



# Comodo Dome Data Protection

Software Version 3.13

## Quick Start Guide

Guide Version 3.13.120318

## Comodo DDP – Quick Start Guide

Comodo Dome Data Protection (CDDP) is a full 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.

This tutorial briefly explains how an admin can setup the Comodo Dome Data Protection and start using it.

- **Step 1 – Install CDDP on Network Server**
- **Step 2 – Login to the Management Console**
- **Step 3 – Install CDDP Agent on Network Computers**
- **Step 4 – Create Data Transfer Rules**
- **Step 5 – Create Data Discovery Rules**
- **Step 6 – Deploy the Policy**
- **Step 7 – View Discovery Reports and Data Transfer Event Logs**

### **Step 1 – Install CDDP on Network Server**

After the CDDP application purchase process is completed, you have to install it on a server and configure it so as to access the management console over local network and over the Internet. For details about installing CDDP on a server and configure, see our installation guide at <https://help.comodo.com/topic-283-1-597-7016-About-CDDP.html>. For any doubts and clarifications, please contact us at [domesupport@comodo.com](mailto:domesupport@comodo.com)

### **Step 2 – Login to the Management Console**

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

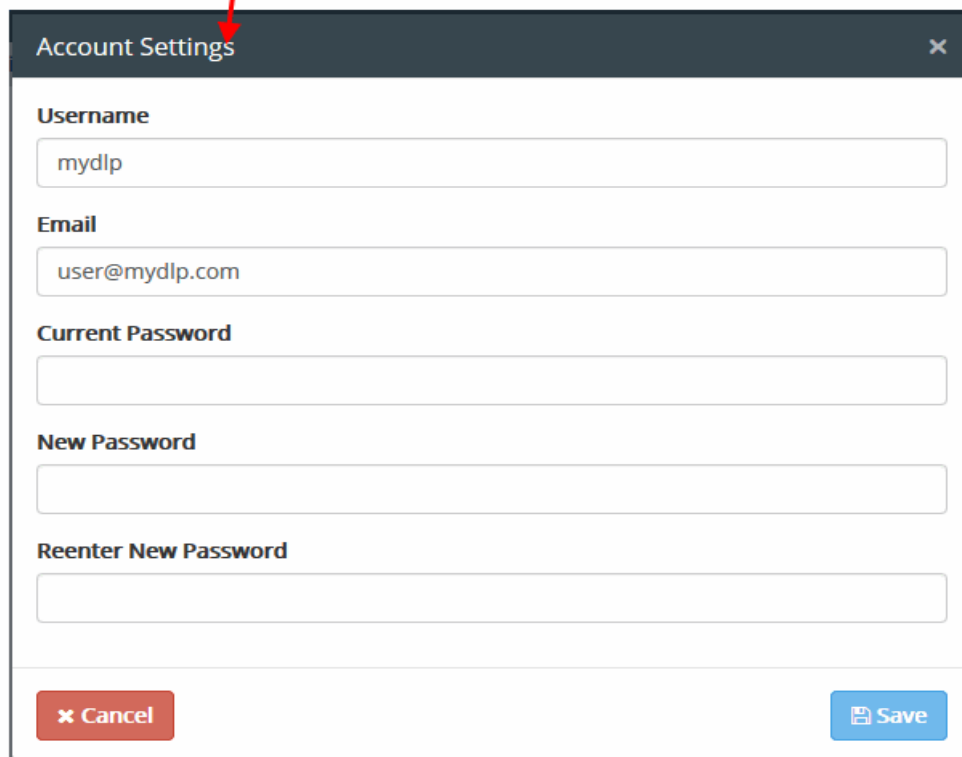
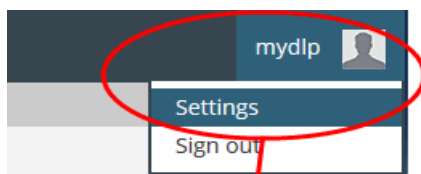
Preliminaries:

- 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 DDP. At the top, the logo reads 'COMODO DOME DATA PROTECTION'. Below the logo, the text 'SIGN IN' is displayed in large white letters on a dark blue background. Underneath, there are two white input fields: one for 'Username' and one for 'Password'. A blue button with a right-pointing arrow and the text 'Login' is located at the bottom right of the form.

- 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. You can change the password by clicking on the username at the top right > Settings.



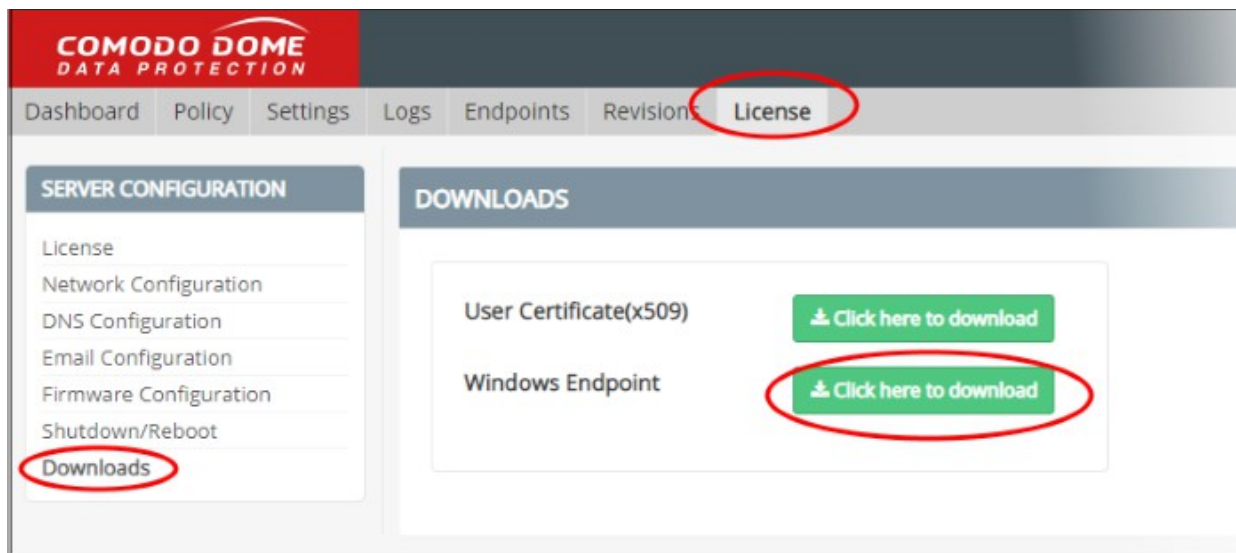
The image shows the 'Account Settings' dialog box. It has a dark header with the title 'Account Settings' and a close button (X). The form contains several input fields: 'Username' (containing 'mydlp'), 'Email' (containing 'user@mydlp.com'), 'Current Password', 'New Password', and 'Reenter New Password'. At the bottom, there are two buttons: a red 'Cancel' button and a blue 'Save' button.

- Change the password and click 'Save'

## Step 3 – Install CDDP Agent on Network Computers

The next step is to install CDDP agent on to endpoints in the network and outside network that you want to monitor and control data passing through them and also run discovery scans to identify confidential data in existing files. You can install the agent via Active Directory Group Policy Object (GPO) method for bulk enrollment or install the agent manually on each endpoint one by one.

To download the CDDP agent, click 'License' > 'Downloads', then 'Click here to download' button beside 'Windows Endpoint'.

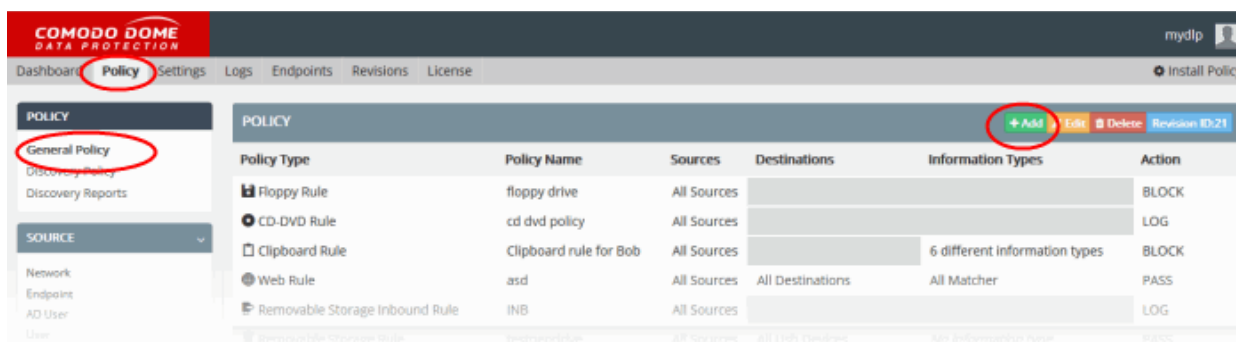


The agent will be stored in your default download location. See the endpoint installation guide at <https://help.comodo.com/topic-283-1-598-7034-About-CDDP.html> for more details about installing agent on to endpoints.

## Step 4 – Create Data Transfer Rules

After installing CDDP agent on to endpoints, the next step is to create a policy according to your organization's requirement. There are two types of rules, Data Transfer Rules and Data Discovery Rules, that comprise a policy. You can add any number of rules as required for a policy. This step explains how to create a data transfer rule and next step how to create a data discovery rule.

To create a data transfer rule, click 'Policy', then 'General Policy' on the left under 'Policy' section



- Click the 'Add' button.

The rule creation wizard will start.

**General Rule Edit** [Close]

**Name**  
[Text Input]

**Type**  
Web Rule [Dropdown]

**Description**  
Place enter your description here [Text Area]

**Message to User**  
[Text Area]

Enable Notifications

[Cancel] [Back] [Next]

- Select the type of the rule to be created from the 'Type' drop-down.

**General Rule Edit** [X]

**Name**  
[Text Input Field]

**Description**  
[Text Area: Place enter your description here]

Enable Notifications

**Type**  
Web Rule [Dropdown Menu]

- 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

[X Cancel] [← Back] [Next →]

There are 13 types of data transfer control rules that can be configured in CDDP.

- **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 memory sticks, removable hard drives and smart phones. See **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 **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 screen function while a sensitive application is running. See **Screenshot rule** for more details.
- **Printer rules** allow you to 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 **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 **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 **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 **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 **Clipboard Rule** for more details.
- **Network Share Rules** are used to monitor and control data traffic from endpoints to Windows share locations. See **Network Share Rules** to find out more.

