COMODO

Creating Trust Online®

Comodo MyDLP

Software Version 3.0

Quick Start Guide

Guide Version 3.0.031716

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo MyDLP – Quick Start Guide

MyDLP 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 MyDLP and start using it.

Step 1 – Install MyDLP on Network Server

After the MyDLP 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 MyDLP on a server and configure, refer to our installation guide at https://help.comodo.com/topic-283-1-597-7016-About-MyDLP.html. For any doubts and clarifications, please contact us at mydlpsupport@comodo.com

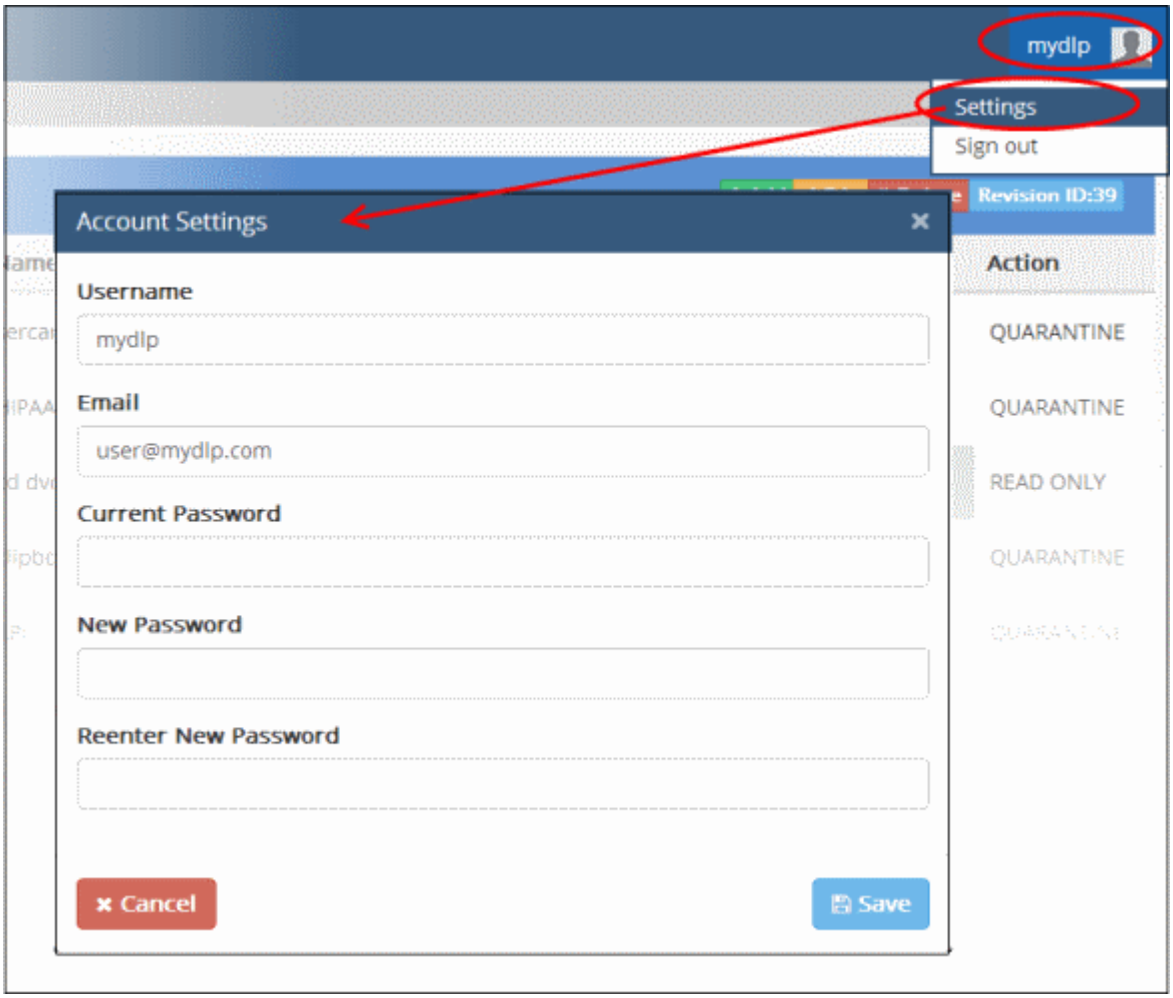
Step 2 – Login to the Management Console

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

Preliminaries:

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

- Default username is "mydlp" and default password is "mydlp" (without the quotes). Please change these to a unique username and password immediately after logging in. You can change the password by clicking on the username at the top right > Settings.

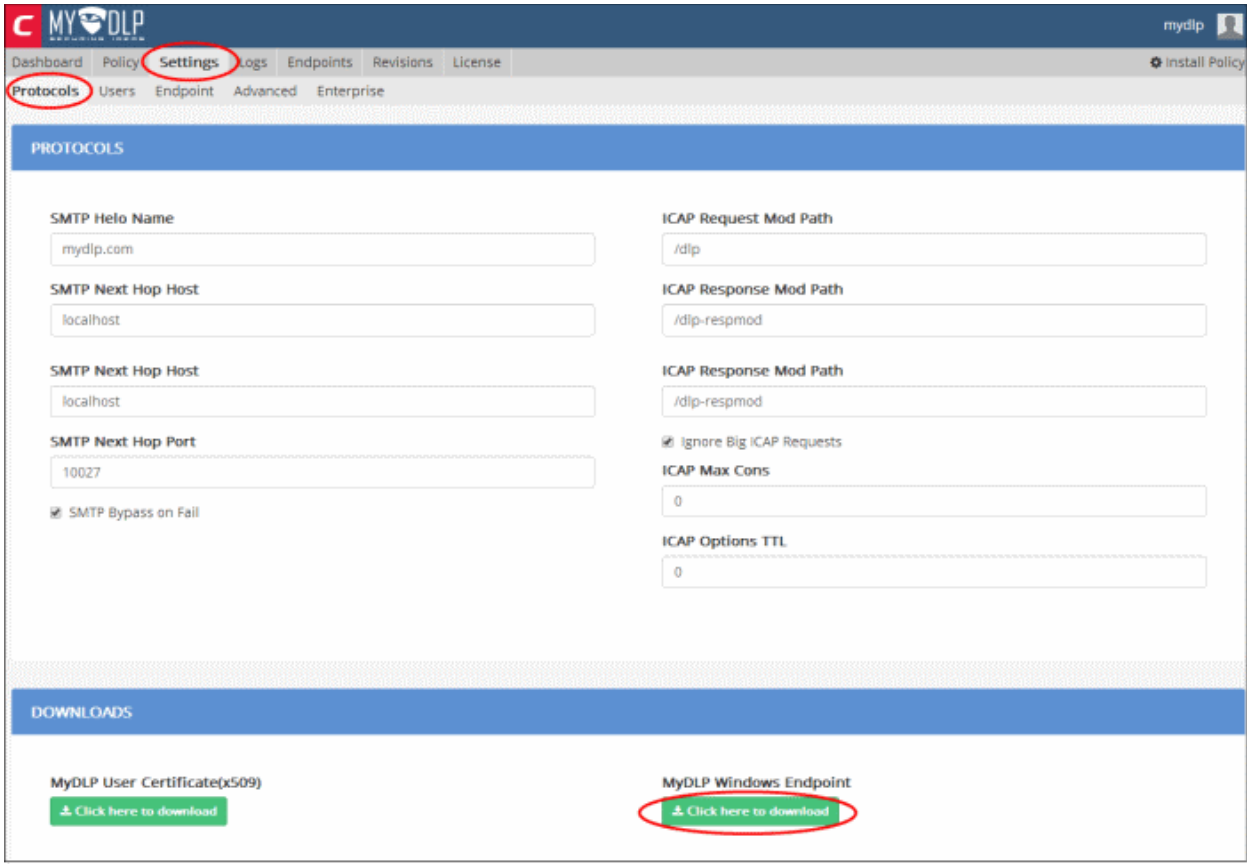


- Change the password and click 'Save'

Step 3 – Install MyDLP Agent on Network Computers

The next step is to install MyDLP 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 MyDLP agent, click 'Settings' > 'Protocols' and then 'Click here to download' button under 'MyDLP Windows Endpoint.

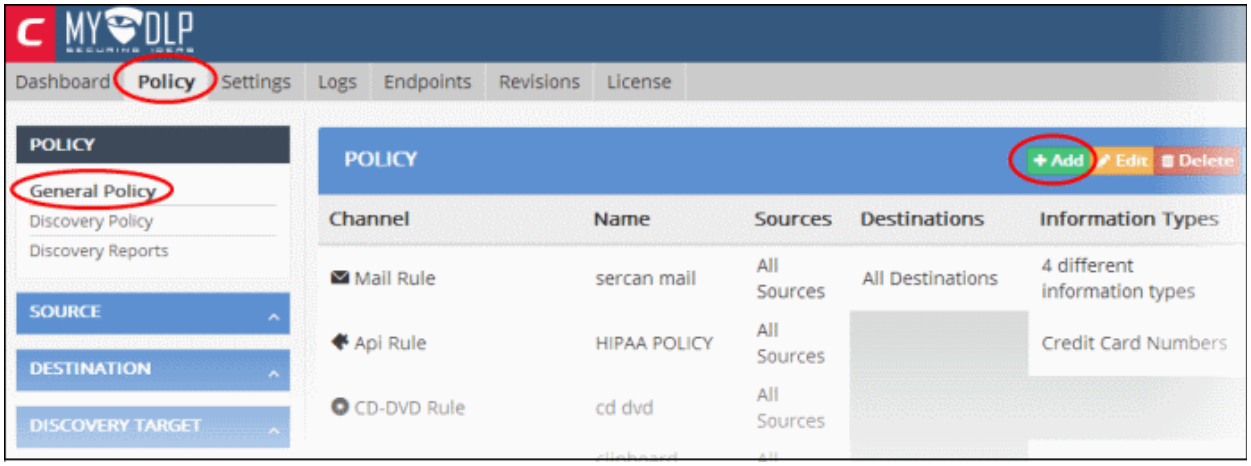


The agent will be stored in your default download location. Refer to our endpoint installation guide at https://help.comodo.com/topic-283-1-598-7034-About-MyDLP-.html for more details about installing agent on to endpoints.

