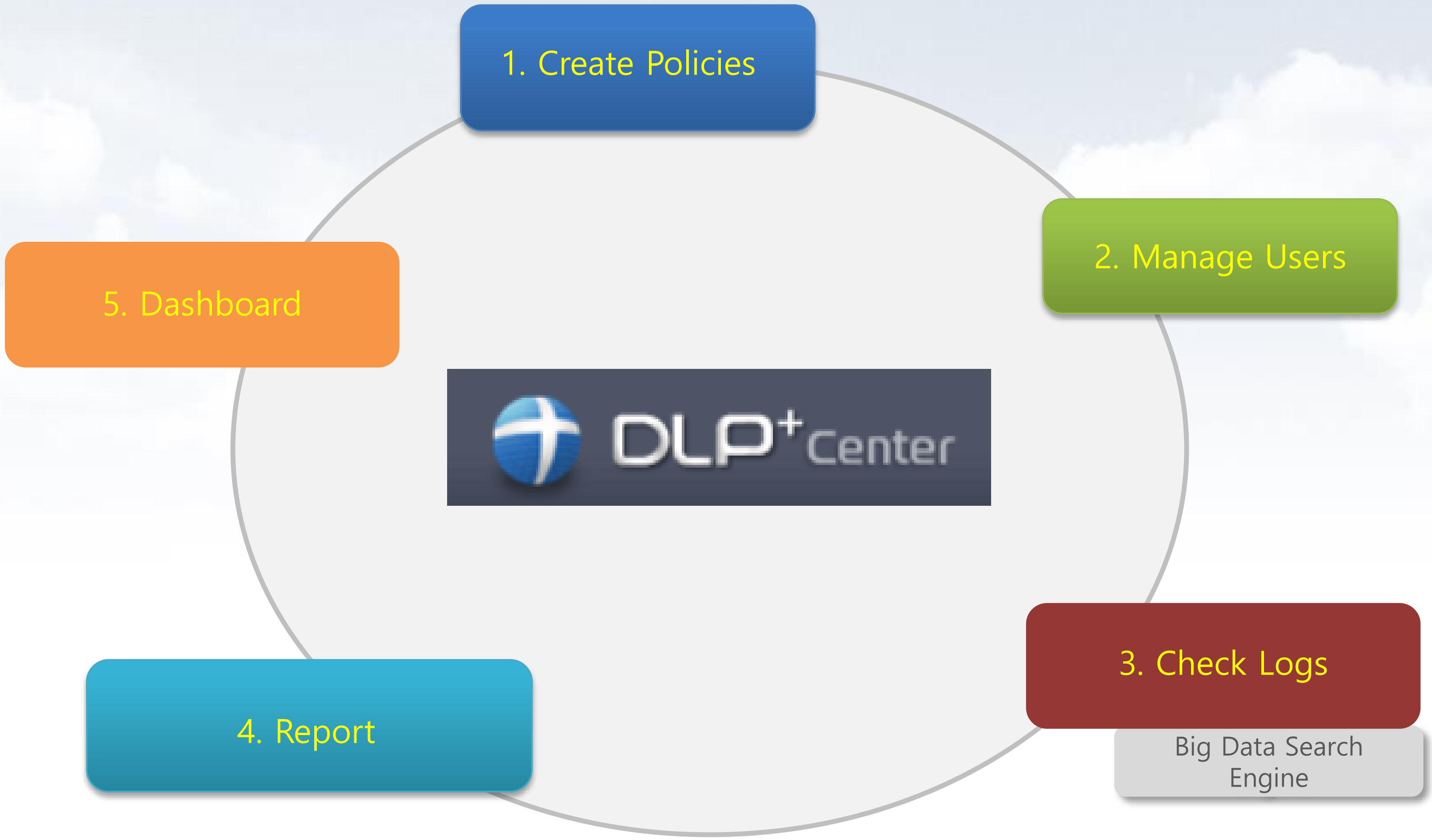
SOMANSA

Data Loss Prevention


1. Create Policies
2. Manage Users
3. Check Logs
Big Data Search Engine
4. Report
5. Dashboard
DLP+ Center

CONTENTS

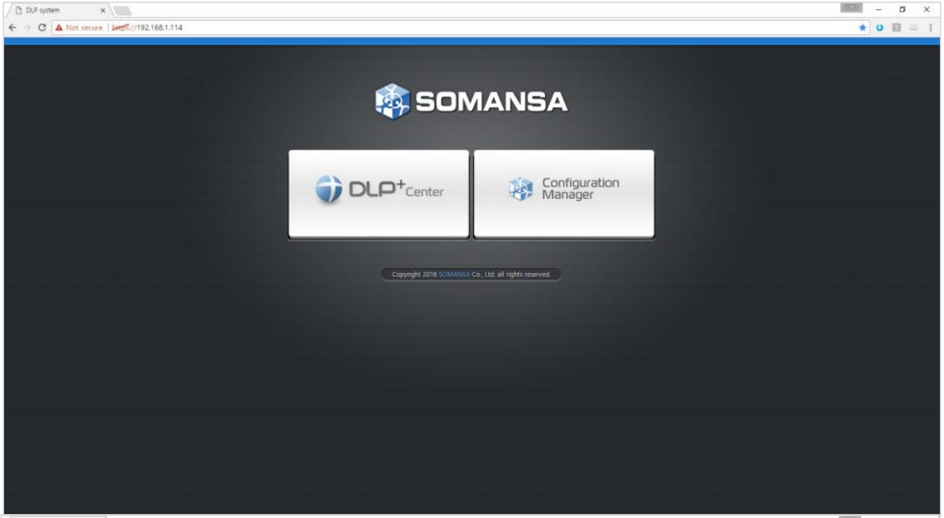
SOMANSA / Mail-i / DLP+Center

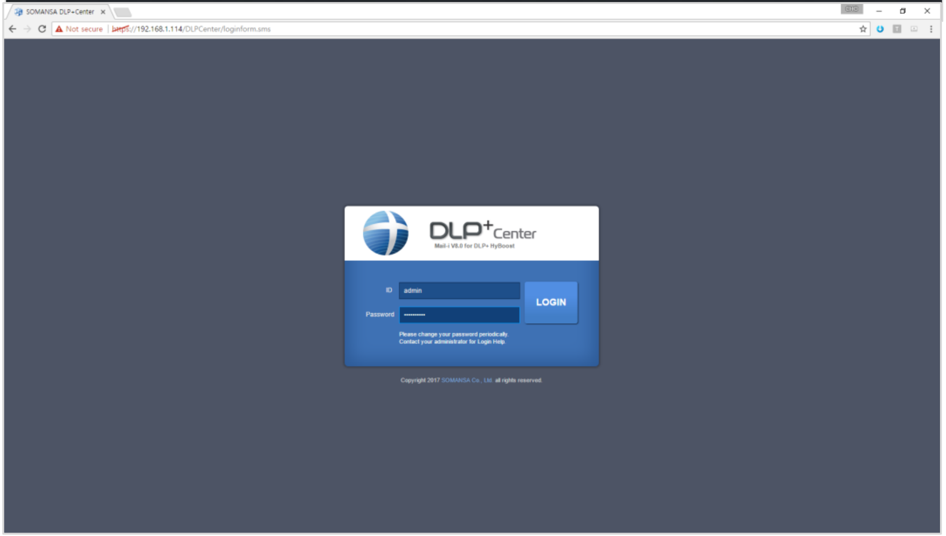
I. DLP+Center Access

1. Access the DLP+Center
   1) Management Console for Mail-i
   2) Enter the **https://IPAddress** in web browser
   3) Click the **DLP+Center**

※ Configuration Manager will be covered in the next section

2. Login
   1) ID/Password can be set-up/changed during the initial setup

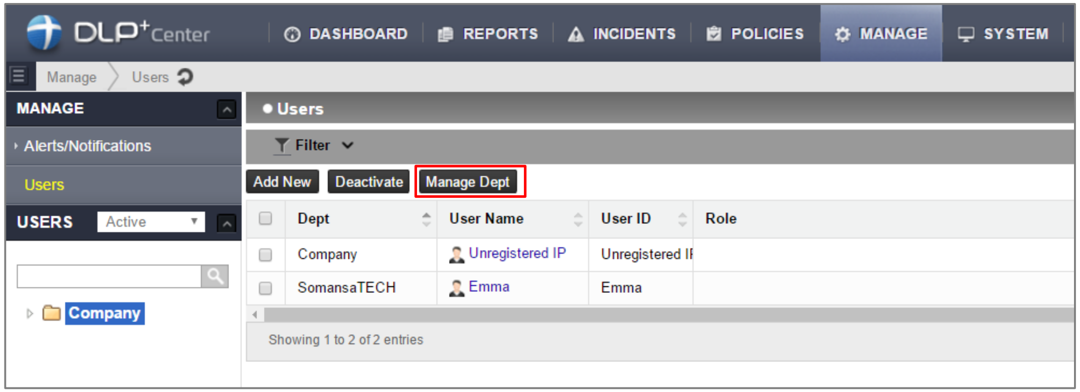




II. Department and Users

1. Add the Department

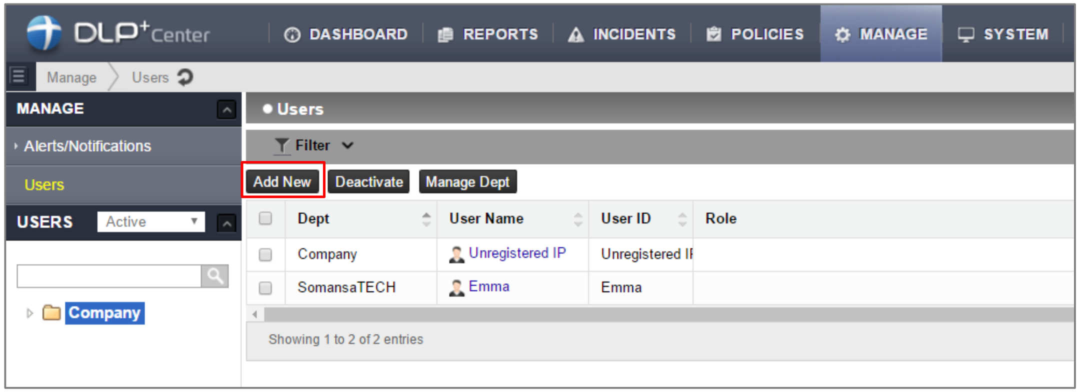
1) Select **MANAGE > Users**
2) Click the **Manage Dept**
3) Click the **Add**
4) Select the upper department as Parent Dept Name, insert the DeptName, and click the **Add**



2. Add the Users

1) Select **MANAGE > Users**
2) Click the **Add New**
3) Insert the User Name, User ID, IP and select Dept, and click **Save**

※ It is available for the same User Name, but duplicating User ID is not allowed. User ID must be unique.)



