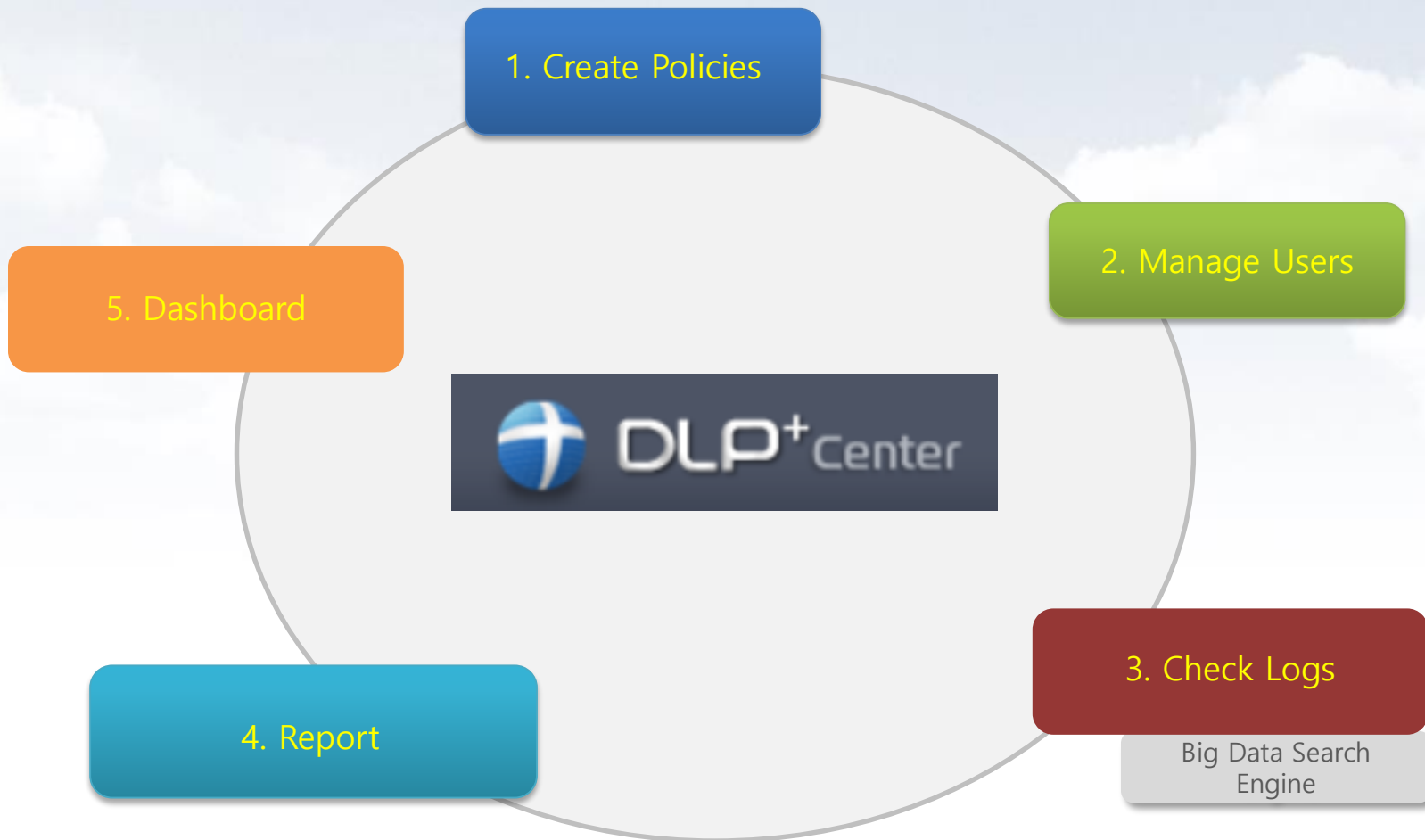




Data Loss Prevention





CONTENTS

- I. DLP+Center (Management console) Access
- II. Department and User Management
- III. Policies
- IV. Incidents (Check and search the logs)
- V. Reports
- VI. Alerts / Notifications
- VII. Dashboard
- VIII. System Settings