Step 4 – Create Data Transfer Rules

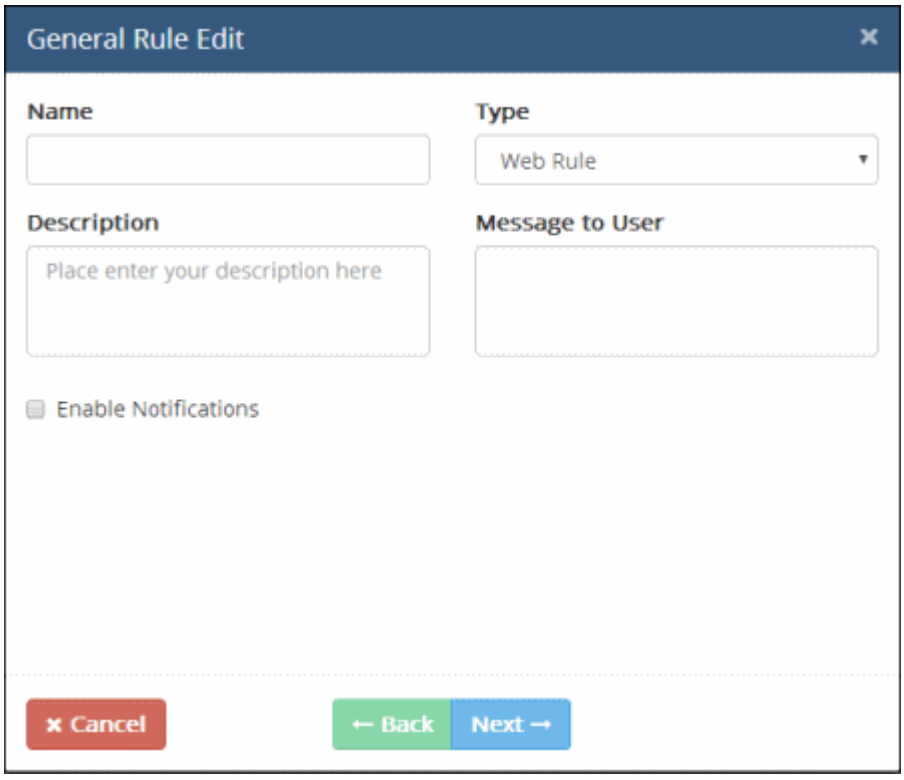
After installing MyDLP agent on to endpoints, the next step is to create a policy according to your organization's requirement. There are two types of rules, Data Transfer Rules and Data Discovery Rules, that comprise a policy. You can add any number of rules as required for a policy. This step explains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

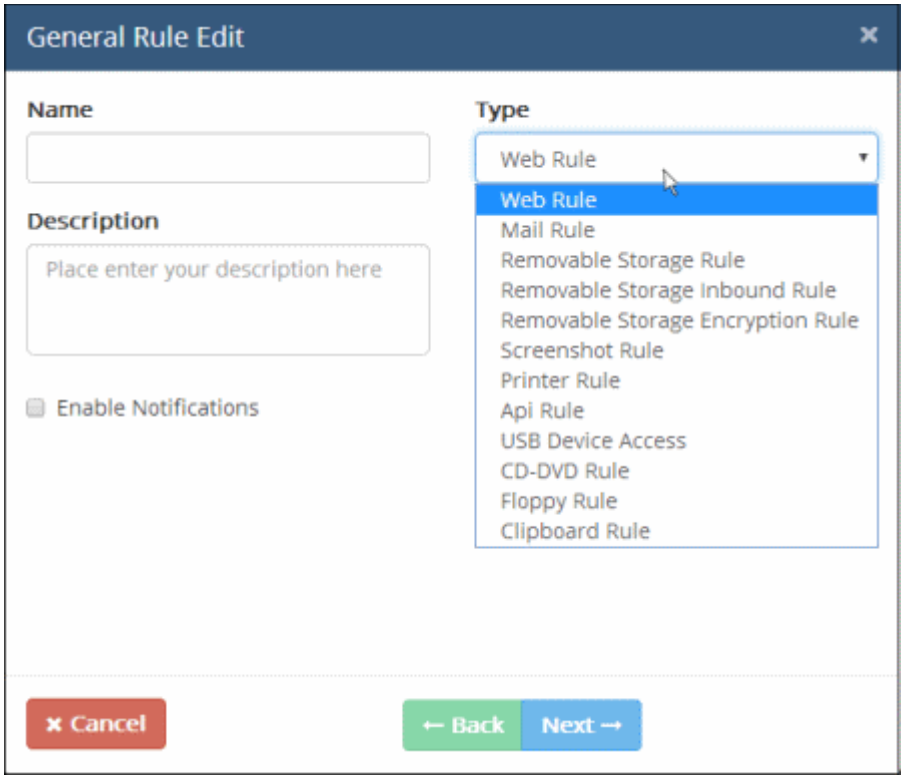


- Click the 'Add' button.

The rule creation wizard will start.



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



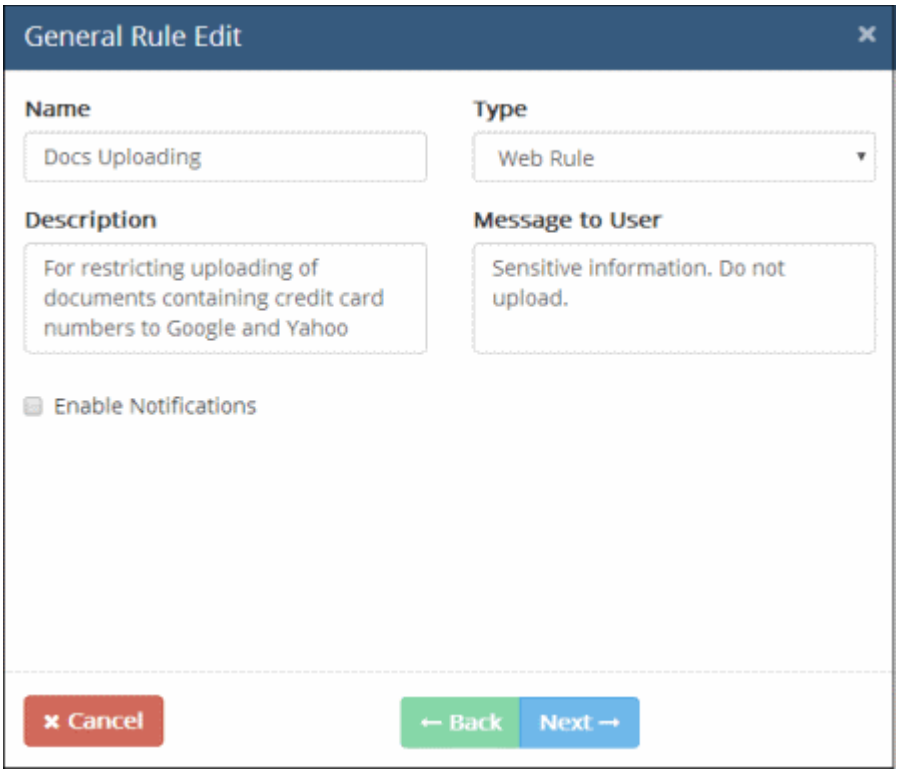
There are 12 types of data transfer control rules that can be configured in MyDLP.

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

the section Mail rule for more details.

- Removable Storage rules control data transferred to external devices such as USB memory sticks, removable hard drives and smart phones. See the section Removable Storage rule for more details.
- Removable Storage Inbound rules are used to archive data copied from removable memory devices on to the computer. See the section Removable Storage Inbound rule for more details.
- Removable Storage Encryption rules allow you to encrypt removable devices connected to endpoints on your network. After encryption, any data on the drive can only be read if it is connected to your network and not by any other network. If you enable this rule for all sources then any new devices will be immediately encrypted as soon as they are connected. This would prevent, for example, any guest or hostile from plugging in a USB drive, downloading data and taking it out of your network. See the section Removable Storage Encryption rule for more details.
- Screenshot rules prevent print screen function while a sensitive application is running. See the section Screenshot rule for more details.
- Printer rules allow you to prevent documents matching specific criteria from being printed. See the section Printer rule for more details.
- API rules are a unique feature which allow you to integrate custom applications with MyDLP. See the section API rule for more details.
- USB Device Access rules are used to monitor or block use of USB memory devices on the selected computers covered by the source object defined in the rule. See the section USB Device Access Rulefor 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.

