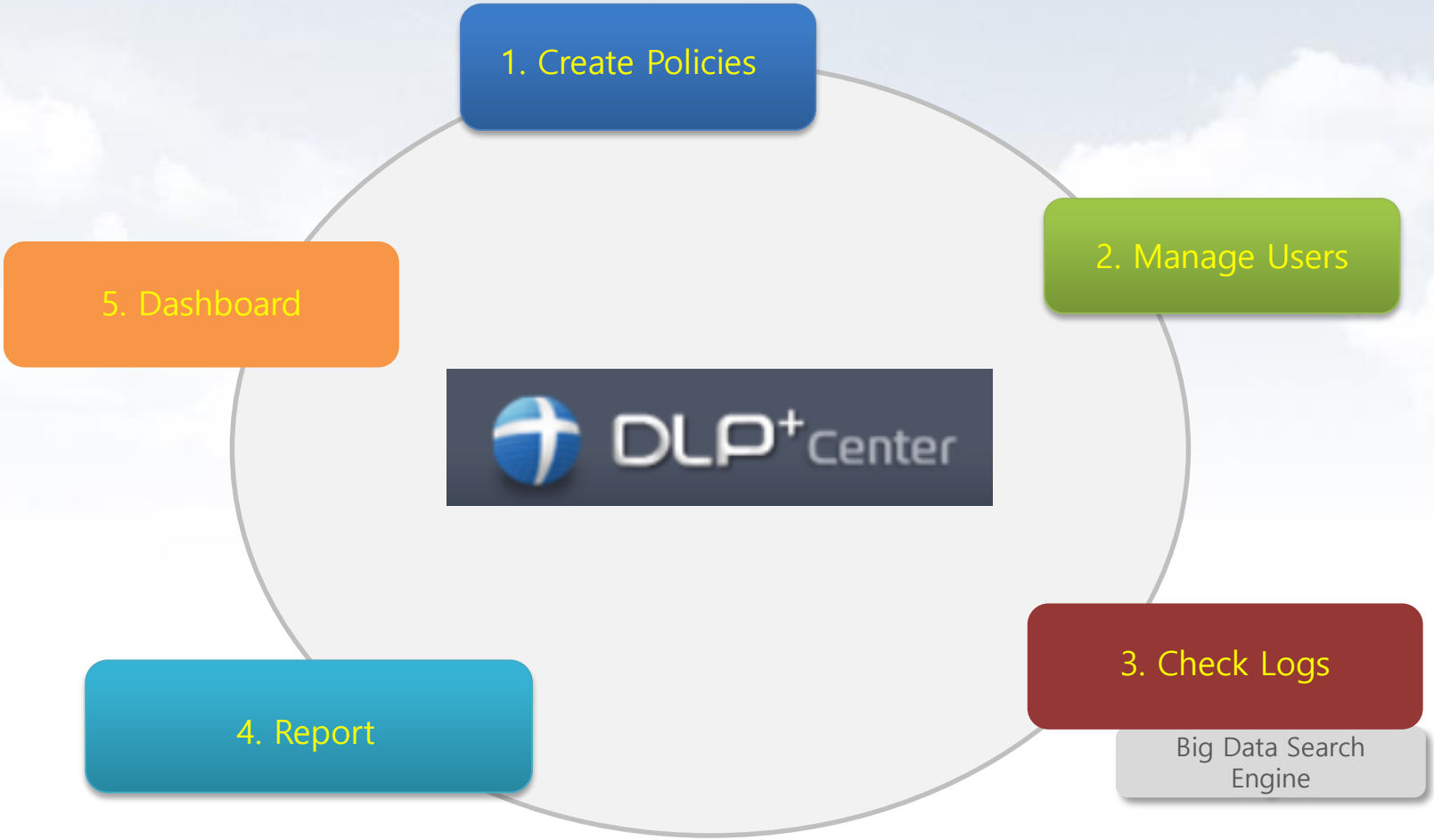
SOMANSA

# Data Loss Prevention

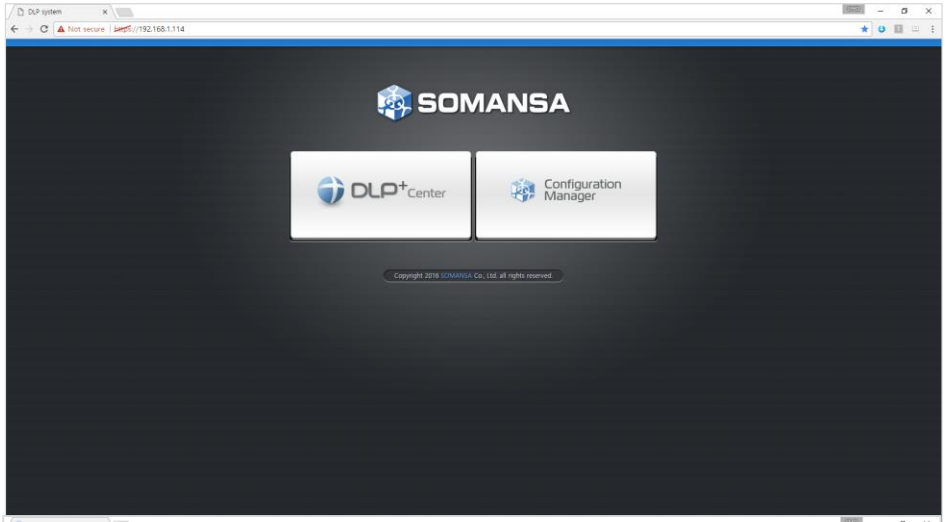

1. Create Policies
2. Manage Users
3. Check Logs
Big Data Search Engine
4. Report
5. Dashboard
DLP+ Center

## CONTENTS

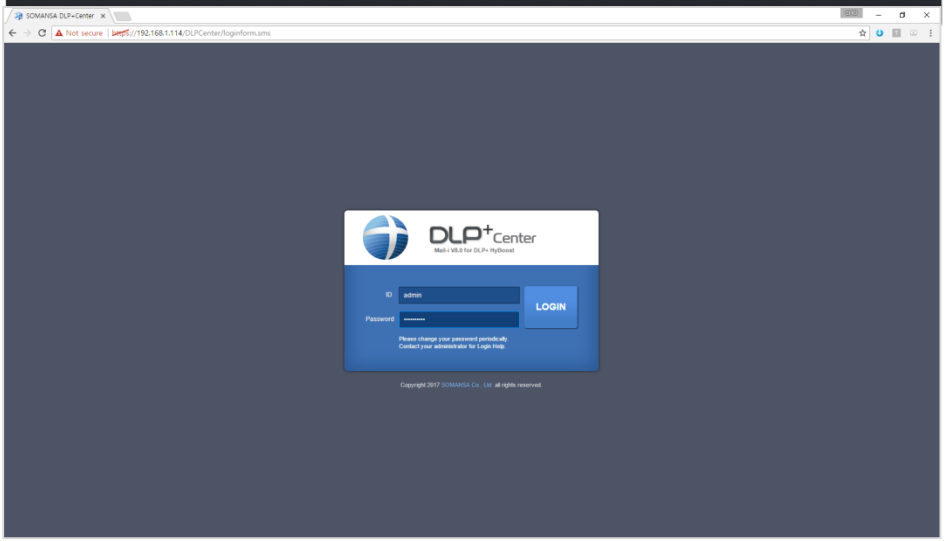
# I. DLP+Center Access

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



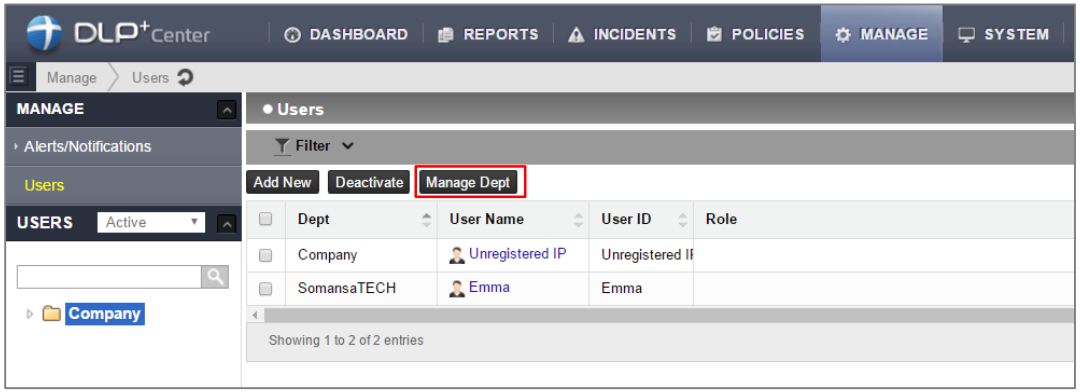

2. Login
   1) ID/Password can be set-up/changed during the initial setup



# II. Department and Users

## 1. Add the Department

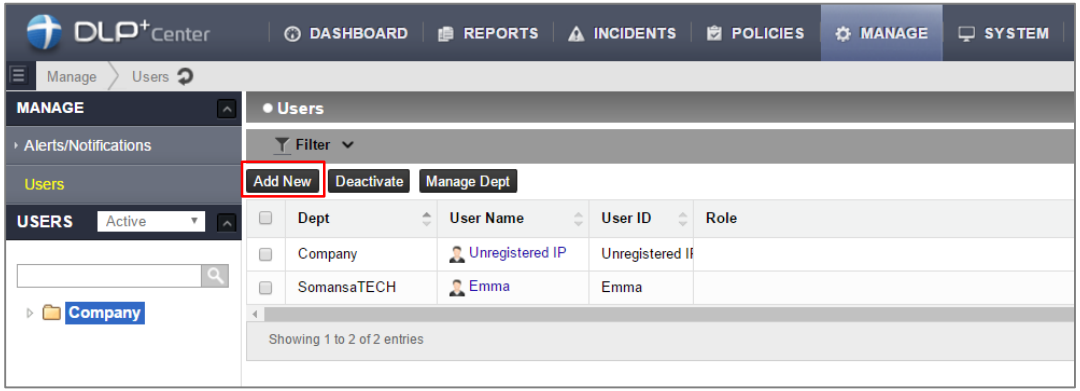
1) Select **MANAGE > Users**
2) Click the **Manage Dept**
3) Click the **Add**
4) Select the upper department as Parent Dept Name, insert the DeptName, and click the **Add**




