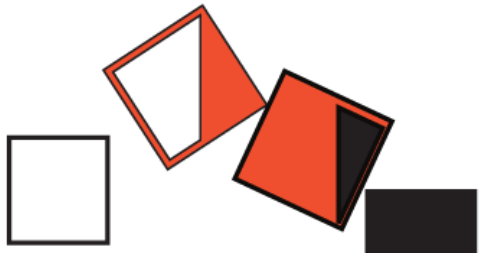


Mail-i™

Mail-i Trial Demo Guide

Contents

I. Setting before using Mail-i Trial Demo 3

II. Test Scenario 7

1. Case 1: Prevent Gmail 8
2. Case 2: Tag Logs 13

III. DLP+ Center 24

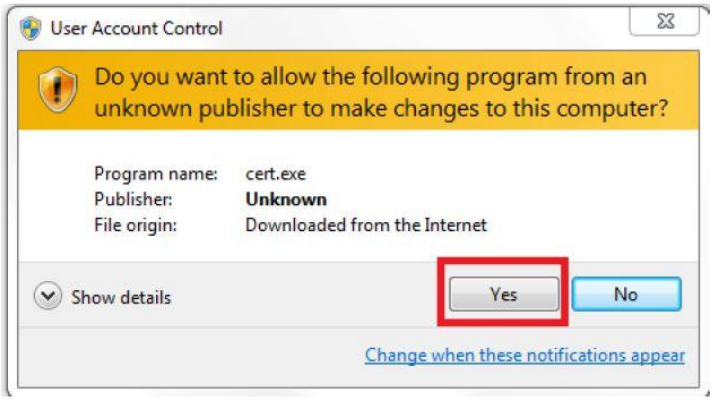
1. Log-in 24
2. Manage 25
3. Policies 26
4. Incidents 33
5. Reports 35
6. Dashboard 36

I. Setting before using Mail-i Trial Demo

- Install the given certificate file

[1]

[2]



I. Setting before using Mail-i Trial Demo

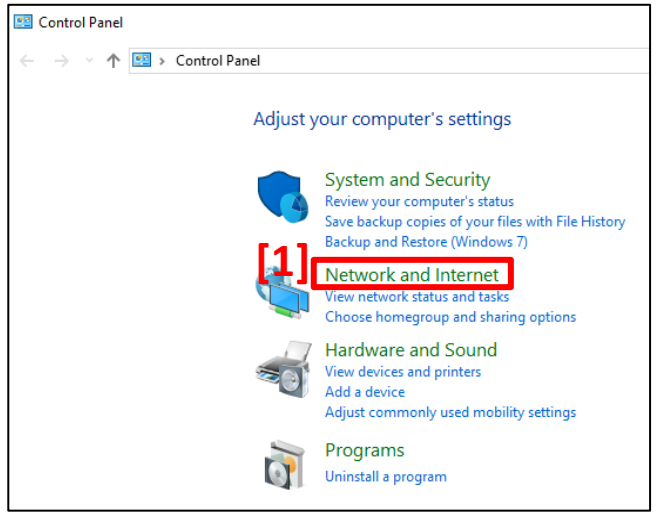
- Proxy Setting

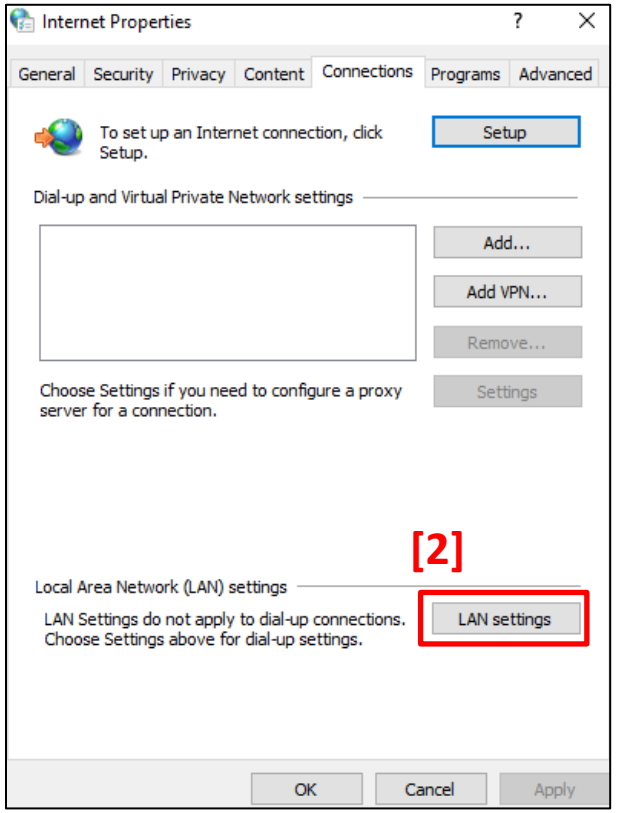
1) **Control Panel > Network and Internet > Internet Options**
2) [Tab] **Connections > LAN settings**
3) Check **Proxy server > Use a Proxy server for your LAN**
4) Click **Advanced**
5) Enter the information in Secure
   A. Proxy address to use: given address
   B. Port: 13128
6) Click ok

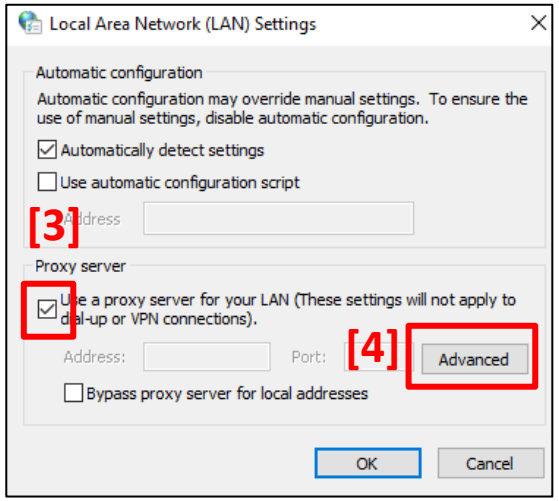
* You need proxy setting because it is based on explicit proxy.

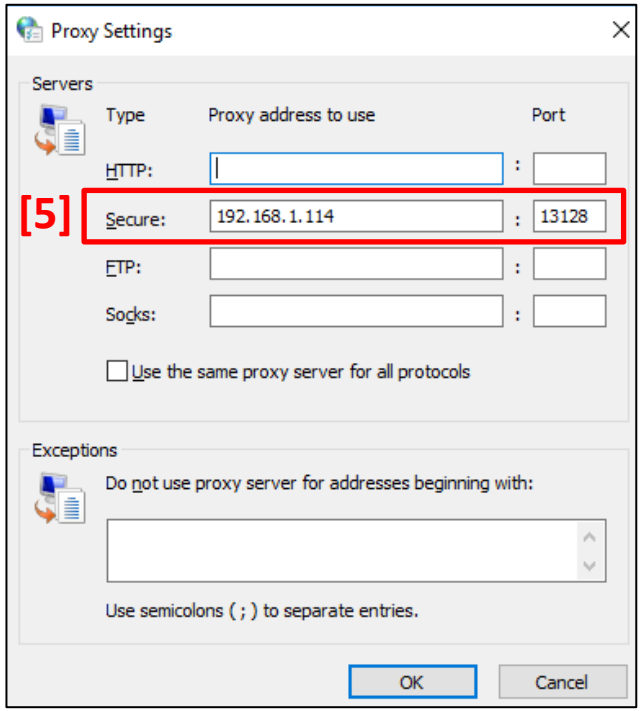
I. Setting before using Mail-i Trial Demo

- Proxy Setting









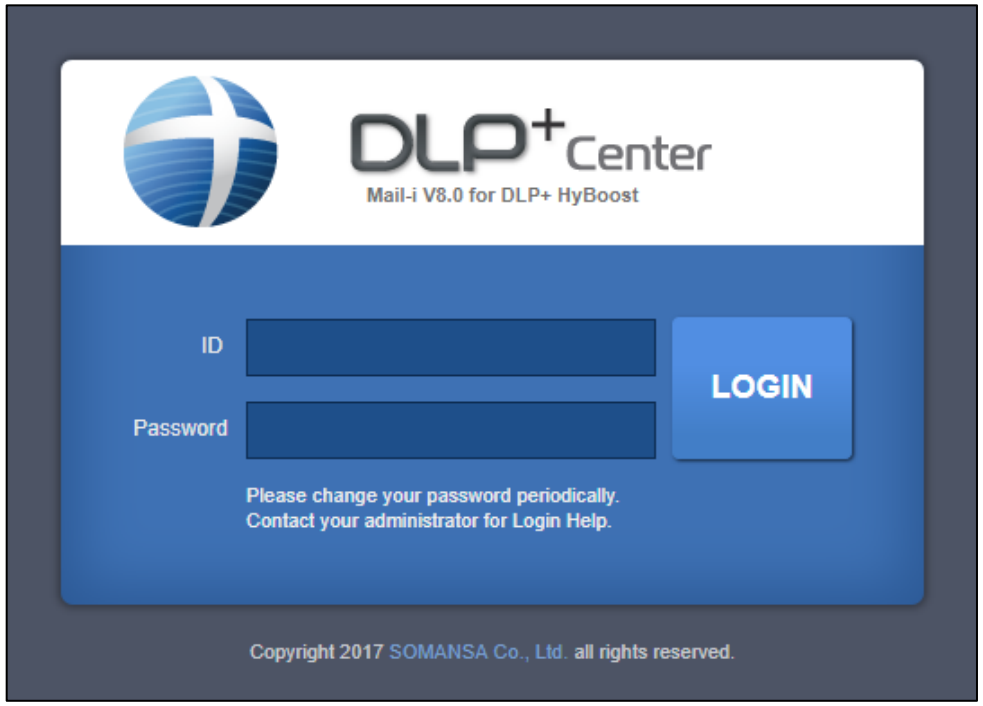
I. Setting before using Mail-i Trial Demo

- Log-in DLP+ Center

https://IP_address/DLPCenter

ID: (Given ID)

PW: (Given Password)

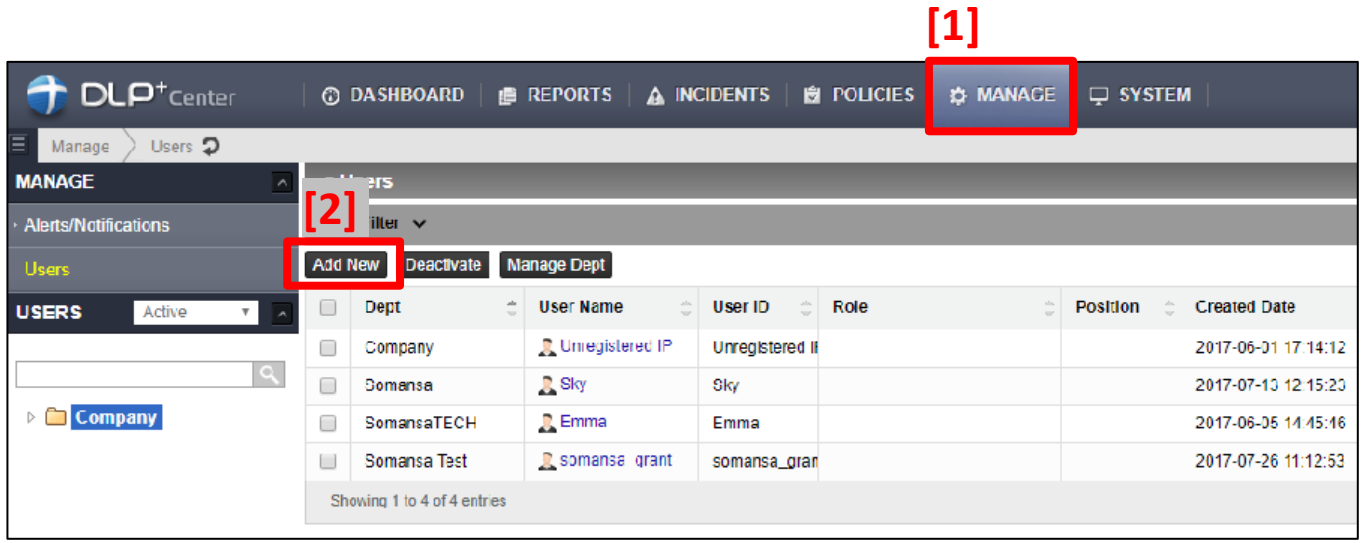


I. Setting before using Mail-i Trial Demo

- Add the Users

1) Select **MANAGE > Users**
2) Click **Add New**
3) Put **User Name, User ID**

   (It is available for the same User Name, but duplicate User ID is not allowed. User ID must be unique.)
4) Check **Use Static IP** for testing.
5) Click **Save**



* You can deactivate the user, but cannot delete the user.

II. Test Scenario

- **Case 1:** Prevent Email if there are credit card numbers more than five.
- **Case 2:** Tag Log if there is a word like ‘security’

There are 2 types of Policy Type (Control / Prevent).

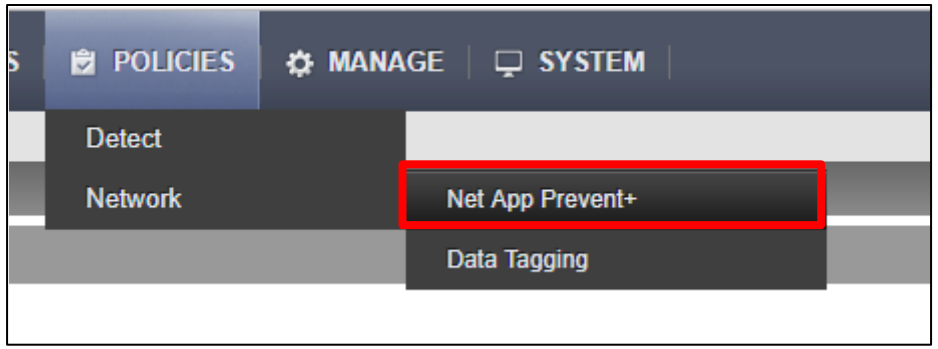
- Control type is block the specified app regardless of contents.