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



Enter the following information:

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

  MyDLP displays the message for the following rule types:

  - Web Rule
  - Mail Rule

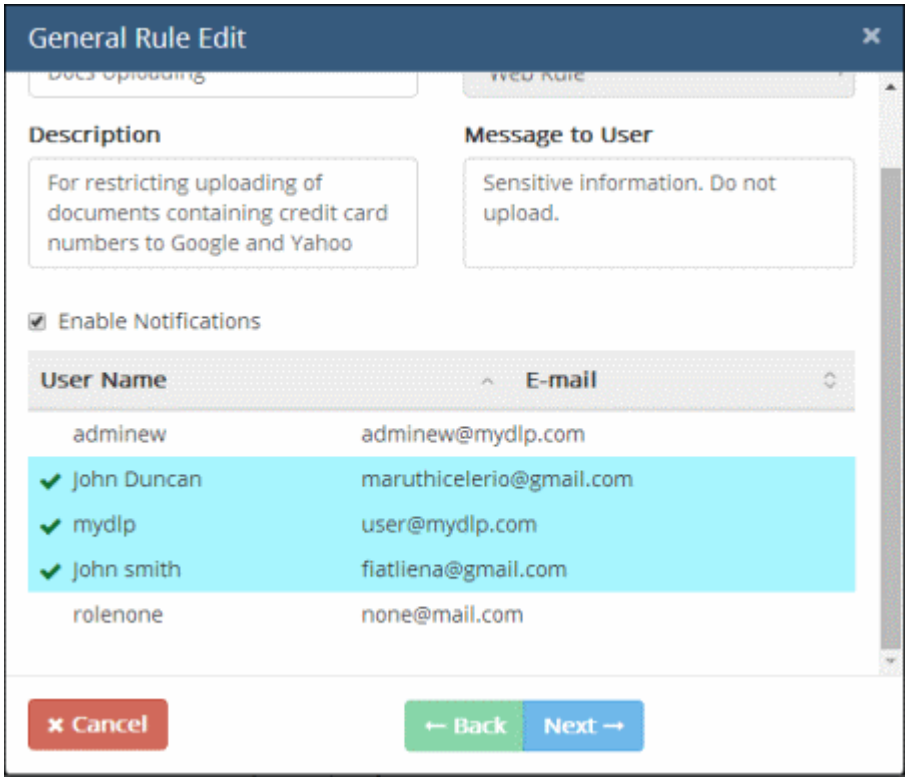
  The message will be displayed only if the action set for the rule is to block or quarantine the intercepted file.
- **Notifications** - Configure the automated notifications to be sent to the administrators and other users when MyDLP intercepts the data traffic from any end-user, based on the new rule. This step allows you to choose the notification type and the intended recipients. The notification messages sent to the recipients can be edited under 'Settings' > 'Enterprise' tab. Refer to the section **Configuring Enterprise Settings** for more details.

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

  - Web Rule
  - Mail Rule

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

The administrators and users lists will be displayed below:

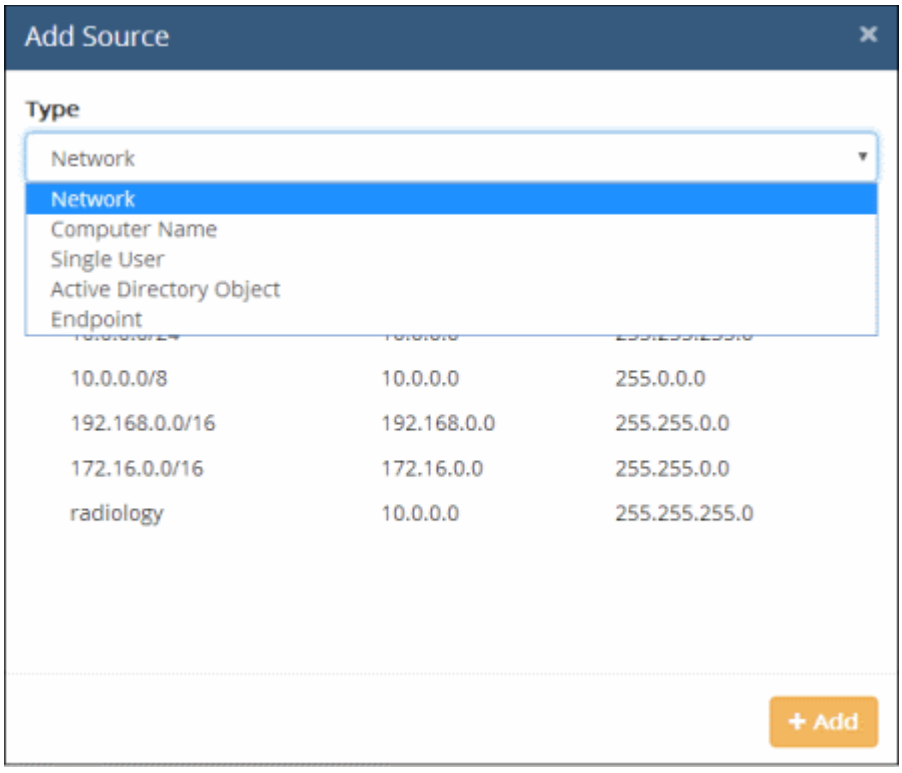


  - Select the administrators and other users that have access to the MyDLP interface, to whom the notifications are to be sent
- Click 'Next'.

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.



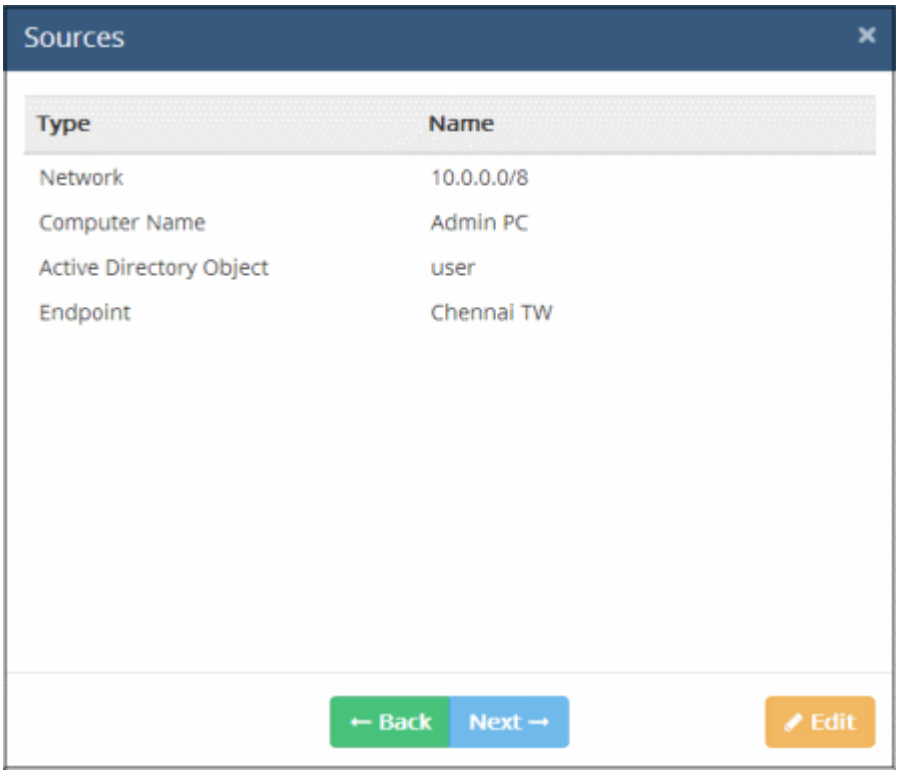
The 'Network' object type has 'All Sources' built-in object and will be available for all rule types. 'All Sources' object when added to a rule as a source type means that all objects in the network, will be scanned for the defined information type. To make the source type more specific to enforce a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

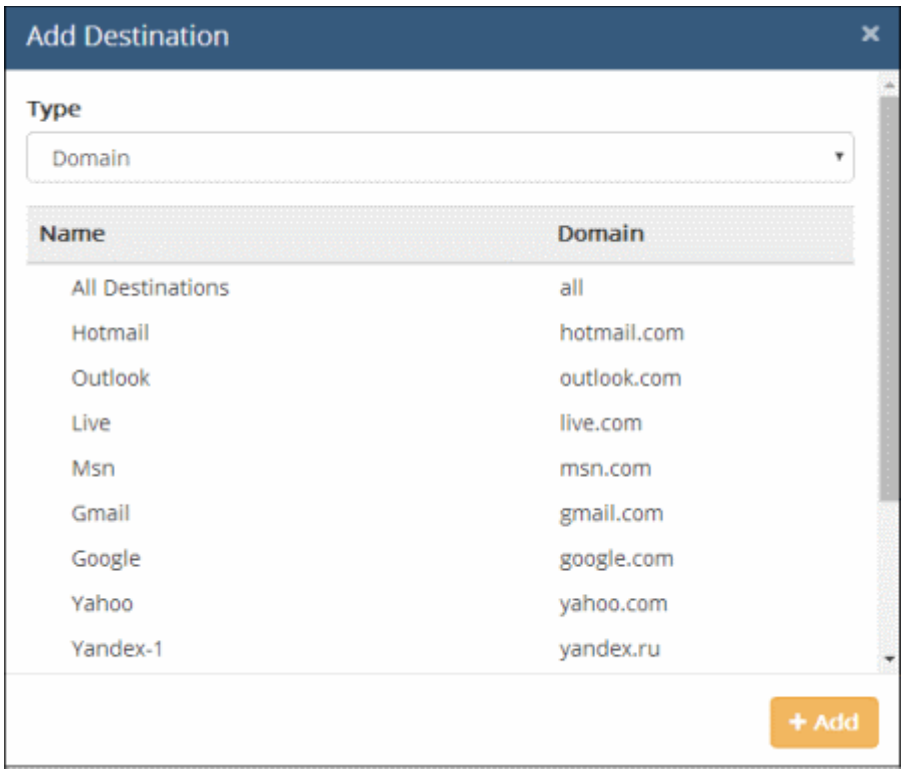


- Click 'Next' to proceed to add destinations

The 'Destinations' dialog will be displayed:

- Click the 'Edit' button

The 'Add Destination' dialog will be displayed.



