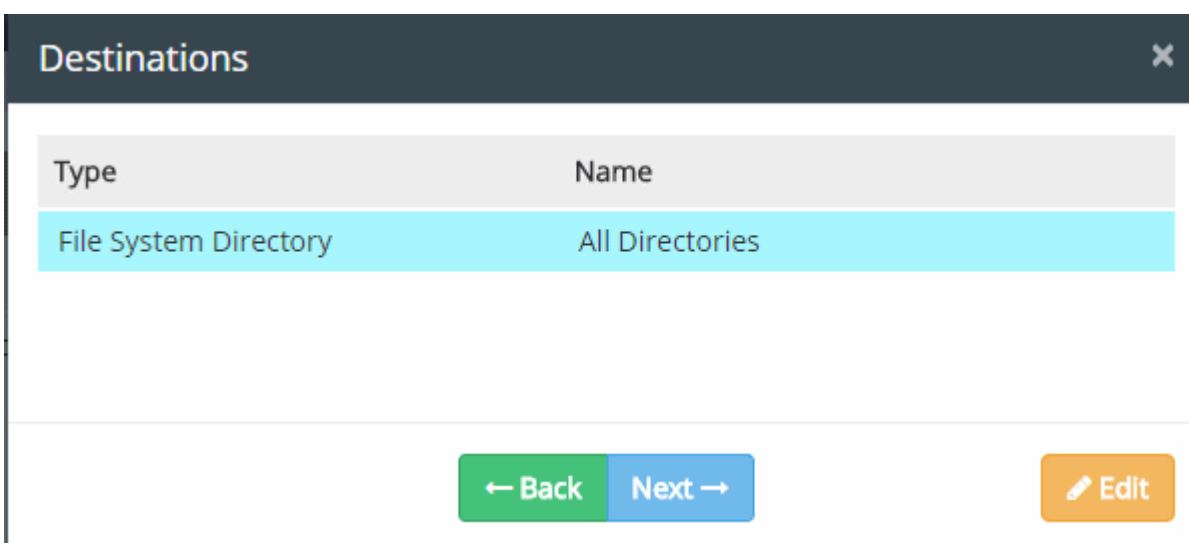
The 'Destination' component of a discovery rule is where you specify the target folder to be scanned in the selected endpoints. The destination is only specified for endpoint discovery rules. For remote storage rules, CDDP scans the full storage (except excluded paths) for the information type specified in the rule.

You can add destinations by selecting a predefined or user-defined 'File System Directory' object from the 'Type' drop-down.

##### To add a destination object

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

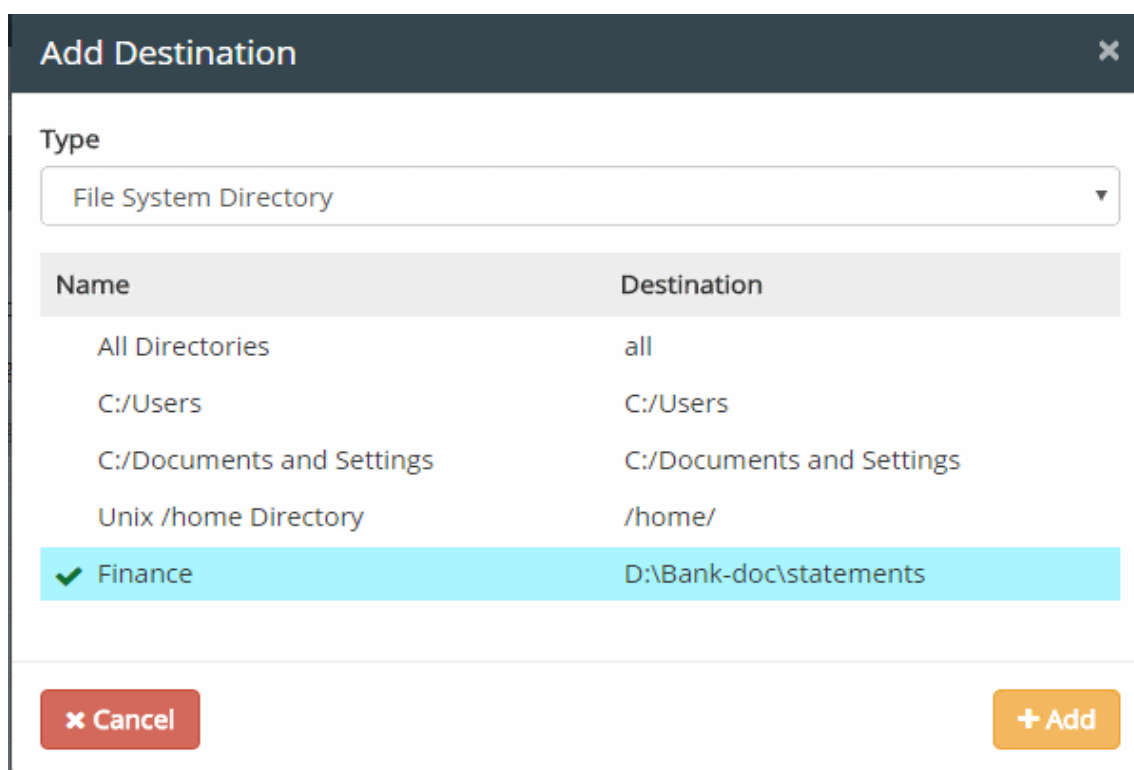
The 'Destinations' dialog will be displayed:



Type	Name
File System Directory	All Directories

← Back   Next →   Edit

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



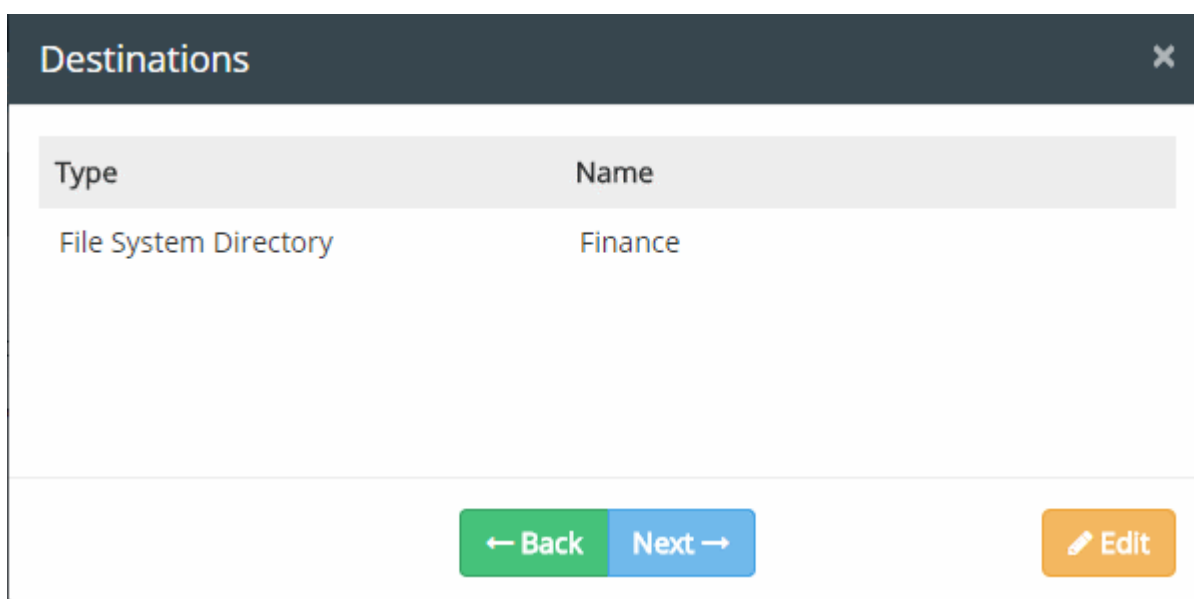
The 'Add Destination' dialog box features a dark header with the title 'Add Destination' and a close button. Below the header, there is a 'Type' dropdown menu currently set to 'File System Directory'. Underneath, a table lists various destinations. The table has two columns: 'Name' and 'Destination'. The rows are: 'All Directories' (all), 'C:/Users' (C:/Users), 'C:/Documents and Settings' (C:/Documents and Settings), 'Unix /home Directory' (/home/), and 'Finance' (D:\Bank-doc\statements). The 'Finance' row is highlighted in light blue and has a green checkmark in the 'Name' column. At the bottom, there are two buttons: a red 'Cancel' button and an orange '+ Add' button.

Name	Destination
All Directories	all
C:/Users	C:/Users
C:/Documents and Settings	C:/Documents and Settings
Unix /home Directory	/home/
✓ Finance	D:\Bank-doc\statements

The objects listed depends on the predefined and user defined objects created for that type. If you haven't added any user-defined objects yet, see [User Defined Objects](#) for more details.

- Select the object(s) from the list
- To add more destinations for other object types, select another object type from the 'Type' drop-down and repeat the procedure.
- Click 'Add' to save your choice.

All selected destinations added will be displayed as a list.



The 'Destinations' window shows a list of added destinations. It has a dark header with the title 'Destinations' and a close button. Below the header, there is a table with two columns: 'Type' and 'Name'. The table contains one row: 'File System Directory' and 'Finance'. At the bottom, there are three buttons: a green '← Back' button, a blue 'Next →' button, and an orange 'Edit' button with a pencil icon.

Type	Name
File System Directory	Finance

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

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

An 'Information Type' is the kind of data which you wish to search for in scanned locations. For example, credit card numbers, social security numbers and so on.

- For CDDP to intercept files containing data of a specific type, an 'Information Type' object needs to be added to the rule.
- CDDP ships with a number of commonly used 'Information Types' and 'Information Type Groups'.
- Each group contains a set of predefined information types that pertain to a category. Information types and groups are available under the 'Information Type' tree on the left.
- Administrators can also add custom information types and groups.

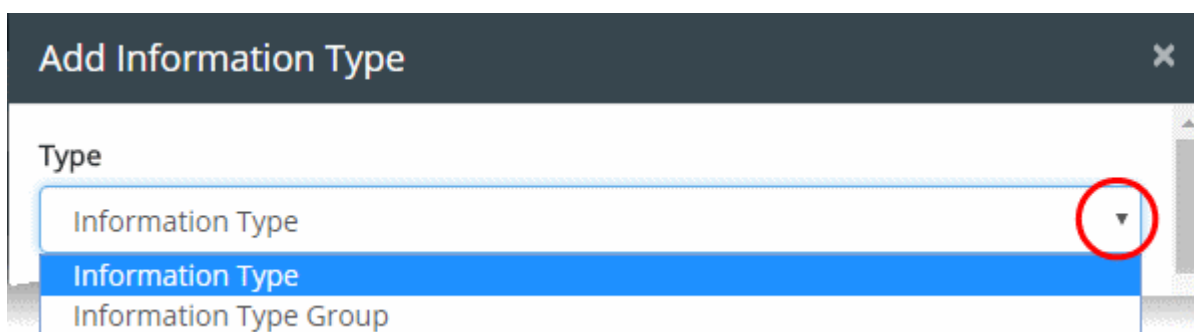
For more details on information types, refer to [Information Types - An Overview](#).

#### To add an Information Type object

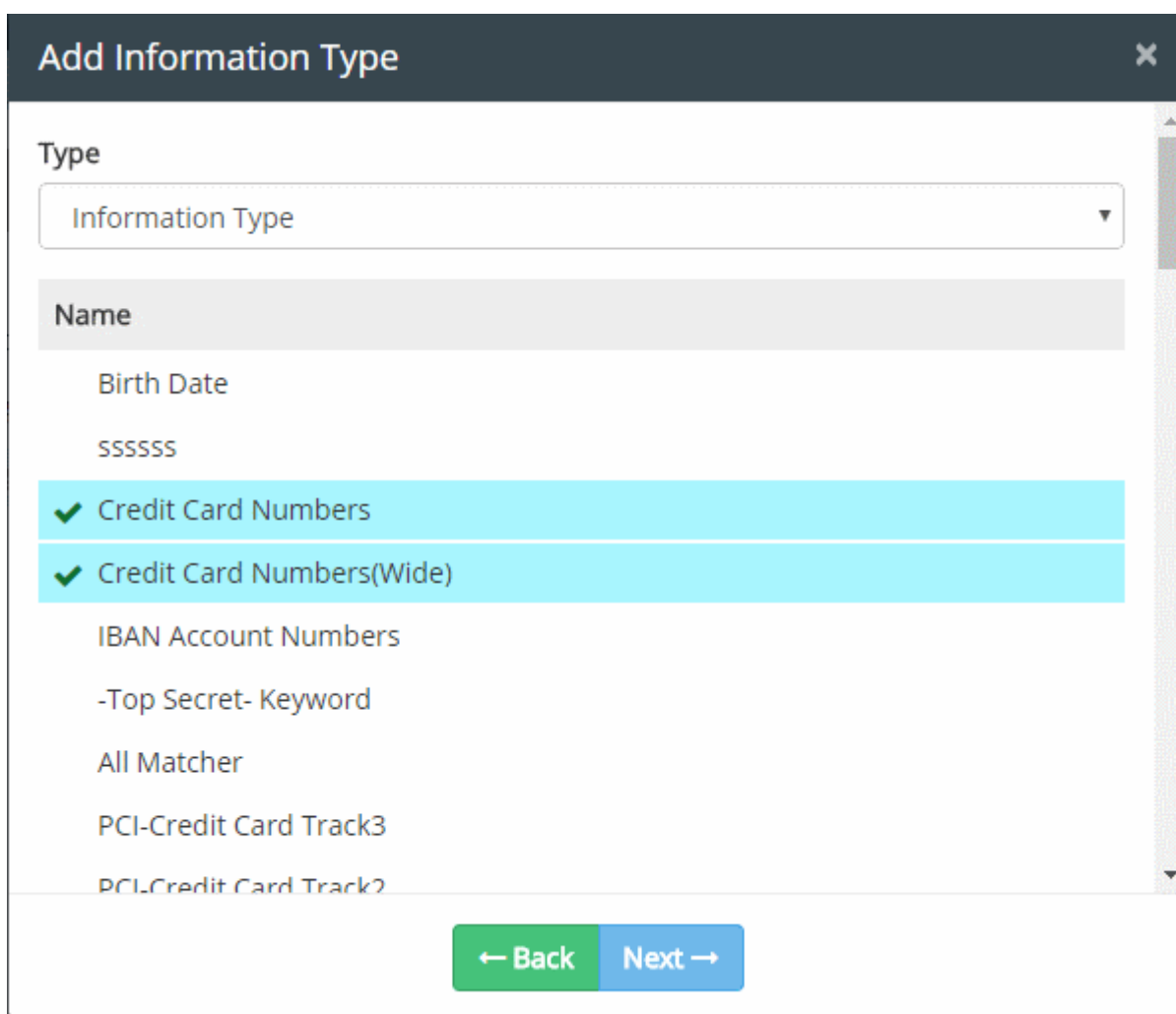
- Click the 'Next' button after selecting the destination type and completing other parameters as explained in Step 4

The 'Add Information Type' dialog will be displayed. Choose whether you want to add individual information types or information groups from the drop-down at the top:

- Choose whether you want to add 'Information Types' or 'Information Type Groups' from the drop-down at the top.



Select your information type(s) from the list.



- The types available depend on the predefined and user defined objects created for it. If you wish to define a custom type, see **'Add a User Defined Information Type'** and **'Add a User Defined Information Type Group'**.
- To add more objects choose 'Information Type' or 'Information Type Group' from the drop-down at the top and repeat the procedure.
- Click 'Next' to specify the action for the rule

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

Next, specify the action to be taken if the rule is triggered:

The available actions depend on the selected source and destination objects:

- **DELETE** – Delete all files which match the rule criteria. It is advised to use this action very carefully. This action is available only for Endpoint Discovery Rules.
- **LOG** - Generates an event log.
- **QUARANTINE** - Removes the identified file from the endpoint and saves a copy in the CDDP server. Administrators can download the file from the 'Logs' interface. It is advised to use this action very carefully. This action is available only for Endpoint Discovery Rules. See [Download Files Archived by CDDP](#) for more details.
- **ARCHIVE** - Generates an event log and archives a copy of the file. Administrators can download the file from the 'Logs' interface. See [Download Files Archived by CDDP](#) for more details.

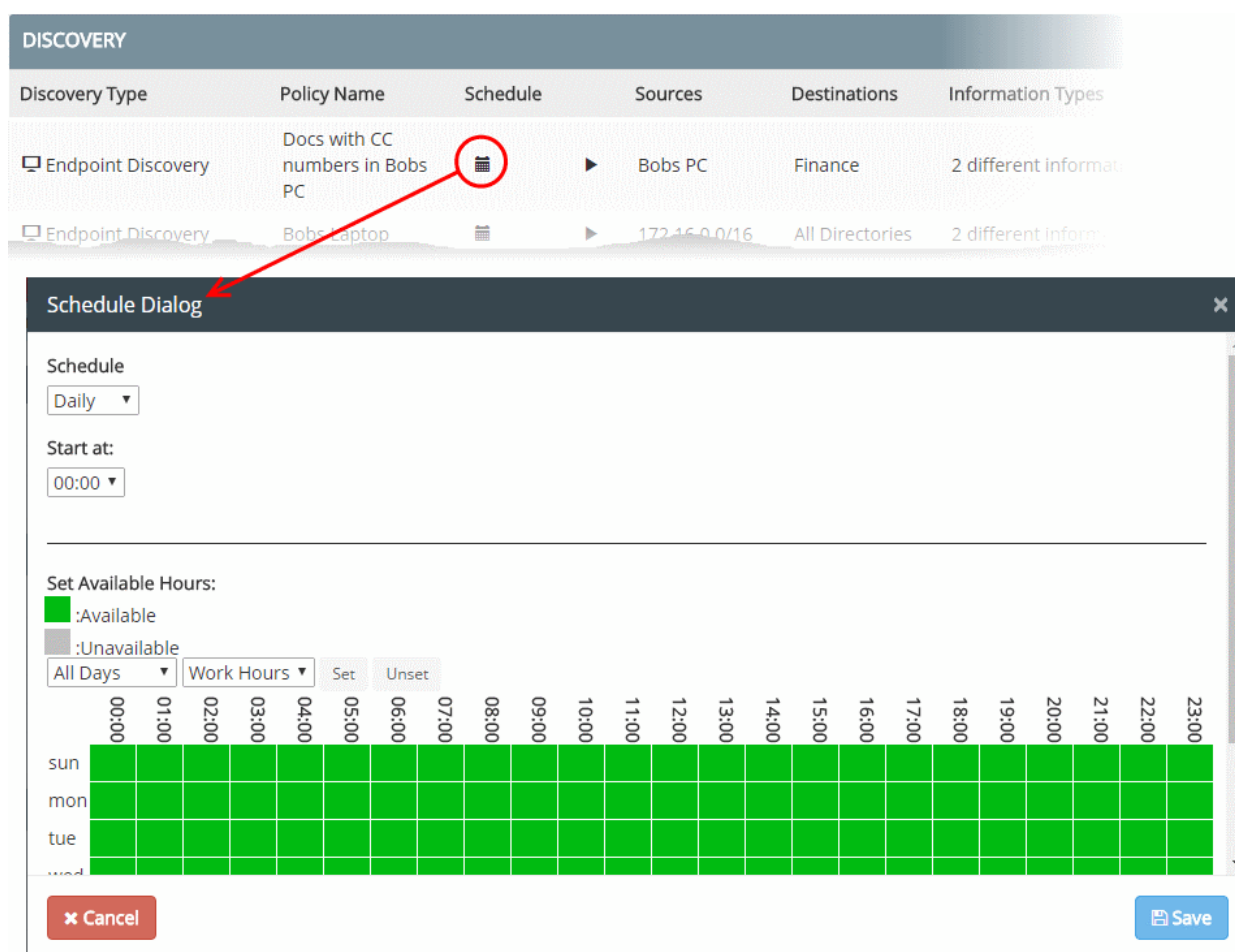
Click 'Save' to finish the rule creation process. You can create as many rules as required. You can also clone rules if you want to create a new rule which has minor changes to an existing rule.

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

The final step is to schedule CDDP to periodically scan your endpoints and storage locations.

#### To set a scan schedule in a rule

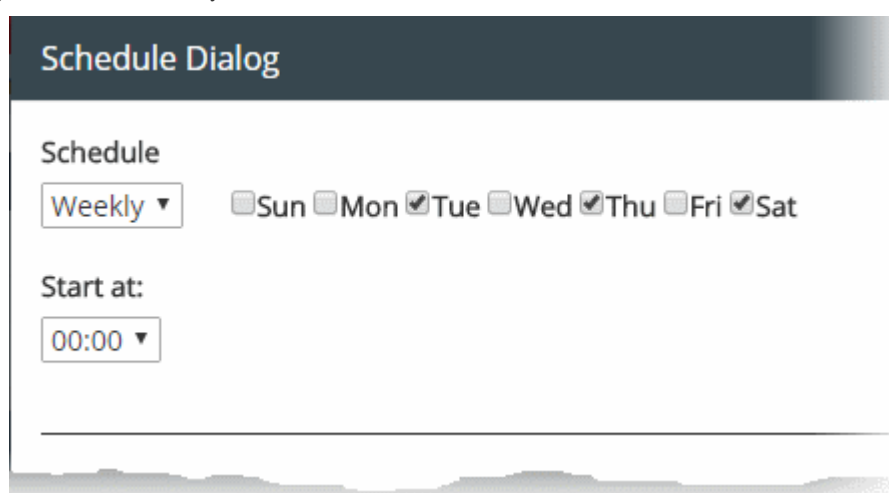
- Click the 'Calendar' button under the 'Schedule' column:



The 'Schedule' dialog will appear:

### Schedule

- Select whether you wish the scans to be run on daily or weekly basis from the drop-down. If you choose weekly, then select the days on which the scan needs to run.



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

### Available/Unavailable Hours

You can also specify times when target endpoints/remote storage will be available for scans. Scans set for unavailable times will be skipped.

The table below 'Available/Unavailable Hours' indicates the time periods at which the endpoints/repositories will be

available/unavailable:

- Green blocks - available for scanning
- Gray blocks – not available for scanning
- Click a block to change available/unavailable hours.
- To 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 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 apply your schedule

The rules take effect only after applying the discovery policy to the network. See [Deploy a Policy](#) for more details.

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

- Click on the rule to view the control buttons at top-right:

DISCOVERY							<a href="#">+ Add</a> <a href="#">Edit</a> <a href="#">Delete</a>
Discovery Type	Policy Name	Schedule	Sources	Destinations	Information Types	Action	
Endpoint Discovery	Docs with CC numbers in Bobs PC		Bobs PC	Finance	2 different information types	LOG	
Endpoint Discovery	Bobs Laptop		172.16.0.0/16	All Directories	2 different information types	QUARANTINE	

Control	Description
	Allows administrators to add a new rule
	Enables administrators to edit the name, source, destination, information type and action settings of the rule. Refer to the section <a href="#">Editing a Rule</a> for more details,
	Removes the rule from the policy. Refer to the section <a href="#">Removing a Rule</a> for more details.
	Available in an expanded rule. Clones the rule so administrators can use it as the starting point for a new rule.
	Available in an expanded rule. Enables the administrator to disable or enable the rule. Refer to the section <a href="#">Enabling or Disabling a rule</a> for more details.


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




### Enabling or disabling a rule

Rules added to a policy are automatically enabled by default. Administrators can disable a rule if required. Disabled rules are shown in gray in the table.



**To disable / disable a rule**

- Click on the rule to reveal the control options
- Click the Disable icon 

DISCOVERY					
Discovery Type	Policy Name	Schedule	Sources	Destinations	
Endpoint Discovery 	Docs with CC numbers in Bobs PC		 Bobs PC	Finance	
			172.16.0.0/16	All Director	

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

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



**Editing a rule**

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

- Any change you make in a rule will take effect only after re-deploying the policy. See [Deploy the Policy](#) for more details on implementing the policy.
- You cannot edit the rule 'Type'.

**To edit a rule**

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

DISCOVERY						
						<a href="#">+ Add</a> <a href="#">Edit</a> <a href="#">Delete</a>
Discovery Type	Policy Name	Schedule	Sources	Destinations	Information Types	Action
Endpoint Discovery	Docs with CC numbers in Bobs PC		 Bobs PC	Finance	2 different information types	LOG
Endpoint			172.16.0.0/16	All	2 different information	QUARANTINE

General Rule Edit ✕

Name

Docs with CC numbers in Bobs PC

Type

Endpoint Discovery ▼

Description

To identify PDF and Office Docs containing two credit card numbers, in Bobs PC

✕ Cancel

← Back

Next →

Edit the 'Name' and 'Description' as required. Click the 'Next' button to edit source, destination, information types and

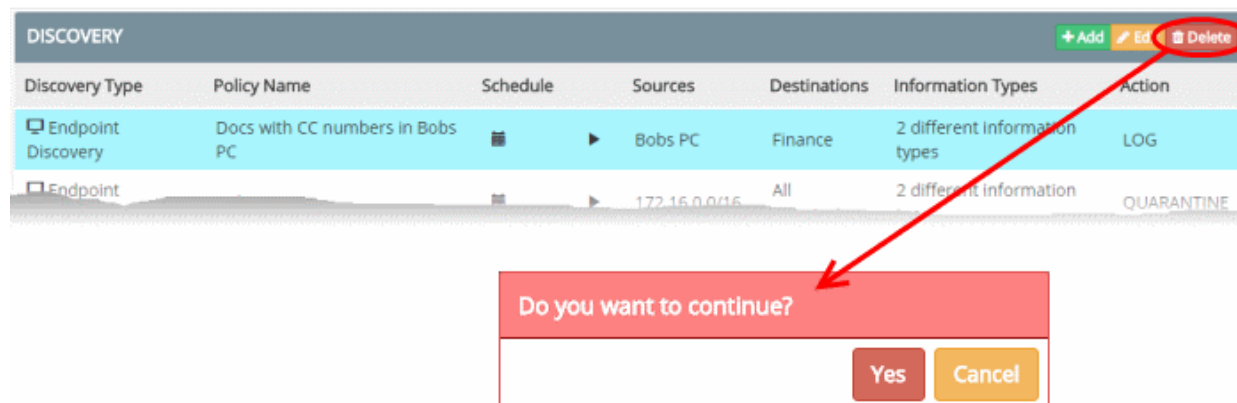
action. Refer to the rule creation wizard from **Step 2** onward for more details.

### Removing a rule

Administrators can remove unwanted rules from the policy at any time.

#### To remove a rule

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

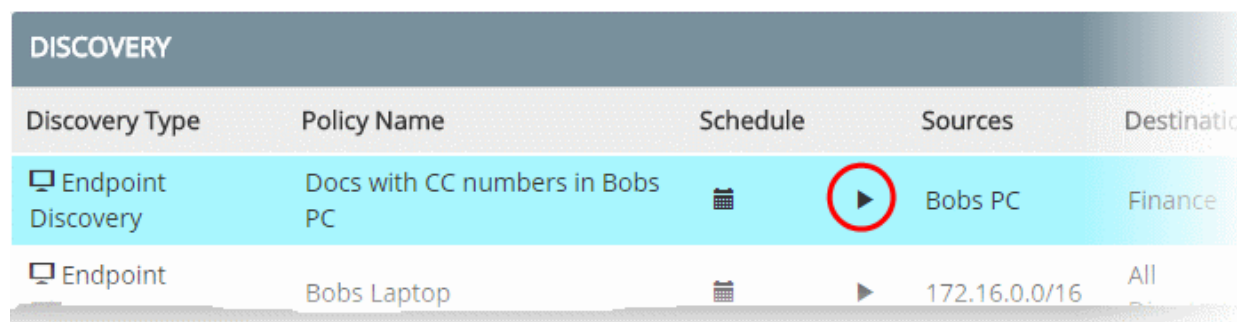


A confirmation dialog will be displayed.

- Click 'Yes' to remove the rule.

### Running On-Demand Scans

Administrators can run an instant scan for any rule at any time by clicking the ► button in the schedule column.



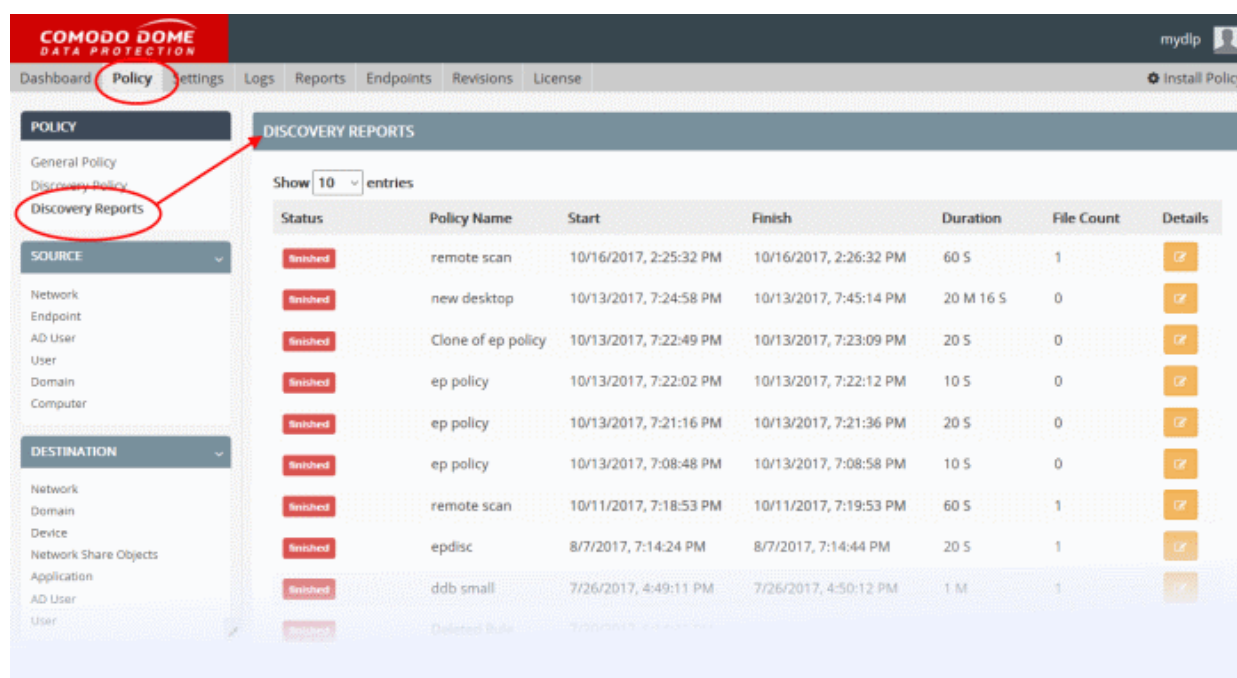
**Note:** You need to deploy the policy before running scans based on a particular rule. See **Deploy a Policy** for more details.

- The scan will start immediately and is indicated in the list of reports under the 'Discovery Reports'.
- You can pause/resume or stop the scan at any time.
- On scan completion, the scan report will be added to the list of reports.


### Viewing discovery scan reports

The Discovery interface enables administrators to quickly access discovery reports generated after scheduled or on-demand scans. The report provides a list of files containing sensitive information based on the rule from which the scan was run. Administrators can save the report as a spreadsheet file for future analysis.


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



Discovery Reports Table - Description of Columns

Column	Description
Status	Indicates whether the on-demand or scheduled scan is under process or completed.
Policy Name	The Discovery rule based on which the scan was executed.
Start	The date and time at which the scan started.
Finish	The date and time the scan was completed.
Duration	Time taken to complete the scan.
File Count	Number of items on target endpoints found to contain the data type specified in the rule.
Details	Clicking the  icon to open a particular discovery report. Refer to the following section <b>The Discovery Report</b> for more details.

## The Discovery Report

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

Log Details					
Show 10 entries			<a href="#">Detailed Search</a> <a href="#">Export to Excel</a> <a href="#">Refresh</a>		
Date	File	Action	Rule Type	Rule	Details
9/21/2016, 7:09:32 PM	Hebele 4111 1111 1111 1111.docx	Archive	Remote Discovery	discovery 81	
9/21/2016, 7:09:32 PM	Hebele 4111 1111 1111 1111 (2).docx	Archive	Remote Discovery	discovery 81	
9/21/2016, 7:09:31 PM	cc1.docx	Archive	Remote Discovery	discovery 81	
9/21/2016, 7:09:26 PM	testfile.pdf	Archive	Remote Discovery	discovery 81	
9/21/2016, 7:09:26 PM	test discover/target 1.txt	Archive	Remote Discovery	discovery 81	
Showing 1 to 5 of 5 entries				Previous	1 Next
<a href="#">Cancel</a>					

The Discovery Report - Description of Columns	
Column	Description
Date	The precise date and time at which the scan was completed.
File	The file name / file path
Action	The action executed on the file as per the discovery rule. See <a href="#">Rule Actions</a> for a list of actions.
Rule Type	The type of discovery rule used to find the file. This can be endpoint discovery, remote storage or database discovery rule.
Rule	The name of the discovery rule which found the file.
Details	View granular information about the incident and download copies of discovered files. See <a href="#">Viewing Details of a Discovery Log Entry</a> for more.

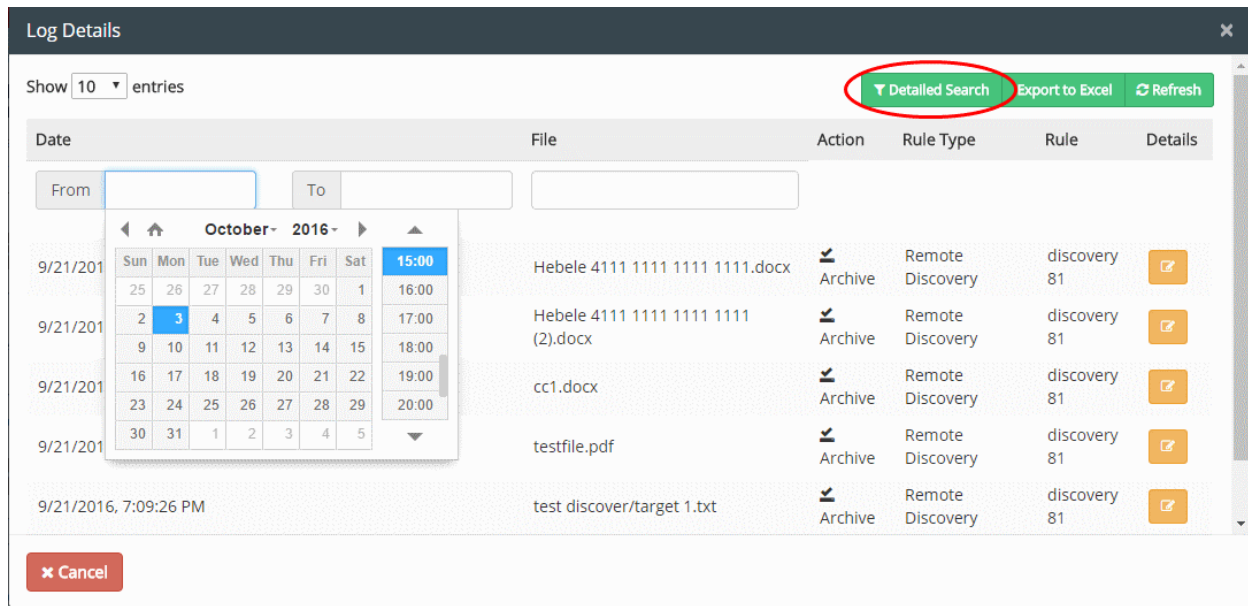
## Filtering and Search Options

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

- [Filtering the Logs for a specific time period](#)
- [Searching Logs based on rule source parameter](#)

### To filter the logs for a specific time period

- Click 'Detailed Search' at the top



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

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

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

### Searching Logs based on Rule Source Parameters


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

#### To search the logs based on rule source parameter

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

### Viewing Details of a Discovery Log Entry

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

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

Log File Details

Date  
9/21/2016, 7:09:32 PM

Target  
192.168.1.100 (Discovery target)

Action  
Archive

Rule Type  
Remote Discovery

Rule Name  
discovery 81

File  
Hebele 4111 1111 1111 1111.docx

Information Type  
Credit Card Numbers

Files  
Hebele 4111 1111 1111 1111.docx ⓘ  
cc\_match count: 2 pattern: 4111 1111 1111 1111

Close

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




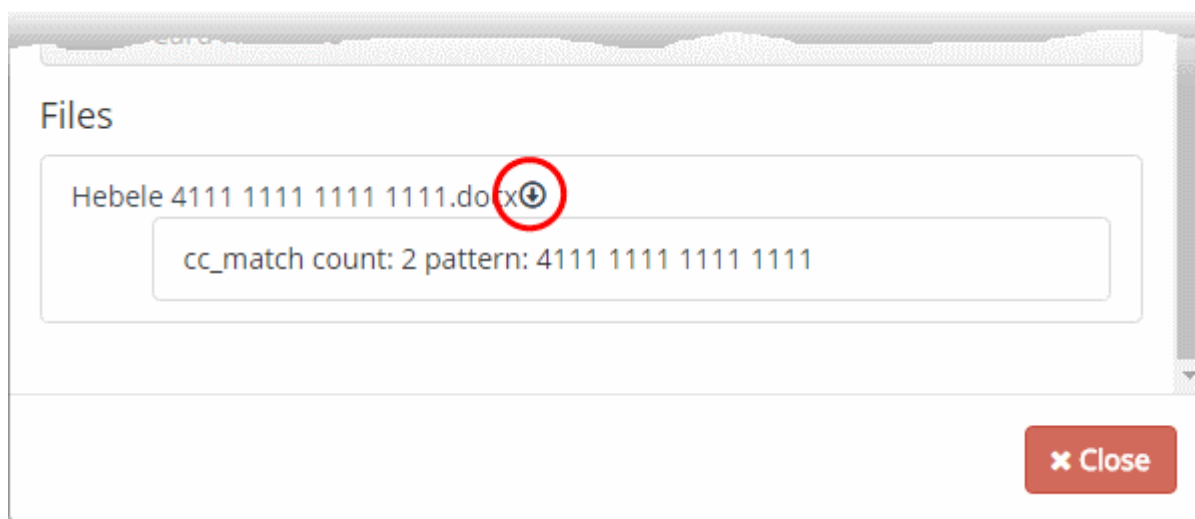
Action	The action executed on the discovered file(s).
Computer Name	The host name of the endpoint computer at which the file(s) were discovered.
Rule Type	The type of discovery rule used to identify the files (Endpoint Discovery or Remote Storage Discovery)
Rule Name	The name of the Discovery Rule based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

### Downloading the Archived Files

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

#### To download an archived file

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

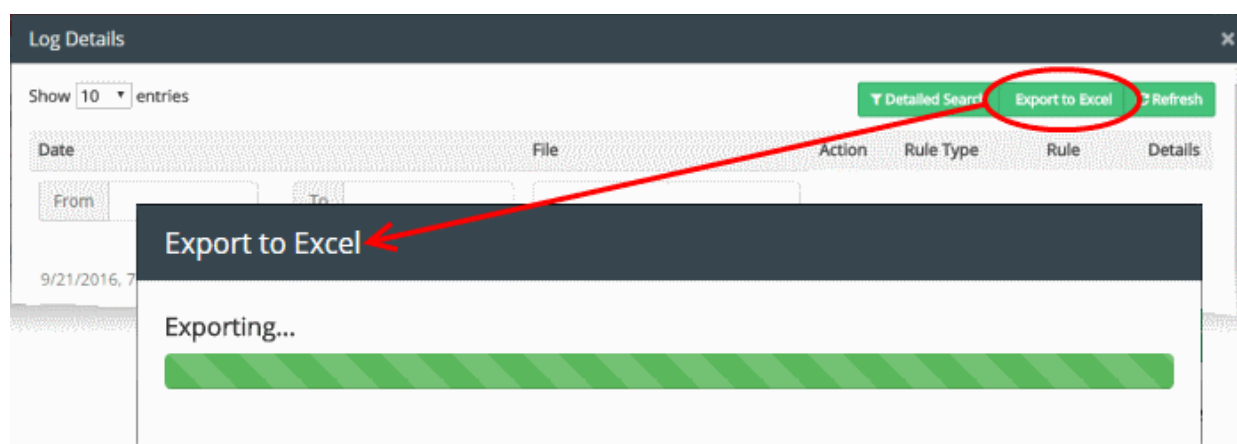


The file will be saved to your default download location.

### Exporting the Logs to a Spreadsheet File

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

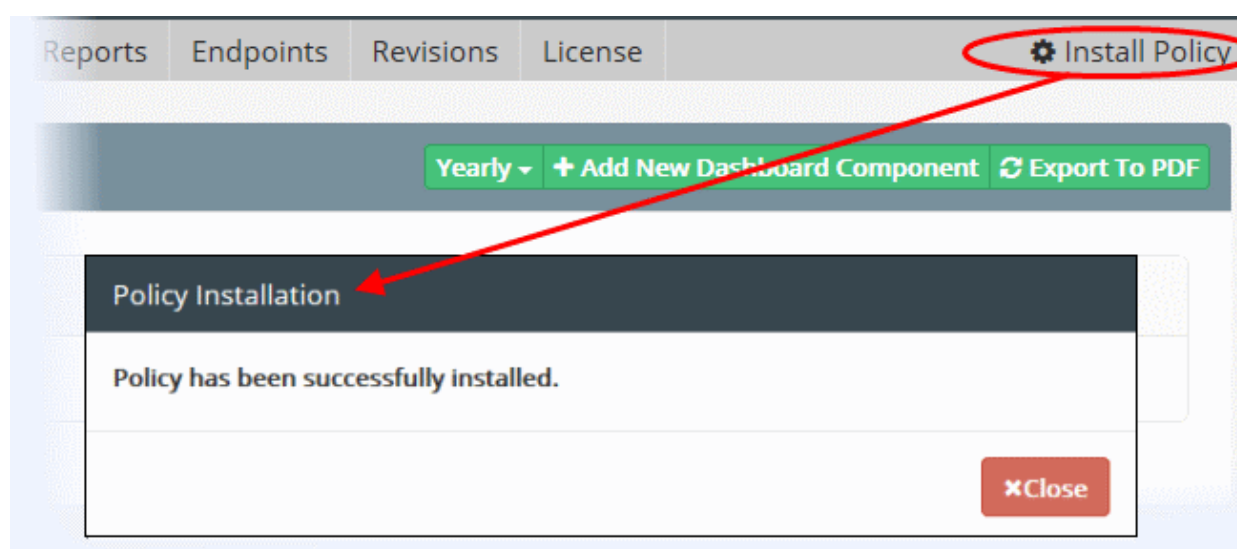
- To export the logs into an Excel file click 'Export to Excel' button at the top and save the file in your local drive.



#### 4.1.6. Deploy a Policy

The rules comprising your data transfer control and discovery policies 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 then the policy will be compiled and installed instantly.
- Incorrect rules will be highlighted and advice shown to correct or disable the rule.

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

## 5. Rule Types, Objects and Matchers

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

- Objects used to construct rules are shown on the left-side of the 'Policy' interface.
- Object categories are - 'Source', 'Destination', 'Discovery Target', 'Information Type' and 'Matcher'.
- These objects can be added to the 'source', 'destination' and 'information' fields when configuring rules. See **'Objects'** for more details.



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

**Tip:** You can click on  collapse button to reveal or hide the left hand pane of the policy interface.

Click on the following links for more information:

- [Rule Types](#)
- [Objects](#)
- [Matchers](#)

## 5.1. Rule Types

There are two types of rules that can be configured in CDDP:

- Data transfer control rules – These are displayed in the 'General Policy' interface.
- Data discovery rules – These are displayed in the 'Discovery Policy' screen.

### Data control rules

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

by the source object. You can choose to monitor or block use of disks. See **CD-DVD Rule** for more details.

- **Floppy rules** are used to control the use of floppy disks on selected computers covered by the source object. You can choose to allow or block use of disks, or set floppy disks to read-only mode. See **Floppy Rule** for more details.
- **Clipboard rules** are used to control the copy and paste function on computers covered by the source object. You can choose actions such as pass, block and more for this rule. See **Clipboard Rule** for more details.

#### Data discovery rules

- **Endpoint Discovery rules** are used to discover and control sensitive data on local storage and hard disks. See **Endpoint Discovery rules** for more details.
- **Remote Storage rules** are used to discover files containing sensitive data of specific type(s) from remote servers and network file systems. See **Remote Storage rule** for more details.
- **Database Discovery rules** are used to identify specific information types stored in databases. For example, credit card details. See **Database Discovery Rules** for more details.

**Note:** You need to configure the Dome Data Protection Network Server appropriately to apply Email, Web, API, Database Discovery and Remote Storage Discovery rules. See **CDDP Installation Guide** for more details. All other rules enforcement require you to install the DDP agent on the endpoints. See **CDDP Endpoint Agent Installation Guide** for details about adding endpoints.

Please contact support at domesupport@comodo.com if you need more information.

### 5.1.1. Web Rule

Web Rules cover the whole web channel and can be used to enforce policies for protocols like HTTP and HTTPS. Web rules let you implement restrictions for almost anything that can be accessed through a web browser, including social networking sites, web-mail, blogs, wikis and forums. To use web rules you need to configure your web traffic to pass through the Comodo Dome Data Protection Network Server. Please see **CDDP Installation Guide**.

Please contact support at domesupport@comodo.com if you need more information.

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

#### Example Web Rule

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

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
Web Rule	PCI	192.168.0.0/16	All Destinations	PCI-Credit Card	QUARANTINE

### 5.1.2. Mail Rule

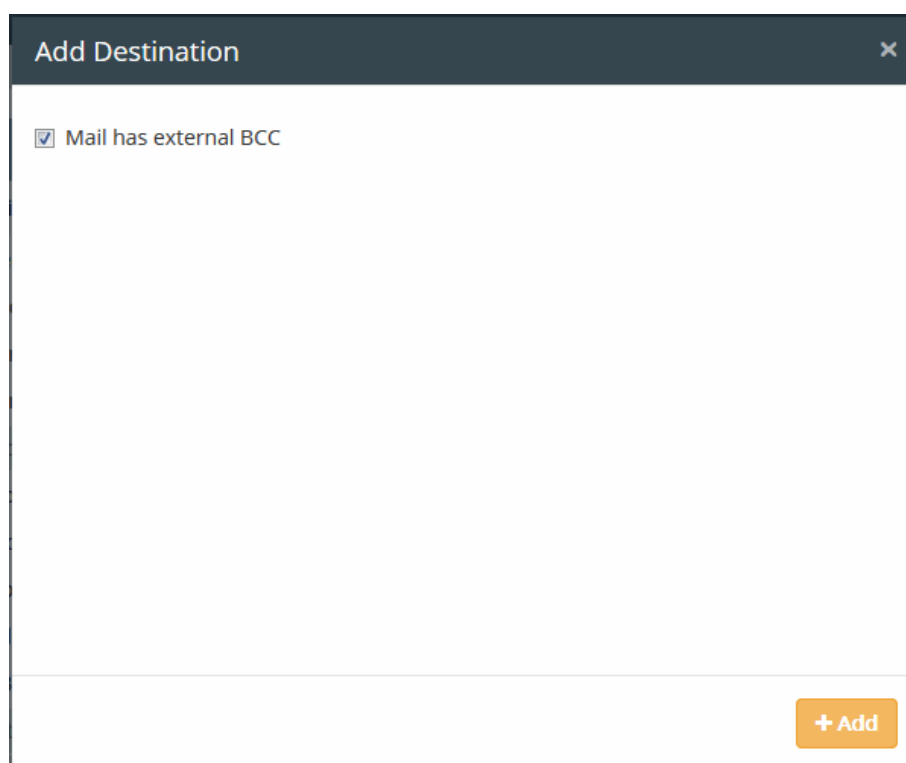
Mail rules cover the mail channel and can be used to enforce policies on the SMTP protocol. Emails that are sent through local mail servers will be analyzed by your CDDP mail rules. See [CDDP Installation Guide](#) for details about integrating your mail server with CDDP.

Please contact support at [domesupport@comodo.com](mailto:domesupport@comodo.com) if you need more information.

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

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

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



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

### Example Mail Rule

An example mail rule is shown below. The rule will archive all mails that contain specific information types sent from all sources to specific mail domain(s).

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
✉ Mail Rule	Credit	All Sources	2 different destinations	2 different information types	ARCHIVE

### 5.1.3. Removable Storage Rule

The 'Removable Storage Rule' is used to control data moved to removable devices which are connected to managed

endpoints. See **CDDP Endpoint Agent Installation Guide** for details about adding endpoints.

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

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

To restrict file copies from all USB devices, choose 'All USB Devices' from the 'Add Destination' screen.

Type	Device Name
✓ All	All Usb Devices
VID/PID	sari kingston
VID/PID	turkuaz toshiba
VID/PID	Jet

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

### Example Removable Storage Rule

An example removable storage rule is shown below. The rule will allow all files that contains specific information types from all sources to all USB devices.

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
Removable Storage Rule	Remote access	All Sources	All Usb Devices	4 different information types	PASS

**Note:** Removable storage rules only restrict files copied to specific devices (destination objects) defined in the rule. If you instead want to restrict access to USB devices altogether for certain endpoints, you should create a 'USB Device Access rule'. See '**USB Device Access Rule**' for more details.

### 5.1.4. Network Share Rule

The 'Network Share Rule' can be used to monitor and control data traffic from endpoints to Windows share locations. The CCDP agent needs to be installed on each endpoint that you want to use this rule. See [CDDP Endpoint Agent Installation Guide](#).

#### Network Share Sources

- You can specify any kind of user as a source, including user-defined users, AD users/groups/organizations, network objects and computer objects. See [The Objects](#) for more details on creating user defined sources.

#### Network Share Information Types

- You can specify any 'Information Type' in Network Share rules.

### Example Network Share Rule

An example network share rule is shown below. The rule will block transfers of all files containing credit card information from a specific endpoint using any network connection.