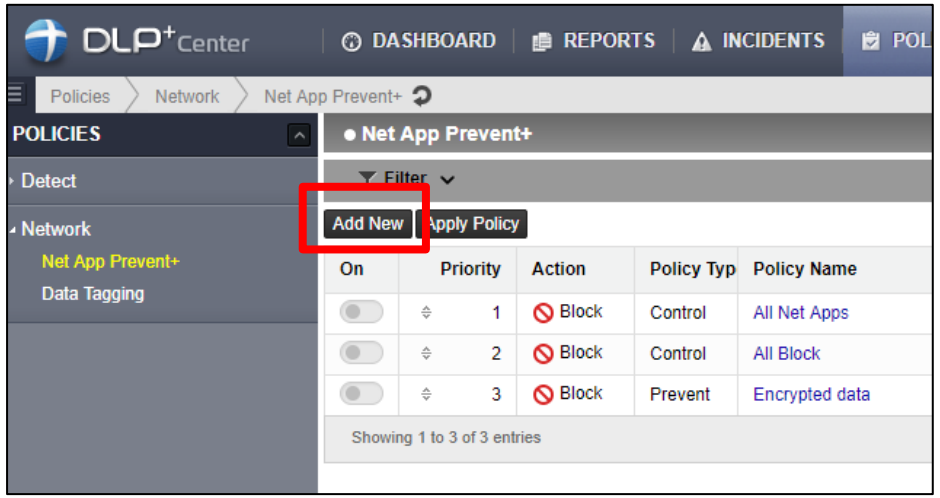
- Prevent type is block the specified app according to setting policies.

Case 1. Prevent Email (If there are credit card numbers more than five times.)

1. Click **POLICIES > Network > Net Apps Prevent**

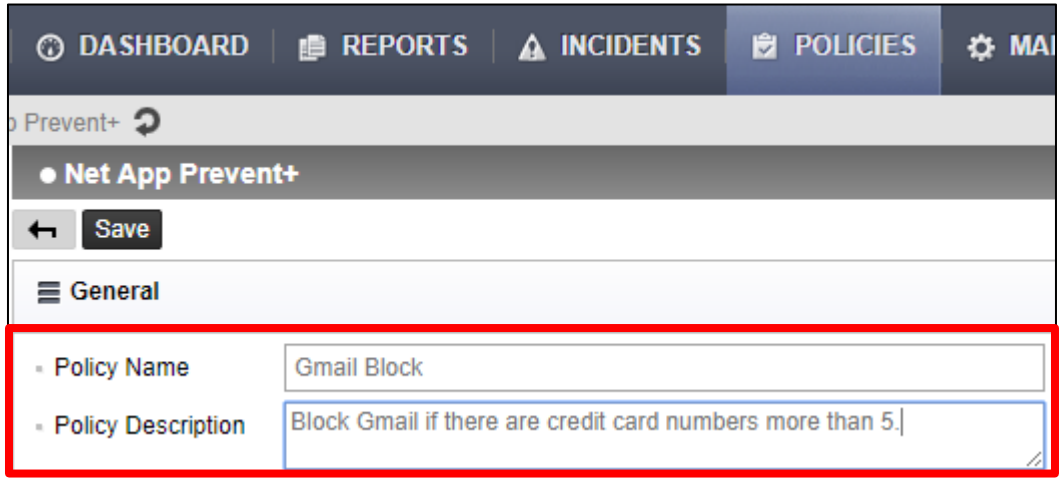
2. Click **Add New** Button



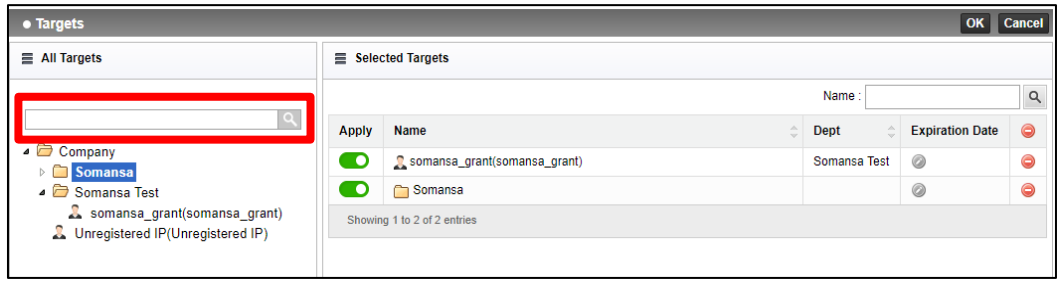


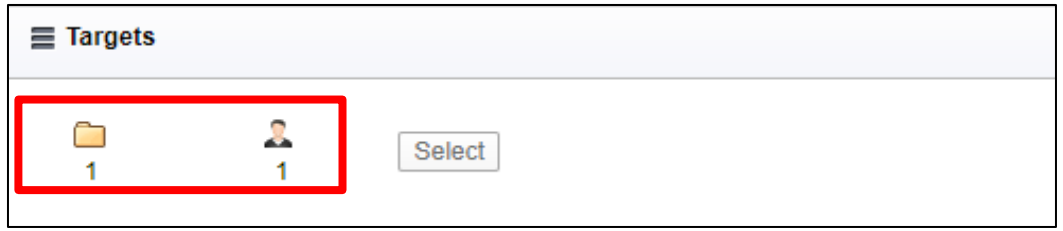
Case 1. Prevent Email

3. Put **policy name** and **policy description.**



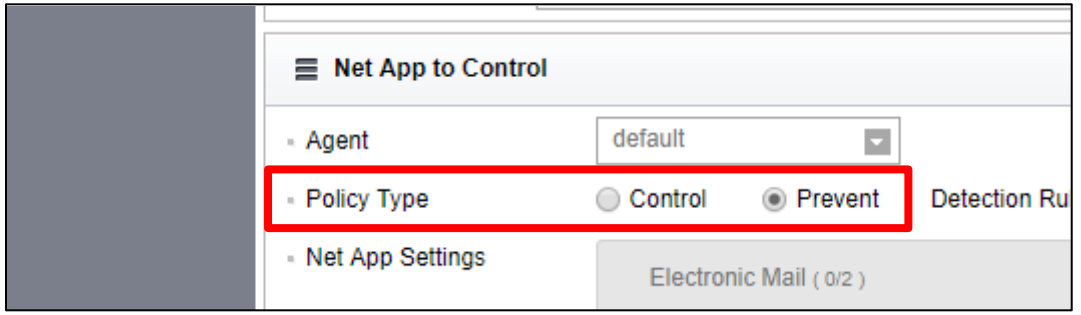
4. Select the **Target**.
   You can choose certain users or departments.
   You can also search existed names or departments.