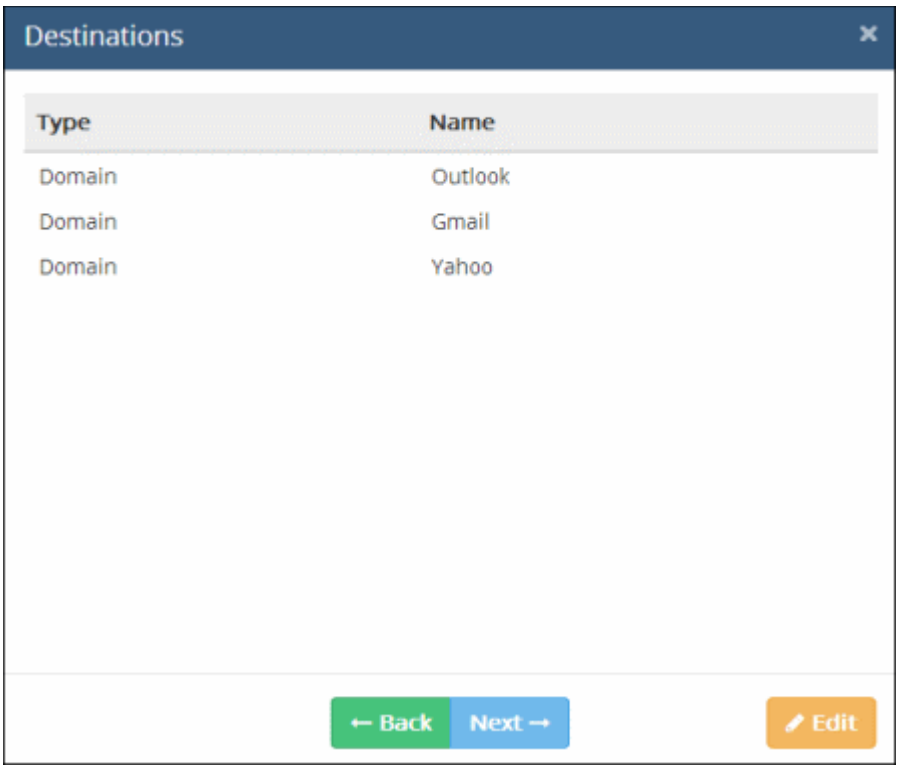
The target of the data transfer can be added as the 'Destination' component of the rule, by selecting the destination object type from the 'Type' drop-down. The following table shows the object types that can be used for defining Destinations and applicable rule types.

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

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

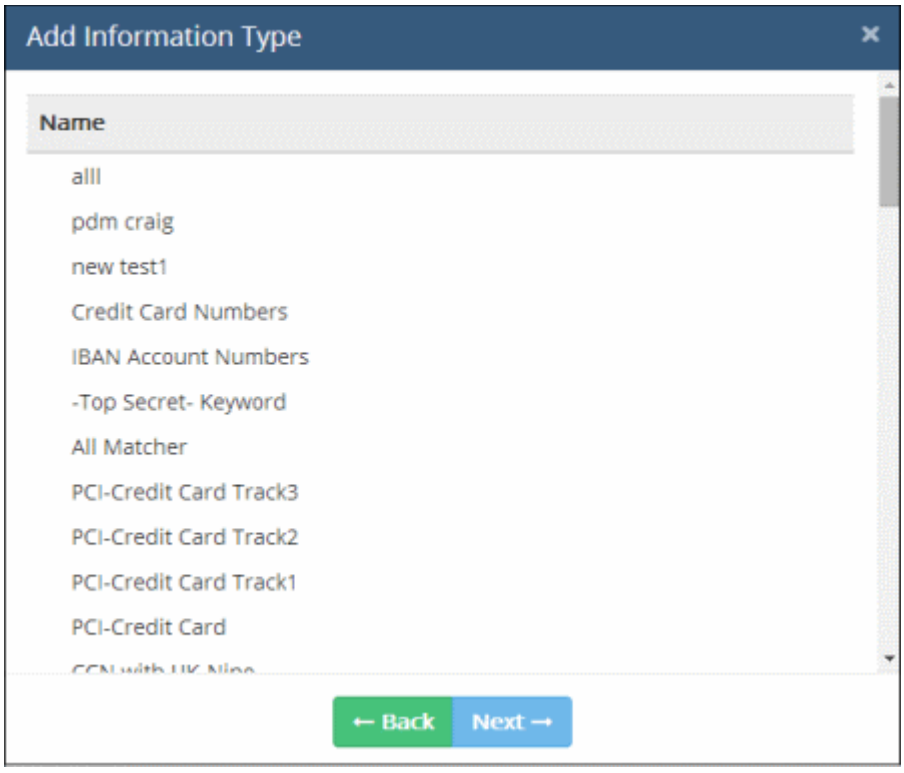
- Select the object(s) from the list
- To add more destinations for other object types, select another object type from the 'Type' drop-down again and follow the same procedure explained above.

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



- Click 'Next' to proceed to add information type that must be checked by MyDLP for the rule

The 'Add Information Type' dialog will be displayed.



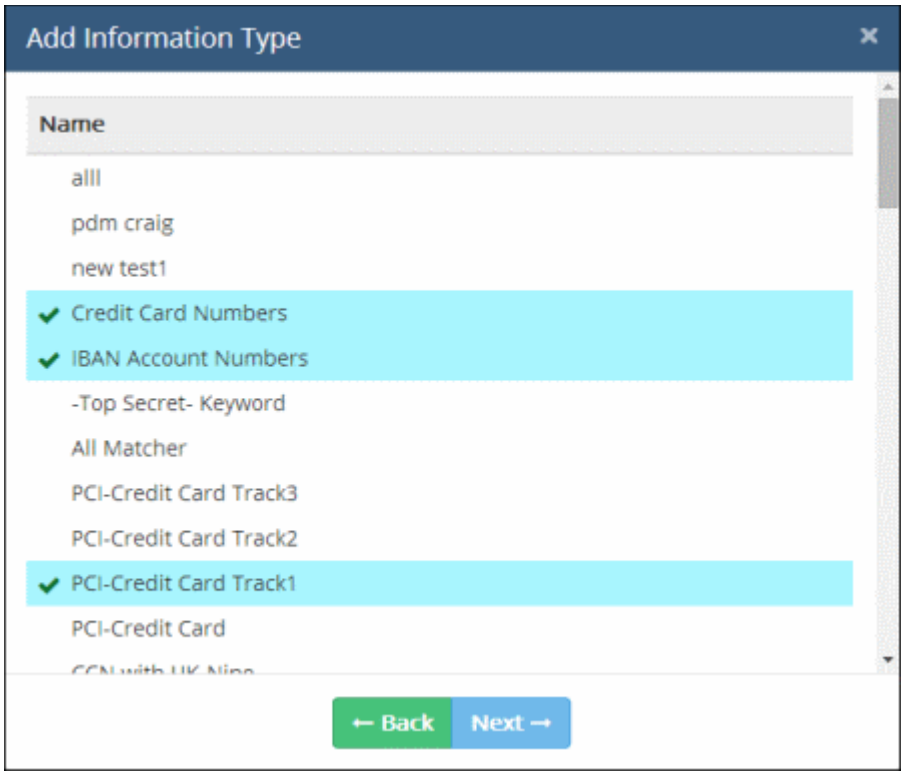
The objects listed for the selected object type depends on the predefined and user defined objects defined for it.

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

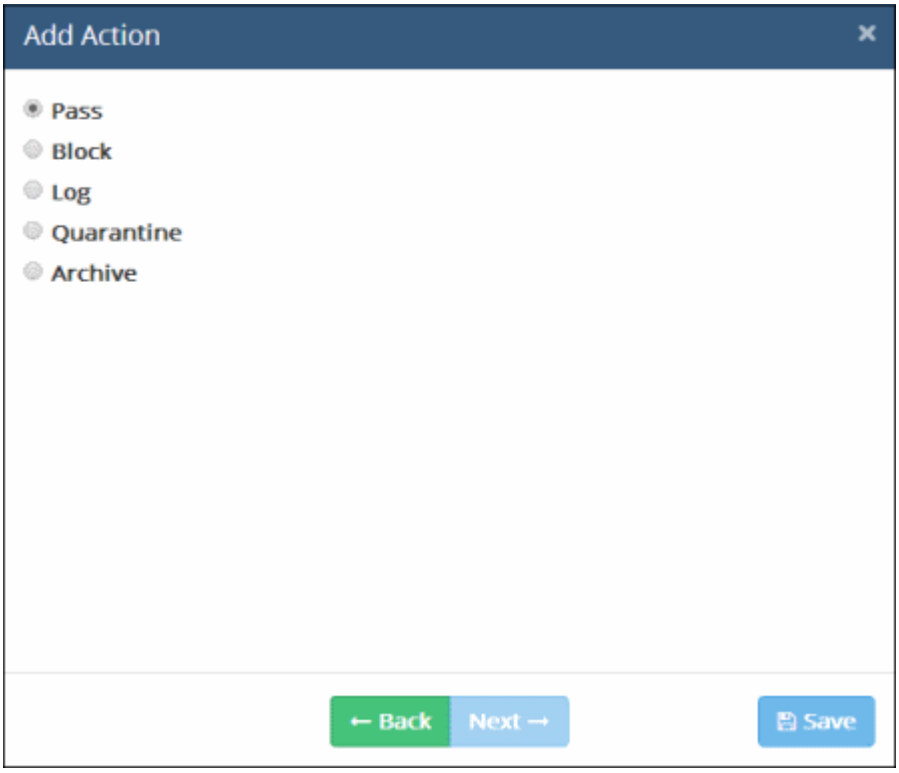
For MyDLP to intercept files containing sensitive data of specific type, the respective information type object is to be added to the rule. The following table shows the object types that can be used for defining Information Types and applicable rule types.