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

**General Rule Edit**

**Name**  
Docs Uploading

**Type**  
Web Rule

**Description**  
For restricting uploading of documents containing credit card numbers to Google and Yahoo

**Message to User**  
Sensitive information. Do not upload

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 the message 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 under 'Settings' > 'Enterprise' tab. See **Configuring 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'

**General Rule Edit**

Name: Docs Uploading      Type: Web Rule

**Description**  
For restricting uploading of documents containing credit card numbers to Google and Yahoo

**Message to User**  
Sensitive information. Do not upload

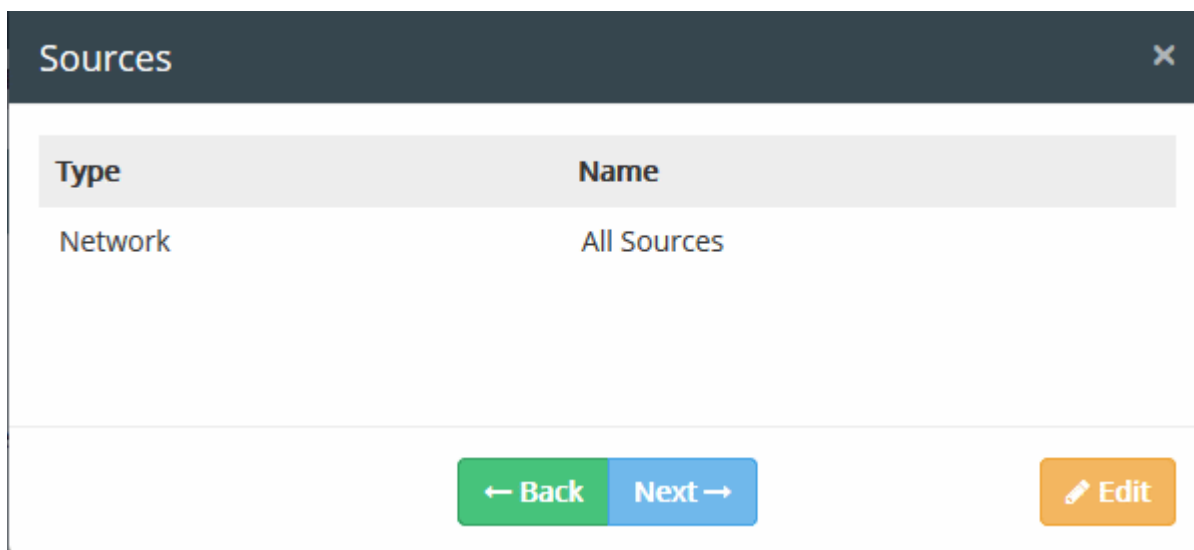
Enable Notifications

User Name	E-mail
✓ mydlp	user@mydlp.com
dlp_ent@yopmail.com	dlp_ent@yopmail.com
✓ johnsmith	uat_q3_ent@yopmail.com
uat_q3_ent@yopmail.com	uat_q3_ent@yopmail.com

Buttons: **Cancel**      **← Back**      **Next →**

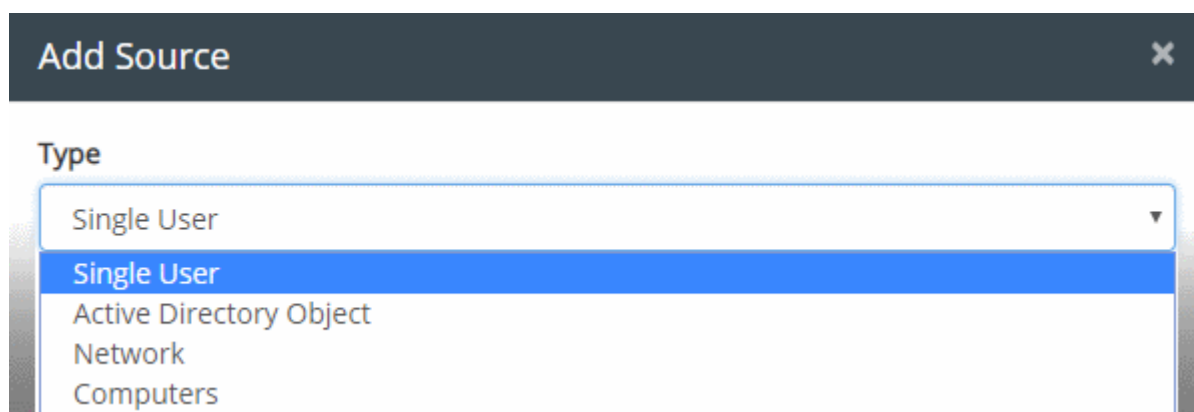
The 'Sources' screen will be displayed.





- Click the 'Edit' button

The origin of the data transfer can be added as the 'Source' component of the rule, by selecting the source object type from the 'Type' drop-down.



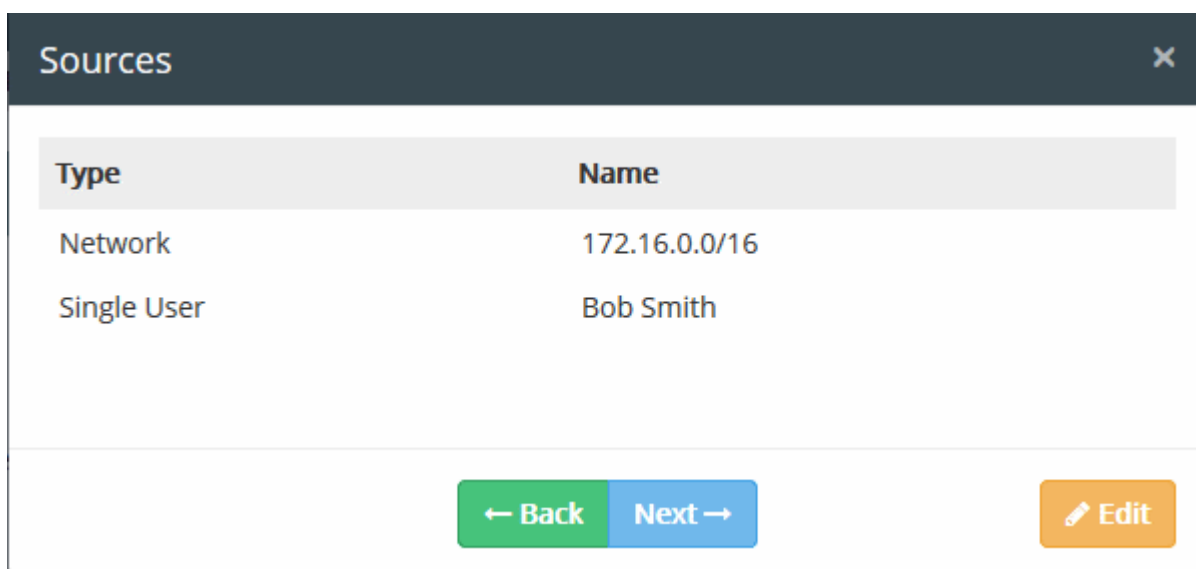
The 'Network' object type has 'All Sources' built-in object and will be available for all rule types. 'All Sources' object when added to a rule as a source type means that all objects in the network, will be scanned for the defined information type. To make the source type more specific to enforce a rule, you have to add custom defined objects for the object types. See **User Defined Objects** for more details.

- Select the object type from the 'Type' drop-down

The objects listed for the selected object type depends on the predefined and user defined objects defined for it.

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

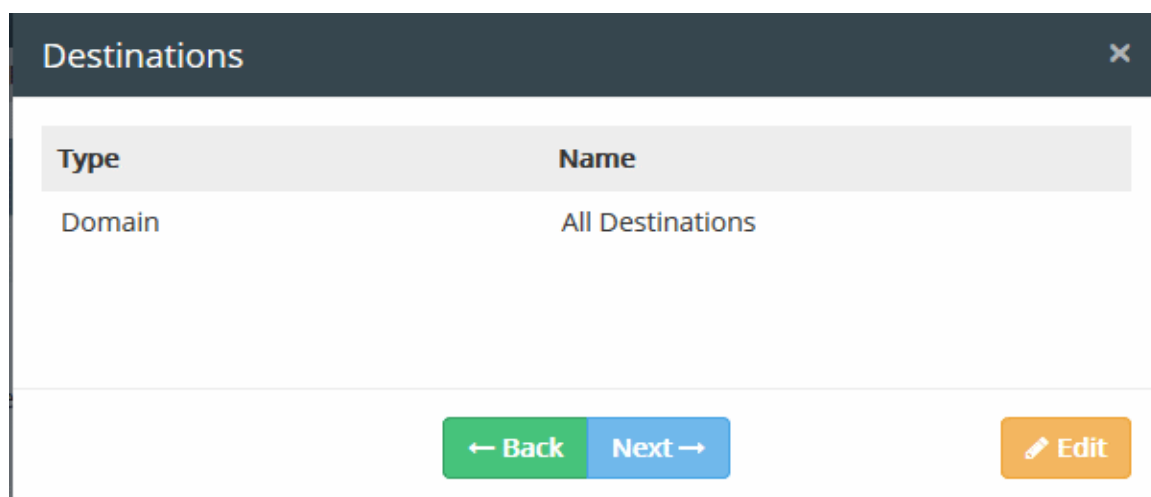
All the sources added for different object types will be listed.



- Click 'Next' to proceed to add destinations

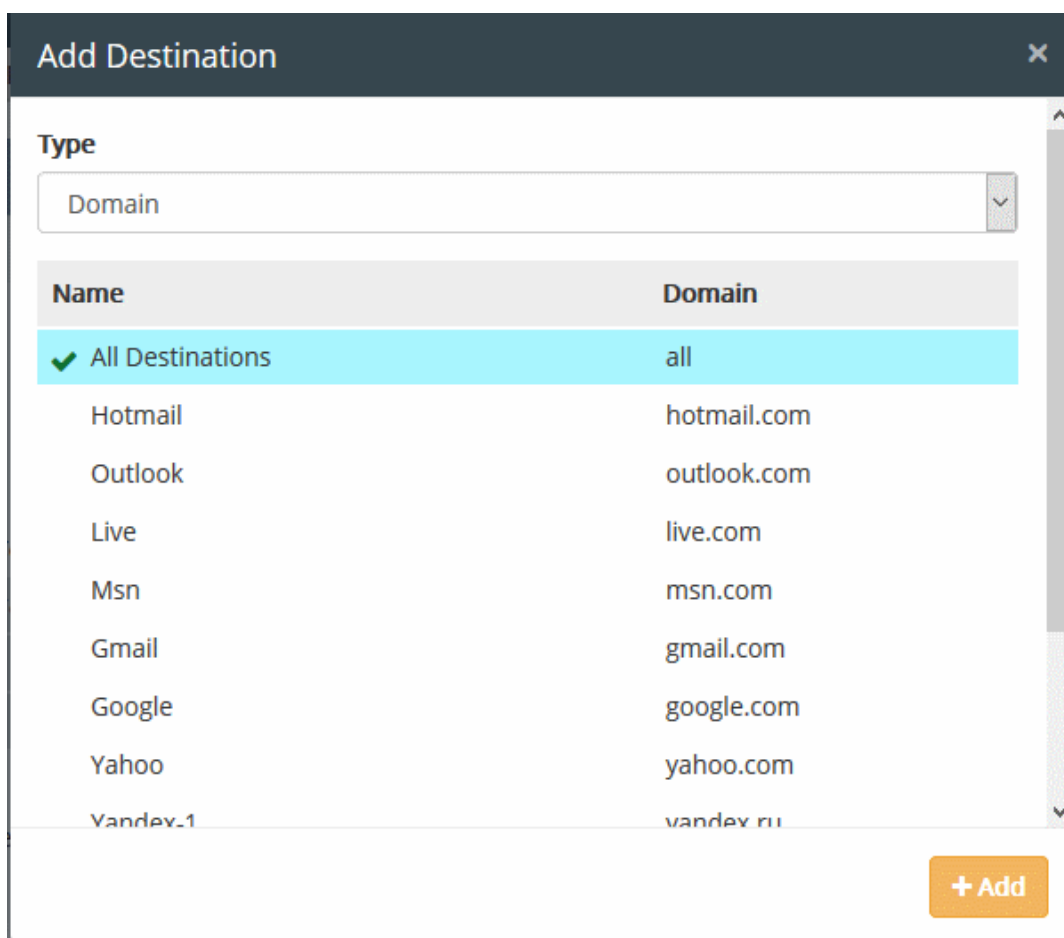
The 'Destinations' dialog will be displayed:

<new image>



- Click the 'Edit' button

The 'Add Destination' dialog will be displayed.