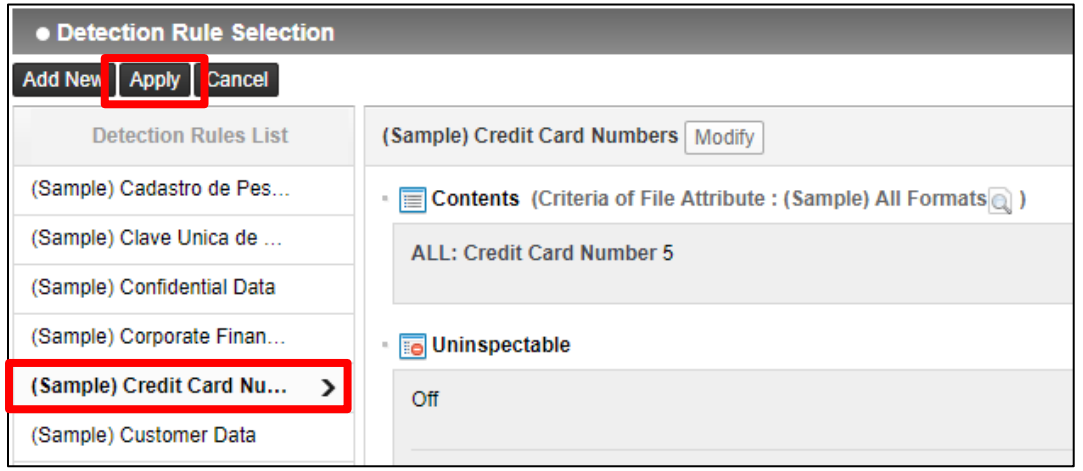


Case 1. Prevent Email

5. Select **Net App to Control > Policy Type** radio button as **Prevent**.

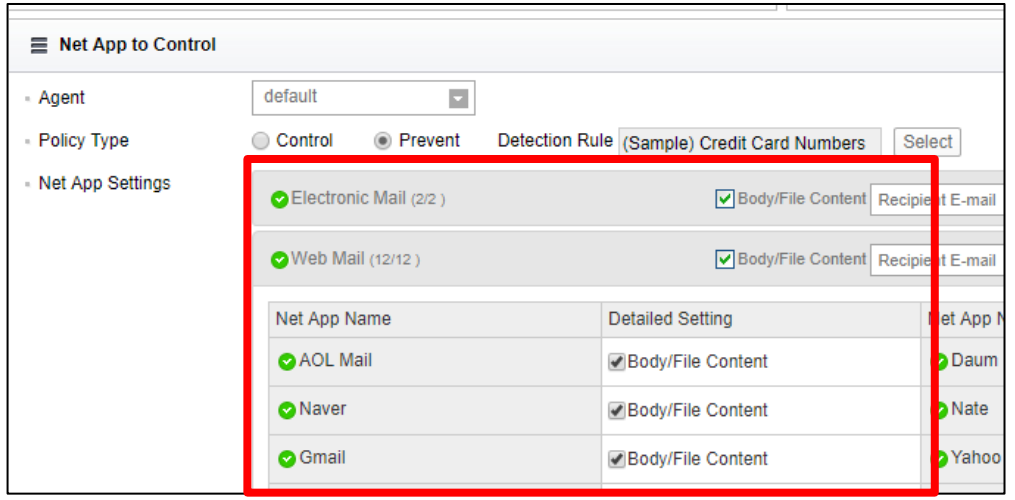


6. Select a **Detection Rule** and click **Apply** button.

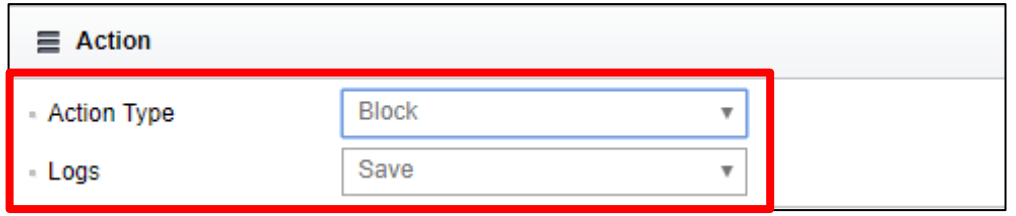


Case 1. Prevent Email

7. Check **Net App Settings**



8. Set **Action Type** as Block

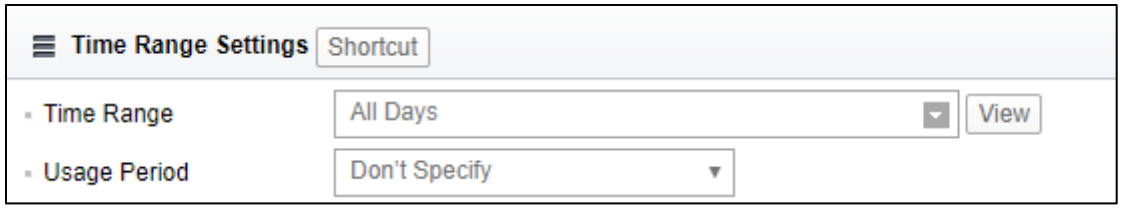


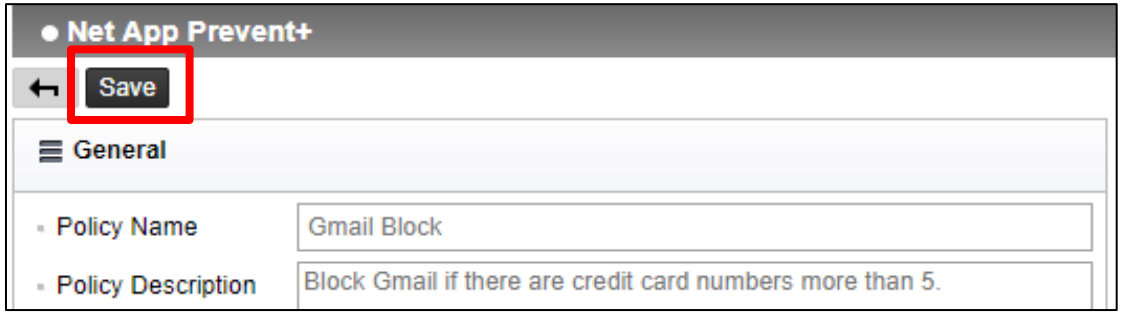
Case 1. Prevent Email

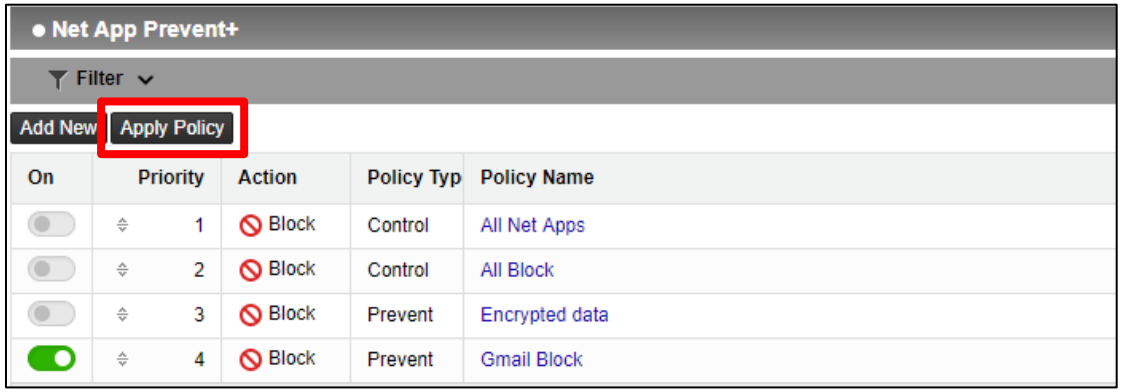
9. Set **Time Schedule**

10. Click **Save** button

11. Click **Apply Policy** button



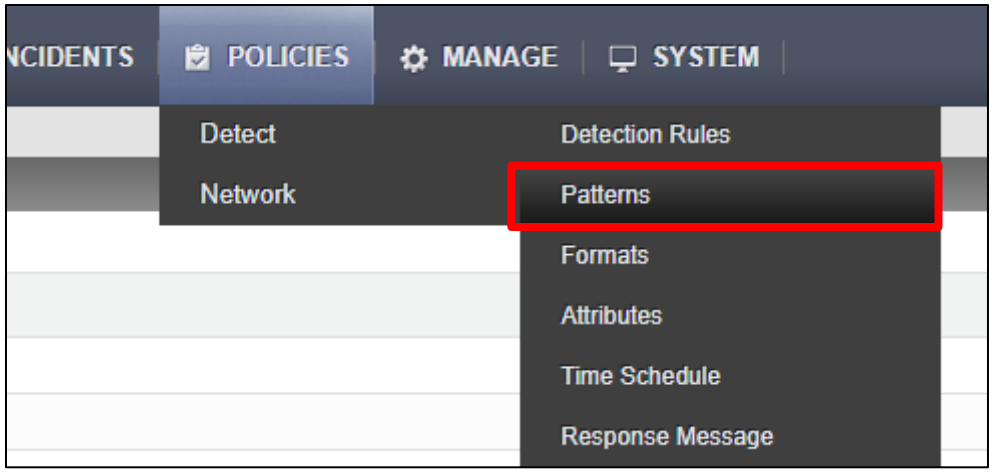




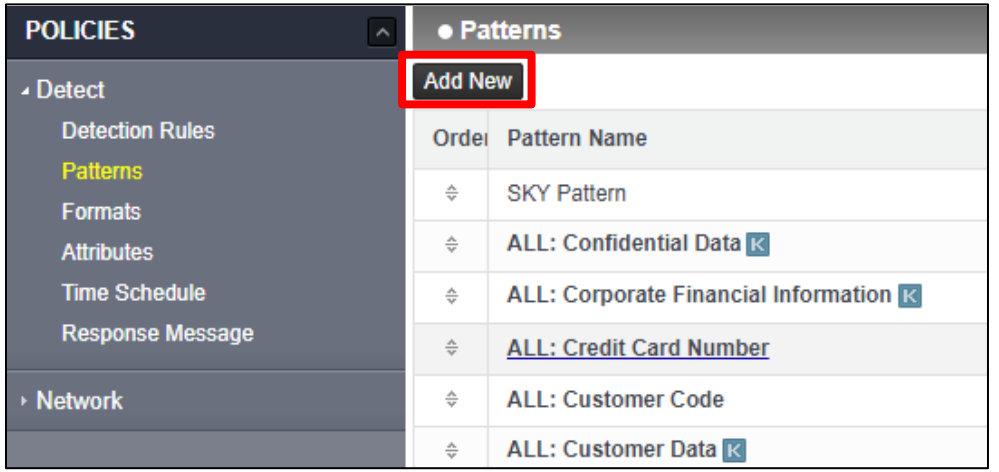
Case 2. Tag Logs

(If there is a word like ‘security’ in a mail.)

