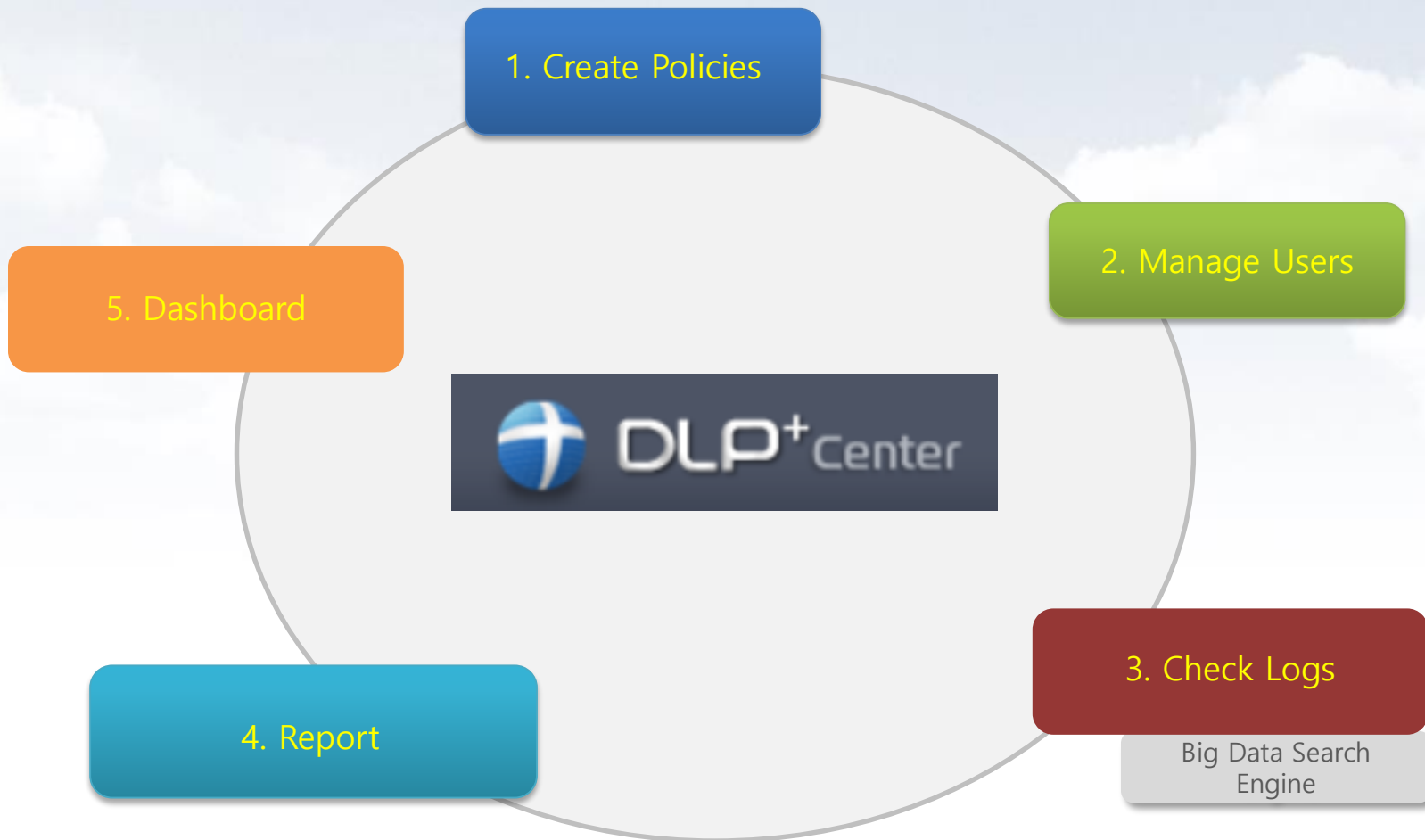




Data Loss Prevention





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 / Privacy-i / DLP+Center



I. DLP+Center Access

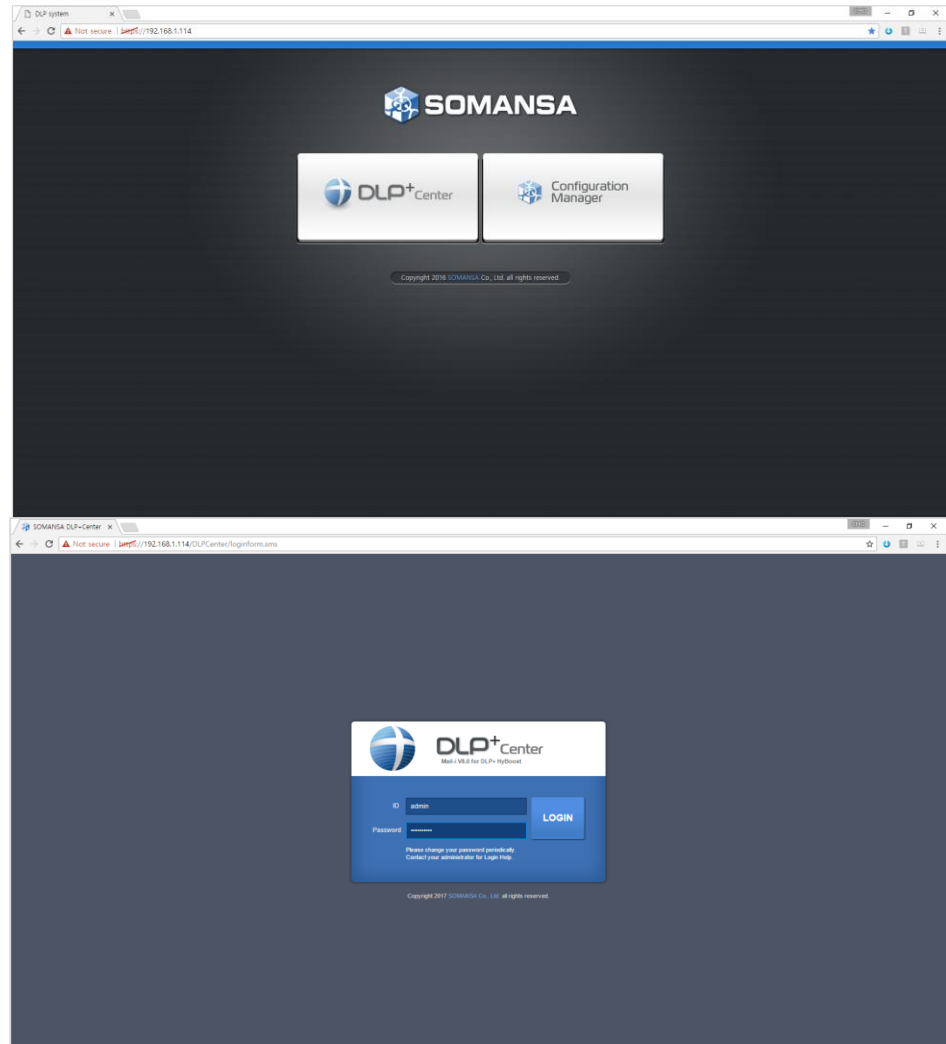
1. Access the DLP+Center

- 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 DLP+Center interface. The top navigation bar includes DASHBOARD, REPORTS, INCIDENTS, POLICIES, MANAGE, and SYSTEM. The left sidebar has a 'Manage' menu with 'Users' selected. The main content area shows the 'Users' management page with a table of users. The 'Manage Dept' button is highlighted with a red box.

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 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 DLP+Center interface. The top navigation bar includes DASHBOARD, REPORTS, INCIDENTS, POLICIES, MANAGE, and SYSTEM. The left sidebar has a 'Manage' menu with 'Users' selected. The main content area shows the 'Users' management page with a table of users. The 'Add New' button is highlighted with a red box.

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

SOMANSA / Privacy-i / DLP+Center



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**

DLP+Center

DASHBOARD REPORTS INCIDENTS POLICIES MANAGE SYSTEM

Manage > Users

MANAGE

Users

Save

General

User Name *

User ID *

Password *

Re-enter Password *

Dept Company Select

Expiration Date Unlimited

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

USERS Active

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

Admin Actions

Alerts/Notifications

Users

Servers

Databases

• Users [Save]

General

User Name *

User ID *

Password *

Re-enter Password *

Dept: Company [Select]

Expiration Date: [] [Unlimited]

Number of Employees: []

Position: []

Role: [] Dept Leader or Admin [] Dept Privacy Officer [] Chief Privacy Officer [] Data Handler

Email: []

Telephone: []

SOMANSA / Privacy-i / DLP+Center



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 is currently 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 is highlighted with a red box and is currently 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

SOMANSA / Privacy-i / DLP+Center



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 'Patterns' configuration page in DLP+Center. The left sidebar is expanded to 'Detect > Patterns'. The main content area has a 'Save' button and a 'Details' section. Under 'Details', 'Pattern Type' is set to 'Regular Expression'. There are input fields for 'Pattern Name' (with a 'Highlight' checkbox) and 'Description'. An 'Expression' field has an 'Add' button. Below these is a 'Severity' scale with three segments: 'Low (0 ~)' in green, 'Mid (~)' in yellow, and 'High (~)' in red. Input boxes are provided for values at 0, 50, and 100.

