



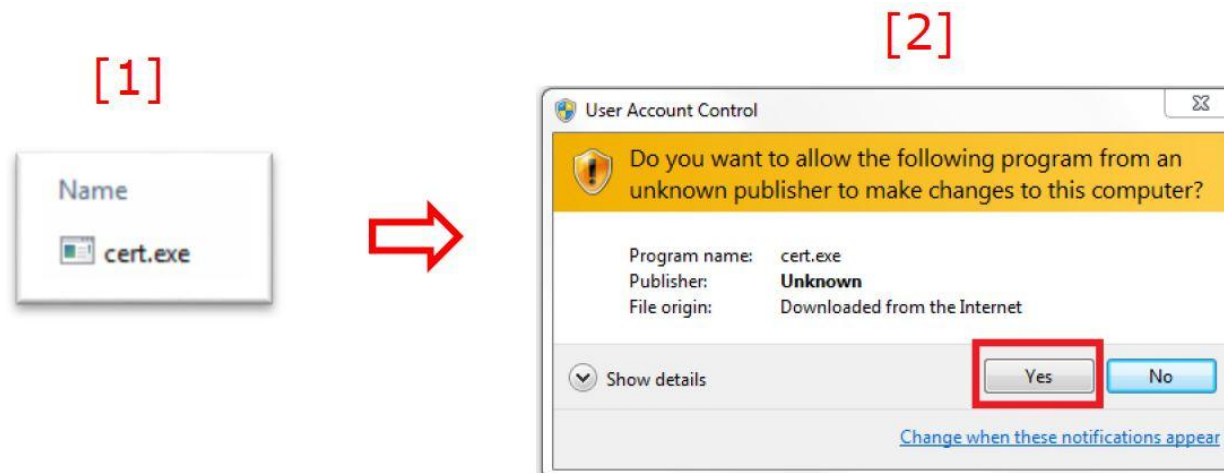
Mail-iTM
Mail-i Trial Demo Guide

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



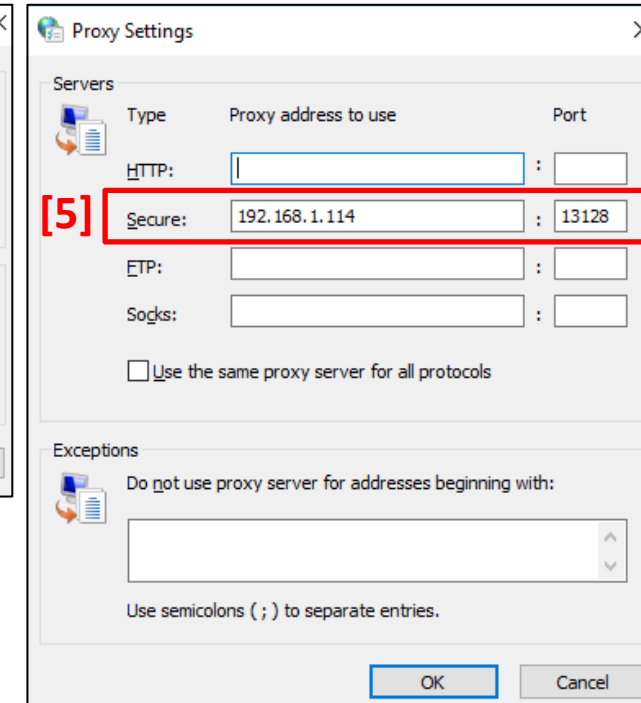
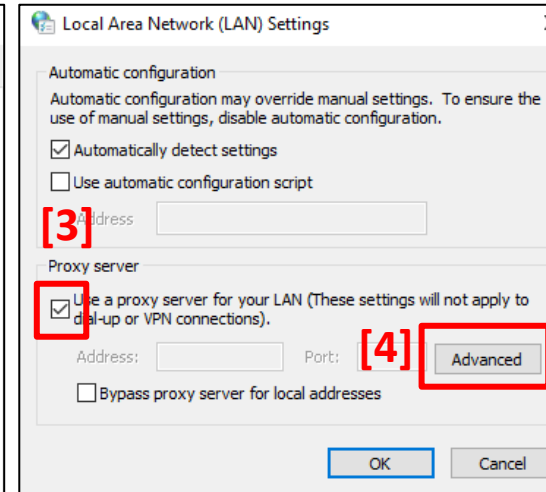
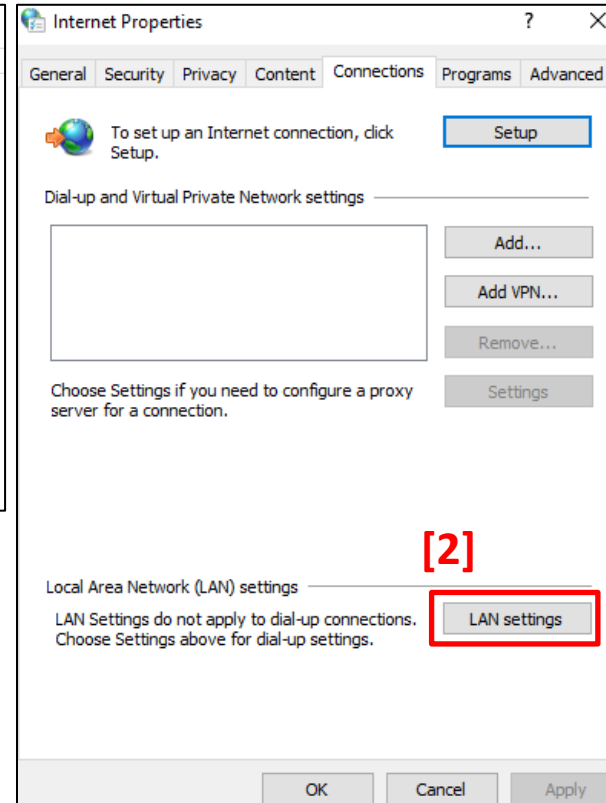
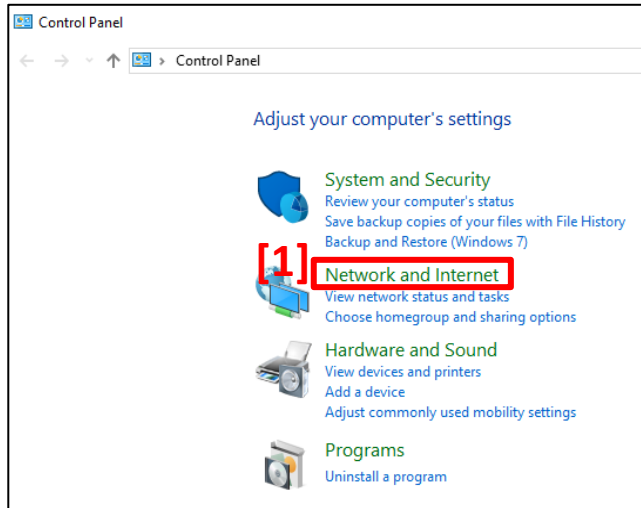
I. Setting before using Mail-i Trial Demo

- 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)



 **DLP+ Center**
Mail-i V8.0 for DLP+ HyBoost

ID

Password

LOGIN

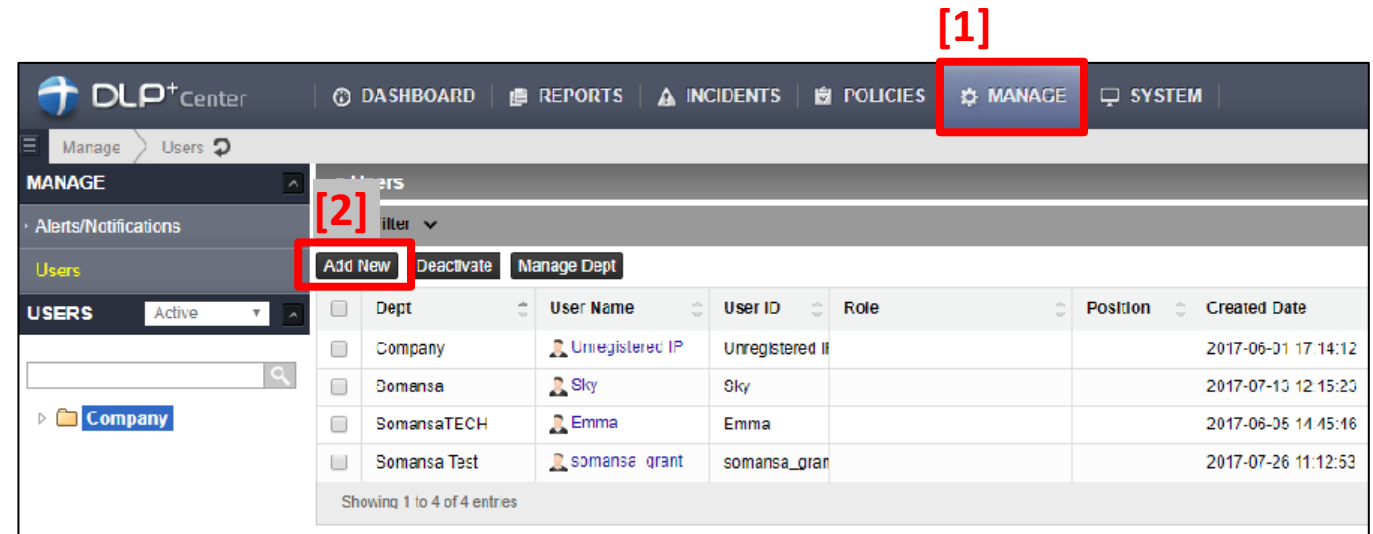
Please change your password periodically.
Contact your administrator for Login Help.