## 2. Add the Users

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

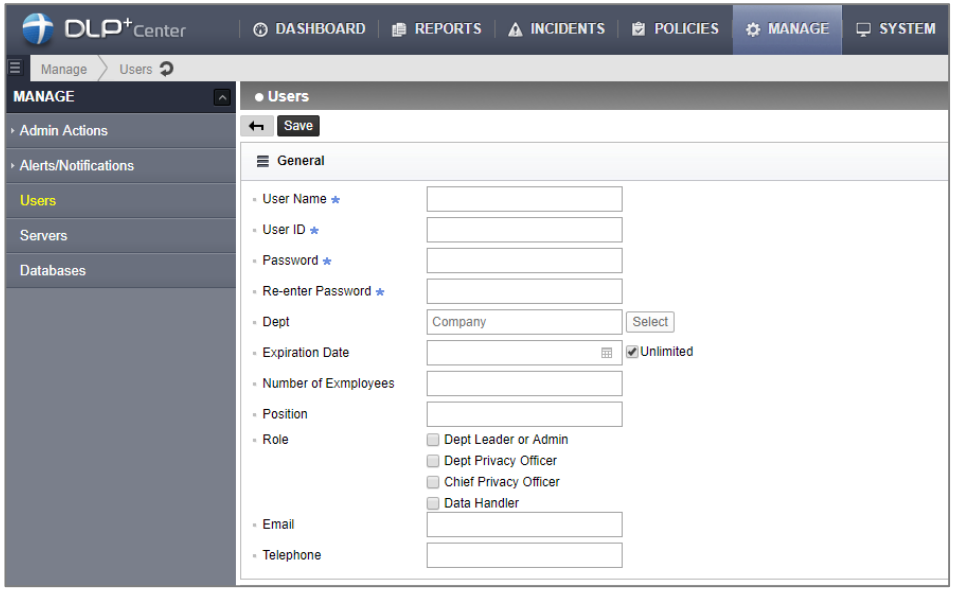
## 3. Add the Users

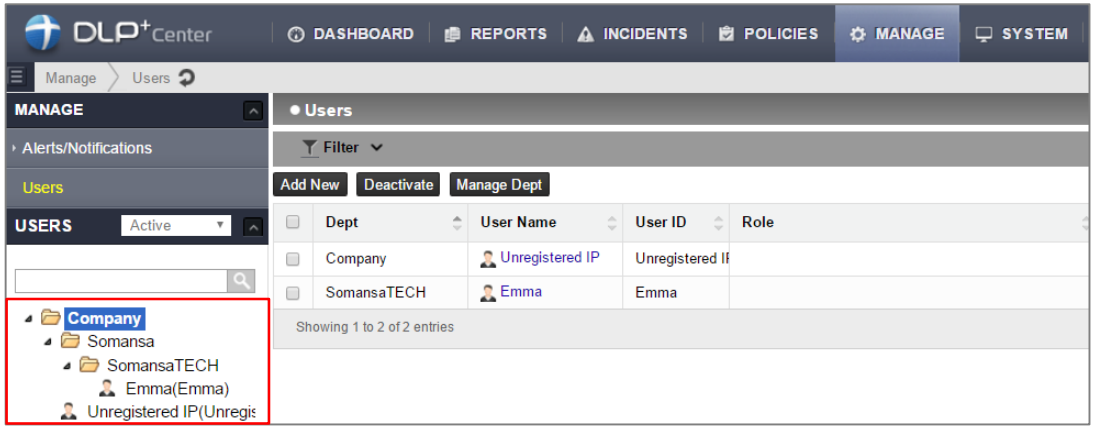
※ Privacy-i have many authentication methods. ID/PW , MAC authentication , IP , SSO , AD ETC

※ When SOMANSA create a install package, SOMANSA select the authentication method.
If you need other method, please contact

## 4. Check Department and Users

1) Select **MANAGE > Users**

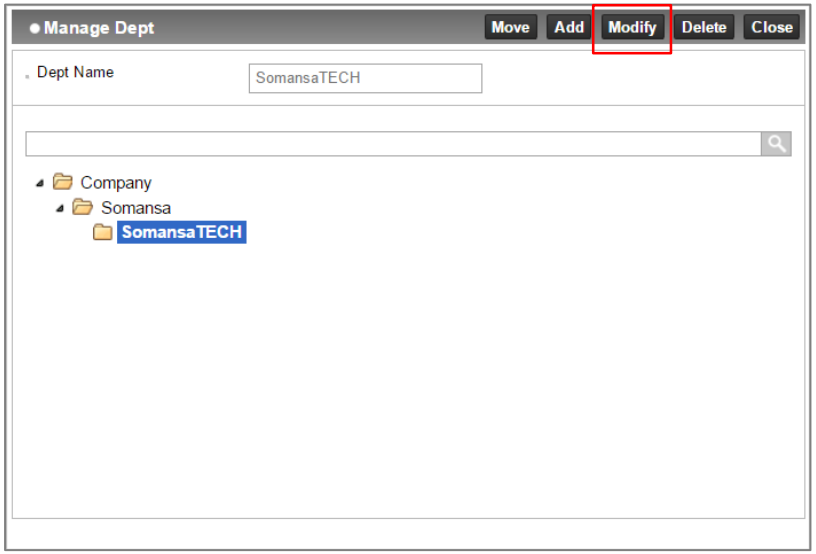


# II. Department and Users

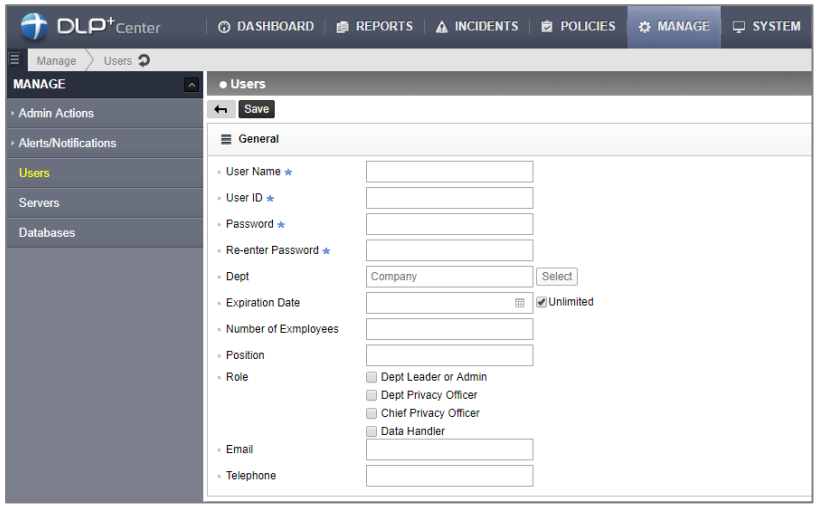
## 5. Modify the Department

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**

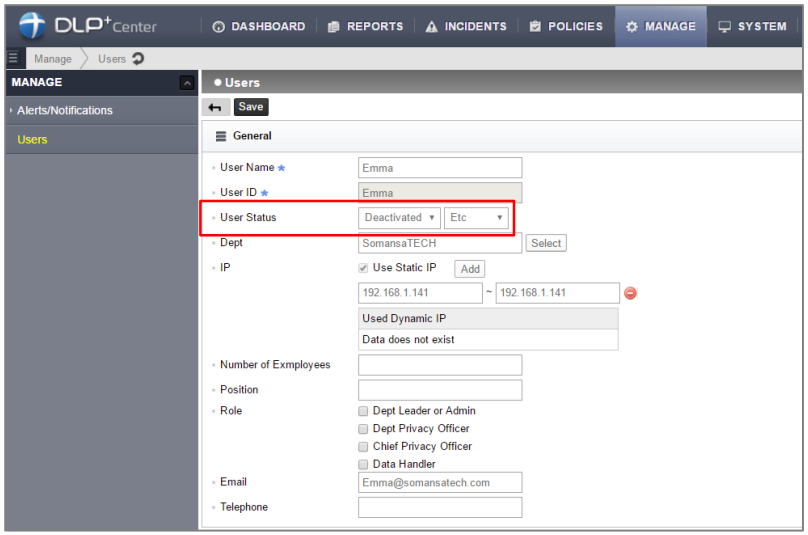


# II. Department and Users

## 7. Deactivate Users

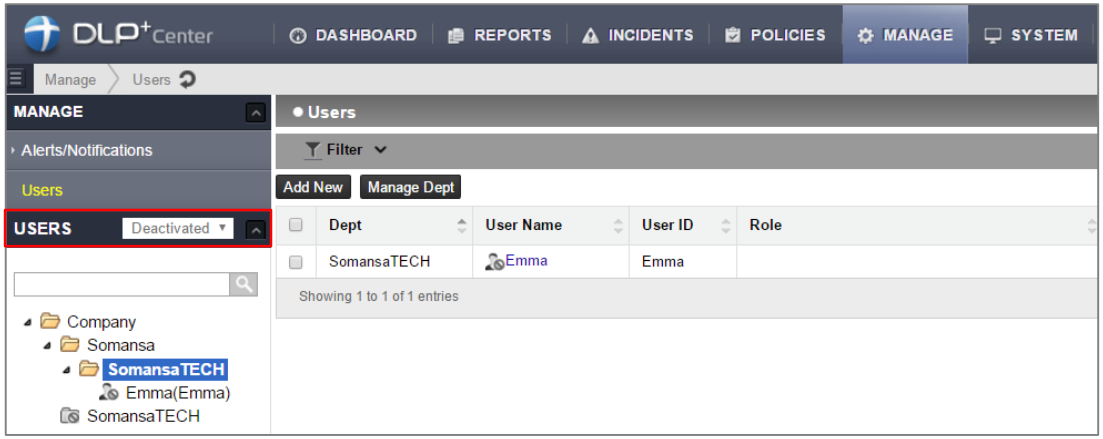
1) Select **MANAGE > Users**
2) Click the User Name you want to disable
3) Select User Status as **Deactivated**
4) Select justification and click **Save**