SOMANSA / Mail-i / DLP+Center



I. DLP+Center Access

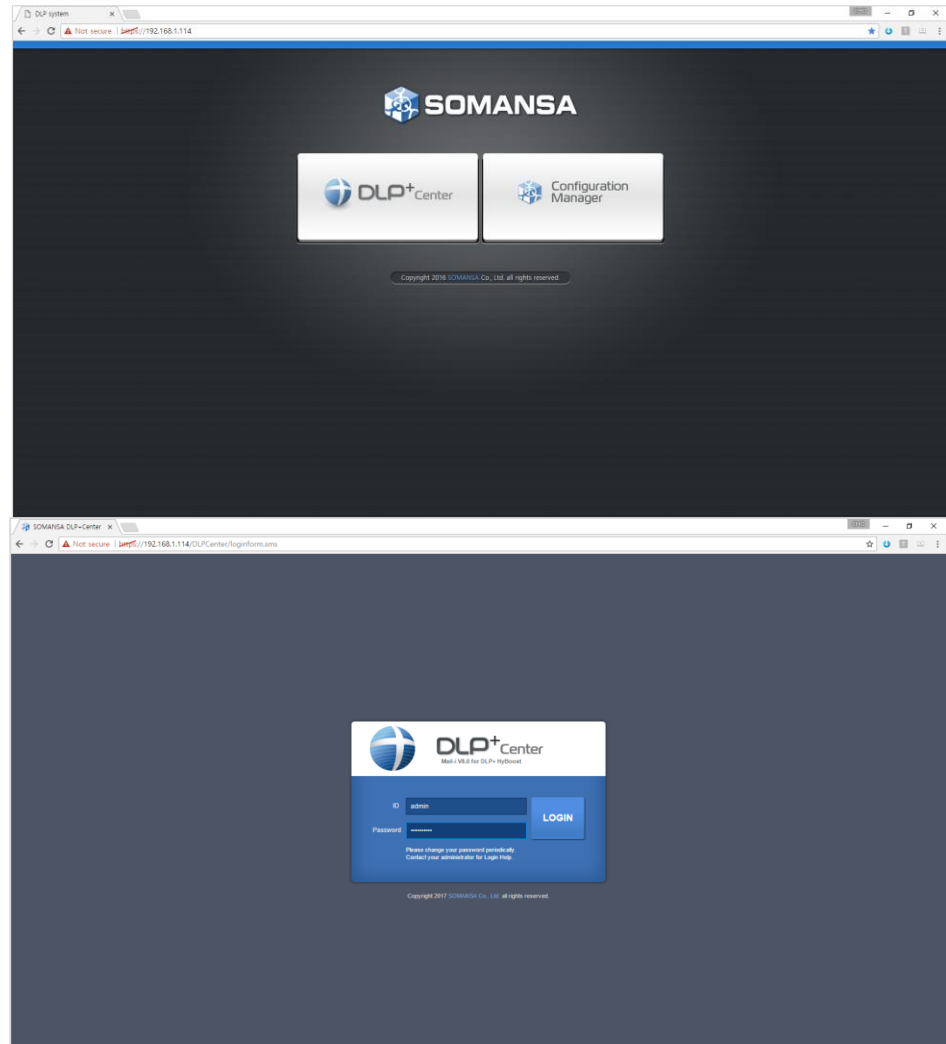
1. Access the DLP+Center

- 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**

The screenshot shows the 'Users' management interface in DLP+Center. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', 'MANAGE', and 'SYSTEM'. The left sidebar has 'MANAGE' selected, with 'Users' in the breadcrumb. The main content area shows a table of users with columns: Dept, User Name, User ID, and Role. The 'Manage Dept' button is highlighted with a red box. The table contains two entries: 'Company' (Unregistered IP) and 'SomansaTECH' (Emma).

Dept	User Name	User ID	Role
Company	Unregistered IP	Unregistered II	
SomansaTECH	Emma	Emma	

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.)

The screenshot shows the 'Users' management interface in DLP+Center. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', 'MANAGE', and 'SYSTEM'. The left sidebar has 'MANAGE' selected, with 'Users' in the breadcrumb. The main content area shows a table of users with columns: Dept, User Name, User ID, and Role. The 'Add New' button is highlighted with a red box. The table contains two entries: 'Company' (Unregistered IP) and 'SomansaTECH' (Emma).