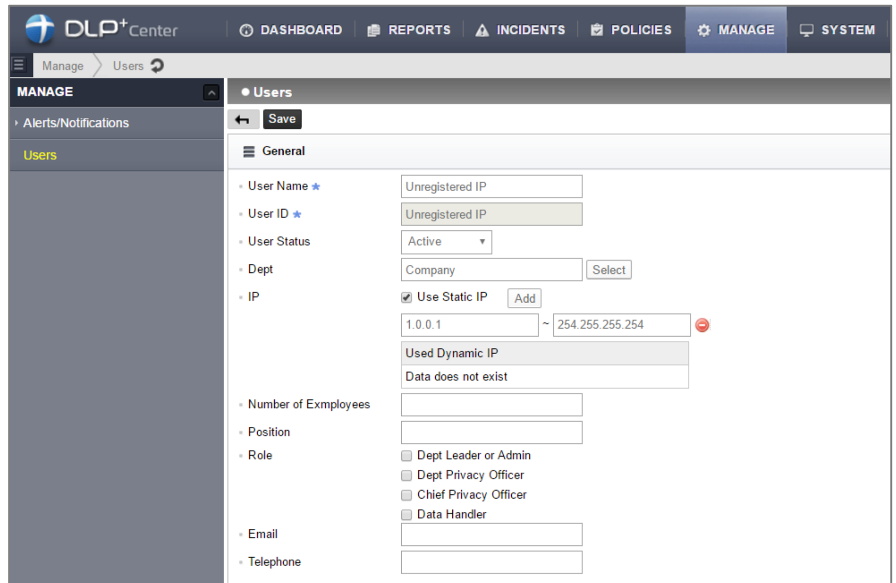
II. Department and Users

3. Add the Users

1) ※ Mail-i creates by users (Unregistered IP) with all IP range. (1.0.0.1~254.255.255.254)

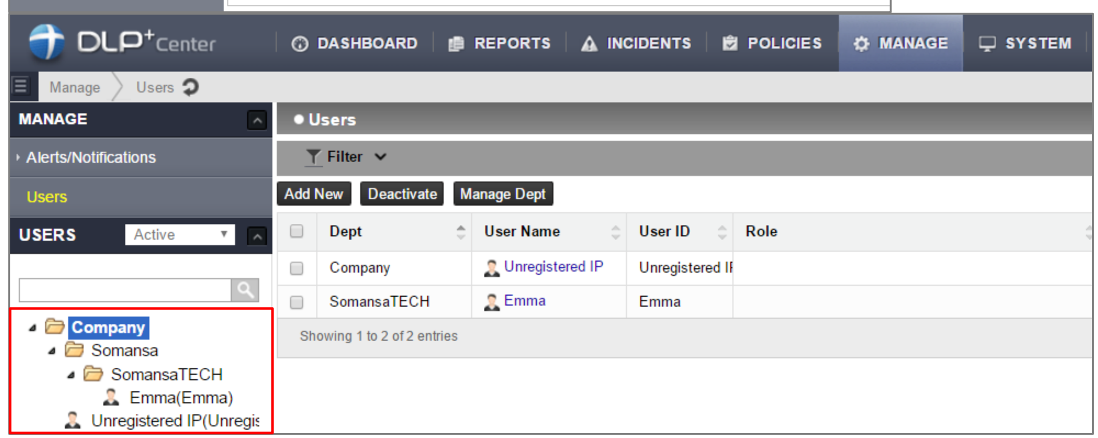
2) ※ Mail-i matches the user based on IP and supports only IPv4

3) ※ IP ranges can also be entered. However, the single IP that is included in the IP range is recognized as a separate user.

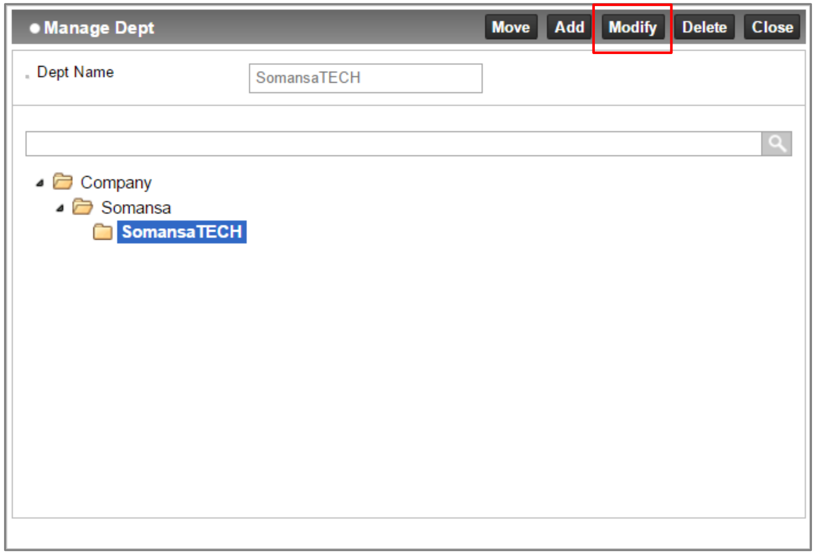


4. Check Department and Users

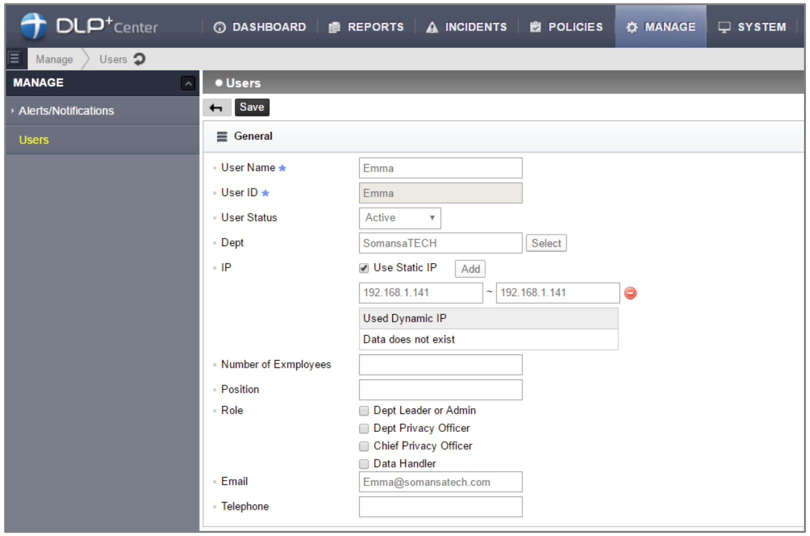
1) Select **MANAGE > Users**



II. Department and Users



5. Modify the Department
    1) Select **MANAGE > Users**
    2) Click the **Manage Dept**
    3) Select the department and enter the department name you want to change. Click **Modify**



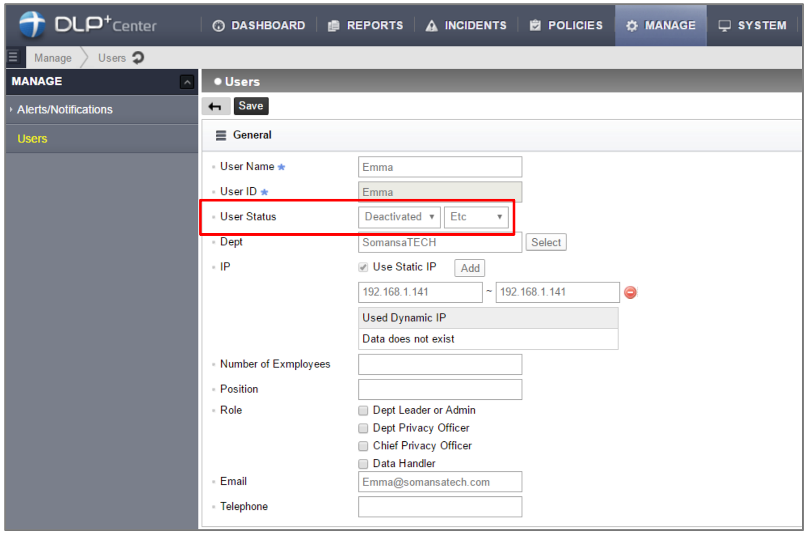
6. Modify the Users
    1) Select **MANAGE > Users**
    2) Click the User Name to change setting
    3) After changes User Dept, ETC, click **Save**

II. Department and Users

7. Deactivate Users

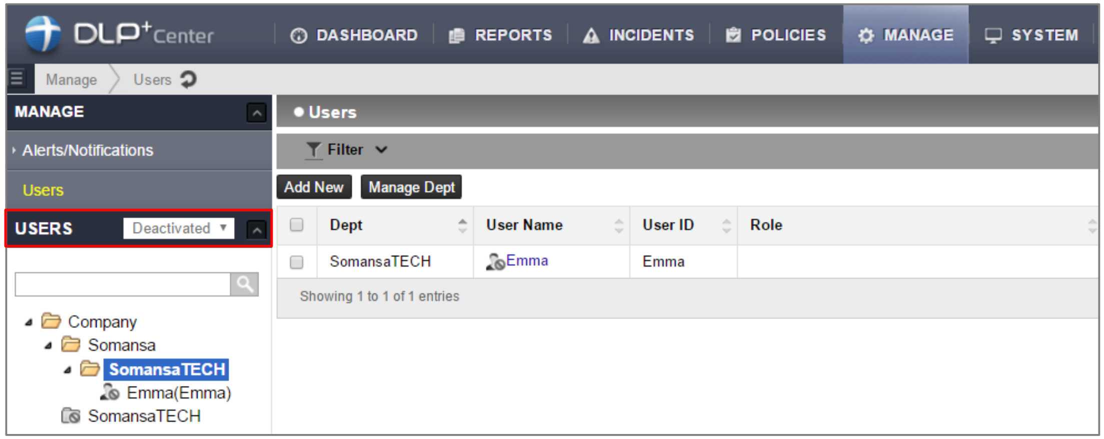
1) Select **MANAGE > Users**
2) Click the User Name you want to disable
3) Select User Status as **Deactivated**
4) Select justification and click **Save**

※ Deactivation is not a deletion. Deactivation only in REPORT of DLP+Center because there are no user`s log.



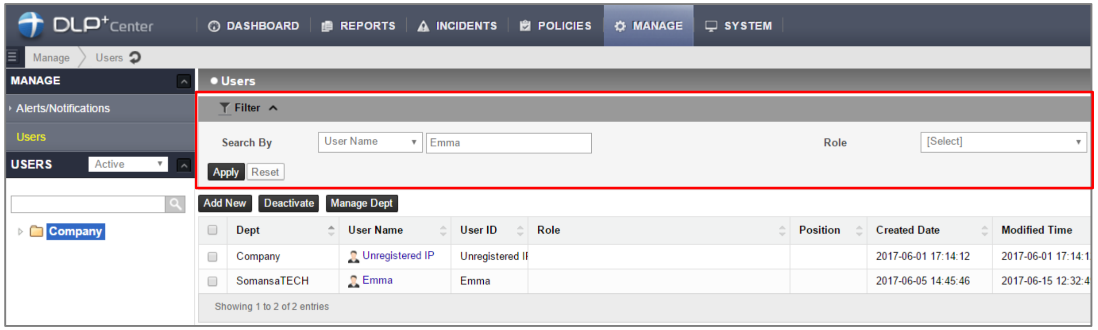
8. Reactivate Deactivated Users

1) Select **MANAGE > Users**
2) Change the USERS to the Deactivate in the left tree.
3) Click the User Name you want to activate
4) Change the User status and Click **Save**



II. Department and Users

9. Apply the Filter
   1) Select **MANAGE > Users**
   2) Expand **Filter** bar
   3) Select condition (UserName, User ID, Dept, User IP) or Role
   4) Click **Apply**



III. POLICIES

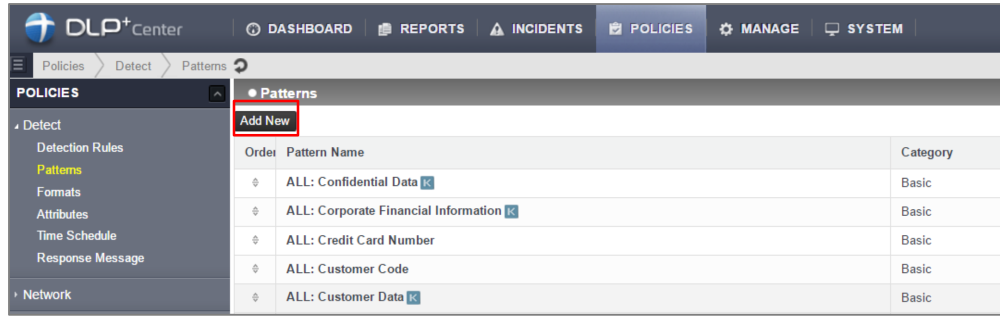
1. Add the Patterns

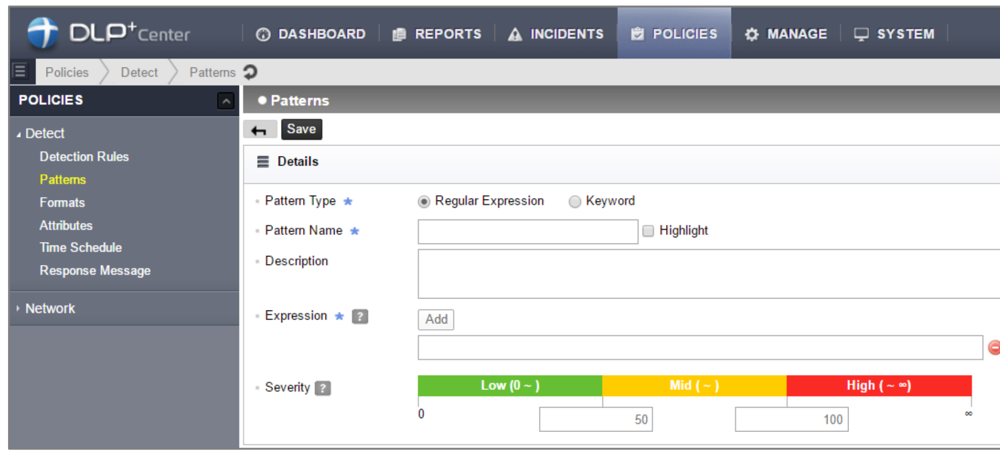
- You can select the basic patterns provided, and create administrator defined patterns.