Copyright 2017 SOMANSA Co., Ltd. all rights reserved.

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**



The screenshot shows the DLP+ Center interface. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', 'MANAGE', and 'SYSTEM'. The 'MANAGE' menu item is highlighted with a red box and labeled [1]. Below the navigation bar, the 'MANAGE' section is active, showing 'Users' and 'Alerts/Notifications'. The 'Users' section has a search bar and a dropdown menu set to 'Active'. The 'Add New' button is highlighted with a red box and labeled [2]. The 'Users' table has the following columns: Dept, User Name, User ID, Role, Position, and Created Date. The table contains four entries:

Dept	User Name	User ID	Role	Position	Created Date
Company	Unregistered IP	Unregistered IP			2017-06-01 17:14:12
Somansa	Sky	Sky			2017-07-13 12:15:23
SomansaTECH	Emma	Emma			2017-06-25 14:45:16
Somansa Test	somansa_grant	somansa_grant			2017-07-26 11:12:53

Showing 1 to 4 of 4 entries

* 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'

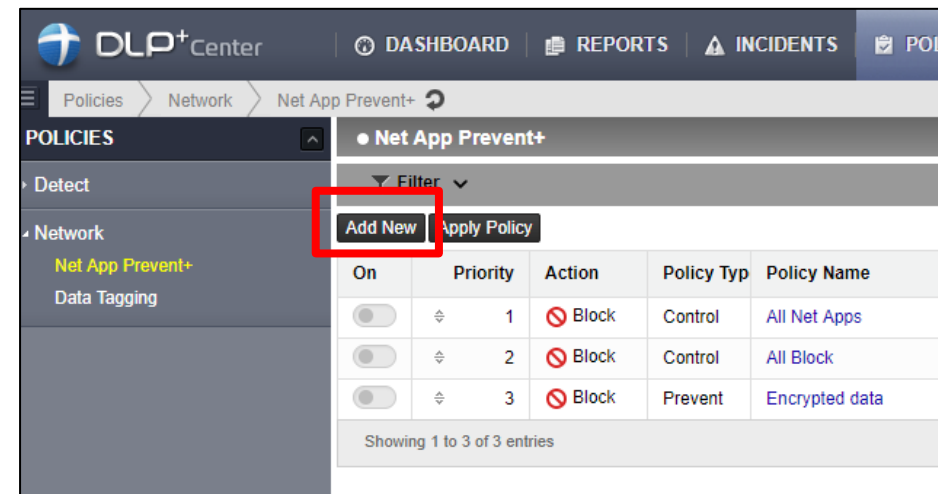
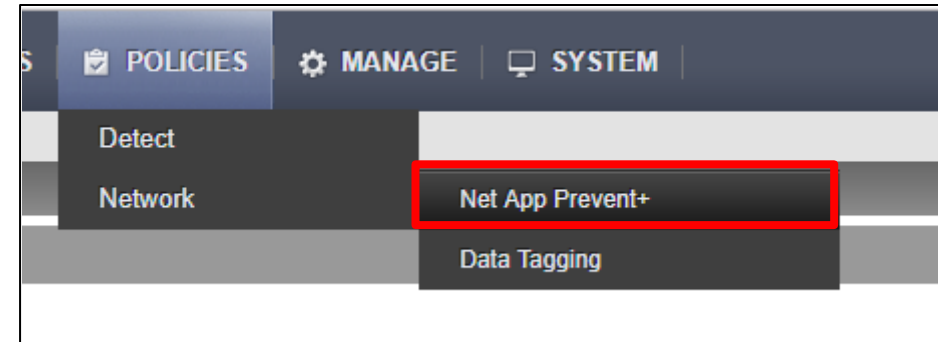
There are 2 types of Policy Type (Control / Prevent).

- 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**.

DASHBOARD | REPORTS | INCIDENTS | **POLICIES** | MAINTENANCE

Prevent+ ↻

• Net App Prevent+

← Save

☰ General

• Policy Name: Gmail Block

• Policy Description: Block Gmail if there are credit card numbers more than 5.

4. Select the **Target**.

You can choose certain users or departments.

You can also search existed names or departments.

• Targets [OK] [Cancel]

☰ All Targets

☰ Selected Targets

Name: []

Apply	Name	Dept	Expiration Date
<input checked="" type="checkbox"/>	somansa_grant(somansa_grant)	Somansa Test	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Somansa		<input checked="" type="checkbox"/>

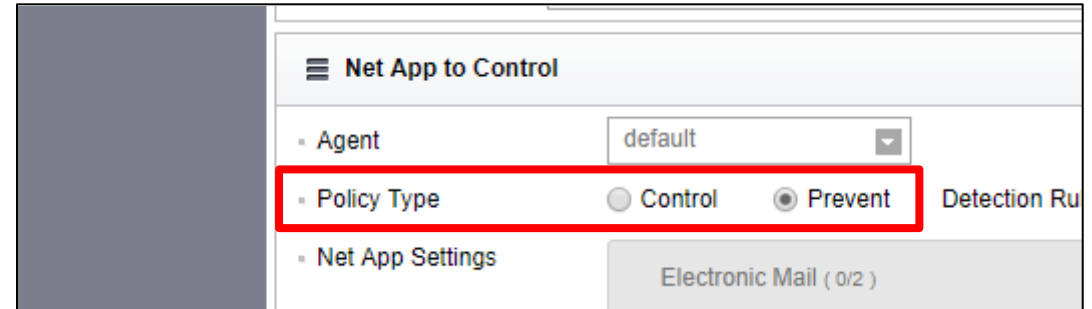
Showing 1 to 2 of 2 entries

☰ Targets

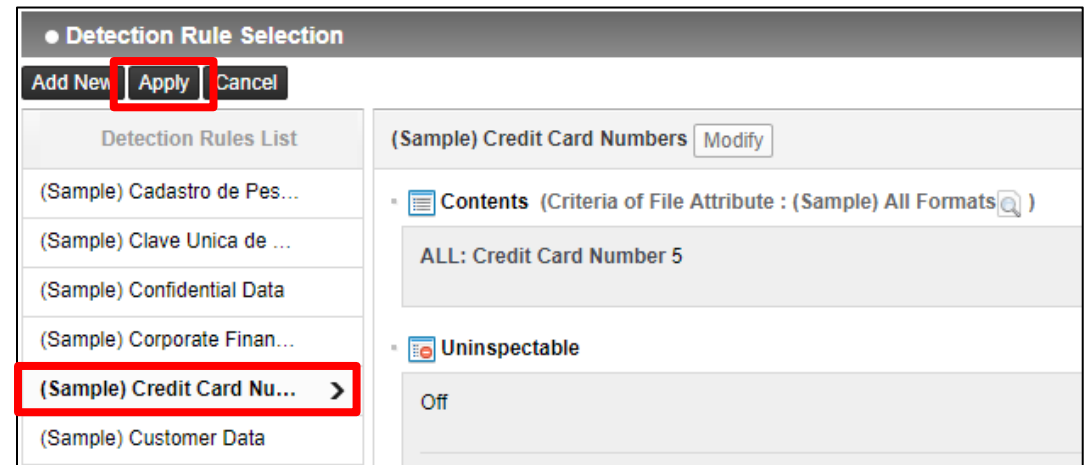
1 1 [Select]