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



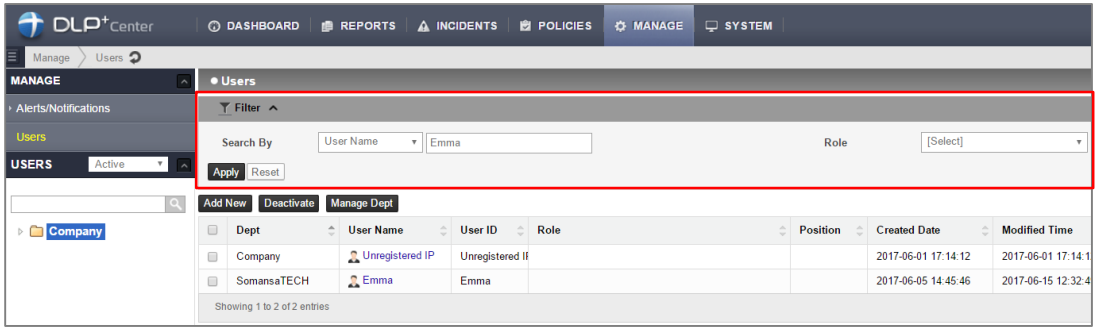

## 8. Reactivate Deactivated Users

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

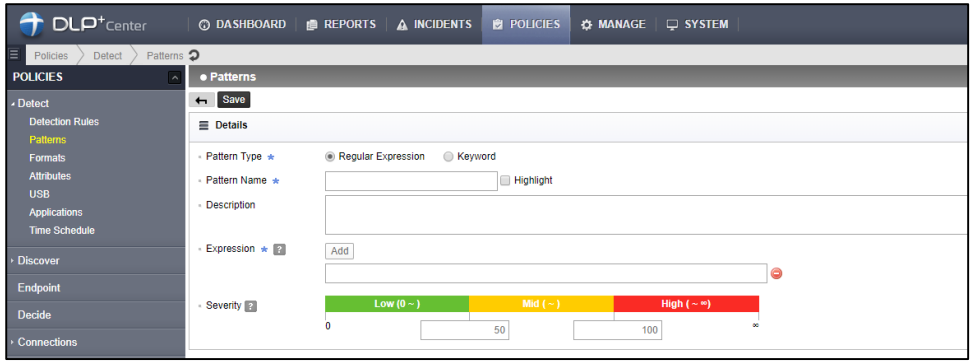
## 1. Add the Patterns

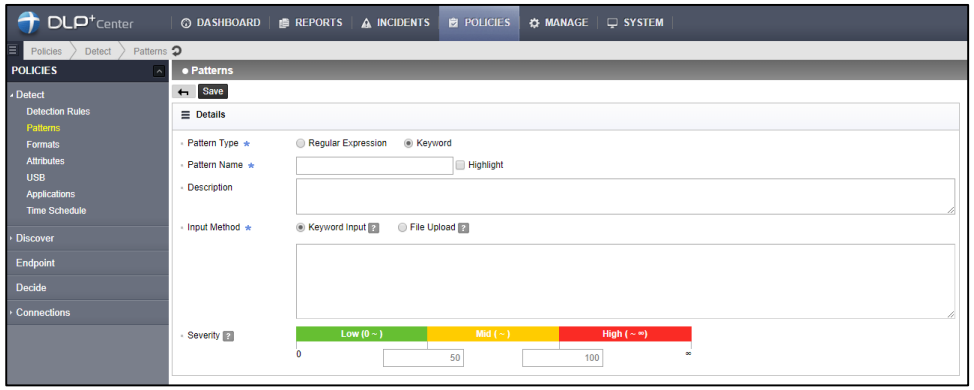
• You can select the basic patterns provided, and create administrator defined patterns.

(regular expression and keyword)

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

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



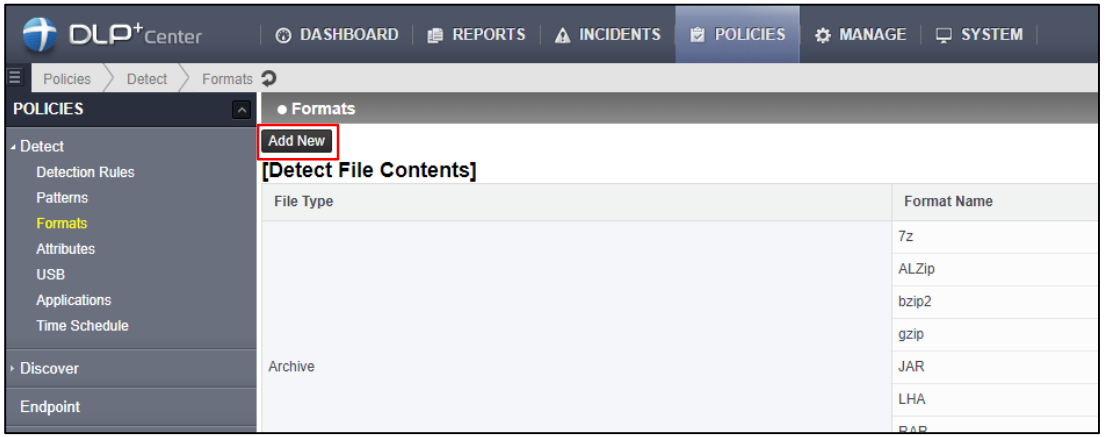
# III. POLICIES

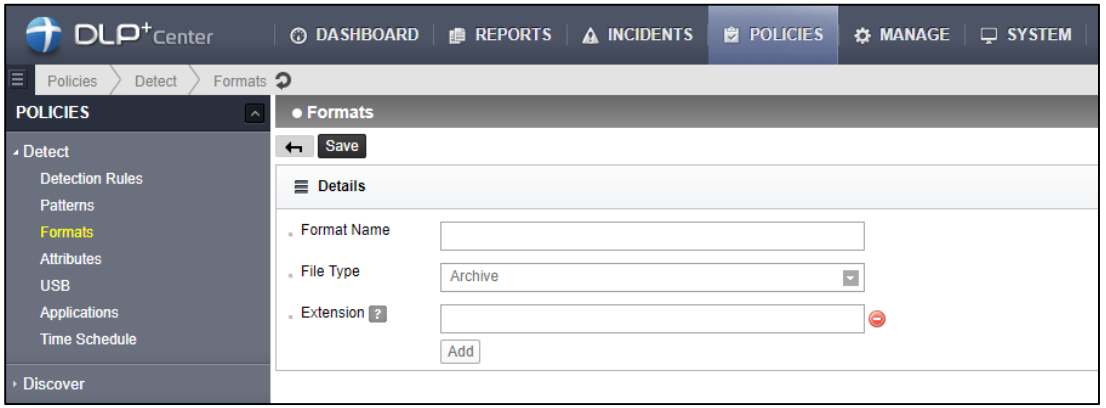
## 2. Add the Formats

• 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



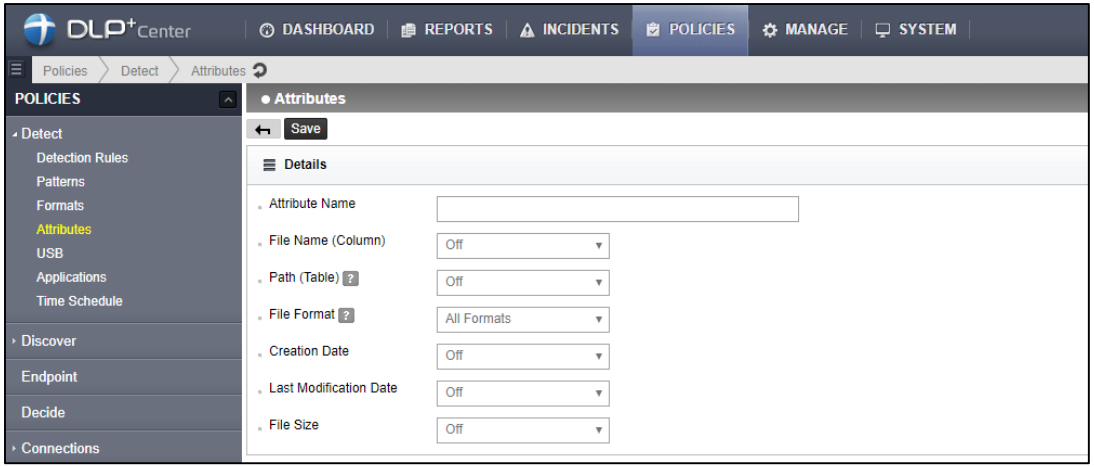



# III. POLICIES

## 3. Add the Attributes

- The file format is now used in Attributes

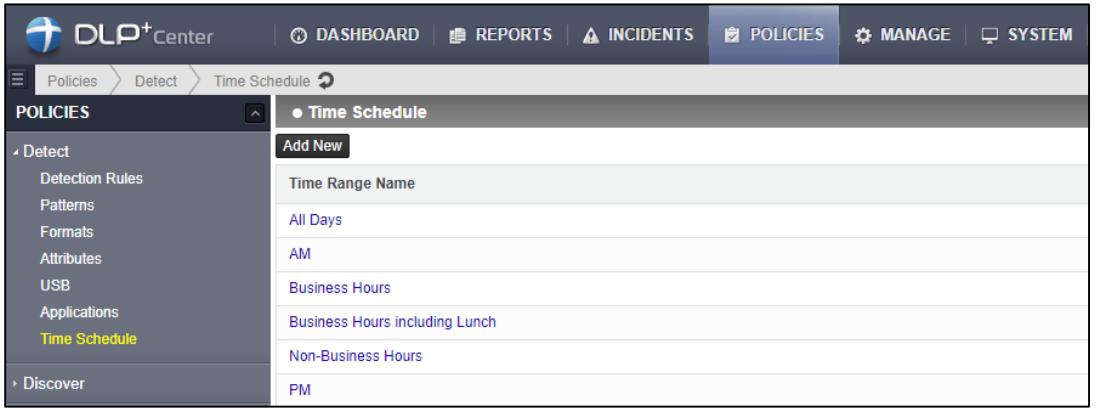
1) Select **POLICIES > Detect > Attributes**
2) Click **Add New**
3) Insert the Attribute Name and select File Name, Path, File Format, File Size and click **Save**