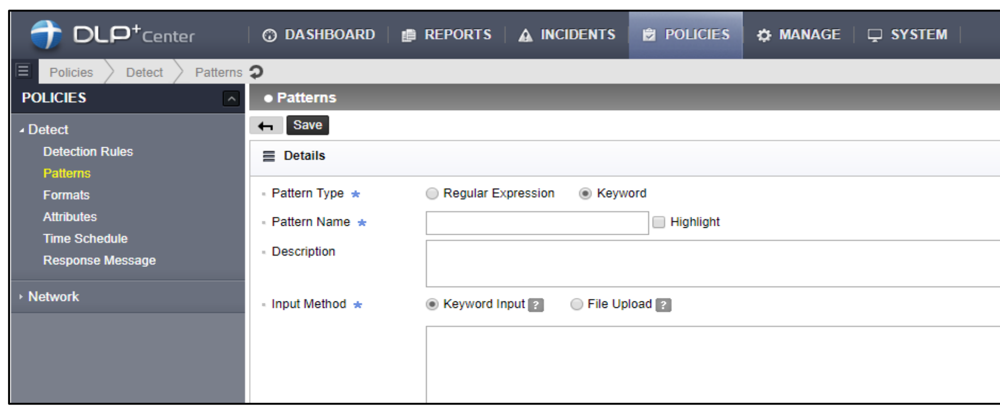
(regular expression and keyword)

1) Select **POLICIES > Detect > Patterns**
2) Click **Add New**
3) Select <u>Pattern Type</u>
4) Insert the <u>Pattern Name</u> and <u>Expression</u> and click **Save**

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







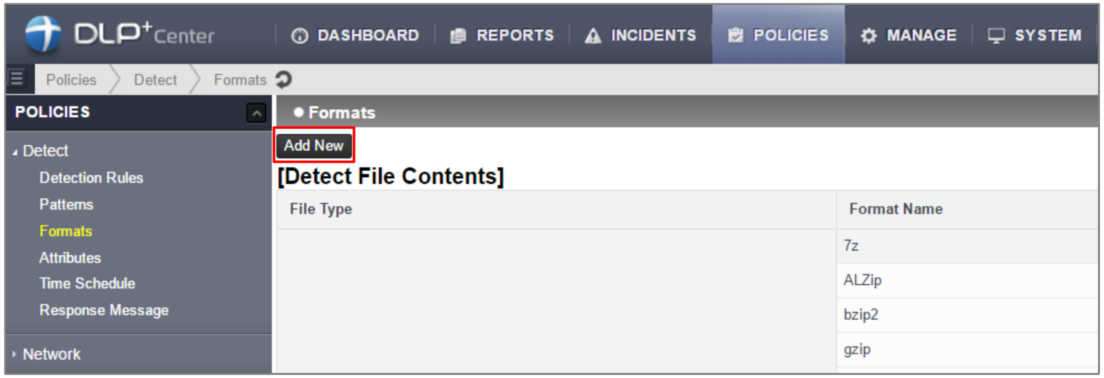
III. POLICIES

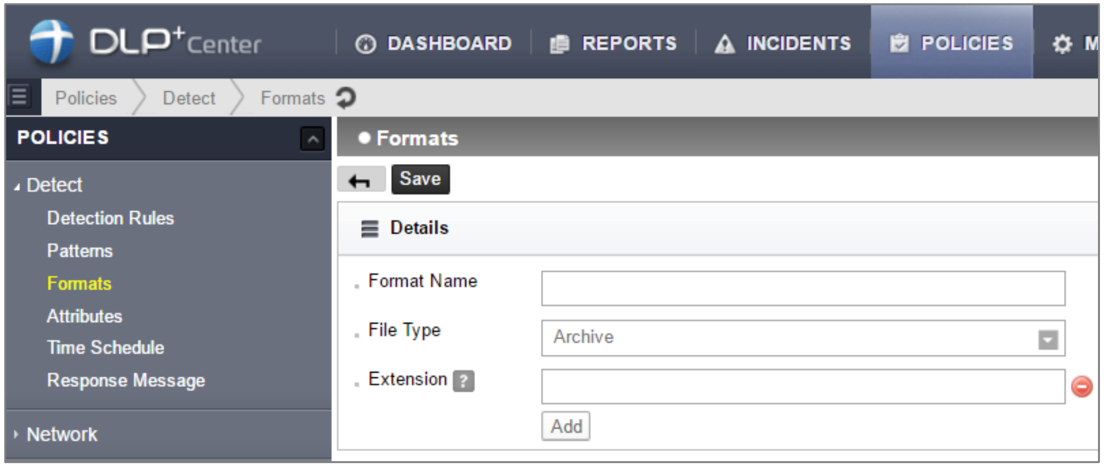
2. Add the Formats

- Select basic formats provided, and create administrator defined format.

1) Select **POLICIES > Detect > Formats**
2) Click **Add New**
3) Insert the Format Name and Expression , select the File Type, and click **Save**

※ User-defined formats can not be analyzed for content

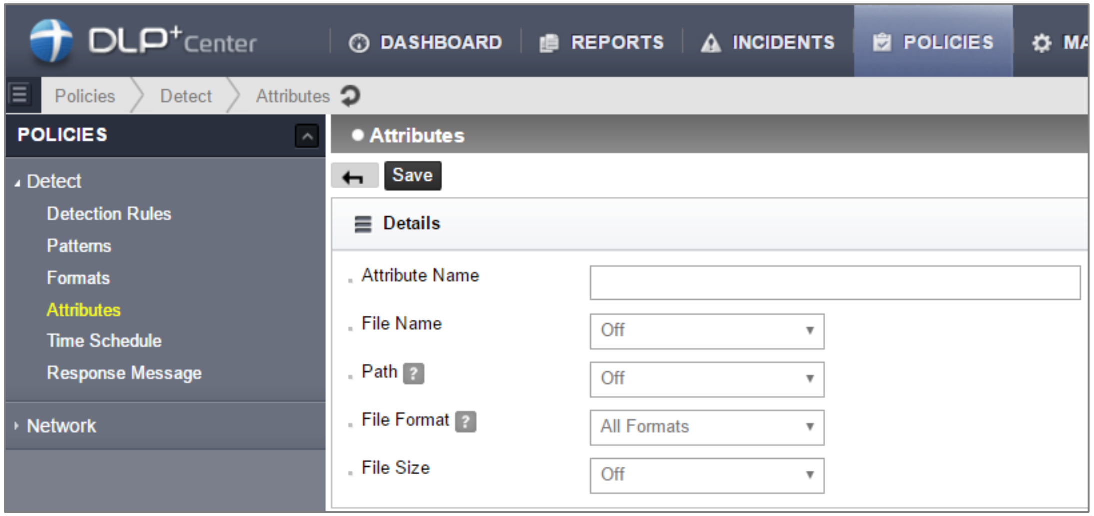




III. POLICIES

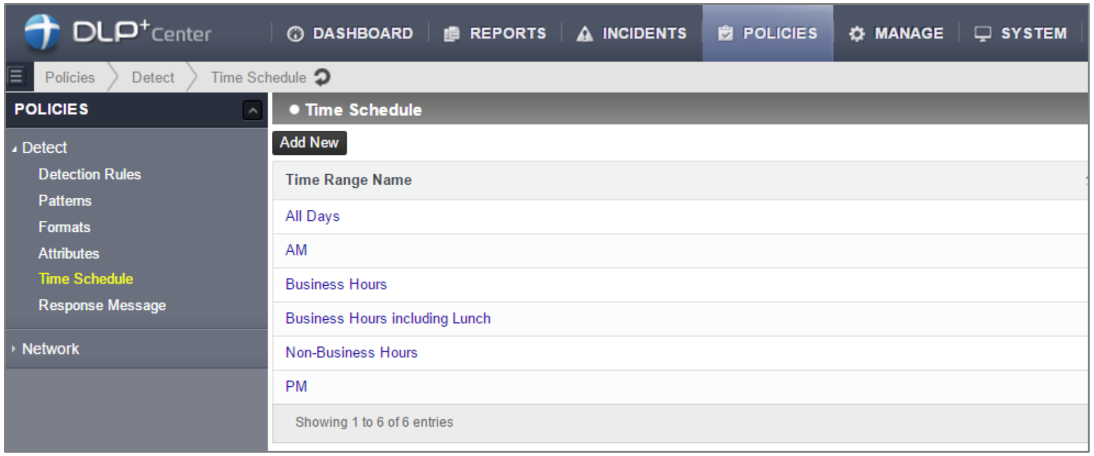
3. Add the Attributes
   - The file format is now used in Attributes

   1) Select **POLICIES > Detect > Attributes**
   2) Click **Add New**
   3) Insert the <u>Attribute Name</u> and select <u>File Name,</u> <u>Path,</u> <u>File Format,</u> <u>File Size</u> and click **Save**



4. Add Time Schedule
   1) Select **POLICIES > Detect > Time Schedule**
   2) Click **Add New**
   3) Insert the <u>Time Range Name</u> and select Setting and click **Save**

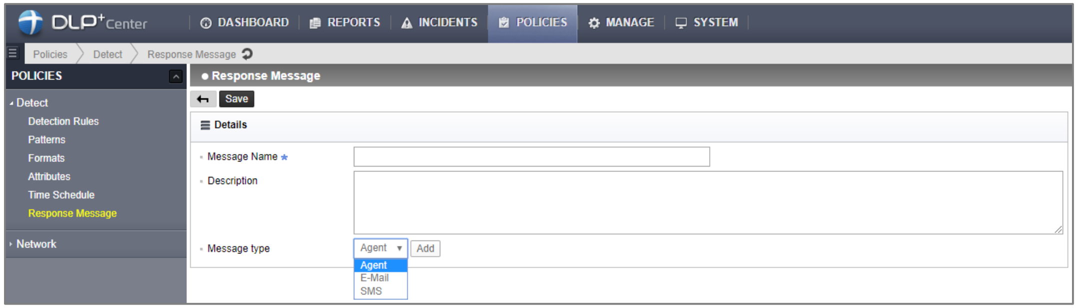
   * It will be used in **Net App Prevent+.**