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
 Network Share Rule	Network Data Restriction	ep	All Network Connections	Credit Card Numbers	BLOCK

### 5.1.5. Removable Storage Inbound Rule

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

For the Removable Storage Inbound Rule to be enforced, the Comodo Dome Data Protection Endpoint Agent should be deployed at each endpoint. See [CDDP 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 and / or computers 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 removable storage inbound rule is shown below. The rule will log files copied from removable storage devices to workstations or laptops. The rule is labeled 'storage logging' and can be used to audit memory stick usage.

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
 Removable Storage Inbound Rule	Storage logging	All Sources			ARCHIVE

**Note:** The Removable Storage Inbound Rule can restrict only the files that are smaller than the Maximum Object Size configured under [Settings > Advanced](#) tab. Refer to the explanation under [Maximum Object Size](#) in the section [Configuring Advanced Settings](#) for more details. If you have specified 'Archive' action, depending on

your users' behavior you may need significant storage to store archived files.

The Logs pertaining to Removable Storage Inbound Rule will be displayed under the 'Logs' tab only if 'Show All' is selected under 'Detailed Search'. See [Detailed Log Search](#) for more details.

### 5.1.6. Removable Storage Encryption Rule

The Removable Storage Encryption Rule can encrypt removable devices connected to the endpoints on the network. This rule cannot make any kind of DDP 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' CDDP detects any new USB storage device connected to the endpoints covered by Source objects of the rule, formats the device and encrypts it, making it usable by the users for storing data from their endpoints. After encryption, any data stored on the device can only be read if it is connected to your network and not by any other network. This would prevent, for example, any guest or hostile from plugging in a USB drive, downloading data and taking it out of the network.

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

For the Removable Storage Encryption Rule to be enforced, the CDDP Endpoint Agent should be deployed at each endpoint. See [CDDP 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 and / or computers 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 removable storage encryption rule is shown below. The rule will encrypt all removable storage devices connected to the specified sources.

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
Removable Storage Encryption Rule	All Encrypted	3 different sources			ENCRYPT

### 5.1.7. Printer Rule

The printer rule is used to control printing of data from endpoints. The rule will inspect print operations sent from endpoints to specific printers.

- After applying a printer rule, virtual printers will be created for each physical printer connected to the network.
- The names of the virtual printers will contain the name of the physical printer as a prefix. They will be available to print documents from endpoints added as sources to the printer rule.
- The physical printers will be shown as 'Unavailable' so end-users are forced to use the virtual printers. This is required so CDDP can monitor the print requests.



- The document will be forwarded to the physical printer if it does not contain any sensitive data as defined by the rule.

The prefix added to the virtual printer name can be configured in the Settings > Endpoint Interface. See **Secure Printer Prefix** in **Configure Endpoint Settings** for more details.

For the Printer Rule to be enforced, the Comodo Dome Data Protection Endpoint Agent should be deployed at each endpoint. See **CDDP 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 and / or computers 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.  
Note – Printer policy cannot be enforced based on data format or extension in 'Information Types'

### Example Printer Rule

An example printer rule is shown below. The rule will quarantine all print jobs that contain credit card information sent by users from specific source endpoints. The print jobs will be blocked and document content is saved as a XPS document on Comodo Dome Data Protection. This rule is named 'PCI' because it is a part of the PCI compliance policy.

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
 Printer Rule	PCI	2 different sources		Network Patterns	BLOCK

### 5.1.8. ScreenShot Rule

The 'Screenshot Rule' can be used to prevent screen captures when certain applications are running or when sensitive documents are open on an endpoint. This rule does not send any logs to the management server.

The endpoint agent needs to be installed on each endpoint for the screenshot rule to be enforced. See **CDDP Endpoint Agent Installation Guide** for more details.

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

### Example ScreenShot Rule

An example screenshot rule is shown below. The rule will prevent the print screen function for any source to the specified five applications.

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
 Screenshot Rule	Screenshot Restriction	All Sources	5 different destinations		BLOCK

### 5.1.9. API Rule

API rules can be configured to manage the behavior of the Comodo Dome Data Protection API. The API helps you integrate CDDP with other applications. API rules enforce the policy in API channel if data being sent via API query. See '[Query API](#)' at the end of this section for details about Query API usage.

To enforce API rules you need to configure the Comodo Dome Data Protection Network Server accordingly. Please see [CDDP Installation Guide](#).

Please contact support at [domesupport@comodo.com](mailto:domesupport@comodo.com) if you need more information.

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

#### Example API Rule

An example API Rule is shown below. The rule is to block responses to web requests from applications on 10.0.0.0/24 network if the request body contains credit card numbers.

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

#### Query API Usage

This section contains information about Query API usage.

##### 1. Authentication

To establish communication with Dome Data Loss Prevention (DLP) servers, a client app IP address must be added into Access Control File from DLP Server. Once an app IP address is added into list (api.conf), user is able to manage policy via API call such as install, list, enable and disable policy. Please follow the steps to add client server IP address into list.

1. Open a SSH session to the Comodo DLP server. You can use Putty to do this on Windows or the SSH command line tool under GNU/Linux or Mac OSX
2. For windows run putty , then enter IP address of server
3. Enter your login name then enter password (login name is ubuntu)
4. You should grant root privilege to make change on configuration file therefore please execute following command  
`sudo su -`
5. Type your password when prompted
6. Execute following command to open file then add IP address of client which sends API call into file.  
`pico -t /etc/mydlp/api.conf`
7. To save and exit please execute following command  
`CTRL+X`

**Note:** If there is a firewall policy between your app and DLP server , please allow connection to DLP server over SSH and HTTP/S ports.

##### 2. Query API

Dome DLP API enables to integrate custom application with DLP to perform DLP analysis.



For example, if your application requires DLP inspection in business logic, you can provide this with using API Policy.

Comodo DLP is offered as Web Service which is accessible by using URL `https://X.X.X.X/api/query`

There are two inputs;

1. **“filename” Request Parameter:** Specifies filename of data.
2. **Raw post data:** Content of file should be sent as HTTP POST payload and returns result as string.  
Possible values are;
  - **“pass”:** Means that file is not blocked according to DLP policy
  - **“block”:** Means that file is blocked according to DLP policy

### 3. Curl Sample

Linux command line tool curl can be used to query Dome DLP API.

- **Suspectedfile.pdf** is the file name and given as example
- **X.X.X.X** is IP address of the COMODO DLP server
- **COMODOUSER** is username defined on DLP system and given as an example.

Please insert correct values instead of the 3 samples above while you are sending data.

#### Sample 1: Default Query Structure

```
curl -k -X POST --data-binary @suspectedfile.pdf https://X.X.X.X/api/query?filename=suspectedfile.pdf
```

#### Sample 2: Query with username

```
curl -k -X POST --data-binary @suspectedfile.pdf  
https://X.X.X.X/api/query?filename=suspectedfile.pdf&username=COMODOUSER'
```

## 5.1.10. USB Device Access Rule

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

For a USB rule to be enforced, the Comodo Dome Data Protection Endpoint Agent should be deployed at each endpoint. See **CDDP Endpoint Agent Installation Guide**.

**USB Device Access Rule Source:** - You can specify any kind(s) of users (User Defined Users, AD users, AD groups, and AD organization units), network objects and / or Computers objects as Source for this rule.

**USB Device Access Rule Destination and Information Type:** - Since Destination is always the endpoint itself and Information Type is not checked in this rule type, these objects are not required and cannot be defined for this rule type.

### Example USB Device Access Rule

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

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

### 5.1.11. CD-DVD Rule

- The CD-DVD rule can control and monitor the use of optical disks on endpoints covered by the source object defined in the rule.
- This rule cannot make any kind of DLP analysis, but can pass, log or block the use of disks.

The CDDP agent needs to be installed on each endpoint in order for this rule to work. See [CDDP Endpoint Agent Installation Guide](#).

**CD-DVD Rule Source:** - You can specify any kind of source object in this rule: user-defined users, AD users, AD groups, AD units, network objects and computers.

**CD-DVD Rule and Information Type** - Information type is not required for this kind of rule.

#### Example CD-DVD Rule

An example CD-DVD Rule is shown below. The rule will set the use of CD-DVD to 'Block' mode on endpoints used by all sources.

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
CD-DVD Rule	Block copy to CD and DVD	All Sources			BLOCK

### 5.1.12. Floppy Rule

- The 'Floppy' rule controls the use of floppy disks on endpoints covered by the source object in the rule.
- This rule cannot make any kind of DLP analysis, but can pass, log or block the use of disks, or set them to 'Read-Only' mode.

The CDDP agent needs to be installed on each endpoint in order for this rule to work. See [CDDP Endpoint Agent Installation Guide](#) for help on this, if required.

**Floppy Rule Source:** - You can specify any kind of source object in this rule: user-defined users, AD users, AD groups, AD units, network objects and computers.

**Floppy Rule and Information Type** - Information type is not required for this kind of rule.

#### Example Floppy Rule

An example floppy rule is shown below. The rule will block the use of floppies on work stations or laptops used by 'Purchase Department' staff.

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
Floppy Rule	Block Floppy disks	Purchase			BLOCK

### 5.1.13. Clipboard Rule

- The 'Clipboard' rule can prevent the copying of sensitive information from documents on endpoints. The rule blocks users from copying certain information types (e.g. credit card numbers) to the clipboard.

The CDDP agent needs to be installed on each endpoint in order for this rule to work. See [CDDP Endpoint Agent Installation Guide](#).

**Clipboard Source** - You can specify any kind of source object in this rule: user-defined users, AD users, AD

groups, AD units, network objects and computers.

**Clipboard Destination**

- Destination is not required for this rule because the destination is always the endpoint itself.

**Clipboard Information Types**

- You can specify any information type in this kind of rule.

### Example Clipboard Rule

An example of rule is shown below. The rule is to block credit card numbers from being copied to the clipboard from any document.

Policy Type	Policy Name	Sources	Destinations	Information Types	Action
 Clipboard Rule	Block Copy Function	All Sources		Credit Card Numbers	BLOCK

## 5.1.14. Endpoint Discovery Rule

- 'Endpoint Discovery' rules can scan local disks/file paths on endpoints to identify files containing sensitive information.

The CDDP agent needs to be installed on each endpoint in order for this rule to work. See [CDDP Endpoint Agent Installation Guide](#).

**Discovery Source:**

- You can specify any kind of source object in this rule: user-defined users, AD users, AD groups, AD units, network objects and computers.

**Discovery Destination**


- You can specify 'File System Directory' objects as destinations for this rule.  
Endpoint folders named as destinations will be scanned to find whether they have data which matches the information type.

**Discovery Information Types**

- You can specify any information type in a discovery rule.

### Example Endpoint Discovery Rule

An example rule is shown below. The rule is to log files containing credit card numbers found in the 'Documents and Settings' folder of endpoints in the 192.168.0.0/16 network.

Discovery Type	Policy Name	Schedule	Sources	Destinations	Information Types	Action
 Endpoint Discovery	Endpoint Credit Card Details		 192.168.0.0/16	2 different destinations	Credit Card Numbers(Wide)	LOG

## 5.1.15. Remote Storage Rule

- The 'Remote Storage' rule scans servers to discover files containing sensitive data.
- Potential targets include FTP servers, web servers, file share locations and network file systems.
- Admins can log or archive files which contain sensitive information

The CDDP agent needs to be installed on each endpoint in order for this rule to work. See [CDDP Installation Guide](#) if you need help with this.

Please contact support at [domesupport@comodo.com](mailto:domesupport@comodo.com) if you need more information.

- Discovery Source:** - Specify a 'Remote storage' object as the rule 'Source'.  
Remote storage objects point to a specific location/server. They can only be created in the 'Discovery' interface. See [Add a User Defined Remote Storage Object](#) for more info.
- Discovery Destination:** - Not required for this type of rule.
- Discovery Information Types:** - You can specify any information type in this kind of rule.

### Example Remote Storage Discovery Rule

An example rule is shown below. The rule will archive Office document files found on the sales team shared drive which contain credit card numbers.

Discovery Type	Policy Name	Schedule	Sources	Destinations	Information Types	Action
Remote Storage Rule	Credit Card Numbers Discovery		Sales Team Share		Credit Card Numbers	ARCHIVE

## 5.1.16. Database Discovery Rule

- 'Database discovery' rules scan database servers to locate sensitive information.
- Admins can log sensitive information identified by the rule.
- Note - CDDP currently only supports data discovery from MySQL databases.

The CDDP agent needs to be installed on each endpoint in order for this rule to work. See [CDDP Installation Guide](#) if you need help with this.

Please contact support at [domesupport@comodo.com](mailto:domesupport@comodo.com) if you need more information.

- Database Discovery Source:** - Specify a 'Database Discovery' object as 'Source' for this type of rule.  
These objects can only be created in the 'Discovery' interface. See [Add a Database Discovery Object](#) for more details.
- Database Discovery Destination:** - Destination is not required for this rule.
- Discovery Information Types:** - You can specify any information type in this kind of rule.

### Example Database Discovery Rule

An example rule is shown below. The rule is to archive details about pricing information found on the database.

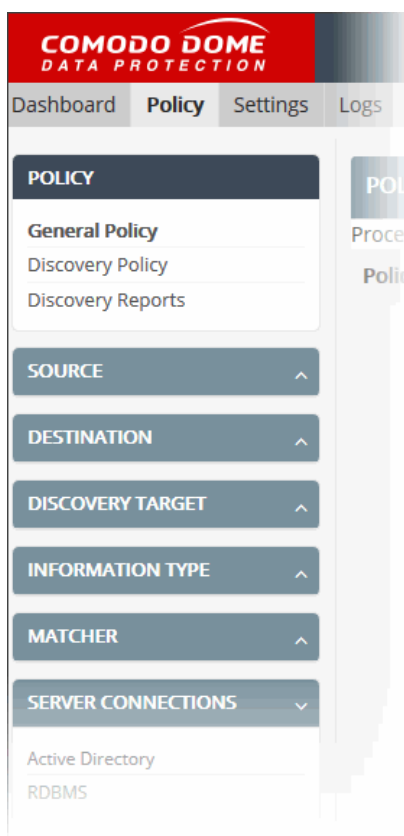
DISCOVERY <span>+ Add  Delete</span>						
Discovery Type	Policy Name	Schedule	Sources	Destinations	Information Types	Action
Database Discovery Rule	db rule		test		Pricing Information	LOG

## 5.2. Objects

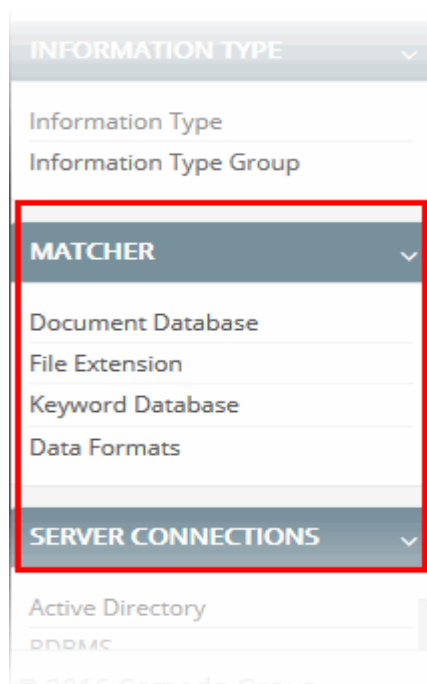
- An object is a named entity which can be referenced in a rule
- An object can be a computer, network, user, domain, device, connection type, file system or information type
- These objects can be used as the 'source', 'destination' and 'information' components of a rule

### View available objects

- Login to CDDP
- Click the 'Policy' tab on the file menu to open the policy interface
- Objects which you can add to a rule are shown on the left. They are grouped under the following headings:
  - Source
  - Destination
  - Discovery Target
  - Information Type
  - Matcher
  - Server Connections



- Click the arrows on the right to view individual objects in that category:



CDDP ships with a set of commonly used, pre-defined objects.

- Predefined sources are common network addresses.
- Information types includes items such as credit card numbers, IBAN, SSN, names and account numbers. It also includes a matcher to match all traffic.
- 'Compliance' is an information type that includes predefined policies such as PCI DSS, HIPAA, SOX, and GLBA etc.
- Predefined destinations can be used in the 'destination' component of a rule.

You can also create custom objects and object groups. See [User Defined Objects](#) for more details.

### 5.2.1. Object Types

'Objects' are the building blocks of a rule. Objects can be used as the 'source', 'destination' and 'information' components of a rule.

Object Type	Description	Application
Network	Available in 'Source' and 'Destination' sections. The 'Network' object is used to define a network or a sub-network by their IP address/Network Mask	As 'Source' and 'Destination' in: <ul style="list-style-type: none"> <li>• All types of Data Transfer Policy rules</li> <li>• Endpoint Discovery rule</li> </ul>
AD User	Available in the 'Source' and 'Destination' sections. The 'AD User' object is used to specify a single user or a group of users.	As 'Source' in all types of Data Transfer Policy rules.
User	Available in the 'Source' and 'Destination' sections. The 'User' object is used to specify a single user or a group of users. <ul style="list-style-type: none"> <li>• After installing the CDDP Endpoint agent, the user logged-on at each endpoint is</li> </ul>	As 'Source' in all types of Data Transfer Policy rules.

Object Type	Description	Application
	<p>shown in the <b>Endpoints</b> interface.</p> <ul style="list-style-type: none"> <li>The user names can be used to specify users when creating 'User' objects.</li> </ul> <p>Rules will only be effective if the user is specified exactly as shown in the 'Endpoints' interface.</p>	
Domain	<p>Available in the 'Source' and 'Destination' sections.</p> <p>The 'Domain' object is used to specify a domain name. It can be used as 'source' or 'destination' when configuring a data transfer control policy.</p>	As 'Source' and 'Destination' in all types of Data Transfer Policy rules.
Computers	<p>Available in the 'Source' section.</p> <p>The 'Computer' object is used to define a single endpoint by specifying its host name.</p> <ul style="list-style-type: none"> <li>After installing the CDDP Endpoint agent, each endpoint is shown as a 'Computer Name' in the <b>Endpoints</b> interface.</li> <li>The 'Computer name' is used to reference the endpoint when creating 'Computer' objects.</li> <li>These are auto-populated when adding / editing a computer object.</li> </ul>	<p>As 'Source' in:</p> <ul style="list-style-type: none"> <li>All types of Data Transfer Policy rules except Mail Rule</li> <li>Endpoint Discovery rule</li> </ul>
Device	<p>Available in the 'Destination' section.</p> <p>The 'Device' object is used to specify USB devices with their name, vendor name and vendor ID.</p> <p>These objects can then be specified as destinations in 'Removable Storage' rules.</p> <p>You must first add USB devices to CDDP by specifying their Vendor and Product ID under 'Devices' in the 'Destination' section. See <b>Add a User Defined USB Device Object</b> for more information on adding USB devices.</p>	As 'Destination' in Removable Storage rule
Endpoint File System	<p>Available in the 'Discovery Target' section.</p> <p>The 'Endpoint File System' object is used to specify file paths on an endpoint for discovering files with sensitive information.</p>	As 'Destination' in Endpoint Discovery Rule
Remote Connections	<p>Available under 'Discovery Target' section.</p> <p>The 'Remote Storage' object is used to specify a remote server, for checking existence of files with sensitive information in it.</p>	As 'Source' in Remote Storage Rule
Information Type	<p>Available in the 'Information Type' section.</p> <p>The 'Information Type' object is used to specify the type of data to which a rule should apply.</p> <p>More details on information types are available in</p>	<p>As 'Information Type' in:</p> <ul style="list-style-type: none"> <li>Web Rule</li> <li>Mail Rule</li> </ul>



Object Type	Description	Application
	the next section, <b>Information Types - An Overview</b> .	<ul style="list-style-type: none"> <li>• Removable Storage Rule</li> <li>• Printer Rule</li> <li>• API Rule</li> <li>• Clipboard Rule</li> <li>• Endpoint Discovery Rule</li> <li>• Remote Storage Rule</li> <li>• Database Discovery Rule</li> </ul>
Database Connections	Available in the 'Discovery Target' section. The 'Database Discovery' object is used to specify a database for the purpose of discovering sensitive data.	As 'Source' in Database Discovery Rule

Admins can also create custom objects and object groups as required. These can also be used in rules. See **User Defined Objects** for more details.

### 5.2.2. Information Types - An Overview

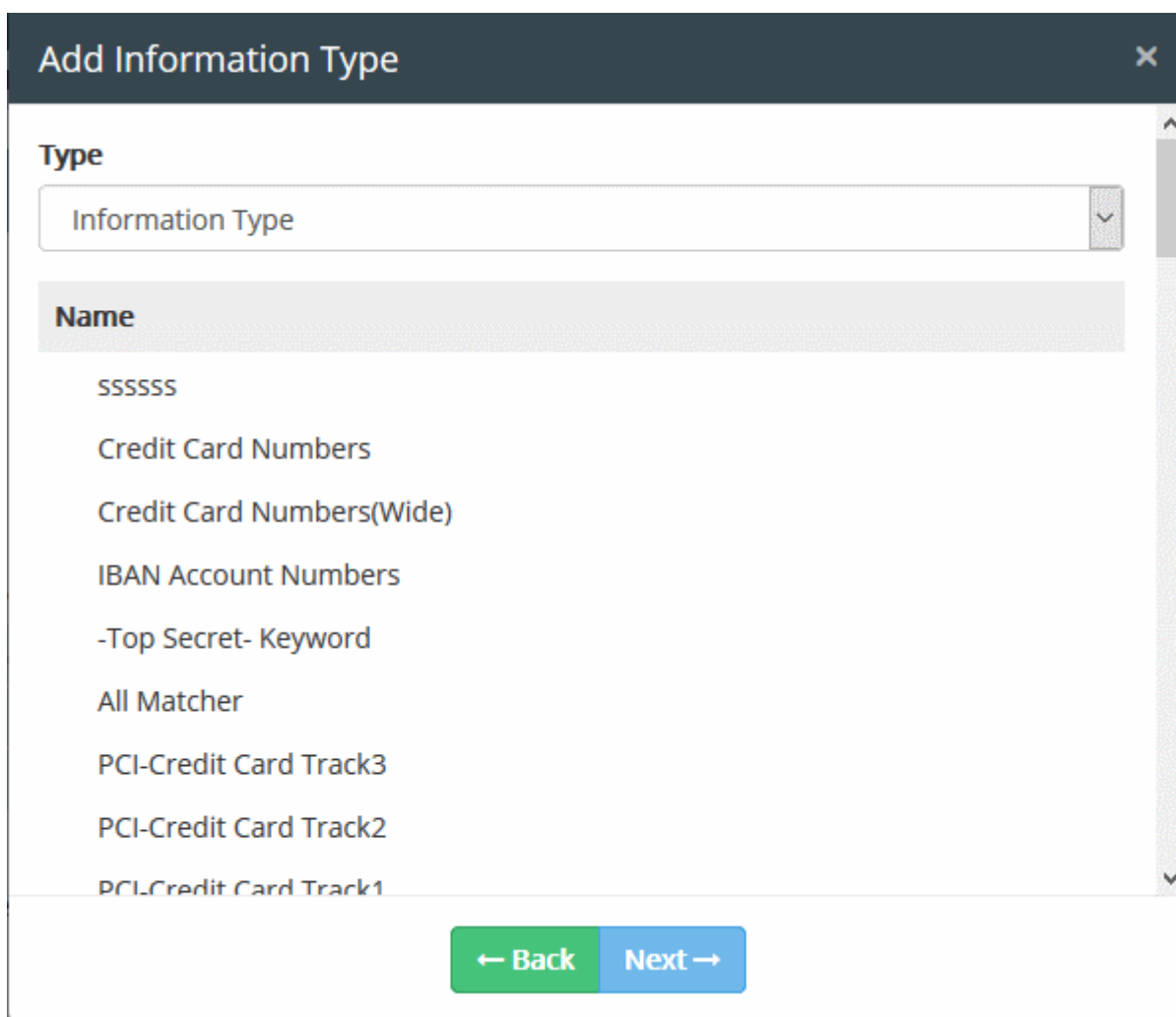
- Click the 'Policy' tab to open the policy interface
- Click the 'Information Type' box on the left
- The section contains two object types – 'Information Type' and 'Information Type Group'

Data loss prevention depends on identifying sensitive information in data at rest and in transit. The 'information type' object in a rule will discover and apply actions to data which matches the information type. Matching information can be allowed, blocked, quarantined, or logged as required.

Information types can also be grouped to form information type groups. CDDP ships with a number of predefined information types and groups that can be used in rules.

The 'Add Information Type' interface lets you choose the type of data you wish to search for in a rule:





**Add Information Type**

Type

Information Type

**Name**

- SSSSSS
- Credit Card Numbers
- Credit Card Numbers(Wide)
- IBAN Account Numbers
- Top Secret- Keyword
- All Matcher
- PCI-Credit Card Track3
- PCI-Credit Card Track2
- PCI-Credit Card Track1

← Back   Next →

Each Information type consists of the following components:

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

Files which match the format/extension + matcher/context can be quarantined, logged, blocked or allowed as required. This is 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 CDDP is shipped with a set of pre-defined Data Formats that are commonly and frequently used. The administrator can add more custom data formats from Matcher > Data Formats interface. See **Manage Data Formats** for more details.

### Extensions

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

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

Comodo CDDP is shipped with a set of pre-defined file extensions that are commonly and frequently used. The administrator can add more custom file extensions from Matcher > File Extension interface. See **ManageFile Extensions** for more details.

### Information Features

'Information Features' are used to refine which files are caught by the rule. There are two types of criteria:

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

#### Matcher

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

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

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

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



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

### Context

The 'Context' is an optional parameter used to specify the minimum extent of data size within which the data matching the 'Matchers' should occur, to consider a file as 'Information Type' object. DLP analysis will return positive only if all the defined Information Features are found within a portion of specified extent in the document. This feature lets you make DLP analysis in a context and drastically decrease false positives in big files. The extent can be specified in terms of number of words, sentences, paragraphs and pages.

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

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

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

Add Information Type

☒ Context
3
Paragraphs

Add Matcher

Matcher Function Name	Threshold
birthdate	2
cc_narrow	2

Add Edit Delete

Cancel
Back Next Save

### Data Transfer Policy Rule

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

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

### Discovery Rule

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

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

#### 5.2.2.1. Predefined Matcher Types

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

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

Feature	Description
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	<p>Identifies occurrences of credit card number in data stream or file, without spaces before or after the credit card number in the stream.</p> <p>For example, 'sometext4111 1111 1111 1111' and '4111 1111 1111 1111sometext'</p> <p>If you use credit card number with threshold 5 it will match any document with 5 or more credit card numbers in it.</p>
Credit Card Number (Wide)	<p>Identifies occurrences of credit card number in data stream or file, with spaces before and after the credit card number in the stream.</p> <p>For example, 'sometext 4111 1111 1111 1111' and '4111 1111 1111 1111 sometext'</p> <p>If you use credit card number (Wide) with threshold 5 it will match any document with 5 or more credit card numbers in it.</p>
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).
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.

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

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

### 5.2.2.2. Predefined Information Types

Comodo Dome Data Protection ships with a series of pre-defined 'Information Types' for use in 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 CDDP under two categories:

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

#### Compliance

CDDP 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. CDDP allows the institution to protect customer's confidential information and meet the requirements of HIPAA with following matchers.

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



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

## Finance

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

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

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

Information Type	Description	Matchers & Threshold Values	Context	
Sub-Category: Pricing				
Pricing Information	Consists of Keyword Group 'Pricing information'	Keyword Group - Pricing informations	5	4 Paragraphs
Sub-Category: SOX (Sarbanes-Oxley Act of 2002 (public company accounting reform))				
Sub-Category: SOX > 10K Forms				
10K Forms Cover Page	Consists of Keyword Group '10K Form Cover Page Keywords'	Keyword Group - 10K Form Cover Page Keywords	6	6 Paragraphs
10K Forms Financial Statements	Consists of Keyword Group '10K Form Financial Statement Keywords'	Keyword Group - 10K Form Financial Statement Keywords	3	6 Sentences
10K Forms Selected Financial Data	Consists of Keyword Group '10K Form Financial Data Keywords'	Keyword Group - 10K Form Financial Data Keywords	3	2 Paragraphs
10K Forms Stock Performance Graph	Consists of Keyword Group '10K Form Performance Graph Keywords'	Keyword Group - 10K Form Performance Graph Keywords	2	5 Sentences
10K Forms Table of Contents Page	Consists of Keyword Group '10K Form Table of Contents Keywords'	Keyword Group - 10K Form Table of Contents Keywords	12	2 Pages
Sub-Category: SOX > 10Q Forms				
10Q Forms Consolidated Balance Sheets	Consists of Keyword Group '10Q Form Consolidated Balance Sheets Keywords'	Keyword Group - 10Q Form Consolidated Balance Sheets Keywords	6	6 Paragraphs
10Q Forms Cover Page	Consists of Keyword Group '10Q Form Cover Page Keywords'	Keyword Group - 10Q Form Cover Page Keywords	5	6 Paragraphs
10Q Forms Other Information	Consists of Keyword Group '10Q Form Other Information Keywords'	Keyword Group - 10Q Form Other Information Keywords	4	8 Paragraphs
10Q Forms Table of Contents Page	Consists of Keyword Group '10Q Form Table of Contents Keywords'	Keyword Group - 10Q Form Table of Contents Keywords	5	2 Pages

## Network Security Information

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

Information Type	Description	Matchers & Threshold Values		Context
IP with Network	Consists of IP Addresses	IP Address	2	5 Sentences

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

### Personal Information

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

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

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

### Sensitive Documents

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

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

Information Type	Description	Matchers & Threshold Values	Context
<b>Sub-Category: Strategic Business Document</b>			
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 without space before and/or after the number.	Credit Card Number	1 Not Specified
Credit Card Numbers (Wide)	Identifies documents containing at least one credit card number with spaces both before and after the number.	Credit Card Number	1 Not Specified
IBAN Account Numbers	Identifies documents containing at least one Bank Account number in IBAN format.	IBAN Account Number	1 Not Specified

### 5.2.2.3. Predefined Information Type Groups

Comodo Dome Data Protection ships with a series of pre-defined 'Information Types Groups' for use in rules. Information types contained in each group 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 Groups available in CDDP.

#### HIPAA

The Information Types in the 'HIPAA' group HIPAA (Health Insurance Portability and Accountability Act). The purpose of Act is to protect billing and the confidential medical records of patients. CDDP 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	Consists of Credit Card	Credit Card Number	1 3 Sentences

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



Information Type	Description	Matchers & Threshold Values		Context
	Names	Drug Names		

**GLBA**

The Information Types in the 'GLBA' group meet requirements of Gramm-Leach-Bliley Act (GLB Act or GLBA) . The purpose of Act is to control the ways that financial institutions deal with the private information of individuals in the US. CDDP allows the institution to protect customer's confidential information and meet the requirements of GLBA with following matchers.

Information Type	Description	Matchers & Threshold Values		Context
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'	Keyword Group - Names	1	3 Sentences
		Keyword Group - Sensitive Drug Names	1	

Information Type	Description	Matchers & Threshold Values	Context
	Names'		

## PCI

The Information Types in the 'PCI' group contains information related to PCI credit cards. CDDP allows the institution to protect customer's credit card information from being leaked to external, using the following matchers.

Information Type	Description	Matchers & Threshold Values	Context	Information Type
PCI-Credit Card	Consists of Credit Card Numbers	Credit Card Number	1	Not Specified
<b>Sub-Category: PCI &gt; PCI Credit Card Tracks</b>				
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

### 5.2.3. User Defined Objects

- Each rule is composed of five 'Objects' - the Channel or Name of the rule, Source, Destination, Information type and Action.
- Comodo Dome Data Protection ships with several predefined objects and allows you to create custom objects.
  - Rule types and pre-defined objects are explained in the sections **Rule Types** and **Objects Types**.
- This section explains on how to create 'User Defined Objects'.

Click the links below for more information.

- [Add a User Defined Network object](#)
- [Add a User Defined Computer Object](#)
- [Add a User Defined Endpoint Object](#)
- [Add a User Defined Information Type](#)
- [Add a User Defined Information Type Group](#)
- [Add a User Defined Domain Name](#)
- [Add a User Defined Application Name](#)
- [Add a User Defined User Object](#)
- [Add a User Defined Active Directory Users Object](#)
- [Add USB Devices Object](#)
- [Add a User Defined File System Directory](#)
- [Add a User Defined Remote Storage](#)

- **Add a Database Discovery Object**

### 5.2.3.1. Add a User Defined Network Object

- Network objects consist of an IP address and mask
- These objects can be used as the source in endpoint discovery rules, and in all types of data transfer policy rules.

#### To create a new network object

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

The 'Network Objects' screen will be displayed:

NETWORK OBJECTS			<a href="#">+ Add</a>	<a href="#">Edit</a>	<a href="#">Delete</a>
Name	IP Address	Subnet			
All Sources	0.0.0.0	0.0.0.0			
10.0.0.0/24	10.0.0.0	255.255.255.0			
10.0.0.0/8	10.0.0.0	255.0.0.0			
192.168.0.0/16	192.168.0.0	255.255.0.0			
172.16.0.0/16	172.16.0.0	255.255.0.0			
Sales Team Network	192.168.111.110	255.255.255.0			

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

Add Network

**Name**

**IP Address**

**IP Mask**

✕ Cancel
Save

3. Enter the parameters:

- Name - Enter a name shortly describing the network object
- IP Address - Enter the start IP address of the network  
Example: 192.168.1.25
- IP Mask - Enter the IP Net Mask  
Example : 255.255.255.0

4. Click 'Save'.

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

NETWORK OBJECTS			+ Add	Edit	Delete
Name	IP Address	Subnet			
All Sources	0.0.0.0	0.0.0.0			
10.0.0.0/24	10.0.0.0	255.255.255.0			
10.0.0.0/8	10.0.0.0	255.0.0.0			
192.168.0.0/16	192.168.0.0	255.255.0.0			
172.16.0.0/16	172.16.0.0	255.255.0.0			
Sales Team Network	192.168.111.110	255.255.255.0			
Purchase	192.168.111.111	255.255.255.0			

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

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

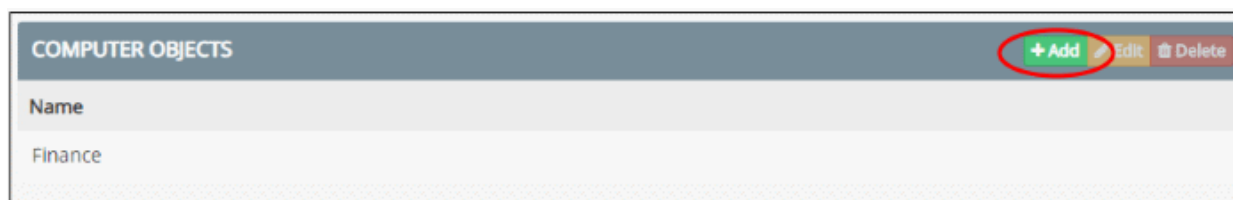
### 5.2.3.2. Add a User Defined Computer Object

- Computer objects consist of an endpoint which has been added to CDDP.
  - You must install the endpoint agent on a computer for it to become available as a potential object. See <https://help.comodo.com/topic-283-1-598-7040-Getting-Started.html> if you need help with this.
- Computer objects can be added as a source in an endpoint discovery rule. They can also be used in all data transfer policy rules except mail rules.

#### To create a Computer object

1. Click the 'Policy' tab then 'Source' > 'Computers'

The 'Computer Objects' screen will be displayed:



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

**Add Computer**

Name

Show 10 entries Search:

Name

DESKTOP-TTPO9PR

DESKTOP-HI950BN

Showing 1 to 2 of 2 entries Previous 1 Next

Cancel Save

3. The dialog shows all endpoints that have the agent installed.
  - Name - Enter a label to identify the computer
  - Search - Enter a computer name to look for a specific endpoint. Clear the search field to view all endpoints.
  - Select the endpoint from the list.
4. Click 'Save'.

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

**COMPUTER OBJECTS** + Add Edit Delete

Name
Finance
Purchase Dept. Computer

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

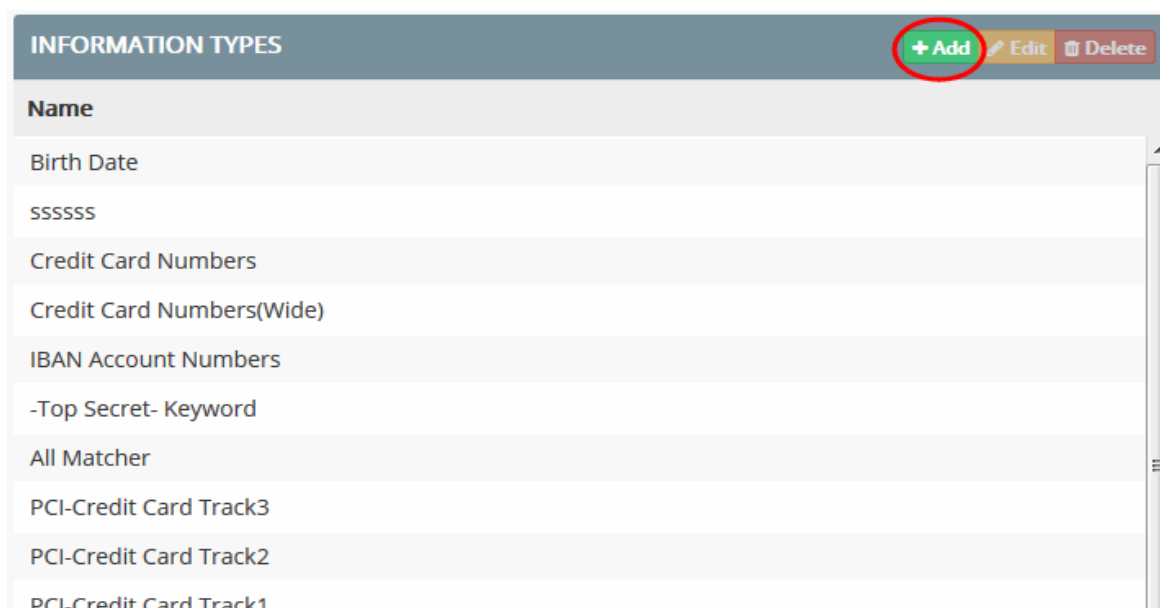
### 5.2.3.3. Add a User Defined Information Type

- CDDP ships with a selection of pre-defined 'Information Types'. Information types are items like birth-dates, credit numbers and so forth.
- You can also create custom information types.
- Information types can be used in the following rules:
  - Web rule
  - Mail rule
  - Removable storage rule
  - Printer rule
  - API rule
  - Clipboard rule
  - Endpoint Discovery rule
  - Remote storage discovery rule
  - Database discovery rule

#### To define a custom information type

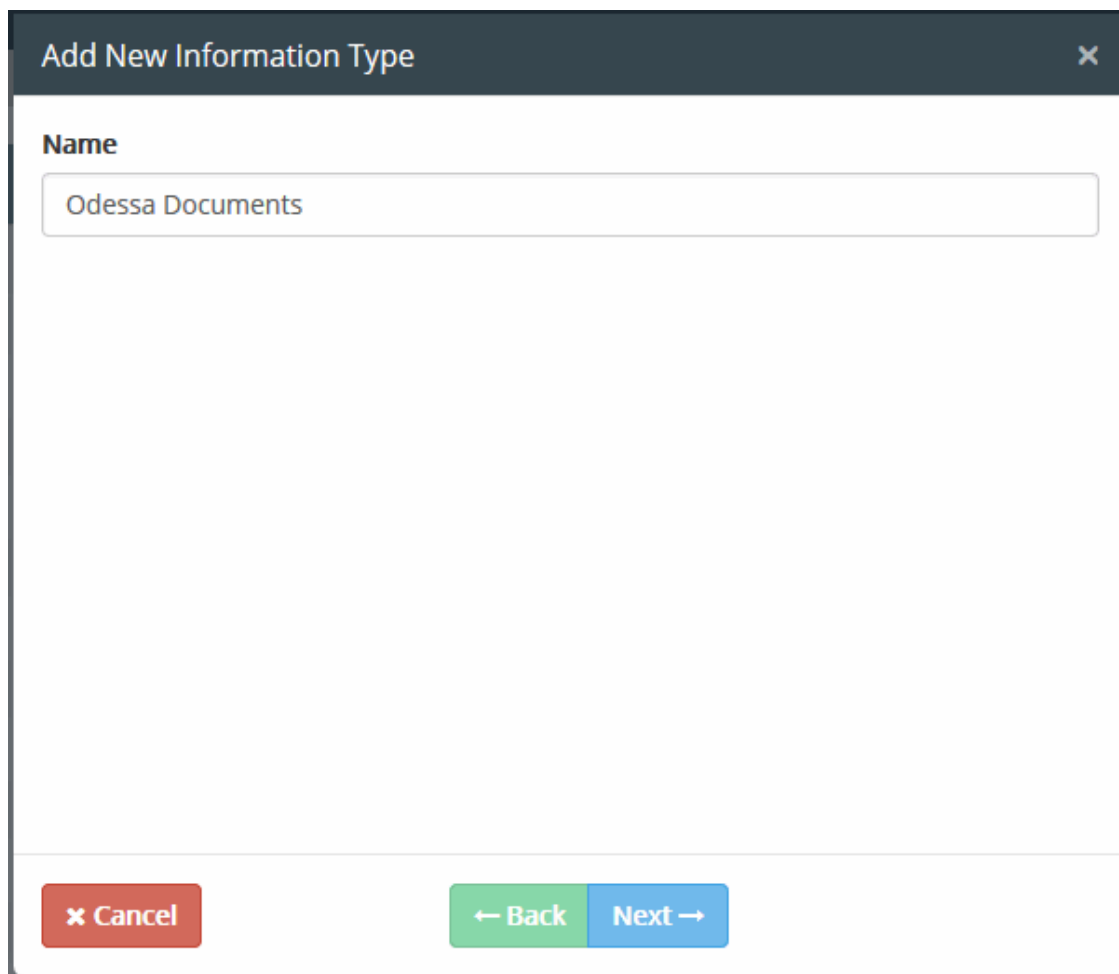
1. Click the 'Policy' tab at the top and then 'Information Type' under 'Information Type' section.

The 'Information Types' screen will be displayed:



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

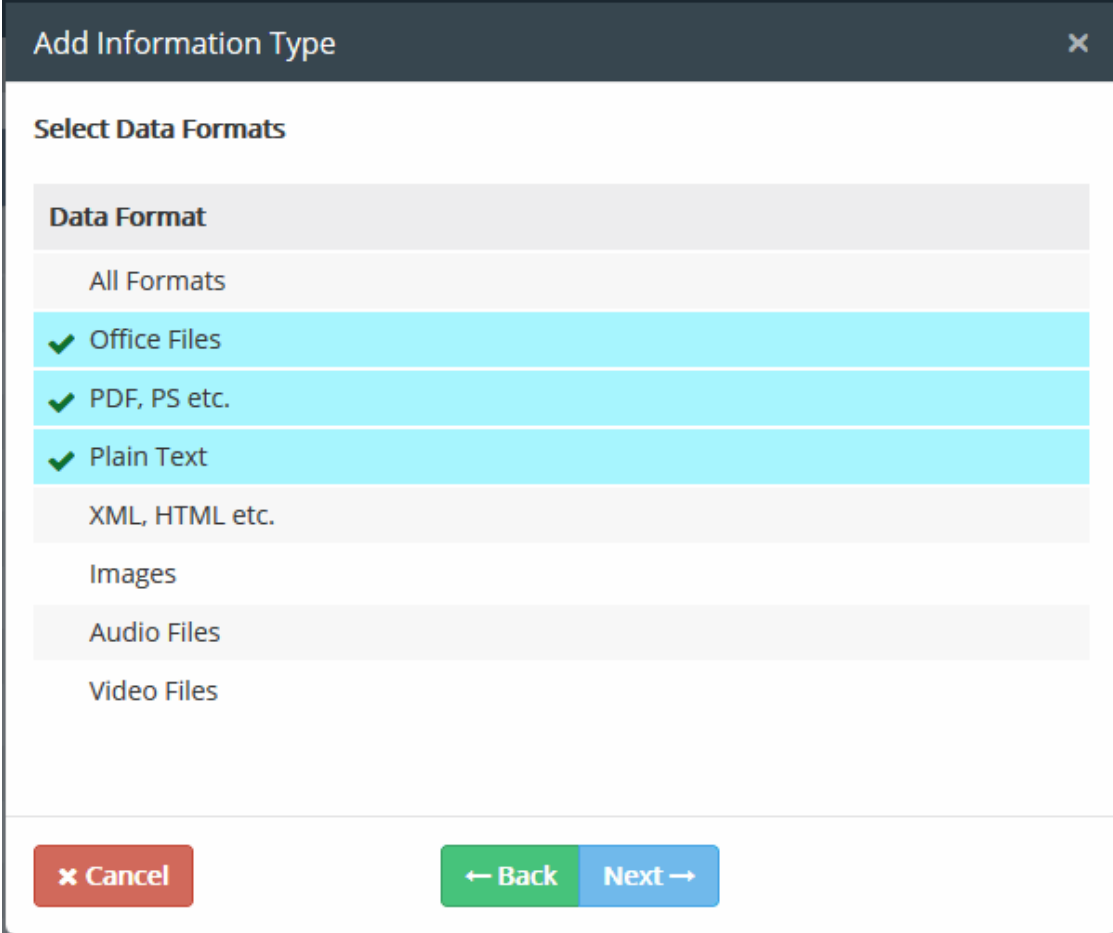




The screenshot shows a dialog box titled "Add New Information Type". It features a close button (X) in the top right corner. Below the title bar, the label "Name" is positioned above a text input field. The input field contains the text "Odessa Documents". At the bottom of the dialog, there are three buttons: a red "Cancel" button, a green "Back" button with a left arrow, and a blue "Next" button with a right arrow.

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

The Select Data Formats dialog will be displayed:



**Add Information Type**

**Select Data Formats**

Data Format
All Formats
✓ Office Files
✓ PDF, PS etc.
✓ Plain Text
XML, HTML etc.
Images
Audio Files
Video Files

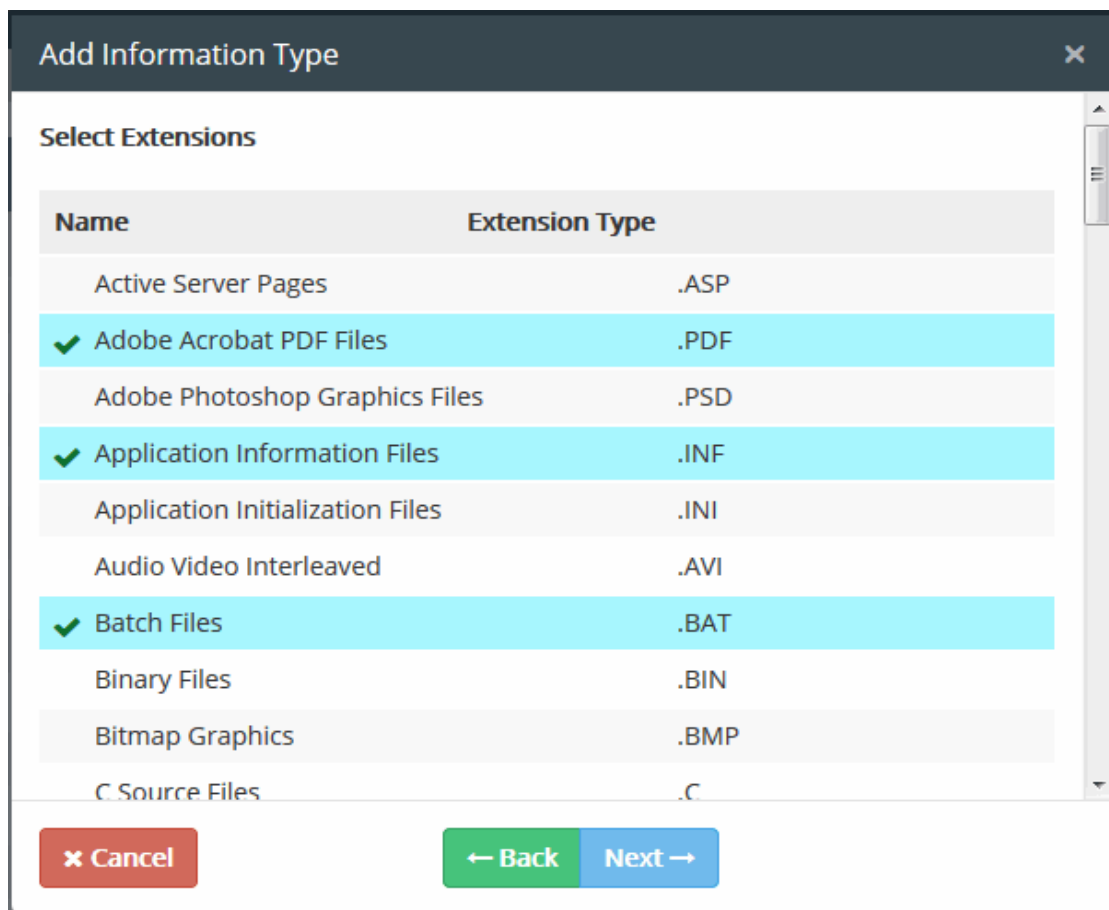
✕ Cancel   ← Back   Next →

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

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

5. Click 'Next'

The Select Extensions dialog will be displayed:

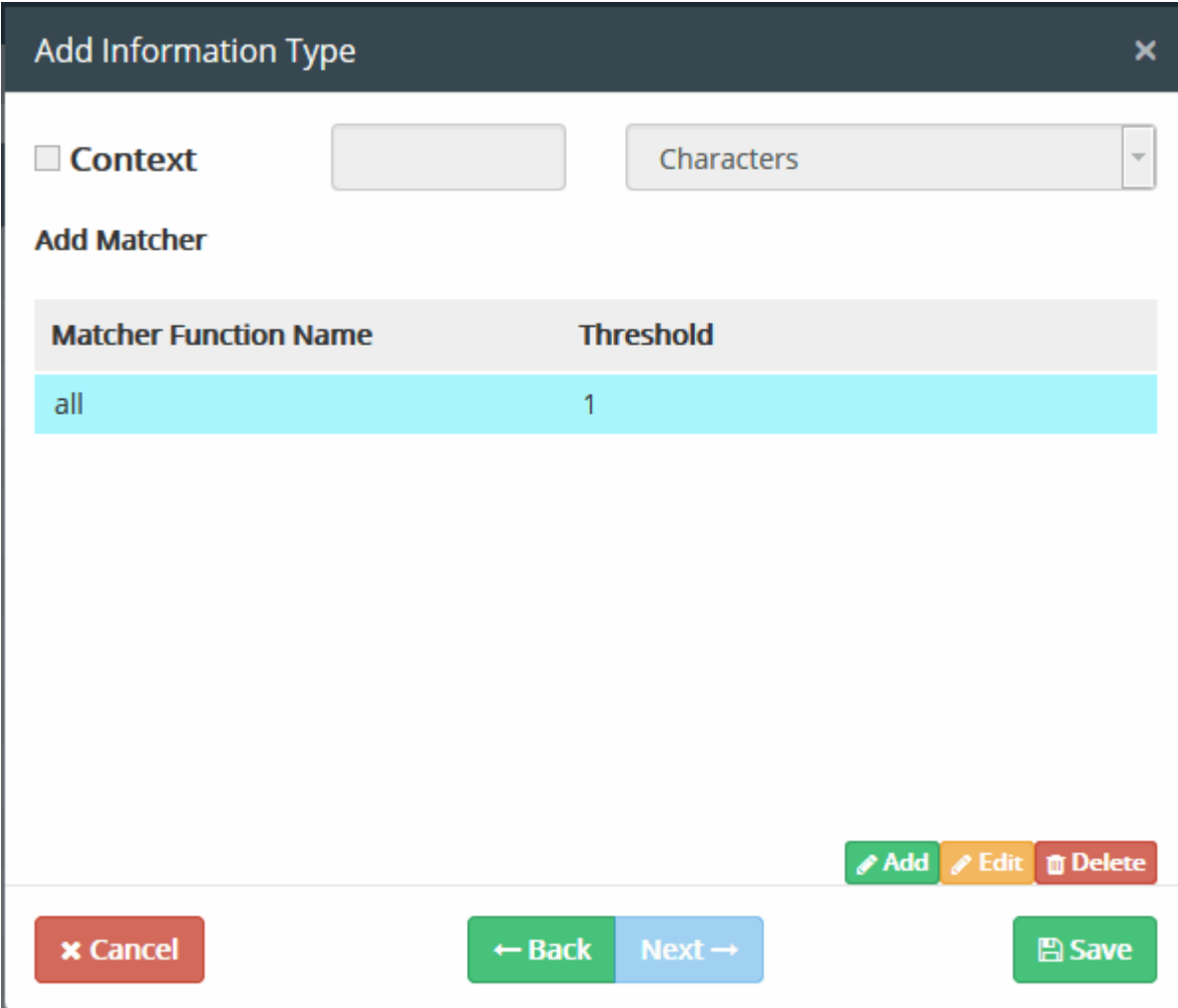


6. Select the extension type(s) to be included in the information type object from the list. To remove an extension, just deselect it.