## 4. Add Time Schedule

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

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



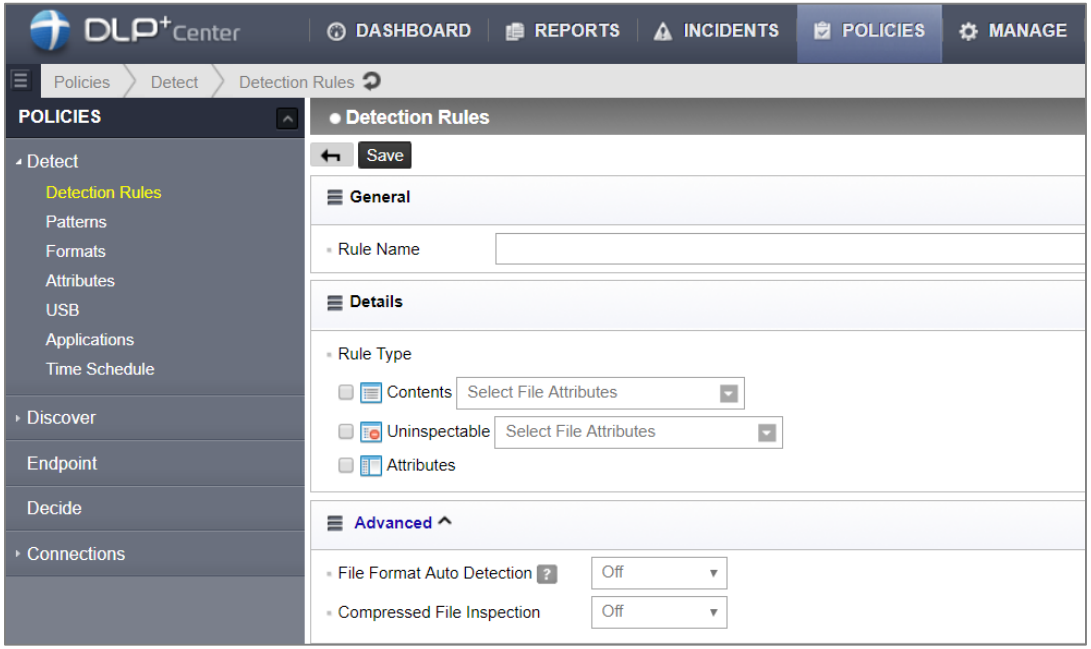
# III. POLICIES

## 5. 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**

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



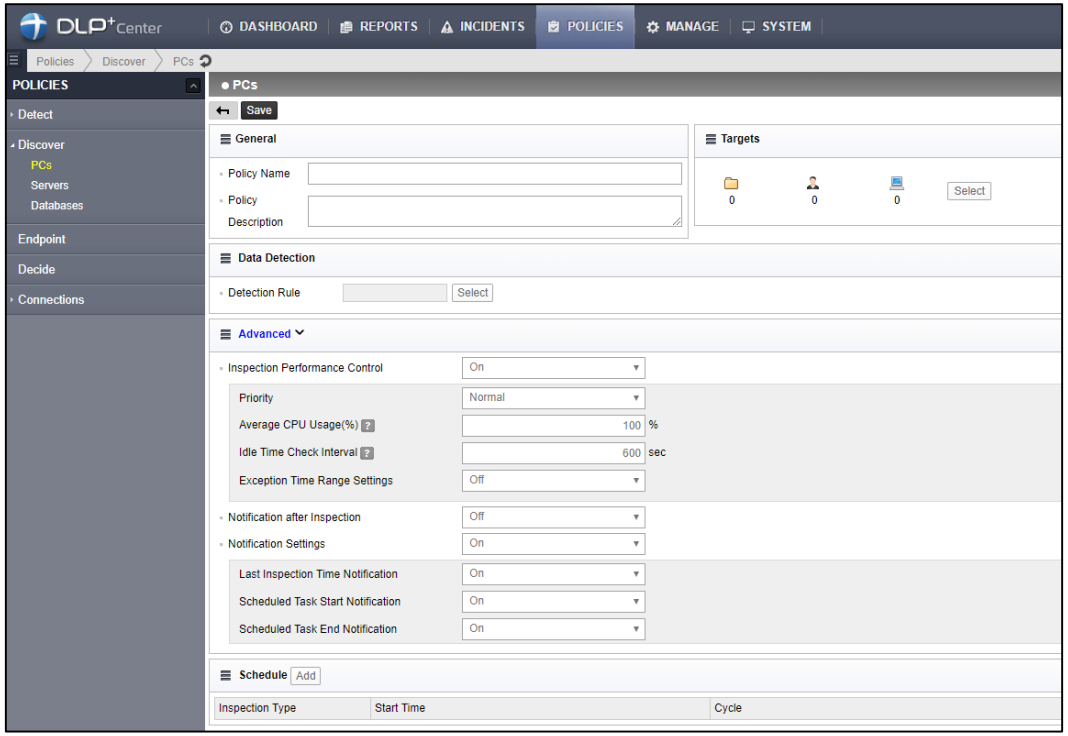
# III. POLICIES

## 6. Add the Discover Policy

- The detection rules are used in discover policy

1) Select **POLICIES > Discover > PCs**
2) Click **Add New**
3) Insert the Policy Name
4) Select Target you want to apply to
5) Select Detection Rule
6) Put numbers for Advanced setting
7) Click **Save**
8) Click **Apply Policy**

※ If you want to delete discover policy, select Policy Name and click delete button.



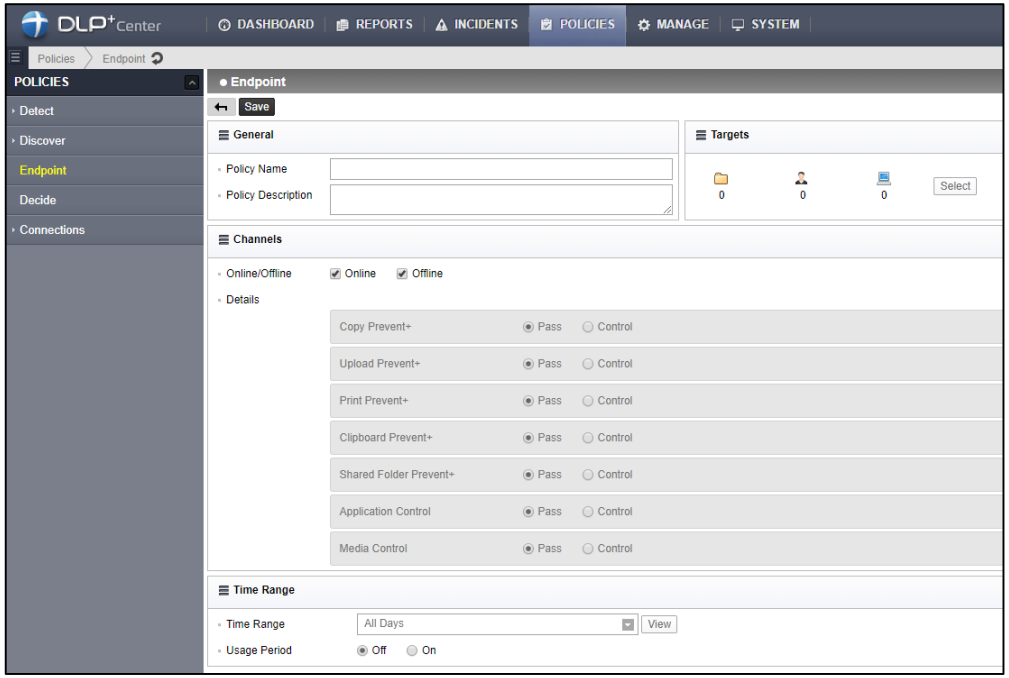
# III. POLICIES

## 7. Add the Endpoint Policy

- The detection rules might be used in endpoint policy

1) Select **POLICIES > Endpoint**
2) Click **Add New**
3) Insert the Policy Name
4) Select Target you want to apply to
5) Select Details
   (There are various endpoint policy: Copy Prevent+, Upload Prevent+, Print Prevent+, Clipboard Prevent+, Shared Folder Prevent+, Application Control, Media Control)
6) Click **Save**
7) Click **Apply Policy**

※ If you want to delete discover policy, select Policy Name and click delete button.



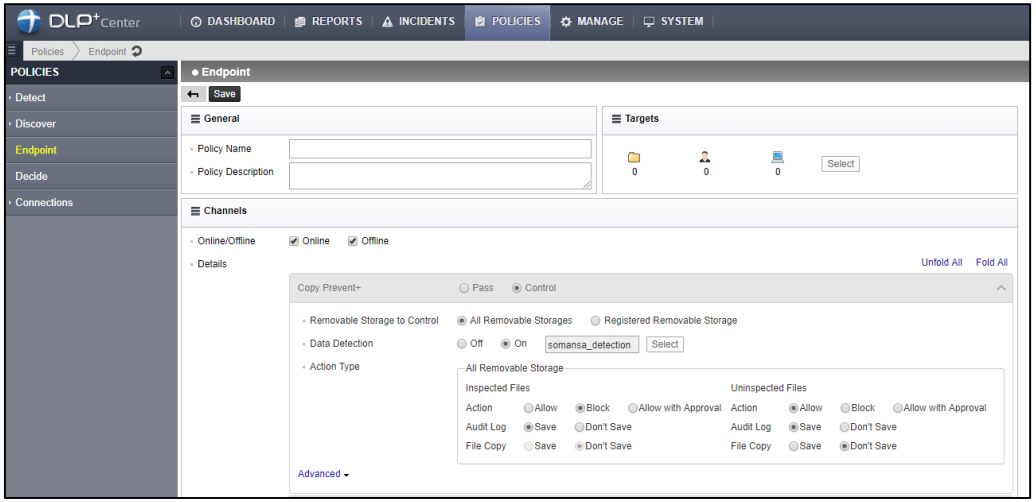
# III. POLICIES

## 7.1 Copy Prevent+

- The detection rules might be used in endpoint policy

1) Select Copy Prevent+ as Control
2) Select Data detection on or off
3) Select Action Type

※ In order to check the log, you should select Audit Log as Save.



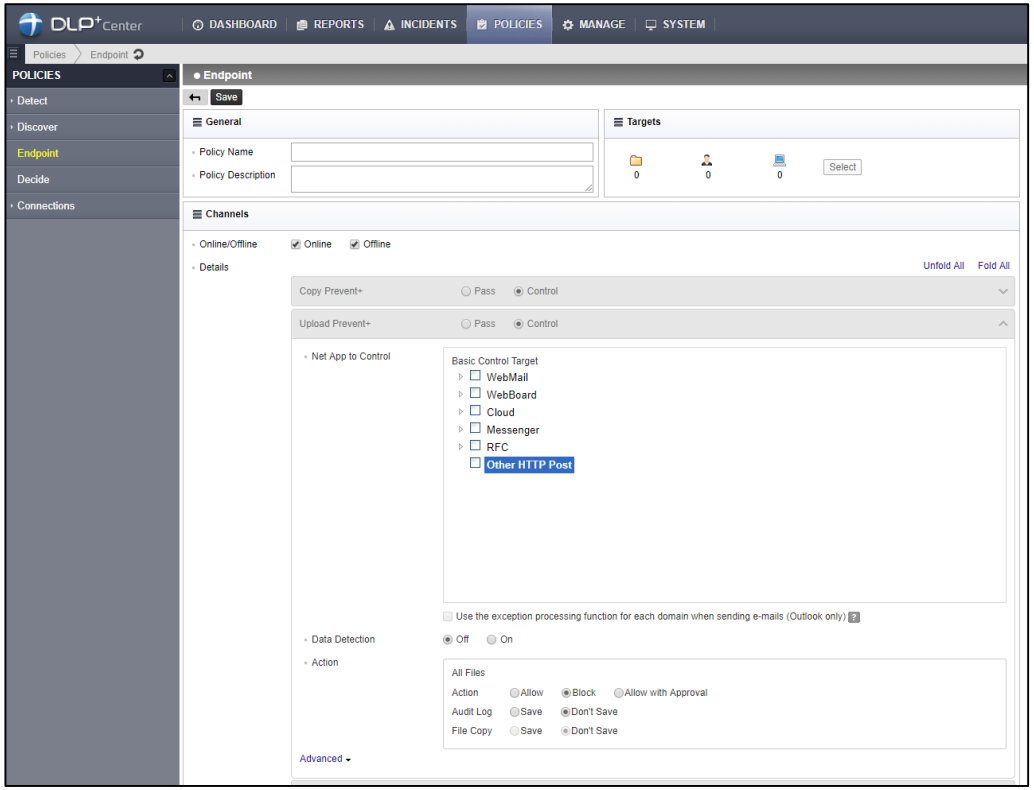
# III. POLICIES

## 7.2 Upload Prevent+

- The detection rules might be used in endpoint policy

1) Select Upload Prevent+ as Control
2) Select Data detection on or off
3) Select Action Type

※ In order to check the log, you should select Audit Log as Save.