III. POLICIES

5. Response Message is an advanced option

※ Message can be delivered according to policy (based on Agent, E-mail, SMS)



III. POLICIES

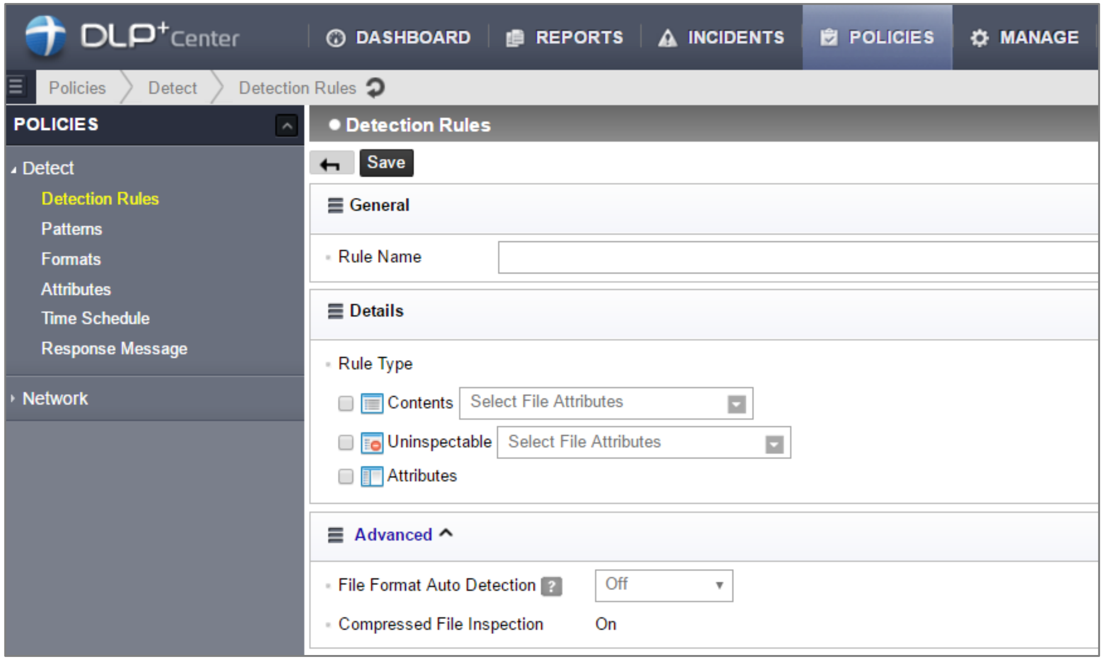
6. Add the Detection Rules

- The Patterns and Attributes are used in Detection Rules

1) Select **POLICIES > Detect > Detection Rules**
2) Click **Add New**
3) Insert the Rule Name
4) Check the Rule Type, select the File Attributes
5) Select Patterns and set the sub properties
6) Click **Add**
7) Select File Format Auto Detection
8) Click **Save**

※ Detection Rules is used in Prevent of Net Apps Prevent+

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



III. POLICIES

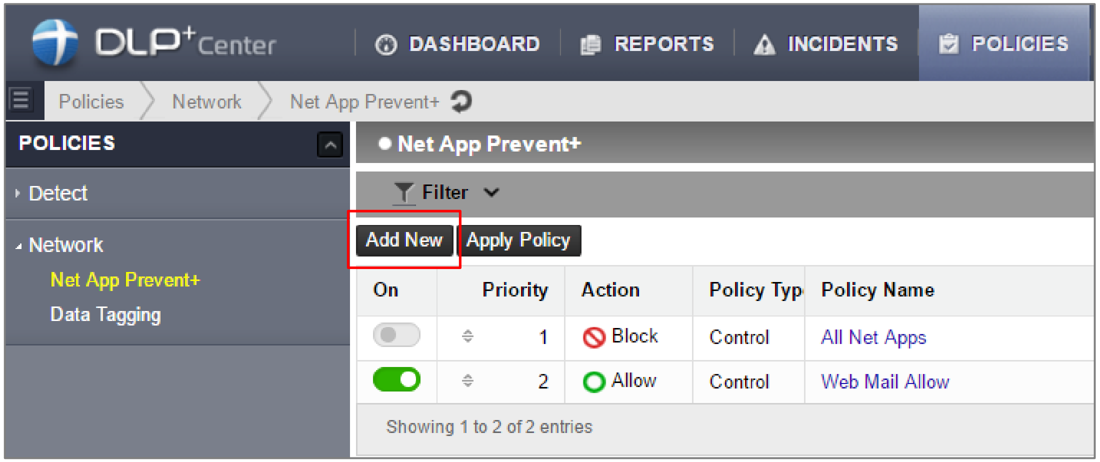
7. Add the Net App Prevent+

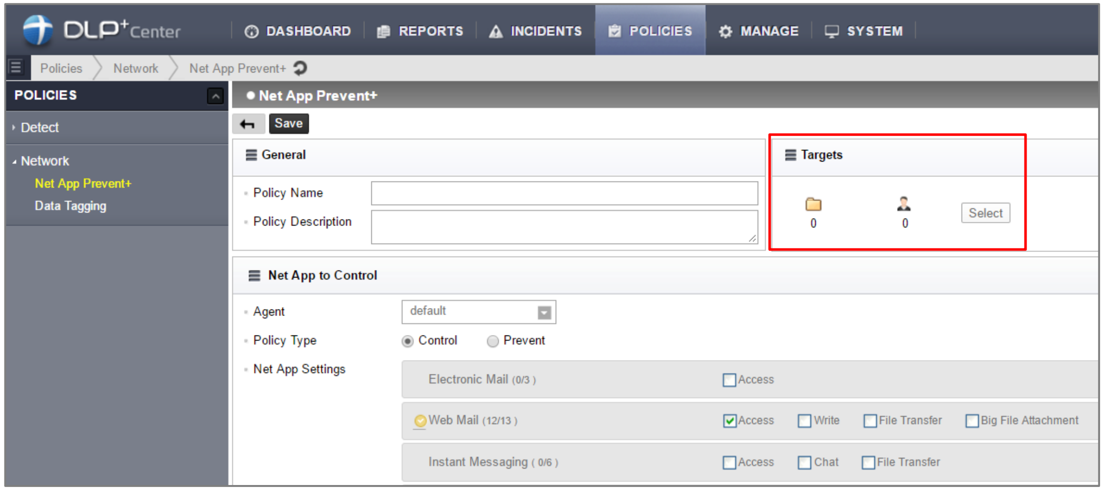
- There are two types of policies. First, The 'Net App Prevent+' policy for prevention and acceptance.

1) Select **POLICIES > Network > Net App Prevent+**
2) Enter **Add New**
3) Insert the <u>Policy Name</u> and select the <u>Targets</u>
4) Select the <u>Agent</u>

※ If multiple agents exist, you can apply the policy to specific agents

※ By default, the application that you activate in the Configure Manager is allowed and logged





III. POLICIES

7.1 Add the Control of Net App Prevent+

- There are two types of Net App Prevent+. First, The ‘Control’ policy for prevention and acceptance. ‘Control’ allows and blocks applications without detection.

a) Check the Control of Policy Type

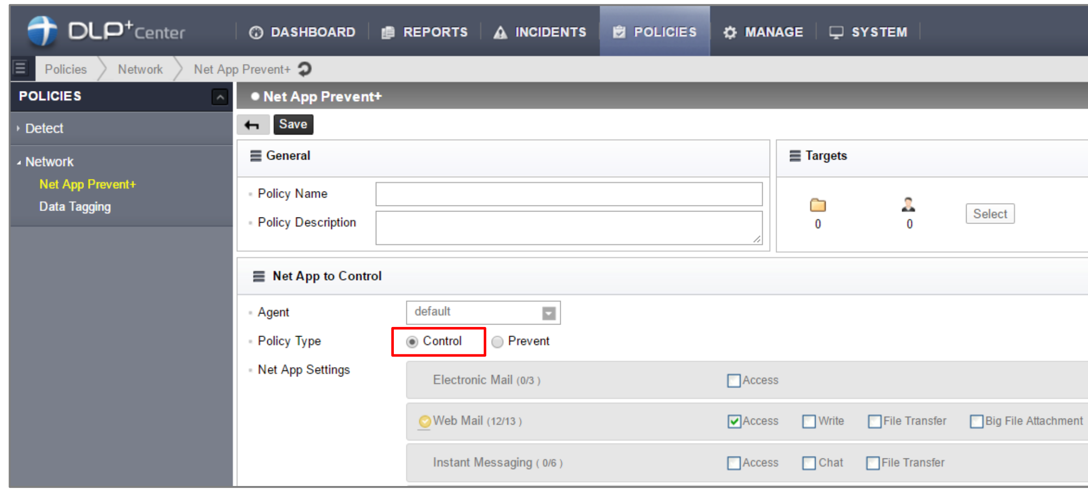
b) Select Net App Settings

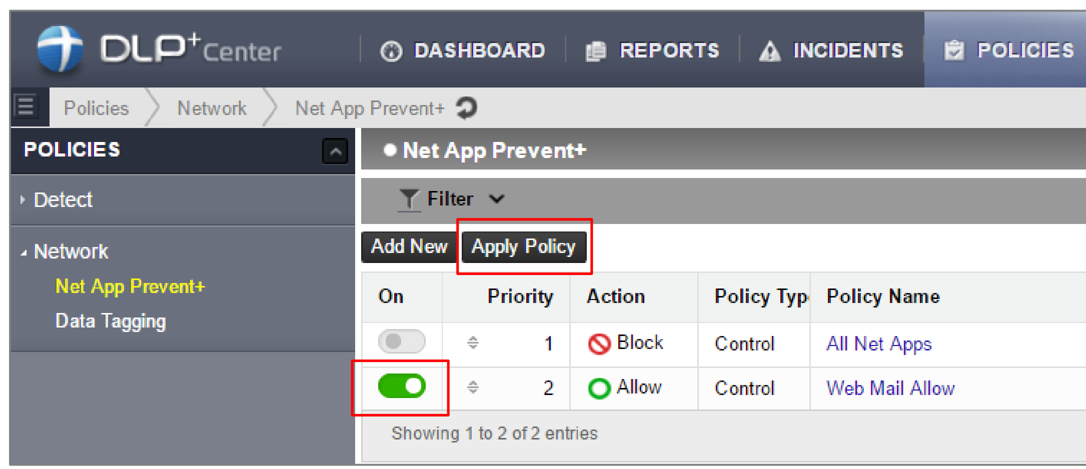
c) Select Time Range settings and Action

d) Click **Save**

e) If you want to apply for policy, you must active and click the **Apply Policy**

※ You can prioritize policies.





III. POLICIES

7.2 Add the Prevent of Net App Prevent+

• There are two types of Net app Prevent+. Second, The 'Prevent' policy can be set by the detection rule.

a) Check the Prevent of Policy Type

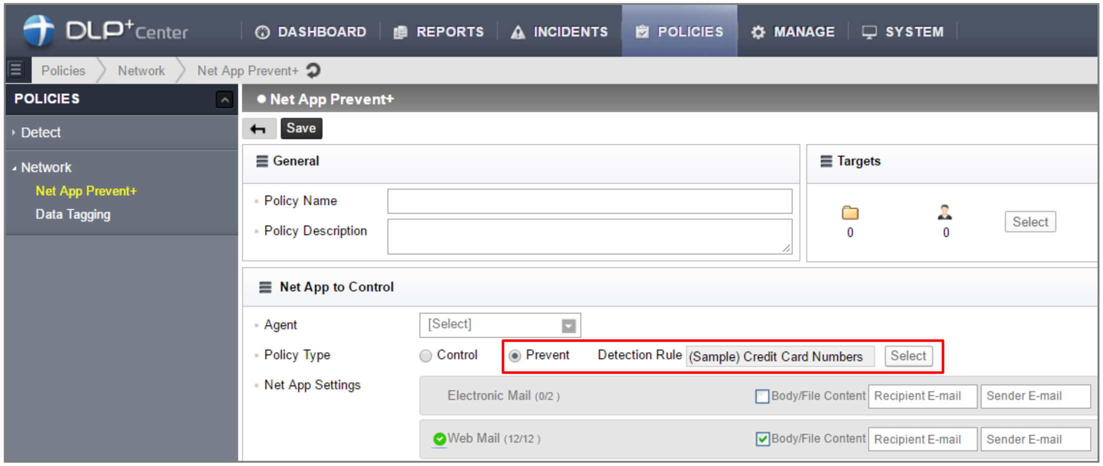
b) Select Net App Settings and Detection Rule

c) Select Time Range settings and Action

d) Click **Save**

e) If you want to apply for policy, you must active and click the **Apply Policy**

※ You can prioritize policies.