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

7. Click 'Next'

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



**Add Information Type**

☐ **Context**

Characters

**Add Matcher**

Matcher Function Name	Threshold
all	1

Add Edit Delete

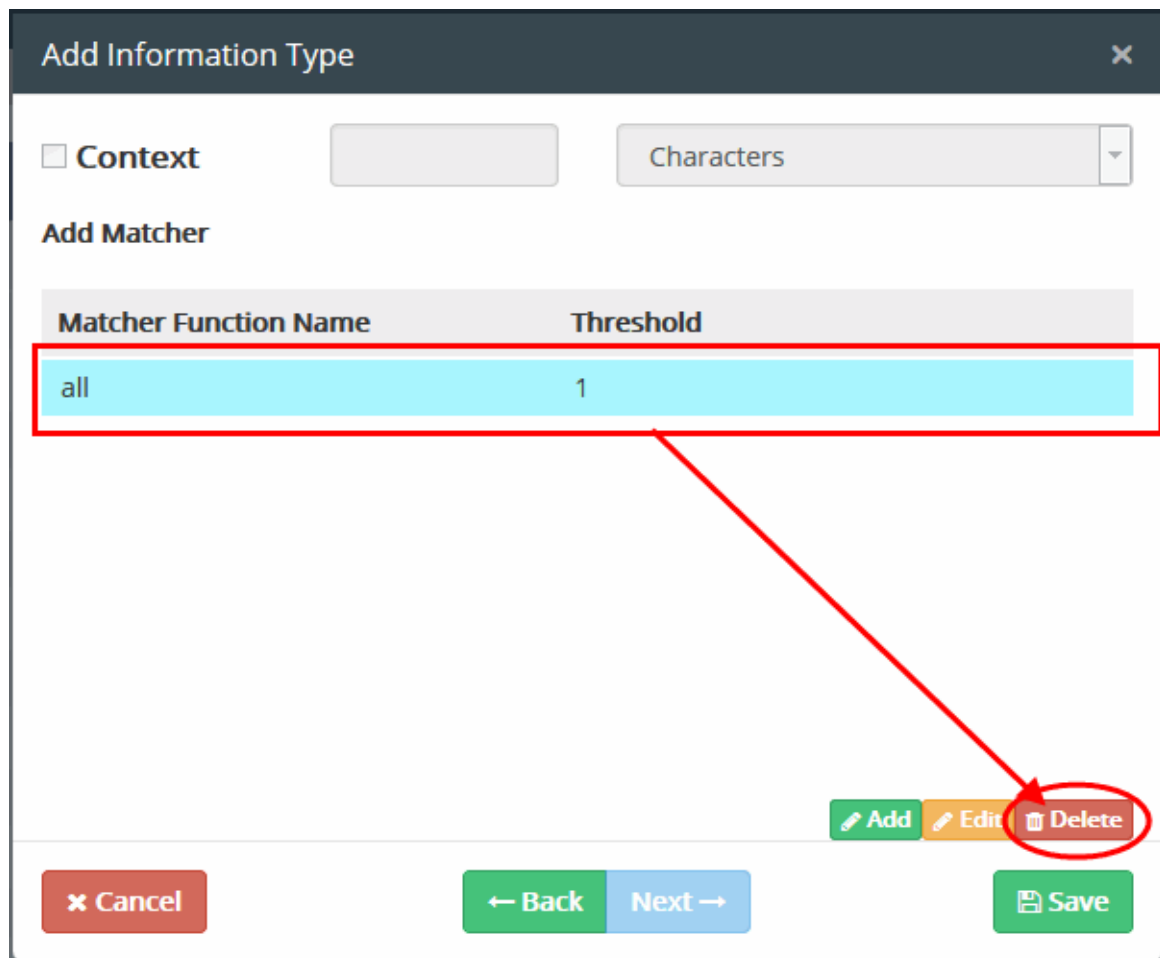
Cancel Back Next Save

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

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

#### Step 1 – Configuring the matcher

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



**Add Information Type**

☐ **Context**  Characters

**Add Matcher**

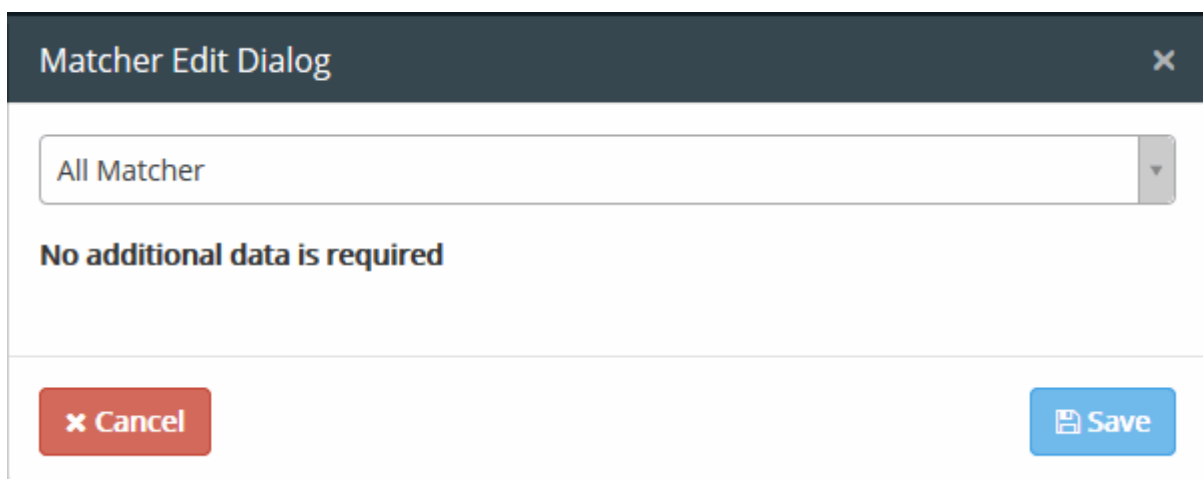
Matcher Function Name	Threshold
all	1

Add Edit Delete

Cancel ← Back Next → Save

- Next, click the 'Add' button

The 'Matcher Edit Dialog' will be displayed:



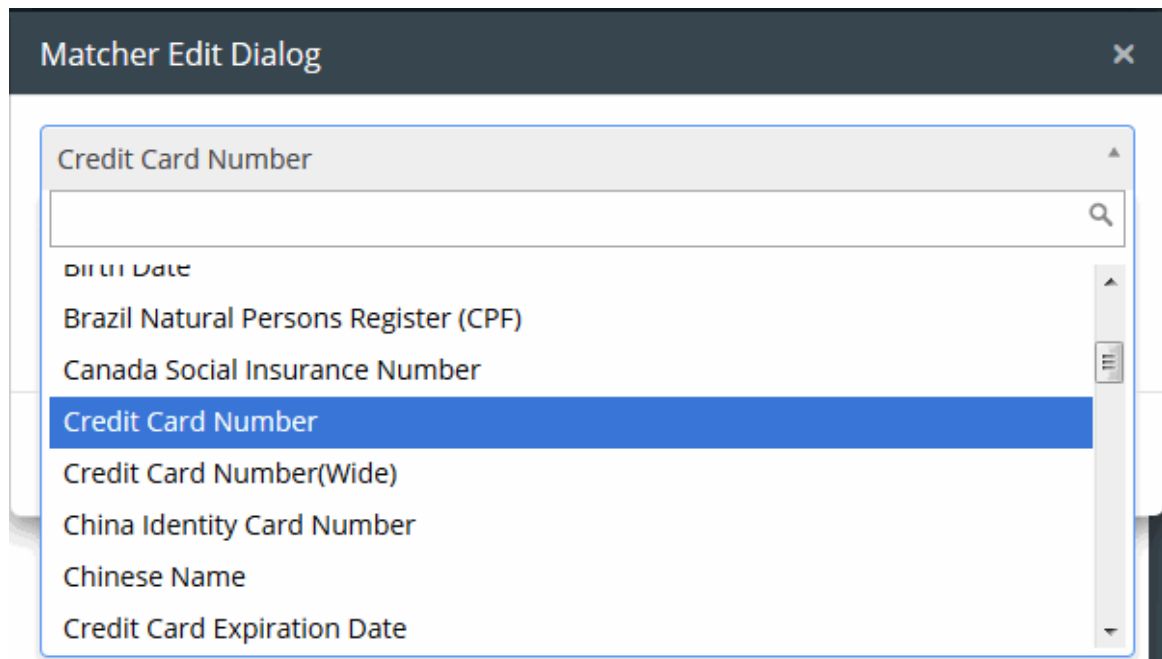
**Matcher Edit Dialog**

All Matcher

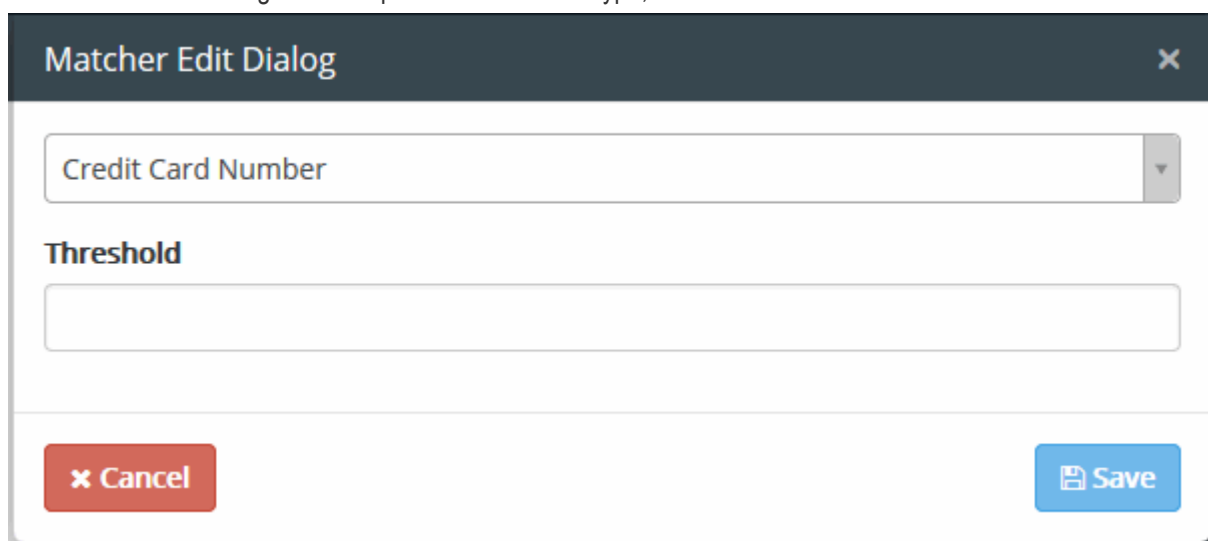
**No additional data is required**

Cancel Save

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



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



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

Add Information Type

☐ Context

Characters

Add Matcher

Matcher Function Name	Threshold
cc_narrow	2
cc_wide	2
birthdate	2
gdate	2

Add

Edit

Delete

✕ Cancel

← Back

Next →

Save

You can edit or remove any matcher at any time.

#### To edit a matcher

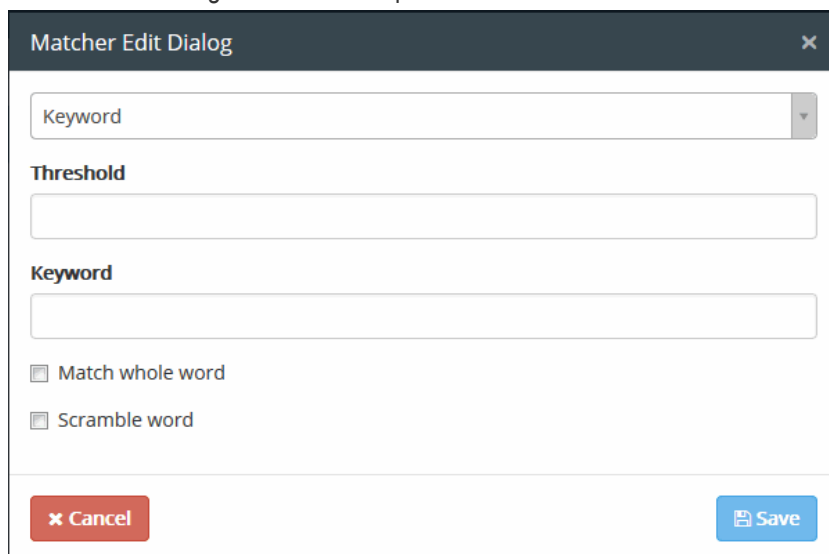
- Select the matcher from the list, click 'Edit' and modify the details from the 'Matcher Edit Dialog'
- Click Save for your changes to take effect

#### To remove a matcher

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



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



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

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

### Step 2 - Specify the Context parameter (Optional)

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

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

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

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

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

#### 5.2.3.4. Add a User Defined Information Type Group

- CDDP ships with three, pre-defined information type groups. Information type groups are a collection of one or more information types.
- You can also create custom information types.
- Information type groups can be added to the following rules:
  - Web rule
  - Mail rule
  - Removable storage rule
  - Printer rule
  - API rule
  - Clipboard rule
  - Endpoint Discovery rule
  - Remote storage discovery rule
  - Database discovery rule

##### To define a custom information type group

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

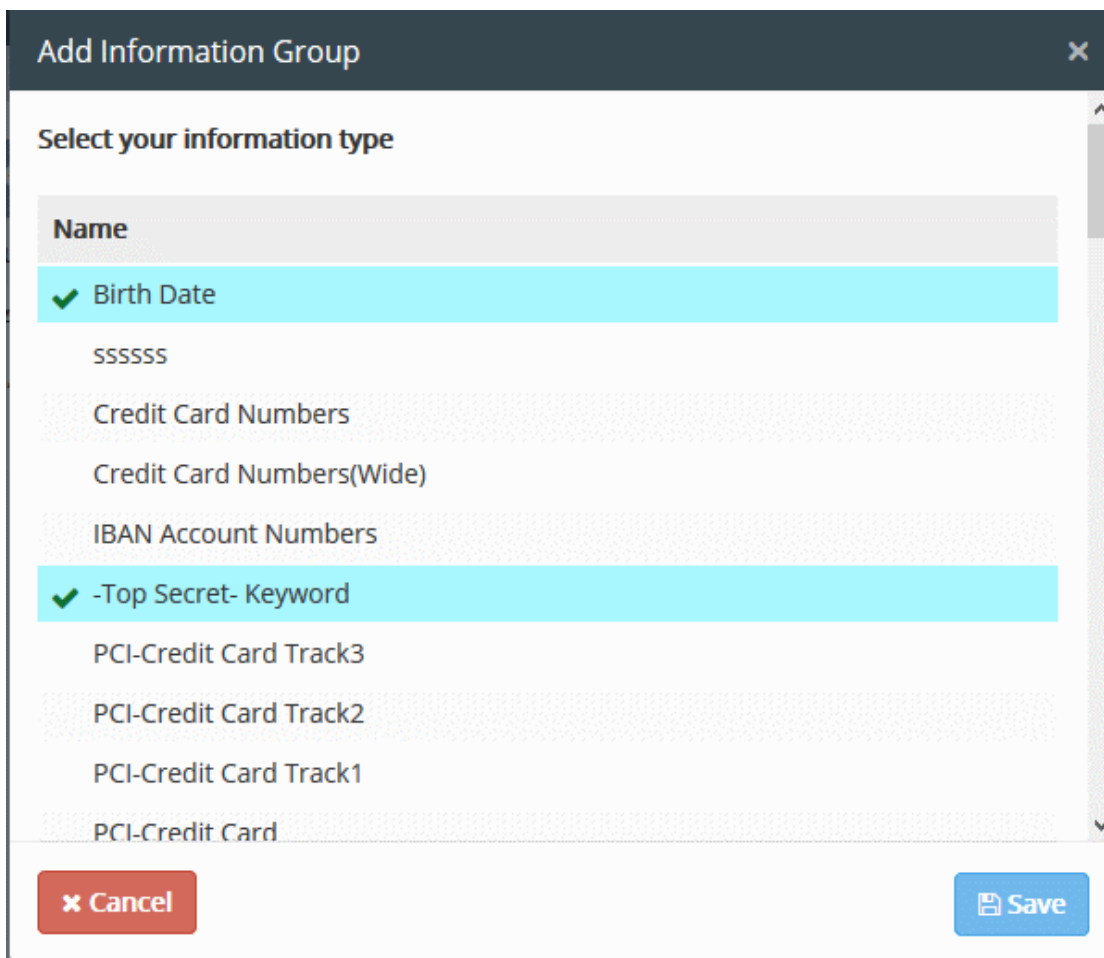
The 'Information Group Objects' screen will be displayed.

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

The screenshot shows the 'INFORMATION GROUP OBJECTS' interface. At the top right, there are buttons for '+ Add', 'Edit', and 'Delete'. A red circle highlights the '+ Add' button, and a red arrow points from it to the 'Add Information Group' dialog box. The dialog box has a title bar 'Add Information Group' with a close button. Inside, there is a section 'Enter Group Name' with a text input field containing 'Custom Information Type Group'. At the bottom, there are three buttons: 'Cancel' (red), 'Back' (green), and 'Next' (blue). The background shows a table with columns 'Group Name' and 'Item Count', listing HIPAA (12), GLBA, and PCI.

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

The 'Select Your Information Type' dialog will be displayed, with a list of both pre-defined and user defined information types added to CDDP.



**Add Information Group**

Select your information type

- Name
- ✓ Birth Date
- SSSSSS
- Credit Card Numbers
- Credit Card Numbers(Wide)
- IBAN Account Numbers
- ✓ -Top Secret- Keyword
- PCI-Credit Card Track3
- PCI-Credit Card Track2
- PCI-Credit Card Track1
- PCI-Credit Card

✕ Cancel Save

- Select the Information Types to be included in the group and click 'Save'.

INFORMATION GROUP OBJECTS		<a href="#">+ Add</a>	<a href="#">Edit</a>	<a href="#">Delete</a>
Group Name	Item Count			
HIPAA	12			
GLBA	10			
PCI	4			
Custom Information Type Group	5			

The new group will be added to the list and will be available for selection while creating a rule.

- To edit a group, select it and click 'Edit'
- To remove a group, select it and click 'Delete'

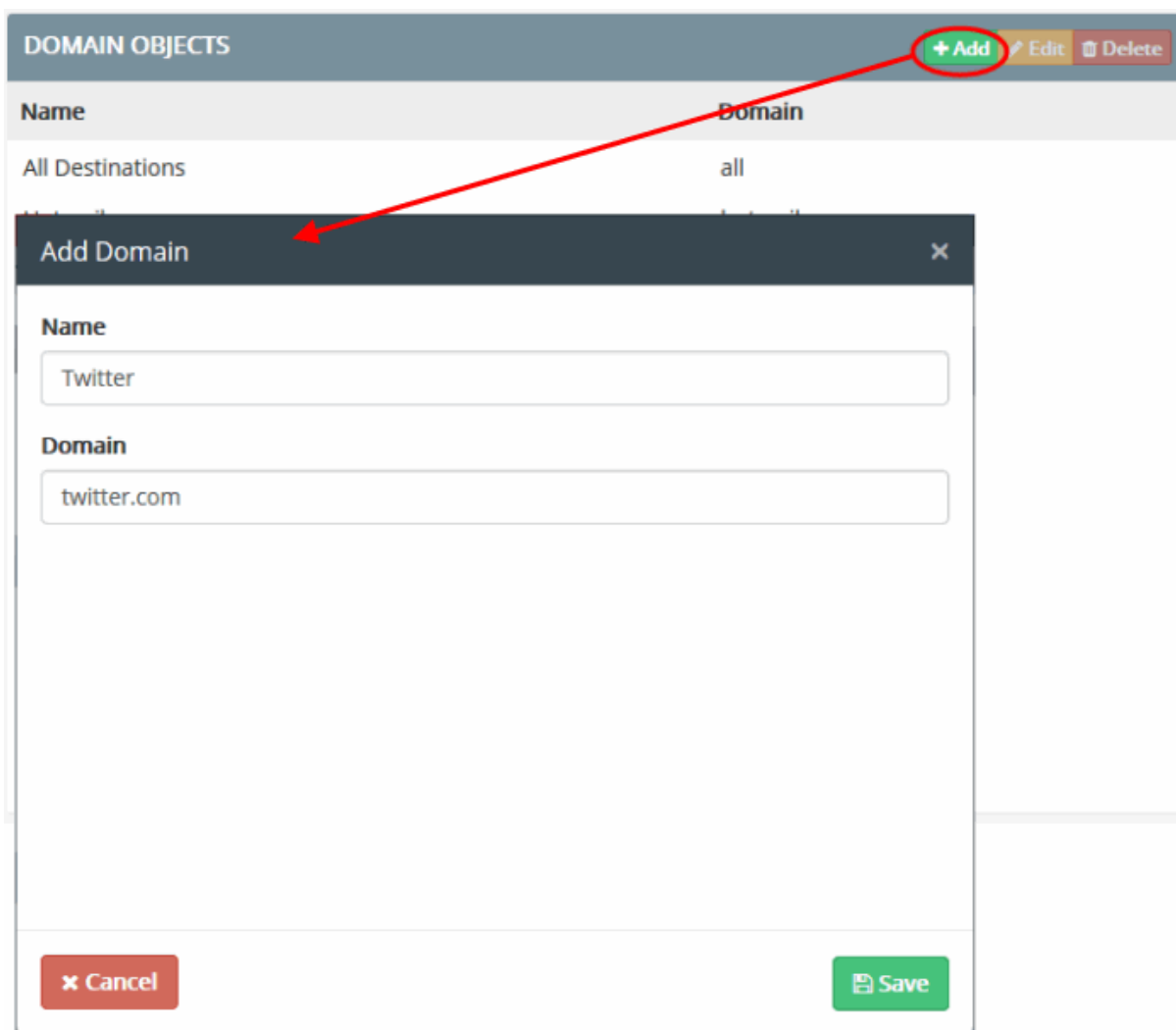
### 5.2.3.5. Add a User Defined Domain Object

- CDDP ships with a number of pre-defined domain objects, including commonly used email domains.
- These objects can be specified as the destination component in a **web rule** or **email rule**.
- You can also create custom domain objects

#### To add a new domain name

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

The 'Domain Objects' screen will be displayed:



2. Click 'Add' at top-right. The 'Add Network' dialog will appear.
3. Enter the parameters:
  - Name - Enter a descriptive name for the domain object
  - Domain - Enter the domain name or the full URL to be added
4. Click 'Save'.

The new user defined domain object will be listed in the 'Domain Objects' screen.

DOMAIN OBJECTS		<a href="#">+ Add</a> <a href="#">Edit</a> <a href="#">Delete</a>
Name	Domain	
All Destinations	all	
Hotmail	hotmail.com	
Outlook	outlook.com	
Live	live.com	
Msn	msn.com	
Gmail	gmail.com	
Google	google.com	
Yahoo	yahoo.com	
Yandex-1	yandex.ru	
Yandex-2	yandex.com	
Facebook	facebook.com	
Microsoft	microsoft.com	
Mail has external BCC	hasBCC	
Twitter	twitter.com	

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

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

#### 5.2.3.6. Add a User Defined Application Object

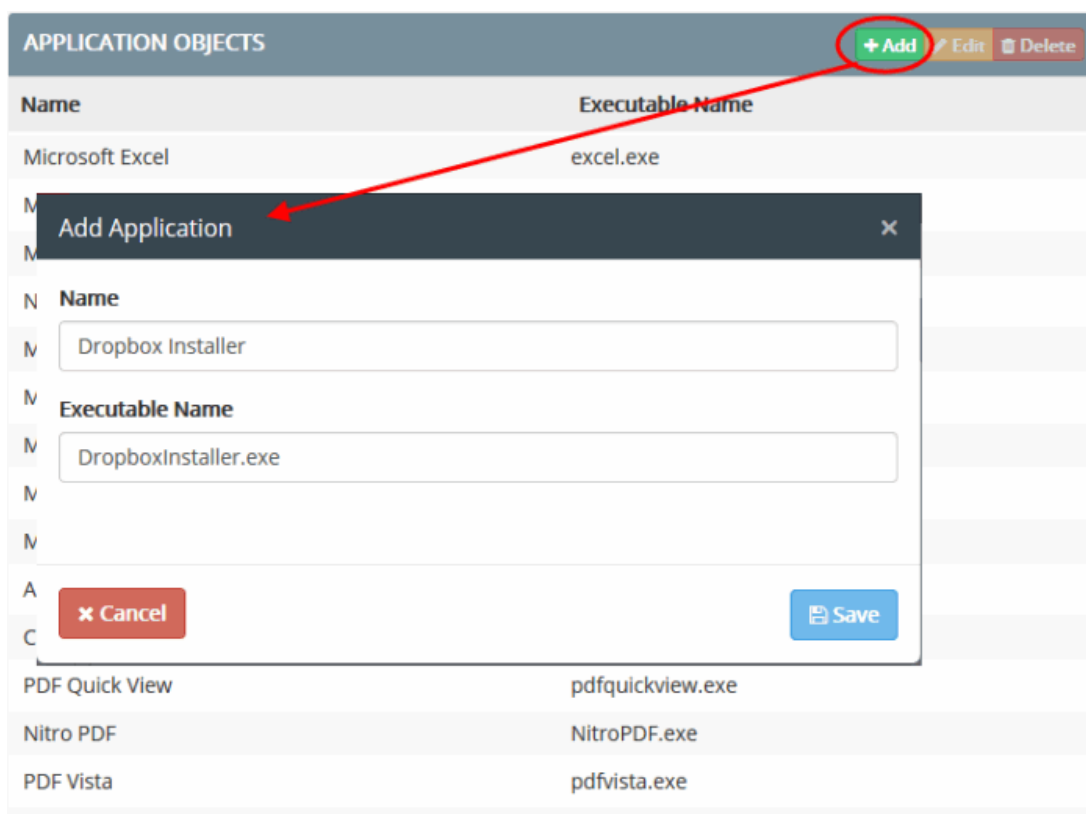
- CDDP ships with a number of pre-defined application objects, including objects for commonly used browsers, Microsoft Office applications and PDF viewers.
- These applications can be used as the destination component in a **Screenshot rule**.
- You can also add custom application names for use in screenshot rules.

##### To add a new Application object

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

The 'Application Objects' screen will be displayed:

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



3. Enter the parameters:

- Name - Enter a descriptive name for the application
- Executable Name - Enter the file name of the application executable of the program, with the file extension.

4. Click 'Save'.

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

APPLICATION OBJECTS		+ Add Edit Delete	
Name	Executable Name		
Microsoft Excel	excel.exe		
Microsoft Access	msaccess.exe		
Microsoft Publisher	mspub.exe		
Notepad	notepad.exe		
Microsoft PowerPoint	powerpnt.exe		
Microsoft Outlook	outlook.exe		
Microsoft OneNote-1	onenote.exe		
Microsoft OneNote-2	onenotem.exe		
Microsoft Word	winword.exe		
Acrobat Reader	AcroRd32.exe		
Cool PDF	coolpdf.exe		
PDF Quick View	pdfquickview.exe		
Nitro PDF	NitroPDF.exe		
PDF Vista	pdfvista.exe		
Nitro PDF 2	nitropdfreader.exe		
Dropbox Installer	DropboxInstaller.exe		

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

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

### 5.2.3.7. Add a User Defined USB Device Object

- USB devices can be added as destinations in 'Removable Storage rules'. This lets you control the transfer of data from source endpoints to USB devices.
- This object type is also used in 'USB Device Access' rules.

#### To add a new USB Device object

1. Click the 'Policy' tab then 'Device' in the 'Destination' section

The 'Device Objects' screen will open.

2. Click 'Add' at top-right to open the 'Add Device' dialog:

The screenshot shows the 'DEVICE OBJECTS' interface. At the top, there are buttons for '+ Add', 'Edit', and 'Delete'. A red circle highlights the '+ Add' button, and a red arrow points from it to the 'Add Device' dialog box. The dialog box has a title bar 'Add Device' and a close button 'X'. It contains the following fields: 'Name' (text input), 'Description' (text input), 'Device Type' (dropdown menu with 'VID/PID' selected), and a table with columns 'Vendor Id' and 'Product Id'. The table is currently empty, showing 'No data available in table'. At the bottom of the dialog, there are 'Cancel' and 'Save' buttons. The background shows a table with columns 'Type', 'Device Name', and 'Description', with one row visible: 'All Usb Devices'.

3. Enter the parameters:
  - Name – Enter a name for the USB device
  - Description - Enter a name which briefly describes the device object
  - Device Type – Select Vendor ID / Product ID or Serial Number of the device.

#### To add device by vendor / product ID

- Select 'VID/PID' from the 'Device Type' drop-down
- Click 'Add'



Description

Device Type

VID/PID

Vendor Id

No data

Device PID/VID

Vendor Id

Product Id

+ Add Edit Delete

Cancel Save

- Vendor ID - Enter the unique identification number assigned to the company that manufactures the device.
- Product ID – Enter the identification number assigned to the USB device by the company.
- Click 'Save' in the 'Device PID/VID' dialog

Add Device

Name

HR Department

Description

USB device for HR

Device Type

VID/PID

+ Add Edit Delete

Vendor Id

8564

Product Id

1000

Cancel Save

- Repeat the process to add more devices
- To edit the device, select it and click 'Edit' and update the details
- To remove a device, select it and click 'Delete'

See **Identifying Vendor ID** for explanation on finding the vendor / product ID and serial number of the device.

4. Click 'Save' in the 'Add Device' dialog

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

DEVICE OBJECTS			<a href="#">+ Add</a> <a href="#">Edit</a> <a href="#">Delete</a>
Type	Device Name	Description	
All	All Usb Devices	all	
VID/PID	sari kingston		
VID/PID	turkuaz toshiba		
Serial Number	gri toshiba serial		
VID/PID	jet	USB	
VID/PID	Check USB Device	test	
Serial Number	Stores	for stores	
VID/PID	HR Department	USB device for HR	

### To add device by serial number

- Select 'Serial Number' from the 'Device Type' drop-down
- Click 'Add'

The 'Add Device' dialog box is shown with the following fields:

- Name:** Security Department
- Description:** USB devices in security department
- Device Type:** Serial Number (selected)

The '+ Add' button is circled in red. A red arrow points from this button to the 'Device Serial Number' dialog box. The 'Device Serial Number' dialog box contains:

- A text input field with the placeholder 'Enter a valid serial number'.
- '+' and '-' buttons for adding or removing serial numbers.
- 'Cancel' and 'Save' buttons.

- Enter a valid serial number of the device and click the '+' button
- Repeat the process to add more serial numbers
- To remove a serial number from the list, select it and click the '-' button

- Click 'Save' in the 'Device Serial Number' dialog

**Add Device**

Name  
Security Department

Description  
USB devices in security department

Device Type  
Serial Number

+ Add Edit Delete

Serial Numbers

001A92053B6ABB4131340023 002B92063B6AAA4131360032 ...

Cancel Save

- Repeat the process to add more devices
- To edit the device, select it and click 'Edit' and update the details
- To remove a device, select it and click 'Delete'

See **Identifying Vendor ID** for explanation on finding the vendor / product ID and serial number of the device.

- Click 'Save' in the 'Add Device' dialog

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

DEVICE OBJECTS			+ Add Edit Delete
Type	Device Name	Description	
All	All Usb Devices	all	
VID/PID	sari kingston		
VID/PID	turkuaz toshiba		
Serial Number	gri toshiba serial		
VID/PID	Jet	USB	
VID/PID	Check USB Device	test	
Serial Number	Stores	for stores	
VID/PID	HR Department	USB device for HR	
Serial Number	Security Department	USB devices in security department	

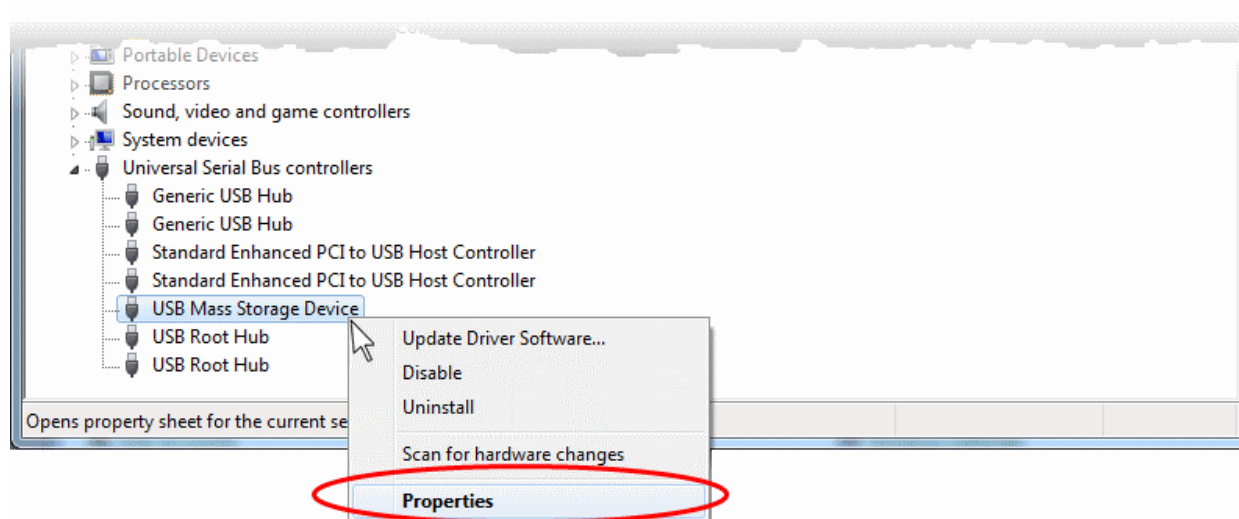
- To edit the details of a device object, select it, click 'Edit' and modify the details as explained above.
- To remove a device object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

### Identifying Vendor ID / Product ID and serial number of a USB Device

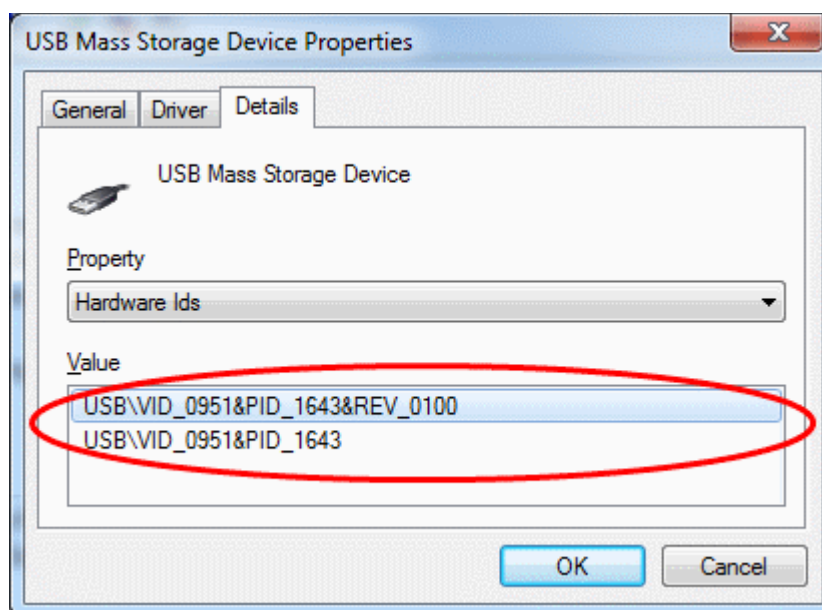
The VID / PID and serial number of a USB device can be identified by plugging-in it on a computer and viewing its properties.

**To obtain the VID / PID and serial number of a USB Device**

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



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



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

- Similarly, you can get the serial number of a device from the 'Properties' interface. Please note the serial number may not be available for some devices. You can also use third party tools such as USBDeview to find the VID/PID and serial numbers of USB devices.

### 5.2.3.8. Add a User Defined User Object

- As the name suggests, a user object consists of a user on your network. These objects can be used to inspect traffic from those users.
  - You must install the endpoint agent on a endpoints for it to become available as a potential object. See <https://help.comodo.com/topic-283-1-598-7040-Getting-Started.html> if you need help with this.
- Multiple users can be added at once by importing from Active Directory (AD). The AD domain needs to be integrated with the CDDP server prior to importing.
  - See [Adding a User Defined Active Directory Users Object](#) for more details.

This section explains how to add single user objects. New users can be defined as source in data transfer policy rules.

#### To add a new user object

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

The 'Single User Objects' screen will be displayed:

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

The screenshot shows the 'SINGLE USER OBJECTS' management interface. At the top right, there are buttons for '+ Add', 'Edit', and 'Delete'. The '+ Add' button is circled in red. A red arrow points from this button to the 'Add Single User' dialog box that is open in the foreground. The dialog box has a title bar with 'Add Single User' and a close button. It contains two input fields: 'Name' with the value 'Peter PC' and 'User Name' with the value 'johnson.peter38@gmail.com'. At the bottom of the dialog are 'Cancel' and 'Save' buttons.

3. Enter the parameters:
  - Name - Enter the name to identify the user
  - Username - Enter the username of the user. The user name can be obtained in two ways:

- The username as per the Active Directory user account, e.g. user@domain.com.
- The email address of the user, e.g. user@domain.com.

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

4. Click 'Save'.

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

SINGLE USER OBJECTS		<a href="#">+ Add</a> <a href="#">Edit</a> <a href="#">Delete</a>
Name	User Name	
John Duncan	johnduncan	
John Smith	johnsmith	
Bob Smith	bobsmith	
Alice Greenwood	alice	
Peter PC	johnson.peter38@gmail.com	

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

### 5.2.3.9. Add a User Defined Active Directory Users Object

- You can add multiple user objects from Active Directory, in addition to single user objects explained in the previous section.
- You have to first integrate Active Directory domains with CDDP to achieve this. See **Integrate Active Directory Domains** for more details.

#### To import Users from AD domain

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

The 'AD User Objects' screen will be displayed:

AD USER OBJECTS		<a href="#">+ Add</a> <a href="#">Edit</a> <a href="#">Delete</a>
Name	AD Domain User	
HR	HR	
New Sales Group	testgroup	
Administrator	testdistributiongroup	

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

**Add AD User**

**Name**

HR

**Active Directory Domain Item**

**Search Text**

Look Up

**AD User List**

Name
HR
testgroup
testdistributiongroup
groupnew
cansintest

Cancel Save

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

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

AD USER OBJECTS		+ Add	Edit	Delete
Name	AD Domain User			
HR	HR			
New Sales Group	testgroup			
Administrator	testdistributiongroup			
Sales	Users			

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

## 5.2.3.10. Add a User Defined File System Directory

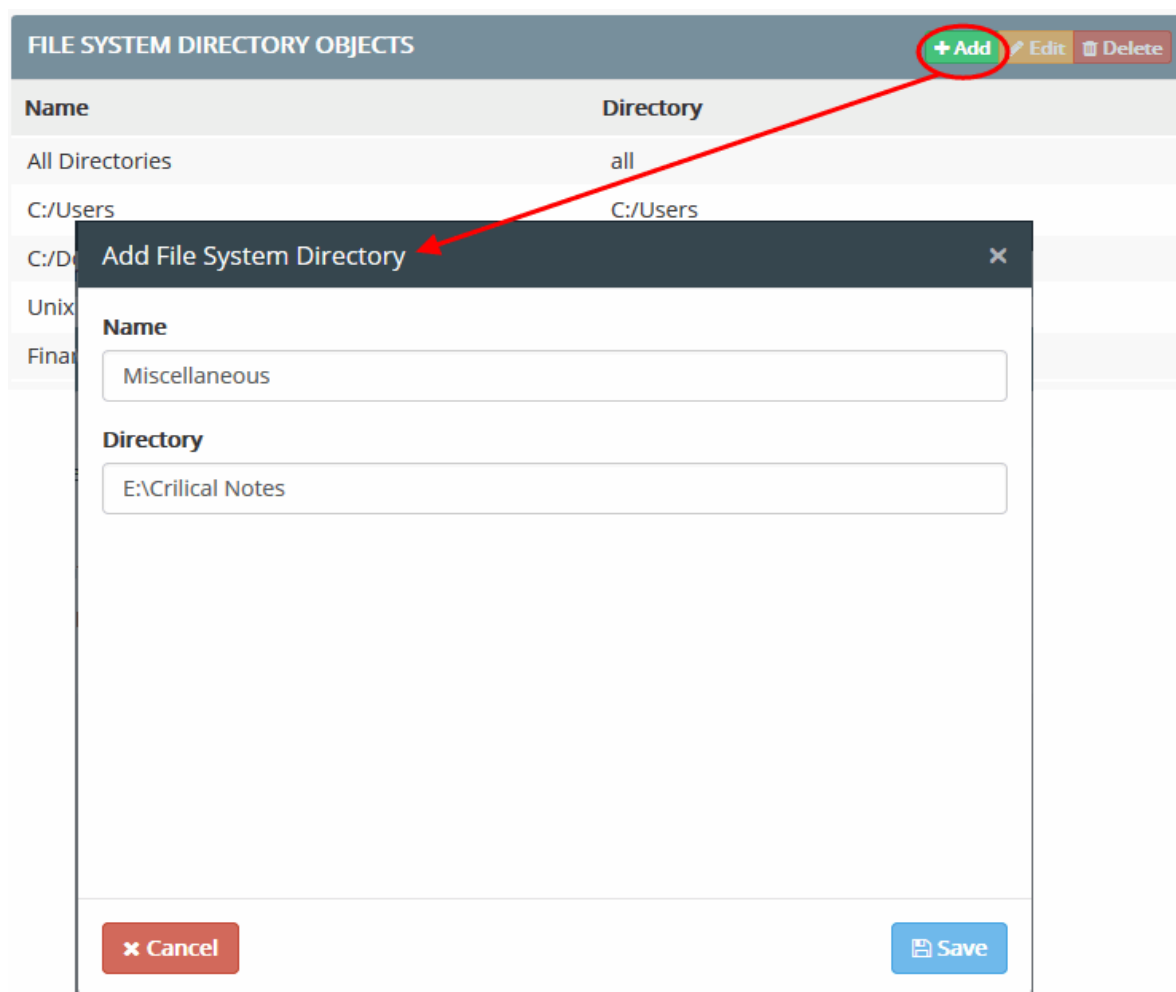
- You can define file paths on endpoint computers that should be checked for sensitive information.
- The file path can be added as a 'File System Directory' object and used as the 'Destination' in **Endpoint Discovery rules**.

**To add a custom file system directory**

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

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

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



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

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



FILE SYSTEM DIRECTORY OBJECTS		<a href="#">+ Add</a>	<a href="#">Edit</a>	<a href="#">Delete</a>
Name	Directory			
All Directories	all			
C:/Users	C:/Users			
C:/Documents and Settings	C:/Documents and Settings			
Unix /home Directory	/home/			
Finance	D:\Bank-doc\statements			
Miscellaneous	E:\Critical Notes			

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

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

#### 5.2.3.11. Add a User Defined Remote Storage Object

- Remote storage objects consist of items like Ftp servers, shared folders and network file systems.
- These items can then be checked for the sensitive information defined in an 'Information Type' object.
- Remote storage objects can be added as 'Source' for a **Remote Storage Rule**.

##### To add a new Remote Storage object

1. Click the 'Policy' tab at the top and then 'Remote Connections' under 'Discovery Target' section
2. Click 'Add' at top-right. The 'Add Remote Storage' dialog will appear.

The screenshot shows the 'REMOTE STORAGE OBJECTS' management interface. At the top, there are buttons for '+ Add', 'Edit', and 'Delete'. A red circle highlights the '+ Add' button, with a red arrow pointing to the 'Add Remote Storage' dialog box that is open in the foreground. The dialog box contains the following fields:

- Select Remote Storage Type:** A dropdown menu currently showing 'Windows Share'.
- Name:** An empty text input field.
- UncPath:** An empty text input field.
- Username:** An empty text input field.
- Password:** An empty text input field.

At the bottom of the dialog box, there are two buttons: 'Cancel' (with a red 'x' icon) and 'Test Connection' (with a blue icon).

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

This is a close-up view of the 'Add Remote Storage' dialog box. The 'Select Remote Storage Type' dropdown menu is open, displaying a list of options: 'Windows Share' (highlighted in blue), 'SSHFS', 'FTP', 'WEB', and 'NFS'. Below the dropdown is an empty text input field.

The following sections explain the processes in detail.

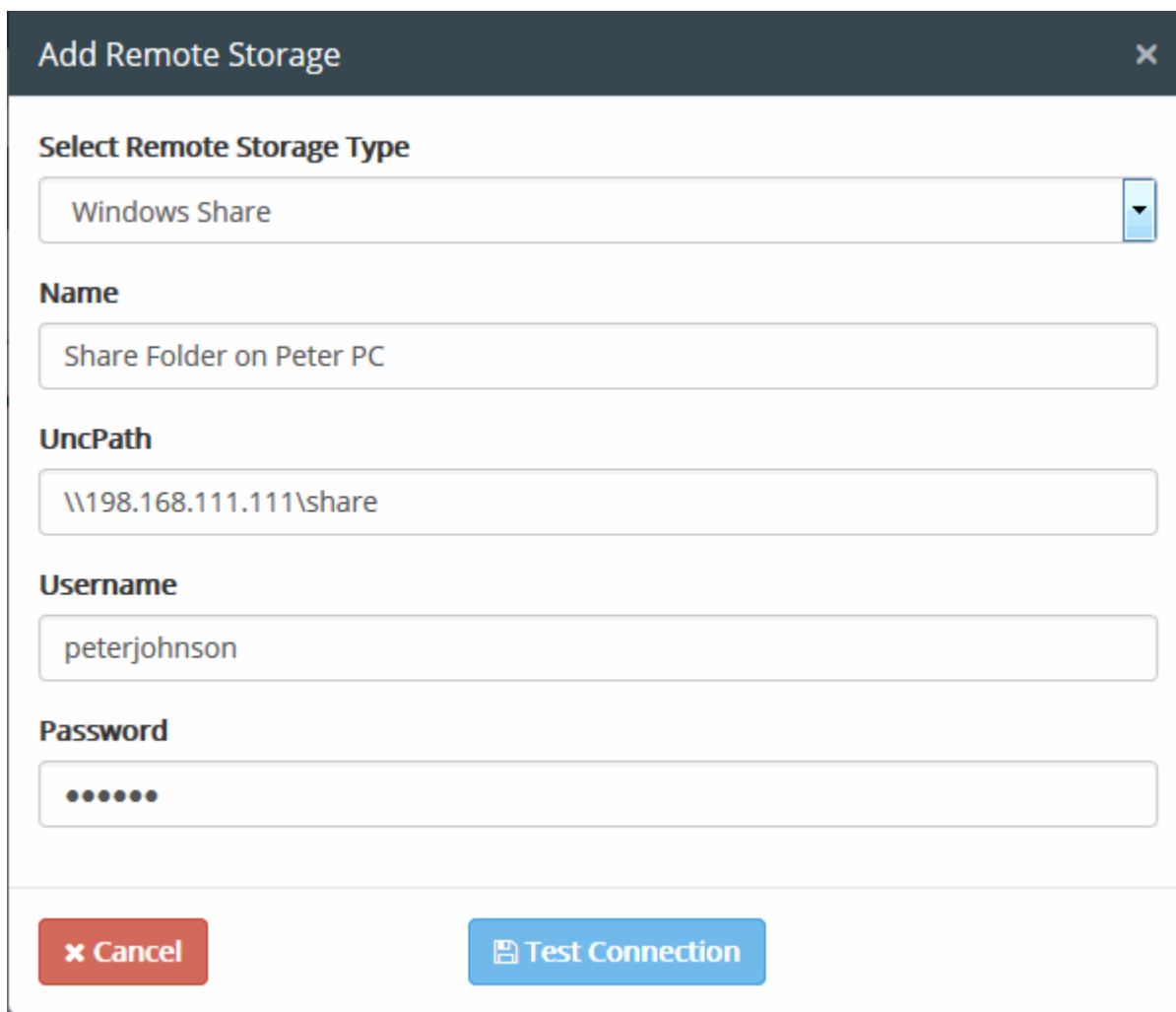
- **Windows Share**
- **SSHFS**
- **FTP**
- **WEB**

- **NFS**

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

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

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



**Add Remote Storage**

Select Remote Storage Type

Windows Share

Name

Share Folder on Peter PC

UncPath

\\198.168.111.111\\share

Username

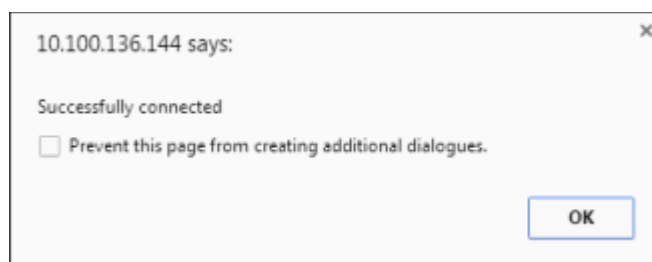
peterjohnson

Password

.....