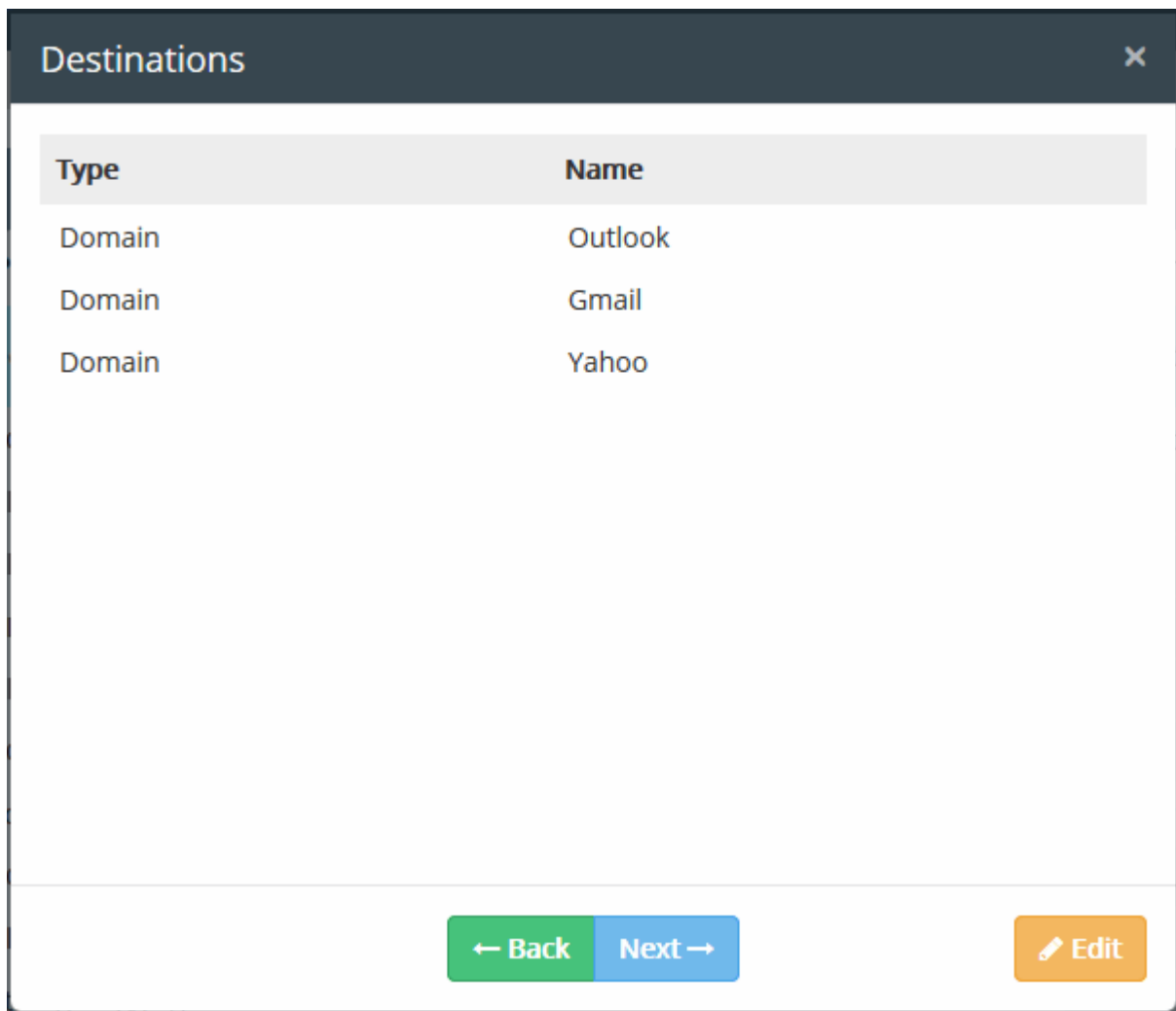
The target of the data transfer can be added as the 'Destination' component of the rule, by selecting the destination object type from the 'Type' drop-down. The following table shows the object types that can be used for defining Destinations and applicable rule types.

Object 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>

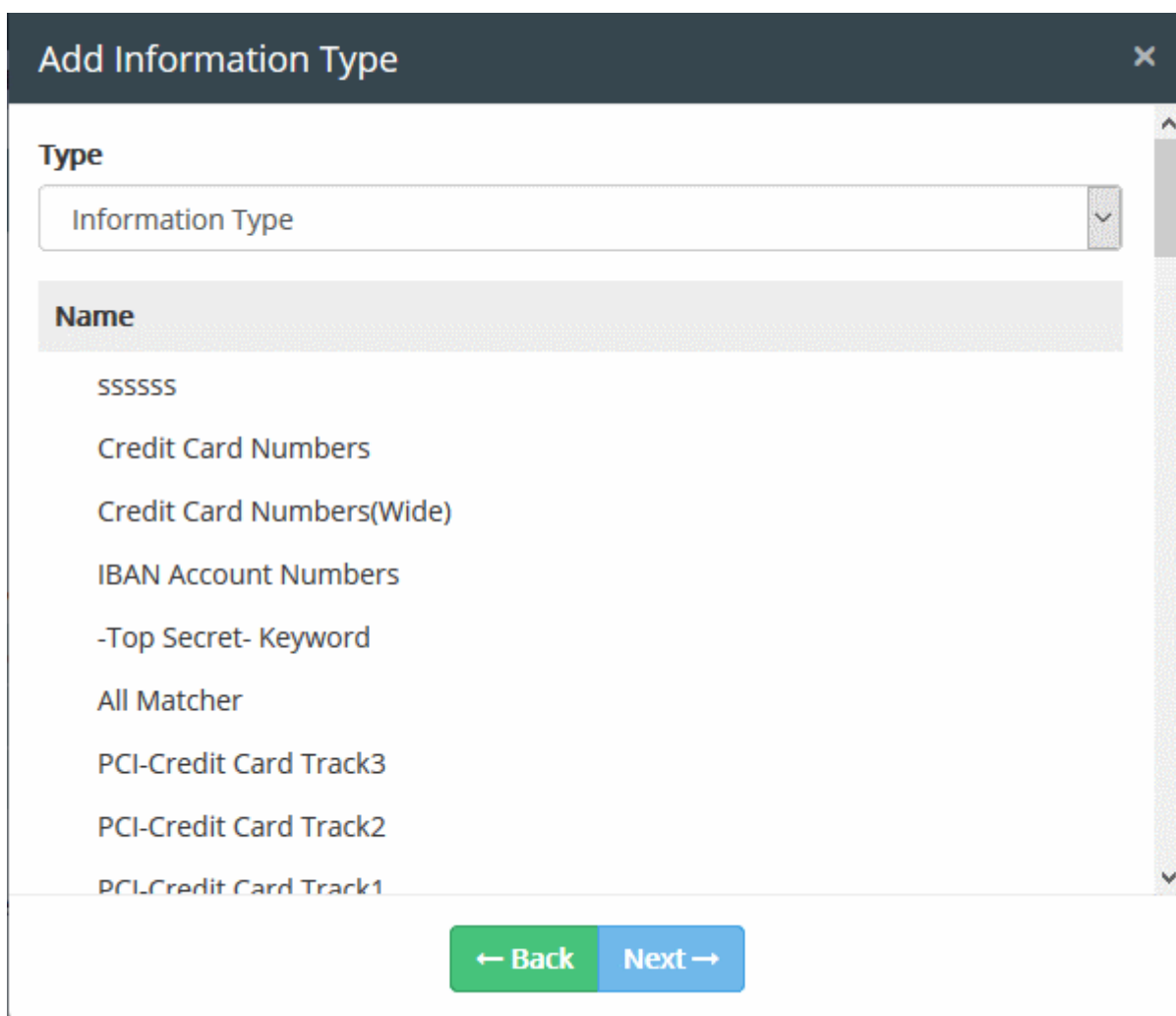
The objects listed for the selected object type depends on the predefined and user defined objects defined for it. See **User Defined Objects** for more details about adding user defined objects. For example, if you choose 'Domains', the predefined and user defined domain objects will be displayed.

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

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



- Click 'Next' to proceed to add information type that must be checked by CDDP for the rule  
The 'Add Information Type' dialog will be displayed.



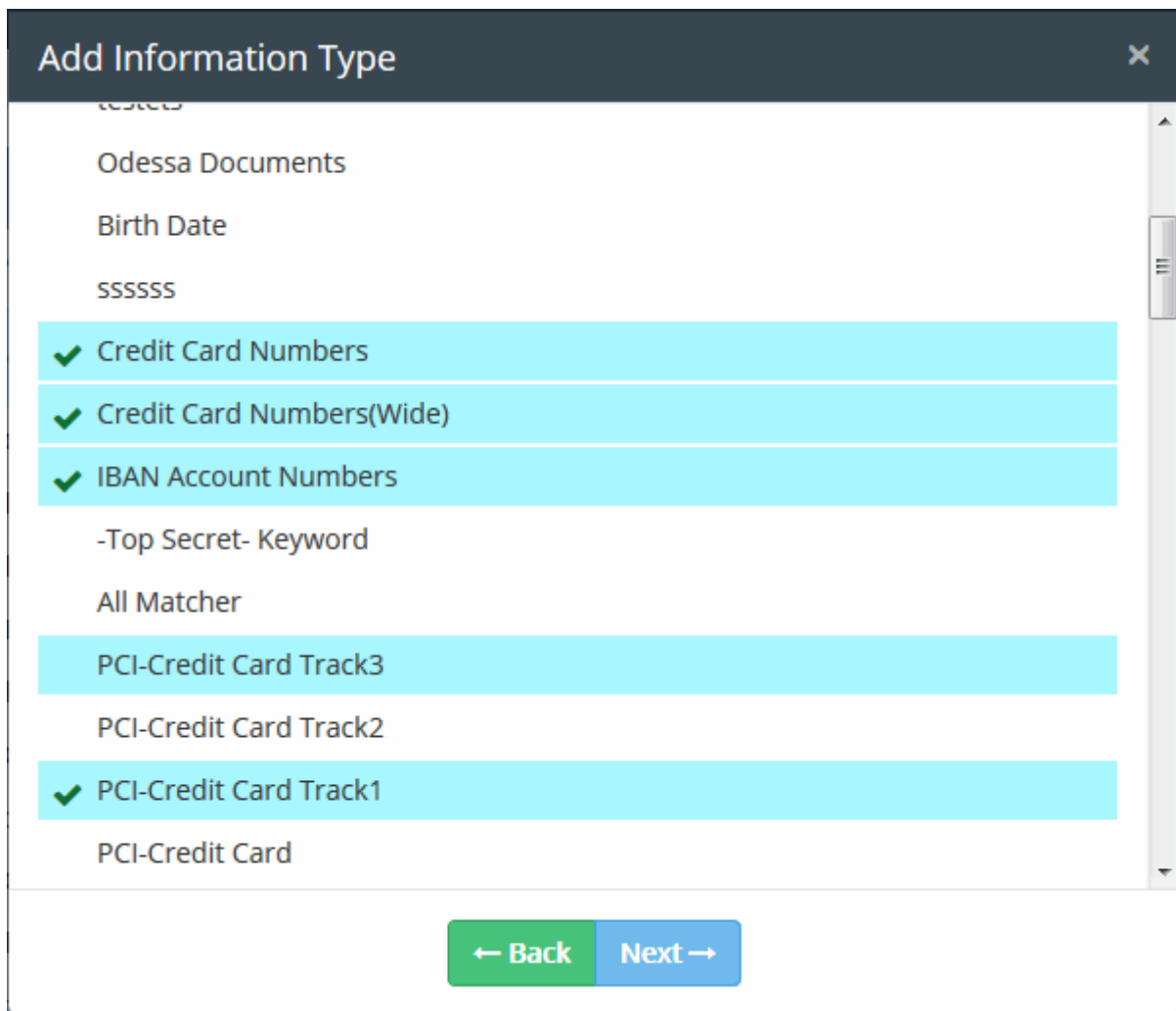
The objects listed for the selected object type depends on the predefined and user defined objects defined for it.