The screenshot shows the 'Patterns' configuration page in DLP+Center. The left sidebar is expanded to 'Detect > Patterns'. The main content area has a 'Save' button and a 'Details' section. Under 'Details', 'Pattern Type' is set to 'Keyword'. There are input fields for 'Pattern Name' (with a 'Highlight' checkbox) and 'Description'. Under 'Input Method', 'Keyword Input' is selected. Below these is a 'Severity' scale with three segments: 'Low (0 ~)' in green, 'Mid (~)' in yellow, and 'High (~)' in red. Input boxes are provided for values at 0, 50, and 100.



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

The screenshot shows the DLP+Center interface with the 'POLICIES' menu open to 'Detect > Formats'. The 'Add New' button is highlighted with a red box. Below it, a table titled '[Detect File Contents]' is visible, showing a list of file types and their corresponding format names.

File Type	Format Name
	7z
	ALZip
	bzip2
	gzip
	JAR
	LHA
	RAR

The screenshot shows the DLP+Center interface with the 'POLICIES' menu open to 'Detect > Formats'. The 'Save' button is highlighted with a red box. Below it, the 'Details' form is visible, showing fields for 'Format Name', 'File Type' (set to 'Archive'), and 'Extension'.

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**

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

Policies > Detect > Attributes

POLICIES

- Detect
 - Detection Rules
 - Patterns
 - Formats
 - Attributes**
 - USB
 - Applications
 - Time Schedule
- Discover
- Endpoint
- Decide
- Connections

Attributes

Save

Details

- Attribute Name
- File Name (Column): Off
- Path (Table): Off
- File Format: All Formats
- Creation Date: Off
- Last Modification Date: Off
- File Size: Off

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+**.

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

Policies > Detect > Time Schedule

POLICIES

- Detect
 - Detection Rules
 - Patterns
 - Formats
 - Attributes
 - USB
 - Applications
 - Time Schedule**
- Discover

Time Schedule

Add New

- Time Range Name
- All Days
- AM
- Business Hours
- Business Hours including Lunch
- Non-Business Hours
- PM



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.

The screenshot displays the DLP+Center web interface. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', and 'MANAGE'. The breadcrumb trail shows 'Policies > Detect > Detection Rules'. The left sidebar is titled 'POLICIES' and lists categories: 'Detect', 'Discover', 'Endpoint', 'Decide', and 'Connections'. Under 'Detect', 'Detection Rules' is highlighted. 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) and 'Select File Attributes' dropdowns; and 'Advanced' with 'File Format Auto Detection' and 'Compressed File Inspection' dropdowns, both currently set to 'Off'.



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.

The screenshot shows the DLP+Center interface with the 'POLICIES' tab selected. The breadcrumb navigation is 'Policies > Discover > PCs'. The left sidebar shows a tree view with 'POLICIES' expanded, containing 'Detect', 'Discover', 'Endpoint', 'Decide', and 'Connections'. Under 'Discover', 'PCs' is selected. The main content area is titled 'PCs' and has a 'Save' button. It is divided into several sections: 'General' with fields for 'Policy Name' and 'Description'; 'Targets' with icons for folders, users, and files, each with a '0' count and a 'Select' button; 'Data Detection' with a 'Detection Rule' dropdown and a 'Select' button; and 'Advanced' settings. The 'Advanced' section includes: 'Inspection Performance Control' (On), 'Priority' (Normal), 'Average CPU Usage(%)' (100%), 'Idle Time Check Interval' (600 sec), 'Exception Time Range Settings' (Off), 'Notification after Inspection' (Off), and 'Notification Settings' (On). Under 'Notification Settings', there are three notification options: 'Last Inspection Time Notification' (On), 'Scheduled Task Start Notification' (On), and 'Scheduled Task End Notification' (On). At the bottom, there is a 'Schedule' section with an 'Add' button and a table with columns for 'Inspection Type', 'Start Time', and 'Cycle'.