Cancel Test Connection

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



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

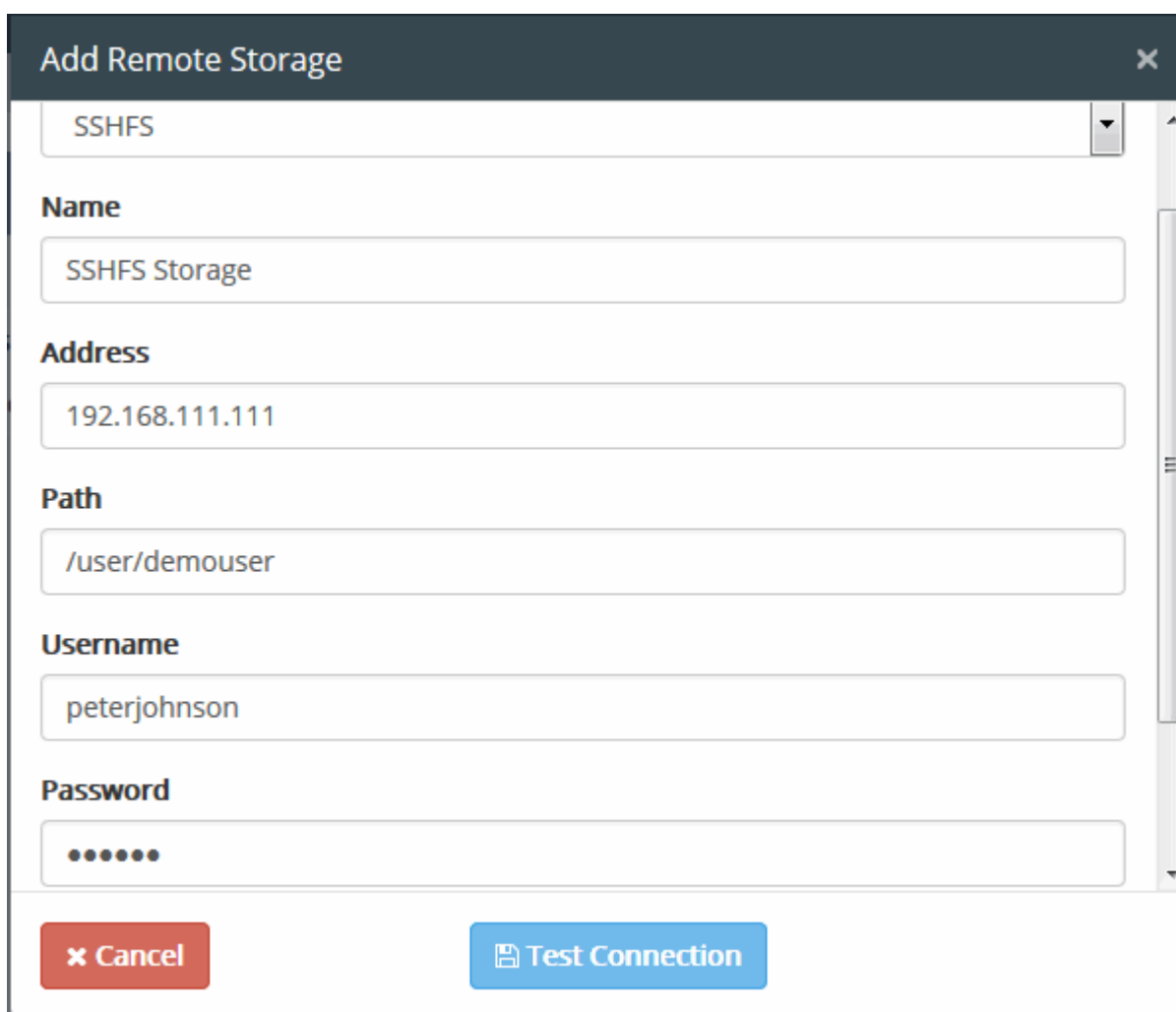
7. Click 'Save'.

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

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

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

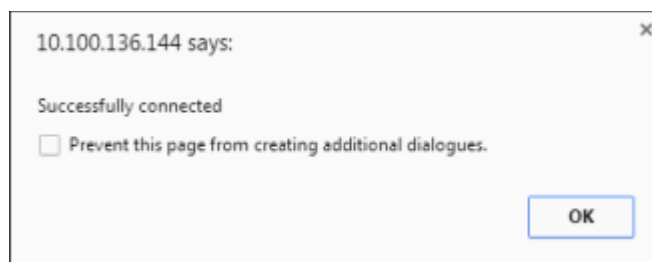
4. Choose SSHFS from the 'Add Remote Storage' dialog



5. Enter the parameters:

- Name - Enter a name shortly describing the SSHFS remote storage
- Address - Enter the IP address or hostname of the server/host, hosting the remote storage
- Path - Enter the file path to be checked in the remote storage
- Username/Password - Enter the username and password of the user account that CDDP can use to login to the server/host
- Port - Enter the connection port for SSH connection to the server/host

6. Click 'Test Connection'. CDDP will check whether the remote storage location is reachable.



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

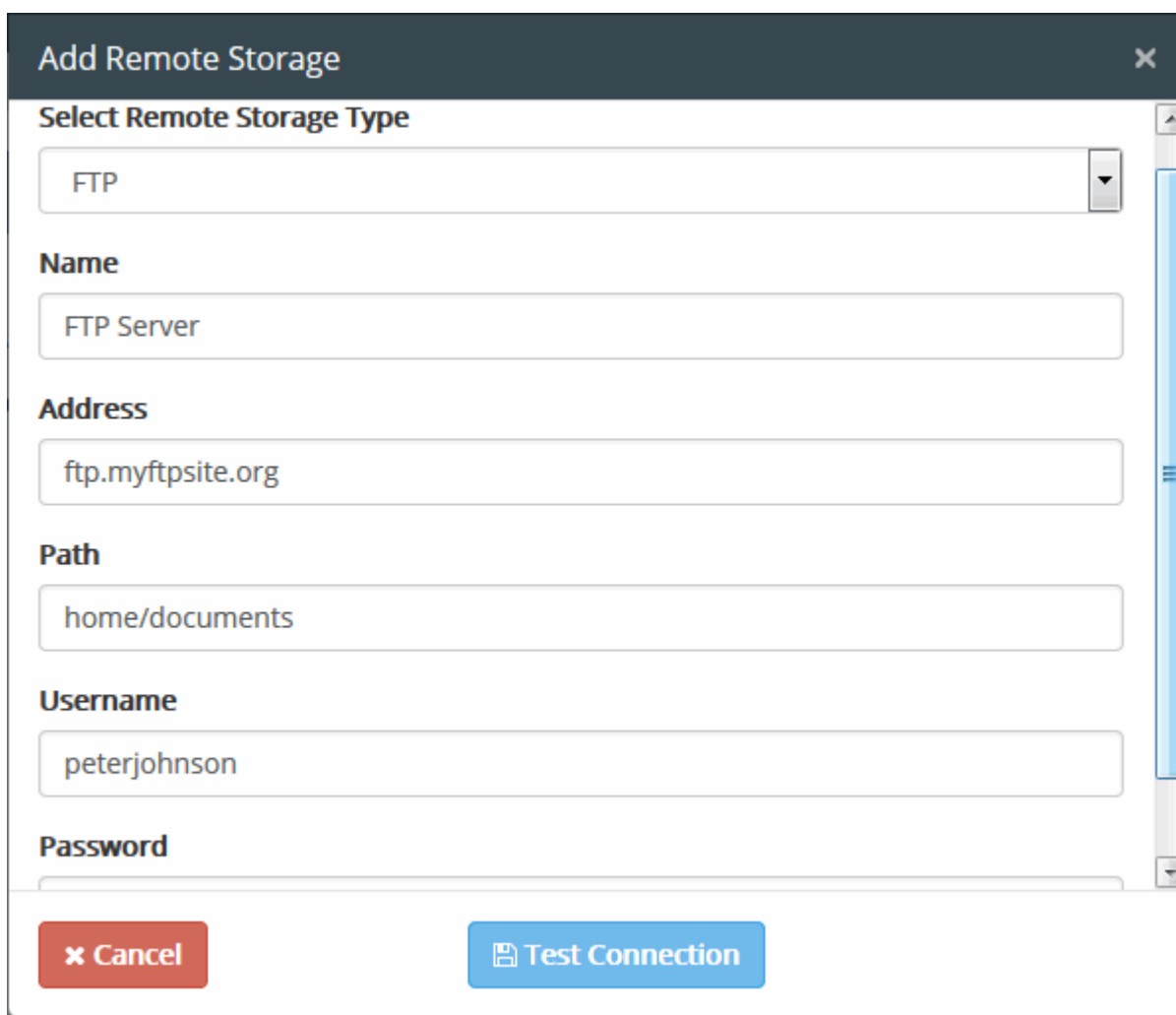
7. Click 'Save'.

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

### Adding a FTP Server

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

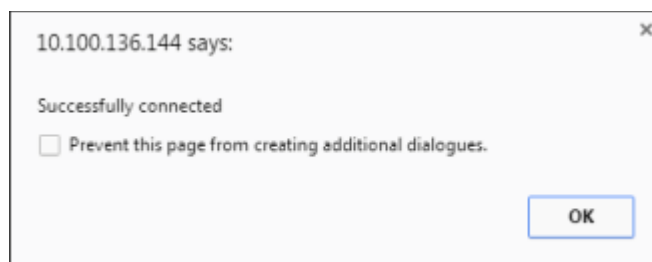
4. Choose FTP from the 'Add Remote Storage' dialog



5. Enter the parameters:

- Name - Enter a name shortly describing the FTP server
- Address - Enter the IP address or hostname of the FTP server
- Path - Enter the file path to be checked in the FTP server

- Username/Password - Enter the username and password of the user account that CDDP can use to login to the FTP server
6. Click 'Test Connection'. CDDP will check whether the remote storage location is reachable.



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

7. Click 'Save'.

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

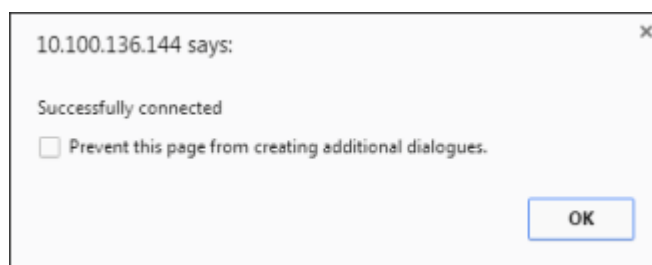
### Adding a WEB Server

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

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

A screenshot of the "Add Remote Storage" dialog box. The dialog has a dark gray header with the title "Add Remote Storage" and a close button (X). The main area is white and contains several fields: a dropdown menu for "Select Remote Storage Type" with "WEB" selected; a text field for "Name" containing "Webserver"; a text field for "Website URL" containing "mywebserver.com"; a text field for "Port" containing "8080"; and a text field for "Depth(Number of links to be followed)" containing "8". At the bottom, there are two buttons: a red "Cancel" button and a blue "Test Connection" button.

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



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

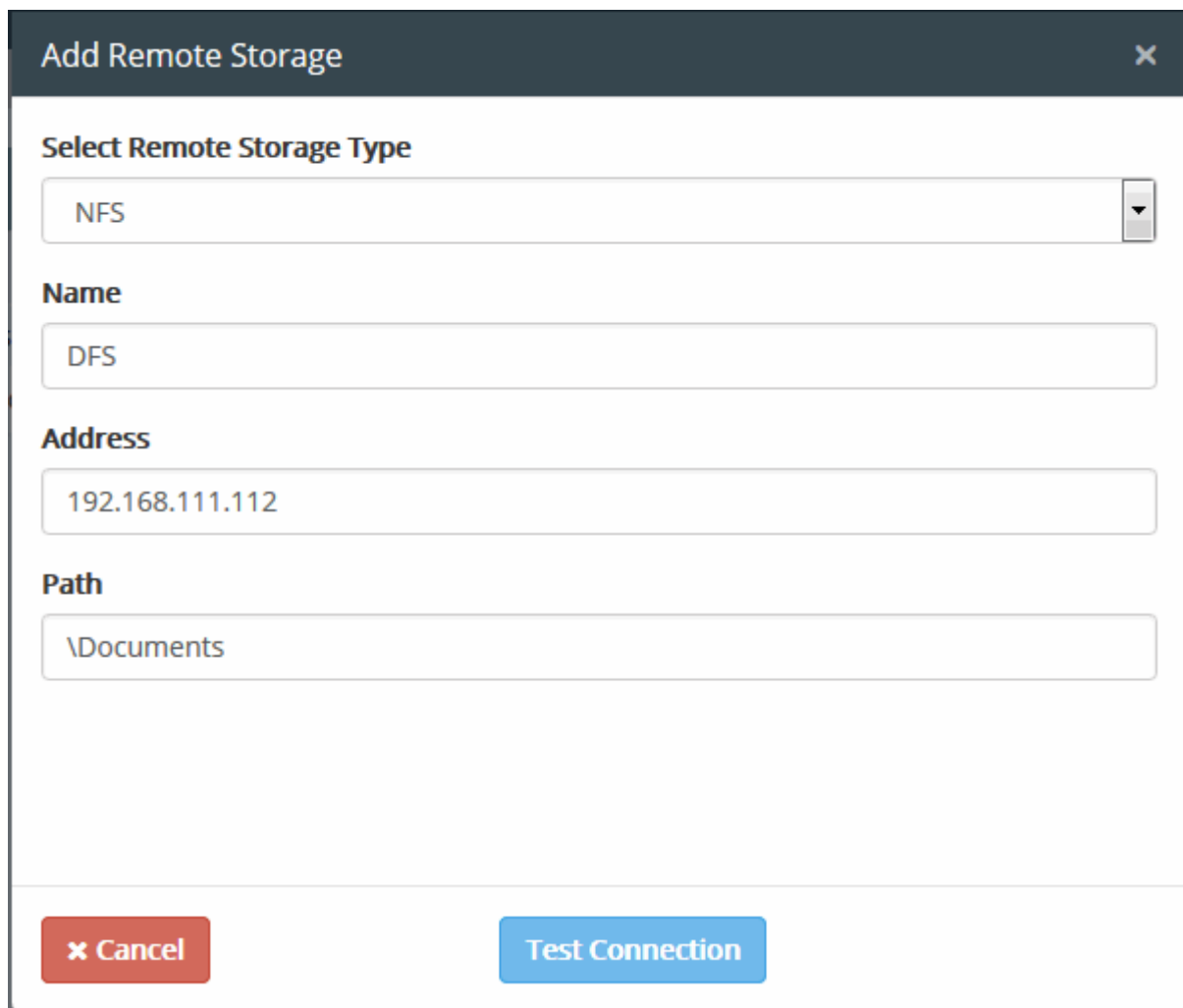
7. Click 'Save'.

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

## Adding a Network File System (NFS)

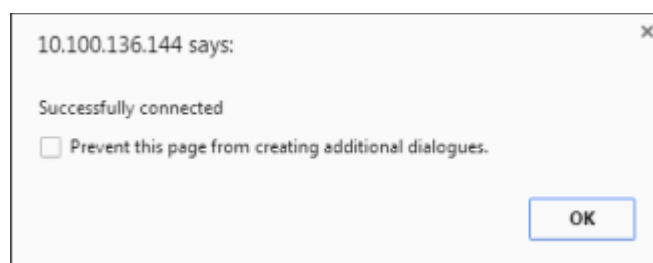
You can add a NFS or Distributed File System (DFS) in the network as a Remote Storage object, by specifying its address and file path to be checked.

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



The 'Add Remote Storage' dialog box is shown. It has a title bar with a close button (X). The main area contains four labeled input fields: 'Select Remote Storage Type' with a dropdown menu showing 'NFS', 'Name' with a text box containing 'DFS', 'Address' with a text box containing '192.168.111.112', and 'Path' with a text box containing '\\Documents'. At the bottom, there are two buttons: a red 'Cancel' button and a blue 'Test Connection' button.

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



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

7. Click 'Save'.

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



## 5.2.3.12. Add a Database Discovery Object

Administrators can add the URL of databases to check them for sensitive information. The database path can be added as a 'Database Discovery' object which can then be specified as a 'Source' in a **Database Discovery rule**.

**To add a database discovery object**

1. Click the 'Policy' tab then 'Database Connections' in the 'Discovery Target' section

The 'Database Discovery Objects' screen will open:

2. Click 'Add' to open 'Add Database Connection' dialog:

The screenshot shows the 'DATABASE DISCOVERY OBJECTS' interface. At the top right, there are buttons for '+ Add', 'Edit', and 'Delete'. A red circle highlights the '+ Add' button, and a red arrow points from it to the 'Add Database Connection' dialog box. The dialog box contains the following fields:

- Database Type: A dropdown menu currently showing 'MYSQL'.
- Name: A text input field.
- JDBC Url: A text input field.
- Login Username: A text input field.
- Login Password: A text input field.

At the bottom of the dialog are 'Cancel' and 'Save' buttons.

- Database Type – Currently only MySQL databases are supported
  - Name - Enter a name to identify the database.
  - JDBC URL - Enter the path to the database
  - Login Username / Password – Enter the credentials required to access the database
3. Click 'Save'.

CDDP will attempt to connect to the database. If the connection is successful then the new object will be listed in the 'Database Discovery Objects' screen:

DATABASE DISCOVERY OBJECTS				+ Add	Edit	Delete
Name	Type	Url	Username			
ddpdiscovery	MYSQL	jdbc:mysql://10.100.136.212/mydip_test	root			
small	MYSQL	jdbc:mysql://10.100.136.212/mydip_test_small	root			
test	MYSQL	jdbc:mysql://10.100.136.212/mydip_test_small	root			
Store	MYSQL	jdbc:mysql://10.100.136.212/mydip_test_Store	root			

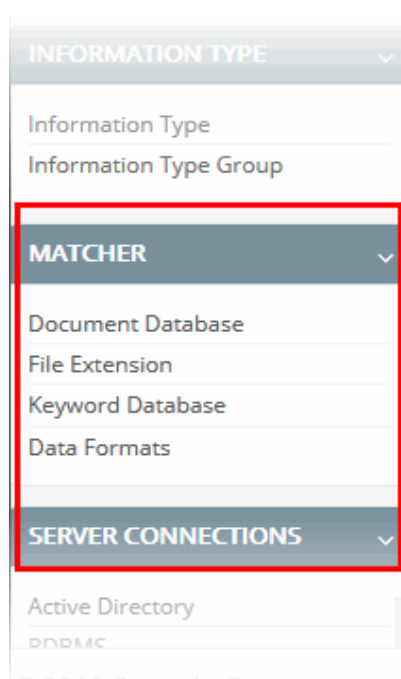
- To edit the details of a database discovery object, select it and click 'Edit'
- To remove a Database Discovery object from the list, select it and click 'Delete'. Click 'Yes' to confirm in the confirmation screen.

## 5.3. Matchers

- A 'Matcher' is a specific piece of data used to narrow the scope of an information type.
- For example, if you create an information type called 'Social Security Numbers', you can refine it by adding matchers for 'Uruguay SSN', 'UK National Insurance Number' etc.
- The information type can then be added to a data control or data discovery rule.

CDDP ships with a set of predefined information types and you can also create custom types. See sections [Information Types – An Overview](#), [Predefined Matcher Types](#) and [Predefined Information Types](#) for more details.

- The 'Matchers' area lets you view, manage and create matchers.
- The items in this interface will be available for selection when creating a new information type object.
- Click 'Policy' > 'Matcher' to get started:

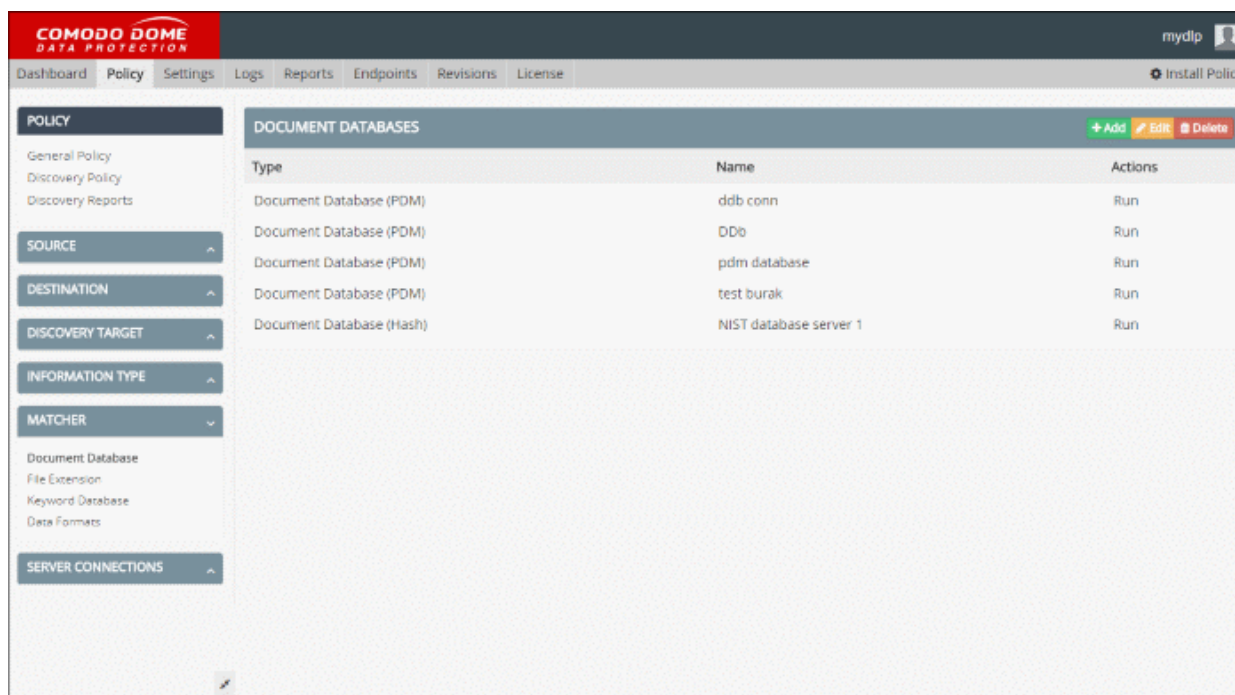


Click following links for more details:

- [Manage Document Databases](#)
- [Manage File Extensions](#)
- [Manage Keyword Groups](#)
- [Manage Data Formats](#)

### 5.3.1. Manage Document Databases

- Document databases are collections of documents stored on your network. CDDP can inspect and flag traffic that contains documents from protected databases.
- Databases can be added as 'Document Database (HASH)' and 'Document Database (PDM)' matcher types when creating an information type object.
- The 'Document Databases' interface lets you add custom document databases to CDDP. Once added, they will be available for selection as a matcher when creating an information type object..
- Click 'Policy' > 'Matcher' > 'Document Database' to open this interface:



- The 'Run' link in the 'Actions' column lets you generate hash values for files in the database. These values are used by 'Document Database (Hash)' matchers to identify files.
  - For more details, see '[Document Database \(Hash\)](#)' in the section [Information Types - An Overview](#).

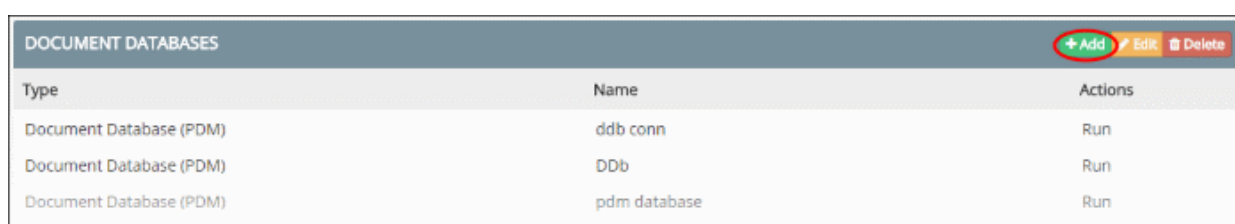
Click the following links to find out how to add and edit a document database:

- [Add a Document Database](#)
- [Edit a Document Database](#)

#### 5.3.1.1. Add a Document Database

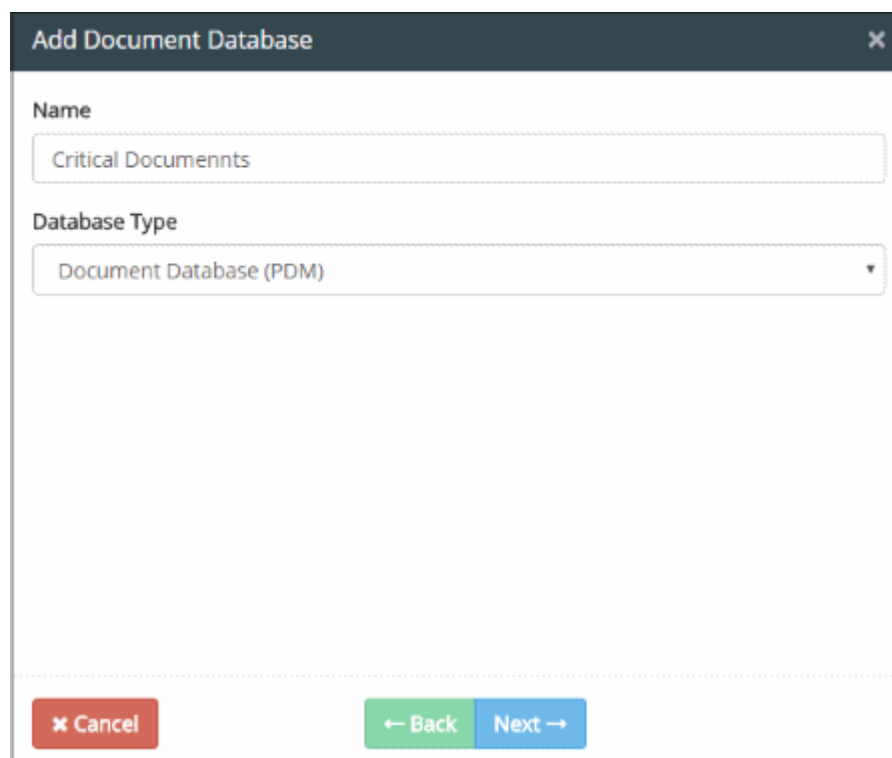
Admins can create a new document database and add files manually or import them from a database.

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



## Step 1 – Enter a name

The 'Add Document Database' dialog will be displayed.

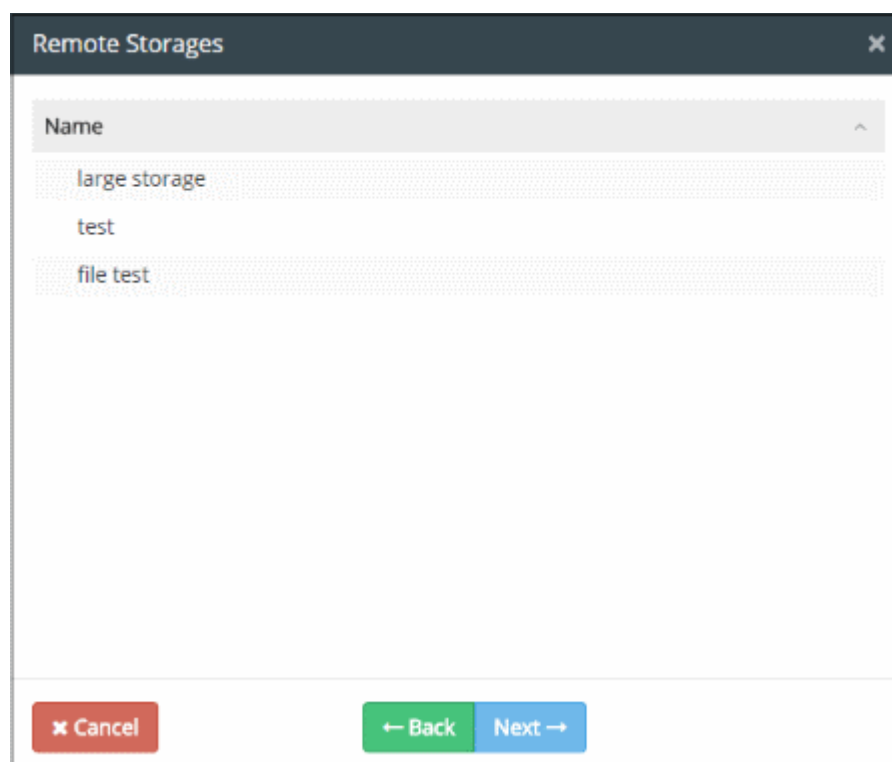


The 'Add Document Database' dialog box is shown. It has a title bar with a close button (X). The main area contains two fields: 'Name' with the text 'Critical Documentnts' and 'Database Type' with a dropdown menu showing 'Document Database (PDM)'. At the bottom, there are three buttons: a red 'Cancel' button, a green 'Back' button, and a blue 'Next' button.

- Enter a name for the document database and select the database type from the drop-down.
- Click 'Next'

## Step 2 – Adding files from remote storage

The remote storage screen will open:



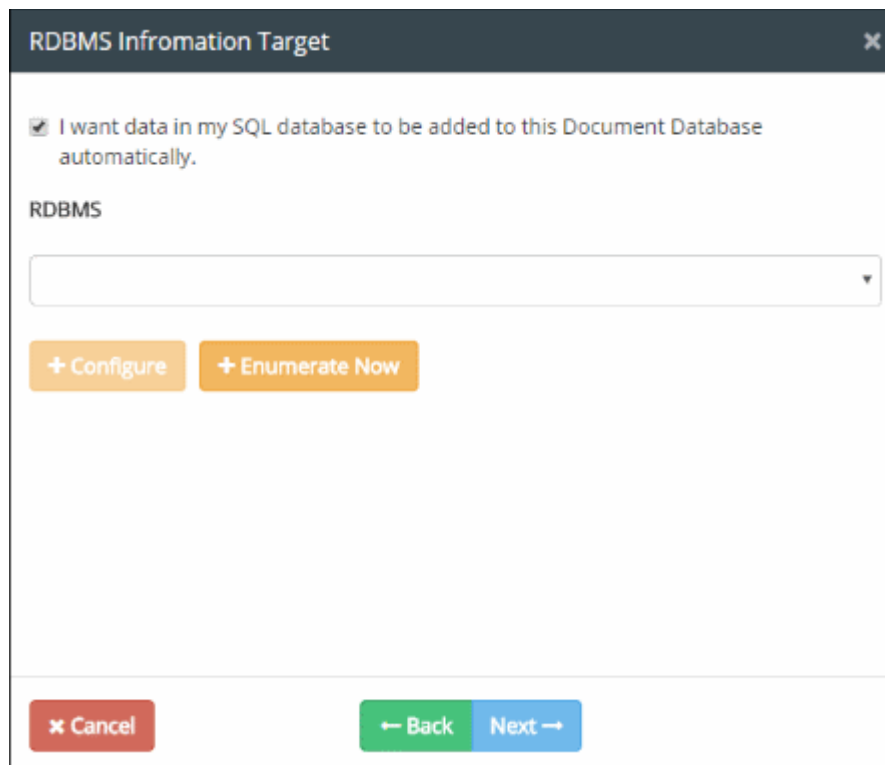
The 'Remote Storages' dialog box is shown. It has a title bar with a close button (X). The main area contains a list of storage names: 'large storage', 'test', and 'file test'. At the bottom, there are three buttons: a red 'Cancel' button, a green 'Back' button, and a blue 'Next' button.

Files displayed here are fetched from remote connections in the 'Discovery Target' section. See '[Adding a User Defined Remote Storage Object](#)' for more details on how to add a remote storage object.

- Select the files and click 'Next'

### Step 3 – Integrating a MySQL Database to Document Database

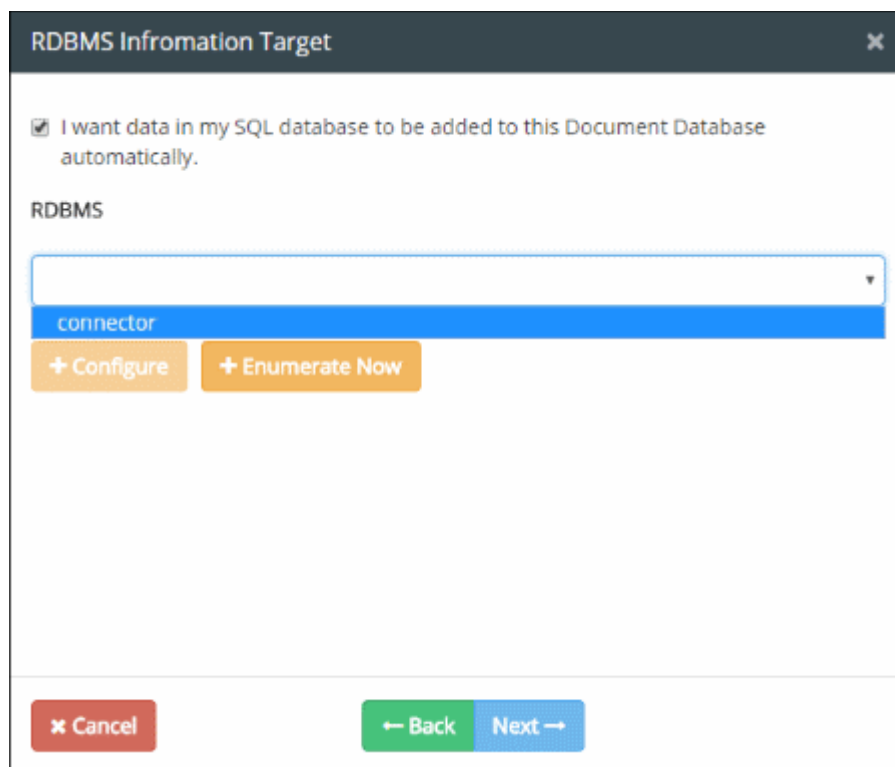
The 'RDBMS Information Target' screen will open:



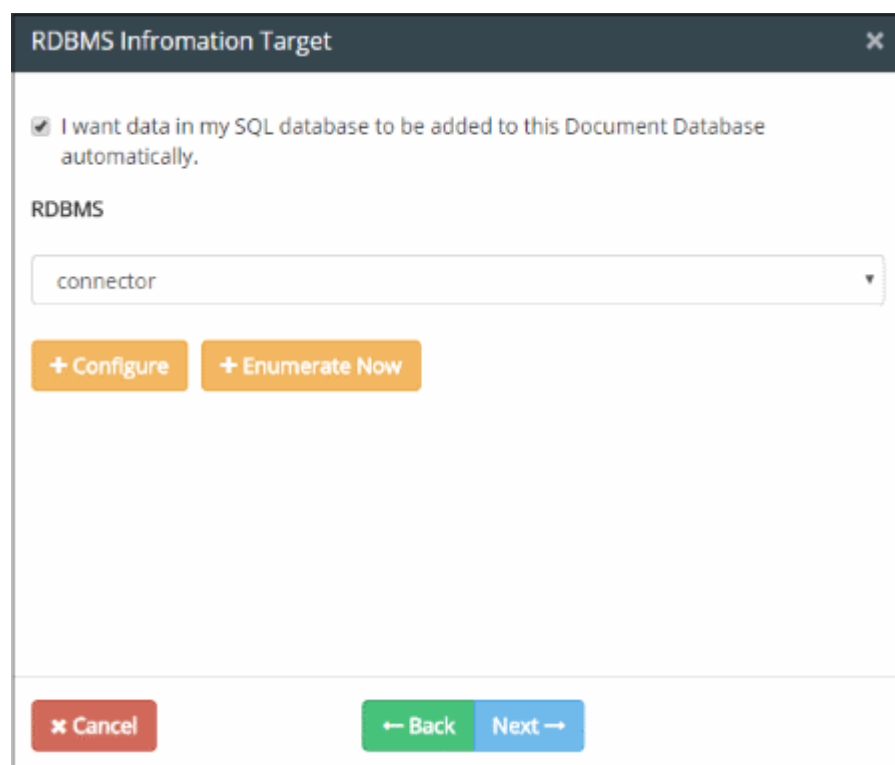
Administrators can import documents from a MySQL database server through an RDBMS connection.

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

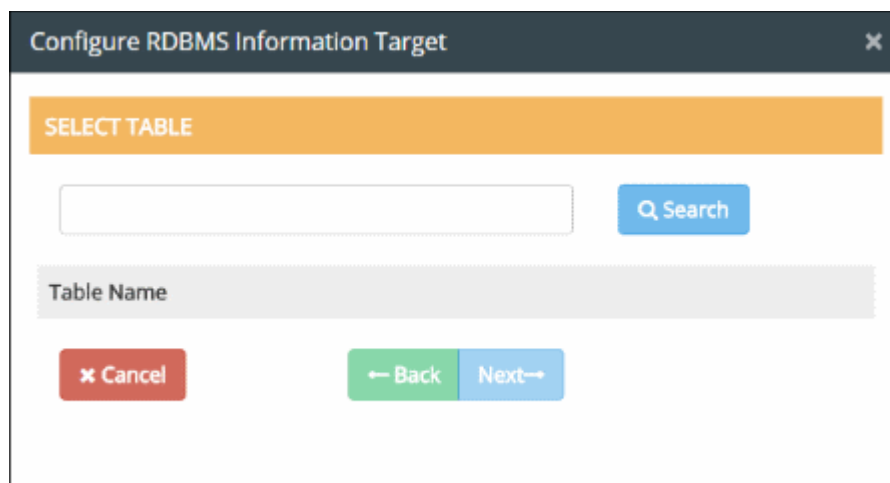
If you have RDBMS Connections configured already, the list of the connections will be displayed. See '[Integrating RDBMS Systems](#)' for more details.



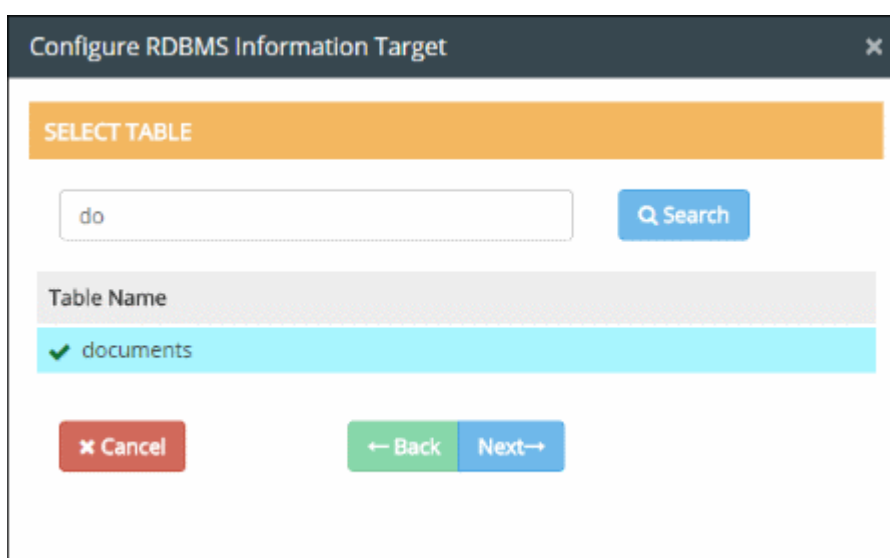
- If you have not configured RDBMS connections, you can configure from this interface by clicking 'Configure'.
- If you have already configured the RDBMS connection, you can re-configure an existing connection if required.



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



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



The 'Select Column' dialog will appear.

The screenshot shows a dialog box titled "Configure RDBMS Information Target" with a close button (X) in the top right corner. Below the title bar is an orange header with the text "SELECT COLUMN". Underneath is a search input field and a blue "Search" button. A list of column names is displayed below the search field, with "Column Name" as the header. The listed columns are "idx", "doc\_name", and "doc\_path". At the bottom of the dialog are three buttons: a red "Cancel" button, a green "Back" button, and a blue "Next" button.

You can search for a specific column by entering the first few characters of the column header in the field and clicking 'Search'. All matching columns will be shown in the list below. To view all items, click 'Search' with the field blank.

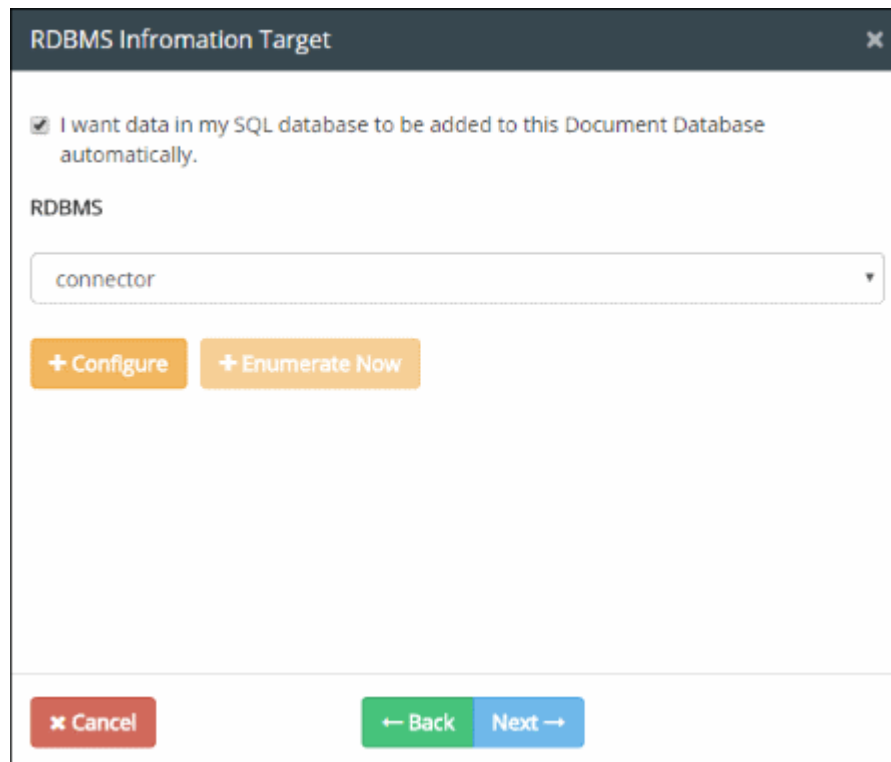
- Select the column header from the list and click 'Next'.

The screenshot shows the same dialog box, now at the "SAMPLES" step. The orange header now says "SAMPLES". Below it, a grey header says "Samples". Underneath, a list of sample items is displayed, with "MyDLP-Administration-Guide.pdf" as the first item. At the bottom of the dialog are three buttons: a green "Back" button, a blue "Next" button, and a green "Save" button with a floppy disk icon.

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

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





RDBMS Information Target

☒ I want data in my SQL database to be added to this Document Database automatically.

RDBMS

connector

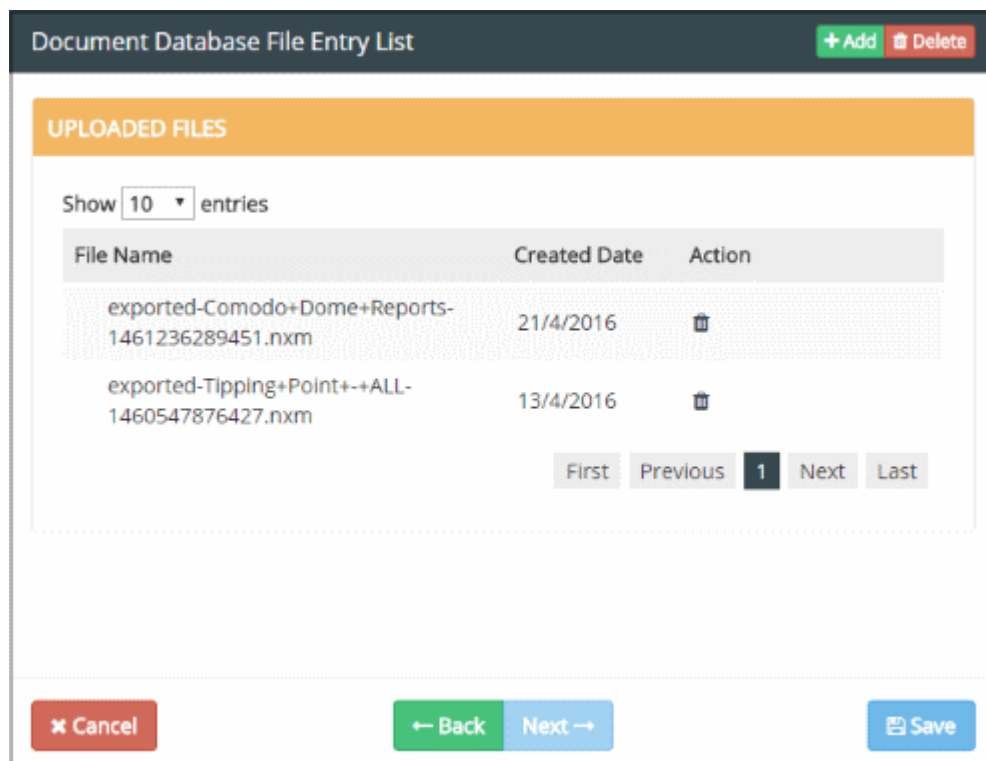
+ Configure + Enumerate Now

Cancel Back Next

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

#### Step 4 – Manually Adding Files to the Database

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



Document Database File Entry List

+ Add Delete

UPLOADED FILES

Show 10 entries

File Name	Created Date	Action
exported-Comodo+Dome+Reports-1461236289451.nxm	21/4/2016	
exported-Tipping+Point+-+ALL-1460547876427.nxm	13/4/2016	

First Previous 1 Next Last

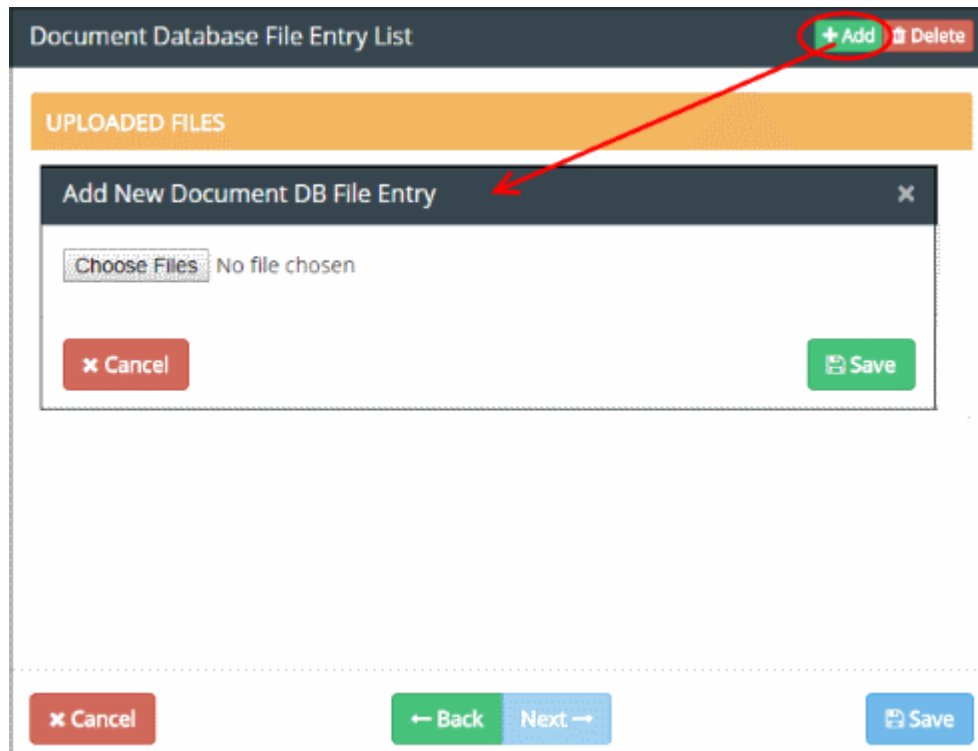
Cancel Back Next Save

The screen shows the details of files uploaded including the document creation date. Delete a file by clicking the trash can icon beside it.

You can upload files from the computer you are using to access the CDDP admin console to build the document database.