1. Click **POLICIES > Detect > Patterns**



2. Click **Add New** button

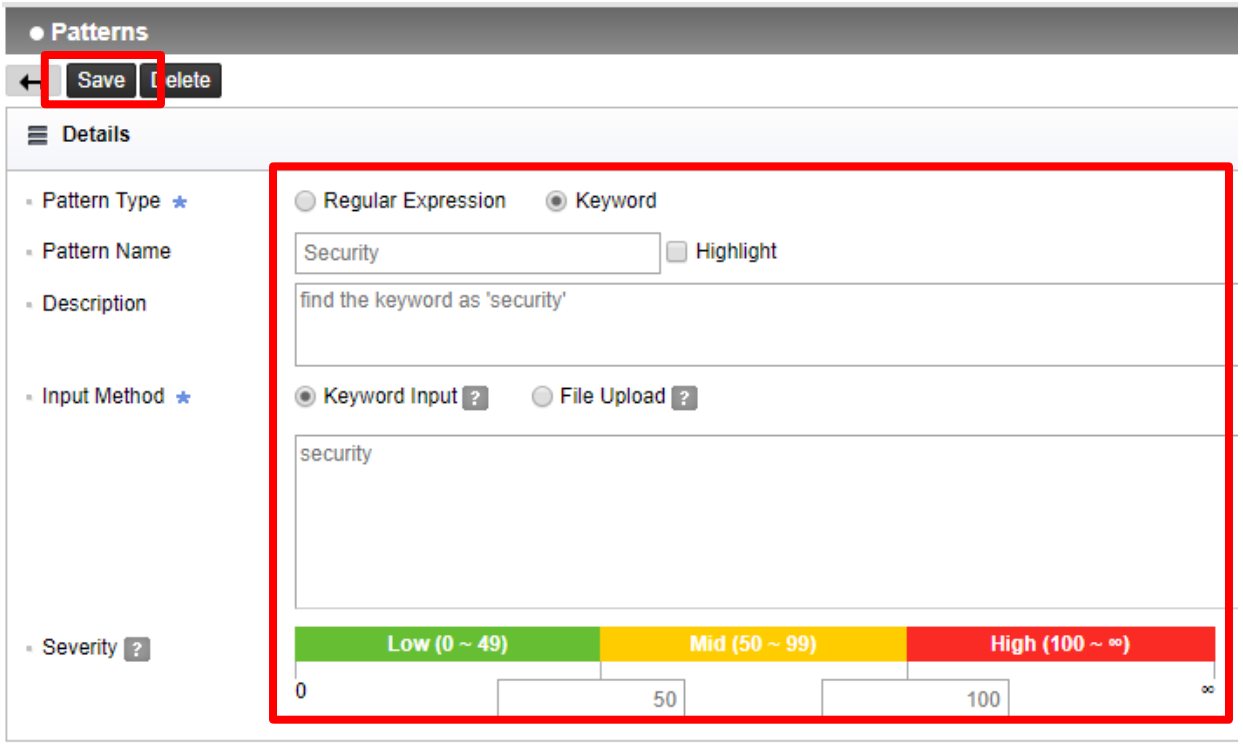


SOMANSA

Case 2. Tag Logs

3. Put **Pattern Name** and **Input Method**

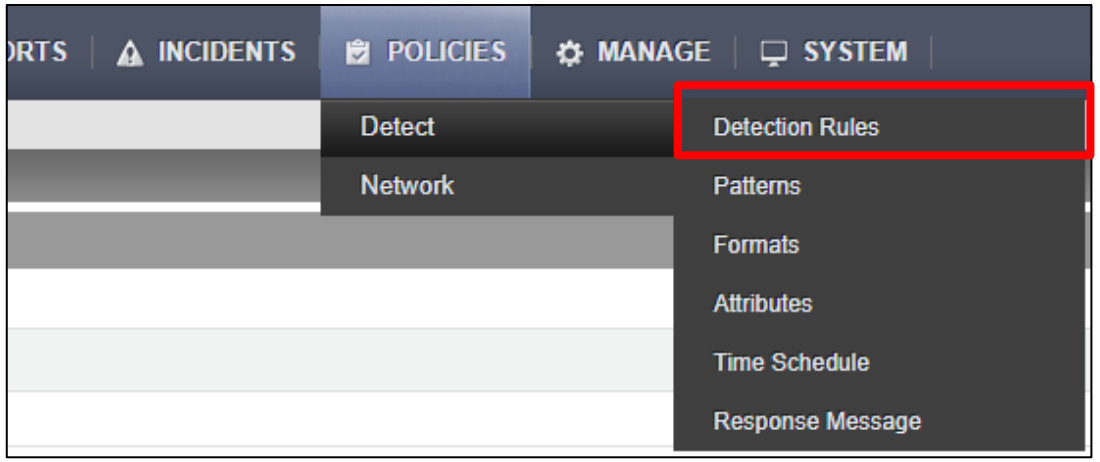
4. Click **Save** button



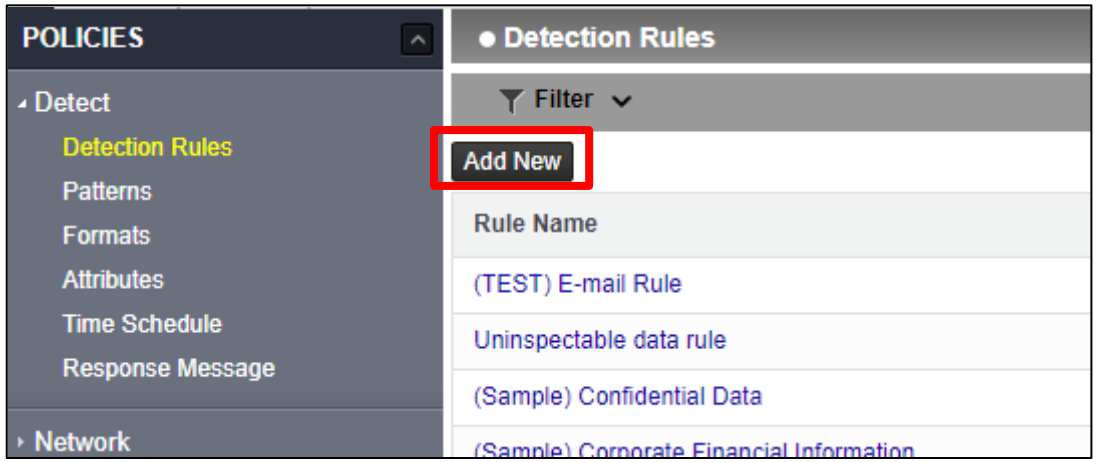
SOMANSA

Case 2. Tag Logs

5. Click **POLICIES > Detect > Detection Rules**



6. Click **Add New** button

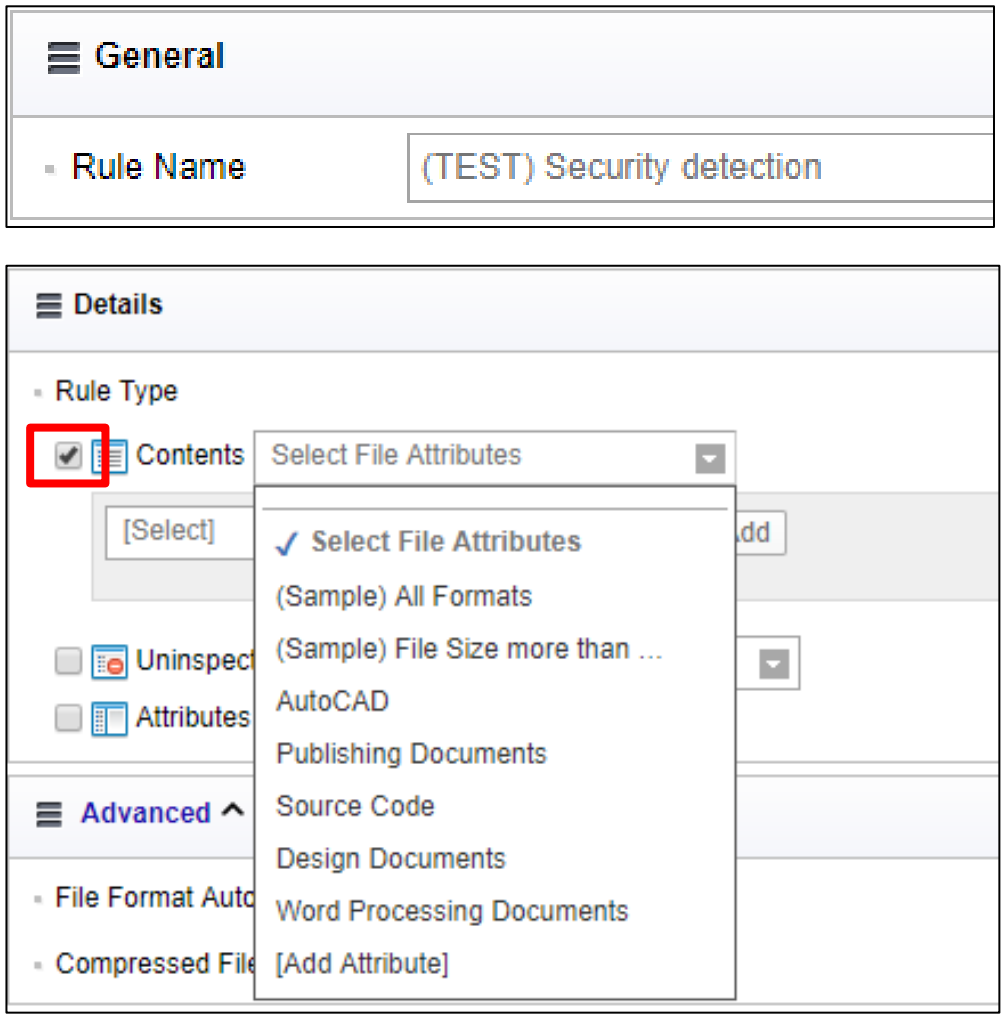


Case 2. Tag Logs

7. Put **Rule Name**

8. Select **Rule Type** as **Contents**

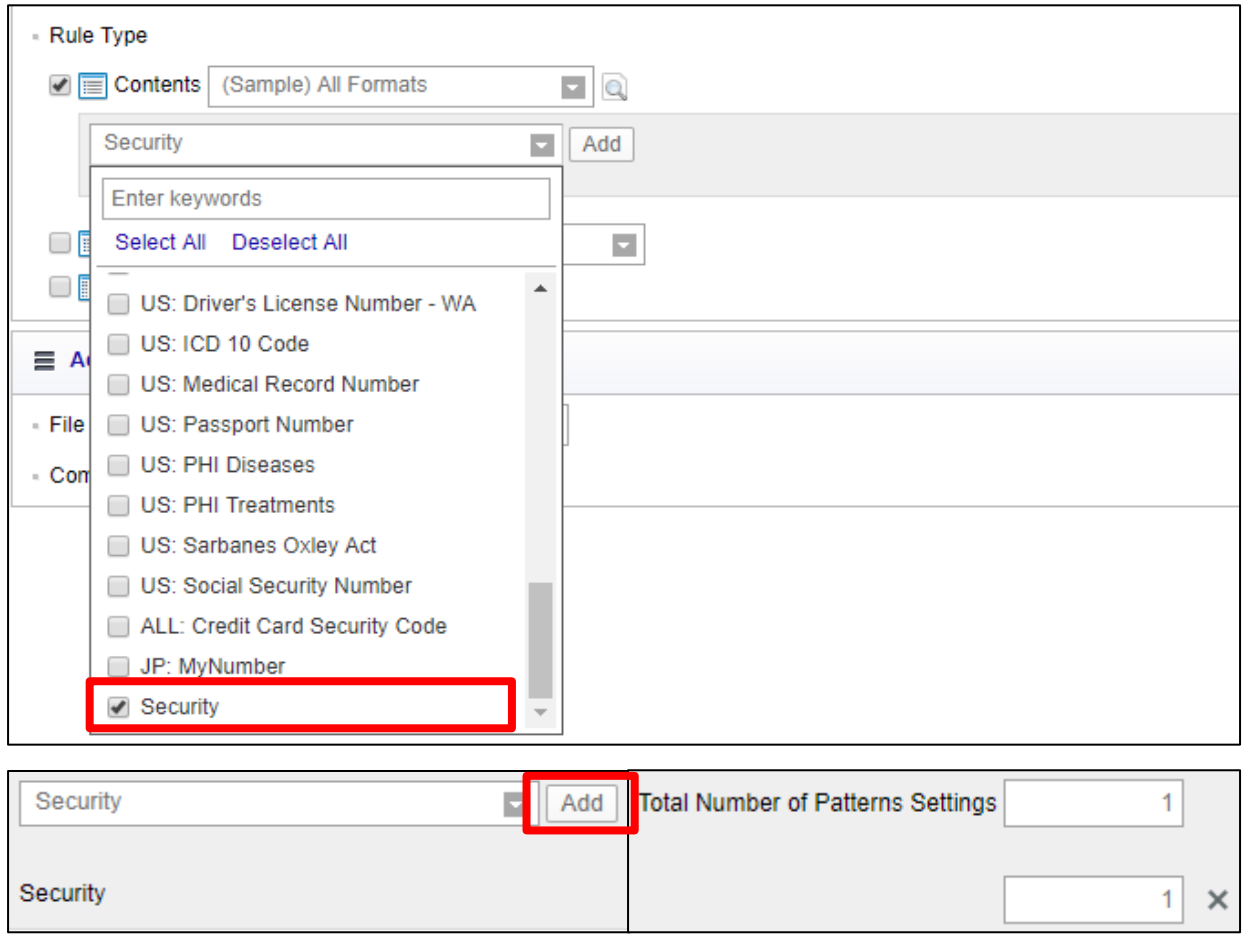
9. Select **File Attributes**



Case 2. Tag Logs

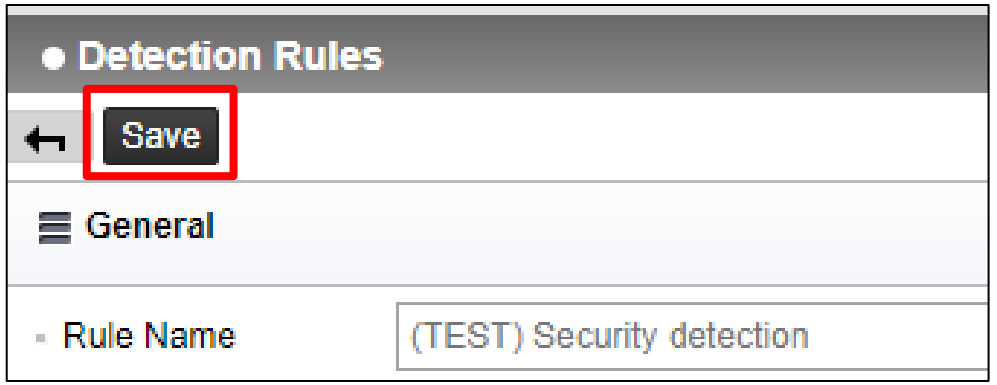
10. Select the **Pattern**

11. Click **Add** button and
    Set **Total Number of Patterns Settings**

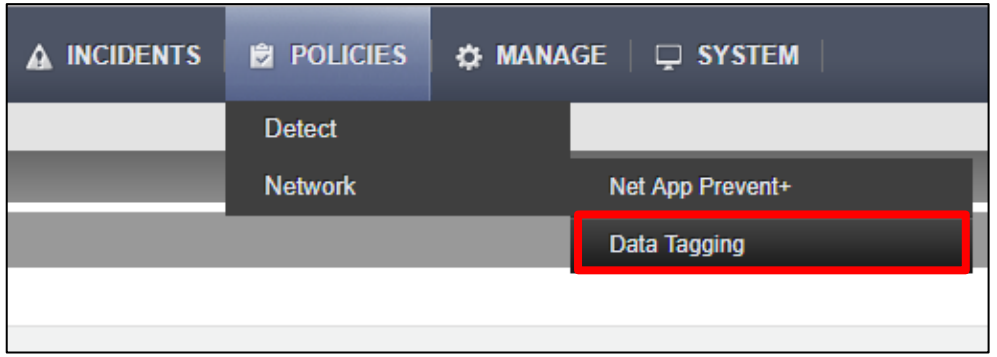


Case 2. Tag Logs

12. Click **Save** button



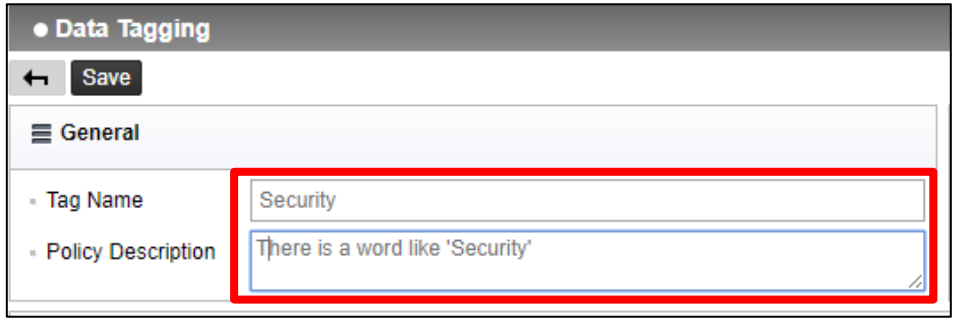
13. Click **POLICIES > Network > Data Tagging**



Case 2. Tag Logs

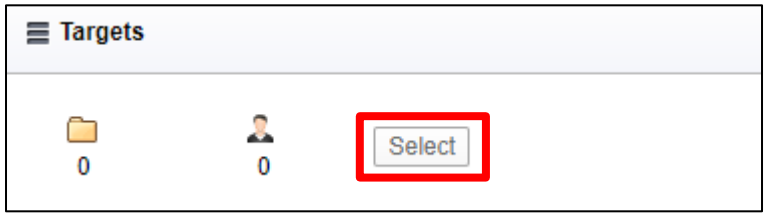
14. Click **Add New** button

15. Put **Tag Name** and **Policy Description**

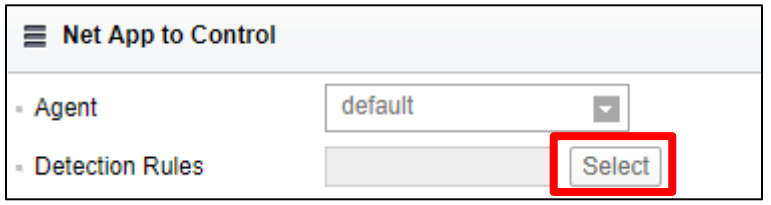


Case 2. Tag Logs

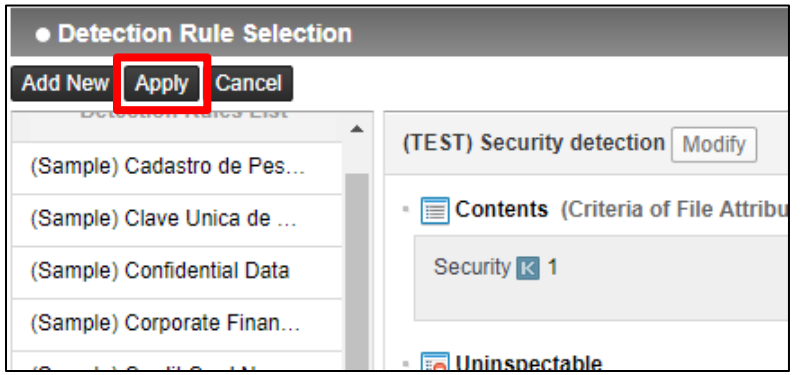
16. Select **Target**



17. Select **Detection Rules**

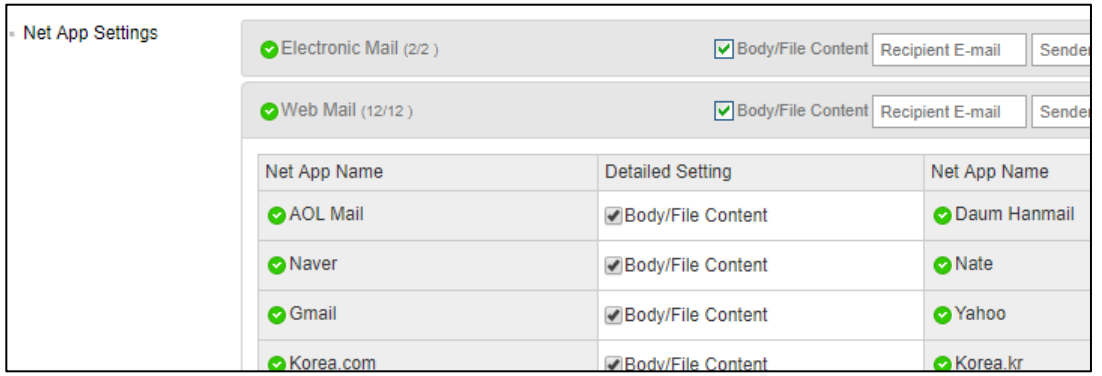


18. Click **Apply** button



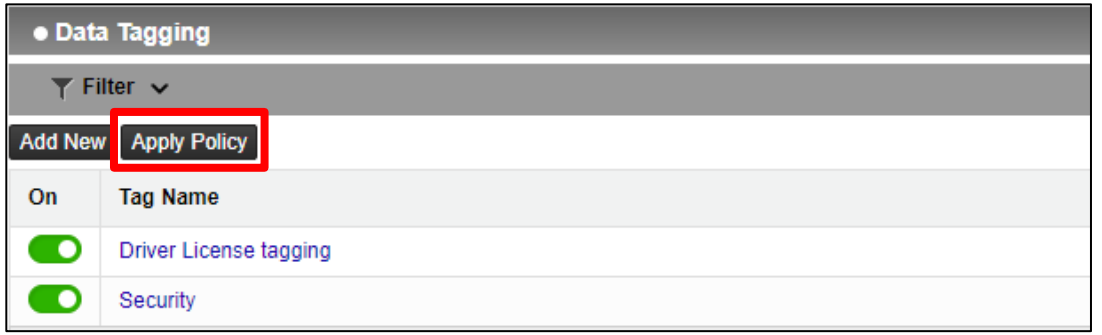
Case 2. Tag Logs

19. Check **Net App Settings**



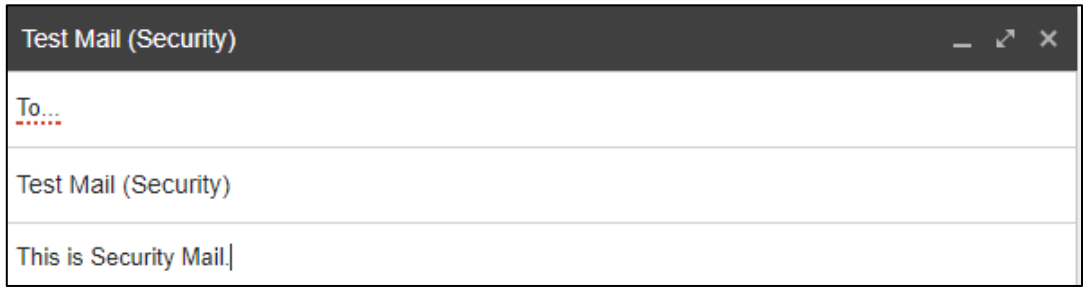
20. Click **Save** button

21. Click **Apply Policy** button



Case 2. Tag Logs

22. Write and Send a test mail



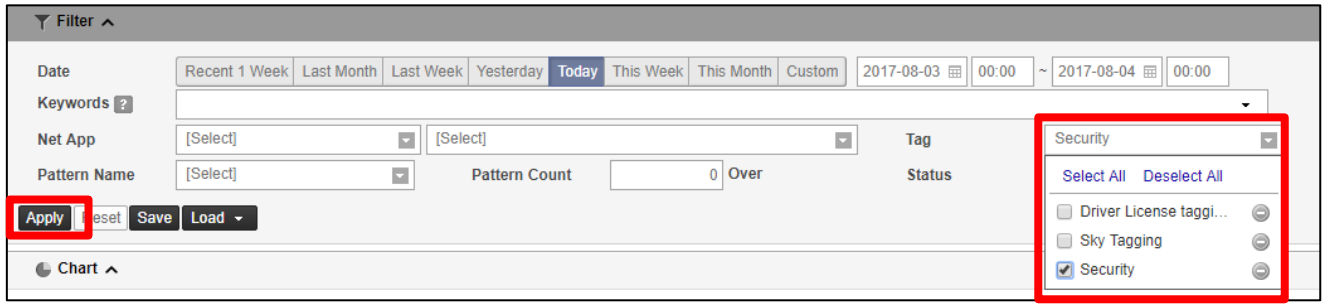
23. Click **INCIENTS >**

Network > Net App

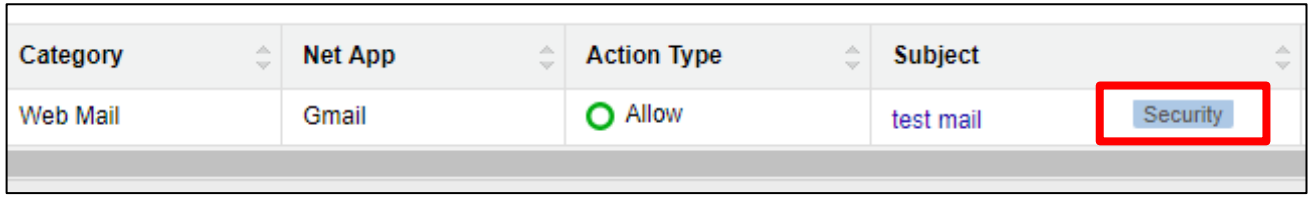
Case 2. Tag Logs

24. Select **Tag** in **Filter**

25. Click **Apply** button



26. You can check a tag next to the subject



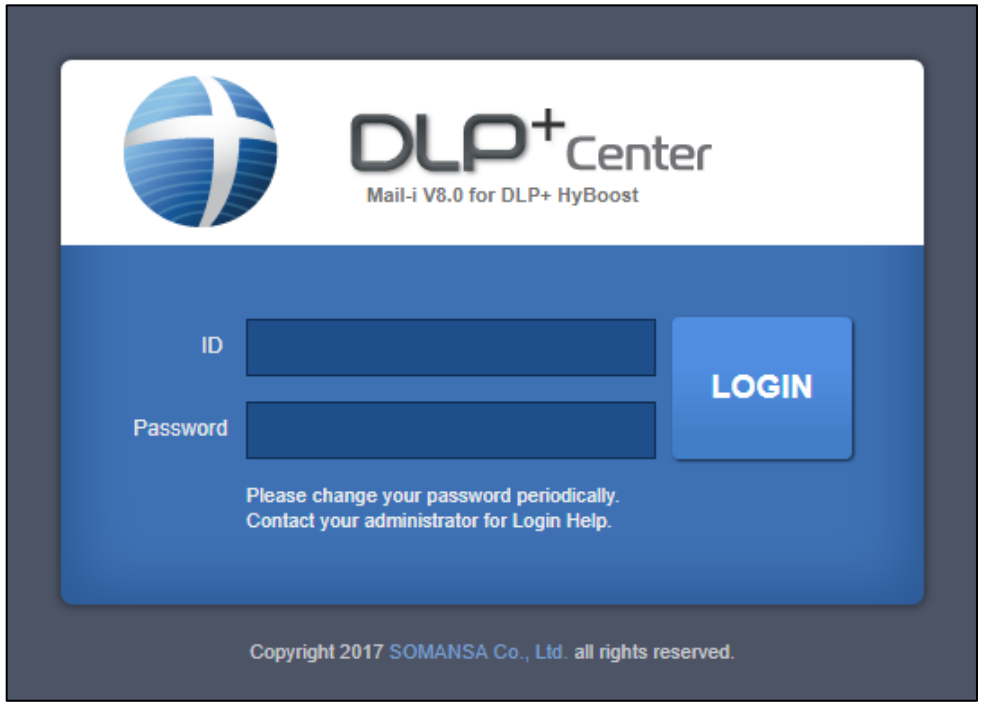
III. DLP+ Center (Detail instructions)