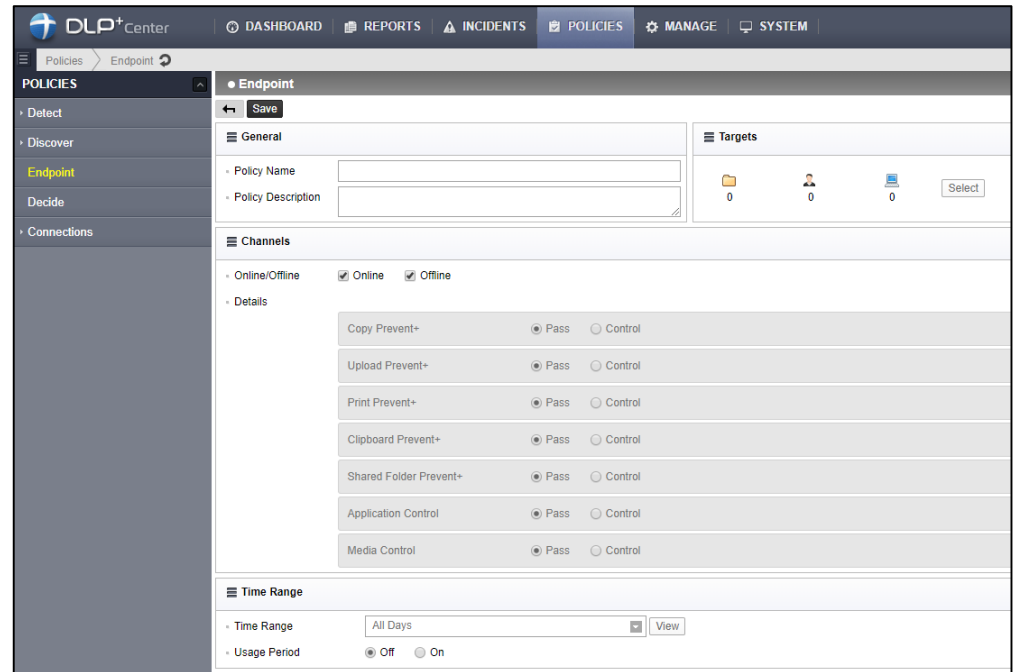
III. POLICIES

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.

The screenshot displays the DLP+Center interface for configuring an Endpoint policy. The navigation menu on the left includes 'Detect', 'Discover', 'Endpoint', 'Decide', and 'Connections'. The main configuration area is titled 'Endpoint' and includes a 'Save' button. The 'General' section contains fields for 'Policy Name' and 'Policy Description'. The 'Channels' section has checkboxes for 'Online' and 'Offline'. The 'Details' section is expanded to show the 'Copy Prevent+' configuration. Under 'Removable Storage to Control', 'All Removable Storages' is selected. 'Data Detection' is set to 'On' with a dropdown menu showing 'somansa_detection'. The 'Action Type' section is divided into 'Inspected Files' and 'Uninspected Files', with options for 'Allow', 'Block', and 'Allow with Approval'. The 'Audit Log' section is set to '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.

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 'POLICIES' menu with options: Detect, Discover, Endpoint (selected), Decide, and Connections. The main content area is titled 'Endpoint' and features a 'Save' button. It is divided into several sections: 'General' with fields for 'Policy Name' and 'Policy Description'; 'Targets' with icons for folders, users, and documents, and a 'Select' button; 'Channels' with 'Online/Offline' status indicators; and 'Details' which is expanded to show configuration for 'Copy Prevent+' and 'Upload Prevent+'. Under 'Upload Prevent+', there is a 'Basic Control Target' list with checkboxes for WebMail, WebBoard, Cloud, Messenger, RFC, and Other HTTP Post (which is highlighted in blue). Below this, there is a checkbox for 'Use the exception processing function for each domain when sending e-mails (Outlook only)'. The 'Data Detection' section has radio buttons for 'Off' (selected) and 'On'. The 'Action' section includes radio buttons for 'Allow', 'Block' (selected), and 'Allow with Approval', as well as 'Audit Log' (Save, Don't Save) and 'File Copy' (Save, Don't Save) options. An 'Advanced' dropdown is visible at the bottom left of the configuration area.



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.

The screenshot displays the DLP+Center interface for configuring an Endpoint policy. The left sidebar shows the 'POLICIES' menu with 'Endpoint' selected. The main content area is titled 'Endpoint' and includes a 'Save' button. The 'General' section has fields for 'Policy Name' and 'Policy Description'. The 'Targets' section shows 0 folders, 0 users, and 0 files. The 'Channels' section has 'Online' and 'Offline' checkboxes. The 'Details' section is expanded to show 'Print Prevent+' settings. Under 'Data Detection', 'Off' is selected. Under 'Action', 'All Files' is selected, and 'Block' is chosen. 'Audit Log' is set to 'Save' and 'File Copy' is set to 'Save'. The 'Advanced' section includes 'Notification' (When Blocked), 'File Size Limit' (500 MB), 'Notification Message' (Off), 'Serial Number' (Don't Display), and 'Watermark' (Off).



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.