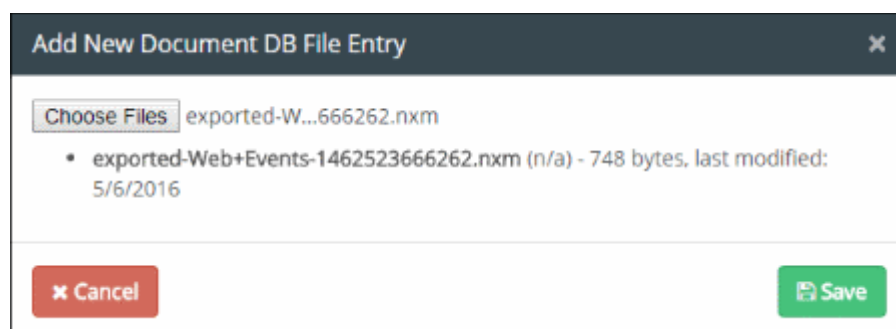
## To upload the files

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



- Click 'Browse' and navigate to the location of the files
- Select the file(s) and click 'Open'

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



- Click 'Save'

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

Document Database File Entry List + Add Delete

UPLOADED FILES

Show  entries

File Name	Created Date	Action
exported-Comodo+Dome+Reports-1461236289451.nxm	21/4/2016	
exported-Tipping+Point+-+ALL-1460547876427.nxm	13/4/2016	

First Previous **1** Next Last

Cancel ← Back Next → Save

- Repeat the process to add more files
- To remove a file from the list, click the trash can icon beside it
- Click 'Back' to review your selections
- Click 'Save' to save the document database.

DOCUMENT DATABASES <span>+ Add</span> <span>Edit</span> <span>Delete</span>		
Type	Name	Actions
Document Database (PDM)	ddb conn	Run
Document Database (PDM)	DDb	Run
Document Database (PDM)	pdm database	Run
Document Database (PDM)	test burak	Run
Document Database (Hash)	NIST database server 1	Run
Document Database (PDM)	Critical Documentnts	Run

The document database will be available for selection to define the Matcher component while creating an Information Type object. But for specifying the document database for Document Database (Hash) matcher, the hash values of the files need to be created and stored, so that CDDP will use the hash values to intercept the data traffic if it contains any of the files from the database. For more details, see '[Document Database \(Hash\)](#)' in the section [Information Types - An Overview](#).

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

Comodo Dome Data Protection creates MD5 Hash values of the files and saves them. You can view the hash values by selecting the database and clicking 'Edit' at the top. Proceed to the 'Document Database File Entry List' screen to view the hash values below the 'Generated Files' section.

**Document Database File Entry List** + Add Delete

**GENERATED FILES**

Show  entries

Search:

File Name	MD5 Hash	Created Date
export		
ed-		
Custo	c80f4693	
m+Qu	e43fe697	24/10/20
ery-	26528d3	17
14615	7cf1afa3f	
76971		
887.nx		
m		
export		

✖ Cancel ← Back Next → Save

**UPLOADED FILES**

Show  entries

File Name	Created Date	Action
No data available in table		

First Previous Next Last

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. See **Deploy a Policy** for more details.

### 5.3.1.2. Edit a Document Database

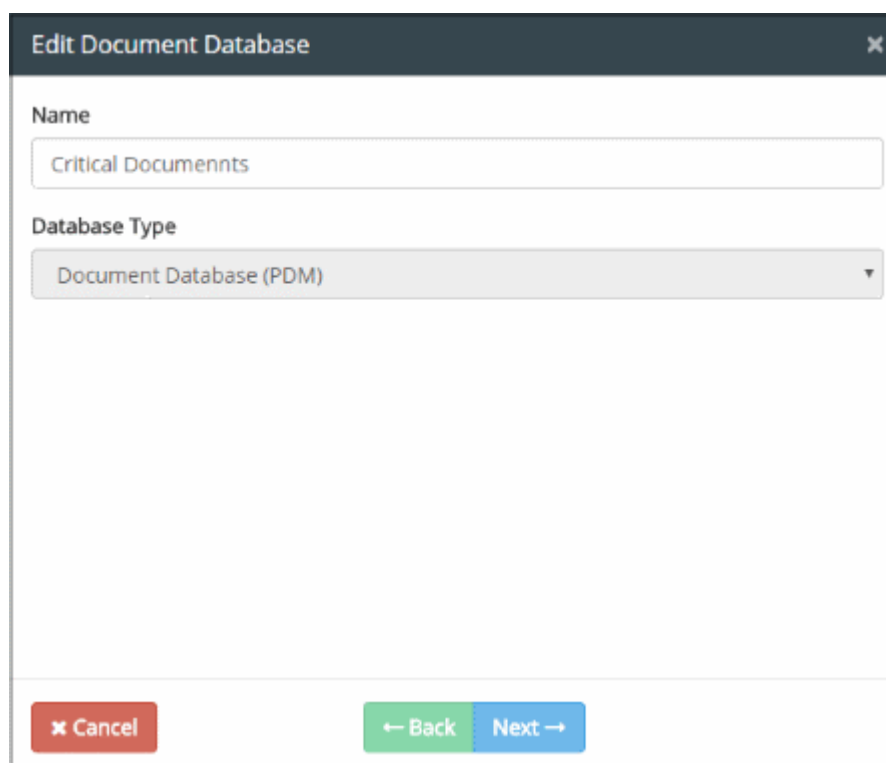
The 'Document Database' interface lets you add new documents or edit/remove unnecessary documents from any database. The changes will take effect immediately after reapplying the policy to the network.

#### To edit a document database

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

DOCUMENT DATABASES			<span>+ Add</span> <span>Edit</span> <span>Delete</span>
Type	Name	Actions	
Document Database (PDM)	ddb conn	Run	
Document Database (PDM)	DDb	Run	
Document Database (PDM)	pdm database	Run	
Document Database (PDM)	test burak	Run	
Document Database (Hash)	NIST database server 1	Run	
Document Database (PDM)	Critical Documents	Run	

The 'Edit Document Database' dialog will be displayed:



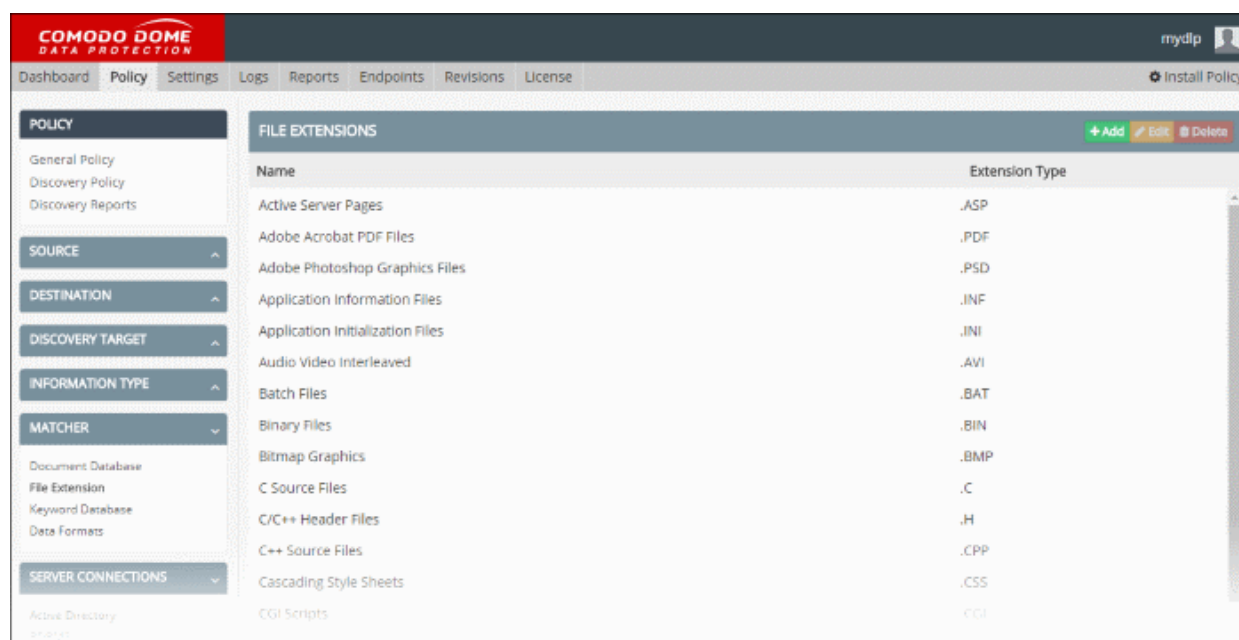
All files imported or added to the document database will be listed here. The process is the same as adding a document database. See '[Add a Document Database](#)' for more details.

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

For the changes in the document database to take effect in the 'Information Type' object in which it is used and in the Rules in which the Information Type object is applied, re-install the policy by clicking the Install Policy at the top right. See [Deploy a Policy](#) for more details.

### 5.3.2. Manage File Extensions

- Click 'Policy' > 'Matcher' > 'File Extension' to open this interface.
- 'File extensions' are used to fine-tune an 'Information Type' object so that it only covers specific extensions
- You can select which extensions you want to include when you create an information object. The information object can then be added as rule component.
- Comodo Dome Data Protection ships with a set of predefined extensions that are commonly used. You can add custom extensions.
- See '[Information Types – An Overview](#)' and '[Add a User Defined Information Type](#)' for help with information type objects.



See the following sections for more details.

- [Add a New File Extension](#)
- [Edit a File Extension](#)

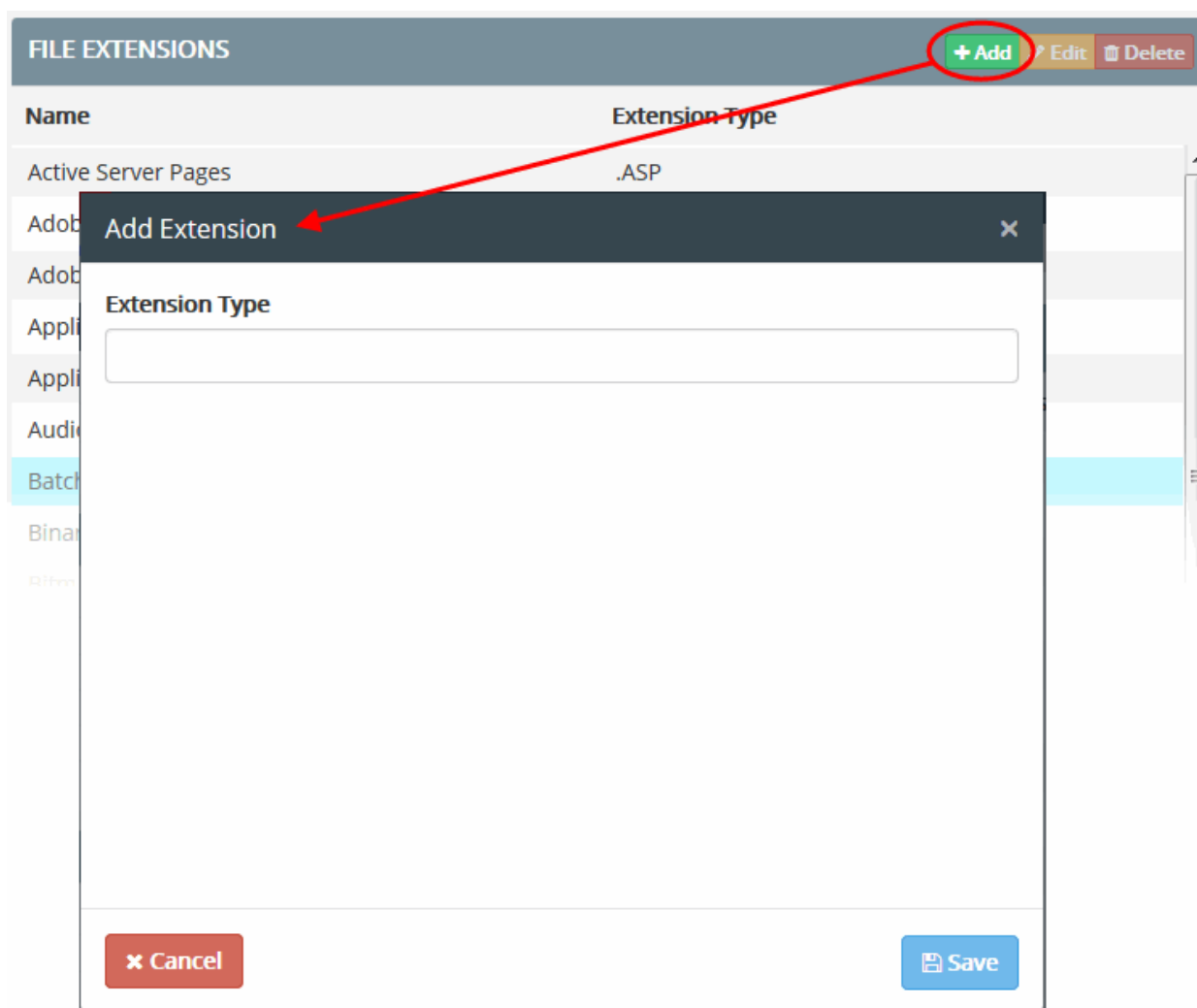
### 5.3.2.1. Add a New File Extension

- In addition to the predefined file extensions, administrators can create custom extensions according to their requirements.

#### To add a new file extension

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

The 'Add Extension' dialog will be displayed.



- Type the extension you wish to add in the the 'Extension Type' field. For example, .swf
- Click 'Save'

The new extension type will be added and displayed in the list. Once added, the file extension will be available for selection when creating a new information type. See '[Add a User Defined Information Type](#)' for more details.

### 5.3.2.2. Edit a File Extension

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

#### To edit an existing extension

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

FILE EXTENSIONS		<a href="#">+ Add</a> <a href="#">Edit</a> <a href="#">Delete</a>
Name	Extension Type	
Active Server Pages	.ASP	
Adobe Acrobat PDF Files	.PDF	
Adobe Photoshop Graphics Files	.PSD	
Application Information Files	.INF	
Application Initialization Files	.INI	
Audio Video Interleaved	.AVI	
Batch Files	.BAT	
Binary Files	.BIN	

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

Edit Extension

Extension Type

.INF

✕ Cancel

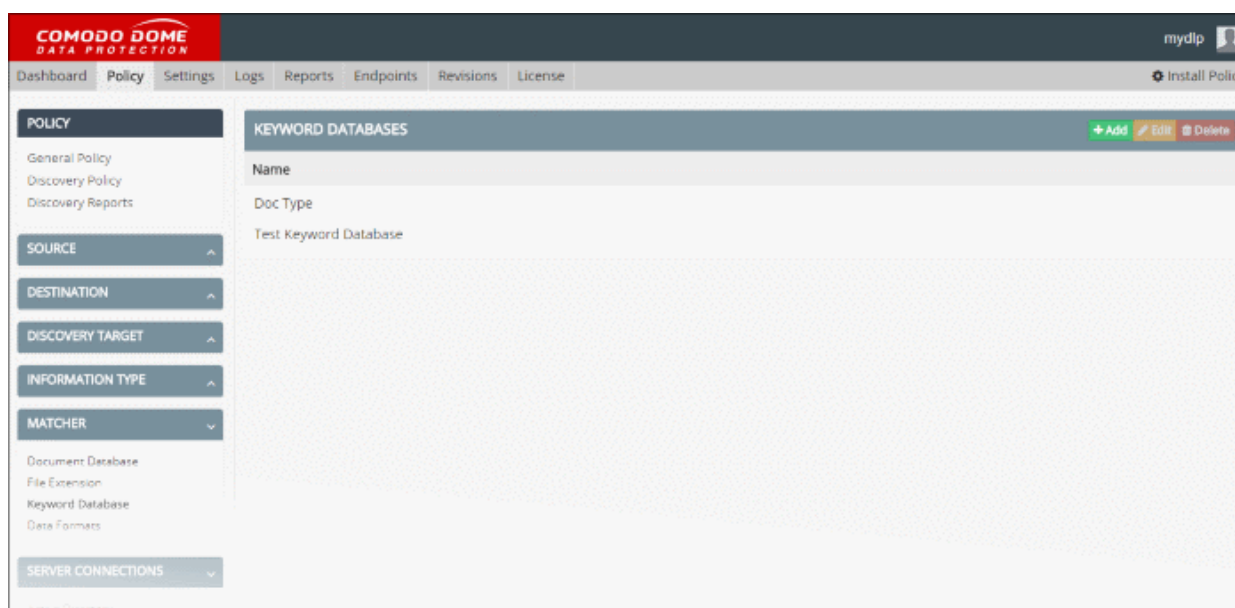
Save

- You must reinstall the policy for the edit to take effect (click the 'Install Policy' button at top right). The change will apply to all rules which have an information object which uses this extension. See [Deploy a Policy](#) for more details.
- To remove a file extension, select it and click 'Delete'. Please note - a file extension cannot be removed if it is in use in a rule.



### 5.3.3. Manage Keyword Databases

- Click 'Policy' > 'Matcher' > 'Keyword Database' to open this interface.
- A 'Keyword Database' is a collection of keywords pertaining to a specific field like business, medicine, finance, banking and so on.
- A keyword database can be specified as a 'Matcher' when creating an 'Information Type' object. You can then add the information object to a rule.
- The rule will then identify files containing the keywords and apply rule actions as configured.
- CDDP ships with a number of pre-defined, non-editable keyword groups. You can also add your own keyword databases. Keywords can be entered manually, imported from a text file or imported from a RDBMS server.



Click the links below to know how to manage the Keyword Databases:

- [Add a user defined Keyword Database](#)
- [Edit a user defined Keyword Database](#)

#### 5.3.3.1. Add a User Defined Keyword Database

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

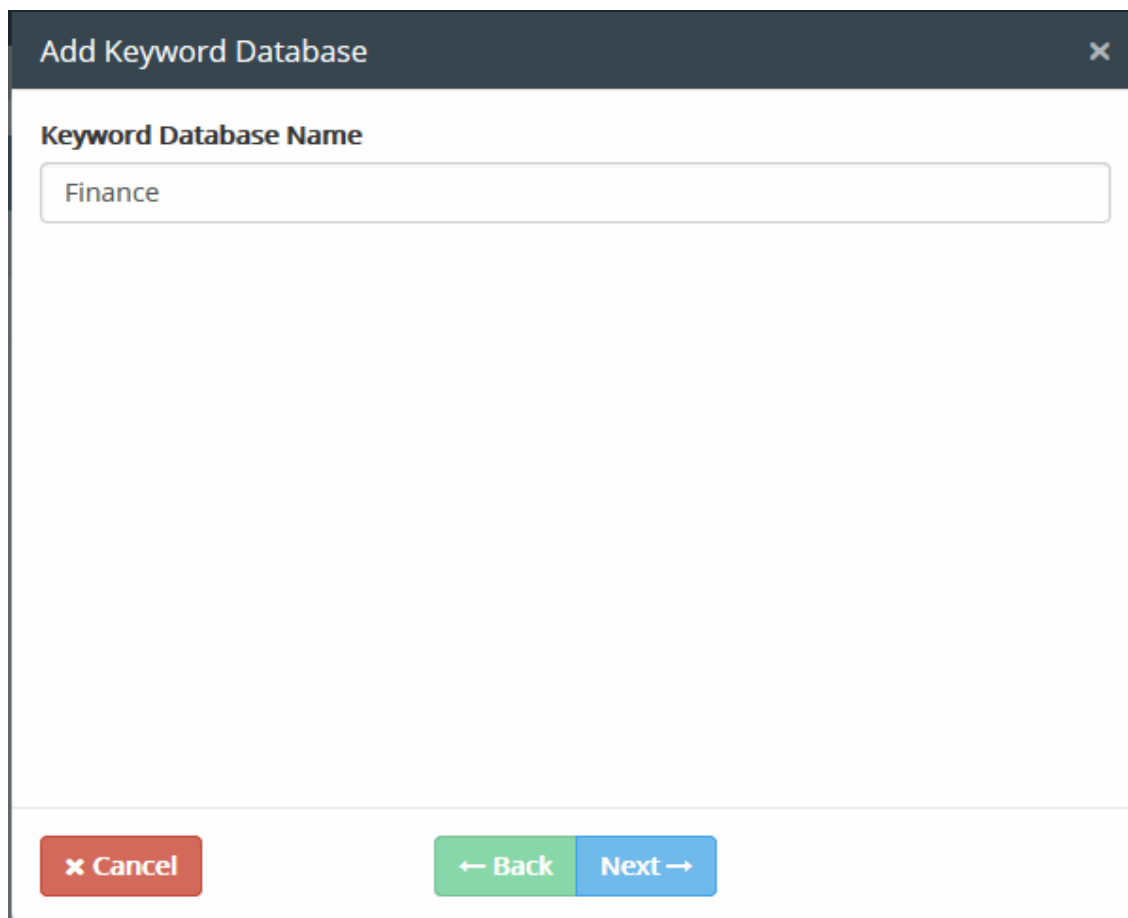
##### To add a new Keyword Database

- Click the 'Policy' tab then 'Matcher' > 'Keyword Database'
- Click 'Add' from the 'Keyword Databases' screen



## Step 1 – Enter a name

The 'Add Keyword Database' dialog will be displayed.

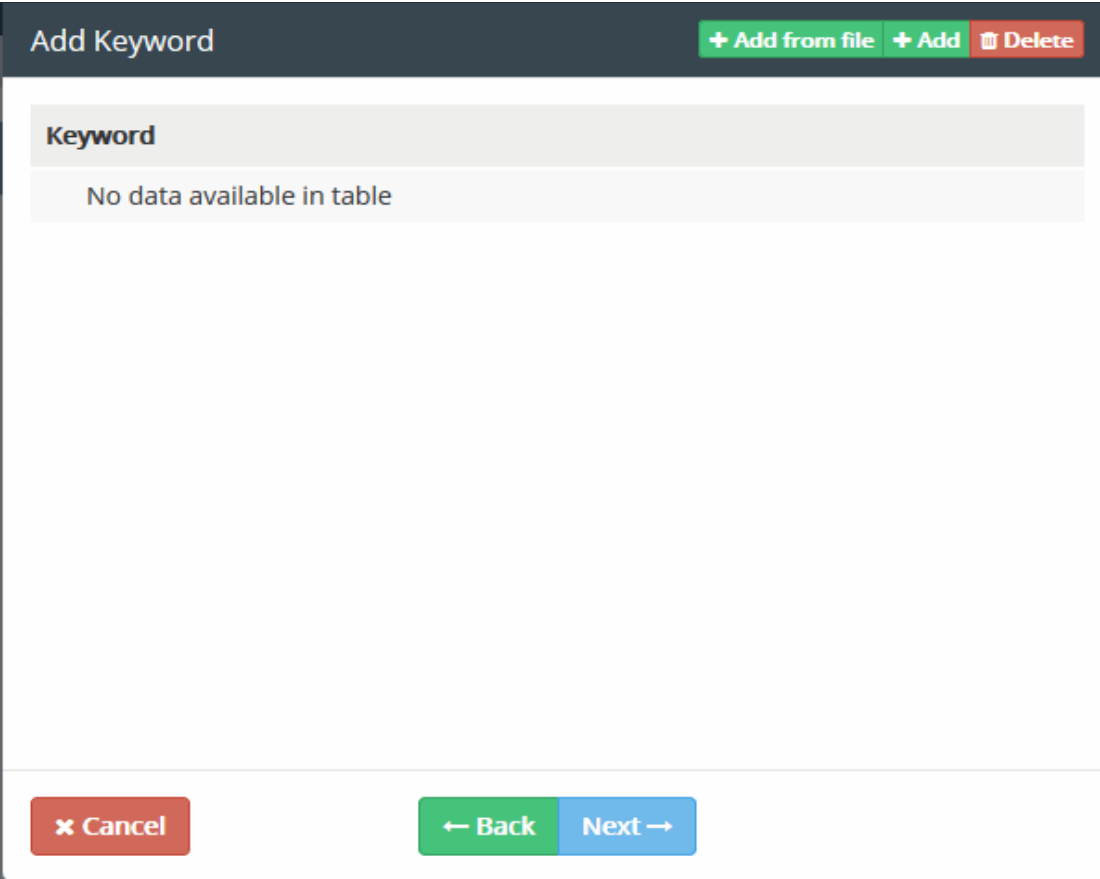


The screenshot shows a dialog box titled "Add Keyword Database". Inside the dialog, there is a label "Keyword Database Name" and a text input field below it. The input field contains the text "Finance". At the bottom of the dialog, there are three buttons: a red "Cancel" button, a green "Back" button with a left arrow, and a blue "Next" button with a right arrow.

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

## Step 2 – Add keywords to the database

The 'Add Keyword' dialog will be displayed. Note – simply click 'Next' here if you only want to add keywords from a SQL database.



**Add Keyword** + Add from file + Add Delete

Keyword
No data available in table

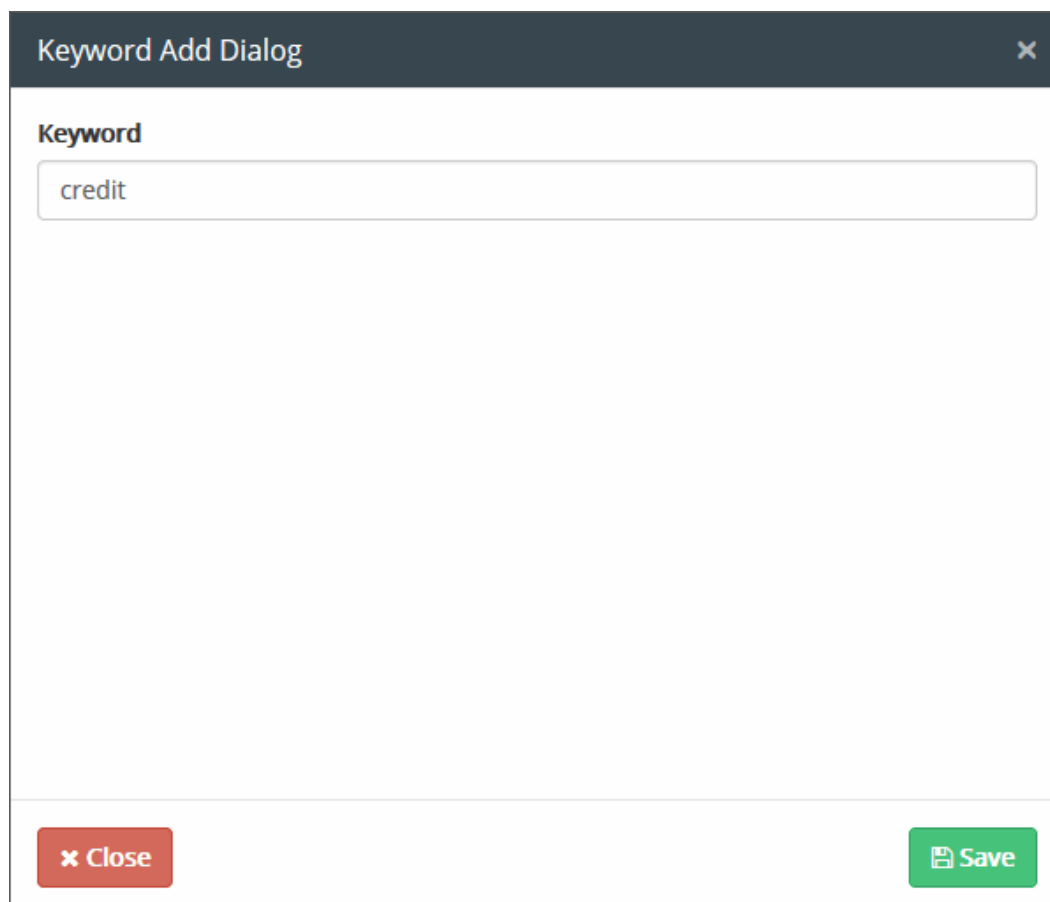
× Cancel ← Back Next →

You can add keywords in two ways:

- **Manually enter keywords**
- **Import keywords from a file**

#### Manually enter keywords

- To manually enter the keywords, click 'Add' at the top of the 'Add Keyword' dialog:



Keyword Add Dialog

Keyword

credit

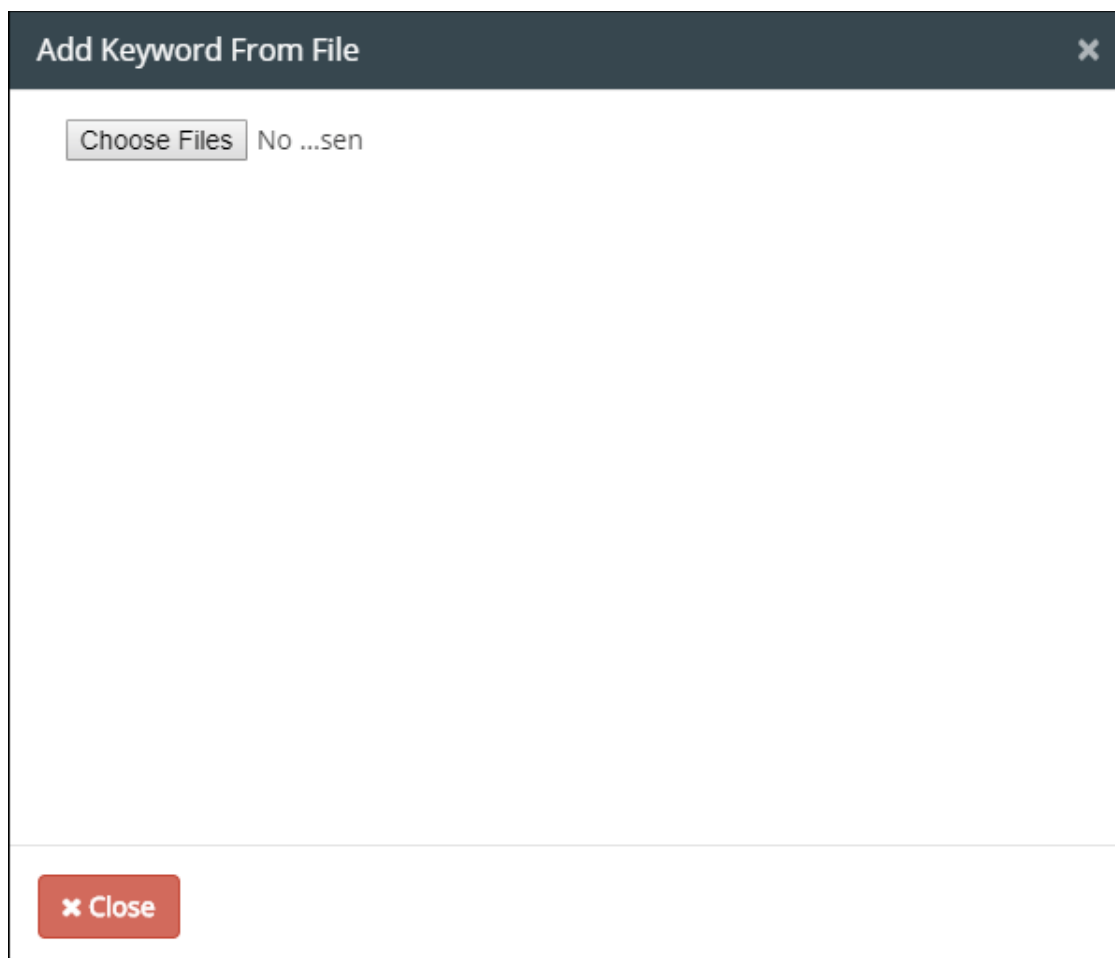
Close Save

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

### Import keywords from a file

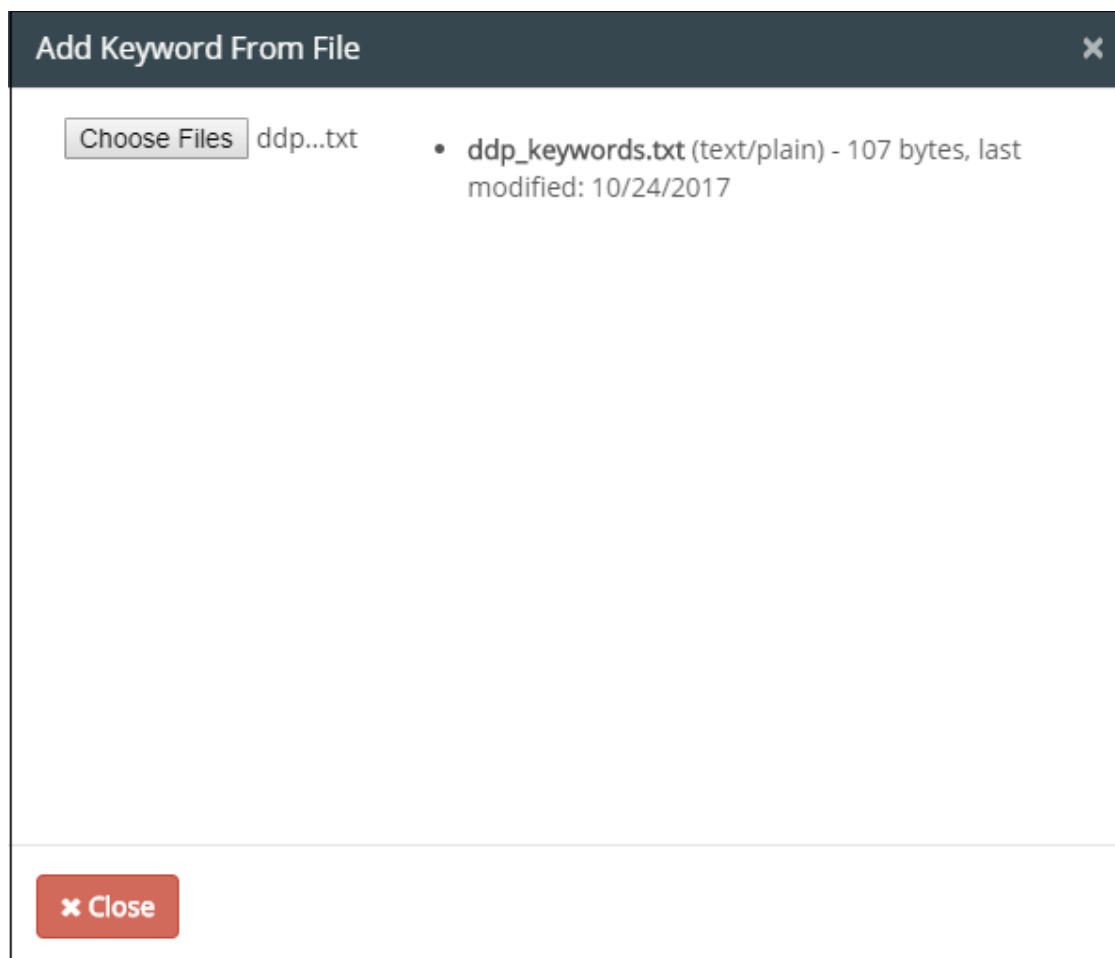
Please note the keywords should be saved on separate lines in the text file.

- Click 'Add from file' at the top of the 'Add Keyword' dialog:



- Click 'Choose Files' and open the text file you wish to import.

The selected file will be listed.



- Click 'Close'.

The list of added keywords will be shown in the interface as follows:

**Add Keyword** + Add from file + Add Delete

**Keyword**

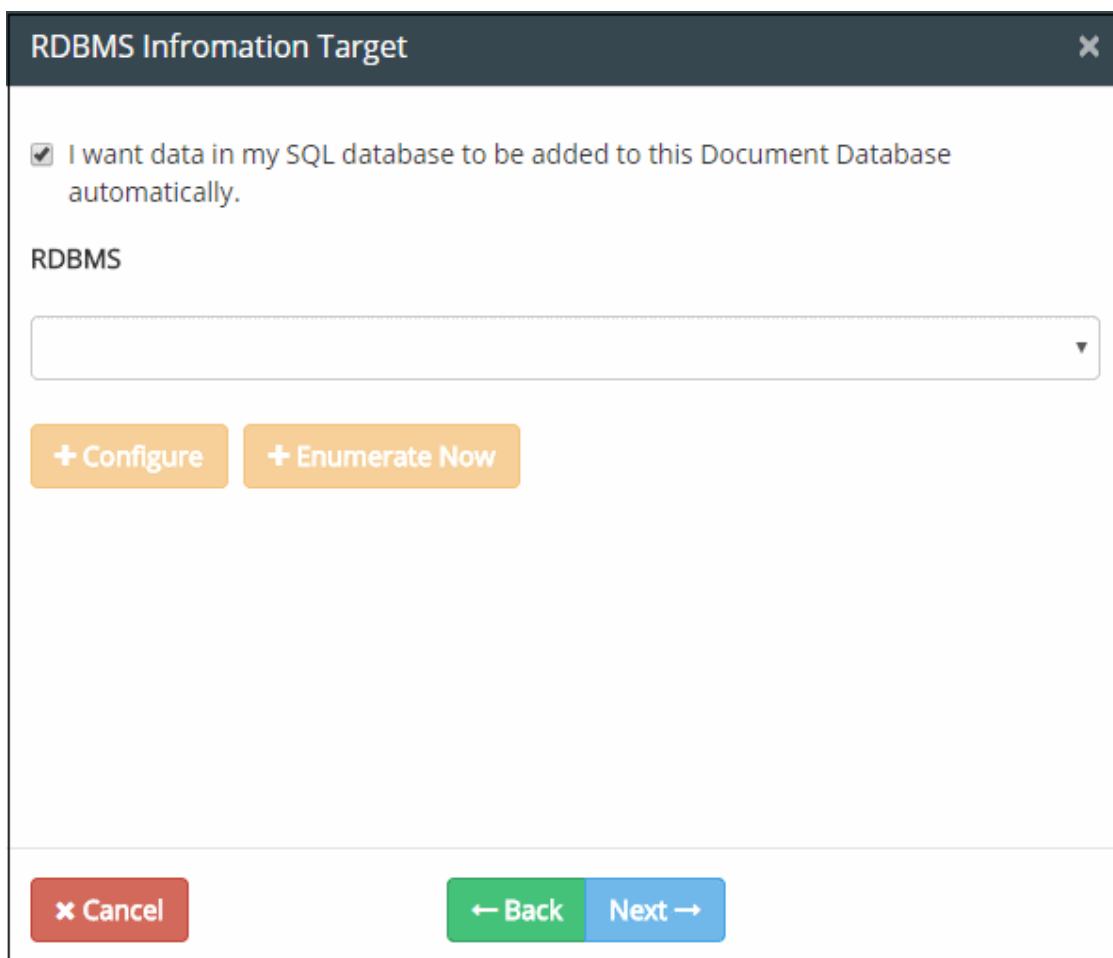
- https://adwords.google/KeywordPlanner
- credit card
- debit credit card
- credit card bank
- credit card number

Cancel ← Back Next →

- By default, all imported keywords will be included in the keyword database.
- To remove a keyword, select it and click 'Delete'. Repeat the process to delete more keywords.
- Click 'Next'

### Step 3 - Integrating a MySQL Database to Keyword Database

The RDMBS Information Target dialog will be displayed.



RDBMS Information Target

☒ I want data in my SQL database to be added to this Document Database automatically.

RDBMS

+ Configure + Enumerate Now

x Cancel ← Back Next →

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

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

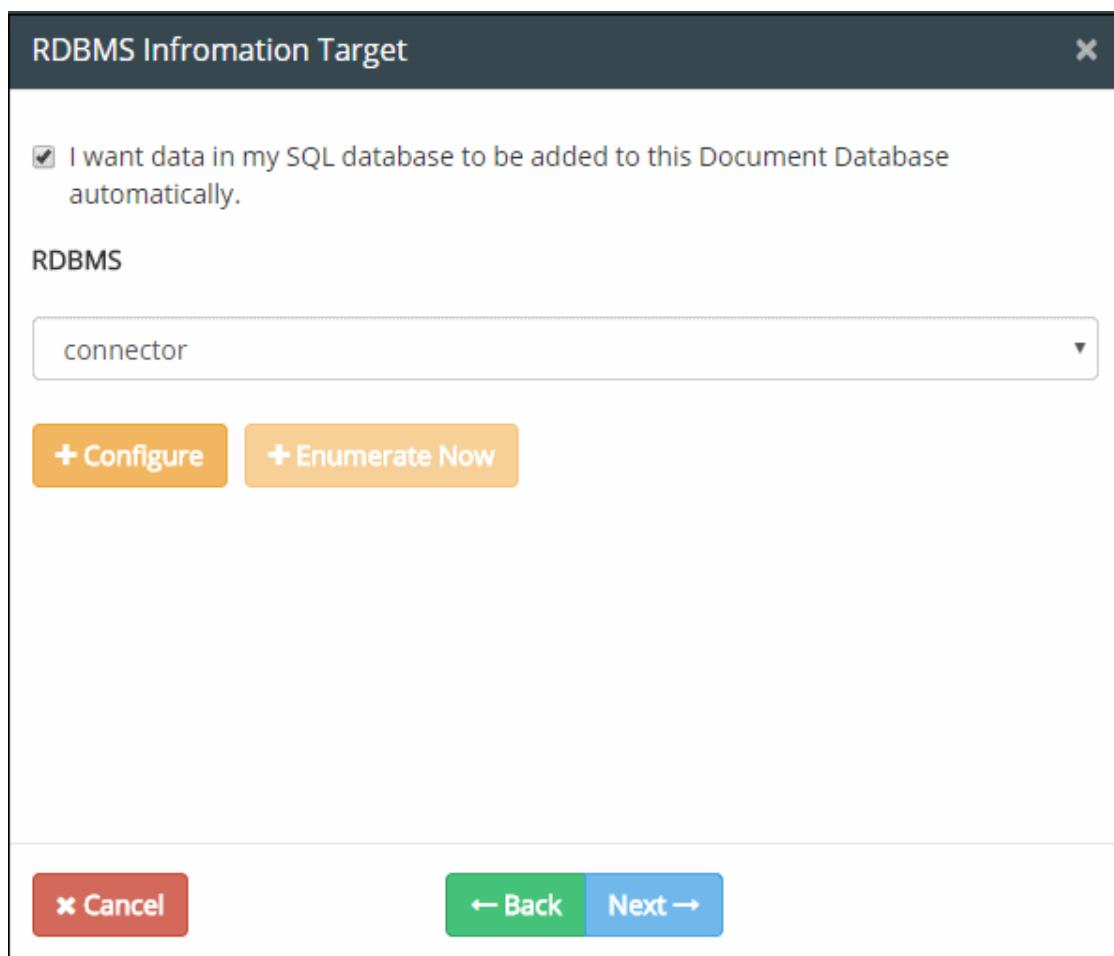
If you have RDBMS Connections configured already, a list of available connections will be shown in the RDBMS drop-down.

**Tip:** You can add RDBMS connections through the 'RDBMS Connections' interface. See [Integrate RDBMS Systems](#) for more details.



The screenshot shows a window titled "RDBMS Information Target" with a close button (X) in the top right corner. Inside the window, there is a checked checkbox with the text "I want data in my SQL database to be added to this Document Database automatically." Below this, the label "RDBMS" is followed by a dropdown menu. The dropdown menu is open, showing a list with the item "connector" selected and highlighted in blue. Below the dropdown menu are two orange buttons: "+ Configure" and "+ Enumerate Now". At the bottom of the window, there are three buttons: a red "X Cancel" button, a green "← Back" button, and a blue "Next →" button.

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



**RDBMS Information Target** [X]

☒ I want data in my SQL database to be added to this Document Database automatically.

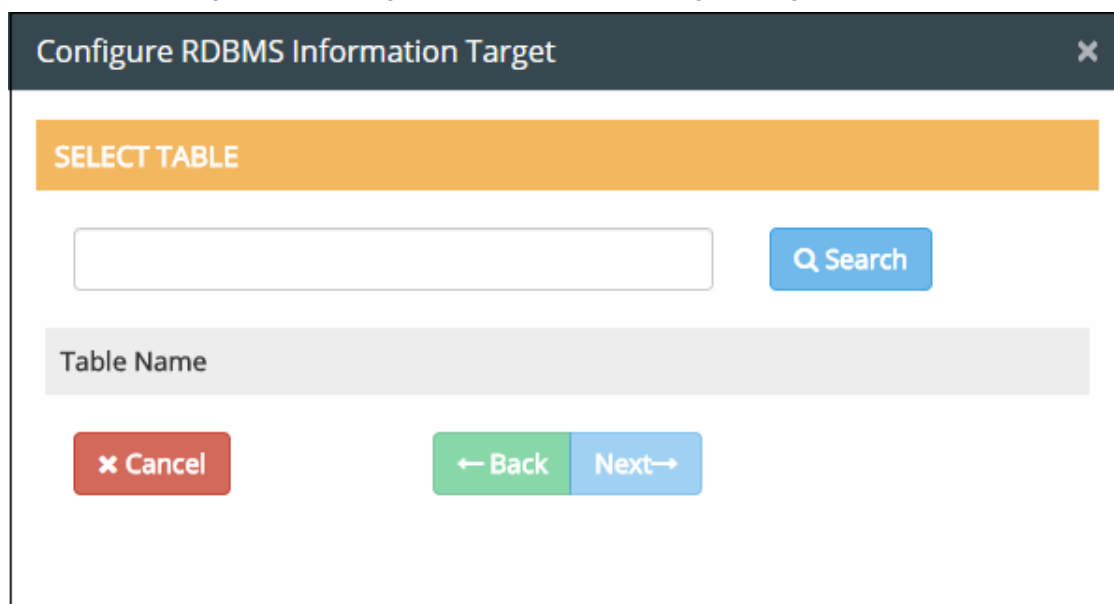
RDBMS

connector [v]

**+ Configure** **+ Enumerate Now**

**X Cancel** **← Back** **Next →**

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



**Configure RDBMS Information Target** [X]

**SELECT TABLE**

[Text Field] **Q Search**

Table Name

**X Cancel** **← Back** **Next →**

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

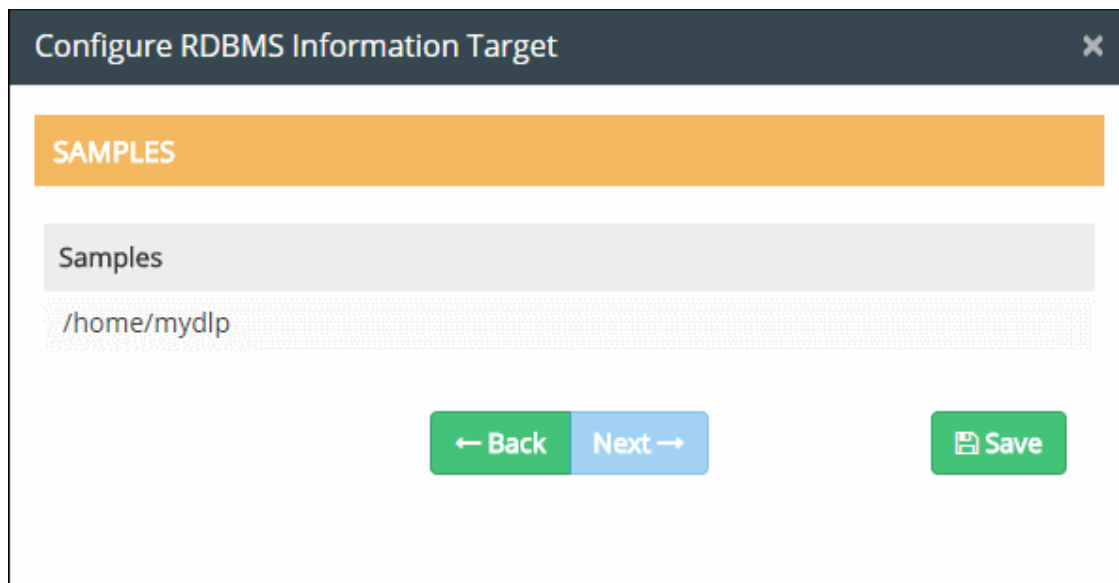
The screenshot shows a dialog box titled "Configure RDBMS Information Target" with a close button (X) in the top right corner. Below the title bar is an orange header labeled "SELECT TABLE". Underneath is a search bar containing the text "do" and a blue "Search" button with a magnifying glass icon. Below the search bar is a list of table names under the heading "Table Name". The first item, "documents", is highlighted in light blue and has a green checkmark to its left. At the bottom of the dialog are three buttons: a red "Cancel" button with a close icon, a green "Back" button with a left arrow, and a blue "Next" button with a right arrow.

The 'Select Column' dialog will appear.

The screenshot shows the same dialog box titled "Configure RDBMS Information Target" with a close button (X) in the top right corner. Below the title bar is an orange header labeled "SELECT COLUMN". Underneath is a search bar and a blue "Search" button with a magnifying glass icon. Below the search bar is a list of column names under the heading "Column Name". The list contains three items: "idx", "doc\_name", and "doc\_path". At the bottom of the dialog are three buttons: a red "Cancel" button with a close icon, a green "Back" button with a left arrow, and a blue "Next" button with a right arrow.