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

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

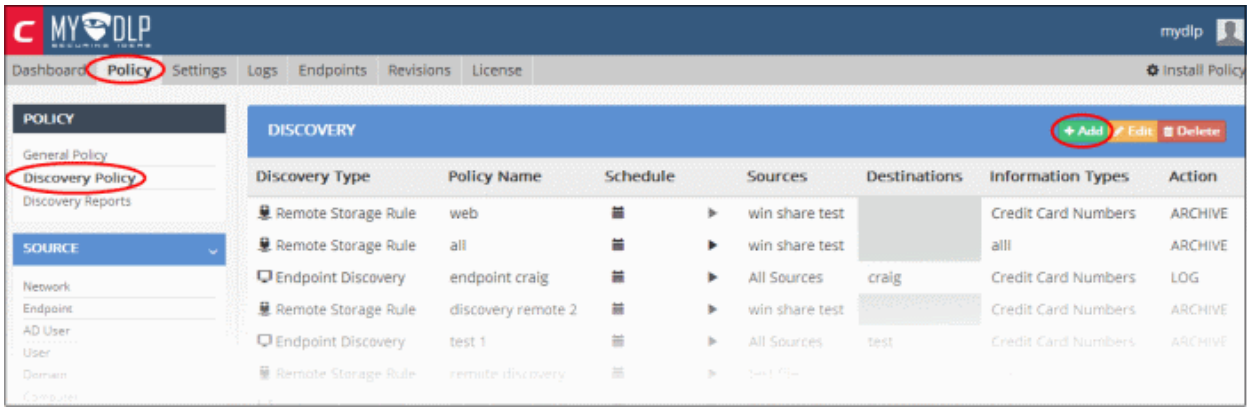
The rule will be saved. You can create as many rules as required. If you are creating a new rule with minor changes from an existing rule, you can clone the rule and edit it to change the required parameters.

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

Step 5 – Create Data Discovery Rules

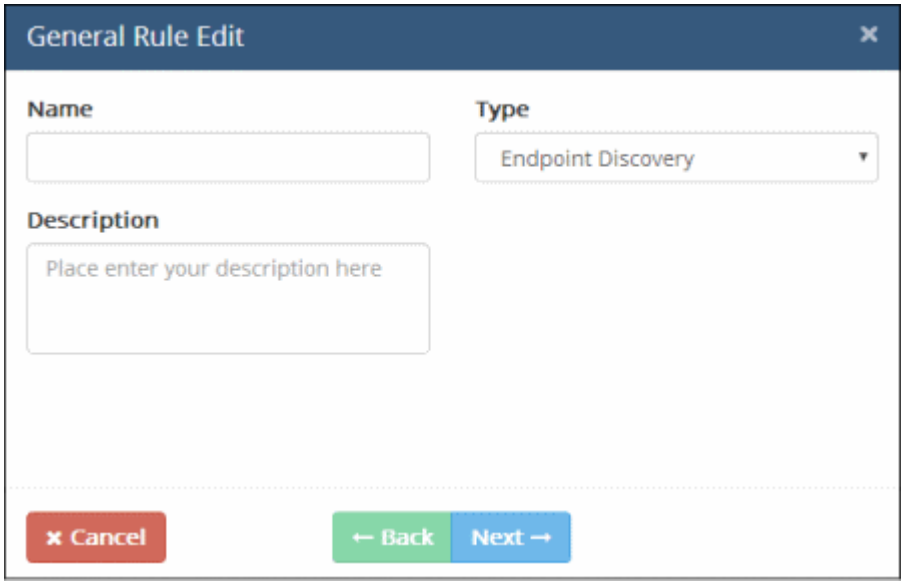
The next step is to create data discovery rules to identify files containing sensitive information. The targets, schedule, information searched for, and the action to be taken is specified in a Discovery Rule.

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

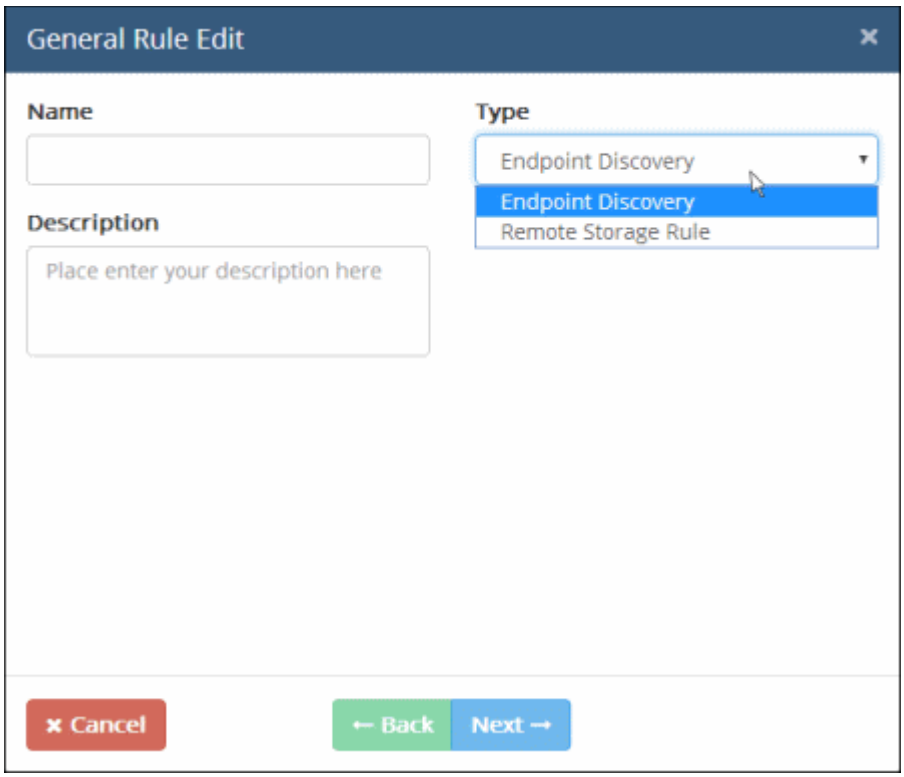


- Click the 'Add' button.

The discovery rule creation wizard will start.



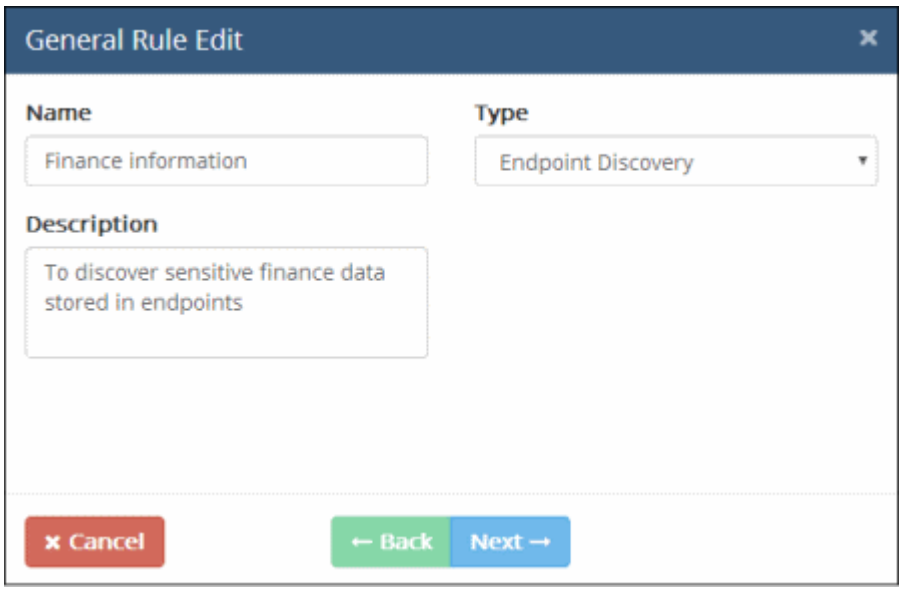
- Select the type of the rule to be created from the 'Type' drop-down.



There are two types of data discovery rules that can be configured in MyDLP.

- 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.