1. Log-in DLP+ Center

   https://IP_address/DLPCenter

   ID: (Given ID)

   PW: (Given Password)

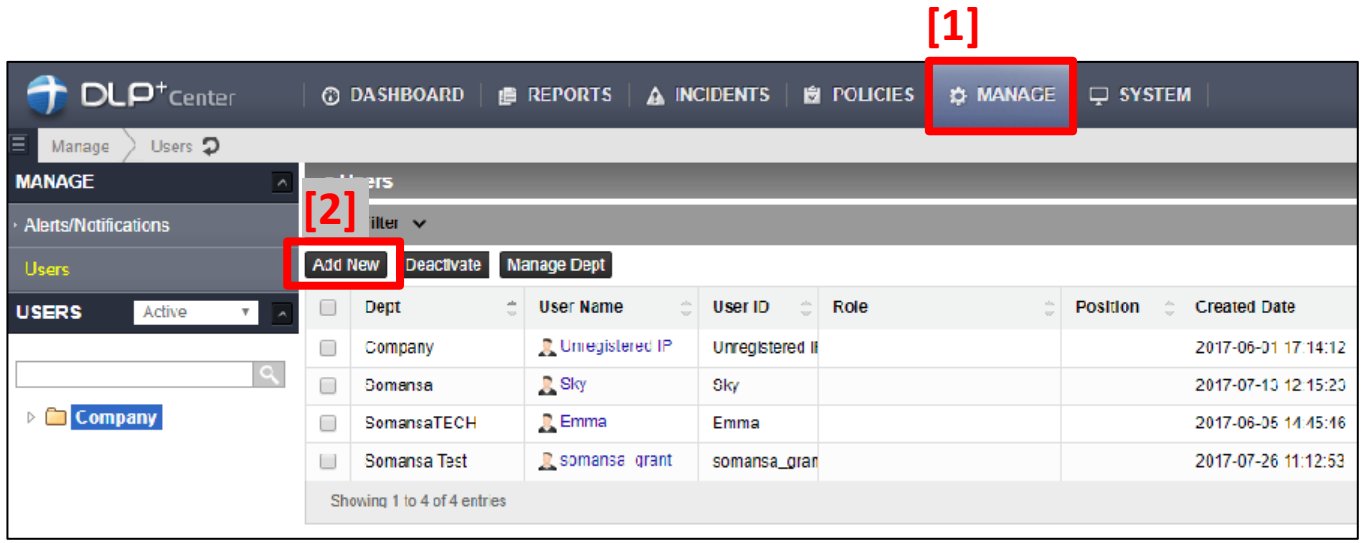


2. Manage

- Add the Users

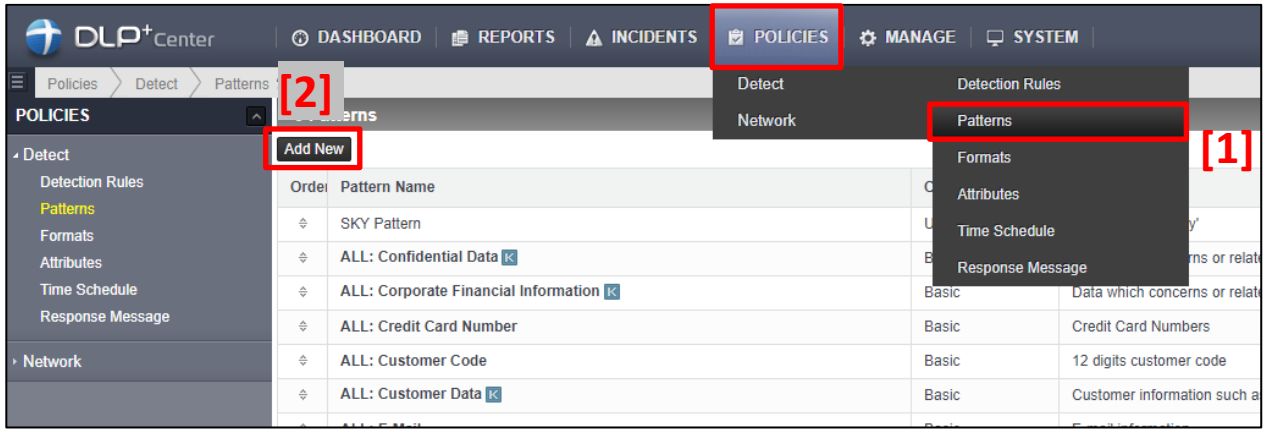
1) Select **MANAGE > Users**
2) Click **Add New**
3) Put **User Name, User ID**

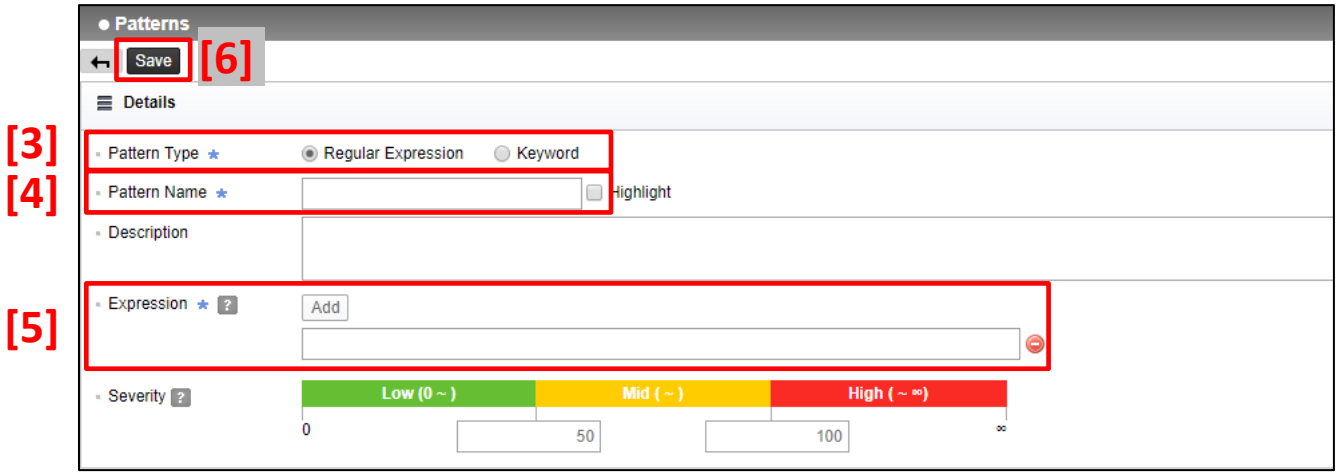
   (It is available for the same User Name, but duplicate User ID is not allowed. User ID must be unique.)
4) Check **Use Static IP** for testing.
5) Click **Save**



* You can deactivate the user, but cannot delete the user.

3. Policies

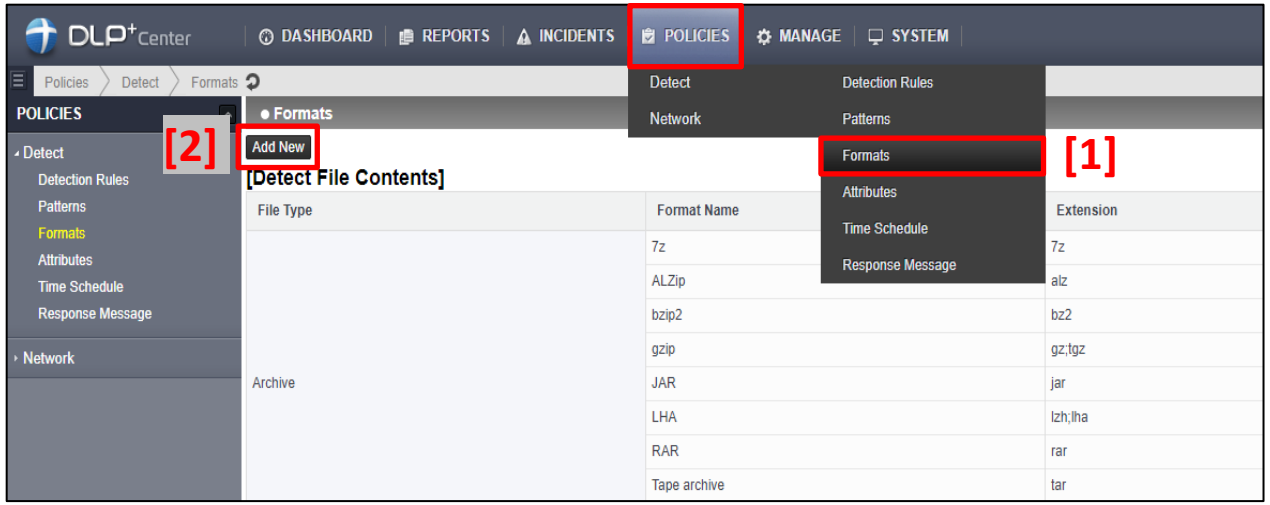


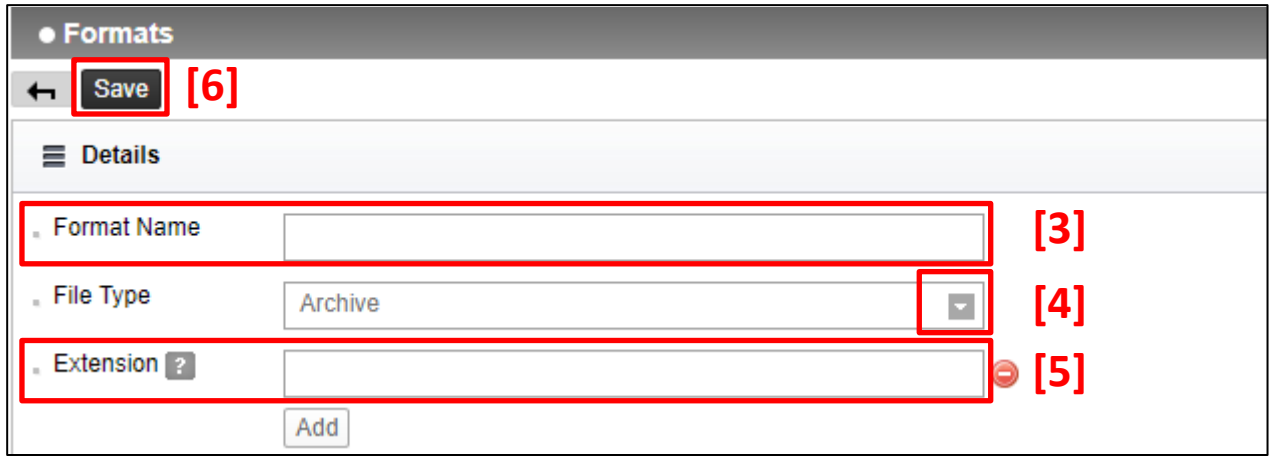


- Add Patterns

1) Select **POLICIES > Detect > Patterns**
2) Click **Add New**
3) Choose **Pattern Type**
   (Regular Expression / Keyword)
4) Put **Pattern Name**
5) Put **Expression**
   (Pattern Type – Regular Expression)
   or **Input Method**
   (Pattern Type – Keyword)
6) Click **Save**

* If you want to **delete** the pattern, select pattern name and click **delete** button.