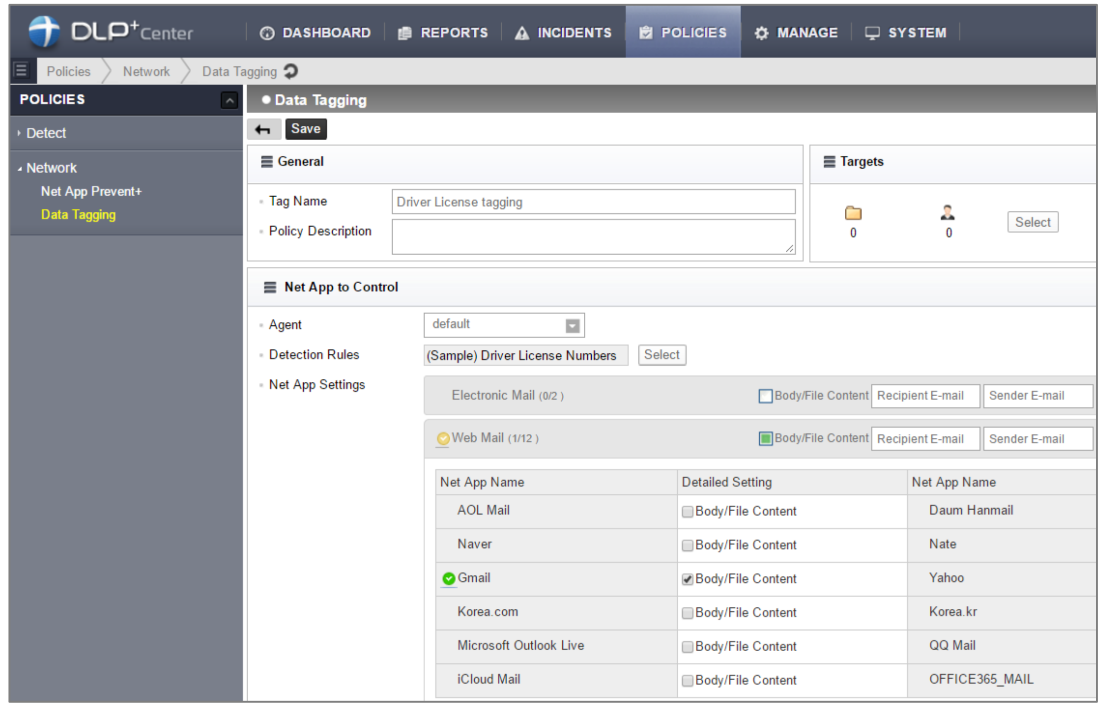
III. POLICIES

8. Add the Data Tagging

- Attach tagging to logs by detection rules.

1) Select **POLICIES > Network > Data Tagging**
2) Enter **Add New**
3) Insert the Tag Name and select the Targets
4) Select the Agent and Detection Rules
5) Select the Net App Settings
6) Select the Time Range Settings
7) Click **Save**

8) If you want to apply for policy, you must active and click the **Apply Policy**



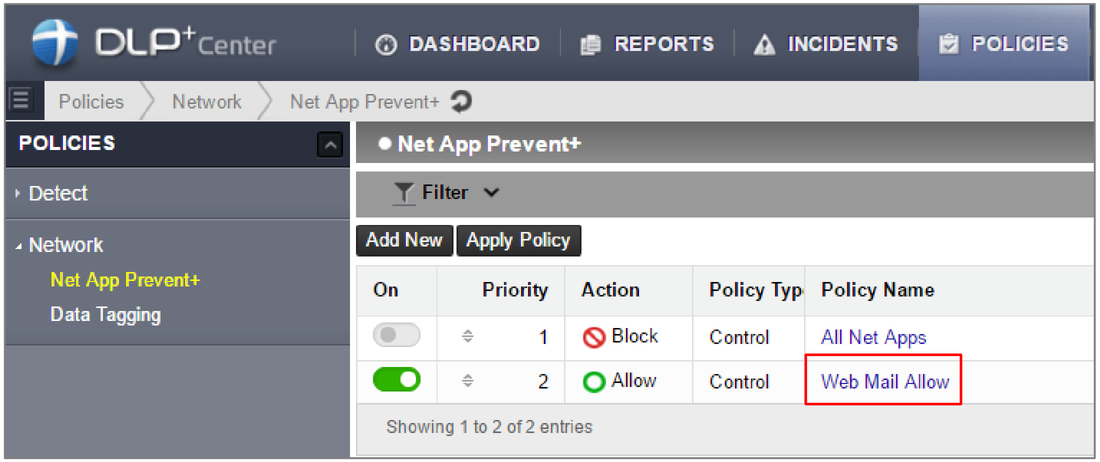
III. POLICIES

9. Modify the Policies

- POLICIES > Detect and Network common

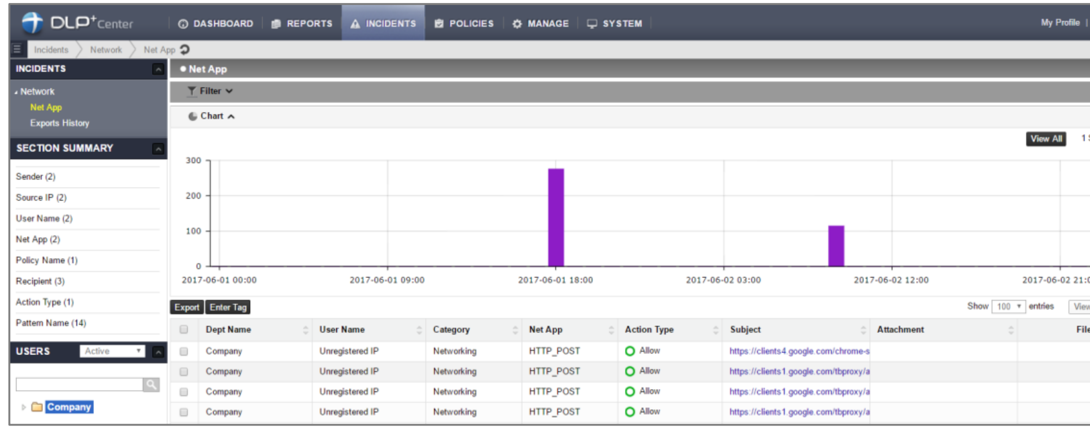
1) Click the policy name that you want to change
2) Modify configure
3) Click the **Save**

4) If you want to apply for policy, you must active and click the **Apply Policy**



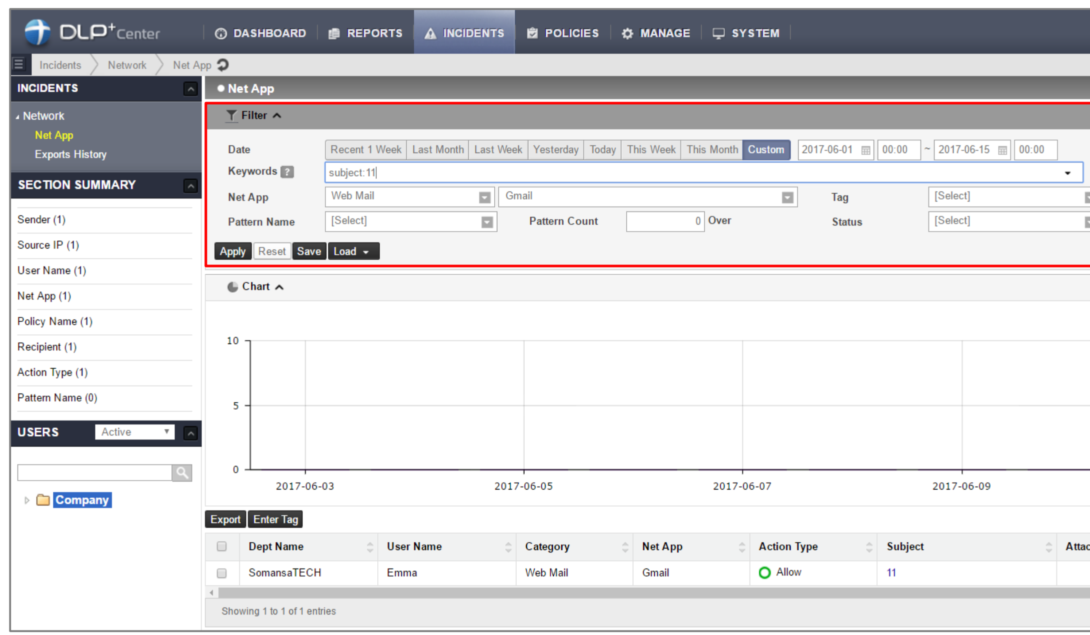
IV. INCIDENTS

1. Check the Logs
   1) Select **INCIDENTS > Network > Net App**



2. Apply the Filter
   1) Select **MANAGE > Users**
   2) Click **Filter**
   3) Select condition(Net App, Tag, Pattern Name, Pattern Count, Status) that you want to filter and Insert Keywords
   4) Click **Apply**

   ※ When searching based on Keyword, you can also search for the contents of the file body. Only possible when file analysis is completed.



IV. INCIDENTS

3. View Log Details

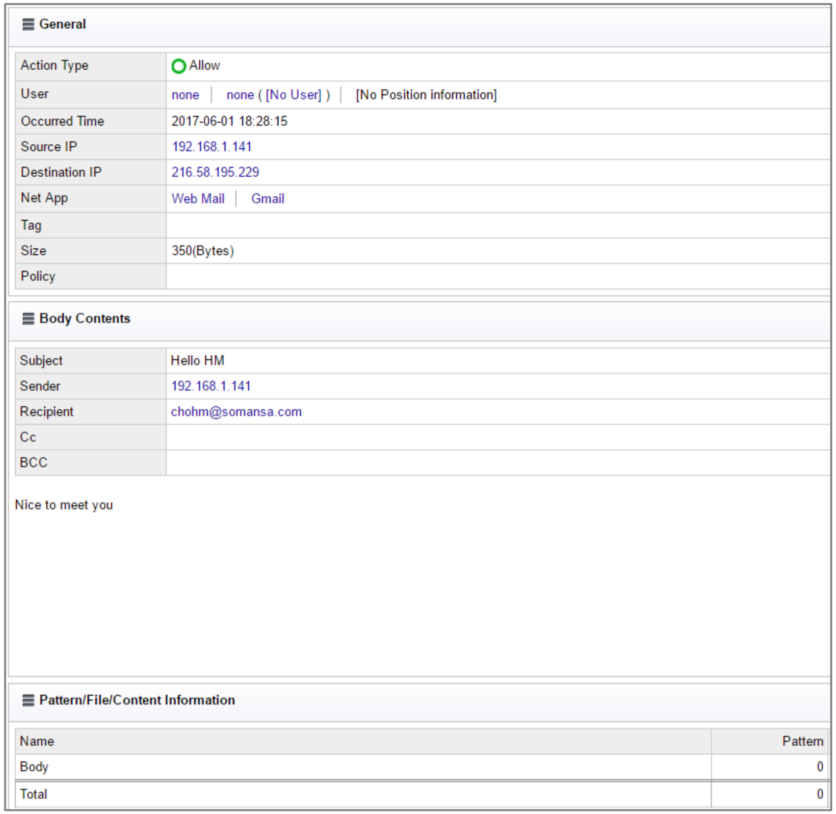
1) Select **INCIDENTS > Net App**
2) Click the log to view details

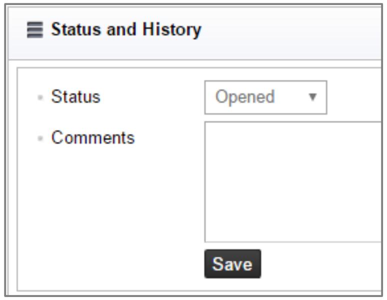
• You can check general information (user information, source/destination IP, policy, ETC). Click on the hyperlink in general information to view the logs filtered under that condition.