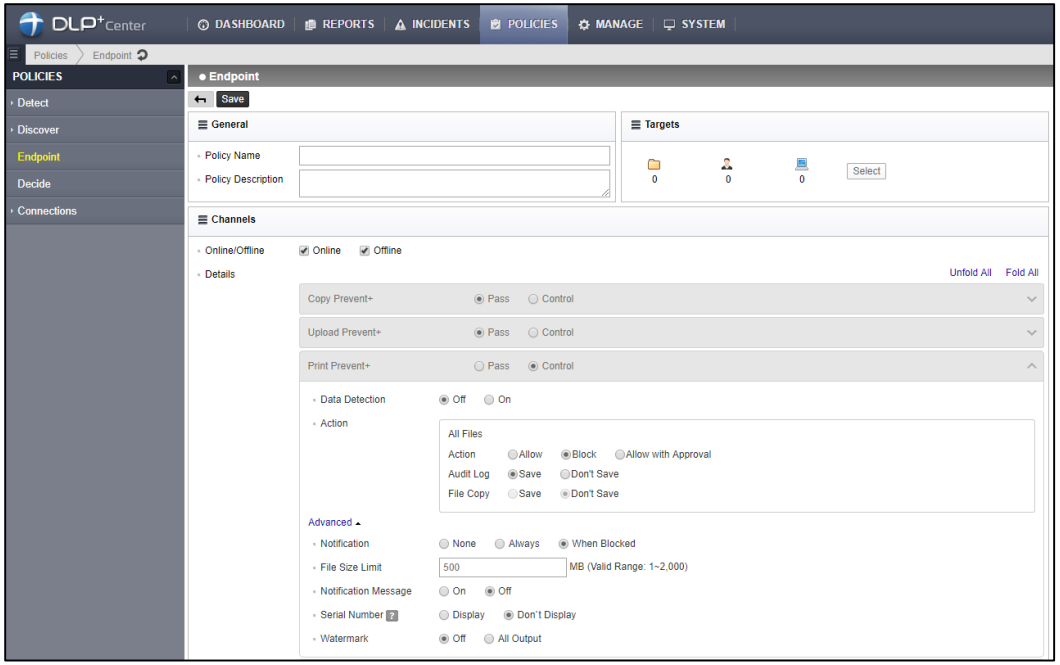
# III. POLICIES

## 7.3 Print Prevent+

- The detection rules might be used in endpoint policy

1) Select Print Prevent+ as Control
2) Select Data detection on or off
3) Select Action Type

※ In order to check the log, you should select Audit Log as Save.



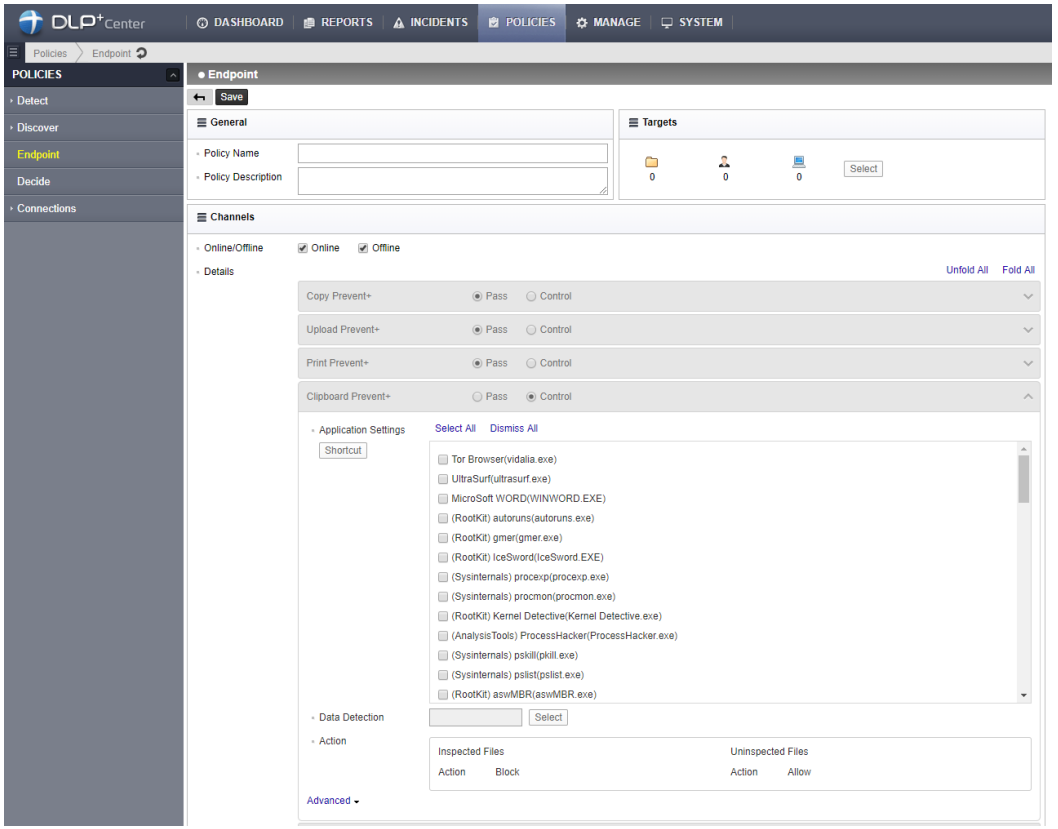
# III. POLICIES

## 7.4 Clipboard Prevent+

- The detection rules might be used in endpoint policy

1) Select Clipboard Prevent+ as Control
2) Select Data detection on or off
3) Select Action Type

※ In order to check the log, you should select Audit Log as Save.



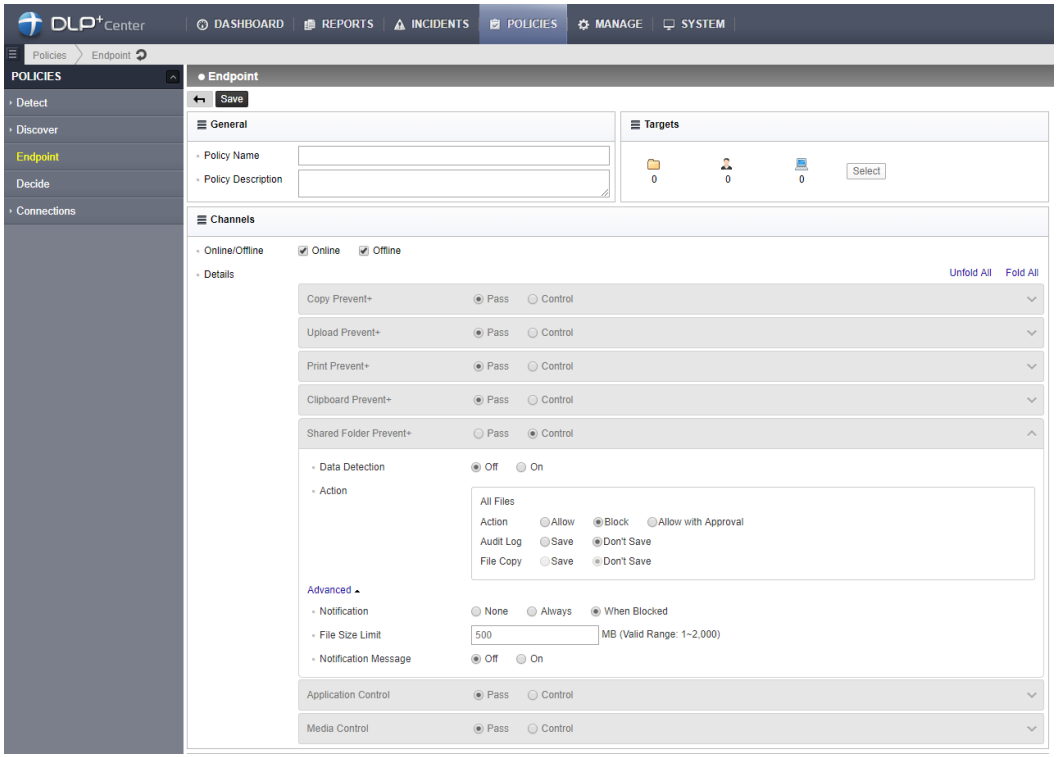
# III. POLICIES

## 7.5 Shared Folder Prevent+

- The detection rules might be used in endpoint policy

1) Select Shared Folder Prevent+ as Control
2) Select Data detection on or off
3) Select Action Type

※ In order to check the log, you should select Audit Log as Save.



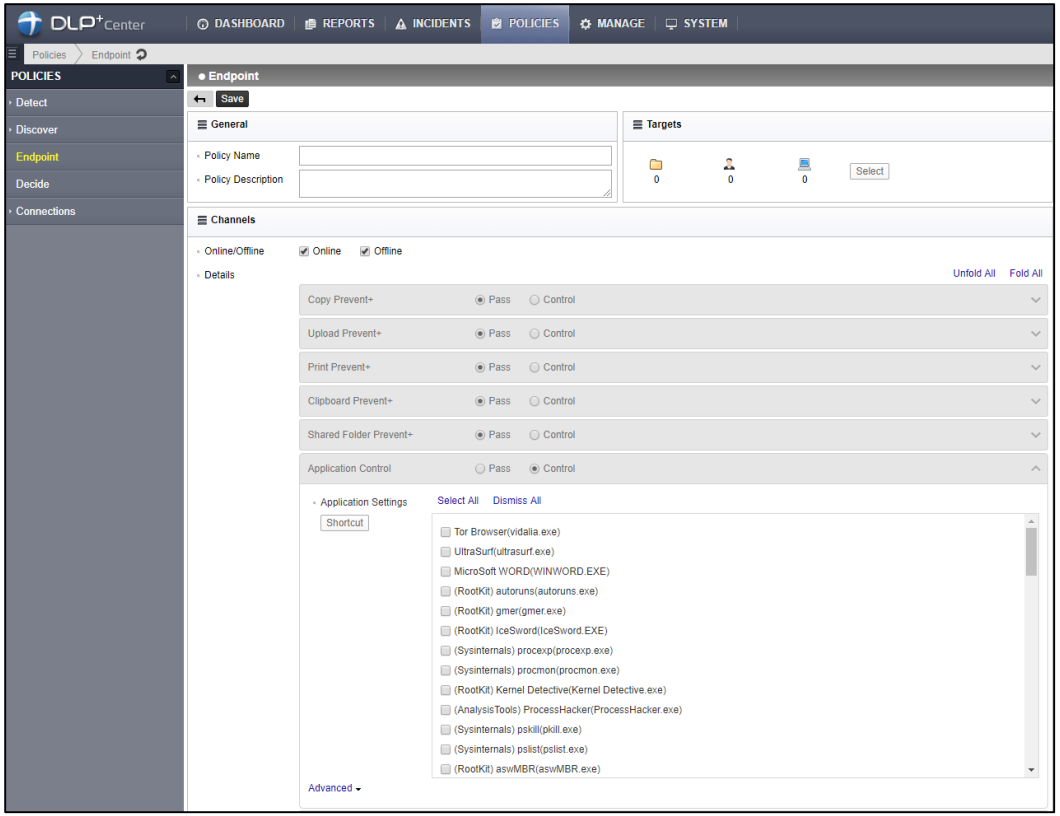
# III. POLICIES

## 7.6 Application Control

- The detection rules might be used in endpoint policy

1) Select Application Control as Control
2) Select Data detection on or off
3) Select Action Type

※ In order to check the log, you should select Audit Log as Save.