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, containing 'Detect', 'Discover', 'Endpoint', 'Decide', and 'Connections'. The main content area is titled 'Endpoint' and features a 'Save' button. It is divided into several sections: 'General' with fields for 'Policy Name' and 'Policy Description'; 'Channels' with 'Online/Offline' checkboxes (both checked) and a 'Details' section; 'Application Settings' with a 'Shortcut' button and a list of applications with checkboxes, including Tor Browser, UltraSurf, Microsoft Word, and various RootKit and Sysinternals tools; 'Data Detection' with a 'Select' button; and 'Action' with a table for 'Inspected Files' and 'Uninspected Files'. The 'Clipboard Prevent+' channel is currently set to 'Control'.



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.

The screenshot displays the DLP+Center web interface for configuring an Endpoint policy. The interface is organized into several sections:

- Navigation:** Includes links for DASHBOARD, REPORTS, INCIDENTS, POLICIES (active), MANAGE, and SYSTEM.
- Left Sidebar:** Lists policy categories: Detect, Discover, Endpoint (highlighted), Decide, and Connections.
- General Section:** Contains fields for Policy Name and Policy Description.
- Targets Section:** Shows counts for folders (0), users (0), and files (0), with a 'Select' button.
- Channels Section:** Includes checkboxes for Online/Offline and a 'Details' section with expandable controls for various actions:
 - Copy Prevent+ (Pass/Control)
 - Upload Prevent+ (Pass/Control)
 - Print Prevent+ (Pass/Control)
 - Clipboard Prevent+ (Pass/Control)
 - Shared Folder Prevent+ (Pass/Control)
- Advanced Section:** Includes:
 - Data Detection (Off/On)
 - Action (All Files) with options: Allow, Block, Allow with Approval, Audit Log (Save/Don't Save), File Copy (Save/Don't Save)
 - Notification (None/Always/When Blocked)
 - File Size Limit (500 MB, Valid Range: 1-2,000)
 - Notification Message (Off/On)
- Bottom Section:** Includes Application Control and Media Control (Pass/Control).



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.

The screenshot displays the DLP+Center web interface for configuring an Endpoint policy. The navigation menu includes Dashboard, Reports, Incidents, Policies, Manage, and System. The current view is 'Policies > Endpoint'. The 'Endpoint' section is active, showing a 'Save' button and a 'General' tab. The 'General' tab contains fields for 'Policy Name' and 'Policy Description'. To the right, there is a 'Targets' section with icons for folders, users, and files, each with a count of 0 and a 'Select' button. Below this is the 'Channels' section, which is expanded to show 'Details'. Under 'Details', there are several rows for different actions: 'Copy Prevent+', 'Upload Prevent+', 'Print Prevent+', 'Clipboard Prevent+', and 'Shared Folder Prevent+', each with radio buttons for 'Pass' and 'Control'. The 'Application Control' row has 'Control' selected. Below the 'Application Control' row is the 'Application Settings' section, which includes a 'Shortcut' button and a list of applications with checkboxes. The list includes: Tor Browser(vidalia.exe), UltraSurf(ultrasurf.exe), MicroSoft WORD(WINWORD.EXE), (RootKit) autoruns(autoruns.exe), (RootKit) gmer(gmer.exe), (RootKit) IceSword(IceSword.EXE), (Sysinternals) procexp(procexp.exe), (Sysinternals) procmon(procmon.exe), (RootKit) Kernel Detective(Kernel Detective.exe), (AnalysisTools) ProcessHacker(ProcessHacker.exe), (Sysinternals) pskill(pskill.exe), (Sysinternals) pslist(pslist.exe), and (RootKit) aswMBR(aswMBR.exe). At the bottom of the 'Application Settings' section, there are 'Select All' and 'Dismiss All' buttons, and an 'Advanced' dropdown menu.



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.

The screenshot displays the DLP+Center interface for configuring an Endpoint policy. The left sidebar shows the 'POLICIES' menu with 'Endpoint' selected. The main area has a 'Save' button and a 'General' section with fields for 'Policy Name' and 'Policy Description'. Below this is the 'Channels' section, which is expanded to show 'Media Control' settings. The 'Media Control' section is set to 'Control' and lists various actions with 'Allow Reading/Writing' and 'Block' options. The 'Targets' section shows counts for folders, users, and files, with a 'Select' button.



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.