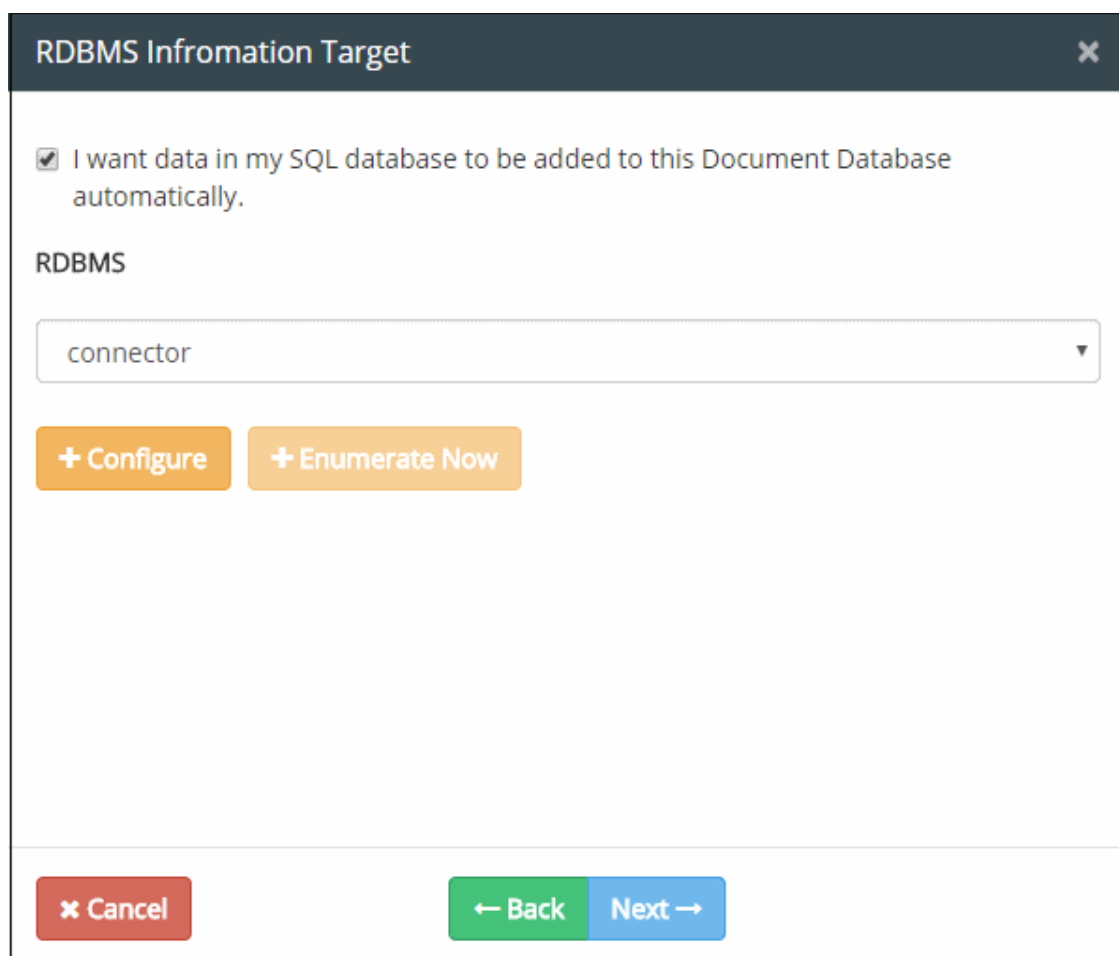
You can search for particular column by entering the first few characters of the column header in the field and clicking 'Search'. All the column headers with the matching names will be displayed in the list below. To view all the items, click 'Search' keeping the field blank.

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



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

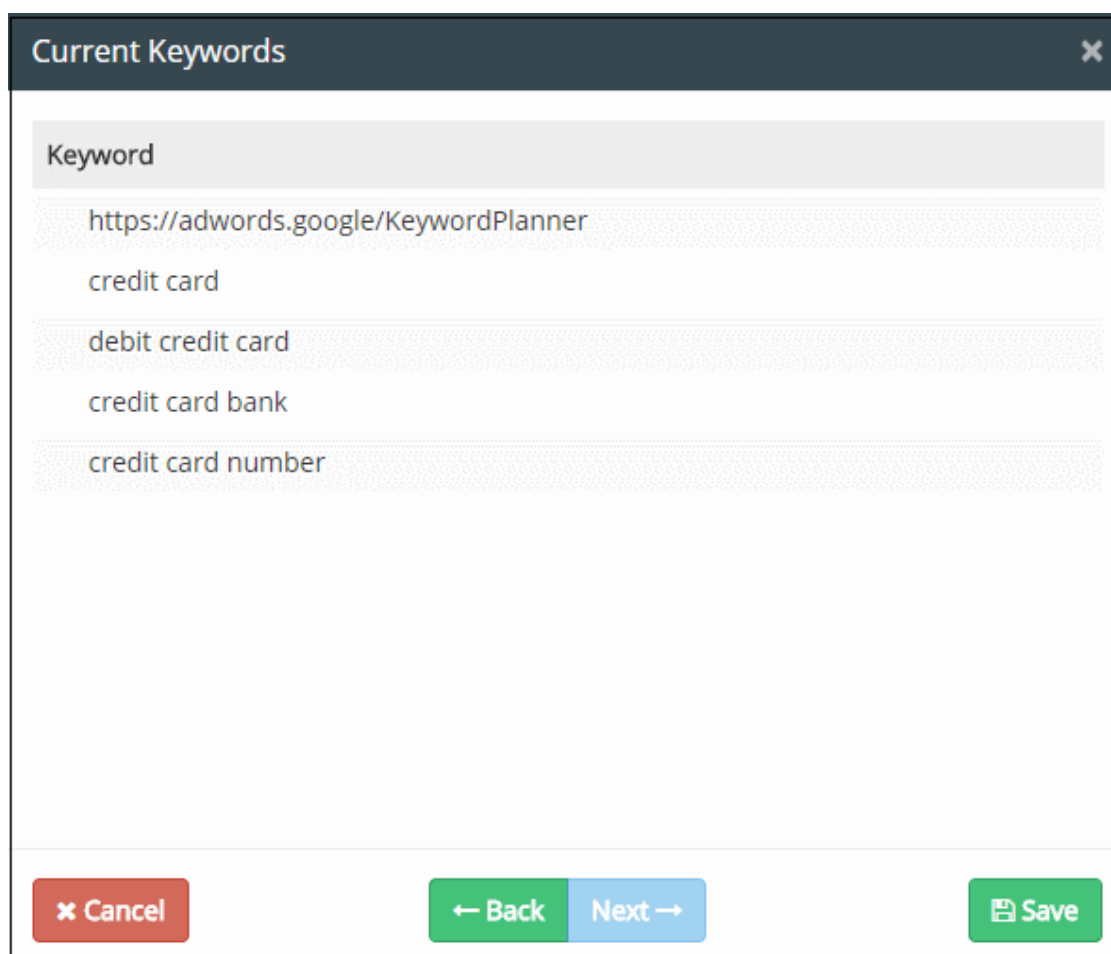
- Check whether the correct table and column are chosen from the displayed keywords. Click 'Back' in any of the screens to review your parameters.
- Click 'Save'



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

- Click 'Next'

The 'Current Keywords' screen will be displayed.



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

The added keyword database will be listed.



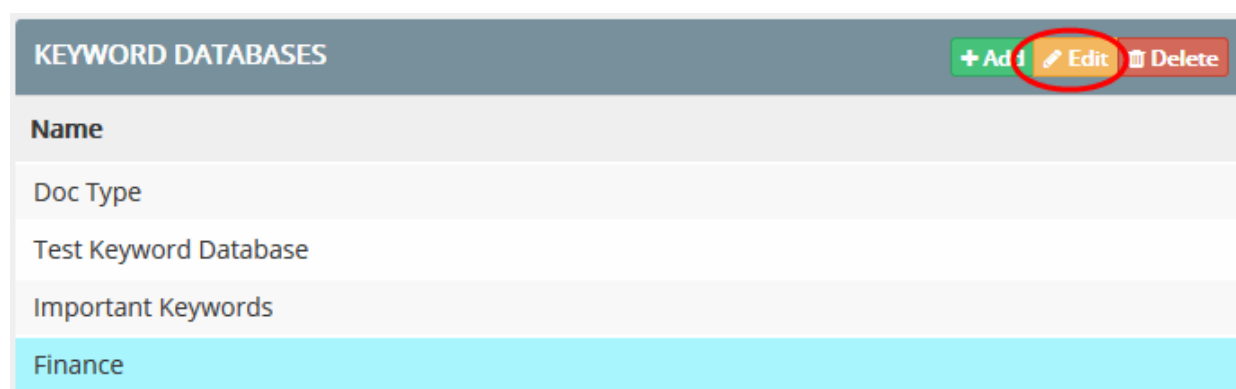
This will be available for selection in the Information Type object for specifying the Keyword Group component. See ['Add a User Defined Information Type'](#) for more details.

#### 5.3.3.2. Edit a User Defined Keyword Database

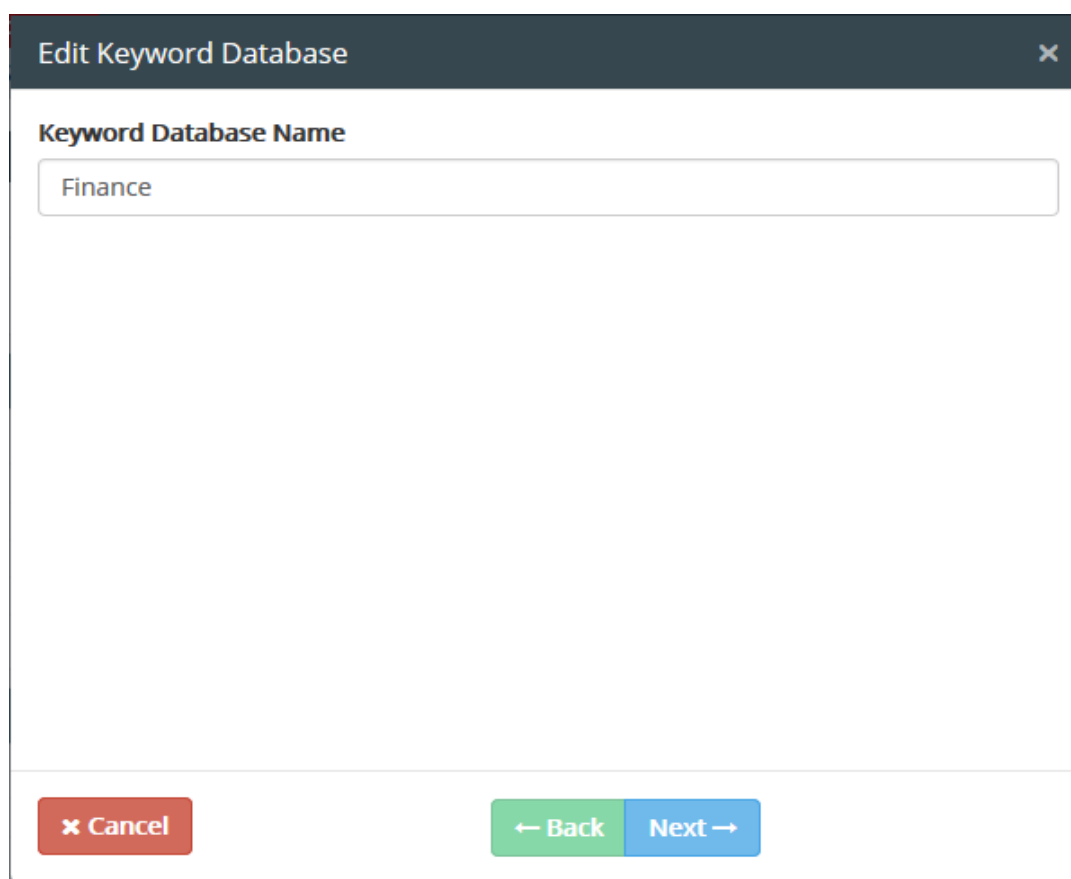
- Administrators can modify a keyword database at anytime to add new keywords or to remove existing keywords from the group.
- If a keyword group is altered, the policy has to be re-deployed to the network for the changes to propagate to the rules. Click 'Install Policy' to do this.

**To edit a keyword database**

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



The 'Edit Keyword Database' dialog will be displayed:



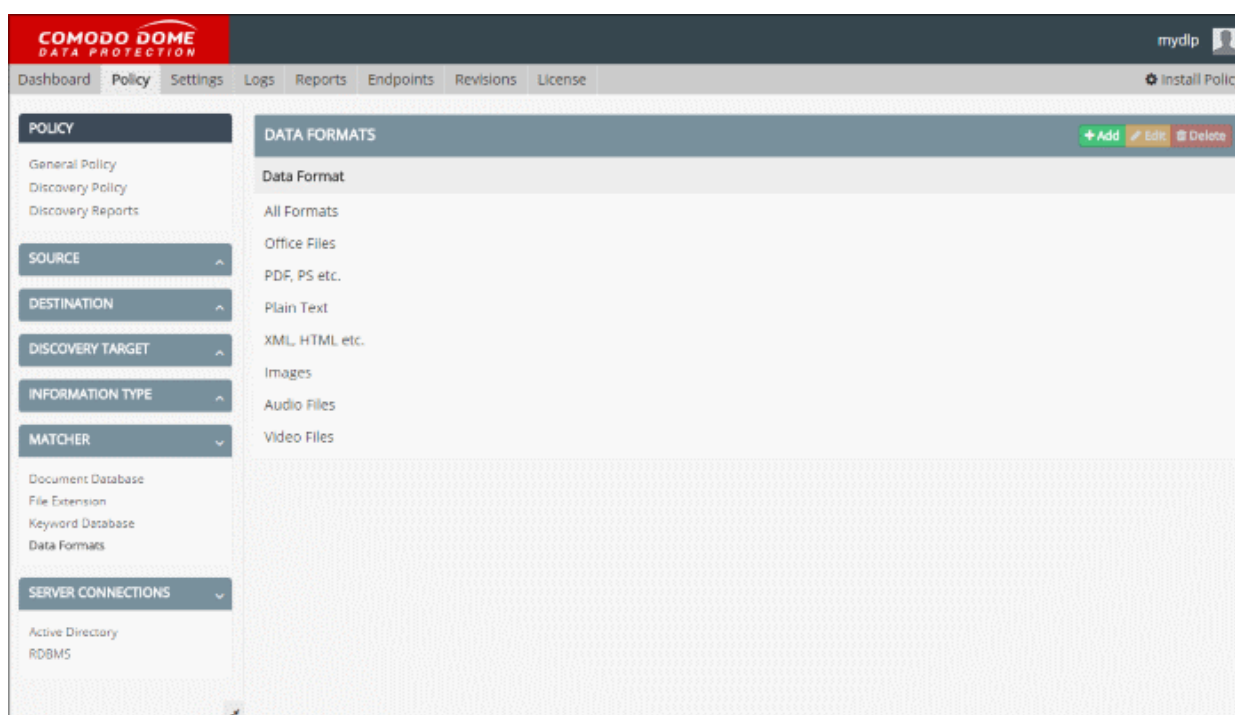
All keywords included in the database will be displayed in the respective screens. The 'Edit' process is same as adding a keyword database. See '[Add a User Defined Keyword Database](#)' for more details.

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

You must reinstall the policy for the edit to take effect (click the 'Install Policy' button at top-right). The change will apply to all rules which have an information object which uses this database. See '[Deploy a Policy](#)' for more details.

### 5.3.4. Manage Data Formats

- CDDP is capable of protecting a wide range of data types and formats.
- Data Formats are organized into broad genres (such as 'Audio Files', 'Images' and so on ) which in turn contain a list of specific types (like '.mp3', '.wav' or '.jpg', '.bmp').
- CDDP also allows you to add custom data formats and file types and to edit existing user defined data formats.
- These data formats will be available for selection when adding or editing an 'Information Type' object.
- You can view, edit and add file genres and file formats by selecting the 'Data Formats' under the 'Matcher' section.
- The file formats for each genre, can be defined as MIME Type or file extension.
- To open the 'Data Formats' screen, click 'Matcher' on the left and then 'Data Formats'



Click the links below to know how to manage the Data Formats:

- [Add a new Data Format](#)
- [Edit a Data Format](#)

#### 5.3.4.1. Add a New User Defined Data Format Entry

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

##### To add a new data format

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

The 'Add Data Format' dialog will be displayed.

**DATA FORMATS** + Add Edit Delete

**Data Format**

All Formats

**Add Data Format** ×

**Data Format Name**

Finance Samples

× Cancel ← Back Next →

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

The 'MIME Type' dialog will appear.

**Add Information Type** + Add Edit Delete

**Mime Type**

No data available in table
----------------------------

× Cancel ← Back Next → Save

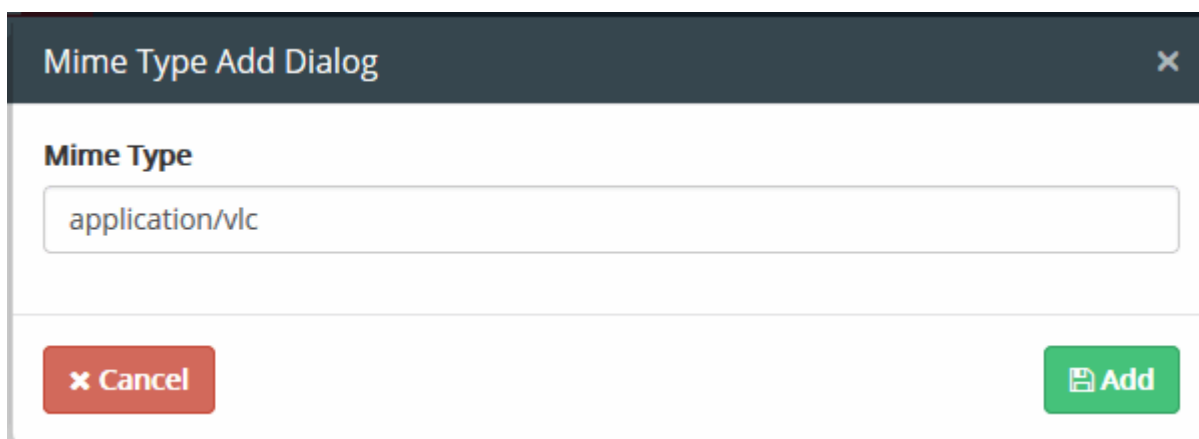


**Background Note:** The MIME type is a two part string identifier for a file type, containing the "type"/ "subtype". The "type" refers to a logical grouping of many MIME types that are closely related to each other. "subtypes" are specific to one file type within the "type".

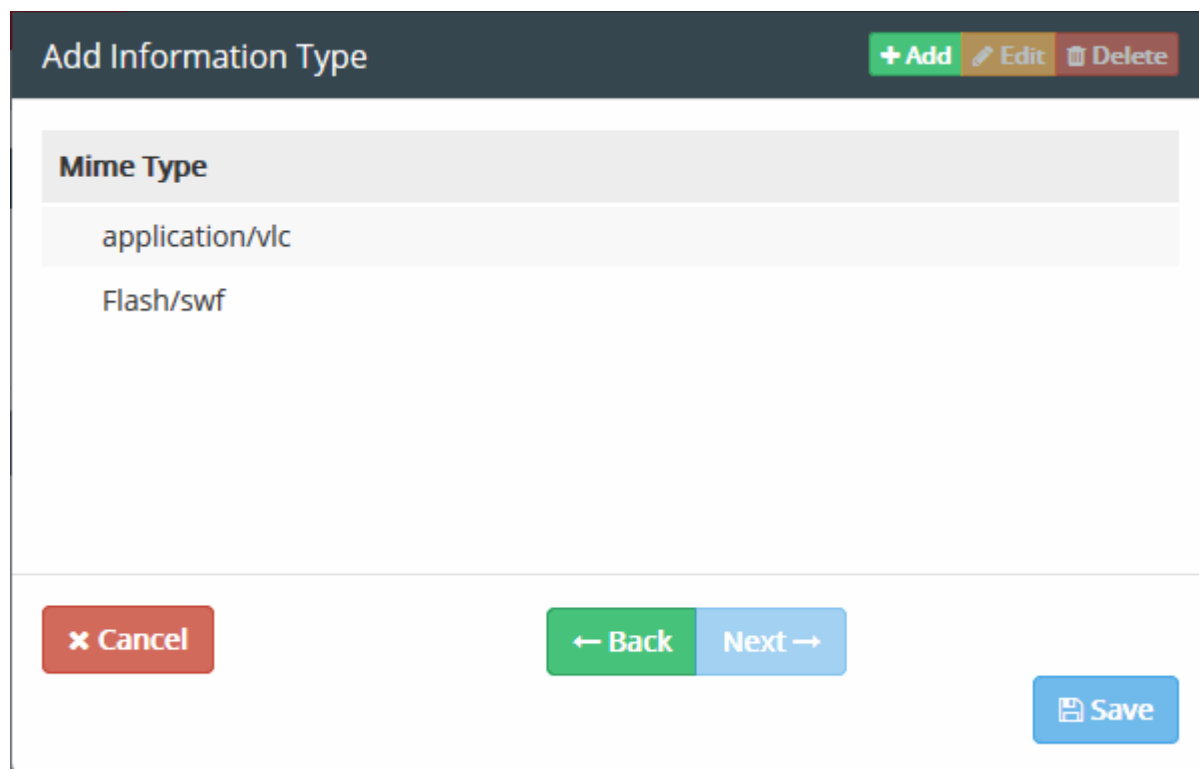
For example, the MIME value "images/jpg" is used for jpeg image files and specifies that the "jpg" subtype belongs to the "image" type.

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

The 'MIME Type Add Dialog' will be displayed.



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



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

The Data Format will be saved and listed.



For the changes to propagate through the rules in which the data format being edited is applied, the policy needs to be re-deployed. See [Deploy a Policy](#) for more details.

#### 5.3.4.2. Edit a Data Format

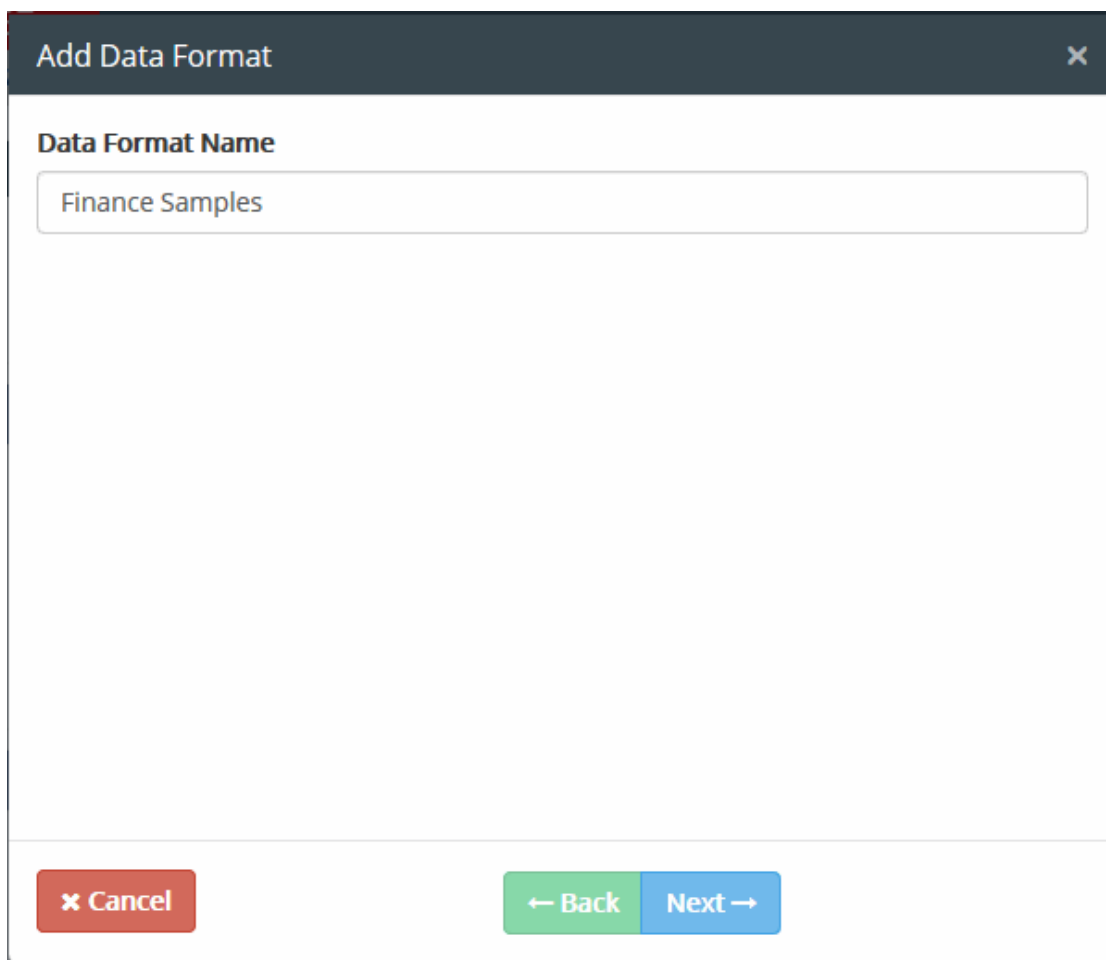
The administrator can add more or remove existing file types by editing the Data Format. Each Data Format contains file types belonging to a genre. CDDP allows the file types to be added as both MIME Type and file extension. Please note you can edit only the user defined data format type.

##### To edit a data format

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



The 'Add Data Format' dialog will be displayed:



**Add Data Format** [X]

**Data Format Name**

Finance Samples

[X] Cancel   ← Back   Next →

- Click 'Next'

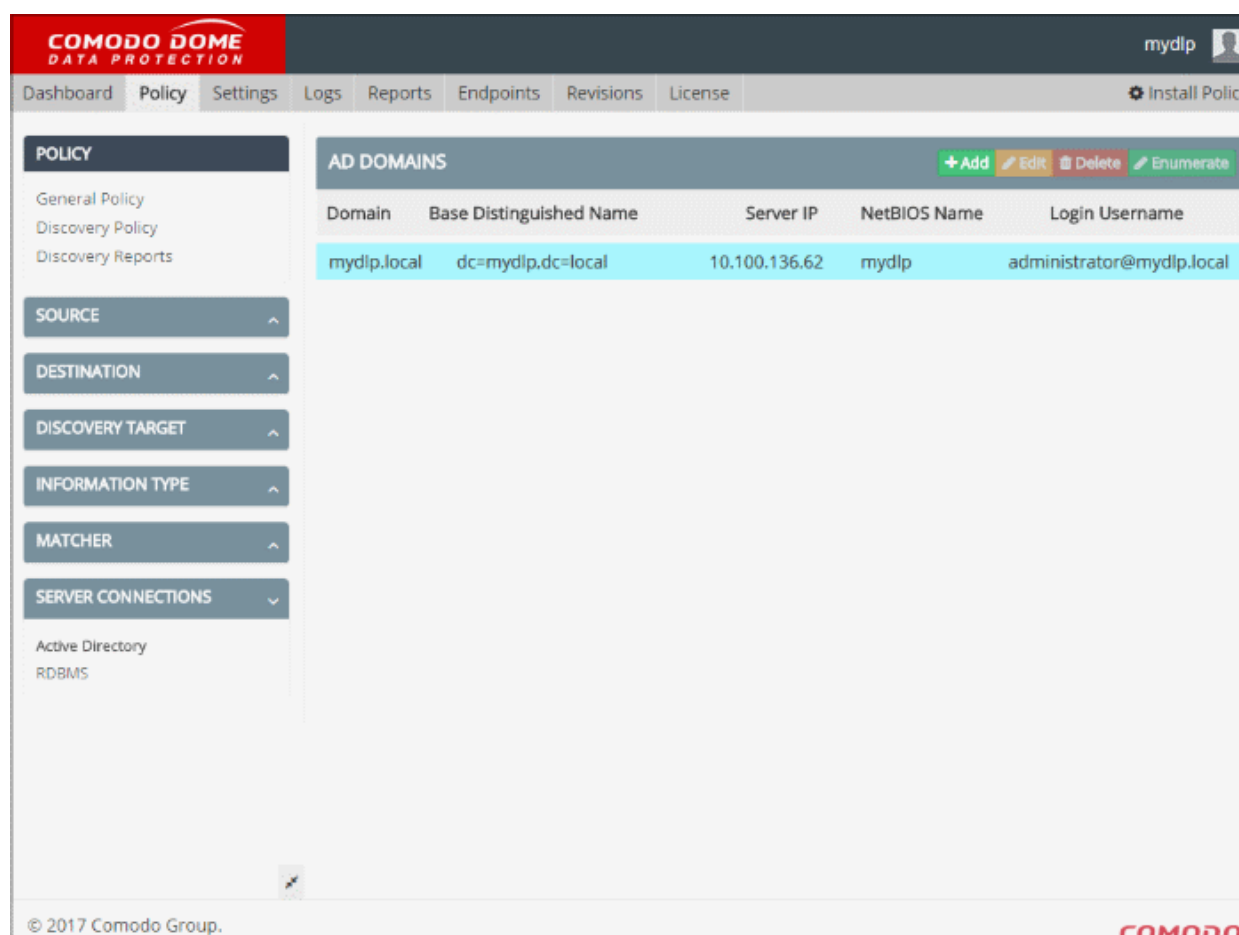
The screenshot shows a window titled "Add Information Type". At the top right of the window are three buttons: "+ Add" (green), "Edit" (orange), and "Delete" (red). The main content area has a header "Mime Type" and a list of items. The first item, "application/vlc", is highlighted in light blue and has a green checkmark to its left. Below it is the text "Flash/swf". At the bottom of the window are four buttons: "Cancel" (red), "Back" (green), "Next" (blue), and "Save" (blue).

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

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

## 5.4. Integrate Active Directory Domains

- Comodo Dome Data Protection allows you to import users from Active Directory (AD) Domains integrated to it.
- The 'Server Connections' > 'Active Directory' section allows to integrate AD domains which in-turn, can be used in User objects.
- The User groups from the AD, can be defined as User Objects for Source Objects for all types of Data Transfer Policy rules.
- Click 'Policy' tab at the top > 'Server Connections' > 'Active Directory' to open the interface



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

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

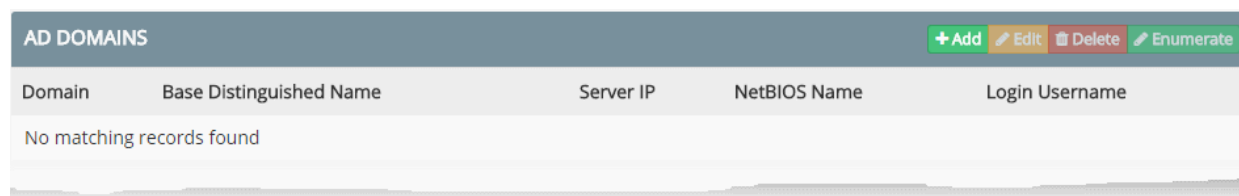
### 5.4.1. Add a New AD Domain

- Integrate new AD Domain by specifying the domain name, IP Address of the Domain Controller (DC) and the login credentials for Comodo Dome Data Protection to access the AD server.
- If there are more than one domain with separate domain controllers, you need to integrate them one-by-one.
- Before starting the integration process, make sure that:
  - Your DDP server has access to the AD server
  - Your local DNS is configured properly

#### To integrate a new AD Domain

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

The AD Domains screen will be displayed.



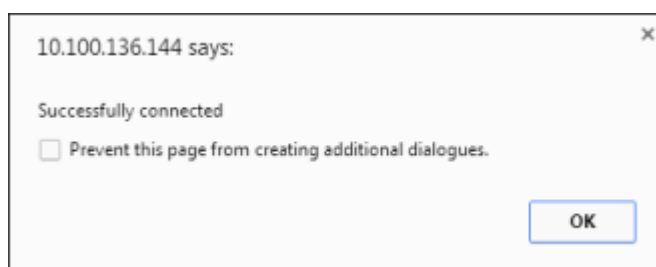
- Click the 'Add' button at top-right

- 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 CDDP to login to the AD server and import the users.  For security reasons, it is advised to create a new account for CDDP with only the required privileges to

	enumerate all users and groups in your AD domain.
Aliases	Click 'Add' and include the Aliases names of the AD domain.

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



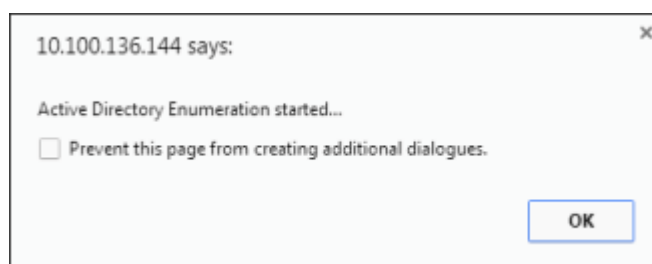
After successful connection, Save button will appear in the 'Add AD Domain' dialog.

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

AD DOMAINS					<a href="#">+ Add</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Enumerate</a>
Domain	Base Distinguished Name	Server IP	NetBIOS Name	Login Username				
mydlp.local	dc=mydlp,dc=local	10.100.136.62	mydlp	administrator@mydlp.local				

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

The AD enumeration process will begin....



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

The AD users now can be added as user object. See '[Add a User Defined Active Directory Users Object](#)' for more details.

### 5.4.2. Edit Existing AD Domains

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

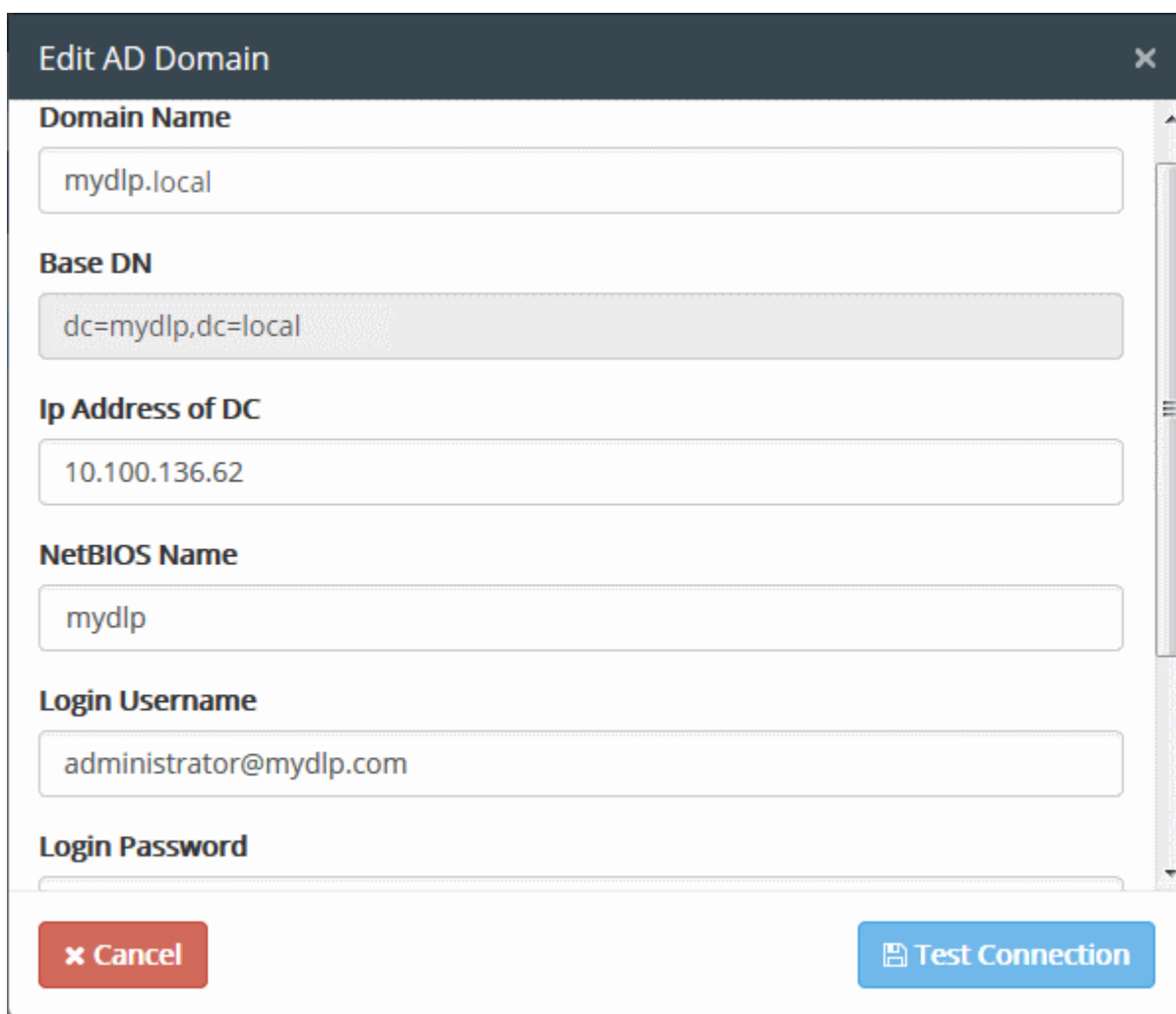
#### To edit an 'AD Domain'

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

AD DOMAINS					<a href="#">+ Add</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Enumerate</a>
Domain	Base Distinguished Name	Server IP	NetBIOS Name	Login Username				
mydlp.local	dc=mydlp,dc=local	10.100.136.62	mydlp	administrator@mydlp.local				

The 'Edit AD Domain' dialog will be displayed.





**Edit AD Domain**

**Domain Name**  
mydlp.local

**Base DN**  
dc=mydlp,dc=local

**Ip Address of DC**  
10.100.136.62

**NetBIOS Name**  
mydlp

**Login Username**  
administrator@mydlp.com

**Login Password**

**Buttons:**  
Cancel Test Connection

The Edit interface is similar to 'Add AD Domain' dialog. The administrator can directly edit the details, test the connections and save the changes. See [Add a New AD Domain](#) for more details on the parameters that can be configured through the interface.

- To remove an AD Domain, select it and click 'Delete'. Please note you cannot delete an AD Domain from which user objects are added. See [Add a User Defined Active Directory Users Object](#) for more details.

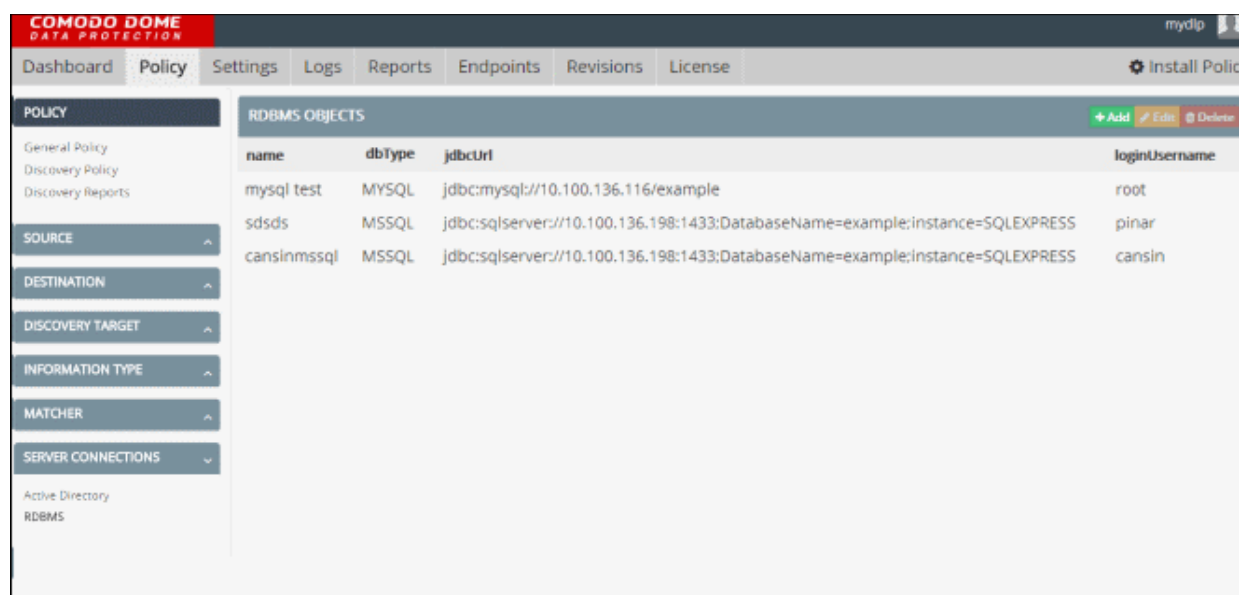
## 5.5. Integrate RDBMS Systems

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

Click the links below for more information on importing data from the MySQL Servers:

- [Integrating a MySQL Database to Keyword Database](#)
- [Integrating a MySQL database to document database](#)

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



Click the links below for more details on:

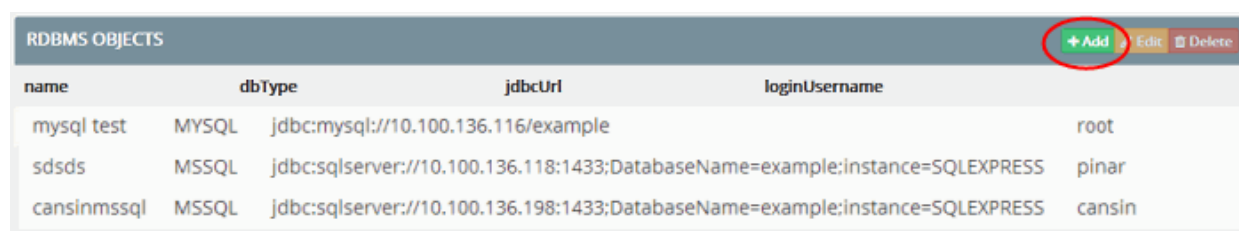
- [Add a new RDBMS Object](#)
- [Edit an RDBMS Object](#)

### 5.5.1. Add a New RDBMS Object

- Add a new RDBMS object to integrate MySQL, MsSQL or Oracle database server with CDDP by specifying the URL and login credentials of the RDBMS server.
- If there are more than one database server, you need to add them one-by-one.

To add a new RDBMS object

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



The 'Add RDBMS Connection' dialog will be displayed.

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

Field	Description
Database Type	Choose the type of database from the drop-down. The available options are: <ul style="list-style-type: none"> <li>• MySQL</li> <li>• MsSQL</li> <li>• Oracle</li> </ul>
Name	Enter a name shortly describing the connection.
JDBC URL	Enter the Java Database Connectivity (JDBC) URL of the RDBMS server
Login username and Login password	Enter the username and password of a valid user account for CDDP to login to the RDBMS server.  For security reasons, it is advised to create a new account in the server for Comodo CDDP with only the required privileges to enumerate required entries from the server.

- Click 'Save'

CDDP will connect to the server and if the credentials are successful, the RDBMS server will be connected to CDDP. The database server will be available for selection for importing keywords or documents when creating

**Keyword Database** and **Document Database** under the Matcher section.

### 5.5.2. Edit an RDBMS Object

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

RDBMS OBJECTS			
name	dbType	jdbcUrl	loginUsername
mysql test	MYSQL	jdbc:mysql://10.100.136.116/example	root
sdsds	MSSQL	jdbc:sqlserver://10.100.136.118:1433;DatabaseName=example;instance=SQLEXPRESS	pinar
cansinmssql	MSSQL	jdbc:sqlserver://10.100.136.198:1433;DatabaseName=example;instance=SQLEXPRESS	cansin

The 'Edit RDBMS Connection' dialog will be displayed.

Edit RDBMS Connection

Database Type

MYSQL

Name

sdsds

JDBC Url

jdbc:sqlserver://10.100.136.118:1433;DatabaseName=example;instance=SQLEXPRESS

Login Username

mydlp

Login Password

•••••

Cancel

Save

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

## 6. Configure Comodo Dome Data Protection Settings

The 'Settings' interface lets you configure various parameters in CDDP.

The screenshot shows the 'Settings' interface of Comodo Dome Data Protection. The top navigation bar includes 'Dashboard', 'Policy', 'Settings' (active), 'Logs', 'Reports', 'Endpoints', 'Revisions', and 'License'. A user profile 'mydlp' is visible in the top right. Below the navigation bar, there are sub-tabs: 'Protocols' (active), 'Users', 'Endpoint', 'Advanced', and 'Enterprise'. The main content area is titled 'PROTOCOLS' and contains two columns of settings. The left column includes 'SMTP Helo Name' (mydlp.com), 'SMTP Next Hop Host' (localhost), 'SMTP Next Hop Port' (10027), and a checked checkbox for 'SMTP Bypass on Fail'. The right column includes 'ICAP Request Mod Path' (/dlp), 'ICAP Response Mod Path' (/dlp-respmod), an unchecked checkbox for 'Ignore Big ICAP Requests', 'ICAP Max Cons' (0), and 'ICAP Options TTL' (0). A 'Save' button is located at the bottom right of the settings area.

The interface contains five tabs:

- **Protocols** – Configure the protocols used by DDP to connect to endpoints and the web proxy server
- **Users** - Add and manage peer admin users
- **Endpoint** - Configure connection parameters for the CDDP server to connect to endpoints.
- **Advanced** - Configure advanced application settings
- **Enterprise** - Configure miscellaneous settings and email notifications

### 6.1. Configure Protocol Settings

- From the 'Protocols' area, you can:

- Configure Simple Mail Transfer Protocol (SMTP) settings to send mails from the CDDP server.
- Configure the Internet Content Adaptation Protocol (ICAP) parameters for your web proxy.
- Click 'Settings' > 'Protocols' to open the interface:

**COMODO DOME DATA PROTECTION** mydlp

Dashboard Policy **Settings** Logs Reports Endpoints Revisions License Install Policy

Protocols Users Endpoint Advanced Enterprise

### PROTOCOLS

**SMTP Hello Name**

**SMTP Next Hop Host**

**SMTP Next Hop Port**

☒ SMTP Bypass on Fail

**ICAP Request Mod Path**

**ICAP Response Mod Path**

☐ Ignore Big ICAP Requests

**ICAP Max Cons**

**ICAP Options TTL**

Save

Field	Description
SMTP Hello Name	The mail domain name used for HELO greeting command in SMTP protocol by the CDDP 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 CDDP 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 CDDP server. Default = 10027.
SMTP Bypass on Fail	Determines the behavior of email engine of CDDP in case of any error. If this option is selected, CDDP will pass mails on error case for availability. If this option is not selected, CDDP will block mails on error for security. Default = Selected.
ICAP Request Mod Path	The ICAP request module path used by the CDDP Server for integration with ICAP enabled web proxy. Default = /dlp

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

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

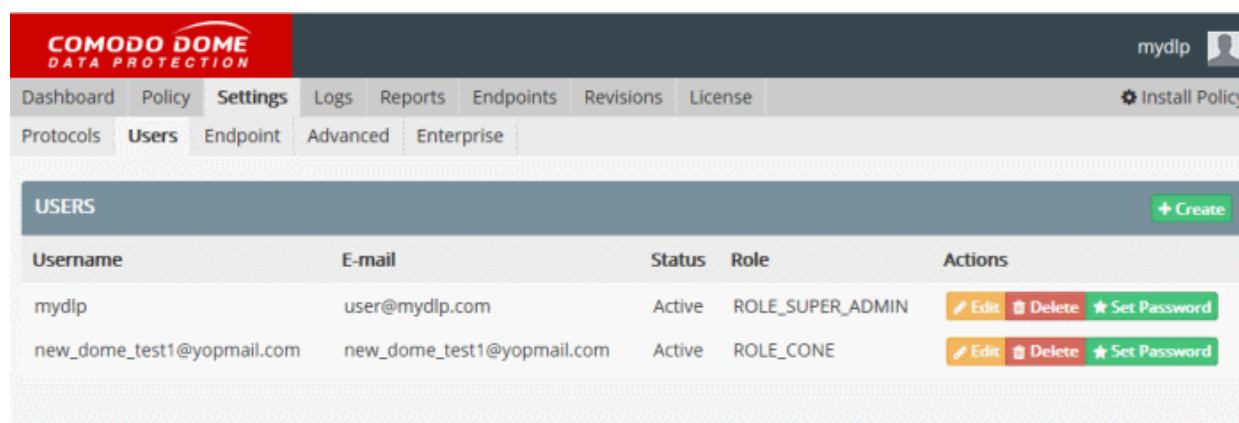
## 6.2. Manage Administrators

- Click 'Settings' > 'Users' to open this interface
- There are five admin roles in CDDP with different privilege levels:

Administrative Role	Description and Privilege Levels
Super Administrator	<p>Super Administrator role has the ultimate authority in a CDDP system. The Super Administrator can set up and configure CDDP during deployment.</p> <p>Super Administrator has all the privileges as shown below:</p> <ul style="list-style-type: none"> <li>Create and manage administrative users of any administrative role.</li> <li>See CDDP event logs and content data attached to event logs.</li> <li>Edit CDDP policy and objects</li> <li>Install policy</li> <li>Edit all settings under Settings Tab.</li> </ul>
Administrator	<p>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 be able to see the content data in CDDP incident logs and cannot download archived files.</p> <p>Administrator has the following privileges:</p> <ul style="list-style-type: none"> <li>Create and manage administrative users with roles of peer Administrator and Classifier and None.</li> <li>See CDDP event logs but cannot access files attached to logs.</li> <li>Edit CDDP policy and objects.</li> <li>Install policy.</li> <li>Edit all settings under Settings Tab, has restricted access to Users Tab.</li> </ul>
Auditor	<p>Auditor has restricted access to Logs Tab. The Auditor does not have the ability to change any settings or DDP policy. The Auditor can be an executive from legal department, will be able to see DDP event logs and can access</p>



	<p>content data attached to these logs.</p> <p>Authority Scope is a restriction which can be defined when CDDP is integrated with Microsoft Active Directory to limit the events that can be seen by the Auditor for one or more specified organization units.</p> <p>Auditor has the following privileges:</p> <ul style="list-style-type: none"> <li>• See all CDDP logs and content data attached to logs (If Authority Scope is not specified)</li> <li>• See CDDP logs related to specified Authority Scope (If Authority Scope Specified)</li> </ul>
Document Classifier	<p>Classifier has restricted access to the Objects Tab. Classifier can upload documents to previously specified Document Databases.</p> <p>Classifier has the following privileges:</p> <ul style="list-style-type: none"> <li>• Upload documents to predefined Document Databases</li> </ul>
None	<p>The administrator with the role 'None' will be able to receive the automated notifications sent by CDDP on occurrences of various incidents intercepted by the data transfer policy and discovery rules configured in CDDP. The administrator does not have any rights to create or modify the rules and cannot access CDDP administrative interface.</p>



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

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

### 6.2.1. Add New Administrative Users

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

#### To add a new administrative user

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



**USERS**

Username	E-mail	Status	Role	Actions
mydlp	user@mydlp.com	Active	ROLE_SUPER_ADMIN	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Set Password</a>

Edit User

Username

E-mail

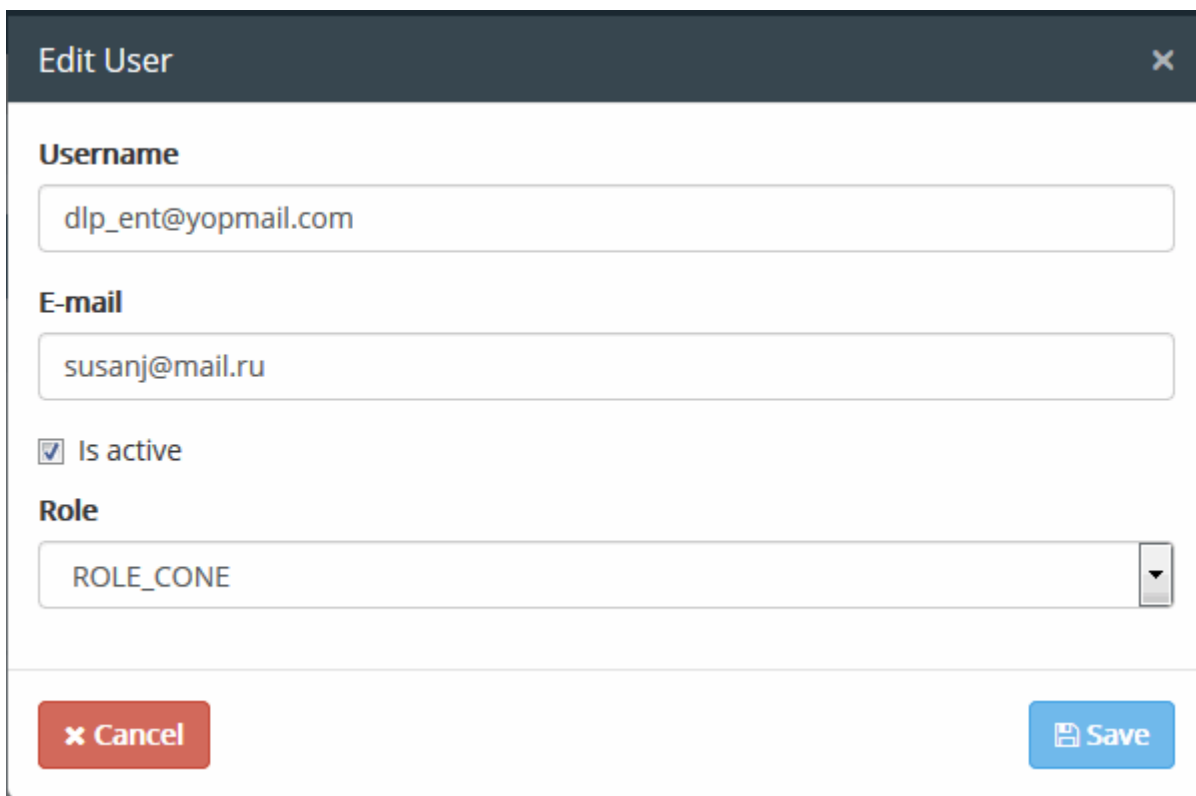
☒ Is active

Role

ROLE\_NONE
ROLE\_ADMIN
ROLE\_AUDITOR
ROLE\_CLASSIFIER
ROLE\_SUPER\_ADMIN
ROLE\_CONE
ROLE\_NONE

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

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



**Edit User**

**Username**  
dlp\_ent@yopmail.com

**E-mail**  
susanj@mail.ru

☒ Is active

**Role**  
ROLE\_CONE

**Cancel** **Save**

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

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

The new user will be added.