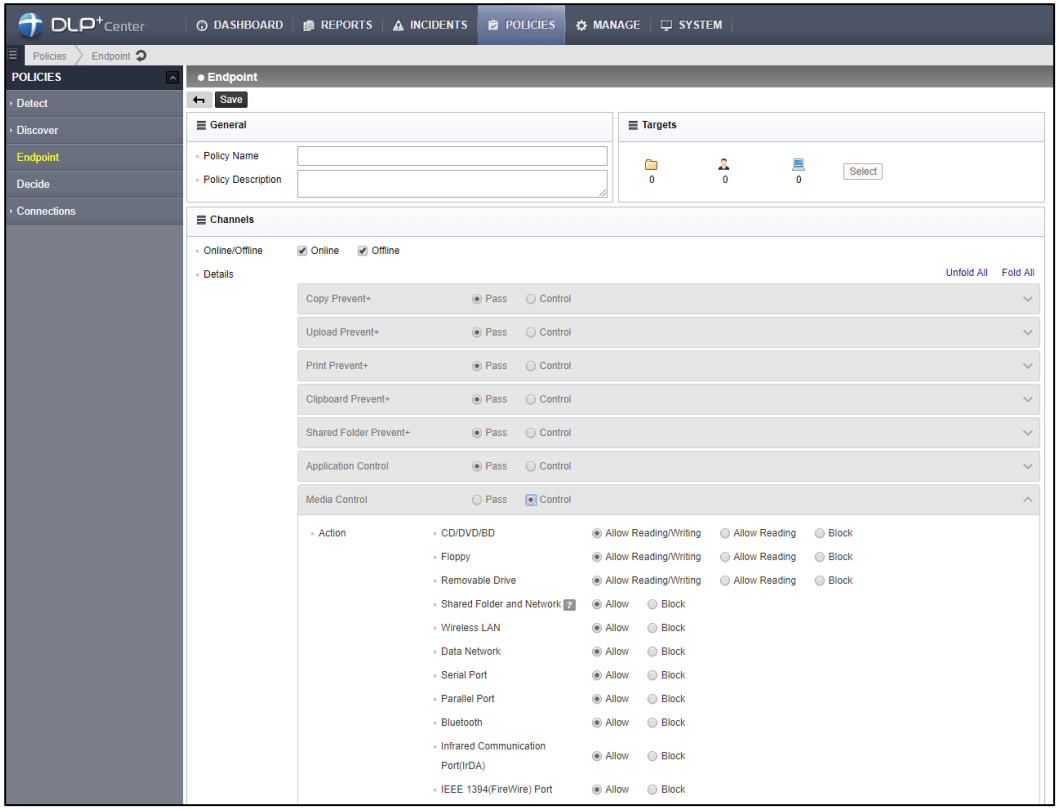
# III. POLICIES

## 7.7 Media Control

• The detection rules might be used in endpoint policy

1) Select Media Control as Control
2) Select Data detection on or off
3) Select Action Type

※ In order to check the log, you should select Audit Log as Save.



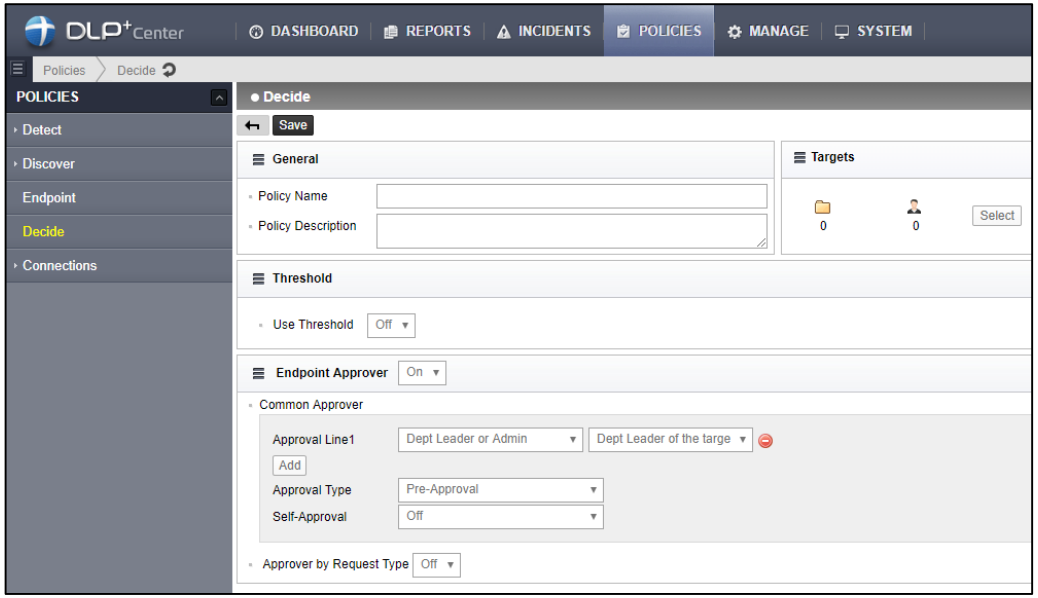
# III. POLICIES

## 8. Add Decide Policy

- The detection rules might be used in endpoint policy

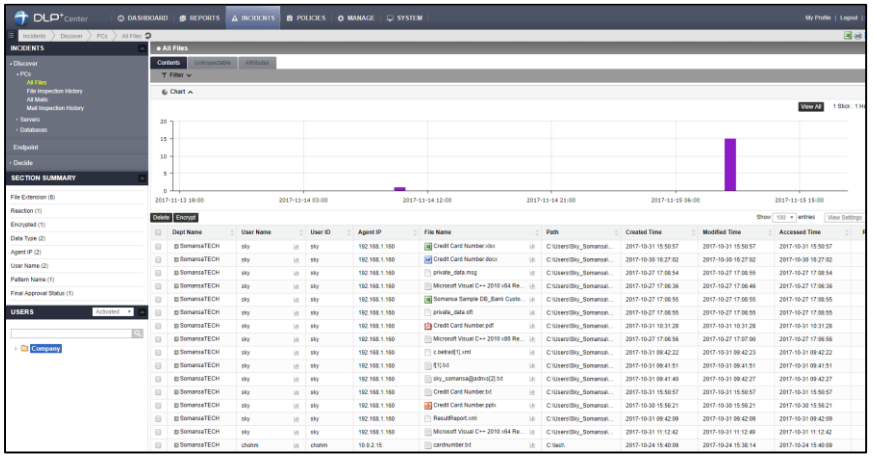
1) Select **POLICIES > Decide**
2) Click **Add New**
3) Insert the Policy Name
4) Select Target you want to apply to
5) Select Approval Line
6) Select Approval Type and Self-Approval
7) Click **Save**
8) Click **Apply Policy**

※ If you want to delete decide policy, select Policy Name and click delete button.

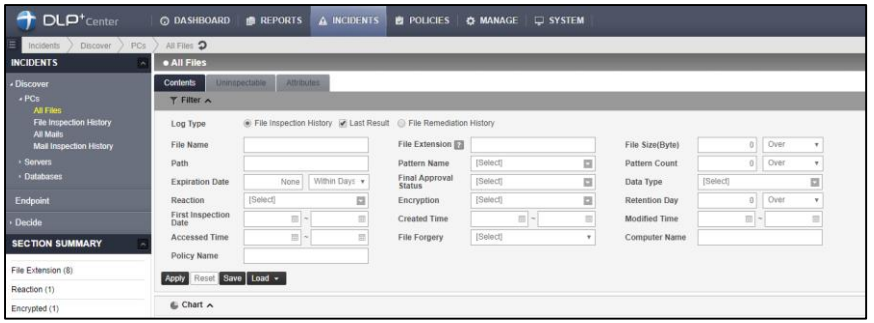


# IV. INCIDENTS

1. Check the Result of Inspection
   1) Select **INCIDENTS > Discover > All Files**



2. Apply the Filter
   1) Select **INCIDENTS > All Files**
   2) Click **Filter**
   3) Select condition(File Name, File Extension, Path, Pattern Name, Policy Name, etc) that you want to filter and Insert Keywords
   4) Click **Apply**

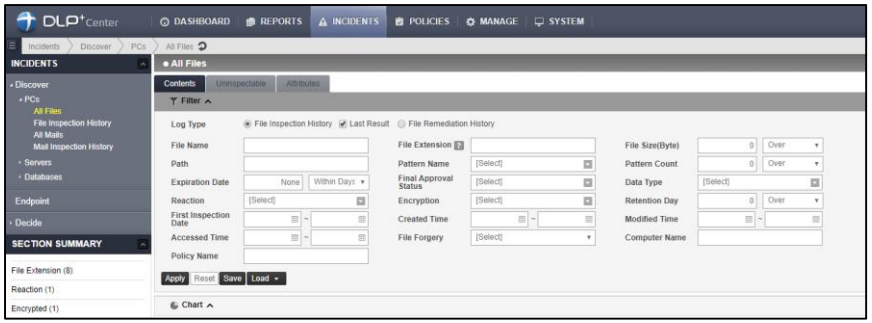


※ When searching based on Keyword, you can also search for the contents of the file body. Only possible when file analysis is completed.