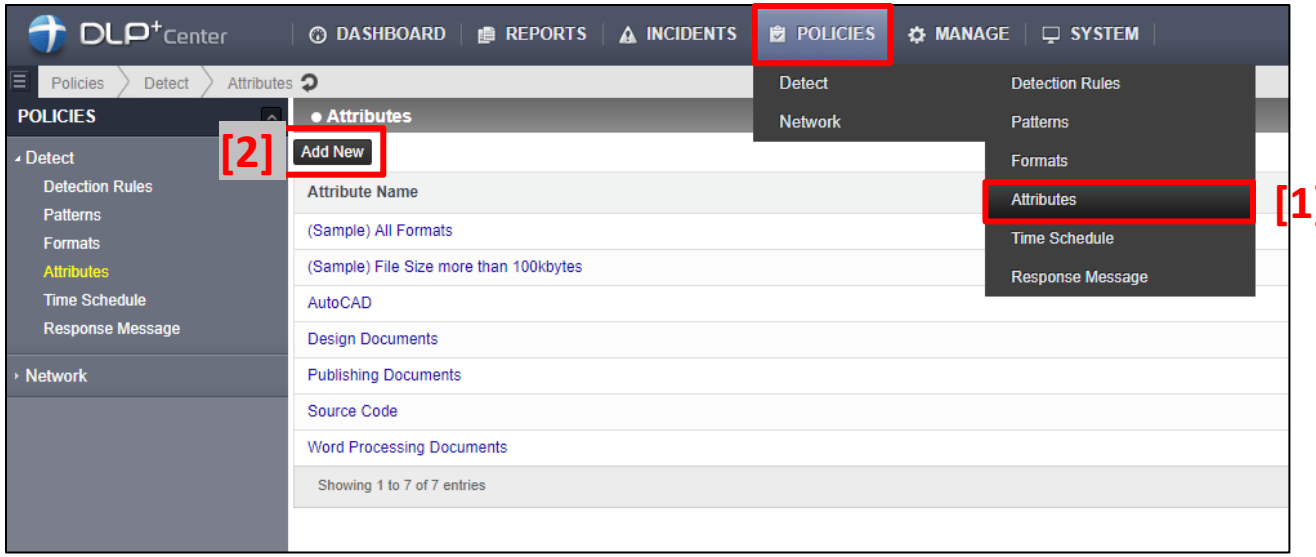


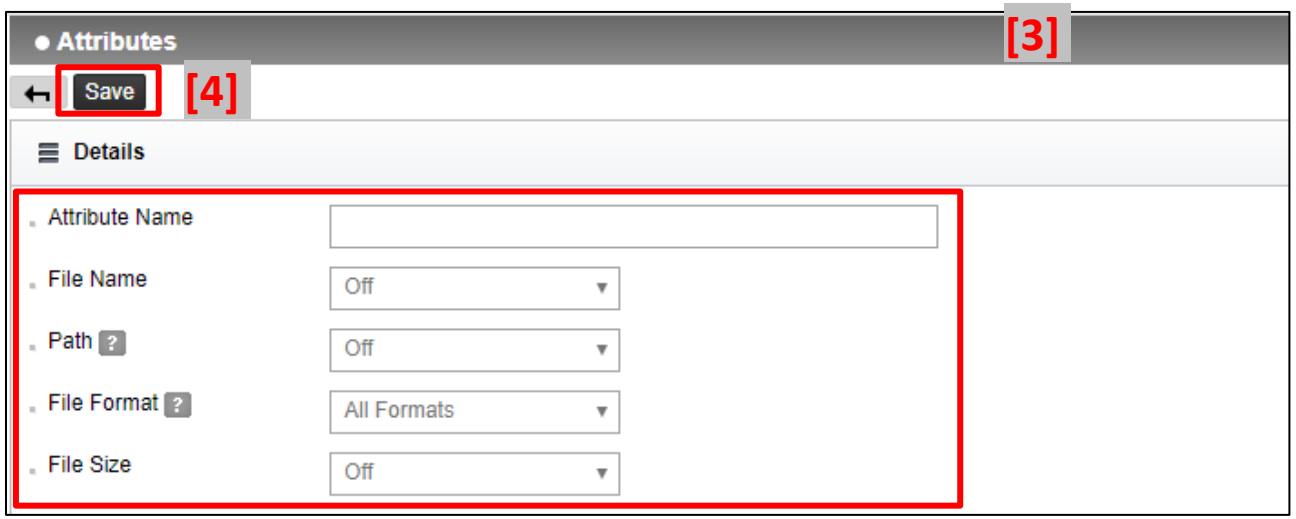


• Add Formats

1) Select **POLICIES > Detect > Formats**
2) Click **Add New**
3) Put **Format Name**
4) Select **File Type** or Add new File type
5) Put **Extension**
6) Click **Save**

* If you want to **delete** formats, select extension and click **delete** button.

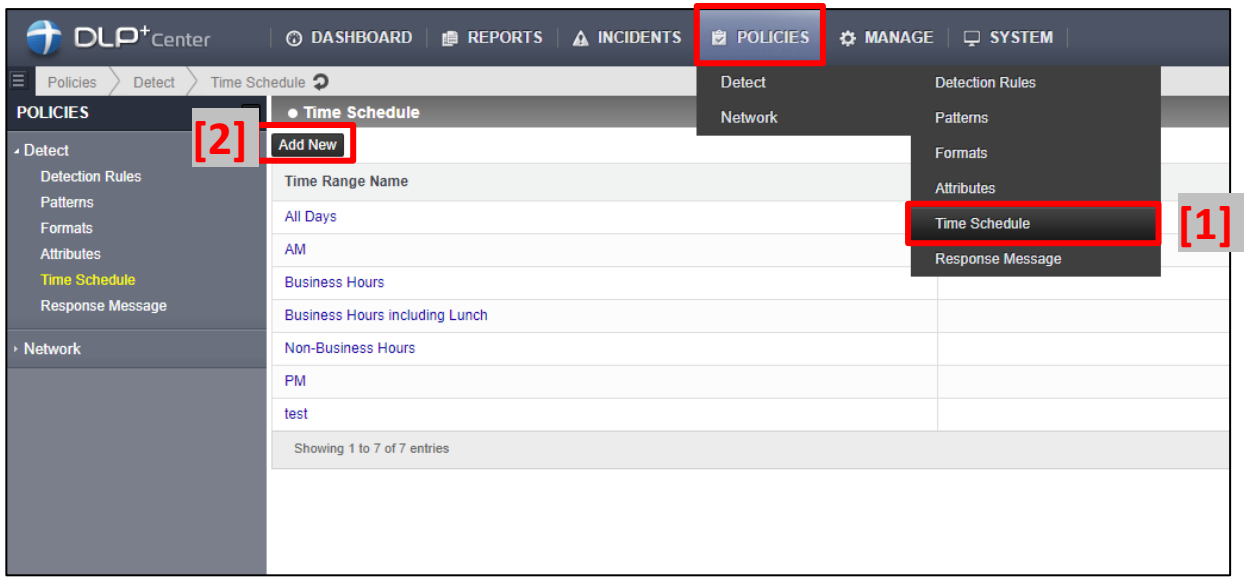


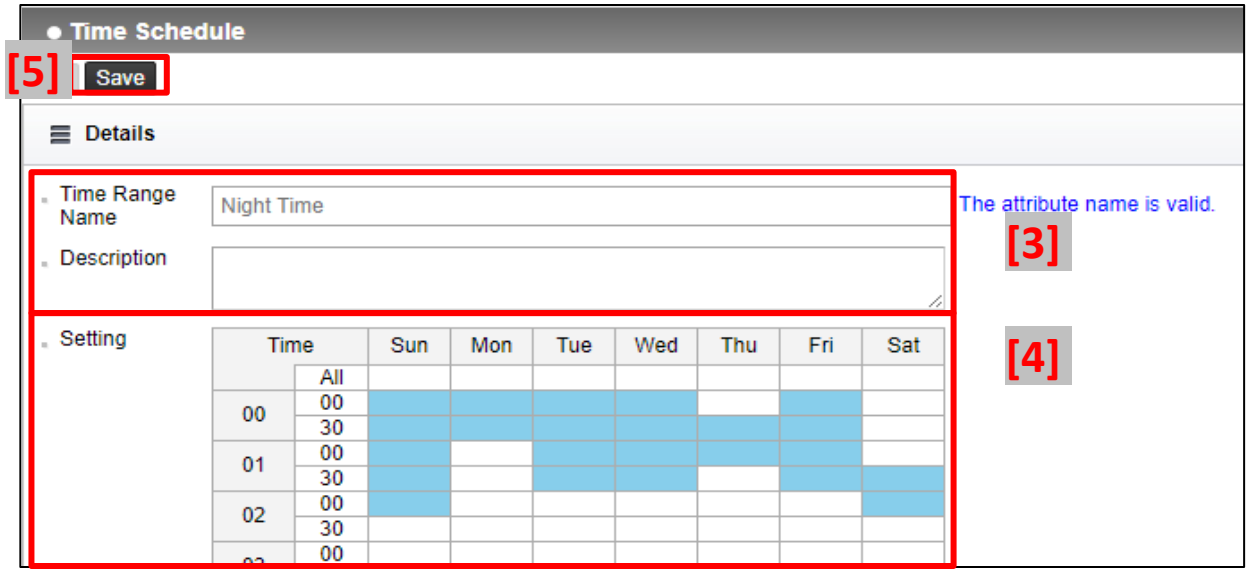


- Add Attributes

1) Select **POLICIES > Detect > Attributes**
2) Click **Add New**
3) Put some information
4) Click **Save**

* If you want to **delete** attributes, select attribute name and click **delete** button.



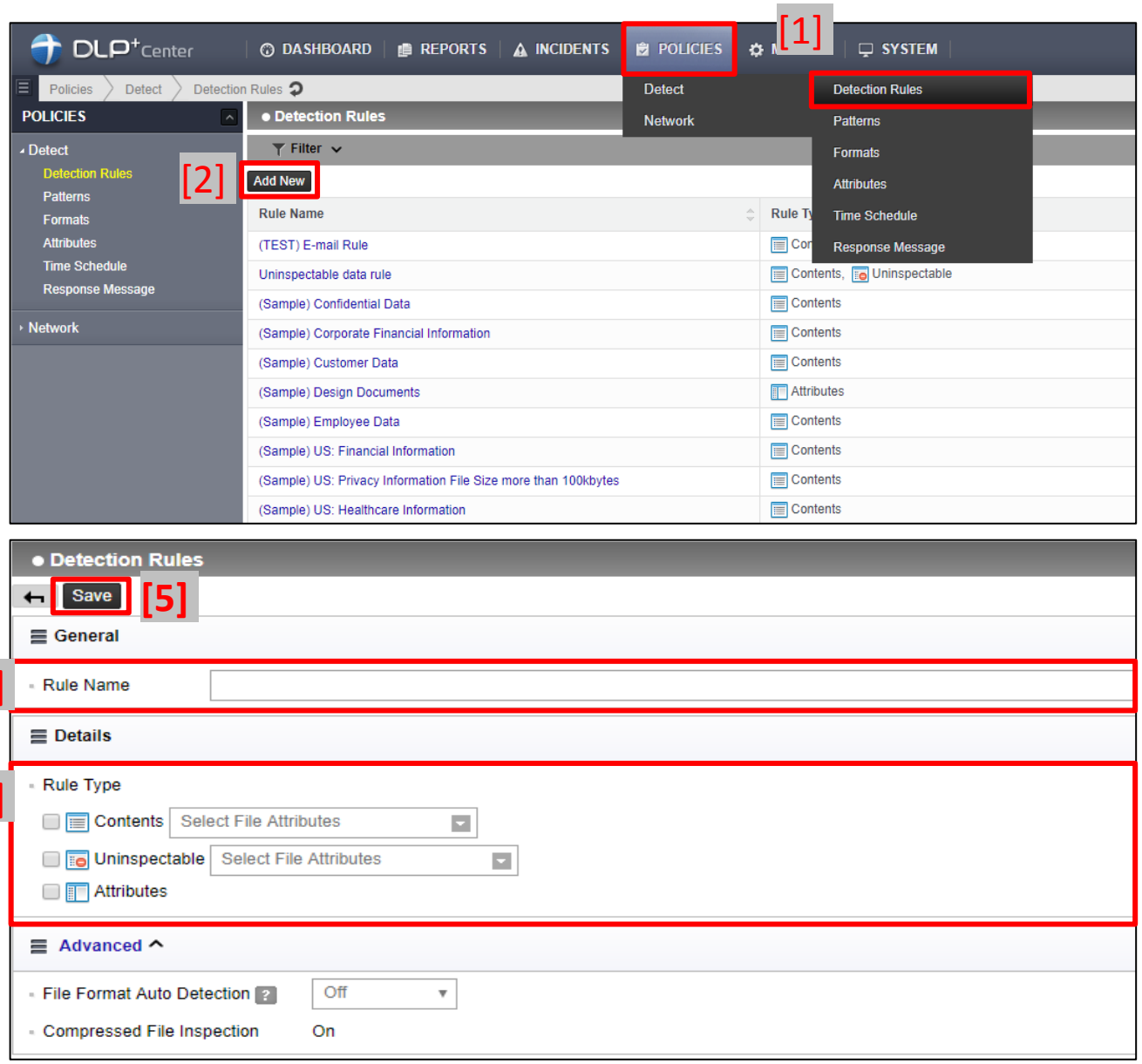


• Add Time Schedule

1) Select **POLICIES > Detect > Time Schedule**
2) Click **Add New**
3) Put **Time Range Name** and **Description**
4) Select Time blocks for **Setting**
5) Click **Save**

* If you want to **delete** time schedule, select time range name and click **delete** button.

* It will be used in **Net App Prevent+**.