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

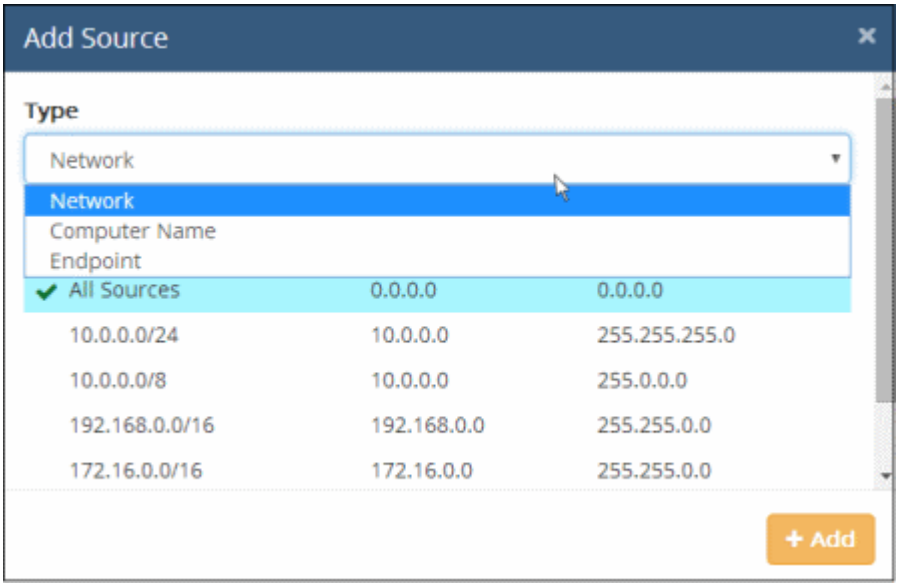


- Enter a name, shortly describing the new rule and description in the respective fields
- Click 'Next'

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	• Endpoint Discovery rule
Computer Name	• Endpoint Discovery rule
Endpoint	• Endpoint Discovery rule
Remote Storage	• Remote Storage rule

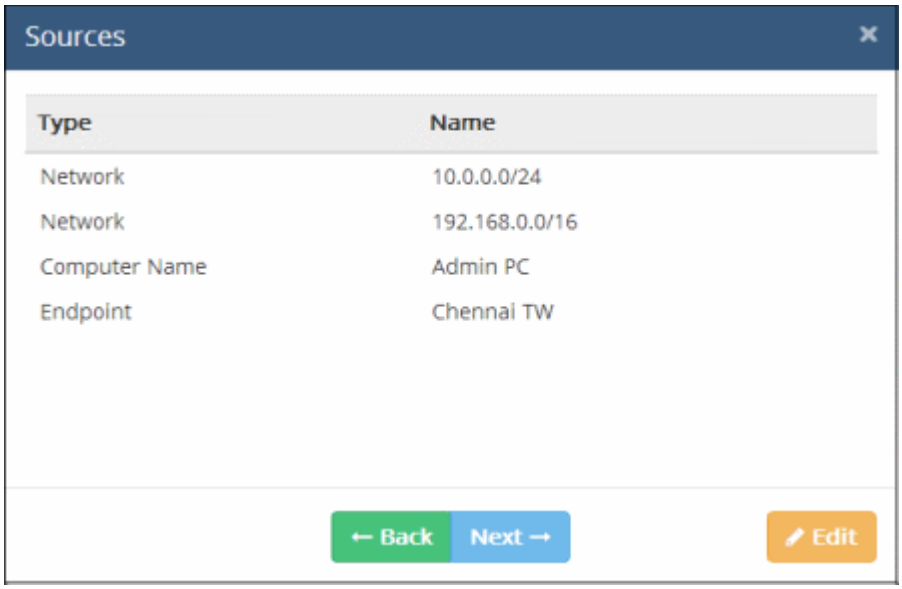
The 'Network' object type has 'All Sources' built-in object and will be available for discovery rule. 'All Sources' object when added to a rule as a source type means that all objects in the network, will be scanned for the defined information type. To make the source type more specific to enforce a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

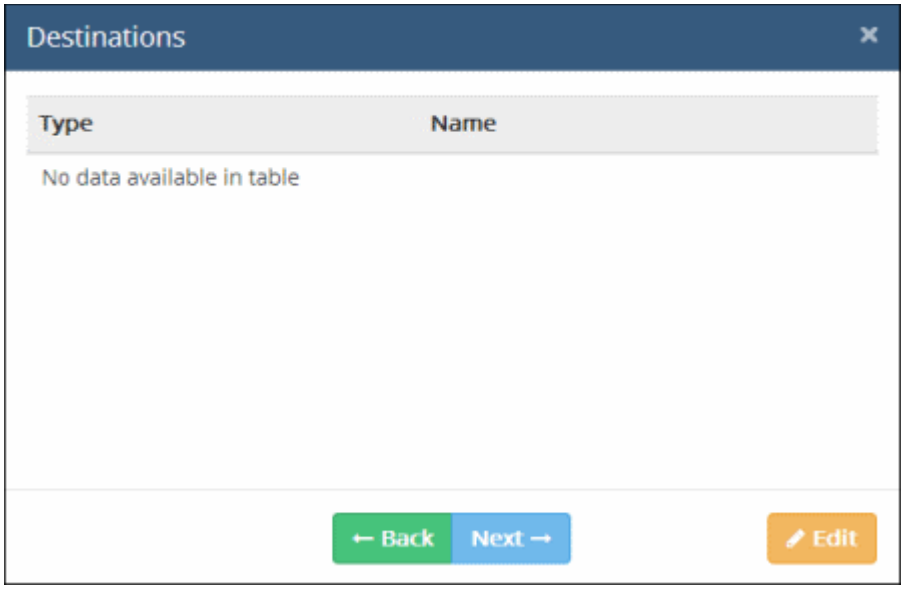
- Select the object(s) from the list
- To add more sources for other object types, select another object type from the 'Type' drop-down again and follow the same procedure explained above. Please note for remote discovery rule, only remote storage object will be available.

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



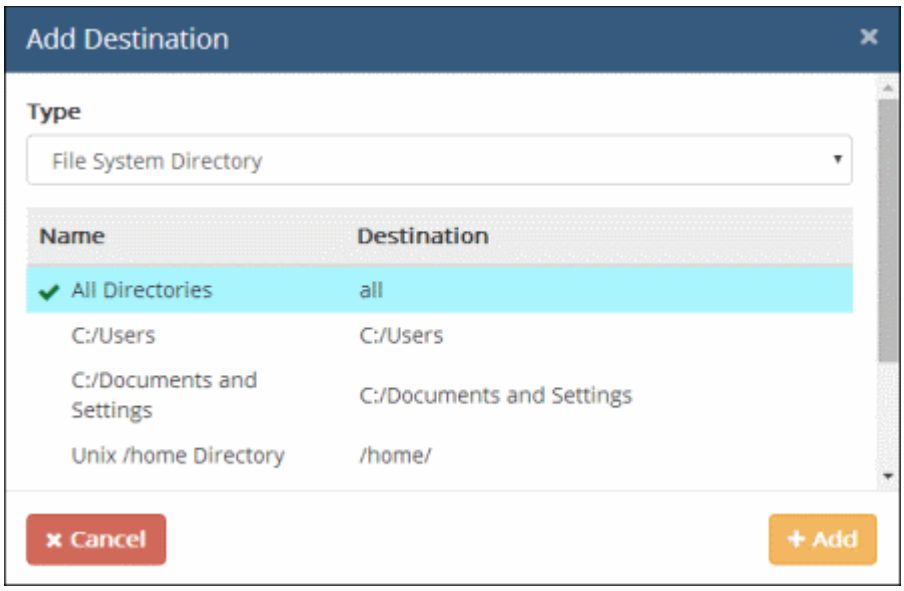
- Click 'Next' to proceed to add destinations

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



- Click the 'Edit' button

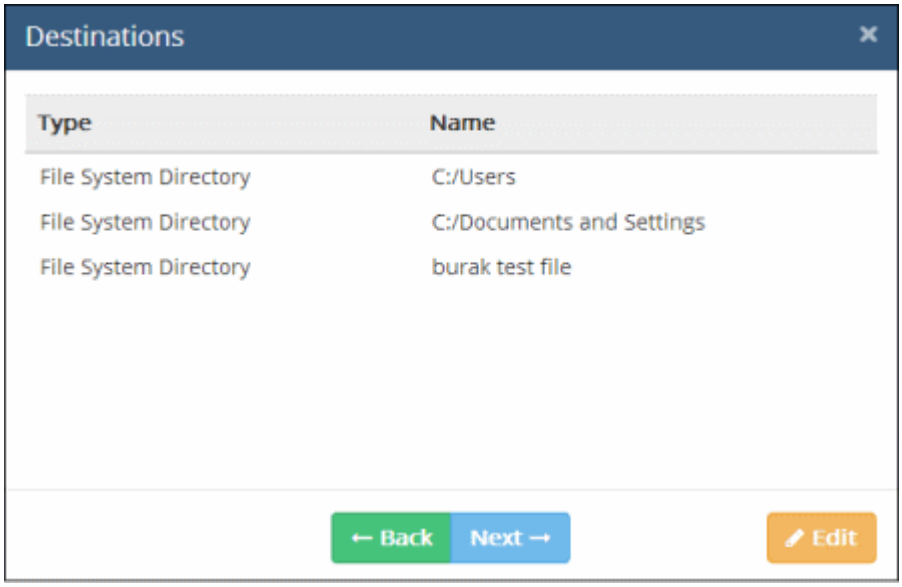
The 'Add Destination' dialog will be displayed.