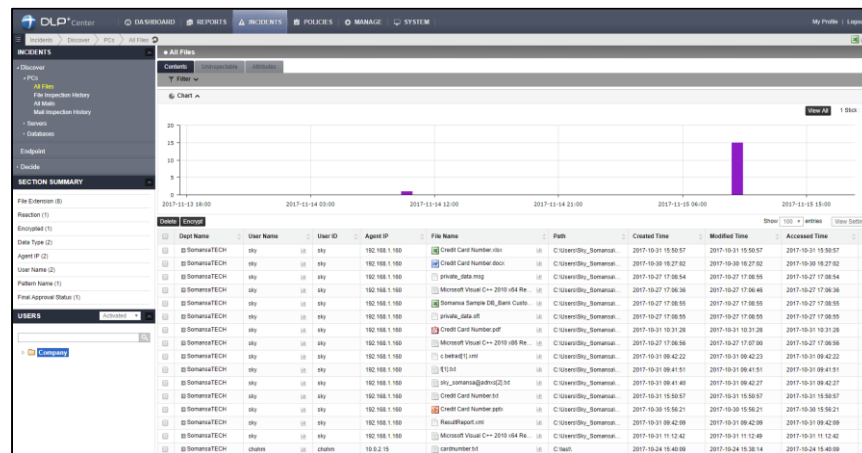
The screenshot displays the DLP+ Center interface for configuring a 'Decide' policy. The top navigation bar includes 'DASHBOARD', 'REPORTS', 'INCIDENTS', 'POLICIES', 'MANAGE', and 'SYSTEM'. The left sidebar shows 'POLICIES' with sub-items: Detect, Discover, Endpoint, Decide (highlighted), and Connections. The main content area is titled 'Decide' and features a 'Save' button. It is divided into several sections: 'General' with fields for 'Policy Name' and 'Policy Description'; 'Threshold' with a 'Use Threshold' dropdown set to 'Off'; 'Endpoint Approver' with a dropdown set to 'On'; and 'Common Approver' with 'Approval Line1' (Dept Leader or Admin, Dept Leader of the target), 'Approval Type' (Pre-Approval), and 'Self-Approval' (Off). A 'Targets' section on the right shows 0 folders and 0 users with a 'Select' button. At the bottom, there is an 'Approver by Request Type' dropdown set to 'Off'.



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**

Log Type: File Inspection History Last Result File Remediation History

File Name:

Path:

File Extension:

Pattern Name:

Final Approval Status:

Encryption:

Created Time:

File Forgery:

File Size(Byte): Over

Patterns Count: Over

Data Type:

Retention Day: Over

Modified Time:

Computer Name:

Apply Reset Save Load

✘ 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**

The screenshot shows the DLP+Center interface with the 'INCIDENTS' menu open and 'All Files' selected. The 'Filter' configuration page is displayed, allowing users to define search criteria for file incidents. The interface includes a sidebar with navigation options like 'Discover', 'PCs', 'All Files', and 'SECTION SUMMARY'. The main area contains a 'Filter' section with various input fields and dropdown menus for selecting conditions and keywords. Buttons for 'Apply', 'Reset', 'Save', and 'Load' are visible at the bottom of the filter configuration area.

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

Dept Name	User Name	User ID	Agent IP	File Name	Path	Created Time	Modified Time	Accessed Time	Retention Day
SomansaTECH	sky	sky	192.168.1.100	Credit Card Number.xlsx	C:\Users\Sky_Somansa\...	2017-10-31 15:50:57	2017-10-31 15:50:57	2017-10-31 15:50:57	0

Agent Information		File Information		Pattern Information	
User ID	sky	File Name	Credit Card Number.xlsx	ALL Credit Card Number	100
Dept	SomansaTECH	Original Format	Not Applicable		
Computer Name	Sky_Somansa-PC	Path	C:\Users\Sky_Somansa\Desktop\2017_...		
Agent IP	192.168.1.100	File Size	10 KB		
		Created Time	2017-10-31 15:50:57		
		Modified Time	2017-10-31 15:50:57		
		Accessed Time	2017-10-31 15:50:57		
		Reached Time			
		Identical File	File / User		

Inspection Information	
Policy Name	Discover credit card number
First Inspection Date	2017-11-15 10:08:23
Inspection Start Time	2017-11-15 10:08:05
Inspection End Time	2017-11-15 10:08:28
Submitted Time	2017-11-15 10:08:28

6. Section Summary

- Quickly search for top 10 Incidents

- 1) Select **INCIDENTS**
- 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 'INCIDENTS' section with a sidebar on the left containing navigation options like 'Discover', 'PCs', 'Servers', and 'Databases'. The main area is titled 'All Files' and has tabs for 'Contents', 'Uninspectable', and 'Attributes'. A 'Filter' section is visible with various search criteria like 'Log Type', 'File Name', 'Path', 'Expiration Date', 'Reaction', 'First Inspection Date', 'Accessed Time', and 'Policy Name'. Below the filter is a 'Chart' section showing a bar chart for '[Pattern Name] Top10' with a value of 16 and 100%.