Case 1. Prevent Email

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

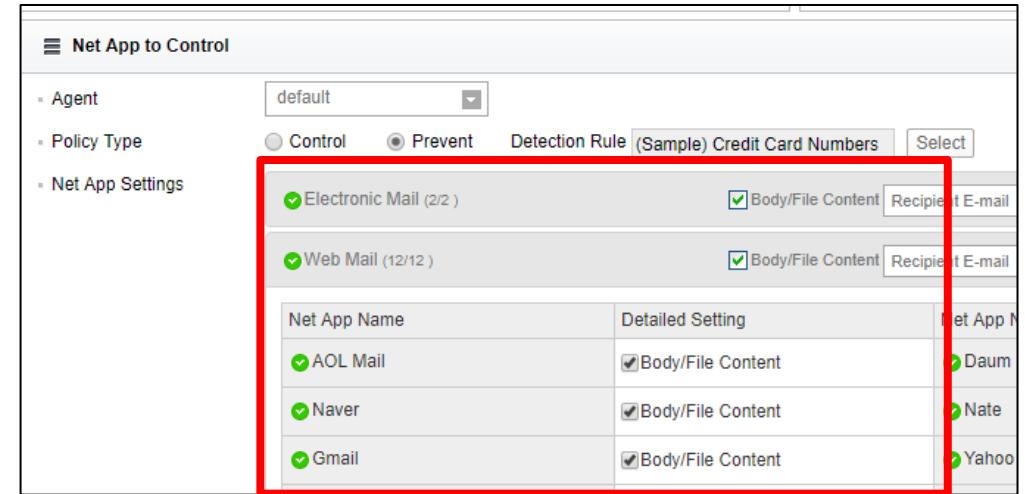


6. Select a **Detection Rule** and click **Apply** button.



Case 1. Prevent Email

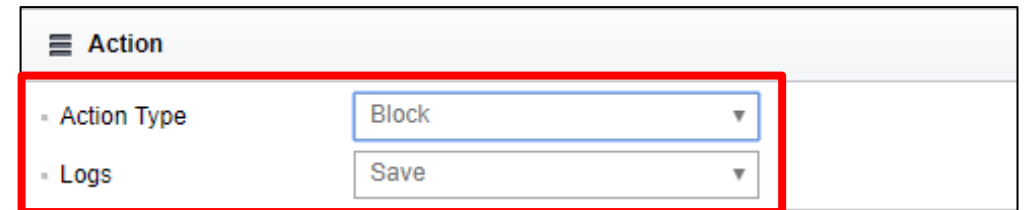
7. Check **Net App Settings**



The screenshot shows the 'Net App to Control' configuration window. The 'Agent' is set to 'default'. The 'Policy Type' is set to 'Prevent'. The 'Detection Rule' is '(Sample) Credit Card Numbers'. The 'Net App Settings' section is highlighted with a red box and contains the following items:

- Electronic Mail (2/2) with 'Body/File Content' checked.
- Web Mail (12/12) with 'Body/File Content' checked.
- AOL Mail with 'Body/File Content' checked.
- Naver with 'Body/File Content' checked.
- Gmail with 'Body/File Content' checked.

8. Set **Action Type** as Block




The screenshot shows the 'Action' configuration window. The 'Action Type' is set to 'Block' and the 'Logs' are set to 'Save'. Both the 'Action Type' and 'Logs' dropdown menus are highlighted with a red box.

Case 1. Prevent Email

9. Set **Time Schedule**

10. Click **Save** button

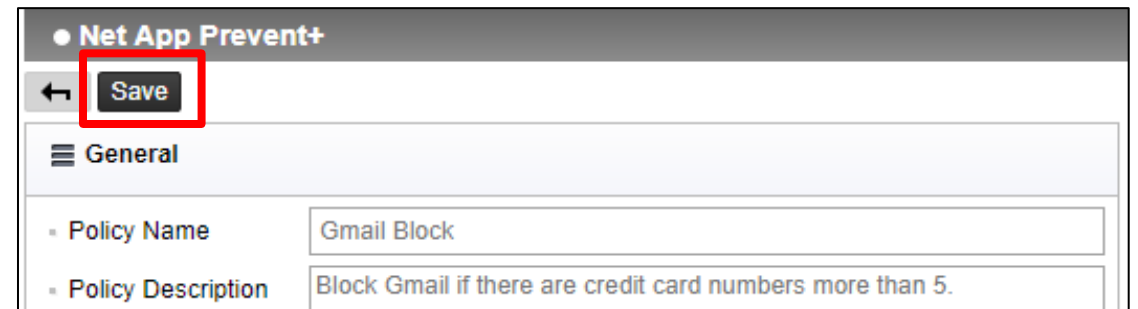
11. Click **Apply Policy** button



Time Range Settings Shortcut

Time Range: All Days View

Usage Period: Don't Specify



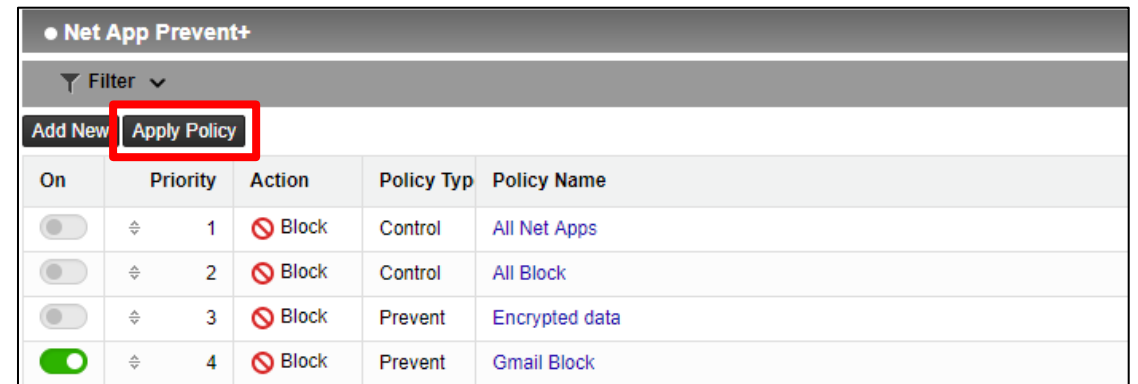
Net App Prevent+

Save

General

Policy Name: Gmail Block

Policy Description: Block Gmail if there are credit card numbers more than 5.



Net App Prevent+

Filter

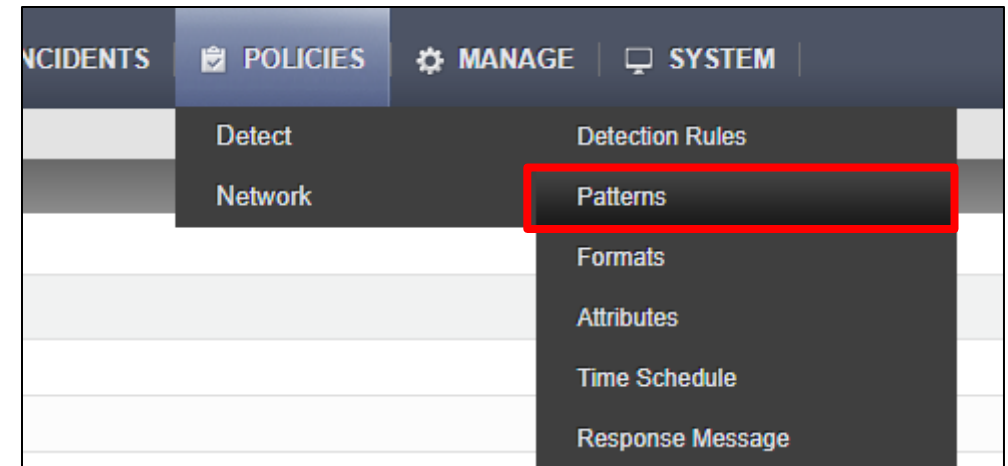
Add New **Apply Policy**

On	Priority	Action	Policy Typ	Policy Name
<input type="checkbox"/>	1	Block	Control	All Net Apps
<input type="checkbox"/>	2	Block	Control	All Block
<input type="checkbox"/>	3	Block	Prevent	Encrypted data
<input checked="" type="checkbox"/>	4	Block	Prevent	Gmail Block