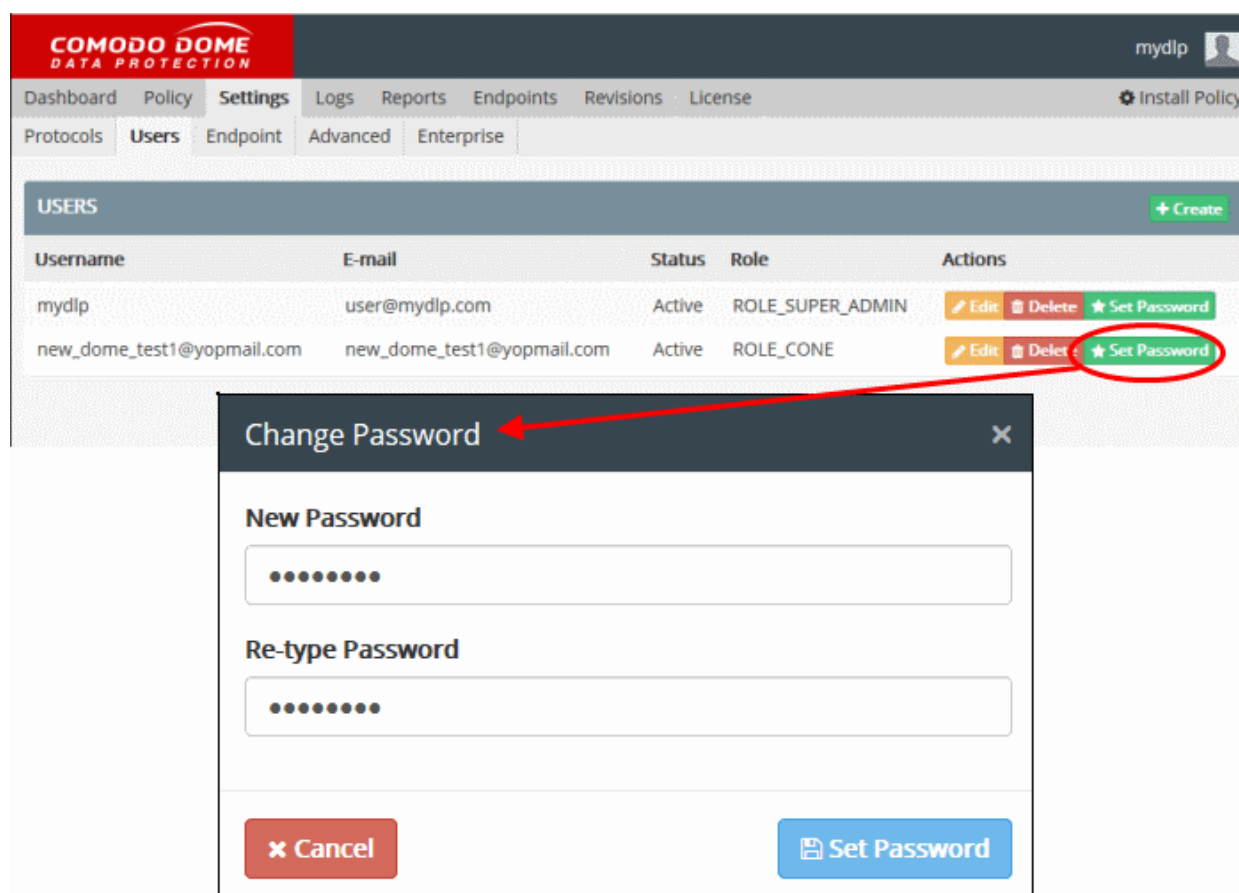
The next step is to set a password for the new administrative user to enable them to login. See **Set and Reset Password for Administrative Users** for explanation on setting password for the new user. Once logged-in the new administrator can change his/her login password by clicking their username displayed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

### 6.2.2. Set and Reset Password for Administrative Users

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

#### To set or Reset password for an administrative user

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



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

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

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

The screenshot displays the Comodo Dome Data Protection Administrator interface. The top navigation bar includes 'Dashboard', 'Policy', 'Settings', 'Logs', 'Reports', 'Endpoints', 'Revisions', and 'License'. The 'Settings' menu is circled in red, and a red arrow points from it to the 'Account Settings' dialog box. The 'Users' tab is selected, showing a table of users. The 'Account Settings' dialog box is open, showing fields for Username, Email, Current Password, New Password, and Reenter New Password. The 'Cancel' and 'Save' buttons are at the bottom.

Username	E-mail	Status	Role	Actions
mydlp	user@mydlp.com	Active	ROLE_SUPER_ADMIN	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Set Password</a>
new_dome_test1@yopmail.com	new_dome_test1@yopmail.com	Active	ROLE_CONE	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Set Password</a>

### Account Settings

**Username**

**Email**

**Current Password**

**New Password**

**Reenter New Password**

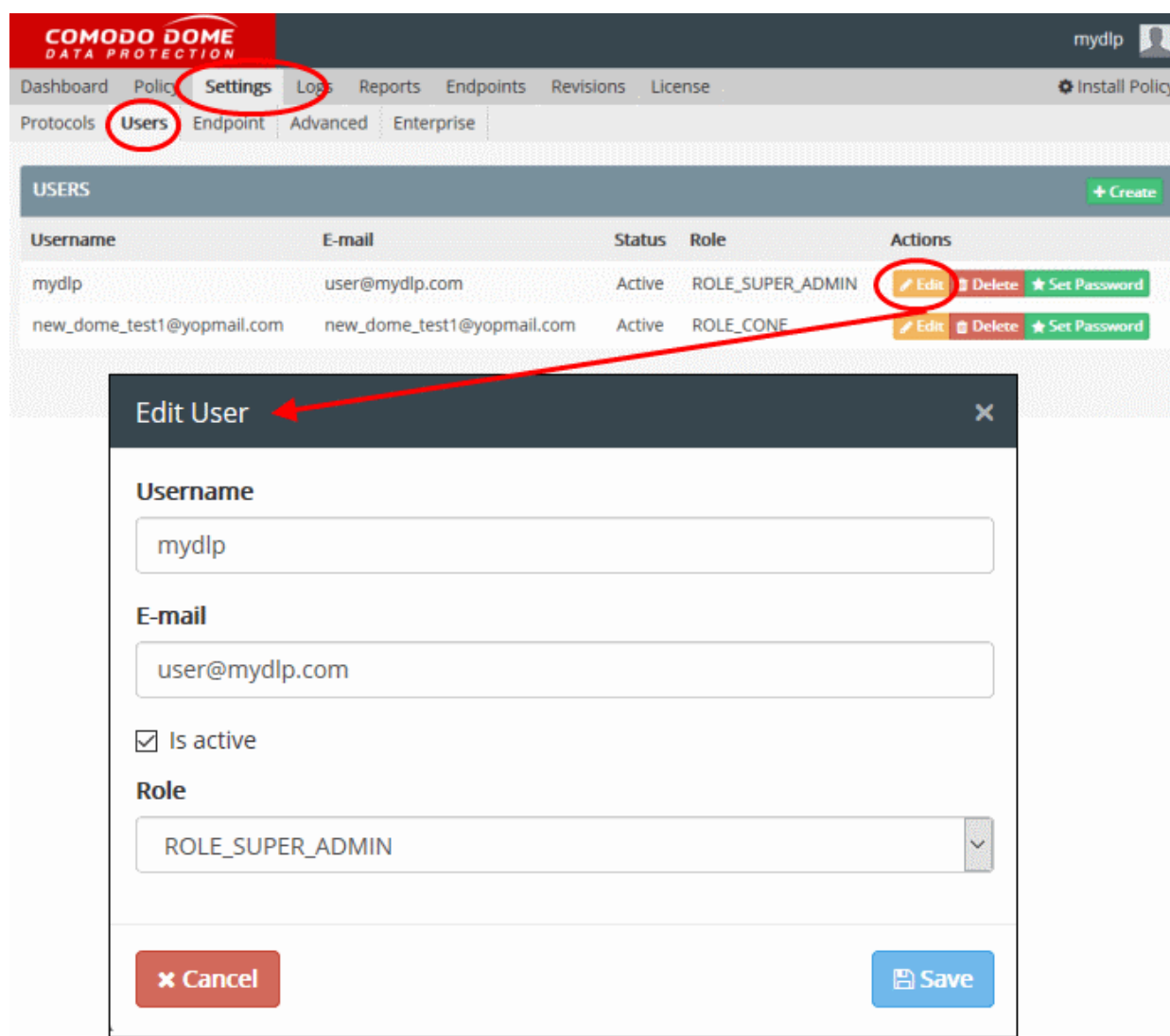
[Cancel](#) [Save](#)

### 6.2.3. Edit and Remove Admin Users

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

#### To edit an admin user

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



The dialog allows you to:

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

Click 'Save' for your changes to take effect.

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

## 6.3. Configure Endpoint Settings

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

- Click 'Settings' > 'Endpoint' to open the interface:

**COMODO DOME DATA PROTECTION** mydlp

Dashboard Policy **Settings** Logs Reports Endpoints Revisions License Install Policy

Protocols Users **Endpoint** Advanced Enterprise

### ENDPOINT

**Log Level**  
debug

**Log Limit**  
10.00 MB

☒ Ignore Max Size Exceeded Logs for Discovery Channel

**Log Spool Soft Limit**  
50.00 MB

**Log Spool Hard Limit**  
75.00 MB

**Secure Printer Prefix**  
MyDLP

**Endpoint Uninstallation Password**  
mydlp

**Default Sync Interval**  
10 Second(s)

### NETWORK BASED ENDPOINT SYNC INTERVALS

+ Create

IP Base	IP Mask	Seconds	Actions
No data available in table			

Save

Field	Description
Log Level	<p>Indicates the level of log details generated by endpoint agent that an administrator wants view.</p> <div> <p><b>ENDPOINT</b></p> <p><b>Log Level</b></p> <p>error</p> <p>error</p> <p>info</p> <p>debug</p> </div> <ul style="list-style-type: none"> <li>Info – Displays only the captured data based on policy</li> <li>Error – Displays error log at endpoint in addition to notification (Default value)</li> <li>Debug – Displays more details logs about system, error and incident logs. Helps system support engineers to get more detailed logs in case of having any problem at endpoint agent.</li> </ul> <p>Default = Error</p>



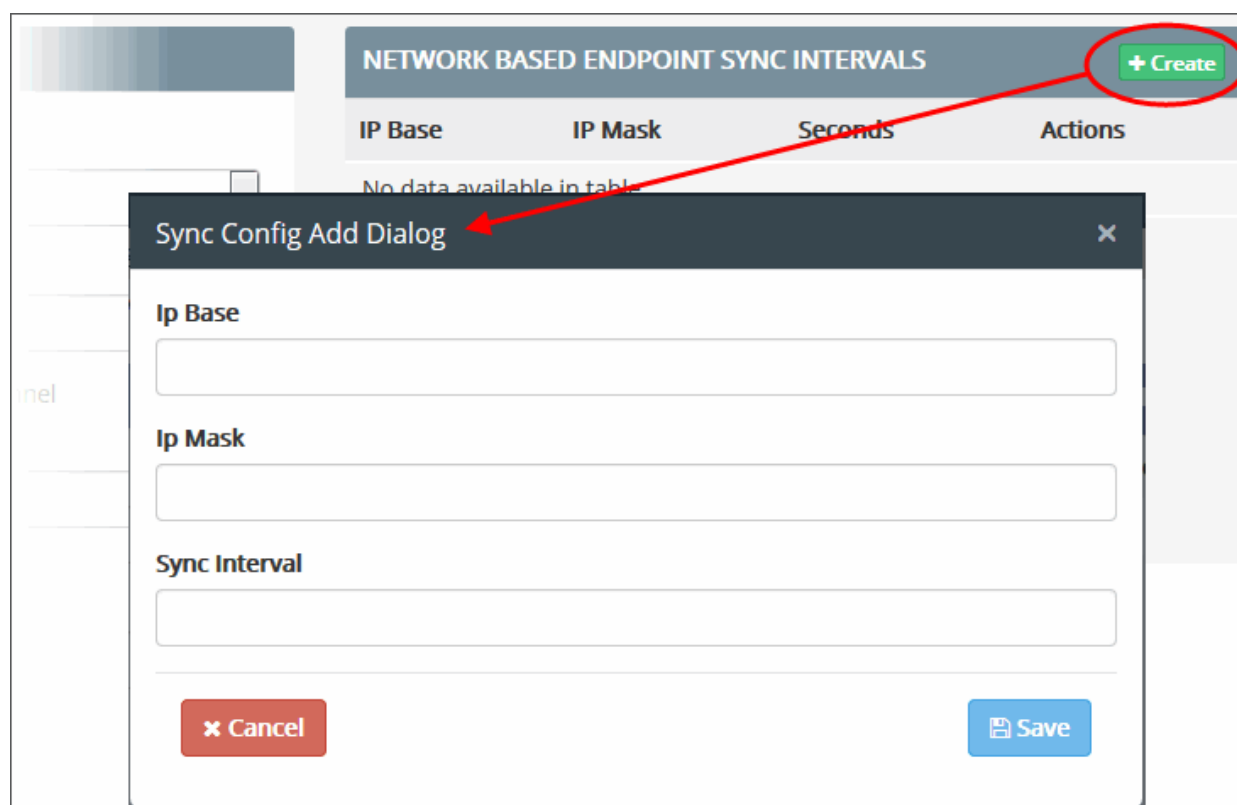
Log Limit	The maximum size (in MB) of the overall log file that can be stored in an endpoint. Default = 10 MB
Ignore Max Size Exceeded logs for Discovery Channel	Instructs CDDP to discard redundant logs that appear on identifying large number of files during discovery scans. Ignoring redundant logs conserves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

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

#### To set custom sync intervals for a network

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

The 'Sync Config Add Dialog' will appear.



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

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

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

## 6.4. Configure Advanced Settings

- The 'Advanced' tab of the 'Settings' interface allows to configure advanced parameters such as time-out periods and maximum sizes of memory objects, chunks and files.
- Comodo Dome Data Protection 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.
- Click 'Settings' > 'Advanced' tab to open the interface



**COMODO DOME DATA PROTECTION** mydlp

Dashboard Policy **Settings** Logs Reports Endpoints Revisions License Install Policy

Protocols Users Endpoint **Advanced** Enterprise

**ADVANCED**

**Maximum Object Size**  
10.00 MB

**Maximum Memory Object**  
0.20 MB

**Maximum Chunk Size**  
1.00 MB

**FSM Timeout**  
120 Second(s)

**Spawn Timeout**  
60 Second(s)

**Thrift Pool Size for Server**  
24

**Thrift Pool Size for Endpoint**  
3

**Supervisor Max Restart Count**  
5

**Supervisor Max Restart Time**  
20

**Supervisor Kill Timeout**  
20

**Query Cache Cleanup Interval**  
900000


**Query Cache Maximum Size**  
2000000

**Error Action**  
pass

**Refresh Time Interval for Log Tab**  
0 Second(s)

Save

Field	Description
Maximum Object Size	<p>The maximum chunk size of object which is processed in CDDP in MB. Default = 10 MB</p> <p>You can increase this value to analyze larger files. Although CDDP 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 '<b>Removable Storage Inbound rule</b>' in the section <b>View Details of a Log Entry</b> for more details.</p>
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 CDDP incident logging process. Default = 1 MB
FSM Timeout	The time-out interval for each state in Finite State Machines (FSM) in CDDP server which are used for processing ICAP, SMTP connections and communication between CDDP server and CDDP endpoints. Default = 120 Seconds

Spawn Timeout	The time-out of each spawned process in CDDP work flow. Default = 60 Seconds
Thrift Pool Size for CDDP Server	Active number of connections to the CDDP backend service which is used for converting files to the meaningful data in CDDP Server. Default = 24
Thrift Pool Size for CDDP Endpoint	Active number of connections to the CDDP backend service which is used for converting files to the meaningful data in CDDP Endpoint. Default = 3
Supervisor Max Restart Count	The maximum number of retry count for restarting worker processes controlled by a supervisor process. Default = 5
Supervisor Max Restart Time	The maximum waiting time (in milliseconds) for restarting workers controlled by the supervisor process. Default = 20 Milliseconds
Supervisor Kill Timeout	Upon termination of child/worker processes, the supervisor process sends 'Terminate' command and makes the child/worker process wait for an exit signal. If no exit signal is received within the specified time the child processes are unconditionally terminated. The 'Supervisor Kill Timeout' specifies the maximum waiting time (in milliseconds) for the 'Exit' signal. Default = 20 Milliseconds
Query Cache Cleanup Interval	The cache containing the queries generated by several channels (Web, Mail, Api, removable storage, etc.) is cleared periodically to maintain the efficiency. The 'Query Cache Cleanup Interval' specifies the time interval at which the cache is cleared. Default = 900000 Milliseconds.
Query Cache Maximum Size	The upper limit of size (in Bytes) of queries to be cached, for speeding up future queries coming from inspecting channels. Default = 2000000 Bytes
Error Action	<p>The action executed on data intercepted or discovered by CDDP if any error occurs in CDDP Server. Default = Pass. You can choose between 'Pass' and 'Block' as required from the drop-down.</p> 
Refresh Time Interval for Log Tab	The interval at which the log of events is updated and displayed under the 'Logs' tab of the CDDP console. Refer to the section <b>The Logs Tab</b> for more details.

## 6.5. Configure Enterprise Settings

- Click 'Settings' > 'Enterprise' tab to open this interface
- This area lets you configure various network, notification and syslog settings. These include mail archive settings, email notifications and more.

### Network Configurations

Comodo Dome Data Protection 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 web-pages 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. See [The Logs tab](#) for more details.

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

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

### Notification Configurations

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

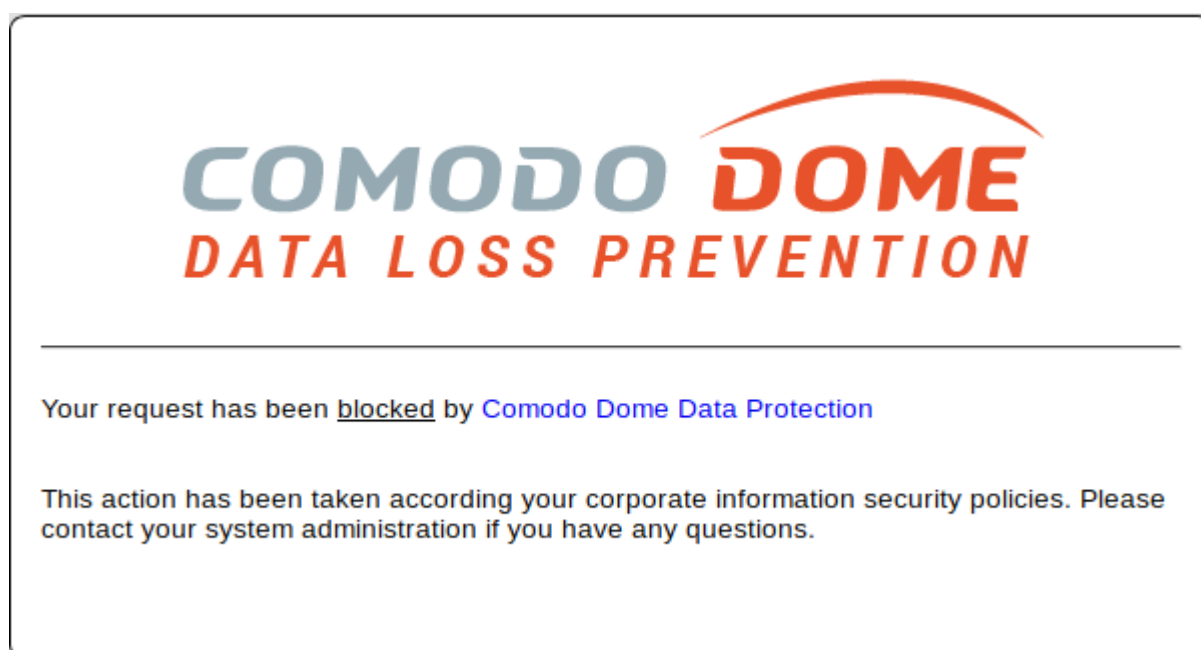
- Web
- Mail
- Removable Storage
- Printer
- API
- Endpoint Discovery
- Remote Discovery

Comodo Dome Data Protection 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.

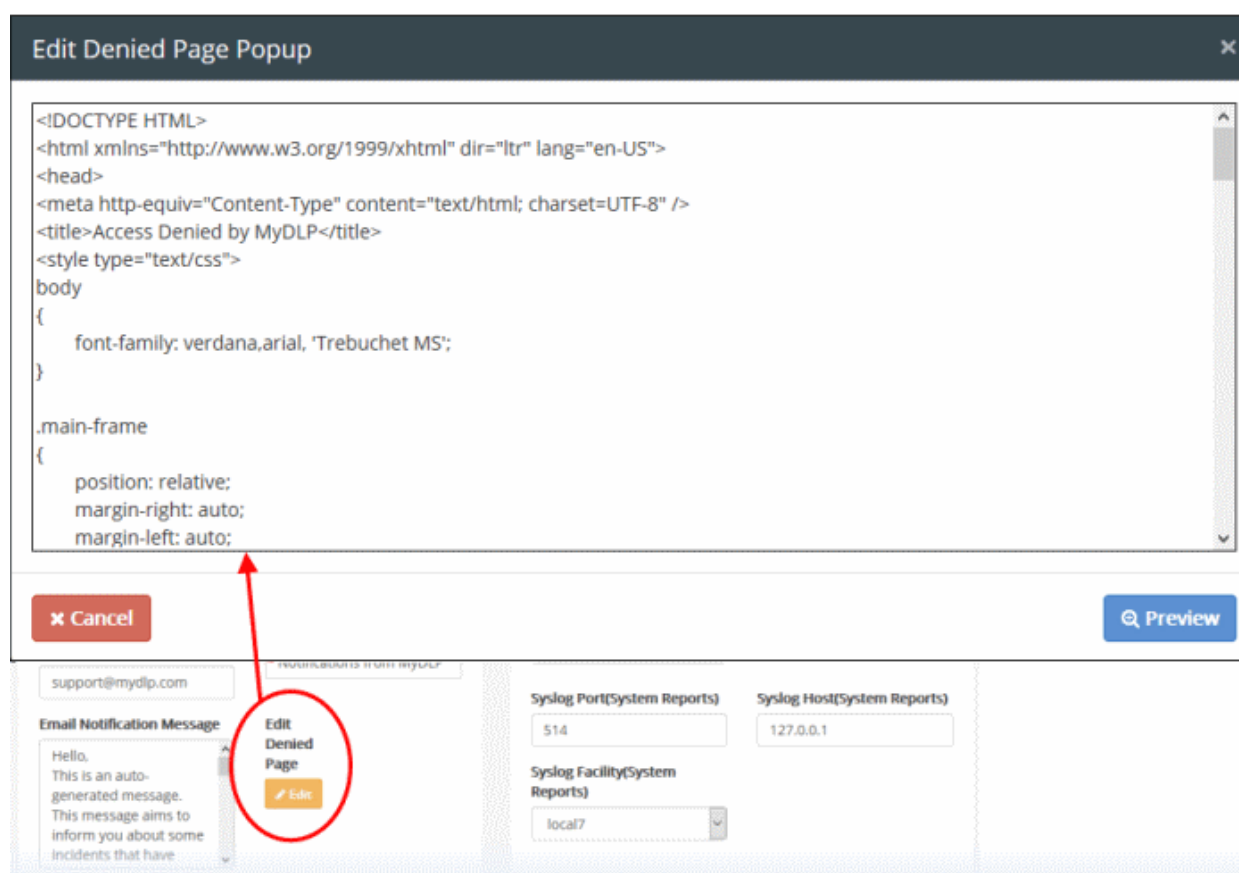
**Edit Denied Page** - Allows the administrator to edit the content in the message pop-up window that is displayed to end-user, when CDDP blocks or quarantines the data traffic. An example is shown below:



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

#### To edit the common template

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



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

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

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

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

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

### Syslog Configurations

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

**Background Note:** CDDP can transfer the logs in both UDP and 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.

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

- **ACL Logs** - The logs of the Comodo Dome Data Protection incidents, pertaining data transfer policy and

discovery rules

- **Diagnostics** - The logs pertaining to operation errors and system health of the Comodo Dome Data Protection server
- **System Reports** - The audit logs which have detail about every action taken on Comodo Dome Data Protection 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 CDDP is 'local6'

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

## 7. The Logs Tab

- The 'Logs' interface lists events triggered by CDDP rules
- Details of the log include the rule name and type, the date the event occurred, the affected endpoint and the action that took place.
- Depending on the rule type, administrators can download the files that triggered the rule, resend legitimate mails that were intercepted, and other actions.
- The logs interface is automatically updated at the interval set under '**Settings**' > '**Advanced**' interface.
- Click the 'Logs' tab at the top to open the interface:



**COMODO DOME DATA PROTECTION** mydlp

Dashboard Policy Settings **Logs** Reports Endpoints Revisions License Install Policy

**LOGS**

Show 10 entries Detailed Search Export to Excel Refresh Search for... Search

Date	Source	Action	Rule Type
10/16/2017, 2:26:08 PM		Archive	Remote Discovery
10/13/2017, 5:50:08 PM		Quarantine	Web
10/13/2017, 5:46:39 PM		Quarantine	Web
10/13/2017, 5:45:28 PM		Quarantine	Web
10/13/2017, 5:24:08 PM		Quarantine	Web
10/13/2017, 5:23:09 PM		Quarantine	Web
10/13/2017, 5:23:02 PM		Quarantine	Web
10/13/2017, 5:22:57 PM		Quarantine	Web
10/13/2017, 5:22:52 PM		Quarantine	Web
10/13/2017, 5:22:14 PM		Log	Web

Showing 1 to 10 of 5,286 entries Previous 1 2 3 4 5 ... 529 Next

Logs Table - Description of Columns

Column Header	Description
Date	Date and time of the incident.
Source	The IP address of the source end-point and the user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted or discovered as per the rule. See <b>Rule Actions</b> for a list of actions.
Rule Type	Indicates the type of the rule based on which files are intercepted or discovered. See <b>Rule Channels / Types</b> for a list of rule types.
Rule	The name of the rule that created the event.
Information Type	The type of data which was covered by the rule.
Details	Enables administrators to view complete details of the incident and download copies of the files intercepted or discovered. See <b>View Details of a Log Entry</b> for more details.

### Filtering and Search Options

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

- Click 'Detailed Search' at the top



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

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

#### To search the logs of archived files containing specified keywords

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

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

Type	Details	Appeared File Names
movable Storage Inbound	Type: text/plain Size: 1.58 KB	xml-core.md5sums
movable Storage Inbound	Type: text/plain Size: 6.21 KB	printer-driver-foo2zjs.md5sums
movable Storage Inbound	Type: text/plain Size: 11 B	[Form Input] email_address
movable Storage Inbound	Type: text/x-chdr Size: 45.63 KB	pgtable.h
movable Storage Inbound	Type: text/x-csrc Size: 56.37 KB	lex.lex.c
movable Storage Inbound	Type: text/plain Size: 56.37 KB	lex.lex.c_shipped
movable Storage	Type: text/plain Size: 56.37 KB	lex.lex.c_shipped
movable Storage Inbound	Type: text/plain Size: 57.53 KB	dtc-lexer.lex.c_shipped
movable Storage Inbound	Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Size: 18.68 KB	cc1.docx
movable Storage Inbound	Type: text/plain	mint-themes.md5sums



Administrators can download any file by clicking the download icon.

The following sections provide detailed explanations about:

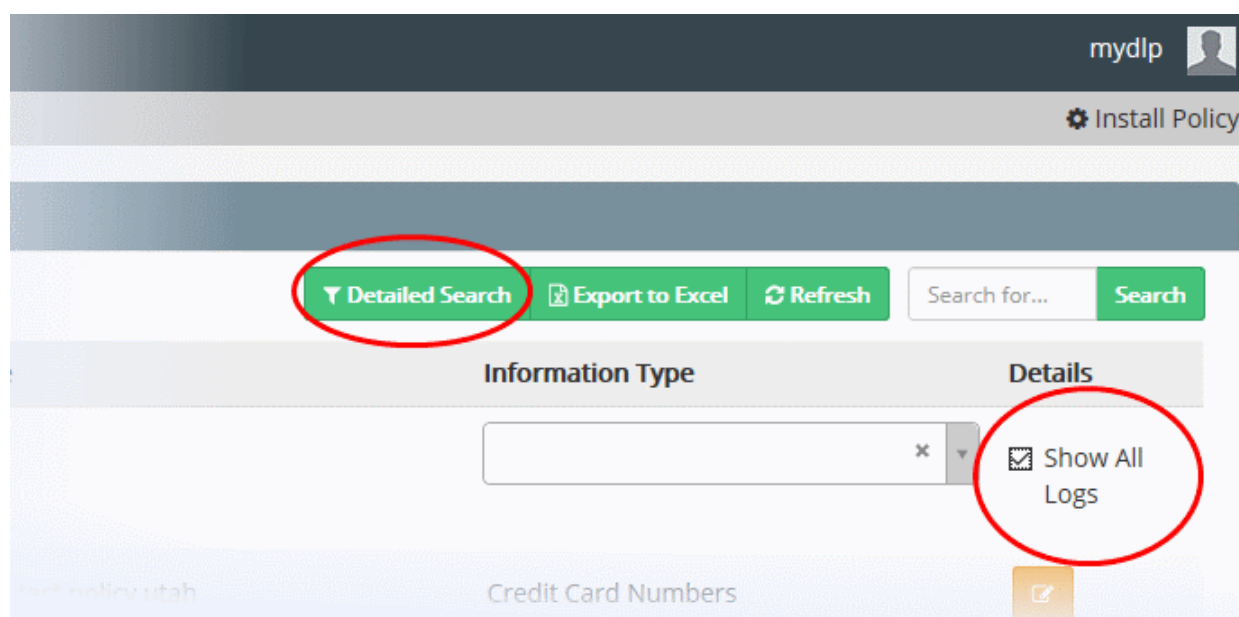
- **View Hidden Archive Logs**
- **View Details of a Log Entry**
- **Download the files archived by CDDP**
- **Resend mails intercepted by mail rules**
- **Export the Logs to a Spreadsheet file**

## 7.1. View Hidden Archive Logs


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

**To view the hidden logs**

- Click the 'Logs' tab at the top then 'Detailed Search' to expand the search panel
- Select the 'Show All Logs' check-box.



## 7.2. View Details of a Log Entry

- View granular details of any logged incident from the 'Log Details' pane
- Log details include source endpoint, user, destination, files intercepted / discovered, information type, serial number and so on
- You can also view the number of events identified from the same user, endpoint and the name of the rule based on which the event was identified
- Click the 'Logs' tab at the top then the details icon  at the end of any log entry row to open its details pane

An example 'Log Details' pane is shown below:

**Log Details** ×

DetailsCorrelations

**Date**  
10/19/2017, 10:25:36 PM

**IP**  
[REDACTED]

**User**  
buraka@COMODO

**Action**  
Quarantine

**Rule Type**  
Web

**Rule Name**  
web test policy utah

**Target**  
http://d36vlfy0df5iql.cloudfront.net/dlp.php?\_sm\_au\_c=iaV161SpvWV2Nq5s0c&P

**Information Type**  
Credit Card Numbers

**Files**  
HTTP URI Paramaters⬇  
cc\_match count: 1 pattern: 5523927719981467

✕ Close

The Log details pane consists of two tabs:

- **Details** - Displays the general details like the date and time, the IP address of the endpoint at which the event triggered, the action taken and more. The details displayed differ depending on the rule type. Administrators can 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.
- **Correlations** - Displays the statistics of events identified from the same endpoint and the user, and the events identified based on the same rule.

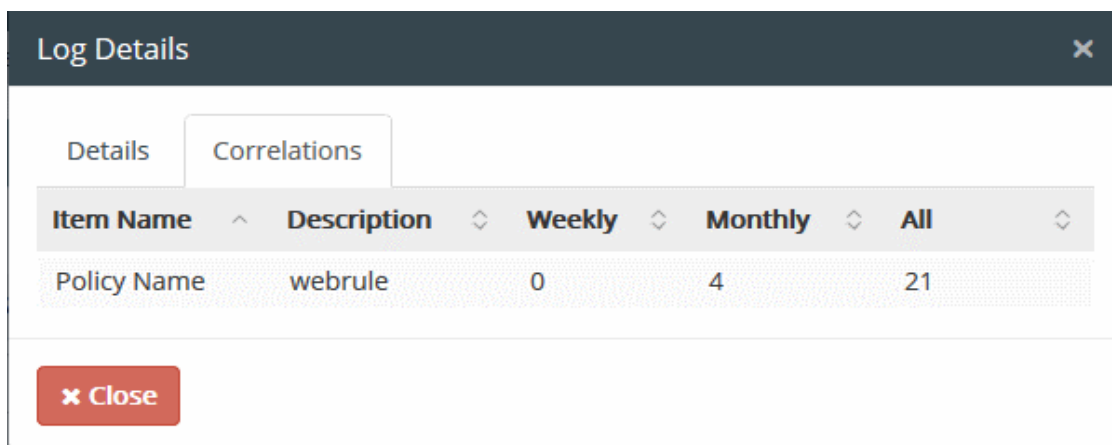
The following sections explain more about the Incident Log Details displayed for different Rule Channels:

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

## Web rule

### Details Pane:

Log Details - Web Rule	
Field	Description
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the file(s) is/are uploaded.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted. See <b>Rule Actions</b> for a list of actions.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
Target	The destination webpage to which the file(s) is/are uploaded.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the web rule. You can download the files by clicking on its name. See <b>Download the Files Archived by CDDP</b> for more details.

**Correlations Tab:**

Item Name	Description	Weekly	Monthly	All
Policy Name	webrule	0	4	21

The 'Correlations' tab displays the numbers of events identified based on the same rule, for the past week, past month and the total number of incidents from the time of installation.

**Mail rule****Details Tab:**

Log Details ×

Details

Correlations

**Date**

9/21/2016, 2:02:26 PM

**User**

sender@domain.com

**Action**

Quarantine

**Rule Type**

Mail

**Rule Name**

mailrule

**From**

sender@domain.com

**To**

<user@example.com>

**Bcc**

<user@example.com>

**Information Type**

Credit Card Numbers

**Files**

Noname Data ⓘ

cc\_match count: 1 pattern: 4111 1111 1111 1111

cc\_match count: 1 pattern: 4111 1111 1111 1111

×

 Close

Requeue

Log Details - Mail Rule	
Field	Description
Date	Precise date and time of the incident.
User	The user logged-in at the end-point during time of incident.
Action	The action executed on the file(s) intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.

From	The email account from which the mail was sent
To	The email address to which the email was sent
BCC	The email address added to the BCC address field of the mail.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the mail rule. You can download the files by clicking on its name. See <a href="#">Downloading the Files Archived by CDDP</a> for more details.
Requeue	Allows the administrator to resend the mail if found legitimate. See <a href="#">Download the Files Archived by CDDP</a> for more details.

**Correlations tab:**

Log Details				
Details		Correlations		
Item Name	Description	Weekly	Monthly	All
User	sender@domain.com	0	2	2
Policy Name	mailrule	0	2	2
✕ Close		Requeue		

The 'Correlations' tab displays the total numbers of incidents identified for the same user and the events based on the same rule, for the past week, past month and the total number of incidents from the time of installation.

## Removable Storage rule

Details Tab:

Log Details ×

Details

Correlations

Date

9/26/2016, 7:13:20 PM

IP

10.100.111.11

User

mischievous@company.net

Action

Quarantine

Computer Name

WIN7CLIENT-PC

Rule Type

Removable Storage

Rule Name

rem stor

Target

H:\testinb.txt

Information Type

Credit Card Numbers

Files

testinb.txt ⓘ

cc\_match count: 1 pattern: 4111 1111 1111 1111

cc\_match count: 1 pattern: 4111 1111 1111 1111

✕ Close

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

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

**Correlations Tab:**

Item Name ^	Description	Weekly	Monthly	All
User	mischeivous@company.net	7	10	16
Computer Name	WIN7CLIENT-PC	7	10	18
Policy Name	rem stor	17	17	20

The 'Correlations' tab displays the total numbers of incidents identified for the same user and from the same endpoint and the events based on the same rule, for the past week, past month and the total number of incidents from the time of installation.



## Removable Storage Inbound rule

Details Tab:

Log Details
×

Details
Correlations

**Date**  
9/27/2016, 6:39:09 PM

**IP**  
10.100.111.81

**User**  
innocent@company.net

**Action**  
Log

**Rule Type**  
Removable Storage Inbound

**Rule Name**  
INB

**Target Path**  
H:\setup.exe

**Files**  
setup.exe

× Close

Log Details - Removable Storage Inbound Rule	
Field	Description
Date	Precise date and time of the incident.
IP	The IP address of the source end-point at which the file(s) is read/copied from a removable storage.
User	The user logged-in at the time of incident

Action	The action executed on the file(s) intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
Target Path	The location in the removable storage from which the file was read/copied.
Files	Displays a list of files that were identified as per the Removable Storage Inbound rule. You can download the files by clicking on its name. See <a href="#">Download the Files Archived by CDDP</a> for more details.

**Correlations Tab:**

Log Details <span>×</span>					
Details		Correlations			
Item Name ^	Description ^	Weekly ^	Monthly ^	All ^	
User	innocent@company.net	7	10	16	
Policy Name	INB	0	0	6	
<span>×</span> Close					

The 'Correlations' tab displays the total numbers of incidents identified for the same user and the events based on the same rule, for the past week, past month and the total number of incidents from the time of installation.

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

**Printer rule**

Details Pane:

Log Details ×

Details

Correlations

**Date**

9/21/2016, 8:24:27 PM

**IP**

10.111.111.11

**User**

steno@company.net

**Action**

Quarantine

**Computer Name**

WIN7CLIENT-PC

**Rule Type**

Printer

**Rule Name**

Printer Use Policy

**Printer Name**

MyDLPSend To OneNote 2013

**Information Type**

SSSSSS

**Files**

asdpdm - Notepad.xps

pdm\_match count: undefined pattern: routing re-quest/reply packet, alter the packet content or construct the forged packet. Therefore,o

× Close

Log Details - Printer Rule	
Field	Description
Date	Precise date and time of the incident.

IP	The IP address of the source end-point from which the file(s) is transferred for printing.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted.
Computer Name	Indicates the host name of the endpoint from which the files are intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
Printer Name	The printer chosen for printing the file.
Information Type	The information type specified in the printer rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the Printer rule. You can download the files by clicking on its name. See <a href="#">Download the Files Archived by CDDP</a> for more details.

**Correlations Pane:**

Item Name	Description	Weekly	Monthly	All
User	steno@company.net	7	10	16
Computer Name	WIN7CLIENT-PC	7	10	18
Policy Name	Printer use Policy	0	1	1

The 'Correlations' tab displays the total numbers of incidents identified for the same user and from the same endpoint and the events based on the same rule, for the past week, past month and the total number of incidents from the time of installation.

## API rule

Log Details

**Date**  
9/21/2016, 1:55:01 PM

**User**  
10.111.111.13

**Action**  
Quarantine

**Rule Type**  
API

**Rule Name**  
apirule

**Information Type**  
Credit Card Numbers(Wide)

**Files**  

suspectedfile.pdf

cc\_match count: 1 pattern: 4111 1111 1111 1111

Close

Log Details - API Rule	
Field	Description
Date	Precise date and time of the incident.
User	The IP address of the source end-point from which the file(s) is transferred through an API
Action	The action executed on the file(s) intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
Information Type	The information type specified in the API rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the API rule. You can download the files by clicking on its name. See <a href="#">Download</a>

the **Files Archived by CDDP** for more details.

## USB Device Access Rule

Details Tab:

Log Details

Details

Correlations

Date

9/29/2016, 4:07:09 PM

IP

10.111.111.115

User

mischeivous@company.net

Action

Device Plugged In

Computer Name

ANM0019

Rule Type

USB Device Access

Rule Name

rem stor

Type

usbplug

Pid

PID\_30D3&MI\_03

Vid

VID\_041E

USB Name

USB Input Device

Serial Number

7&947172&0&0003

Manufacturer

(Standard system devices)

✕ Close

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

**Correlations Tab:**

Log Details					
Details		Correlations			
Item Name	Description	Weekly	Monthly	All	
User	mischeivous@company.net	12	13	48	
Computer Name	ANM0019	12	14	50	
Policy Name	rem stor	17	17	20	
<div> <div></div> <div></div> </div>					
<div> <div></div> <div></div> </div>					

The 'Correlations' tab displays the numbers of incidents identified for the same user and from the same endpoint and the events based on the same rule, for the past week, past month and the total number of incidents from the time of installation.

**CD-DVD Rule**

Details Tab:

Log Details

Details
Correlations

**Date**  
9/29/2016, 4:21:07 PM

**IP**  
10.111.111.113

**User**  
cduser@company.net

**Action**  
Device Plugged Out

**Computer Name**  
ANM0019

**Rule Type**  
CD-DVD Rule

**Rule Name**  
cd dvd policy

Close

Incident Log Details - CD-DVD Rule	
Field	Description
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the file(s) is copied/moved to CD or DVD.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted.



Computer Name	Indicates the host name of the endpoint from which the files are intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.

**Correlations Tab:**

Log Details <span>×</span>					
Details		Correlations			
Item Name ^	Description	Weekly	Monthly	All	
User	cduser@company.net	12	13	48	
Computer Name	ANM0019	12	14	50	
Policy Name	cd dvd policy	2	2	4	

× Close

The 'Correlations' tab displays the numbers of incidents identified for the same user and from the same endpoint and the events based on the same rule, for the past week, past month and the total number of incidents from the time of installation.

## Floppy Rule

Log Details

Details
Correlations

**Date**  
9/29/2016, 4:21:07 PM

**IP**  
10.100.111.111

**User**  
oldman@company.net

**Action**  
Device Plugged Out

**Computer Name**  
ANM0019

**Rule Type**  
Floppy Rule

**Rule Name**  
Floppy Use policy

Close

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

## Correlations Tab:

Log Details

Details

Correlations

Item Name	Description	Weekly	Monthly	All
User	oldman@company.net	12	13	48
Computer Name	ANM0019	12	14	50
Policy Name	Floppy Use policy	2	2	4

Close

The 'Correlations' tab displays the numbers of incidents identified for the same user and from the same endpoint and the events based on the same rule, for the past week, past month and the total number of incidents from the time of installation.

## Clipboard Rule

Details Tab:

Log Details

Details

Correlations

Date

9/29/2016, 2:11:51 PM

IP

10.111.11.114

User

bob@company.net

Action

Block

Computer Name

DESKTOP-8B38R40

Rule Type

Clipboard

Rule Name

Clipboard rule for Bob

Information Type

-Top Secret- Keyword

Files

seap-data

keyword\_match count: 1 pattern: top secret

Close

Log Details - Clipboard Rule	
Field	Description
Date	Precise date and time of the incident.
IP	The IP address of the source end-point from which the file(s) is copied.
User	The user logged-in at the time of incident.
Action	The action executed on the file(s) intercepted.
Computer Name	Indicates the host name of the endpoint from which the files are intercepted.
Rule Type	Indicates the type of the rule based on which the files are intercepted.
Rule Name	The name of the rule based on which the files are intercepted.
Information Type	The information type specified in the Clipboard rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the Clipboard rule. You can download the files by clicking on its name. See <a href="#">Download the Files Archived by CDDP</a> for more details.

**Correlations tab:**

Log Details					
Details		Correlations			
Item Name ^	Description	Weekly	Monthly	All	
User	bob@company.net	1	1	1	
Computer Name	DESKTOP-8B38R40	1	1	1	
Policy Name	Clipboard rule for Bob	1	1	2	
✕ Close					

The 'Correlations' tab displays the numbers of incidents identified for the same user and from the same endpoint and the events based on the same rule, for the past week, past month and the total number of incidents from the time of installation.

**Screenshot Rule**

Details Pane:

**Log Details** [Close]

**Details** | Correlations

**Date**  
8/1/2016, 4:18:18 PM

**IP**  
10.111.111.118

**User**  
mischeivous@company.net

**Action**  
Block

**Computer Name**  
ANM0019

**Rule Type**  
Screenshot

**Rule Name**  
screenshot capture restriction

[Close]

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

## Correlations Tab:

Log Details						×
Details		Correlations				
Item Name	Description	Weekly	Monthly	All		
User	mischeivous@company.net	12	13	48		
Computer Name	ANM0019	12	14	50		
Policy Name	screenshot capture restriction	0	1	3		
< >						
✕ Close						

The 'Correlations' tab displays the total numbers of incidents identified for the same user and from the same endpoint and the events based on the same rule, for the past week, past month and the total number of incidents from the time of installation.

## Endpoint Discovery Rule

Log Details
×

**Date**  
7/22/2016, 7:32:25 PM

**IP**  
10.111.111.80

**User**  
administrator@company

**Action**  
Quarantine

**Computer Name**  
win7client-pc

**Rule Type**  
Endpoint Discovery

**Rule Name**  
rem stor

**File**  
c:/Users/Administrator/Desktop/discoverytest/cc number.txt

**Information Type**  
Credit Card Numbers

**Files**  
cc number.txt ⓘ  
cc\_match count: 1 pattern: 4111 1111 1111 1111

× Close

Log Details - Endpoint Discovery Rule	
Field	Description
Date	Precise date and time at which the file(s) were discovered.
IP	The IP address of the source end-point at which the file(s) is discovered.
User	The user logged-in at the time of incident.



Action	The action executed on the discovered file(s).
Computer Name	Indicates the host name of the endpoint on which the files were discovered.
Rule Type	Indicates the type of the rule based on which the files were discovered.
Rule Name	The name of the rule based on which the files were discovered.
File	The file path in the local drive of the end-point, from which the the files were discovered.
Information Type	The information type specified in the rule, matching which, the sensitive data were contained in the file(s)
Files	Displays a list of files that were identified as containing sensitive data matching the Information type specified in the Endpoint Discovery rule. You can download the files by clicking on its name. See <a href="#">Download the Files Archived by CDDP</a> for more details.

### Remote Storage Discovery Rule

Log Details

**Date**  
9/21/2016, 7:09:32 PM

**User**  
\\10.111.111.81\windows7\columbus

**Action**  
Archive

**Rule Type**  
Remote Discovery

**Rule Name**  
discovery 81

**File**  
Hebele 4111 1111 1111 1111.docx

**Information Type**  
Credit Card Numbers

**Files**  

Hebele 4111 1111 1111 1111.docx

cc\_match count: 2 pattern: 4111 1111 1111 1111

Close

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

## Network Share Rule

Log Details

Details
Correlations

**Date**  
10/23/2017, 3:39:18 PM

**IP**  
10.108.51.243

**User**  
Administrator@DESKTOP-HI950BN

**Action**  
Block

**Computer Name**  
DESKTOP-HI950BN

**Rule Type**  
Network Share

**Rule Name**  
Chennai NSR

**Target**  
\\10.104.70.191\Groups\Documentation\credit\_card\_nos.txt

**Information Type**  
Credit Card Numbers

**Files**  

credit\_card\_nos.txt

birthdate\_match count: 1 pattern: 10 10 1990
cc\_match count: 1 pattern:

Close

Log Details – Network Share Rule	
Field	Description
Date	Precise date and time at which the file(s) were discovered.