Dept	User Name	User ID	Role
Company	Unregistered IP	Unregistered II	
SomansaTECH	Emma	Emma	



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**

DLP+Center DASHBOARD REPORTS INCIDENTS POLICIES MANAGE SYSTEM

Manage Users

MANAGE

Alerts/Notifications

Users

Save

General

User Name * Unregistered IP

User ID * Unregistered IP

User Status Active

Dept Company Select

IP Use Static IP Add 1.0.0.1 ~ 254.255.255.254

Used Dynamic IP Data does not exist

Number of Employees

Position

Role Dept Leader or Admin Dept Privacy Officer Chief Privacy Officer Data Handler

Email

Telephone

DLP+Center DASHBOARD REPORTS INCIDENTS POLICIES MANAGE SYSTEM

Manage Users

MANAGE

Alerts/Notifications

Users

Filter

Add New Deactivate Manage Dept

Dept	User Name	User ID	Role
Company	Unregistered IP	Unregistered IP	
SomansaTECH	Emma	Emma	

Showing 1 to 2 of 2 entries

Company
Somansa
SomansaTECH
Emma(Emma)
Unregistered IP(Unregis)



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**

• Manage Dept

Move Add **Modify** Delete Close

Dept Name: SomansaTECH

Company

Somansa

SomansaTECH

6. Modify the Users

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

DLP+Center

DASHBOARD REPORTS INCIDENTS POLICIES **MANAGE** SYSTEM

Manage > Users

MANAGE

Alerts/Notifications

Users

Save

General

User Name * Emma

User ID * Emma

User Status Active

Dept SomansaTECH Select

IP Use Static IP Add

192.168.1.141 - 192.168.1.141

Used Dynamic IP

Data does not exist

Number of Employees

Position

Role

Dept Leader or Admin

Dept Privacy Officer

Chief Privacy Officer

Data Handler

Email Emma@somansatech.com

Telephone



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**

The screenshot shows the 'Users' management form in DLP+Center. The 'User Status' dropdown menu is highlighted with a red box and set to 'Deactivated'. Other fields include 'User Name' (Emma), 'User ID' (Emma), 'Dept' (SomansaTECH), and 'IP' (192.168.1.141).

The screenshot shows the 'Users' management interface in DLP+Center. The 'USERS' dropdown menu is highlighted with a red box and set to 'Deactivated'. The table below shows the user list.

Dept	User Name	User ID	Role
SomansaTECH	Emma	Emma	

Showing 1 to 1 of 1 entries



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**

The screenshot shows the DLP+Center interface with the 'Users' management page. The 'Filter' bar is expanded, showing search options for User Name, User ID, Role, etc. The 'Apply' button is highlighted. The table below shows the user data:

Dept	User Name	User ID	Role	Position	Created Date	Modified Time
Company	Unregistered IP	Unregistered IP			2017-06-01 17:14:12	2017-06-01 17:14:11
SomansaTECH	Emma	Emma			2017-06-05 14:45:46	2017-06-15 12:32:4

Showing 1 to 2 of 2 entries



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.

The screenshot shows the DLP+Center interface with the 'POLICIES' menu open to 'Detect' > 'Patterns'. The 'Add New' button is highlighted with a red box. Below it is a table of existing patterns:

Order	Pattern Name	Category
1	ALL: Confidential Data <input type="checkbox"/>	Basic
2	ALL: Corporate Financial Information <input type="checkbox"/>	Basic
3	ALL: Credit Card Number	Basic
4	ALL: Customer Code	Basic
5	ALL: Customer Data <input type="checkbox"/>	Basic

The screenshot shows the 'Add New' form for a pattern. The 'Pattern Type' is set to 'Regular Expression'. The 'Pattern Name' field is empty. The 'Expression' field has an 'Add' button. The 'Severity' is set to 'Low (0 - 50)'. The 'Save' button is visible at the top left of the form.

The screenshot shows the 'Add New' form for a pattern. The 'Pattern Type' is set to 'Keyword'. The 'Input Method' is set to 'Keyword Input'. The 'Save' button is visible at the top left of the form.