• You can download a copy for attachment files.

• You can set the status and add some comments in order to manage the log.

a. Check Status and History
b. Select the Status
c. Enter the Comments and click **Save**



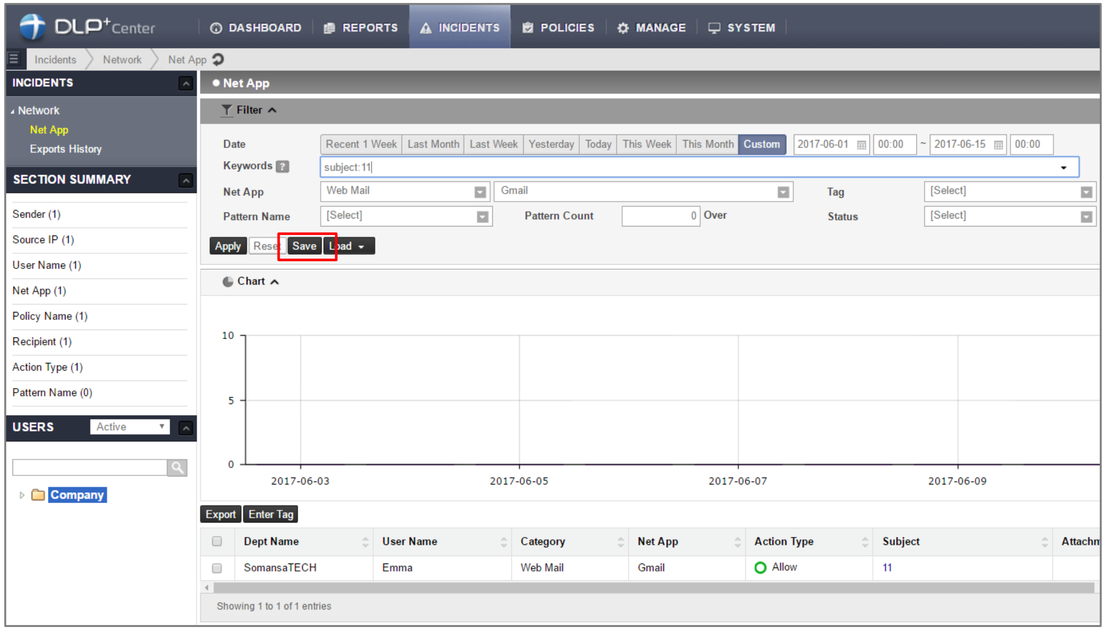


IV. INCIDENTS

4. Save the Filter

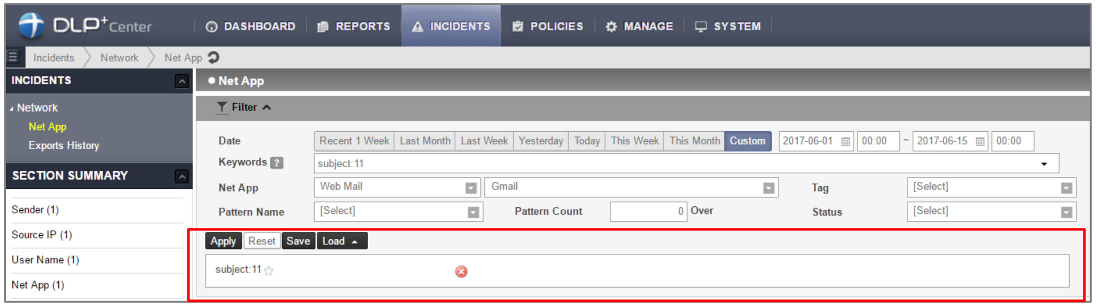
- You can save frequently used filters.

1) Select **INCIDENTS > Network > Net App**
2) Click **Filter**
3) Select the conditions that you use frequently or Insert keywords
4) Click **Save**
5) Insert the Filter Name and Click **Save**



5. Load the Filter

1) Select **INCIDENTS > Network > Net App**
2) Click **Load** and select the saved Filter
3) Click **Apply**



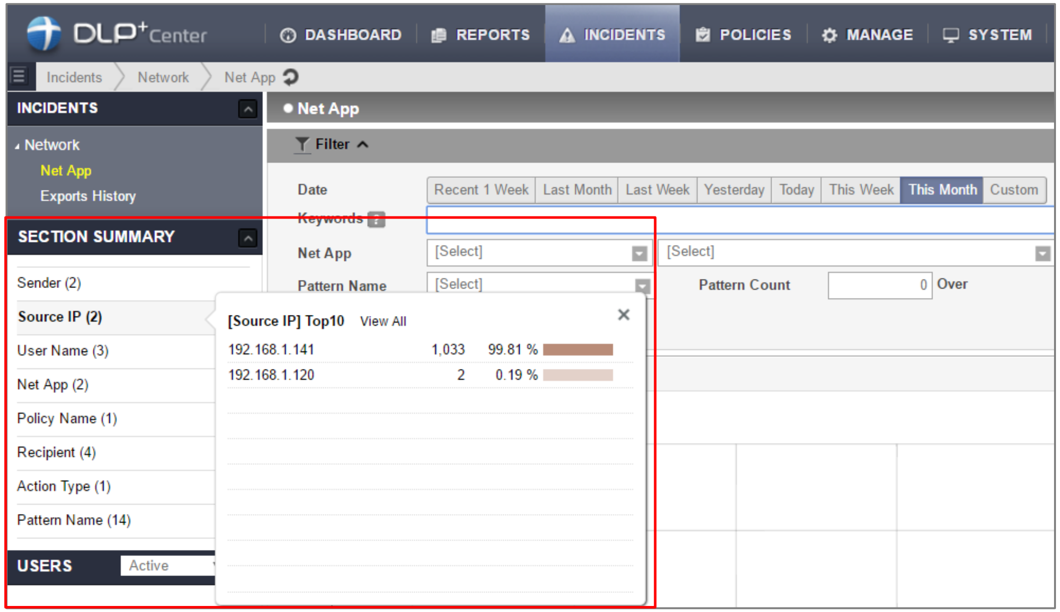
IV. INCIDENTS

6. Section Summary

- Quickly search for top 10 Incidents

1) Select **INCIDENTS > Network > Net App**
2) Mouse over the search condition in left <u>SECTION SUMMARY</u>
3) Click the condition that you want to view

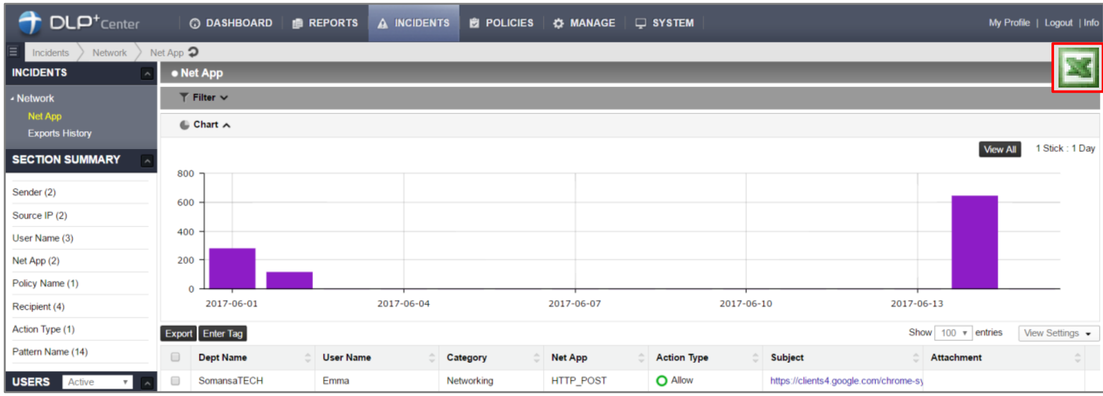
※ This search will continue to be filtered to suit the condition whenever you click the condition



7. Export the Logs (format .csv)

1) Select **INCIDENTS > Network > Net App**
2) Apply <u>Filter</u> the log to export
3) Click the **Excel button** in upper right
4) Select the <u>Body Contents</u> and click **Save**
5) Select where to save and click **Save**

Sample.csv



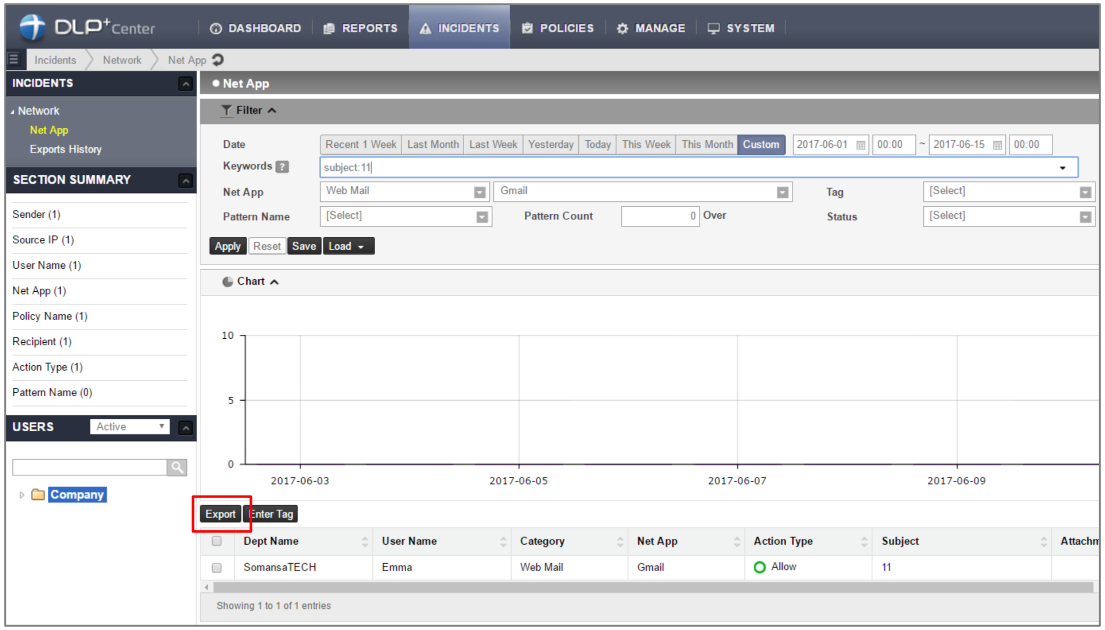
SOMANSA

IV. INCIDENTS

8. Export the Log (format .html)

- You can also export a copy of the attachment.