# IV. INCIDENTS

## 3. Save the Filter

1) Select **INCIDENTS > Discover > All Files**
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**




## 4. Load the Filter

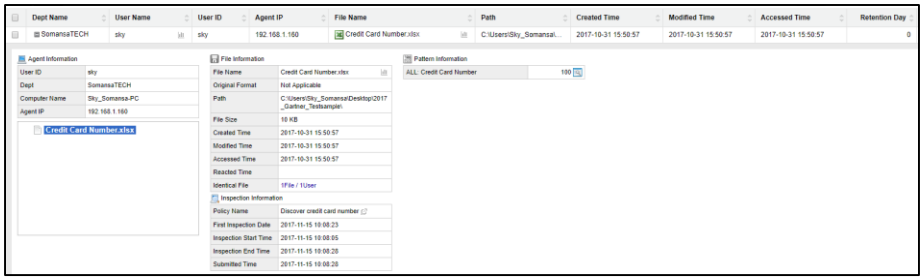
1) Select **INCIDENTS**
2) Click **Filter**
3) Select condition(File Name, File Extension, Path, Pattern Name, Policy Name, etc) that you want to filter and Insert Keywords
4) Click **Apply**

※ 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

## 5. View the Logs in detail

1) Select **INCIDENTS > Discover > All Files**
2) Click the plus icon in front of Dept Name
3) You can check detail information such as Agent information, File information, Pattern Information

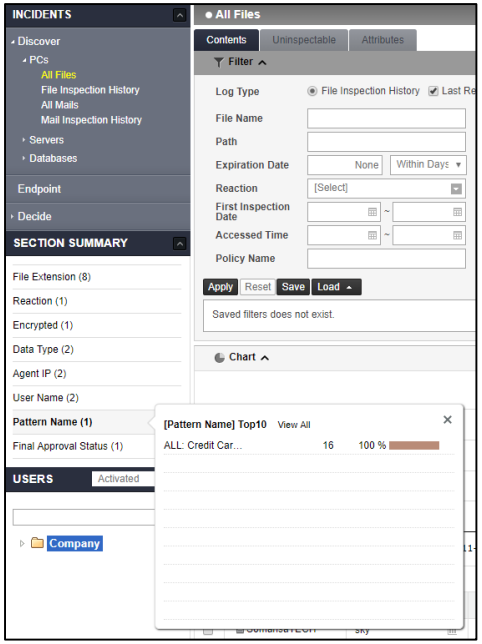



## 6. Section Summary

- Quickly search for top 10 Incidents

1) Select **INCIDENTS**
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



# IV. INCIDENTS

## 7. Encrypt the Inspected File

1) Select **INCIDENTS > Discover > All Files**
2) Apply Filter the log to export
3) Click the **Excel button** in upper right
4) Select the Body Contents and click **Save**
5) Select where to save and click **Save**

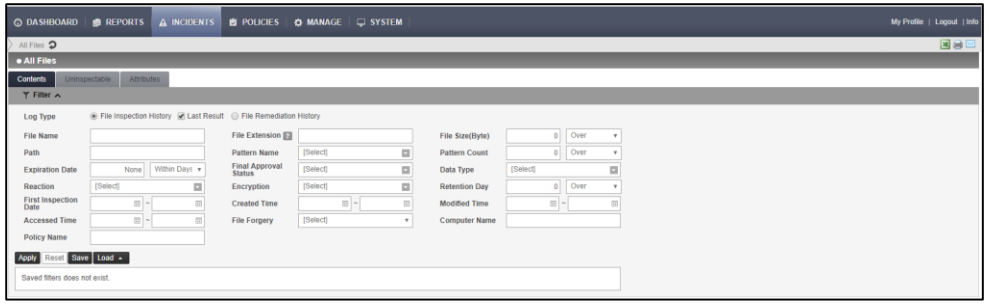

## 8. Delete the Inspected File

1) Select **INCIDENTS**
2) Select the file you want to delete
3) Click the **Delete** button
4) Input details such as Task Name, User consent
5) Select the Target
6) Select the Schedule
7) Click **Save**

# IV. INCIDENTS

## 9. Export the Log

1) Select **INCIDENTS > Discover > All Files**
2) Select the file you want to encrypt
3) Click the **Encrypt** button
4) Input details such as Task Name, User consent
5) Select the Target
6) Select the Schedule
7) Click **Save**



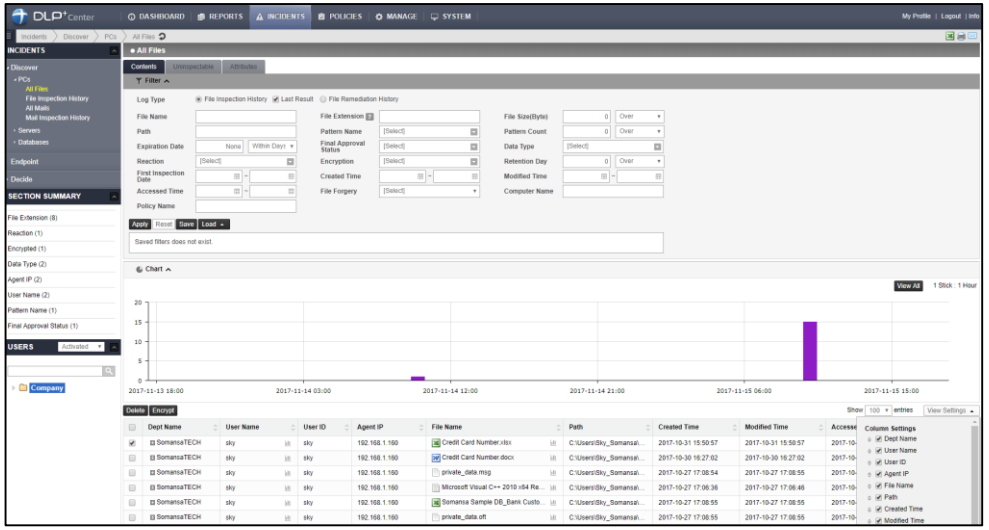

## 10. Log View Options

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

1) Select **INCIDENTS**
2) Change the number next to Show on the right

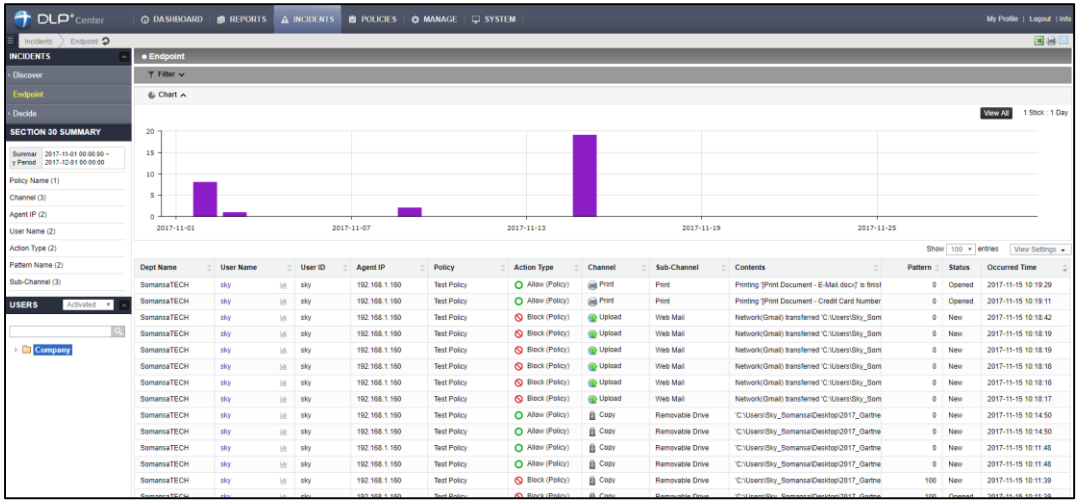
• You can select the column to show in the log and change the order

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



# IV. INCIDENTS

11. Export the Endpoint Log
    1) Select **INCIDENTS > Endpoint**

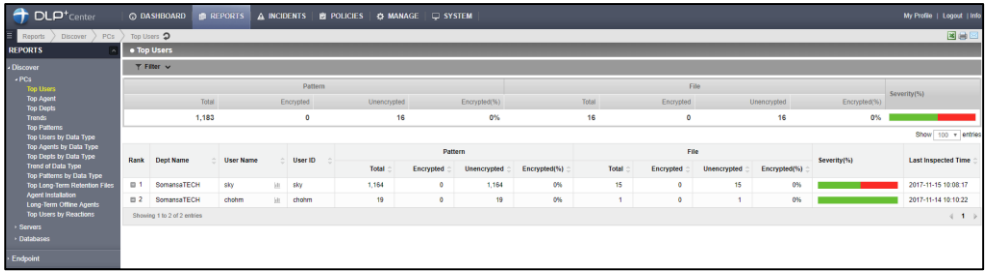


# V. REPORTS

## 1. Check the Report

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

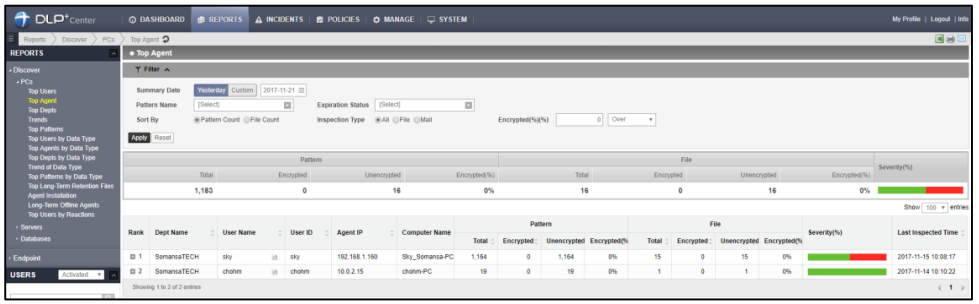
1) Select **REPORTS > Discover** or **REPORTS > Endpoint**
2) Select the report criteria you want in the left tree



## 2. Apply the Filter

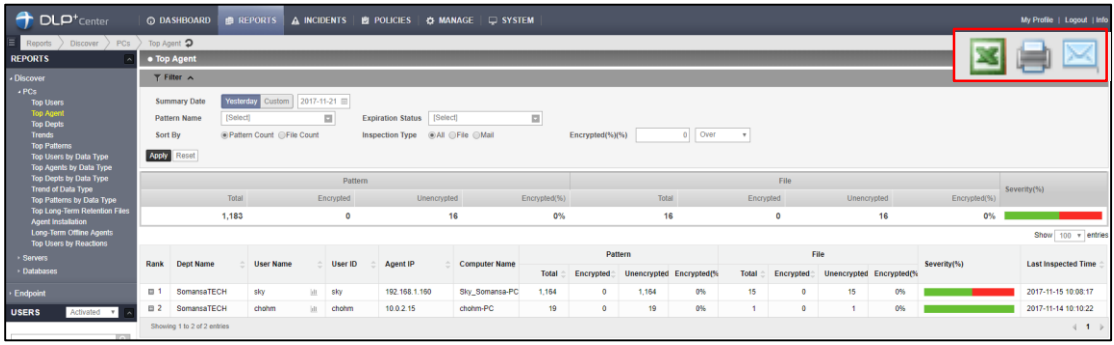
1) Select **REPORTS**
2) Select the report criteria you want in the left tree
3) Click Filter
4) Select condition(Date, Pattern Name, ETC) that you want to filter
5) Click **Apply**

• 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 **REPORTS**
   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 | |