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

File Type	Format Name
	7z
	ALZip
	bzip2
	gzip

Save

Details

Format Name

File Type

Extension ?

Add



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 All Days, AM, Business Hours, Business Hours including Lunch, Non-Business Hours, PM and click **Save**

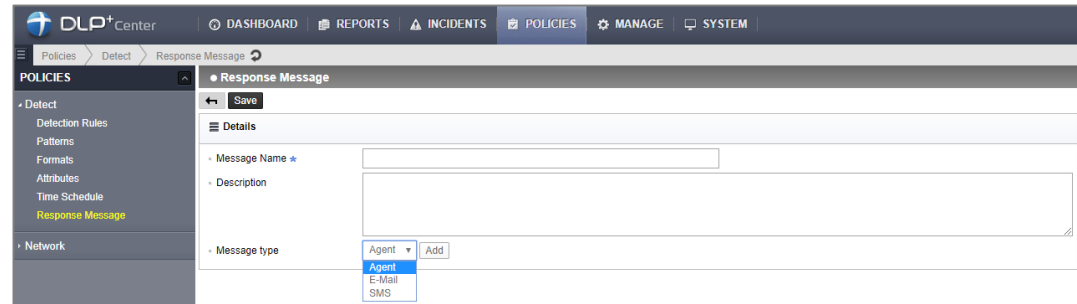
* It will be used in **Net App Prevent+**.



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.

The screenshot displays the DLP+Center web interface. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', and 'MANAGE'. The left sidebar shows a tree view with 'POLICIES' expanded to 'Detect', which includes 'Detection Rules', 'Patterns', 'Formats', 'Attributes', 'Time Schedule', and 'Response Message'. The main content area is titled 'Detection Rules' and features a 'Save' button. It is divided into sections: 'General' with a 'Rule Name' input field; 'Details' with 'Rule Type' options (Contents, Uninspectable, Attributes) each with a 'Select File Attributes' dropdown; and 'Advanced' with 'File Format Auto Detection' set to 'Off' and 'Compressed File Inspection' set to 'On'.



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 Policy Name and select the Targets
- 4) Select the Agent

※ 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

The screenshot shows the DLP+Center interface with the 'Net App Prevent+' policy configuration page. The 'Add New' button is highlighted with a red box. The page displays a table of existing policies.

On	Priority	Action	Policy Typ	Policy Name
<input type="checkbox"/>	1	Block	Control	All Net Apps
<input checked="" type="checkbox"/>	2	Allow	Control	Web Mail Allow

Showing 1 to 2 of 2 entries

The screenshot shows the DLP+Center interface with the 'Net App Prevent+' policy configuration page. The 'Targets' section is highlighted with a red box. The page displays the 'General' and 'Net App to Control' sections.

General

Policy Name:

Policy Description:

Targets

0 folders, 0 users,

Net App to Control

Agent: default

Policy Type: Control Prevent

Net App Settings:

- Electronic Mail (0/3) Access
- Web Mail (12/13) Access Write File Transfer Big File Attachment
- Instant Messaging (0/6) Access Chat File Transfer



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.

The screenshot shows the configuration page for a Net App Prevent+ policy. The 'Policy Type' is set to 'Control'. Under 'Net App Settings', the following settings are visible:

Net App	Access	Write	File Transfer	Big File Attachment
Electronic Mail (0/3)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Web Mail (12/13)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Instant Messaging (0/6)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The screenshot shows the policy list table. The 'Apply Policy' button is highlighted. The table contains the following entries:

On	Priority	Action	Policy Typ	Policy Name
<input type="checkbox"/>	1	Block	Control	All Net Apps
<input checked="" type="checkbox"/>	2	Allow	Control	Web Mail Allow



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.

- Check the Prevent of Policy Type
- Select Net App Settings and Detection Rule
- Select Time Range settings and Action
- Click **Save**
- If you want to apply for policy, you must active and click the **Apply Policy**

✘ You can prioritize policies.