IP	The IP address of the source end-point
User	The user logged-in at the time of incident.
Action	The action executed on the file
Computer Name	The host name of the endpoint
Rule Type	The type of rule used to discover files
Rule Name	The label of the rule
Target	The file path in the source host computer
Information Type	The information type specified in the rule, matching with the sensitive data were contained in the file(s)
Files	A list of files that were identified as containing data matching the Information type specified in the Remote Discovery rule. You can download the files by clicking their names. See <b>Download the Files Archived by CDDP</b> for more details.

Correlations tab:

**Log Details** ✕

Details Correlations

Item Name ^	Description	Weekly	Monthly	All
User	Administrator@DESKTOP-HI950BN	8	8	8
Computer Name	DESKTOP-HI950BN	8	8	8
Policy Name	Chennai NSR	6	6	6

< >


✕ Close

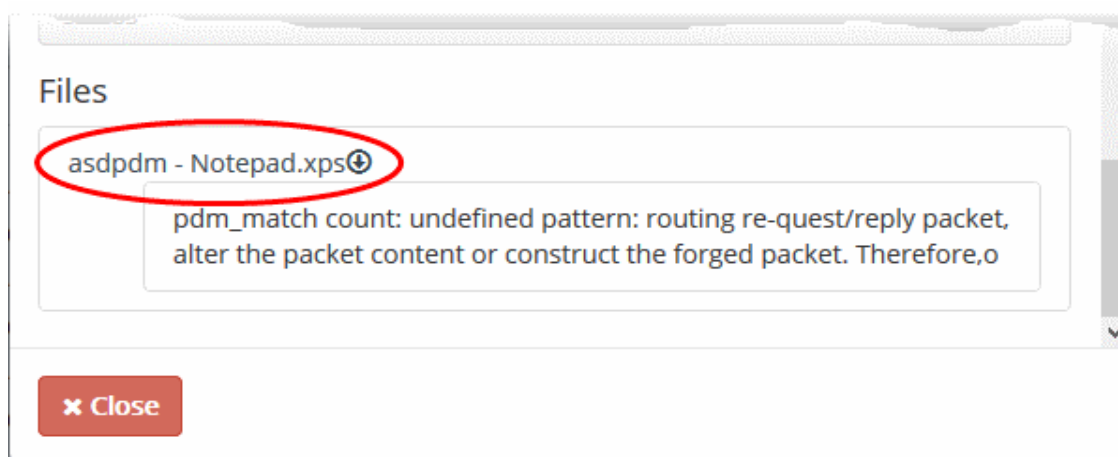
The 'Correlations' tab displays the total numbers of incidents by users for the past week, past month and all-time.

## 7.3. Download the Files Archived by CDDP

- Files with sensitive information are archived / quarantined based on data transfer policy rules / discovery rules
- You can download copies of these files from the 'Logs' interface

**To download an archived file**

- Click the 'Logs' tab at the top
- Search for the log entry of the required incident using the search options. See '**Filtering and Search Options**' in the section '**The Logs tab**' for more details.
- Click the  icon for the log entry under the Details column. The Log Details pane will open.
- Click on the file name, under 'Files'




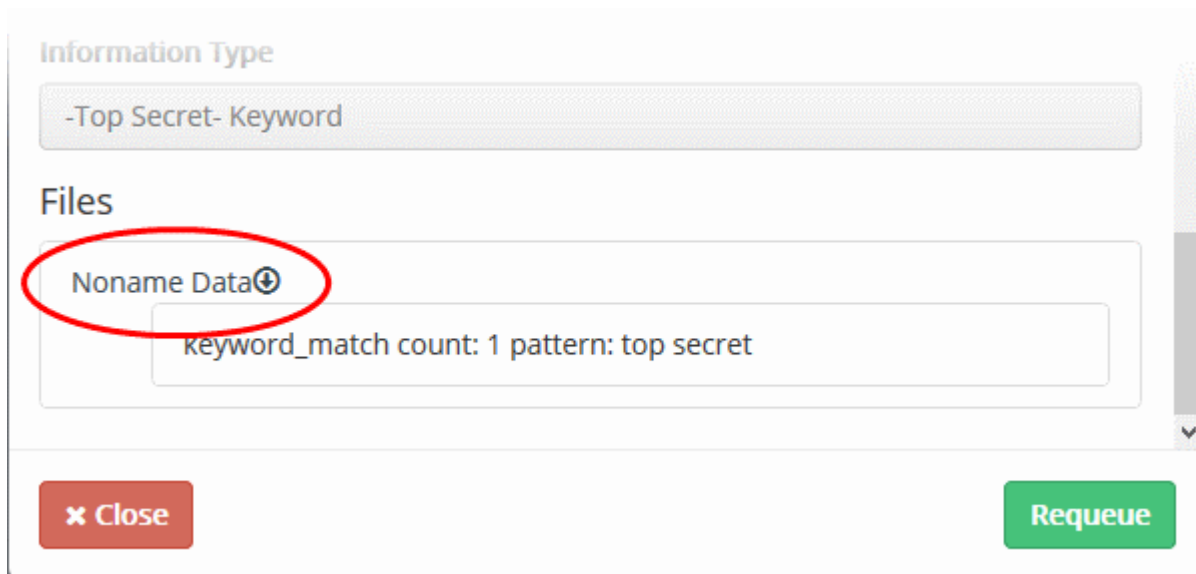
The file will be saved to your default download location.

## 7.4. Resend Mails Intercepted by Mail Rules

- CDDP passes, logs, archives, blocks or quarantines emails according to the mail rules
- The emails that are passed, logged or archived will reach their recipients.
- Blocked emails are discarded and prevented from reaching the intended recipients.
- Quarantined emails are prevented from reaching their recipients and a copy of them are saved in the CDDP archives.
- You can examine these emails by downloading the archived copies of them from the 'Log Details' pane. If these emails are found legitimate, they can be forwarded to the intended recipients from the 'Log Details' pane.

**To resend the archived emails**

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



Information Type

-Top Secret- Keyword

Files

Noname Data

keyword\_match count: 1 pattern: top secret

Close Requeue

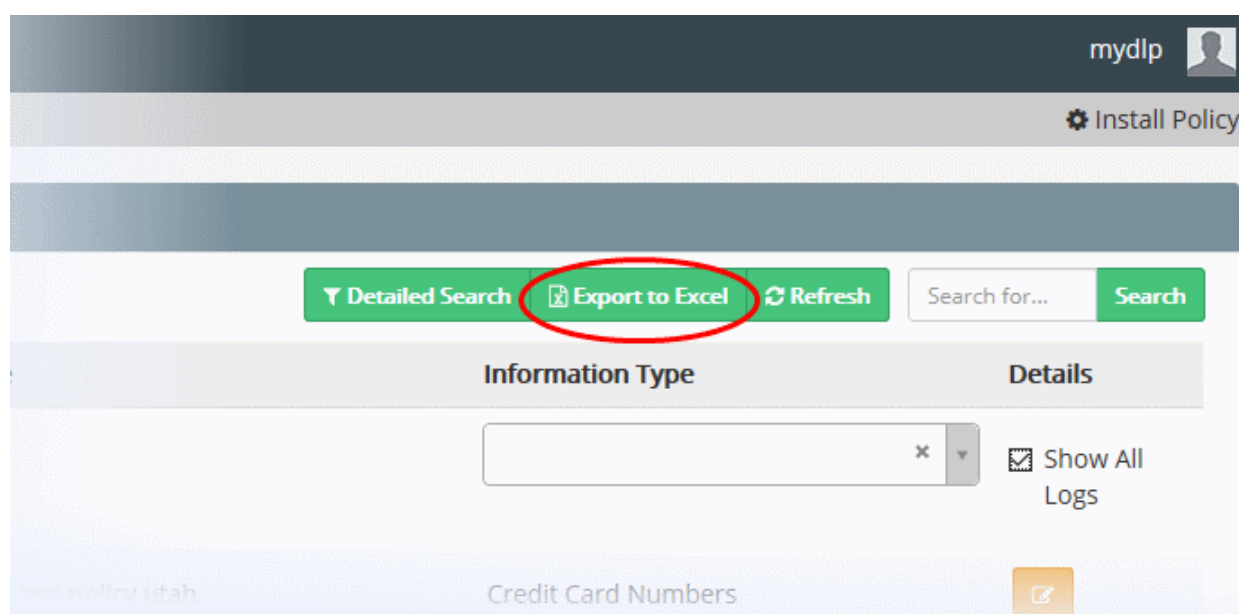
- If the email is found legitimate, click 'Requeue' at the bottom.

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

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

## 7.5. Export the Logs to a Spreadsheet File

- CDDP logs can be saved as a spreadsheet file in 'Microsoft Excel' file format for later analysis.
- The spreadsheet file will contain the first 1000 entries in the log.
- If required, apply filters and search options to export the log pertaining to a specific time period or to export logs pertaining to specified filtering criteria.
- See '**Filtering and Search Options**' in the section '**The Logs tab**' for more details.
- Click the 'Logs' tab then 'Export to Excel' at the top



mydlp

Install Policy

Detailed Search Export to Excel Refresh Search for... Search

Information Type Details

Show All Logs

Credit Card Numbers

The file will be saved to your default download location.

## 8. The Endpoints Tab

- Comodo Dome Data Protection monitors and controls data passing to and from endpoints and can also run discovery scans to identify confidential data in existing files.
- In order for CDDP to monitor and scan endpoints, the Comodo Dome Data Protection Agent needs to be installed on each endpoint.
- The endpoint agent can be installed on the network computers in different ways.
- For more details on installing the endpoint agent, refer to the CDDP Endpoint Agent Installation Guide available from <https://help.comodo.com/product-283-Comodo-Dome-Data-Protection.html>
- Click the 'Endpoints' tab to open the interface

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

Private IP	Public IP	Computer Name	Logged on User	Installed Agent Version	Last Update	First Seen
	10.108.51.121	DESKTOP-HI950BN	Administrator@DESKTOP-HI950BN	3.12.3(windows)	8/24/2018, 2:56:39 PM	8/20/2018, 12:18:58 PM
	10.108.51.202	DESKTOP-TTPO9PR	Vega@DESKTOP-TTPO9PR	3.12.3(windows)	8/24/2018, 2:56:35 PM	8/22/2018, 12:00:57 PM

Endpoints Table - Column Descriptions

Column	Description
Private IP	The local IP address of the endpoint.
Public IP	The external IP address of the network to which the endpoint belongs
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 CDDP 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 CDDP server.

- Click 'Refresh' to add any new endpoints and remove endpoints from which the agent has been uninstalled.
- Click 'Agent Summary' to the latest agent version number, the number of endpoints that are currently online and offline, the total number of endpoints on which the agent is installed, and the number of endpoints running outdated agents.
- To remove an endpoint from the list, click 'Delete' at the top, then 'Yes' in the confirmation dialog. Please note computers on which policies are applied cannot be deleted from the list.



## 9. The Revisions Tab

- Comodo Dome Data Protection saves the installed policies with their set of rules
- The 'Revisions' interface displays the list of policies in chronological order, that is, the last applied policy will be listed at the top
- You can bookmark the policies by specifying a name shortly describing the changes done.
- Apply an old policy to enforce the set of rules that were in action at that point of time
- Click the 'Restore' button beside a policy to apply it

You can backup the currently active policy to a safe location and recover policies from saved backup files. This is useful if you are planning to uninstall/re-install Comodo Dome Data Protection and reuse the same policy.

The 'Revisions' interface allows administrators to view the list of saved policy revisions, bookmark them, revert Data Protection to a previous revision and backup/restore revision.

- Click the 'Revisions' tab at the top.

The screenshot displays the 'Revisions' tab in the Comodo Dome Data Protection interface. The top navigation bar includes 'Dashboard', 'Policy', 'Settings', 'Logs', 'Reports', 'Endpoints', 'Revisions' (highlighted), and 'License'. The 'Revisions' section is divided into two panels: 'NAMED REVISIONS' and 'ALL REVISIONS'. The 'NAMED REVISIONS' panel shows a table with columns 'Date' and 'Name', but it is currently empty. The 'ALL REVISIONS' panel shows a table with columns 'Date', 'Name', 'Parent', and 'Restore'. It lists 10 revisions, each with a date and time, a bookmark icon, and a restore icon. At the bottom of the 'ALL REVISIONS' section, there is a pagination bar showing 'Showing 1 to 10 of 89 entries' and a set of page numbers from 1 to 9, with '1' being the active page.

The right hand side of the interface displays the list of all the policy revisions automatically created by Comodo Dome, 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.

Following sections explain more about:

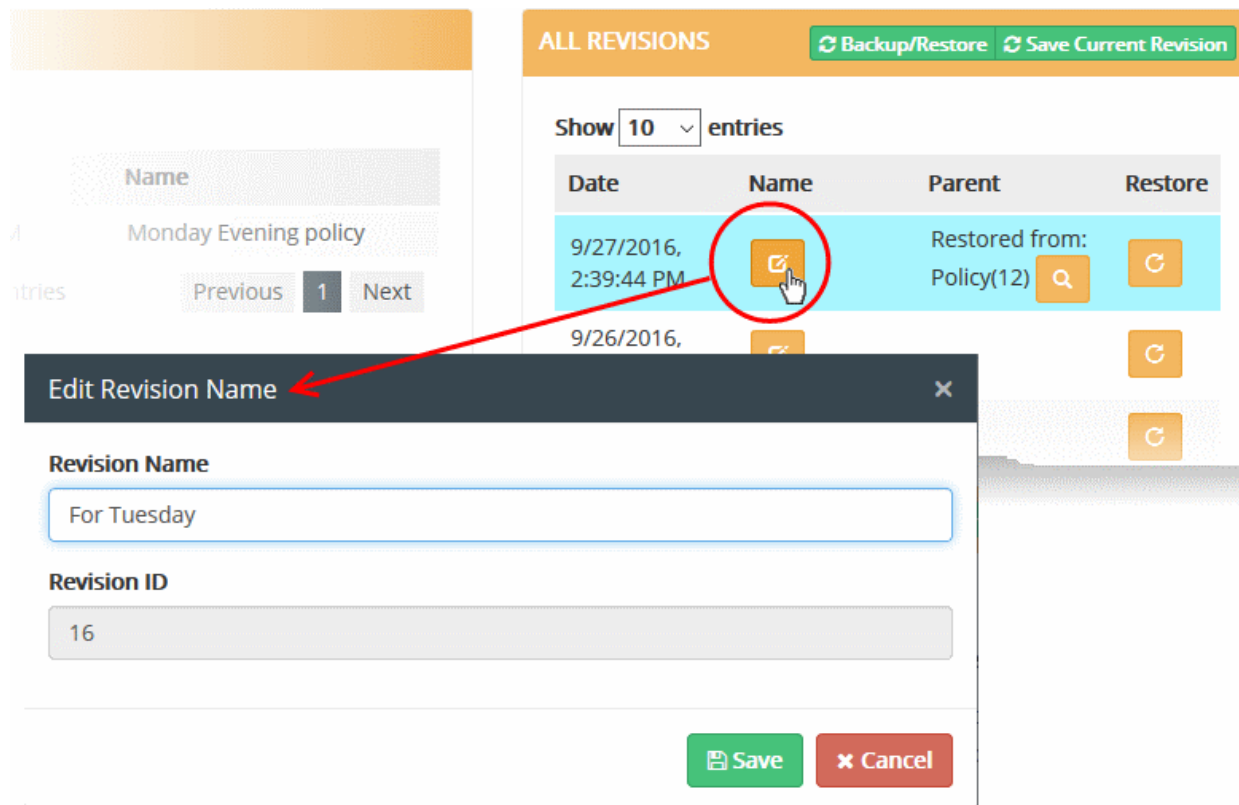
- **Bookmarking a Policy revision**
- **Re-applying Policy from a revision**



- **Creating Backup of the current Policy**
- **Restoring Policy from Backup**






To bookmark a policy

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



**ALL REVISIONS** Backup/Restore Save Current Revision

Show  entries

Date	Name	Parent	Restore
9/27/2016, 2:39:44 PM		Restored from: Policy(12) 	
9/26/2016,			

**Edit Revision Name** ×

Revision Name

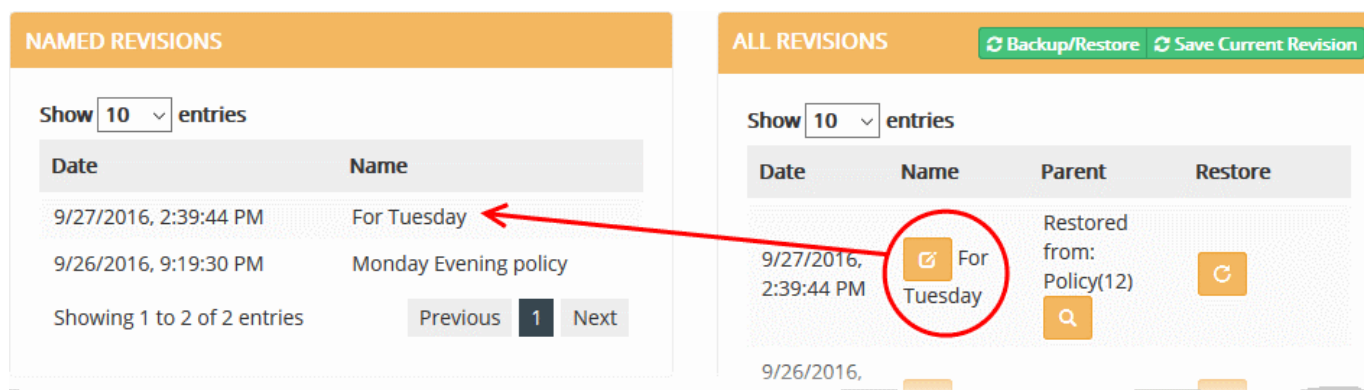
Revision ID

Save Cancel

The 'Edit Revision Name' dialog will appear.

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

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



**NAMED REVISIONS**






Show  entries

Date	Name
9/27/2016, 2:39:44 PM	For Tuesday
9/26/2016, 9:19:30 PM	Monday Evening policy


Showing 1 to 2 of 2 entries Previous 1 Next

**ALL REVISIONS** Backup/Restore Save Current Revision

Show  entries

Date	Name	Parent	Restore
9/27/2016, 2:39:44 PM	 For Tuesday	Restored from: Policy(12) 	
9/26/2016,			

To re-apply a policy from the revisions

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

The screenshot displays the 'ALL REVISIONS' section of the Comodo Dome Data Protection interface. At the top, there are buttons for 'Backup/Restore' and 'Save Current Revision'. Below this, a 'Show 10 entries' dropdown is visible. The main table lists revisions with columns for Date, Name, Parent, and Restore. The first row shows a revision from 9/27/2016, 2:39:44 PM, named 'For Tuesday', with a parent 'Restored from: Policy(12)'. The second row, highlighted in blue, shows a revision from 9/26/2016, 10:12:22 PM, named 'For Tuesday', with a parent 'Restored from: Policy(12)'. A red circle highlights the 'Restore' button (a circular arrow icon) for the second row. A red arrow points from this button to a 'Restore Policy' dialog box. The dialog box has fields for 'Revision Name' and 'Revision ID' (containing the value '15'). At the bottom of the dialog are 'Restore' and 'Cancel' buttons.

Date	Name	Parent	Restore
9/27/2016, 2:39:44 PM	For Tuesday	Restored from: Policy(12)	
9/26/2016, 10:12:22 PM	For Tuesday	Restored from: Policy(12)	

**Restore Policy**

Revision Name

Revision ID

15

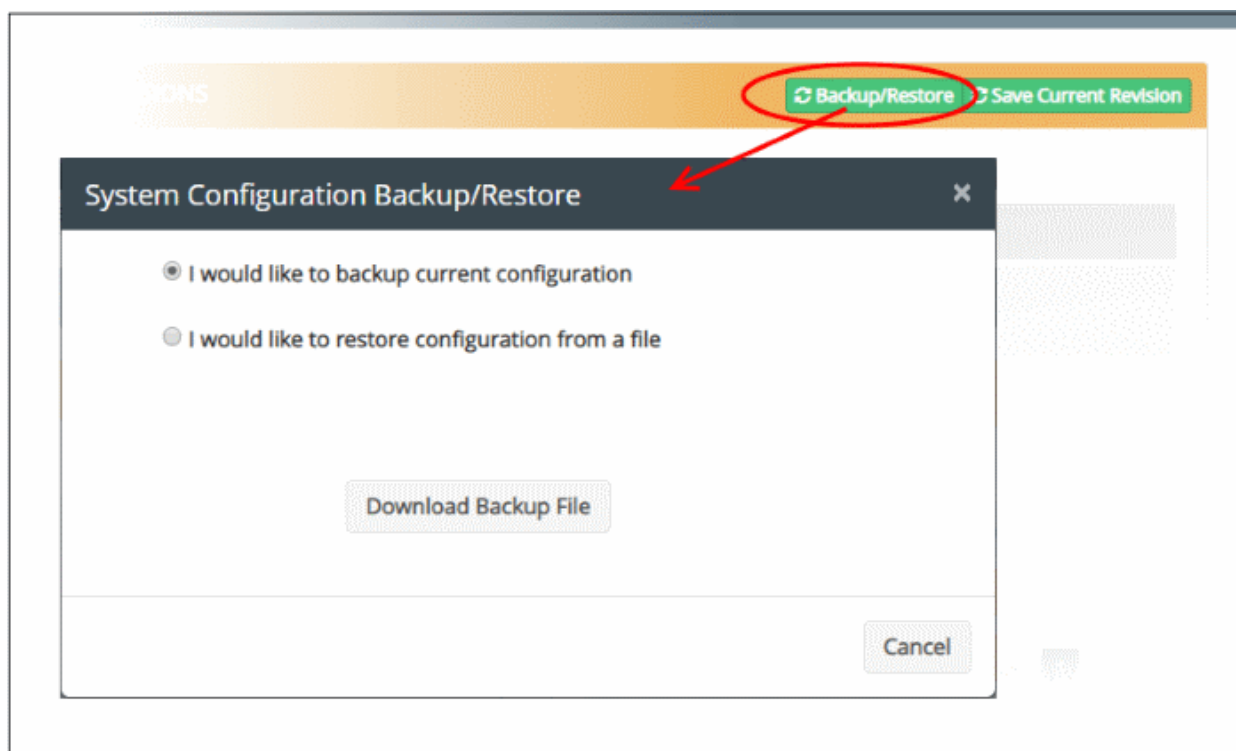
Restore Cancel

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

Comodo Dome Data Protection will apply the policy to the network with the rules that were in action at that point of time.

#### To Backup the currently active policy

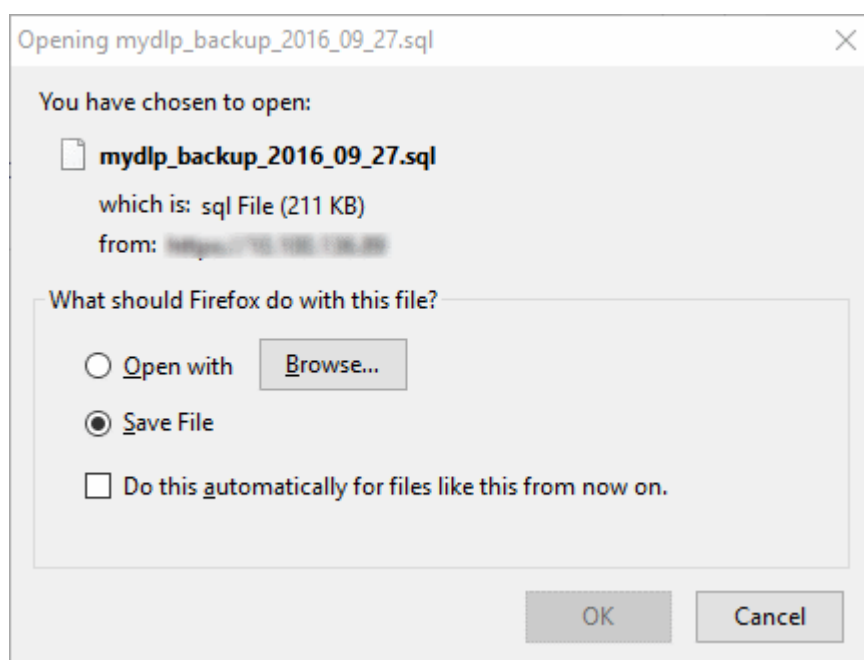
- Click the Backup/Restore button at the top right



The System Configuration Backup/Restore dialog will appear.

- Choose 'I would like to backup current configuration'
- Click 'Download Backup File'

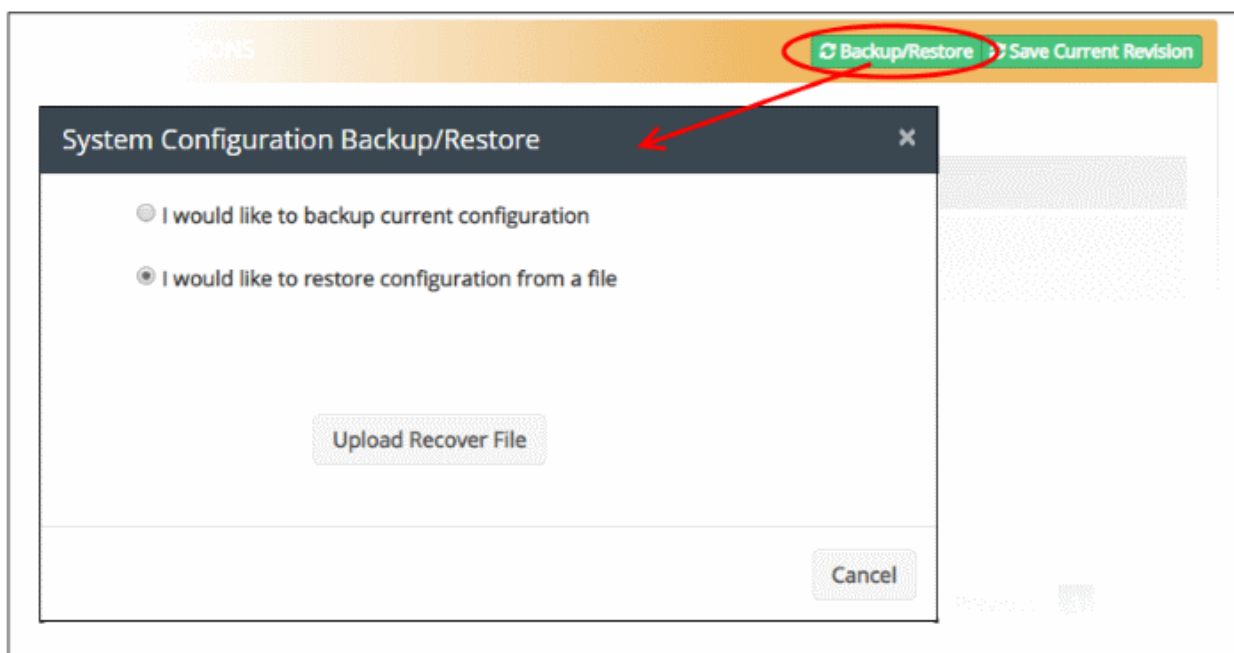
The configuration and the rules in the currently active Policy will be compiled and downloaded in structured query language (.sql) file format.



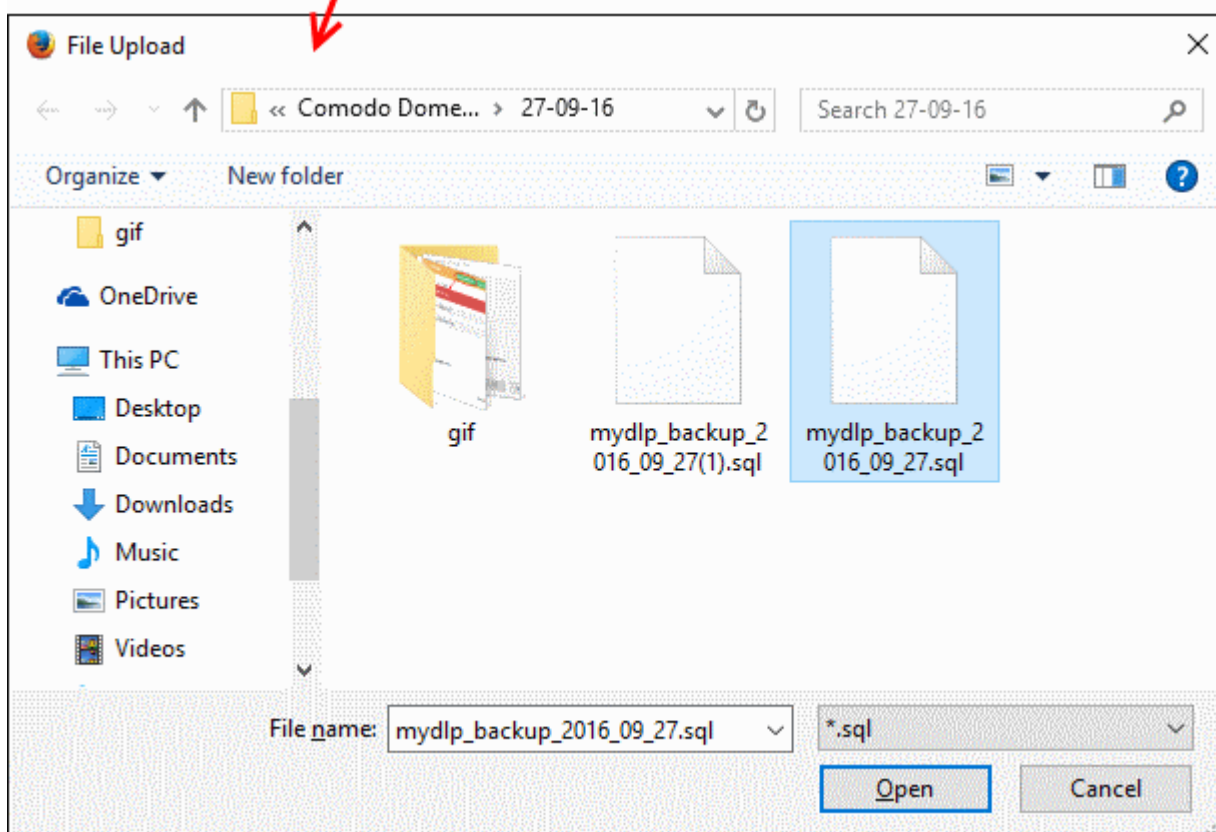
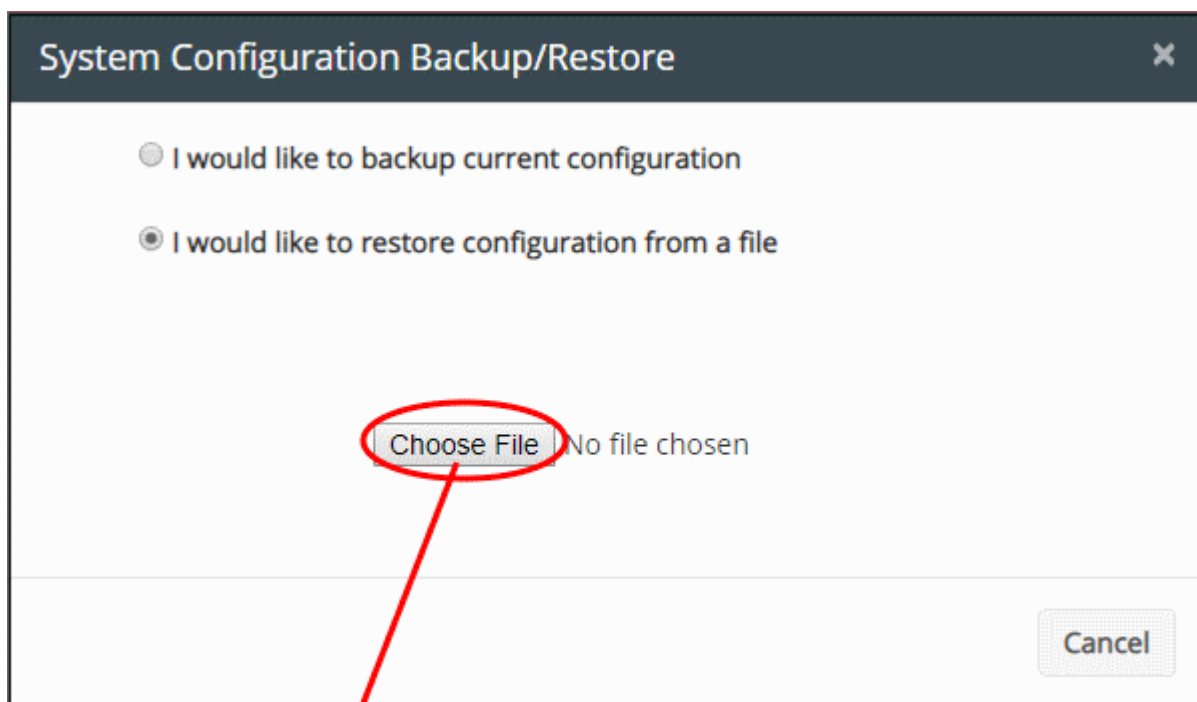
- Save the file at a safe location.

#### To restore Policy configuration from a Backup file

- Click the Backup/Restore button at the top right



- Choose 'I would like to restore configuration from a file' and click 'Upload Recover File'



- Click 'Browse', navigate to the location of the saved backup file, select the file and click 'Open'

The backup file will be uploaded and added to the list of policy revisions.

- Click 'Install Policy' at top-right to apply the restored policy. See '**Deploy a Policy**' for more details.

Comodo Dome Data Protection will apply the policy to the network with the rules pertaining to that policy.

## 10. Configure License and CDDP Server settings

The license tab allows you to view existing license information, including subscription ID and expiry date, and to activate new licenses. In addition, admins can view and configure network settings, DNS settings, email servers and can shutdown/restart the server.

The screenshot shows the 'License' tab in the Comodo Dome Data Protection administrator interface. The top navigation bar includes 'Dashboard', 'Policy', 'Settings', 'Logs', 'Endpoints', 'Revisions', and 'License'. The left sidebar, titled 'SERVER CONFIGURATION', lists 'License', 'Network Configuration', 'DNS Configuration', 'Email Configuration', 'Firmware Configuration', 'Shutdown/Reboot', and 'Downloads'. The main content area displays license details: a red warning box indicates '19 days remaining to the expiration date'. Below this, fields show 'Server Version' (3.13.0-01), 'License Type' (Enterprise), 'Subscription ID' (439d46a772), 'Expiration Date' (16/9/2018), 'Number of Allocated Seats' (2), and 'Max Number of Seats' (354). At the bottom, there is an 'Enter License Key' text box and a blue 'Enter License Key' button.

### Renew or Upgrade your License

You can purchase licenses for Comodo Dome Data Protection by logging-in to <https://accounts.comodo.com/mydlp/management/signup>. You will receive your license key via email after completing your purchase.

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

Once verified, your license will take effect immediately.

The left-hand menu also contains links for the following items:

- **Network Configuration**
- **DNS Configuration**
- **Shutting Down or Restarting the Server**

- [Email Server Configuration](#)
- [Manual Firmware Configuration](#)

## 10.1. Network Configuration

The 'Network Configuration' interface allows administrators to define server connection properties for items like the IP address of the CDDP server, the default internet gateway for the server and broadcast address for the server.

Note – Please make sure to configure the correct settings, otherwise the connection between the server and CDDP agent will be lost.

To open the 'Network Configuration' interface

- Click the 'License' tab
- Click 'Network Configuration' in the 'Server Configuration' area on the left

The screenshot displays the 'NETWORK CONFIGURATIONS' interface. It features a table with four rows for network settings. Each row has a label on the left and a text input field on the right. The values entered in the fields are: Server IP Address (10.100.136.64), Mask (255.255.255.0), Default Gateway (10.100.136.1), and Broadcast (10.100.136.255). At the bottom right of the interface is an orange 'Save' button with a floppy disk icon.

NETWORK CONFIGURATIONS	
Server IP Address	10.100.136.64
Mask	255.255.255.0
Default Gateway	10.100.136.1
Broadcast	10.100.136.255

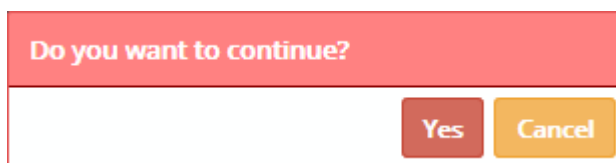
Save

You can configure the following network connection properties for the Comodo Dome Data Protection server:

- **Server IP** - If the server was assigned an IP address during installation it will be displayed in this field (for example, if the IP address was assigned by DHCP). If not, you can assign a new address. You can change the assigned IP address at anytime by entering the new IP address in the 'Server IP' field.
- **Mask** – Enter the network mask address
- **Default Gateway** – Enter the IP address of the default gateway of the network
- **Broadcast** – Enter the broadcast IP address of the network to enable the server to receive datagrams.
- Click 'Save'.



A confirmation dialog will appear.



- Click 'Yes' for your settings to take effect.

## 10.2. DNS Configuration

The 'DNS Configuration' interface lets you define DNS servers that the CDDP server will use. To ensure that the server resolves device names in the network, you should also specify the internal network domain name. This will enable the server to access internal network resources like FTP server, the Windows File Share and other devices and endpoints connected to the network.

### To open the 'DNS Configuration' interface

- Click the 'License' tab on the top
- Click 'DNS Configuration' from the server configuration area on the left



## DNS CONFIGURATIONS

## DNS Server IP Address

10.100.129.100

8.8.8.8

Enter a valid DNS Server IP Address



## Domain

Save

- **DNS Server IP Address** - To add a DNS server, enter the IP address and click the '+' button. Repeat the process to add more DNS servers to the list. To remove a DNS server from the list, select it and click the '-' button.
- **Domain** - Enter the internal domain name of the network so the server can access all devices connected to the network.
- Click 'Save'

A confirmation dialog will appear.

Do you want to continue?

Yes

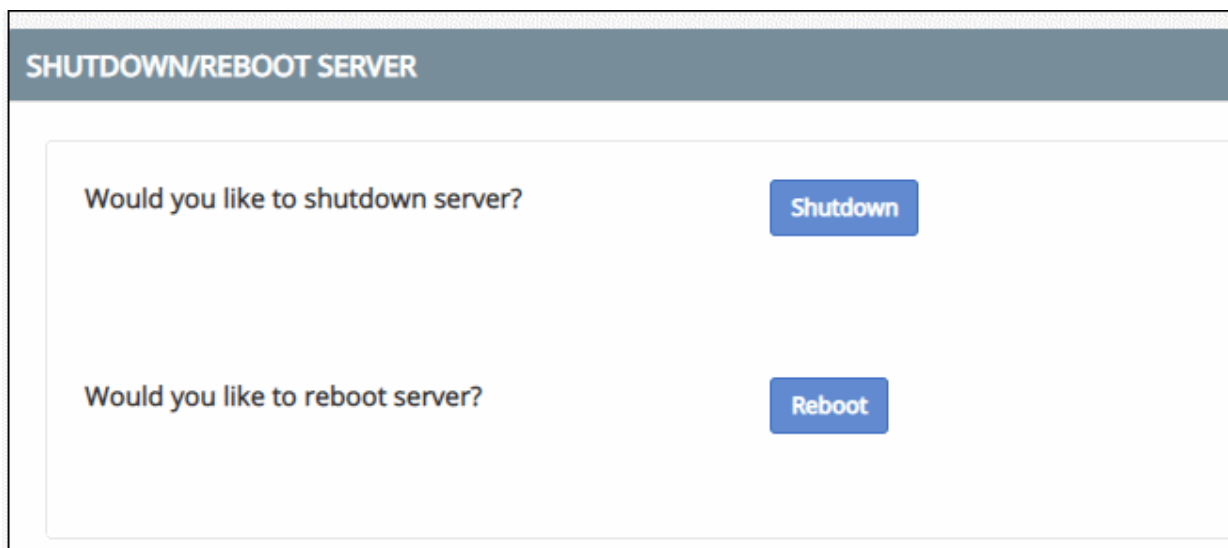
Cancel

- Click 'Yes' for your settings to take effect.

## 10.3. Shutting Down or Restarting the Server

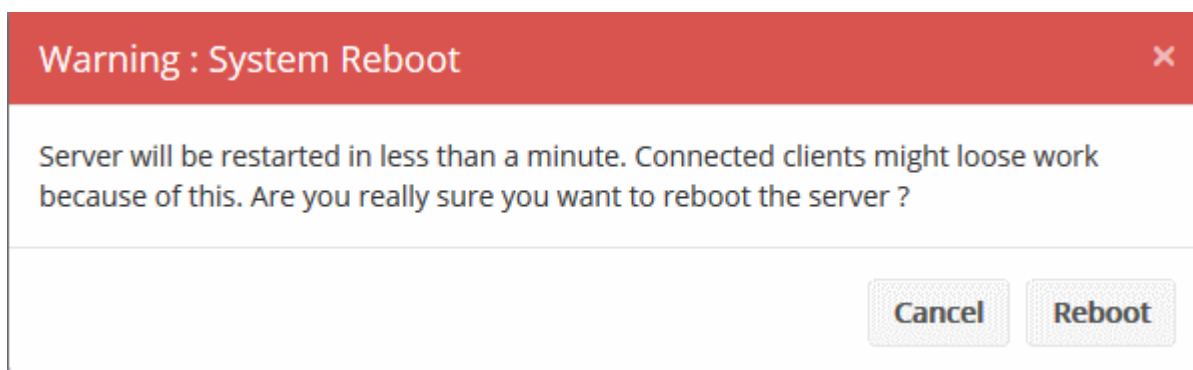
Administrators can shutdown or restart the CDDP server as follows:

- Click the 'License' tab
- Click 'Shutdown/Reboot' in the server configuration area on the left



The screenshot shows a web interface titled "SHUTDOWN/REBOOT SERVER". It contains two sections. The first section asks "Would you like to shutdown server?" with a blue "Shutdown" button. The second section asks "Would you like to reboot server?" with a blue "Reboot" button.

- Choose 'Shutdown' or 'Reboot' as required
- A confirmation dialog will be displayed:



The screenshot shows a red warning dialog box titled "Warning : System Reboot" with a close button (X) in the top right corner. The main text reads: "Server will be restarted in less than a minute. Connected clients might loose work because of this. Are you really sure you want to reboot the server ?". At the bottom right, there are two buttons: "Cancel" and "Reboot".

- Click 'Shutdown' or 'Reboot' to continue.

## 10.4. Email Server Configuration

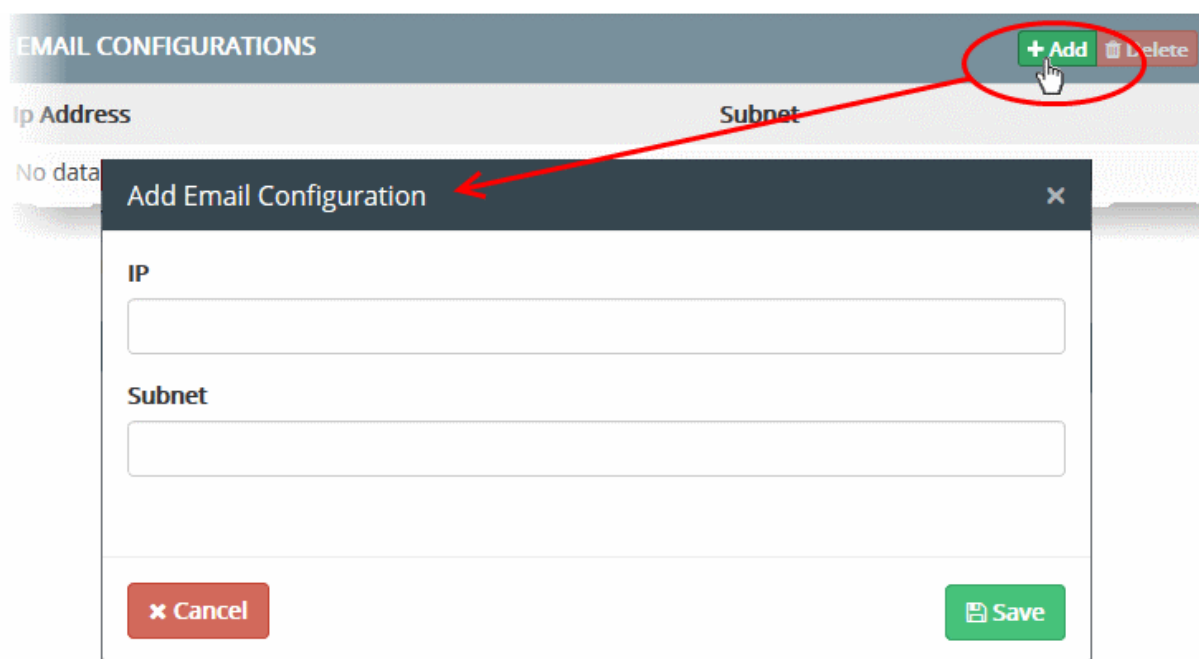
Outgoing messages from your mail server(s) are redirected through the CDDP server so they can be inspected according to your policy rules. To ensure that the CDDP filters mail traffic, the IP address of each mail server needs to be added to the 'Email Configuration Interface'.

**To open the Email Configuration interface**

- Click the 'License' tab
- Click 'Email Configuration' from the server configuration area on the left

**To add an email server**

- Click the 'Add' button at the top right



The 'Add Email Configuration' dialog will appear.

- Enter the IP address of the mail server in the 'IP' field
- Enter the subnet mask of the network as per CIDR notation in the 'Subnet' field
- Click 'Save'

The mail server will be added to the list in the 'Email Configuration' interface.

- Repeat the process to add more email servers

All traffic from the mail servers will pass through the Data Protection server for filtering as per the mail rules in the policy.

**To remove an email server from the list**

- Select the mail server from the list
- Click the 'Delete' button at the top right


The mail server will be removed from the list. The traffic from the mail server will not be accepted by the Data Protection server and the outgoing mails from it will not be intercepted.

## 10.5. Manually Update the CDDP Server


The 'Firmware Configuration' interface allows you to check whether any updates are available for the service. if available, please install the latest version to keep CDDP up-to-date.

**To open the Firmware Configuration interface**

- Click the 'License' tab
- Click 'Firmware Configuration' from the server configuration area on the left

FIRMWARE CONFIGURATIONS		
Current Version	Candidate Version	Action
3.12.0-11	Up to date 	<a href="#">Install</a>

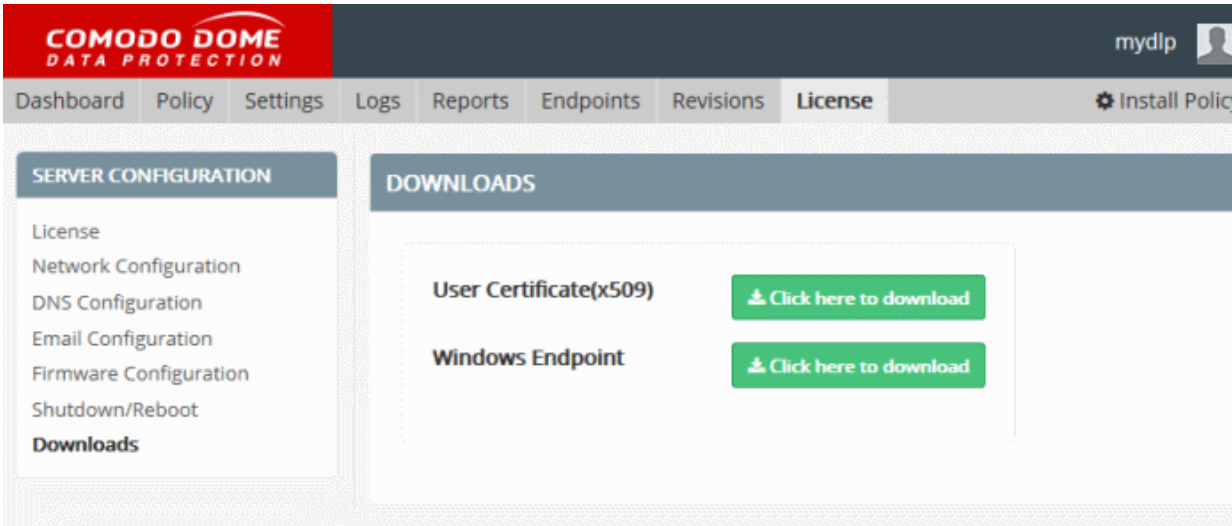
The 'Candidate Version' column indicates whether you have the latest version of the firmware or any updates are available.

- To manually check for availability of updated version, click the refresh button  in the 'Candidate Version' column.
- If any updates are available, click the 'Install' button in the 'Action' column

The latest version of the firmware will be automatically installed on your server. Your server will restart for the update to take effect.

## 10.6. Download and Configure Certificate Settings for CDDP

Admins can download the user and endpoint certificates for the purpose of authenticating endpoint connections to the CDDP server.



**User Certificate (x509)** - CDDP intercepts even SSL enabled webpages and relays them to the endpoints for monitoring the web-based 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 CDDP 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.

**CDDP Windows Endpoint** - The CDDP admin console requires CDDP agents installed on all the endpoints to be monitored in the network. The agent is responsible for deploying the data transfer policy at the endpoint in order to

monitor the data traffic through various channels and to allow, log, quarantine, block the data as per the rules. The agent also scans the endpoint to identify the data that match the discovery rules and to log, allow, quarantine or delete them as per the rules. The endpoint agent installation is password protected and cannot be uninstalled from the endpoint without entering the password set in the Settings Endpoint interface. [See \*\*Configuring Endpoint Settings\*\*](#) for more details.

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

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

For more details on CDDP Endpoint deployment, please refer to the [CDDP Endpoint Installation Guide](#).

# About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

## About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)