CDDP is shipped with a number of commonly and frequently used Information Types. In addition, the administrator can add more number of custom information types. See **User Defined Objects** for more details about adding user defined information type objects.

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

Object	Applicable Rule Types
Information Type	<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>

- Select the information type(s) from the list



The screenshot shows a dialog box titled "Add Information Type" with a close button (X) in the top right corner. The dialog contains a list of information types, each with a checkbox. The following items are checked:

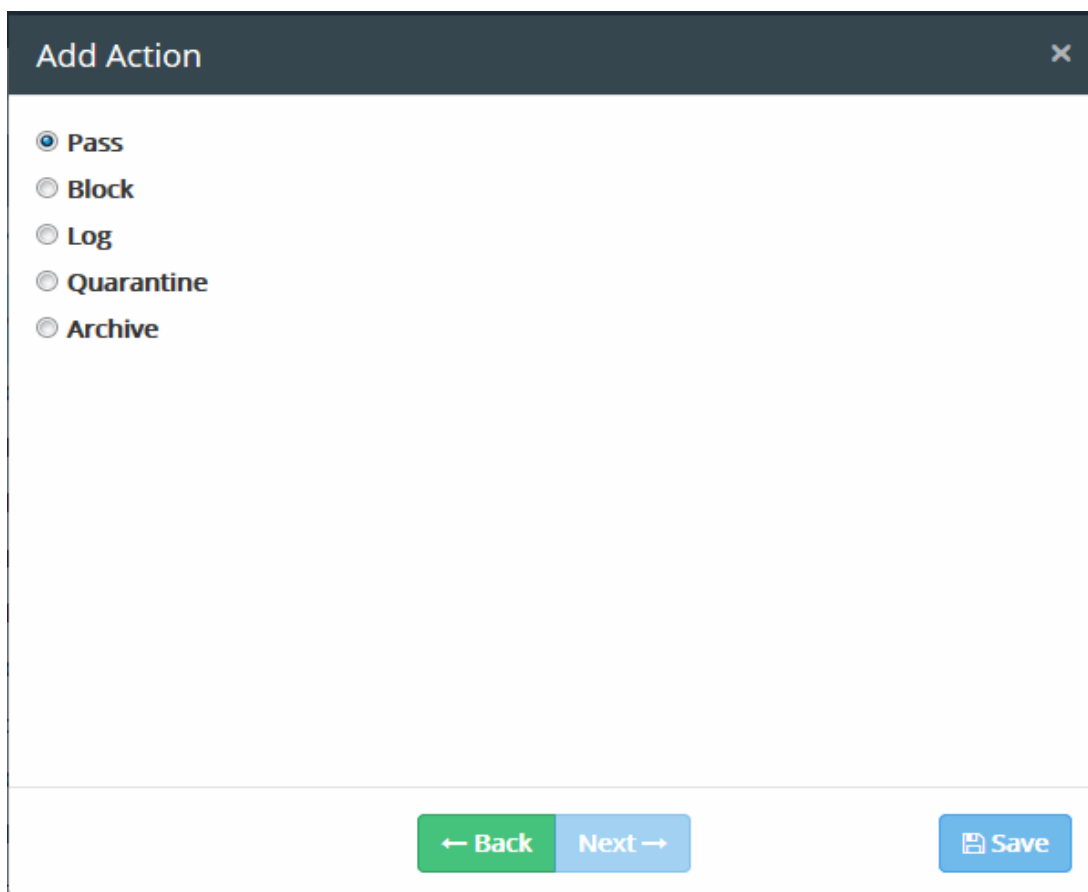
- Credit Card Numbers
- Credit Card Numbers(Wide)
- IBAN Account Numbers
- PCI-Credit Card Track3
- PCI-Credit Card Track1

Other items in the list include:

- Odessa Documents
- Birth Date
- SSSSSS
- Top Secret- Keyword
- All Matcher
- PCI-Credit Card Track2
- PCI-Credit Card

At the bottom of the dialog, there are two buttons: "← Back" (green) and "Next →" (blue). The "Next" button is highlighted.

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



The screenshot shows a dialog box titled "Add Action" with a close button (X) in the top right corner. Inside the dialog, there are five radio button options: "Pass" (selected), "Block", "Log", "Quarantine", and "Archive". At the bottom of the dialog, there are three buttons: "Back" (green), "Next" (blue), and "Save" (blue).

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

- Choose the action from the options. The available actions are:
  - **PASS** - Allows information to pass through the data channel freely without generation of any log entries. This action is the default action and available for all rule types.
  - **BLOCK** - Prevents information to pass through data channel and generates event log. This action is not available for removable storage inbound rules.
  - **LOG** - Creates a log entry when data passes through the data channel. This action is not available for screenshot rule and Floppy rule.
  - **QUARANTINE** - Prevents information to pass, generates event log and archives a copy of information in the Comodo Dome Data Protection Server. The Administrator can download the file from the Logs interface. See [Downloading 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 through data channel, generates event log and archives a copy of information. The Administrator can download the file from the Logs interface. See [Downloading 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'

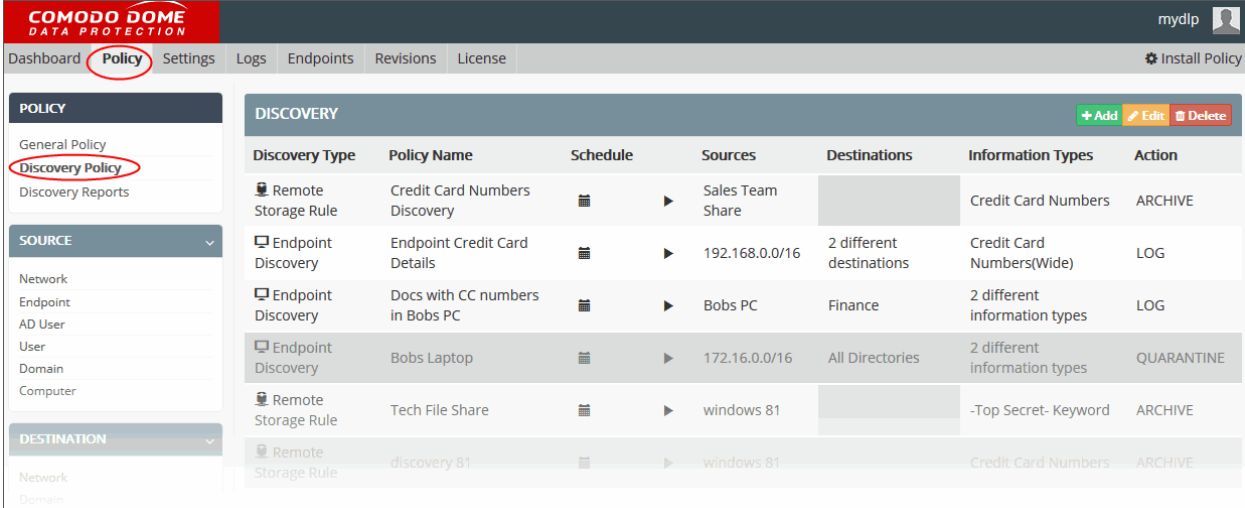
The rule will be saved. You can create as many rules as required. If you are creating a new rule with minor changes from an existing rule, you can clone the rule and edit it to change the required parameters.

The rules take effect only on applying/reapplying the policy to the network. See **Step 6 - Deploy the Policy** for more details.

## Step 5 – Create Data Discovery Rules

The next step is to create data discovery rules to identify files containing sensitive information. The targets, schedule, information searched for, and the action to be taken is specified in a Discovery Rule.

To create a data discovery rule, click 'Policy', then 'Discovery Policy' on the left under 'Policy' section

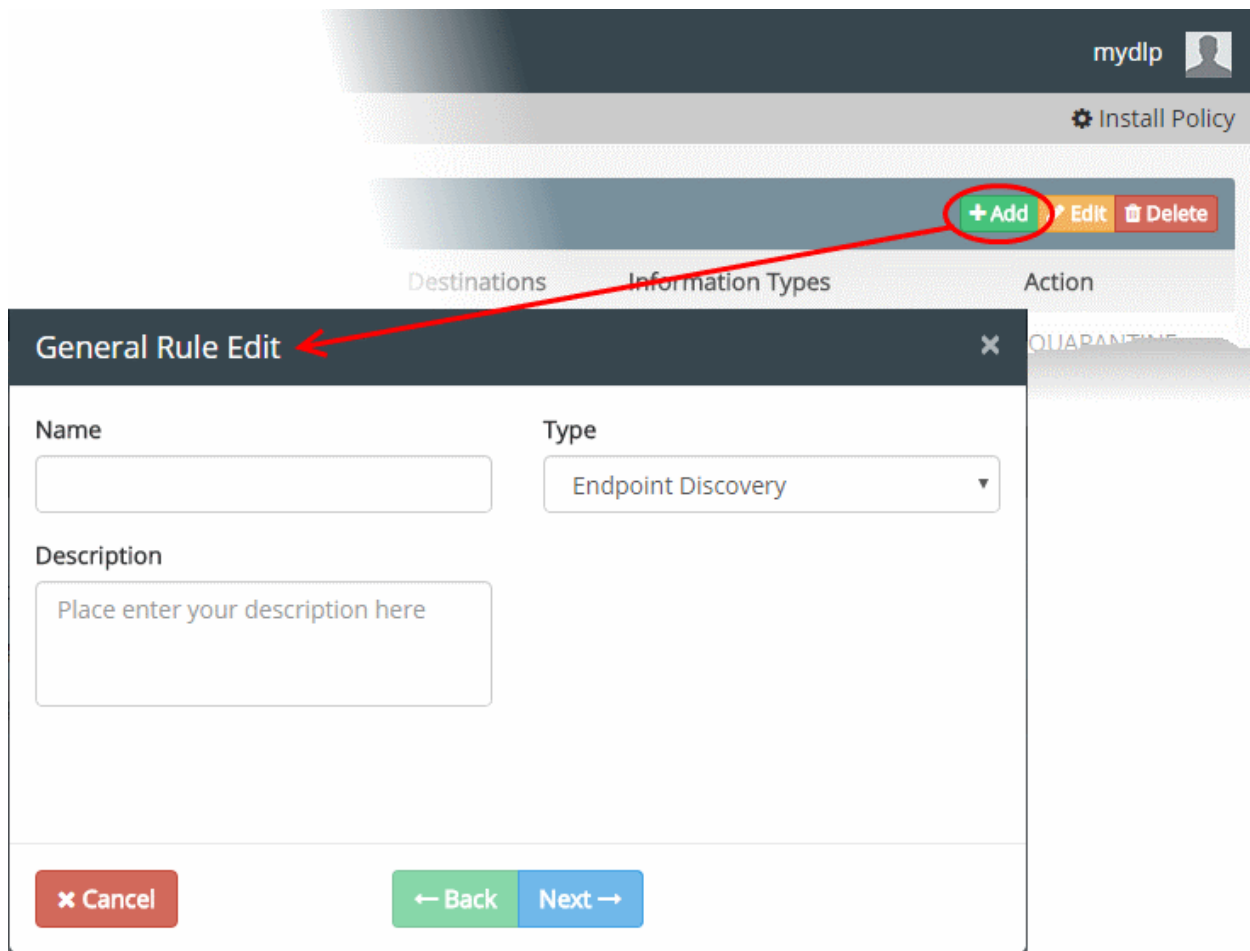


Discovery Type	Policy Name	Schedule	Sources	Destinations	Information Types	Action
Remote Storage Rule	Credit Card Numbers Discovery		Sales Team Share		Credit Card Numbers	ARCHIVE
Endpoint Discovery	Endpoint Credit Card Details		192.168.0.0/16	2 different destinations	Credit Card Numbers(Wide)	LOG
Endpoint 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
Remote Storage Rule	Tech File Share		windows 81		-Top Secret- Keyword	ARCHIVE
Remote Storage Rule	discovery 81		windows 81		Credit Card Numbers	ARCHIVE