The screenshot shows the DLP+Center interface for configuring a 'Net App Prevent+' policy. The breadcrumb trail is 'Policies > Network > Net App Prevent+'. A 'Save' button is visible. The configuration is split into several sections:

- General:** Fields for 'Policy Name' and 'Policy Description'.
- Net App to Control:** A dropdown menu for 'Agent' set to '[Select]'. Radio buttons for 'Control' and 'Prevent' (selected).
- Net App Settings:** Two rows of settings. The first row is for 'Electronic Mail (0/2)' with checkboxes for 'Body/File Content' (unchecked) and 'Recipient E-mail' (checked). The second row is for 'Web Mail (12/12)' with checkboxes for 'Body/File Content' (checked) and 'Recipient E-mail' (checked). A 'Sender E-mail' field is also present.

A red box highlights the 'Prevent' radio button and the 'Detection Rule ((Sample) Credit Card Numbers)' dropdown menu.



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**

The screenshot displays the DLP+Center web interface. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', 'MANAGE', and 'SYSTEM'. The left sidebar shows a tree view with 'POLICIES' expanded to 'Network' and 'Data Tagging' selected. The main content area is titled 'Data Tagging' and contains a 'Save' button, a 'General' section with 'Tag Name' (Driver License tagging) and 'Policy Description' fields, and a 'Targets' section with a 'Select' button. Below these are 'Net App to Control' settings, including 'Agent' (default), 'Detection Rules' ((Sample) Driver License Numbers), and 'Net App Settings' for Electronic Mail (0/2) and Web Mail (1/12). A table lists various Net App Names and their detailed settings.

Net App Name	Detailed Setting	Net App Name
AOL Mail	<input type="checkbox"/> Body/File Content	Daum Hanmail
Naver	<input type="checkbox"/> Body/File Content	Nate
<input checked="" type="checkbox"/> Gmail	<input checked="" type="checkbox"/> Body/File Content	Yahoo
Korea.com	<input type="checkbox"/> Body/File Content	Korea.kr
Microsoft Outlook Live	<input type="checkbox"/> Body/File Content	QQ Mail
iCloud Mail	<input type="checkbox"/> Body/File Content	OFFICE365_MAIL



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**

The screenshot shows the DLP+Center interface. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', and 'POLICIES'. The breadcrumb trail is 'Policies > Network > Net App Prevent+'. The left sidebar shows 'POLICIES' with a dropdown arrow, and 'Network' with sub-items 'Net App Prevent+' (highlighted in yellow) and 'Data Tagging'. The main content area is titled 'Net App Prevent+' and features a 'Filter' dropdown, 'Add New', and 'Apply Policy' buttons. Below these is a table with the following data:

On	Priority	Action	Policy Typ	Policy Name
<input type="checkbox"/>	⇅ 1	🚫 Block	Control	All Net Apps
<input checked="" type="checkbox"/>	⇅ 2	🟢 Allow	Control	Web Mail Allow