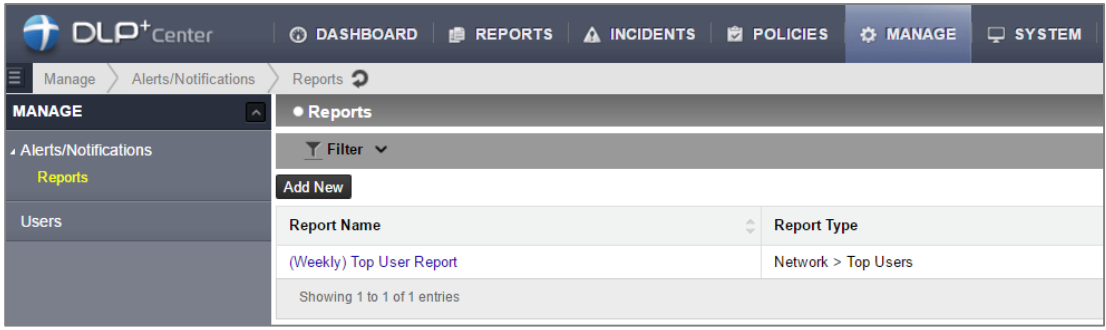
# VI. Alerts/Notifications

## 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.

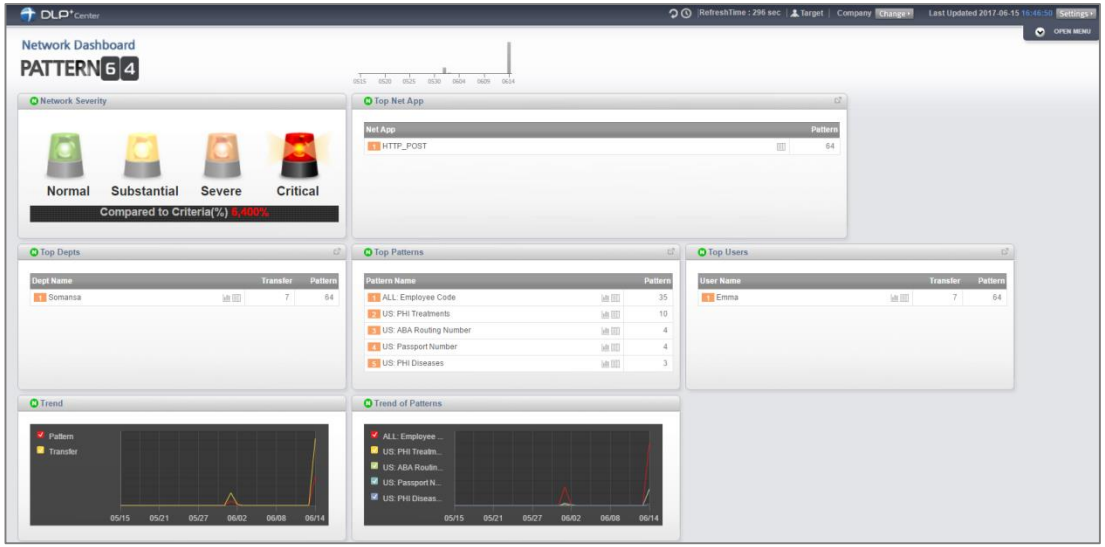


# VII. Dashboard

## 1. Settings

• Sets the patterns and components to activate on the dashboard

1) Select **Dashboard > Settings**
2) Enter the Update Cycle, select the Patterns and Components
3) Components 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.

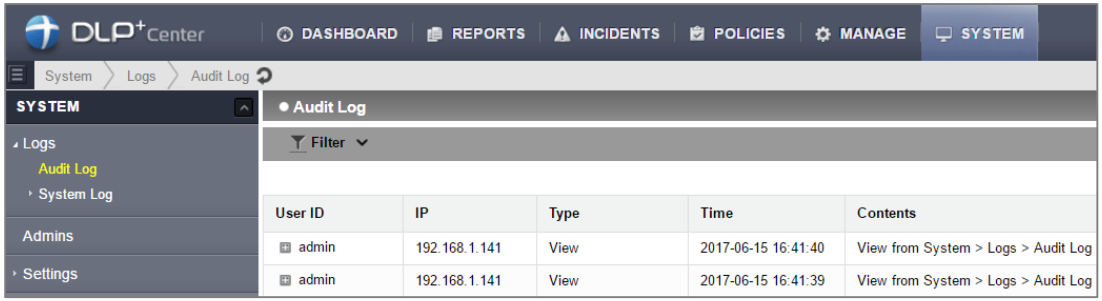
1) Click the **Change** at the top
2) Click the desired user or department
3) Click **Apply**

# VIII. System

## 1. Audit Log

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

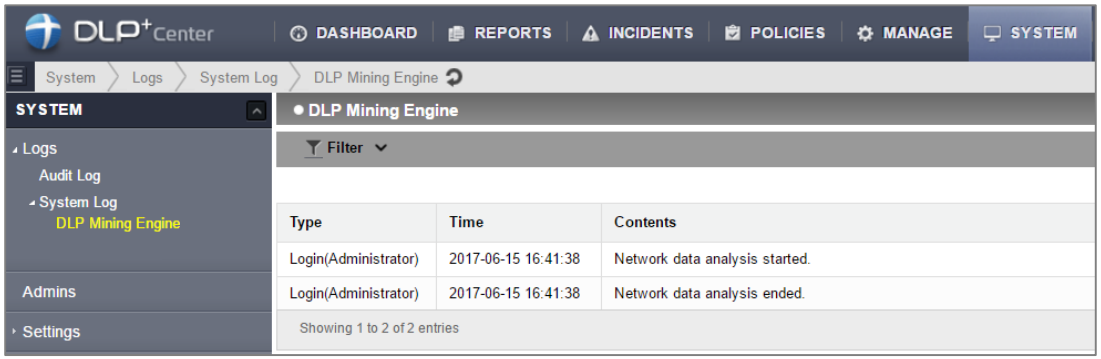
1) Select **SYSTEM > Audit Log**




## 2. DLP Mining Engine

- You can check the log of data analysis status.

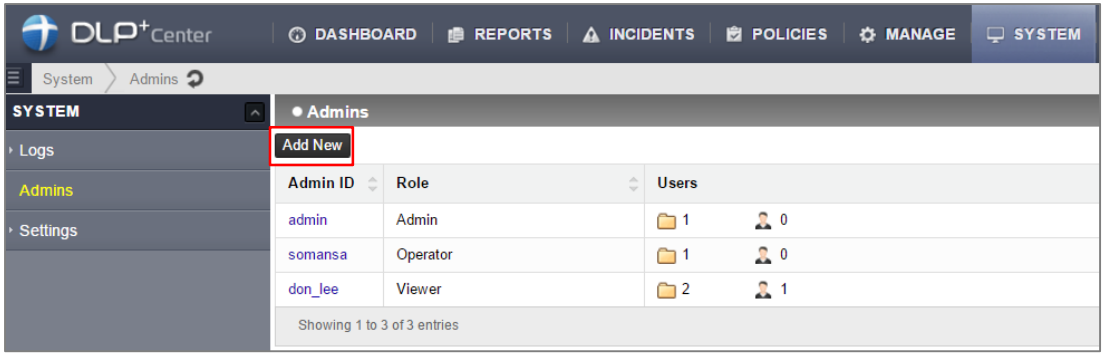
1) Select **SYSTEM > System Log > DLP Mining Engine**



# VIII. System

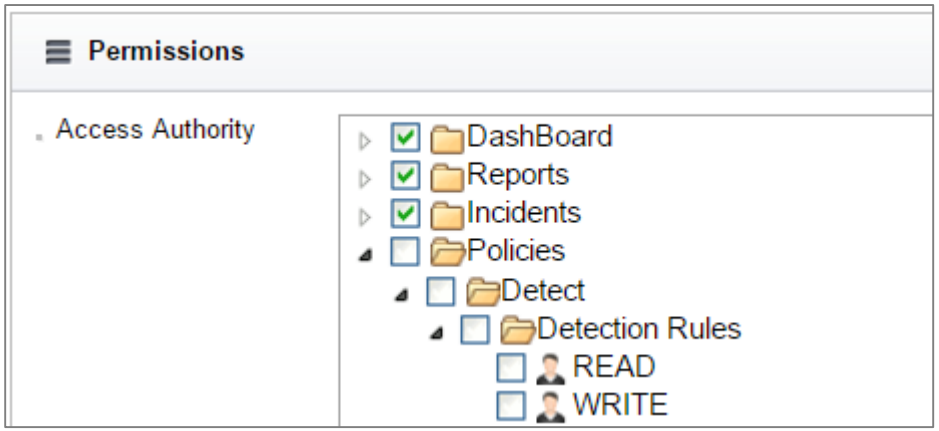
## 4. Add the Admin

• 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.



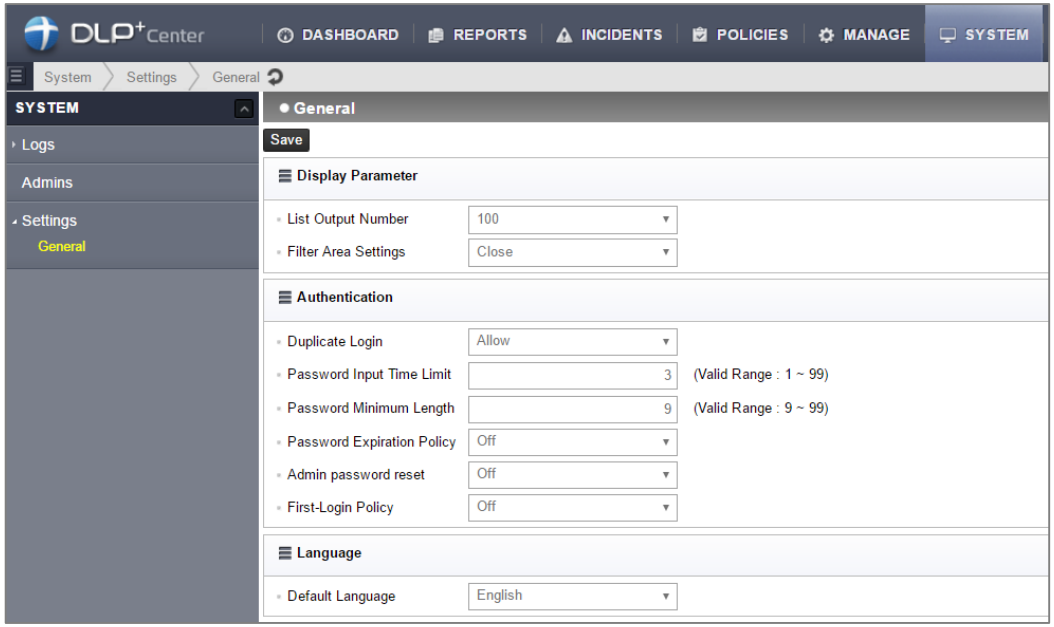
# VIII. System

## 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