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**

The screenshot shows the 'Details' page for a task in the DLP+Center. The task name is 'PC Tasks(2017-11-21 18:18:00)'. The task type is 'Encryption'. The user consent is set to 'Running without user consent'. The schedule is set to 'Run Immediately' with a valid date of '2017-12-21 00:00'. The 'Targets' section shows 0 folders, 0 users, and 1 file selected.

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**

The screenshot shows the 'Details' page for a task in the DLP+Center. The task name is 'PC Tasks(2017-11-21 18:20:05)'. The task type is 'Deletion'. The user consent is set to 'Running without user consent'. The schedule is set to 'Run Immediately' with a valid date of '2017-12-21 00:00'. The 'Targets' section shows 0 folders, 0 users, and 1 file selected.



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

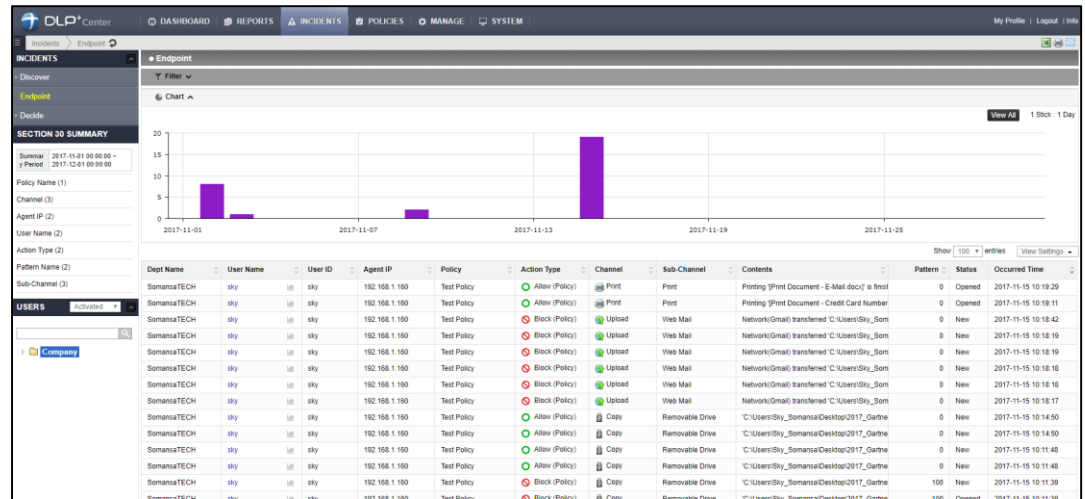
- 1) Select **INCIDENTS**
- 2) Click **View Settings**
- 3) Only check the column to show
- 4) Change the order you want and click **Save**



IV. INCIDENTS

11. Export the Endpoint Log

- 1) Select **INCIDENTS > Endpoint**



SOMANSA / Mail-i / DLP+Center



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

The screenshot shows the 'Top Users' report in the DLP Center interface. The left sidebar contains a navigation tree with 'Discover' selected. The main area displays a table with columns for 'Patterns' and 'File'. The 'Patterns' table has columns: Total, Encrypted, Unencrypted, Encrypted(%). The 'File' table has columns: Total, Encrypted, Unencrypted, Encrypted(%), Severity(%). The data shows 1,182 total patterns, 0 encrypted, and 16 unencrypted (0% encrypted). There are 16 total files, 0 encrypted, and 15 unencrypted (0% encrypted). A 'Filter' button is visible at the top right of the table area.

The screenshot shows the 'Top Agent' report in the DLP Center interface. The left sidebar contains a navigation tree with 'Discover' selected. The main area displays a table with columns for 'Patterns' and 'File'. Above the table, there are filter options: 'Summary Date' (Yesterday, Custom, 2017-11-21), 'Patterns Name' (Select), 'Expiration Status' (Select), 'Sort By' (Pattern Count, File Count), and 'Inspection Type' (All, Mail). There are also input fields for 'Encrypted(%)' and 'Over'. The data shows 1,182 total patterns, 0 encrypted, and 16 unencrypted (0% encrypted). There are 16 total files, 0 encrypted, and 15 unencrypted (0% encrypted). A 'Filter' button is visible at the top right of the table area.



V. REPORTS

3. Export the Report (format .csv, 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**

The screenshot shows the DLP+Center interface with the 'REPORTS' tab selected. The 'Top Agent' report is chosen, and the 'Filter' button is highlighted with a red box. The interface displays a summary table and a detailed data table.