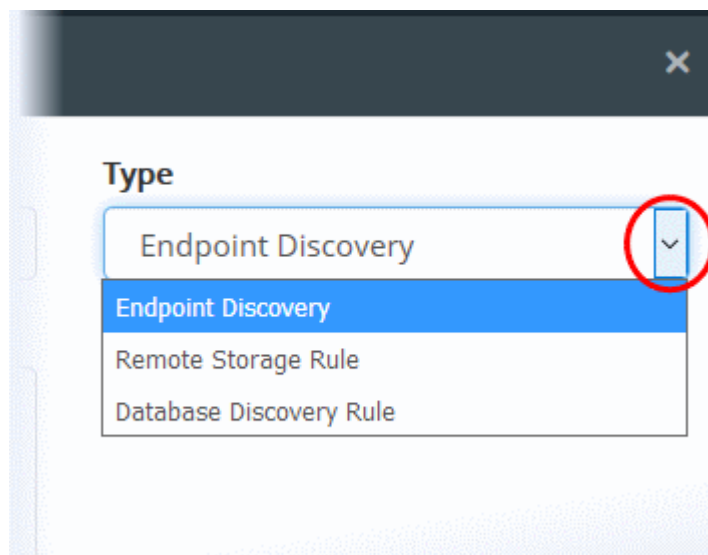
- Click the 'Add' button.

The discovery rule creation wizard will start.





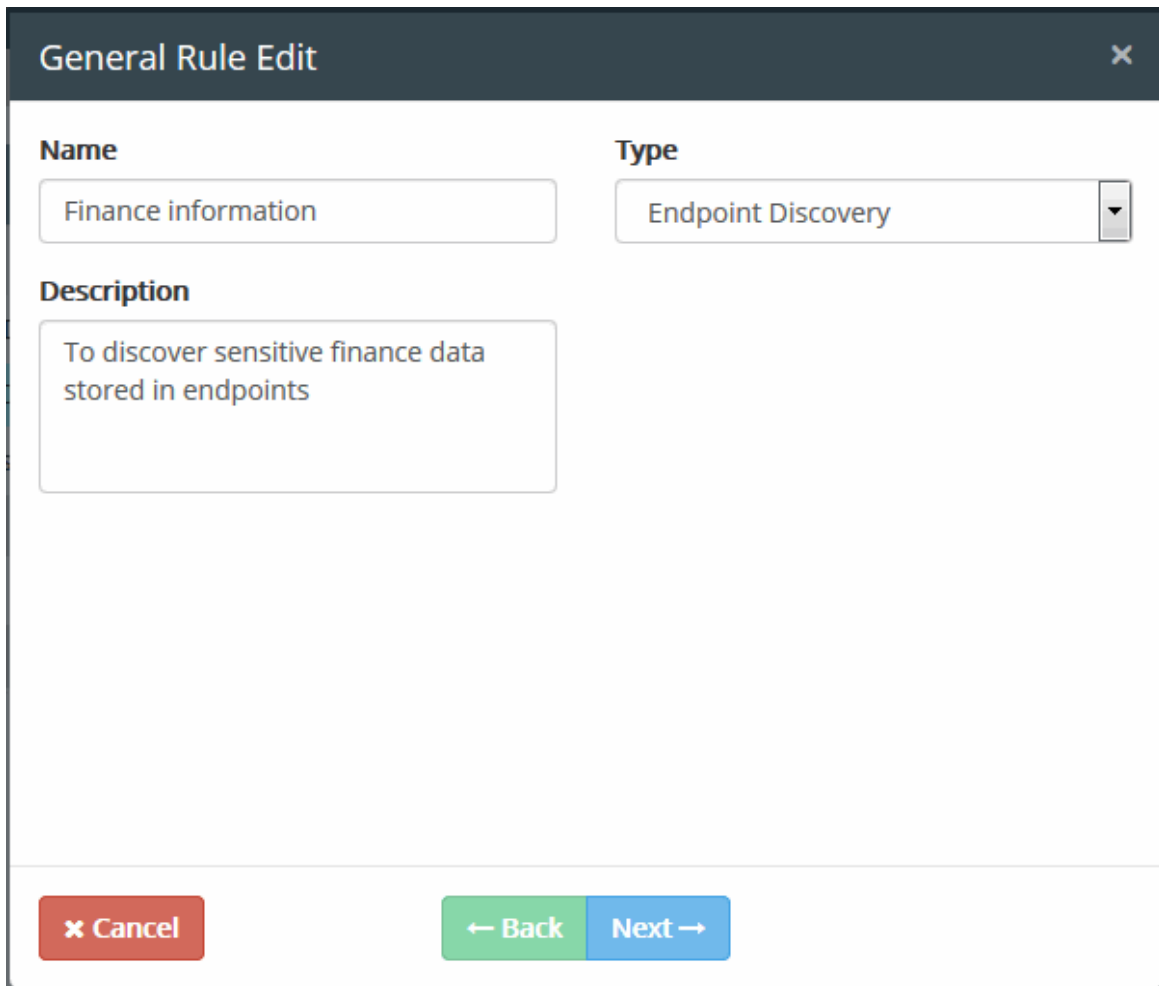
- Select the type of the rule to be created from the 'Type' drop-down.



There are three types of data discovery rules that can be configured in CDDP.

- **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 scan databases to find out sensitive information stored on them.

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



**General Rule Edit** [X]

**Name**  
Finance information

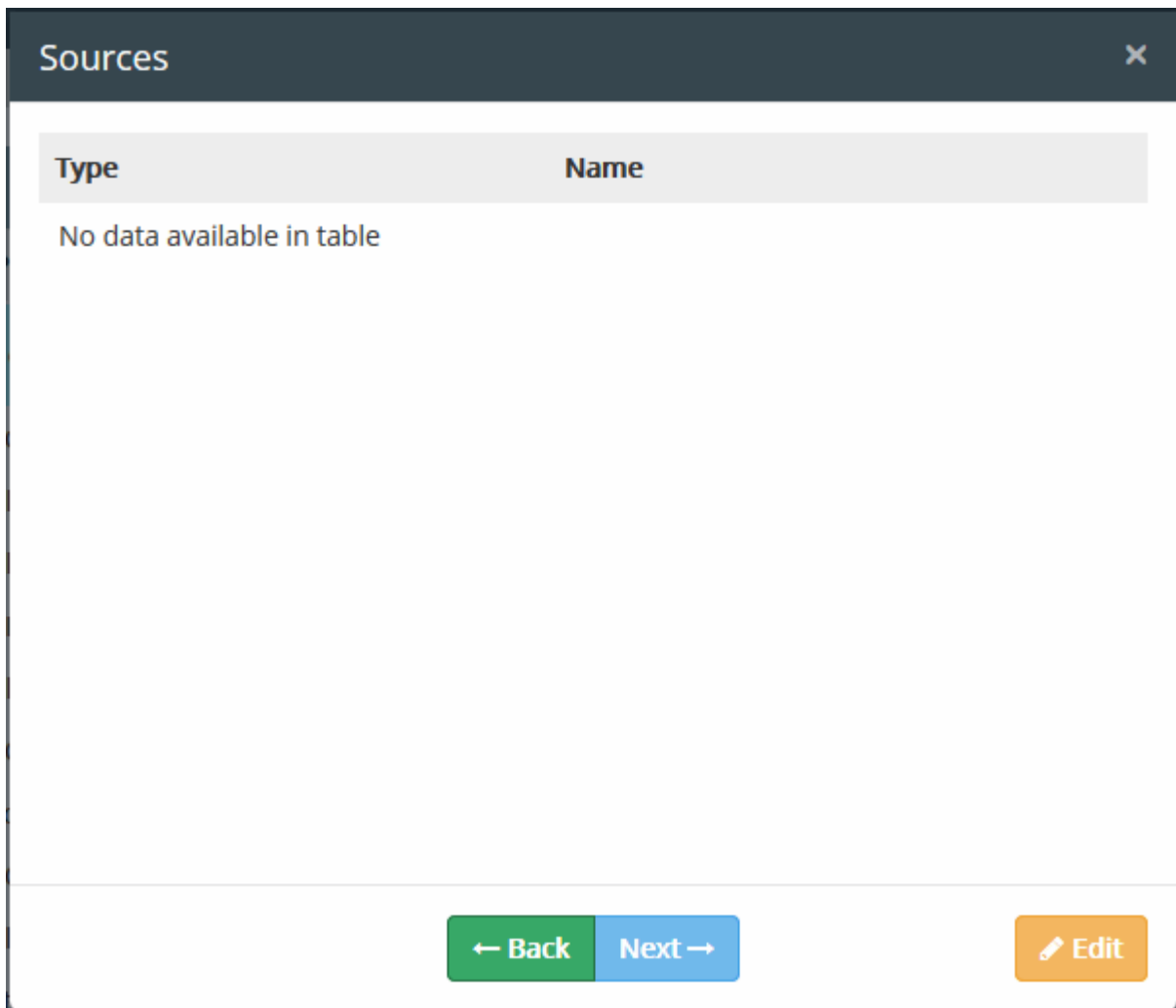
**Type**  
Endpoint Discovery

**Description**  
To discover sensitive finance data stored in endpoints

[X] Cancel   ← Back   Next →

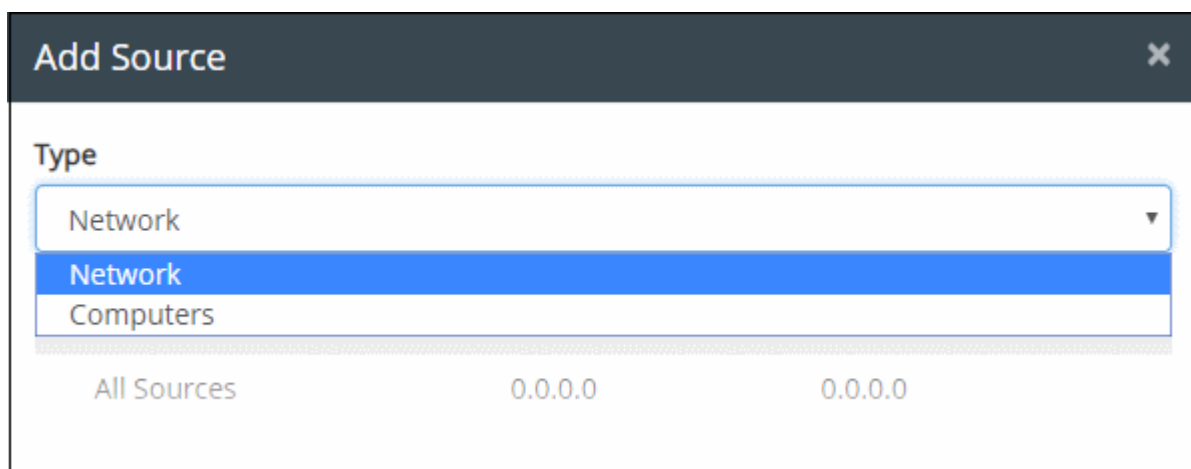
- Enter a name, shortly describing the new rule and description in the respective fields
- Click 'Next'

The 'Sources' screen will be displayed.