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

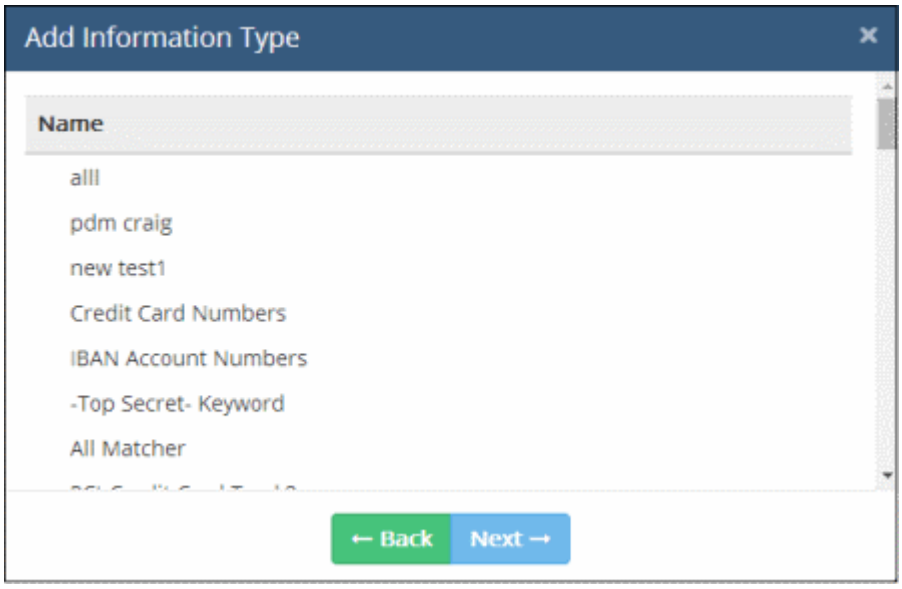
- Select an object(s) from the list

All the destinations added will be listed.



- Click 'Next' to proceed to add information type that must be checked by MyDLP for the rule

The 'Add Information Type' dialog will be displayed.

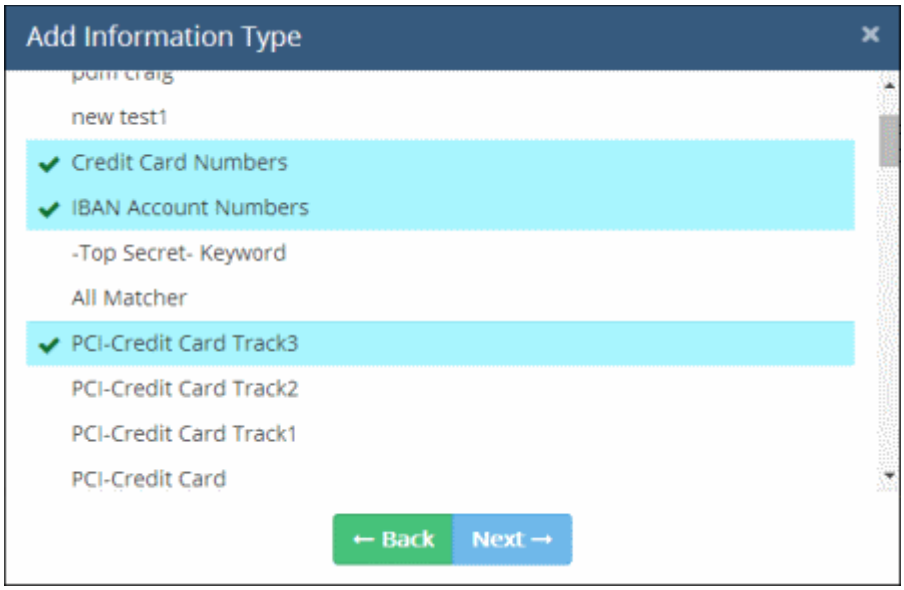


The objects listed for the selected object type depends on the predefined and user defined objects defined for it.

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

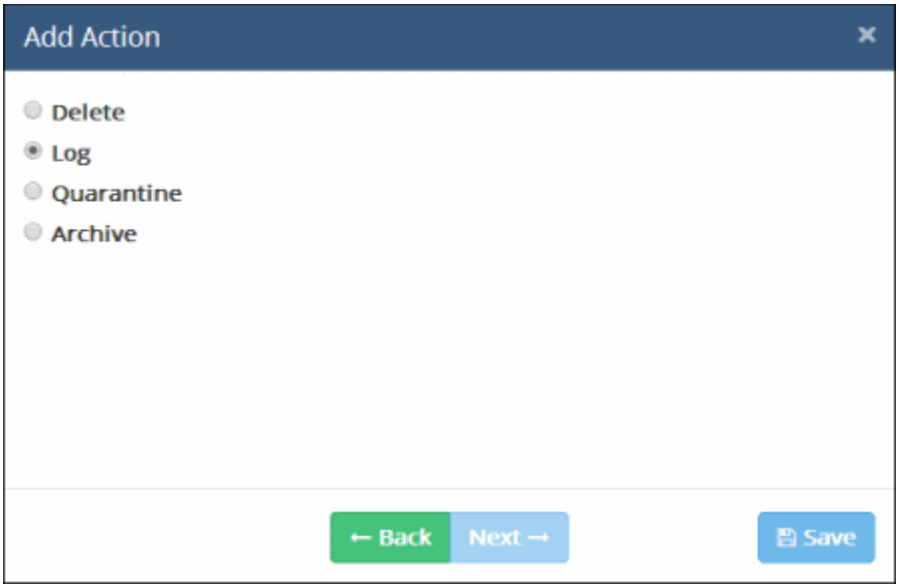
For MyDLP to discover files containing sensitive data of specific type, the respective information type object is to be added to the rule. The following table shows the object types that can be used for defining Information Types and applicable rule types.

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

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

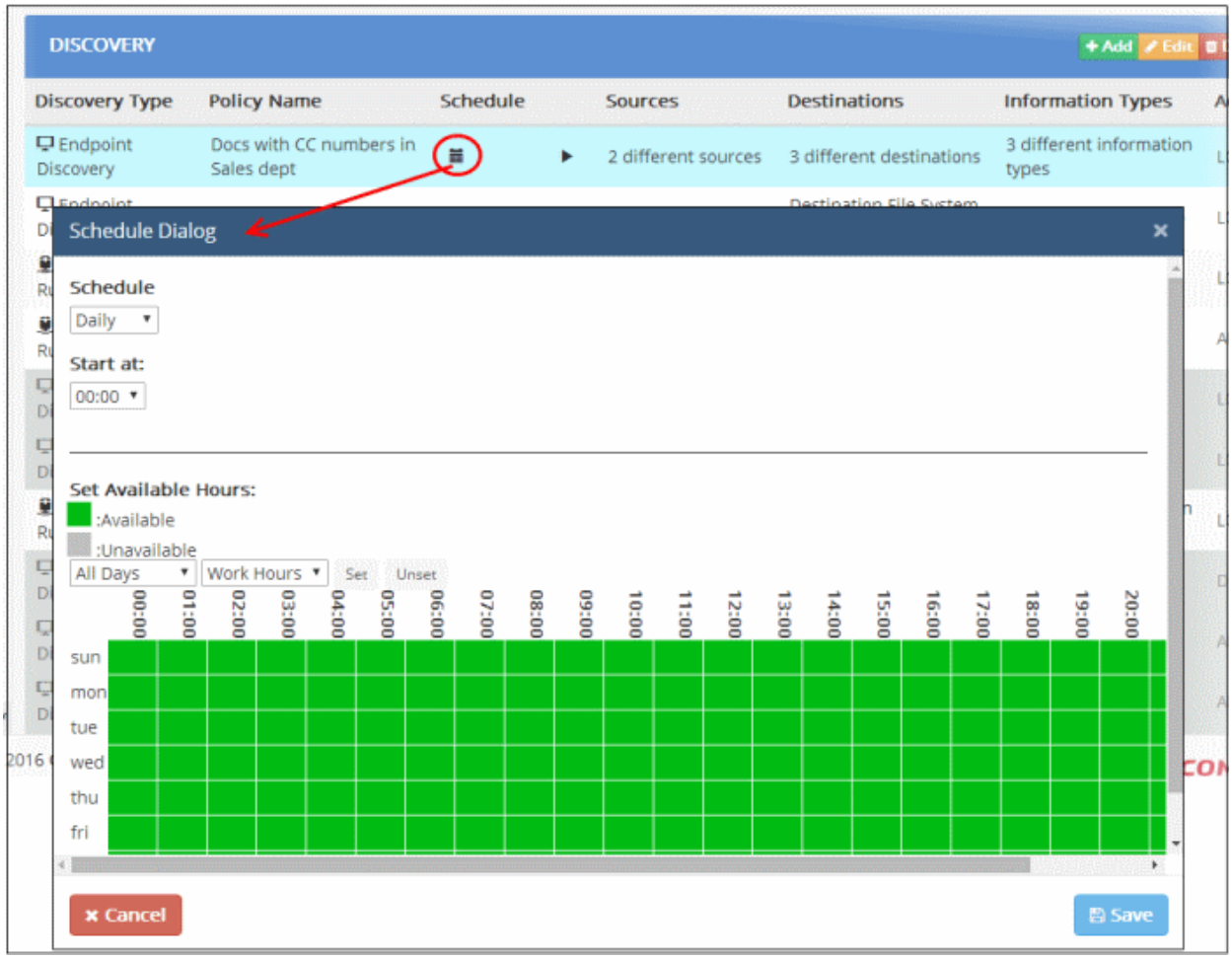
- At any time during the rule creation, click 'Back' to review your configuration for the rule
- Click 'Save'

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

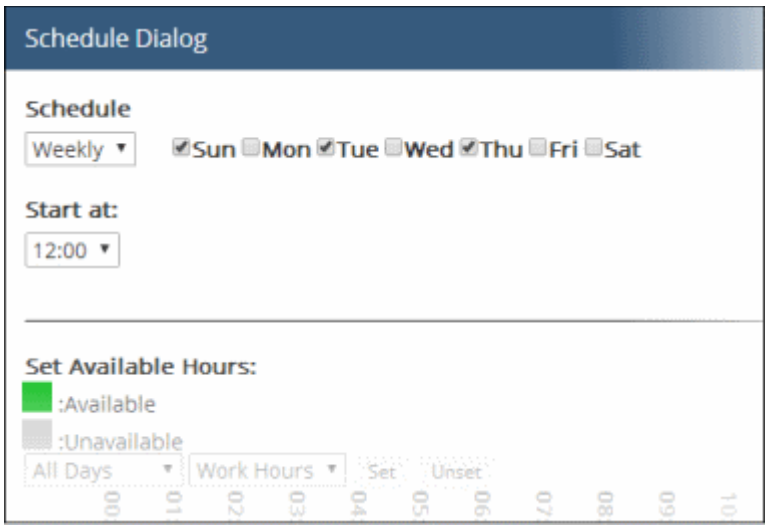
- Click 'Policy', then 'Discovery Policy' on the left under 'Policy' section
- Click the Calendar button beside the rule under the Schedule column.