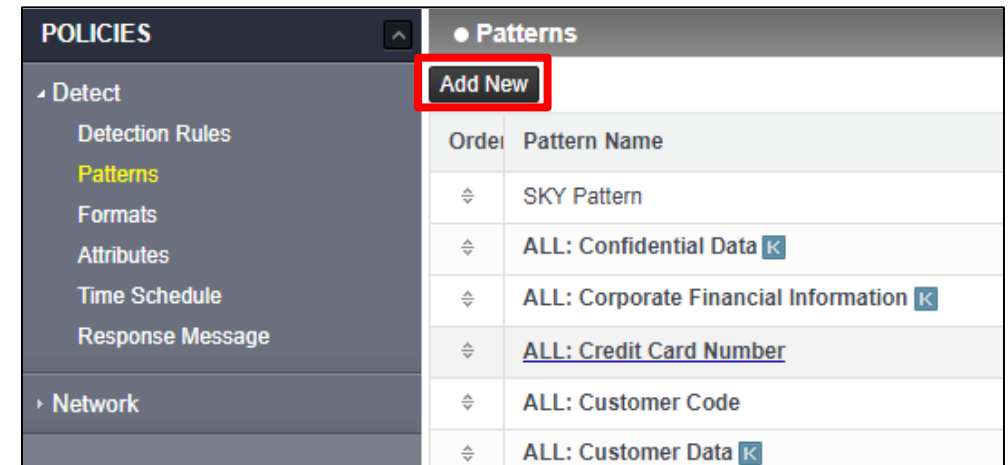
Case 2. Tag Logs

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

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



2. Click **Add New** button



Case 2. Tag Logs

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

4. Click **Save** button

Patterns

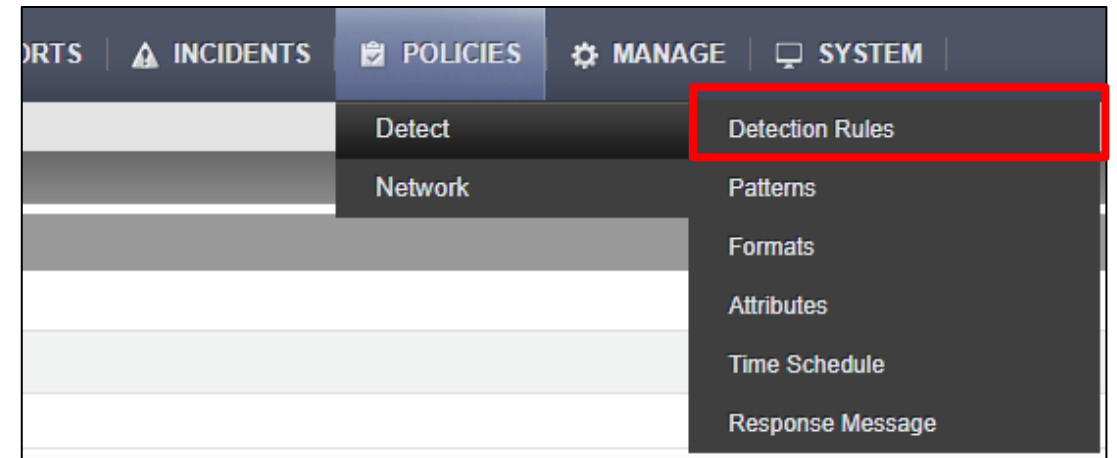
← Save Delete

Details

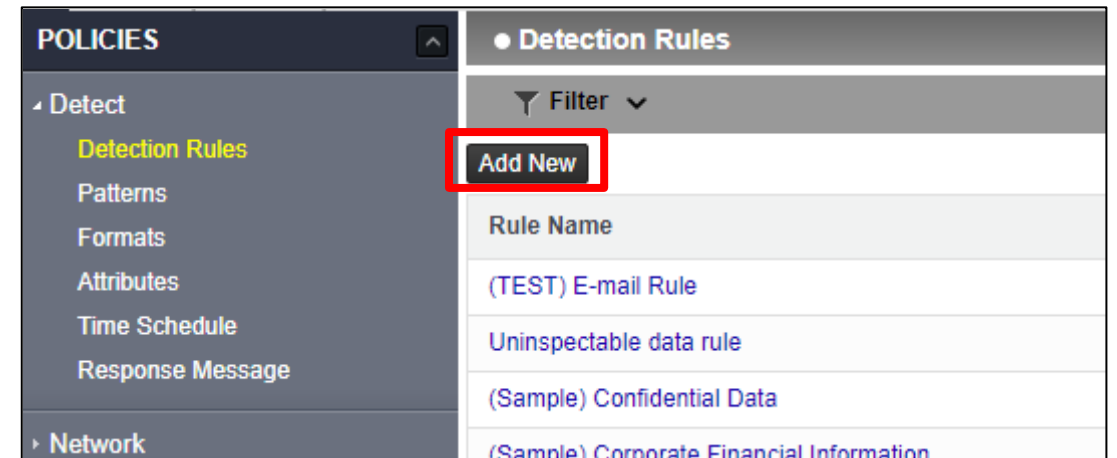
- Pattern Type *
 - Regular Expression
 - Keyword
- Pattern Name
 - Security Highlight
- Description
 - find the keyword as 'security'
- Input Method *
 - Keyword Input ?
 - File Upload ?
- Severity ?
 - 0 **Low (0 ~ 49)** **Mid (50 ~ 99)** **High (100 ~ ∞)** ∞

Case 2. Tag Logs

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



6. Click **Add New** button

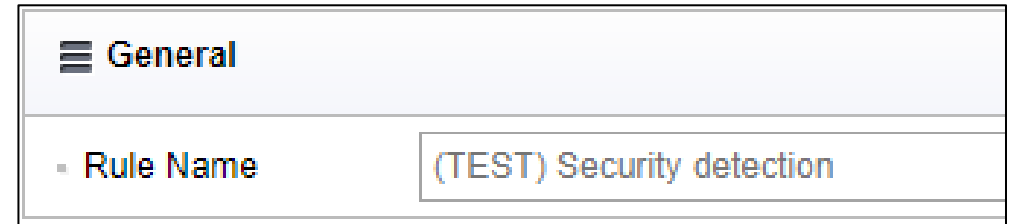


Case 2. Tag Logs

7. Put **Rule Name**

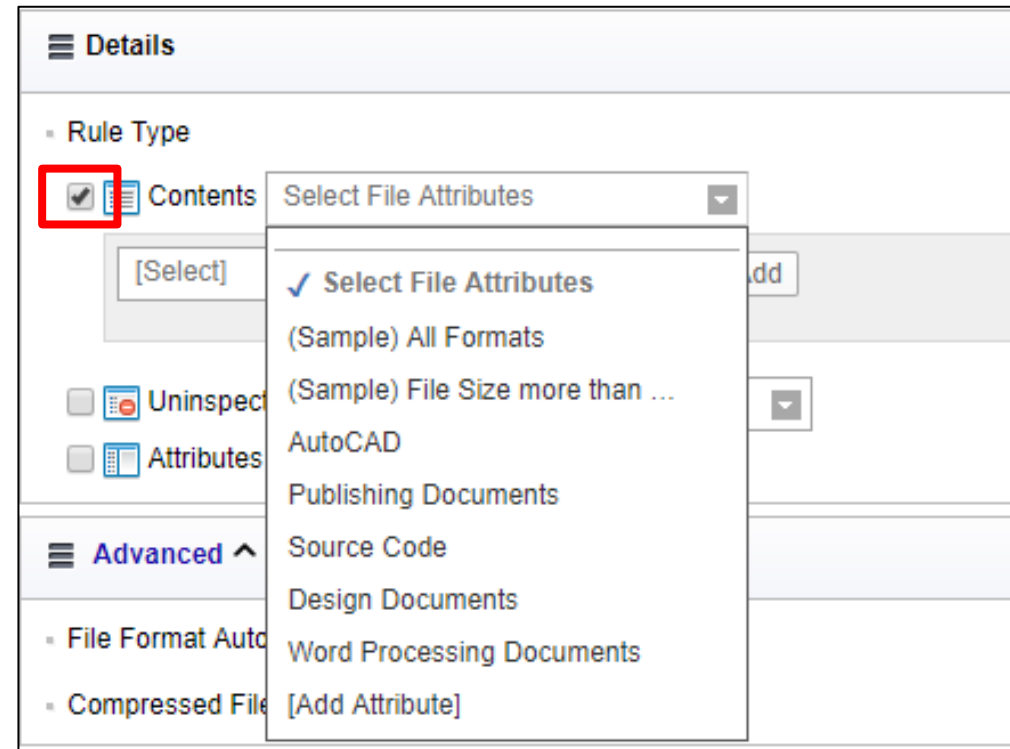
8. Select **Rule Type** as **Contents**

9. Select **File Attributes**



General

Rule Name (TEST) Security detection



Details

Rule Type

Contents Select File Attributes

[Select]

Uninspect

Attributes

Advanced ^

File Format Auto

Compressed File

Select File Attributes

- ✓ Select File Attributes
- (Sample) All Formats
- (Sample) File Size more than ...
- AutoCAD
- Publishing Documents
- Source Code
- Design Documents
- Word Processing Documents
- [Add Attribute]

Case 2. Tag Logs

10. Select the **Pattern**

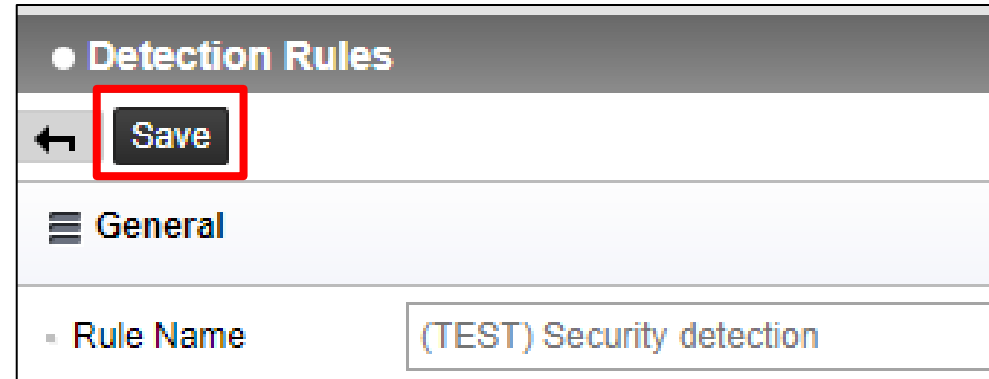
11. Click **Add** button and
Set **Total Number of Patterns**
Settings

The screenshot displays a software interface for configuring tag logs. It is divided into two main sections. The top section, titled "Rule Type", contains a dropdown menu set to "(Sample) All Formats" and a "Security" dropdown menu. Below the "Security" menu is a list of patterns with checkboxes: "US: Driver's License Number - WA", "US: ICD 10 Code", "US: Medical Record Number", "US: Passport Number", "US: PHI Diseases", "US: PHI Treatments", "US: Sarbanes Oxley Act", "US: Social Security Number", "ALL: Credit Card Security Code", "JP: MyNumber", and "Security". The "Security" pattern is selected and highlighted with a red box. An "Add" button is visible to the right of the "Security" dropdown. The bottom section shows a table with two columns. The first column contains the name of the pattern, "Security". The second column is labeled "Total Number of Patterns Settings" and contains a text input field with the value "1". An "Add" button is also present in this section, highlighted with a red box.