- Click the 'Edit' button

The origin of the data discovery can be added as the 'Source' component of the rule, by selecting the source object type from the 'Type' drop-down.



The following table shows the object types that can be used for defining Sources and applicable rule types:

Object	Applicable Rule Types
Network	<ul style="list-style-type: none"> <li>• Endpoint Discovery rule</li> </ul>

Computers	<ul style="list-style-type: none"> <li>Endpoint Discovery rule</li> </ul>
Remote Storage	<ul style="list-style-type: none"> <li>Remote Storage rule</li> </ul>
Database Connections	<ul style="list-style-type: none"> <li>Database Discovery Rule</li> </ul>

The 'Network' object type has 'All Sources' built-in object and will be available for discovery rule. 'All Sources' object when added to a rule as a source type means that all objects in the network, will be scanned for the defined information type. To make the source type more specific to enforce a rule, you have to add custom defined objects for the object types. See **User Defined Objects** for more details.

- Select the object type from the 'Type' drop-down

The objects listed for the selected object type depends on the predefined and user defined objects defined for it.

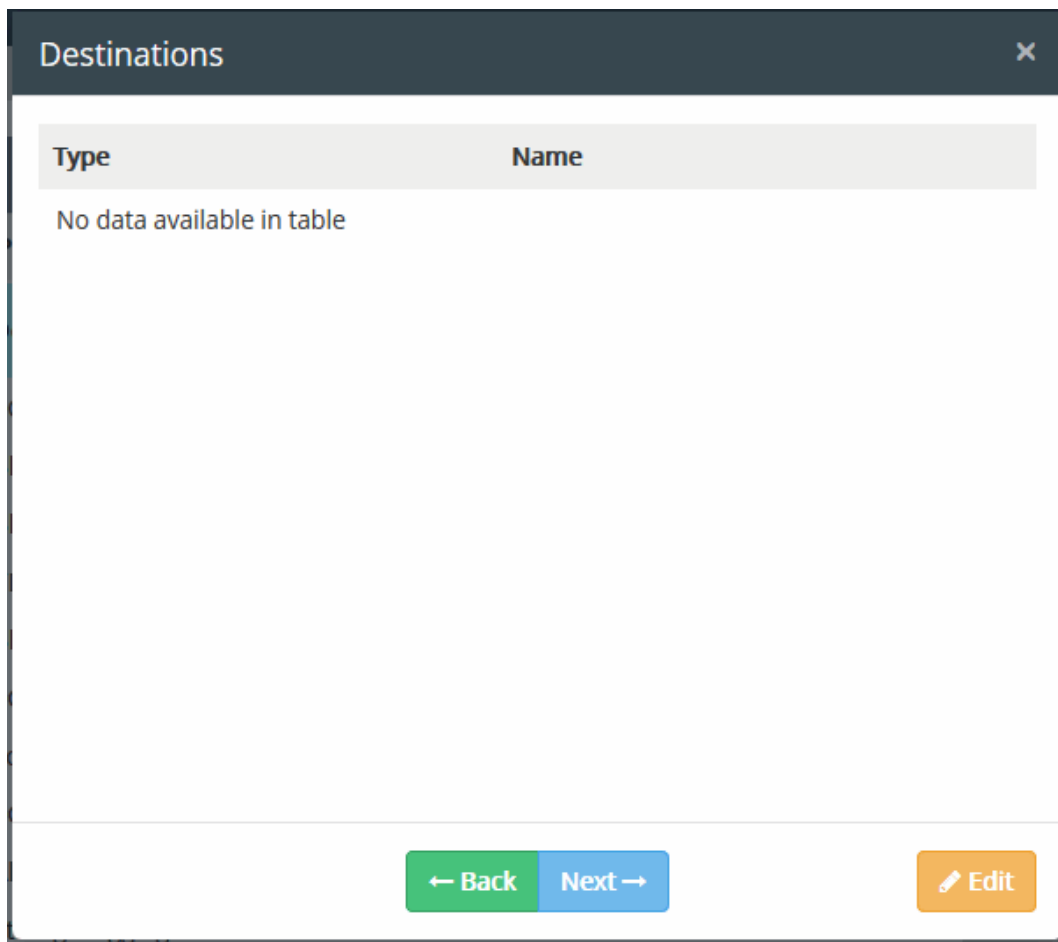
- Select the object(s) from the list
- To add more sources for other object types, select another object type from the 'Type' drop-down again and follow the same procedure explained above.
- Please note for remote discovery rule and database discovery rule, only remote storage and database connection objects, respectively will be available.

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

Type	Name
Network	10.0.0.0/24
Network	192.168.0.0/16
Computers	Finance
Computers	Purchase Dept. Computer

- Click 'Next' to proceed to add destinations

The 'Destinations' dialog will be displayed. Please note for remote discovery rule and database discovery rule, destination is not applicable.



- Click the 'Edit' button

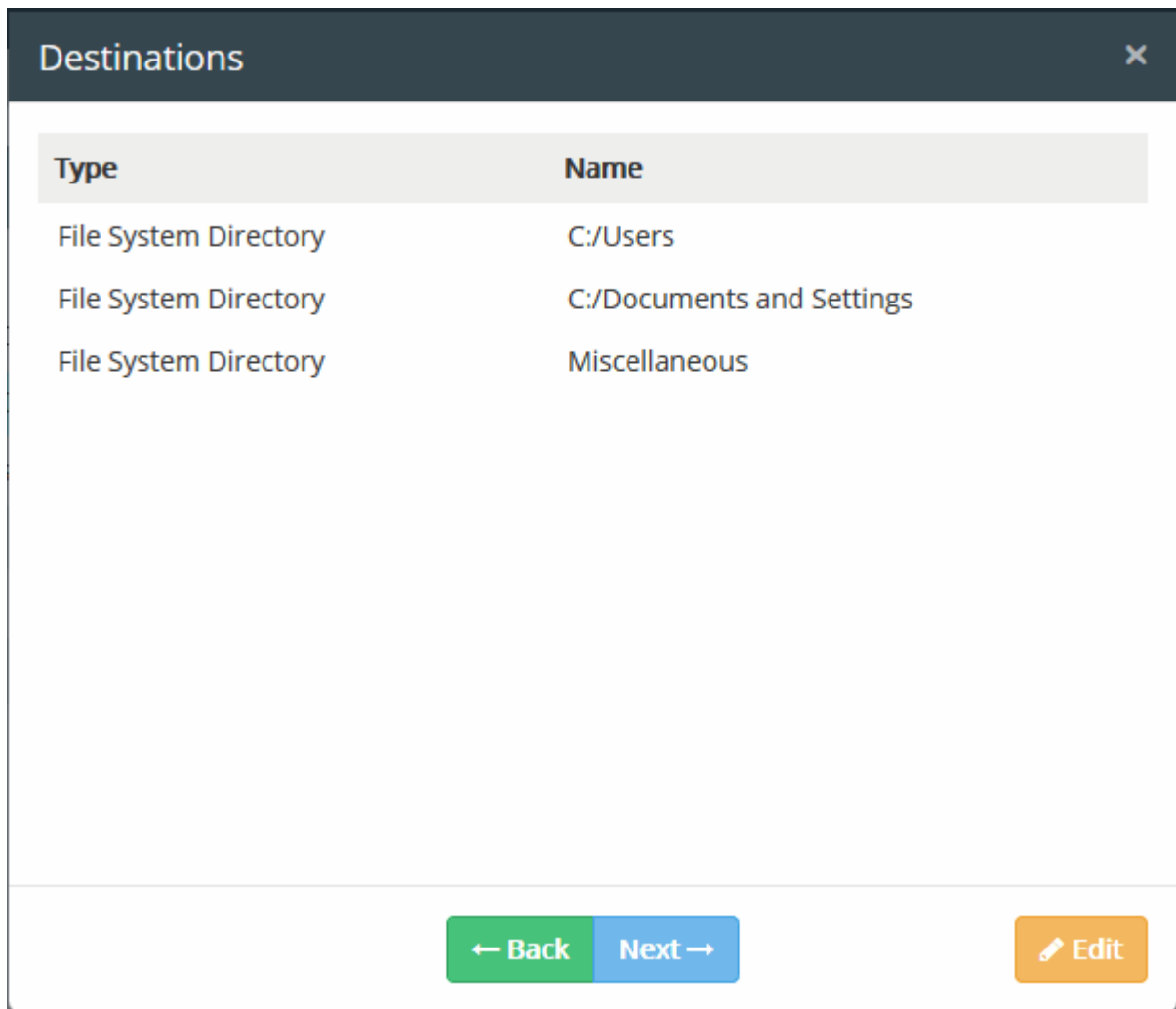
The 'Add Destination' dialog will be displayed.

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
Miscellaneous	E:\Critical Notes

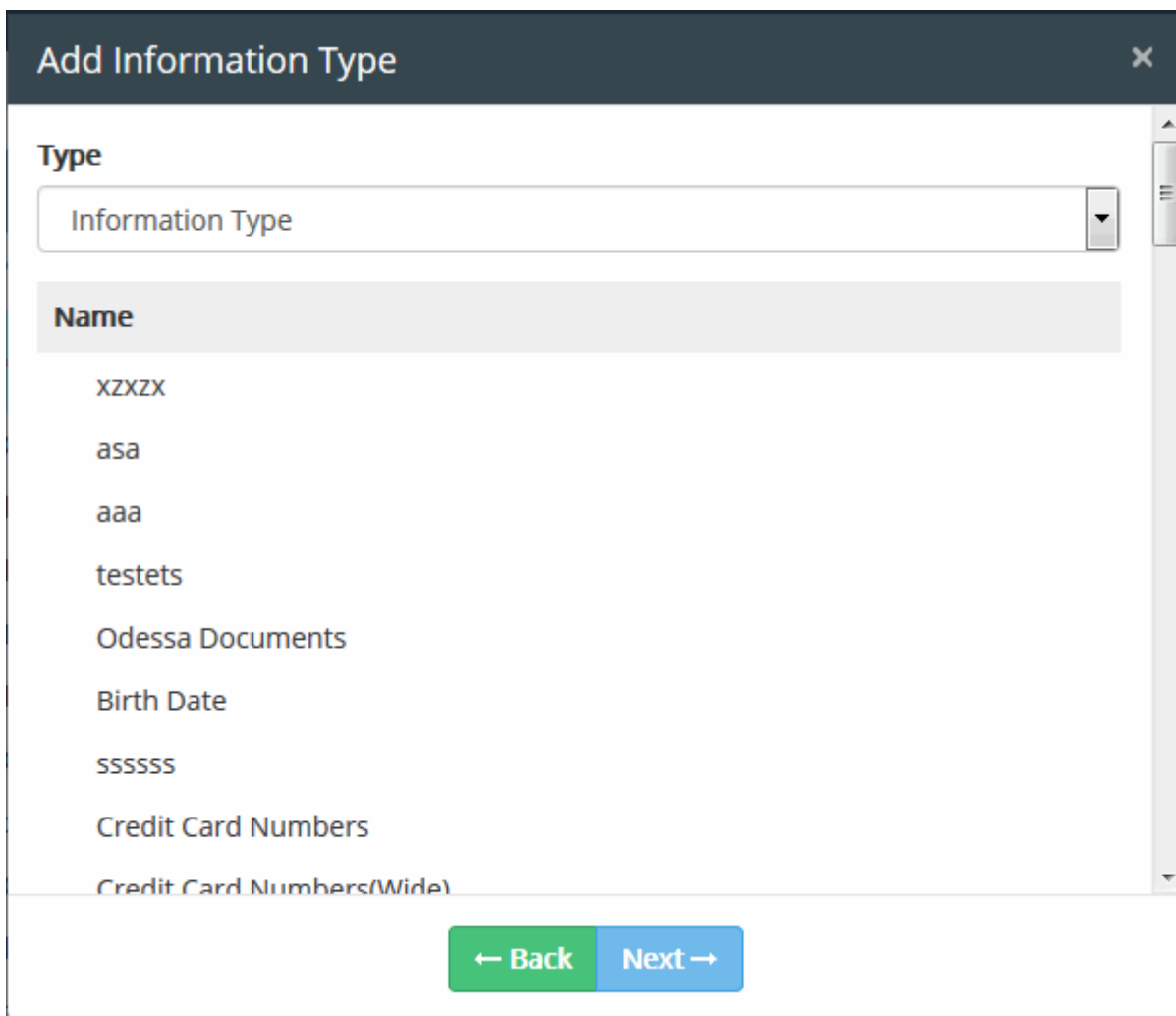
The objects listed for the selected object type depends on the predefined and user defined objects defined for it. See **User Defined Objects** for more details. Please note for Endpoint Discovery rule, only File System Directory object type is available. The predefined and user defined file system objects will be displayed.