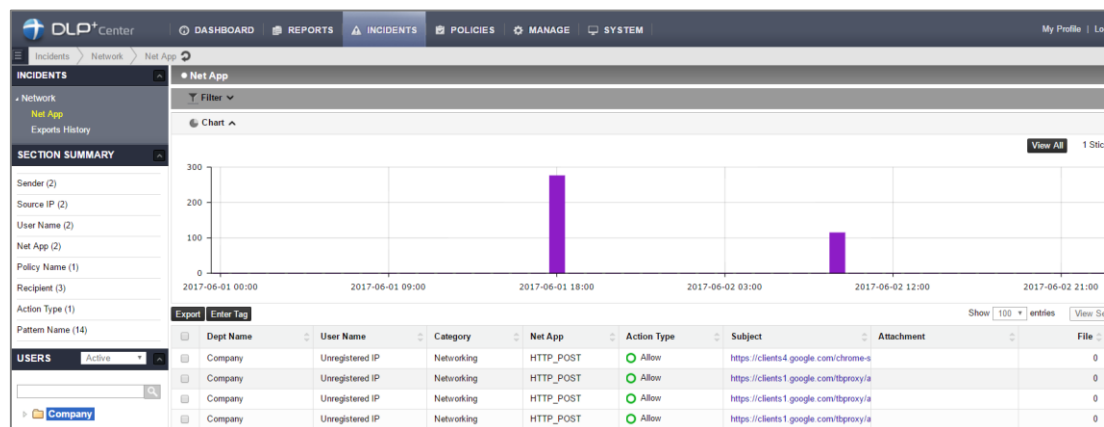
Showing 1 to 2 of 2 entries



IV. INCIDENTS

1. Check the Logs

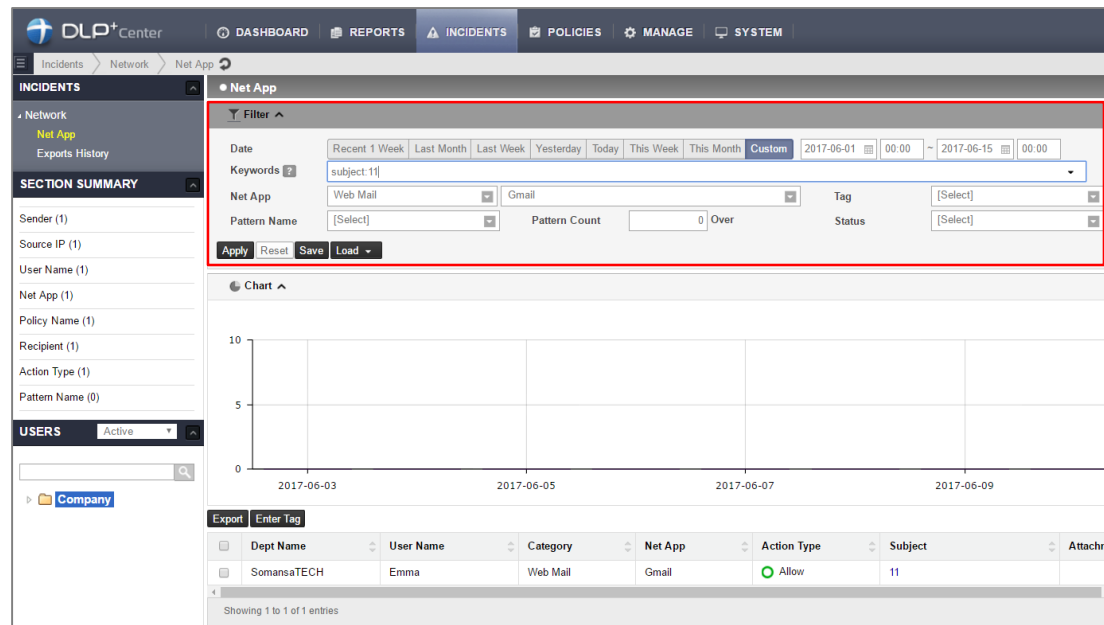
- 1) Select **INCIDENTS > Network > Net App**



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**

General	
Action Type	<input checked="" type="radio"/> Allow
User	none none ([No User]) [No Position information]
Occurred Time	2017-06-01 18:28:15
Source IP	192.168.1.141
Destination IP	216.58.195.229
Net App	Web Mail Gmail
Tag	
Size	350(Bytes)
Policy	

Body Contents	
Subject	Hello HM
Sender	192.168.1.141
Recipient	chohm@somansa.com
Cc	
BCC	

Nice to meet you

Pattern/File/Content Information	
Name	Pattern
Body	0
Total	0

Status and History	
• Status	<input type="text" value="Opened"/>
• Comments	<input type="text"/>
<input type="button" value="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**

The screenshot shows the DLP+Center interface with the 'INCIDENTS' tab selected. The left sidebar shows the navigation path: Network > Net App. The main area displays the 'Filter' configuration page for 'Net App'. The 'Keywords' field contains 'subject 11'. The 'Net App' dropdown is set to 'Web Mail' and the 'Tag' dropdown is set to 'Gmail'. The 'Pattern Name' dropdown is set to '[Select]'. The 'Pattern Count' is 0. The 'Apply', 'Reset', 'Save', and 'Load' buttons are visible at the bottom of the filter configuration area. The 'Save' button is highlighted with a red box. Below the filter configuration, there is a chart showing a single data point for '2017-06-03' with a value of 11. The table below the chart shows one entry: Dept Name: SomansaTECH, User Name: Emma, Category: Web Mail, Net App: Gmail, Action Type: Allow, Subject: 11.