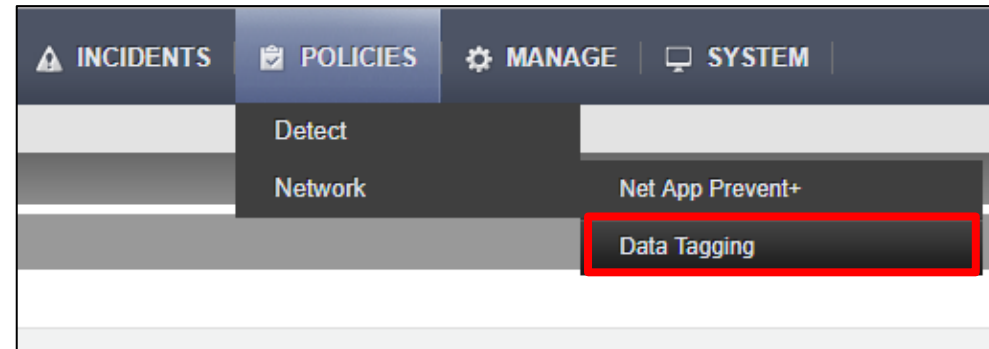
Pattern Name	Total Number of Patterns Settings
Security	1

Case 2. Tag Logs

12. Click **Save** button



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

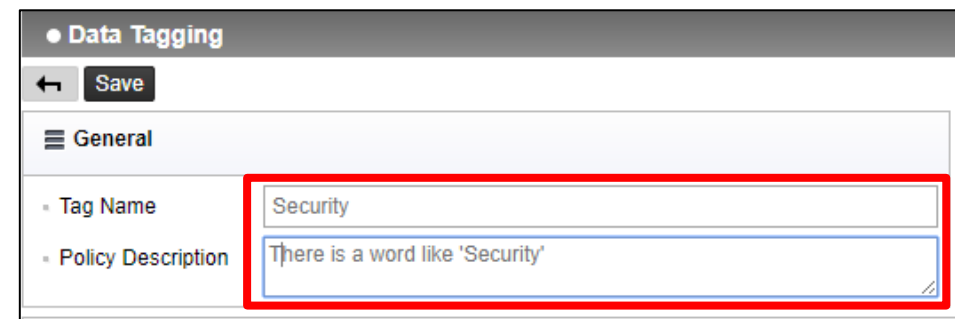


Case 2. Tag Logs

14. Click **Add New** button

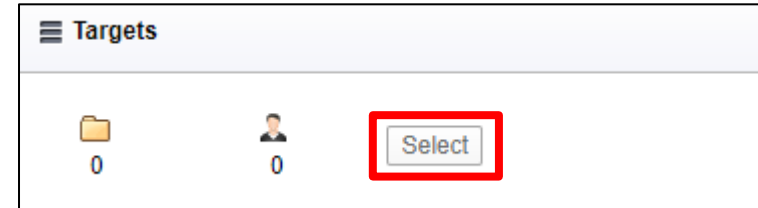


15. Put **Tag Name** and **Policy Description**

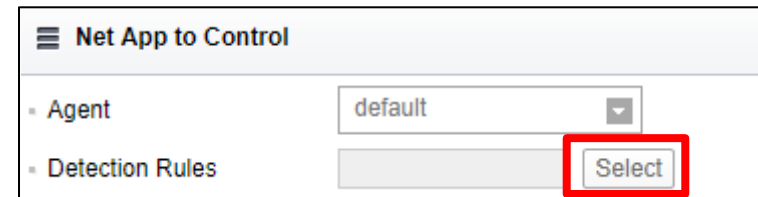


Case 2. Tag Logs

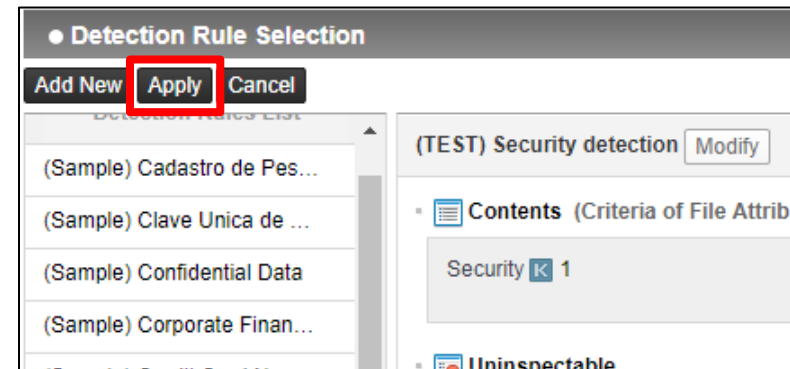
16. Select **Target**



17. Select **Detection Rules**



18. Click **Apply** button



Case 2. Tag Logs

19. Check **Net App Settings**

Net App Settings

Electronic Mail (2/2) Body/File Content Recipient E-mail Sender

Web Mail (12/12) Body/File Content Recipient E-mail Sender

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

20. Click **Save** button

Data Tagging

← Save

≡ General

21. Click **Apply Policy** button

Data Tagging

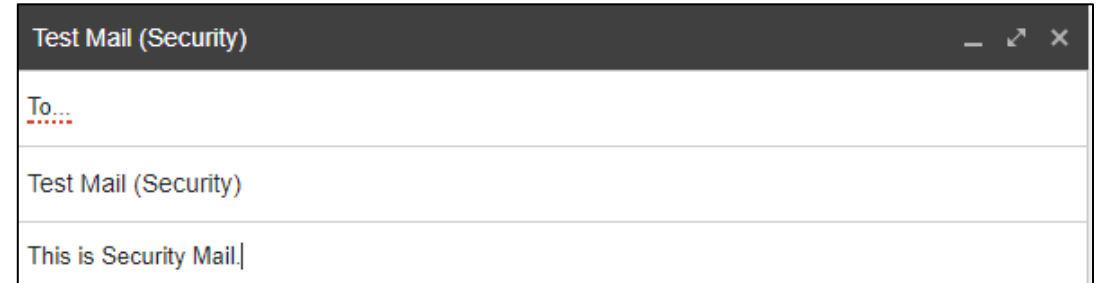
Filter ▾

Add New **Apply Policy**

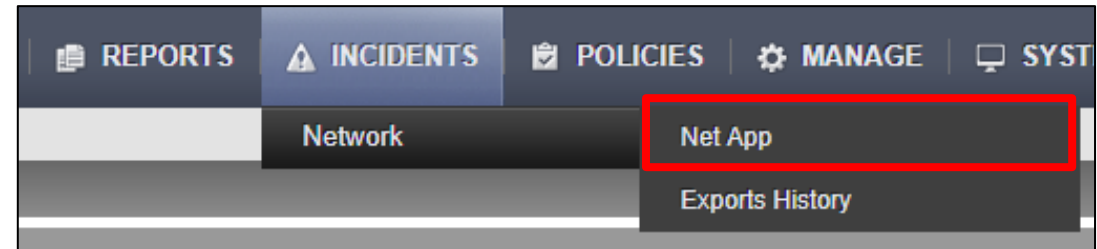
On	Tag Name
<input checked="" type="checkbox"/>	Driver License tagging
<input checked="" type="checkbox"/>	Security

Case 2. Tag Logs

22. Write and Send a test mail



23. Click **INCIDENTS** >
Network > **Net App**

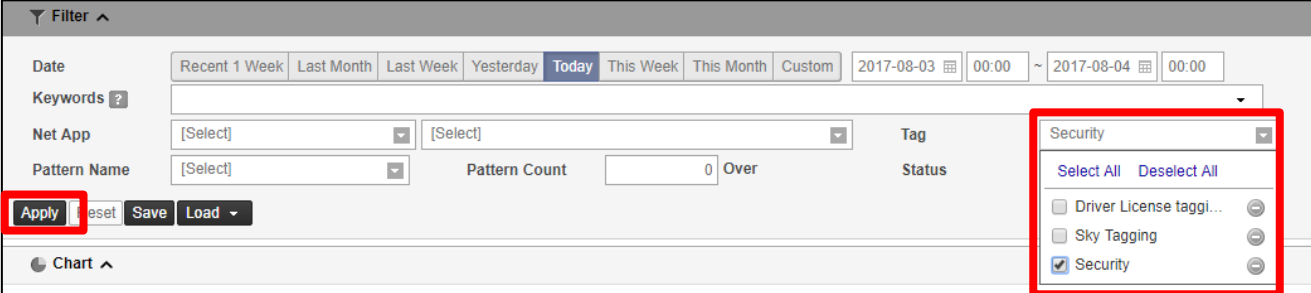


Case 2. Tag Logs

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

25. Click **Apply** button

26. You can check a tag next to the subject



The screenshot shows a 'Filter' panel with various search criteria. The 'Tag' dropdown menu is open, displaying a list of tags: 'Security' (checked), 'Driver License taggi...', 'Sky Tagging', and 'Security'. The 'Apply' button is highlighted with a red box.