Pattern		File		Severity(%)				
Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)	Severity(%)
1,183	0	16	0%	16	0	16	0%	<div style="width: 100%; height: 10px; background-color: green;"></div>

Rank	Dept Name	User Name	User ID	Agent IP	Computer Name	Pattern				File				Severity(%)	Last Inspected Time
						Total	Encrypted	Unencrypted	Encrypted(%)	Total	Encrypted	Unencrypted	Encrypted(%)	Severity(%)	
1	SomansaTECH	sky	sky	192.168.1.150	Sky_Somansa-PC	1,154	0	1,154	0%	15	0	15	0%	<div style="width: 100%; height: 10px; background-color: green;"></div>	2017-11-15 10:08:17
2	SomansaTECH	chohm	chohm	10.0.2.15	chohm-PC	19	0	19	0%	1	0	1	0%	<div style="width: 100%; height: 10px; background-color: green;"></div>	2017-11-14 10:10:22

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	<div style="width: 100%; height: 10px; background-color: green;"></div>

Rank	Dept Name	User Name	Pattern	Transfer	Severity Low	Severity Medium	Severity High	Severity(%)
1	Company	Unregistered IP	1,090	162	51	8	5	<div style="width: 100%; height: 10px; background-color: green;"></div>
2	SomansaTECH	Emma	351	46	14	4	1	<div style="width: 100%; height: 10px; background-color: green;"></div>



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 shows the DLP+Center web interface. The top navigation bar includes: DASHBOARD, REPORTS, INCIDENTS, POLICIES, MANAGE, and SYSTEM. The left sidebar has a 'MANAGE' section with 'Alerts/Notifications' and 'Reports' (highlighted in yellow) under it. The main content area is titled 'Reports' and features a 'Filter' dropdown and an 'Add New' button. Below this is a table with two columns: 'Report Name' and 'Report Type'. One entry is visible: '(Weekly) Top User Report' with a 'Report Type' of 'Network > Top Users'. At the bottom of the table, it says 'Showing 1 to 1 of 1 entries'.



VII. Dashboard

1. Settings

- Sets the patterns and components to activate on the dashboard

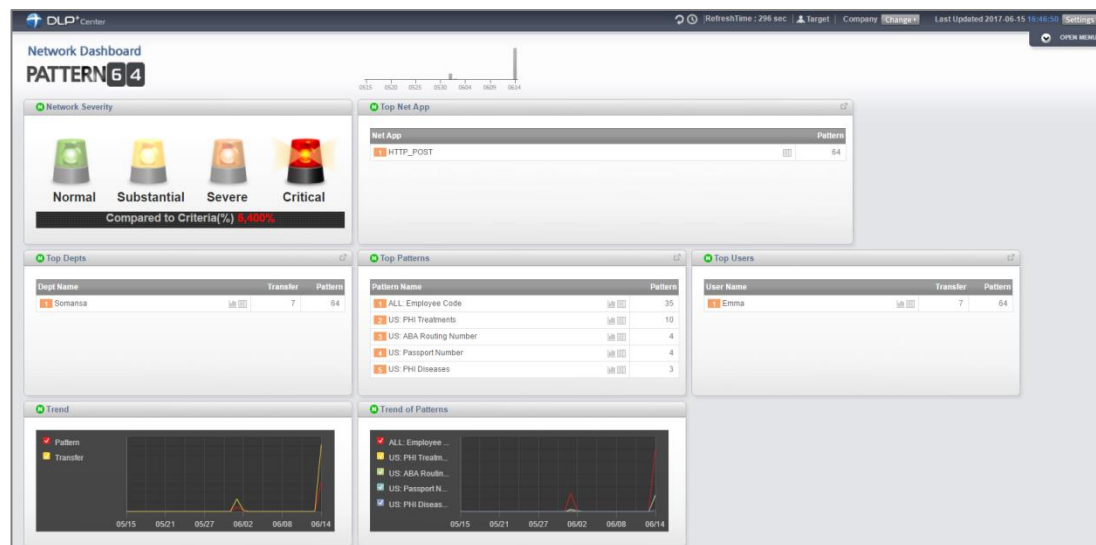
- 1) Select **Dashboard > Settings**
- 2) Enter the Update Cycle, select the Patterns and Components
- 3) Components can be reordered using the cross-shaped buttons and detailed settings can be made by clicking the down arrow
- 4) Click **Apply**

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 shows the DLP+Center interface with the following settings:

SYSTEM	
Logs	
Admins	
Settings	
General	

General	
Save	
Display Parameter	
List Output Number	100
Filter Area Settings	Close
Authentication	
Duplicate Login	Allow
Password Input Time Limit	3 (Valid Range : 1 ~ 99)
Password Minimum Length	9 (Valid Range : 9 ~ 99)
Password Expiration Policy	Off
Admin password reset	Off
First-Login Policy	Off
Language	
Default Language	English



SOMANSA

www.somansatech.com