5. Load the Filter

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

The screenshot shows the DLP+Center interface with the 'INCIDENTS' tab selected. The left sidebar shows the navigation path: Network > Net App. The main area displays the 'Filter' configuration page for 'Net App'. The 'Keywords' field contains 'subject 11'. The 'Net App' dropdown is set to 'Web Mail' and the 'Tag' dropdown is set to 'Gmail'. The 'Pattern Name' dropdown is set to '[Select]'. The 'Pattern Count' is 0. The 'Apply', 'Reset', 'Save', and 'Load' buttons are visible at the bottom of the filter configuration area. The 'Load' button is highlighted with a red box. Below the filter configuration, there is a dropdown menu showing 'subject 11' with a red 'x' icon next to it. The table below the dropdown shows one entry: Dept Name: SomansaTECH, User Name: Emma, Category: Web Mail, Net App: Gmail, Action Type: Allow, Subject: 11.



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 **SECTION SUMMARY**
- 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

The screenshot shows the DLP+Center interface. The 'INCIDENTS' tab is active, and the 'Net App' filter is selected. The 'SECTION SUMMARY' panel on the left lists various conditions: Sender (2), Source IP (2), User Name (3), Net App (2), Policy Name (1), Recipient (4), Action Type (1), and Pattern Name (14). A popup window titled '[Source IP] Top10' is displayed over the 'Source IP (2)' condition, showing a table of top source IP addresses.

Source IP	Count	Percentage
192.168.1.141	1,033	99.81 %
192.168.1.120	2	0.19 %

7. Export the Logs (format .csv)

- 1) Select **INCIDENTS > Network > Net App**
- 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**



Sample.csv

The screenshot shows the DLP+Center interface with the 'SECTION SUMMARY' panel on the left and a bar chart on the right. The bar chart displays the number of incidents for different dates in June 2017. An 'Export' button is visible in the top right corner of the main content area.

Date	Count
2017-06-01	300
2017-06-04	100
2017-06-13	600



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**

The screenshot shows the DLP+Center web interface. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', 'MANAGE', and 'SYSTEM'. The left sidebar shows 'INCIDENTS' with sub-items for 'Network' and 'Net App'. The main content area is titled 'Net App' and features a 'Filter' section with options for Date, Keywords, Net App, Pattern Name, Tag, and Status. Below the filter is a 'Chart' area and a table of incident entries. The 'Export' button is highlighted with a red box.

Dept Name	User Name	Category	Net App	Action Type	Subject	Attachment
SomansaTECH	Emma	Web Mail	Gmail	Allow	11	



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**

Export Name
ee
test

File Name	File Size(KB)	
test.zip	648 (KB)	



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 Show 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 order you want and click **Save**

The screenshot displays the DLP+Center web interface. The top navigation bar includes DASHBOARD, REPORTS, INCIDENTS, POLICIES, MANAGE, and SYSTEM. The left sidebar shows the navigation menu with 'INCIDENTS > Net App' selected. The main content area is titled 'Net App' and contains a filter section with options for Date, Keywords, Net App, and Patterns Name. Below the filter is a chart showing incident counts over time. At the bottom, a table lists incidents with columns for Dept Name, User Name, Category, Net App, Action Type, Subject, Attachment, and File. A red box highlights the 'Show 100 entries View Settings' link in the bottom right corner of the table.

Dept Name	User Name	Category	Net App	Action Type	Subject	Attachment	File
SomansaTECH	Emma	Web Mail	Gmail	Allow	11		0



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

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	Emna	351	46	14	4	1	

2. Apply the Filter

- 1) Select **REPORTS > Network**
- 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**

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

- 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 .csv, 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**

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	

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 **Alerts/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.

The screenshot displays the DLP+Center web interface. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', 'MANAGE', and 'SYSTEM'. The 'MANAGE' tab is active, and the breadcrumb trail shows 'Manage > Alerts/Notifications > Reports'. A left sidebar menu has 'MANAGE' selected, with sub-items for 'Alerts/Notifications' and 'Reports'. The main content area shows a table with one report entry: '(Weekly) Top User Report' with a 'Report Type' of 'Network > Top Users'. An 'Add New' button is visible above the table. The footer of the table indicates 'Showing 1 to 1 of 1 entries'.