Category	Net App	Action Type	Subject	
Web Mail	Gmail	Allow	test mail	Security

III. DLP+ Center (Detail instructions)

1. Log-in DLP+ Center

https://IP_address/DLPcenter

ID: (Given ID)

PW: (Given Password)



The screenshot shows the login page for the DLP+ Center. At the top left is a logo consisting of a blue and white globe. To its right is the text "DLP+ Center" in a bold, sans-serif font, with "Mail-i V8.0 for DLP+ HyBoost" in a smaller font below it. The main content area has a dark blue background. It features two input fields: one labeled "ID" and one labeled "Password". To the right of these fields is a blue button with the word "LOGIN" in white capital letters. Below the input fields, there is a small white text box containing the message: "Please change your password periodically. Contact your administrator for Login Help." At the bottom of the page, there is a copyright notice: "Copyright 2017 SOMANSA Co., Ltd. all rights reserved."

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**

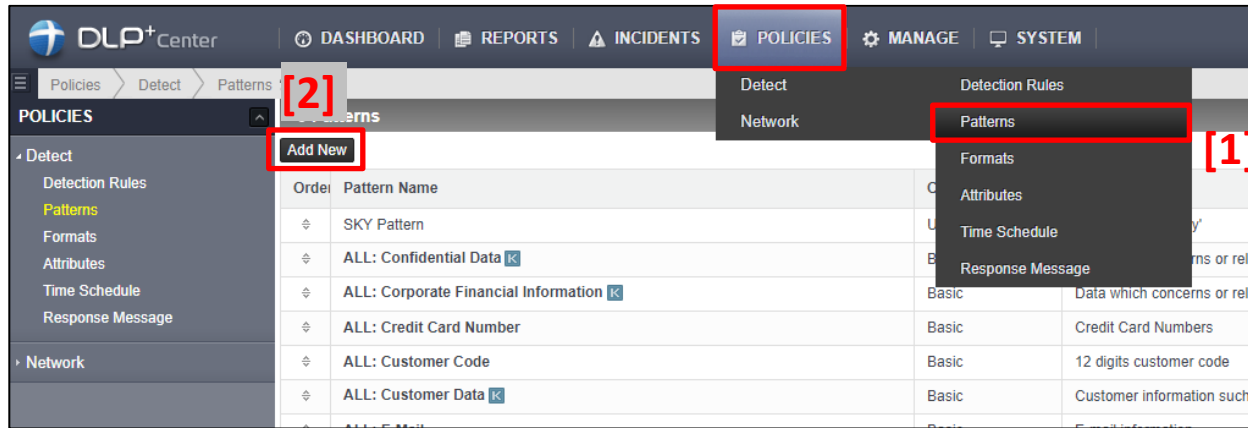
The screenshot shows the DLP+ Center interface. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', 'MANAGE', and 'SYSTEM'. The 'MANAGE' menu item is highlighted with a red box and labeled [1]. Below the navigation bar, the 'MANAGE' section is active, showing a breadcrumb 'Manage > Users'. The 'Users' table is displayed with columns: Dept, User Name, User ID, Role, Position, and Created Date. The 'Add New' button is highlighted with a red box and labeled [2]. The table contains four entries:

Dept	User Name	User ID	Role	Position	Created Date
Company	Unregistered IP	Unregistered IP			2017-06-01 17:14:12
Somansa	Sky	Sky			2017-07-13 12:15:23
SomansaTECH	Emma	Emma			2017-06-25 14:45:16
Somansa Test	somansa_grant	somansa_grant			2017-07-26 11:12:53

Showing 1 to 4 of 4 entries

* 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**

The screenshot shows the 'Patterns' configuration form. The 'Save' button is highlighted with a red box and labeled [6]. The 'Pattern Type' is set to 'Regular Expression' (labeled [3]). The 'Pattern Name' field is highlighted with a red box and labeled [4]. The 'Expression' field is highlighted with a red box and labeled [5]. The 'Severity' is set to 'Low (0 ~ 50)'.

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

File Type	Format Name	Extension
	7z	7z
	ALZip	alz
	bzip2	bz2
	gzip	gz,tgz
	JAR	jar
	LHA	lzh,lha
	RAR	rar
Archive	Tape archive	tar

• 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.

DLP+ Center | DASHBOARD | REPORTS | INCIDENTS | **POLICIES** | MANAGE | SYSTEM

Policies > Detect > Attributes

POLICIES

- Detect
 - Detection Rules
 - Patterns
 - Formats
 - Attributes**
 - Time Schedule
 - Response Message
- Network

Attributes

[2] Add New

[1] Attributes

Attribute Name
(Sample) All Formats
(Sample) File Size more than 100kbytes
AutoCAD
Design Documents
Publishing Documents
Source Code
Word Processing Documents

Showing 1 to 7 of 7 entries

• 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.

Attributes **[3]**

[4] Save

Details

Attribute Name	<input type="text"/>
File Name	Off
Path ?	Off
File Format ?	All Formats
File Size	Off

The screenshot shows the DLP+ Center interface. At the top, there is a navigation bar with 'POLICIES' highlighted. Below it, a dropdown menu is open, showing 'Detect' and 'Network' categories. Under 'Detect', there are sub-options: 'Detection Rules', 'Patterns', 'Formats', 'Attributes', 'Time Schedule', and 'Response Message'. The 'Time Schedule' option is highlighted with a red box and labeled [1]. On the left sidebar, under 'POLICIES', the 'Time Schedule' option is also highlighted with a red box and labeled [2]. The main content area shows a list of time ranges with columns for 'Time Range Name' and 'Description'. The list includes 'All Days', 'AM', 'Business Hours', 'Business Hours including Lunch', 'Non-Business Hours', 'PM', and 'test'. At the bottom, it says 'Showing 1 to 7 of 7 entries'.

• 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**

The screenshot shows the 'Time Schedule' details form. At the top, there is a 'Save' button highlighted with a red box and labeled [5]. Below it, there is a 'Details' section. The 'Time Range Name' field is filled with 'Night Time' and has a blue message 'The attribute name is valid.' next to it, labeled [3]. The 'Description' field is empty. Below the 'Description' field is the 'Setting' section, which contains a table with columns for 'Time', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'. The table is highlighted with a red box and labeled [4]. The table has rows for 'All' and '00', '01', '02', and '03'.

Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat
All							
00							
01							
02							
03							

- * If you want to **delete** time schedule, select time range name and click **delete** button.
- * It will be used in **Net App Prevent+**.

[1] POLICIES

[2] Add New

Rule Name	Rule Type
(TEST) E-mail Rule	Contents, Uninspectable
Uninspectable data rule	Contents, Uninspectable
(Sample) Confidential Data	Contents
(Sample) Corporate Financial Information	Contents
(Sample) Customer Data	Contents
(Sample) Design Documents	Attributes
(Sample) Employee Data	Contents
(Sample) US: Financial Information	Contents
(Sample) US: Privacy Information File Size more than 100kbytes	Contents
(Sample) US: Healthcare Information	Contents

• 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**

[3] Save

[4] Rule Type

- Contents Select File Attributes
- Uninspectable Select File Attributes
- Attributes

[5] Save

General

Rule Name

Details

Advanced

- File Format Auto Detection Off
- Compressed File Inspection On

- * If you want to **delete** detection rules, select Rule Name and click **delete** button.
- * It will be used in **Net App Prevent+**.

Navigation: DASHBOARD | REPORTS | INCIDENTS | **POLICIES** [1] | SYSTEM

Sub-navigation: Policies > Network > Net App Prevent+

Buttons: [2] Add New, [7] Apply Policy

On	Priority	Action	Policy Type	Policy Name	Targets
<input checked="" type="checkbox"/>	1	Block	Prevent	Do not mention sky	Folder: 1, User: 1
<input type="checkbox"/>	2	Block	Control	All Net Apps	Folder: 0, User: 0
<input type="checkbox"/>	3	Block	Control	All Block	Folder: 1, User: 0
<input type="checkbox"/>	4	Block	Prevent	Encrypted data	Folder: 0, User: 1

Showing 1 to 4 of 4 entries

Buttons: [6] Save, [4] Targets

[3] Policy Name:
 Policy Description:

Targets: 0 folders, 0 users, [Select]

[5] Policy Type: Control Prevent

Net App to Control:

- Agent: [Select]
- Electronic Mail (0/3): Access
- Web Mail (0/13): Access Write File Transfer Big File Attachment
- Instant Messaging (0/6): Access Chat File Transfer
- Remote Access (0/7): Access
- Networking (0/3): Access Include URL Exclude URL
- Social Network Service (0/13): Access Write File Transfer
- File Storage and Sharing (0/19): Access Write File Transfer File Download

• 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.