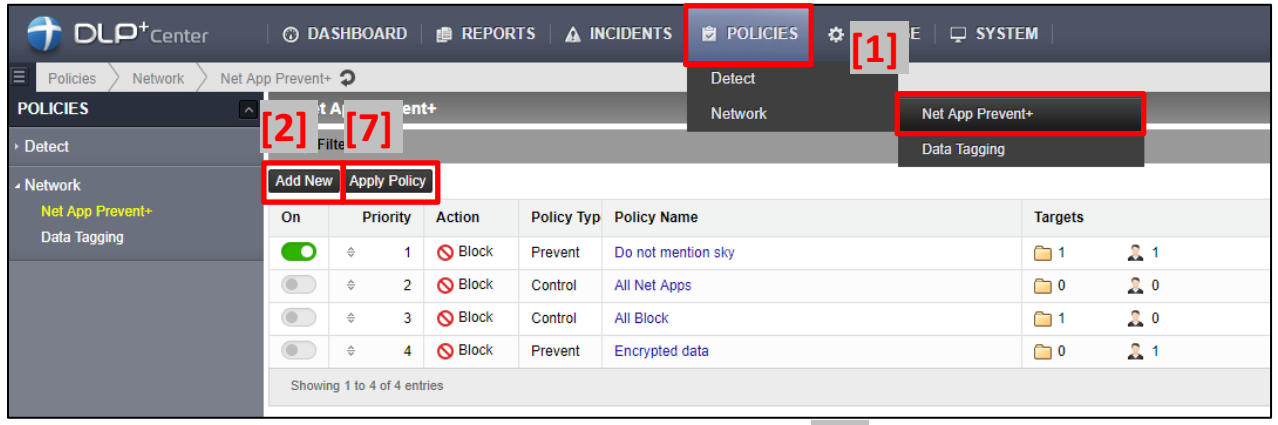


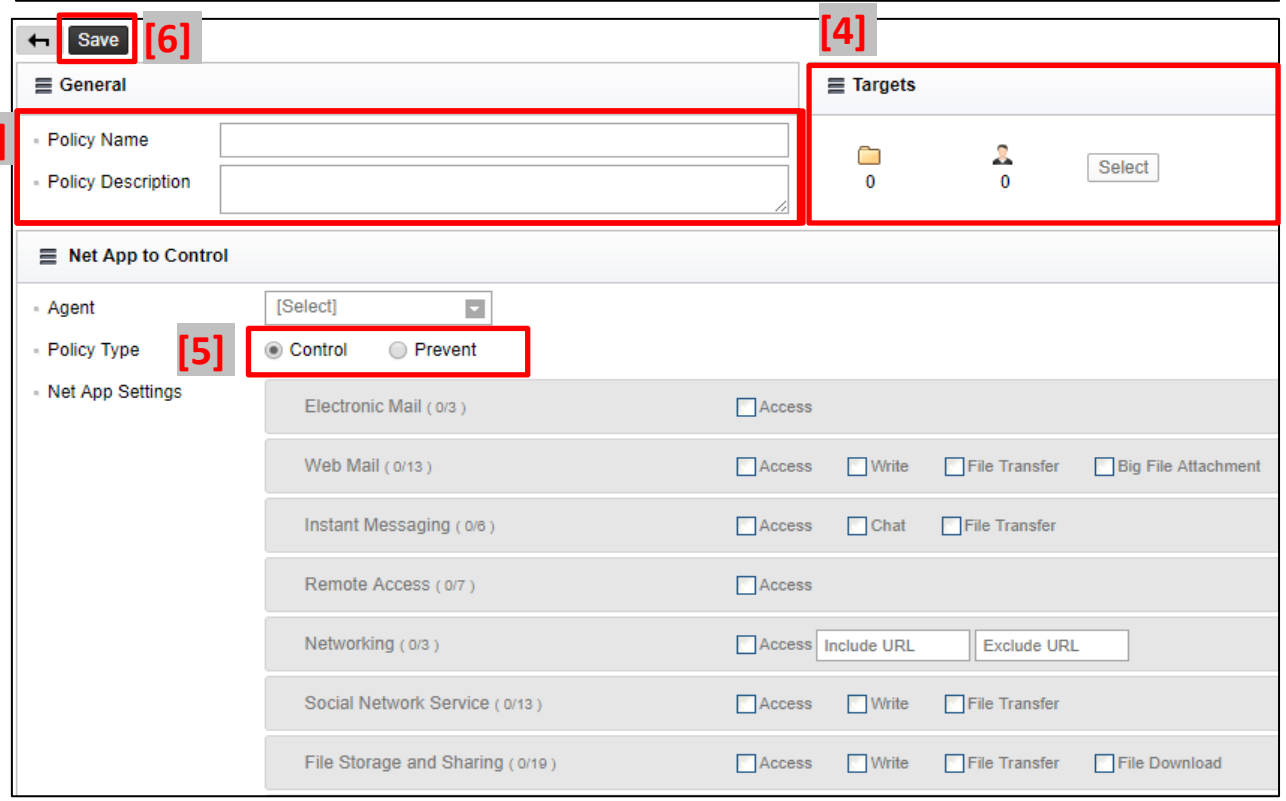
• Add Detection Rules

1) Select **POLICIES > Detect > Detection Rules**
2) Click **Add New**
3) Put **Rule Name**
4) Check **Rule Type** and Select **File Attributes**
5) Click **Save**

* If you want to **delete** detection rules, select Rule Name and click **delete** button.

* It will be used in **Net App Prevent+.**



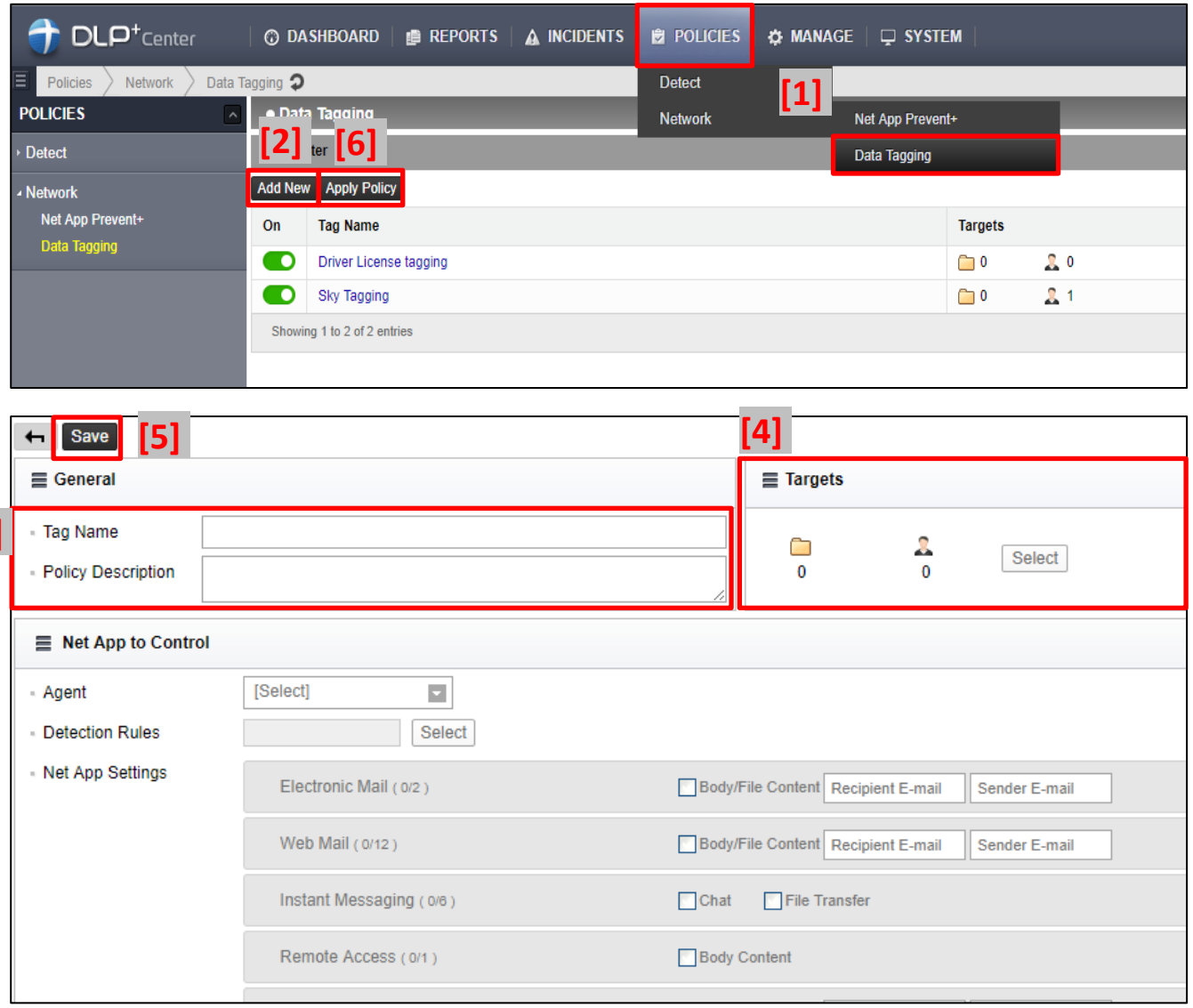


• Add Net App Prevent+

1) Select **POLICIES > Network > Net App Prevent+**
2) Click **Add New**
3) Put **Policy Name** and **Policy Description**
4) Select **Targets**
5) Choose **Policy Type** (Control or Prevent)
   - Control: allow or block the action without detection
   - Prevent: allow or block according to detection rule.
6) Click **Save**
7) You must click **Apply Policy** button.

* You can prioritize policies.

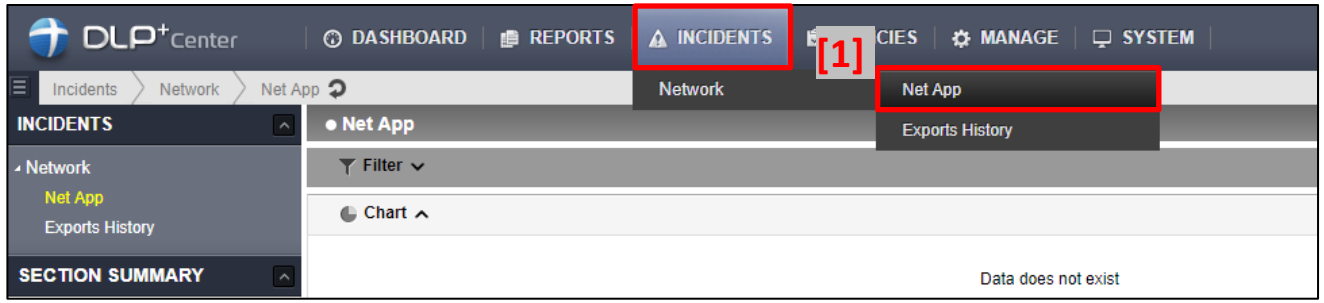
* If you want to delete the policy, select Policy Name and click **delete** button.

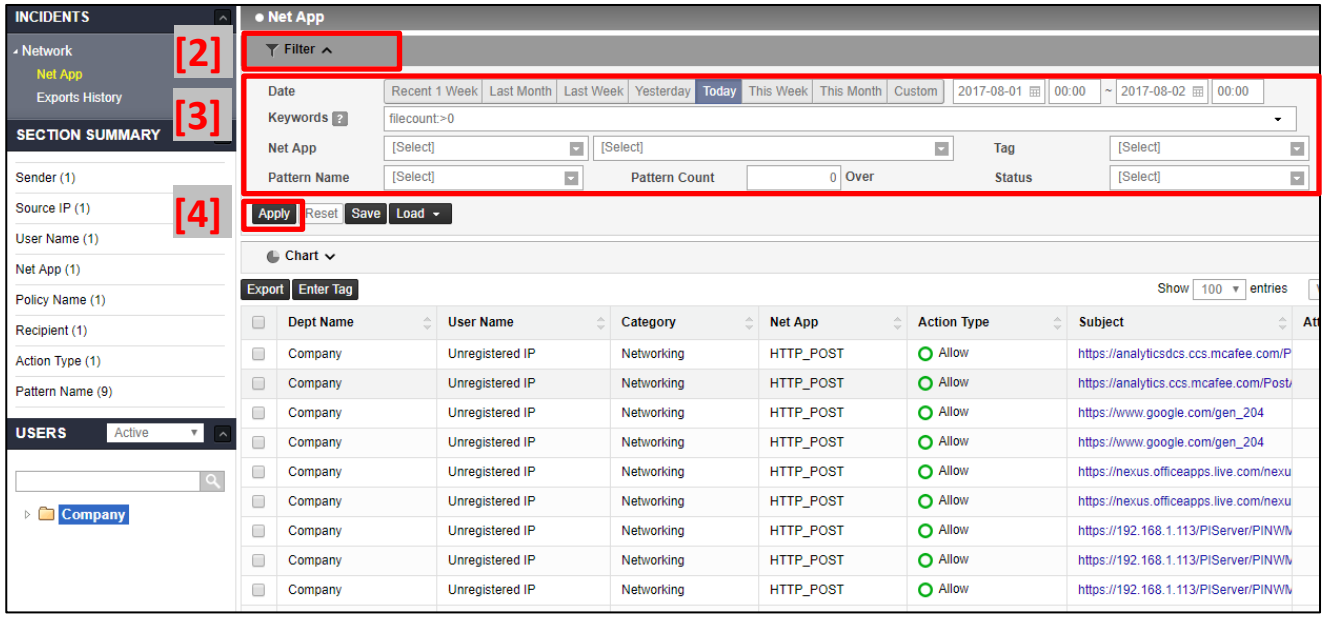


• Add Data Tagging

1) Select **POLICIES > Network > Data Tagging**
2) Click **Add New**
3) Put information like Net App Prevent+
4) Select **Targets**
5) Click **Save**
6) You must click **Apply Policy** button.

4. Incidents





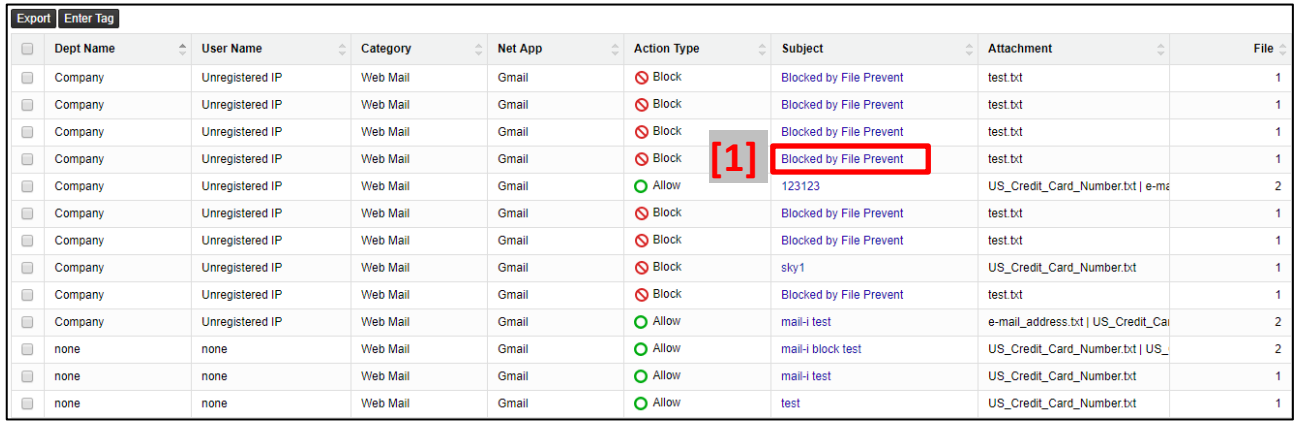
- Check the Log

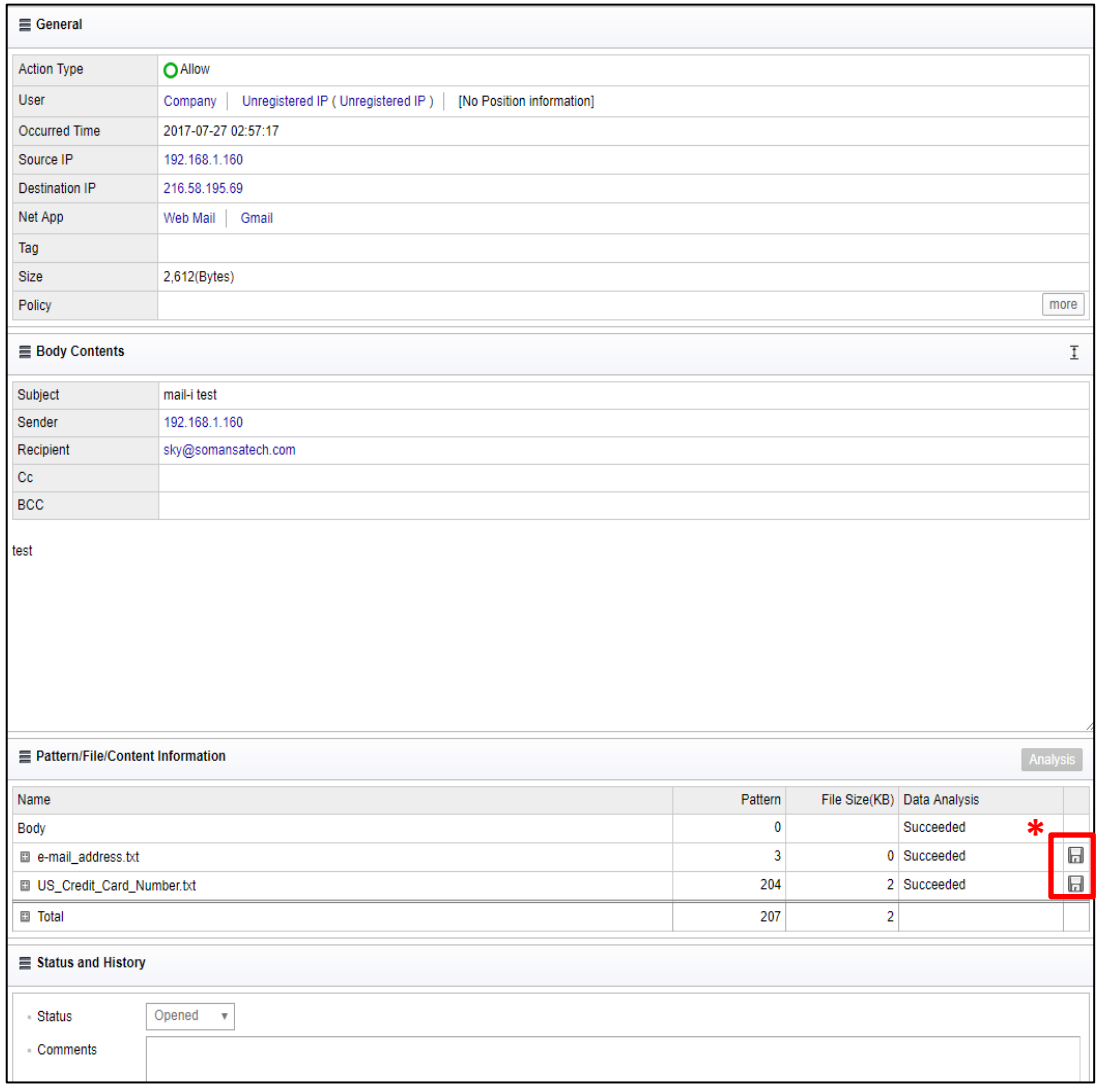
1) Select **INCIDENTS > Network > Net App**
   (You can check today's log)
2) Expand **Filter** bar
3) Put information as you want
4) Click **Apply**