Report Name	Report Type
(Weekly) Top User Report	Network > Top Users



VII. Dashboard

1. Settings

- Sets the patterns and components to activate on the dashboard

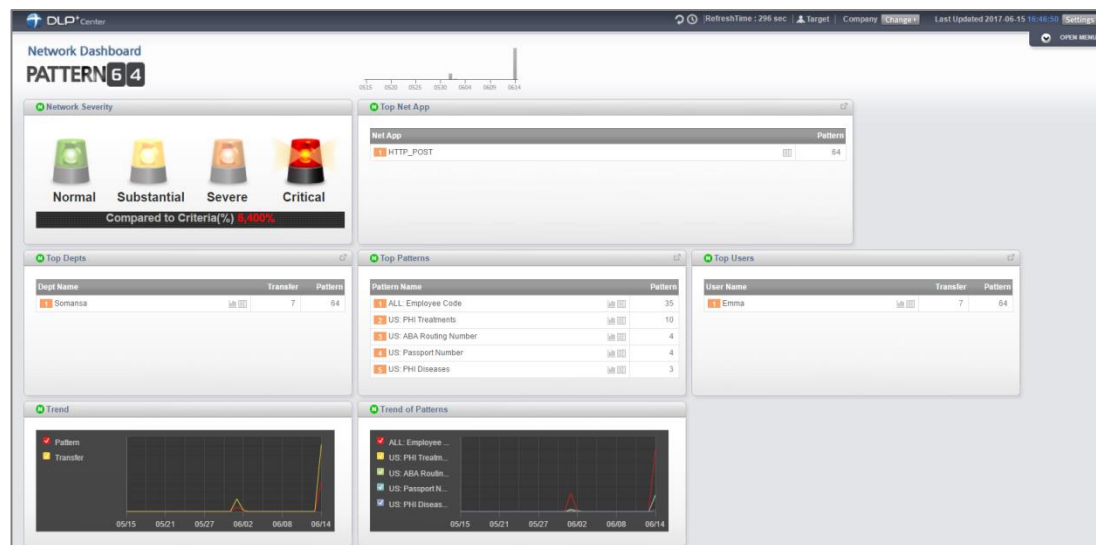
- 1) Select **Dashboard > Settings**
- 2) Enter the Update Cycle, select the Patterns and Components
- 3) Components can be reordered using the cross-shaped buttons and detailed settings can be made by clicking the down arrow
- 4) Click **Apply**

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**

User ID	IP	Type	Time	Contents
admin	192.168.1.141	View	2017-06-15 16:41:40	View from System > Logs > Audit Log
admin	192.168.1.141	View	2017-06-15 16:41:39	View from System > Logs > Audit Log

2. DLP Mining Engine

- You can check the log of data analysis status.

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

Type	Time	Contents
Login(Administrator)	2017-06-15 16:41:38	Network data analysis started.
Login(Administrator)	2017-06-15 16:41:38	Network data analysis ended.

Showing 1 to 2 of 2 entries



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.

Admin ID	Role	Users
admin	Admin	1 0
somansa	Operator	1 0
don_lee	Viewer	2 1

Showing 1 to 3 of 3 entries

Permissions

Access Authority

- Dashboard
- Reports
- Incidents
- Policies
 - Detect
 - Detection Rules
 - READ
 - WRITE



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.

The screenshot displays the DLP+Center web interface. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', 'MANAGE', and 'SYSTEM'. The left sidebar shows a tree view with 'SYSTEM' expanded, containing 'Logs', 'Admins', and 'Settings', with 'General' selected under 'Settings'. The main content area is titled 'General' and features a 'Save' button. It is divided into three sections: 'Display Parameter' with 'List Output Number' (100) and 'Filter Area Settings' (Close); 'Authentication' with 'Duplicate Login' (Allow), 'Password Input Time Limit' (3), 'Password Minimum Length' (9), 'Password Expiration Policy' (Off), 'Admin password reset' (Off), and 'First-Login Policy' (Off); and 'Language' with 'Default Language' (English). Valid ranges for password settings are noted as 1-99 for time limit and 9-99 for length.



SOMANSA

www.somansatech.com