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 MyDLP scans, so that the scans

scheduled at the periods at which the endpoints and the repositories are not available, will be skipped.

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

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

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

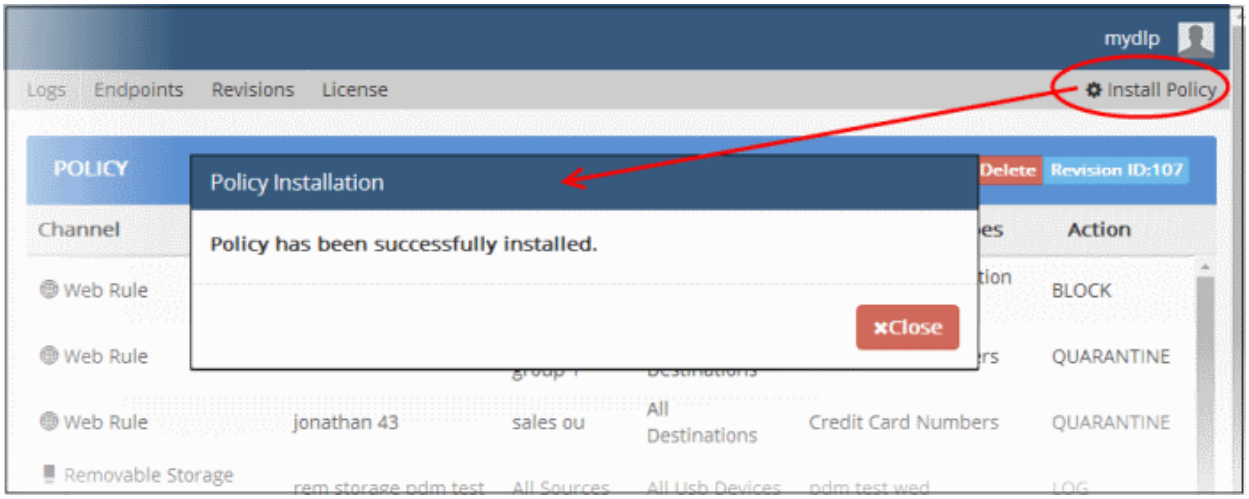
To run the scan instantly, click the play button beside it under the Schedule column.

The rules take effect only on applying/reapplying the policy to the network. Refer to **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.

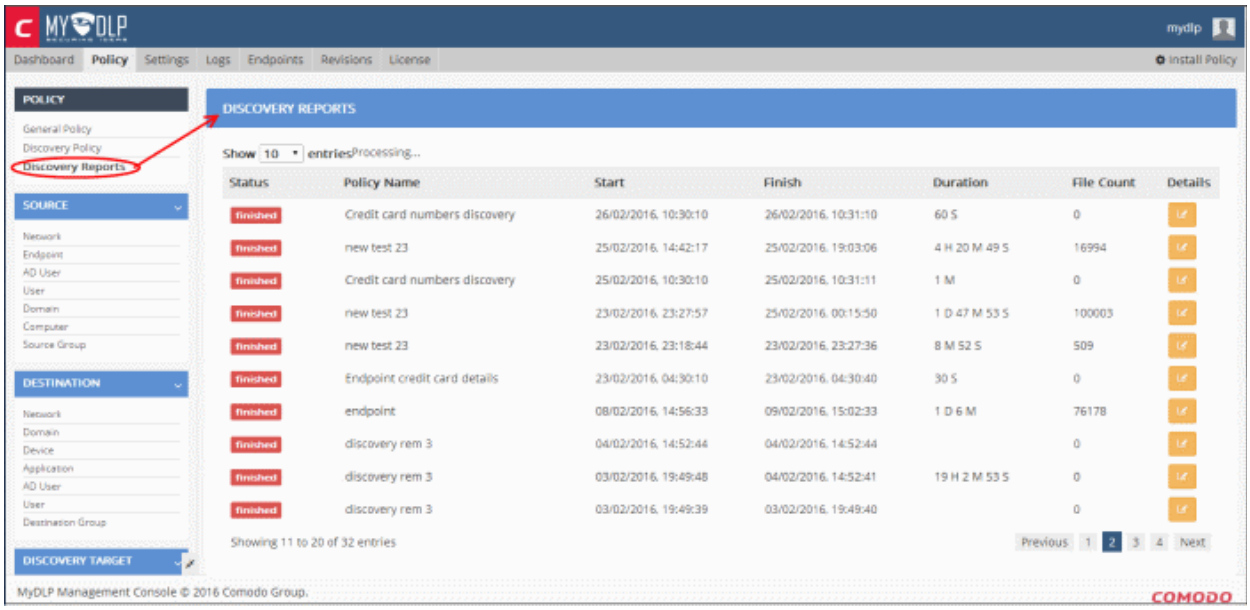
After the policy is deployed, MyDLP assigns a revision ID no. for the policy in order to track which policy is enforced at endpoints. Refer to the section '**The Revisions Tab**' for more details.

Step 7 – View Discovery Reports and Data Transfer Event Logs

MyDLP 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'.

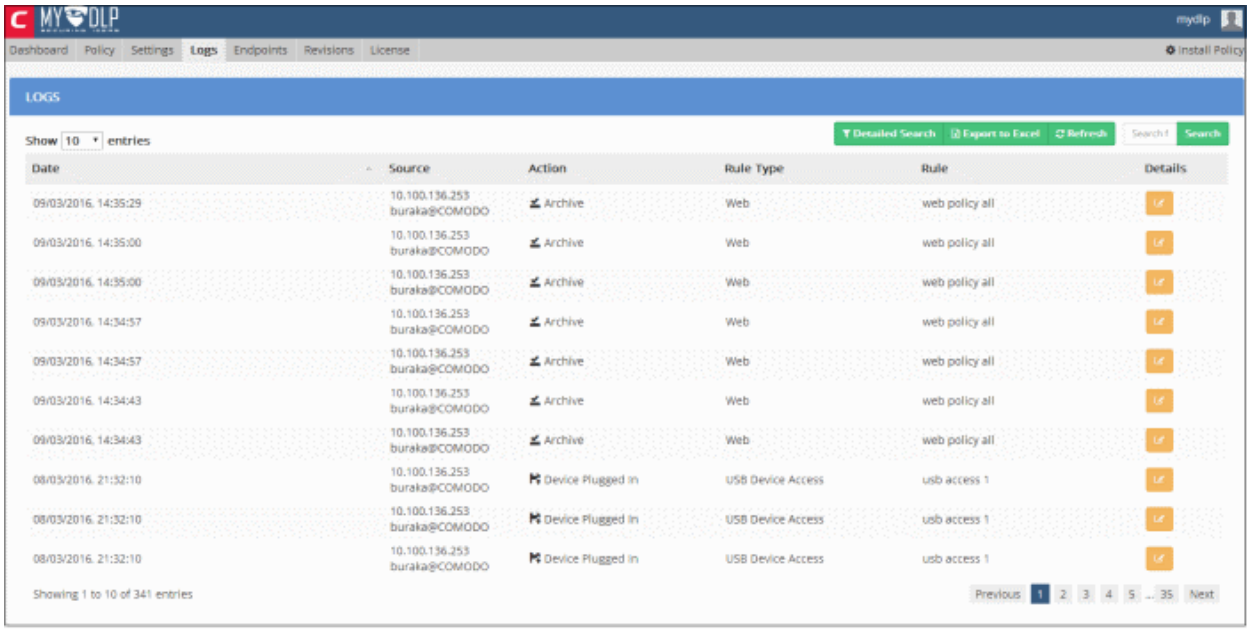


You can view detailed reports of each scan, use the filter option to search for particular reports and more. Refer to the section **Viewing Discovery Scan Reports** for more details.

Data Transfer Event Logs

MyDLP 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



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 even occurred and more. Refer to the section '**The Logs Tab**' for more details.

Refer to our admin guide at **https://help.comodo.com/topic-283-1-596-7050-Introduction-to-Comodo-MyDLP.html** for detailed tutorial.

About Comodo

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

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

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: EnterpriseSolutions@Comodo.com

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