- Select an object(s) from the list

All the destinations added will be listed.



- Click 'Next' to proceed to add information type that must be checked by CDDP for the rule. The 'Add Information Type' dialog will be displayed.



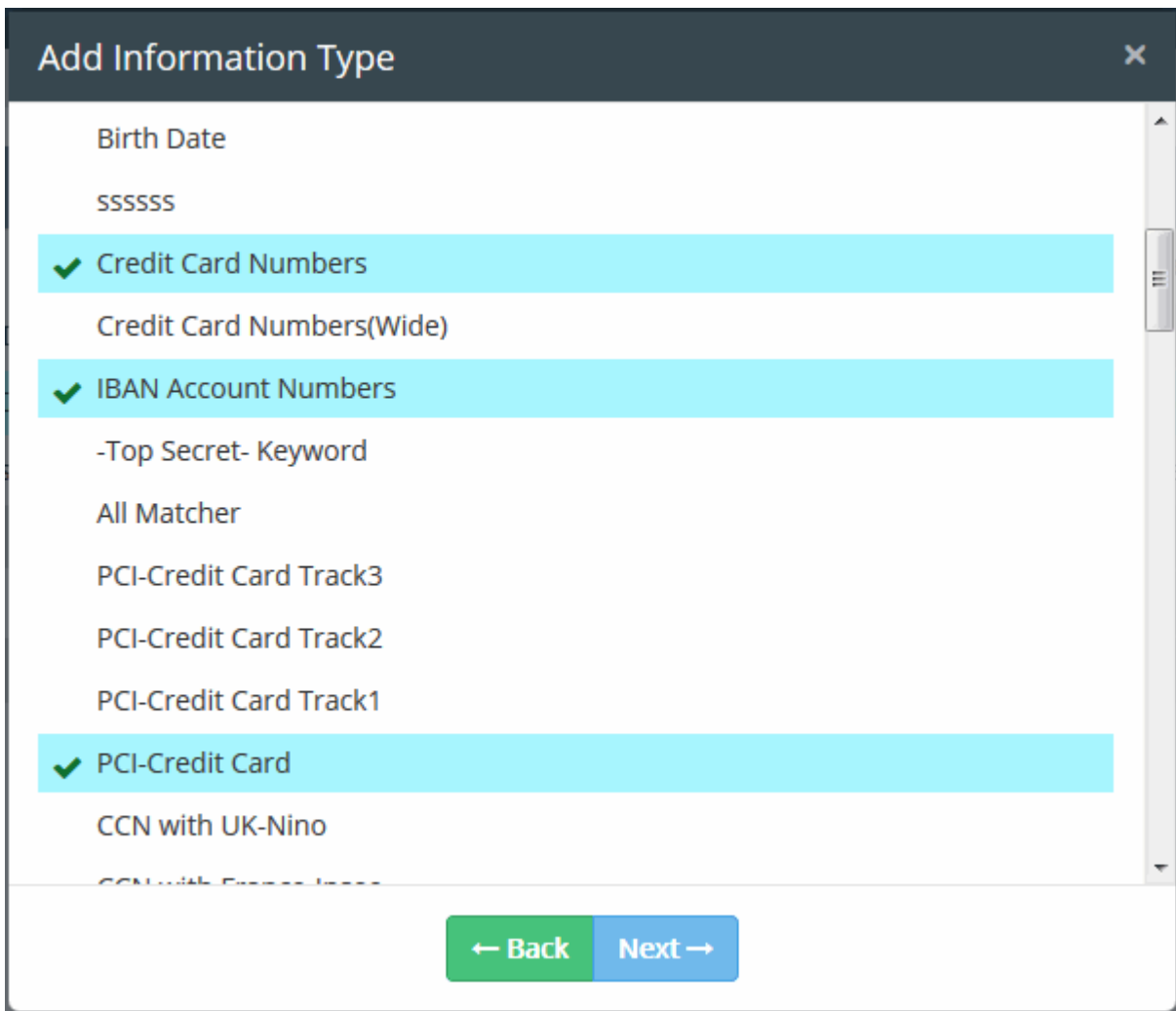
The objects listed for the selected object type depends on the predefined and user defined objects defined for it.

CDDP is shipped with a number of commonly and frequently used Information Types. In addition, the administrator can add more number of custom information types. See **User Defined Objects** for more details about adding user defined information type objects.

For CDDP to discover files containing sensitive data of specific type, the respective information type object is to be added to the rule.

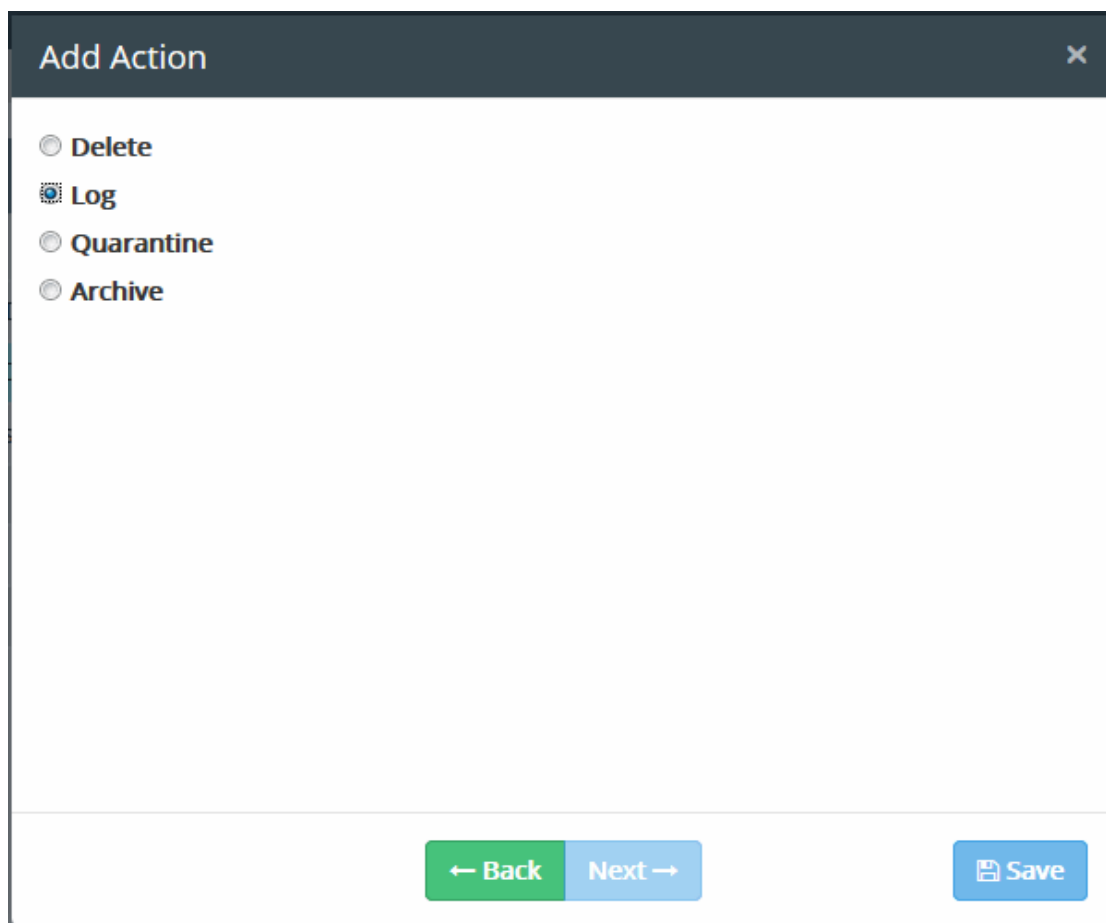
- Select the information type(s) from the list





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

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



- Choose the action from the options. Please note the available actions depends on the selected source and destination objects. The available actions are:
  - **DELETE** - Deletes matched discovered files. It is advised to use this action very carefully. This action is available only for Endpoint Discovery Rules.
  - **LOG** - Generates event log.
  - **QUARANTINE** - Removes the identified file from the endpoint and saves an archive copy in the Comodo Dome Data Protection server. The Administrator can download the file from the Logs interface. See [Downloading the Files Archived by CDDP](#) for more details.
  - **ARCHIVE** - Generates event log and archives a copy of information. The Administrator can download the file from the Logs interface. See [Downloading the Files Archived by CDDP](#) for more details.