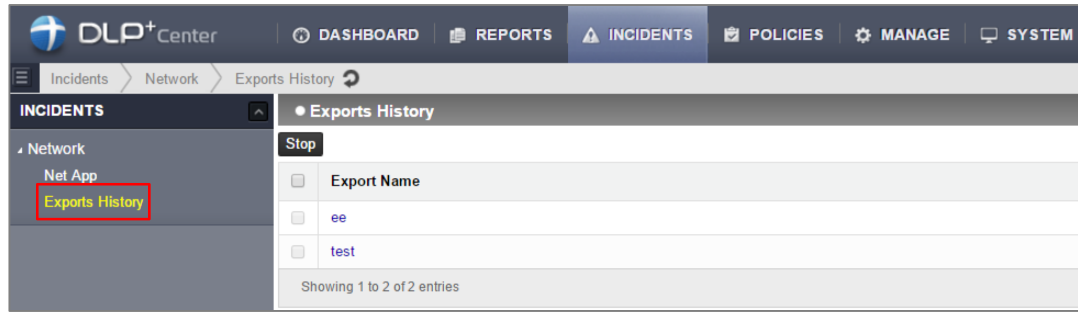
1) Select **INCIDENTS > Network > Net App**
2) Apply Filter the log to export
3) Click **Export**
4) Insert the Export Name and select Export Logs, Attachment, Log Count in One File and Fields
5) Click **Save**
6) Click **Ok**

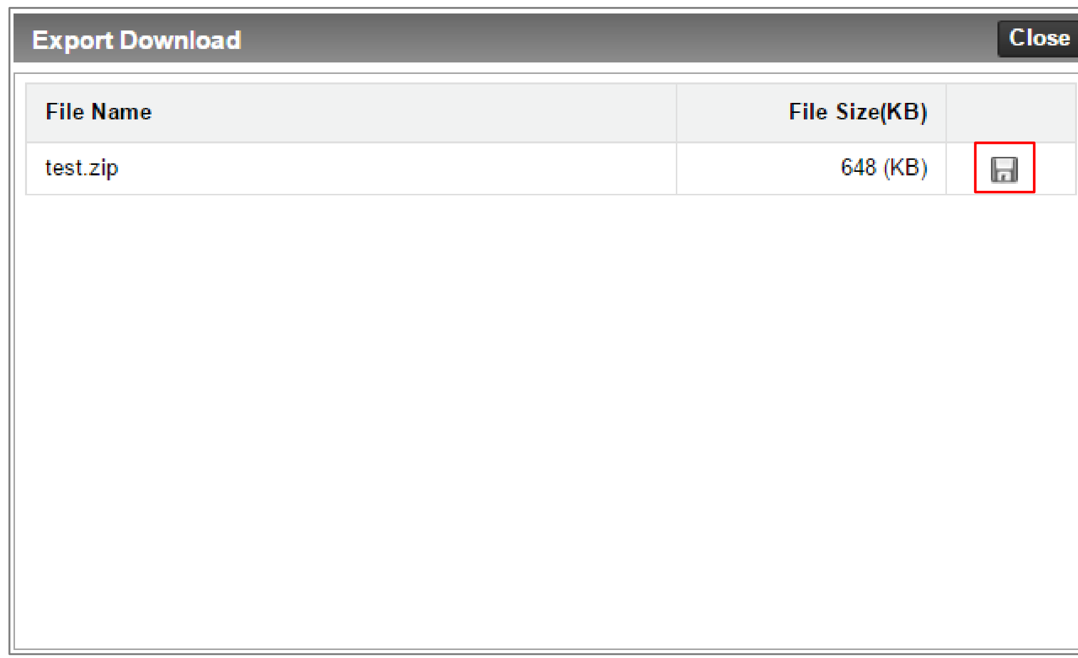


IV. INCIDENTS

9. Check the Exports History
   - To download the export log, proceed as follows

1) Select **INCIDENTS > Network > Exports History**
2) Click Export Name
3) Click the Download button
4) Select where to save and click **Save**





Sample.zip

IV. INCIDENTS

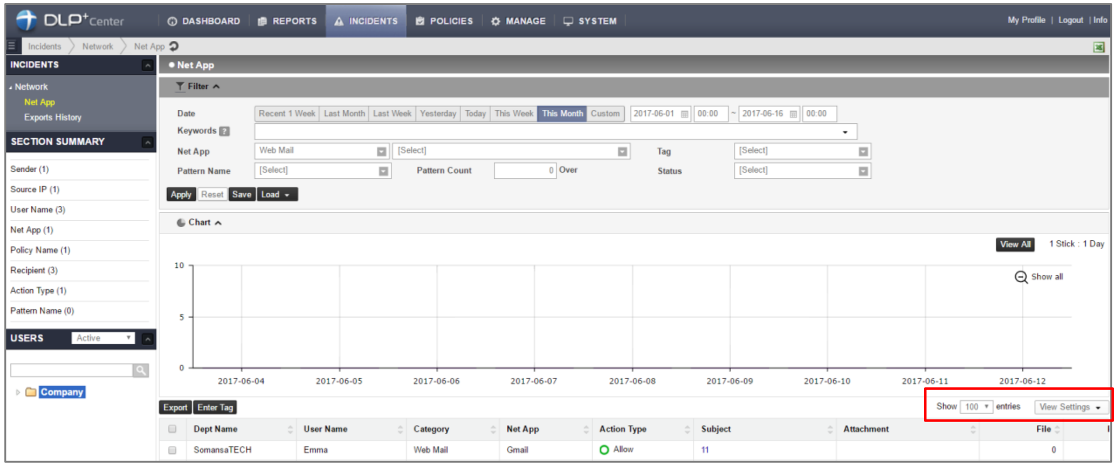
10. Log View Options

- You can set the number of log shown on one page.

1) Select **INCIDENTS > Net App**
2) Change the number next to <u>Show</u> on the right

- You can select the column to show in the log and change the order

1) Select **INCIDENTS > Net App**
2) Click **View Settings**
3) Only check the column to show
4) Change the <u>order</u> you want and click **Save**

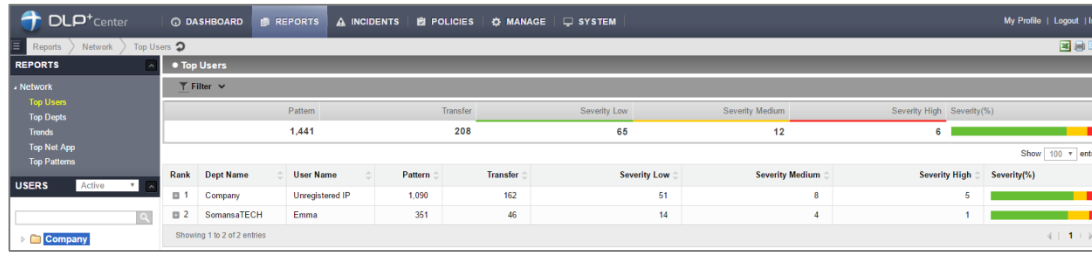


V. REPORTS

1. Check the Reports

- Provide reports on a variety of criteria (Users, Depts, Trends, Net App, Patterns)

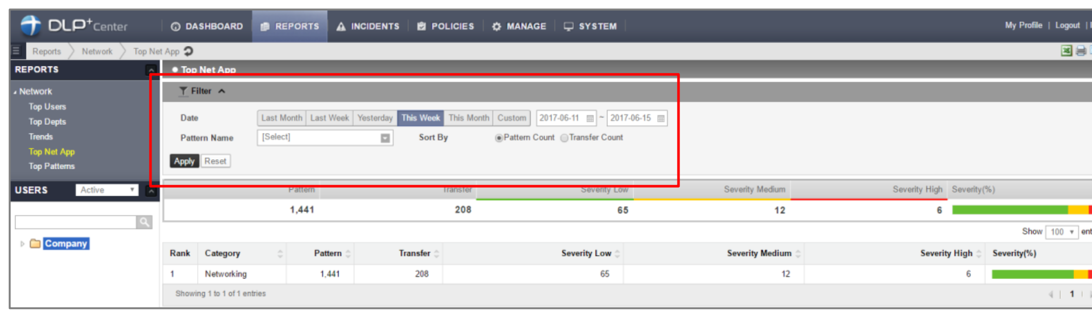
1) Select **REPORTS > Network**
2) Select the report criteria you want in the left tree



2. Apply the Filter

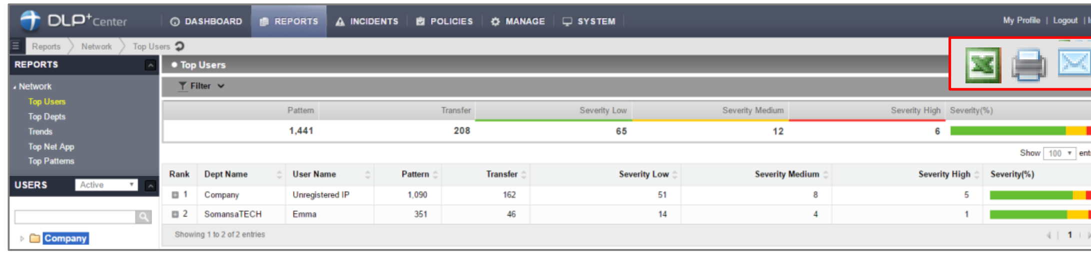
1) Select **REPORTS > Network**
2) Select the report criteria you want in the left tree
3) Click <u>Filter</u>
4) Select <u>condition</u>(Date, Pattern Name, ETC) that you want to filter
5) Click **Apply**

- If you click the dept or user in the left tree, you can see the report for that condition

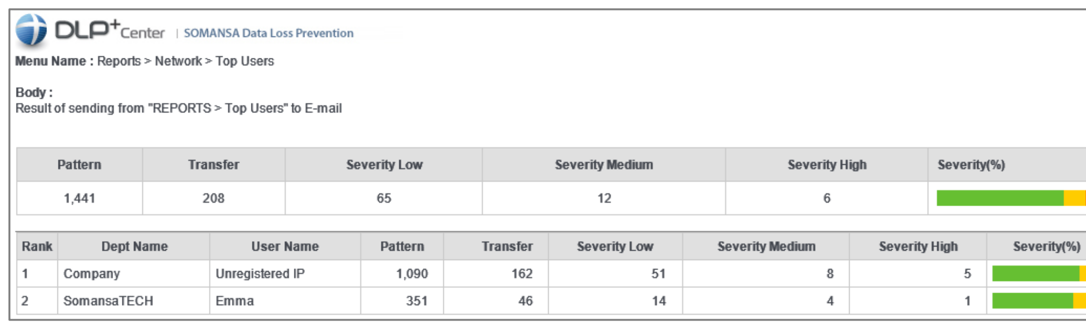


V. REPORTS

3. Export the Report (format .cvs, Print and E-mail)
   1) Select **INCIDENTS > Net App**
   2) Select the report criteria you want in the left tree
   3) Click Filter
   4) Select condition(Date, Pattern Name, ETC) that you want to filter
   5) Select **desired export option**



For sample : E-mail



DLP+Center | SOMANSA Data Loss Prevention

Menu Name : Reports > Network > Top Users

Body :
Result of sending from "REPORTS > Top Users" to E-mail

Pattern	Transfer	Severity Low	Severity Medium	Severity High	Severity(%)
1,441	208	65	12	6	

Rank	Dept Name	User Name	Pattern	Transfer	Severity Low	Severity Medium	Severity High	Severity(%)
1	Company	Unregistered IP	1,090	162	51	8	5	
2	SomansaTECH	Emma	351	46	14	4	1	

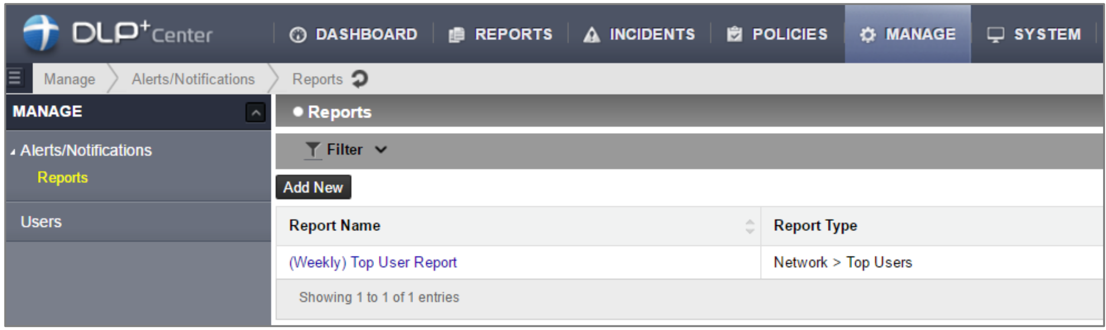
VI. Alerts/Notifications

1. Report

- Send email alerts/notification reports one-time or schedule periodically

1) Select **Alters/Notifications > Reports**
2) Click **Add New**
3) Insert the Report Name
4) Configure Report Settings, Notification Settings and Schedule
5) Click **Save**
6) Email can be checked according to schedule setting

※ To use this feature, SMTP in CM must be configured and the user information must have an e-mail address. User setting may also be required.