Navigation: POLICIES > Network > Data Tagging

Buttons: Add New [2], Apply Policy [6]

On	Tag Name	Targets
<input checked="" type="checkbox"/>	Driver License tagging	Folder 0, User 0
<input checked="" type="checkbox"/>	Sky Tagging	Folder 0, User 1

Showing 1 to 2 of 2 entries

• 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.

Buttons: Save [5]

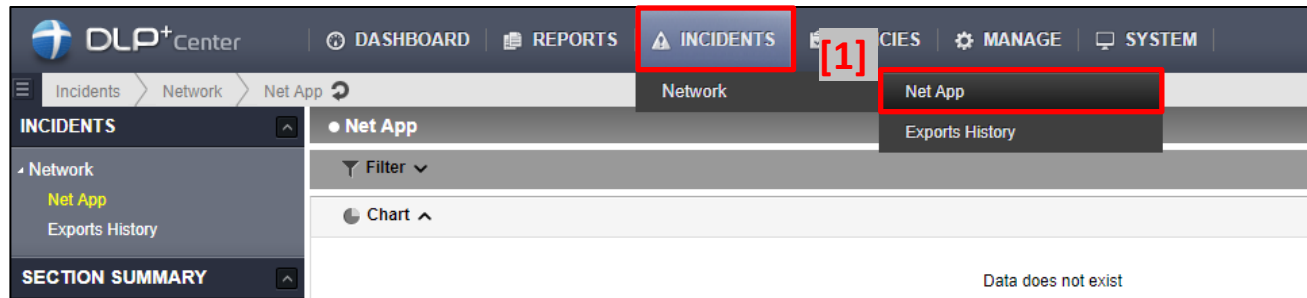
Fields: Tag Name [3], Policy Description [3]

Targets [4]: Folder 0, User 0, Select

Net App to Control:

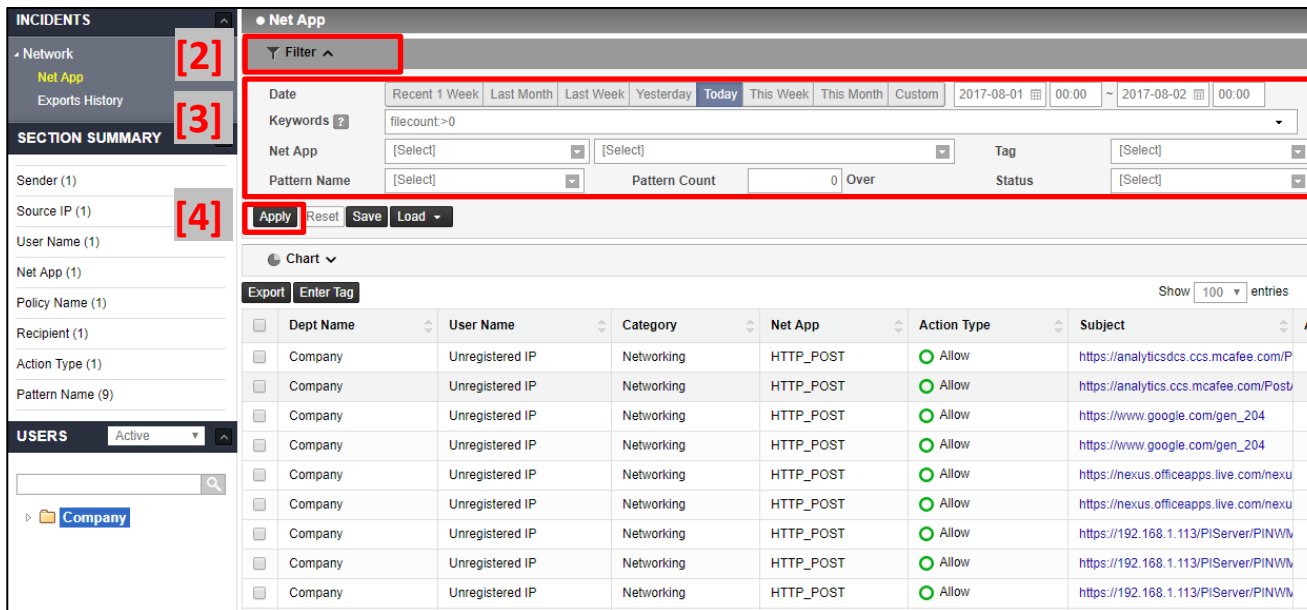
- Agent: [Select]
- Detection Rules: [Select]
- Net App Settings:
 - Electronic Mail (0/2): Body/File Content, Recipient E-mail, Sender E-mail
 - Web Mail (0/12): Body/File Content, Recipient E-mail, Sender E-mail
 - Instant Messaging (0/6): Chat, File Transfer
 - Remote Access (0/1): Body Content

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.

Dept Name	User Name	Category	Net App	Action Type	Subject	Attachment	File
Company	Unregistered IP	Web Mail	Gmail	Block	Blocked by File Prevent	test.txt	1
Company	Unregistered IP	Web Mail	Gmail	Block	Blocked by File Prevent	test.txt	1
Company	Unregistered IP	Web Mail	Gmail	Block	Blocked by File Prevent	test.txt	1
Company	Unregistered IP	Web Mail	Gmail	Block	Blocked by File Prevent	test.txt	1
Company	Unregistered IP	Web Mail	Gmail	Allow	123123	US_Credit_Card_Number.txt e-me	2
Company	Unregistered IP	Web Mail	Gmail	Block	Blocked by File Prevent	test.txt	1
Company	Unregistered IP	Web Mail	Gmail	Block	Blocked by File Prevent	test.txt	1
Company	Unregistered IP	Web Mail	Gmail	Block	sky1	US_Credit_Card_Number.txt	1
Company	Unregistered IP	Web Mail	Gmail	Block	Blocked by File Prevent	test.txt	1
Company	Unregistered IP	Web Mail	Gmail	Allow	mail-i test	e-mail_address.txt US_Credit_Ca	2
none	none	Web Mail	Gmail	Allow	mail-i block test	US_Credit_Card_Number.txt US_	2
none	none	Web Mail	Gmail	Allow	mail-i test	US_Credit_Card_Number.txt	1
none	none	Web Mail	Gmail	Allow	test	US_Credit_Card_Number.txt	1

General

Action Type: ● Allow

User: Company | Unregistered IP (Unregistered IP) | [No Position information]

Occurred Time: 2017-07-27 02:57:17

Source IP: 192.168.1.160

Destination IP: 216.58.195.69

Net App: Web Mail | Gmail

Tag:

Size: 2,612(Bytes)

Policy: more

Body Contents

Subject: mail-i test

Sender: 192.168.1.160

Recipient: sky@somansatech.com

Cc:

BCC:

test

Pattern/File/Content Information Analysis

Name	Pattern	File Size(KB)	Data Analysis
Body	0		Succeeded *
e-mail_address.txt	3	0	Succeeded
US_Credit_Card_Number.txt	204	2	Succeeded
Total	207	2	

Status and History

Status: Opened

Comments:

5. Reports

The screenshot shows the DLP+ Center interface. The top navigation bar includes DASHBOARD, REPORTS (highlighted with a red box and [1]), INCIDENTS, POLICIES, MANAGE, and SYSTEM. Below the navigation bar, the Reports section is active, showing a tree view with Network, Top Users, Top Depts, Trends, Top Net App, and Top Patterns. The Network report is selected, and a dropdown menu (highlighted with a red box and [2]) shows the following options: Top Users, Top Depts, Trends, Top Net App, and Top Patterns. The main content area displays a summary for the Network report, including a Filter dropdown, a table with columns for Pattern, Severity Low, and Severity Medium, and a table with columns for Rank, Dept Name, User Name, Pattern, Transfer, Severity Low, Severity Medium, Severity High, and Severity(%).