- View Log in detail

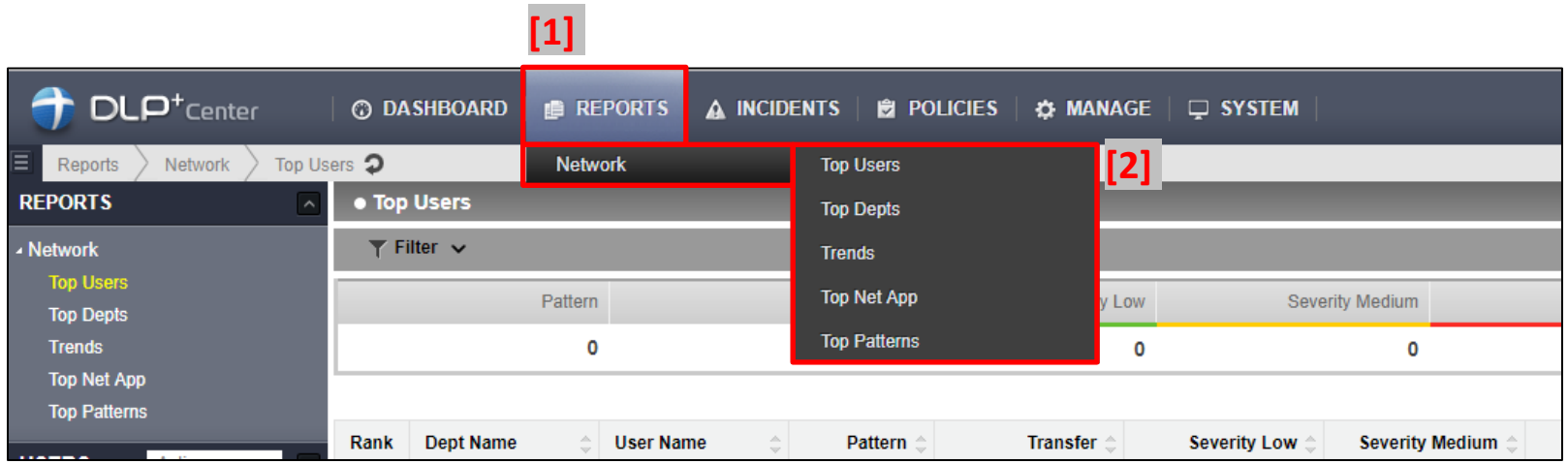
1) Select **Subject**
2) Check general information

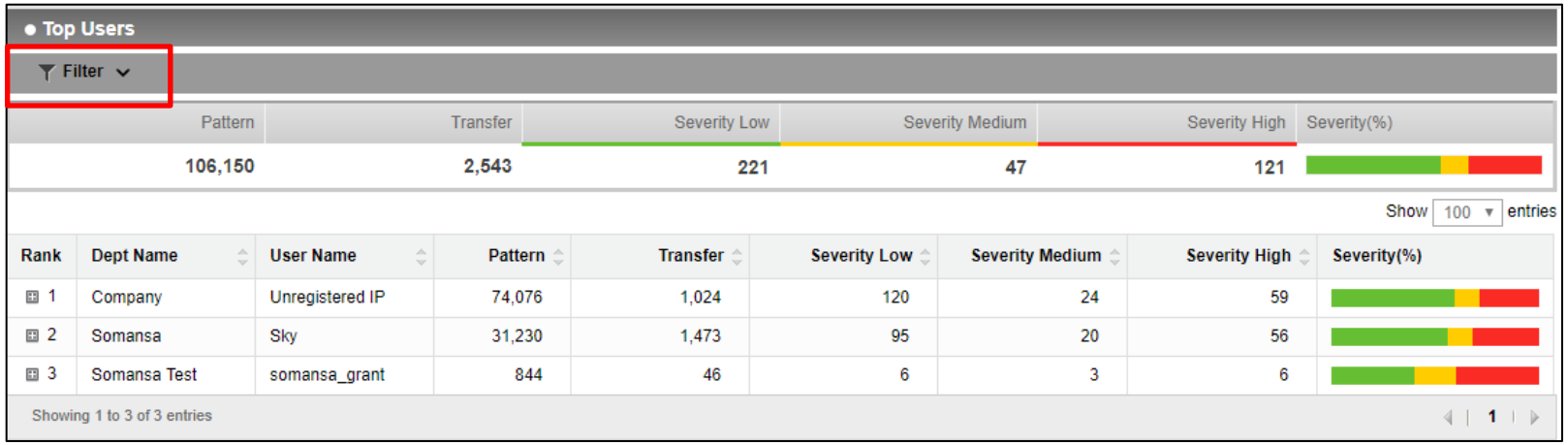
* You can download a copy for attachment files.





5. Reports





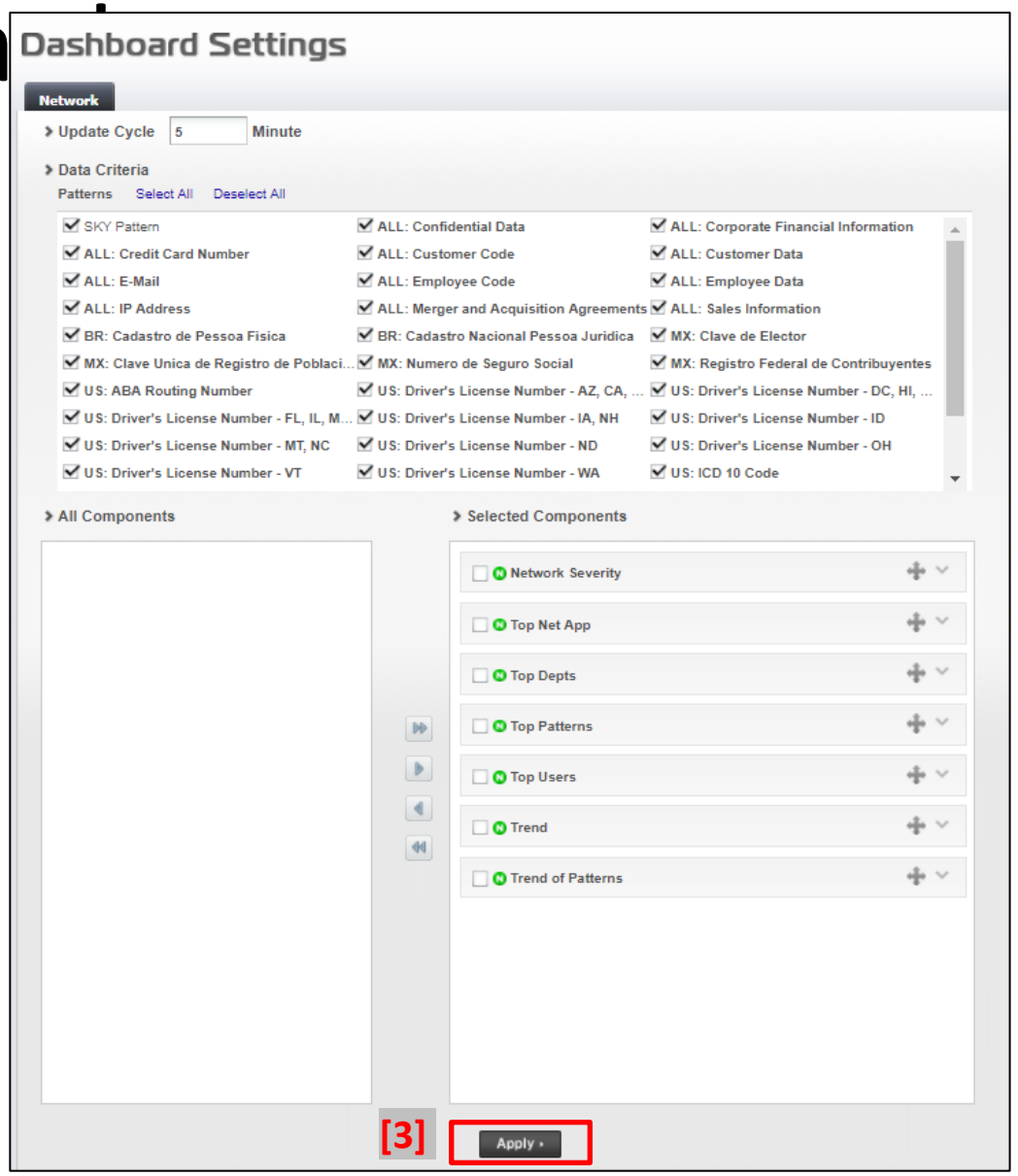
- Check Reports

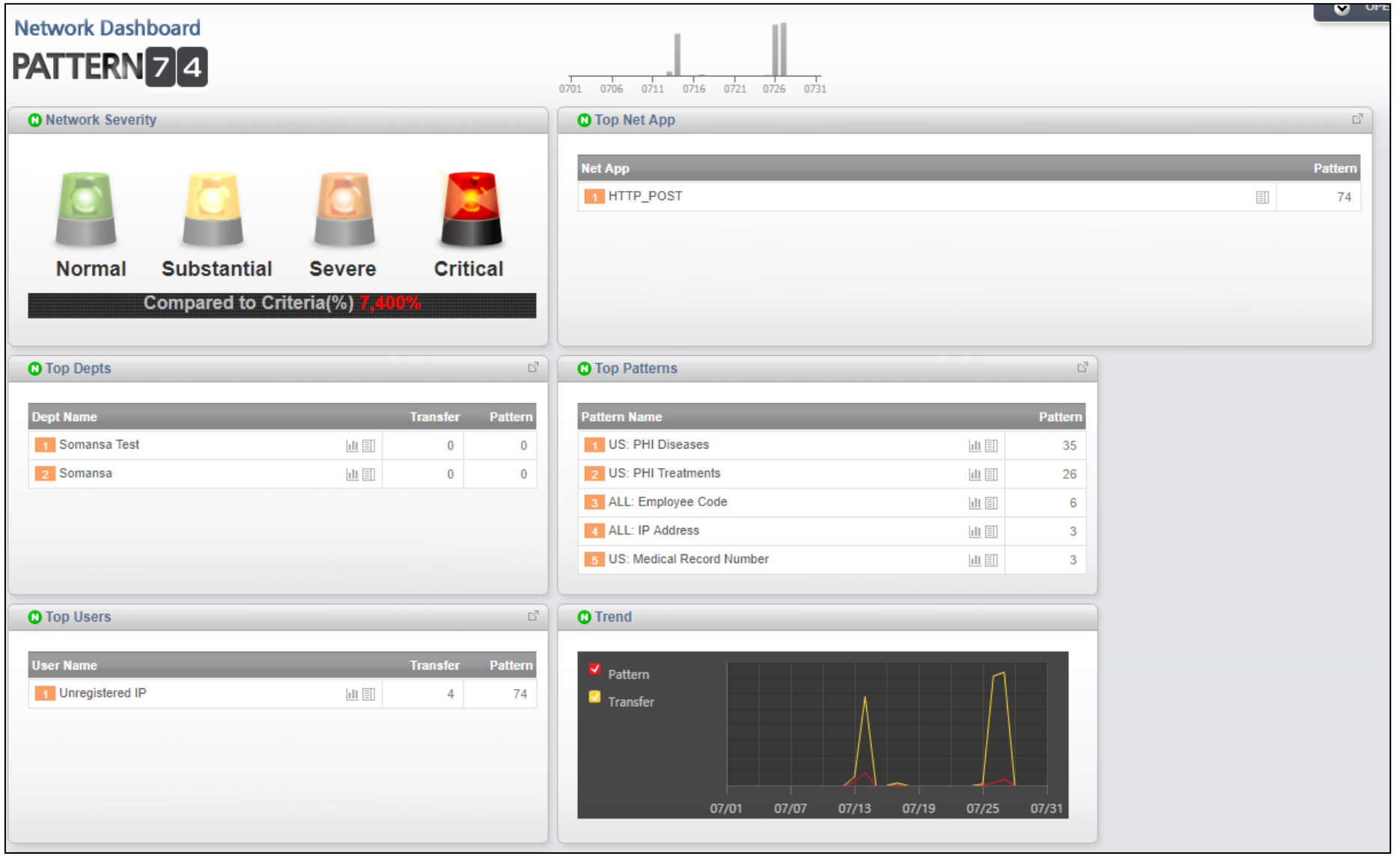
1) Select REPORTS > Network
2) Select the report criteria from the tree of Network
3) Check the Report using Filter

6. Dashboa

- Use the Dashboard

1) Select **DASHBOARD > Settings**
2) Check what you want to see
3) Click **Apply** button





* You can check some information on the dashboard as shown above.