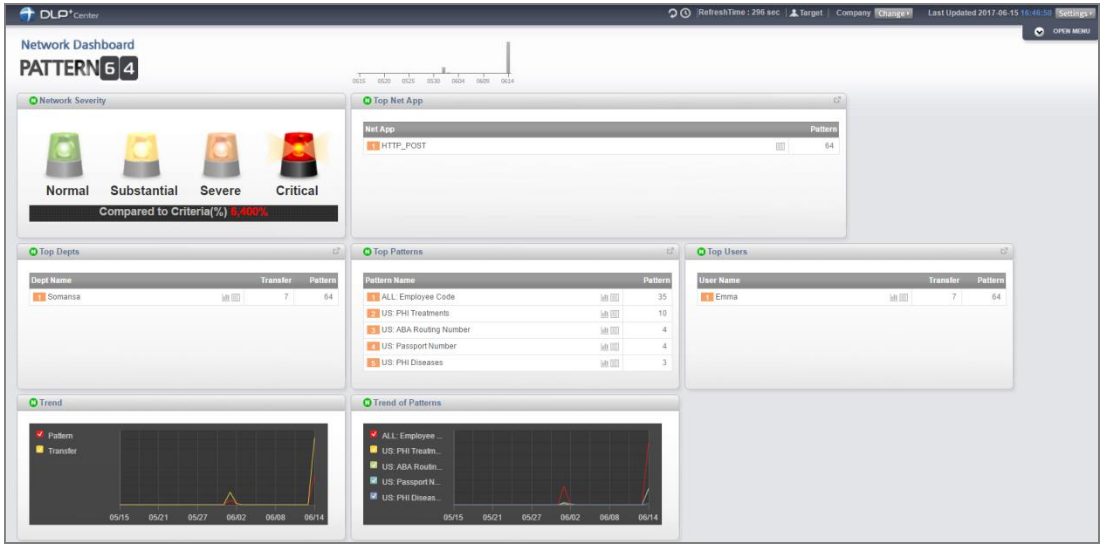


VII. Dashboard

1. Settings

- Sets the patterns and components to activate on the dashboard

1) Select **Dashboard > Settings**
2) Enter the <u>Update Cycle</u>, select the <u>Patterns</u> and <u>Components</u>
3) <u>Components</u> can be reordered using the cross-shaped buttons and detailed settings can be made by clicking the down arrow
4) Click **Apply**



2. Dashboard

1) Select **Dashboard > Network**

- It is possible to change the status for the user and department.

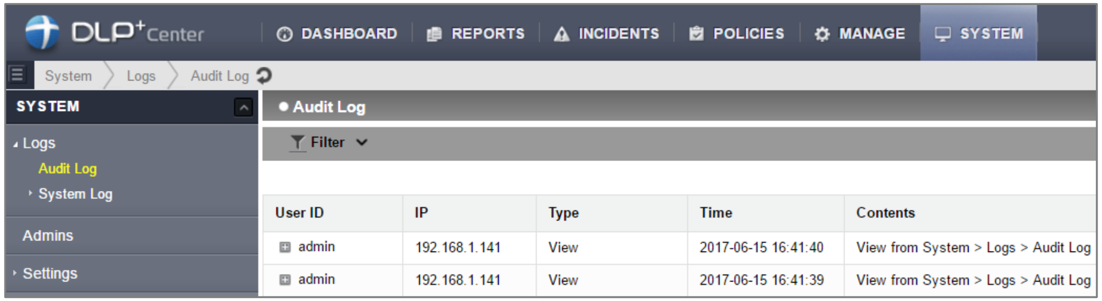
1) Click the **Change** at the top
2) Click the desired <u>user or department</u>
3) Click **Apply**

VIII. System

1. Audit Log

- The administrator’s actions are recorded in the DLP+Center.
- Mail-i provide various options in audit log

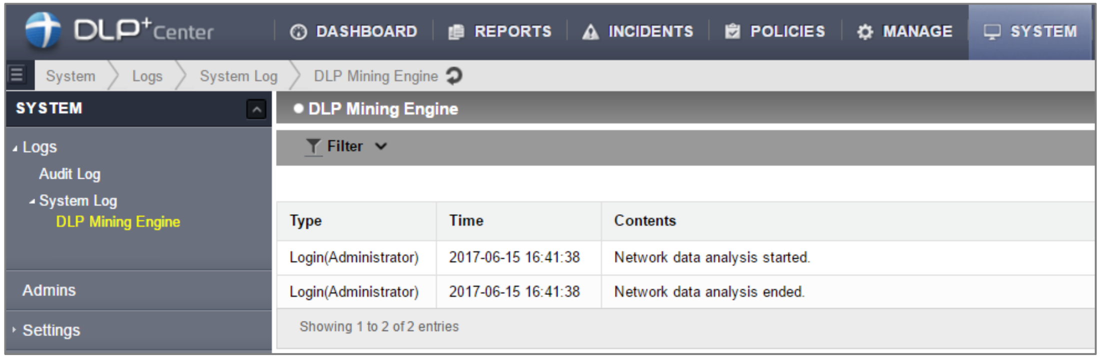
1) Select **SYSTEM > Audit Log**



2. DLP Mining Engine

- You can check the log of data analysis status.

1) Select **SYSTEM > System Log > DLP Mining Engine**



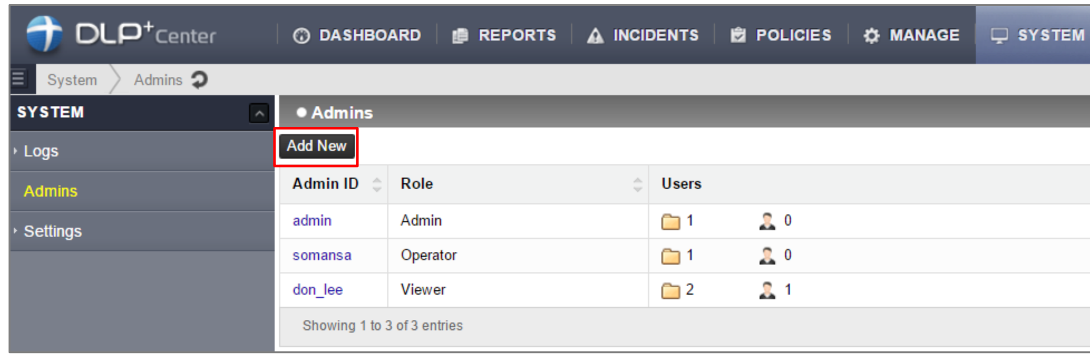
VIII. System

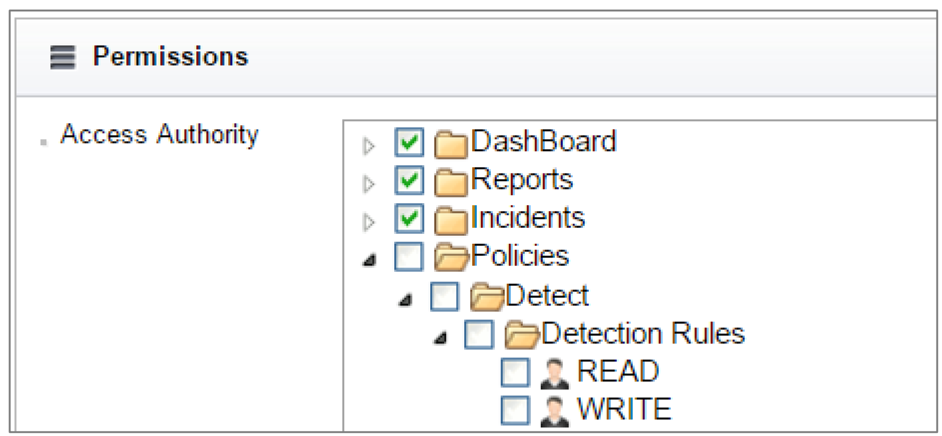
4. Add the Admin

• Create an administrator for DLP+Center. Various rights can be set.

1) Select **SYSTEM > Admins**
2) Click **Add New**
3) Insert General and select Details
4) Select the department to be managed by the manager and Select Management details
5) Select Role and click **OK.** By default, there is a Role provided, but you can customize.
6) Click **Save**

※ The permission setting must be confirmed by sub setting. For example, **Policies > Detect > Detection Rules** has READ and WRITE two permission.





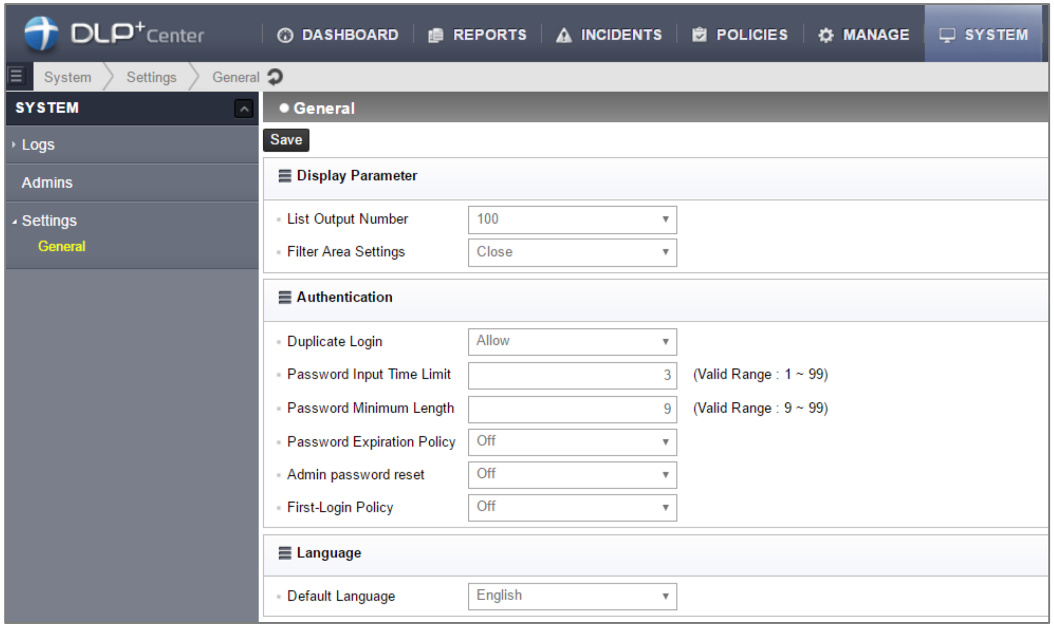
VIII. System

5. General

- Menu to set basic settings for DLP+Center.

1) Select **SYSTEM > Settings > General**
2) Select Display Parameter, Authentication and Language.
3) Click **Save**

※ It is not recommended that multiple users modify the policy with one ID.



SOMANSA

www.somansatech.com