• Check Reports

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

The screenshot shows the DLP+ Center interface with the Top Users report selected. A red box highlights the Filter dropdown (labeled [3]). The main content area displays a summary for the Top Users report, including a table with columns for Pattern, Transfer, Severity Low, Severity Medium, Severity High, and Severity(%). Below the summary, a table with columns for Rank, Dept Name, User Name, Pattern, Transfer, Severity Low, Severity Medium, Severity High, and Severity(%) is shown. The table contains three entries:

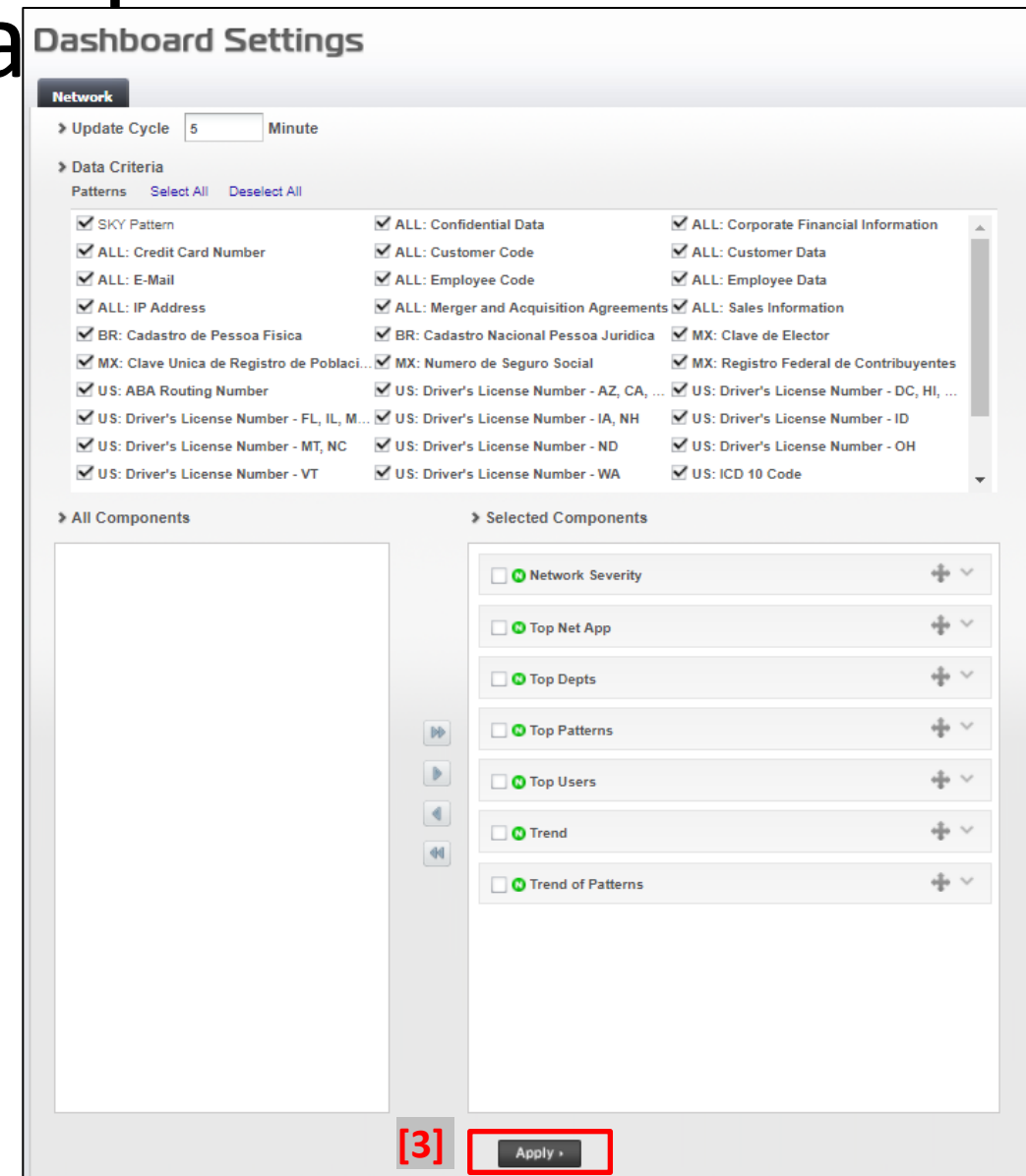
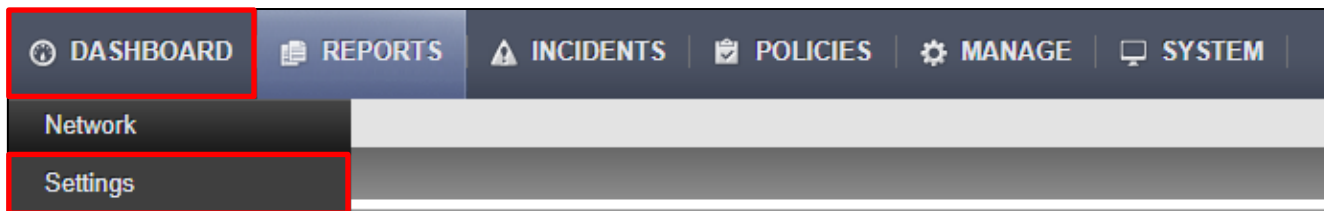
Rank	Dept Name	User Name	Pattern	Transfer	Severity Low	Severity Medium	Severity High	Severity(%)
1	Company	Unregistered IP	74,076	1,024	120	24	59	
2	Somansa	Sky	31,230	1,473	95	20	56	
3	Somansa Test	somansa_grant	844	46	6	3	6	

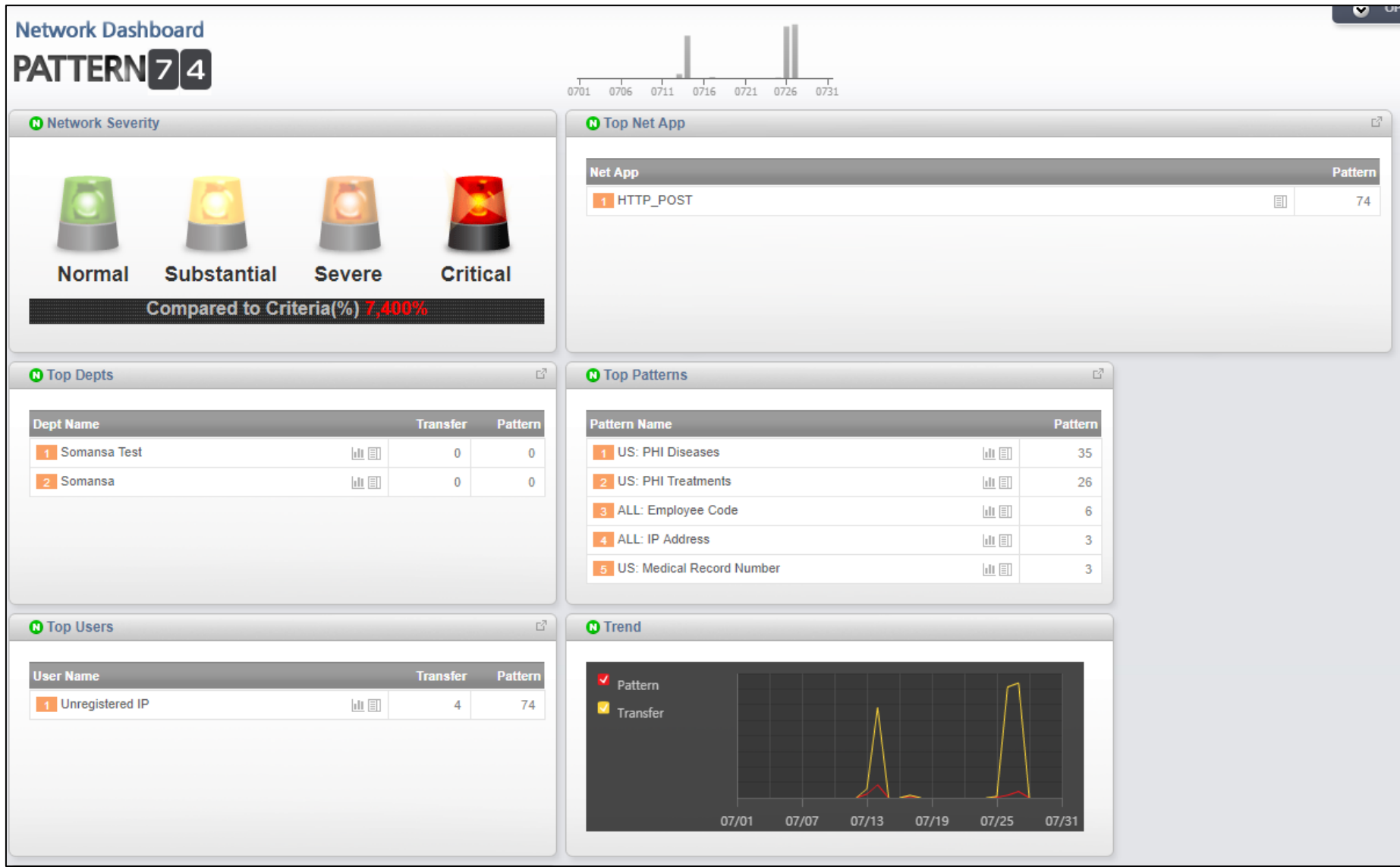
Showing 1 to 3 of 3 entries

6. Dashboard

- 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.