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

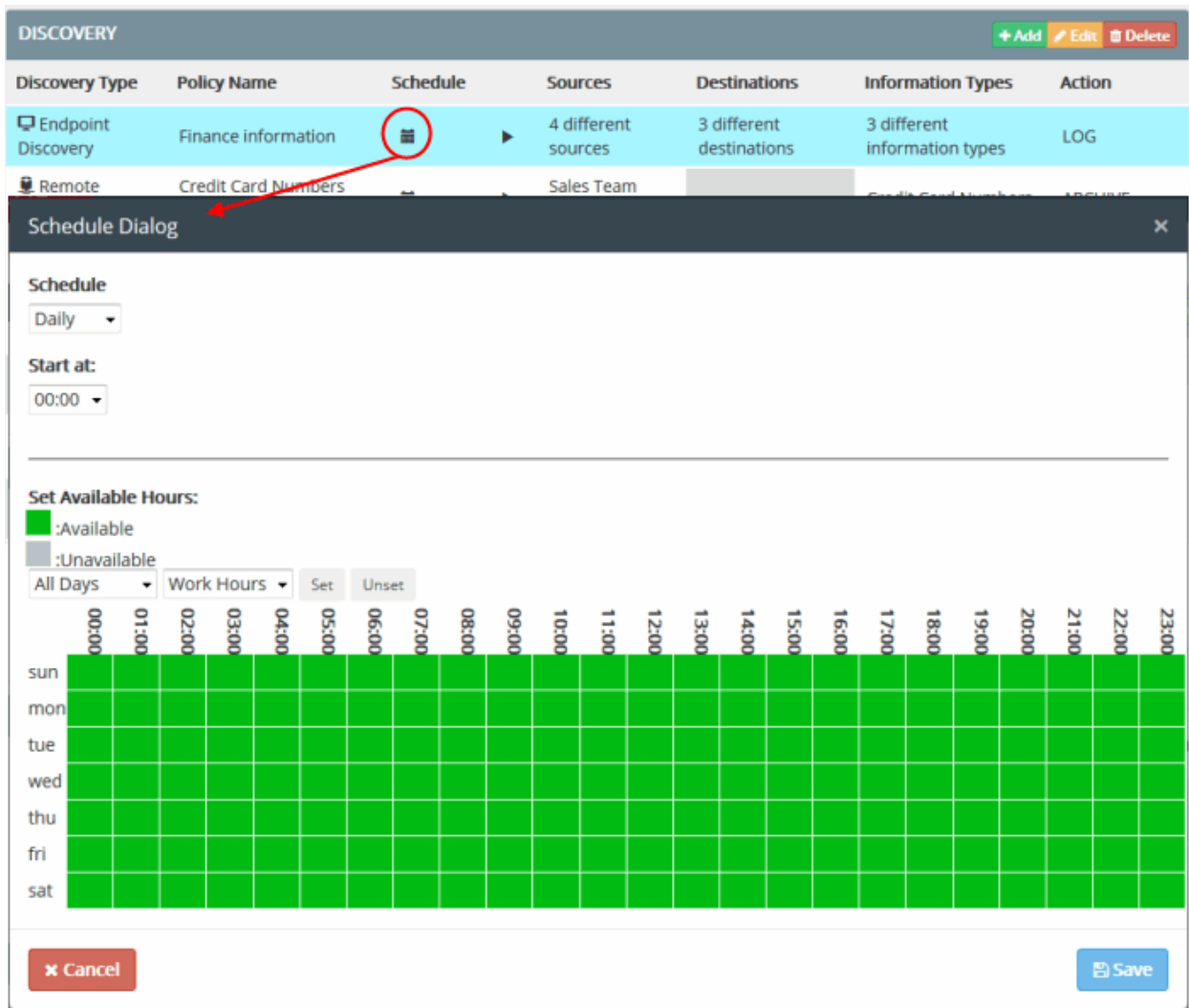
- At any time during the rule creation, click 'Back' to review your configuration for the rule
- Click 'Save'

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 data discovery rules can be scheduled to run periodically or can be run instantly.

### To set a scan schedule in a rule

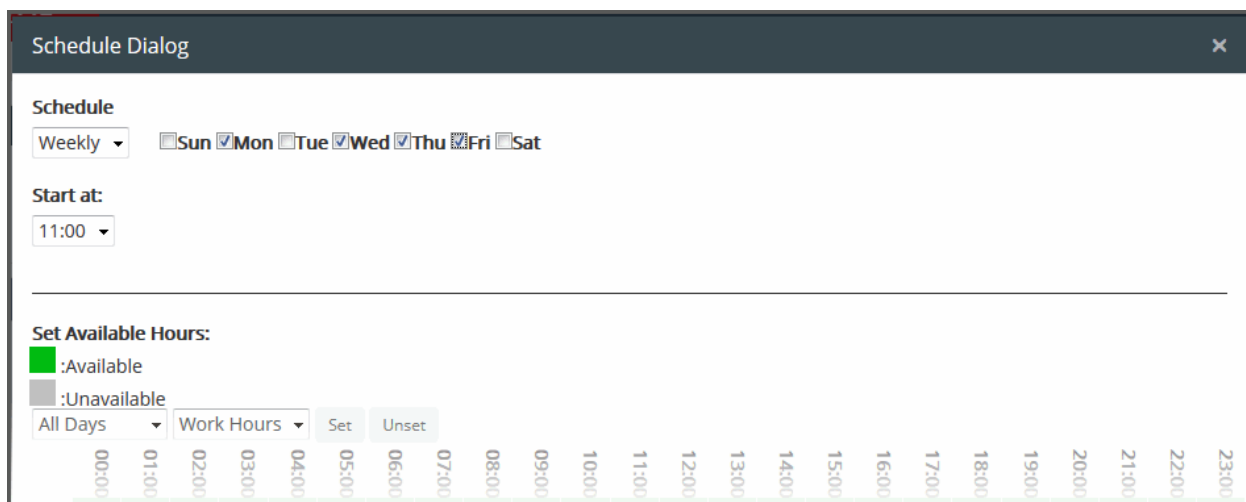
- Click 'Policy', then 'Discovery Policy' on the left under 'Policy' section
- Click the Calendar button beside the rule under the Schedule column.



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

## Schedule

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



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

## Available/Unavailable Hours

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

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

- Green blocks indicate that the endpoints/repositories are available for scanning
- Gray blocks indicate that the endpoints/repositories are not available for scanning
- To manually switch specific hours of days at which the endpoints/repositories will be unavailable, click the respective blocks.
- To automatically set specific time periods as unavailable hours,
  - Choose the day(s) of the week from the first drop-down.
  - Choose the hours from the second drop-down
  - Click 'Unset'
- To automatically set specific time periods as available hours,
  - Choose the day(s) of the week from the first drop-down.
  - Choose the hours from the second drop-down
  - Click 'Set'
- Click 'Save' to save the schedule

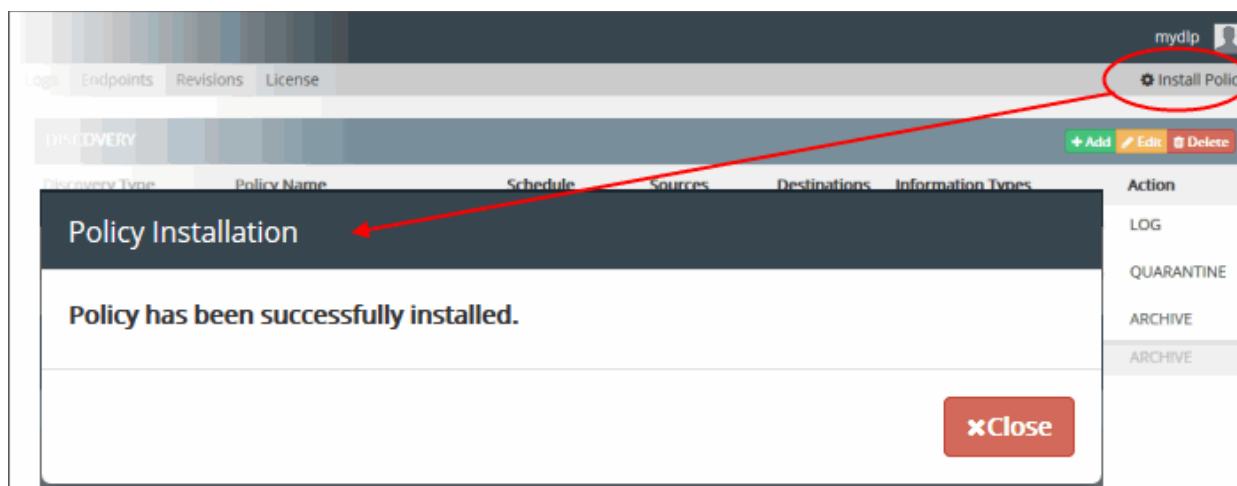
To run the scan instantly, click the play button beside it under the Schedule column.

The rules take effect only on applying/reapplying the policy to the network. See **Step 6 - Deploy the Policy** for more details.

## Step 6 – Deploy the Policy

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

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



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

After the policy is deployed, 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.

## Step 7 – View Discovery Reports and Data Transfer Event Logs

CDDP generates comprehensive reports for the discovery scans and data control event logs.

### Discovery Reports

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

The screenshot shows the Comodo DDP web interface. The top navigation bar includes 'Dashboard', 'Policy', 'Settings', 'Logs', 'Endpoints', 'Revisions', and 'License'. The 'Policy' tab is selected. The left sidebar has a 'POLICY' section with 'Discovery Reports' highlighted. The main content area is titled 'DISCOVERY REPORTS' and shows a table of reports. The table has columns for Status, Policy Name, Start, Finish, Duration, File Count, and Details. The reports listed are:

Status	Policy Name	Start	Finish	Duration	File Count	Details
finished	Docs with CC numbers in Bobs PC	06.10.2016, 00:00:10	06.10.2016, 00:00:20	10 S	0	[Details]
finished	Docs with CC numbers in Bobs PC	05.10.2016, 16:26:40	05.10.2016, 16:26:50	10 S	0	[Details]
finished	Docs with CC numbers in Bobs PC	04.10.2016, 11:04:50	04.10.2016, 11:09:20	4 M 30 S	0	[Details]
finished	Docs with CC numbers in Bobs PC	04.10.2016, 00:00:10	04.10.2016, 00:00:20	10 S	0	[Details]
finished	discovery 81	26.09.2016, 13:32:01	26.09.2016, 13:33:01	60 S	0	[Details]
finished	discovery 81	21.09.2016, 16:39:23	21.09.2016, 16:40:24	1 M	5	[Details]
finished	cd dvd policy	10.08.2016, 11:11:17	10.08.2016, 11:11:45	28 S	2	[Details]
finished	floppy drive	10.08.2016, 11:09:25	10.08.2016, 11:12:25	3 M	2	[Details]
finished	testpendrive	10.08.2016, 10:27:25	10.08.2016, 10:28:25	60 S	2	[Details]
finished	testpendrive	10.08.2016, 10:26:07	10.08.2016, 10:26:38	31 S	2	[Details]

Showing 1 to 10 of 25 entries

Previous 1 2 3 Next

You can view detailed reports of each scan, use the filter option to search for particular reports and more. See [Viewing Discovery Scan Reports](#) for more details.

### Data Transfer Event Logs

CDDP logs all the events that was triggered by data control rules. The 'Logs' interface displays details such as rule name and type, the date of event and more.

To view the logs, click the 'Logs' tab.

COMODO DOME  
DATA PROTECTION

mydlp

Dashboard Policy Settings **Logs** Endpoints Revisions License

LOGS

Show 10 entries

Detailed Search Export to Excel Refresh Search for... Search

Date	Source	Action	Rule Type	Rule	Details
29.09.2016, 13:51:07	10.100.136.253 buraka@COMODO	Device Plugged Out	CD-DVD Rule	cd dvd policy	
29.09.2016, 13:50:50	10.100.136.253 buraka@COMODO	Device Plugged Out	CD-DVD Rule	cd dvd policy	
29.09.2016, 13:37:09	10.100.136.253 buraka@COMODO	Device Plugged In	USB Device Access	rem stor	
29.09.2016, 13:37:09	10.100.136.253 buraka@COMODO	Device Plugged In	USB Device Access	rem stor	
29.09.2016, 13:37:09	10.100.136.253 buraka@COMODO	Device Plugged In	USB Device Access	rem stor	
29.09.2016, 13:37:07	10.100.136.253 buraka@COMODO	Device Plugged Out	USB Device Access	rem stor	
29.09.2016, 13:37:07	10.100.136.253 buraka@COMODO	Device Plugged Out	USB Device Access	rem stor	
29.09.2016, 13:37:07	10.100.136.253 buraka@COMODO	Device Plugged Out	USB Device Access	rem stor	
29.09.2016, 13:36:42	10.100.136.253 buraka@COMODO	Device Plugged In	USB Device Access	rem stor	
29.09.2016, 13:36:42	10.100.136.253 buraka@COMODO	Device Plugged In	USB Device Access	rem stor	

Showing 1 to 10 of 288 entries

Previous 1 2 3 4 5 ... 29 Next

© 2016 Comodo Group.

You can filter the logs based on a rule, date, source and action. The log details dialog provides comprehensive information such as the IP, user, name of the computer from where the event occurred and more. See **'The Logs Tab'** for more details.

See the admin guide at <https://help.comodo.com/topic-283-1-596-7050-Introduction-to-Comodo-CDDP.html> for detailed tutorial.

## 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)